UDV DATAPK Industrial Kit

Руководство по внедрению и поддержке

Версия 3.0

udv.group

support@udv.group

Содержание

1. Изменения в Руководстве по внедрению и поддержке

В таблице ниже приведена история изменений документа «Руководство по внедрению и поддержке» для UDV DATAPK Industrial Kit.

ДАТА ИЗМЕНЕНИЯ	СОДЕРЖАНИЕ ИЗМЕНЕНИЙ
12.09.2025	Первоначальная версия

2. Системные требования

В таблицах ниже приведены минимальные и рекомендуемые системные требования, которые необходимо учитывать при проектировании систем обеспечения кибербезопасности с использованием со всеми установленными модулями. Системные требования приведены для всех уровней (компонентов) :

- Sensor (сенсор)
- Management
- Supervision

Требования для компонентов Management сгруппированы по количеству подключенных сенсоров и объему входящего трафика; для компонентов Supervision — по количеству подключенных компонентов Management.

> Прим.:
>
> Системные требования актуальны при развертывании в том числе в средах виртуализации.
>
> Дополнительные условия поддержки каждого компонента указаны для рекомендуемых системных требований этого компонента.

Требования компонента Sensor

> Внимание:
>
> Данные системные требования не учитывают дополнительный объем дискового пространства для хранения файлов `PCAP` сетевого трафика и файлов, извлеченных из сетевого трафика модулем «Анализ промышленного сетевого трафика». Необходимый дополнительный объем рассчитывается индивидуально для каждой инфраструктуры.

Табл. 1. Системные требования для установки и работы UDV DATAPK Industrial Kit уровня Sensor

ХАРАКТЕРИСТИКА	СЕНСОР	
	МИНИМАЛЬНЫЕ	РЕКОМЕНДУЕМЫЕ
Процессор	14 потоков, 3100 МГц	18 потоков, 3100 МГц
ОЗУ	32 ГБ, DDR4 (2933 МГц)	32 ГБ, DDR4 (2933 МГц)
Диск	SSD 512 ГБ	SSD 1 ТБ
Материнская плата	Поддержка UEFI	
Операционная система	«Альт СП» Сервер 10.2	

Табл. 1. Системные требования для установки и работы UDV DATAPK Industrial Kit уровня Sensor

ХАРАКТЕРИСТИКА	СЕНСОР	
	МИНИМАЛЬНЫЕ	РЕКОМЕНДУЕМЫЕ
	Прим.: ОС не входит в комплект поставки UDV DATAPK и приобретается отдельно.	
Ширина канала между сенсором и коммутатором	1 Гбит/с	1 Гбит/с

Дополнительные условия поддержки каждого компонента Sensor:

УСЛОВИЕ ПОДДЕРЖКИ	ЗНАЧЕНИЕ
Пропускная способность для обработки сетевого трафика модулем «Анализ промышленного сетевого трафика»	1 Гбит/сек для одного сенсора на аппаратной платформе Axiomtek eBOX671-521-FL-DC-6GbE с процессором Intel Core i7-8700
Максимальное число активов, с которых возможно завершить активный сбор данных 1 раз в 240 минут с помощью модуля «Управление конфигурациями».	100 активов

Требования компонента Management

Внимание:

Данные системные требования не учитывают дополнительный объем дискового пространства под репозитории для хранения проектов ПЛК модулем «Управление проектами ПЛК». Необходимый дополнительный объем рассчитывается индивидуально для каждой инфраструктуры.

Табл. 3. Системные требования для установки и работы UDV DATAPK уровня Management

ХАРАКТЕРИСТИКА	1 СЕНСОР, 1 ГБИТ/С		5 СЕНСОРОВ, 5 ГБИТ/С		10 СЕНСОРОВ, 10 ГБИТ/С		15 СЕНСОРОВ, 15 ГБИТ/С	
	МИНИ-МАЛЬНЫЕ	РЕКОМЕН-ДУЕМЫЕ	МИНИ-МАЛЬНЫЕ	РЕКОМЕН-ДУЕМЫЕ	МИНИ-МАЛЬНЫЕ	РЕКОМЕН-ДУЕМЫЕ	МИНИ-МАЛЬНЫЕ	РЕКОМЕН-ДУЕМЫЕ
Процессор	12 потоков, 2400 МГц	12 потоков, 3100 МГц или 16 потоков, 2400 МГц	16 потоков, 2400 МГц	16 потоков, 3100 МГц или 18 потоков, 2400 МГц	20 потоков, 2400 МГц	24 потока, 3100 МГц	24 потока, 2400 МГц	28 потоков, 3100 МГц
ОЗУ	32 ГБ, DDR4 (2933 МГц)	32 ГБ, DDR4 (2933 МГц)	32 ГБ, DDR4 (2933 МГц)	32 ГБ, DDR4 (2933 МГц)	32 ГБ, DDR4 (2933 МГц)	32 ГБ, DDR4 (2933 МГц)	32 ГБ, DDR4 (2933 МГц)	32 ГБ, DDR4 (2933 МГц)
Диск	SSD 1,5 ТБ	SSD 3 ТБ	SSD 2 ТБ	SSD 4 ТБ	SSD 2 ТБ	SSD 4 ТБ	SSD 2 ТБ	SSD 4 ТБ
	Прим.: Рекомендуется аппаратный RAID.							
Материнская плата	Поддержка UEFI							
Операционная система	«Альт СП» Сервер 10.2							
	Прим.: ОС не входит в комплект поставки UDV DATAPK и приобретается отдельно.							

Табл. 3. Системные требования для установки и работы UDV DATAPK уровня Management

ХАРАКТЕРИСТИКА	1 СЕНСОР, 1 ГБИТ/С		5 СЕНСОРОВ, 5 ГБИТ/С		10 СЕНСОРОВ, 10 ГБИТ/С		15 СЕНСОРОВ, 15 ГБИТ/С	
	МИНИ-МАЛЬНЫЕ	РЕКОМЕН-ДУЕМЫЕ	МИНИ-МАЛЬНЫЕ	РЕКОМЕН-ДУЕМЫЕ	МИНИ-МАЛЬНЫЕ	РЕКОМЕН-ДУЕМЫЕ	МИНИ-МАЛЬНЫЕ	РЕКОМЕН-ДУЕМЫЕ
Ширина канала между компонентом Management и сенсором с модулем «Управление внешними событиями» (EEM) и без него	• 20 Мбит/с с EEM • 2 Мбит/с без EEM	• 40 Мбит/с с EEM • 4 Мбит/с без EEM	• 30 Мбит/с с EEM • 15 Мбит/с без EEM	• 50 Мбит/с с EEM • 30 Мбит/с без EEM	• 40 Мбит/с с EEM • 20 Мбит/с без EEM	• 70 Мбит/с с EEM • 40 Мбит/с без EEM	• 70 Мбит/с с EEM • 45 Мбит/с без EEM	• 100+ Мбит/с с EEM • 70+ Мбит/с без EEM

Дополнительные условия поддержки каждого компонента Management:

УСЛОВИЕ ПОДДЕРЖКИ	ЗНАЧЕНИЕ
Максимальное число подключаемых сенсоров	15 сенсоров
Максимальное активов для их корректного отображения в веб-интерфейсе компонента Management	10.000 активов
Максимальное число задач сбора данных для их корректного отображения в веб-интерфейсе компонента Management с установленным модулем «Управление конфигурациями»	200-500 задач
Максимальное число активов, которые можно назначить на 1 задачу сбора данных с 60 сканерами, чтобы завершить активный сбор данных с этих активов по расписанию 1 раз в 240 минут с помощью модуля «Управление конфигурациями». Прим.: Скорость активного сбора данных в первую очередь зависит от скорости обработки запроса на стороне актива, поэтому для каждой инфраструктуры необходим индивидуальный расчет количества активов или сканеров. В типовом ограничении выше использовалась средняя скорость обработки одного запроса на активе, равная 4,25 сек.	100 активов
Максимальное число входящих внешних событий, которое способен обработать установленный модуль «Управление внешними событиями»	3000 событий/сек

Требования компонента Supervision

Внимание:

Данные системные требования не учитывают дополнительный объем дискового пространства под репозитории для хранения проектов ПЛК модулем «Управление проектами ПЛК». Необходимый дополнительный объем рассчитывается индивидуально для каждой инфраструктуры.

Табл. 4. Системные требования для установки и работы UDV DATAPK уровня Supervision

ХАРАКТЕРИСТИКА	1 МЕНЕДЖМЕНТ		20 МЕНЕДЖМЕНТОВ	
	МИНИМАЛЬНЫЕ	РЕКОМЕНДУЕМЫЕ	МИНИМАЛЬНЫЕ	РЕКОМЕНДУЕМЫЕ
Процессор	6 потоков 2400 МГц	8 потоков, 3100 МГц	16 потоков, 2400 МГц	20 потоков, 3100 МГц
ОЗУ	32 ГБ, DDR4 (2933 МГц)	32 ГБ, DDR4 (2933 МГц)	32 ГБ, DDR4 (2933 МГц)	32 ГБ, DDR4 (2933 МГц)
Диск[1]	SSD 192 ГБ		SSD 432 ГБ	
	Прим.: Рекомендуется аппаратный RAID.			
Материнская плата	Поддержка UEFI			
Операционная система	«Альт СП» Сервер 10.2 Прим.: ОС не входит в комплект поставки UDV DATAPK и приобретается отдельно.			
Ширина канала между всеми компонентами Management и компонентом Supervision	15 Мбит/с	100 Мбит/с	100 Мбит/с	250 Мбит/с

1. В случае использования модуля «Управление проектами ПЛК» за каждый подключенный компонент Management добавляется 320 ГБ

Дополнительные условия поддержки каждого компонента Supervision:

УСЛОВИЕ ПОДДЕРЖКИ	ЗНАЧЕНИЕ
Максимальное число подключаемых компонентов Management	20 компонентов Management

Требования к клиентским обозревателям

Для работы с веб-интерфейсом UDV DATAPK рабочие станции должны быть подключены к подсети управляющего контура UDV DATAPK и поддерживать один из браузеров:

- браузеры семейства Chromium (Google Chrome, Microsoft Edge, Яндекс.Браузер) версии 124 и выше;
- Mozilla Firefox версии 125 и выше.

Не поддерживаются следующие версии браузеров:

- браузеры семейства Chromium (Google Chrome, Microsoft Edge, Яндекс.Браузер) версии 123 и ниже;
- Mozilla Firefox версии 124 и ниже.

Требования к разрешению экрана

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

Масштабирование веб-интерфейса UDV DATAPK не поддерживается.

См. также

Список модулей UDV DATAPK Industrial Kit

3. Установка и настройка

В этом разделе:

> Прим.:
>
> В этом разделе приведена настройка и установка компонентов Management и Sensor. Установка и настройка компонента Supervision приведена в отдельном Руководстве по внедрению и поддержке.

3.1. Установка и настройка на базе ОС Альт Сервер

> Внимание:
>
> При возникновении затруднений в процессе установки обратитесь в техническую поддержку.

В этом разделе:

Перед установкой Комплекса ознакомьтесь с системными требованиями к аппаратным платформам (серверам) для разных уровней Комплекса в разделе «Системные требования».

Порядок включения аппаратной платформы (сервера) Комплекса для выполнения установки:

1. Соедините сетевым кабелем разъем управляющего контура сервера с разъемом сетевой карты рабочей станции администратора.
2. Один конец кабеля питания вставьте в разъем питания сервера, другой – в заземленную сетевую розетку.
3. Включите сервер. Для этого кратковременно нажмите кнопку питания. Комплекс издаст одиночный звуковой сигнал, запустится операционная система.

3.1.1. Файлы, необходимые для установки

1. Актуальный сертифицированный дистрибутив ОС Альт Сервер 10.2 SP.

   > Внимание:
   >
   > В данном Руководстве по внедрению и поддержке описана установка ОС Альт Сервер 10.2 SP с использованием дистрибутива `alt-sp-server-20241127-x86_64.iso`.

2. Архив с репозиторием сертифицированных модулей UDV DATAPK `release-[версия_Комплекса]_[дата_архива].tar.gz`.
3. Архив с репозиторием дополнительных несертифицированных модулей UDV DATAPK `release-[версия_Комплекса]-external-modules_[дата_архива].tar.gz`.

> Прим.:
>
> Информация о назначении остальных файлов в составе дистрибутива UDV DATAPK, в том числе его пакетов экспертиз, приведена в разделе «Назначение файлов дистрибутива Комплекса».

3.1.2. Установка и настройка сертифицированной ОС Альт Сервер 10.2 SP

Для установки и настройки сертифицированной ОС Альт Сервер 10.2 SP выполните следующие инструкции:

1. Установка сертифицированной ОС Альт Сервер 10.2 SP
2. Настройка сертифицированной ОС Альт Сервер 10.2 SP

Если Комплекс уровня Management и уровня Sensor будут устанавливаться на разные серверы, выполните инструкции выше для каждого сервера.

Инструкции в текущем разделе предназначены для настройки ОС перед установкой следующих модулей и сервисов Комплекса:

- базовый модуль (Core)
- модуль «Анализ промышленного сетевого трафика»
- модуль «Управление проектами ПЛК»
- модуль «Управление конфигурациями»
- модуль «Управление уязвимостями»
- модуль «Управление внешними событиями»
- сервис «Swagger UI»
- сервис «Supervision Backend»

Настройки перед установкой модуля UDV DATAPK EDR for PLC приведены в следующем разделе «Установка модуля «EDR for PLC»».

3.1.2.1. Установка сертифицированной ОС Альт Сервер 10.2 SP

Для установки ОС Альт Сервер 10.2 SP:

1. Подключите ISO-образ или оптический диск актуальной сертифицированной ОС Альт Сервер к серверу, на котором будет установлен Комплекс.

   > Внимание:
   >
   > В данном Руководстве по внедрению и поддержке описана установка ОС Альт Сервер 10.2 SP с использованием дистрибутива `alt-sp-server-20241127-x86_64.iso`.

   ▸ **Результат шага:** окно установки откроется автоматически или по нажатию любой клавиши.
2. Выберите пункт меню **Rescue LiveCD** и нажмите клавишу **Enter**.

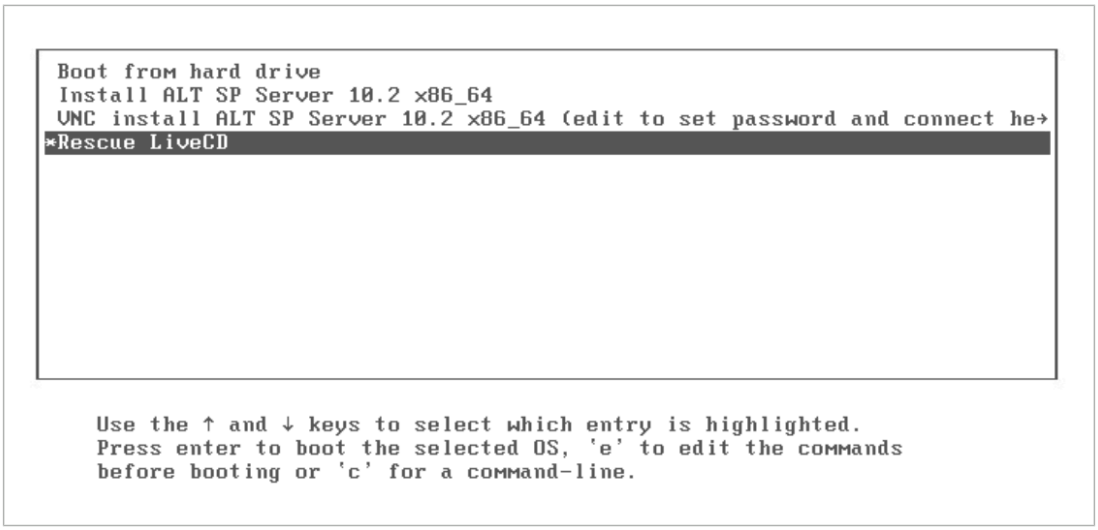


Рис. 1. Загрузка платформы в режиме Rescue LiveCD

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

3. Для подготовки к разметке дискового пространства:

   a. Зафиксируйте наименование диска, для которого будет выполняться разметка дискового пространства:

```
fdisk -lu
```

Пример

Результат команды:

```
Disk /dev/sda: 120 GiB, 128849018880 bytes, 251658240 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
```

где `/dev/sda` — наименование диска.

Внимание:

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

Для проверки разметки диска выполните следующие действия:

- Отобразите все существующие группы томов, выполнив команду:

```
vgscan
```

Прим.:

Если вывод команды пустой — значит, диск не был ранее размечен, и можно сразу перейти к шагу 3.b.

- Удалите все существующие группы томов, выполнив команду для каждой группы `[название_группы_томов]`:

```
vgremove [название_группы_томов]
```

б. Создайте переменную `D` и присвойте ей наименование диска из предыдущего шага:

```
D=[наименование_диска]
```

Пример

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

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

в. Последовательно введите следующие команды для создания дисковых разделов:

```
wipefs -af $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
```

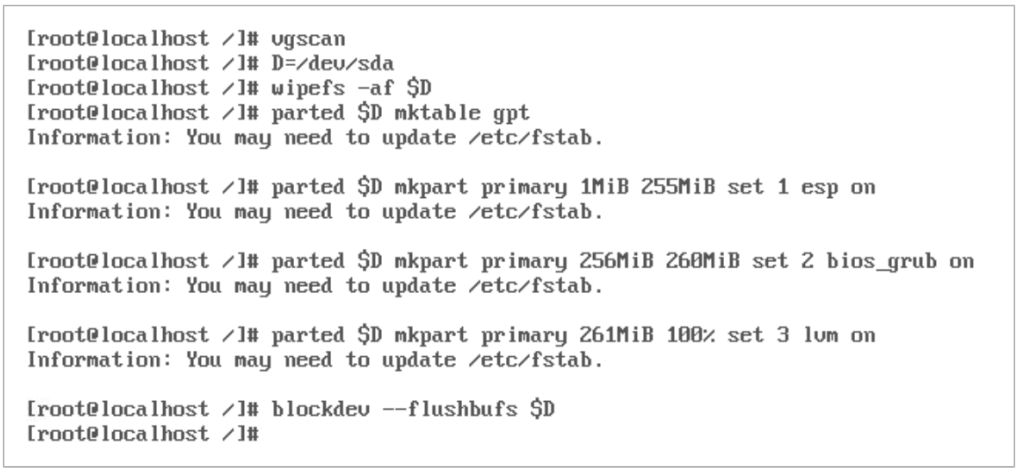


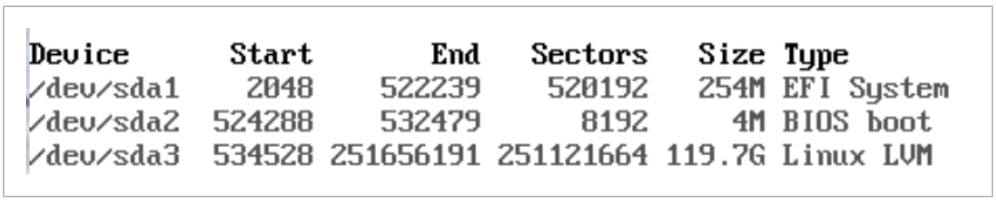
Рис. 3. Команды для создания дисковых разделов

г. Просмотрите наименования созданных разделов диска:

```
fdisk -lu
```

Пример

Результат команды:



где `sda1`, `sda2`, `sda3` — наименования созданных разделов диска `/dev/sda`.

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

```
V=${D}[номер_раздела]
```

Пример

Создание переменной `V` с номером подраздела `3`:

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

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

```
pvcreate $V
vgcreate udv $V
blockdev --flushbufs $D
reboot
```

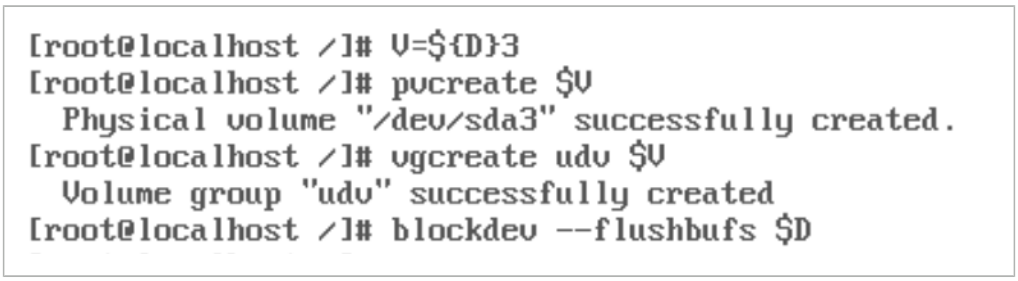


Рис. 5. Команды для настройки физических разделов диска

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

4. После перезагрузки выберите пункт меню **Install ALT SP Server 10.2 x86_64** и нажмите клавишу **Enter**.

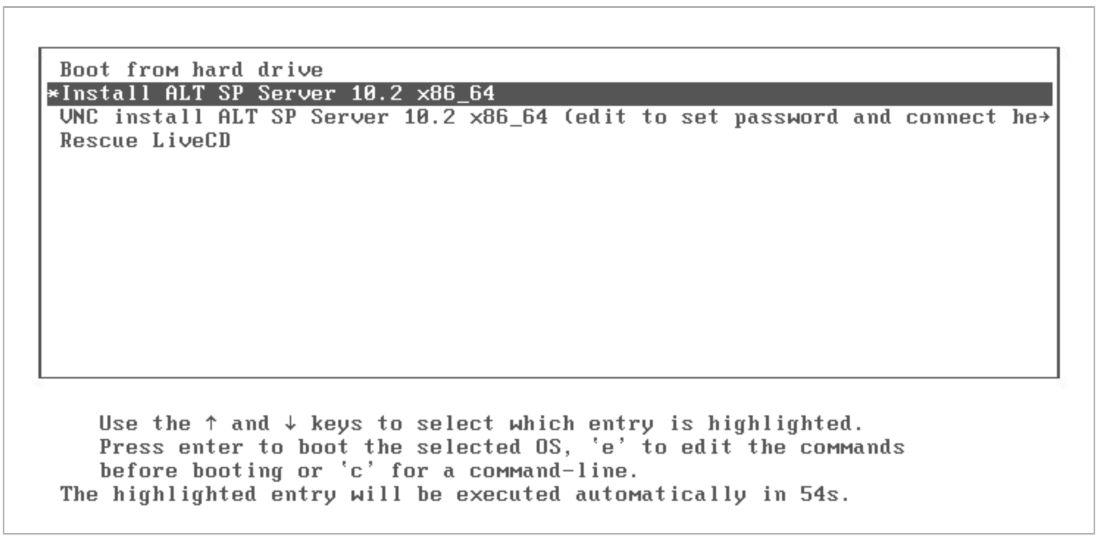


Рис. 7. Окно установки ОС Альт Сервер

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

5. Если после выбора пункта меню **Install ALT SP Server 10.2 x86_64** отображается пустой экран и установка не начинается, необходимо отключить загрузку видеодрайверов. Для этого:

а. Выберите пункт меню **Install ALT SP Server 10.2 x86_64** и нажмите клавишу **E**.

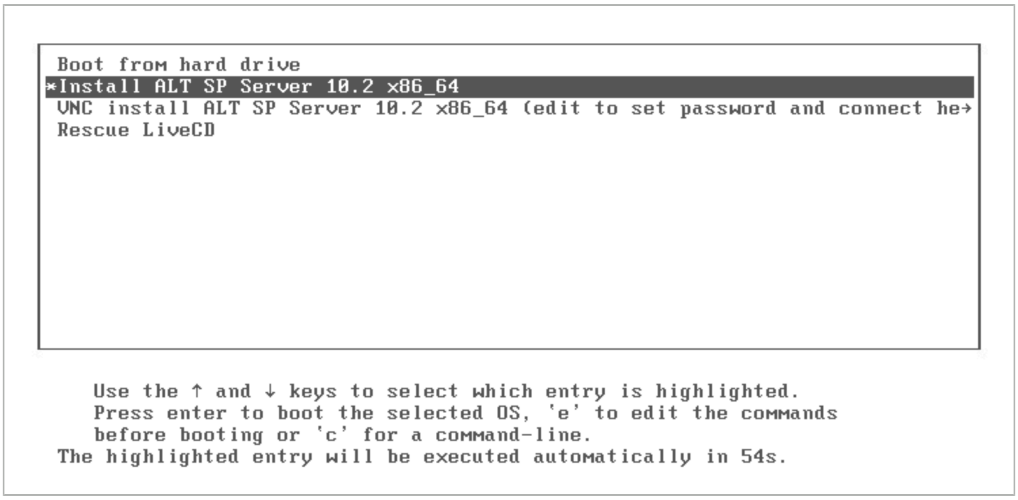


Рис. 9. Экран выбора действия после монтирования образа ОС Альт Сервер

б. Добавьте параметр `nomodeset` между параметрами `ramdisk_size` и `lang`, как указано на рисунке ниже.

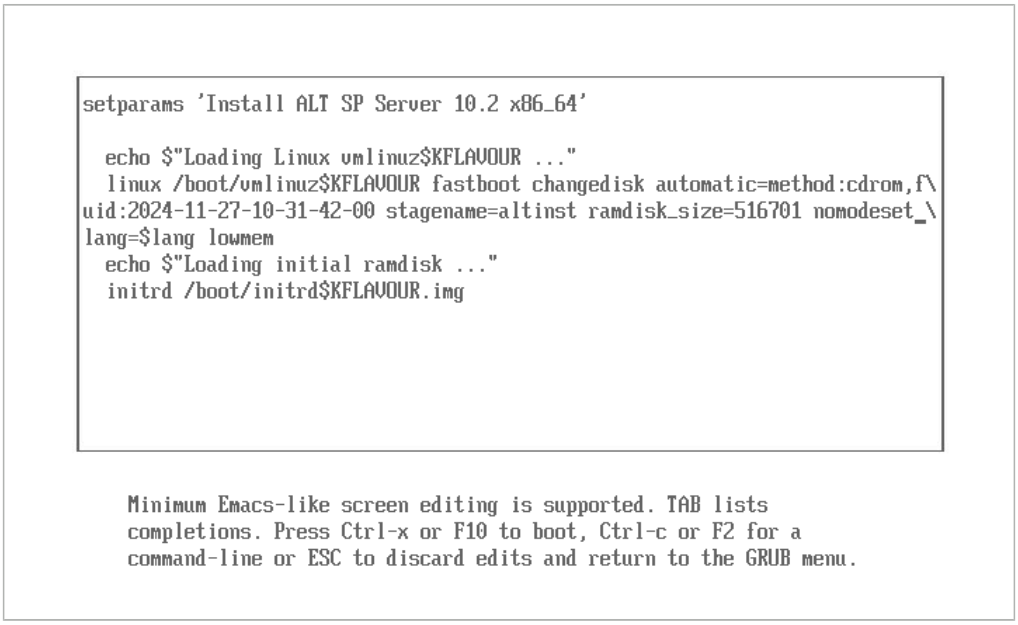


Рис. 11. Добавление параметра «nomodeset»

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**.

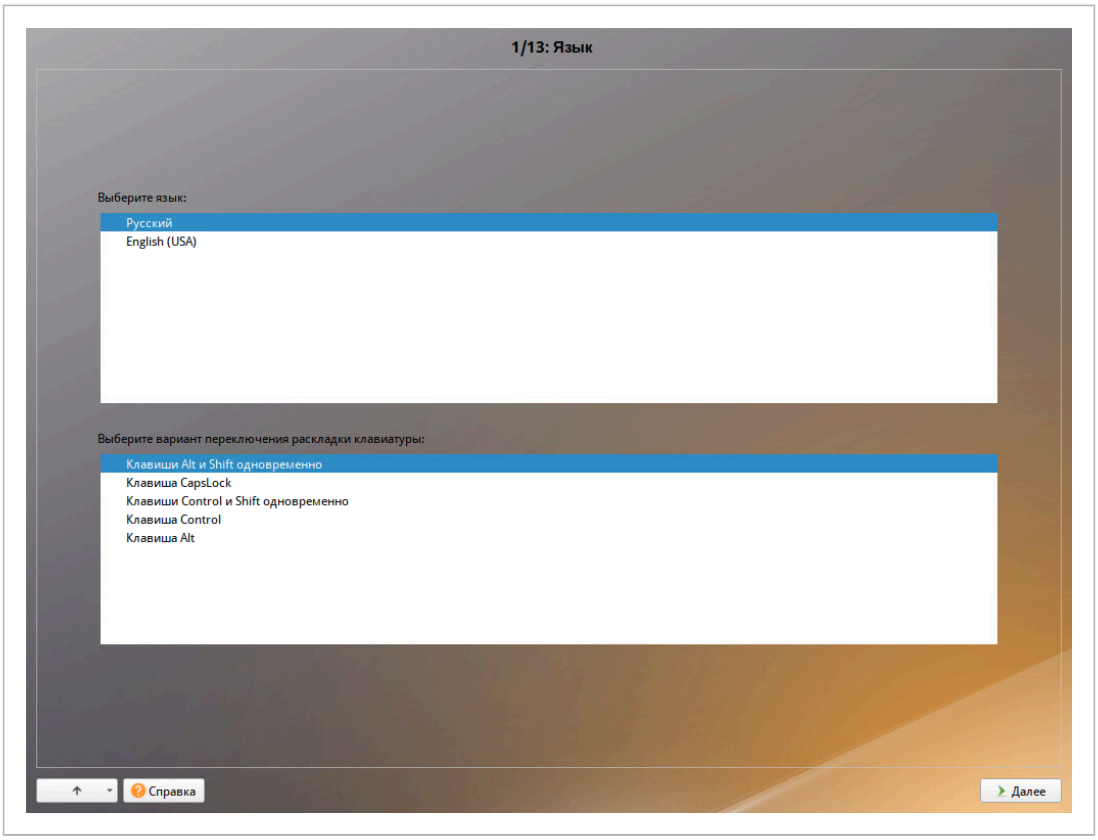


Рис. 12. Окно настройки языка и раскладки клавиатуры ОС Альт Сервер

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

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

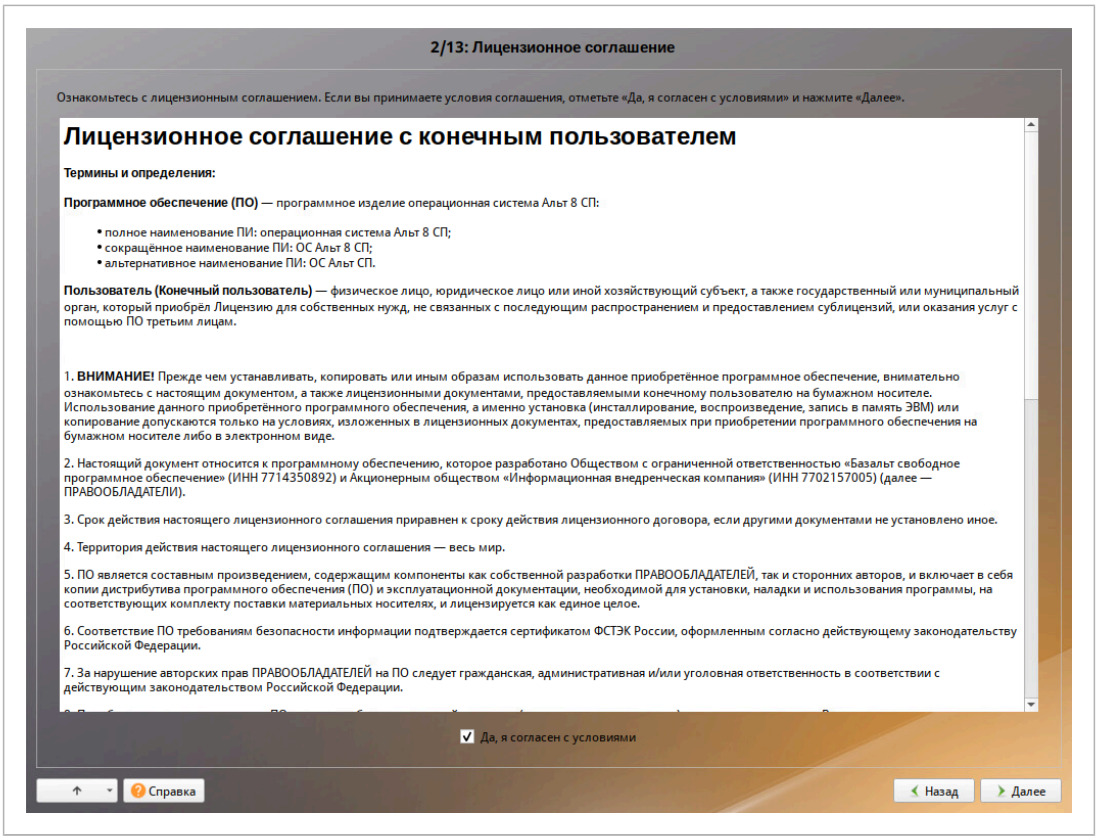


Рис. 13. Окно лицензионного соглашения установки ОС Альт Сервер

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

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

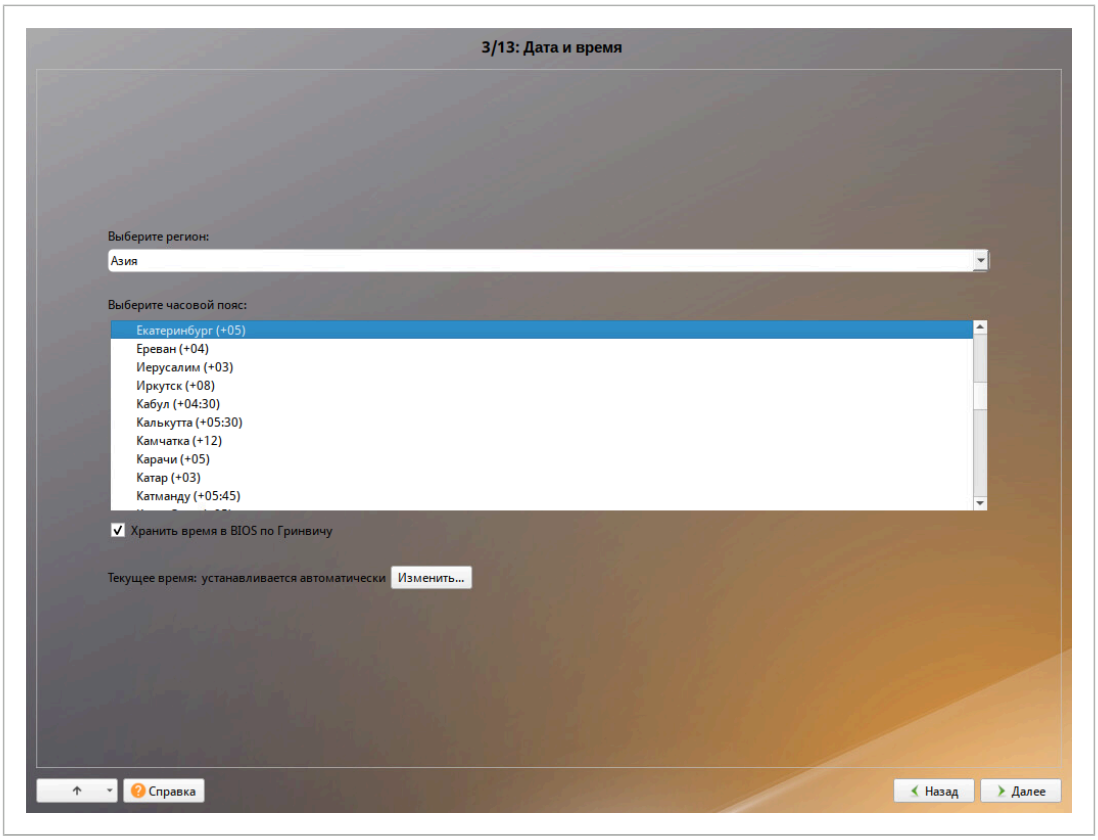


Рис. 14. Окно «Дата и время»

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

9. Выполните разметку дискового пространства. Для этого:

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

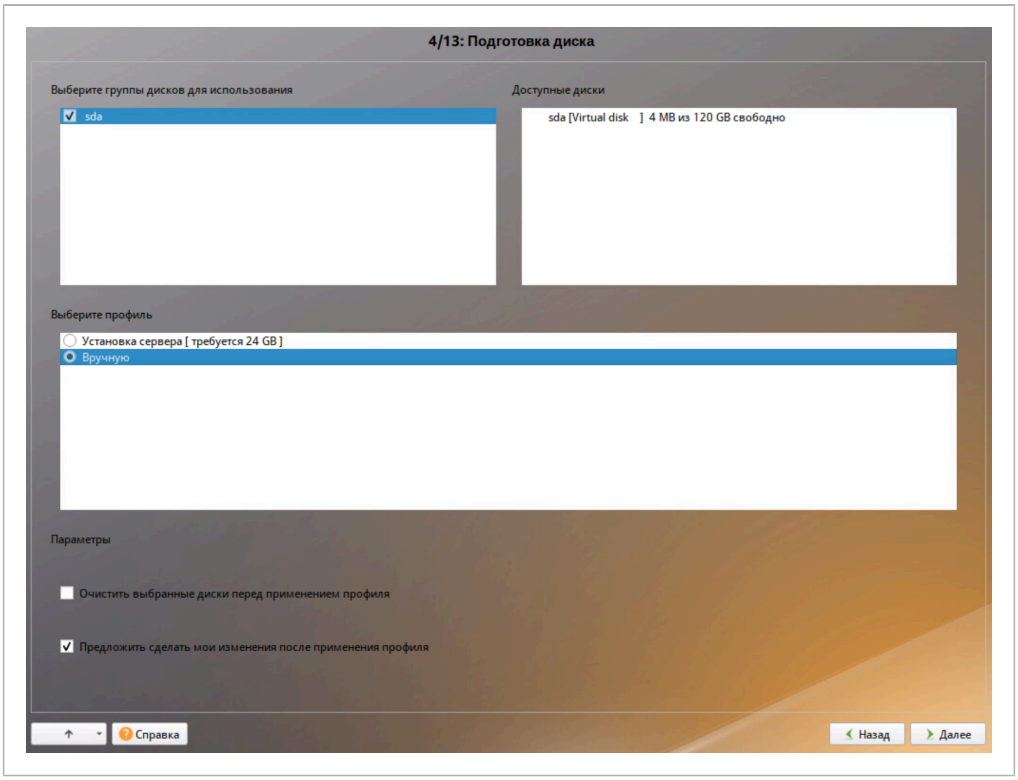


Рис. 15. Окно «Подготовка диска»

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

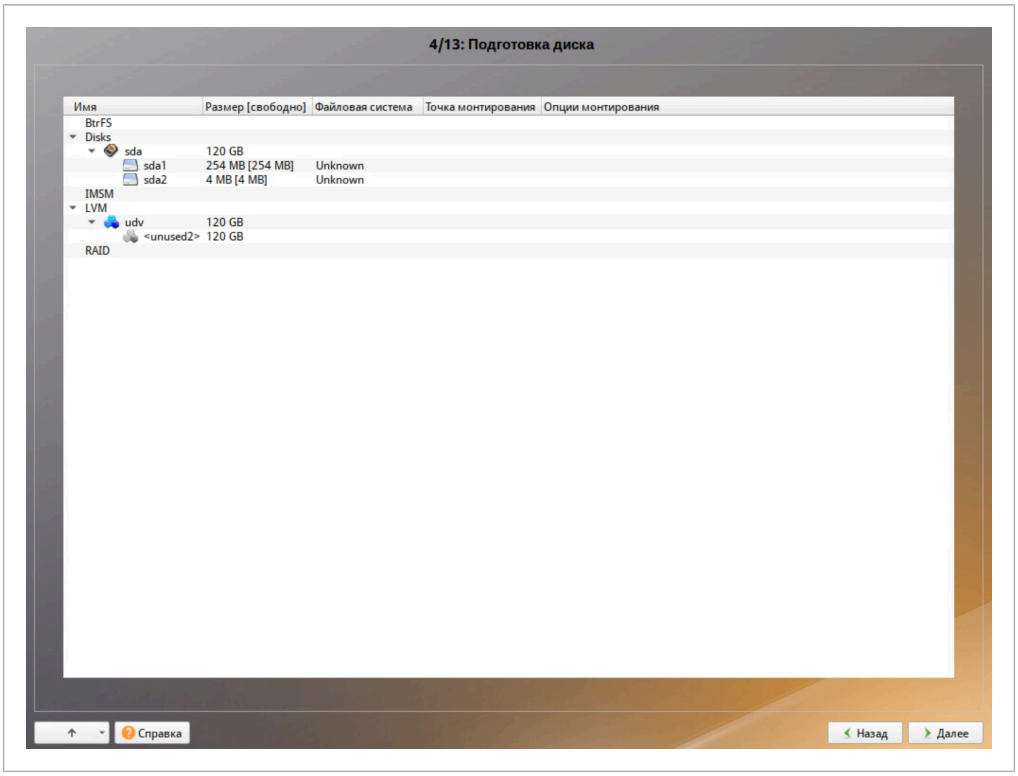


Рис. 16. Окно «Подготовка диска» после выбора ручной разметки дисков

б. В раскрывающемся списке **Disks** выберите настроенный ранее раздел диска (например, `sda1` или `nvme0n1p1`) и нажмите **Создать файловую систему**.

Прим.:

При отсутствии кнопки **Создать файловую систему** нажмите **Удалить файловую систему**, затем повторно нажмите **Создать файловую систему**.

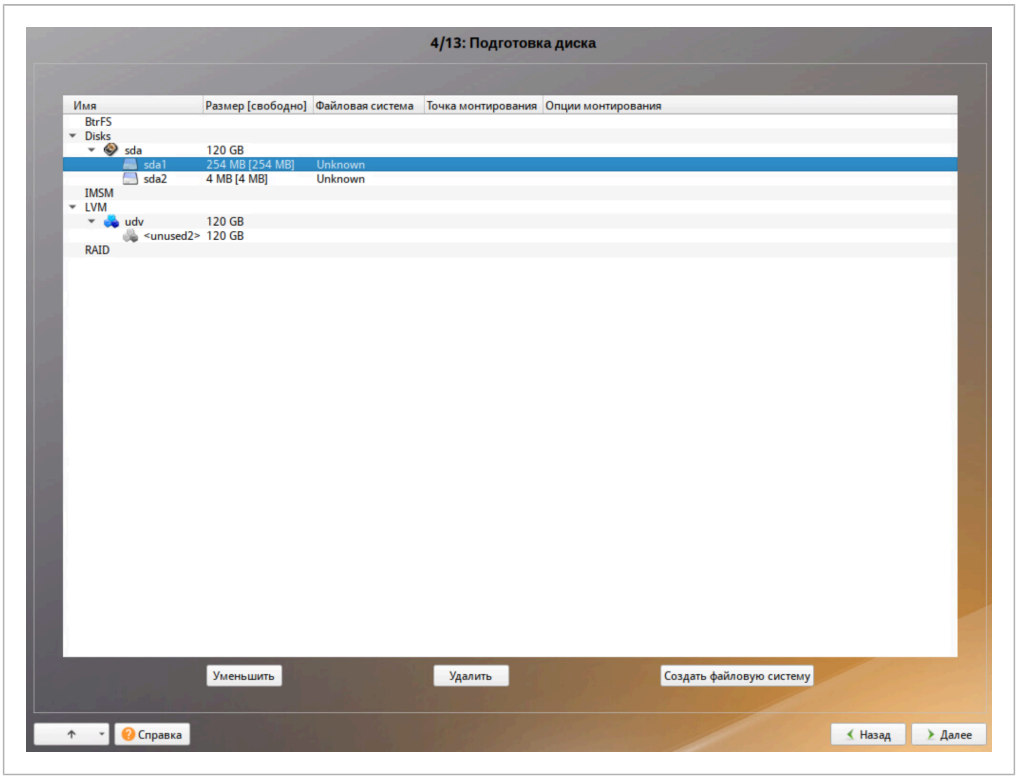


Рис. 17. Окно «Подготовка диска» (выбор диска sda1)

в. В новом окне **Создать файловую систему** выберите **Файловая система FAT32** и нажмите **ОК**.

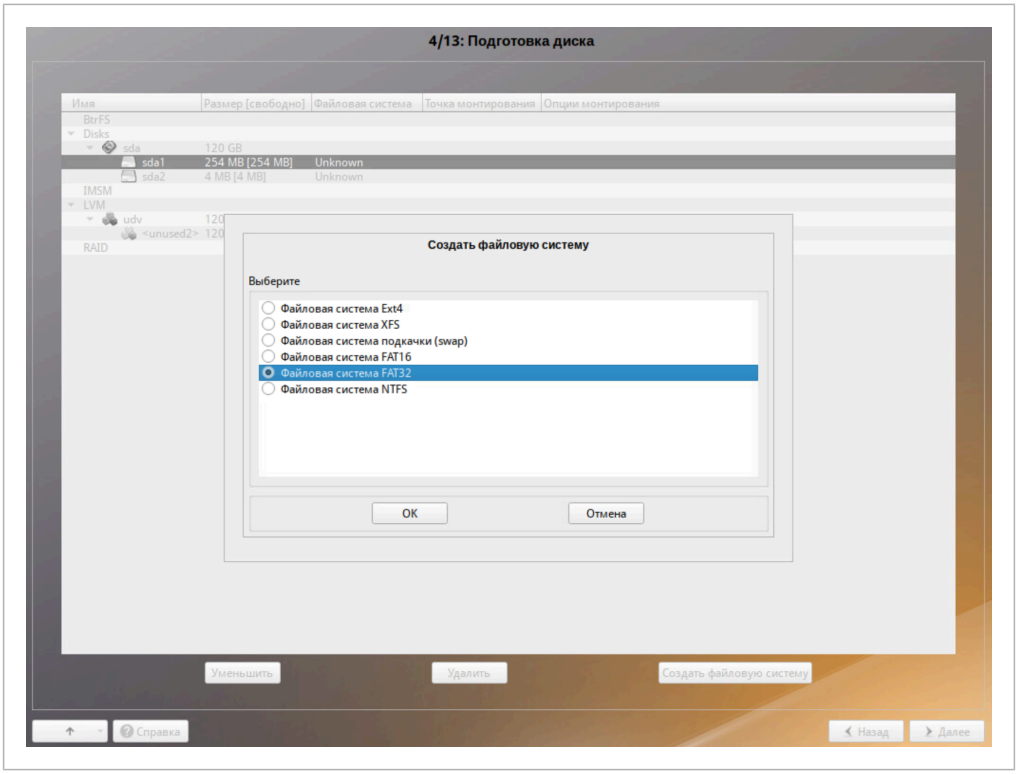


Рис. 18. Окно «Создать файловую систему» (выбор файловой системы FAT32)

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

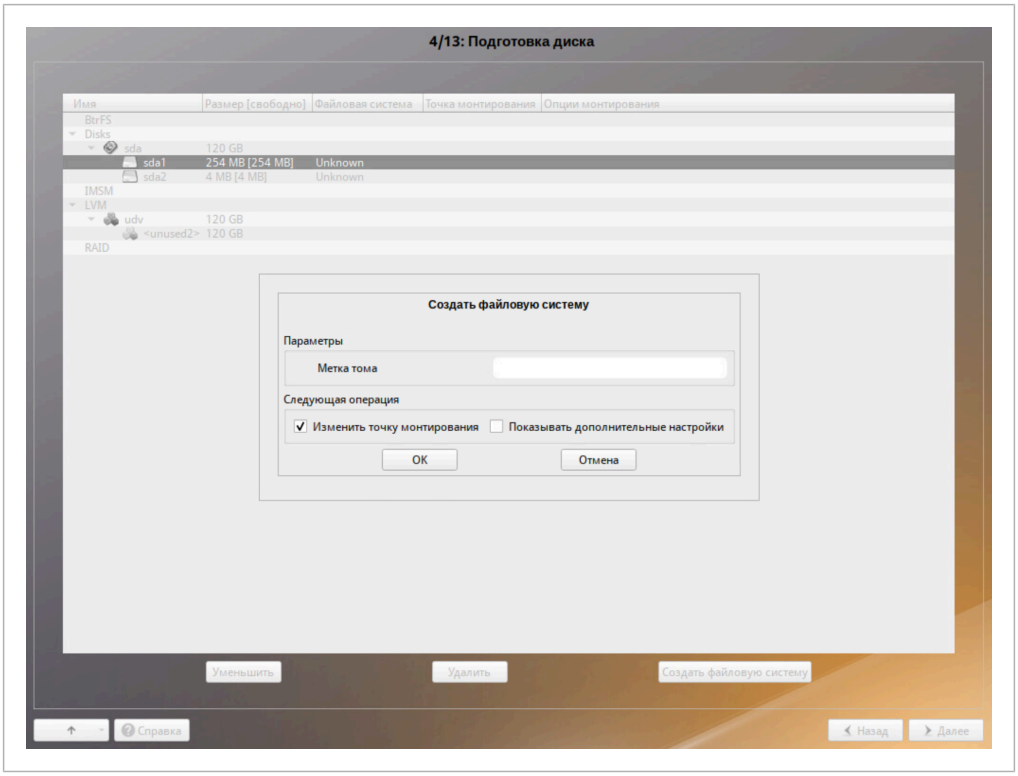


Рис. 19. Окно «Создать файловую систему» (настройка метки тома)

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

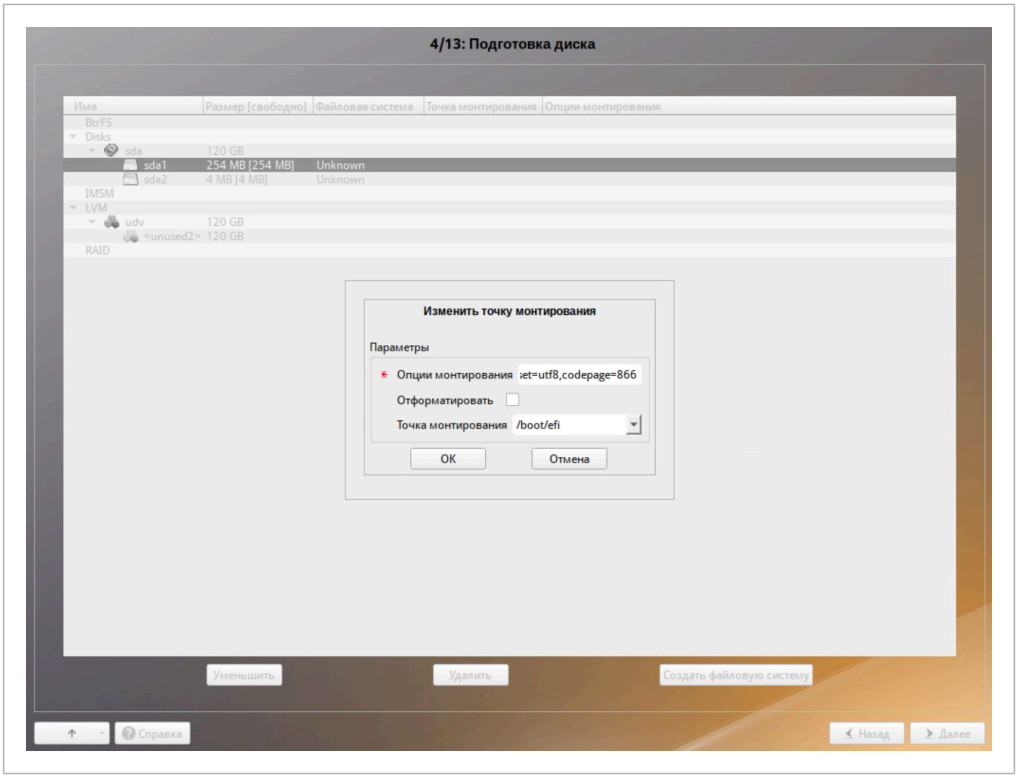


Рис. 20. Окно «Создать файловую систему» (настройка точки монтирования)

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

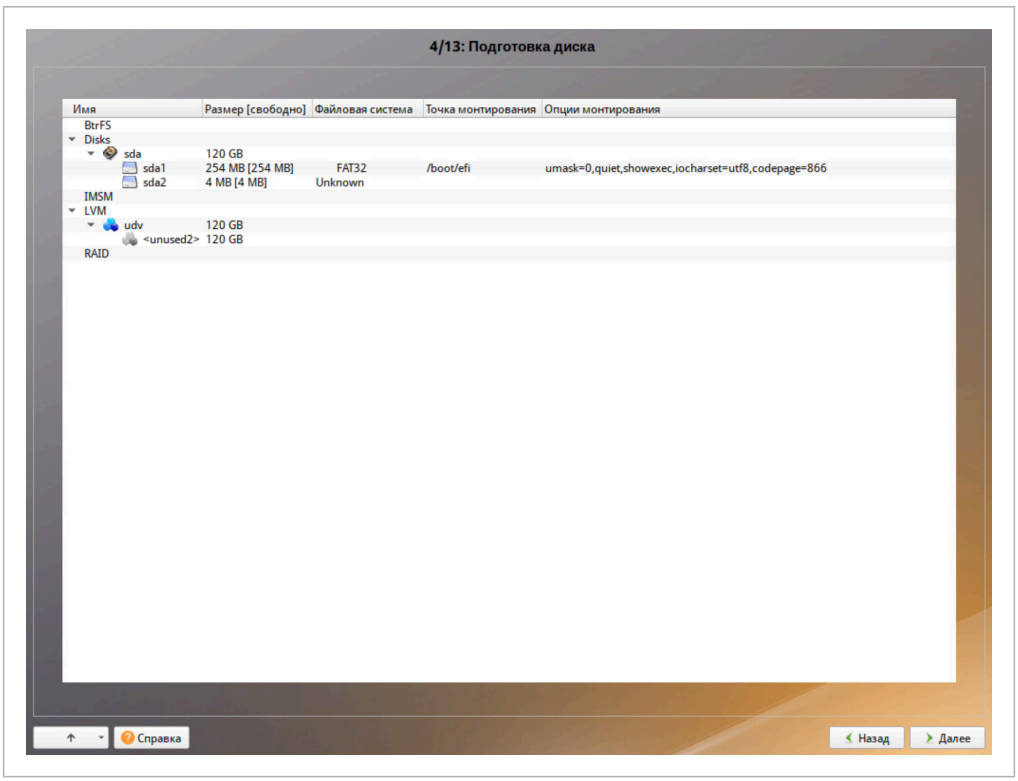


Рис. 21. Окно «Подготовка диска» (результат форматирования раздела на примере sda1)

e. Создайте первый том `rootfs` для корневого раздела. Для этого в раскрывающемся списке **LVM** выберите `<unused2>` и нажмите **Создать том**.

> **Прим.:**
>
> При отсутствии кнопки **Создать том** нажмите **Удалить том**, затем повторно нажмите **Создать том**.

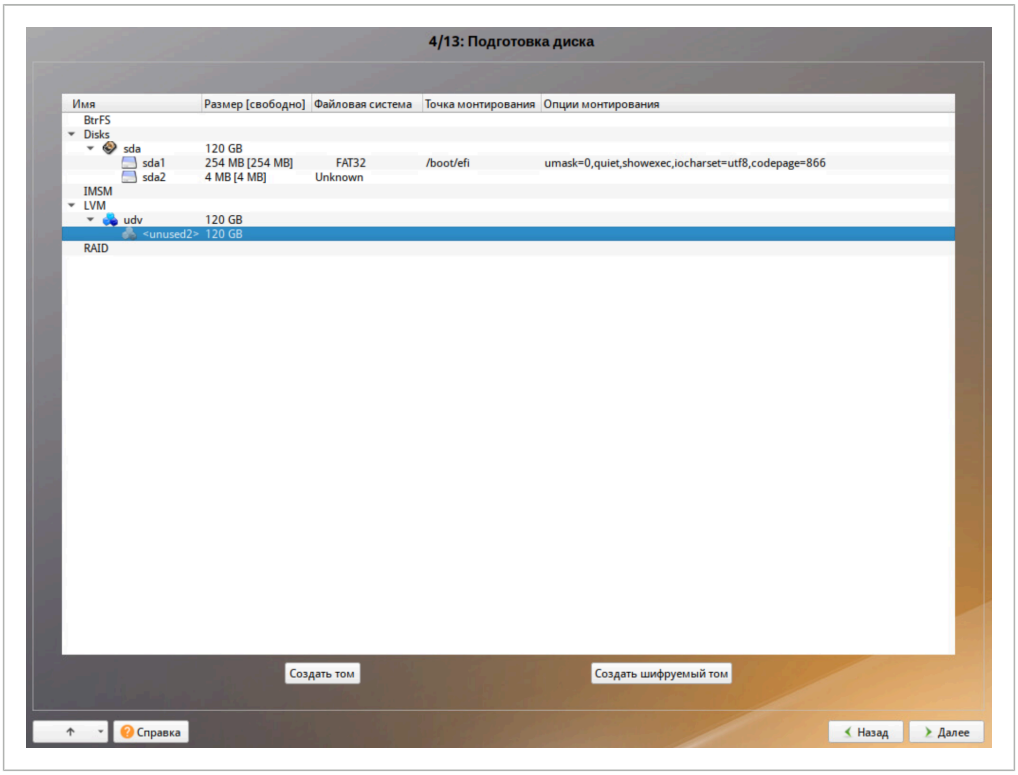


Рис. 22. Окно «Подготовка диска» (создание первого тома)

ж. В открывшемся окне **Создать том** выполните следующие действия:

- Введите имя тома: `rootfs`.
- Выберите размер тома. Рекомендуемый размер тома — 75 ГБ (для этого укажите `75000` MB). Если в дальнейшем планируется устанавливать модуль Комплекса UDV DATAPK EDR for PLC, укажите размер тома `200000` MB (200 ГБ).

> **Внимание:**
>
> На этапе установки ОС Альт Сервер необходимо создавать разделы объемом не более 400 ГБ, если на этом же этапе разметку дискового пространства планируется выполнять в файловой системе xfs. При необходимости после установки ОС объем тома или раздела можно увеличить. Подробнее об этом см. в разделе «Настройка сертифицированной ОС Альт Сервер 10 SP»

- Нажмите **ОК**.

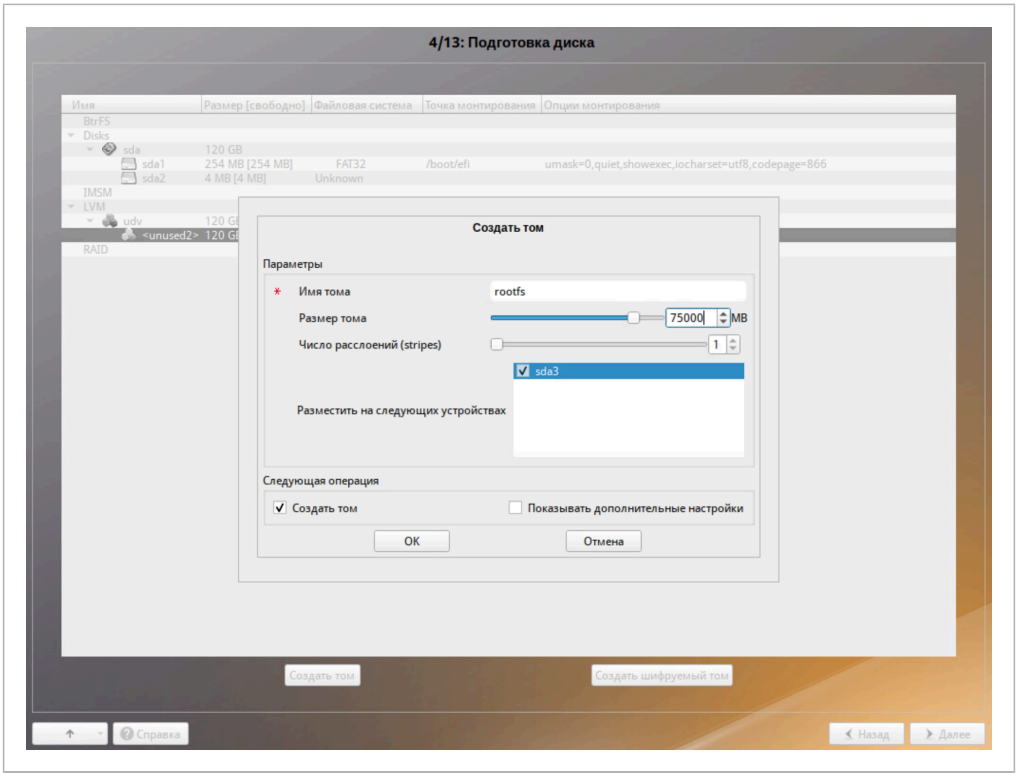


Рис. 23. Окно «Создать том» для rootfs

з. В новом окне **Создать файловую систему** выберите **Файловая система XFS** и нажмите **OK**.

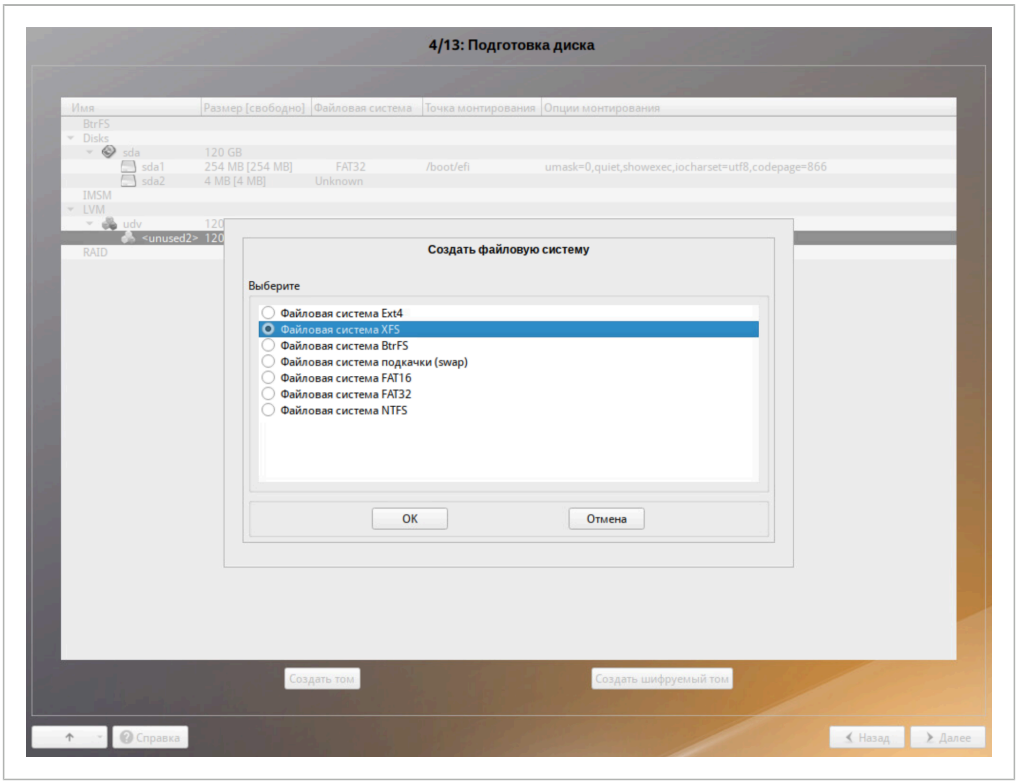


Рис. 24. Окно «Создать файловую систему» для rootfs

и. В новом окне **Изменить точку монтирования** убедитесь, что в поле **Точка монтирования** указано `/`, и нажмите **OK**.

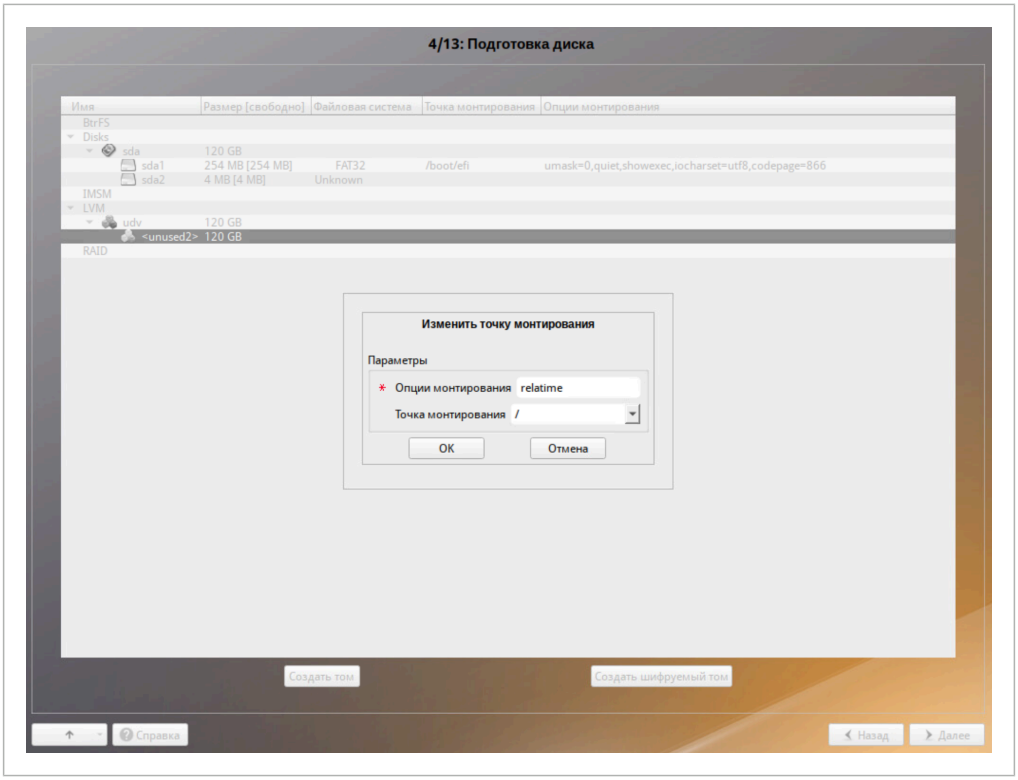


Рис. 25. Окно «Изменить точку монтирования» для rootfs

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

к. Создайте второй том `logs` для системных журналов. Для этого в раскрывающемся списке **LVM** выберите `<unused2>` и нажмите **Создать том**.

> Внимание:
>
> При отсутствии кнопки **Создать том** нажмите **Удалить том**, затем повторно нажмите **Создать том**.

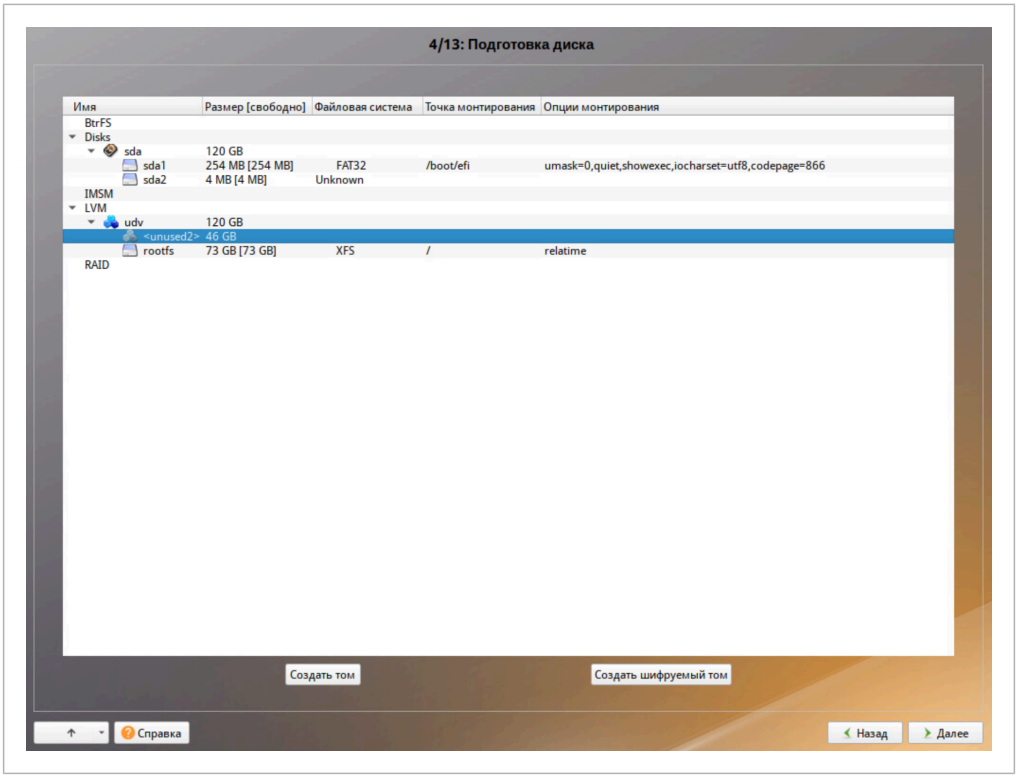


Рис. 26. Окно «Подготовка диска» (создание второго тома)

л. В открывшемся окне **Создать том** выполните следующие действия:

- Введите имя тома: `logs`.
- Выберите размер тома. Рекомендуемый размер тома — 25 ГБ (для этого укажите `25000` MB).
- Нажмите **ОК**.

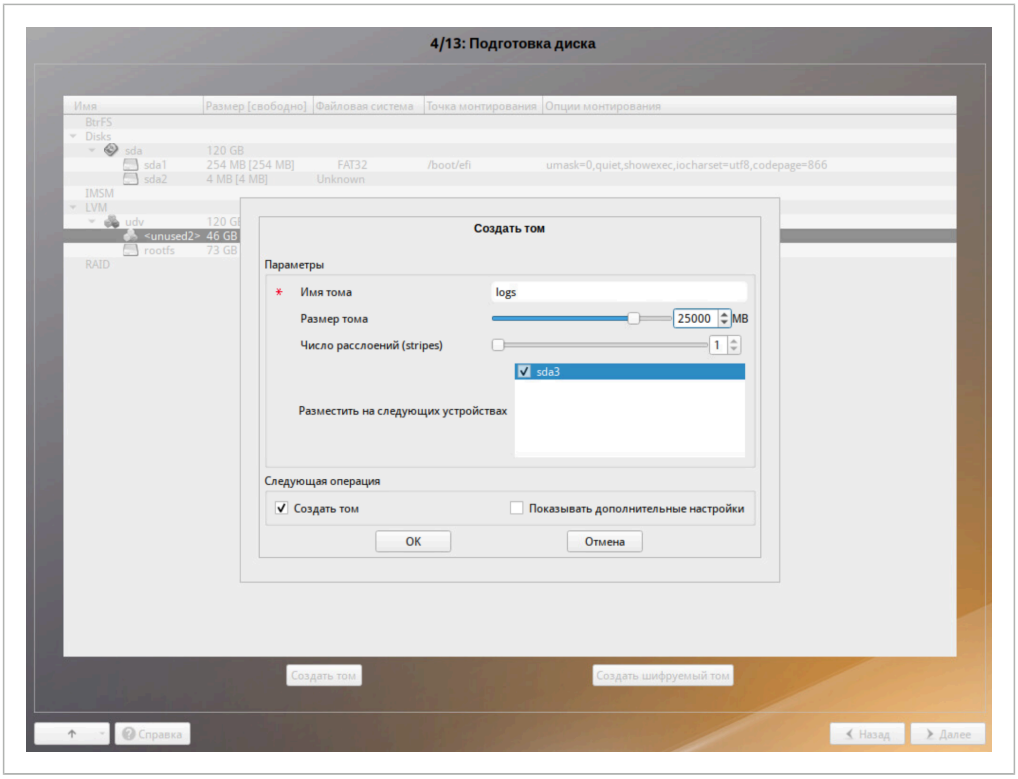


Рис. 27. Окно «Создать том» для logs

м. В новом окне **Создать файловую систему** выберите **Файловая система XFS** и нажмите **OK**.

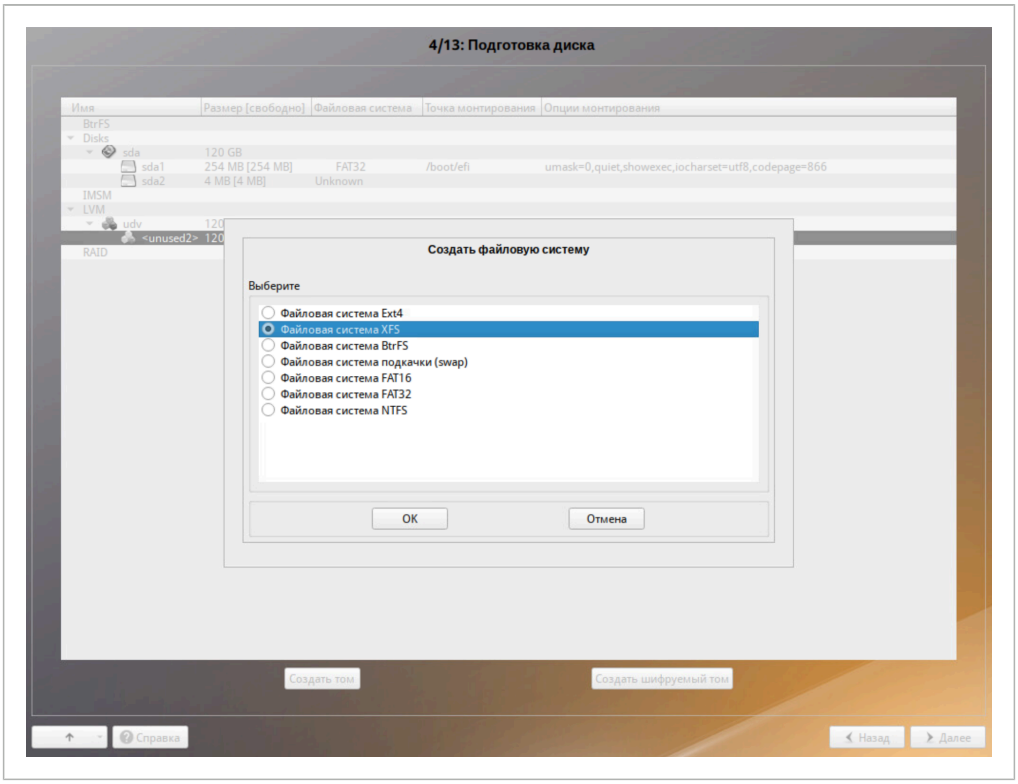


Рис. 28. Окно «Создать файловую систему» для logs

н. В новом окне **Изменить точку монтирования** выполните следующие действия:

- в поле **Точка монтирования** укажите значение `/var/log`;
- нажмите на поле **Опции монтирования** и убедитесь, что автоматически установилось значение `nosuid,nodev,noexec`;
- нажмите **ОК**.

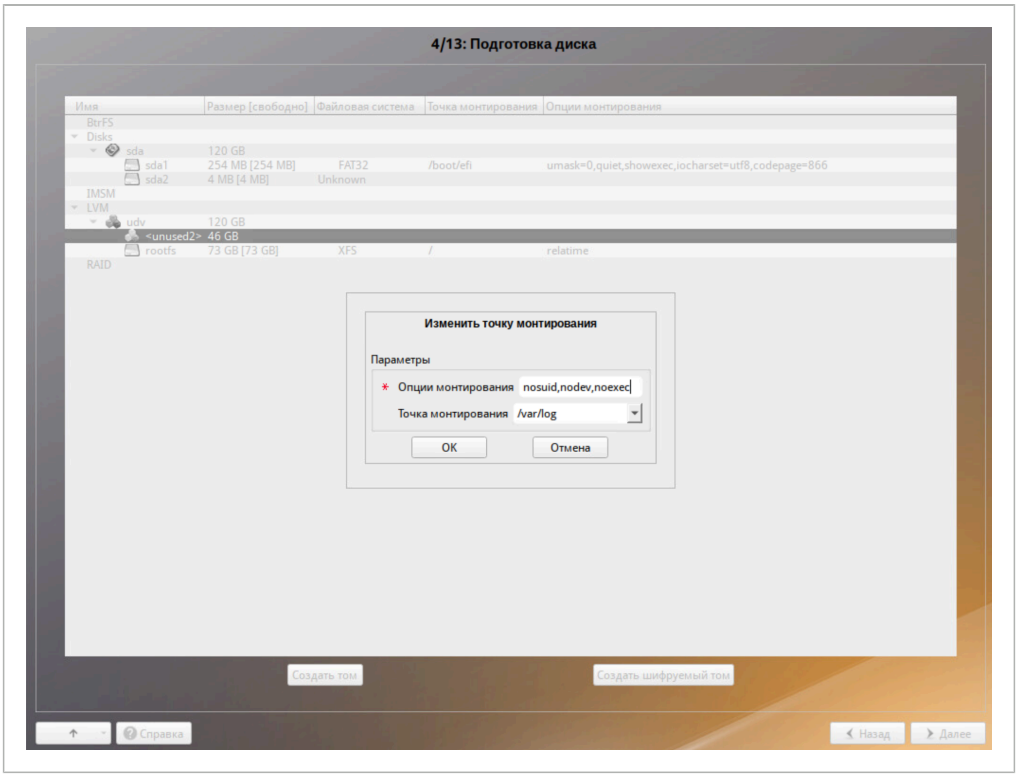


Рис. 29. Окно «Изменить точку монтирования» для logs

▸ **Результат шага:** появится окно подготовки диска со списком томов `rootfs` и `logs` в созданной группе.

o. Для применения настроек нажмите **Далее**.

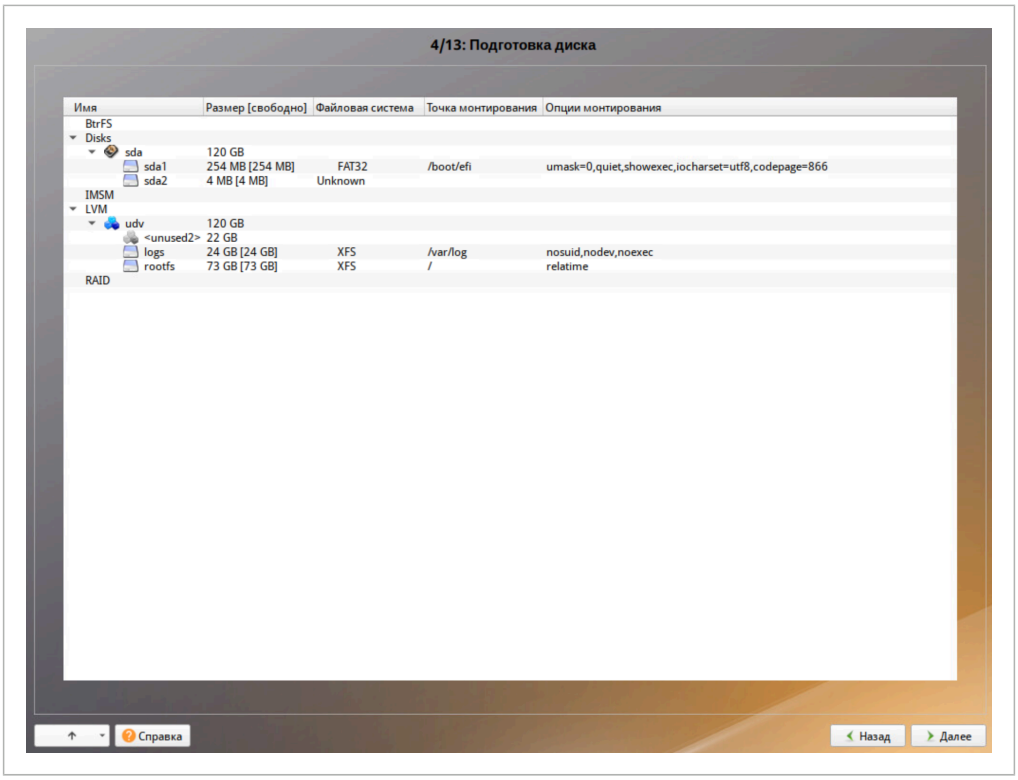


Рис. 30. Окно «Подготовка диска» (итоговые настройки)

п. В новом окне с запланированными операциями нажмите **OK**.

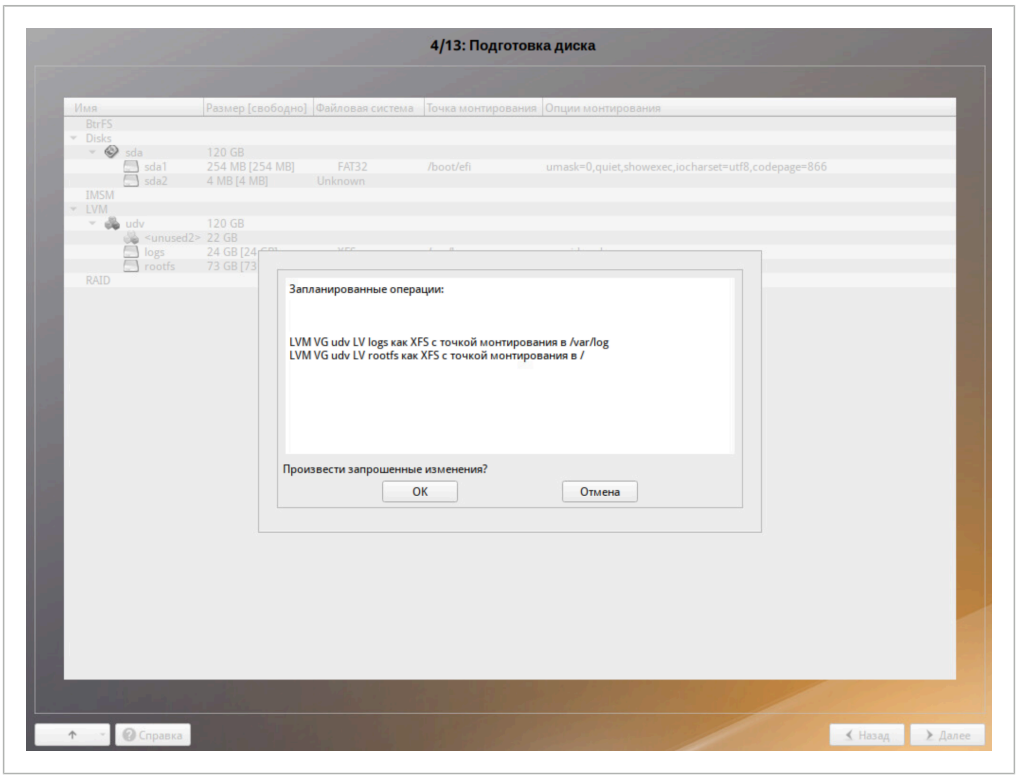


Рис. 31. Подтверждение параметров разметки дискового пространства

10. В окне **Установка системы** отмените выбор чекбоксов со всех компонентов в поле **Дополнительные приложения** и нажмите **Далее.**

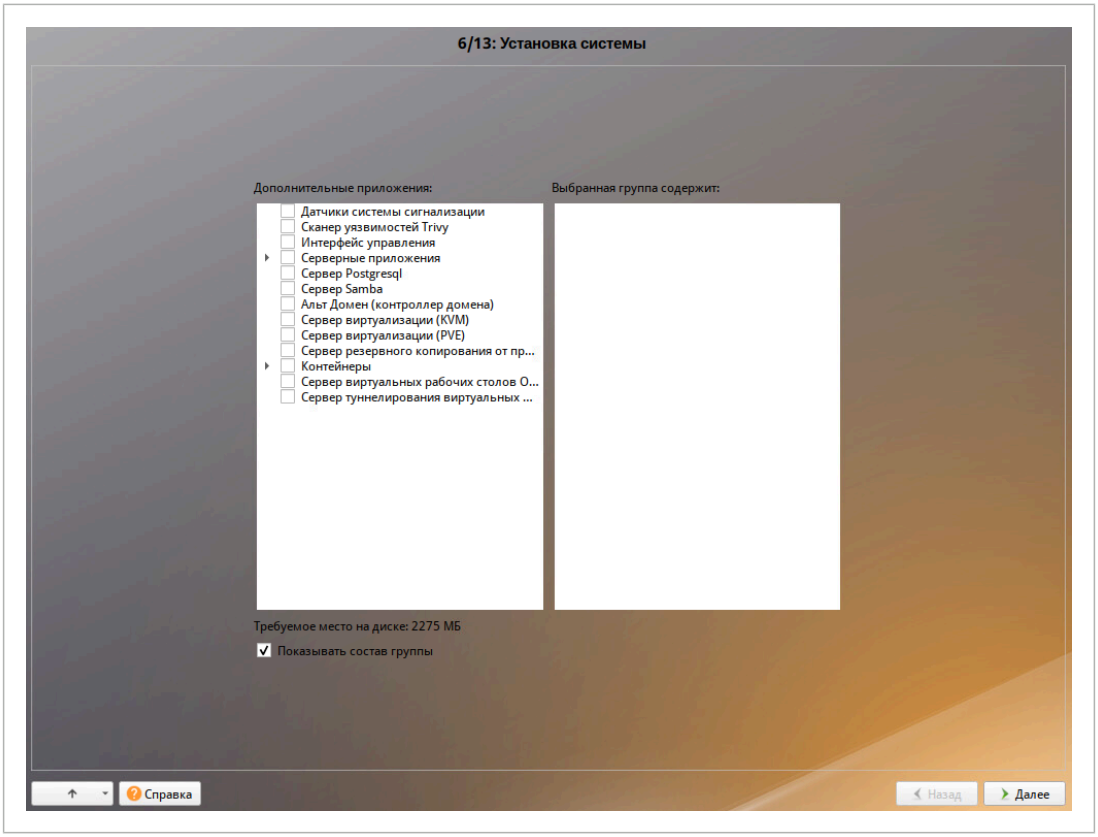


Рис. 32. Окно «Установка системы» (выбор дополнительных компонентов)

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

11. Дождитесь окончания установки ОС Альт Сервер.
    - **Результат шага:** появится окно **Установка загрузчика**.
12. В новом окне **Установка загрузчика** выполните следующие действия:
    - Убедитесь, что в поле **Устройство:** выбрано устройство **EFI (рекомендуемый)** для установки загрузчика.
    - При необходимости установите пароль на вход в загрузчик. Если пароль не нужен, отмените выбор чекбокса **Установить или сбросить пароль**.
    - Нажмите **Далее**.

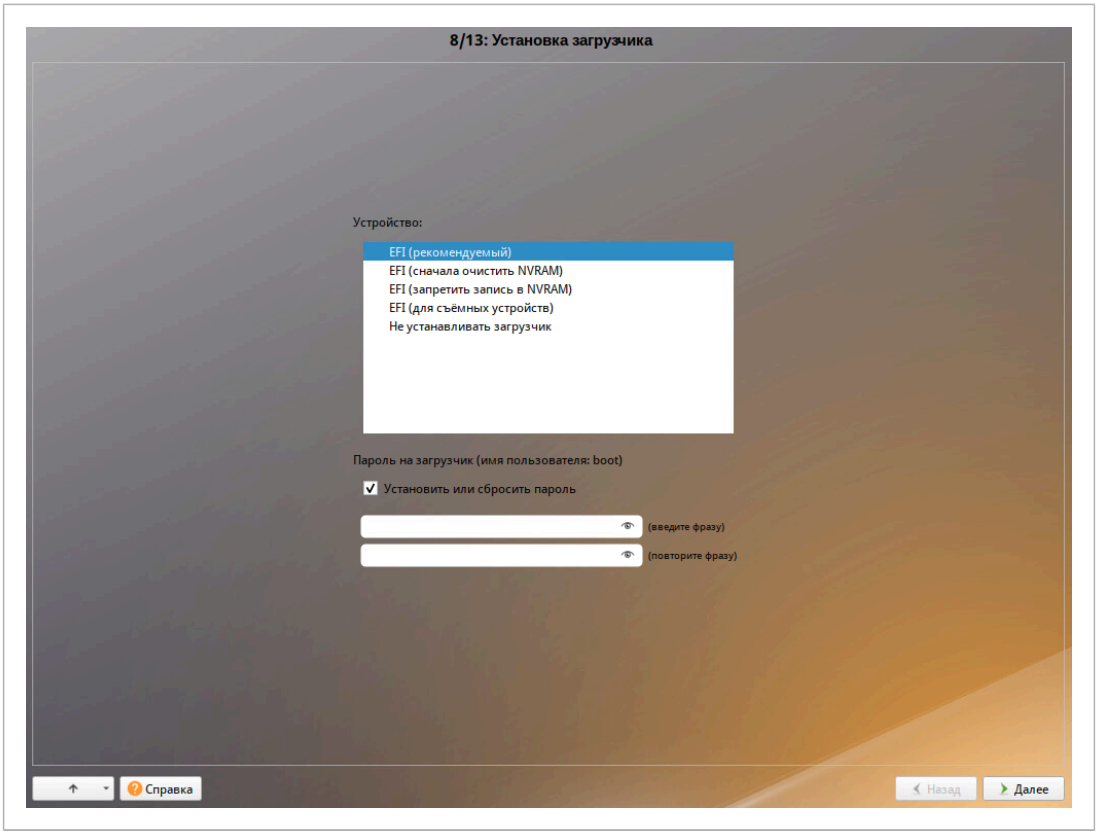


Рис. 33. Окно «Установка загрузчика»

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

13. Выполните настройку сетевого интерфейса управления:

> 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 DATAPK.

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

> Подсказка:
>
> 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. Если серверов несколько, укажите их через пробел.

ж. Нажмите **Далее**.

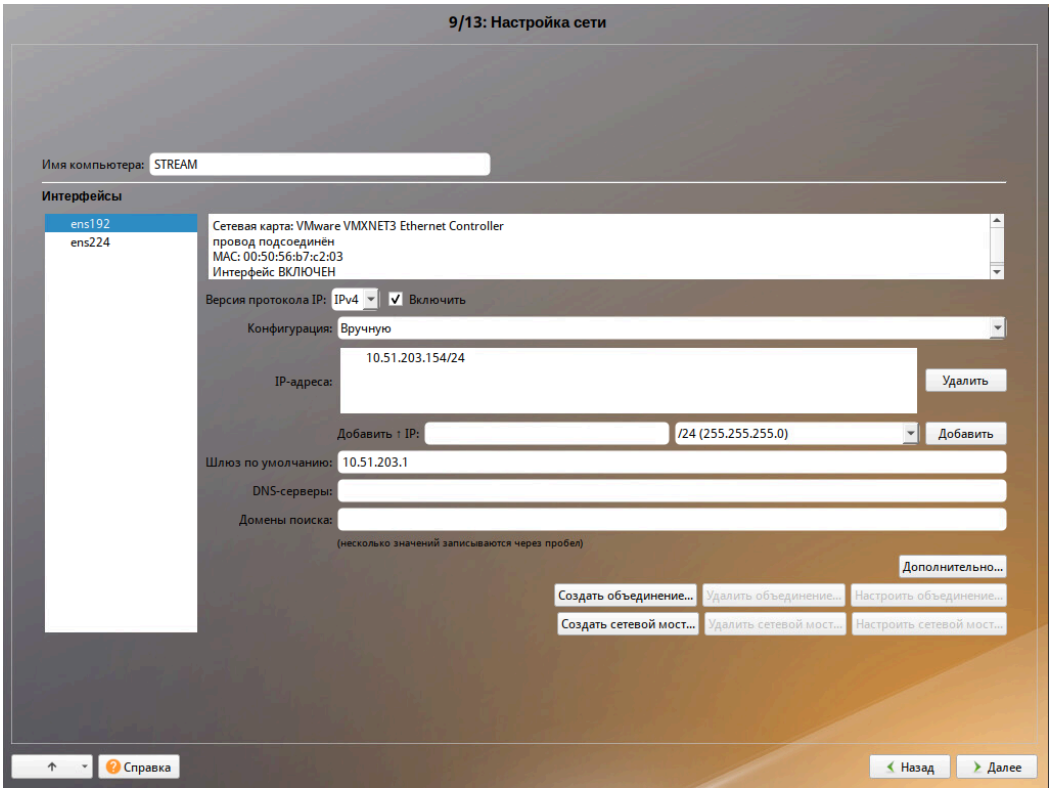


Рис. 34. Окно «Настройка сети»

- **Результат шага:**
  - будет настроен сетевой интерфейс управления UDV DATAPK;
  - появится окно **Администратор системы**.

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

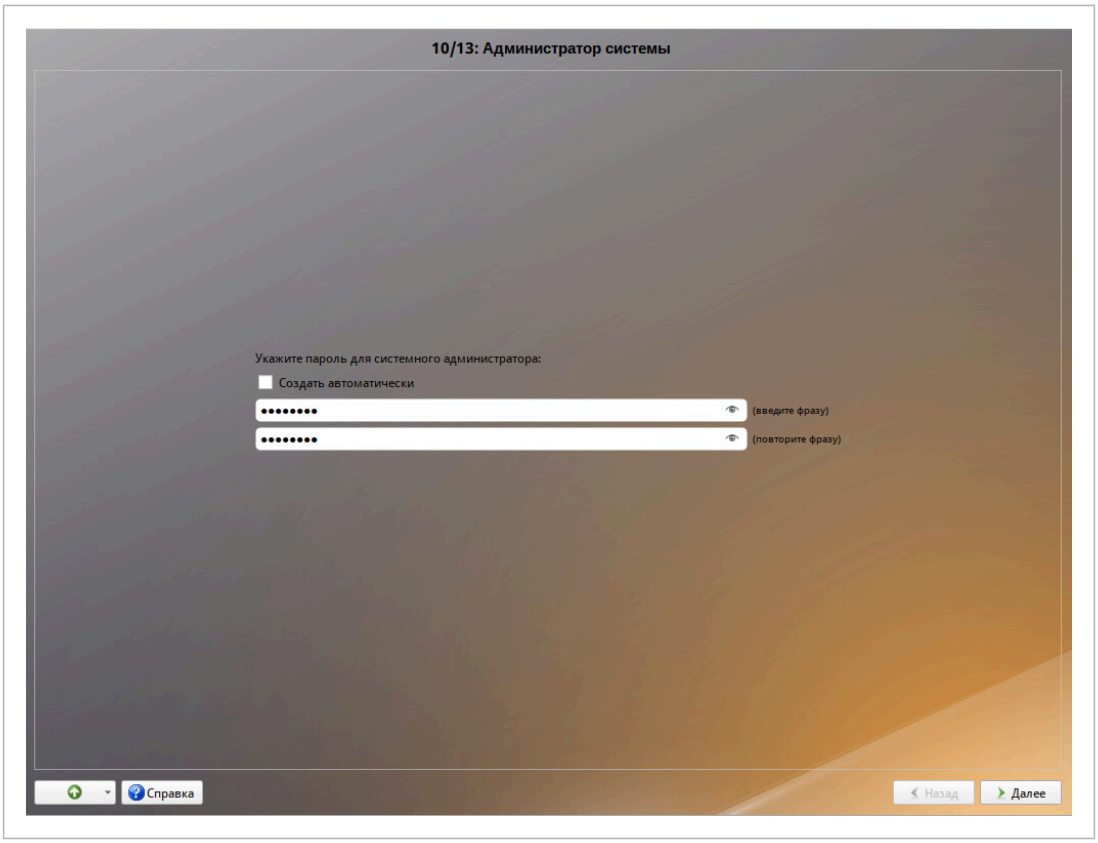


Рис. 35. Окно «Администратор системы»

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

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

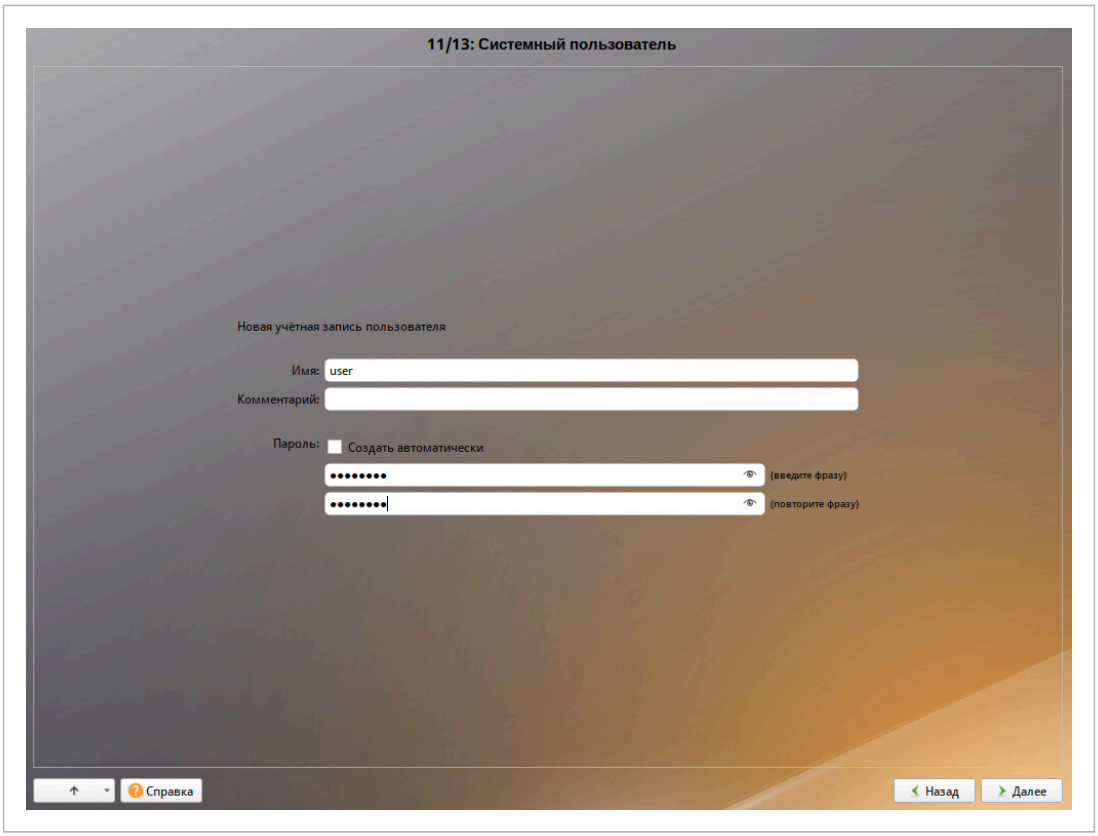


Рис. 36. Окно «Системный пользователь»

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

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

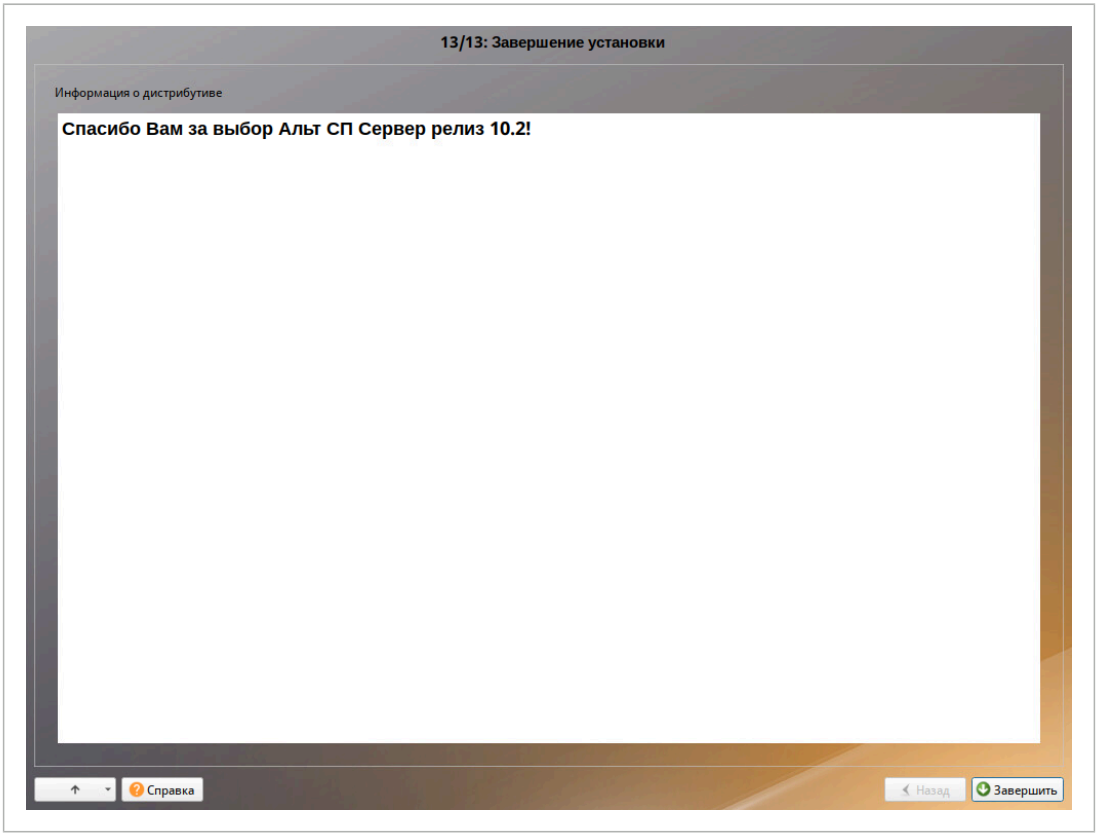


Рис. 37. Окно «Завершение установки»

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

Что дальше: 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».

3.1.2.2. Настройка сертифицированной ОС Альт Сервер 10.2 SP

1. Подключитесь к UDV DATAPK по протоколу SSH:

> Внимание:
>
> Если подключение по протоколу SSH в UDV DATAPK недоступно, убедитесь, что был корректно настроен сетевой интерфейс на шаге 13 инструкции «Установка сертифицированной ОС Альт Сервер 10.2 SP». При необходимости настройте интерфейс UDV DATAPK вручную по инструкции «Настройка сетевых интерфейсов в терминале Комплекса» и повторите подключение по SSH.

   а. Откройте программу-клиент SSH и выполните подключение к Комплексу с учетной записью, созданной на этапе установки (например, `user`).

   б. В окне подключения введите пароль учетной записи и нажмите **Enter**

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

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

```
su -
```

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

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

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

2. > Внимание:
   >
   > Если установлена более ранняя версия ОС Альт Сервер 10.1, перед началом обновления ПО предварительно требуется выполнить переключение на новые репозитории версии 10.2 согласно официальной документации ОС Альт Сервер, либо обратитесь в сервисный центр «Базальт СПО».

> Внимание:
>
> Если обновление компонентов ОС Альт Сервер выполняется через сеть Интернет, для установки Комплекса также потребуется наличие доступа в сеть Интернет. В таком случае при наличии доступа в сеть Интернет дальнейшие попытки обновления компонентов ОС Альт Сервер с ISO-образа или оптического диска будут неуспешными.

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

> Прим.:
>
> При отсутствии доступа в сеть Интернет сразу перейдите на следующий шаг 3.

а. Установите пакет `sudo`, выполнив команду:

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

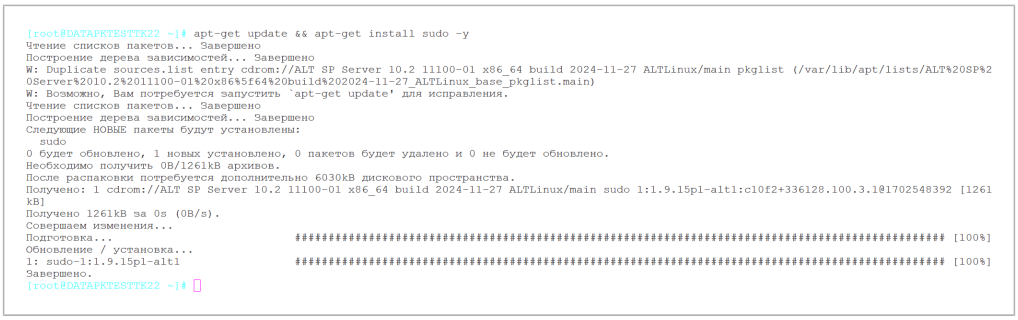


Рис. 38. Установка пакета sudo

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`, либо все с `rsync` в адресе), удалив символ `#`:

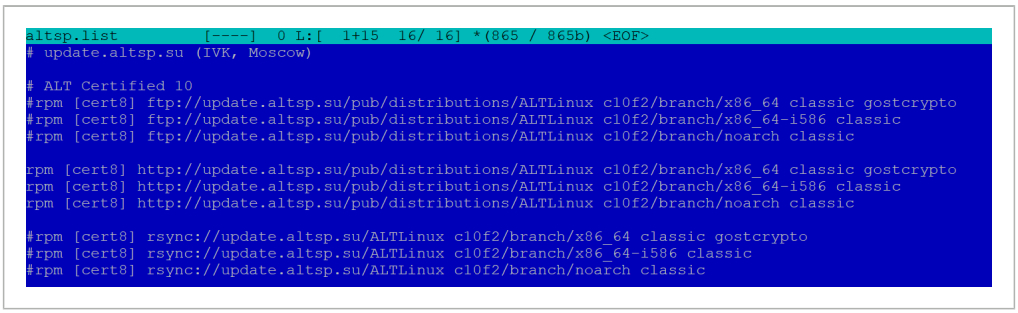


Рис. 39. Подключение репозиториев ОС Альт Сервер по протоколу HTTP

> ОСТОРОЖНО:
>
> Может быть выбран только один тип репозиториев из трех (`http`, `ftp` или `rsync`), иначе попытки обновления ОС Альт Сервер будут неудачны.

д. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

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.

3. Прим.:

   Если компоненты ОС Альт Сервер уже были обновлены с помощью предыдущего шага 2, сразу перейдите на следующий шаг 4.

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

   а. Убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.

   б. Установите пакет `sudo`, выполнив команду:

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

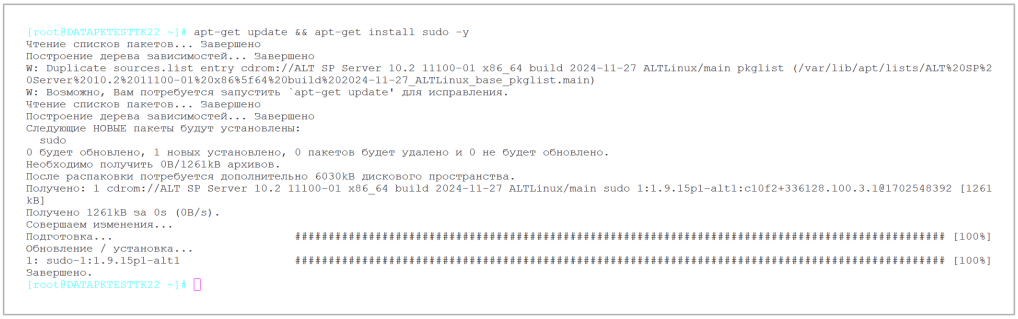
   

   Рис. 41. Установка пакета sudo

   в. 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.

4. Выполните перезагрузку ОС Альт Сервер:

   ```
   shutdown -r now
   ```

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

5. Повторно выполните вход в ОС Альт Сервер под учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
6. 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
```

> Подсказка:
>
> 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. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

г. Для применения новых настроек перезапустите службу SSH:

```
systemctl restart sshd
```

7. Добавьте возможность использования `sudo:`

> Внимание:
>
> При работе в учетной записи `user` может потребоваться использование `sudo` для выполнения некоторых команд.

а. Откройте для редактирования конфигурационный файл `sudoers`, выполнив команду:

```
mcedit /etc/sudoers
```

б. В поле `User privilege specification` добавьте запись:

```
user ALL=(ALL:ALL) ALL
```

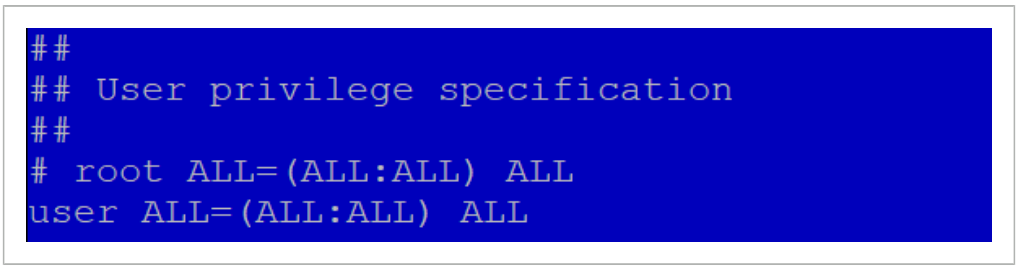


Рис. 42. Добавление прав для пользователя user в файл sudoers

в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

8. Для применения настроек выполните повторный вход под учетной записью `user` по протоколу SSH и повысьте привилегии до администратора с помощью команды `su -`
9. 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
```

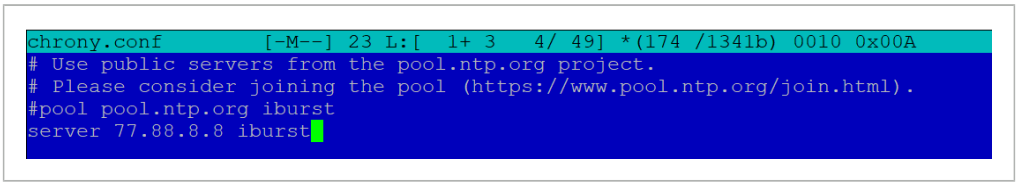


Рис. 44. Файл конфигурации службы chronyd

в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

г. Запустите службу `chronyd` и добавьте ее в автозагрузку:

```
systemctl enable chronyd
```

д. Выполните команду для перезапуска службы `chronyd`:

```
systemctl restart chronyd
```

е. Выполните команду для проверки синхронизации времени:

```
chronyc sources
```

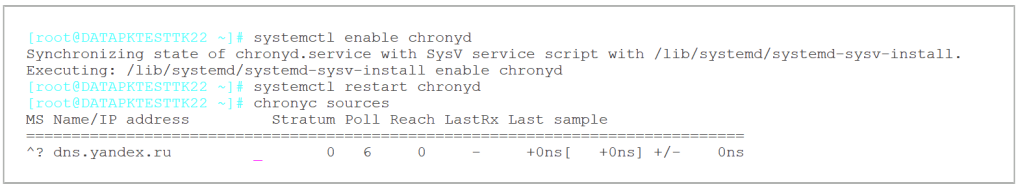


Рис. 46. Пример корректного вывода команды chronyc sources

> 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 DATAPK.

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

10. Измените настройки ядра ОС в конфигурационном файле `99-udv.conf`. Для этого:

а. Откройте файл `99-udv.conf` для редактирования, выполнив команду:

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

> Подсказка:
>
> Если файл `99-udv.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
```

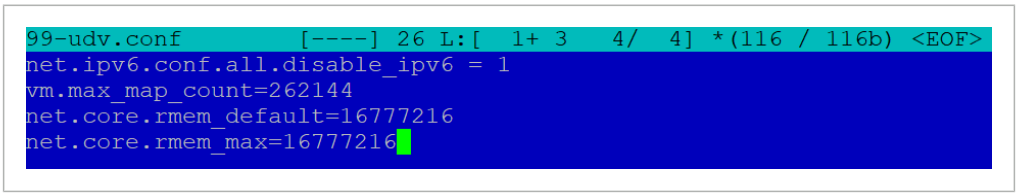


Рис. 48. Создание конфигурационного файла 99-udv.conf

в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

г. Примените новые настройки по команде:

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

д. 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.rmem_max'
```

Рис. 50. Корректный вывод значений конфигурационного файла 99-udv.conf

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

Что дальше:

При необходимости вы можете изменить увеличить объем дискового раздела `/dev/udv/rootfs`. Для этого последовательно выполните следующие команды (пример увеличения объема на 100 ГБ):

```
lvextend /dev/udv/rootfs -l +100G
xfs_growfs /
```

3.1.3. Подготовка к установке Комплекса

Для подготовки к установке Комплекса выполните следующие инструкции:

- Разметка диска для установки Комплекса уровня Management;
- Разметка диска для установки Комплекса уровня Sensor;
- Подключение репозиториев Комплекса.

3.1.3.1. Разметка диска для установки Комплекса уровня Management

3.1.3.1.1. Разметка диска для хранения очереди системных сообщений

> Прим.:
>
> Рекомендуется выполнять разметку диска для Комплекса уровня Management до выполнения разметки для уровня Sensor.

Чтобы выполнить разметку диска для хранения очереди системных сообщений Комплекса уровня Management:

1. Подключитесь к Комплексу уровня Management по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. Создайте логический раздел размера `[размер раздела в ГБ]` в группе `udv` с именем `rmq`, выполнив команду:

   ```
   lvcreate -L [размер раздела в ГБ]G -n rmq udv
   ```

   > Прим.:
   >
   > Рекомендуемый размер раздела — 20 ГБ.

3. Создайте файловую систему `xfs` на созданном разделе, выполнив команду:

   ```
   mkfs.xfs /dev/udv/rmq
   ```

   ```
   [root@DATAPKTESTTK22 ~]# lvcreate -L 20G -n rmq udv
     Logical volume "rmq" created.
   [root@DATAPKTESTTK22 ~]# mkfs.xfs /dev/udv/rmq
   meta-data=/dev/udv/rmq           isize=512    agcount=4, agsize=1310720 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=5242880, 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. 51. Создание файловой системы для хранения системных сообщений

4. Создайте директорию, к которой будет подключаться раздел, выполнив команду:

   ```
   mkdir -p /var/lib/rabbitmq
   ```

5. Внесите изменения в файл `/etc/fstab` для автоматического подключения раздела при перезагрузке. Для этого:

а. Откройте на редактирование файл, выполнив команду:

```
mcedit /etc/fstab
```

б. Добавьте следующую строку в конец файла:

```
/dev/mapper/udv-rmq /var/lib/rabbitmq xfs nosuid,nodev 0 0
```

в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

6. Подключите добавленный раздел на основе `/etc/fstab`, выполнив команду:

```
mount -a
```

7. Убедитесь, что необходимый раздел подключен. Для этого выполните команду:

```
df -h | grep -E "rmq"
```

```
[root@DATAPKTESTTK22 ~]# mount -a
[root@DATAPKTESTTK22 ~]# df -h | grep -E "rmq"
/dev/mapper/udv-rmq       20G         175M   20G            1% /var/lib/rabbitmq
```

Рис. 52. Успешное подключение раздела для хранения системных сообщений

3.1.3.1.2. Разметка диска для хранения репозиториев модуля «Управление проектами ПЛК»

Перед установкой модуля «Управление проектами ПЛК» необходимо выполнить разметку диска для хранения репозиториев. Для разметки диска:

1. Создайте логический раздел `vc-repos` размера `[размер раздела в ГБ]` в группе `udv`, выполнив команду:

```
lvcreate -L [размер раздела в ГБ]G -n vc-repos udv
```

> Прим.:
>
> Рекомендуемый размер раздела рассчитывается по следующей формуле:
>
> $5 * PLC_{ave} * PLC_{total}$
>
> Где:
>
> - PLC_{ave} — средний размер проекта ПЛК;
> - PLC_{total} — количество проектов ПЛК.

2. Создайте файловую систему `xfs` на созданном разделе, выполнив команду:

```
mkfs.xfs /dev/udv/vc-repos
```

```
[root@STREAM ~]# mkfs.xfs /dev/udv/vc-repos
meta-data=/dev/udv/vc-repos      isize=512    agcount=4, agsize=393216 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=1572864, 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. 53. Создание файловой системы для хранения репозиториев

3. Создайте директорию, к которой будет подключаться раздел, выполнив команду:

```
mkdir -p /var/lib/udv/vc-repos-backend
```

4. Внесите изменения в файл `/etc/fstab` для автоматического подключения раздела при перезагрузке. Для этого:

   а. Откройте на редактирование файл, выполнив команду:

   ```
   mcedit /etc/fstab
   ```

   б. Добавьте следующую строку в конец файла:

   ```
   /dev/mapper/udv-vc--repos /var/lib/udv/vc-repos-backend xfs defaults 0 0
   ```

   в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

5. Подключите добавленный раздел на основе `/etc/fstab`, выполнив команду:

```
mount -a
```

6. Убедитесь, что необходимый раздел подключен. Для этого выполните команду:

```
df -h | grep -E "vc-repos"
```

```
[root@STREAM ~]# df -h | grep -E "vc-repos"
/dev/mapper/udv-vc--repos   6,0G          76M  6,0G           2% /var/lib/udv/vc-repos-backend
```

Рис. 54. Успешное подключение раздела для хранения репозиториев

3.1.3.1.3. Разметка диска для хранения сетевых соединений модуля «Анализ промышленного сетевого трафика»

Перед установкой модуля «Анализ промышленного сетевого трафика» необходимо выполнить разметку диска для хранения сетевых соединений. Для разметки диска:

1. Создайте логический раздел `clickhouse` размера `[размер раздела в ГБ]` в группе `udv`, выполнив команду:

```
lvcreate -L [размер раздела в ГБ]G -n clickhouse udv
```

> **Прим.:**
>
> Выделяемый размер раздела зависит от количества поступающих сетевых пакетов и необходимой длительности их хранения. Рекомендуемый минимальный размер раздела — 300 ГБ.

2. Создайте файловую систему `ext4` на созданном разделе, выполнив команду:

```
mkfs.ext4 /dev/udv/clickhouse
```

```
[root@STREAM ~]# mkfs.ext4 /dev/udv/clickhouse
mke2fs 1.46.2 (28-Feb-2021)
Discarding device blocks: done
Creating filesystem with 1572864 4k blocks and 393216 inodes
Filesystem UUID: 04bfc48f-217f-452f-81bb-f63cbcf4c317
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
```

Рис. 55. Создание файловой системы для хранения сетевых соединений

3. Создайте директорию, к которой будет подключаться раздел, выполнив команду:

```
mkdir -p /var/lib/clickhouse
```

4. Внесите изменения в файл `/etc/fstab` для автоматического подключения раздела при перезагрузке. Для этого:

   а. Откройте на редактирование файл, выполнив команду:

   ```
   mcedit /etc/fstab
   ```

   б. Добавьте следующую строку в конец файла:

   ```
   /dev/mapper/udv-clickhouse /var/lib/clickhouse ext4 noatime 0 0
   ```

   в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

5. Подключите добавленный раздел на основе `/etc/fstab`, выполнив команду:

```
mount -a
```

6. Убедитесь, что необходимый раздел подключен. Для этого выполните команду:

```
df -h | grep -E "clickhouse"
```

```
[root@STREAM ~]# df -h | grep -E "clickhouse"
/dev/mapper/udv-clickhouse   5,9G          24K  5,6G           1% /var/lib/clickhouse
```

Рис. 56. Успешное подключение раздела для хранения сетевых соединений

3.1.3.1.4. Разметка диска для хранения резервных копий Комплекса

Для корректного выполнения резервного копирования данных Комплекса необходимо создать и подключить новый диск. В зависимости от носителя можно разметить как отдельный физический диск, так и логический раздел. Чтобы выполнить разметку диска для хранения резервных копий:

1. Подключите новый физический или логический диск.

   > Прим.:
   >
   > Рекомендуемый минимальный размер диска — 500 ГБ.

2. Уточните название диска:
   - если подключен отдельный физический диск, найдите его название (например, `sdb`) в выводе команды:

     ```
     lsblk
     ```

     ```
     [root@STREAM ~]# lsblk
     NAME           MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
     sda              8:0    0   80G  0 disk
     ├─sda1           8:1    0  254M  0 part /boot/efi
     ├─sda2           8:2    0    4M  0 part
     └─sda3           8:3    0 79.7G  0 part
       └─udv-rootfs 253:0    0 48.8G  0 lvm  /
     sdb              8:16   0   80G  0 disk
     sr0             11:0    1 1024M  0 rom
     ```

     Рис. 57. Список подключенных физических дисков

   - если необходимо использовать логический раздел текущего диска, создайте раздел `backups` размера `[размер раздела в ГБ]` в группе `udv`, выполнив команду:

     ```
     lvcreate -L [размер раздела в ГБ]G -n backups udv
     ```

3. Создайте файловую систему `xfs` на новом диске (например `sdb`) или логическом разделе (например, `backups`), выполнив команду:

   ```
   mkfs.xfs /dev/[название нового диска или раздела]
   ```

4. Создайте директорию `backups`, к которой будет подключаться новый диск или раздел. Для этого выполните команду:

   ```
   mkdir -p /var/backups
   ```

5. Уточните идентификатор нового диск или раздела, выполнив команду:

   ```
   blkid -s UUID /dev/[название нового диска или раздела]
   ```

   Скопируйте или сохраните полученный идентификатор без кавычек.

```
[root@STREAM ~]# blkid -s UUID /dev/sdb
/dev/sdb: UUID="1ec1dd38-ddf2-4dfa-bfae-1e8c73ea43fa"
```

Рис. 58. Идентификатор диска

6. Внесите изменения в файл `/etc/fstab` для автоматического подключения раздела при перезагрузке. Для этого:

    а. Откройте на редактирование файл, выполнив команду:

    ```
    mcedit /etc/fstab
    ```

    б. Добавьте следующую строку в конец файла:

    ```
    UUID=[UUID диска или раздела] /var/backups xfs defaults 0 0
    ```

    где `[UUID диска или раздела]` — идентификатор диска или раздела, скопированный в шаге 5.

    в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

7. Подключите добавленный диск на основе `/etc/fstab`, выполнив команду:

    ```
    mount -a
    ```

8. Убедитесь, что необходимый диск подключен. Для этого выполните команду:

    ```
    df -h | grep -E "[название диска или раздела]"
    ```

    Пример

    Для диска `sdb` команда будет выглядеть следующим образом:

    ```
    df -h | grep -E "sdb"
    ```

3.1.3.1.5. Разметка диска для хранения внешних событий

Перед установкой модуля «Управление внешними событиями» необходимо выполнить разметку диска для хранения внешних событий. Для разметки диска:

1. Создайте логический раздел `opensearch` размера `[размер раздела в ГБ]` в группе `udv`, выполнив команду:

    ```
    lvcreate -L [размер раздела в ГБ]G -n opensearch udv
    ```

    Прим.:

    Рекомендуемый минимальный размер раздела — 100 ГБ.

2. Создайте файловую систему `xfs` на созданном разделе, выполнив команду:

    ```
    mkfs.xfs /dev/udv/opensearch
    ```

```
[root@STREAM ~]# mkfs.xfs /dev/udv/opensearch
meta-data=/dev/udv/opensearch    isize=512    agcount=4, agsize=393216 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=1572864, 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. 59. Создание файловой системы для хранения внешних событий

3. Создайте директорию, к которой будет подключаться раздел, выполнив команду:

```
mkdir -p /var/lib/opensearch
```

4. Внесите изменения в файл `/etc/fstab` для автоматического подключения раздела при перезагрузке. Для этого:

   а. Откройте на редактирование файл, выполнив команду:

   ```
   mcedit /etc/fstab
   ```

   б. Добавьте следующую строку в конец файла:

   ```
   /dev/mapper/udv-opensearch /var/lib/opensearch xfs nosuid,nodev 0 0
   ```

   в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

5. Подключите добавленный раздел на основе `/etc/fstab`, выполнив команду:

```
mount -a
```

6. Убедитесь, что необходимый раздел подключен. Для этого выполните команду:

```
df -h | grep -E "opensearch"
```

```
[root@STREAM ~]# df -h | grep -E "opensearch"
/dev/mapper/udv-opensearch   6,0G          76M  6,0G           2% /var/lib/opensearch
```

Рис. 60. Успешное подключение раздела для хранения внешних событий

Что дальше:

Если Комплекс уровня Sensor (сенсор) будет установлен на тот же сервер, что и уровень Management, следующим шагом выполните разметку дискового пространства для сенсора на текущем сервере по инструкции «Разметка диска для установки Комплекса уровня Sensor».

Прим.:

Порядок разметки для сенсора не отличается в случае его установки на тот же сервер, что и Management, и в случае его установки на отдельный сервер.

При необходимости вы можете увеличить объем дисковых разделов. Для этого последовательно выполните следующие команды (пример увеличения объема раздела `/dev/udv/opensearch` с файловой системой xfs на 100 ГБ):

```
lvextend /dev/udv/opensearch -l +100G
xfs_growfs /dev/udv/opensearch
```

3.1.3.2. Разметка диска для установки Комплекса уровня Sensor

3.1.3.2.1. Разметка диска для хранения файлов, извлеченных из сетевого трафика с помощью модуля «Анализ промышленного сетевого трафика»

Перед выполнением: Перед выполнением разметки дискового пространства для Комплекса уровня Sensor (сенсора) необходимо выполнить разметку для Комплекса уровня Management.

Перед установкой модуля «Анализ промышленного сетевого трафика» необходимо выполнить разметку диска для хранения извлеченных файлов. Для разметки диска:

1. Если сенсор будет устанавливаться на сервер, отдельный от Комплекса уровня Management, подключитесь к сенсору по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. Создайте логический раздел `files` размера `[размер раздела в ГБ]` в группе `udv`, выполнив команду:

   ```
   lvcreate -L [размер раздела в ГБ]G -n files udv
   ```

   > Прим.:
   >
   > Рекомендуемый минимальный размер раздела — 10 ГБ.

3. Создайте файловую систему `ext4` на созданном разделе, выполнив команду:

   ```
   mkfs.xfs /dev/udv/files
   ```

   ```
   [root@STREAM ~]# mkfs.xfs /dev/udv/files
   meta-data=/dev/udv/files         isize=512    agcount=4, agsize=393216 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=1572864, 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. 61. Создание файловой системы для хранения извлеченных файлов

4. Создайте директорию, к которой будет подключаться раздел, выполнив команду:

   ```
   mkdir -p /usr/share/udv/zeek-wrapper/extracted_files
   ```

5. Внесите изменения в файл `/etc/fstab` для автоматического подключения раздела при перезагрузке. Для этого:

a. Откройте на редактирование файл, выполнив команду:

```
mcedit /etc/fstab
```

б. Добавьте следующую строку в конец файла:

```
/dev/mapper/udv-files /usr/share/udv/zeek-wrapper/extracted_files \
xfs async,auto,nodev,noatime,noexec,nouser,suid,rw 0 0
```

в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

6. Подключите добавленный раздел на основе `/etc/fstab`, выполнив команду:

```
mount -a
```

7. Убедитесь, что необходимый раздел подключен. Для этого выполните команду:

```
df -h | grep -E "files"
```

```
[root@STREAM ~]# df -h | grep -E "files"
/dev/mapper/udv-files        6,0G          76M  6,0G            2% /usr/share/ud
v/zeek-wrapper/extracted_files
```

Рис. 62. Успешное подключение раздела для хранения извлеченных файлов

3.1.3.2.2. Разметка диска для хранения PCAP-файлов сетевых соединений, извлеченных модулем «Анализ промышленного сетевого трафика»

Перед установкой модуля «Анализ промышленного сетевого трафика» необходимо выполнить разметку диска для хранения PCAP-файлов сетевых соединений. Для разметки диска:

1. Создайте логический раздел `pcaps` размера `[размер раздела в ГБ]` в группе `udv`, выполнив команду:

```
lvcreate -L [размер раздела в ГБ]G -n pcaps udv
```

> Прим.:
>
> Выделяемый размер раздела зависит от количества поступающих сетевых пакетов и необходимой длительности хранения информации о них. Рекомендуемый минимальный размер раздела — 400 ГБ.

2. Создайте файловую систему `xfs` на созданном разделе, выполнив команду:

```
mkfs.xfs /dev/udv/pcaps
```

```
[root@STREAM ~]# mkfs.xfs /dev/udv/pcaps
meta-data=/dev/udv/pcaps         isize=512    agcount=4, agsize=12800 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=51200, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=1368, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
Discarding blocks...Done.
```

Рис. 63. Создание файловой системы для хранения PCAP-файлов

3. Создайте директорию, к которой будет подключаться раздел, выполнив команду:

```
mkdir -p /var/cache/udv/stenographer/
```

4. Внесите изменения в файл `/etc/fstab` для автоматического подключения раздела при перезагрузке. Для этого:

   а. Откройте на редактирование файл, выполнив команду:

   ```
   mcedit /etc/fstab
   ```

   б. Добавьте следующую строку в конец файла:

   ```
   /dev/mapper/udv-pcaps /var/cache/udv/stenographer/ \
   xfs async,auto,nodev,noatime,noexec,nouser,suid,rw 0 0
   ```

   в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

5. Подключите добавленный раздел на основе `/etc/fstab`, выполнив команду:

```
mount -a
```

6. Убедитесь, что необходимый раздел подключен. Для этого выполните команду:

```
df -h | grep -E "pcaps"
```

```
[root@STREAM ~]# df -h | grep -E "pcaps"
/dev/mapper/udv-pcaps        195M          12M  184M            6% /var/cache/udv/stenographer
```

Рис. 64. Успешное подключение раздела для хранения PCAP-файлов

Что дальше: При необходимости вы можете увеличить объем дисковых разделов. Для этого последовательно выполните следующие команды (пример увеличения объема раздела `/dev/udv/pcaps` с файловой системой xfs на 100 ГБ):

```
lvextend /dev/udv/pcaps -l +100G
xfs_growfs /dev/udv/pcaps
```

3.1.3.3. Подключение репозиториев Комплекса

Инструкция предназначена для подключения репозиториев Комплекса уровня Management и Комплексов уровня Sensor (сенсора), которые устанавливаются как на одном сервере, так и на сервере, отдельном от уровня Management.

Для подключения репозиториев Комплекса:

1. Примонтируйте диск с дистрибутивом Комплекса, либо с помощью приложения для обмена файлами по протоколу SFTP (или аналогичным способом по сети) скопируйте архивы с репозиториями Комплекса `release-[версия_Комплекса]_[дата_архива].tar.gz` и `release-[версия_Комплекса]-external-modules_[дата_архива].tar.gz` в директорию `/home/user` операционной системы.
2. Выполните вход в ОС Альт Сервер под учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
3. Распакуйте архивы `release-[версия_Комплекса]_[дата_архива].tar.gz` и `release-[версия_Комплекса]-external-modules_[дата_архива].tar.gz`, выполнив команды:

   ```
   tar -xvzf /home/user/release-[версия_Комплекса]_[дата_архива].tar.gz -C /var/opt
   tar -xvzf /home/user/release-[версия_Комплекса]-external-modules_[дата_архива].tar.gz
    -C /var/opt
   ```

4. Просмотрите получившийся список директорий внутри директории `/var/opt/[версия_Комплекса]`, выполнив команду:

   ```
   ls /var/opt/release-[версия_Комплекса]
   ```

   Сохраните полученный список директорий.

   Пример

   Пример возможного списка директорий внутри директории `/var/opt/release-[версия_Комплекса]`:

   ```
   controlversion
   nta
   ours
   tools
   third
   zeek
   ```

5. Добавьте названия распакованных модулей Комплекса в новый конфигурационный файл репозитория. Для этого:

   a. Создайте конфигурационный файл `/etc/apt/sources.list.d/udv.list` репозитория, выполнив команду:

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

   б. Добавьте в конфигурационный файл следующую структуру для каждой директории из шага 4 :

   ```
   #[Название директории]
   rpm file:/var/opt/release-[версия_Комплекса]/[название директории] noarch classic
   rpm file:/var/opt/release-[версия_Комплекса]/[название директории] x86_64 classic
   ```

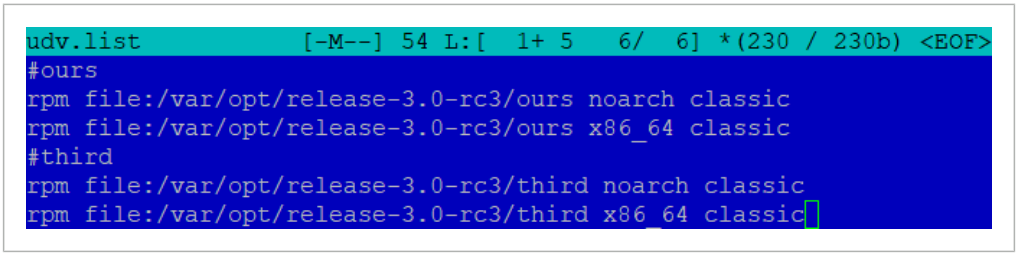


Рис. 65. Пример структуры для установки базового модуля (Core) Комплекса уровня Management

Пример конфигурационного файла `udv.list` для установки Комплекса:

```
#controlversion
rpm file:/var/opt/release-3.0.0.0/controlversion noarch classic
rpm file:/var/opt/release-3.0.0.0/controlversion x86_64 classic
#nta
rpm file:/var/opt/release-3.0.0.0/nta noarch classic
rpm file:/var/opt/release-3.0.0.0/nta x86_64 classic
#ours
rpm file:/var/opt/release-3.0.0.0/ours noarch classic
rpm file:/var/opt/release-3.0.0.0/ours x86_64 classic
#tools
rpm file:/var/opt/release-3.0.0.0/tools noarch classic
rpm file:/var/opt/release-3.0.0.0/tools x86_64 classic
#third
rpm file:/var/opt/release-3.0.0.0/third noarch classic
rpm file:/var/opt/release-3.0.0.0/third x86_64 classic
#zeek
rpm file:/var/opt/release-3.0.0.0/zeek noarch classic
rpm file:/var/opt/release-3.0.0.0/zeek x86_64 classic
```

в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

6. Внимание:

В зависимости от наличия доступа в сеть Интернет подключение репозиториев ОС Альт Сервер можно выполнить как онлайн, так и офлайн.

Если обновление компонентов ОС Альт Сервер выполняется через сеть Интернет, для установки Комплекса также потребуется наличие доступа в сеть Интернет. В таком случае при наличии доступа в сеть Интернет дальнейшие попытки обновления компонентов ОС Альт Сервер с ISO-образа или оптического диска будут неуспешными.

Подключите репозитории ОС Альт Сервер одним из следующих способов:

a. При наличии доступа в сеть Интернет:

> Прим.:
>
> При отсутствии доступа в сеть Интернет сразу перейдите к шагу 6.b.

- Откройте для редактирования конфигурационный файл со ссылками на репозитории, выполнив команду:

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

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

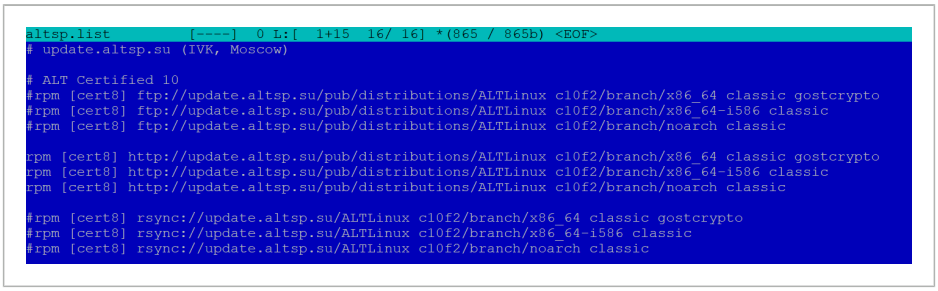


Рис. 66. Подключение репозиториев ОС Альт Сервер по протоколу HTTP

> ОСТОРОЖНО:
>
> Может быть выбран только один тип репозиториев из трех (`http`, `ftp` или `rsync`), иначе попытки обновления ОС Альт Сервер будут неудачны.

б. При отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.

> Прим.:
>
> Если репозитории ОС Альт Сервер уже подключены способом из предыдущего шага 6.a при наличии доступа в Интернет, сразу перейдите на следующий шаг 7.

7. Обновите репозиторий, выполнив команду:

```
apt-get update
```

```
[root@DATAPKTESTTK22 ~]# apt-get update
Получено: 1 http://update.altsp.su c10f2/branch/x86_64 release [3578B]
Получено: 2 http://update.altsp.su c10f2/branch/x86_64-i586 release [1033B]
Получено: 3 http://update.altsp.su c10f2/branch/noarch release [2199B]
Получено 6810B за 0s (38,5kB/s).
Найдено http://update.altsp.su c10f2/branch/x86_64/classic pkglist
Найдено http://update.altsp.su c10f2/branch/x86_64/classic release
Найдено http://update.altsp.su c10f2/branch/x86_64/gostcrypto pkglist
Найдено http://update.altsp.su c10f2/branch/x86_64/gostcrypto release
Найдено http://update.altsp.su c10f2/branch/x86_64-i586/classic pkglist
Найдено http://update.altsp.su c10f2/branch/x86_64-i586/classic release
Найдено http://update.altsp.su c10f2/branch/noarch/classic pkglist
Найдено http://update.altsp.su c10f2/branch/noarch/classic release
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
```

Рис. 67. Обновление репозитория

Что дальше: Выполните данную инструкцию для сенсоров, которые установлены на других серверах отдельно от Комплекса уровня Management.

3.1.4. Установка и запуск модулей Комплекса

Для установки и запуска Комплекса выполните следующие инструкции:

1. Установка модулей Комплекса уровня Management;
2. Установка модулей Комплекса уровня Sensor;
3. Запуск Комплекса.

Инструкции в текущем разделе предназначены для установки следующих модулей и сервисов Комплекса:

- базовый модуль (Core)
- модуль «Анализ промышленного сетевого трафика»
- модуль «Управление проектами ПЛК»
- модуль «Управление конфигурациями»
- модуль «Управление уязвимостями»
- модуль «Управление внешними событиями»
- сервис «Swagger UI»
- сервис «Supervision Backend»

Установка модуля «EDR for PLC» приведена в следующем разделе «Установка модуля «EDR for PLC»».

3.1.4.1. Установка модулей Комплекса уровня Management

Установка модулей Комплекса уровня Management допускается только при наличии установленного базового модуля Комплекса уровня Management.

3.1.4.1.1. Установка базового модуля (Core) Комплекса уровня Management

Для установки базового модуля Комплекса уровня Management:

1. Подключитесь к Комплексу уровня Management по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:

- при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
- при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.

3. Установите базовый модуль, выполнив команду:

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

4. Измените значения переменных в конфигурационном файле `manager.env` Комплекса уровня Management. Для этого:

   а. Откройте файл `manager.env`, выполнив команду:

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

   б. Укажите IP-адрес Комплекса уровня Management в значении переменной `HOST_IP`.

   в. Рекомендуется изменить ограничения на хранение внутренних событий, изменив значения следующих переменных:

   - `EVENTS_RETENTION_DISK_CAPACITY_SIZE_MB` — максимально допустимый объем архива событий, хранящегося в модуле внутренних событий. По умолчанию ограничение отсутствует (`0`), что может привести к переполнению корневого раздела ОС. Если ограничение задано, при его достижении регистрация событий отключается;
   - `EVENTS_RETENTION_MONTHS` — период в месяцах, по истечении которого удаляются внутренние события старше срока, указанного в этой переменной.

   > Прим.:
   >
   > Подробнее о рекомендациях по использованию переменных см. в разделе «Рекомендации по использованию переменных файлов manager.env и sensor.env» Руководства по эксплуатации.

   г. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

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

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

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

   > Внимание:
   >
   > 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 файл `iptables` на Комплексе уровня Management в зависимости от места установки сенсора:

- если уровень Management и сенсор устанавливаются на разные серверы, скопируйте следующие правила в файл `iptables` на уровне Management:

```
*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

#Base
-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
```

- если уровень Management и сенсор устанавливаются на один сервер, скопируйте следующие общие правила в файл `iptables` на уровне Management:

```
*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

#Base
-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
```

Прим.:

Если необходимо выполнять вход в web-интерфейс Комплекса без обязательного ввода `https://` в адресе, можно настроить автоматическое перенаправление на HTTPS. Для этого добавьте в файл `iptables` следующее правило сразу после правила `-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT`:

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
```

Прим.:

Если к серверу уровня Management, на котором будет также установлен сенсор, планируется в дальнейшем подключать по сети другие сенсоры, добавьте в файл следующие правила сразу после строки `#Base`:

```
-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
```

Пример содержимого файла `iptables` уровня Management, на котором будет также установлен сенсор и планируется подключать по сети другие сенсоры (в случае установки на уровень Management только базового модуля):

```
*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

#Base
-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 -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. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

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

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

3.1.4.1.2. Установка модуля «Анализ промышленного сетевого трафика»

Для установки модуля «Анализ промышленного сетевого трафика»:

1. Убедитесь, что необходимые репозитории настроены. Для этого:

   а. Убедитесь, что репозитории присутствуют в системе, выполнив команду:

```
ls /var/opt/[версия_Комплекса] | grep -E '(ours|third|nta|zeek)'
```

```
[root@STREAM ~]# ls /var/opt/master | grep -E '(ours|third|nta|zeek)'
nta
ours
third
zeek
```

Рис. 69. Проверка наличия репозиториев для установки модуля «Анализ промышленного сетевого трафика»

   б. Убедитесь, что присутствующие репозитории подключены, выполнив команду:

```
apt-repo list | grep -E '(ours|third|nta|zeek)'
```

```
[root@STREAM ~]# apt-repo list | grep -E '(ours|third|nta|zeek)'
rpm file:/var/opt/master/nta noarch classic
rpm file:/var/opt/master/nta x86_64 classic
rpm file:/var/opt/master/zeek noarch classic
rpm file:/var/opt/master/zeek x86_64 classic
rpm file:/var/opt/master/ours noarch classic
rpm file:/var/opt/master/ours x86_64 classic
rpm file:/var/opt/master/third noarch classic
rpm file:/var/opt/master/third x86_64 classic
```

Рис. 70. Проверка подключенных репозиториев для установки модуля «Анализ промышленного сетевого трафика»

Внимание:

Если репозитории не подключены, настройте их путем внесения следующих строк в конфигурационный файл `/etc/apt/sources.list.d/udv.list`:

```
#Ours
rpm file:/var/opt/[версия_Комплекса]/ours noarch classic
```

```
rpm file:/var/opt/[версия_Комплекса]/ours x86_64 classic
#Third
rpm file:/var/opt/[версия_Комплекса]/third noarch classic
rpm file:/var/opt/[версия_Комплекса]/third x86_64 classic
#NTA
rpm file:/var/opt/[версия_Комплекса]/nta noarch classic
rpm file:/var/opt/[версия_Комплекса]/nta x86_64 classic
#Zeek
rpm file:/var/opt/[версия_Комплекса]/zeek noarch classic
rpm file:/var/opt/[версия_Комплекса]/zeek x86_64 classic
```

в. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:

- при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
- при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.

г. Обновите репозитории, выполнив команду:

```
apt-get update
```

2. Установите модуль «Анализ промышленного сетевого трафика», выполнив команду:

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

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

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

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

> Внимание:
>
> 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 файл `iptables` на Комплексе уровня Management в зависимости от места установки сенсора:

- если сенсор и Комплекс уровня Management устанавливаются на разные серверы, добавьте следующие правила в файл `iptables` на уровне Management сразу после правил `#Base`:

```
#NTA
-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
```

Пример итогового содержимого файла `iptables` на уровне Management для установки модуля «Анализ промышленного сетевого трафика»:

```
*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

#Base
-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

#NTA
-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 -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT
```

- если сенсор и Комплекс уровня Management устанавливаются на один сервер, оставьте в файле `iptables` на уровне Management правила такими же, как при установке модуля Core.

г. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

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

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

3.1.4.1.3. Установка модуля «Управление проектами ПЛК»

Для установки модуля «Управление проектами ПЛК»:

1. Убедитесь, что необходимые репозитории настроены. Для этого:

   а. Убедитесь, что репозитории присутствуют в системе, выполнив команду:

   ```
   ls /var/opt/[версия_Комплекса] | grep -E '(ours|third|controlversion)'
   ```

б. Убедитесь, что присутствующие репозитории подключены, выполнив команду:

```
apt-repo list | grep -E '(ours|third|controlversion)'
```

> Внимание:
>
> Если репозитории не подключены, настройте их путем внесения в конфигурационный файл `/etc/apt/sources.list.d/udv.list` следующих строк:
>
> ```
> #Ours
> rpm file:/var/opt/[версия_Комплекса]/ours noarch classic
> rpm file:/var/opt/[версия_Комплекса]/ours x86_64 classic
> #Third
> rpm file:/var/opt/[версия_Комплекса]/third noarch classic
> rpm file:/var/opt/[версия_Комплекса]/third x86_64 classic
> #CV
> rpm file:/var/opt/[версия_Комплекса]/controlversion noarch classic
> rpm file:/var/opt/[версия_Комплекса]/controlversion x86_64 classic
> ```

в. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:

- при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
- при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.

г. Обновите репозитории, выполнив команду:

```
apt-get update
```

2. Установите модуль «Управление проектами ПЛК», выполнив команду:

```
apt-get install udv-control-version -y
```

3.1.4.1.4. Установка модуля «Управление конфигурациями»

Для установки модуля «Управление конфигурациями»:

1. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:
   - при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
   - при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.
2. Установите модуль «Управление конфигурациями», выполнив команду:

```
apt-get install udv-datapk-configuration-management -y
```

3.1.4.1.5. Установка модуля «Управление уязвимостями»

Перед выполнением:

> Внимание:
>
> Перед установкой модуля «Управление уязвимостями» убедитесь, что установлен модуль «Управление конфигурациями».

Для установки модуля «Управление уязвимостями»:

1. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:
   - при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
   - при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.
2. Установите модуль «Управление уязвимостями», выполнив команду:

```
apt-get install udv-datapk-vulnerability-management -y
```

3.1.4.1.6. Установка модуля «Управление внешними событиями»

Для установки модуля «Управление внешними событиями»:

1. Убедитесь, что необходимые репозитории настроены. Для этого:

   а. Убедитесь, что репозитории присутствуют в системе, выполнив команду:

   ```
   ls /var/opt/[версия_Комплекса] | grep -E '(ours|third|tools)'
   ```

   б. Убедитесь, что присутствующие репозитории подключены, выполнив команду:

   ```
   apt-repo list | grep -E '(ours|third|tools)'
   ```

   > Внимание:
   >
   > Если репозитории не подключены, настройте их путем внесения в конфигурационный файл `/etc/apt/sources.list.d/udv.list` следующих строк:
   >
   > ```
   > #Ours
   > rpm file:/var/opt/[версия_Комплекса]/ours noarch classic
   > rpm file:/var/opt/[версия_Комплекса]/ours x86_64 classic
   > #Third
   > rpm file:/var/opt/[версия_Комплекса]/third noarch classic
   > rpm file:/var/opt/[версия_Комплекса]/third x86_64 classic
   > #Tools
   > rpm file:/var/opt/[версия_Комплекса]/tools noarch classic
   > rpm file:/var/opt/[версия_Комплекса]/tools x86_64 classic
   > ```

в. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:

- при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
- при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.

г. Обновите репозитории, выполнив команду:

```
apt-get update
```

2. Установите модуль «Управление внешними событиями», выполнив команду:

```
apt-get install udv-external-events-system -y
```

3.1.4.1.7. Установка сервиса «Swagger UI»

Для установки сервиса «Swagger UI»:

1. Убедитесь, что необходимые репозитории настроены. Для этого:

а. Убедитесь, что репозитории присутствуют в системе, выполнив команду:

```
ls /var/opt/[версия_Комплекса] | grep -E '(ours|third|tools)'
```

б. Убедитесь, что присутствующие репозитории подключены, выполнив команду:

```
apt-repo list | grep -E '(ours|third|tools)'
```

Внимание:

Если репозитории не подключены, настройте их путем внесения в конфигурационный файл `/etc/apt/sources.list.d/udv.list` следующих строк:

```
#Ours
rpm file:/var/opt/[версия_Комплекса]/ours noarch classic
rpm file:/var/opt/[версия_Комплекса]/ours x86_64 classic
#Third
rpm file:/var/opt/[версия_Комплекса]/third noarch classic
rpm file:/var/opt/[версия_Комплекса]/third x86_64 classic
#Tools
rpm file:/var/opt/[версия_Комплекса]/tools noarch classic
rpm file:/var/opt/[версия_Комплекса]/tools x86_64 classic
```

в. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:

- при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
- при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.

г. Обновите репозитории, выполнив команду:

```
apt-get update
```

2. Установите сервис «Swagger UI», выполнив команду:

```
apt-get install udv-swagger-ui -y
```

▸ **Результат шага:** После запуска Комплекса сервис «Swagger UI» доступен по адресу: `https://[IP-адрес Комплекса]/api/`

3.1.4.1.8. Установка модуля «Supervision Backend»

Для установки модуля «Supervision Backend»:

1. Убедитесь, что необходимые репозитории настроены. Для этого:

а. Убедитесь, что репозитории присутствуют в системе, выполнив команду:

```
ls /var/opt/[версия_Комплекса] | grep -E '(ours|third|tools)'
```

б. Убедитесь, что присутствующие репозитории подключены, выполнив команду:

```
apt-repo list | grep -E '(ours|third|tools)'
```

> Внимание:
>
> Если репозитории не подключены, настройте их путем внесения в конфигурационный файл `/etc/apt/sources.list.d/udv.list` следующих строк:
>
> ```
> #Ours
> rpm file:/var/opt/[версия_Комплекса]/ours noarch classic
> rpm file:/var/opt/[версия_Комплекса]/ours x86_64 classic
> #Third
> rpm file:/var/opt/[версия_Комплекса]/third noarch classic
> rpm file:/var/opt/[версия_Комплекса]/third x86_64 classic
> #Tools
> rpm file:/var/opt/[версия_Комплекса]/tools noarch classic
> rpm file:/var/opt/[версия_Комплекса]/tools x86_64 classic
> ```

в. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:

- при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
- при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.

г. Обновите репозитории, выполнив команду:

```
apt-get update
```

2. Установите модуль «Supervision Backend», выполнив команду:

```
apt-get install udv-supervision-backend -y
```

3.1.4.2. Установка модулей Комплекса уровня Sensor

Установка модулей Комплекса уровня Sensor (сенсора) допускается только при наличии установленного базового модуля (Core) Комплекса уровня Sensor.

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

3.1.4.2.1. Установка базового модуля (Core) Комплекса уровня Sensor

Для установки базового модуля сенсора:

1. Если сенсор будет устанавливаться на сервер, отдельный от Комплекса уровня Management, подключитесь к сенсору по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:
   - при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
   - при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.
3. Установите базовый модуль, выполнив команду:

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

4. Откройте файл `sensor.env` сенсора, выполнив команду:

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

5. Укажите IP-адрес Комплекса уровня Management в значении переменной `MANAGER_NODE_ADDRESS`.

> Прим.:
>
> Если Комплекс уровня Management и сенсор устанавливаются на один сервер, переменной `MANAGER_NODE_ADDRESS` необходимо оставить значение `127.0.0.1`.

6. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.
7. Если Комплекс уровня Management и сенсор устанавливаются на разные серверы, настройте межсетевой экран `iptables` на сенсоре. Для этого:

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

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

   > Внимание:
   >
   > Значение параметра `CONFIG_FW` должно быть `no`.

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

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

   в. Скопируйте следующие правила межсетевого экрана в файл `iptables` на сенсоре:

   ```
   *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

   #Base
   -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. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

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

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

3.1.4.2.2. Установка модуля «Анализ промышленного сетевого трафика» Комплекса уровня Sensor

Для установки модуля «Анализ промышленного сетевого трафика» сенсора:

1. Убедитесь, что необходимые репозитории настроены. Для этого:

   а. Убедитесь, что репозитории присутствуют в системе, выполнив команду:

   ```
   ls /var/opt/[версия_Комплекса] | grep -E '(ours|third|nta|zeek)'
   ```

   б. Убедитесь, что присутствующие репозитории подключены, выполнив команду:

   ```
   apt-repo list | grep -E '(ours|third|nta|zeek)'
   ```

   Внимание:

   Если репозитории не подключены, настройте их путем внесения в конфигурационный файл `/etc/apt/sources.list.d/udv.list` следующих строк:

   ```
   #Ours
   rpm file:/var/opt/[версия_Комплекса]/ours noarch classic
   rpm file:/var/opt/[версия_Комплекса]/ours x86_64 classic
   #Third
   rpm file:/var/opt/[версия_Комплекса]/third noarch classic
   rpm file:/var/opt/[версия_Комплекса]/third x86_64 classic
   #NTA
   rpm file:/var/opt/[версия_Комплекса]/nta noarch classic
   rpm file:/var/opt/[версия_Комплекса]/nta x86_64 classic
   #Zeek
   rpm file:/var/opt/[версия_Комплекса]/zeek noarch classic
   rpm file:/var/opt/[версия_Комплекса]/zeek x86_64 classic
   ```

   в. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:

   - при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
   - при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.

   г. Обновите репозитории, выполнив команду:

   ```
   apt-get update
   ```

2. Установите модуль «Анализ промышленного сетевого трафика», выполнив команду:

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

3. Настройте сетевой интерфейс для прослушивания сетевого трафика. Для этого:

а. Просмотрите название интерфейса для прослушивания трафика по команде:

```
ip a
```

> Прим.:
>
> Интерфейс для прослушивания трафика не будет иметь назначенного IP-адреса.

б. Если отсутствует, создайте директорию с наименованием сетевого интерфейса, выполнив команду:

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

> Прим.:
>
> Название интерфейса `ens224` приведено в качестве примера.

в. Скопируйте в созданную директорию `ens224` конфигурационный файл `options` уже существующего сетевого интерфейса управления, настроенного при установке ОС, выполнив команду:

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

> Прим.:
>
> Названия интерфейсов `ens192` и `ens224` приведены в качестве примера.

г. 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
```

> Прим.:
>
> Название интерфейса `ens224` приведено в качестве примера.

д. Перезагрузите сетевой сервис, выполнив команду:

```
systemctl restart network
```

- **Результат шага:** сетевой интерфейс для прослушивания (анализа) трафика переключен в режим прослушивания всех пакетов.

4. Если необходимо анализировать трафик с нескольких интерфейсов сенсора, повторите шаг 3 для других прослушивающих интерфейсов сенсора.

> Внимание:
>
> Если необходимо анализировать трафик с нескольких интерфейсов, создайте единый виртуальный интерфейс (bond). Подробнее об этом см. в разделе «Создание единого виртуального интерфейса (bond) для прослушивания и записи трафика с нескольких физических интерфейсов».

5. Откройте файл `sensor.env`, выполнив команду:

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

6. Укажите через запятую наименования сетевых интерфейсов для прослушивания сетевого трафика в переменной `LISTENING_INTERFACES`.

> Внимание:
>
> Запись трафика в файлы `.pcap` модулем «Анализ промышленного сетевого трафика» будет доступна только для первого интерфейса из перечисленных в переменной `LISTENING_INTERFACES`. Если необходимо записывать трафик с нескольких интерфейсов, создайте для них единый виртуальный интерфейс (bond).

7. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

3.1.4.3. Установка модуля «EDR for PLC»

Для установки модуля UDV DATAPK EDR for PLC последовательно выполните следующие инструкции:

1. Установка модуля «EDR for PLC» в Комплексе уровня Management
2. Установка модуля «EDR for PLC» в Комплексе уровня Sensor

3.1.4.3.1. Файлы, необходимые для установки модуля «EDR for PLC»

> Внимание:
>
> Перед установкой модуля UDV DATAPK EDR for PLC обязательно должны быть установлены модули «Анализ промышленного сетевого трафика» и «Управление внешними событиями».

1. Актуальный сертифицированный дистрибутив ОС Альт Сервер 10.2 SP.

> Внимание:
>
> В данном Руководстве по внедрению и поддержке описана установка ОС Альт Сервер 10.2 SP с использованием дистрибутива `alt-sp-server-20241127-x86_64.iso`.

2. Установочный архив `agentless_edr-[версия]_[дата].tar.gz` с образами модуля UDV DATAPK EDR for PLC.

3.1.4.3.2. Установка модуля «EDR for PLC» в Комплексе уровня Sensor

Перед выполнением:

> Внимание:
>
> Данную инструкцию необходимо выполнить в случае, если сенсор устанавливается на сервер, отдельный от Комплекса уровня Management.

Перед началом установки убедитесь в следующем:

1. Ранее на сенсоре был установлен модуль «Анализ промышленного сетевого трафика», необходимый для функционирования модуля UDV DATAPK EDR for PLC.

   > Прим.:
   >
   > Для того, чтобы проверить, что модуль «Анализ промышленного сетевого трафика» установлен и запущен (имеет статус `active`), выполните команду:
   >
   > ```
   > systemctl list-units 'udv-*' --all
   > ```
   >
   > Список сервисов модуля «Анализ промышленного сетевого трафика» см. в разделе «Состав модулей Комплекса в сервисах».

2. Ранее на сенсоре не устанавливался модуль UDV DATAPK EDR for PLC.

   > Прим.:
   >
   > Проверьте, установлены ли сервисы UDV DATAPK EDR for PLC для сенсора, с помощью команд:
   >
   > ```
   > systemctl list-units udv-agentless-edr* --all
   > podman ps | grep thymus_controller
   > ```

3. Подготовлены необходимые для установки файлы, приведенные в разделе «Файлы, необходимые для установки модуля «EDR for PLC»».

Для установки модуля UDV DATAPK EDR for PLC на уровень Sensor, если ранее он не был установлен:

1. Если сенсор будет устанавливаться на сервер, отдельный от Комплекса уровня Management, подключитесь к сенсору по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. Примонтируйте диск с дистрибутивом Комплекса, либо с помощью приложения для обмена файлами по протоколу SFTP (или аналогичным способом по сети) скопируйте установочный архив модуля UDV DATAPK EDR for PLC `agentless_edr-[версия]_[дата].tar.gz` в директорию `/home/user` операционной системы.
3. Создайте директорию `/tmp/thymus`, выполнив команду:

   ```
   mkdir -p /tmp/thymus
   ```

4. Распакуйте установочный архив в директорию `/tmp/thymus`, выполнив команду:

```
tar -xvzf /home/user/agentless_edr-[версия]_[дата].tar.gz -C /tmp/thymus
```

5. Переместите скрипт установки модуля в директорию `/opt`, выполнив команду:

```
mv /tmp/thymus/thymus_deploy.sh /opt
```

6. Установите права на выполнение для скрипта установки, выполнив команду:

```
chmod +x /opt/thymus_deploy.sh
```

7. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:
   - при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
   - при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.
8. Запустите скрипт с ключами в зависимости от типа установленного Комплекса:
   - Если Комплекс уровня Management и Комплекс уровня Sensor установлены на один сервер:

     ```
     /opt/thymus_deploy.sh -i /tmp/thymus/agentless-edr.tar.gz
     ```

   - Если на текущем сервере установлен только Комплекс уровня Management:

     ```
     /opt/thymus_deploy.sh -mi /tmp/thymus/agentless-edr.tar.gz
     ```

   - Если в текущей ОС установлен только Комплекс уровня Sensor:

     ```
     /opt/thymus_deploy.sh -si /tmp/thymus/agentless-edr.tar.gz
     ```

9. Перезагрузите Комплекс командой:

```
shutdown -r now
```

См. также

Конфигурационные файлы модуля «EDR for PLC»

3.1.4.3.3. Установка модуля «EDR for PLC» в Комплексе уровня Management

Перед выполнением:

Перед началом установки убедитесь в следующем:

1. Выполнена инструкция «Установка модуля «EDR for PLC» в Комплексе уровня Sensor» в случае, если Комплекс уровня Management устанавливается на сервер, отдельный от сенсора.
2. Ранее на Комплексе уровня Management были установлены модули «Анализ промышленного сетевого трафика» и «Управление внешними событиями», необходимые для функционирования модуля UDV DATAPK EDR for PLC.

> Прим.:
>
> Для того, чтобы проверить, что эти модули установлены и запущены (имеют статус `active`), выполните команду:

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

Список сервисов модулей «Анализ промышленного сетевого трафика» и «Управление внешними событиями» см. в разделе «Состав модулей Комплекса в сервисах».

3. Ранее на уровень Management с сенсором, установленным на том же сервере, не устанавливался модуль UDV DATAPK EDR for PLC.

> Прим.:
>
> Проверьте, установлены ли сервисы UDV DATAPK EDR for PLC для сенсора, с помощью команд:
>
> ```
> systemctl list-units udv-agentless-edr* --all
> podman ps | grep thymus_controller
> ```

4. Подготовлены необходимые для установки файлы, приведенные в разделе «Файлы, необходимые для установки модуля «EDR for PLC»».

Для установки модуля UDV DATAPK EDR for PLC на уровень Management, если ранее он не был установлен:

1. Подключитесь к Комплексу уровня Management по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. Примонтируйте диск с дистрибутивом Комплекса, либо с помощью приложения для обмена файлами по протоколу SFTP (или аналогичным способом по сети) скопируйте установочный архив модуля UDV DATAPK EDR for PLC `agentless_edr-[версия]_[дата].tar.gz` в директорию `/home/user` операционной системы.
3. Создайте директорию `/tmp/thymus`, выполнив команду:

   ```
   mkdir -p /tmp/thymus
   ```

4. Распакуйте установочный архив в директорию `/tmp/thymus`, выполнив команду:

   ```
   tar -xvzf /home/user/agentless_edr-[версия]_[дата].tar.gz -C /tmp/thymus
   ```

5. Переместите скрипт установки модуля в директорию `/opt`, выполнив команду:

   ```
   mv /tmp/thymus/thymus_deploy.sh /opt
   ```

6. Установите права на выполнение для скрипта установки, выполнив команду:

   ```
   chmod +x /opt/thymus_deploy.sh
   ```

7. В зависимости от наличия доступа в сеть Интернет убедитесь, что репозитории ОС Альт Сервер подключены одним из следующих способов:
   - при наличии доступа в сеть Интернет убедитесь, что уже настроен конфигурационный файл `/etc/apt/sources.list.d/altsp.list` со ссылками на репозитории ОС Альт Сервер согласно шагу 6.а инструкции «Подключение репозиториев Комплекса»;
   - при отсутствии доступа в сеть Интернет убедитесь, что к серверу, на который устанавливается Комплекс, подключен ISO-образ или оптический диск ОС Альт Сервер.
8. Запустите скрипт, выполнив команду:

- Если Комплекс уровня Management и Комплекс уровня Sensor устанавливаются на один сервер:

```
/opt/thymus_deploy.sh -i /tmp/thymus/agentless-edr.tar.gz
```

- Если на текущий сервер устанавливается только Комплекс уровня Management:

```
/opt/thymus_deploy.sh -mi /tmp/thymus/agentless-edr.tar.gz
```

См. также

Конфигурационные файлы модуля «EDR for PLC»

3.1.4.3.4. Установка службы adminer

> Внимание:
>
> Установка службы `udv-agentless-edr-adminer` не является обязательной, поскольку данная служба является функциональной и может быть запущена вручную в особых случаях (например, при проведении пуско-наладочных работ).
>
> Файл службы `udv-agentless-edr-adminer` настроен таким образом, чтобы автозапуск службы не выполнялся. При необходимости сервис нужно запускать вручную. Поэтому правило межсетевого экранирования для порта 8080 временное и создается только для текущего сеанса.

Для установки `adminer`:

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

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

2. Добавьте правила для работы `adminer` в файл:

```
-A INPUT -p tcp -m tcp --dport 8080 -j ACCEPT
```

3. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.
4. Выполните перезапуск службы `iptables`:

```
systemctl restart iptables
```

5. Запустите `adminer` командой:

```
systemctl start udv-agentless-edr-adminer.service
```

3.1.4.4. Запуск Комплекса

Инструкция предназначена для запуска сервисов Комплекса уровня Management и уровня Sensor (сенсора), установленных как на одном сервере, так и на разных. Для запуска на разных серверах рекомендуется сначала запустить сервисы уровня Management, а затем сервисы всех сенсоров, которые настроены на подключение к этому уровню Management.

Для запуска сервисов Комплекса:

1. Убедитесь, что на Комплексе уровня Management и подключаемых к нему сенсорах задан уникальный идентификатор машины в файле `/etc/machine-id`

   > Прим.:
   >
   > Для изменения `machine-id` см. раздел дополнительных настроек «Изменение machine-id».

2. Перезапустите ОС, выполнив команду:

   ```
   shutdown -r now
   ```

   > Прим.:
   >
   > В случае, если изменения вносились только в конфигурационные файлы, перезапустите только сервисы Комплекса командой:
   >
   > ```
   > systemctl restart udv-* --all
   > ```

3. После запуска ОС или сервисов подождите несколько минут и убедитесь, что все сервисы Комплекса запущены (имеют статус `active`), выполнив команду:

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

   > Прим.:
   >
   > Сервисы `udv-event-correlator.service` (при наличии модуля «Управление внешними событиями» в комплекте поставки) и `udv-sensor-registrar.service` могут штатно находиться в состоянии `inactive (dead)`, так как их запуск выполняется по необходимости в процессе работы Комплекса.

Что дальше: Выполните данную инструкцию для каждого сенсора, если они установлены на других серверах отдельно от уровня Management.

3.1.5. Установка дополнительных утилит

Для работы Комплекса может потребоваться установка следующих дополнительных утилит:

- `snmpwalk`;
- `Zabbix`;
- `ssh1`;
- `winexe`.

Для установки этих утилит выполните следующие инструкции:

- Установка утилиты snmpwalk
- Установка агента Zabbix
- Установка утилит ssh1 и winexe

3.1.5.1. Установка утилиты snmpwalk

Утилита `snmpwalk` предназначена для опроса SNMP-устройств при мониторинге сетевого оборудования.

Перед выполнением:

Перед установкой убедитесь, что подключен репозиторий сертифицированной ОС Альт Сервер. Подробнее о подключении репозитория см. в шагах 2 или 3 раздела «Настройка сертифицированной ОС Альт Сервер 10.2 SP» (в зависимости от наличия или отсутствия доступа в сеть Интернет).

Установить `snmpwalk` можно на любой компонент: сенсор или Комплекс уровня Management.

1. Подключитесь к сенсору или Комплексу уровня Management, на который нужно установить `snmpwalk`, по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора.
2. Выполните команду для установки утилиты `snmpwalk`:

```
apt-get install net-snmp-clients
```

3.1.5.2. Установка агента Zabbix

Агент `Zabbix` предназначен для сбора показателей с узлов (CPU, память, диски), на которых он установлен, и отправки собранных данных на сервер. Позволяет контролировать состояние серверов и сетевых устройств в реальном времени.

> Прим.:
>
> На Комплекс возможна установка простого или продвинутого агента `Zabbix`.
>
> Установить `Zabbix` можно на любой компонент: сенсор или Комплекс уровня Management.

3.1.5.2.1. Установка простого агента Zabbix

Перед выполнением:

Перед установкой убедитесь, что подключен репозиторий сертифицированной ОС Альт Сервер. Подробнее о подключении репозитория см. в шагах 2 или 3 раздела «Настройка сертифицированной ОС Альт Сервер 10.2 SP» (в зависимости от наличия или отсутствия доступа в сеть Интернет).

Для установки простого агента `Zabbix`:

1. Подключитесь к сенсору или Комплексу уровня Management, на который нужно установить `Zabbix`, по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора.
2. Установите простой агент `Zabbix`, выполнив команду:

```
apt-get install zabbix-agent
```

3. Активируйте и запустите агент, выполнив команду:

```
systemctl enable --now zabbix_agentd.service
```

3.1.5.2.2. Установка продвинутого агента Zabbix

Перед выполнением: Перед установкой убедитесь, что подключен онлайн-репозиторий сертифицированной ОС Альт Сервер.При установке продвинутого агента `Zabbix` при отсутствии Интернет-соединения подготовьте

пакеты `zabbix-agent-sudo`, `zabbix-agent2` и `zabbix-common`. Подробнее об этом см. в разделе «Настройка сертифицированной ОС Альт Сервер 10.2 SP».

Для установки продвинутого агента `Zabbix`:

1. Подключитесь к сенсору или Комплексу уровня Management, на который нужно установить `Zabbix`, по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора.
2. Установите продвинутый агент `Zabbix`, выполнив команду:

   ```
   apt-get install zabbix-agent2
   ```

3. Активируйте и запустите агент, выполнив команду:

   ```
   systemctl enable --now zabbix_agent2.service
   ```

3.1.5.3. Установка утилит ssh1 и winexe

Утилита `ssh1` требуется для подключения к удаленным устройствам по протоколу SSH-1, а утилита `winexe` необходима для выполнения команд на удаленных Windows-устройствах.

> Прим.:
>
> Для поддержки данных утилит необходимо установить пакет `udv-terminal-connector-old-protocols` на Комплексе уровня Sensor.

Перед выполнением:

Перед установкой утилит убедитесь, что необходимые репозитории подключены, выполнив команду `apt-repo list | grep -E '(ours|third|tools)'`

Для установки утилит `ssh1` и `winexe`:

1. Если сенсор будет устанавливаться на сервер, отдельный от Комплекса уровня Management, подключитесь к сенсору по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. Выполните команду для установки утилит:

   ```
   apt-get install udv-terminal-connector-old-protocols
   ```

3.2. Первичное подключение

В этом разделе:

- Подключение к веб-интерфейсу по протоколу HTTPS
- Первоначальная настройка

Порядок включения аппаратной платформы установленного Комплекса для выполнения первичной настройки:

1. Соедините сетевым кабелем разъем управляющего контура Комплекса с разъемом сетевой карты рабочей станции администратора.
2. Один конец кабеля питания вставьте в разъем питания Комплекса, другой – в заземленную сетевую розетку.
3. Включите Комплекс. Для этого кратковременно нажмите кнопку питания. Комплекс издаст одиночный звуковой сигнал, запустится операционная система, системное и прикладное ПО.

3.2.1. Подключение к веб-интерфейсу по протоколу HTTPS

Для подключения к веб-интерфейсу Комплекса по протоколу HTTPS:

1. Проверьте возможность подключения к UDV DATAPK уровня Management по протоколу HTTPS. Для этого:
    a. Откройте веб-браузер на клиентском компьютере.
    б. Введите адрес для подключения в веб-интерфейсу в формате `https://[IP-адрес]`, где `[IP-адрес]` — IP-адрес интерфейса управления Комплекса уровня Management.

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

Рис. 71. Окно входа в веб-интерфейс Комплекса

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

a. Нажмите кнопку **Дополнительные**.

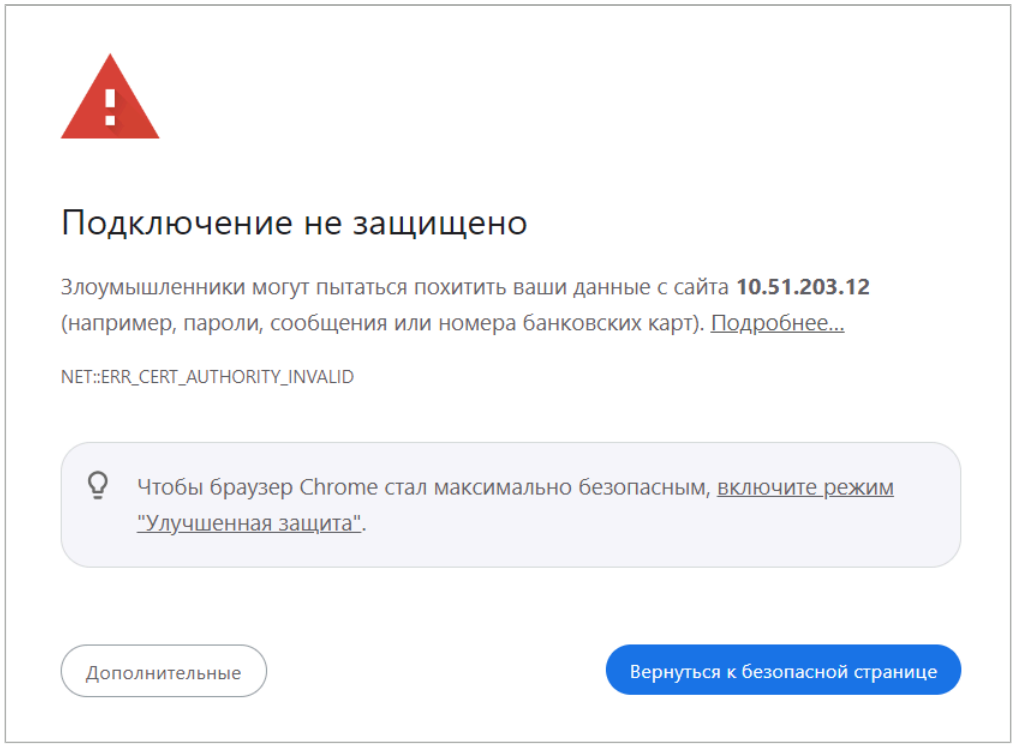


Рис. 72. Окно предупреждения о незащищенном подключении

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

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

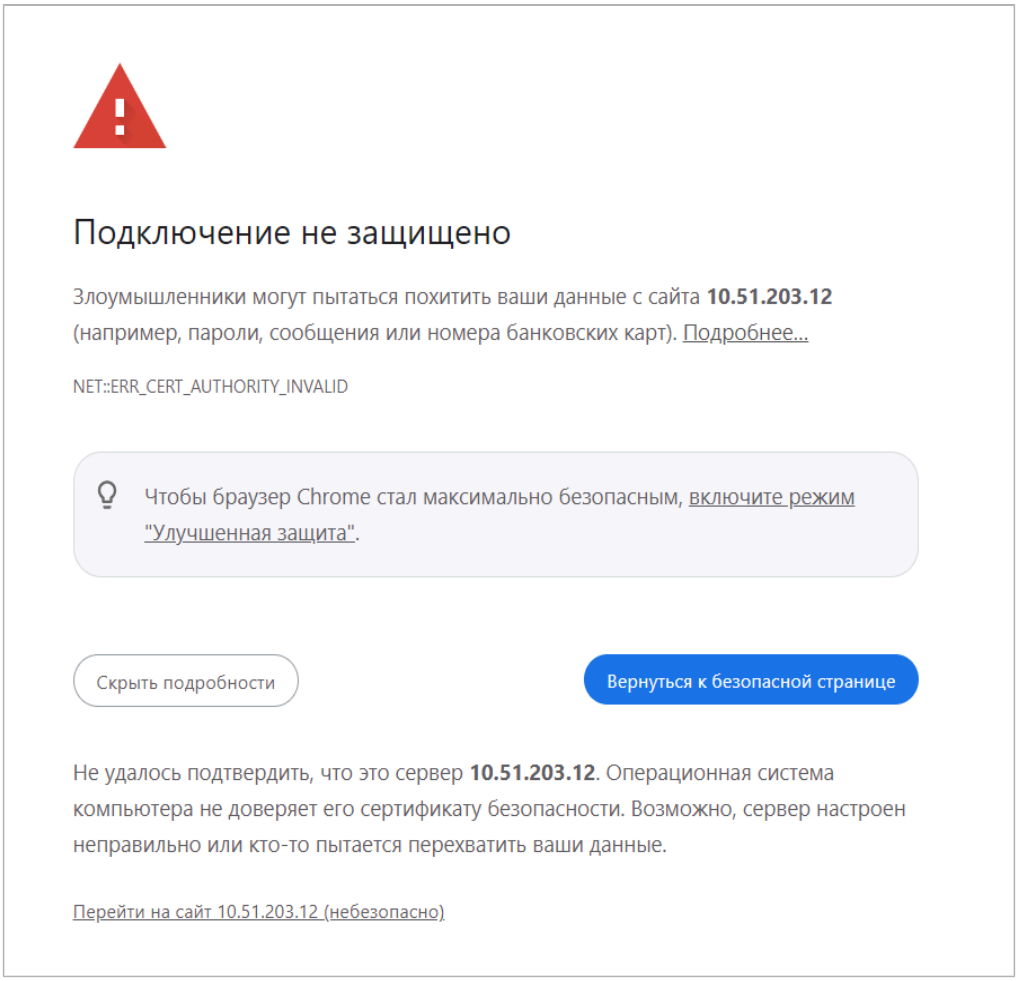


Рис. 73. Подключение к ПК UDV DATAPK по HTTPS

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

3. Введите в поля окна входа предустановленное для первичной настройки Комплекса имя пользователя (логин): `datapk` и пароль: `datapk`. Нажмите кнопку **Войти**.

> Внимание:
>
> Количество неудачных попыток ввода пароля по умолчанию равно 3.
>
> По умолчанию при превышении неудачных попыток ввода пароля учетная запись блокируется на 600 секунд (10 минут).

Количество неудачных попыток и время блокировки регулируются администратором на странице **Парольная политика**.

Внимание:

Сеанс доступа к веб-интерфейсу Комплекса автоматически завершается по истечении периода времени, заданного в переменной `USER_SESSION_INACTIVITY_TIMEOUT` в файле `manager.env`. По умолчанию значение переменной составляет 600 секунд (10 минут).

См. также

Настройка парольной политики

3.2.2. Первоначальная настройка

При первом входе в веб-интерфейс Комплекса вам будет предложено произвести первоначальную настройку.

Подсказка:

Обязательными шагами являются только принятие лицензионного соглашения и создание пользователя. Остальные настройки можно выполнить позже.

Для настройки:

1. Ознакомьтесь с условиями лицензионного соглашения. В случае согласия с условиями лицензионного соглашения установите чекбокс **Принимаю условия лицензионного соглашения** и нажмите кнопку **Далее**.

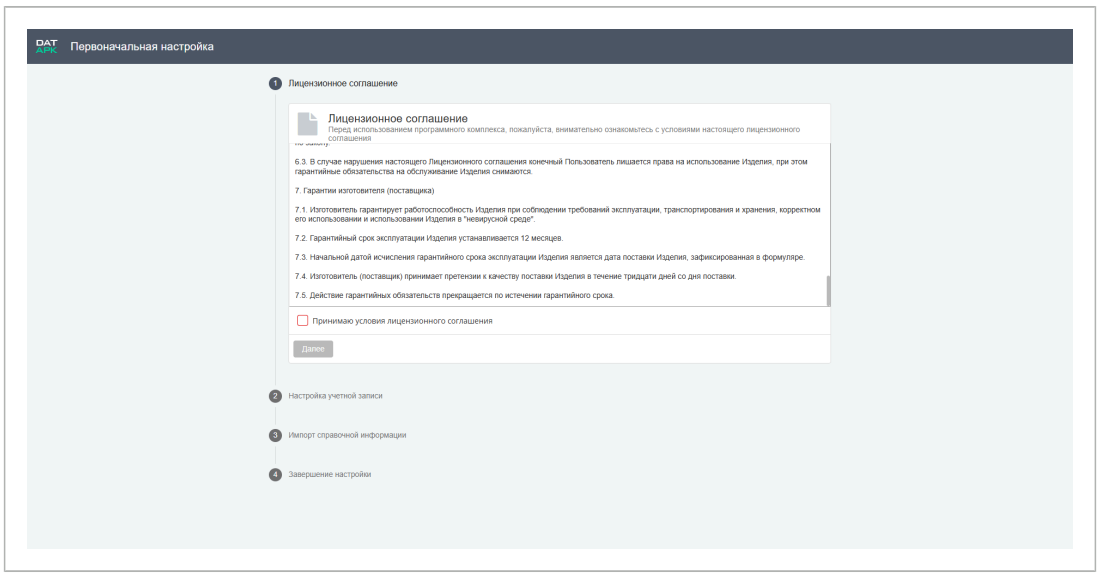


Рис. 74. Окно «Лицензионное соглашение» при выполнении первоначальной настройки

- **Результат шага:** появится окно **Настройка учетной записи**.

2. Настройте предустановленную учетную запись администратора Комплекса. Для этого:

a. В окне **Настройка учетной записи** введите следующие параметры:

- введите новый логин в поле **Логин**;
- пароль учетной записи и его подтверждение в полях **Новый пароль** и **Подтверждение нового пароля**;

> Внимание:
>
> Пароль не должен содержать старый или новый логин учетной записи, должен состоять не менее, чем из 6 символов, содержать не менее одной буквы и числа. После завершения настройки парольную политику можно изменить на странице **Администрирование** → **Пользователи** → **Пользователи** → **Парольная политика**.

- фамилию, имя и отчество пользователя учетной записи в соответствующих полях.

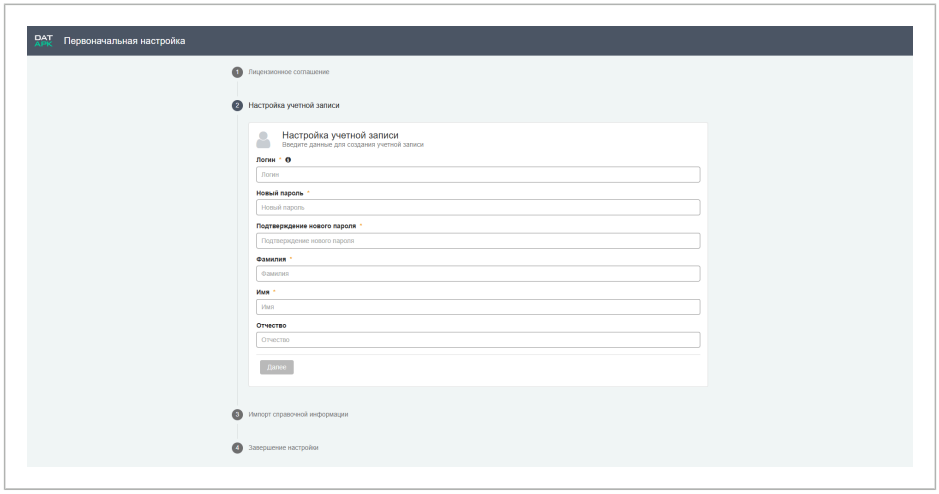


Рис. 75. Окно «Настройка учетной записи»

б. Нажмите кнопку **Далее** для сохранения данных и перехода к следующему шагу.

▸ **Результат шага:** появится окно **Импорт справочников.**

3. Импортируйте справочники. Для этого:

a. Нажмите кнопку **Выбрать файл**.

б. Выберите архив формата `.tar`, содержащий справочники, и нажмите кнопку **Открыть**.

> Подсказка:
>
> Если результат импорта вас не устраивает или файл был выбран ошибочно, то можно сразу отменить импорт, нажав кнопку **Сбросить**.

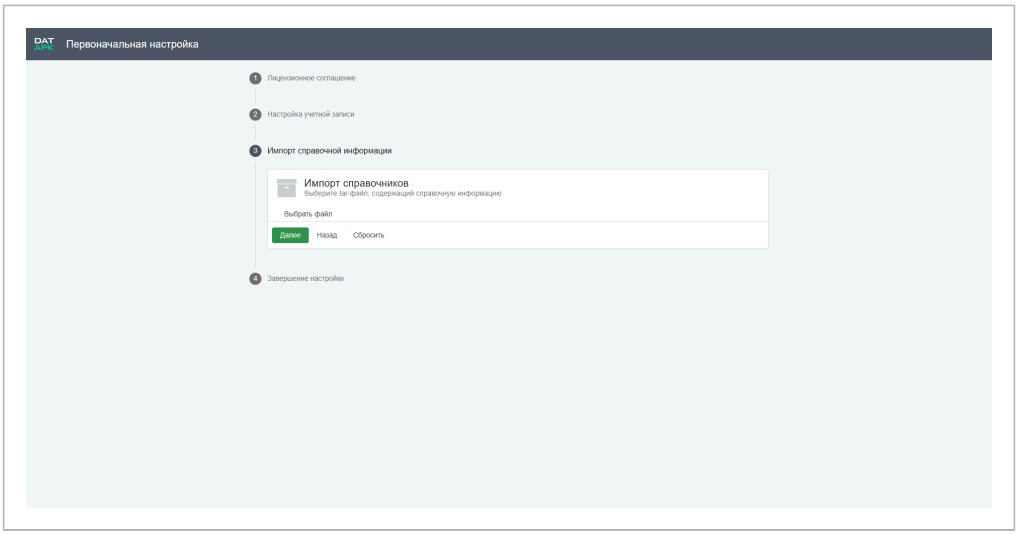


Рис. 76. Окно «Импорт справочников»

в. Нажмите кнопку **Далее** для сохранения данных и перехода к следующему этапу.

4. Если необходимая начальная настройка выполнена, нажмите кнопку **Завершить**.

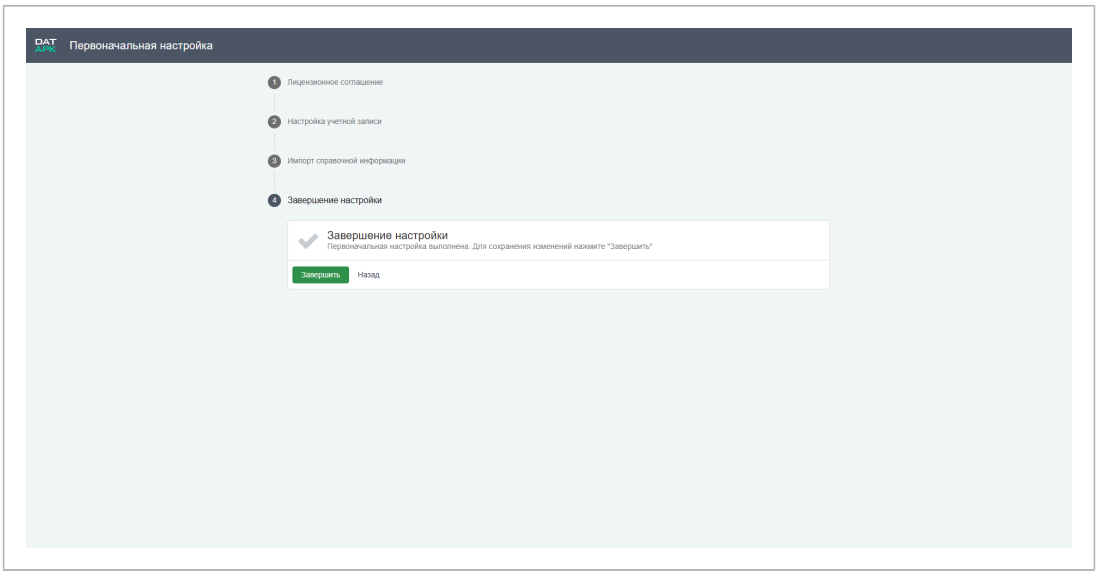


Рис. 77. Окно «Завершение настройки»

5. Войдите в веб-интерфейс Комплекса с новым логином и паролем.

6. Если в правом верхнем углу отобразится ошибка: `Непредвиденная ошибка. Перезапустить синхронизацию`, нажмите на ссылку **Перезапустить синхронизацию** для перезапуска синхронизации сенсоров с Комплексом.

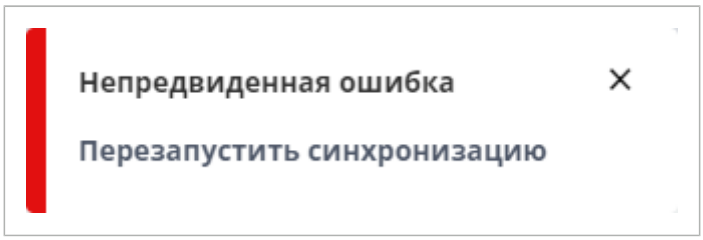


Рис. 78. Ошибка синхронизации сенсоров с Комплексом

3.3. Установка Version Control Desktop App

> Внимание:
>
> Для корректной работы Version Control Desktop App установка приложения должна производиться пользователем с правами администратора.
> Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:
>
> ```
> git config --global core.autocrlf false
> ```

Для установки Version Control Desktop App на ОС Windows 7 SP1 используйте инструкцию Установка Version Control Desktop App на ОС Windows 7 SP1.

Для установки Version Control Desktop App на более новые версии ОС Windows используйте инструкцию Установка Version Control Desktop App на ОС Windows новее 7.

Для установки Version Control Desktop App на ОС Astra Linux используйте подходящую инструкцию:

- Установка Version Control Desktop App на ОС Astra Linux 1.7
- Установка Version Control Desktop App на ОС Astra Linux 1.8

Для установки Version Control Desktop App на ОС РЕД ОС используйте подходящую инструкцию:

- Установка Version Control Desktop App на ОС РЕД ОС 7.3
- Установка Version Control Desktop App на ОС РЕД ОС 8

3.3.1. Установка Version Control Desktop App на ОС Windows 7 SP1

1. Перенесите следующие файлы и каталоги на ОС Windows 7 SP1:
   - `vc_redist.[разрядность ОС].exe`;
   - `windows6.1-kb4474419-v3-[разрядность ОС]_b5614c6cea5cb4e198717789633dca16308ef79c`;
   - `Git-2.45.1-[разрядность ОС]-bit.exe`;
   - `VersionControl.Installer.Windows-[разрядность ОС]-[номер версии Version Control]-[дата релиза версии].msi`.

> Прим.:
>
> Выберите файлы с подходящей разрядностью ОС.

2. Установите `Автономный установщик обновлений Windows`:

    a. Запустите файл `vc_redist.x[разрядность ОС].exe`.

    - **Результат шага:** Откроется окно установки установщика обновлений.

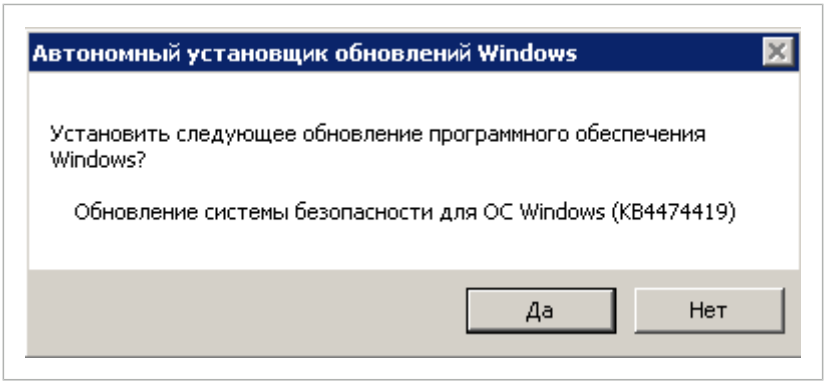


Рис. 79. Окно установки установщика обновлений

    б. Нажмите кнопку **Да**.

    в. После завершения установки нажмите кнопку **Перезагрузить сейчас**.

3. Установите `Microsoft Visual C++`:

    a. Запустите файл `windows6.1-kb4474419-v3-x[разрядность ОС]_b5614c6cea5cb4e198717789633dca16308ef79c`.

    - **Результат шага:** Откроется окно установки `Microsoft Visual C++`.

    б. Установите чекбокс **Я принимаю условия лицензии**.

    в. Нажмите кнопку **Установить**.

    г. После завершения установки нажмите кнопку **Закрыть**.

4. Установите Git-клиент:

> Внимание:
>
> Установка Git-клиента должна выполняться только пользователем с правами администратора.

    a. Запустите файл `Git-2.45.1-[разрядность ОС]-bit.exe`.

    - **Результат шага:** Откроется окно установки.

    б. Нажмите кнопку **Next**.

    в. Выберите место установки и нажмите кнопку **Next**.

г. Установите чекбоксы как на рисунке:

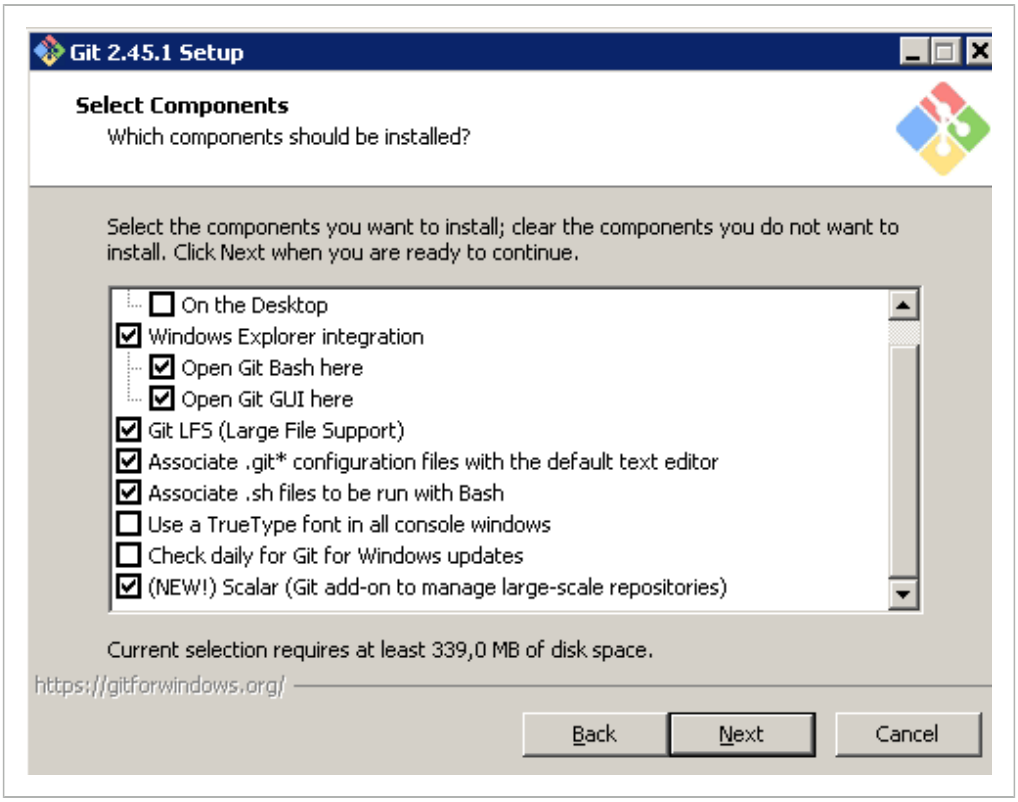


Рис. 80. Выбор чекбоксов

д. Нажмите кнопку **Next**.

е. Нажимайте кнопку **Next** на всех следующих страницах, пока не откроется страница `Configuring experimental options`.

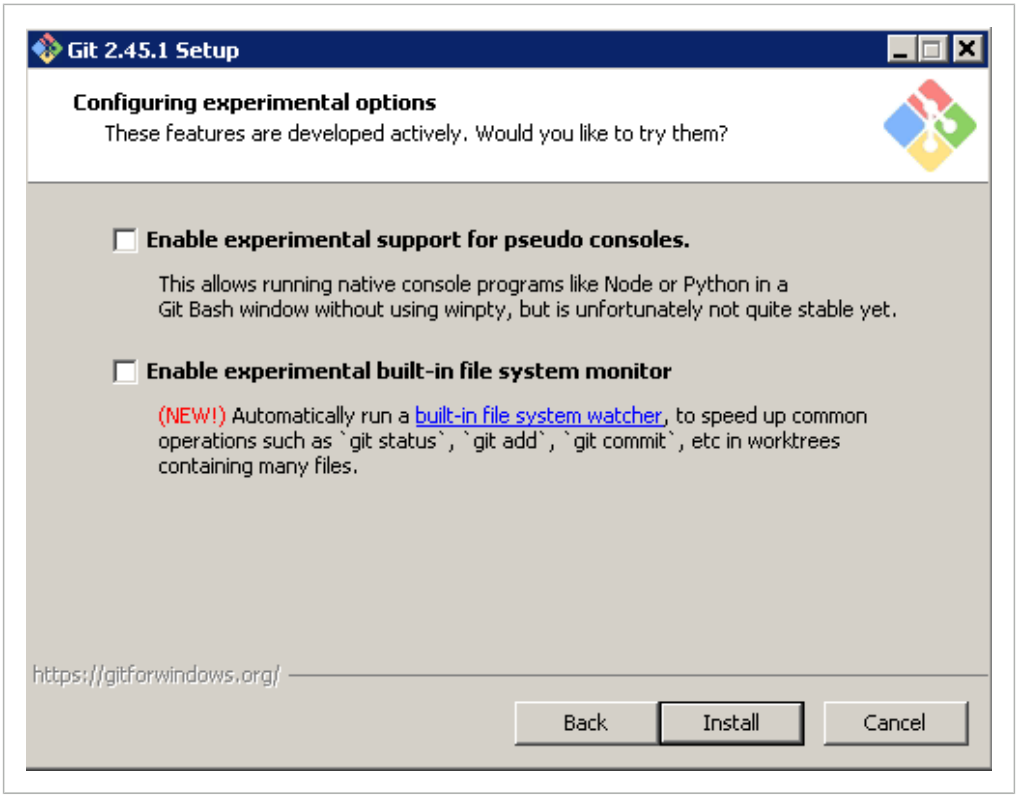


Рис. 81. Configuring experimental options

ж. Нажмите кнопку **Install**.

з. После завершения установки нажмите кнопку **Finish**.

5. Установите Version Control Desktop App:

   а. Запустите установочный файл `VersionControl.Installer.Windows-[разрядность ОС]-[номер версии Version Control]-[дата релиза версии].msi`.

   ▸ **Результат шага:** Откроется окно установки Version Control Desktop App.

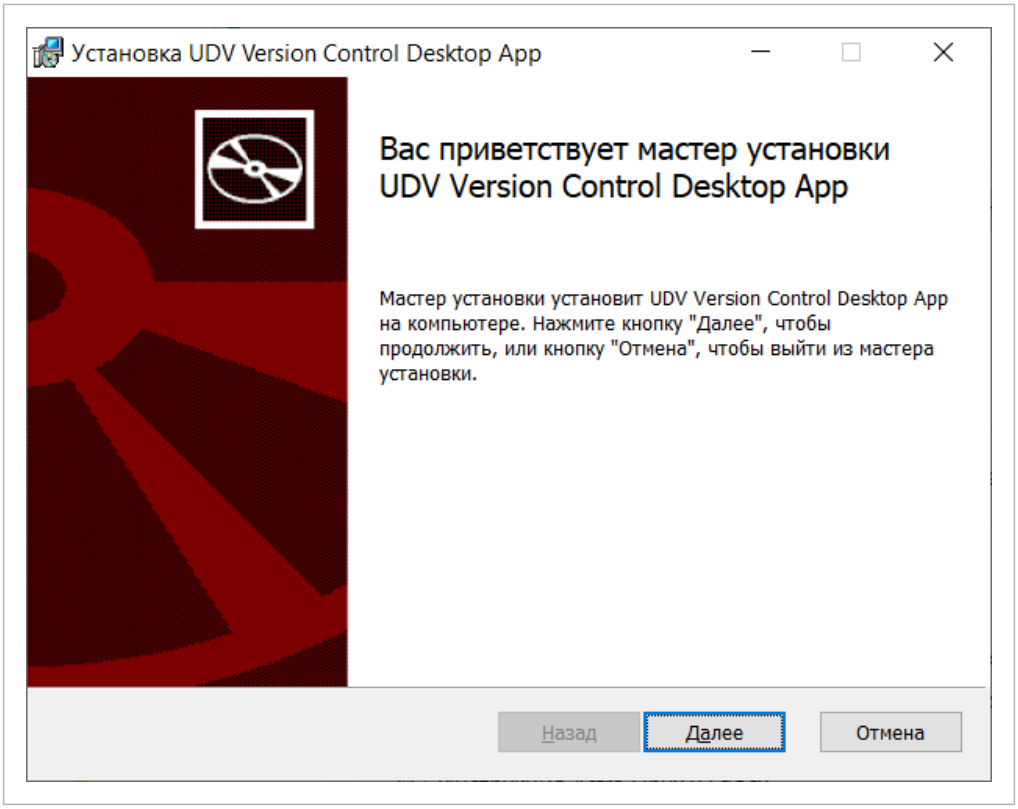


Рис. 82. Окно установки Version Control Desktop App

б. Нажмите кнопку **Далее**.

в. Установите чекбокс **Я принимаю условия лицензионного соглашения**.

г. Нажмите кнопку **Далее**.

д. Выберите место установки и нажмите кнопку **Далее**.

е. Нажмите кнопку **Установить**.

ж. Разрешите этому приложению вносить изменения на устройстве.

з. После завершения установки нажмите кнопку **Готово**.

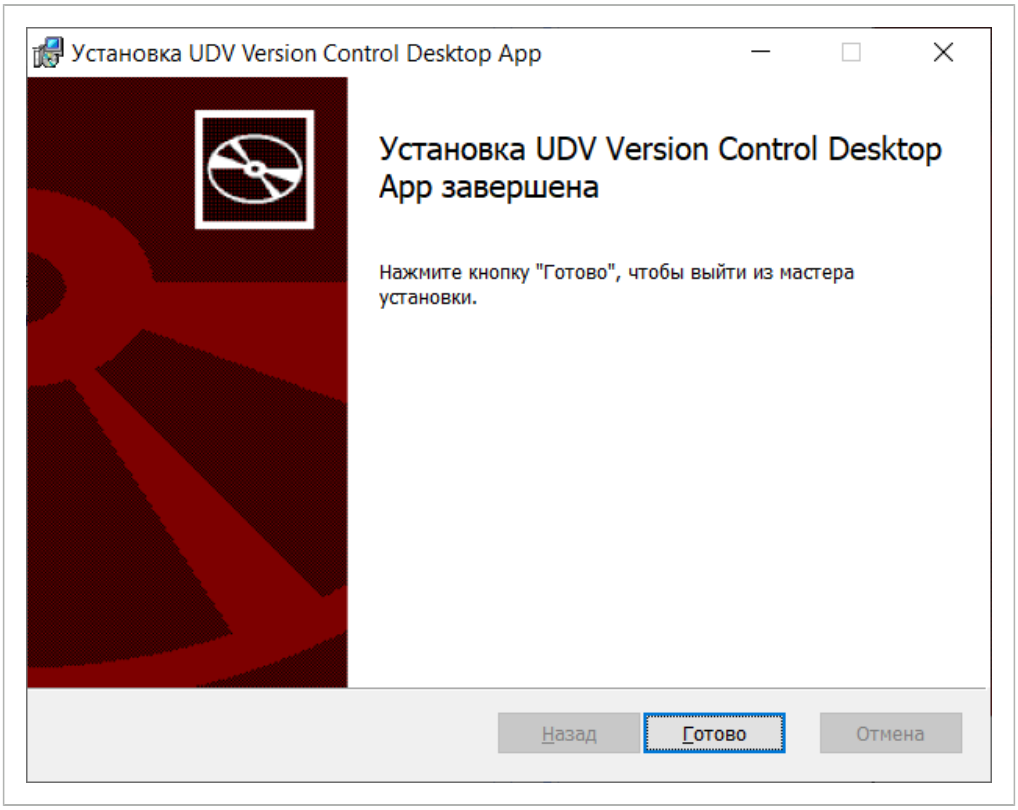


Рис. 83. Окно установки Version Control Desktop App

6. Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:

   а. Запустите консоль.

   б. Введите команду в консоли:

```
git config --global core.autocrlf false
```

3.3.2. Установка Version Control Desktop App на ОС Windows новее 7

1. Скачайте файл-установщик Git-клиента версии 2.37.0 или новее с подходящей разрядностью ОС с официального сайта.
2. Установите Git-клиент:

> Внимание:
>
> Установка Git-клиента должна выполняться только пользователем с правами администратора.

   а. Запустите файл-установщик Git-клиента.

   ▸ **Результат шага:** Откроется окно установки.

б. Нажмите кнопку **Install**.

в. После завершения установки нажмите кнопку **Finish**.

3. Установите Version Control Desktop App:

а. Запустите установочный файл `VersionControl.Installer.Windows-[разрядность ОС]-[номер версии Version Control]-[дата релиза версии].msi`.

- **Результат шага:** Откроется окно установки Version Control Desktop App.

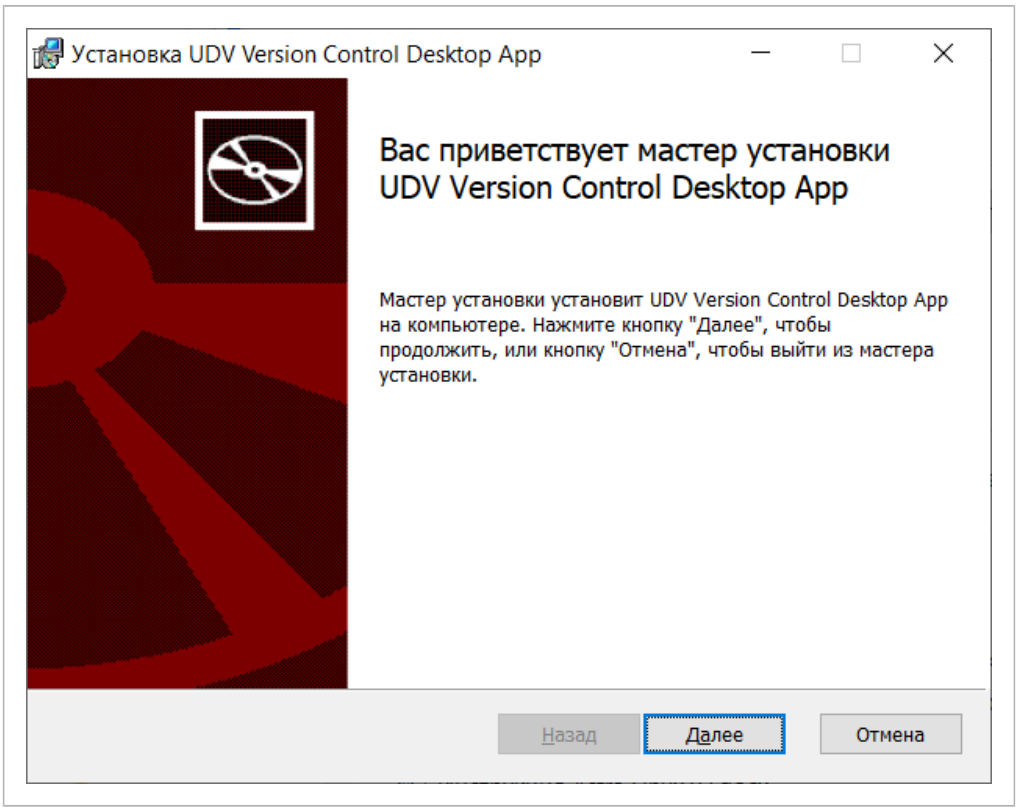


Рис. 84. Окно установки Version Control Desktop App

б. Нажмите кнопку **Далее**.

в. Установите чекбокс **Я принимаю условия лицензионного соглашения**.

г. Нажмите кнопку **Далее**.

д. Выберите место установки и нажмите кнопку **Далее**.

е. Нажмите кнопку **Установить**.

ж. Разрешите этому приложению вносить изменения на устройстве.

з. После завершения установки нажмите кнопку **Готово**.

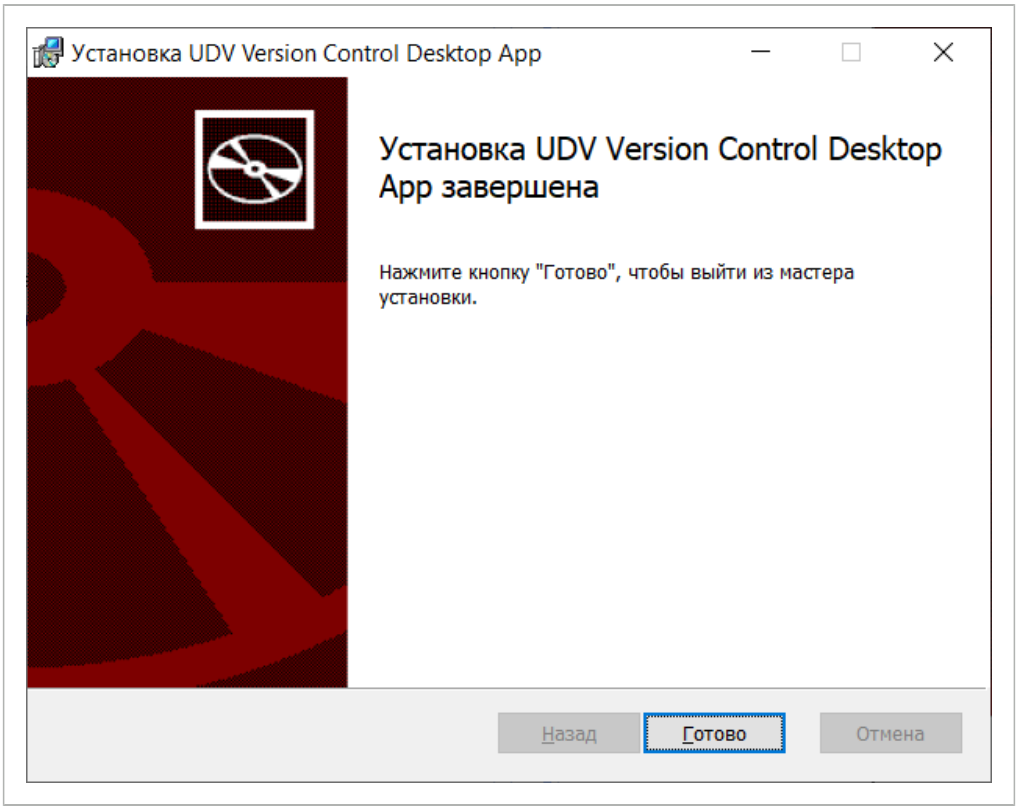


Рис. 85. Окно установки Version Control Desktop App

4. Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:

   а. Запустите консоль.

   б. Введите команду в консоли:

```
git config --global core.autocrlf false
```

3.3.3. Установка Version Control Desktop App на ОС Astra Linux 1.7

В зависимости от доступности Интернета выберите подходящий способ установки Version Control Desktop App на ОС Astra Linux 1.7:

- Установка при наличии доступа в Интернет
- Установка при отсутствии доступа в Интернет

3.3.3.1. Установка при наличии доступа в Интернет

1. Убедитесь, что в ОС установлен Git-клиент версии 2.37.0 или новее:

   а. Для проверки версии `git` выполните команду:

```
git --version
```

б. Если `git` не установлен или номер версии меньше 2.37.0, установите `git` последней версии:

```
sudo apt install git
```

2. Поместите установочный deb-пакет Version Control Desktop App в выбранную директорию.
3. Установите Version Control Desktop App:

```
sudo apt install /[путь к пакету]/[название пакета]
```

▸ **Результат шага:** Version Control Desktop App будет успешно установлен. Из-за настроек безопасности ОС Astra Linux отобразится следующее сообщение: `N: Загрузка выполняется от лица суперпользователя без ограничений песочницы, так как файл «/[путь к пакету]/[название пакета]» недоступен для пользователя «_apt». - pkgAcquire::Run (13: Отказано в доступе)`.

4. Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:

   а. Запустите консоль.

   б. Введите команду в консоли:

```
git config --global core.autocrlf false
```

5. Для запуска Version Control Desktop App:
   а. Откройте меню **Пуск**.
   б. Выберите **Разработка → Version Control**.

3.3.3.2. Установка при отсутствии доступа в Интернет

1. Убедитесь, что в ОС установлен Git-клиент версии 2.37.0 или новее:

   а. Для проверки версии `git` выполните команду:

```
git --version
```

   б. Если `git` не установлен или номер версии меньше 2.37.0, установите `git`:
   - Поместите архив с зависимостями `dependencies_vc_desktop_astra1.7.tar.gz` в директорию `/opt`.
   - Распакуйте архива с зависимостями:

```
sudo tar -xvzf /opt/dependencies_vc_desktop_astra1.7.tar.gz -C /opt
```

   - Выполните установку зависимостей:

```
sudo apt install /opt/packages/*.deb
```

2. Поместите установочный deb-пакет Version Control Desktop App на ОС Astra Linux в выбранную директорию.
3. Установите пакет Version Control Desktop App:

```
sudo apt install /[путь к пакету]/[название пакета]
```

▸ **Результат шага:** Version Control Desktop App будет успешно установлен. Из-за настроек безопасности ОС Astra Linux отобразится следующее сообщение: `N: Загрузка выполняется от лица`

`суперпользователя без ограничений песочницы, так как файл «/[путь к пакету]/[название пакета]» недоступен для пользователя «_apt». - pkgAcquire::Run (13: Отказано в доступе)`.

4. Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:

    a. Запустите консоль.

    б. Введите команду в консоли:

    ```
    git config --global core.autocrlf false
    ```

5. Для запуска Version Control Desktop App:

    a. Откройте меню **Пуск**.

    б. Выберите **Разработка → Version Control**.

3.3.4. Установка Version Control Desktop App на ОС Astra Linux 1.8

В зависимости от доступности Интернета выберите подходящий способ установки Version Control Desktop App на ОС Astra Linux 1.8:

- Установка при наличии доступа в Интернет
- Установка при отсутствии доступа в Интернет

3.3.4.1. Установка при наличии доступа в Интернет

1. Убедитесь, что в ОС установлен Git-клиент версии 2.37.0 или новее:

    a. Для проверки версии `git` выполните команду:

    ```
    git --version
    ```

    б. Если `git` не установлен или номер версии меньше 2.37.0, установите `git` последней версии:

    ```
    sudo apt install git
    ```

2. Поместите установочный deb-пакет Version Control Desktop App на ОС Astra Linux в выбранную директорию.
3. Установите Version Control Desktop App:

    ```
    sudo apt install /[путь к пакету]/[название пакета]
    ```

    ▸ **Результат шага:** Version Control Desktop App будет успешно установлен. Из-за настроек безопасности ОС Astra Linux отобразится следующее сообщение: `N: Загрузка выполняется от лица суперпользователя без ограничений песочницы, так как файл «/[путь к пакету]/[название пакета]» недоступен для пользователя «_apt». - pkgAcquire::Run (13: Отказано в доступе)`.
4. Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:

a. Запустите консоль.

б. Введите команду в консоли:

```
git config --global core.autocrlf false
```

5. Для запуска Version Control Desktop App:
   a. Откройте меню **Пуск**.
   б. Выберите **Программы → Разработка → Version Control**.

3.3.4.2. Установка при отсутствии доступа в Интернет

1. Убедитесь, что в ОС установлен Git-клиент версии 2.37.0 или новее:

   a. Для проверки версии `git` выполните команду:

   ```
   git --version
   ```

   б. Если `git` не установлен или номер версии меньше 2.37.0, установите `git` последней версии, создав архив с зависимостями на ПК с доступом в Интернет с такой же версией ОС:

   > Прим.:
   >
   > Шаги **i-v** выполняются на ПК с доступом в Интернет, шаги **vi-viii** — на ПК, на который ставится Version Control Desktop App.

   - Создайте директорию для пакетов с зависимостями:

     ```
     sudo mkdir /opt/packages
     ```

   - Для корректного создания архива удалите `git` и его зависимости:

     ```
     sudo apt remove git
     ```

     ```
     sudo apt autoremove
     ```

   - Скачайте необходимые зависимости:

     ```
     sudo apt --download-only -o dir::cache::archives='/opt/packages' install git
     ```

   - Создайте архив:

     ```
     sudo rm -rf /opt/packages/{lock,partial}
     ```

     ```
     sudo tar -cvzf /opt/dependencies_vc_desktop_astra1.8.tar.gz -C /opt packages
     ```

   - Установите обратно `git`:

     ```
     sudo apt install git
     ```

   - Поместите архив с зависимостями `dependencies_vc_desktop_astra1.8.tar.gz` в директорию `/opt` на ПК без доступа в Интернет.
   - Распакуйте архива с зависимостями:

     ```
     sudo tar -xvzf /opt/dependencies_vc_desktop_astra1.8.tar.gz -C /opt
     ```

- Выполните установку зависимостей:

```
sudo apt install /opt/packages/*.deb
```

2. Поместите установочный deb-пакет Version Control Desktop App в выбранную директорию.
3. Установите пакет Version Control Desktop App:

```
sudo apt install /[путь к пакету]/[название пакета]
```

▸ **Результат шага:** Version Control Desktop App будет успешно установлен. Из-за настроек безопасности ОС Astra Linux отобразится следующее сообщение: `N: Загрузка выполняется от лица суперпользователя без ограничений песочницы, так как файл «/[путь к пакету]/[название пакета]» недоступен для пользователя «_apt». - pkgAcquire::Run (13: Отказано в доступе)`.

4. Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:

   a. Запустите консоль.

   б. Введите команду в консоли:

```
git config --global core.autocrlf false
```

5. Для запуска Version Control Desktop App:
   a. Откройте меню **Пуск**.
   б. Выберите **Программы → Разработка → Version Control**.

3.3.5. Установка Version Control Desktop App на ОС РЕД ОС 7.3

В зависимости от доступности Интернета выберите подходящий способ установки Version Control Desktop App на ОС РЕД ОС 7.3:

- Установка при наличии доступа в Интернет
- Установка при отсутствии доступа в Интернет

3.3.5.1. Установка при наличии доступа в Интернет

1. Убедитесь, что в ОС установлен Git-клиент версии 2.37.0 или новее:

   a. Для проверки версии `git` выполните команду:

```
git --version
```

   б. Если `git` не установлен или номер версии меньше 2.37.0, установите `git` последней версии:

```
sudo dnf install git
```

2. Поместите установочный rpm-пакет Version Control Desktop App на ОС РЕД ОС в выбранную директорию.
3. Установите Version Control Desktop App:

```
sudo dnf install /[путь к пакету]/[название пакета]
```

▸ **Результат шага:** после окончания установки появится сообщение об успешном завершении операции.

4. Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:

    a. Запустите консоль.

    б. Введите команду в консоли:

```
git config --global core.autocrlf false
```

5. Для запуска Version Control Desktop App:

    a. Откройте меню **Пуск**.

    б. Выберите **Программирование → Version Control**.

3.3.5.2. Установка при отсутствии доступа в Интернет

1. Убедитесь, что в ОС установлен Git-клиент версии 2.37.0 или новее:

    a. Для проверки версии `git` выполните команду:

```
git --version
```

    б. Если `git` не установлен или номер версии меньше 2.37.0, установите `git` последней версии, создав архив с зависимостями на ПК с доступом в Интернет с такой же версией ОС:

> Прим.:
>
> Шаги **i-v** выполняются на ПК с доступом в Интернет, шаги **vi-viii** — на ПК, на который ставится Version Control Desktop App.

- Создайте директорию для пакетов с зависимостями:

```
sudo mkdir /opt/packages
```

- Для корректного создания архива удалите `git` и его зависимости:

```
sudo dnf remove git
```

```
sudo dnf autoremove
```

- Скачайте необходимые зависимости:

```
sudo dnf --downloadonly --downloaddir=/opt/packages install git
```

- Создайте архив:

```
sudo tar -cvzf /opt/dependencies_vc_desktop_redos7.3.tar.gz -C /opt packages
```

- Установите обратно `git`:

```
sudo dnf install git
```

- Поместите архив с зависимостями `dependencies_vc_desktop_redos7.3.tar.gz` в директорию `/opt` на ПК без доступа в Интернет.
- Распакуйте архива с зависимостями:

```
sudo tar -xvzf /opt/dependencies_vc_desktop_redos7.3.tar.gz -C /opt
```

- Выполните установку зависимостей:

```
sudo dnf install /opt/packages/*.rpm
```

2. Поместите установочный rpm-пакет Version Control Desktop App в выбранную директорию.
3. Установите пакет Version Control Desktop App:

```
sudo dnf install /[путь к пакету]/[название пакета]
```

- **Результат шага:** после окончания установки появится сообщение об успешном завершении операции.

4. Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:

   a. Запустите консоль.

   б. Введите команду в консоли:

```
git config --global core.autocrlf false
```

5. Для запуска Version Control Desktop App:

   a. Откройте меню **Пуск**.

   б. Выберите **Программирование** → **Version Control**.

3.3.6. Установка Version Control Desktop App на ОС РЕД ОС 8

В зависимости от доступности Интернета выберите подходящий способ установки Version Control Desktop App на ОС РЕД ОС 8:

- Установка при наличии доступа в Интернет
- Установка при отсутствии доступа в Интернет

3.3.6.1. Установка при наличии доступа в Интернет

1. Убедитесь, что в ОС установлен Git-клиент версии 2.37.0 или новее:

   a. Для проверки версии `git` выполните команду:

```
git --version
```

   б. Если `git` не установлен или номер версии меньше 2.37.0, установите `git` последней версии:

```
sudo dnf install git
```

2. Поместите установочный rpm-пакет Version Control Desktop App на ОС РЕД ОС в выбранную директорию.
3. Установите Version Control Desktop App:

```
sudo dnf install /[путь к пакету]/[название пакета]
```

- **Результат шага:** после окончания установки появится сообщение об успешном завершении операции.

4. Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:

a. Запустите консоль.

б. Введите команду в консоли:

```
git config --global core.autocrlf false
```

5. Для запуска Version Control Desktop App:
   a. Откройте меню **Пуск**.
   б. Выберите **Программирование → Version Control**.

3.3.6.2. Установка при отсутствии доступа в Интернет

1. Убедитесь, что в ОС установлен Git-клиент версии 2.37.0 или новее:

   a. Для проверки версии `git` выполните команду:

   ```
   git --version
   ```

   б. Если `git` не установлен или номер версии меньше 2.37.0, установите `git` последней версии, создав архив с зависимостями на ПК с доступом в Интернет с такой же версией ОС:

   > Прим.:
   >
   > Шаги **i-v** выполняются на ПК с доступом в Интернет, шаги **vi-viii** — на ПК, на который ставится Version Control Desktop App.

   - Создайте директорию для пакетов с зависимостями:

     ```
     sudo mkdir /opt/packages
     ```

   - Для корректного создания архива удалите `git` и его зависимости:

     ```
     sudo dnf remove git
     ```

     ```
     sudo dnf autoremove
     ```

   - Скачайте необходимые зависимости:

     ```
     sudo dnf --downloadonly --downloaddir=/opt/packages install git
     ```

   - Создайте архив:

     ```
     sudo tar -cvzf /opt/dependencies_vc_desktop_redos8.tar.gz -C /opt packages
     ```

   - Установите обратно `git`:

     ```
     sudo dnf install git
     ```

   - Поместите архив с зависимостями `dependencies_vc_desktop_redos8.tar.gz` в директорию `/opt` на ПК без доступа в Интернет.
   - Распакуйте архива с зависимостями:

     ```
     sudo tar -xvzf /opt/dependencies_vc_desktop_redos8.tar.gz -C /opt
     ```

- Выполните установку зависимостей:

```
sudo dnf install /opt/packages/*.rpm
```

2. Поместите установочный rpm-пакет Version Control Desktop App в выбранную директорию.
3. Установите пакет Version Control Desktop App:

```
sudo dnf install /[путь к пакету]/[название пакета]
```

▸ **Результат шага:** после окончания установки появится сообщение об успешном завершении операции.

4. Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:

   а. Запустите консоль.

   б. Введите команду в консоли:

```
git config --global core.autocrlf false
```

5. Для запуска Version Control Desktop App:

   а. Откройте меню **Пуск**.

   б. Выберите **Программирование → Version Control**.

4. Обновление Комплекса

Поддерживается обновление Комплекса до следующих версий:

- с версии 1.19 до версии 3.0;
- с версии 2.1 до версии 3.0.

Для обновления Комплекса с версии 1.18 необходимо сначала обновить Комплекс до версии 1.19.

Внимание:

Обновление Комплекса с версии 2.2 до версии 3.0 не поддерживается.

5. Дополнительные настройки Комплекса

В этом разделе:

В этом разделе приведены настройки, которые можно выполнить при необходимости на ОС Альт Сервер 10.2 после ее установки и развертывания всех уровней Комплекса:

- Подключение сенсора к другому Комплексу уровня Management
- Настройка сетевых интерфейсов в терминале Комплекса
- Настройка парольной политики и аудита ОС Альт Сервер 10.2 SP
- Изменение сетевого имени сенсора
- Изменение сетевого имени Комплекса
- Изменение часового пояса
- Добавление статического маршрута
- Настройка Комплекса уровня Management в качестве NTP-сервера для сенсоров
- Вход в Комплекс уровня Management по сетевому имени с доверенным сертификатом
- Создание единого виртуального интерфейса (bond) для прослушивания и записи трафика с нескольких физических интерфейсов
- Подключение к trunk-порту коммутатора или маршрутизатора
- Изменение стандартного порта NGINX для доступа к веб-интерфейсу Комплекса
- Изменение локали Комплекса
- Настройка отправки обратного DNS для обнаруженных активов
- Изменение machine-id

- Уменьшение количества ложных срабатываний модулей анализа сетевых данных с использованием белого списка
- Настройка автоматического обновления IP-адресов активов при динамической адресации DHCP

5.1. Подключение сенсора к другому Комплексу уровня Management

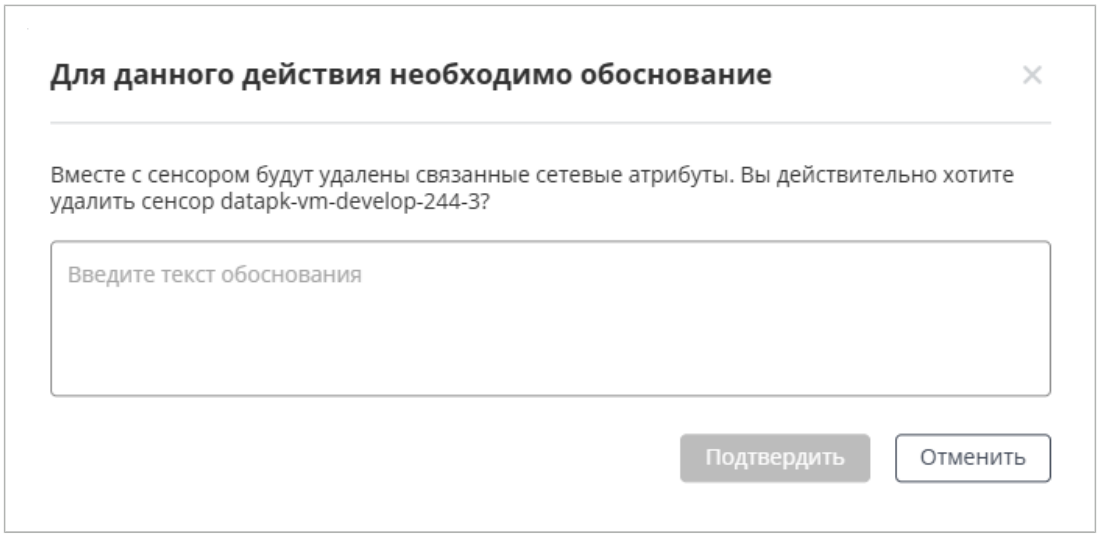
Перед выполнением: Если сенсор уже удален в веб-интерфейсе Комплекса уровня Management, сразу перейдите к шагу 6.

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

Чтобы подключить Комплекс уровня Sensor к другому Комплексу уровня Management:

1. Выполните вход в веб-интерфейс Комплекса уровня Management.
2. Перейдите на страницу **Сенсоры** веб-интерфейса Комплекса уровня Management.
3. Выберите сенсор из списка.
   - **Результат шага:** справа откроется карточка выбранного сенсора.
4. В открывшейся панели нажмите внизу кнопку **Удалить сенсор**.
   - **Результат шага:** Появится окно с предупреждением: `Вместе с сенсором будут удалены связанные сетевые атрибуты. Вы действительно хотите удалить сенсор [имя]?`
5. > ОСТОРОЖНО:
   >
   > - При удалении сенсора будут удалены связанные с ним данные: сетевые атрибуты активов, конфигурации, статусы сбора.
   > - Если при удалении связанных сетевых атрибутов актива будет удален его интерфейс сбора данных, то новым интерфейсом сбора данных станет случайный из оставшихся сетевых атрибутов.
   > - Актив не будет удален, если у него не останется ни одного сетевого атрибута после удаления сенсора. При необходимости измените или удалите такие активы вручную.

   Введите обоснование удаления сенсора и нажмите кнопку **Подтвердить**.



- **Результат шага:** сенсор и связанные с ним данные будут удалены из Комплекса уровня Management.

6. Подключитесь к операционной системе Комплекса уровня Management.
7. Убедитесь, что в операционной системе Комплекса уровня Management настроены правила межсетевого экрана `iptables` согласно шагу 14 раздела «Установка Комплекса уровня Management». Правила, которые должны быть в конфигурационном файле `/etc/sysconfig/iptables` для взаимодействия с сенсорами:

```
-A INPUT -p tcp -m tcp --dport 15673 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 16379 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 19091 -j ACCEPT
```

8. Если необходимые правила `iptables` не настроены на Комплексе уровня Management:

   а. Подключитесь к операционной системе Комплекса уровня Management.

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

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

   в. Добавьте следующие правила межсетевого экрана в конец конфигурационного файла `iptables`:

   ```
   -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
   ```

   > ⚠ Внимание:
   >
   > Данные правила необходимо добавить перед правилами `REJECT`.

   г. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Yes**.

д. Перезапустите сервис `iptables`:

```
systemctl restart iptables
```

9. Подключитесь к операционной системе сенсора.
10. В конфигурационном файле сенсора `/usr/share/udv/datapk/sensor.env` укажите новый IP-адрес Комплекса уровня Management для подключения. Для этого:

    а. Откройте файл `sensor.env` для редактирования:

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

    б. Измените значение переменной `MANAGER_NODE_ADDRESS` на новый IP-адрес сетевого интерфейса управления Комплекса уровня Management.

    в. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Yes**.

11. Перезапустите сервис `udv-rabbitmq-sensor` по команде:

    ```
    systemctl restart udv-rabbitmq-sensor.service
    ```

12. Убедитесь, что сенсор успешно подключился к Комплексу уровня Management. Для этого убедитесь, что в логах сервиса сенсора `udv-redis-sensor` нет ошибок, по команде:

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

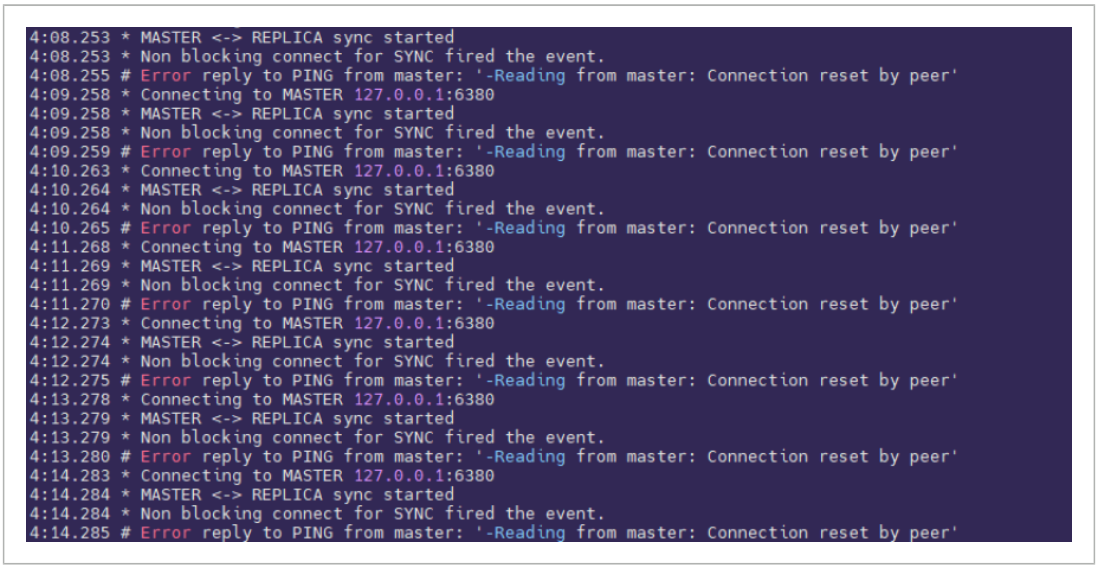


Рис. 86. Ошибки подключения сенсора к Комплексу уровня Management

13. Перейдите в веб-интерфейс Комплекса.

14. Если в правом верхнем углу отобразится ошибка: `Непредвиденная ошибка. Перезапустить синхронизацию`, нажмите на ссылку **Перезапустить синхронизацию** для перезапуска синхронизации сенсоров с Комплексом.

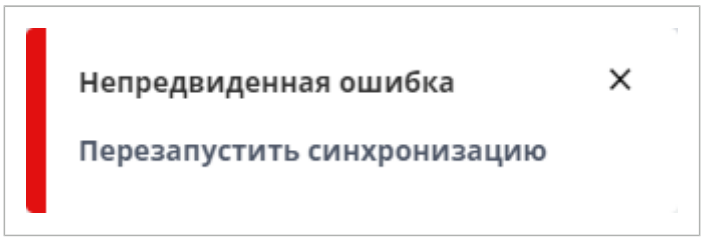


Рис. 87. Ошибка синхронизации сенсоров с Комплексом

5.2. Настройка сетевых интерфейсов в терминале Комплекса

Для настройки сетевых интерфейсов через терминал Комплекса выполните следующие команды:

1. Отобразите наименование сетевых интерфейсов Комплекса, которые были инициализированы или переименованы в ходе запуска ОС Альт Сервер. Для этого выполните команду:

```
dmesg -T | grep -E "NIC|renamed"
```

```
[root@datapk-1 ~]# dmesg -T | grep -E "NIC|renamed"
[Пн окт 16 11:00:54 2023] VMware vmxnet3 virtual NIC driver - version 1.7.0.0-k-NAPI
[Пн окт 16 11:00:54 2023] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[Пн окт 16 11:00:54 2023] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[Пн окт 16 11:00:54 2023] vmxnet3 0000:0b:00.0 ens192: renamed from eth0
[Пн окт 16 11:00:54 2023] vmxnet3 0000:13:00.0 ens224: renamed from eth1
[Пн окт 16 11:01:02 2023] vmxnet3 0000:0b:00.0 ens192: NIC Link is Up 10000 Mbps
```

Рис. 88. Вывод сетевых интерфейсов, инициализированных в ходе запуска ОС Альт Сервер

2. Остановите работу Комплекса, выполнив команду:

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

3. Создайте директорию нового сетевого интерфейса командой:

```
mkdir /etc/net/ifaces/ens192
```

> Прим.:
>
> Имя интерфейса управления `ens192` задано для примера.

4. Создайте файл с IP-адресом и маской сетевого интерфейса управления Комплекса:

```
echo [ip_addr]/[subnet_mask] > /etc/net/ifaces/ens192/ipv4address
```

Где `[ip_addr]` — IP-адрес сетевого интерфейса управления Комплекса, `[subnet_mask]` — маска сетевого интерфейса управления Комплекса.

5. Создайте файл со шлюзом сетевого интерфейса управления Комплекса:

```
echo default via [ip_addr] > /etc/net/ifaces/ens192/ipv4route
```

Где `[ip_addr]` — IP-адрес шлюза сетевого интерфейса управления Комплекса.

6. Создайте файл с адресами DNS-серверов интерфейса управления Комплекса:

```
echo nameserver [ip_addr] > /etc/net/ifaces/ens192/resolv.conf
```

Где `[ip_addr]` — IP-адрес DNS-сервера сетевого интерфейса управления Комплекса.

7. Создайте конфигурационный файл сетевого интерфейса со стандартными настройками:

```
echo -e
 'TYPE=eth\nCONFIG_WIRELESS=no\nBOOTPROTO=static\nCONFIG_IPV4=yes\nDISABLED=no\nNM_CONTRO
LLED=no' > /etc/net/ifaces/ens192/options
```

8. Выполните перезапуск сетевой службы для применения настроек:

```
systemctl restart network
```

9. Запустите сервисы Комплекса, выполнив команду:

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

5.3. Настройка парольной политики и аудита ОС Альт Сервер 10.2 SP

Для настройки парольной политики и аудита операционной системы ОС Альт Сервер, на которой установлен Комплекс:

1. Настройте парольную политику на Комплексах всех уровней:

   а. Измените параметры конфигурационного файла `login.defs`. Для этого:

   - Откройте для редактирования файл `login.defs`:

     ```
     mcedit /etc/login.defs
     ```

   - Раскомментируйте следующие строки, удалив символ `#`:

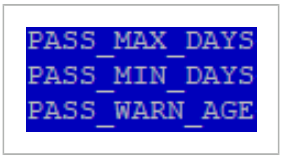
     

     Рис. 89. Параметры файла login.defs

     Описание изменяемых параметров:

     - `PASS_MAX_DAYS` — максимальное количество дней использования пароля. По истечении указанного срока запустится процедура смены пароля.
     - `PASS_MIN_DAYS` — минимальное количество дней между изменениями пароля. Попытка сменить пароль раньше заданного срока не будет выполнена.
     - `PASS_WARN_AGE` — количество дней до окончания срока действия пароля, в течение которых будет отображаться предупреждение о необходимости его смены.

   б. Измените параметры конфигурационного файла `passwdqc.conf`. Для этого:

   - Откройте для редактирования файл `passwdqc.conf`:

     ```
     mcedit /etc/passwdqc.conf
     ```

   - Отредактируйте файл `passwdqc.conf` и приведите к следующему виду:

```
min=disabled,disabled,disabled,disabled,6
max=72
passphrase=3
match=4
similar=deny
random=47
enforce=everyone
retry=3
# The below are just examples, by default none of these are used
#wordlist=/usr/share/john/password.lst
#denylist=/etc/passwdqc.deny
#filter=/opt/passwdqc/hibp.pwq
```

Рис. 90. Параметры файла passwdqc.conf

Описание изменяемых параметров:

- `min` — при значении `disabled,disabled,disabled,disabled,6` минимальная длина пароля равна 6, и он должен содержать все четыре класса символов: цифры, строчные буквы, заглавные буквы, специальные символы;
- `enforce` — при значении `everyone` политика будет применяться к новым паролям всех учетных записей.

в. Сохраните файл нажатием клавиши **F2**.

г. Подтвердите сохранение и закройте сохраненный файл нажатием клавиши **F10**.

- **Результат шага:** выполнены настройки парольной политики UDV DATAPK.

2. Убедитесь в корректности настроек журнала аудита. Для этого:

а. Откройте на редактирование конфигурационный файл `auditd.conf`:

```
mcedit /etc/audit/auditd.conf
```

б. Убедитесь, что параметры внутри файла соответствуют приведенным ниже, и измените их при необходимости:

```
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
```

Рис. 91. Параметры файла auditd.conf

Описание изменяемых параметров:

- `max_log_file` — максимальный размер журнала в мегабайтах;
- `num_logs` — максимальное количество сохраненных файлов журнала;
- `max_log_file_action` — действие с журналом по достижении им максимального размера. При значении `ROTATE` будет перезаписан самый старый файл журнала.

в. Сохраните и закройте файл.

3. Перезагрузите ОС Альт Сервер командой:

```
shutdown -r now
```

▸ **Результат шага:** ОС успешно перезагружена.

5.4. Изменение сетевого имени сенсора

Для изменения сетевого имени сенсора:

1. Подключитесь к сенсору по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. Выполните команду для смены сетевого имени сенсора:

```
hostnamectl set-hostname [новое имя сенсора]
```

3. Перезапустите ОС сенсора командой:

```
reboot now
```

▸ **Результат шага:** После выполнения вышеописанных действие сетевое имя сенсора будет изменено в веб-интерфейсе уровня Management.

Прим.:

Название сенсора останется прежним для событий и сессий, зарегистрированных до изменения сетевого имени сенсора, на следующих страницах:

- **События** — поля **Сенсор**, **Регистратор**;
- **Сетевые соединения** — поле **Сенсор**;

5.5. Изменение сетевого имени Комплекса

Для изменения сетевого имени Комплекса через терминал после установки выполните следующие команды:

1. Остановите работу Комплекса, выполнив команду:

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

2. Измените сетевое имя Комплекса:

```
hostnamectl set-hostname [новое-сетевое-имя]
```

3. Перезагрузите Комплекс для изменения сетевого имени:

```
shutdown -r now
```

5.6. Изменение часового пояса

Для изменения часового пояса Комплекса:

1. Остановите работу Комплекса, выполнив команду:

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

2. Откройте список часовых поясов по команде:

```
timedatectl list-timezones
```

Прим.:

Используя клавиши стрелок **Вверх** и **Вниз**, найдите свой часовой пояс.

3. Перенастройте часовой пояс:

```
timedatectl set-timezone Asia/Yekaterinburg
```

Внимание:

В данной команде часовой пояс `Asia/Yekaterinburg` указан в качестве примера. Вместо него укажите свой часовой пояс.

4. Запустите сервисы Комплекса, выполнив команду:

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

5.7. Добавление статического маршрута

При необходимости добавьте временные или постоянные статические маршруты сетевому интерфейсу Комплекса. Для этого:

1. Посмотрите список текущих сетевых маршрутов:

   ```
   ip route
   ```

2. Остановите работу Комплекса, выполнив команду:

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

3. Для добавления интерфейсу Комплекса временного маршрута к необходимой IP-подсети выполните команду:

   ```
   ip route add [subnet]/[subnet_mask] via [subnet_gateway] dev [iface_name]
   ```

   где:

   - `[subnet]/[subnet_mask]` — подсеть, в которую необходимо проложить маршрут, и маска этой подсети;
   - `[subnet_gateway]` — IP-адрес шлюза, через который можно получить доступ к подсети;
   - `[iface_name]` — имя сетевого интерфейса Комплекса, для которого будет добавлен маршрут.

   > Подсказка:
   >
   > Можно создавать маршруты до отдельных хостов командой:
   >
   > ```
   > ip route add [ip_addr] via [gateway] dev [iface_name]
   > ```
   >
   > где:
   >
   > - `[ip_addr]` — IP-адрес хоста, до которого необходимо проложить маршрут;
   > - `[gateway]` — IP-адрес шлюза, через который можно получить доступ к хосту;
   > - `[iface_name]` — имя сетевого интерфейса Комплекса, для которого будет добавлен маршрут.

   ▸ **Результат шага:** Будет создан временный маршрут: это значит, что после перезапуска сетевой службы `network` либо ОС Альт Сервер данные маршруты будут удалены.

4. Для добавления интерфейсу Комплекса постоянного маршрута к необходимой IP-подсети:

   а. Откройте конфигурационный файл `ipv4route` в директории сетевого интерфейса `[iface_name]`, которому необходимо добавить маршрут:

   ```
   mcedit /etc/net/ifaces/[iface_name]/ipv4route
   ```

   б. Добавьте в новой строке статический маршрут:

   ```
   [subnet]/[subnet_mask] via [subnet_gateway]
   ```

   где:

   - `[subnet]/[subnet_mask]` — подсеть, в которую необходимо проложить маршрут, и маска этой подсети;
   - `[subnet_gateway]` — IP-адрес шлюза, через который можно получить доступ к подсети.

> Подсказка:
>
> Каждый новый маршрут добавляется в новой строке.
>
> Можно создавать маршруты до отдельных хостов, добавляя в конфигурационный файл `ipv4route` интерфейса новые строки вида:
>
> ```
> [ip_addr] via [subnet_gateway]
> ```
>
> где:
> - `[ip_addr]` — IP-адрес хоста, до которого необходимо проложить маршрут;
> - `[subnet_gateway]` — IP-адрес шлюза, через который можно получить доступ к хосту.

в. Сохраните изменения в файле `ipv4route` нажатием клавиши **F2**.

г. Подтвердите сохранение и закройте сохраненный файл `ipv4route` нажатием клавиши **F10**.

5. Для применения настроек выполните команду:

```
systemctl restart network
```

6. Запустите сервисы Комплекса, выполнив команду:

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

5.8. Настройка Комплекса уровня Management в качестве NTP-сервера для сенсоров

В этом разделе приведена инструкция по подключению Комплекса уровня Sensor к NTP-серверу, которым будет выступать Комплекс уровня Management.

> Подсказка:
>
> Подключение Комплекса уровня Management к NTP-серверу выполняется в шаге 9 раздела «Настройка сертифицированной ОС Альт Сервер 10.2 SP».

1. На Комплексе уровня Management:

а. Перейдите в рабочую директорию Комплекса и остановите работу сервисов:

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

б. Убедитесь, что на межсетевом экране открыт 123/udp порт:

```
iptables -nvL | grep 123
```

▸ **Результат шага:** в выводе команды должна быть строка с разрешающим правилом, как на рисунке ниже.

```
[root@cl-datapk-nuvo ~]# iptables -nvL | grep 123
   56  4256 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:123
```

Рис. 92. Корректный вывод команды запроса правила iptables

в. Откройте для редактирования файл `chrony.conf`:

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

г. Добавьте новую строку в конце раздела `Allow NTP client access from local network`:

```
allow [ip_addr]
```

Где `[ip_addr]` — сетевой адрес комплекса уровня Sensor.

> Подсказка:
>
> Также можно разрешить всей подсетиКомплекса уровня Sensor подключение к NTP-серверу: в таком случае `[ip_addr]` замените на адрес подсети Комплекса уровня Sensor и через **/** укажите маску данной подсети, например `10.51.203.0/24`.

```
# Allow NTP client access from local network.
#allow 192.168.0.0/16
#allow 10.51.203.0/24
allow 10.51.203.12
```

Рис. 93. Настройка Комплекса уровня Sensor в качестве NTP-клиента в файле chrony.conf

д. Перезапустите службу `chronyd`:

```
systemctl restart chronyd
```

е. Запустите сервисы Комплекса по команде:

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

2. На Комплексе уровня Sensor:

а. Перейдите в рабочую директорию Комплекса и остановите работу сервисов:

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

б. Откройте для редактирования файл `chrony.conf`:

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

в. Убедитесь, что в качестве NTP-сервера указан IP-адрес Комплекса уровня Management.

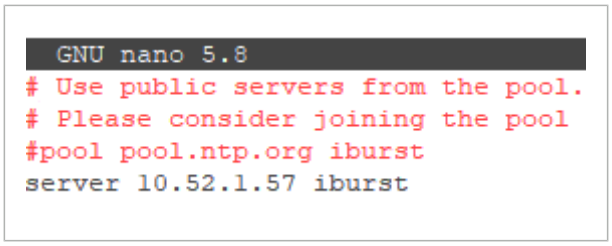


Рис. 94. Настройка Комплекса уровня Management в качестве NTP-сервера в файле chrony.conf

г. Перезапустите службу `chronyd`:

```
systemctl restart chronyd
```

д. Запустите сервисы Комплекса по команде:

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

5.9. Вход в Комплекс уровня Management по сетевому имени с доверенным сертификатом

Данная инструкция предназначена для устранения ошибок о недоверенных сертификатах при входе в веб-интерфейс Комплекса.

> **Внимание:**
>
> Инструкция применима при использовании ОС Windows и веб-браузера Google Chrome на клиентской машине, с которой выполняется подключение к веб-интерфейсу Комплекса.

1. На клиентской машине с ОС Windows добавьте в файл `C:\Windows\System32\drivers\etc\hosts` строку:

   ```
   [ip_addr]    [hostname]
   ```

   где `[ip_addr]` — IP-адрес сетевого интерфейса управления Комплекса, `[hostname]` — сетевое имя Комплекса.

   > **Подсказка:**
   >
   > Для входа в веб-интерфейс Комплекса по сетевому имени можно на DNS-сервере клиентской машины вместо добавления записи в файл `hosts` создать правило типа `A` с IP-адресом и сетевым именем Комплекса.

2. Откройте веб-интерфейс Комплекса в новой вкладке браузера.
3. Нажмите кнопку **Не защищено** слева от адресной строки браузера.
   - **Результат шага:** откроется меню настройки сайтов.

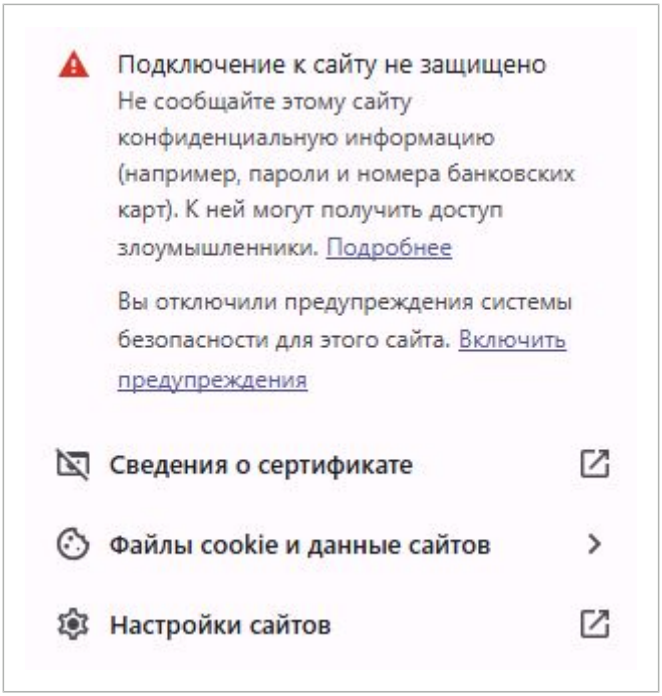


Рис. 95. Меню настройки сайтов

4. Перейдите во вкладку **Сведения о сертификате → Подробнее** и нажмите кнопку **Экспорт**.
5. Подтвердите сохранение сертификата на ПК.
   - **Результат шага:** сертификат с разрешением `.crt` будет сохранен на ПК.
6. Для добавления сертификата в «доверенные» нажмите на него два раза, затем выберите **Установить сертификат**.
7. Выберите, устанавливать ли сертификат для текущего пользователя или для локального компьютера. Нажмите **Далее**.
8. Выберите **Поместить все сертификаты в следующее хранилище** и нажмите **Обзор**.
9. В новом окне выберите **Доверенные корневые центры сертификации** и нажмите **ОК**.
10. В окне мастера импорта сертификатов нажмите **Далее**, затем нажмите **Готово**.

> Подсказка:
>
> Если все сделано верно, появится окно с сообщением об успешном импорте сертификата.

11. Импортируйте сертификат в установленное антивирусное ПО, если такое ПО установлено.
12. Выполните очистку данных веб-браузера (кэша и файлов cookie) и перезапустите его.
13. Выполните подключение к Комплексу по сетевому имени. Для этого введите в строке поиска веб-браузера адрес `https://[hostname]`, где `[hostname]` — сетевое имя Комплекса.

5.10. Создание единого виртуального интерфейса (bond) для прослушивания и записи 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 сетевые соединения 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 имена сетевых интерфейсов, которые планируется объединить, неизвестны, 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]` — имя проверяемого сетевого интерфейса.

3. Остановите работу Комплекса 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 две 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\nHOST="[iface_name_1]
 [iface_name_2]"\nBONDMODE=3\nBONDOPTIONS="miimon=100 downdelay=200 updelay=200"'
 > /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. Удалите настройки отдельных интерфейсов, выполнив команды:

```
rm -f /etc/net/ifaces/[iface_name_1]/{i,r}*
rm -f /etc/net/ifaces/[iface_name_2]/{i,r}*
```

    Где `[iface_name_1]` и `[iface_name_2]` — названия подключенных сетевых интерфейсов, которые будут объединены.

12. Для применения новых настроек перезапустите службу сети командой `systemctl restart network` или перезапустите ОС Альт Сервер командой `reboot`.
13. 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.

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

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

5.11. Подключение к trunk-порту коммутатора или маршрутизатора

Для подключения к trunk-порту сетевого устройства (коммутатора или маршрутизатора) с выбранным идентификатором VLAN сетевого устройства (`[vlan_id]`):

1. Запросите у администратора, отвечающего за настройку VLAN `[vlan_id]` на сетевом устройстве, свободный IP-адрес и его маску подсети из этого VLAN.
2. Выберите из сетевых интерфейсов ОС Альт Сервер интерфейс для создания VLAN. Получить список сетевых интерфейсов можно по команде:

   ```
   ip a
   ```

   > **Внимание:**
   >
   > Выбранный сетевой интерфейс не должен быть сетевым интерфейсом Комплекса для прослушивания трафика. Если у Комплекса имеется всего два сетевых интерфейса, рекомендуется выбрать сетевой интерфейс управления.

3. Остановите работу Комплекса, выполнив команду:

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

4. Перейдите в директорию с сетевыми интерфейсами `/etc/net/ifaces`:

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

5. Создайте директорию, содержащую наименование выбранного сетевого интерфейса и идентификатор создаваемого VLAN (должен совпадать с идентификатором VLAN сетевого устройства):

   ```
   mkdir [iface_name].[vlan_id]
   ```

   где:
   - `[iface_name]` — наименование выбранного сетевого интерфейса;
   - `[vlan_id]` — идентификатор создаваемого VLAN, равный идентификатору VLAN сетевого устройства.

6. Создайте для выбранного сетевого интерфейса `[iface_name]` файл, содержащий полученный ранее IP-адрес в VLAN `[vlan_id]`:

   ```
   echo [ip_addr]/[subnet_mask] > /etc/net/ifaces/[iface_name].[vlan_id]/ipv4address
   ```

   где:
   - `[ip_addr]` — полученный IP-адрес в VLAN `[vlan_id]`;
   - `[subnet_mask]` — маска подсети для VLAN `[vlan_id]`.

7. Создайте файл с параметрами сетевого интерфейса `[iface_name]`:

   ```
   echo -e 'TYPE=vlan\nBOOTPROTO=static\nHOST=[iface_name]\nVID=[vlan_id]' > \
   /etc/net/ifaces/[iface_name].[vlan_id]/options
   ```

8. Если необходимо подключить тот же сетевой интерфейс Комплекса к trunk-порту с другим VLAN, повторите шаги 5-7 для создания подинтерфейсов с нужным идентификатором VLAN (`[vlan_id]`).
9. Для применения новых настроек перезапустите службу сети командой `systemctl restart network` или перезапустите ОС Альт Сервер командой `reboot`
10. Проверьте статус созданных подинтерфейсов `[iface_name].[vlan_id]` по команде:

```
cat /proc/net/vlan/[iface_name].[vlan_id]
```

Пример

Пример вывода команды для интерфейса `eth0`, подключенного к VLAN `43`:

```
[root@datapk-alt3 eth0]# cat /proc/net/vlan/eth0.43
eth0.43  VID: 43         REORDER_HDR: 0  dev->priv_flags: 1021
         total frames received            0
          total bytes received            0
      Broadcast/Multicast Rcvd            0

      total frames transmitted            0
       total bytes transmitted            0
Device: eth0
INGRESS priority mappings: 0:0  1:0  2:0  3:0  4:0  5:0  6:0 7:0
 EGRESS priority mappings:
```

Рис. 96. Вывод команды статуса подключения к trunk-порту

Подсказка:

При корректной настройке подинтерфейсов проходящий трафик отразится на значениях `received` и `transmitted`: при повторном выводе результата команды эти параметры будут отличаться от нуля и будут постоянно возрастать.

11. Запустите сервисы Комплекса, выполнив команду:

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

5.12. Изменение стандартного порта NGINX для доступа к веб-интерфейсу Комплекса

Для изменения стандартного порта NGINX для доступа к веб-интерфейсу Комплекса:

1. Выполните вход под учетной записью `root` в терминал Комплекса уровня Management.
2. Откройте на редактирование файл `manager.env`, выполнив команду:

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

3. Измените номер порта в переменной `NGINX_HTTPS_PORT`.
4. Сохраните и закройте файл `manager.env`, последовательно нажав клавиши **F2** и **F10**.
5. Откройте на редактирование конфигурационный файл `iptables`, выполнив команду:

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

6. Укажите необходимый порт в следующем правиле для порта подключения к веб-интерфейсу Комплекса:

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport [порт подключения] -j ACCEPT
```

Внимание:

Убедитесь, что данное правило расположено выше правил `REJECT`.

7. Сохраните и закройте конфигурационный файл `iptables`.

8. Перезапустите службу iptables, выполнив команду:

   ```
   systemctl restart iptables
   ```

9. Перезапустите службу `udv-nginx`, выполнив команду:

   ```
   systemctl restart udv-nginx.service
   ```

10. Введите адрес для подключения к веб-интерфейсу Комплекса в формате `https://[IP-адрес]:[порт подключения]`, где `[IP-адрес]` — IP-адрес интерфейса Комплекса, `[порт подключения]` — порт для подключения к веб-интерфейсу Комплекса.

5.13. Изменение локали Комплекса

Для изменения локали Комплекса:

1. Выполните вход в ОС под учетной записью администратора системы `root`.
2. Выполните следующую команду для установки локали:

   ```
   localectl set-locale [локаль_Комплекса]
   ```

   где `[локаль_Комплекса]` — устанавливаемая локаль Комплекса (`LANG=en_US.utf8` или `LANG=ru_RU.utf8`).

3. Перезагрузите Комплекс, выполнив команду:

   ```
   shutdown -r now
   ```

4. Дождитесь перезагрузки Комплекса.
5. Введите адрес для подключения к веб-интерфейсу в формате `https://[IP-адрес]/[локаль_Комплекса]/login`, где `[IP-адрес]` — IP-адрес интерфейса управления Комплекса, `[локаль_Комплекса]` — установленная локаль Комплекса (`en-US` или `ru-RU`).

▸ **Результат шага:** в веб-браузере будет отображаться страница авторизации Комплекса на английском или русском языке, в зависимости от установленной локали.

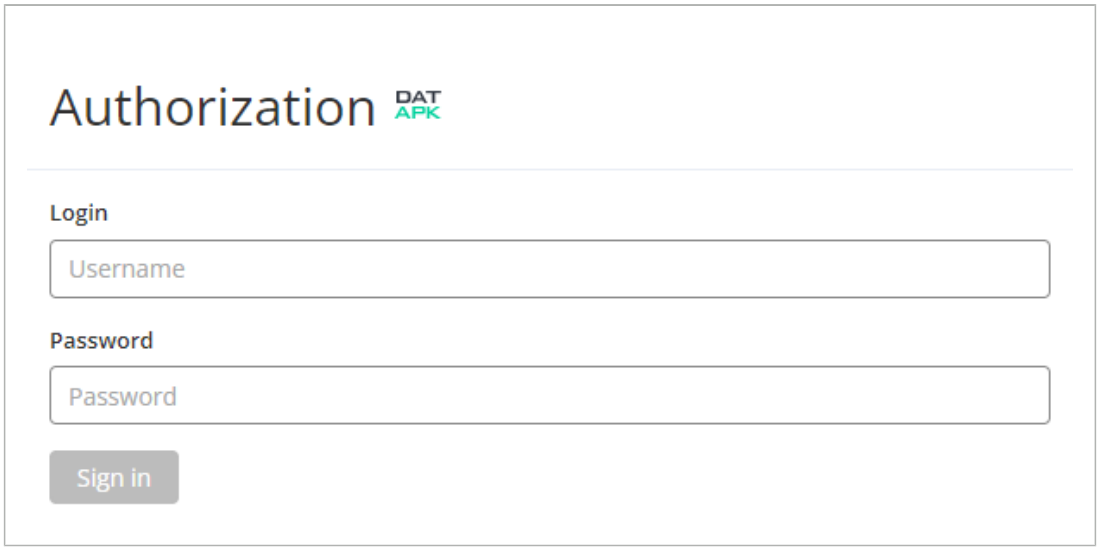


Рис. 97. Страница авторизации Комплекса на английском языке

5.14. Настройка отправки обратного DNS для обнаруженных активов

Обратный поиск DNS, обратный DNS (reverse DNS lookup, rDNS) — технология, которая позволяет по IP-адресу определить соответствующее ему доменное имя. Это обратный процесс по отношению к стандартному DNS-запросу, где по доменному имени определяется IP-адрес.

В Комплексе отправка обратного DNS применяется для поиска доменного имени обнаруженных активов. За управление данной функцией отвечает параметр `KnownHosts::reverse_dns_enable` в файле `/usr/share/udv/zeek-wrapper/configs/general.dat`

Возможные значения параметра:

- `T` — включить функцию;
- `F` — отключить функцию.

Для включения или отключения на сенсоре функции отправки обратного DNS:

1. Подключитесь к сенсору по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. Откройте файл `general.dat` для редактирования:

   ```
   mcedit /usr/share/udv/zeek-wrapper/configs/general.dat
   ```

3. Установите параметру в файле `general.dat` соответствующее значение:

   ```
   KnownHosts::reverse_dns_enable [параметр]
   ```

   Где вместо `[параметр]` укажите одно из значений:
   - `T` — включить функцию;
   - `F` — отключить функцию.

   Пример строки с включенной функцией:

   ```
   KnownHosts::reverse_dns_enable T
   ```

> Внимание:
>
> Если параметр в указанном файле отсутствует, функция считается включенной по умолчанию. Для ее отключения сначала добавьте параметр.

4. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

5.15. Изменение machine-id

`machine-id` — это уникальный идентификатор машины, который устанавливается в процессе установки Комплекса. Хранится в файле `/etc/machine-id`

> Внимание:
>
> `machine-id` должен быть уникальным и не должен повторяться на других машинах, особенно на тех, которые расположены в одной локальной сети.

Проверка `machine-id` необходима в следующих случаях:

- при установке и запуске нового Комплекса необходимо убедиться, что значение `machine-id` является уникальным;
- при восстановлении из резервной копии — в этом случае значение `machine-id` заменяется на значение, актуальное на момент создания резервной копии.

Узнать `machine-id` можно с помощью команды `cat /etc/machine-id`

Для изменения `machine-id`:

1. Остановите все пакеты Комплекса, выполнив команду:

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

2. Удалите старые файлы `machine-id`, последовательно выполнив команды:

   ```
   rm -f /etc/machine-id
   rm -f /var/lib/dbus/machine-id
   ```

3. Создайте новый `machine-id` и обновите файлы, последовательно выполнив команды:

   ```
   dbus-uuidgen --ensure=/etc/machine-id
   dbus-uuidgen --ensure
   ```

4. Перезагрузите Комплекс, выполнив команду:

   ```
   shutdown -r now
   ```

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

С основными переменными, доступными для использования в этом файле, вы можете ознакомиться в разделе «Переменные файла белого списка» Руководства по эксплуатации UDV DATAPK Industrial Kit.

Для внесения изменений в белый список:

1. Откройте для редактирования файл `general.dat`:

   ```
   mcedit /usr/share/udv/zeek-wrapper/configs/general.dat
   ```

2. Добавьте, измените или удалите запись:

   а. Чтобы добавить в файл новую запись или изменить имеющуюся, следуйте формату:

   ```
   [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.

   Примеры записей:

   ```
   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
   ```

   б. Чтобы удалить запись из файла, выделите ее и нажмите клавишу **Delete**, **Del** или **Backspace**.

3. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

См. также

Переменные файла белого списка

5.17. Настройка автоматического обновления IP-адресов активов при динамической адресации DHCP

Функция позволяет автоматически менять IP-адреса активов, а не создавать новые активы при динамической адресации через DHCP.

За управление данной функцией отвечает параметр `KnownHosts::dhcp_ip_update` в файле `/usr/share/udv/zeek-wrapper/configs/general.dat`

Возможные значения параметра:

- `T` — включить функцию;
- `F` — отключить функцию.

> Прим.:
>
> Если функция включена, актив с IP-адресом `0.0.0.0` не создается. Активы, обнаруживаемые в broadcast- (MAC-адрес `FF:FF:FF:FF:FF:FF`) и multicast-трафике (MAC-адрес начинается с `01:00:5E`), также не создаются.

При изменении IP-адреса актива создается внутреннее событие с кодом `1080028`. Если IP-адрес актива меняется на уже существующий, то создаются внутренние события: `1080028` об изменении IP-адреса и `1080016` о дублировании IP-адреса. Подробнее о событиях см. раздел «События Комплекса».

Для включения или отключения функции на сенсоре:

1. Подключитесь к сенсору по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. Откройте для редактирования файл `general.dat`:

   ```
   mcedit /usr/share/udv/zeek-wrapper/configs/general.dat
   ```

3. Установите параметру в файле `general.dat` соответствующее значение:

   ```
   KnownHosts::dhcp_ip_update [значение_параметра]
   ```

   Где вместо `[значение_параметра]` укажите одно из значений:
   - `T` — включить функцию;
   - `F` — отключить функцию.

   Пример строки с включенной функцией:

   ```
   KnownHosts::dhcp_ip_update T
   ```

   > Прим.:
   >
   > Если параметр в указанном файле отсутствует, функция считается выключенной. Для включения функции добавьте в файл `general.dat` строку из примера выше.

4. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

6. Нештатные ситуации и действия по их устранению

В этом разделе:

Комплекс функционирует круглосуточно. В процессе использования Комплекса возможно появление неполадок, ограничивающих возможности управления защитными механизмами или открывающих возможности для атаки на активы.

Если вам не удается самостоятельно устранить нештатную ситуацию, заполните анкету (см. раздел Анкета при обращении в сервисный центр) и отправьте на адрес сервисного центра UDV Group: support@udv.group.

6.1. Диагностика проблем

6.1.1. Настройка ОС / Начальная настройка Комплекса / Запускаются не все сервисы

Некорректные конфигурационные файлы, директории или сертификаты

- Убедитесь в корректности структуры каталогов, сертификатов.
- Убедитесь в корректном значении переменной `LISTENING_INTERFACES` и др.

Некорректные настройки сети

- Проверьте настройки сети на сервере узла сети, убедитесь в корректной маршрутизации пакетов на активных интерфейсах.
- Убедитесь в поступлении трафика на SPAN-порт для прослушивающих интерфейсов.
- Убедитесь в корректном функционировании сетевого сервиса с помощью команды (для ОС Альт Сервер 10):

```
systemctl status network
```

Достигнут предел свободного места на диске

- Очистите ненужные файлы на Комплексе уровня Management.
- Убедитесь в корректности разметки разделов — должен быть один корневой раздел, занимающий весь объем диска (за исключением подкачки).
- Отредактируйте настройки файла `manager.env` (размеры оперативного и глубокого архива).
- В отдельных случаях может потребоваться очистка таблиц или баз данных, вывод `udv-opensearch` из read-only.

Проблемы с сервисами комплекса / SSH / iptables

- Посмотрите статус служб, убедитесь в их корректном функционировании.
- Пропишите необходимые конфигурации сервисов `ssh` / `iptables` в ОС.

6.1.2. Настройка актива

ОС Windows

- XP и старше: настройте права локального администратора, доступ по протоколам Winexe, WMI, WinRM (при наличии).
- Vista и новее: для полного функционала (включая OVAL) настройте права локального администратора, доступ по протоколам WinRM, WMI, Winexe (при проблемах с WinRM).
- Для диагностики подключения используйте `wbemtest` (для WMI), `psexec` (для Winexe).
- В случае проблем с настройкой ОС: журналы System, Security, WinAudit.

ОС Linux

- Настройте доступ по SSH, в большинстве случаев хватит прав обычного пользователя.
- Для диагностики подключения используйте утилиты `ssh`, `putty` и пр.

Cisco IOS/прочее АСО

- Настройте доступ по SSH (telnet при отсутствии SSH), права на выполнение команд просмотра начальной / текущей конфигурации, версии ОС, ARP-таблицы, таблицы маршрутизации (возможно понадобится пароль от привилегированного режима).
- Для диагностики подключения используйте утилиты `ssh`, `telnet`, `putty` и пр.

SNMP

- Доступ в режиме чтения конфигураций по SNMP версии 1, 2c или 3.
- Настройте отправку SNMP-trap сообщений версии 1 или 2 на Комплексе.
- Для диагностики подключения используйте утилиту `snmpwalk`.

ПЛК

- S7
  - Уточните значения `rack`, `slot`.
  - Для диагностики подключения используйте утилиту `Snap7`.
- Modbus
  - Необходим доступ на чтение регистров.
  - Определитесь с перечнем собираемых регистров, отредактируйте Python-скрипт сбора данных.

OPC UA

- Доступ на чтение регистров (порт зависит от конкретного OPC сервера).
- Определитесь с перечнем собираемых данных, отредактируйте Python-скрипт сбора данных.

6.1.3. Настройка Комплекса

6.1.3.1. Не работает сбор событий

Полностью отсутствуют события

- Проверьте свободное место на корневом разделе диска на Комплексе и его сенсорах.

```
df -h /
```

> Подсказка:
>
> При необходимости освободите место.

- Проверьте настройки ОС на Комплексе и его сенсорах. Значение переменной `vm.max_map_count` должно быть не менее 262144.
- Убедитесь, что сенсоры подключены к Комплексу.
- Проанализируйте логи `udv-event-receiver` сенсоров.
- Проанализируйте логи сервисов Комплекса уровня Management: `udv-event-manager`, `udv-event-processor`, `udv-logstash`, `udv-opensearch`, `udv-opensearch-dashboards`, `udv-rabbitmq`.
- При необходимости выведите сервис `udv-opensearch` из режима read-only.
- Расширьте временное окно поиска событий на странице **События**. Проверьте настройки времени на Комплексе и АРМ, с которого осуществляется подключение. Время и часовой пояс должны совпадать для просмотра событий в реальном времени.

Отсутствуют внутренние события Комплекса (о сессиях, действиях пользователей, изменении конфигураций и т.д.)

- Проверьте настройки файла `manager.env` Комплекса на предмет включенных и отключенных источников.
- Проанализируйте логи сервисов Комплекса уровня Management: `udv-event-manager`, `udv-event-processor`, `udv-logstash`, `udv-opensearch`, `udv-opensearch-dashboards`, `udv-rabbitmq`.

Отсутствуют Syslog-события

- Проверьте наличие событий на активе.
- Проверьте события в интерфейсе Комплекса от конкретного актива по источнику Syslog.
- Проверьте корректность созданных источников событий на странице **Администрирование** → **Настройка активов** → **Источники**. В Комплексе не должно быть несколько локальных активов с одинаковым IP-адресом.
- Проверьте поступление событий от активов на прослушивающий интерфейс сенсора: на сенсоре, прослушивающем активы, выполните команду для записи трафика в файл:

```
tcpdump -i [название прослушивающего интерфейса] host [ip-адрес актива] -w [путь к
 pcap-файлу]
```

- Проверьте, что есть обратный маршрут от этого интерфейса к активу:

```
route -n
ip route show
```

- Проанализируйте логи сервисов Комплекса уровня Management: `udv-event-manager`, `udv-event-processor`, `udv-logstash`, `udv-opensearch`, `udv-opensearch-dashboards`, `udv-rabbitmq`. Проверьте таблицу маршрутизации.

Отсутствуют SMNP-trap события

- Проверьте наличие событий на активе.
- Проверьте события на Комплексе (по сенсору SNMP).
- Проверьте корректность источника SNMP на странице **Администрирование** → **Настройка активов** → **Источники**. В поле **Community** должно быть введено корректное наименование параметра `Community` SNMP-сервиса актива. Один из интерфейсов Актив, для которого настроен источник, должен иметь IP-адрес, с которого приходят trap-события.
- Проверьте поступление событий от активов на прослушивающий интерфейс сенсора: на сенсоре, прослушивающем активы, выполните команду для записи трафика в файл:

```
tcpdump -i [название прослушивающего интерфейса] host [ip-адрес актива] -w [путь к
 pcap-файлу]
```

- Проверьте, что есть обратный маршрут от интерфейса сенсора к активу:

```
route -n
ip route show
```

- Проанализируйте логи сервисов Комплекса уровня Management: `udv-event-manager`, `udv-event-processor`, `udv-logstash`, `udv-opensearch`, проанализируйте дамп трафика.

6.1.3.2. Не фиксируются сессии / активы

- Убедитесь в корректном запуске сервисов сессий `udv-godpi` и `udv-data-flows-service`.
- Убедитесь в корректности настроек сетевых интерфейсов.
- Убедитесь в корректности настроек контролируемой сети.
- Запишите дамп трафика на прослушивающем интерфейсе, убедитесь в наличии интересующих пакетов. Актив появляется только тогда, когда зафиксирован прямой пакет на этот адрес и обратный пакет с этого адреса.
- Проверьте с помощью поиска по IP-адресу или порту, есть ли в интерфейсе сессии (возможно, не до конца описанные).

6.1.3.3. Не работает функционал корреляции

- Убедитесь, что служба корреляции активна.
- Убедитесь в наличии инцидента на странице **Инциденты**. Если инцидент отсутствует, проанализируйте причину отклонения инцидента в логах `udv-incident-manager` Комплекса уровня Management.
- Убедитесь в корректности и активности нужных правил корреляции — после применения правил в веб-интерфейсе ошибки валидации отображаются в логах `udv-esper` Комплекса уровня Management.
- Просмотрите интересующее правило корреляции на странице **Администрирование** → **События и инциденты** → **Правила корреляции** и убедитесь в наличии событий на странице **События**, на основе которых правило генерирует инцидент.

- Убедитесь в наличии скоррелированного события (`event_type = incident`) на странице **События**.
- Проанализируйте логи сервисов Комплекса уровня Management: `udv-event-manager`, `udv-event-processor`, `udv-logstash`, `udv-opensearch`, `udv-opensearch-dashboards`, `udv-rabbitmq`.

6.1.3.4. Не работает сервис обнаружения вторжений

- Убедитесь, что служба обнаружения вторжений запущена на требуемых сенсорах на странице **Сенсоры** и нет ошибок при запуске.
- Убедитесь, что правила обнаружения вторжений синхронизированы с сенсорами по кнопке (**Синхронизация правил**) на странице **Администрирование** → **Правила обнаружения**.
- Убедитесь, что нужные правила обнаружения вторжений применены на странице **Администрирование** → **Правила обнаружения** и нет ошибок при применении.
- Убедитесь, что интересующие пакеты поступают на прослушивающие интерфейсы сенсоров: запишите трафик в pcap-файл с помощью утилиты `tcpdump` и проанализируйте его.
- Проанализируйте логи `udv-suricata-wrapper` на сенсорах и `udv-suricata-backend` на Комплексе уровня Management.
- В веб-интерфейсе на странице **События** проверьте поступление событий от подключенных сенсоров.
- В веб-интерфейсе просмотрите график **События от сенсора к Комплексу** в карточке сенсора на странице **Сенсоры**. Проверьте получение событий с сенсоров в логах сервиса `udv-event-manager` Комплекса уровня Management.
- Если не удается получить событие службы обнаружения вторжений о срабатывании выбранной сигнатуры, проверьте, есть ли события о срабатывании других сигнатур, например протестируйте сигнатуру для обнаружения ICMP-пакетов.

6.1.3.5. Не работает отправка оповещений об инцидентах

- Проверьте корректность настроек уведомлений в интерфейсе Комплекса.
- Проанализируйте логи `udv-alerting` — в них отображается информация в том числе по недоступности и некорректной авторизации на почтовом сервере, OPC/UA сервере.
- Убедитесь в доступности почтового или OPC-сервера в зависимости от типа оповещения.
- Убедитесь в наличии инцидентов.

6.1.3.6. Не работает сбор данных с актива

- Проанализируйте ошибки сбора на странице .
- Убедитесь в сетевом доступе к активу по требуемым портам.
- Убедитесь в корректности идентификационных данных (тег, логин, пароль), назначенных учетной записи актива.
- Убедитесь в корректной настройке активов, корректном выполнении на активе команды из Python-скрипта сбора данных.
- Проанализируйте журналы сервиса `udv-command-processor` и интересующих коннекторов на сенсорах.

6.2. Диагностика сервисов и иерархии

Скрипт `dtpk_get_logs-3_0.bash` однократно собирает количество запросов оперативных данных по иерархии и журналы всех сервисов Комплекса уровней Management и Sensor на текущем сервере за заданный период времени в часах.

Для диагностики работоспособности сервисов и иерархии в операционной системе Комплекса:

1. Примонтируйте диск с дистрибутивом Комплекса, либо с помощью приложения для обмена файлами по протоколу SFTP (или аналогичным способом по сети) скопируйте скрипт `dtpk_get_logs-3_0.bash` в директорию `/opt` операционной системы Комплекса.
2. Подключитесь к выбранному Комплексу по протоколу SSH с учетной записью обычного пользователя и повысьте привилегии до администратора с помощью команды `su -`
3. Перейдите в директорию `/opt` по команде:

   ```
   cd /opt
   ```

4. Запустите скрипт `dtpk_get_logs-3_0.bash` командой:

   ```
   bash dtpk_get_logs-3_0.bash N
   ```

   где `N` — период, за который будут собраны журналы (в часах).

   > **Пример**
   > Чтобы собрать журналы за последние 6 часов, выполните команду:
   >
   > ```
   > bash dtpk_get_logs-3_0.bash 6
   > ```

   ▸ **Результат шага:** в текущей директории `/opt` будет создан архив `logs-[hostname]-[текущая_дата].tar.gz` с журналами сервисов текущего Комплекса за выбранный период времени.
5. Заполните анкету и отправьте с ней архив на адрес сервисного центра UDV Group : support@udv.group.

6.3. Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных

При эксплуатации Комплекса пользователь может столкнуться с различными видами затруднений, которые также возможно самостоятельно устранить. Основные типы затруднений:

- Веб-интерфейс не загружается
- Соединение с главной страницей веб-интерфейса осуществляется по протоколу HTTP вместо HTTPS
- Время на Комплексе отличается от времени получения события
- После запуска Комплекса при попытке загрузки веб-интерфейса открывается пустая страница
- 502-я ошибка при загрузке страницы авторизации, 500-е ошибки сразу после авторизации
- Не обнаруживаются новые сессии
- Комплекс не обнаруживает активы в автоматическом режиме
- Комплекс не обнаруживает активы без IP-адреса
- Два актива с одинаковым IP-адресом
- Не осуществляется сбор необходимых событий или конфигураций с активов
- При попытке сбора данных в результатах выводится предупреждение «Превышено время ожидания выполнения задачи сбора событий»
- Сбор конфигураций осуществляется, но результаты сбора не отображаются
- Отсутствуют внешние или внутренние события на странице «События»
- Не принимаются Syslog-сообщения от активов
- Не принимаются сообщения от службы обнаружения вторжений
- Не принимаются сообщения от службы корреляции
- Не инициализируются сервисы udv-opensearch, udv-opensearch-dashboards, udv-logstash модуля «Управление внешними событиями»
- Не создается индекс в экспертном режиме страницы «События»

- Не удается отфильтровать записи в экспертном режиме страницы «События» по новым значениям полей после нормализации
- Объекты мониторинга и визуализации импортируются с ошибкой
- Не удается импортировать сканер сбора данных в веб-интерфейсе
- Не выполняется архивация внешних событий при превышении размера или времени хранения индекса
- Ошибки вида «<...>Cannot start service <...>. Bind for <ip_address>:<TCP/UDP_port> is ready allocated» при попытке запуска сервисов
- Недоступен сервис корреляции событий
- При бездействии в веб-интерфейсе сеанс завершается раньше, чем через 10 минут
- Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России
- Не устанавливается соединение с сенсором
- Не работает сложное исключение для правила службы обнаружения вторжений
- Обнаружен конфликт версий проектов ПЛК
- Каталог проекта ПЛК содержит информацию других файлов
- Путь к файлу превышает допустимую длину

6.3.1. Веб-интерфейс не загружается

В качестве причины недоступности веб-интерфейса рассмотрены следующие:

- Некорректная инициализация сервисов Комплекса
- Некорректная генерация серверного сертификата и ключа Комплекса уровня Management
- Запрет на доступ к веб-интерфейсу Комплекса с текущей рабочей станции
- Отсутствие свободного места на диске

Некорректная инициализация сервисов Комплекса

Способ устранения

Для устранения затруднения:

1. Подключитесь к операционной системе Комплекса.
2. Просмотрите состояние сервисов, выполнив команду:

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

   > Внимание:
   >
   > `Все сервисы в полученном списке должны быть в состоянии active (поле Active).` Сервисы `udv-event-correlator.service` (при наличии модуля «Управление внешними событиями» в комплекте поставки) и `udv-sensor-registrar.service` могут штатно находиться в состоянии `inactive (dead)`, так как их запуск выполняется по необходимости в процессе работы Комплекса.

3. Если какие-либо сервисы не запущены или имеют статус, отличный от `active`, остановите работу сервисов, выполнив команду:

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

4. Дождитесь остановки работы всех сервисов.
5. В рабочей директории Комплекса уровня Management проверьте и, в случае необходимости, откорректируйте файл `manager.env`.

6. В рабочей директории Комплекса уровня Sensor проверьте и, в случае необходимости, откорректируйте файл `sensor.env`.
7. В случае необходимости восстановите данные из резервной копии.

> Подсказка:
>
> Порядок восстановления данных приведен в разделе «Восстановление данных из резервных копий».

8. Запустить работу сервисов командой:

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

9. Дождитесь запуска работы всех сервисов.

> Внимание:
>
> При запуске не должно быть ошибок или предупреждений.

Некорректная генерация серверного сертификата и ключа Комплекса уровня Management

Способ устранения

Для устранения затруднения:

1. Убедитесь, что серверный сертификат и ключ в директории `/var/cache/udv/nginx/certs` корректно инициализированы, срок действия сертификата не истек. При необходимости сгенерируйте или замените сертификат и ключ.
2. Убедитесь, что файл серверного сертификата имеет расширение `.cert`.
3. Убедитесь, что значение переменной `HOST_IP` в файле `manager.env` соответствует наименованию серверного сертификата. Для этого выполните команду:

```
cat /usr/share/udv/datapk/manager.env | grep HOST_IP
```

4. Если значение переменной не соответствует наименованию серверного сертификата, выполните следующие действия:

    а. Остановите работу сервисов, выполнив команду:

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

    б. Откройте файл `manager.env` на редактирование, выполнив команду:

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

    в. Измените значение переменной `HOST_IP`.

    г. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Yes**.

    д. Запустите работу сервисов, выполнив команду:

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

Запрет на доступ к веб-интерфейсу Комплекса с текущей рабочей станции

Способ устранения

Для устранения затруднения:

1. Убедитесь, что в правилах межсетевого экрана `iptables` в файле `/etc/sysconfig/iptables` не указаны правила, разрешающие доступ к веб-интерфейсу Комплекса только с рабочих станций определенной подсети и запрещающий доступ со всех остальных. Для этого проверьте наличие следующего правила:

   ```
   -A INPUT -p tcp -s [IP-адрес_подсети/маска_подсети] -m state --state NEW -m tcp
   --dport 443 -j ACCEPT
   ```

2. Если правила присутствуют в файле `/etc/sysconfig/iptables`, выполните вход в веб-интерфейс Комплекса из подсети, разрешенной правилами.

Отсутствие свободного места на диске

Способ устранения

Для устранения затруднения:

1. Проверьте свободное место на диске, выполнив команду:

   ```
   df -h /
   ```

2. При отсутствии свободного места:
   a. Остановите сервисы Комплекса.
   б. Удалите ненужные данные с диска.
   в. Запустите сервисы Комплекса.

6.3.2. Соединение с главной страницей веб-интерфейса осуществляется по протоколу HTTP вместо HTTPS

Причина: отсутствие серверного сертификата и ключа

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

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

2. Убедитесь, что серверный сертификат и ключ в директории `/var/cache/udv/nginx/certs` корректно инициализированы, срок действия сертификата не истек. При необходимости сгенерируйте или замените их.
3. Убедитесь, что в файле `manager.env`, расположенном в рабочей директории Комплекса, значение переменной **HOST_IP** совпадает с наименованием серверного сертификата.
4. Запустите работу сервисов, выполнив команду:

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

6.3.3. Время на Комплексе отличается от времени получения события

В качестве причин некорректного отображения времени в Комплексе рассмотрены следующие:

- Время на активе отличается от времени на операционной системе Комплекса
- Время на рабочей станции отличается от времени на операционной системе Комплекса
- Некорректная настройка часового пояса в операционной системе Комплекса
- Часовой пояс в базе данных PostgreSQL отличается от часового пояса на сервере Комплекса

Время на активе отличается от времени на операционной системе Комплекса

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на операционной системе актива.
2. Измените часовой пояс операционной системы.
3. При необходимости перезагрузите актив.

Время на рабочей станции отличается от времени на операционной системе Комплекса

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на рабочей станции, с которой ведется работа с веб-интерфейсом Комплекса уровня Management.
2. Измените часовой пояс рабочей станции так, чтобы он совпадал с часовым поясом Комплекса.

Некорректная настройка часового пояса в операционной системе Комплекса

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на операционной системе Комплекса уровня Management.
2. Настройте синхронизацию времени Комплекса с NTP-сервером.

> Подсказка:
>
> Подробнее о настройке NTP-сервера см. в инструкции Руководства по внедрению и поддержке «Настройка сертифицированной ОС Альт Сервер 10.2 SP».

Часовой пояс в базе данных PostgreSQL отличается от часового пояса на сервере Комплекса

Способ устранения

Для устранения затруднения:

1. Убедитесь, что часовые пояса на сервере и в базе данных `PostgreSQL` не совпадают:

   а. Команда покажет часовой пояс сервера:

   ```
   timedatectl show
   ```

   б. Команда покажет часовой пояс базы данных:

   ```
   cat /var/lib/pgsql/data/postgresql.conf | grep "^timezone ="
   ```

2. Если часовые пояса не совпадают, при необходимости измените часовой пояс сервера.

   > Подсказка:
   >
   > Подробнее об изменении часового пояса Комплекса см. в инструкции Руководства по внедрению и поддержке «Изменение часового пояса»

3. Измените часовой пояс базы данных так, чтобы он совпадал с часовым поясом сервера. Для этого:

   а. Откройте для редактирования конфигурационный файл сервиса базы данных:

   ```
   mcedit /usr/share/udv/postgresql/postgresql.conf
   ```

   б. В строке `timezone` укажите тот же часовой пояс, что на сервере.

   > Важное замечание:
   >
   > При изменении часового пояса на более ранний, чем предыдущий (сдвиг в минус), старые события могут оказаться новее по времени, чем новые события. Учитывайте это при работе с данными.

   в. Сохраните внесенные изменения, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

4. Перезагрузите сервис `udv-postgresql` командой:

   ```
   sudo systemctl restart udv-postgresql.service
   ```

См. также

Отображение времени в Комплексе

6.3.4. После запуска Комплекса при попытке загрузки веб-интерфейса открывается пустая страница

Причина: некорректный файл environment.json, либо его отсутствие

Способ устранения

Для устранения затруднения:

1. Проверьте наличие и корректность файла `environment.json` в директории `/usr/share/udv/frontend`, расположенной в рабочей директории Комплекса уровня Management.
2. При необходимости переустановите сервис `udv-frontend`, выполнив команду:

```
apt-get install --reinstall udv-frontend -y
```

▸ **Результат шага:** Если файл `environment.json` был изменен или удален, при переустановке сервиса `udv-frontend` он будет восстановлен до состояния по умолчанию.

6.3.5. 502-я ошибка при загрузке страницы авторизации, 500-е ошибки сразу после авторизации

В качестве причин ошибок в веб-интерфейсе Комплекса рассмотрены следующие:

- Комплекс не до конца инициализировался после запуска работы сервисов
- Некорректно настроены правила межсетевого экрана для доступа к сервисам Комплекса
- Отсутствие свободного места на диске

Комплекс не до конца инициализировался после запуска работы сервисов

Способ устранения

Для устранения затруднения:

1. Подождите 3-5 минут после запуска сервисов.
2. При повторяющихся ошибках выполните команду:

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

3. Все сервисы должны быть в состоянии `active`. При ошибках в журналах сервисов см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

Некорректно настроены правила межсетевого экрана для доступа к сервисам Комплекса

Способ устранения

Для устранения затруднения:

1. Убедитесь, что на Комплексе уровня установлены корректные правила межсетевого экранирования `iptables` в файле `/etc/sysconfig/iptables`:
    - правила для уровня Management:

```
*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

# Правило, когда M выступает в роли ntp-сервера для S:
-A INPUT -p udp -m udp --dport 123 -j ACCEPT
```

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT

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

COMMIT
```

- правила для уровня Management+Sensor:

```
*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 udp -m udp --dport 162 -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 -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT
```

2. При необходимости настройте правила `iptables`:

   a. Остановите работу сервисов, выполнив команду:

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

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

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

   в. Добавьте правила в конфигурационный файл `iptables` в зависимости от конфигурации Комплекса согласно шагу 1.

   г. Перезапустите сервис `iptables`:

   ```
   systemctl restart iptables
   ```

д. Запустите работу сервисов, выполнив команду:

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

Отсутствие свободного места на диске

Способ устранения

Для устранения затруднения:

1. Проверьте свободное место на диске, выполнив команду:

   ```
   df -h /
   ```

2. При отсутствии свободного места:
   а. Остановите сервисы Комплекса.
   б. Удалите ненужные данные с диска.
   в. Запустите сервисы Комплекса.

6.3.6. Не обнаруживаются новые сессии

В качестве причин отсутствия обнаружения новых сессий рассмотрены следующие:

- Некорректные настройки контролируемой сети на странице Сенсоры
- Комплекс получает информацию о новых сессиях с задержкой
- Некорректные настройки интерфейса сенсора, выполняющего прослушивание всего трафика контролируемой сети (listening interface)
- Некорректные настройки зеркалирования трафика на активном сетевом оборудовании (АСО) или отсутствие сетевого трафика
- Некорректное значение переменной сенсора LISTENING_INTERFACES
- Ошибки сервиса udv-zeek-wrapper

Некорректные настройки контролируемой сети на странице Сенсоры

Способ устранения

Для устранения проблемы:

1. На странице **Сенсоры** веб-интерфейса Комплекса убедитесь, что добавлены все контролируемые сети, которые прослушивают подключенные сенсоры.
2. Убедитесь, что IP-адрес актива принадлежит хотя бы одному из диапазонов адресов контролируемой сети сенсоров.
3. Выполните сканирование контролируемой сети (см. раздел «Сканирование сети и определение интерфейсов активного сетевого оборудования»).

Комплекс получает информацию о новых сессиях с задержкой

Способ устранения

Для устранения проблемы:

1. Выполните настройку контролируемой сети сенсоров согласно инструкции «Некорректные настройки контролируемой сети на странице Сенсоры».
2. Дождитесь обновления информации о сессиях на вкладке **Сессии** на странице **Инспекция сети** → **Сетевые соединения** (до 5 минут) — такая задержка допустима из-за особенностей передачи данных с сенсоров на Комплекс.

Некорректные настройки интерфейса сенсора, выполняющего прослушивание всего трафика контролируемой сети (listening interface)

Способ устранения

Для устранения проблемы:

1. Выведите информацию о прослушивающем интерфейсе, выполнив команду в операционной системе сенсора:

   ```
   ifconfig [наименование прослушивающего интерфейса сенсора]
   ```

   или:

   ```
   ip -a link show [наименование прослушивающего интерфейса сенсора]
   ```

   > Подсказка:
   >
   > Интерфейсы пишутся через запятую без пробелов.

2. Убедитесь, что интерфейс — в состоянии `UP` и режиме `PROMISC`.
3. При необходимости откорректируйте сетевые настройки.

Некорректные настройки зеркалирования трафика на активном сетевом оборудовании (АСО) или отсутствие сетевого трафика

Способ устранения

Для устранения проблемы:

1. Несколько раз выполните команду в операционной системе сенсора:

   ```
   ifconfig [наименование прослушивающего интерфейса сенсора]
   или:
   ip -s -s link show [наименование прослушивающего интерфейса сенсора]
   ```

   > Подсказка:
   >
   > Интерфейсы пишутся через запятую без пробелов.

2. Убедитесь, что параметр `RX packets` постепенно увеличивается.
3. Проверьте настройки зеркалирования на АСО. При необходимости откорректируйте их.
4. Убедитесь в наличии связи между интерфейсами АСО и сенсором.
5. Сгенерируйте сетевую активность. Для этого отправьте ICMP-пакеты с интерфейса сенсора на интерфейс любого актива.

Некорректное значение переменной сенсора LISTENING_INTERFACES

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

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

2. Укажите значения слушающих интерфейсов в переменной `LISTENING_INTERFACES` файла `sensor.env`.

   > Подсказка:
   >
   > Переменная может быть представлена в виде списка интерфейсов через запятую, и одно из значений должно быть равно названию интерфейса сенсора, выполняющего прослушивание всего трафика.

3. Запустите сервисы, выполнив команду:

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

Ошибки сервиса udv-zeek-wrapper

Способ устранения

Для устранения проблемы:

1. Просмотрите состояние сервисов, выполнив команду:

   ```
   systemctl list-units udv-*
   ```

   > Внимание:
   >
   > Все сервисы в полученном списке должны быть в состоянии `active` (поле **Active**).

2. Просмотрите журнал `udv-zeek-wrapper` на наличие критичных ошибок:

   ```
   journalctl -feu udv-zeek-wrapper
   ```

3. Убедитесь, что в начале инициализации `udv-zeek-wrapper` корректно подключился к базе, загрузил правила, и публикация событий о сессиях начата. При ошибках см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

6.3.7. Комплекс не обнаруживает активы в автоматическом режиме

В качестве причин отсутствия автоматического обнаружения активов рассмотрены следующие:

- Некорректные настройки контролируемой сети на странице «Сенсоры»
- Отсутствие трафика с актива
- Комплекс получает информацию о новых активах с задержкой
- Частичное зеркалирование сетевого трафика

Некорректные настройки контролируемой сети на странице «Сенсоры»

Способ устранения

Для устранения затруднения:

1. На странице **Сенсоры** веб-интерфейса Комплекса убедитесь, что добавлены все контролируемые сети, которые прослушивают подключенные сенсоры.
2. Убедитесь, что IP-адрес актива принадлежит хотя бы одному из диапазонов адресов контролируемой сети сенсоров.
3. Выполните сканирование контролируемой сети (см. раздел «Сканирование сети и определение интерфейсов активного сетевого оборудования» Руководства по эксплуатации).

Отсутствие трафика с актива

Способ устранения

Для устранения затруднения:

Сгенерируйте сетевую активность требуемого актива. Для этого отправьте ICMP-трафик между интерфейсами сенсора и актива.

▸ **Результат шага:** при отсутствии проблем с обнаружением сессий требуемый актив должен появиться в списке активов на странице **Активы** веб-интерфейса Комплекса.

Комплекс получает информацию о новых активах с задержкой

Способ устранения

Для устранения затруднения:

1. Выполните настройку контролируемой сети сенсоров согласно п. выше «Некорректные настройки контролируемой сети на странице «Сенсоры»».
2. Сгенерируйте сетевую активность на активе согласно п. выше «Отсутствие трафика с актива».
3. Дождитесь обновления информации о сессиях на странице **Сессии** (до 5 минут) — такая задержка допустима из-за особенностей передачи данных с сенсоров на Комплекс.
4. Дождитесь обновления информации об активах на странице **Активы** (до 5 минут) — такая задержка допустима из-за особенностей передачи данных с сенсоров на Комплекс.

Частичное зеркалирование сетевого трафика

Способ устранения

Для устранения затруднения:

1. Создайте актив вручную на странице **Активы** веб-интерфейса Комплекса.
2. Отредактируйте сетевые настройки в реквизитах созданного актива.

> Подсказка:
>
> Подробнее см. раздел «Работа с активами» Руководства по эксплуатации.

6.3.8. Комплекс не обнаруживает активы без IP-адреса

Комплекс не обнаруживает активы, все или некоторые интерфейсы которых не имеют IP-адреса (узлы, работающие на канальном уровне модели OSI).

Причина: переменная в файле manager.env AUTOMATIC_HOST_CREATION_BY_MAC имеет значение true

Способ устранения

Для устранения затруднения:

1. Подключитесь к операционной системе Комплекса уровня Management.
2. Остановите работу сервисов, выполнив команду:

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

3. Дождитесь остановки работы всех сервисов.
4. В конфигурационном файле `manager.env` присвойте переменной `AUTOMATIC_HOST_CREATION_BY_MAC` значение `false`.
5. Запустить работу сервисов командой:

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

6. Дождитесь запуска работы всех сервисов.
7. Убедитесь, что активы, интерфейсы которых не имеют IP-адреса, обнаруживаются и отображаются на странице **Активы** веб-интерфейса Комплекса.

6.3.9. Два актива с одинаковым IP-адресом

В списке на странице **Активы** отображается новый актив с IP-адресом актива, который уже был в списке. Возможные причины:

- При снятии трафика с нескольких точек актив был обнаружен с MAC-адресом маршрутизатора
- Один актив был обнаружен несколькими сенсорами

При снятии трафика с нескольких точек актив был обнаружен с MAC-адресом маршрутизатора

> Подсказка:
>
> Если актив был обнаружен сперва со своим IP-адресом и MAC-адресом маршрутизатора, а уже после был распознан MAC-адрес самого актива, то на странице **Активы** будут отображаться оба актива (с одинаковым IP и разными MAC-адресами). Такое поведение необходимо для отслеживания попыток подмены MAC-адреса.

Способ устранения

Для устранения затруднения:

В карточке более раннего актива присвойте ему интерфейс с MAC-адресом маршрутизатора:

a. Перейдите в **карточку актива**.

б. Нажмите кнопку ✎ напротив блока **Сетевые атрибуты**.

- **Результат шага:** появится окно **Редактирование сетевых атрибутов актива**.

в. Отметьте параметр **Выбрать сетевой атрибут неизвестного актива**.

г. В выпадающем списке выберите интерфейс неизвестного актива с тем же IP-адресом.

д. Нажмите  (**Создать сетевой атрибут**) для подтверждения изменений.

е. Установите чекбокс **Интерфейс для сбора данных** напротив интерфейса с собственным MAC-адресом.

ж. Нажмите  (**Сохранить изменения**) для подтверждения изменений.

> Подсказка:
>
> Подробнее о присвоении активам интерфейсов других активов см. раздел «Редактирование актива» Руководства по эксплуатации.

▸ **Результат шага:** Актив, чей единственный интерфейс был привязан к другому активу, будет удален из списка на странице **Активы**.

Один актив был обнаружен несколькими сенсорами

Способ устранения

Для устранения затруднения:

1. На странице **Сенсоры** веб-интерфейса Комплекса убедитесь, что добавленные контролируемые сети сенсоров не пересекаются друг с другом.
2. В карточке одного актива присвойте ему интерфейс другого актива согласно инструкции в п. выше «При снятии трафика с нескольких точек актив был обнаружен с MAC-адресом маршрутизатора».

6.3.10. Не осуществляется сбор необходимых событий или конфигураций с активов

Для проблем со сбором событий или конфигураций могут быть следующие причины:

- Некорректные настройки актива
- Ошибки в Python-скрипте сбора данных, неверные настройки учетных данных актива или расписания задачи сбора данных

> Подсказка:
>
> Список возможных проблем сбора данных см. в разделе «Рекомендуемые действия в случае обнаружения событий на панели мониторинга "Сбор данных"» Руководства по эксплуатации.

Некорректные настройки актива

Способ устранения

Для устранения затруднения:

1. Убедитесь в корректности настроек служб и разрешений для сбора данных с выбранного актива.
2. Убедитесь, что активу присвоены учетные данные с правами, которые:
    - позволяют получать информацию удаленно;
    - позволяют получать критичную информацию, запрашиваемую скриптом сбора данных.

Ошибки в Python-скрипте сбора данных, неверные настройки учетных данных актива или расписания задачи сбора данных

Способ устранения

Для устранения затруднения:

1. Проанализируйте сообщения об ошибках на страницах **Статус сбора**, **Задачи сбора**, **События**, на панели мониторинга Сбор данных и на диаграммах в карточке актива.
2. Просмотрите содержание Python-скриптов сбора данных из сканеров, работа которых завершается ошибками, и найдите в них названия сервисов, участвующих в сборе данных (коннекторов). Название расположено в скобках после команды `execute`.

```
table = execute('sql',protocol_args, expiration)
return {
    'visible_keys': {
        'ID': 'Идентификатор группы',
        'name': 'Имя группы',
        'EXPTIME': 'Параметры отключения пользователей',
    },
    'keys': ['ID','name','EXPTIME'],
    'data': [[str(row[col]) for col in ['ID','name','EXPTIME']] for row in table]
}
```

Рис. 98. Расположение названия коннектора в Python-скрипте сбора данных

3. На странице **Сенсоры** найдите сенсор, прослушивающий контролируемую сеть актива.
4. Подключитесь к операционной системе сенсора, который собирает данные из контролируемой сети актива.
5. Просмотрите список имеющихся сервисов-коннекторов:

```
systemctl list-units *-connector.service --all
```

▸ **Результат шага:** будет выведен список сервисов-коннекторов.

```
[root@DATAPKTESTTK22 ~]# systemctl list-units *-connector.service --all
  UNIT                                LOAD   ACTIVE SUB     DESCRIPTION
  udv-modbus-connector.service        loaded active running Modbus connector
  udv-opc-connector.service           loaded active running Opc connector service
  udv-plc-config-connector.service loaded active running Config acquisition from PLC
  udv-plc-connector.service           loaded active running Data acquisition from PLC by oven and s7comm protocol.
  udv-snmp-connector.service          loaded active running SNMP connector
  udv-sql-connector.service           loaded active running Service for connecting to a database
  udv-terminal-connector.service      loaded active running Terminal connector

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.
7 loaded units listed.
To show all installed unit files use 'systemctl list-unit-files'.
```

Рис. 99. Список коннекторов Комплекса

6. Найдите подходящий коннектор.

> Подсказка:
>
> Название коннектора в выводе команды не полностью совпадает с названием в Python-скрипте сбора данных. За исключением `msrpc` название коннектора в выводе команды содержит `_connector`.

7. Просмотрите журналы коннекторов, на которых обнаружены проблемы. Например `udv-host-data-collector`:

   ```
   journalctl -fu udv-host-data-collector.service
   ```

8. Посмотрите журналы сервиса `udv-command-processor`, который отвечает за все запущенные процессы сбора данных:

   ```
   journalctl -fu udv-command-processor.service
   ```

9. При необходимости отредактируйте сканеры сбора данных, расписание задачи, учетные данные актива.

6.3.11. При попытке сбора данных в результатах выводится предупреждение «Превышено время ожидания выполнения задачи сбора событий»

Для получения предупреждения `Превышено время ожидания выполнения задачи сбора событий` возможны следующие причины:

- Актив не может принять несколько одновременных подключений к нему по одному или нескольким протоколам
- Переполнена очередь задач сбора данных в сервисе udv-rabbitmq Комплекса
- Заканчивается максимальное время ожидания выполнения задачи сбора данных

> Подсказка:
>
> Список возможных проблем сбора данных см. в разделе «Рекомендуемые действия в случае обнаружения событий на панели мониторинга "Сбор данных"» Руководства по эксплуатации.

Актив не может принять несколько одновременных подключений к нему по одному или нескольким протоколам

Рекомендации по настройке запуска задач сбора данных с одного актива

Для устранения затруднения:

1. Настраивайте сбор событий с промежутком между запусками задач (для каждой задачи установите отдельное от остальных задач время выполнения).
2. Используйте сканеры сбора событий с ОС Windows, которые собирают только критичные события.
3. В одну задачу добавляйте не более одного сканера сбора данных.

Переполнена очередь задач сбора данных в сервисе udv-rabbitmq Комплекса

Способ устранения

Для устранения затруднения:

1. Перейдите в карточку актива (или нескольких активов), для которого настроено расписание задачи сбора данных.
2. Отмените выполнение одной или нескольких задач сбора данных по расписанию (отмените выбор чекбокса ☑ в строке с названием задачи).
3. Подключитесь к операционной системе Комплекса уровня Management.
4. Остановите работу сервисов, выполнив команду:

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

5. Выполните команду очистки очереди сервиса udv-rabbitmq. Для этого выполните команду:

```
rm -rf /var/lib/rabbitmq/mnesia/*
```

6. Запустите работу сервисов командой:

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

7. Дождитесь запуска работы всех сервисов.
8. Выполните повторный запуск сбора данных.

Заканчивается максимальное время ожидания выполнения задачи сбора данных

Способ устранения

Увеличьте максимальное время ожидания выполнения задачи сбора данных для одного сканера.

1. Перейдите на страницу **Администрирование → Инспекция активов → Сканеры**.
2. Откройте необходимый сканер сбора данных на редактирование.
3. Увеличьте значение в поле **Максимальное время ожидания выполнения задачи**.
4. Нажмите кнопку **Сохранить** для подтверждения изменений.
5. Дождитесь сбора задачи сбора данных, создайте новую или запустите сканер.

6.3.12. Сбор конфигураций осуществляется, но результаты сбора не отображаются

Подсказка:

Список возможных проблем сбора данных см. в разделе «Рекомендуемые действия в случае обнаружения событий на панели мониторинга "Сбор данных"» Руководства по эксплуатации.

Причина: некорректный Python-скрипт сбора данных, неверное регулярное выражение

Способ устранения

Для устранения затруднения:

Проверьте на корректность Python-скрипт из сканера, работа которого завершается с ошибкой.

Внимание:

Для первого запуска рекомендуется отказаться от синтаксического разбора данных в скрипте посредством регулярных выражений.

6.3.13. Отсутствуют внешние или внутренние события на странице «События»

На странице **События** частично или полностью отсутствуют события. В качестве причин рассмотрены следующие:

- Генерация внутренних событий отключена в настройках переменных
- Диск операционной системы Комплекса заполнен более, чем на 90%, и внешние события больше не принимаются

Генерация внутренних событий отключена в настройках переменных

В конфигурационном файле `manager.env` Комплекса уровня Management переменным, отвечающим за отключение и включение генерации внутренних событий от служебных источников, присвоены значения `true` (генерация событий отключена).

Способ устранения

Для устранения затруднения:

Присвойте необходимым переменным значение `false` или удалите переменные из файла `manager.env`.

> Подсказка:
>
> Порядок работы с указанными переменными приведен в подразделе «Включение и отключение служебных источников» Руководства по эксплуатации.

Диск операционной системы Комплекса заполнен более, чем на 90%, и внешние события больше не принимаются

Сервис хранения и поиска внешних событий недоступен в результате заполнения дискового пространства более, чем на 90%.

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на операционной системе Комплекса уровня Management.
2. Убедитесь, что сервис хранения и поиска событий недоступен:

   ```
   journalctl -fu udv-logstash.service
   ```

   - **Результат шага:** в журнале будут отображаться события вида `Opensearch в режиме read-only`.
3. Остановите работу сервисов Комплекса:

   ```
   systemctl stop udv-* --all
   ```
4. Удалите ненужные файлы с дискового пространства.
5. При необходимости измените значения переменных `EVENT_INDICES_MAX_SIZE_GB` и `EVENT_ARCHIVES_MAX_SIZE_GB`:

   a. Откройте на редактирование файл `manager.env`.

   б. Найдите и измените значения переменных:

```
EVENT_INDICES_MAX_SIZE_GB=[значение]
EVENT_ARCHIVES_MAX_SIZE_GB=[значение]
```

> Внимание:
>
> Суммарный объем с `EVENT_ARCHIVES_MAX_SIZE_GB` не должен составлять более 50-60% объема дискового пространства
>
> На Комплексах базового уровня и (или) с HDD — не более 100 ГБ. На Комплексах среднего и верхнего уровней с SSD — не более 300 ГБ

6. Очистите репозиторий с пакетами.
7. Если предыдущие способы не дали результата, очистите метаданные сервиса.

> ОСТОРОЖНО:
>
> При очистке будут утеряны все индексы событий и элементы раздела **Мониторинг**: шаблон индекса, панели мониторинга, сохраненные поиски, фильтры.

Для очистки выполните команду:

```
rm -rf /var/lib/opensearch/nodes/*
```

8. Восстановите утерянные данные.

> Подсказка:
>
> Подробнее о настройке см. разделы «Создание шаблона индекса», «Импорт сохраненных объектов» Руководства по эксплуатации.

9. Запустите сервисы Комплекса:

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

10. Убедитесь в работоспособности сервиса хранения и поиска событий:

    а. Выполните следующий запрос:

    ```
    curl -XPUT "http://127.0.0.1:9200/_settings" -H 'Content-Type: application/json' -d
     '{"index":{"blocks":{"read_only_allow_delete":"false"}}}'
    ```

    ▸ **Результат шага:** запись вида `"acknowledged":true` свидетельствует об успешном выполнении запроса.

    б. Выполните действия, в результате которых должны появиться события.

> Подсказка:
>
> Например, создайте и удалите новые элементы справочников (правил, классификаторов), выполните сбор событий или конфигураций с актива.

в. Перейдите на страницу **События**.

г. Найдите события по результатам выполненных действий.

11. Если события отсутствуют, ознакомьтесь с инструкциями ниже по устранению нештатных ситуаций.

См. также

Не инициализируются сервисы udv-opensearch, udv-opensearch-dashboards, udv-logstash модуля «Управление внешними событиями»

6.3.14. Не принимаются Syslog-сообщения от активов

Для отсутствия сообщений Syslog от активов могут быть следующие причины:

- Наименование актива не совпадает с сетевым именем (hostname) узла или в списке активов присутствуют активы с такими же IP-адресами
- Не создан или некорректно создан источник для приема Syslog-сообщений
- Некорректная настройка отправки Syslog-сообщений на активе

Наименование актива не совпадает с сетевым именем (hostname) узла или в списке активов присутствуют активы с такими же IP-адресами

Способ устранения

Для устранения затруднения:

1. Убедитесь, что наименование актива совпадает с его hostname.
2. Убедитесь в отсутствии известных активов с такими же IP-адресами.

Не создан или некорректно создан источник для приема Syslog-сообщений

Способ устранения

Для устранения затруднения:

Убедитесь, что источник для приема Syslog-сообщений выбранного актива корректно инициализирован на странице **Администрирование → Настройка активов → Источники**.

Некорректная настройка отправки Syslog-сообщений на активе

Способ устранения

Для устранения затруднения:

Проверьте настройки отправки Syslog-сообщений на активе, убедитесь, что актив отправляет события на требуемый IP-адрес и порт.

6.3.15. Не принимаются сообщения от службы обнаружения вторжений

Причина: наименование служебного актива не совпадает с сетевым именем (hostname) Комплекса

Способ устранения

Для устранения затруднения:

1. Убедитесь, что наименование Комплекса уровня Management совпадает с его сетевым именем на странице **Администрирование → О системе**.
2. Подключитесь к операционной системе Комплекса уровня Management.
3. Выполните команду `export`. Убедитесь, что переменная `HOSTNAME` присутствует в выводе команды и содержит сетевое имя Комплекса.
4. Если переменная `HOSTNAME` отсутствует в выводе команды `export`:

    а. Остановите работу сервисов Комплекса без удаления накопленных данных.

    б. Откройте файл `/etc/profile` в режиме редактирования с помощью редактора `mcedit`:

    ```
    mcedit /etc/profile
    ```

    в. Добавьте в конец файла строку:

    ```
    export HOSTNAME
    ```

    г. Сохраните изменения и закройте файл `/etc/profile`.

    д. Перезагрузите сеанс пользователя или перезагрузите ОС.

    е. Запустите работу сервисов Комплекса.

    ж. Убедитесь, что наименование Комплекса совпадает с его сетевым именем на странице **Администрирование → О системе**.

6.3.16. Не принимаются сообщения от службы корреляции

В качестве причин рассмотрены следующие:

- Наименование служебного актива не совпадает с сетевым именем (hostname) Комплекса
- Некорректная или устаревшая директория logstash

Наименование служебного актива не совпадает с сетевым именем (hostname) Комплекса

Способ устранения

Для устранения затруднения:

1. Убедитесь, что наименование Комплекса уровня Management совпадает с его сетевым именем на странице **Администрирование → О системе**.
2. Подключитесь к операционной системе Комплекса уровня Management.
3. Выполните команду `export`. Убедитесь, что переменная `HOSTNAME` присутствует в выводе команды и содержит сетевое имя Комплекса.

4. Если переменная `HOSTNAME` отсутствует в выводе команды `export`:

    а. Остановите работу сервисов Комплекса без удаления накопленных данных.

    б. Откройте файл `/etc/profile` в режиме редактирования с помощью редактора `mcedit`:

    ```
    mcedit /etc/profile
    ```

    в. Добавьте в конец файла строку:

    ```
    export HOSTNAME
    ```

    г. Сохраните изменения и закройте файл `/etc/profile`.

    д. Перезагрузите сеанс пользователя или перезагрузите ОС.

    е. Запустите работу сервисов Комплекса.

    ж. Убедитесь, что наименование Комплекса совпадает с его сетевым именем на странице **Администрирование → О системе**.

Некорректная или устаревшая директория logstash

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

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

2. Дождитесь остановки работы всех сервисов.
3. Переустановите сервис `udv-logstash`, выполнив команду:

    ```
    apt-get install --reinstall udv-logstash -y
    ```

4. Запустите работу сервисов командой:

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

5. Дождитесь запуска работы всех сервисов.

6.3.17. Не инициализируются сервисы udv-opensearch, udv-opensearch-dashboards, udv-logstash модуля «Управление внешними событиями»

Возможны следующие причины:

- Некорректное значение системной переменной vm.max_map_count
- Ошибки в настройках нормализациии

Некорректное значение системной переменной vm.max_map_count

Способ устранения

Для устранения затруднения:

1. Проверьте значение переменной в операционной системе Комплекса уровня Management. Для этого выполните команду:

```
sysctl vm.max_map_count
```

2. Убедитесь, что данная переменная имеет значение `262144`.
3. При необходимости откорректируйте значение переменной. Для этого:
    a. Откройте файл `/etc/sysctl.conf`.
    б. Добавьте строку `vm.max_map_count=262144`.
    в. Либо, если строка с переменной уже была добавлена, измените значение переменной.
4. Выполните команду для немедленной установки переменной `vm.max_map_count` (без перезагрузки):

```
sysctl -w vm.max_map_count=262144
```

Ошибки в настройках нормализациии

Способ устранения

Для устранения затруднения:

1. Посмотрите журнал сервиса `udv-logstash`. Для этого введите команду:

```
journalctl -fu udv-logstash.service
```

2. Остановите работу сервисов, выполнив команду:

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

3. Дождитесь остановки работы всех сервисов.
4. Переустановите сервис udv-logstash, выполнив команду:

```
apt-get install --reinstall udv-logstash -y
```

5. Запустите работу сервисов командой:

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

6. Дождитесь запуска работы всех сервисов.

См. также

Отсутствуют внешние или внутренние события на странице «События»

6.3.18. Не создается индекс в экспертном режиме страницы «События»

Причина: отсутствуют события в Комплексе

Способ устранения

Для устранения затруднения:

1. Сгенерируйте события действий в веб-интерфейсе.

> Подсказка:
>
> Например, создайте и удалите новые элементы справочников (правил, классификаторов), выполните сбор событий или конфигураций с актива.

2. Создайте или включите источники активов и сгенерируйте на них события.

6.3.19. Не удается отфильтровать записи в экспертном режиме страницы «События» по новым значениям полей после нормализации

Причина: отсутствуют события с новыми полями, не обновлен шаблон индекса

Способ устранения

Для устранения затруднения:

1. Обновите шаблон индекса на странице **Администрирование → Настройки мониторинга**, вкладка **Шаблоны Индексов**.
2. Убедитесь, что после нормализации было принято событие с новыми полями (помеченными желтым восклицательным знаком на странице **События → Экспертный режим**).

6.3.20. Объекты мониторинга и визуализации импортируются с ошибкой

Причина: отсутствуют нужные поля в шаблоне индекса

Способ устранения

Для устранения затруднения:

1. Убедитесь в целостности директории `/etc/logstash`, расположенном в рабочей директории Комплекса уровня Management.
2. Убедитесь, что все нужные поля присутствуют в шаблоне индекса.
3. При отсутствии необходимых полей:
    a. Обновите шаблон индекса.
    б. Убедитесь, что было принято событие с новыми полями.
    в. Удалите сохраненные объекты (страница **Мониторинг → Настройки мониторинга**, вкладка **Сохраненные Объекты**).
    г. Повторите импорт.

6.3.21. Не удается импортировать сканер сбора данных в веб-интерфейсе

Для проблем с импортом сканера сбора данных могут быть следующие причины:

- Неверная цепочка сертификатов для проверки цифровой подписи Python-скрипта в сканере
- Неверная кодировка Python-скрипта сбора данных
- Сканер сбора данных был изменен с момента создания его последней цифровой подписи

Неверная цепочка сертификатов для проверки цифровой подписи Python-скрипта в сканере

Способ устранения

Для устранения затруднения:

1. Убедитесь, что конечный сертификат `datapk_script.crt`, используемый для проверки подлинности Python-скриптов сбора данных, является клиентским для корневого сертификата `ca.crt`. Для этого выполните следующую команду:

   ```
   openssl verify
    -CAfile /usr/share/udv/certs/ca.crt /usr/share/udv/scripts-certs/datapk_script.crt
   ```

   ▸ **Результат шага:** если верификация пройдет успешно, в командную строку будет выведена следующая информация:

   ```
   /usr/share/udv/scripts-certs/datapk_script.crt: OK
   ```

2. При необходимости замените конечный сертификат `datapk_script.crt` и повторно выполните верификацию.
3. Повторно выполните цифровую подпись Python-скрипта. Подробнее см. раздел «Цифровая подпись Python-скрипта».
4. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

Неверная кодировка Python-скрипта сбора данных

Способ устранения

Для устранения затруднения:

1. Откройте Python-скрипт сбора данных с помощью текстового редактора.
2. Убедитесь, что Python-скрипт имеет кодировку UTF-8 без BOM. При необходимости измените кодировку и сохраните изменения.
3. Повторно выполните цифровую подпись Python-скрипта. Подробнее см. раздел «Цифровая подпись Python-скрипта».
4. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

Сканер сбора данных был изменен с момента создания его последней цифровой подписи

Python-скрипт, размещенный и подписываемый в операционной системе Комплекса, не совпадает со скриптом, размещенным на локальной ОС и загружаемым в веб-интерфейсе Комплекса) при создании сканера.

Способ устранения

Для устранения затруднения:

1. Убедитесь в целостности Python-скрипта сбора данных.
2. Повторно выполните цифровую подпись Python-скрипта. Подробнее см. раздел «Цифровая подпись Python-скрипта».
3. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

См. также

Создание сканера сбора данных

Управление сканерами сбора данных

Импорт сканеров и их групп

6.3.22. Не выполняется архивация внешних событий при превышении размера или времени хранения индекса

Возможны следующие причины:

- Директориям, в которые выполняется загрузка архивов, не присвоены права для загрузки в них файлов
- В переменной файла manager.env настроено удаление индексов вместо сохранения в архив

Директориям, в которые выполняется загрузка архивов, не присвоены права для загрузки в них файлов

Способ устранения

Для устранения затруднения:

1. Подключитесь к операционной системе Комплекса уровня Management.
2. Убедитесь, что следующим директориям, расположенным в рабочей директории Комплекса уровня Management, присвоены права доступа `drwxrwxrwx`:
   - `/var/backups/elasticsearch`:
     - `/var/backups/elasticsearch/indices`
     - `/var/backups/elasticsearch/uploads`

   Для этого введите команду:

   ```
   ls -la [путь к директории]
   ```

3. При необходимости измените права на указанные директории с помощью следующих команд:

   ```
   chmod -R 777 /var/backups/elasticsearch
   ```

   где ключ `-R` — рекурсивное изменение прав (они будут применены и к вложенным директориям).
4. Повторно выполните архивацию событий (индексов) через веб-интерфейс Комплекса (подробнее см. раздел «Выгрузка событий Комплекса в архив» Руководства по эксплуатации).

В переменной файла manager.env настроено удаление индексов вместо сохранения в архив

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

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

2. В конфигурационном файле `manager.env` присвойте переменной `EVENT_INDICES_ACTION_SIZE_EXCEEDED` значение `rotate`.
3. Запустите работу сервисов командой:

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

4. Дождитесь запуска работы всех сервисов.

6.3.23. Ошибки вида «<...>Cannot start service <...>. Bind for <ip_address>:<TCP/UDP_port> is ready allocated» при попытке запуска сервисов

Причина: указанный в тексте ошибки TCP или UDP-порт требуется для запуска сервиса, но он занят сторонним сервисом или утилитой

Способ устранения

Для устранения затруднения:

1. Измените номер используемого порта для стороннего сервиса в настройках сервиса.
2. При невозможности изменения номера порта отключите сторонний сервис, которым занят порт:

   а. Узнайте наименование сервиса, которым занят порт, с помощью команды:

```
netstat -tulpn | grep [номер_порта]
```

   ▸ **Результат шага:** в выводе команды в последнем столбце отображаются наименование сервиса, занятый им порт и идентификатор процесса.

```
[root@DATAPKTESTTK22 ~]# netstat -tulpn | grep 9300
tcp        0      0 127.0.0.1:9300            0.0.0.0:*               LISTEN      13005/java
```

Рис. 100. Наименование сервиса, занятый им порт и идентификатор процесса в последнем столбце вывода команды

   б. Остановите процесс с полученным номером:

```
kill -9 [идентификатор_процесса]
```

   в. При необходимости остановки процесса и его дочерних процессов:

```
killall [идентификатор_процесса]
```

   г. Повторите запуск работы сервисов Комплекса.

6.3.24. Недоступен сервис корреляции событий

Причина: ретроспективный анализ был удален до того, как проверка была завершена

Способ устранения

Для устранения затруднения:

1. Подключитесь к операционной системе Комплекса уровня Management.
2. Перезапустите сервис корреляции событий. Для этого введите следующую команду:

```
systemctl restart udv-esper.service
```

3. Дождитесь окончания перезапуска сервиса.
4. Убедитесь в работоспособности службы корреляции событий в веб-интерфейсе.

6.3.25. При бездействии в веб-интерфейсе сеанс завершается раньше, чем через 10 минут

В качестве причин раннего завершения сеанса рассмотрены следующие:

- Время завершения сеанса пользователя при бездействии задано меньше 10 минут
- Под уже используемой учетной записью совершил вход другой пользователь

Время завершения сеанса пользователя при бездействии задано меньше 10 минут

Время бездействия в веб-интерфейсе, после которого текущая сессия пользователя автоматически завершается и происходит переход на страницу авторизации, настраивается в переменной `USER_SESSION_INACTIVITY_TIMEOUT` файла `manager.env` Комплекса уровня Management и по умолчанию равно 600 секунд.

Способ устранения

Для устранения затруднения:

1. Перейдите в командную строку операционной системы Комплекса уровня Management.
2. Остановите работу сервисов, выполнив команду:

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

3. Дождитесь остановки работы всех сервисов.
4. В конфигурационном файле `manager.env` присвойте переменной `USER_SESSION_INACTIVITY_TIMEOUT` необходимый лимит времени бездействия в секундах.
5. Запустить работу сервисов командой:

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

6. Дождитесь запуска работы всех сервисов.

   ▸ **Результат шага:** сессия пользователей будет завершаться после времени бездействия, указанного в переменной `USER_SESSION_INACTIVITY_TIMEOUT`.

Под уже используемой учетной записью совершил вход другой пользователь

Ограничение на количество сессий под одной учетной записью настраивается в переменной `LIMIT_USER_SESSIONS` файла `manager.env` Комплекса уровня Management. По умолчанию разрешается вход с неограниченного количества устройств под одной учетной записью (переменная имеет значение `false`) — при создании новой сессии предыдущая завершается.

Способ устранения

Для устранения затруднения:

1. При необходимости создайте в веб-интерфейсе новые учетные записи для других пользователей.
2. При необходимости отключите ограничение на вход под одной учетной записью:

а. Остановите работу сервисов, выполнив команду:

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

б. В конфигурационном файле `manager.env` добавьте переменную `LIMIT_USER_SESSIONS` и установите ей значение `false`.

в. Запустите работу сервисов командой:

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

г. Дождитесь запуска работы всех сервисов.

▸ **Результат шага:** станет возможным вход в веб-интерфейс под любой учетной записью с любого количества устройств.

6.3.26. Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России

Возможны следующие ошибки поиска уязвимостей в базах Common Vulnerabilities and Exposures и Common Platform Enumeration:

- Ошибка вида «Не удалось получить список ПО. Убедитесь, что данные об установленном ПО были собраны корректно»
- Ошибка вида «Не удалось сохранить отчет. Убедитесь в работоспособности Комплекса или обратитесь к администратору»
- Ошибка вида «Непредвиденная ошибка. Убедитесь в работоспособности Комплекса или обратитесь к администратору»
- Ошибка вида «ПО для сканирования уязвимостей в реестре CPE не обнаружено»

6.3.26.1. Ошибка вида «Не удалось получить список ПО. Убедитесь, что данные об установленном ПО были собраны корректно»

Возможны следующие причины:

- Не удается запустить сканер сбора списка ПО, либо запуск завершается с ошибками
- Сканер запустился, но не отображает результаты на странице «Список ПО»

Не удается запустить сканер сбора списка ПО, либо запуск завершается с ошибками

Способ устранения

Для устранения затруднения перейдите в раздел «Не осуществляется сбор необходимых событий или конфигураций с активов» или «При попытке сбора данных в результатах выводится предупреждение «Превышено время ожидания выполнения задачи сбора событий»».

Сканер запустился, но не отображает результаты на странице «Список ПО»

Способ устранения

Для устранения затруднения перейдите в раздел «Сбор конфигураций осуществляется, но результаты сбора не отображаются».

6.3.26.2. Ошибка вида «Не удалось сохранить отчет. Убедитесь в работоспособности Комплекса или обратитесь к администратору»

Возможны следующие причины:

- Отсутствие свободного места на диске
- Ошибки в сервисе udv-vulnerability-backend

Отсутствие свободного места на диске

Способ устранения

Для устранения затруднения:

1. Проверьте свободное место на диске, выполнив команду:

   ```
   df -h /
   ```

2. При отсутствии свободного места:
   a. Остановите сервисы Комплекса.
   б. Удалите ненужные данные с диска.
   в. Запустите сервисы Комплекса.

Ошибки в сервисе udv-vulnerability-backend

Способ устранения

Для устранения затруднения:

1. Убедитесь, что в журнале системных сообщений сервиса `udv-vulnerability-backend` нет ошибок, по команде:

   ```
   journalctl -fu udv-vulnerability-backend.service
   ```

2. При ошибках в журналах сервисов см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

6.3.26.3. Ошибка вида «Непредвиденная ошибка. Убедитесь в работоспособности Комплекса или обратитесь к администратору»

Причина: ошибки в сервисе поиска уязвимостей

Способ устранения

Для устранения затруднения:

1. Убедитесь, что в журналах системных сообщений сервиса `udv-vulnerability-backend` нет ошибок, по команде:

   ```
   journalctl -fu udv-vulnerability-backend.service
   ```

2. При ошибках в журналах сервисов см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

6.3.26.4. Ошибка вида «ПО для сканирования уязвимостей в реестре CPE не обнаружено»

Причина: для ПО, по которому выполнялся поиск уязвимостей, элементы CPE подобраны с недостаточной точностью, либо их не удалось подобрать

Способ устранения

Для устранения затруднения перейдите в раздел «Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE».

6.3.27. Не устанавливается соединение с сенсором

В качестве причины недоступности сенсора при первом подключении рассмотрены следующие:

- Отключен межсетевой экран iptables на сенсоре или Комплексе уровня Management
- Некорректные настройки подключения сенсора

Если сенсор стал недоступен в процессе корректной работы, см. причину «Ошибки в работе сервисов в период корректной работы иерархии».

Отключен межсетевой экран iptables на сенсоре или Комплексе уровня Management

> Внимание:
>
> Если сенсор или Комплекс установлены на ОС Альт Сервер, необходимо использовать `iptables` в качестве межсетевого экрана.

Способ устранения

Для устранения затруднения:

1. В командной строке операционной системы сенсора:

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

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

   > Внимание:
   >
   > Значение параметра `CONFIG_FW` должно быть `no`.

   б. Убедитесь, что межсетевой экран `iptables` запущен:

   ```
   systemctl status iptables
   ```

   > Подсказка:
   >
   > Сервис должен быть в состоянии `active`.

в. При необходимости выполните настройки `iptables` сенсора и запустите `iptables` согласно инструкциям в следующих разделах Руководства по внедрению и поддержке:

- «Установка Комплекса уровня Sensor» и «Установка Комплекса уровня Management» (при установке сенсора и Комплекса уровня Management на разных серверах);
- «Установка Комплекса уровня Management+Sensor на одном аппаратном средстве» (при установке сенсора и Комплекса уровня Management на одном сервере).

2. Выполните шаг 1 в командной строке операционной системы Комплекса уровня Management.

Некорректные настройки подключения сенсора

Способ устранения

Для устранения затруднения убедитесь в корректности настроек подключения сенсора к Комплексу уровня Management — для этого вы можете воспользоваться инструкцией «Подключение сенсора к другому Комплексу уровня Management».

Ошибки в работе сервисов в период корректной работы иерархии

Способ устранения

Если сенсор стал недоступен в процессе корректной работы, ошибки будут отображаться на странице **Сенсоры** веб-интерфейса Комплекса. В таблице ниже приведен список возможных ошибок, причины их возникновения и сервисы, работоспособность которых необходимо проверить.

Табл. 5. Возможные ошибки в процессе работы иерархии

НАИМЕНОВАНИЕ ОШИБКИ	ВОЗМОЖНАЯ ПРИЧИНА	СЕРВИС, ОТВЕЧАЮЩИЙ ЗА РАБОТУ ИЕРАРХИИ
Не удается получить статус	Не поступает информация о состоянии сервисов `udv-rabbitmq`, `udv-rabbitmq-sensor`, `udv-redis` или `udv-redis-sensor`	Уровень Sensor: • `udv-node-exporter-sensor` • `udv-pushgateway` Уровень Management: • `udv-node_exporter` • `udv-prometheus`
Получение данных недоступно	Затруднения в работе сервиса отправки оперативных данных с сенсора	`udv-rabbitmq-sensor` (уровень Sensor)
	Затруднения в работе сервиса получения оперативных данных с сенсора на Комплексе	`udv-rabbitmq` (уровень Management)
Синхронизация настроек недоступна	Затруднения в работе сервиса отправки справочников с Комплекса на сенсор	`udv-redis` (уровень Management)

Табл. 5. Возможные ошибки в процессе работы иерархии

НАИМЕНОВАНИЕ ОШИБКИ	ВОЗМОЖНАЯ ПРИЧИНА	СЕРВИС, ОТВЕЧАЮЩИЙ ЗА РАБОТУ ИЕРАРХИИ
	Затруднения в работе сервиса получения справочников на сенсоре	`udv-redis-sensor` (уровень Sensor)
Не удается установить соединение с сенсором	Совокупность причин, приведенных выше	Все сервисы, приведенные выше

Для устранения затруднения:

1. Просмотрите ошибку на странице **Сенсоры** веб-интерфейса Комплекса.
2. По таблице выше определите список сервисов, для которых необходимо просмотреть журнал.
3. Просмотрите журнал выбранного сервиса при помощи команды:

```
journalctl -fu [наименование_сервиса] -n [количество последних строк журнала, которое
 нужно показать]
```

4. При ошибках в журналах сервисов см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

6.3.28. Не работает сложное исключение для правила службы обнаружения вторжений

Причина: при создании исключения в виде pass-правила использовалась конструкция вида threshold: type both и/или threshold: type limit

Способ устранения

Для устранения затруднения:

1. Деактивируйте нерабочее правило службы обнаружения вторжений.
2. Создайте новое правило, добавив исключения для IP-адресов и портов.

> **Пример**
>
> в Комплексе создано правило службы обнаружения вторжений с конструкцией `threshold: type both`:
>
> ```
> alert tcp any any -> any any (msg:"ET SCAN NMAP -sS window 1024"; fragbits:!D;
>  dsize:0; flags:S,12; ack:0; window:1024; threshold: type both, track by_dst, count 1,
>  seconds 60; reference:url,doc.emergingthreats.net/2009582; classtype:attempted-recon;
>  sid:2009582; rev:3; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
> ```
>
> Измененное правило будет выглядеть следующим образом:
>
> ```
> pass tcp 192.168.0.1 any -> 192.168.0.2 any (msg:"ET SCAN NMAP -sS
>  window 1024"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:1024;
>  reference:url,doc.emergingthreats.net/2009582; classtype:attempted-recon; sid:
>  94000000-94999999;)
> ```

6.3.29. Ошибка «An HTTP request took too long to complete» при запуске docker-контейнеров модуля обнаружения и реагирования для ПЛК (EDR for PLC)

Причина: Недостаточный размер оперативной памяти аппаратного комплекса или виртуальной машины, на которой развернут Комплекс

Способ устранения

Для устранения затруднения:

Увеличьте размер оперативной памяти.

6.3.30. Обнаружен конфликт версий проектов ПЛК

При одновременной работе разных пользователей с одним проектом возникает ошибка Обнаружен конфликт версий.

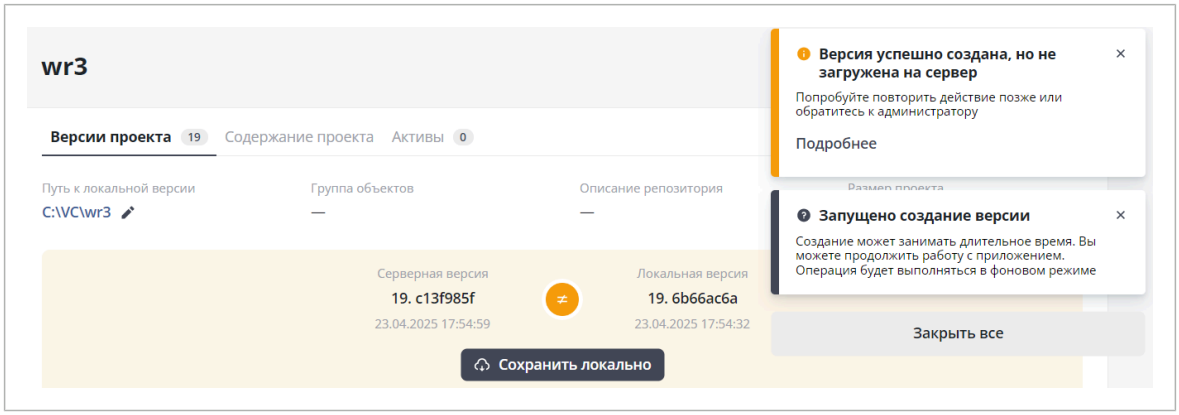


Рис. 101. Обнаружен конфликт версий

Причина

При одновременной работе разных пользователей с одним проектом возможна ситуация, когда пользователь 1 загрузил изменения на сервер, и проект получил новую версию. В таком случае при попытке пользователя 2 загрузить изменения предыдущей версии проекта возникнет ошибка Обнаружен конфликт версий.

Способ устранения

1. Нажмите кнопку **Сохранить локально**.
   - **Результат шага:** откроется окно **Обнаружен конфликт версий**.

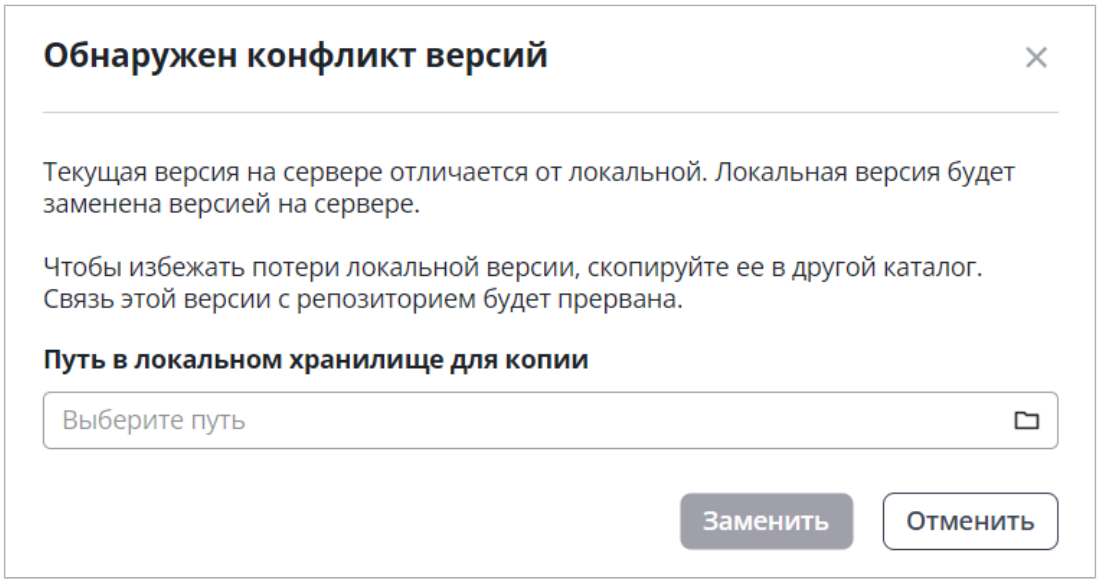


Рис. 102. Обнаружен конфликт версий

2. Укажите новый путь к файлам репозитория или выберите новое локальное хранилище с помощью кнопки 🗀
3. Нажмите кнопку **Заменить**.

   ▸ **Результат шага:** система переместит файлы проекта в указанный каталог. После этого в исходный каталог будет загружена актуальная версия проекта с сервера Version Control Management.

6.3.31. Каталог проекта ПЛК содержит информацию других файлов

При добавлении файлов в каталог проекта возникает ошибка `Каталог содержит информацию других файлов`.

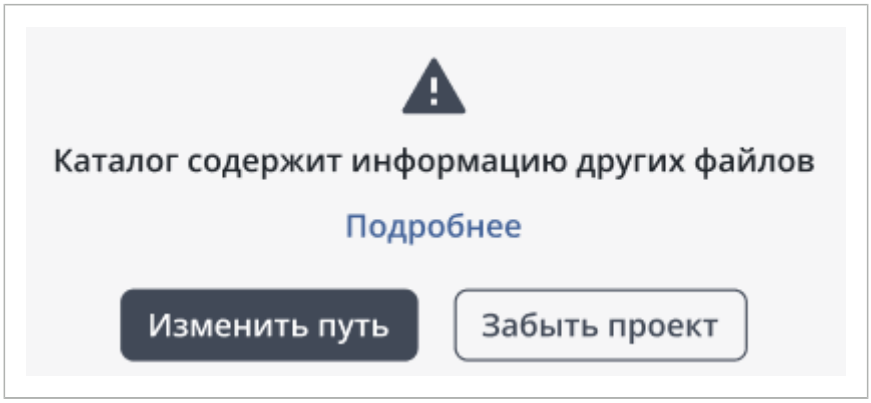


Рис. 103. Сообщение об ошибке

Причина

В каталог проекта были добавлены файлы других Git-платформ или серверов Version Control Management.

Способ устранения

Выберите способ устранения ошибки:

- Изменить каталог проекта с помощью кнопки **Изменить путь**.
- Удалить связь между локальным и серверным репозиторием с помощью кнопки **Забыть проект**.

6.3.32. Путь к файлу превышает допустимую длину

В процессе работы с Version Control Desktop App могут возникнуть следующие ошибки:

Рис. 104. Ошибка создания версии

Рис. 105. Ошибка подключения репозитория

Рис. 106. Ошибка редактирования пути

Рис. 107. Ошибка отмены изменений

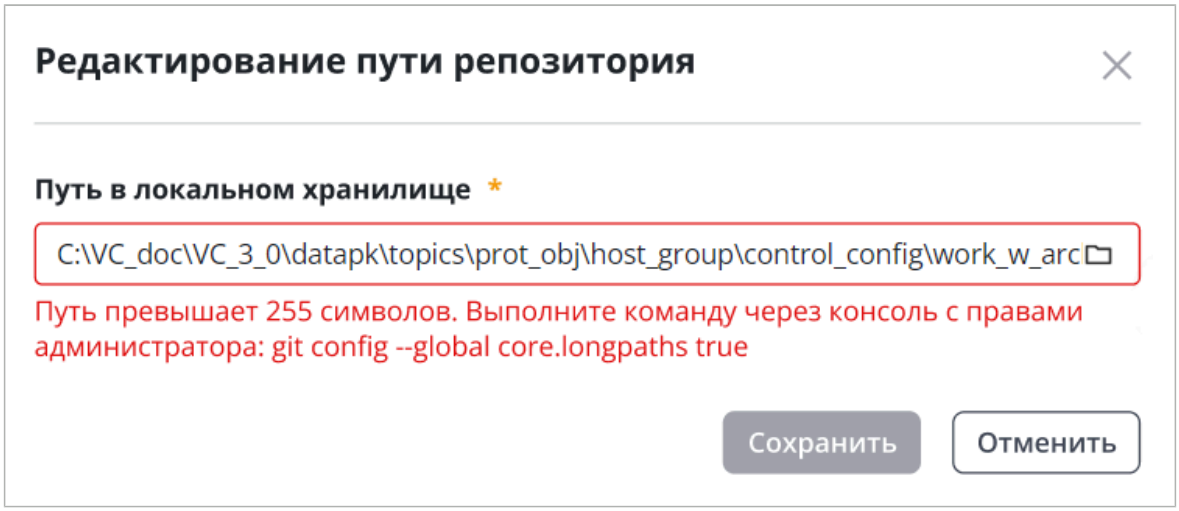


Рис. 108. Ошибка длины пути

Причина

При снятии ограничений на длину пути к файлу может произойти ситуация, когда путь к файлу репозитория превышает допустимые 255 символов.

Способ устранения

1. Откройте консоль с правами администратора.
2. Введите следующую команду:

```
git config --global core.longpaths true
```

6.4. Восстановление данных из резервных копий

Восстановление данных на текущей версии Комплекса уровня Management возможно только из резервной копии, выполненной для той же версии Комплекса уровня Management.

Восстановление данных рекомендуется выполнять в следующем порядке Комплекса уровня Management:

1. Резервное копирование данных.
2. Проверка наличия резервной копии.
3. Восстановление данных из резервной копии.

Комплексы уровня Sensor не хранят данные, поэтому их восстановление из резервной копии заключается в их развертывании с нуля — необходимо только скопировать сохраненные файлы `machine-id`, `sensor.env`, .

> Внимание:
>
> Не рекомендуется использовать резервную копию данных с целью развернуть еще одну копию Комплекса — идентификатор в файле `machine-id` должен быть уникальным на каждом Комплексе, и не допускается наличие двух Комплексов с одинаковыми идентификаторами в одной сети.

6.4.1. Восстановление данных из резервных копий Комплекса уровня Management и Комплекса уровня Management+Sensor

Для восстановления данных из резервных копий Комплекса уровня Management или Комплекса уровня Management+Sensor необходимо выполнить следующие действия:

- Проверка наличия резервной копии Комплекса уровня Management и Комплекса уровня Management +Sensor;
- Восстановление данных из резервной копии Комплекса уровня Management и Комплекса уровня Management+Sensor.

Для подготовки к восстановлению данных Комплекса уровня Management из резервной копии необходимо подготовить следующие файлы, заранее сохраненные на отдельном носителе на этапе создания резервной копии:

- архив `dtpk-backup-v3.0.[минорная_версия].[патч_версия]-{ГГГГММДДччммсс}.tar` с резервной копией;
- архив `nta-backup-[версия_Комплекса]-[дата]` с резервной копией БД `clickhouse`, если на восстанавливаемом Комплексе установлен модуль «Анализ промышленного сетевого трафика» и необходимо восстановить его базу данных;
- конфигурационный файл `manager.env`;
- конфигурационный файл `sensor.env`, если на Комплексе также будет восстанавливаться уровень Sensor (сенсор);
- индексы внешних событий, если на восстанавливаемом Комплексе установлен модуль «Управление внешними событиями».

6.4.1.1. Проверка наличия резервной копии Комплекса уровня Management и Комплекса уровня Management+Sensor

Для проверки наличия резервной копии:

1. Подключитесь к Комплексу уровня Management по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. Убедитесь, что архив резервной копии `dtpk-backup-v3.0.[минорная_версия].[патч_версия]-{ГГГГММДДччммсс}.tar` расположен в директории `/var/backups`
3. Если на восстанавливаемом Комплексе установлен модуль «Анализ промышленного сетевого трафика» и необходимо восстановить его данные, убедитесь, что архив `nta-backup-[версия_Комплекса]-[дата]` резервной копии БД `clickhouse` расположен в директории `/var/backups`
4. Проверьте целостность архива резервной копии. Для этого выполните команду из любой директории:

```
python3 -m backup_manager check
 --file=dtpk-backup-v3.0.[минорная_версия].[патч_версия]-{ГГГГММДДччммсс}.tar
 --password='1234567890'
```

где `--password` — пример пароля, заданного для архива при создании резервной копии.

- **Результат шага:** пример вывода в терминале при успешной проверке целостности архива:

```
INFO:backup_manager.operations.check:Start
 checking /var/backups/dtpk-backup-v3.0.1.0-rc1-20250827104814.tar backup file
INFO:backup_manager.operations.check:Version 3.0.1.0-rc1
INFO:backup_manager.operations.check:data.tar.bz2 Ok
INFO:backup_manager.operations.check:repos_data.tar.bz2 Ok
INFO:backup_manager.operations.check:maria_db_dump.sql Ok
INFO:backup_manager.operations.check:postgres_db_dump.sql Ok
INFO:backup_manager.operations.check:dump.rdb Ok
INFO:backup_manager.main:Backup checked
```

5. Убедитесь в отсутствии ошибок после окончания проверки резервной копии.

6.4.1.2. Восстановление данных из резервной копии Комплекса уровня Management и Комплекса уровня Management+Sensor

ОСТОРОЖНО:

При восстановлении Комплекса уровня Management уникальный идентификатор `/etc/machine-id` и `/var/lib/dbus/machine-id` будет заменен на идентификатор из резервной копии. Во избежание проблем убедитесь в следующем:

- если восстановление Комплекса выполняется на другом устройстве, то на предыдущем устройстве в ОС необходимо изменить `machine-id` во избежание наличия в сети двух устройств с одинаковым `machine-id`;
- на ОС отсутствуют приложения, работа которых может быть нарушена в связи с изменением `machine-id`.

Для восстановления данных из резервной копии:

1. Остановите работу всех сервисов Комплекса, кроме `udv-postgresql.service`. Для этого выполните команду:

```
/usr/bin/stop_services.sh
```

2. Если на восстанавливаемом Комплексе установлен модуль «Анализ промышленного сетевого трафика» и необходимо восстановить его базу данных, запустите СУБД `clickhouse`:

```
systemctl restart udv-clickhouse-service.service
```

3. После остановки работы сервисов выполните из любой директории команду для восстановления Комплекса из резервной копии:

```
python3 -m backup_manager restore --include-nta [путь_к_резервной_копии_NTA]
 --file=dtpk-backup-v3.0.[минорная_версия].[патч_версия]-{ГГГГММДДччммсс}.tar
 --password='1234567890' --db-username DB_USER --db-password DB_PASS
```

где:

- `--include-nta` — путь к файлу `nta-backup-[версия_Комплекса]-[дата]` резервной копии базы данных `clickhouse`, если на восстанавливаемом Комплексе установлен модуль «Анализ промышленного сетевого трафика». Если модуль не установлен, удалите параметр и его значение из команды.
- `--password` — пример пароля от архива резервной копии, который был задан при создании резервной копии;
- `--db-username` — логин пользователя базы данных, значение которого необходимо было скопировать из переменной `DB_USER` конфигурационного файла `/usr/share/udv/datapk/manager.env` при создании архива резервной копии (либо можно скопировать из файла `manager.env` в архиве резервной копии);
- `--db-password` — пароль доступа к базе данных, значение которого необходимо было скопировать из переменной `DB_PASS` конфигурационного файла `/usr/share/udv/datapk/manager.env` при создании архива резервной копии (либо можно скопировать из файла `manager.env` в архиве резервной копии).

4. Выполните восстановление внешних событий. Для этого поместите сохраненные ранее индексы событий в директорию `/var/backups/elasticsearch/uploads`.

   а. Поместите с заменой файлы `manager.env` и `sensor.env` (если на восстанавливаемом Комплексе будет развернут сенсор), сохраненные ранее отдельно, в директорию `/usr/share/udv/datapk`.

   б. После успешного восстановления перезагрузите Комплекс, выполнив команду:

   ```
   shutdown -r now
   ```

   Результат шага: перезагрузка Комплекс успешно выполнена.

   в. Войдите в веб-интерфейс Комплекса под учетной записью администратора.

   г. Перейдите в раздел **События → Экспертный режим**.

   д. Нажмите **Create index pattern**.

   е. В поле **Index pattern name** введите `datapk-events-*` и нажмите **Next step**.

   ж. В поле **Time field** выберите **create_time** и нажмите **Create index pattern**.

   з. Перейдите в раздел **Администрирование → События и инциденты → Индексы**.

   и. Нажмите **Восстановить индексы**.

6.4.2. Восстановление данных из резервных копий Комплекса уровня Sensor

Для восстановления данных из резервных копий Комплекса уровня Sensor необходимо выполнить следующие действия:

- Резервное копирование данных Комплекса уровня Sensor;
- Восстановление данных из резервной копии Комплекса уровня Sensor.

6.4.2.1. Резервное копирование данных Комплекса уровня Sensor

Для выполнения резервного копирования данных:

1. Войдите в терминал Комплекса под учетной записью `root`.
2. Сохраните файл `machine-id` из директории `/etc`.
3. Сохраните файл `machine-id` из директории `/var/lib/dbus`.
4. Сохраните файл `sensor.env` из директории `/usr/share/udv/datapk`.
5. Если на сенсоре был установлен модуль «Анализ промышленного сетевого трафика», сохраните конфигурационные файлы `/usr/share/udv/zeek-wrapper/configs/general.dat` и `/usr/share/udv/zeek-wrapper/configs/ics-function.dat`.

6.4.2.2. Восстановление данных из резервной копии Комплекса уровня Sensor

Для восстановления данных из резервной копии:

1. Выполните развертывание Комплекса уровня Sensor в соответствии с разделом «Установка Комплекса уровня Sensor».
2. Замените файл `/etc/machine-id` на файл, сохраненный при резервном копировании.
3. Сохраните файл `machine-id` в директории `/var/lib/dbus`.
4. Замените файл `/usr/share/udv/datapk/sensor.env` на файл, сохраненный при резервном копировании.
5. Если на сенсоре был установлен модуль «Анализ промышленного сетевого трафика», замените конфигурационные файлы `/usr/share/udv/zeek-wrapper/configs/general.dat` и `/usr/share/udv/zeek-wrapper/configs/ics-function.dat` на файлы, сохраненные при резервном копировании.
6. Перезагрузите Комплекс, выполнив команду:

   ```
   shutdown -r now
   ```

7. Войдите в веб-интерфейс Комплекса уровня Management, к которому подключен данный Комплекс уровня Sensor.
8. Перейдите в раздел **Сенсоры** и убедитесь, что Комплекс уровня Sensor успешно подключился к Комплексу уровня Management.

6.5. Действия в случаях несанкционированного доступа к данным

После обнаружения нелегитимных действий со стороны пользователя администратор может воспользоваться следующими возможностями по блокировке пользователей:

- Просмотр журнала действий пользователей Комплекса
- Изменение статуса активности учетной записи пользователя Комплекса

6.5.1. Просмотр журнала действий пользователей Комплекса

Все действия пользователей Комплекса журналируются. При установлении фактов попыток несанкционированных действий пользователей их работа в веб-интерфейсе Комплекса блокируется. Дальнейшая работа пользователя с Комплексом возможна только после расследования администратора комплекса по выявлению причин возникновения аварийной ситуации.

Для самостоятельного установления или подтверждения фактов несанкционированного доступа администратор может обратиться к журналу действий пользователей. Для просмотра журнала действий пользователей Комплекса:

1. Перейдите на страницу **События**.
2. Настройте фильтрацию событий по значениям `user_action_control` или `appliance_authentication` поля **Тип**.
3. Нажмите кнопку **Сохранить** для применения фильтра.
4. В «быстром» фильтре **Дата создания** выберите временной интервал, за который необходимо получить события действий пользователей.
5. Проанализируйте полученные события на предмет несанкционированного доступа.

6.5.2. Изменение статуса активности учетной записи пользователя Комплекса

Чтобы изменить статус активности учетной записи пользователя Комплекса:

1. Перейдите на страницу **Администрирование → Пользователи**.
2. Выберите учетную запись в списке и нажмите (**Редактировать учетную запись**).
3. В зависимости от желаемого действия:
   - установите чекбокс Учетная запись **пользователя активна**, чтобы активировать (разблокировать) доступ пользователя к веб-интерфейсу Комплекса;
   - отмените установку чекбокса Учетная запись **пользователя активна** для учетной записи, чтобы заблокировать пользователю доступ к веб-интерфейсу Комплекса.
4. Сохраните изменения.
   - **Результат шага:** после подтверждения активность учетной записи пользователя будет изменена.

6.6. Действия в других аварийных ситуациях

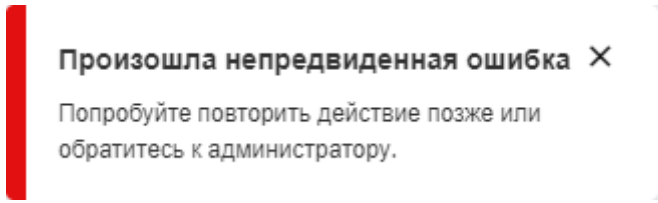
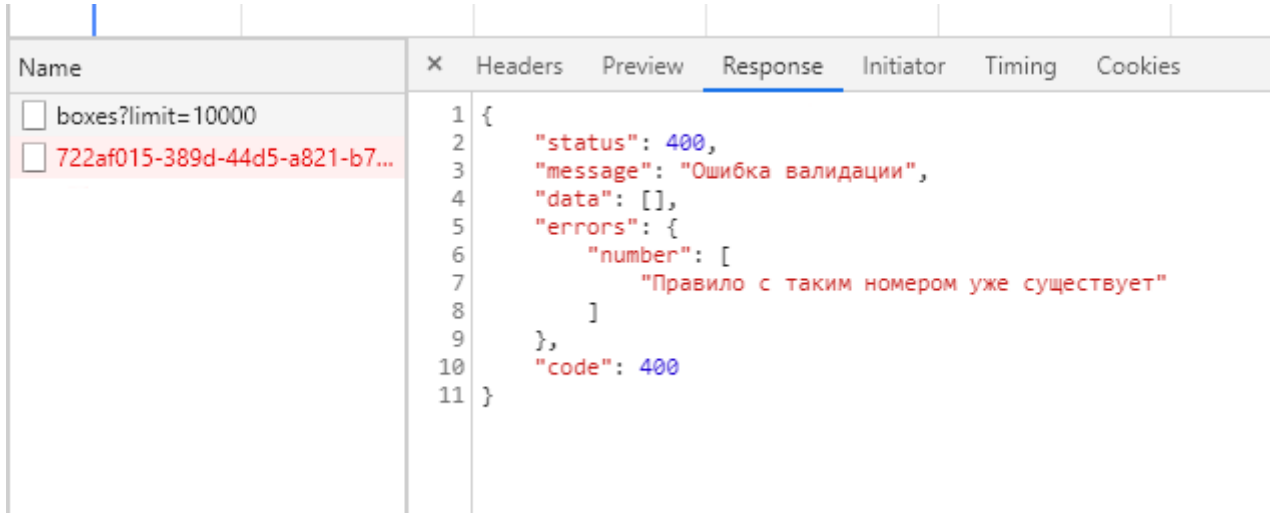
Действия в экстремальных условиях осуществляются по правилам, принятым в эксплуатирующей организации.

Аварийные ситуации, связанные с некорректным функционированием Комплекса в сетевой инфраструктуре АСУ ТП, устраняются путем проверки и исправлений настроек сети управляющего контура комплекса и локальных настроек Комплекса.

6.7. Анкета при обращении в сервисный центр

> Внимание:
>
> Поля, отмеченные знаком «*», обязательны для заполнения

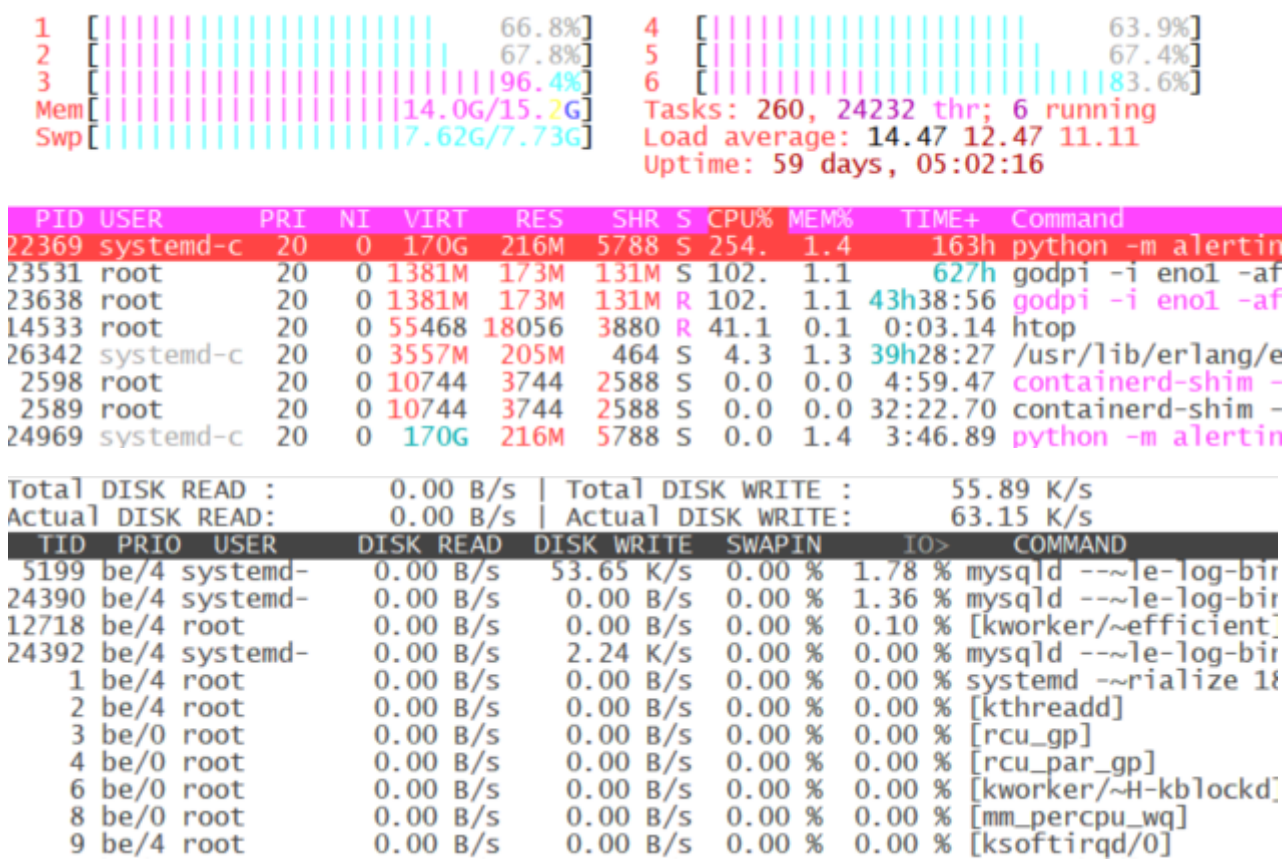
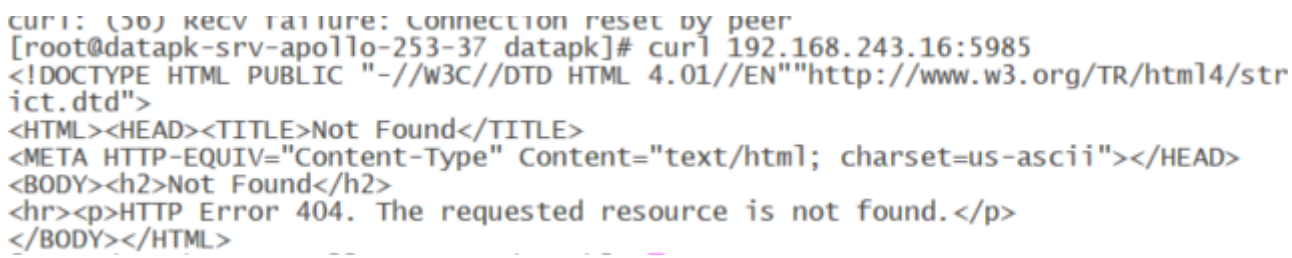
ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ
ФИО, должность обратившегося, контактные данные *		Иванов Иван Иванович, системный инженер, ООО «Партнер», partner@partner.ru, +7(900)-012-34-56
Проект/место установки, уровень в иерархии *		ООО «Заказчик», КС-1, уровень Management
Сертификат технической поддержки *		CI-12345678
Версия Комплекса *		3.0.0.0
Общее количество активов, сетевых сессий, событий в сутки на проблемном (включая полученные снизу)		150 активов, 300 тыс. сессий, 250 тыс. событий в сутки
Количество подчиненных		2 уровня Sensor
Краткое описание ошибки (словесное) *		Не создается правило сессий
Действия, которые привели к ошибке (подробное описание шагов, приведших к ошибке) *		Перешел на страницу правил сессий, создал новое правило, задал диапазон IP-адресов и последний распознанный протокол, при сохранении ошибка валидации.

ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ
Скриншот ошибки в веб-интерфейсе		
Результаты ошибочных запросов (панель разработчика в браузере, вкладка response у проблемного запроса)		
Логи сопутствующих сервисов *		Во вложении логи udv-zeek-backend, udv-rules-backend
Архив всех логов сервисов (скрипт `get_logs.bash` на файловом сервере)		Архив во вложении
Данные по аппаратной платформе (сервер, процессор, объем оперативной памяти, объем дискового пространства, тип дисков)*		Сервер Huawei X6000, Xeon Bronze 3104, 1.7 GHz. 16 ГБ RAM, 4 ТБ HDD (SATA 7200 rpm)

ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ
Версия ОС *		ОС Альт Сервер 10.2 SP

Вывод таблицы маршрутизации (`route -n` или `ip route show`)		`[root@datapk-srv-apollo-253-37 datapk]# ip route show`
		`default via 192.168.253.1 dev eno1 proto static metric 100`
		`172.8.0.0/24 dev br-48bed0f17439 proto kernel scope link src 172.8.0.1`
		`172.8.0.0/24 dev br-48bed0f17439 proto kernel scope link src 172.8.0.1 metric 42 8`
		`172.10.0.0/16 dev br-842698bddad2 proto kernel scope link src 172.10.0.1`
		`172.11.0.0/16 dev br-3221910b41eb proto kernel scope link src 172.11.0.1`
		`172.17.2.0/24 via 172.17.100.1 dev eno1 proto static metric 100`
		`172.17.100.1 dev eno1 proto static scope link metric 100`
		`172.18.0.0/16 dev docker0 proto kernel scope link src 172.18.0.1 linkdown`
		`172.18.0.0/16 dev docker0 proto kernel scope link src 172.18.0.1 metric 430 link down`
		`172.19.0.0/16 dev br-40ac11103665 proto kernel scope link src 172.19.0.1`
		`172.19.0.0/16 dev br-40ac11103665 proto kernel scope link src 172.19.0.1 metric 427`
		`172.20.0.0/16 dev br-3ed25b69f5c4 proto kernel scope link src 172.20.0.1`
		`172.20.0.0/16 dev br-3ed25b69f5c4 proto kernel scope link src 172.20.0.1 metric 426`
		`192.168.253.0/24 dev eno1 proto kernel scope link src 192.168.253.37 metric 100`

Свободное место на корневом разделе диска (`df -h /`) Свободная оперативная память, текущий список процессов (`htop`) Значение Load Average Загрузка диска (`iotop`)		Свободное место на корневом разделе: 2.5 ТБ Свободная оперативная память: 1 МБ Load Average: 14

ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ
		
Наличие сетевых доступов до проблемного актива/ (`curl [ip_addr]:[port_number]`)		


```
curl: (56) Recv failure: Connection reset by peer
[root@datapk-srv-apollo-253-37 datapk]# curl 192.168.243.16:5985
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/str
ict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr><p>HTTP Error 404. The requested resource is not found.</p>
</BODY></HTML>
```

ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ
Запись трафика (PCAP-файл) с прослушивающего интерфейса сенсора для заявок с проблемами, связанными с обнаружением сессий или вторжений		Во вложении
Сведения о проблемном активе (тип, версия ОС, настроенные протоколы сбора данных) для заявок с проблемами в запуске сканеров сбора данных		АРМ оператора, Windows 7, сбор данных по WinRM HTTPS
Проблемные сканеры сбора данных для заявок с проблемами в запуске сканеров		Во вложении

6.8. Диагностика сервиса сбора данных по протоколам SSH, Telnet, WinRM, winexe

Перед выполнением:

Внимание:

Данная инструкция актуальна для следующих сервисов и портов:

- `udv-msrpc`, порт `10008`;
- `udv-plc-connector`, порт `10206`;
- `udv-opc-connector`, порт `10205`;
- `udv-terminal-connector`, порт `10208`;
- `udv-modbus-connector`, порт `10203`;
- `udv-sql-connector`, порт `10202`;
- `udv-snmp-connector`, порт `10204`;

Для расследования причин появления ошибок сбора данных по протоколам SSH, Telnet, WinRM, winexe:

1. Подключитесь к операционной системе Комплекса.
2. Просмотрите текущее состояние журналирования сервиса, выполнив команду:

   ```
   curl https://[IP_адрес_сервиса]:[порт_сервиса]/log/level
   ```

   Пример

   Сервис имеет состояние `NOTSET`. Это значит, что уровень журналирования для этого сервиса не задан.


   ```
   "msrpc.cancellable_pool":"NOTSET","msrpc":"NOTSET","im_lib":"NOTSET",
   ```


   Рис. 109. Состояние «NOTSET» журналирования сервиса «msrpc»

3. Измените уровень журналирования сервиса, выполнив команду:

   ```
   curl -X POST
    "https://[IP_адрес_сервиса]:[порт_сервиса]/log/level?logger_name=[название_сервиса/назва
   ние_пакета_в_сервисе]&log_level=[уровень_журналирования]"
   ```

   где:

   - `[IP_адрес_сервиса]` — IP-адрес необходимого сервиса;
   - `[порт_сервиса]` — порт необходимого сервиса;
   - `[название_сервиса/название_пакета_в_сервисе]` — имя необходимого сервиса или пакета в сервисе;
   - `[уровень_журналирования]` — требуемый уровень журналирования сервиса (`INFO` или `DEBUG`).

   Внимание:

   На данном шаге название сервиса вводится через нижнее подчеркивание, без добавления приставки `udv-` (например, `udv-terminal-connector.service` → `terminal_connector`)

4. В веб-интерфейсе Комплекса однократно повторите сбор данных с активов, на которых ранее были ошибки сбора.
5. Проверьте установленный уровень журналирования сервиса, выполнив команду:

```
curl https://[IP_адрес_сервиса]:[порт_сервиса]/log/level
```

Пример

Сервис имеет состояние `DEBUG`

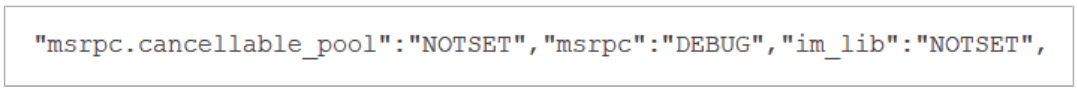


Рис. 110. Состояние «DEBUG» журналирования сервиса «msrpc»

6. Посмотрите журнал сервиса при помощи команды:

```
journalctl -fu [полное_название_сервиса].service -n [количество последних строк журнала,
 которое нужно показать]
```

- **Результат шага:** Отображается указанное количество последних строк журнала сервиса.

Рис. 111. Отображение последних пять строк журнала сервиса «udv-msrpc»

7. Справочная информация

В этом разделе:

7.1. Глоссарий

7.1.1. Автоматизированная система

Автоматизированная система (АС) — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аббревиатура: АС

7.1.2. Актив

Актив — сетевой узел, подлежащий защите от потенциальных угроз и неправомерных действий, например несанкционированного доступа и изменения данных третьими лицами.

Аббревиатура: Актив

7.1.3. Активная и неактивная модель

Активная модель — модель в рамках модуля UDV DATAPK EDR for PLC, которая находится на любом этапе, кроме паузы.

Неактивная модель — модель в рамках модуля UDV DATAPK EDR for PLC, которая находится на паузе.

7.1.4. Автоматизированная система управления производственными и технологическими процессами

Автоматизированная система управления производственными и технологическими процессами — группа решений технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.

Аббревиатура: АСУ ТП

Автоматизированная система управления производственно-технологическим комплексом

Аббревиатура: АСУ ПТК

7.1.5. Банк данных угроз безопасности информации ФСТЭК России

Банк данных угроз безопасности информации ФСТЭК России (БДУ ФСТЭК России) — база данных уязвимостей, созданная ФСТЭК России. Содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов.

Аббревиатура: БДУ ФСТЭК России

7.1.6. Бесклассовая адресация

Бесклассовая адресация (англ. Classless Inter-Domain Routing) — метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации.

Аббревиатура: CIDR

7.1.7. Виджет

Виджет (визуализация) — представление информации о событиях в виде, удобном для зрительного наблюдения и анализа.

7.1.8. Глобальная сеть

Глобальная сеть — совокупность сетевых узлов за пределами локальной и контролируемой сетей.

См. также

Просмотр карты сети

7.1.9. Группа объектов

Группа объектов — группа репозиториев, объединенная по каким-либо признакам.

7.1.10. Дообучение модели

Дообучение модели — процесс передачи в модель набора данных в специальном формате с использованием интерфейса API с целью расширения представления модели о допустимом сетевом взаимодействии.

7.1.11. Задача сбора данных

Сущность, позволяющая при помощи групп сканеров собирать конфигурации и события с активов и их групп, в том числе с использованием расписания cron.

7.1.12. Индекс событий

Индекс событий — совокупность событий за сутки.

7.1.13. Информационная безопасность

Информационная безопасность — состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц. Безопасность данных также подразумевает управление рисками, которые связаны с разглашением информации или влиянием на аппаратные и программные модули защиты.

Аббревиатура: ИБ

7.1.14. Источник событий

Источник событий — объект или сервис от которого поступают события.

7.1.15. Карта сети

Карта сети — модель, описывающая состав вычислительной сети предприятия: узлы и сессии между узлами на сетевом и канальном уровнях.

7.1.16. Классификатор

Классификатор — сгруппированный по различным признакам перечень наименованных объектов, где каждому из них присвоен уникальный код в соответствии с их общими признаками или различиями.

7.1.17. Компонент

Автономная часть в составе всего решения , устанавливаемая на определенном физическом или сетевом уровне инфраструктуры предприятия с АСУ ТП (технологическом комплексе, филиале или верхнем уровне всего предприятия) для выполнения отдельного набора функций на этом уровне (сбора, анализа и визуализации данных). Для обеспечения максимальной заявленной киберзащиты АСУ ТП средствами компоненты на одном предприятии необходимо настроить для взаимодействия друг с другом по сети. содержит три компонента:

- Management;
- Sensor;
- Supervision.

См. также

Модуль

Сервис

7.1.18. Конечная точка

Конечная точка — это конкретный URL-адрес или путь, по которому клиентское приложение может отправлять запросы к API для взаимодействия с сервером и получения данных или выполнения определенных действий.

7.1.19. Контролируемая сеть

Контролируемая сеть — список подсетей, настраиваемый вручную на странице **Сенсоры**. Узлы этих подсетей автоматически обнаруживаются ом как контролируемые активы. Взаимодействие контролируемой сети с локальной сетью регистрируется как событие, с глобальной сетью — как инцидент.

См. также

Просмотр карты сети

Настройка контролируемой сети

7.1.20. Конфигурация актива

Конфигурация актива — набор параметров актива, связанных с состоянием информационной безопасности. Как правило, каждому набору параметров соответствует своя конфигурация. Например, для ПЛК Siemens могут проверяться конфигурации по протоколу snap 7 на соответствие эталонным настройкам системы, ее версии и контрольным суммам блоков.

7.1.21. Корреляция

Корреляция — способность системы выявлять неочевидные закономерности в событиях и формировать инциденты на их основе.

7.1.22. Локальная сеть

Локальная сеть — список подсетей, зарезервированных для локального использования.

7.1.23. Локальная учетная запись

Учетная запись пользователя на компьютере, которая хранится только на одном конкретном устройстве и не синхронизируется с другими устройствами или серверами. Она используется для входа в систему и управления правами доступа локально.

7.1.24. Маска данных модели

Маска данных модели — механизм дополнительной фильтрации данных, поступающих в модели на основе временного автомата и иерархического словаря для протокола CIP. Основным предназначением маски является фильтрация данных с высокой энтропией (как правило это могут быть случайные данные или шум). Для каждой модели конфигурация маски и ее расчет выполняются индивидуально.

7.1.25. Модель

Модель — объект, формируемый в рамках модуля UDV DATAPK EDR for PLC различными методами машинного обучения. Модель формируется с целью выявления каких-либо закономерностей и позволяющий генерировать прогноз поведения сетевого взаимодействия двух конечных точек.

7.1.26. Модуль

Отдельный набор функциональностей Комплекса, объединенных по принципу решения одной группы задач (например, контроль версий ПЛК или анализ сетевого трафика) или удовлетворения одной группе функций безопасности. Отсутствие модуля в комплекте поставки Комплекса не влияет на работоспособность других поставляемых модулей (за исключением некоторых модулей — подробнее см. раздел «Список модулей UDV DATAPK Industrial Kit»). Каждый модуль приобретается отдельно.

7.1.27. Немодельные аномалии

Немодельные аномалии — аномалии, которые формируются без участия набора моделей, анализирующих сетевое взаимодействие контроллера с другими устройствами, на этапе разбора трафика, формирования адресной иерархии или словаря сигналов.

7.1.28. Неразрешенная сессия

Неразрешенная сессия — входящее соединение, зарегистрированное Комплексом в контролируемой сети, и признанное нелегитимным согласно правилам сессий.

7.1.29. Несанкционированный доступ

Несанкционированный доступ (НСД) — доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

> Внимание:
>
> Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

Аббревиатура: НСД

7.1.30. Нормализация событий

Нормализация событий — приведение событий из разных источников к единому формату, принятому в Комплексе.

7.1.31. Операционная система

Операционная система (ОС) — комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.

Аббревиатура: ОС

7.1.32. Панель мониторинга

Панель мониторинга — тип графического интерфейса, использующий интерактивные визуализации для обзора ключевых показателей.

Dashboard

7.1.33. Программируемый логический контроллер

Программируемый логический контроллер (ПЛК) — унифицированная цифровая управляющая электронная система, специально разработанная для использования в производственных условиях.

Аббревиатура: ПЛК

7.1.34. Политика корреляции событий

Политика корреляции событий — справочник, который содержит схему и правила корреляции.

7.1.35. Правила корреляции событий

Правила корреляции событий — набор команд, которые оперируют событиями из разных источников и выдают на основе их анализа инциденты. На основе инцидентов могут быть сформированы уведомления, которые отправляются инженеру информационной безопасности или другим сотрудникам.

7.1.36. Программно-техническое средство

Программно-техническое средство (ПТС) — комплексное решение, состоящее из программных и аппаратных компонентов.

Аббревиатура: ПТС

7.1.37. Программное обеспечение

Программное обеспечение (ПО) — программа или множество программ, используемых для управления компьютером.

Аббревиатура: ПО

7.1.38. Программный комплекс

Программный комплекс (ПК) — набор программных средств, работающих совместно для выполнения одной или нескольких сходных задач.

Аббревиатура: ПК

7.1.39. Проект

Проект — каталог с набором файлов и подкаталогов, с которым работает пользователь.

7.1.40. Разрешенная сессия

Разрешенная сессия — входящее соединение, зарегистрированное Комплексом в контролируемой сети, и признанное легитимным согласно правилам сессий.

7.1.41. Регламентные работы

Регламентные работы — комплекс профилактических работ и проверок, выполняемых на объектах систем автоматики в определенные (регламентированные) моменты времени периода эксплуатации и направленных на поддержание их надежности в течение межрегламентного срока.

7.1.42. Репозиторий

Репозиторий — серверное хранилище данных, состоящее из проекта и истории его изменений.

7.1.43. Роль пользователя

Роль пользователя — совокупность возможностей, которые получает пользователь Комплекса, входящий в определенное множество встроенных групп доступа, и оперирующий с заданными наборами возможностей.

7.1.44. Сервис

Программная единица компонента Комплекса или модуля компонента Комплекса, реализующая определенные технические функции и взаимодействующая с другими сервисами, модулями и компонентами.

См. также

Компонент

Модуль

7.1.45. Сервис глубокой инспекции пакетов

Сервис глубокой инспекции пакетов — технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому. В отличие от брандмауэра, производится анализ полного содержимого трафика на уровнях модели OSI со второго и выше.

Аббревиатура: DPI

Deep packet inspection

См. также

UDV Network Traffic Analyzer

7.1.46. Сессия

Установленное сетевое соединение между клиентом и сервером для возможности обмена данными в ограниченный промежуток времени. Сессия имеет признак начала и конца. Начало определяется по соответствующим пакетам протоколов транспортного уровня; завершение также определяется по пакетам, либо по таймауту, установленному в модуле «Анализ промышленного сетевого трафика» для каждого протокола транспортного уровня.

См. также

Просмотр сессий и пакетов

7.1.47. Система обнаружения вторжений

Система обнаружения вторжений (СОВ) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими через Интернет.

Аббревиатура: СОВ

7.1.48. Сканер

Сканер — исполняемый скрипт сбора данных.

7.1.49. Скрипт

Скрипт — исполняемый файл, содержащий последовательность действий на скриптовом языке программирования Python. Предназначен для сбора данных с активов с помощью сканеров.

7.1.50. Справочник

Справочник — систематизированный список данных об одном или нескольких компонентах конкретного Комплекса.

7.1.51. Служба обнаружения вторжений

Служба обнаружения вторжений — служба Комплекса, которая позволяет обнаруживать подозрительную сетевую активность, сравнивая встроенные правила обнаружения вредоносного трафика с данными, проходящими по локальной сети.

7.1.52. Средство защиты информации

Средство защиты информации (СрЗИ) — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Аббревиатура: СрЗИ

7.1.53. Статус модели

Статус модели — отображение текущего этапа жизненного цикла модели в рамках модуля UDV DATAPK EDR for PLC.

7.1.54. Схема корреляции событий

Схема корреляции событий — набор сущностей, используемый для представления и обработки событий, включает в себя представления различных типов событий, таких как: окна данных, таблицы, контексты, переменные.

7.1.55. Тег

Тег — параметр технологического процесса или оборудования, передаваемый в промышленной сети по определенным протоколам. Теги используются для мониторинга и управления оборудованием через системы автоматизации (например, ПЛК).

См. также

Правила контроля тегов

7.1.56. Технические условия

Технические условия (ТУ) — документ, устанавливающий технические требования, которым должны соответствовать конкретное изделие, материал, вещество и пр. или их группа.

Аббревиатура: ТУ

7.1.57. Техническое обслуживание

Техническое обслуживание — комплекс организационно-технических мероприятий и работ, производимых на объекте и направленных на поддержание в рабочем или исправном состоянии оборудования (программного обеспечения) технических систем в процессе их использования по назначению с целью повышения надежности и эффективности их работы.

Аббревиатура: ТО

7.1.58. Туннелирование DNS

Туннелирование DNS — сетевая атака, которая направляет DNS-запросы на сервер злоумышленника для предоставления ему скрытого канала управления и контроля, а также для кражи данных. DNS-туннелирование выполняется через межсетевые экраны путем кодирования сообщений управления и контроля (C&C) или небольших объемов данных в незаметные ответы и запросы DNS. Для выявления DNS-туннелирования среди обычного DNS-трафика, как правило, применяются технологии машинного обучения.

Аббревиатура: Туннелирование DNS

7.1.59. Узел

Узел — элемент сети предприятия, взаимодействующий с другими элементами сети.

7.1.60. Уровень индикации

Уровень индикации — уровень, определяющий уровень детализации (глубину) разбора передаваемых данных. Он указывает, какая часть информации отображается или обрабатывается при мониторинге или дешифровке трафика. В зависимости от настроек уровень индикации может показывать:

- только высокоуровневую информацию (например, тип пакета);
- часть информации (отдельные поля протокола);
- полную информацию (все уровни вложенности).

7.1.61. Условие сходимости модели

Условие сходимости модели — набор условий, при достижении которых возможно досрочное завершение этапа обучения с последующим переходом на следующий этап жизненного цикла модели.

7.1.62. Учетная запись

Учетная запись — хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

7.1.63. Федеральная служба по техническому и экспортному контролю

Федеральная служба по техническому и экспортному контролю — орган исполнительной власти, осуществляющий контроль за сертификацией и аттестацией автоматизированных систем с учетом требований информационной безопасности.

Аббревиатура: ФСТЭК России

7.1.64. Фильтрация

Фильтрация — способ вывода нужных пользователю данных при помощи встроенных фильтров.

7.1.65. Этап жизненного цикла модели

Этап жизненного цикла модели — элемент структуры, описывающей процесс существования модели.

7.1.66. Common Platform Enumeration

Common Platform Enumeration (CPE) — структурированная схема именования систем информационных технологий, программного обеспечения и пакетов.

Аббревиатура: CPE

7.1.67. Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) — база данных общеизвестных уязвимостей информационной безопасности.

Аббревиатура: CVE

7.1.68. Open Vulnerability and Assessment Language

OVAL — основанный на xml формат, предназначенный для автоматизированной оценки безопасности систем и предоставляющий средства для описания исследуемой системы, анализа ее состояния и формирования отчетов о результатах проверки.

Аббревиатура: OVAL

7.1.69. Syslog

Syslog — стандарт отправки и регистрации сообщений о происходящих в системе событиях. Используется в компьютерных сетях, работающих по протоколу IP. Термином Syslog называют как ныне стандартизированный сетевой протокол Syslog, так и программное обеспечение (приложение, библиотеку), которое занимается отправкой и получением системных сообщений.

system log

7.1.70. Version Control

Version Control — система, состоящая из серверной части Version Control Management и клиентской части Version Control Desktop App.

7.1.71. Version Control Desktop App

Version Control Desktop App — клиентское ПО, предназначенное для работы с репозиториями Version Control Management.

7.1.72. Version Control Management

Version Control Management — серверное ПО, предназначенное для централизованного управления репозиториями проектов ПЛК, резервного копирования и восстановления проектов ПЛК, отслеживания и контроля изменений в исходном коде проектов ПЛК.

7.1.73. UDV DATAPK уровня Management

UDV DATAPK уровня Management с функциями управления сенсорами и анализа полученных с них данных.

Аббревиатура: Management

См. также

Комплекс

7.1.74. UDV DATAPK уровня Sensor

UDV DATAPK уровня Sensor — UDV DATAPK с базовым набором функций по получению информации с активов технологического комплекса.

Аббревиатура: Sensor

7.1.75. UDV DATAPK уровня Supervision

UDV DATAPK с функциями управления UDV DATAPK уровня Management.

Аббревиатура: Supervision

7.1.76. UDV DATAPK EDR for PLC

Маркетинговое наименование модуля UDV DATAPK Industrial Kit «Обнаружение и реагирование для ПЛК».

Аббревиатура: UDV DATAPK EDR for PLC

7.1.77. UDV DATAPK Version Control

Маркетинговое наименование модуля UDV DATAPK Industrial Kit «Управление проектами ПЛК» и отдельного программного комплекса «UDV DATAPK Version Control».

Аббревиатура: UDV DATAPK Version Control

7.1.78. UDV Network Traffic Analyzer

Маркетинговое наименование модуля UDV DATAPK Industrial Kit «Анализ промышленного сетевого трафика» и отдельного программного комплекса «Система контроля и анализа сетевого трафика UDV NTA».

7.1.79. Модуль «Анализ промышленного сетевого трафика»

Программный комплекс для защиты сетевой инфраструктуры от кибератак, основанный на глубоком анализе трафика. Основной целью функционирования модуля является выявление и инвентаризация устройств, обнаружение вторжений, построение карты сети.

Аббревиатура: Модуль «Анализ промышленного сетевого трафика»

7.1.80. Модуль «Обнаружение и реагирование для ПЛК»

Программный комплекс для обнаружения инцидентов ИБ в автоматизированных системах, основанный на интеллектуальных алгоритмах. Основной целью функционирования модуля является детектирование отклонений в работе контроллеров автоматизированных систем.

Аббревиатура: Модуль «Обнаружение и реагирование для ПЛК»

7.1.81. Модуль «Управление внешними событиями»

Программный модуль для получения и обработки событий информационной безопасности из сторонних источников и других модулей, нормализации и корреляции событий, формирования инцидентов ИБ и отправки событий/инцидентов в сторонние системы по протоколу Syslog.

Аббревиатура: Модуль «Управление внешними событиями»

7.1.82. Модуль «Управление конфигурациями»

Программный модуль для контроля конфигурационных параметров, влияющих на защищенность, и выявления отклонений параметров от эталонных значений.

Аббревиатура: Модуль «Управление конфигурациями»

7.1.83. Модуль «Контроль версий»

Программное обеспечение, предназначенное для централизованного управления репозиториями проектов ПЛК, резервного копирования и восстановления проектов ПЛК, отслеживания и контроля изменений в исходном коде проектов ПЛК

Аббревиатура: Модуль «Контроль версий»

7.1.84. Модуль «Управление уязвимостями»

Программный модуль для выявления угроз информационной безопасности и проверки соответствия требованиям ИБ с помощью технологий OVAL и CPE to CVE, а также обнаружения уязвимостей из БДУ ФСТЭК России.

Аббревиатура: Модуль «Управление уязвимостями»

7.2. Логическая структура комплекса и режимы функционирования

Комплекс предназначен для оперативного мониторинга состояния информационной безопасности и контроля состояния защищенности АСУ ТП на всех уровнях иерархии АСУ ТП.

Подсистема идентификации и аутентификации субъектов доступа и объектов доступа в рамках ведения каталога активов создает, присваивает, изменяет, уничтожает идентификаторы, позволяет вести каталог активов АСУ ТП и выявлять изменения в их составе.

Подсистема регистрации событий безопасности компонентов АСУ ТП собирает, записывает и хранит информацию о событиях безопасности, позволяет просматривать результаты регистрации событий безопасности с генерированием временных меток и защищает информацию о таких событиях.

Подсистема контроля (анализа) защищенности информации выявляет и анализирует уязвимости, контролирует установку обновлений программного обеспечения и контролирует состав технических средств, программного обеспечения и средств защиты информации в АСУ ТП.

Подсистема защиты автоматизированной системы и ее компонентов защищает настройки средств защиты информации, программного обеспечения и иные данные, которые не должны меняться при обработке информации в АСУ ТП.

Подсистема выявления инцидентов и реагирования на них обнаруживает и регистрирует инциденты ИБ на активах.

Подсистема управления конфигурацией АСУ ТП и ее механизмов защиты управляет изменениями конфигурации активов АСУ ТП и документирует такие изменения.

Подсистема управления доступом Комплекса выполняет идентификацию, проверку подлинности и контроль доступа пользователей в Комплекс и к его отдельным функциям.

В Комплексе предусмотрено два режима функционирования:

1. Режим наблюдения (пассивный мониторинг), который подразумевает:
    - однонаправленное получение данных;
    - прослушивание сетевого трафика и прием событий.
2. Режим «запрос-ответ» (активный мониторинг), который подразумевает:
    - получение конфигурации и событий;
    - взаимодействие с активами в режиме «запрос-ответ» с использованием штатных механизмов и протоколов;
    - выявление уязвимостей и проверки на соответствие требованиям ИБ.

Табл. 6. Режимы функционирования Комплекса

ФУНКЦИИ	РЕЖИМ НАБЛЮДЕНИЯ	РЕЖИМ ОПРОСА
Сбор событий ИБ	× ✓	✓
Обнаружение атак	✓	✓
Выявление сетевых аномалий	✓	✓
Сбор конфигураций	×	✓
Определение текущего состава активов	✓	✓
Выявление изменений в составе активов	✓	✓
Проверка активов на уязвимости	× ✓	✓

7.3. Сведения о сертификатах

Сертификат соответствия ФСТЭК России № 4719 от 28 сентября 2023 г. (действительный до 28 сентября 2028 г.) удостоверяет, что , разработанный и производимый , является системой обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по

безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) — по 6 уровню доверия, «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети шестого класса защиты. ИТ.СОВ.С6.ПЗ» (ФСТЭК России, 2012) и задании по безопасности 05028144.620129.118-ЗБ при выполнении указаний по эксплуатации, приведенных в формуляре 05028144.620129.118-ФО.

Сертификат выдан на основании технического заключения от 25.08.2023, оформленного по результатам сертификационных испытаний, проведенных испытательной лабораторией ООО «КБ-Лаб» (аттестат аккредитации от 29.12.2020 г. № СЗИ RU.0001.01БИ00.Б041), и экспертного заключения от 01.09.2023, оформленного органом по сертификации ЗАО «НПП «БИТ» (аттестат аккредитации от 22.05.2017 № СЗИ RU.0001.01БИ00.А008).

Заявитель: .

7.4. Архитектура UDV DATAPK Industrial Kit

В этом разделе:

- Интерфейс Комплекса
- Дополнительные функции Комплекса

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

- UDV DATAPK уровня Sensor (Сенсор) обладает следующим набором функций:
  - Получение данных от компонентов АСУ ТП, их обработка и передача в Комплекс уровня Management;
  - Пассивный анализ копии сетевого трафика;
  - Активный сбор данных о конфигурациях, уязвимостях и т.д.;
  - Пассивное получение событий из внешних источников по протоколу Syslog.

> **Внимание:**
>
> Сенсор не имеет веб-интерфейса. Управление сенсорами выполняет Комплекс уровня Management.

- UDV DATAPK уровня Management (UDV DATAPK среднего уровня) обладает следующим набором функций:
  - Детализированное представление данных;
  - Базовые панели мониторинга и отчетность;
  - Настройка анализа защищенности, парольной политики, правил сессий;
  - Анализ и корреляция событий безопасности;
  - Управление сенсорами;
  - Управление конфигурациями системы;
  - Интеграция со сторонними сервисами и автоматизация процессов ИБ с помощью REST API.
- UDV DATAPK уровня Supervision (UDV DATAPK верхнего уровня) обладает следующим набором функций:
  - Централизованный мониторинг состояния защищенности АСУ ТП и контроль деятельности распределенных отделов по ИБ АСУ ТП;
  - Получение аналитических данных для принятия обоснованных управленческих решений;
  - Централизованное управление учетными записями пользователей Комплексов уровня Management

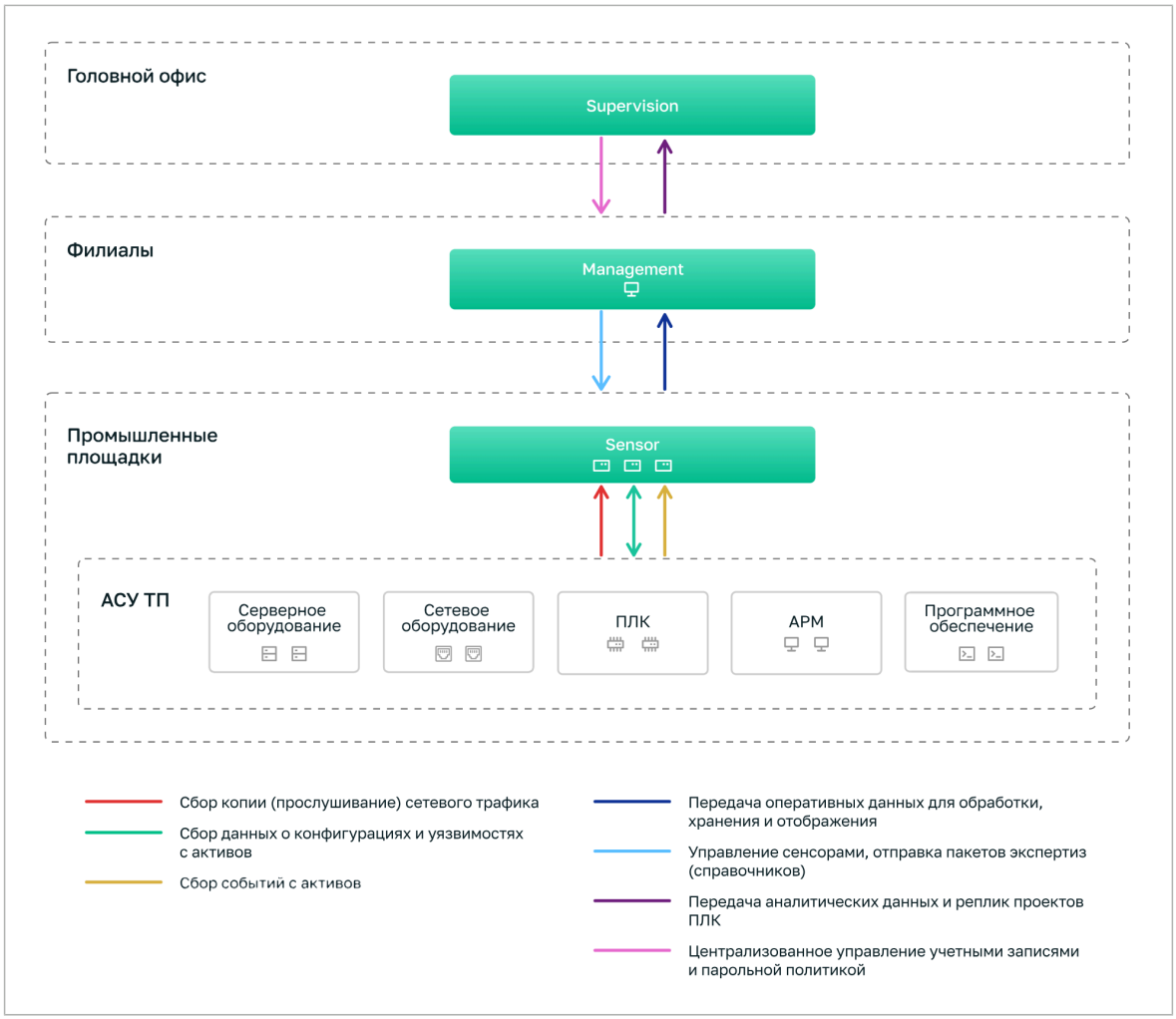


Рис. 112. Структурная схема иерархии

Порядок передачи информации по иерархии Комплексов

Предусмотрен следующий порядок взаимодействия между уровнями иерархии:

- Сенсор (Sensor) → Комплекс среднего уровня (Management) → Комплекс верхнего уровня (Supervision) – передача оперативных данных (результатов анализа сетевого трафика, событий и конфигураций, проверок на уязвимости и соответствие требованиям ИБ).
- Комплекс верхнего уровня (Supervision) → Комплекс среднего уровня (Management) – передача (репликация) учетных записей пользователей и парольной политики.
- Комплекс среднего уровня (Management) → Комплекс верхнего уровня (Supervision) – передача статистической информации об оперативных данных, о состоянии сенсоров и самих Комплексов уровня Management.

Перечень данных, передаваемых по иерархии «снизу вверх» (от сенсоров до Комплексов уровня Management), приведен в таблице ниже (Таблица 7. Перечень данных, передаваемых по иерархии «снизу вверх»).

Табл. 7. Перечень данных, передаваемых по иерархии «снизу вверх»

ДАННЫЕ	СЕНСОР → КОМПЛЕКС УРОВНЯ MANAGEMENT
События	✔

Табл. 7. Перечень данных, передаваемых по иерархии «снизу вверх»

ДАННЫЕ	СЕНСОР → КОМПЛЕКС УРОВНЯ MANAGEMENT
Активы	✔
Сетевые соединения	✔
Конфигурации	✔
Результаты проверок на уязвимости	✔
Результаты проверок на соответствие требованиям ИБ	✔
Инциденты ИБ	-

7.4.1. Список модулей UDV DATAPK Industrial Kit

Модульная архитектура UDV DATAPK Industrial Kit включает в себя 6 модулей:

- **Контроль версий (Version Control)** — предоставляет программистам и инженерам АСУ ТП инструменты для централизованного отказоустойчивого хранения проектов ПЛК, аудита изменений в проектах ПЛК, их резервирования и восстановления, а также отслеживания неизменности программ на ПЛК. Подробнее о работе с модулем см. раздел «Управление проектами ПЛК».
- **Анализ промышленного сетевого трафика (Industrial NTA)** — позволяет организациям находить устройства внутри сети и сетевые взаимодействия между ними, быстро выявлять атаки и проводить расследования, а также контролировать параметры технологических процессов, опираясь на данные из копии промышленного сетевого трафика. Подробнее о работе с модулем см. раздел «Анализ промышленного сетевого трафика».
- **Управление конфигурациями (Configuration Management)** — позволяет инженерам АСУ ТП и специалистам по ИБ контролировать соответствие любых конфигурационных параметров IT-устройств и устройств АСУ ТП на соответствие необходимым значениям, отслеживать изменения в значениях, проводить аудит и оперативно реагировать на изменения. Подробнее о работе с модулем см. раздел «Активный сбор данных с активов».
- **Управление уязвимостями (Vulnerability Management)** — позволяет специалистам по ИБ возможность проводить неинвазивный аудит защищенности компонентов АСУ ТП методом белого ящика (White Box), выявлять угрозы информационной безопасности, устранять их, а также провести проверку соответствия требованиям ИБ. Подробнее о работе с модулем см. раздел «Поиск уязвимостей и проверка соответствия требованиям информационной безопасности».

  > ⚠ Внимание:
  >
  > Для работы модуля «Управление уязвимостями» необходимо установить модуль «Управление конфигурациями».

- **Управление внешними событиями (External Events Management)** — предоставляет организациям набор инструментов для обработки и анализа событий ИБ, собранных с внешних источников. В составе модуля

механизмы сбора, нормализации и корреляции событий ИБ, поиска по событиям ИБ, визуализации данных на основе событий ИБ с возможностью дальнейшей отправки данных в сторонние системы класса SIEM. Подробнее о работе с модулем см. разделы:

- Просмотр событий и создание запросов в экспертном режиме
- Импортируемые панели мониторинга
- Настройка и управление мониторингом
- Работа с инцидентами

- **Обнаружение и реагирование для ПЛК (EDR for PLC)** — позволяет организациям оперативно начать выявлять аномалии в поведении ПЛК посредством безагентного поведенческого анализа на основе запатентованных методов машинного обучения, а также реагировать на них. Подробнее о работе с модулем см. раздел «Управление модулем обнаружения и реагирования для ПЛК («EDR for PLC»)».

> Внимание:
>
> Для работы модуля EDR for PLC необходимо установить модули «Анализ промышленного сетевого трафика» и «Управление внешними событиями».

7.4.2. Архитектура модуля «Управление проектами ПЛК»

Архитектура модуля «Управление проектами ПЛК» (Version Control) описывается следующими уровнями:

- **Supervision**. Верхний уровень серверной архитектуры, предназначенный для централизованного мониторинга и управления всей системой. На этом уровне осуществляется:
  - Централизованное управление решением, получение данных со всех площадок.
  - Централизованное хранение копий проектов.
  - Просмотр панелей мониторинга, отчетов, инфографики по всем объектам предприятия.
- **Management**. Реализован как Version Control Management. Серверная часть, которая устанавливается отдельно и хранит всю информацию об изменениях исходного кода версий ПЛК. На этом уровне осуществляется:
  - Учет и контроль изменений в ПО (проекты ПЛК/АСУ ТП), в том числе сравнение версий проекта.
  - Хранение резервных копий ПО и восстановление ПО.
  - Формирование и отправка событий ИБ в сторонние системы.
- **Sensor**. На этом уровне осуществляется сбор данных с ПЛК для контроля неизменности ПО и конфигураций ПЛК.
- **Desktop App**. Реализован как приложение Version Control Desktop App.Возможности этого уровня:
  - Устанавливается на инженерные станции.
  - Позволяет загружать проекты в Version Control Management.
  - Позволяет скачивать проекты с Version Control Management.
  - Позволяет вносить обоснования изменений проектов ПЛК и просматривать историю изменений.
  - Проверяет соответствие версий проектов ПЛК в Version Control Desktop App и Version Control Management.

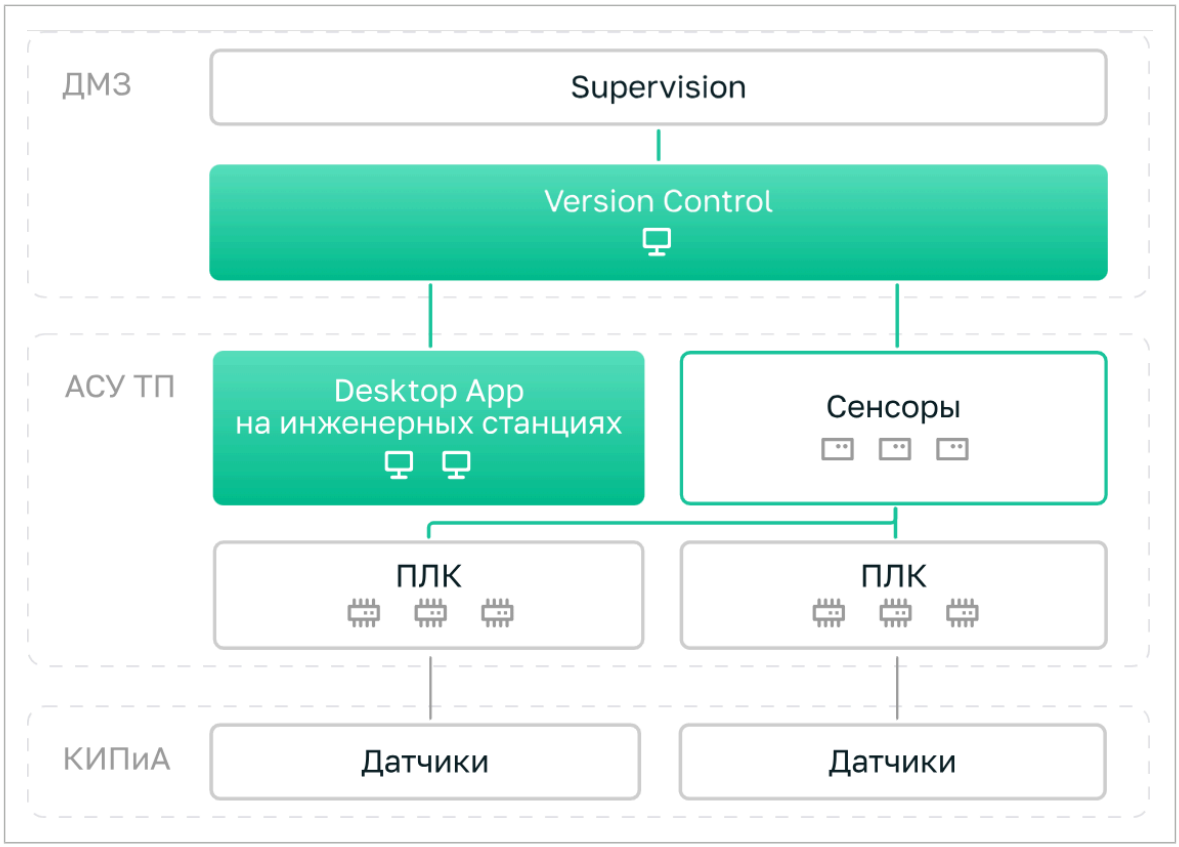


Рис. 114. Архитектура Version Control

7.4.3. Общие сведения о модуле «EDR for PLC»

Модуль UDV DATAPK EDR for PLC формирует комплексную Модель системы, в том числе схему ее работы, и выявляет отклонения в работе ее компонентов. Совместим с любыми автоматизированными системами, не требует информации о топологии, особенностях применяемых протоколов и алгоритмов.

Модуль UDV DATAPK EDR for PLC выявляет признаки инцидента на ранней стадии и формирует подробную информацию о затронутых процессах и компонентах.

Принципы работы модуля:

- применение технологий машинного обучения для раннего выявления аномалий;
- инвентаризация компонентов системы и их взаимодействие;
- поведенческий анализ компонентов системы;
- автоматизированное моделирование системы.

Алгоритмы построения модели основан на пассивном наблюдении за работой каждого компонента защищаемой системы и не требует активного взаимодействия с ней.

7.4.4. Общие сведения о модуле «Анализ промышленного сетевого трафика»

В этом разделе:

- Поддерживаемые протоколы передачи данных
- Поддерживаемые функции промышленных протоколов

Модуль «Анализ промышленного сетевого трафика» (Industrial Network Traffic Analyzer, Industrial NTA)— модуль для анализа трафика промышленной сети с целью обнаружения в ней подозрительной активности.

Основные функции Industrial NTA:

- хранение истории активности и длительности обнаруженных сетевых соединений;
- встроенный механизм глубокой инспекции (Deep Packet Inspection, DPI) сетевых протоколов;
- выявление туннелей и доменных имен, сгенерированных алгоритмом (Domain Generation Algorithm, DGA) посредством технологий машинного обучения;
- контроль параметров технологических процессов по протоколам Modbus, OPC UA, Emerson DeltaV;
- выгрузка переданных по сети файлов из сетевого трафика;
- извлечение файлов, передаваемых в сетевом трафике;
- выгрузка файлов сетевого трафика (`.pcap`) в пользовательском интерфейсе;
- фильтрация копии сетевого трафика;
- выявление активов из сетевого трафика;
- автоматическое создание правил сессий.

7.4.4.1. Поддерживаемые протоколы передачи данных

Модуль «Анализ промышленного сетевого трафика» способен разбирать различные данные в трафике активов на следующих уровнях:

- индикация — базовое распознавание протокола в трафике: его наличие и наименование без дополнительной информации о содержании его полей. Такие протоколы отображаются в столбце **Протоколы** вкладки **Сессии** и в поле **Протоколы** карточки сессии;
- анализ событий ИБ — выявление в трафике подозрительных или вредоносных действий с определением использованной техники атаки — доступно на страницах **События** и **Инциденты**;
- подробный анализ полей протоколов — подробный анализ и отображение детальной информации о содержании полей протокола. Список таких протоколов представлен в группе вкладок **Протоколы** на странице **Сетевые соединения**;
- контроль параметров технологического процесса — мониторинг и валидация значений, критичных для техпроцесса, с целью выявления несанкционированных изменений;
- выявление аномалий ПЛК — выявление отклонений в поведении программируемых логических контроллеров — например, появление новых узлов в контролируемой сети, запуск на узлах новой службы;
- извлечение файлов из трафика — обнаружение, анализ и сохранение файлов, передаваемых в рамках сессий — доступно на вкладке **Файлы** страницы **Сетевые соединения**.

В таблице ниже представлена информация о поддерживаемых протоколах и уровнях их разбора. Протоколы сгруппированы по назначению: общие и промышленные. Наличие галочки (✓) означает поддержку соответствующего уровня анализа, крестик (×) — отсутствие.

Табл. 8. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
Протоколы общего назначения						
ARP (Address Resolution Protocol)	×	✓	×	Непри-менимо	Непри-менимо	×
AYIYA (Anything In Anything)	✓	×	×			×
DCE/RPC (Distributed Computing Environment / Remote Procedure Calls)	✓	✓	✓			×
DHCP (Dynamic Host Configuration Protocol)	✓	×	×			×
DNS (Domain Name System)	✓	✓	✓			×
DTLS (Datagram Transport Layer Security)	✓	×	×			×
Finger	✓	×	×			×
FTP (File Transfer	✓	×	×			✓

Табл. 8. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
Protocol) — Control connection						
Geneve	✓	×	×			×
GSSAPI (Generic Security Service Application Program Interface)	✓	×	×			×
GTPV1 (GPRS Tunneling Protocol Version 1)	✓	×	×			×
HTTP (Hyper Text Transfer Protocol)	✓	✓	✓			✓
ICMP (Internet Control Message Protocol)	✓	✓	×			×
IMAP (Internet Message Access Protocol)	✓	×	×			×
IRC (Internet Relay Chat)	✓	×	×			✓

Табл. 8. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
Kerberos	✓	×	✓			✓
LDAP (Lightweight Directory Access Protocol)	✓	×	×			×
LLMNR (Link-local Multicast Name Resolution)	×	✓	×			×
MDNS (Multicast Domain Name System)	×	✓	×			×
MQTT (Message Queue Telemetry Transport)	✓	×	×			×
MySQL	✓	×	×			×
NBNS (Network Basic Input/ Output System Name Service)	✓	×	×			×
NTLM (New Technology	✓	✓	✓			×

Табл. 8. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
LAN Manager)						
NTP (Network Time Protocol)	✓	×	×			×
POP3 (Post Office Protocol Version 3)	✓	×	×			×
PGSQL (PostgreSQL)	✓	×	×			×
QUIC	✓	×	×			×
RADIUS (Remote Authentication Dial-In User Service)	✓	×	×			×
RDP (Remote Desktop Protocol)	✓	×	✓			✓[2]
RFB/VNC (Remote Framebuffer)	✓	×	×			×
SIP (Session Initiation Protocol)	✓	×	×			×

2. Извлеченные файлы содержат только данные об использованном в соединении сертификате SSL/TLS.

Табл. 8. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
SMB (Server Message Block)	✓	✓	✓			✓
SMTP (Simple Mail Transfer Protocol)	✓	×	✓			✓
SNMP (Simple Network Management Protocol)	✓	×	×			×
SOCKS	✓	×	×			×
SSH (Secure Shell)	✓	✓	✓			×
SSL (Secure Sockets Layer)	✓	×	✓			✓
SYSLOG	✓	×	×			×
TDS (Tabular Data Stream)	✓	×	×			×
TELNET	✓	×	×			×
TFTP	✓	×	×			×
TNS (Transparent Network Substrate)	✓	×	×			×

Табл. 8. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
TPKT/COTP (Connection-Oriented Transport Protocol)	✓	×	×			×
VXLAN (Virtual Extensible LAN)	✓	×	×			×
WS DISCOVERY (Web Services Dynamic Discovery)	✓	×	×			×
XMPP (Extensible Messaging and Presence Protocol)	✓	×	×			×
Протоколы промышленного назначения						
DNP3 (Distributed Network Protocol 3)	✓	✓	×	×	×	×
Emerson DeltaV	✓	✓	✓	✓	×	×
ENIP/CIP (Ethernet Industrial Protocol/ Common	✓	✓	×	×	✓	×

Табл. 8. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИНДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПОДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРОТОКОЛОВ	КОНТРОЛЬ ПАРАМЕТРОВ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
Industrial Protocol)						
IEC 60870-5-104	✓	✓	×	×	✓	×
IEC 61850 MMS (Manufacturing Message Specification)	✓	×	×	×	✓	×
Modbus	✓	×	✓	✓	✓	×
OPC UA (Open Platform Communications Unified Architecture)	✓	×	✓	✓	✓	×
S7 Communication	✓	✓	×	×	✓	×
S7 Plus Communication	✓	✓	×	×	✓	×
UMAS (Unified Messaging Application Services)	✓	✓	×	×	×	×

7.4.4.2. Поддерживаемые функции промышленных протоколов

В данном разделе приведен перечень функций техпроцесса, обнаруживаемых модулем «Анализ промышленного сетевого трафика». Функции сгруппированы по поддерживаемым промышленным протоколам. Для каждого протокола функции разделены на «Управляющие» и «Критичные». Функции из группы «Критичные» по умолчанию

заданы в конфигурационном файле `ics-function.dat`, который можно настроить в соответствии со своими задачами (см. раздел «Изменение списка критичных функций»).

Функции протокола CIP

Управляющие:

- Find Next Object Instance
- Get Instance Attribute List
- Get Instance Attribute List Reply
- Group Sync
- Mask
- Read/Modify/Write Tag
- Read/Modify/Write Tag Reply
- Read Tag
- Read Tag Fragmented
- Read Tag Fragmented Reply
- Read Tag Reply
- Response Mask
- Write Tag
- Write Tag Fragmented
- Write Tag Fragmented Reply
- Write Tag Reply

Критичные:

- Apply Attributes
- Create
- Delete
- Error Response
- Execute PCCC Service
- Forward Open
- Forward Open Reply
- Get Attribute List
- Get Attribute List Reply
- Get Attributes All
- Get Attributes All Reply
- Get Attribute Single Reply
- Get Attributes Single
- Get Connection Point Member List
- Get Member
- Insert Member
- Multiple Service Packet
- Multiple Service Packet Reply
- No Forward Open
- Remove Member
- Reset
- Restore

- Save
- Set Attribute List
- Set Attributes All
- Set Attributes Single
- Set Member
- Start
- Stop

Функции протокола DeltaV

Управляющие:

- Close module session
- Create subscription
- Get config card info
- Get phys card info
- Get running modules
- Open device session
- Open module session
- Switchover
- Write tag

Критичные:

- Debug force module input
- Debug start
- Debug stop
- Download
- Online mode enable
- Select mode
- Upgrade
- Upload parameters

Функции протокола DNP3

Управляющие

- ASSIGN_CLASS
- AUTHENTICATE_RESP
- CONFIRM
- DELAY_MEASURE
- DIRECT_OPERATE
- DIRECT_OPERATE_NR
- FREEZE_AT_TIME
- FREEZE_AT_TIME_NR
- FREEZE_CLEAR
- FREEZE_CLEAR_NR
- IMMED_FREEZE
- IMMED_FREEZE_NR
- OPERATE

- READ
- RECORD_CURRENT_TIME
- RESPONSE
- SELECT
- UNSOLICITED_RESPONSE
- WRITE

Критичные:

- ABORT_FILE
- ACTIVATE_CONFIG
- AUTHENTICATE_FILE
- AUTHENTICATE_REQ
- AUTHENTICATE_REQ_NR
- CLOSE_FILE
- COLD_RESTART
- DELETE_FILE
- DISABLE_UNSOLICITED
- ENABLE_UNSOLICITED
- GET_FILE_INFO
- INITIALIZE_APPL
- INITIALIZE_DATA
- OPEN_FILE
- SAVE_CONFIG
- START_APPL
- STOP_APPL
- WARM_RESTART

Функции протокола IEC104

Табл. 9. Управляющие функции протокола IEC104, поддерживаемые модулем «Анализ промышленного сетевого трафика»

ФУНКЦИЯ (ОБОЗНАЧЕНИЕ В КОНФИГУРАЦИИ)	ОПИСАНИЕ (ОБОЗНАЧЕНИЕ В СОБЫТИИ)
C_BO_NA_1	bit string 32 bit
C_BO_TA_1	bit string 32 bit with time tag CP56Time2a
C_CD_NA_1	delay acquisition command
C_CI_NA_1	counter interrogation command
C_CS_NA_1	clock synchronization command
C_DC_TA_1	double command with time tag CP56Time2a

Табл. 9. Управляющие функции протокола IEC104, поддерживаемые модулем «Анализ промышленного сетевого трафика»

ФУНКЦИЯ (ОБОЗНАЧЕНИЕ В КОНФИГУРАЦИИ)	ОПИСАНИЕ (ОБОЗНАЧЕНИЕ В СОБЫТИИ)
C_IC_NA_1	(general-) interrogation command
C_RC_NA_1	regulating step command
C_RC_TA_1	regulating step command with time tag CP56Time2a
C_RD_NA_1	read command
C_SC_TA_1	single command with time tag CP56Time2a
C_SE_NA_1	setpoint command; normalized value
C_SE_NB_1	setpoint command; scaled value
C_SE_NC_1	setpoint command; short floating point value
C_SE_TA_1	setpoint command; normalized value with time tag CP56Time2a
C_SE_TB_1	setpoint command; scaled value with time tag CP56Time2a
C_SE_TC_1	setpoint command; short floating point value with time tag CP56Time2a
C_TS_NA_1	test command
C_TS_TA_1	test command with time tag CP56Time2a
F_AF_NA_1	ack file; ack section
F_DR_TA_1	directory
F_FR_NA_1	file ready
F_LS_NA_1	last section; last segment
F_SC_NB_1	queryLog - request archive file
F_SG_NA_1	segment
F_SR_NA_1	section ready
M_BO_NA_1	bit string of 32 bit

Табл. 9. Управляющие функции протокола IEC104, поддерживаемые модулем «Анализ промышленного сетевого трафика»

ФУНКЦИЯ (ОБОЗНАЧЕНИЕ В КОНФИГУРАЦИИ)	ОПИСАНИЕ (ОБОЗНАЧЕНИЕ В СОБЫТИИ)
M_BO_TA_1	bit string of 32 bit with time tag
M_BO_TB_1	bit string of 32 bit with time tag CP56Time2a
M_DP_NA_1	double point information
M_DP_TA_1	double point information with time tag
M_DP_TB_1	double point information with time tag CP56Time2a
M_EI_NA_1	end of initialization
M_EP_TA_1	event of protection equipment with time tag
M_EP_TB_1	packed start events of protection equipment with time tag
M_EP_TC_1	packed output circuit information of protection equipment with time tag
M_EP_TD_1	event of protection equipment with time tag CP56Time2a
M_EP_TE_1	packed start events of protection equipment with time tag CP56time2a
M_EP_TF_1	packed output circuit information of protection equipment with time tag CP56Time2a
M_IT_NA_1	integrated totals
M_IT_TA_1	integrated totals with time tag
M_IT_TB_1	integrated totals with time tag CP56Time2a
M_ME_NA_1	measured value; normalized value
M_ME_NB_1	measured value; scaled value
M_ME_NC_1	measured value; short floating point value
M_ME_ND_1	measured value; normalized value without quality descriptor
M_ME_TA_1	measured value; normalized value with time tag
M_ME_TB_1	measured value; scaled value with time tag

Табл. 9. Управляющие функции протокола IEC104, поддерживаемые модулем «Анализ промышленного сетевого трафика»

ФУНКЦИЯ (ОБОЗНАЧЕНИЕ В КОНФИГУРАЦИИ)	ОПИСАНИЕ (ОБОЗНАЧЕНИЕ В СОБЫТИИ)
M_ME_TC_1	measured value; short floating point value with time tag
M_ME_TD_1	measured value; normalized value with time tag CP56Time2a
M_ME_TE_1	measured value; scaled value with time tag CP56Time2a
M_ME_TF_1	measured value; short floating point value with time tag CP56Time2a
M_PS_NA_1	packed single-point information with status change detection
M_SP_NA_1	single point information
M_SP_TA_1	single point information with time tag
M_SP_TB_1	single point information with time tag CP56Time2a
M_ST_NA_1	single point information
M_ST_TA_1	step position information with time tag
M_ST_TB_1	step position information with time tag CP56Time2a
P_AC_NA_1	parameter activation
P_ME_NA_1	parameter of measured value; normalized value
P_ME_NB_1	parameter of measured value; scaled value
P_ME_NC_1	parameter of measured value; short floating point value

Табл. 10. Критичные функции протокола IEC104, поддерживаемые модулем «Анализ промышленного сетевого трафика»

ФУНКЦИЯ (ОБОЗНАЧЕНИЕ В КОНФИГУРАЦИИ)	ОПИСАНИЕ (ОБОЗНАЧЕНИЕ В СОБЫТИИ)
C_DC_NA_1	double command
C_RP_NA_1	reset process command
C_SC_NA_1	single command

Табл. 10. Критичные функции протокола IEC104, поддерживаемые модулем «Анализ промышленного сетевого трафика»

ФУНКЦИЯ (ОБОЗНАЧЕНИЕ В КОНФИГУРАЦИИ)	ОПИСАНИЕ (ОБОЗНАЧЕНИЕ В СОБЫТИИ)
Change_Value_Command	IEC104_change_value_command in netpdl.xml
F_SC_NA_1	call directory; select file; call file; call section
Insert_Command	IEC104_insert_command and IEC104_insert_off_command in netpdl.xml

Функции протокола Modbus

Управляющие:

- DIAGNOSTICS
- ENCAP_INTERFACE_TRANSPORT
- GET_COMM_EVENT_COUNTER
- GET_COMM_EVENT_LOG
- MASK_WRITE_REGISTER
- READ_COILS
- READ_DISCRETE_INPUTS
- READ_EXCEPTION_STATUS
- READ_FIFO_QUEUE
- READ_FILE_RECORD
- READ_HOLDING_REGISTERS
- READ_INPUT_REGISTERS
- READ_WRITE_MULTIPLE_REGISTERS
- REPORT_SLAVE_ID
- WRITE_FILE_RECORD
- WRITE_MULTIPLE_COILS
- WRITE_MULTIPLE_REGISTERS
- WRITE_SINGLE_COIL
- WRITE_SINGLE_REGISTER

Критичные:

- не заданы

Функции протокола S7 Communication

Управляющие:

- CPU Services
- Mode Transition
- Read Variable
- Setup Communication
- Write Variable

Критичные:

- Download Block
- Download Ended
- End Upload
- PLC Control
- PLC Stop
- Request Download
- Start Upload
- Upload

Функции протокола S7 Plus Communication

Управляющие:

- HW_Config_Change

Критичные:

- Program_Transfer_From_Plc
- Program_Transfer_To_Plc
- Start_CPU
- Stop_CPU

Функции протокола UMAS

Управляющие:

- RESPONSE_ERROR
- RESPONSE_OK
- UMAS_CHECK_PLC
- UMAS_GET_STATUS_MODULE
- UMAS_INIT_COMM
- UMAS_KEEP_ALIVE
- UMAS_MONITOR_PLC
- UMAS_READ_CARD_INFO
- UMAS_READ_COILS_REGISTERS
- UMAS_READ_ETH_MASTER_DATA
- UMAS_READ_ID
- UMAS_READ_IO_OBJECT
- UMAS_READ_MEMORY_BLOCK
- UMAS_READ_PLC_INFO
- UMAS_READ_PROJECT_INFO
- UMAS_READ_VARIABLES
- UMAS_RELEASE_PLC_RESERVATION
- UMAS_REPEAT
- UMAS_TAKE_PLC_RESERVATION
- UMAS_WRITE_COILS_REGISTERS
- UMAS_WRITE_IO_OBJECT
- UMAS_WRITE_VARIABLES

Критичные:

- UMAS_END_TRANSFER_PROJECT_FROM_PLC
- UMAS_END_TRANSFER_PROJECT_TO_PLC
- UMAS_INITIALIZE_TRANSFER_PROJECT_FROM_PLC
- UMAS_INITIALIZE_TRANSFER_PROJECT_TO_PLC
- UMAS_START_PLC
- UMAS_STOP_PLC
- UMAS_TRANSFER_PROJECT_FROM_PLC
- UMAS_TRANSFER_PROJECT_TO_PLC

См. также

Управление сервисом регистрации событий техпроцесса

Изменение списка критичных функций

7.5. Условия эксплуатации Комплекса

По условиям эксплуатации аппаратная часть для Комплекса предназначена для установки в стационарных, специальных и временных отапливаемых помещениях и укрытиях в условиях круглосуточной работы с перерывами на техническое обслуживание.

Нормальными климатическими условиями эксплуатации аппаратной части для Комплекса являются:

- температура окружающего воздуха – от –10 до +60 °С;
- относительная влажность воздуха – от 5 до 95%;
- атмосферное давление – от 630 до 800 мм рт.ст.

Способ подключения аппаратной части для Комплекса к оборудованию объекта информатизации определяется на этапе предпроектного обследования.

7.6. Содержание архива с резервной копией Комплекса

Модуль резервного копирования `backup_manager` Комплекса уровня Management позволяет выполнять резервное копирование основных данных и сохранять их в архив `dtpk-backup-[version]-[YYYYmmddhhmmss].tar`. Архив содержит следующие файлы:

- `data.tar.bz2` — архив, включающий в себя следующие файлы:
  - директория `/usr/share/udv/vulnerability-backend`, содержащая справочники уязвимостей (CPE, CVE и Банк данных угроз безопасности информации ФСТЭК России) для работы модуля «Управление уязвимостями»;
  - директория `/etc/logstash/pipeline` с файлом `09-custom-filter.conf`, содержащим пользовательские фильтры для нормализации внешних событий модулем «Управление внешними событиями»;
  - директория `/var/backup/` с файлом `nta-backup-[версия_Комплекса]-[дата]` резервной копии базы данных `clickhouse` модуля «Анализ промышленного сетевого трафика» (если в команде

создания резервной копии был задан параметр `--include-nta` для создания копии этой БД и модуль был установлен при выполнении резервного копирования);

- директория `/usr/share/udv/datapk` с конфигурационным файлом `manager.env` сервисов Комплекса.

- `repos_data.tar.bz2`— архив, содержащий репозитории ПЛК, которые хранятся в модуле «Управление проектами ПЛК»;
- `maria_db_dump.aes`, `redis_db_dump.aes` и `postgres_db_dump.aes` — резервные копии баз данных, зашифрованные паролем, который задается при запуске резервного копирования (в ключе `--password`);
- `info.json` — метаданные, включающие контрольные суммы файлов резервной копии.

См. также

Восстановление данных из резервной копии Комплекса уровня Management и Комплекса уровня Management+Sensor

7.7. Переменные Комплекса

Для Комплексов уровня Management и Sensor, а также их сервисов устанавливаются разные конфигурационные файлы с различным набором переменных.

Конфигурационные файлы с переменными и их расположение представлены в таблице ниже.

Табл. 11. Конфигурационные файлы с переменными и их расположение

ТИП КОМПЛЕКСА	МОДУЛЬ
Комплекс уровня Management	Базовый модуль (Core)
	Управление внешними событиями
	Анализ промышленного сетевого трафика
Комплекс уровня Sensor	Базовый модуль (Core)
	Анализ промышленного сетевого трафика
	EDR for PLC

См. также

Переменные Комплекса уровня Management

Переменные Комплекса уровня Sensor

Переменные службы обнаружения вторжений

Конфигурационные файлы модуля «EDR for PLC»

Рекомендации по использованию переменных файлов manager.env и sensor.env

7.7.1. Переменные Комплекса уровня Management

Обязательные переменные файла manager.env

Переменные файла `manager.env` устанавливаются в директории `/usr/share/udv/datapk`

Список обязательных переменных, содержащийся в файле `manager.env` Комплекса уровня Management, представлен в таблице ниже.

Табл. 12. Обязательные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`DB_USER`	Пользователь базы данных. ОСТОРОЖНО: Изменение значения переменной может привести к отсутствию доступа к базе данных.	`postgres`
`DB_PASS`	Пароль доступа к базе данных.	`P@ssw0rd`

Табл. 12. Обязательные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
	ОСТОРОЖНО: Изменение значения переменной может привести к отсутствию доступа к базе данных.	
`HOST_IP`	Интерфейс управления Комплекса. В качестве значения переменной задается IP-адрес одного из активных интерфейсов Комплекса	`10.51.15.104`
`DB_ENCRYPTION_KEY`	Ключ шифрования базы данных в сборщике данных (`udv-host-data-collector`). Ключ должен иметь длину 24 символа. ОСТОРОЖНО: Изменение значения переменной может привести к отсутствию доступа к базе данных.	`dJ2ZOZeU0nJhHwjfhqlOwF1x`
`EVENT_INDICES_MAX_SIZE_GB`	Максимально допустимый объем оперативного архива внешних событий. Суммарный объем с `EVENT_ARCHIVES_MAX_SIZE_GB` не должен составлять более 50-60% объема дискового пространства Внимание: На Комплексах базового уровня и (или) с HDD — не более 100 ГБ. На Комплексах среднего и верхнего уровней с SSD — не более 300 ГБ	`10`
`EVENT_INDICES_ACTION_SIZE_EXCEEDED`	Действие в случае переполнения оперативного архива внешних событий. Возможные варианты значений переменной:	`rotate`

Табл. 12. Обязательные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
	• `nothing`; • `break`; • `rotate`.	
`EVENT_INDICES_LIFETIME_DAYS`	Время хранения внешних событий в оперативном архиве, задается в днях	`30`
`EVENT_ARCHIVES_LIFETIME_DAYS`	Время хранения внешних событий в глубоком архиве, события старше указанного значения удаляются. Значение задается в днях	`60`
`EVENT_ARCHIVES_MAX_SIZE_GB`	Максимально допустимый объем глубокого архива внешних событий. Суммарный объем с `EVENT_INDICES_MAX_SIZE_GB` должен составлять не более 50-60% объема дискового пространства. Значение задается в гигабайтах	`5`
`EVENT_ARCHIVES_ACTION_SIZE_EXCEEDED`	Действие, выполняемое при превышении лимита на размер глубокого архива внешних событий. Возможные значения переменной: • `nothing` • `break` • `rotate`	`rotate`
`EVENTS_RETENTION_DISK_CAPACITY_SIZE_MB`	Максимально допустимый объем архива событий, хранящегося в модуле внутренних событий. При достижении предельного значения, заданного в этой переменной, регистрация внутренних событий останавливается. Значение задается в мегабайтах. При значении `0` лимит на хранение архива внутренних событий отключен	`0`
`EVENTS_RETENTION_MONTHS`	Временной период, по истечении которого удаляются внутренние события старше срока, указанного в этой переменной. Значение задается в месяцах	`3`

Дополнительные переменные файла manager.env

Переменные, которые не включены в автоматически генерируемый файл `manager.env` Комплекса уровня Management и добавляются при необходимости, указаны в таблице ниже.

Табл. 13. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`API_SKIP_FIRST_INITIALIZATION`	Отключение первичной инициализации при первом запуске Комплекса при значении переменной `true`	`false`
`AUTOMATIC_HOST_CREATION_BY_MAC`	При значении переменной `true` Комплекс фиксирует активы только по MAC-адресу независимо от наличия у них IP-адреса. В списке активов отображаются все найденные активы (до настройки контролируемой сети активы отображаются только с MAC-адресами). При значении переменной `false`, Комплекс фиксирует активы по MAC-адресу (если IP-адрес не обнаружен) и по связке MAC-адреса и IP-адреса. В списке активов будут отображаться только активы, IP-адреса которых входят в контролируемую сеть, а также активы, IP-адреса которых не обнаружены	`false`
`ASSETS_INACTIVITY_TIMEOUT`	Время, по истечении которого при отсутствии трафика от актива на активных интерфейсах формируется событие о его недоступности и индикатор на странице **Активы** становится серым. Значение задается в секундах. ⚠ Внимание: Значение переменной не может быть меньше `600` секунд.	`600`
`LIMIT_USER_SESSIONS`	При значении переменной `true` ограничивает до одной количество одновременных активных сессий в веб-интерфейсе Комплекса для каждой учетной записи. При значении переменной `false` ограничений на количество сессий нет	`false`
`NGINX_HTTPS_PORT`	Порт для подключения к Комплексу по протоколу HTTPS	`443`

Табл. 13. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`USER_SESSION_INACTIVITY_TIMEOUT`	Ограничение сессии при отсутствии активности пользователя. Значение задается в секундах	`600`
`LDAP_CONNECTION_STRING`	IP-адрес LDAP-сервера Active Directory для создания пользователей из службы каталогов	`ldaps://192.168.243.121`
`LDAP_TLS`	Использовать TLS-шифрование для Active Directory	`false`
`LOG_LEVEL`	Минимальная критичность системных событий, которые генерирует Комплекс уровня Management. Возможные значения: • `CRITICAL` • `FATAL` • `ERROR` • `WARNING` • `INFO` • `DEBUG` • `NOTSET`	`INFO`
`MAX_ROWS_PER_REPORT`	Максимальное количество строк, выгружаемых при формировании отчета. Если значение переменной более 1000, в отчет выгрузится только 1000 строк	`1000`
`DISABLE_CONFIGURATION_CONTROL_EVENTS`	При значении переменной `true` события об изменении конфигурации не создаются	`false`
`DISABLE_HOST_DATA_COLLECTING_EVENTS`	При значении переменной `true` события сбора данных не создаются	`false`
`DISABLE_USER_ACTION_CONTROL_EVENTS`	При значении переменной `true` события о действиях пользователей не создаются	`false`

Табл. 13. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`DISABLE_HOST_CONTROL_EVENTS`	При значении переменной `true` события о появлении новых, изменении и удалении узлов не создаются	`false`
`DISABLE_AVAILABILITY_CONTROL_EVENTS`	При значении переменной `true` события о доступности узлов не создаются	`false`
`DISABLE_OVAL_ASSESSMENT_CONTROL_EVENTS`	При значении переменной `true` события о проверках на соответствие требованиям ИБ не создаются	`false`
`DISABLE_INCIDENT_CONTROL_EVENTS`	При значении переменной `true` события об инцидентах не создаются	`false`
`DISABLE_OVAL_DEFINITIONS_CONTROL_EVENTS`	При значении переменной `true` события об удалении проверок на соответствие требованиям ИБ не создаются	`false`
`DISABLE_OVAL_GROUPS_CONTROL_EVENTS`	При значении переменной `true` события об удалении групп Open Vulnerability and Assessment Language-определений не создаются	`false`
`DISABLE_BACKUP_CONTROL_EVENTS`	При значении переменной `true` события о резервном копировании не создаются	`false`
`DISABLE_SURICATA_CONTROL_EVENTS`	При значении переменной `true` события службы обнаружения вторжений не собираются	`false`
`DISABLE_HOME_NET_SCAN_CONTROL_EVENTS`	При значении переменной `true` события при сканировании контролируемой сети не собираются	`false`
`DISABLE_SCRIPT_VERIFICATION_EVENTS`	При значении переменной `true` события регистрации скриптов не собираются	`false`
`DISABLE_SYSTEM_CONTROL_EVENTS`	При значении переменной `true` системные события не собираются	`false`
`CONFIGURATION_CONTROL_EVENTS_SEVERITY`	Важность событий изменения конфигурации	`low`

Табл. 13. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`HOST_DATA_COLLECTING_EVENTS_SEVERITY`	Важность событий сбора и ошибок сбора данных	`low`
`USER_ACTION_CONTROL_EVENTS_SEVERITY`	Важность событий по действиям пользователей	`low`
`HOST_CONTROL_EVENTS_SEVERITY`	Важность событий появления новых узлов	`low`
`AVAILABILITY_CONTROL_EVENTS_SEVERITY`	Важность событий доступности узлов	`low`
`OVAL_ASSESSMENT_CONTROL_EVENTS_SEVERITY`	Важность событий об объектах OVAL	`low`
`INCIDENT_CONTROL_EVENTS_SEVERITY`	Важность событий о создании, удалении, изменении инцидентов	`low`
`OVAL_DEFINITIONS_CONTROL_EVENTS_SEVERITY`	Важность событий удаления проверок на соответствие требованиям ИБ	`low`
`OVAL_GROUPS_CONTROL_EVENTS_SEVERITY`	Важность событий удаления групп OVAL-определений	`low`
`BACKUP_CONTROL_EVENTS_SEVERITY`	Важность событий резервного копирования	`low`
`EVENT_CONTROL_EVENTS_SEVERITY`	Важность событий, полученных от сервиса регистрации событий	`critical`
`HOME_NET_SCAN_CONTROL_EVENTS_SEVERITY`	Важность событий, полученных при сканировании контролируемой сети	`low`
`SCRIPT_VERIFICATION_EVENTS_SEVERITY`	Важность событий верификации скриптов	`low`
`SYSTEM_CONTROL_EVENTS_SEVERITY`	Важность системных событий	`low`
`IDS_CONTROL_EVENTS_SEVERITY`	Важность событий службы обнаружения вторжений	`critical`
`DPI_CONTROL_EVENTS_SEVERITY`	Важность событий `dpi_notice`	`critical`

Табл. 13. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ML_CONTROL_EVENTS_SEVERITY`	Важность событий `ml_notice`	`critical`
`SESSION_CONTROL_EVENTS_SEVERITY`	Важность событий, связанных с сетевыми соединениями	`critical`
`FSTEC_MAPPINGS_ENABLED`	При значении переменной `false`: • скрывает на странице **Импорт и экспорт** импорт справочника БДУ ФСТЭК России; • скрывает в окне **Просмотр уязвимостей** столбец **БДУ ФСТЭК** с дополнительной информацией об уязвимостях из БДУ ФСТЭК России; • скрывает в CSV-отчете результатов поиска уязвимостей столбцы с дополнительной информацией об уязвимостях из БДУ ФСТЭК России	`true`
`OVAL_IMPORT_TIMEOUT_MINUTES`	Время, по истечении которого импорт OVAL-групп завершается с ошибкой. Значение задается в минутах	`10`
`ENABLE_DNS_PINNING_PROTECTION`	Включение защиты от атаки Anti DNS Pinning. При значении переменной `true` веб-сервер будет отправлять 404 ошибку, если запрос пришел на адрес, не равный CN серверного сертификата	`false`
`API_TOKEN_SECRET`	Ключ, необходимый для подписи токена доступа по REST API	`dJ2ZOZeU0nJhHwjfhqlOwF1x`
`CPE_PRODUCT_THRESHOLD`	Пороговое значение для сопоставления наименования ПО актива при поиске уязвимостей	`0.6`
`CPE_VENDOR_THRESHOLD`	Пороговое значение для сопоставления поставщика ПО актива при поиске уязвимостей	`0.6`
`CPE_VERSION_THRESHOLD`	Пороговое значение для сопоставления версии ПО актива при поиске уязвимостей	`0.95`

Табл. 13. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`REPOS_DIR`	Директория, в которой располагаются репозитории для модуля «Управление проектами ПЛК»	`/var/lib/udv/cv-repos-backend/repositories`
`EVENT_SYSLOG_SEND`	При значении переменной `true` выполняется отправка внутренних событий во внешние системы по протоколу Syslog	`false`
`EVENT_SYSLOG_HOST`	IP-адрес внешнего сервера, используемого для передачи событий по протоколу Syslog	`127.0.0.1`
`EVENT_SYSLOG_PORT`	Порт, используемый для отправки внутренних событий по протоколу Syslog	`514`
`EVENT_SYSLOG_PROTOCOL`	Протокол передачи внутренних событий по Syslog. Возможные варианты значения переменной: • TCP; • UDP.	`UDP`
`EVENT_SYSLOG_FACILITY`	Категория источника внутренних событий при их передаче во внешние системы по Syslog	`LOC0`
`EVENT_SYSLOG_SEVERITY`	Уровень критичности сообщений о передаче внутренних событий во внешние системы по Syslog. Доступны следующие значения переменной: • `INFORMATIONAL` • `CRITICAL` При значении переменной `INFORMATIONAL` будут отображаться информационные сообщения. При значении переменной `CRITICAL` будут отображаться информационные сообщения, а также сообщения о состоянии системы, сообщения об ошибках, предупреждения о возможных проблемах	`INFORMATIONAL`

Табл. 13. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`SV_EVENTS_QUEUE_MAX_LENGTH`	Максимальная длина очереди для отправки событий репозиториев на UDV Supervision. Минимальное значение — `100`	`200000`

Переменные сервиса udv-prometheus

Переменные сервиса `udv-prometheus` устанавливаются в директории `/etc/sysconfig/udv-prometheus`

Список переменных сервиса `udv-prometheus` Комплекса уровня Management, представлен в таблице ниже.

Табл. 14. Список переменных сервиса udv-prometheus

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`MAX_DISK_SPACE_CONSUMED_PERCENTAGE`	Лимит заполнения ПЗУ (HDD, SSD) операционной системы Комплекса. Значение задается в процентах	`80`
`MAX_CPU_LOAD_CONSUMED_PERCENTAGE`	Лимит нагрузки на центральный процессор (CPU) операционной системы Комплекса. Значение задается в процентах	`80`
`MAX_LA`	Лимит средней нагрузки (Load average) операционной системы Комплекса. Значение задается в количестве ядер	`8`
`MAX_RAM_CONSUMED_PERCENTAGE`	Максимальный допустимый объем используемой оперативной памяти. Значение задается в процентах	`90`
`RMQ_LOW_AVAILABLE_DISK_SPACE_WATERMARK_BYTES`	Минимальный уровень свободного дискового пространства для брокера сообщений `rabbitmq`, при достижении которого в веб-интерфейсе появляется соответствующее событие 1180013, а при его нормализации появляется событие 1180014. Значение задается в байтах	`500000000`

Табл. 14. Список переменных сервиса udv-prometheus

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`RMQ_LOW_AVAILABLE_MEMORY_WATERMARK_BYTES`	Минимальный уровень свободной оперативной памяти для брокера сообщений `rabbitmq`, при достижении которого в веб-интерфейсе появляется соответствующее событие 1180011, а при его нормализации появляется событие 1180012. Значение задается в байтах	`500000000`
`PUSHGATEWAY_MAX_DELAY_METRICS`	Максимальный интервал задержки между отправкой значений в систему мониторинга. Значение задается в секундах	`600`

Переменные сервиса udv-logstash

Переменные сервиса `udv-logstash` устанавливаются в директории `/etc/sysconfig/udv-logstash`

Список переменных сервиса `udv-logstash` Комплекса уровня Management, представлен в таблице ниже.

Табл. 15. Список переменных сервиса udv-logstash

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`LOG_LEVEL`	Минимальная критичность системных событий, которые генерирует Комплекс уровня Management. Возможные значения: • `CRITICAL` • `FATAL` • `ERROR` • `WARNING` • `INFO` • `DEBUG` • `NOTSET`	`INFO`

Табл. 15. Список переменных сервиса udv-logstash

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ESPER_PORT`	Порт сервиса корреляции событий	`517`
`LS_JAVA_OPTS`	Объем оперативной памяти, выделяемой под сервис `udv-logstash`. Значение задается в мегабайтах	`-Dlog4j2.formatMsgNoLookups=true-Xmx1024m-Xms1024m`
`INDEX_NAME`	Наименование индексов событий Комплекса	`"datapk-events-%{+YYYY.MM.dd}"`
`TEMPLATE_NAME`	Наименование шаблона событий Комплекса	`"datapk-event.json"`

Переменные сервиса udv-opensearch

Переменные сервиса `udv-opensearch` устанавливаются в директории `/etc/sysconfig/udv-opensearch`

Список переменных сервиса `udv-opensearch` Комплекса уровня Management представлен в таблице ниже.

Табл. 16. Список переменных сервиса udv-opensearch

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ES_JAVA_OPTS`	Объем оперативной памяти, выделяемой под сервис `opensearch`. Задается в мегабайтах	`-Dlog4j2.formatMsgNoLookups=true-Xmx1024m-Xms1024m`
`OPENSEARCH_PATH_CONF`	Директория, в которой расположен конфигурационный файл сервиса `opensearch`	`/etc/opensearch`

Табл. 16. Список переменных сервиса udv-opensearch

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`OPENSEARCH_STARTUP_SLEEP_TIME`	Время ожидания перед началом проверки успешного запуска сервиса `opensearch`	`5`
`OPENSEARCH_SD_NOTIFY`	При значении переменной `true` в систему будут отправляться уведомления `systemd`	`true`

Переменные сервиса udv-esper

Переменные сервиса `udv-esper` устанавливаются в директории `/etc/sysconfig/udv-esper`

Список переменных сервиса `udv-esper` Комплекса уровня Management, представлен в таблице ниже.

Табл. 17. Список переменных сервиса udv-esper

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ESPER_RMQ_MAX_QUEUE_SIZE`	Максимальный размер очереди сервиса `udv-rabbitmq` для отправки событий на корреляцию. Задается в количестве сообщений	`100000`
`ESPER_JAVA_OPTS`	Объем оперативной памяти, выделяемой под сервис корреляции событий. Задается в мегабайтах	`-Djava.net.prefer-IPv4Stack=true-Dlog4j2.format-MsgNoLookups=true-Xmx1024m`
`JETTY_PORT`	Порт сервера `Jetty`, по которому доступен API модуля «Управление внешними событиями»	`10007`
`ESPER_STARTUP_TIMEOUT`	Задержка при запуске модуля «Управление внешними событиями». Значение переменной задается в секундах	`180`
`HOST_MANAGER_API_PORT`	Порт API, по которому доступен модуль управления узлами	`10012`

Табл. 17. Список переменных сервиса udv-esper

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ESPER_ELASTICSEARCH_HOST`	IP-адрес узла, используемого модулем «Управление внешними событиями»	`127.0.0.1`
`ESPER_ELASTICSEARCH_PORT`	Порт, по которому доступен модуль «Управление внешними событиями»	`9200`
`ESPER_INCIDENT_ANALYSIS`	При значении переменной `disabled` функция повторной обработки инцидентов будет недоступна	`disabled`
`ESPER_ELASTICSEARCH_BATCH_COUNT`	Количество записей из модуля «Управление внешними событиями», читаемых за одну минуту	`2000`
`ESPER_RETRO_TIME_FIELD`	Название поля, по которому сортируются события при запросе	`create_time`
`ESPER_RETRO_SCROLL_TIMEOUT_MIN`	Задержка при выполнении запроса к модулю «Управление внешними событиями». Значение переменной задается в минутах	`3`
`ESPER_MAX_SERVICE_INFO_SIZE`	Максимальное количество сообщений о состоянии службы, хранимое в оперативной памяти	`50`
`ESPER_EVENT_COUNTER_INTERVAL`	Интервал между выводом счетчика внешних событий, полученных при текущем анализе. Значение переменной задается в миллисекундах	`300000`
`ESPER_INCIDENT_SENDER_CONNECT_TIMEOUT_MS`	Задержка установления соединения с модулем управления инцидентами. Значение переменной задается в миллисекундах	`1000`
`ESPER_INCIDENT_SENDER_READ_TIMEOUT_MS`	Задержка времени ответа о создании инцидента от модуля управления инцидентами. Значение переменной задается в миллисекундах	`5000`
`ESPER_INCIDENT_SENDER_THREADPOOL_SIZE`	Объем потоков, используемого для связи с модулем управления инцидентов	`40`

Табл. 17. Список переменных сервиса udv-esper

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`INCIDENT_MANAGER_API_PORT`	Порт API, по которому доступен модуль управления инцидентами	`10011`
`API_CONNECTION_RETRY_COUNT`	Количество повторных попыток подключения к API Комплекса	`3`

Переменные сервиса udv-vector-manager

Переменные сервиса `udv-vector-manager` устанавливаются в директории `/lib/systemd/system/udv-vector.service`

Список переменных сервиса `udv-vector-manager` Комплекса уровня Management представлен в таблице ниже.

Табл. 18. Список переменных сервиса udv-vector-manager

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`BUFFER_SIZE`	Размер буфера одного обработчика в сервисе `udv-vector-manager` (один обработчик — один протокол). Задается в байтах	`268435488`
`MANAGER_NETWORK_GATEWAY`	Адрес для отправки данных в сервис `udv-clickhouse`	`127.0.0.1`

Переменные сервиса udv-zeek-backend

Если Комплекс еще не запускался, переменные сервиса `udv-zeek-backend` устанавливаются в файле `manager.env` в директории `/usr/share/udv/datapk/manager.env`.

Если Комплекс уже запускался, переменные сервиса `udv-zeek-backend` устанавливаются с помощью запроса в базу данных `Redis` (см. инструкцию «Установка переменных модуля «Анализ промышленного сетевого трафика» через запрос в Redis»).

Список переменных сервиса `udv-zeek-backend` Комплекса уровня Management представлен в таблице ниже.

Табл. 19. Список переменных сервиса udv-zeek-backend

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`DPI_PASSWORD_CAPTURE`	При значении переменной `true` обрабатываются пароли в трафике HTTP	`false`

Переменные сервиса udv-rules-backend

Если Комплекс еще не запускался, переменные сервиса `udv-rules-backend` устанавливаются в файле `manager.env` в директории `/usr/share/udv/datapk/manager.env`.

Если Комплекс уже запускался, переменные сервиса `udv-rules-backend` устанавливаются через запрос в базу данных `Redis` (см. инструкцию «Установка переменных модуля «Анализ промышленного сетевого трафика» через запрос в Redis»).

Список переменных сервиса `udv-rules-backend` Комплекса уровня Management представлен в таблице ниже.

Табл. 20. Список переменных сервиса udv-rules-backend

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`SESSION_RULES_ENABLED`	При значении переменной `true` будет включен сервис правил сессий	`true`

См. также

Переменные службы обнаружения вторжений

Конфигурационные файлы модуля «EDR for PLC»

Рекомендации по использованию переменных файлов manager.env и sensor.env

7.7.1.1. Установка переменных модуля «Анализ промышленного сетевого трафика» через запрос в Redis

Инструкция применима для установки переменных сервисов udv-zeek-backend и udv-rules-backend на Комплексе, который уже запускался.

Для установки переменных через запрос в базу данных `Redis` в терминале сервера, на котором установлен Комплекс уровня Management:

1. Подключитесь к базе данных `Redis` командой:

```
redis-cli
```

2. Выполните запрос текущих настроек сервиса:

    а. Для сервиса `udv-zeek-backend` введите команду:

    ```
    get /v1/nodes/[node_id]/v1/zeek/service/settings/items/
    ```

    б. Для сервиса `udv-rules-backend` введите команду:

    ```
    get /v1/nodes/[node_id]/v1/rules/settings/items/
    ```

Где `[node_id]` — идентификатор сенсора, на котором требуется установить переменные. Например, `fc30d73435387abbfbb61c10676106ae`.

> Подсказка:
>
> Узнать `node_id` можно командой:
>
> ```
> curl -X GET http://127.0.0.1:32456/sensors_nodes
> ```

3. Скопируйте в любой текстовый редактор вывод команды, полученный в шаге 2, и измените в нем значения переменных (подробнее о переменных см. пункты «Переменные сервиса udv-zeek-backend» и «Переменные сервиса udv-rules-backend» раздела «Переменные Комплекса уровня Management»).
4. Выполните команду, подставив в нее значение `node_id` и строку из шага 3 с новыми настройками:

    ```
    set /v1/nodes/[node_id]/v1/zeek/service/settings/items/ [новые_настройки]
    ```

7.7.2. Переменные Комплекса уровня Sensor

Обязательные переменные файла sensor.env

Переменные файла `sensor.env` устанавливаются в директории `/usr/share/udv/datapk`

Список обязательных переменных, содержащийся в файле `sensor.env` Комплекса уровня Sensor, представлен в таблице ниже.

Табл. 21. Обязательные переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`MANAGER_NODE_ADDRESS`	IP-адрес для подключения сенсора к Комплексу уровня Management. Значение `127.0.0.1` задается в случае, если сенсор и Management установлены на одном сервере.	`127.0.0.1`
`LISTENING_INTERFACES`	Наименования всех интерфейсов, с которых сенсор анализирует трафик. Можно указывать интерфейсы в любом режиме (не только прослушивания трафика). Интерфейсы перечисляются через запятую без пробелов. Все интерфейсы должны быть в состоянии up, иначе сенсор не сможет корректно инициализироваться. ⚠ Внимание: Запись трафика в файлы `.pcap` модулем «Управление сетевым трафиком» будет доступна только для первого интерфейса из перечисленных в переменной. Если необходимо записывать трафик с нескольких интерфейсов, создайте для них единый виртуальный интерфейс (bond) — подробнее см. в разделе «Создание единого виртуального интерфейса (bond) для прослушивания и записи трафика с нескольких физических интерфейсов» Руководства по внедрению и поддержке.	`ens32,ens33,ens35,dummy0`
`LOG_LEVEL`	Минимальная критичность системных событий, которые генерирует Комплекс уровня Management. Возможные значения: • `CRITICAL` • `FATAL` • `ERROR` • `WARNING` • `INFO`	`INFO`

Табл. 21. Обязательные переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
	• `DEBUG` • `NOTSET`	

Дополнительные переменные файла sensor.env

Переменные, которые не включены в автоматически генерируемый файл `sensor.env` Комплекса уровня Sensor и добавляются при необходимости, указаны в таблице ниже.

Табл. 22. Дополнительные переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`TERMINAL_CONNECTOR_SSH_TIMEOUT`	Максимальное время ожидания выполнения задачи сбора данных по протоколу SSH. Задается в секундах	`30`
`COMMAND_PROCESSOR_WORKER_MAX_MEMORY_LIMIT_MB`	Лимит памяти для обработки одного процесса сбора данных. При превышении лимита в результаты сбора выводится ошибка `Сбор данных был прерван в результате обнаружения большего объема данных, чем ожидалось.` Задается в мегабайтах	`256`
`MIBS_TO_COMPILE`	Список MIB-словарей для интерпретации данных, получаемых с сетевых устройств помощью сканеров сбора данных по протоколу SNMP	`<mib1>`, `<mib2>`
`COMMAND_PROCESSOR_USER_SCRIPT_MODULES`	Список Python-модулей, доступных для сканеров сбора данных	`re, string, unicodedata, hashlib,datetime, _strptime, textwrap, struct,dbfread, dateutil, dateutil.tz, parsel, random`

Переменные модуля «EDR for PLC»

Переменные модуля UDV DATAPK EDR for PLC устанавливаются в директории `/opt/sensor/.env`

Список переменных сервиса модуля UDV DATAPK EDR for PLC Комплекса уровня Sensor представлен в таблице ниже.

Табл. 23. Список переменных модуля «EDR for PLC»

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`LOG_LEVEL`	Минимальная критичность системных событий, которые генерирует модуль	`INFO`
`CONTROLLER_API_PORT`	Порт для доступа к API модуля	`8081`
`SOCKET_HOST`	Адреса, с которых доступно API управления модулем	`0.0.0.0`
`DB_PATH`	Путь до базы данных внутри контейнера модуля «EDR for PLC»	`/db/store.db`
`TZ`	Часовой пояс	`Asia/Yekaterinburg`

Переменные сервиса udv-zeek-wrapper

Переменные сервиса `udv-zeek-wrapper` устанавливаются в директории `/lib/systemd/system/udv-zeek-wrapper.service`

Список переменных сервиса `udv-zeek-wrapper` Комплекса уровня Sensor представлен в таблице ниже.

Табл. 24. Список переменных сервиса udv-zeek-wrapper

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ZEEK_ROTATION_INTERVAL`	Период ротации системных журналов сервиса `udv-zeek-wrapper`. Задается в минутах	1
`ARCHIVE_COMPRESS_LOG`	Перевод создаваемых копий журналов событий сервиса `udv-zeek-wrapper` в сжатый формат хранения при значении `true`.	`true`

Табл. 24. Список переменных сервиса udv-zeek-wrapper

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
	ОСТОРОЖНО: Изменение значения переменной может привести к отказу в работе a.	
`ARCHIVE_COPY_LOG`	Создание копии журналов событий сервиса `udv-zeek` при значении `true`. ОСТОРОЖНО: Изменение значения переменной может привести к отказу в работе a.	`false`

Переменные сервиса udv-dns-classifier

Переменные сервиса `udv-dns-classifier` устанавливаются в директории `/etc/sysconfig/udv-dns-classifier`

Список переменных сервиса `udv-dns-classifier` Комплекса уровня Sensor представлен в таблице ниже.

Табл. 25. Список переменных сервиса udv-dns-classifier

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`REQUEST_LOG_THRESHOLD`	Граница вероятности, с которой события считаются туннелями для dns_request-модели	`0.8`
`RESPONSE_LOG_THRESHOLD`	Граница вероятности, с которой события считаются туннелями для dns_-response-модели	`0.8`
`REQUEST_ANOMALY_THRESHOLD`	Граница вероятности, с которой события dns_request отправляются в сервис `udv-event-manager`	`0.5`

Табл. 25. Список переменных сервиса udv-dns-classifier

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`RESPONSE_ANOMALY_THRESHOLD`	Граница вероятности, с которой события dns_response отправляются в сервис `udv-event-manager`	`0.75`
`DGA_ANOMALY_THRESHOLD`	Граница вероятности, с которой DGA-события отправляются в сервис `udv-event-manager`	**0.75**
`DGA_LOG_THRESHOLD`	Граница вероятности, с которой события считаются DGA	`0.75`
`DEBUG_MODE`	Перевод сервиса `udv-dns-classifier` в debug-режим при значении `true`. При этом модели сервиса сохраняют на диск датафреймы с результатами работы. ОСТОРОЖНО: Изменение значения переменной может привести к отказу в работе а.	`false`

См. также

Переменные службы обнаружения вторжений

Конфигурационные файлы модуля «EDR for PLC»

Рекомендации по использованию переменных файлов manager.env и sensor.env

7.7.3. Переменные службы обнаружения вторжений

Для службы обнаружения вторжений Комплекса уровня Sensor устанавливается конфигурационный файл с набором переменных, расположенный в директории `/etc/sysconfig/suricata-wrapper`.

Значения переменных указываются следующим образом:

- одиночный IP-адрес или порт указываются в следующем формате: `20` или `192.168.0.0`;
- несколько IP-адресов указываются в следующем формате: `[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]`;
- несколько портов указываются в следующем формате: `[20,21]`.

Список переменных, содержащихся в данного конфигурационном файле, представлен в таблице ниже.

Табл. 26. Переменные службы обнаружения вторжений

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ADDRESS_VARIABLEA`	Переменные для добавления пользовательского IP-адреса или диапазона IP-адресов	`$HOME_NET`
`ADDRESS_VARIABLEB`		
`ADDRESS_VARIABLEC`		
`ADDRESS_VARIABLED`		
`AIM_SERVERS`	Домашняя (контролируемая) сеть серверов AIM (AOL Instant Messenger)	`$EXTERNAL_NET`
`DC_SERVERS`	Домашняя (контролируемая) сеть серверов DC (Domain Controllers)	`$HOME_NET`
`DNP3_CLIENT`	Домашняя (контролируемая) сеть клиентов DNP3-протокола	`$HOME_NET`
`DNP3_PORT`	Порты DNP3-протокола	`20000`
`DNP3_SERVER`	Домашняя (контролируемая) сеть серверов DNP3	`$HOME_NET`
`DNS_SERVERS`	Домашняя (контролируемая) сеть серверов DNS	`$HOME_NET`
`ENIP_CLIENT`	Домашняя (контролируемая) сеть клиентов ENIP-протокола	`$HOME_NET`
`ENIP_SERVER`	Домашняя (контролируемая) сеть серверов ENIP	`$HOME_NET`

Табл. 26. Переменные службы обнаружения вторжений

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
EXTERNAL_NET	IP-адреса, не входящих в домашнюю (контролируемую) сеть	!$HOME_NET
FILE_DATA_PORTS	Порты, через которые выполняется передача файлов	[$HTTP_PORTS,110,143]
FTP_PORTS	Порты, используемые для соединения по протоколу FTP	21
HOME_NET	IP-адреса домашней (контролируемой) сети	[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]
HTTP_PORTS	Порты, используемые для HTTP-трафика	80
HTTP_SERVERS	Домашняя (контролируемая) сеть HTTP-серверов	$HOME_NET
MODBUS_CLIENT	Домашняя (контролируемая) сеть клиентов протокола Modbus	$HOME_NET
MODBUS_PORTS	Порты протокола Modbus	502
MODBUS_SERVER	Домашняя (контролируемая) сеть серверов Modbus	$HOME_NET
ORACLE_PORTS	Порты для подключения к серверам Oracle	1521
PORT_VARIABLEA	Переменные для добавления пользовательского порта, предназначенного для определенных протоколов	!80
PORT_VARIABLEB		
PORT_VARIABLEC		
PORT_VARIABLED		

Табл. 26. Переменные службы обнаружения вторжений

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`SHELLCODE_PORTS`	Порты, на которых выполняется мониторинг попыток выполнения shell-кодов	`!80`
`SMTP_SERVERS`	Домашняя (контролируемая) сеть SMTP-серверов	`$HOME_NET`
`SQL_SERVERS`	Домашняя (контролируемая) сеть серверов баз данных SQL	`$HOME_NET`
`SSH_PORTS`	Домашняя (контролируемая) сеть SSH-серверов	`22`
`TELNET_SERVERS`	Домашняя (контролируемая) сеть Telnet-серверов	`$HOME_NET`

7.7.4. Конфигурационные файлы модуля «EDR for PLC»

Для настройки модуля UDV DATAPK EDR for PLC используются файлы, описанные в таблице ниже. Конфигурационные файлы UDV DATAPK EDR for PLC хранятся и настраиваются в Комплексе уровня Sensor.

Табл. 27. Конфигурационные файлы модуля «EDR for PLC»

ФАЙЛ	ДИРЕКТОРИЯ, В КОТОРОЙ РАСПОЛОЖЕН ФАЙЛ	НАЗНАЧЕНИЕ ФАЙЛА
`protocol-fields.yaml`	`/opt/sensor/protocol-fields.yaml`	Используется для классификации полей сетевых протоколов
`.env`	`/opt/sensor/.env`	Используется для настройки переменных окружения модуля UDV DATAPK EDR for PLC
`configuration.yaml`	`/opt/sensor/configuration.yaml`	Основной файл конфигурации, которые определяет набор и параметры моделей

7.7.4.1. Файл protocol-fields.yaml

Файл `protocol-fields.yaml` предназначен для классификации полей сетевых протоколов с целью их последующей обработки в аналитической системе.

Описание классов полей представлено в таблице ниже.

Табл. 28. Описание классов полей в файле protocol-fields.yaml

КЛАСС	ОПИСАНИЕ	ХАРАКТЕРИСТИКИ
`address`	Используется для определения полей, содержащих адресную информацию для маршрутизации данных	• Эти поля содержат идентификаторы узлов или сервисов (например: IP-адрес, TCP-порт); • Используются только для маршрутизации данных до целевой модели; • Не передаются в модель для анализа.
`payload`	Используется для определения полей, содержащих полезную нагрузку для анализа моделями	• Эти поля передаются на анализ в модели; • Обычно содержат данные о состоянии или управлении технологическим процессом; • Для моделей на основе гибридного автомата набор анализируемых полей задается в `configuration.yaml`.
`other`	Используется для определения полей, исключаемых из анализа	• Такие поля игнорируются при анализе; • Обычно содержат случайно генерируемые или нерелевантные данные; • Включение таких полей в анализ снижает точность моделей.

7.7.4.2. Файл .env

В данном файле настраиваются следующие переменные:

- `LOG_LEVEL`;
- `CONTROLLER_API_PORT`;
- `SOCKET_HOST`;

- `DB_PATH`;
- `TZ`.

Подробное описание переменных приведено в разделе «Переменные модуля «EDR for PLC»».

7.7.4.3. Файл configuration.yaml

Файл `configuration.yaml` состоит из следующих блоков:

1. Блок входных данных модуля — определяет параметры приема проанализированного трафика от механизма DPI.
2. Блок выходных данных модуля — определяет способ отправки событий модуля в вышестоящие системы. Существует два способа отправки событий:
    - с помощью сервиса `udv-rabbitmq` — основной способ отправки событий, настраиваемый при установке Комплекса;
    - по протоколу Syslog — альтернативный способ отправки событий с поддержкой стандарта RFC 5424/UDP.

> **Внимание:**
>
> При отправке в сторонние системы необходимо проверить настройки межсетевого экранирования.

3. Блок контроллера моделей — определяет перечень моделей анализа и их параметры. Для конфигурации модели необходимо указать следующие данные:
    - способ представления модели;
    - адресная информация конечных точек для анализа;
    - специфичные параметры модели.

> **Прим.:**
>
> Для каждого типа модели и набора конечных точек определяются специфичные параметры. Если определенный тип модели не указан для набора конечных точек, соответствующий блок параметров не включается в конфигурацию.

При определении конечных точек доступны два режима сопоставления адресов:

- `starts_with` — адресная информация сетевого взаимодействия должна начинаться с адресов, указанных в поле `layers`;
- `equal` — адресная информация сетевого взаимодействия должна точно соответствовать адресам конечных точек из поля `layers`. Данный режим обеспечивает более строгую фильтрацию по сравнению с режимом `starts_with`.

Пример

Пример режима сопоставления `starts_with`:

Для узла с настройкой IP `192.168.1.1` будут обрабатываться все соединения с данного IP-адреса, для узла `192.168.1.2:102` — соединения с указанного IP и TCP-порта `102`.

Результирующий анализ: `192.168.1.1:* ↔ 192.168.1.2:102`

Подробное содержание файла `configuration.yaml`, формируемое по умолчанию, представлено ниже.

```
# Блок входных данных модуля

# Получение проанализированного трафика от механизма DPI
socket_config:
  enabled: true

# Блок входных данных модуля

# Конфигурация отправки событий по syslog (rfc5424/udp)
syslog:
  - enabled: false # активность отправки по syslog
    ip_or_domain: logstash # ip-адрес или DNS имя хоста для отправки событий
    port: 5514 # порт для отправки событий
    models_metrics:
      enabled: true # активность отправки событий о текущих метриках моделей
      send_interval: 30 # интервал отправки событий о текущих метриках моделей

# Конфигурация отправки событий в RabbitMQ
rabbitmq_config:
    enabled: true  # активность отправки в RabbitMQ
    host: '127.0.0.2' # ip-адрес или DNS имя хоста для отправки событий
    port: 5672 # порт для отправки событий
    models_metrics:
      enabled: true # активность отправки событий о текущих метриках моделей
      send_interval: 30 # интервал отправки событий о текущих метриках моделей
```

```
# Конфигурация контроллера моделей
models_controller_config:
  nodes_configurations: # далее идет задание моделей
    - models: [otala, qdict, hybrid_automaton] # указывается тип моделей для следующих далее конечных точек взаимодействия, доступны три варианта: otala
 и/или qdict и/или hybrid_automaton
      first_node: # описание первой конечной точки
        mode: 'starts_with' # режим сопоставления адресной информации
        layers: # уровни представления адресной информации (их может быть несколько, важно соблюдать порядок согласно модели OSI)
          - value: '192.168.1.1' # значение, которое учитывается в адресной информации
            protocol: 'ip' # сетевой протокол, для которого учитывается указанное выше значение
            format: 'ip' # формат, в котором задается значение в поле value
      second_node: # описание второй конечной точки
        mode: 'starts_with' # режим сопоставления адресной информации
        layers: # уровни представления адресной информации (их может быть несколько)
          - value: '192.168.1.2' # значение, которое учитывается в адресной информации
            protocol: 'ip' # сетевой протокол, для которого учитывается указанное выше значение
            format: 'ip' # формат, в котором задается значение в поле value
            - value: '1f6' # значение, которое учитывается в адресной информации (для hex формата указывается без лидирующих нулей, например, в данном
 случае это 502 порт)
            protocol: 'tcp' # сетевой протокол, для которого учитывается указанное выше значение
            format: 'hex' # формат, в котором задается значение в поле value
      qdict_configuration: # конфигурация модели на основе иерархического словаря (для взаимодействия, описанного выше)
        separation: # управление режимом формирования маски данных
          enabled: false # активность режима формирования маски данных (поддерживается только для протокола CIP)
        max_stagnation_number: 10 # условие сходимости модели
        max_buffer_len: 10000 # предельный размер буфера данных при формировании иерархического словаря (фактически определяет "глубину" иерархии)
        max_qdict_len: 100000 # предельное количество записей в иерархическом словаре
        validation: # блок настроек режима валидации для модели
          min_checks_count_before_validation: 1000 # минимальный размер данных (запрос-ответ) необходимых для выполнения валидации модели
        min_probability_of_correct_prediction: 50.0 # минимальная предсказательная способность модели (в %), необходимая для успешного прохождения валидации
      otala_configuration: # конфигурация модели на основе временного автомата (для взаимодействия, описанного выше)
        separation: # управление режимом формирования маски данных (поддерживается только для протокола CIP)
          enabled: true # активность режима формирования маски данных
```

```
        max_group_commands_count: 100 # количество команд одной группы CIP, которое необходимо накопить для начала расчета энтропии
        entropy_threshold: 0.5 # пороговое значение энтропии, определяющее попадание в маску данных
      convergence_number_max: null # условие сходимости модели
    hybrid_automaton_configuration: # конфигурация модели на основе гибридного автомата (для взаимодействия, описанного выше)
      controlled_data: # определение областей памяти протокола Modbus, которые будут переданы в модель
        discrete_inputs: [0,1,2] # перечень анализируемых дискретных входов
        coils: [8,9,10,17,21] # перечень анализируемых регистров флагов
        input_registers: [] # перечень анализируемых входных регистров
        holding_registers: [45,32] # перечень анализируемых регистров хранения
      controlled_func: [1,2,3,4] # перечень номеров анализируемых функций протокола Modbus
      modbus_detectors: # описание активности и параметров modbus детекторов в рамках модели на основе гибридного автомата
        detector_new_tags: # детектор для контроля используемых областей памяти в рамках обмена по протоколу modbus
          enabled: true # состояние активности данного детектора
        detector_exception: # детектор для сигнализации о возникновении исключений на уровне протокола modbus
          enabled: true # состояние активности данного детектора
        detector_event_type: # детектор для выявления modbus-запросов без ответов и/или modbus-ответов без запросов
          enabled: true # состояние активности данного детектора
        detector_empty_request_address: # детектор для выявления неправильно сформированных запросов
          enabled: true # состояние активности данного детектора
        detector_stacked_coils_request: # детектор для выявления неверного формата данных (например, передача строки в бинарном регистре)
          enabled: true # состояние активности данного детектора
        detector_unknown_func: # детектор для выявления отсутствующих в режиме обучения функций протокола modbus
          enabled: true # состояние активности данного детектора
        detector_long_delay_in_requests: # детектор для выявления задержек между запросами, превосходящих предельные значения режима обучения
          enabled: true # состояние активности данного детектора
          skip_max_ejection: 2 # количество отсортированных выбросов в режиме обучения, которые игнорируются при формировании предельных значений
        detector_large_number_of_requests_over_time: # детектор для выявления слишком частых запросов (относительно режима обучения)
          enabled: true # состояние активности данного детектора
          skip_max_ejection: 2 # количество отсортированных выбросов в режиме обучения, которые игнорируются при формировании предельных значений
      train_connections_num: 100000 # количество сформированных входных векторов, необходимых для прохождения обучения
          part_of_data_training_the_model: 0.7 # определяет какая часть от сформированных входных векторов, необходимых для прохождения обучения
(train_connections_num) будет использована для формирования автомата, оставшиеся данные используются для формирования граничных значений
      min_checks_count_before_validation: 50000 # количество сформированных входных векторов для прохождения этапа валидации автомата
```

```
    min_probability_of_correct_prediction: 80 # минимальное значение метрики "предсказательная способность" (в %) для успешного прохождения этапа валидации
      sync_connections_num: 5000 # количество сформированных входных векторов, необходимых для синхронизации гибридного автомата
      validation: true # активность этапа валидации после этапа обучения
    states_ode_model_type: 'RidgeCV' # тип модели, используемой для предсказания следующего значения регистра (допустимы LinearRegression, Ridge, RidgeCV)
      max_ape_coef: 2.0 # допустимая величина ошибки предсказания по сравнению с аналогичной на валидационных данных
      turn_on_forbidden_transitions: true # активность формирования события при детектировании несуществующего перехода в рамках гибридного автомата
       filter_anomalies_after_transitions: false # игнорирование ошибок предсказания значений регистров в области перехода между состояниями гибридного
автомата
     area_after_transition_to_filter_anomalies: 0 # количество входных векторов, для которых выполняется игнорирование ошибок предсказания после перехода
между состояниями гибридного автомата (только при filter_anomalies_after_transitions: true)
        unknown_function_ignore_notification: false # отображение информации о детектировании функций Modbus, которые не входят в анализируемые (не
указаны в controlled_func)
     input_vector_creation_time_limit_sec: 180 # лимит времени (в секундах), отведенный на формирование входного вектора. При его превышении формируется
предупреждение в логах
      input_vector_waiting_sleep_delay_sec: 5 # пауза (в секундах) при формировании входного вектора
      log_input_vector_description_delay_commands: 4 # пауза (в секундах) для логирования входного вектора в логах
      separation: # управление режимом формирования маски данных
        enabled: false # активность режима формирования маски данных (для гибридного автомата всегда False)
      segmentation_threshold: 0 # порог принятия решения о границе сегмента для переменной
      ignore_segments_shorter_then: 0 # указание минимальной длины сегмента, допустимой для анализа в рамках гибридного автомата
       number_of_folds: 5 # количество фолдов для кросс-валидации при подборе коэффициентов уравнений состояния гибридного автомата (применимо только
для states_ode_model_type: 'RidgeCV')
```

См. также

Модель на основе гибридного автомата

Модель на основе временного автомата

Модель на основе иерархического словаря

7.7.5. Рекомендации по использованию переменных файлов manager.env и sensor.env

Не все доступные для использования переменные, которые могут быть в файле `manager.env` или `sensor.env`, сразу находятся в нем. Некоторые из них необходимо вводить самостоятельно или раскомментировать.

При использовании переменных объема и времени рекомендуется использовать форматы, предложенные производителем Комплекса. Значительные отклонения от значений по умолчанию могут повлечь некорректную работу, недоступность системы или ее частей.

Список рекомендаций приведен в таблице ниже.

Табл. 29. Рекомендации по использованию переменных файлов manager.env и sensor.env

ПЕРЕМЕННАЯ	РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ	ПРИМЕНИМО ДЛЯ УРОВНЯ КОМПЛЕКСА
`EVENT_INDICES_MAX_SIZE_GB`	Если присутствует дисковый раздел под оперативный архив, установите значение переменной не более 90% от общего объема раздела (например, 90 ГБ для 100 ГБ). Если отдельного раздела нет, то установите значение не более 300 ГБ	Management
`EVENT_ARCHIVES_MAX_SIZE_GB`	Рекомендуется установить значение переменной около 30% от общего объема раздела	Management
`EVENT_INDICES_LIFETIME_DAYS`	Установите значение около 30 дней	Management
`EVENT_ARCHIVES_LIFETIME_DAYS`	Установите адекватную системе длительность хранения глубокого архива. Она должна быть больше длительности хранения оперативного архива — например, укажите на несколько дней больше, чем указано в `EVENT_INDICES_LIFETIME_DAYS`	Management
`EVENTS_RETENTION_DISK_CAPACITY_SIZE_MB`	Установите значение не более 20-30 ГБ	Management
`EVENTS_RETENTION_MONTHS`	Установите значение от 1 до 3 месяцев	Management

См. также

Переменные Комплекса уровня Management

7.8. Отображение времени в Комплексе

Дата и время в Комплексе хранится во временной зоне UTC, а при отображении в интерфейсе адаптируется под часовой пояс клиента. Это позволяет пользователям просматривать события и другую информацию в своем часовом поясе.

На страницах раздела **Мониторинг** и **События** время отображается в соответствии со временем на АРМ пользователя. В случае расхождения времени между АРМ клиента и операционной системой Комплекса могут обнаруживаться несоответствия при которых события отображаются «в будущем» или «в прошлом». Такое расхождение не следует принимать за сбой работы системы регистрации событий.

Подобное поведение также наблюдается при получении событий от актива, на котором некорректно настроено время. При сортировке по полю `create_time` такое событие может отображаться «в прошлом» или «в будущем» относительно событий, полученных в то же время.

См. также

Время на Комплексе отличается от времени получения события

7.9. Перечень данных, собираемых Комплексом с помощью сканеров

В таблице ниже приведен максимально возможный список данных, которые возможно собирать с помощью сканеров сбора данных Комплекса.

Список сканеров сбора данных, входящих в минимальный сертифицированный комплект дистрибутива Комплекса, см. в разделе «Реестр сканеров Комплекса» Руководства по эксплуатации.

Табл. 30. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Windows	События Security	RPC (WMI/MSEVEN)
Windows	События System	RPC (WMI/MSEVEN)
Windows	События Application	RPC (WMI/MSEVEN)
Windows	События Kaspersky Event Log	RPC (WMI/MSEVEN)
Windows	Список процессов	RPC (WMI/MSEVEN)
Windows	Список установленных обновлений	RPC (WMI/MSEVEN)
Windows	Список пользователей (локальные)	RPC (WMI/MSEVEN)
Windows	Список пользователей (все)	RPC (WMI/MSEVEN)
Windows	Список устройств	RPC (WMI/MSEVEN)
Windows	Список групп пользователей	RPC (WMI/MSEVEN)
Windows	Автозагрузка	RPC (WMI/MSEVEN)
Windows	Список служб (автозапуск)	RPC (WMI/MSEVEN)

Табл. 30. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Windows	Список служб	RPC (WMI/MSEVEN)
Windows	Список установленных обновлений	WinRM
Windows	Содержимое файла Hosts	WinRM
Windows	Содержимое файла Hosts	WinRM over HTTPS
Windows	Содержимое файла Hosts	WinEXE
Windows	Общие папки	WinRM
Windows	Сетевые порты в режиме «LISTENING»	WinRM
Windows	Сетевые порты в режиме «LISTENING»	WinRM over HTTPS
Windows	Сетевые порты в режиме «LISTENING»	WinEXE
Windows	Список процессов с указанием пользователя	WinRM
Windows	Список процессов с указанием пользователя	WinRM over HTTPS
Windows	Список процессов с указанием пользователя	WinEXE
Windows	Параметры сетевых интерфейсов	WinRM
Windows	Параметры сетевых интерфейсов	WinRM over HTTPS
Windows	Параметры сетевых интерфейсов	WinEXE

Табл. 30. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Windows	ARP-таблица	WinRM
Windows	ARP-таблица	WinRM over HTTPS
Windows	ARP-таблица	WinEXE
Windows	Таблица маршрутизации	WinRM
Windows	Таблица маршрутизации	WinRM over HTTPS
Windows	Таблица маршрутизации	WinEXE
Windows	Установленное ПО (по ключам реестра)	WinRM
Windows	Версия Windows (ver)	WinRM
Windows	Версия Windows (ver)	WinRM over HTTPS
Windows	Версия Windows (ver)	WinEXE
Windows	Версия Windows (winver)	WinRM
Windows	Версия Windows (winver)	WinRM over HTTPS
Windows	Версия Windows (winver)	WinEXE
Windows	Имя актива	WinRM
Windows	Имя актива	WinRM over HTTPS

Табл. 30. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Windows	Имя актива	WinEXE
Windows	Политика безопасности	WinRM
Windows	Настройки парольной политики	WinRM
Windows	Правила МЭ	WinRM
Windows	Правила МЭ	WinRM over HTTPS
Windows	Правила МЭ	WinEXE
Windows	Состояние МЭ	WinRM
Windows	Состояние МЭ	WinRM over HTTPS
Windows	Состояние МЭ	WinEXE
Windows	Настройки аудита	WinRM
UNIX	ARP-таблица	SSH
UNIX	Таблица маршрутизации	SSH
UNIX	Имя сетевого узла	SSH
UNIX	Подключенные носители информации	SSH
UNIX	Список пользователей	SSH

Табл. 30. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
UNIX	Список групп пользователей и их членов	SSH
UNIX	Список процессов	SSH
UNIX	Список установленного ПО	SSH
UNIX	Содержимое файла /etc/sudoers	SSH
UNIX	Используемые DNS-серверы	SSH
UNIX	Содержимое файла /etc/hosts	SSH
UNIX	Сетевые порты в режиме LISTENINIG	SSH
UNIX	Правила межсетевого экрана iptables	SSH
UNIX	Объекты автозапуска	SSH
UNIX	Контроль целостности критичных файлов (/etc/network/interfaces и др.)	SSH
Debian	Список включенных служб	SSH
Debian	Список сервисов	SSH
Debian	Установленное ПО	SSH
Debian	Список устройств	SSH
Debian	Контрольные суммы файлов конфигурации	SSH

Табл. 30. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
QNX	Параметры DNS	SSH
QNX	Список групп	SSH
QNX	Сетевые порты в режиме прослушивания	SSH
QNX	Список пользователей	SSH
QNX	Файл hosts	SSH
RHEL	ARP-таблица	SSH
RHEL	Список служб	SSH
RHEL	Планировщик задач	SSH
RHEL	Параметры DNS	SSH
RHEL	Файл hosts	SSH
RHEL	Правила iptables	SSH
RHEL	Список sudoers	SSH
RHEL	Список групп	SSH
RHEL	Имя актива	SSH
RHEL	Подключенные носители информации	SSH

Табл. 30. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
RHEL	Список пользователей	SSH
RHEL	Сетевые порты в режиме прослушивания	SSH
RHEL	Список процессов	SSH
RHEL	Таблица маршрутизации	SSH
RHEL	Установленное ПО	SSH
RHEL	Список устройств	SSH
ACO Cisco IOS	Текущая конфигурация	SSH
ACO Cisco IOS	Начальная конфигурация	SSH
ACO Cisco IOS	ARP-таблица	SSH
ACO Cisco IOS	Таблица MAC-адресов	SSH
ACO Cisco IOS	Версия ОС	SSH
ACO HP	Текущая конфигурация	SSH
ACO HP	Начальная конфигурация	SSH
ACO HP	Версия ОС	SSH
ACO Cisco ASA	ARP-таблица	SSH

Табл. 30. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
ACO Cisco ASA	Таблица маршрутизации	SSH
ACO Cisco ASA	Текущая конфигурация	SSH
ACO Cisco ASA	Стартовая конфигурация	SSH
ACO Cisco ASA	Версия ОС	SSH
ACO Hirschmann	ARP-таблица	SSH
ACO Hirschmann	Таблица MAC-адресов	SSH
ACO Hirschmann	Текущая конфигурация	SSH
ACO Hirschmann	Версия ОС	SSH
ACO Comware	ARP-таблица	SSH
ACO Comware	Текущая конфигурация	SSH
ACO Comware	Таблица маршрутизации	SSH
ACO Comware	Таблица MAC-адресов	SSH
ACO Comware	Стартовая конфигурация	SSH
ACO Comware	Версия ОС	SSH
ACO Huawei	ARP-таблица	SSH

Табл. 30. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
АСО Huawei	Таблица маршрутизации	SSH
АСО Huawei	Таблица MAC-адресов	SSH
АСО Huawei	Текущая конфигурация	SSH
АСО Huawei	Серийный номер	SSH
АСО Huawei	Стартовая конфигурация	SSH
АСО Huawei	Версия ОС	SSH
АСО Huawei	Параметры интерфейсов	SNMP
АСО/шлюзы/конвертеры MOXA	Таблица MAC-адресов	SSH
АСО/шлюзы/конвертеры MOXA	Текущая конфигурация	SSH
АСО/шлюзы/конвертеры MOXA	Стартовая конфигурация	SSH
АСО/шлюзы/конвертеры MOXA	Версия ОС	SSH
АСО/шлюзы/конвертеры MOXA	Параметры интерфейсов	SSH
MSSQL	Список логинов	MSSQL
MSSQL	Список пользователей	MSSQL
MSSQL	Права пользователей	MSSQL

Табл. 30. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
MySQL	Список пользователей	MySQL
MySQL	Права пользователей	MySQL
ПЛК ALLEN BRADLEY Control Logix	Сбор конфигураций ПЛК. • Сведения о ПЛК: вендор, тип ПЛК, код продукта, версия, серийный номер, наименование или модель ПЛК и его версия, режим работы ПЛК; • Программа(проект) ПЛК: контрольная сумма проекта, чтение проекта ПЛК; • Значения тегов, список тегов.	Ethernet/IP
ПЛК Siemens	Сбор конфигураций ПЛК (код заказа, версия ОС, тип модуля, наименование модуля, серийный номер, состояние ПЛК, контрольные суммы, размер, дата последней модификации программных блоков)	S7comm
ПЛК SCHNEIDER ELECTRIC	Сбор конфигураций ПЛК. • Сведения о проекте: дата компиляции проекта, время компиляции проекта, версия проекта, имя проекта; • Сведения о ПЛК: наименование, идентификатор, семейство ПЛК, тип ПЛК, версия firmware, идентификатор hardware; • Состояние ПЛК: контрольная сумма проекта ПЛК, статус ПЛК; • Программа(проект) ПЛК.	Modbus
Прочие активы с поддержкой SNMP	Параметры из раздела System – обобщенные данные о системе (имя, время работы с момента последней перезагрузки);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела Interfaces – данные о сетевых интерфейсах (статус, количество, типы, размер пакетов);	SNMP

Табл. 30. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Прочие активы с поддержкой SNMP	Параметры из раздела TCP – данные протокола TCP (количество соединений, получено и отправлено пакетов, количество ошибок);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела ICMP – данные протокола обмена управляющими сообщениями ICMP (количество сообщений получено и отправлено, количество ошибок и их виды);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела EGP – протокол обмена информацией о состоянии маршрутизации (получено и отправлено пакетов, количество ошибок);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела UDP – данные протокола UDP (получено и отправлено датаграмм, количество ошибок);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела SNMP – статистика работы одноименного протокола (количество входящих и исходящих пакетов, обработано запросов, ошибки);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела IP – данные о функционировании этого протокола (количество пакетов получено и отправлено, количество ошибок и их разновидности)	SNMP
ПЛК ОВЕН	Сбор конфигураций ПЛК ОВЕН: • сведения о проекте; • сведения о ПЛК: тип ПЛК, его текущее состояние, настройки, наличие парольной защиты	PLC-Browser

7.10. Перечень SCADA, с которых поддерживается сбор данных

- Программный комплекс Сириус-ИС
- SIMATIC WinCC
- TrainView
- TRACE MODE Runtime
- HMI/SCADA IFIX3.5 GE Fanuc Automation
- Wonderware InTouch
- Аргус
- ICONICS GENESIS-32
- НИИИС ПИК Орион
- MasterSCADA
- CitectSCADA
- DeltaV
- RSView32
- Proficy HMI/SCADA-Cimplicity
- Foxboro FowView/FoxDraw
- Программный комплекс Redkit SCADA

7.11. Поддерживаемые протоколы передачи данных

Модуль «Анализ промышленного сетевого трафика» способен разбирать различные данные в трафике активов на следующих уровнях:

- индикация — базовое распознавание протокола в трафике: его наличие и наименование без дополнительной информации о содержании его полей. Такие протоколы отображаются в столбце **Протоколы** вкладки **Сессии** и в поле **Протоколы** карточки сессии;
- анализ событий ИБ — выявление в трафике подозрительных или вредоносных действий с определением использованной техники атаки — доступно на страницах **События** и **Инциденты**;
- подробный анализ полей протоколов — подробный анализ и отображение детальной информации о содержании полей протокола. Список таких протоколов представлен в группе вкладок **Протоколы** на странице **Сетевые соединения**;
- контроль параметров технологического процесса — мониторинг и валидация значений, критичных для техпроцесса, с целью выявления несанкционированных изменений;
- выявление аномалий ПЛК — выявление отклонений в поведении программируемых логических контроллеров — например, появление новых узлов в контролируемой сети, запуск на узлах новой службы;
- извлечение файлов из трафика — обнаружение, анализ и сохранение файлов, передаваемых в рамках сессий — доступно на вкладке **Файлы** страницы **Сетевые соединения**.

В таблице ниже представлена информация о поддерживаемых протоколах и уровнях их разбора. Протоколы сгруппированы по назначению: общие и промышленные. Наличие галочки (✓) означает поддержку соответствующего уровня анализа, крестик (×) — отсутствие.

Табл. 31. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИНДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПОДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРОТОКОЛОВ	КОНТРОЛЬ ПАРАМЕТРОВ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
Протоколы общего назначения						
ARP (Address Resolution Protocol)	×	✓	×	Неприменимо	Неприменимо	×
AYIYA (Anything In Anything)	✓	×	×			×
DCE/RPC (Distributed Computing Environment / Remote Procedure Calls)	✓	✓	✓			×
DHCP (Dynamic Host Configuration Protocol)	✓	×	×			×
DNS (Domain Name System)	✓	✓	✓			×
DTLS (Datagram Transport Layer Security)	✓	×	×			×
Finger	✓	×	×			×
FTP (File Transfer	✓	×	×			✓

Табл. 31. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
Protocol) — Control connection						
Geneve	✓	×	×			×
GSSAPI (Generic Security Service Application Program Interface)	✓	×	×			×
GTPV1 (GPRS Tunneling Protocol Version 1)	✓	×	×			×
HTTP (Hyper Text Transfer Protocol)	✓	✓	✓			✓
ICMP (Internet Control Message Protocol)	✓	✓	×			×
IMAP (Internet Message Access Protocol)	✓	×	×			×
IRC (Internet Relay Chat)	✓	×	×			✓

Табл. 31. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИНДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПОДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРОТОКОЛОВ	КОНТРОЛЬ ПАРАМЕТРОВ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
Kerberos	✓	×	✓			✓
LDAP (Lightweight Directory Access Protocol)	✓	×	×			×
LLMNR (Link-local Multicast Name Resolution)	×	✓	×			×
MDNS (Multicast Domain Name System)	×	✓	×			×
MQTT (Message Queue Telemetry Transport)	✓	×	×			×
MySQL	✓	×	×			×
NBNS (Network Basic Input/ Output System Name Service)	✓	×	×			×
NTLM (New Technology	✓	✓	✓			×

Табл. 31. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
LAN Manager)						
NTP (Network Time Protocol)	✓	×	×			×
POP3 (Post Office Protocol Version 3)	✓	×	×			×
PGSQL (PostgreSQL)	✓	×	×			×
QUIC	✓	×	×			×
RADIUS (Remote Authentication Dial-In User Service)	✓	×	×			×
RDP (Remote Desktop Protocol)	✓	×	✓			✓[3]
RFB/VNC (Remote Framebuffer)	✓	×	×			×
SIP (Session Initiation Protocol)	✓	×	×			×

3. Извлеченные файлы содержат только данные об использованном в соединении сертификате SSL/TLS.

Табл. 31. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИНДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПОДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРОТОКОЛОВ	КОНТРОЛЬ ПАРАМЕТРОВ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
SMB (Server Message Block)	✓	✓	✓			✓
SMTP (Simple Mail Transfer Protocol)	✓	×	✓			✓
SNMP (Simple Network Management Protocol)	✓	×	×			×
SOCKS	✓	×	×			×
SSH (Secure Shell)	✓	✓	✓			×
SSL (Secure Sockets Layer)	✓	×	✓			✓
SYSLOG	✓	×	×			×
TDS (Tabular Data Stream)	✓	×	×			×
TELNET	✓	×	×			×
TFTP	✓	×	×			×
TNS (Transparent Network Substrate)	✓	×	×			×

Табл. 31. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИНДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПОДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРОТОКОЛОВ	КОНТРОЛЬ ПАРАМЕТРОВ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
TPKT/COTP (Connection-Oriented Transport Protocol)	✓	×	×			×
VXLAN (Virtual Extensible LAN)	✓	×	×			×
WS DISCOVERY (Web Services Dynamic Discovery)	✓	×	×			×
XMPP (Extensible Messaging and Presence Protocol)	✓	×	×			×
Протоколы промышленного назначения						
DNP3 (Distributed Network Protocol 3)	✓	✓	×	×	×	×
Emerson DeltaV	✓	✓	✓	✓	×	×
ENIP/CIP (Ethernet Industrial Protocol/ Common	✓	✓	×	×	✓	×

Табл. 31. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
Industrial Protocol)						
IEC 60870-5-104	✓	✓	×	×	✓	×
IEC 61850 MMS (Manufacturing Message Specification)	✓	×	×	×	✓	×
Modbus	✓	×	✓	✓	✓	×
OPC UA (Open Platform Communications Unified Architecture)	✓	×	✓	✓	✓	×
S7 Communication	✓	✓	×	×	✓	×
S7 Plus Communication	✓	✓	×	×	✓	×
UMAS (Unified Messaging Application Services)	✓	✓	×	×	×	×

7.12. Длина очереди сообщений

В Комплексе существуют следующие очереди сообщений о событиях и сетевых соединениях:

- очередь сообщений о событиях службы обнаружения вторжений и событиях Syslog;
- очередь сообщений о сетевой активности активов;
- очередь сообщений о сессиях.

Данные очереди сообщений сохраняются на сенсоре.

В некоторых случаях очередь сообщений может переполняться, в результате чего более старые сообщения будут удалены. Ниже приведены причины переполнения очереди сообщений:

- невозможность передачи и сохранения данных на Комплексе уровня Management в результате потери связи между ним и сенсором;
- слишком большая скорость приема данных, в результате чего Комплекс уровня Management не успевает обработать получаемые данные.

По умолчанию очереди сообщений имеют следующую длину:

- длина очереди сообщений о событиях службы обнаружения вторжений и событиях Syslog — 3072 байта;
- длина очереди сообщений о сессиях — 1024 байта.

Данные значения настраиваются в момент развертывания Комплекса. При необходимости настройки других значений рекомендуется обратиться в сервисный центр ООО «СайберЛимфа».

7.13. Сетевые взаимодействия Комплексов

Порты назначения указаны в формате: `[TCP или UDP] [номер порта TCP или UDP] ([протокол или сервис назначения])`

Табл. 32. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕНЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
UDV DATAPK уровня Sensor	TCP 135 (MSRPC) TCP 139 TCP 445 (Winexe) TCP 1024-5000 (MSRPC в Windows XP) TCP 49152-65535 (MSRPC в Windows Vista и новее) TCP 5985 TCP 5986 (WinRM) TCP 3306 (MySQL) TCP 1433 (MSSQL)	Активы на базе ОС Windows, СУБД	Взаимодействие с активом (режим опроса)
	TCP 22 (SSH) TCP 23 (Telnet)	Активы на базе ОС Unix, АСО	
	UDP 161 (SNMP) TCP 102 (S7) TCP 502 (Modbus) TCP 44818 (EthernetIP)	ПЛК	
Активы, поддержи-вающие передачу событий через	UDP 514 (Syslog 3164) UDP 515 (Syslog 5424) TCP 514 (Syslog 3164 TCP)	UDV DATAPK уровня Sensor	Пассивный сбор событий от активов

Табл. 32. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕНЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
стандарт syslog/SNMP-trap	TCP 515 (Syslog 5424 TCP) UDP 162 (SNMP-trap)		
UDV DATAPK уровня Sensor	TCP 16379 (redis) — синхронизация настроек TCP 19091 (prometheus) — метрики TCP 15673 (rabbitmq) — получение данных UDP 123 (если Management выступает в роли NTP-сервера для Sensor)	UDV DATAPK уровня Management	Взаимодействие уровня Sensor с уровнем Management. Инициирует соединения всегда сенсор, поэтому его действительный IP-адрес допускается скрывать по технологии NAT (SNAT). Если межсетевой экран стоит уже после SNAT, доступы к уровню Management нужно открывать с использованием виртуального адреса сенсора
UDV DATAPK уровня Sensor	TCP 20085 — получение pcap-файлов сетевого трафика	UDV DATAPK уровня Management	Получение данных с сенсора
	TCP 20044 — получение архива с файлами		
	TCP 20104 — получение данных о сетевых соединениях		
UDV DATAPK уровня Sensor (опционально) UDV DATAPK уровня Management	UDP 123 (NTP)	NTP-серверы	Синхронизация времени

Табл. 32. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕНЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
UDV DATAPK уровня Management	UDP 514 TCP 514 TCP 25 (SMTP) TCP 465 (SMTPS)	Смежная система	Отправка событий и почтовых уведомлений в смежные системы
UDV DATAPK уровня Management	TCP 389 (LDAP) или TCP 636 (LDAPS)	LDAP-сервер	Для возможности авторизации пользователей UDV DATAPK через службу каталогов
АРМ административного персонала	TCP 443 (HTTPS) TCP 22 (SSH)	UDV DATAPK уровня Management	Администрирование UDV DATAPK. SSH — для сервисного обслуживания в терминале операционной системы
	TCP 22 (SSH)	UDV DATAPK уровня Sensor	Администрирование UDV DATAPK (сервисное обслуживание)

7.15. Структура директорий Комплекса

Список общих директорий и файлов настроек, а также их описание представлены в таблице ниже (Таблица 35. Общие директории и файлы настроек).

Табл. 35. Общие директории и файлы настроек

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
`/usr/share/udv`	Основная директория Комплекса
`/usr/share/udv/scripts-certs`	Директория для хранения сертификата для верификации сканеров сбора данных
`/usr/share/udv/scripts-certs/datapk_script.crt`	Сертификат для верификации сканеров сбора данных
`/usr/share/udv/certs/ca.crt`	Корневой сертификат

Список директорий и основных файлов Комплекса уровня Management, а также их описание представлены в таблице ниже (Таблица 36. Директории и основные файлы настроек Комплекса уровня Management).

Табл. 36. Директории и основные файлы настроек Комплекса уровня Management

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
`/usr/share/udv/datapk/manager.env`	Основные настройки Комплекса
`/var/cache/udv/nginx/certs`	Серверные сертификаты
`/usr/share/udv/nginx`	Шаблоны `nginx`
`/usr/share/udv/frontend`	Настройки меню (интерфейса)
`/etc/logstash`	Правила нормализации
`/var/backups`	Директория для хранения резервных копий. Содержит tar-архивы с резервными копиями (`dtpk-backup-version-timestamp.tar`)
`/var/backups/elasticsearch`	Директория для хранения резервных копий событий
`/var/backups/elasticsearch/indices`	Архивированные индексы событий

Табл. 36. Директории и основные файлы настроек Комплекса уровня Management

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
`/var/backups/elasticsearch/uploads`	Индексы событий для импорта
`/usr/share/udv/vulnerability-backend`	Директория для хранения импортированного справочника ПО и уязвимостей (CPE и CVE), импортированной базы сопоставления собранного сканерами ПО со справочником CPE и отчета с последними результатами поиска уязвимостей
`/var/opt/udv`, `/var/cache/udv`	Служебные директории Комплекса

Список директорий и основных файлов Комплекса уровня Sensor, а также их описание представлены в таблице ниже (Таблица 37. Директории и основные файлы настроек Комплекса уровня Sensor).

Табл. 37. Директории и основные файлы настроек Комплекса уровня Sensor

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
`/usr/share/udv/datapk/sensor.env`	Основные настройки Комплекса
`/usr/share/udv/snmp-connector/snmp_mibs`	Словари SNMP

7.16. Состав модулей Комплекса в сервисах

Табл. 38.

НАИМЕНОВАНИЕ МОДУЛЯ	КОМПЛЕКС УРОВНЯ MANAGEMENT	КОМПЛЕКС УРОВНЯ SENSOR
Базовый модуль (Core)	udv-alerting udv-alertmanager udv-auth-backend udv-event-manager udv-event-processor udv-exporter udv-host-manager udv-hosts-bff	udv-rabbitmq-sensor-stunnel udv-rabbitmq-stunnel udv-redis-sensor-stunnel udv-redis-stunnel udv-event-receiver udv-nmap-sensor udv-node-exporter udv-pushgateway-exporter

Табл. 38.

НАИМЕНОВАНИЕ МОДУЛЯ	КОМПЛЕКС УРОВНЯ MANAGEMENT	КОМПЛЕКС УРОВНЯ SENSOR
	udv-incident-manager udv-nginx udv-nmap-manager udv-node-exporter-sensor udv-page-views-backend udv-postgresql udv-prometheus udv-pushgateway-cleaner udv-pushgateway-stunnel udv-pushgateway udv-rabbitmq-sensor-stunnel udv-rabbitmq-stunnel udv-rabbitmq udv-redis-sensor-stunnel udv-redis-stunnel udv-redis udv-report-generator udv-sensors-backend udv-system-backend-sensor udv-system-backend udv-user-service	udv-pushgateway-stunnel-sensor udv-rabbitmq-exporter-sensor udv-rabbitmq-sensor udv-redis-exporter-sensor udv-redis-sensor udv-sensor-heartbeat
Анализ промышленного сетевого трафика	udv-clickhouse-service udv-dpi-backend udv-files-backend udv-files-watcher-stunnel udv-rules-backend udv-steno-backend-stunnel udv-steno-backend udv-suricata-backend udv-tags-control-backend udv-vector-sensor-stunnel udv-vector-stunnel	udv-files-watcher-stunnel udv-steno-backend-stunnel udv-vector-sensor-stunnel udv-vector-stunnel udv-vector udv-activity-logger udv-dns-classifier udv-enrich-processor udv-files-watcher udv-rules-filter udv-steno-wrapper-stunnel

Табл. 38.

НАИМЕНОВАНИЕ МОДУЛЯ	КОМПЛЕКС УРОВНЯ MANAGEMENT	КОМПЛЕКС УРОВНЯ SENSOR
	udv-vector udv-zeek-backend udv-zeek-wrapper udv-zeek	udv-steno-wrapper udv-stenographer udv-suricata-exporter udv-suricata-wrapper udv-suricata udv-tags-control-filter udv-vector-sensor
Управление проектами ПЛК	udv-cv-repos-backend udv-cv-repositories-server	—
Управление конфигурациями	udv-configs-manager udv-host-data-collector udv-software-backend	udv-command-processor udv-modbus-connector udv-msrpc udv-opc-connector udv-plc-config-connector udv-plc-connector udv-snmp-connector udv-sql-connector udv-terminal-connector
Управление уязвимостями	udv-mariadb udv-oval-scanner udv-vulnerability-backend	—
Управление внешними событиями	udv-esper udv-logstash udv-opensearch-controller udv-opensearch-dashboards udv-opensearch	udv-opensearch-dashboards
Swagger UI	udv-external-api	—
EDR for PLC	—	udv-agentless-edr
Supervision Backend	udv-supervision-backend	—