РУКОВОДСТВО ПО ЛАБОРАТОРНЫМ РАБОТАМ

Система анализа и мониторинга ИБ UDV DATAPK Industrial Kit

ВНЕДРЕНИЕ И ЭКСПЛУАТАЦИЯ

udv|group

CLOUD
УЧЕБНЫЙ ЦЕНТР

Описание лабораторного стенда

Структура виртуального стенда представлена на рисунке (**Рисунок 1**).

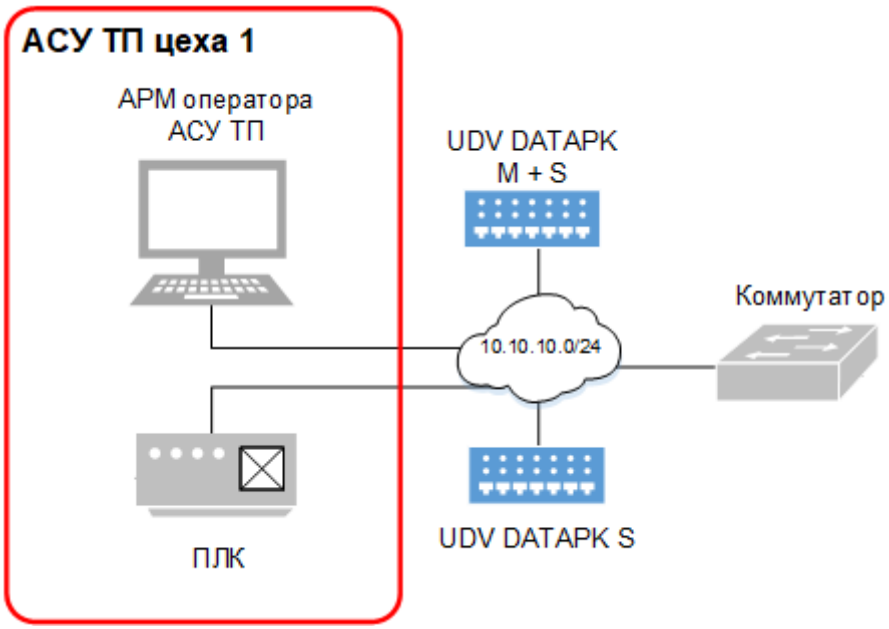


Рисунок 1 — Структурная схема лабораторного стенда

Логин/ пароль для первого входа в веб-интерфейс комплекса: datapk/datapk

На виртуальном стенде UDV DATAPK Industrial Kit представлен следующими компонентами:

- Management + Sensor (в рамках данного стенда используется для управления Sensor'ами и проигрывания дампов сетевого трафика);
- Sensor (в рамках данного стенда используется для получения копии сетевого трафика и передачи данных на Management).

Виртуальный стенд состоит из виртуальных машин (ВМ), моделирующих оборудование автоматизированных систем управления технологическими процессами (АСУ ТП). Параметры стендовых ВМ приведены в таблице (**Таблица 1**).

Таблица 1 – Параметры стендовых ВМ

Наименование	**ОС**	**Имя компьютера**	**IP-адрес / маска подсети**	**Логин / Пароль**
АРМ оператора АСУ ТП	Windows 10	WIN10-Lab	10.10.10.50/24	admin / P@ssw0rd
Коммутатор АСУ ТП цеха 1	Cisco IOS	cisco	10.10.10.30/24	cisco / cisco
ПЛК АСУ ТП цеха 1	Windows XP	PLC-lab	10.10.10.40/24	admin / P@ssw0rd
UDV DATAPK M + S	Альт Сервер 10 SP	datapk-1	10.10.10.10/24	root / P@ssw0rd
UDV DATAPK S	Альт Сервер 10 SP	datapk-2	10.10.10.11/24	root / P@ssw0rd

Системные требования виртуальных стендов (

Таблица 2):

Таблица 2 – Системные требования к стендовым ВМ

	vCPU, ядра	**RAM, ГБ**	**HDD/SSD, ГБ**
UDV DATAPK Management + Sensor	4	16	70
UDV DATAPK Sensor	4	12	70
Windows 10	2	2	40
Windows XP	2	1	40
Коммутатор	2	1	10

Системные требования к устройству (ноутбуку или ПК) для каждого студента:

- не менее 4 физических ядер CPU;
- не менее 32 ГБ RAM;
- не менее 300 ГБ HDD/SSD.

Лабораторная работа 1. Установка UDV DATAPK Industrial Kit

Разделы документации

- Установка и настройка сертифицированной ОС Альт Сервер 10.2 SP;
- Подготовка к установке Комплекса;
- Установка и запуск модулей Комплекса;
- Первичное подключение.

Справочная информация

ПО UDV DATAPK Industrial Kit может быть развернуто только сертифицированной редакции ОС Альт Сервер СП. На любых других редакциях ОС Альт Сервер работоспособность не гарантирована.

Процесс настройки ОС Альт Сервер СП более подробно описан в официальной документации к Комплексу.

Предполагается, что ВМ с ОС Альт Сервер СП имеет доступ к сети Интернет.

Разметка дискового пространства для установки Комплекса подробно описана в официальной документации к Комплексу. В данной лабораторной работе дисковое пространство будет размечено в «необходимом минимуме», чтобы Комплекс функционировал.

Если планируется подключать более одного сетевого интерфейса с копией трафика к Комплексу, то их необходимо объединить в один (bond), иначе, корректное получение копии сетевого трафика невозможно.

Процесс объединения нескольких физических сетевых интерфейсов в один логический описан в соответствующем разделе официальной документации к Комплексу.

Файлы для лабораторных работ

- Образ ОС Альт Сервер СП 10.2;
- Архив с репозиторием сертифицированных модулей UDV DATAPK: **release-[версия_Комплекса]_[дата_архива].tar.gz**.
- Архив с репозиторием дополнительных несертифицированных модулей UDV DATAPK: **release-[версия_Комплекса]-external-modules_[дата_архива].tar.gz**.

Лабораторное задание 1.1. Установка ОС Альт Сервер СП

Цель: сформировать умение установки ОС Альт Сервер СП для развертывания комплекса.

Ход работы:

Подключите ISO-образ или оптический диск актуальной сертифицированной ОС Альт Сервер к виртуальной машине, на которой будет установлен Комплекс. Запустите виртуальную машину.

> **Примечание:**
> ПО UDV DATAPK Industrial Kit может быть развернуто только сертифицированной редакции ОС Альт Сервер СП. На любых других редакциях ОС Альт Сервер работоспособность не гарантирована

Выберите пункт меню «Rescue LiveCD» и нажмите клавишу «Enter» (**Рисунок 2**).

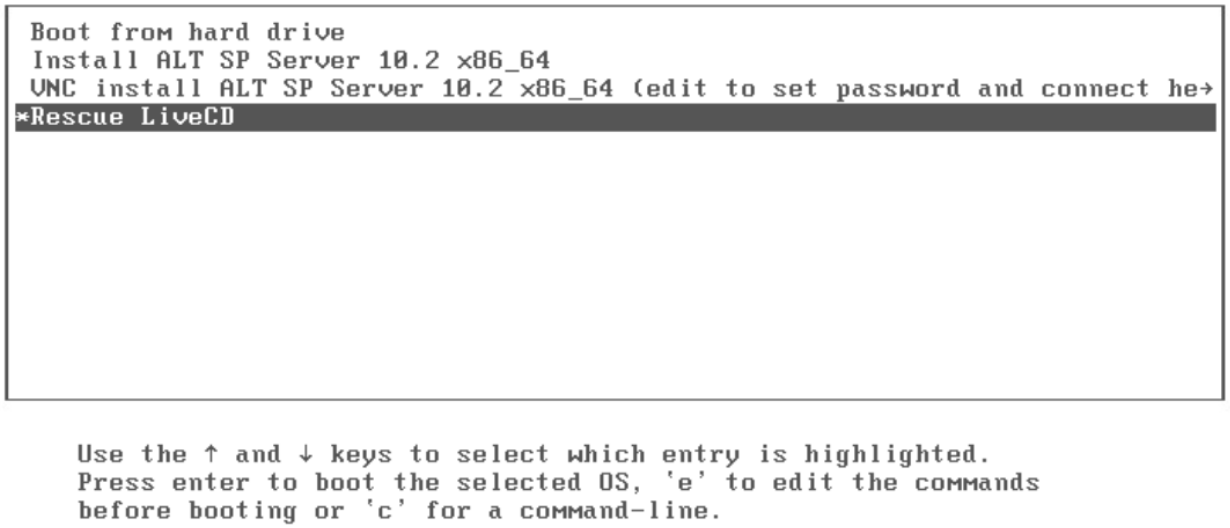


Рисунок 2 — Загрузка платформы в режиме Rescue LiveCD

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
```

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

```
V=${D}[номер_раздела]
```

Последовательно введите следующие команды для настройки физических разделов диска:

```
pvcreate $V

vgcreate udv $V

blockdev --flushbufs $D

reboot
```

После перезагрузки выберите пункт меню «Install ALT SP Server 10.2 x86_64» и нажмите клавишу «Enter» (**Рисунок 3**).

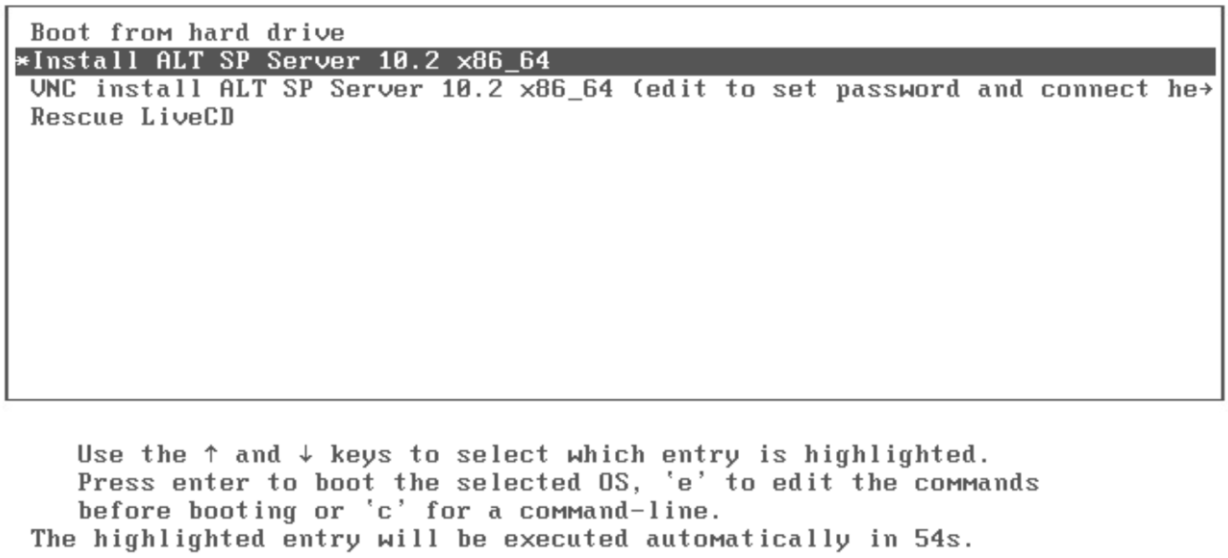


Рисунок 3 — Окно установки

В окне «Язык» настройте русский язык и переключение раскладки клавиатуры, нажмите «Далее» (**Рисунок 4**):

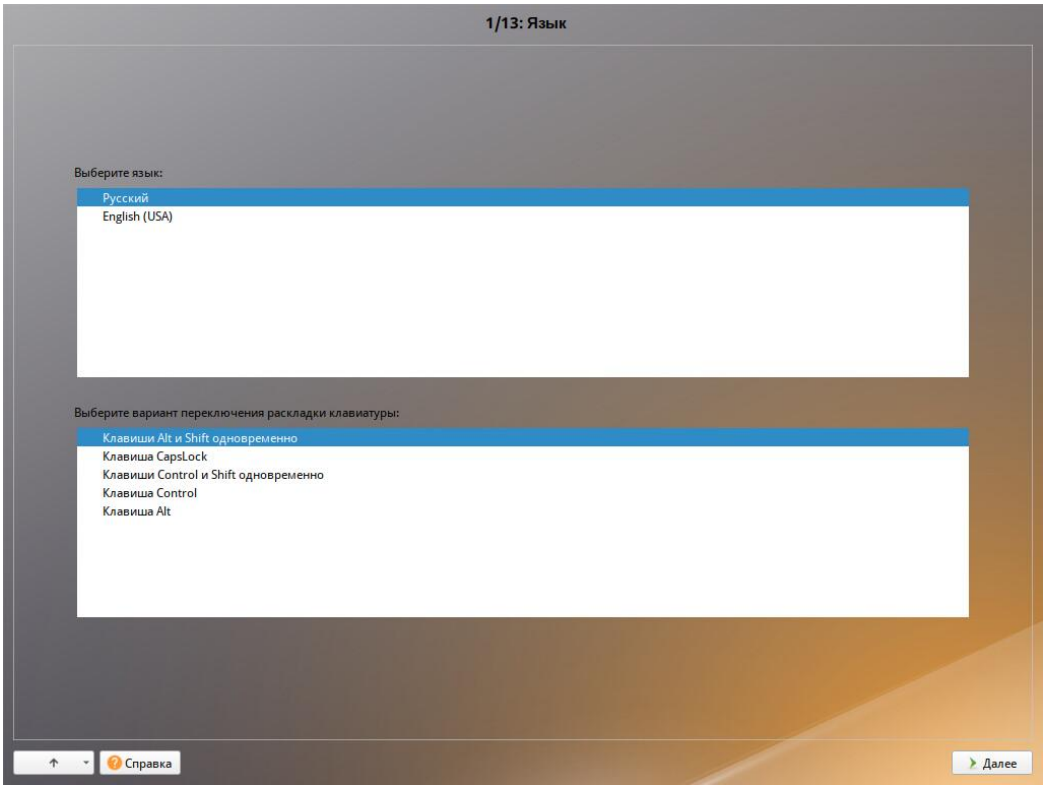


Рисунок 4 — Окно настройки языка и раскладки клавиатуры

Ознакомьтесь с лицензионным соглашением. Установите чекбокс «Да, я согласен с условиями» и нажмите «Далее».

В окне «Дата и время» выберите текущий регион и часовой пояс и нажмите «Далее» (**Рисунок 5**):

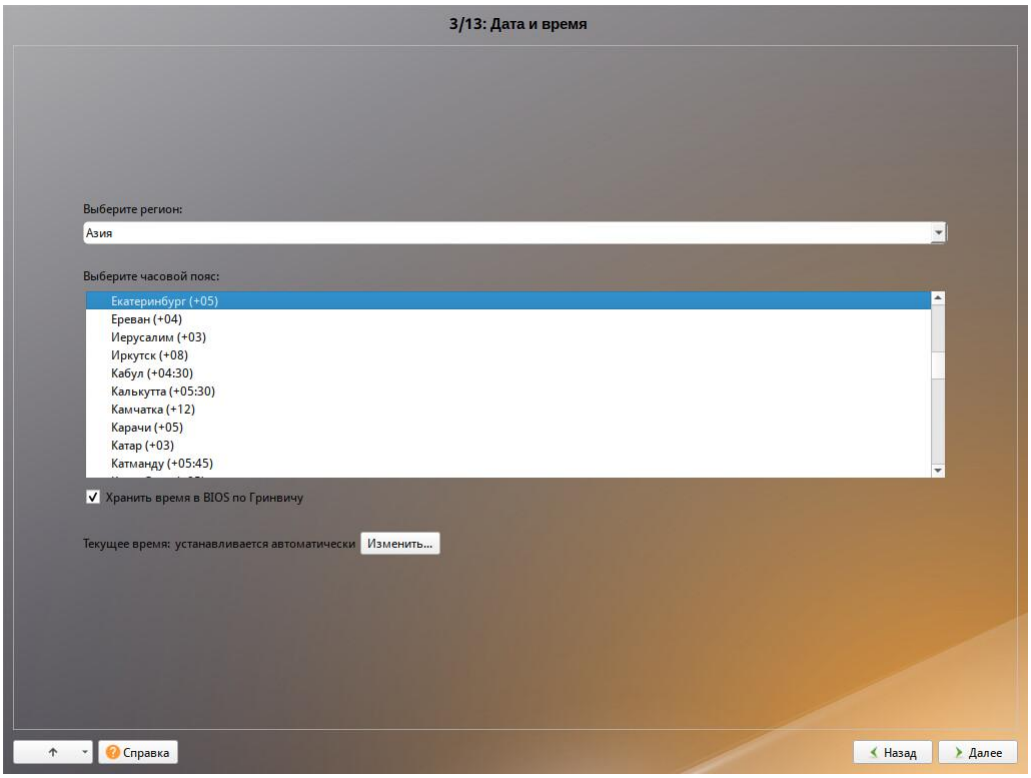


Рисунок 5 — Окно «Дата и время»

Выполните разметку дискового пространства. В поле «Выберите профиль» установите чекбокс «Вручную» и нажмите «Далее» (**Рисунок 6**):

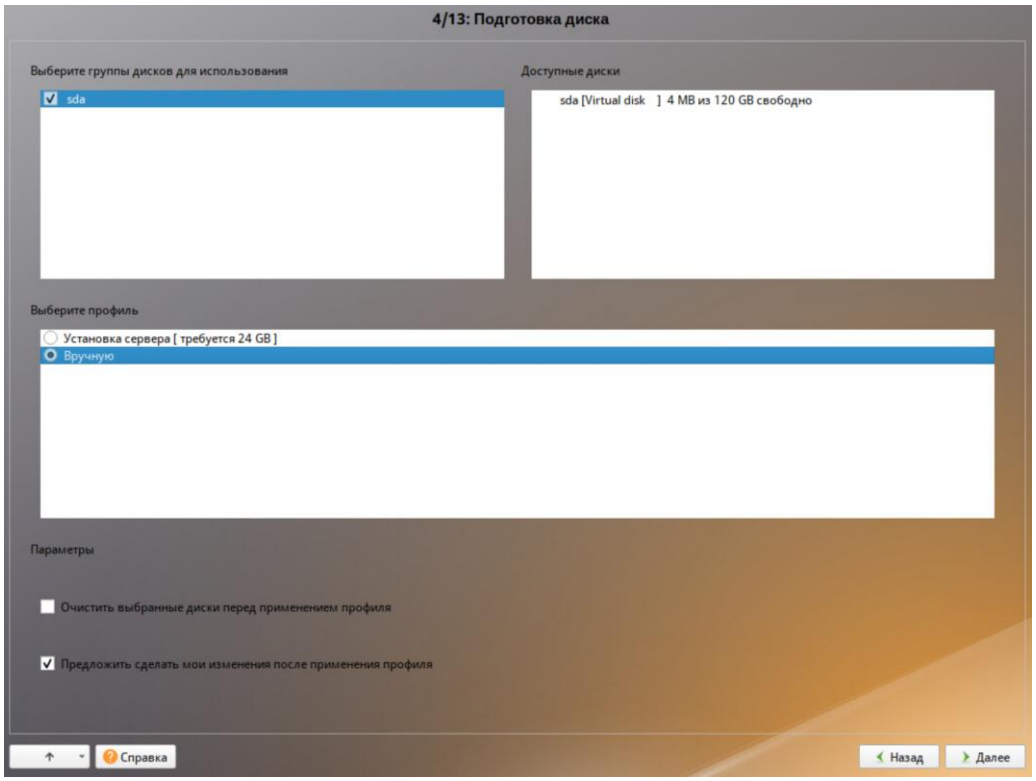


Рисунок 6 — Окно «Подготовка диска»

В раскрывающемся списке «Disks» выберите настроенный ранее раздел диска (например, sda1) и нажмите «Создать файловую систему» (**Рисунок 7**):

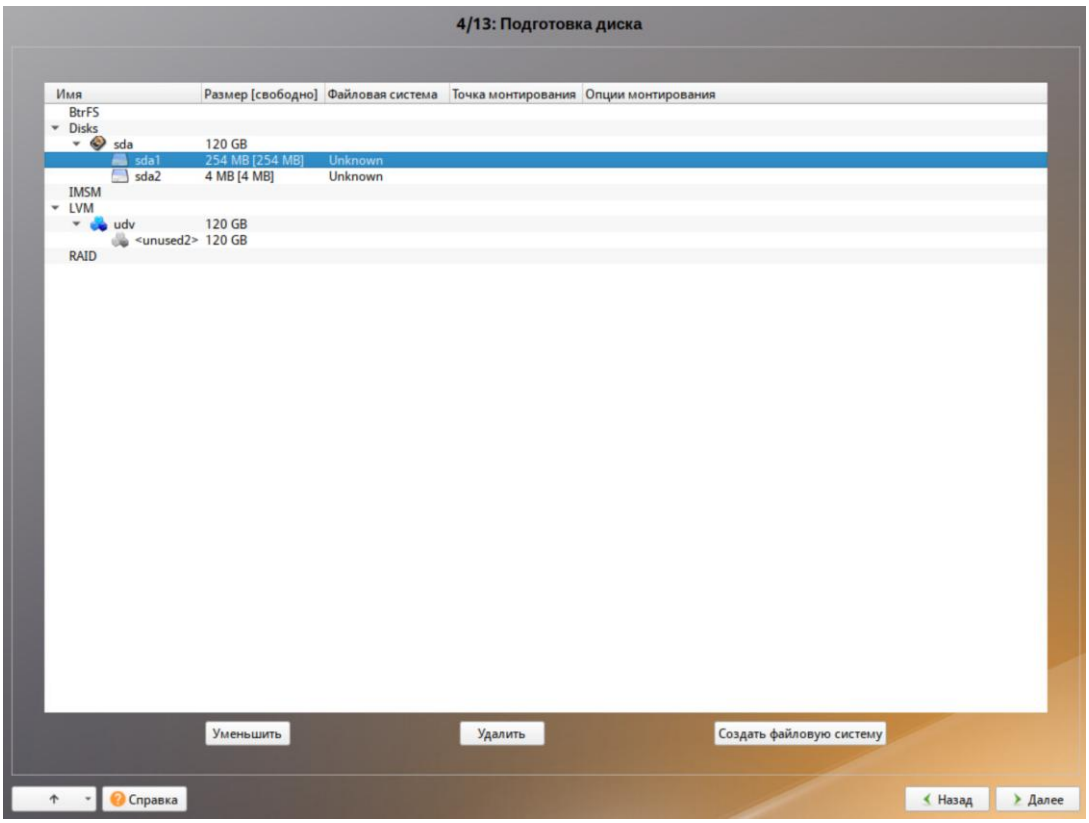


Рисунок 7 — Окно «Подготовка диска» (выбор диска sda1)

В новом окне «Создать файловую систему» выберите «Файловая система FAT32» и нажмите «ОК» (**Рисунок 8**):

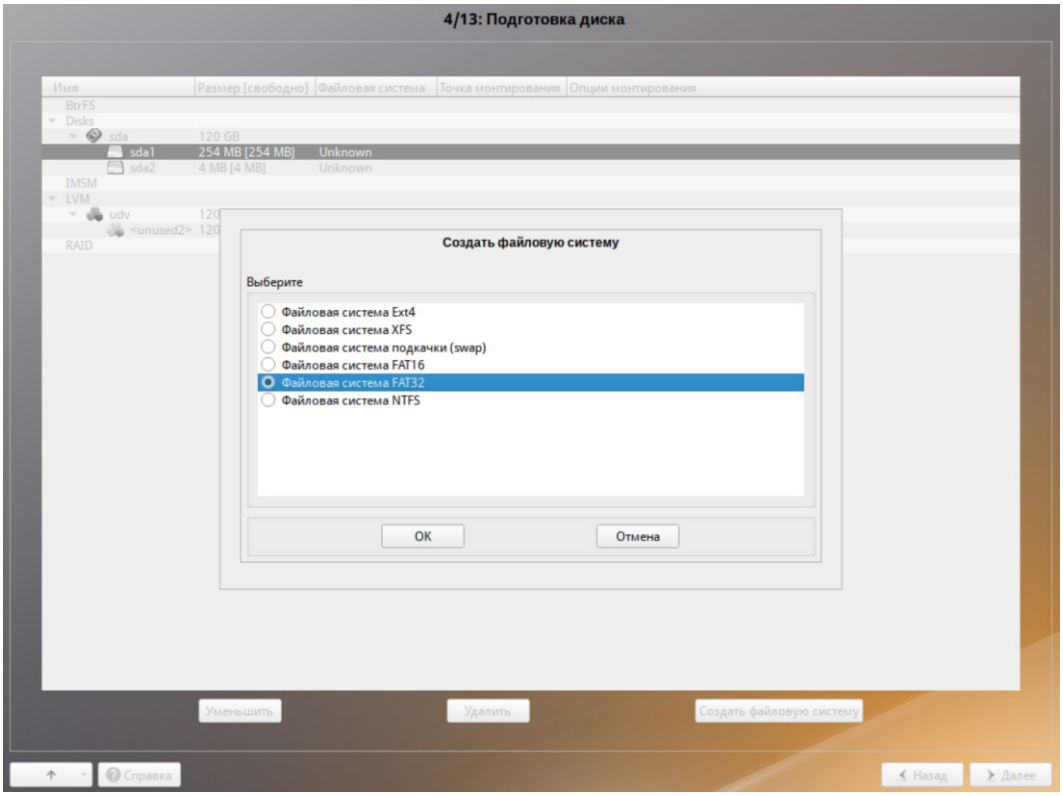


Рисунок 8 — Окно «Создать файловую систему» (выбор файловой системы FAT32)

В новом окне оставьте поле «Метка тома» пустым и нажмите «ОК» (**Рисунок 9**):

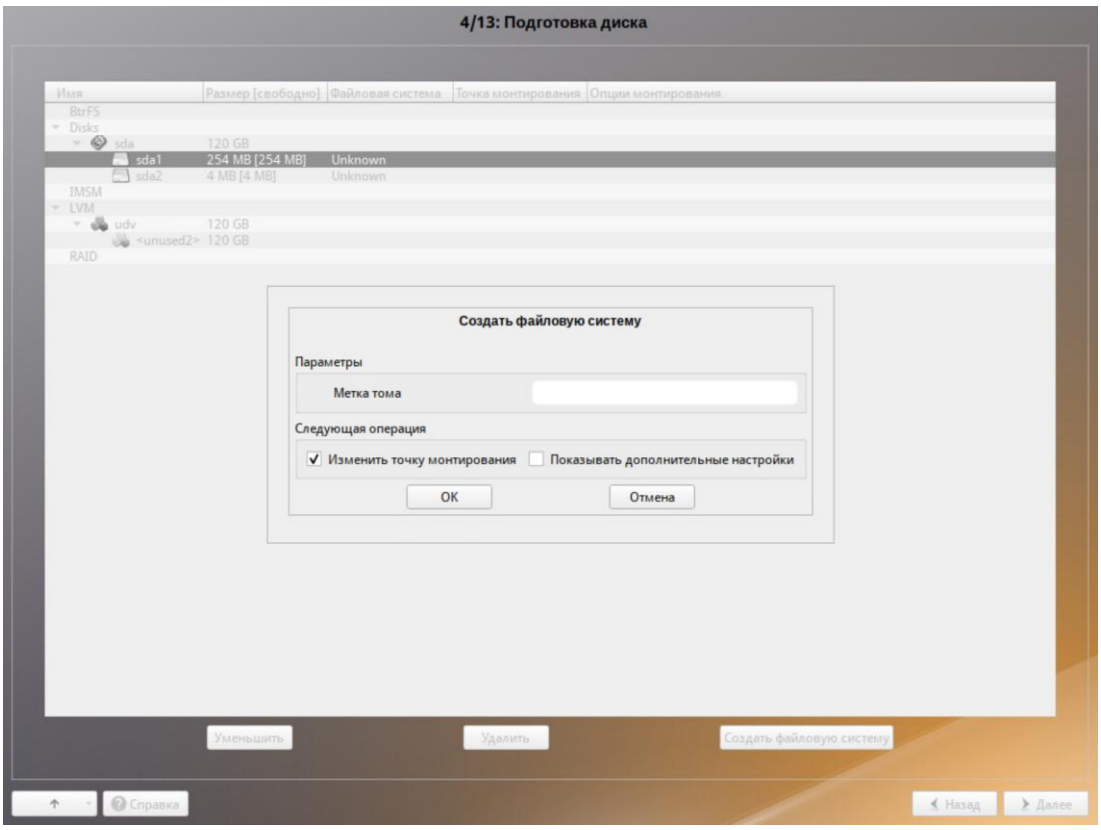


Рисунок 9 — Окно «Создать файловую систему» (настройка метки тома)

В следующем окне убедитесь, что в поле «Точка монтирования» указано «/boot/efi», и нажмите «ОК» (**Рисунок 10**):

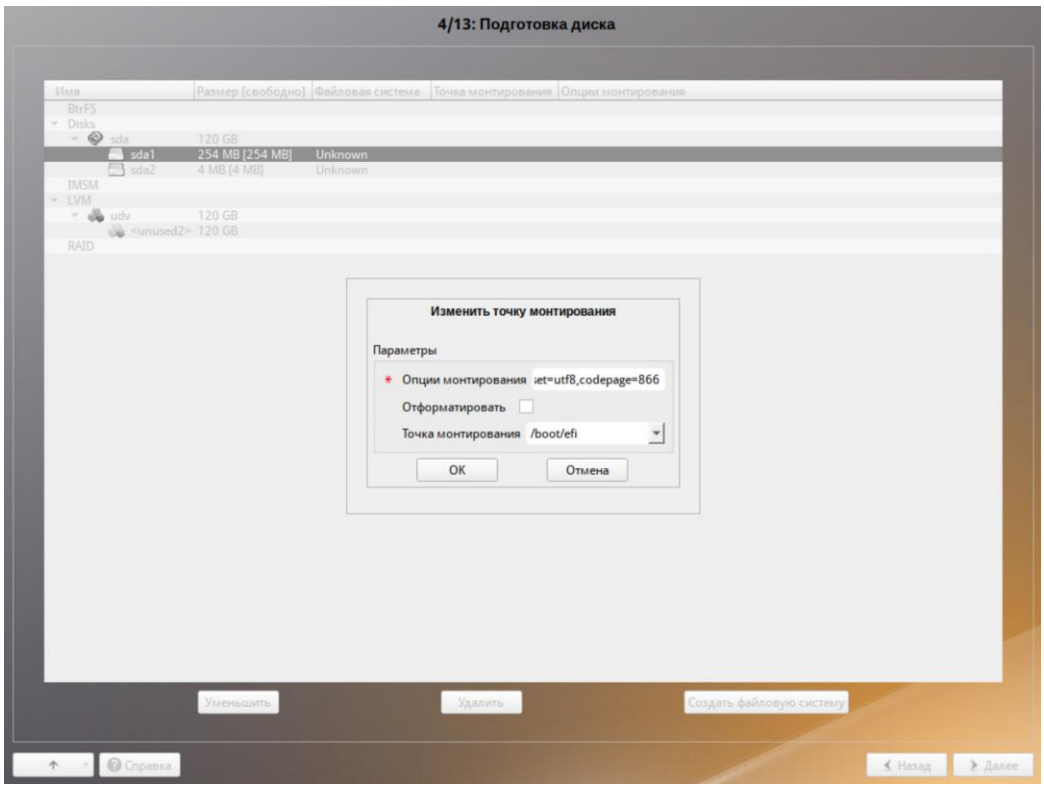


Рисунок 10 — Окно «Создать файловую систему» (настройка точки монтирования)

Создайте первый том «rootfs» для корневого раздела. Для этого в раскрывающемся списке «LVM» выберите «<unused2>» и нажмите «Создать том» (**Рисунок 11**):

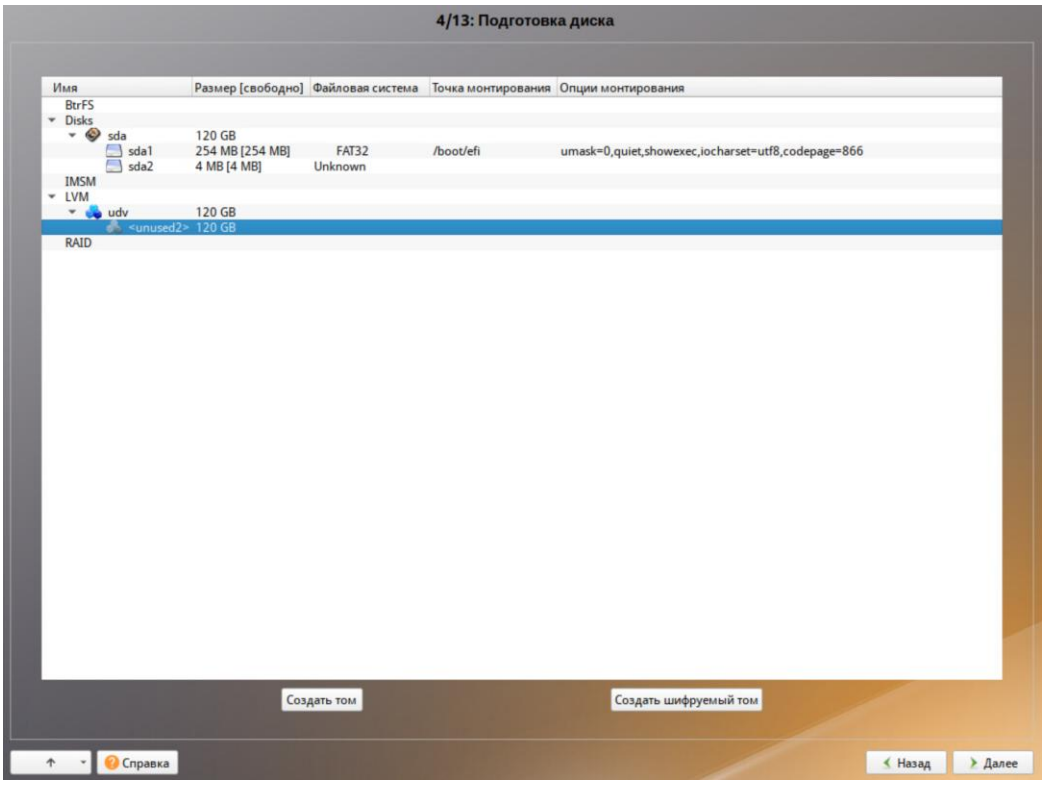


Рисунок 11 — Окно «Подготовка диска» (создание первого тома)

В открывшемся окне «Создать том» выполните следующие действия:

- введите имя тома: «rootfs»;

- выберите размер тома. Рекомендуемый размер тома в реальных инсталляциях — 75 ГБ (75000 MB) (**Рисунок 12**).

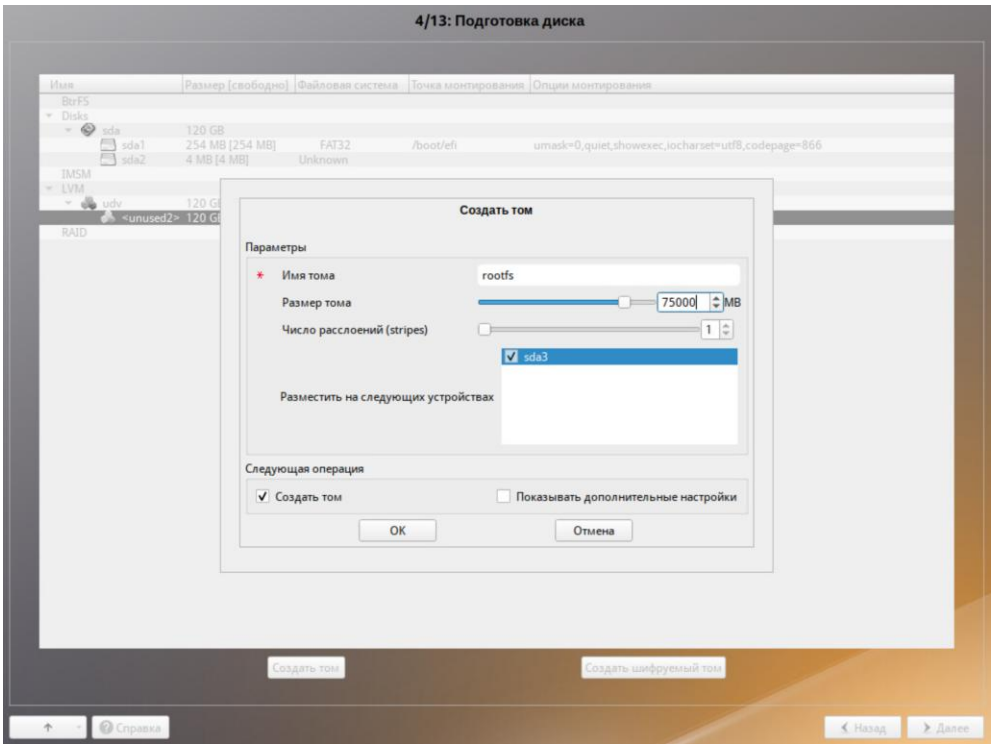


Рисунок 12 — Окно «Создать том» для rootfs

В новом окне «Создать файловую систему» выберите «Файловая система XFS» и нажмите «ОК» (**Рисунок 13**):

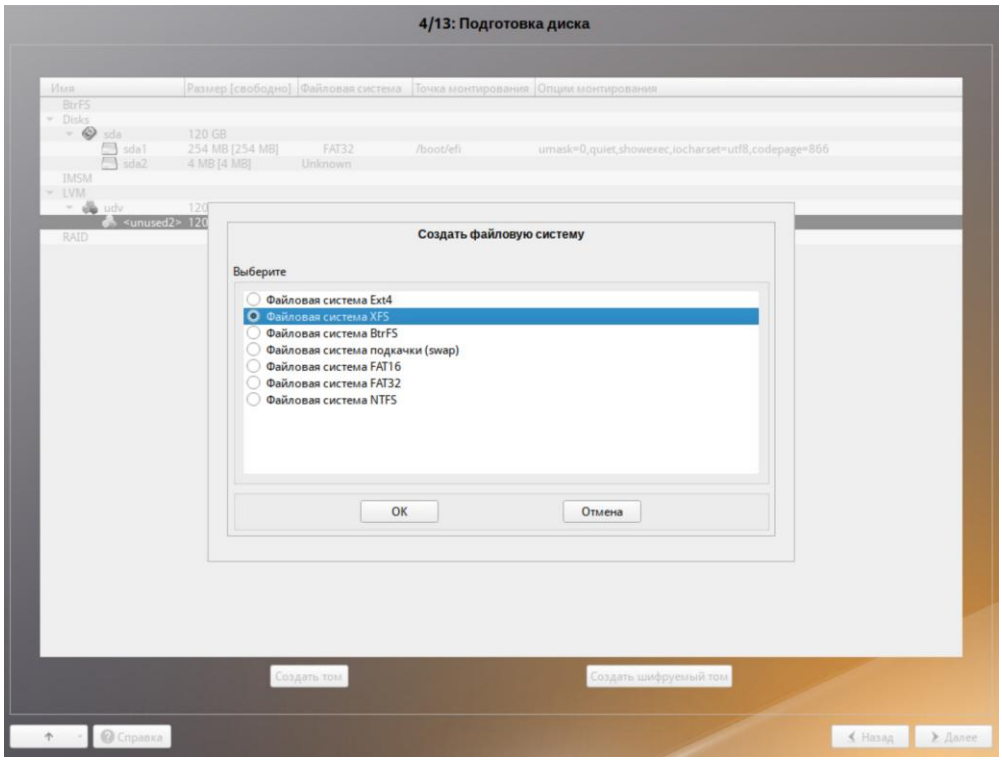


Рисунок 13 — Окно «Создать файловую систему» для rootfs

В новом окне «Изменить точку монтирования» убедитесь, что в поле «Точка монтирования» указано «/», и нажмите «ОК» (**Рисунок 14**):

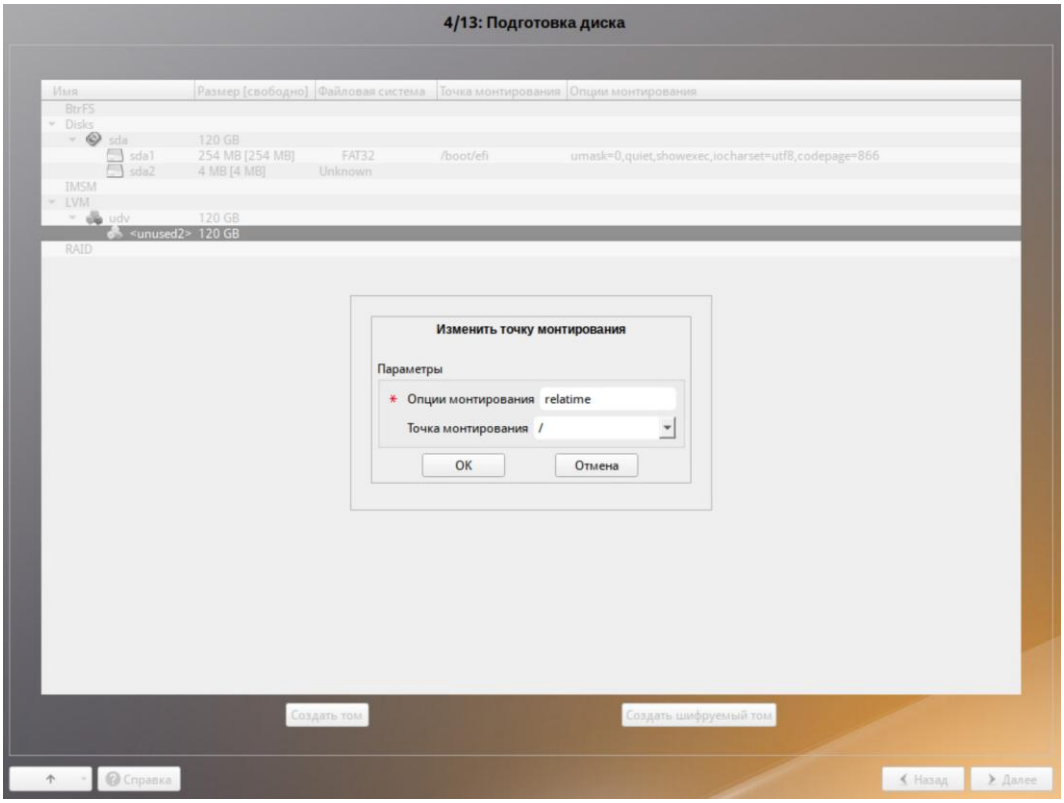


Рисунок 14 — Окно «Изменить точку монтирования» для rootfs

Создайте второй том «logs» для системных журналов. Для этого в раскрывающемся списке «LVM» выберите «<unused2>» и нажмите «Создать том» (**Рисунок 15**):

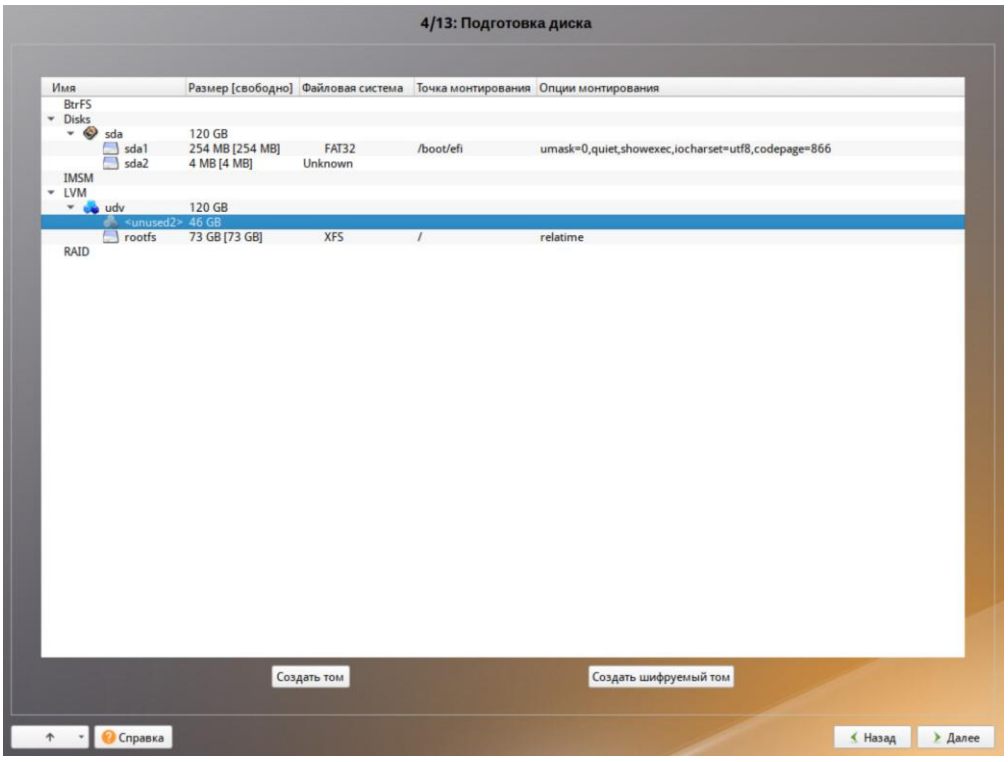


Рисунок 15 — Окно «Подготовка диска» (создание второго тома)

В открывшемся окне «Создать том» выполните следующие действия:

- введите имя тома: «logs»;

- выберите размер тома. Рекомендуемый размер тома в реальных инсталляциях — 25 ГБ (25000 MB) (**Рисунок 16**).

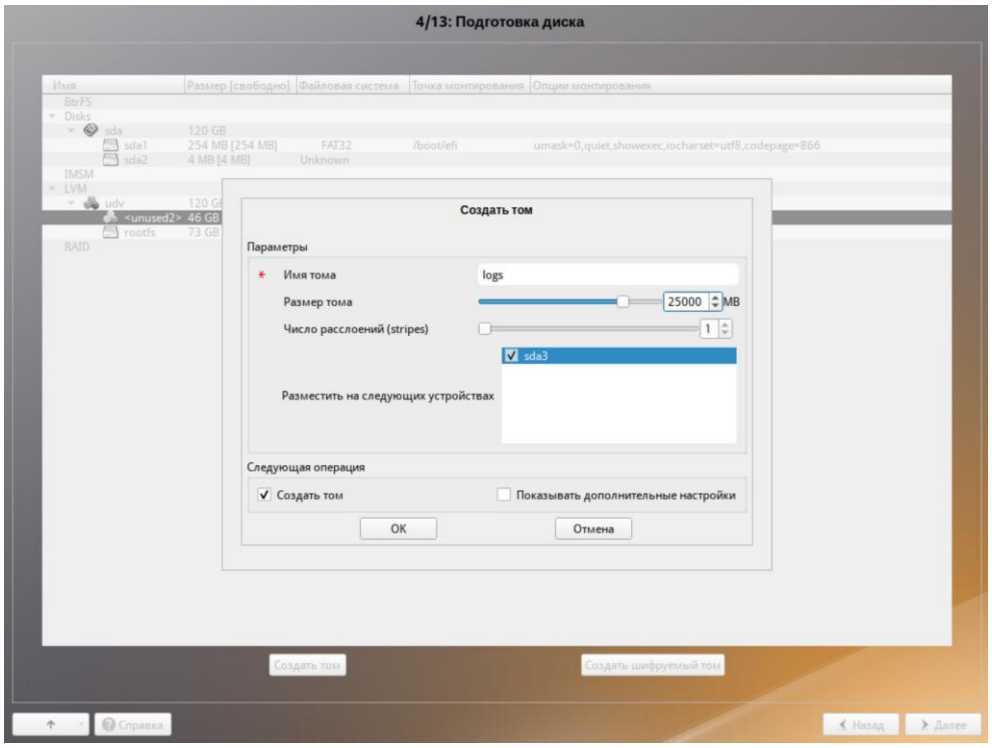


Рисунок 16 — Окно «Создать том» для logs

В новом окне «Создать файловую систему» выберите «Файловая система XFS» и нажмите «ОК» (**Рисунок 17**):

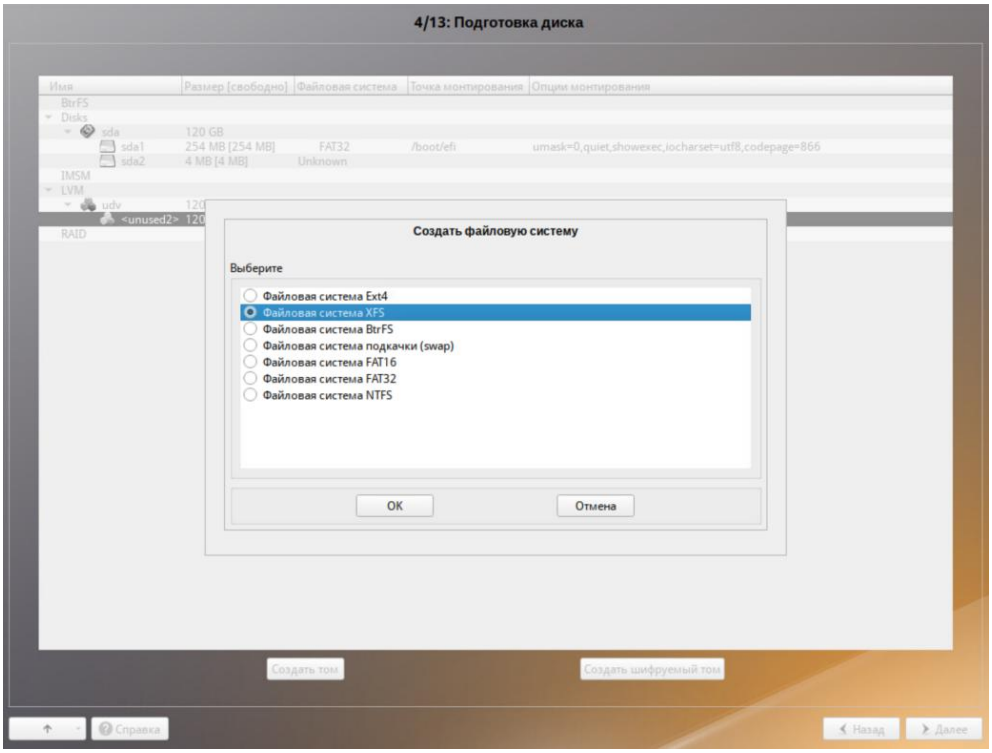


Рисунок 17 — Окно «Создать файловую систему» для logs

В открывшемся 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» (**Рисунок 18**).

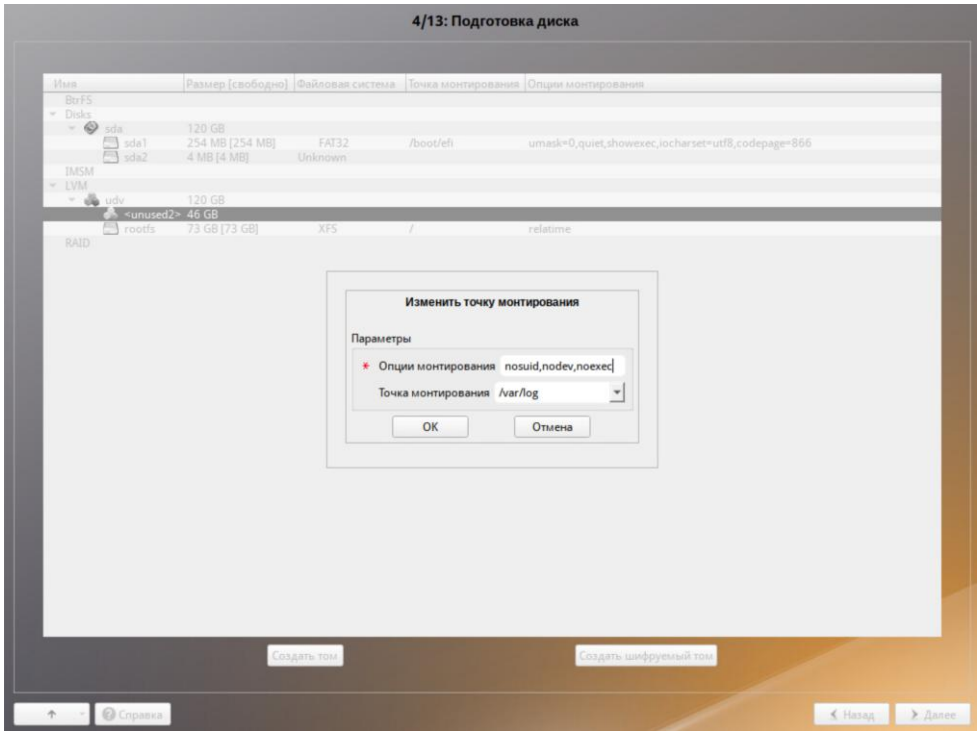


Рисунок 18 — Окно «Изменить точку монтирования» для logs

Для применения настроек нажмите «Далее» (**Рисунок 19**):

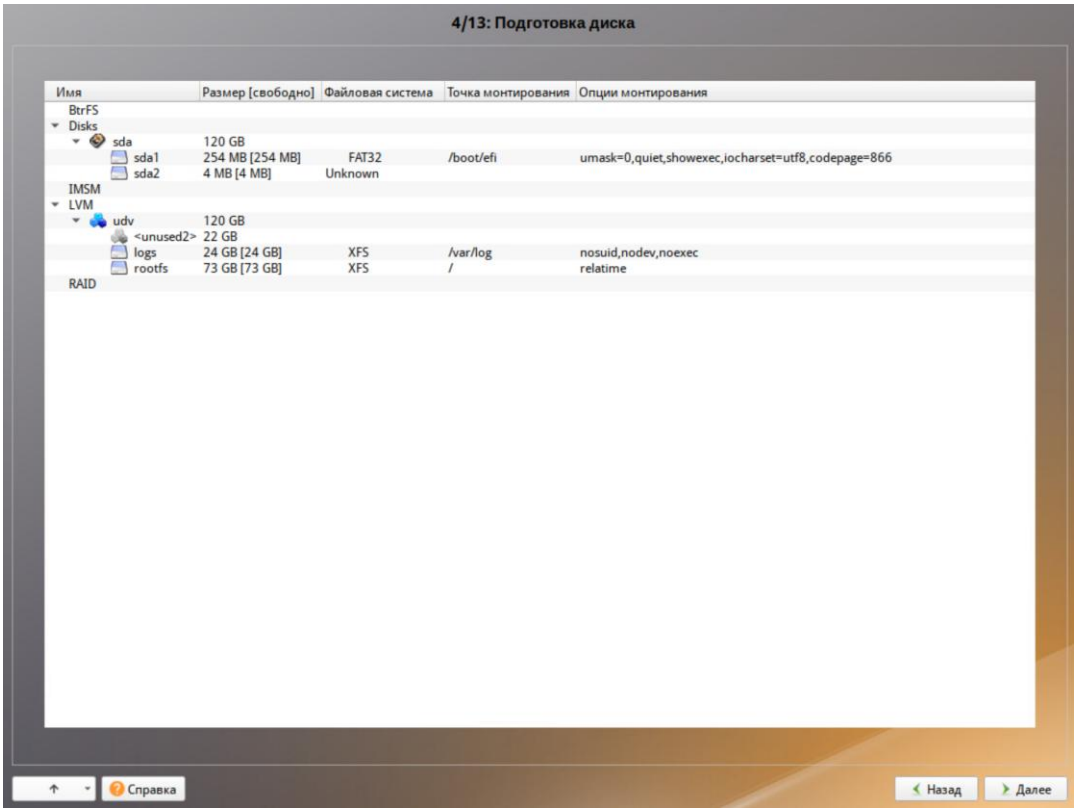


Рисунок 19 — Окно «Подготовка диска» (итоговые настройки)

В новом окне с запланированными операциями нажмите «ОК» (**Рисунок 20**):

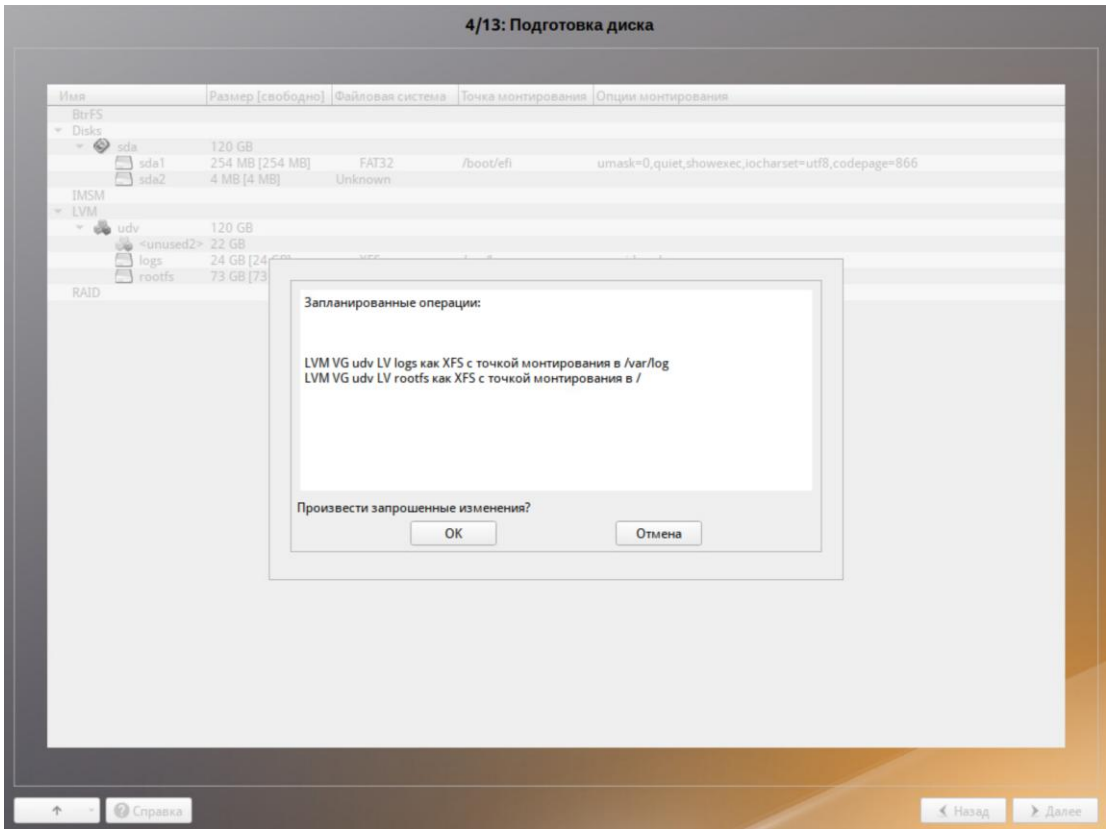


Рисунок 20 — Подтверждение параметров разметки дискового пространства

В окне «Установка системы» отмените выбор чекбоксов со всех компонентов в поле «Дополнительные приложения» и нажмите «Далее» (**Рисунок 21**):

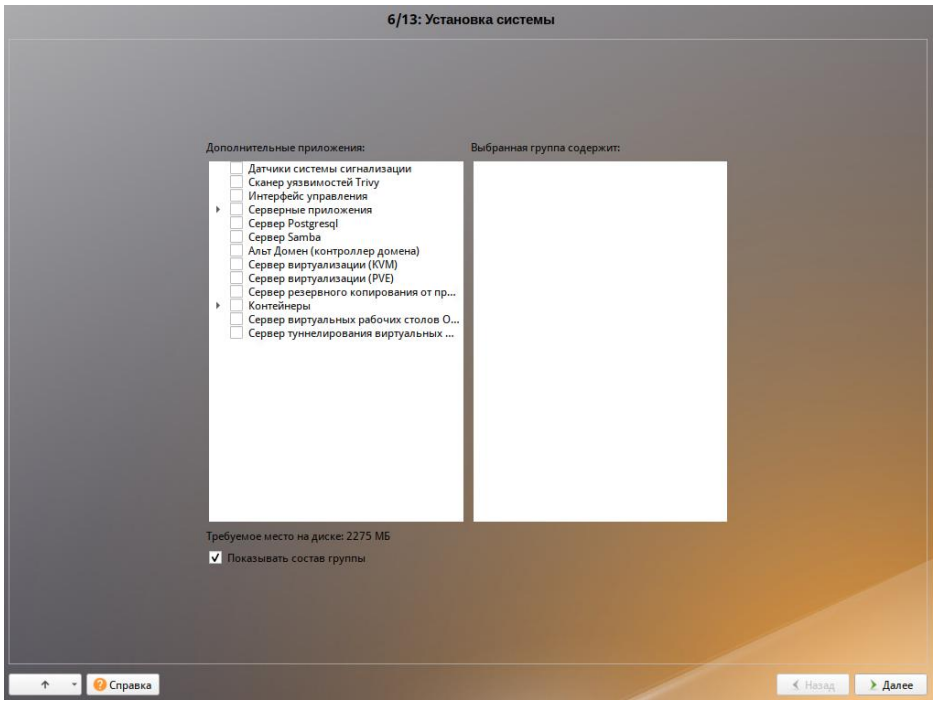


Рисунок 21 — Окно «Установка системы» (выбор дополнительных компонентов)

Дождитесь окончания установки ОС Альт Сервер.

В новом окне «Установка загрузчика» выполните следующие действия:

- убедитесь, что в поле «Устройство:» выбрано устройство «EFI (рекомендуемый)» для установки загрузчика;
- нажмите «Далее» (**Рисунок 22**).

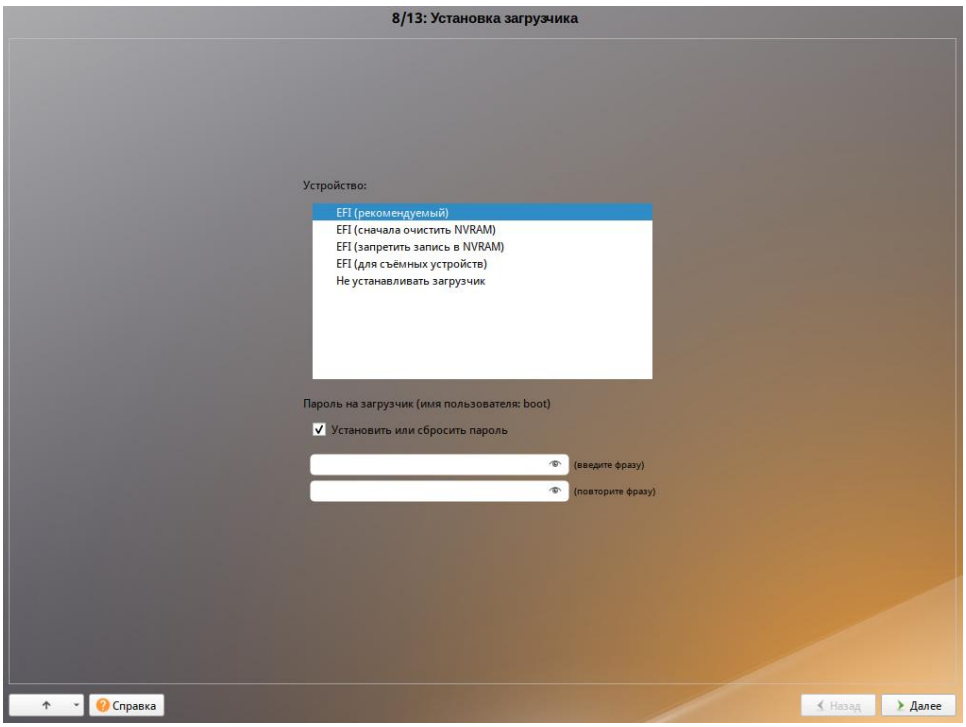


Рисунок 22 — Окно «Установка загрузчика»

Выполните настройку сетевого интерфейса управления:

- в поле «Имя компьютера»: введите сетевое имя для UDV DATAPK;
- в поле «Интерфейсы» выберите сетевой интерфейс, который будет использоваться для управления UDV DATAPK;
- в поле «Конфигурация:» выберите «Вручную»;
- в поле «IP:» введите IP-адрес интерфейса и выберите маску для интерфейса управления. Нажмите «Добавить»;
- в поле «Шлюз по умолчанию:» введите IP-адрес шлюза для интерфейса управления;
- в поле «DNS-серверы:» введите адреса DNS-серверов для интерфейса управления. Если серверов несколько, укажите их через пробел;
- нажмите «Далее» (**Рисунок 23**).

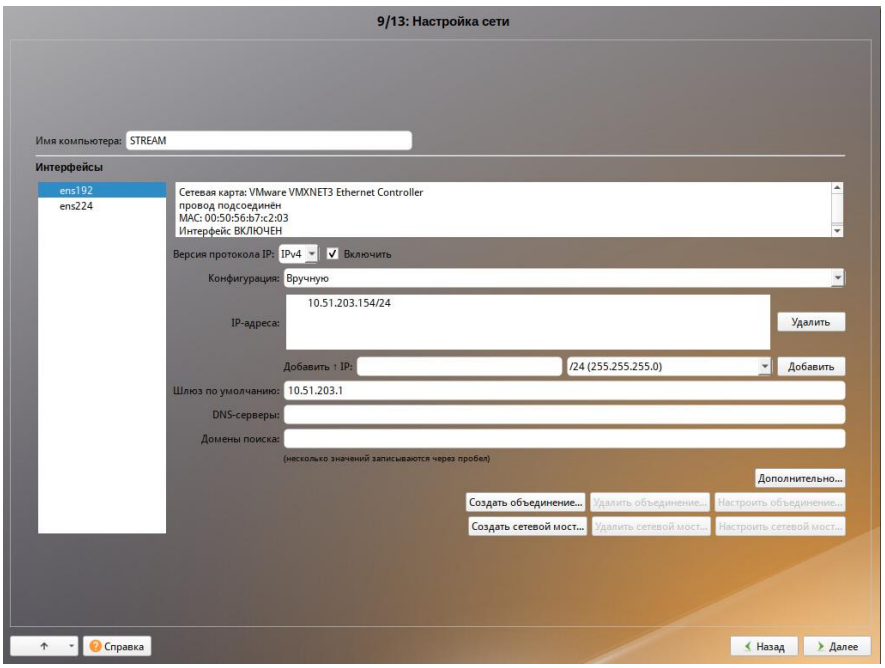


Рисунок 23 — Окно «Настройка сети»

Введите и подтвердите новый пароль администратора «root». Нажмите «Далее» (**Рисунок 24**):

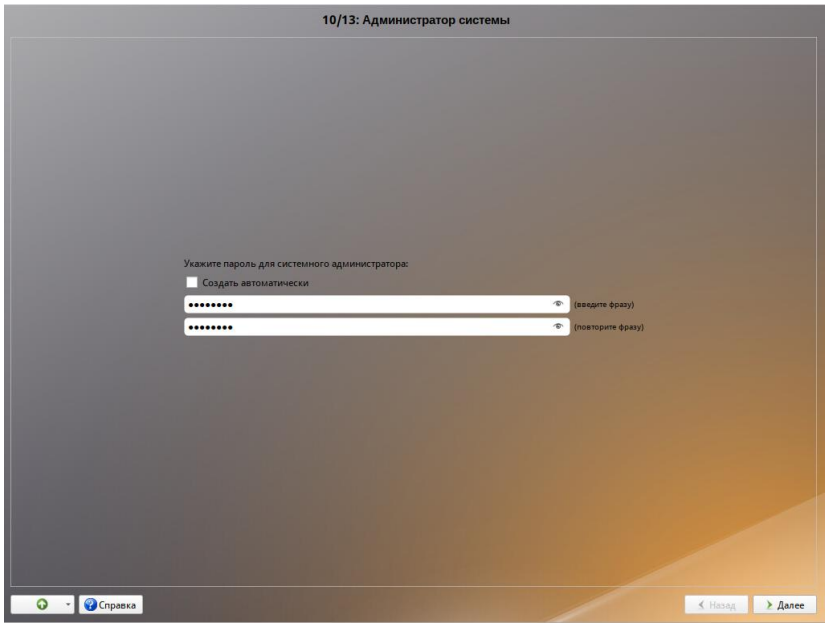


Рисунок 24 — Окно «Администратор системы»

Выполните настройку новой учетной записи пользователя с правами администратора:

- введите имя (логин) пользователя «user»;
- введите и подтвердите новый пароль пользователя;
- нажмите «Далее» (**Рисунок 25**).

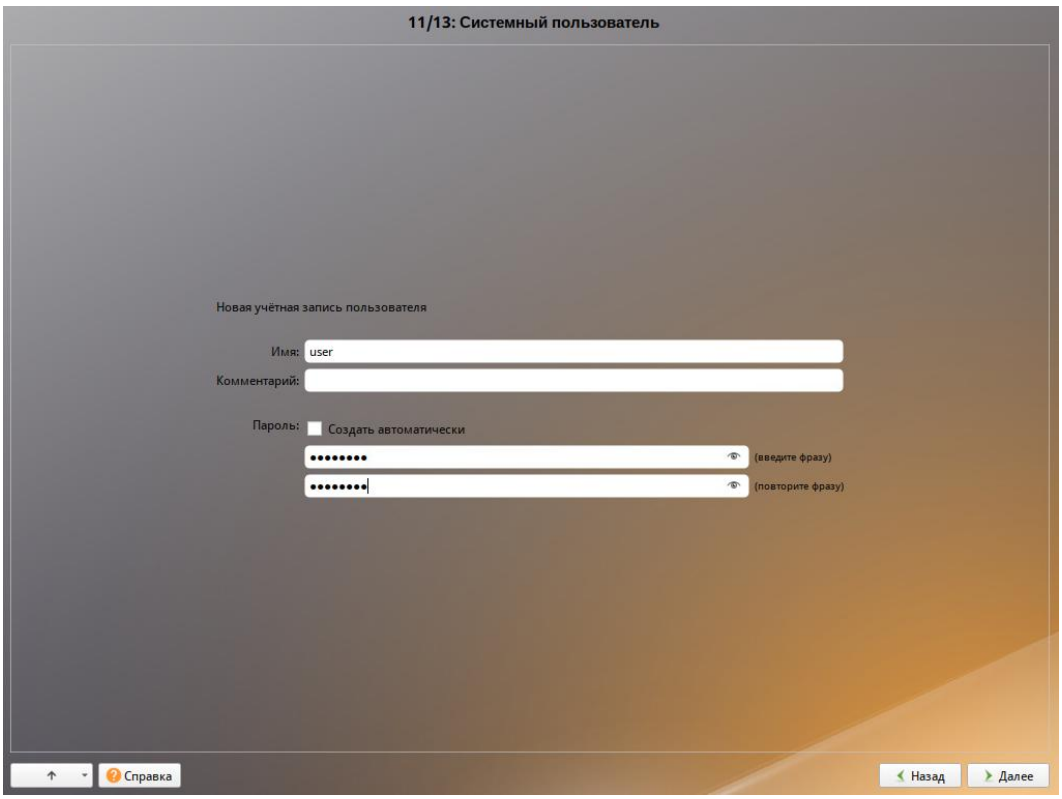


Рисунок 25 — Окно «Системный пользователь»

Нажмите «Завершить» и дождитесь перезагрузки ОС Альт Сервер.

Лабораторное задание 1.2. Настройка ОС Альт Сервер СП

Цель: сформировать умение настройки ОС Альт Сервер для последующей установки UDV DATPAK Industrial Kit.

Ход работы:

> **Примечание:**
> Процесс настройки ОС Альт Сервер СП более подробно описан в официальной документации к Комплексу.

Подключитесь к UDV DATAPK по протоколу SSH:

- откройте программу-клиент SSH и выполните подключение к Комплексу с учетной записью, созданной на этапе установки (например, «user»);
- в окне подключения введите пароль учетной записи и нажмите «Enter»;
- повысьте привилегии, выполнив команду для смены учетной записи на «root»:

```
su -
```

- введите пароль учетной записи «root» и нажмите клавишу «Enter».

> **Примечание:**
> Предполагается, что ВМ с ОС Альт Сервер СП имеет доступ к сети Интернет.

Обновите необходимое ПО и ядро ОС Альт Сервер:

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

Удалите все текущие репозитории:

```
apt-repo rm all
```

Откройте для редактирования конфигурационный файл со ссылками на репозитории и приведите его к виду (**Рисунок 26**):

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

```
altsp.list          [----]  0 L:[  1+15  16/ 16] *(865 / 865b) <EOF>
# update.altsp.su (IVK, Moscow)

# ALT Certified 10
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux c10f2/branch/x86_64 classic gostcrypto
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux c10f2/branch/x86_64-i586 classic
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux c10f2/branch/noarch classic

rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f2/branch/x86_64 classic gostcrypto
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f2/branch/x86_64-i586 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f2/branch/noarch classic

#rpm [cert8] rsync://update.altsp.su/ALTLinux c10f2/branch/x86_64 classic gostcrypto
#rpm [cert8] rsync://update.altsp.su/ALTLinux c10f2/branch/x86_64-i586 classic
#rpm [cert8] rsync://update.altsp.su/ALTLinux c10f2/branch/noarch classic
```

Рисунок 26 — Подключение репозиториев

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

Выполните обновление ПО в составе ОС Альт Сервер, а также установку дополнительного ПО:

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

Выполните перезагрузку ОС Альт Сервер:

```
shutdown -r now
```

Повторно выполните вход в ОС Альт Сервер под учетной записью «user» и повысьте привилегии до администратора.

Настройте доступ по протоколу SSH:

- откройте конфигурационный файл «sshd_config»:

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

- раскомментируйте следующие параметры, удалив символ «#»:

```
GSSAPIAuthentication no
UseDNS no
```

- Сохраните изменения в файле, нажав клавишу «F10», и подтвердите сохранение изменений, выбрав «Да» или «Yes»:
- Для применения новых настроек перезапустите службу SSH:

```
systemctl restart sshd
```

Измените настройки ядра ОС в конфигурационном файле «99-udv.conf»:

- откройте файл «99-udv.conf» для редактирования, выполнив команду:

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

- 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
```

- сохраните изменения в файле, нажав клавишу «F10», и подтвердите сохранение изменений, выбрав «Да» или «Yes».
- примените новые настройки:

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

- 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_defau
lt|net.core.rmem_max'
```

Лабораторное задание 1.3. Разметка дискового пространства

Цель: сформировать общее понимание разметки диска, в зависимости от развертываемых компонентов и модулей Комплекса.

Ход работы:

Компонент — автономная часть в составе всего решения UDV DATAPK Industrial Kit, 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 UDV DATAPK компоненты на одном предприятии необходимо настроить для взаимодействия друг с другом по сети.
UDV DATAPK содержит три компонента:

- Management;
- Sensor;
- Supervision.

Функционал Комплекса реализуется за счет его модулей, которые могут быть задействованы или отключены.

Модуль — набор функциональных возможностей в составе того или иного компонента, реализующий часть уникальных функций. Наличие модулей позволяет организациям приобретать функциональные возможности, соответствующие их потребностям. UDV DATAPK Industrial Kit включает в себя следующие 7 модулей (**Таблица 3**):

Таблица 3 – Описание модулей Комплекса

Имя	Описание
Ядро (Core)	реализует корневые функциональные возможности, такие как администрирование, REST API, управление инцидентами и другие. Необходим для функционирования любого другого модуля.
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.
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.
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.

Имя	Описание
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.
Контроль версий (Version Control)	предоставляет программистам и инженерам АСУ ТП спектр инструментов для централизованного отказоустойчивого хранения проектов ПЛК, аудита изменений в проектах ПЛК, их резервирования и восстановления, а также отслеживания неизменности программ непосредственно на ПЛК.
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.

Примечание:
Разметка дискового пространства для установки Комплекса подробно описана в официальной документации к Комплексу. В данной лабораторной работе дисковое пространство будет размечено в «необходимом минимуме», чтобы Комплекс функционировал.

В текущей лабораторной работе, будут развернуты следующие модули Комплекса:

- Core;
- iNTA;
- CM;
- VM.

Так как в составе лабораторного стенда имеется два Комплекса с разным набором компонентов и модулей, то и разметка будет производиться для каждого Комплекса отдельно.

Стенд UDV DATAPK Industrial Kit M + S

Данный Комплекс имеет IP-адрес: 10.10.10.10/24.

Так как в данной лабораторной работе специальной разметки не производится, то необходимо только создать каталоги для модулей.

Для этогоE,hf, подключитесь к Комплексу по SSH, переключитесь на учетную запись «root» и выполните последовательно следующие команды:

```
mkdir -p /var/lib/rabbitmq
mkdir -p /var/lib/clickhouse
mkdir -p /var/backups
mkdir -p /var/lib/opensearch
mkdir -p /usr/share/udv/zeek-wrapper/extracted_files
mkdir -p /var/cache/udv/stenographer
```

Стенд UDV DATAPK Industrial Kit S

Данный Комплекс имеет IP-адрес: 10.10.10.11/24.

Так как в данной лабораторной работе специальной разметки не производится, то необходимо только создать каталоги для модулей.

Для этого, подключитесь к Комплексу по SSH, переключитесь на учетную запись «root» и выполните последовательно следующие команды:

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

Лабораторное задание 1.4. Подключение репозиториев и установка модулей комплекса

Цель: сформировать умение установки модулей Комплекса из подключаемых репозиториев.

Ход работы:

Для развертывания Комплекса требуется архив с пакетами для установки, существует несколько типа архивов:

- **release-[версия_Комплекса]_[дата_архива].tar.gz** — компоненты «Sensor» и «Management», модули «Core», «Анализ промышленного сетевого трафика», «Управление проектами ПЛК», «Управление конфигурациями», «Управление уязвимостями»;
- **release-[версия_Комплекса]-external-modules_[дата_архива].tar.gz** — модуль «Управление внешними событиями», сервис «Supervision backend», сервисом «Swagger UI» для уровня «Management»;
- **agentless_edr-[версия_Комплекса]_[дата_архива].tar.gz** — модуль «EDR for PLC»;
- **sv-release-[версия_Комплекса]_[дата_архива].tar.gz** — компонент «Supervision».

Примечание:
Действия ниже выполняются на обоих Комплексах, по очереди или одновременно.

С помощью ПО WinSCP скопируйте с хостовой ОС в директорию «/home/user» на Комплексе следующие файлы:

- **release-[версия_Комплекса]_[дата_архива].tar.gz**;
- **release-[версия_Комплекса]-external-modules_[дата_архива].tar.gz.**

Выполните вход в ОС Альт Сервер учетной записью «user» и повысьте привилегии до администратора:

```
su -
```

Распакуйте архивы, выполнив по очереди 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
```

Просмотрите получившийся список директорий внутри директории «/var/opt/[версия_Комплекса]», выполнив команду:

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

Создайте конфигурационный файл «/etc/apt/sources.list.d/udv.list» репозитория:

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

Содержимое файла «/etc/apt/sources.list.d/udv.list»:

```
#nta
rpm file:/var/opt/release-3.0/nta noarch classic
rpm file:/var/opt/release-3.0/nta x86_64 classic
#ours
rpm file:/var/opt/release-3.0/ours noarch classic
rpm file:/var/opt/release-3.0/ours x86_64 classic
#tools
rpm file:/var/opt/release-3.0/tools noarch classic
rpm file:/var/opt/release-3.0/tools x86_64 classic
#third
rpm file:/var/opt/release-3.0/third noarch classic
rpm file:/var/opt/release-3.0/third x86 64 classic
```

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

Обновите репозитории, выполнив команду:

```
apt-get update
```

В зависимости от настраиваемого Комплекса, выполните команду установки модулей:

- стенд UDV DATAPK Industrial Kit M + S (IP-адрес: 10.10.10.10/24):

```
apt-get install udv-datapk udv-datapk-sensor udv-datapk-dpi udv-datapk-dpi-sensor udv-datapk-configuration-management udv-datapk-vulnerability-management -y
```

- стенд UDV DATAPK Industrial Kit S (IP-адрес: 10.10.10.11/24):

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

После завершения установки, выполните настройку установленных модулей, в зависимости от настраиваемого Комплекса:

- стенд UDV DATAPK Industrial Kit M + S (IP-адрес: 10.10.10.10/24):

  Откройте для редактирования файл «/usr/share/udv/datapk/manager.env» и укажите IP-адрес Комплекса в переменную **HOST_IP**:

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

  Откройте для редактирования файл «/usr/share/udv/datapk/sensor.env» и укажите IP-адрес **127.0.0.1** в переменную **MANAGER_NODE_ADDRESS**:

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

- стенд UDV DATAPK Industrial Kit S (IP-адрес: 10.10.10.11/24):

  Откройте для редактирования файл «/usr/share/udv/datapk/sensor.env» и укажите IP-адрес сервера управления (10.10.10.10) в переменную **MANAGER_NODE_ADDRESS**:

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

  Выполните настройку сетевых интерфейсов в зависимости от настраиваемого Комплекса:

- стенд UDV DATAPK Industrial Kit M + S (IP-адрес: 10.10.10.10/24):

  Для проигрывания сетевого трафика, настройте сетевой интерфейс:

```
mkdir /etc/net/ifaces/dummy0
```

  Откройте для редактирования файл «/etc/net/ifaces/dummy0/iplink»:

```
mcedit /etc/net/ifaces/dummy0/iplink
```

  Заполните файл «/etc/net/ifaces/dummy0/iplink» следующим содержимым, затем сохраните и закройте его:

```
promisc on
arp on
up
mtu 9000
```

  Выполните перезапуск службы сети для применения настроек:

```
systemctl restart network
```

  Укажите созданный сетевой интерфейс «dummy0» в качестве интерфейса для прослушивания сетевого трафика, откройте для редактирования файл «/usr/share/udv/datapk/sensor.env»:

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

  В переменной «LISTENING_INTERFACES» укажите значение «dummy0». Сохраните и закройте файл.

- стенд UDV DATAPK Industrial Kit S (IP-адрес: 10.10.10.11/24):

  Проверьте список сетевых интерфейсов командой:

```
ip a
```

  Уточните наименование интерфейсов для прослушивания сетевого трафика, в зависимости от количества сетевых интерфейсов, на которые была подана копия сетевого трафика. В

Примечание:
Если планируется подключать более одного сетевого интерфейса с копией трафика к Комплексу, то их **необходимо** объединить в один (bond), иначе, корректное получение копии сетевого трафика невозможно.
Процесс объединения нескольких физических сетевых интерфейсов в один логический описан в соответствующем разделе официальной документации к

лабораторной работе предполагается наличие одного сетевого интерфейса с копией сетевого трафика, например «ens224».

Создайте каталог с конфигурационными файлами для сетевого интерфейса «ens224»:

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

Скопируйте в созданную директорию «ens224» конфигурационный файл «options» уже существующего сетевого интерфейса управления (например, «ens192»), настроенного при установке ОС:

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

Создайте новый файл «iplink» и добавьте в него команду переключения интерфейса в режим прослушивания всех пакетов (promisc):

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

Перезагрузите сетевой сервис:

```
systemctl restart network
```

Укажите созданный сетевой интерфейс «dummy0» в качестве интерфейса для прослушивания сетевого трафика, откройте для редактирования файл «/usr/share/udv/datapk/sensor.env»:

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

В переменной «LISTENING_INTERFACES» укажите значение «ens224». Сохраните и закройте файл.

Внимание! Переменная «LISTENING_INTERFACES» принимает в качестве значение только один сетевой интерфейс.

Лабораторная работа 2. Настройка подсистемы инвентаризации

Разделы документации

- Обнаружение новых объектов защиты;
- Обнаружение новых потоков IPv4;
- Управление активами;
- Группировка активов;
- Анализ промышленного сетевого трафика.

Справочная информация

Актив – сетевой узел, подлежащий защите от потенциальных угроз и неправомерных действий, например, несанкционированного доступа и изменения данных третьими лицами.

Классификатор — сгруппированный, по различным признакам, перечень наименованных объектов, где каждому из них присвоен уникальный код, в соответствии с их общими признаками или различиями.

Контролируемая сеть – совокупность IPv4-подсетей, которые контролирует UDV DATAPK. Контролируемая сеть влияет на:

- обнаружение новых объектов защиты;
- обнаружение новых потоков IPv4;
- отображение результатов сканирования сети.

При задании контролируемой сети активируется автоматического обнаружения хостов - на каждое уникальное сетевое соединения (IP+MAC), полученное сенсором, будет создан актив, если актив с этой связкой адресов существует, то будет обновлена его активность.

Сессия — зарегистрированное взаимодействие между двумя узлами сети.

Режим обучения — режим работы правил сессий, при котором правила будут создаваться автоматически для всех обнаруженных сессий, такие сессии будут иметь статус «Не определен».

Для переключения режима необходимо перейти в раздел «Сенсоры», выбрать сенсор и в появившемся окне переключить «Автоматическое создание правил сессий» (режим обучения соответствует включенному переключателю).

- правила применяются только для новых сессий;
- по умолчанию правила генерируются автоматически;
- если поток попал под правило, на следующие правила не проверяется.
- если поток не попал под правило и выключен режим обучения, то будет сгенерировано событие с типом - **session_control**

Для управления сессиями в интерфейсе Комплекса предусмотрены соответствующие правила. Они позволяют задать необходимые параметры для автоматических действий по отношению к соединениям.

Файлы для лабораторных работ

- **ECI_метки.json** — файл с метками для Комплекса;
- **rules_datapk_IDS-3-0.json** — пачка правил обнаружения вторжений;
- **test+eicar.rules** — правила в формате Suricata для выполнения лабораторной работы;
- **only_eicar.pcap** — дамп сетевого трафика для выполнения лабораторной работы;
- **tags.pcap** — дамп сетевого трафика для выполнения лабораторной работы.

Лабораторное задание 2.1. Ведение классификаторов и групп активов

Цель: сформировать умение работы с классификаторами и группами активов.

Ход работы:

Актив – сетевой узел, подлежащий защите от потенциальных угроз и неправомерных действий, например, несанкционированного доступа и изменения данных третьими лицами.

Классификатор — сгруппированный, по различным признакам, перечень наименованных объектов, где каждому из них присвоен уникальный код, в соответствии с их общими признаками или различиями.

Перейдите в подраздел управления «Администрирование» → «Настройка активов» → «Классификаторы» (**Рисунок 27**).

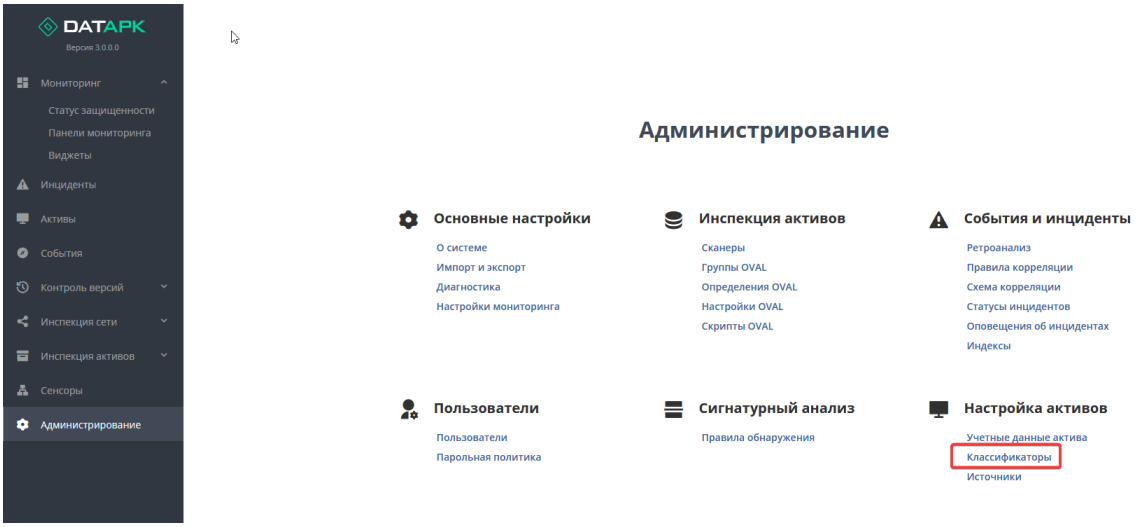


Рисунок 27 — Путь к разделу «Классификаторы»

Просмотрите встроенные в Комплекс классификаторы АСУ ТП и Метки (**Рисунок 28**), которые будут применяться в дальнейшем для классификации активов при их создании и редактировании, а также в фильтрации активов.

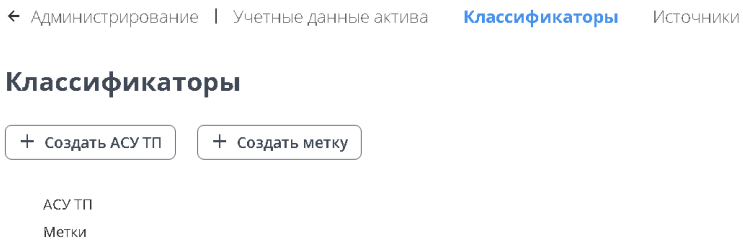


Рисунок 28 — Предустановленные классификаторы

Информация о классификаторах приведена в таблице (**Таблица 4**).

Таблица 4 – Классификаторы Комплекса

Классификатор	**Характеристика классификатора**	**Отношение к активам**
АСУ ТП	предустановленный редактируемый классификатор	необязательный атрибут классификации актива

Классификатор	Характеристика классификатора	Отношение к активам
Операционные системы, распознанные Комплексом	предустановленный, автоматически дополняемый нередактируемый классификатор	необязательный атрибут классификации активов; присваивается активам с ОС семейства Windows автоматически (при возможности получения информации от актива по протоколу «Microsoft Windows Browser Protocol»)
OVAL	Редактируемый классификатор	необязательный атрибут классификации активов
Комплекс	предустановленный, автоматически дополняемый с добавлением Комплексов нередактируемый классификатор	обязательный атрибут классификации активов, появляется при наличии иерархии Комплексов
Производители	предустановленный нередактируемый классификатор	обязательный атрибут классификации активов
Активы	предустановленный, автоматически дополняемый с добавлением актива нередактируемый классификатор	обязательный атрибут классификации активов
Типы активов	предустановленный нередактируемый классификатор	обязательный атрибут классификации активов
Метки	редактируемый классификатор	необязательный атрибут классификации активов

Создайте классификатор активов АСУ ТП цеха 1. Для этого:

Нажмите кнопку «Создать АСУ ТП».

В появившемся окне «Создание АСУ ТП» введите следующие параметры:

в поле «Наименование» введите название группы — «АСУ ТП цеха 1»;

в списке «Вышестоящая АСУ ТП» выберите «АСУ ТП».

Нажмите кнопку «Сохранить» (**Рисунок 29**).

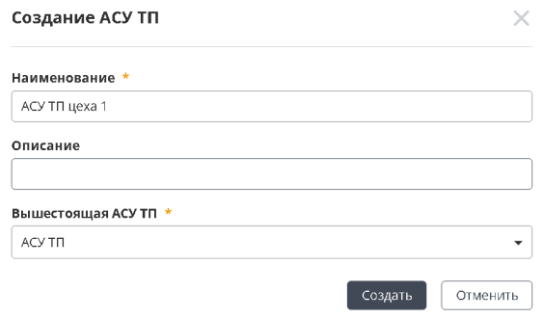


Рисунок 29 — Окно создания новой АСУ ТП

Просмотрите полученный классификатор АСУ ТП.

На панели фильтров в поле «Справочники» оставьте только «АСУ ТП», остальные удалите.

Нажмите кнопку «Применить» (**Рисунок 30**).

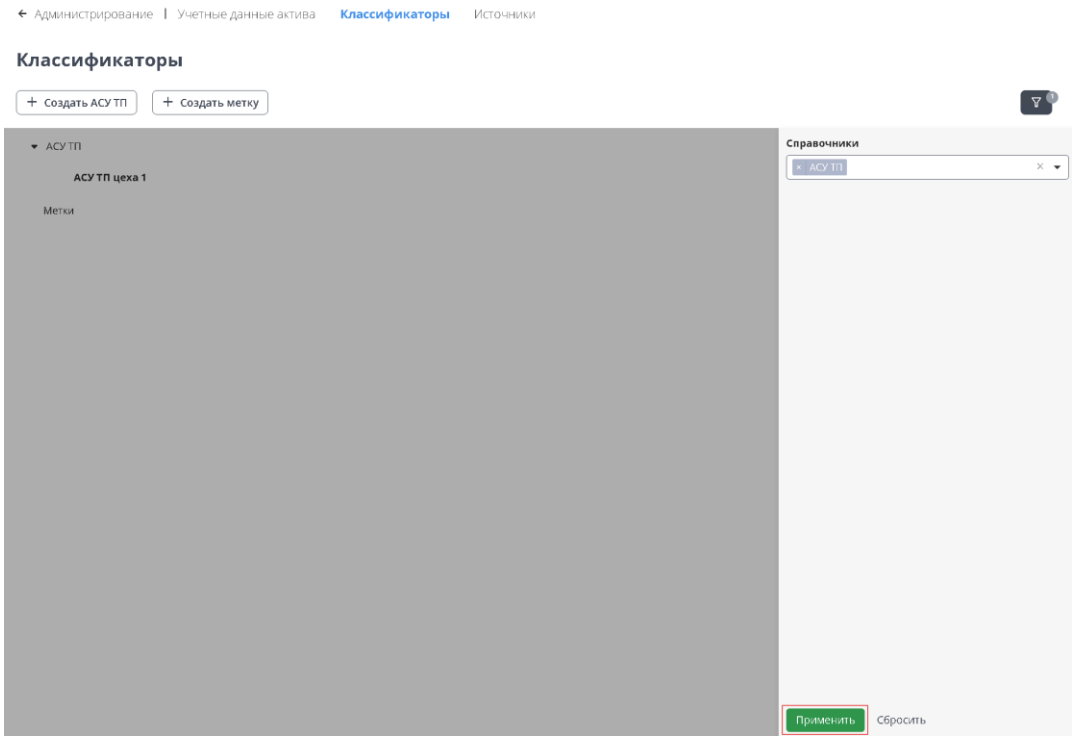


Рисунок 30 — Просмотр справочника АСУ ТП

Убедитесь в возможности дальнейшего использования созданного справочника АСУ ТП при навигации по списку активов. Для этого:

Перейдите в раздел «Активы».

На панели фильтров разверните список классификаторов «АСУ ТП». В списке должны отображаться названия созданных АСУ ТП (**Рисунок 31**).

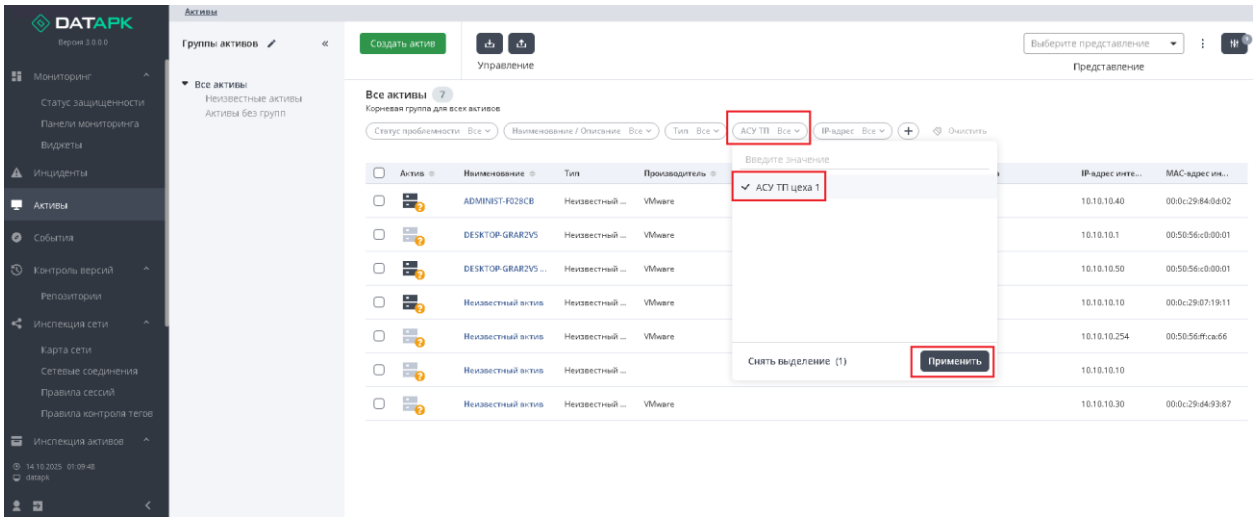


Рисунок 31 — Классификатор АСУ ТП в разделе «Активы»

Загрузите метки операционных систем для активов. Для этого:

Перейдите на страницу «Администрирование» → «Импорт и экспорт».

В блоке «Элементы иерархии» строке «Иерархии меток активов» нажмите (**Рисунок 32**).

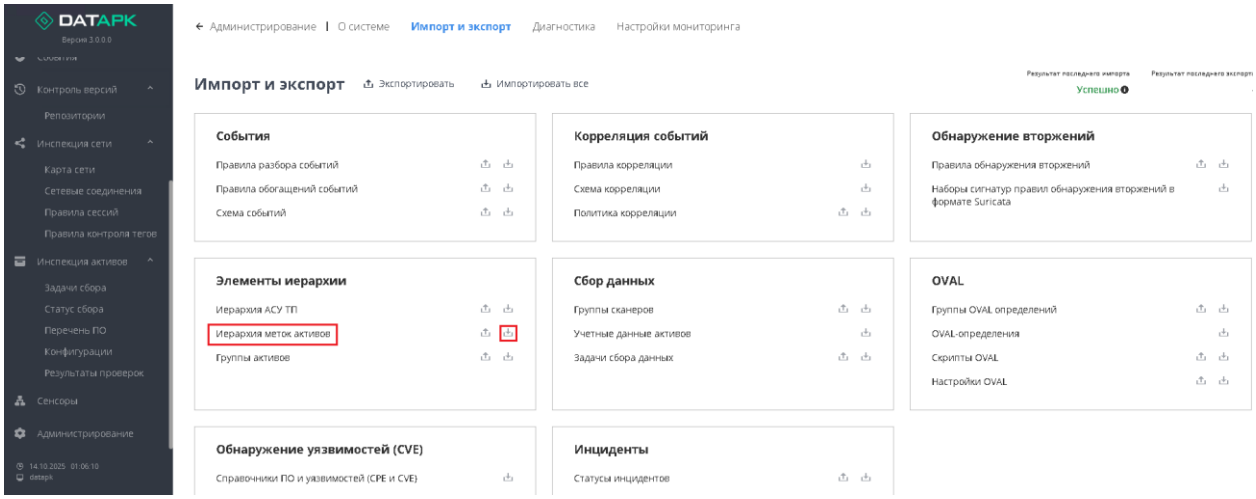


Рисунок 32 — Страница «Обмен»

Выберите файл **ECI_метки.json** и нажмите «Открыть».

В открывшемся окне нажмите «Импортировать» (**Рисунок 33**).

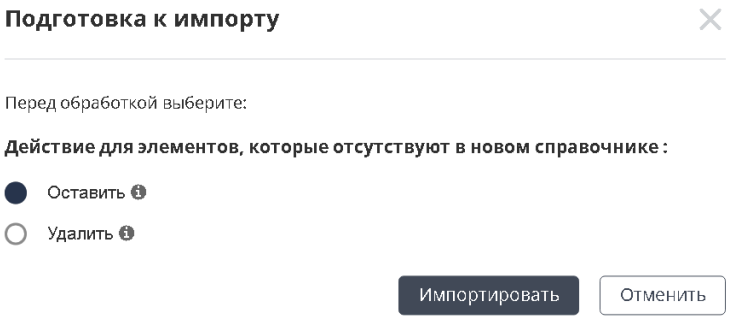


Рисунок 33 — Импорт меток ECI

Убедитесь в том, что метки операционных систем был импортированы. Для этого:

Перейдите на страницу «Администрирование» → «Классификаторы».

На панели фильтров выберите «Метки».

Убедитесь в наличии импортированных ранее меток (**Рисунок 34**).

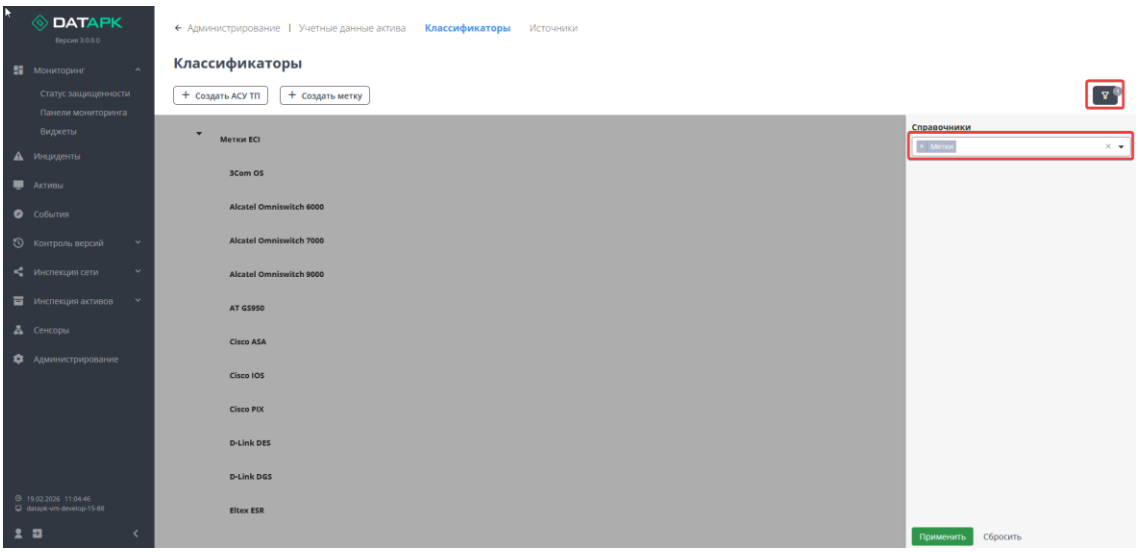


Рисунок 34 — Метки операционных систем на странице «Классификаторы»

Создайте собственный классификатор с двумя метками. Для этого:

Нажмите «Создать метку».

Задайте следующие параметры (**Рисунок 35**) создаваемому классификатору:

Наименование — Режим работы.

Родительская группа — Метки.

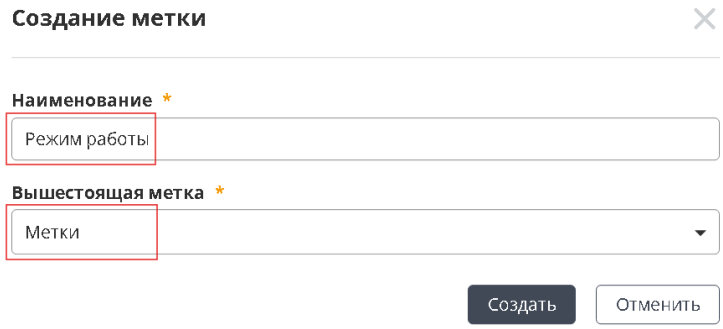


Рисунок 35 — Создание классификатора «Режим работы»

Создайте две метки, дочерние классификатору «Режим работы» — «Непрерывный» и «Сменный». Для этого в окне создания элемента классификатора (**Рисунок 36**) задайте «Режим работы» в поле «Вышестоящая метка».

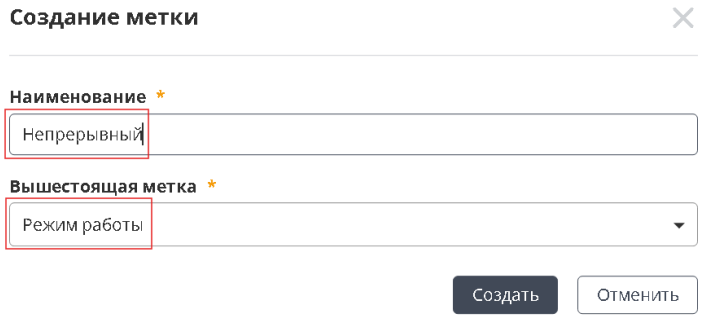


Рисунок 36 — Создание элемента классификатора «Режим работы»

Результат шага: появится классификатор типа «Метки» с названием «Режим работы» и двумя нижестоящими элементами: «Сменный» и «Непрерывный» (**Рисунок 37**).

Рисунок 37 — Элементы классификатора «Режим работы»

Лабораторное задание 2.2. Создание актива

Цель: сформировать умение создания актива в ручном режиме.

Ход работы:

Создайте новый актив «АРМ АСУ ТП цеха 1» в ручном режиме. Для этого:

Перейдите в раздел «Активы».

Нажмите на панели инструментов кнопку «Создать актив» (**Рисунок 38**).

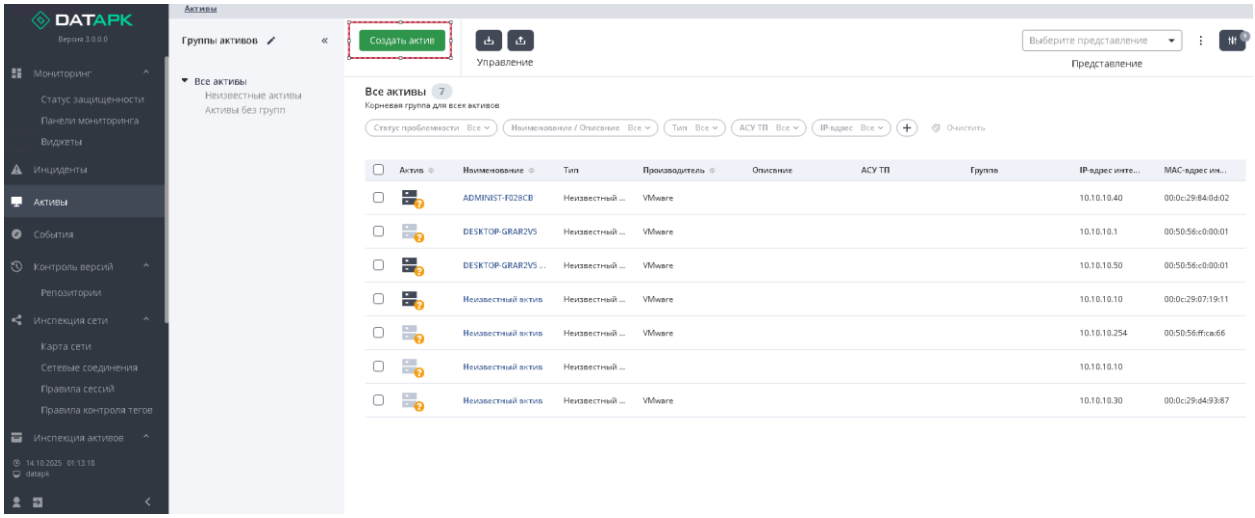


Рисунок 38 – Создание нового актива в разделе «Активы»

В открывшемся окне введите параметры для создаваемого актива в следующем порядке:

- в поле «Тип» выберите из списка тип «АРМ»;
- в поле «Наименование» введите наименование актива: «АРМ оператора АСУ ТП цеха 1»;
- в поле «АСУ ТП» отметьте параметр «АСУ ТП цеха 1».

Нажмите кнопку «Создать» (**Рисунок 39**).

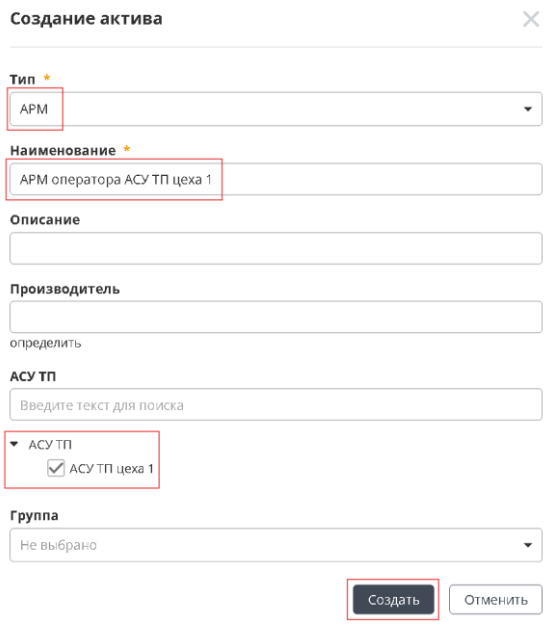


Рисунок 39— Окно создания нового актива

Результат шага: откроется окно с карточкой актива.

Назначьте активу новую метку, которая будет классифицировать актив по виду операционной системы. Для этого:

- Создайте собственный справочник операционных систем
- Перейдите в подраздел «Администрирование» → «Классификаторы».
- Нажмите кнопку «Создать метку».

Результат шага: появится окно создания метки.

Задайте следующие параметры создаваемой метке (**Рисунок 40**):

- Вышестоящая метка — «Метки».
- Наименование — ОС.

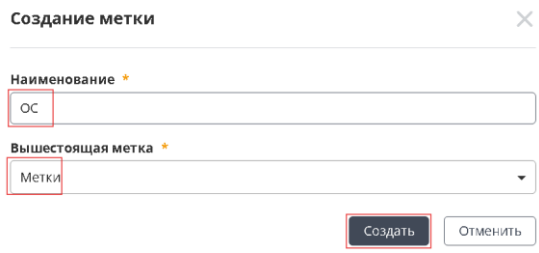


Рисунок 40 — Создание собственной метки с операционными системами

Создайте метку «Windows 10» с вышестоящей меткой «ОС». Для этого в окне создания метки задайте следующие параметры (**Рисунок 41**):

- Вышестоящая метка — ОС.
- Наименование — Windows 10.

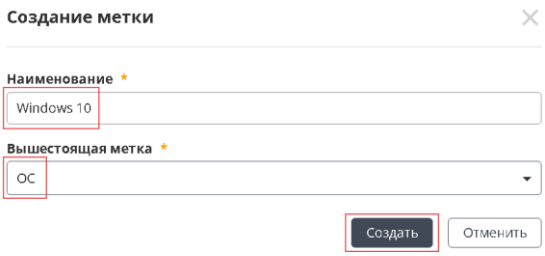


Рисунок 41 — Создание метки «Windows 10»

Присвойте созданную метку активу АСУ ТП цеха 1. Для этого:

На вкладке «Метки» карточки актива нажмите кнопку «Редактировать», **Рисунок 42**.

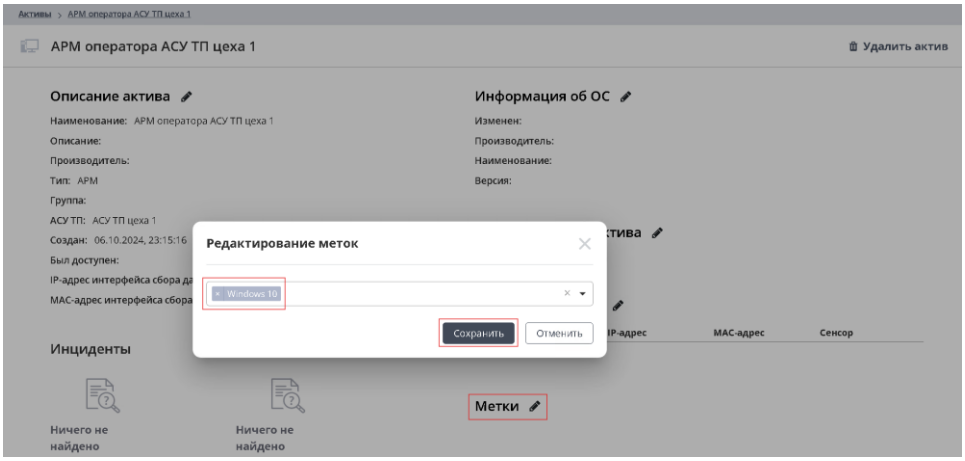


Рисунок 42 — Вкладка «Метки» на странице настройки актива

В открывшемся окне «Редактирование меток» выберите из списка метку «Windows 10» и нажмите кнопку «Сохранить» (**Рисунок 43**).

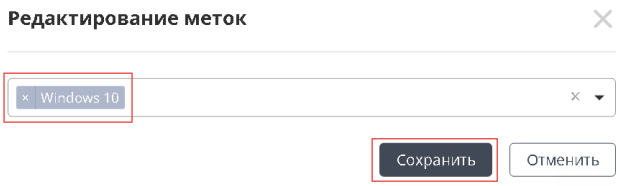


Рисунок 43 — Окно добавления групп и меток активу

Самостоятельное задание. Присвойте активу метку «Непрерывный» [Режим работы].

Назначьте активу сетевые атрибуты.

В карточке актива в разделе «Сетевые атрибуты» нажмите кнопку «✎», **Рисунок 44**.

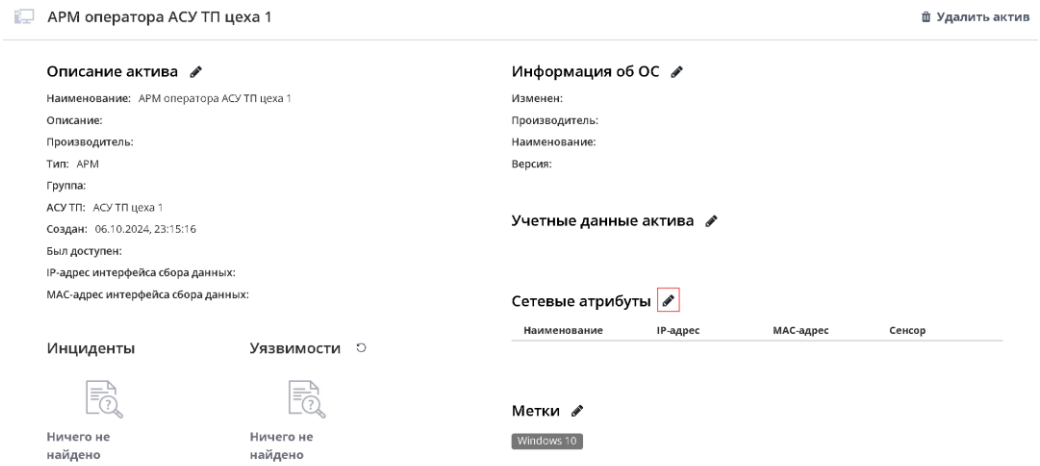


Рисунок 44 — Раздел «Сетевые атрибуты»

В открывшемся окне «Редактирование сетевых атрибутов актива» введите в соответствующие поля IP-адрес и MAC-адрес интерфейса «АРМ АСУ ТП цеха 1» (в соответствии с **Таблица 1**).

Нажмите кнопку «+» («Создать интерфейс», **Рисунок 45**).

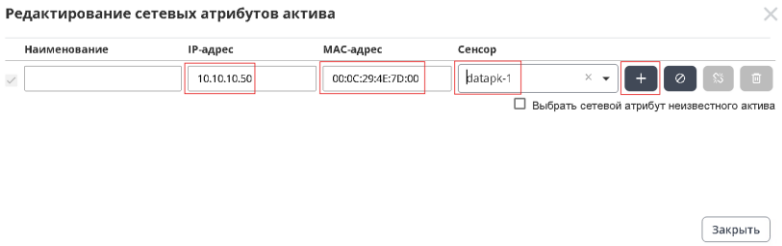


Рисунок 45 — Окно редактирования сетевых атрибутов актива

Внимание!

В поле «Сенсор» выбирается Комплекс уровня Sensor, который будет осуществлять активный сбор с данного актива. Важно указывать корректный Sensor, чтобы не возникало ошибок в ходе сбора данных с активов. Это возможно в ситуации, когда к Management подключено 2 и более Комплексов Sensor (**Рисунок 46**).

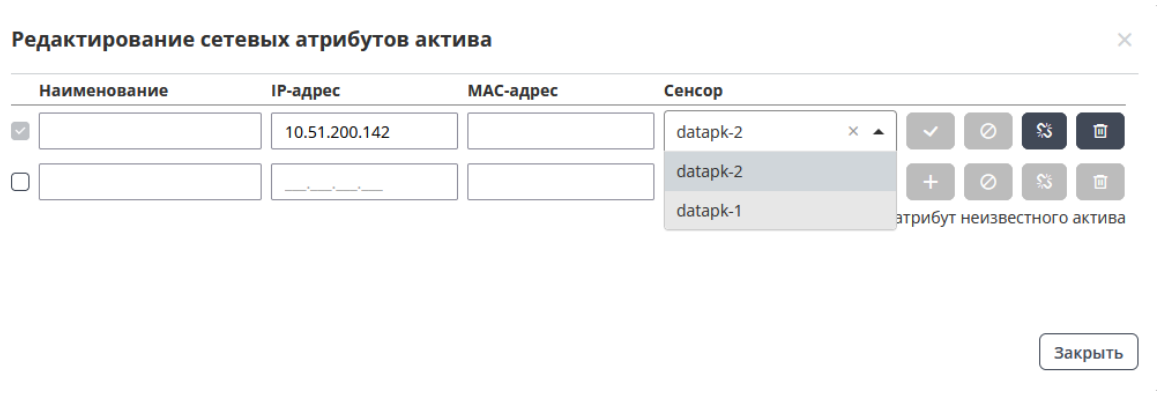


Рисунок 46 — Выбор Комплекса уровня Сенсор

Лабораторное задание 2.3. Сканирование сети

Цель: сформировать навык сканирования контролируемой сети.

Ход работы:

Контролируемая сеть – совокупность IPv4-подсетей, которые контролирует UDV DATAPK. Контролируемая сеть влияет на:

- обнаружение новых объектов защиты;
- обнаружение новых потоков IPv4;
- отображение результатов сканирования сети.

При задании контролируемой сети активируется автоматического обнаружения хостов - на каждое уникальное сетевое соединения (IP+MAC), полученное сенсором, будет создан актив, если актив с этой связкой адресов существует, то будет обновлена его активность.

Для автоматизации привязки интерфейсов с MAC-адресом маршрутизирующего устройства к существующим активам в DATAPK реализован следующий алгоритм:

1. Обнаружен новый узел с IP-адресом существующего актива (в т.ч. неизвестного);
2. MAC-адрес этого узла совпадает с MAC-адресом одного из интерфейсов коммутатора, маршрутизатора, или сетевого средства защиты, уже заведенного в DATAPK;
3. Тогда интерфейс добавляется существующему активу с пометкой with_router_mac и формированием соответствующего события (***Рисунок 47***).

Рисунок 47 — Пример привязки интерфейса

Задайте контролируемую сеть:

Откройте веб-интерфейс DATAPK.

Перейдите в подраздел управления «Сенсоры» нажмите на datapk-1.

В разделе «Контролируемая сеть» добавьте две сети - 10.10.10.0/24 и 192.168.0.0/16, нажав «Добавить сеть», затем нажать «Применить» и согласиться с изменением сети (***Рисунок 48***). Повторите для каждого сенсора.

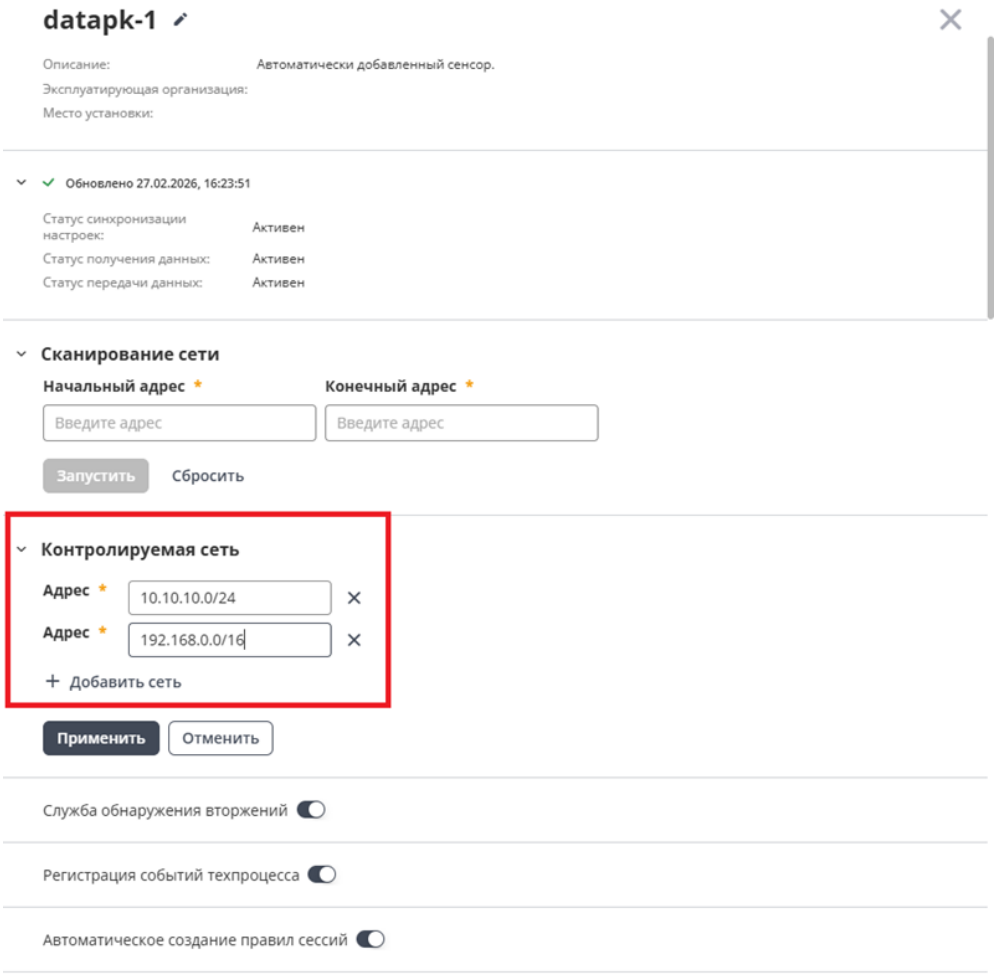


Рисунок 48 — Панель «Контролируемая сеть» в настройках сенсора

Выполните сканирование сети:

Откройте веб-интерфейс DATAPK.

Перейдите в подраздел управления «Сенсоры» нажмите на datapk-1.

В разделе «Сканирование сети» настройте следующие параметры: в полях «Начальный адрес сканирования» и «Конечный адрес сканирования» введите начальный и конечный IP адрес из диапазона IP-адресов, которые необходимо просканировать (**Рисунок 49**).

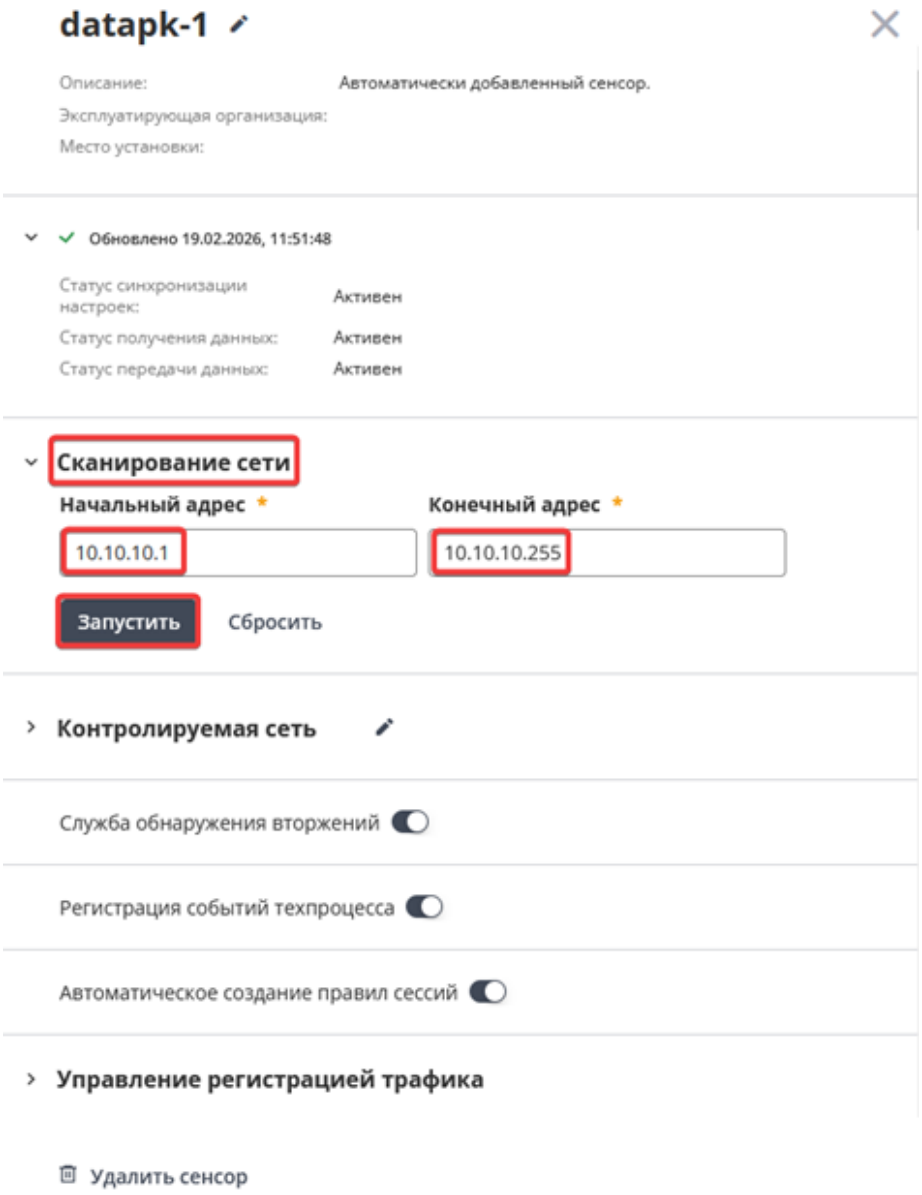


Рисунок 49 — Панель «Сканирование сети» в настройках сенсора

Нажмите кнопку «Запустить» для запуска сканирования сети.

Примечание:
При уменьшении количества IP-адресов, входящих в контролируемую сеть (при изменении сети в меньшую сторону), активы с типом «Неизвестный тип», IP-адреса которых больше не входят в нее, будут удалены из списка активов (даже при наличии сетевого имени).

Лабораторное задание 2.4. Редактирование реквизитов актива

Цель: сформировать умение редактирования реквизитов активов.

Ход работы:

Перейдите на страницу «Активы».

Найдите в списке актив со знаком вопроса (неизвестный актив), IP-адрес которого совпадает с IP-адресом ВМ «ПЛК АСУ ТП цеха 1» (**Рисунок 50**).

Перейдите в карточку данного актива.

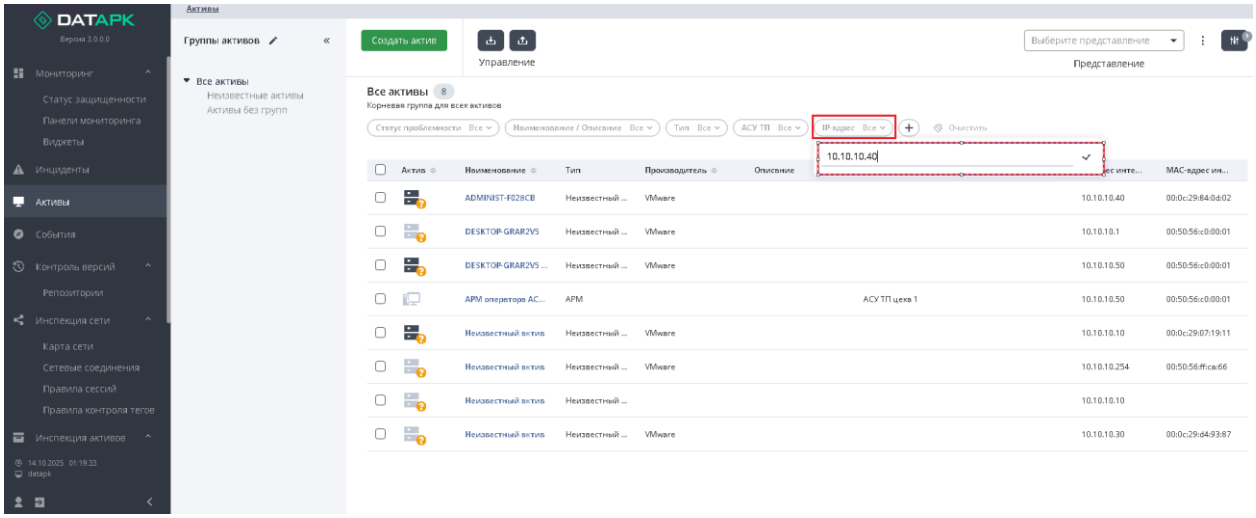


Рисунок 50 — Актив с IP-адресом ВМ «ПЛК АСУ ТП цеха 1»

Отредактируйте реквизиты этого актива. Для этого:

Нажмите на кнопку «✎» для редактирования описания выбранного актива (**Рисунок 51**).

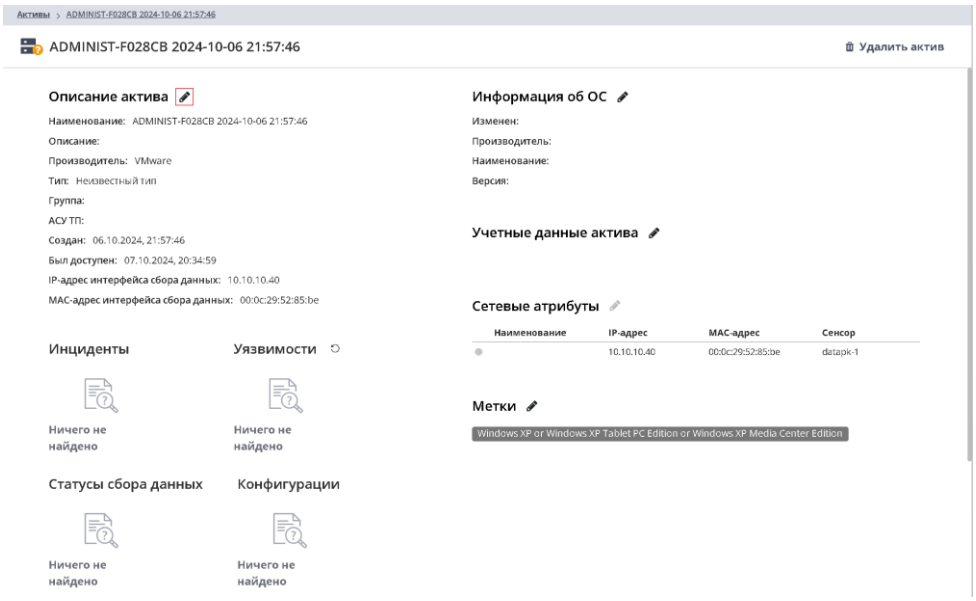


Рисунок 51 — Кнопка редактировать «Описание актива» на карточке актива

В открывшемся окне измените параметры актива в следующем порядке:

в списке «Тип» выберите тип «ПЛК»;

в поле «Наименование» введите наименование актива: «ПЛК АСУ ТП цеха 1»;

в поле «АСУ ТП» отметьте параметр «АСУ ТП цеха 1».

Нажмите кнопку «Сохранить» (**Рисунок 52**).

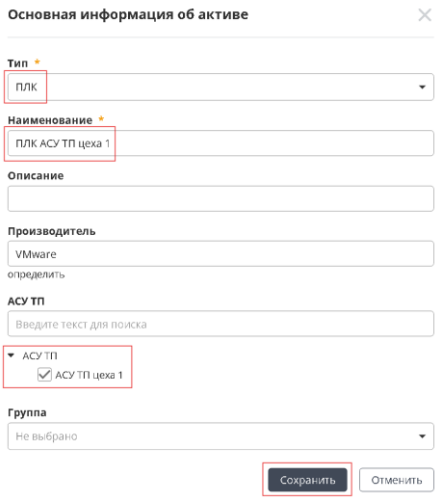


Рисунок 52 — Окно редактирования описания актива

Найдите актив с ip-адресом совпадающим с ip-адресом комплекса datapk согласно схеме (**Рисунок 53**).

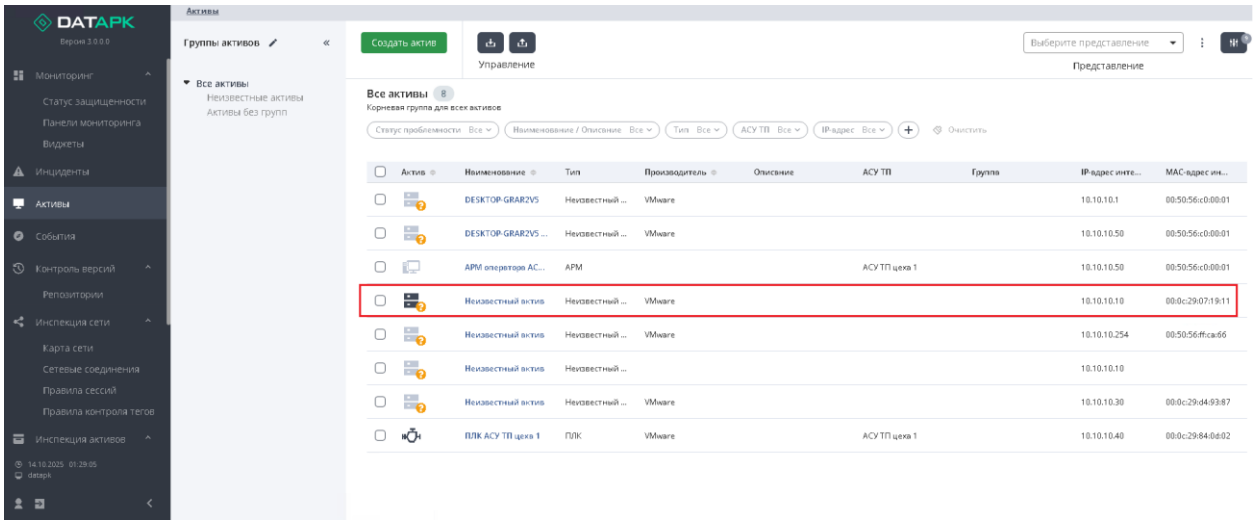


Рисунок 53 — Поиск нужного актива

В разделе «Описание актива» нажмите кнопку « ».

Измените тип актива на «Комплекс»;

в поле «АСУ ТП» отметьте параметр «АСУ ТП цеха 1» (**Рисунок 54**).

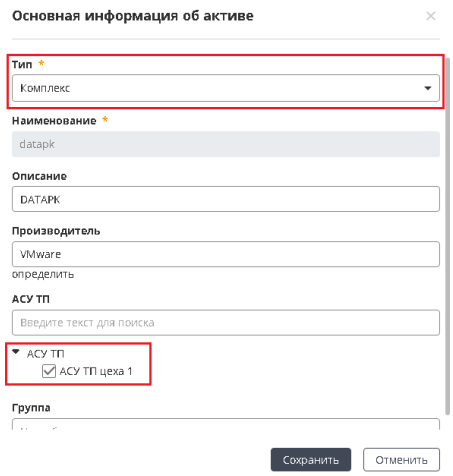


Рисунок 54 — Окно редактирования информации об активе

Создайте актив «Коммутатор АСУ ТП цеха 1».

Для этого на вкладке «Активы» нажмите «Создать актив» и заполните поля следующим образом:

Тип: «Коммутатор»;

Наименование: «Коммутатор АСУ ТП цеха 1»;

в поле «АСУ ТП» отметьте параметр «АСУ ТП цеха 1» (**Рисунок 55**).

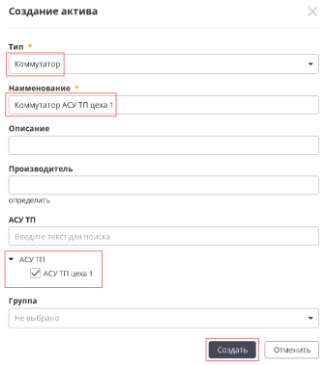


Рисунок 55 — Настройки коммутатора

В разделе «Сетевые атрибуты» нажмите кнопку « ».

В открывшемся окне «Сетевые атрибуты актива» отметьте параметр «Выбрать интерфейс неизвестного актива».

> **Примечание:**
> Если несколько сенсоров видят один и тот же интерфейс, то на уровне Management можно в актив добавить несколько таких интерфейсов

В поле «IP-адрес» выберите из списка IP-адрес Коммутатора согласно схеме стенда.

Нажмите кнопку «» («Создать интерфейс», **Рисунок 56**).

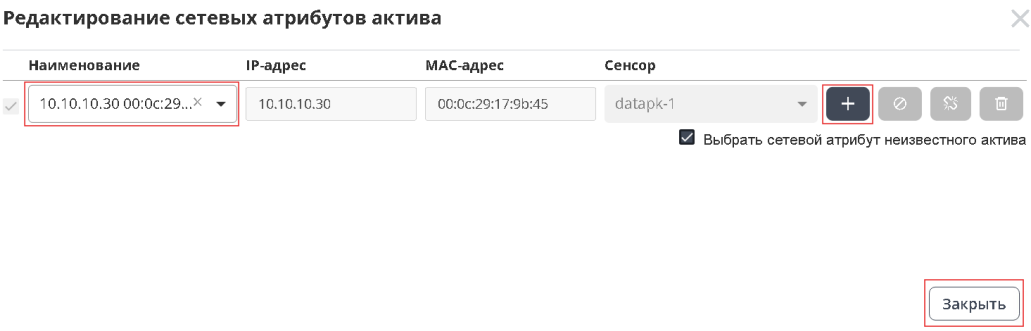


Рисунок 56 — Настройка сетевых атрибутов для служебного актива «DATAPK»

Настройте работу со списком активов. Для этого:

Перейдите в раздел «Активы».

Измените количество отображаемых столбцов списка активов.

Отметьте параметр «Дата создания» в правом верхнем углу.

Отмените параметр «Описание», посмотрите результат (**Рисунок 57**).

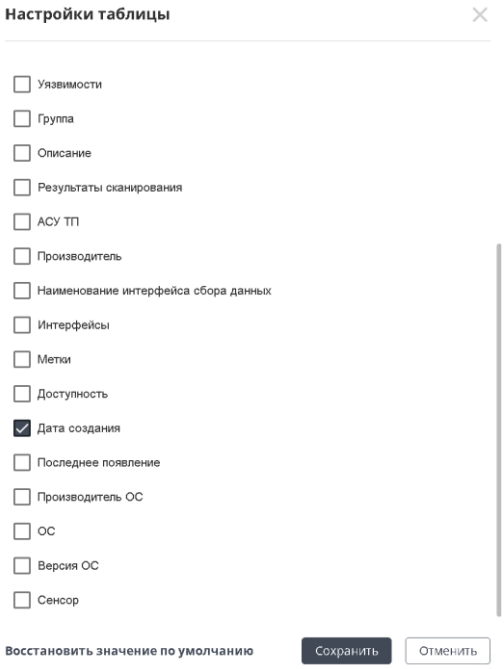


Рисунок 57 — Настройка количества отображаемых столбцов таблицы активов

На странице «Активы» в фильтрах списка активов. выберите актив, которым присвоена «АСУ ТП цеха 1».

На панели фильтров разверните область групп «АСУ ТП» и отметьте параметр «АСУ ТП цеха 1».

Нажмите кнопку «Применить».

Просмотрите полученный список активов (**Рисунок 58**).

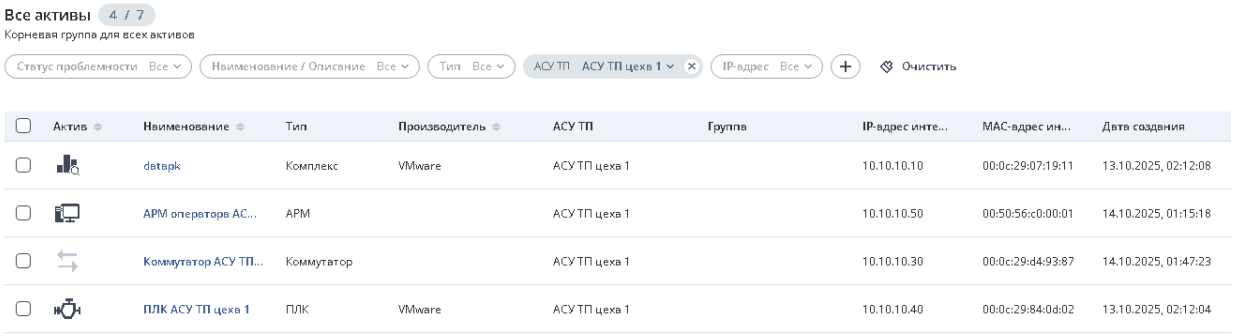


Рисунок 58 — Линейный список активов АСУ ТП цеха 1

Лабораторное задание 2.5. Работа с картой сети предприятия

Цель: сформировать умение работы с картой сети предприятия.

Ход работы:

Карта сети предприятия создаётся автоматически после настройки домашней сети. Для просмотра карты: Перейдите подраздел «Карта сети» раздела «Инспекция сети».

Для расположения активов на сетке нажмите кнопку «⌗», расположить на сетке (**Рисунок 59**).

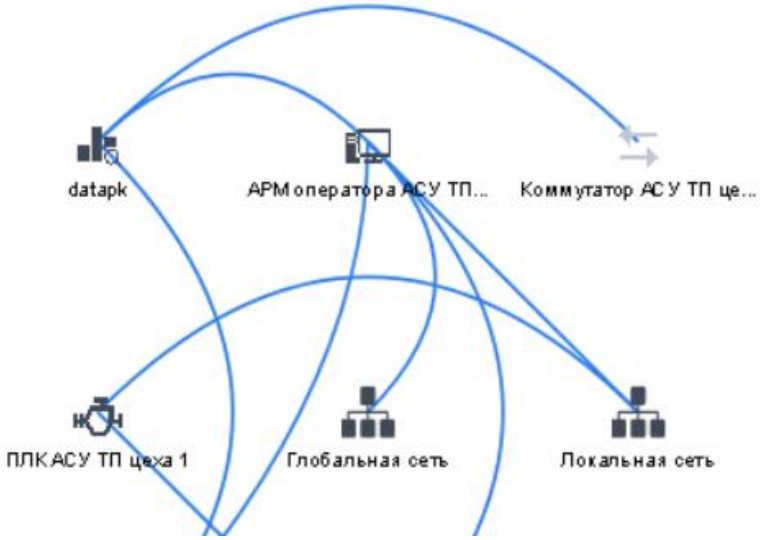


Рисунок 59 — Расположение активов на сетке

Для расположения активов на круге нажмите кнопку «◎» (**Рисунок 60**).

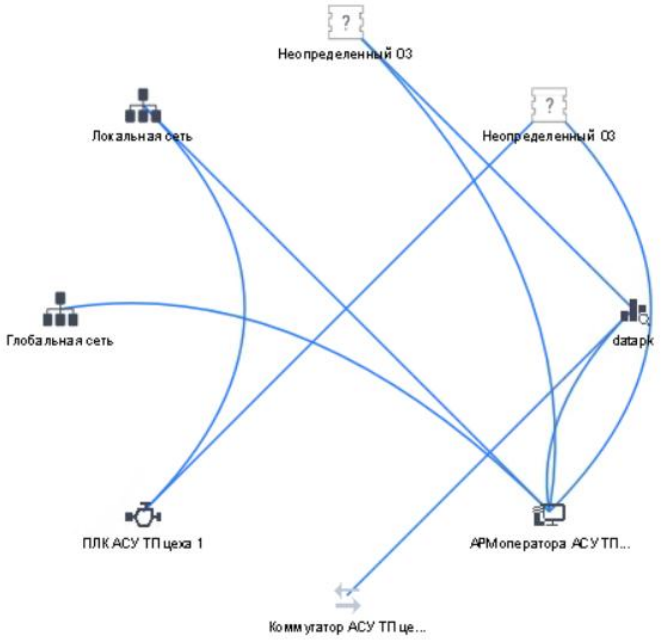


Рисунок 60 — Круговое расположение активов

Для группировки активов в соответствии с количеством сессий нажмите кнопку «▪▪» (**Рисунок 61**).

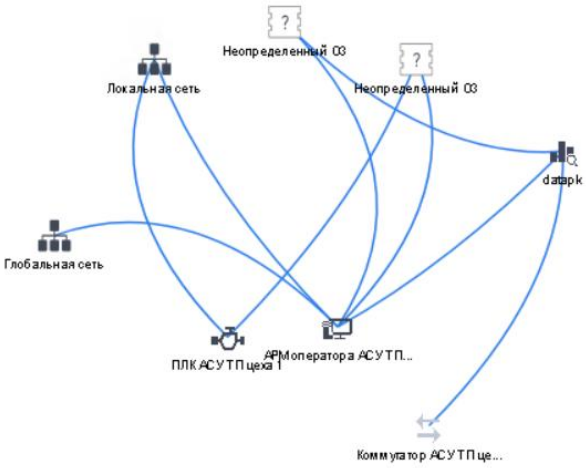


Рисунок 61 — Группировка активов по количеству сессий

Измените расположение активов на карте при необходимости.

Примечание. Вы можете выделять активы и (или) сессии при помощи клавиш Ctrl и Shift (**Рисунок 62**).

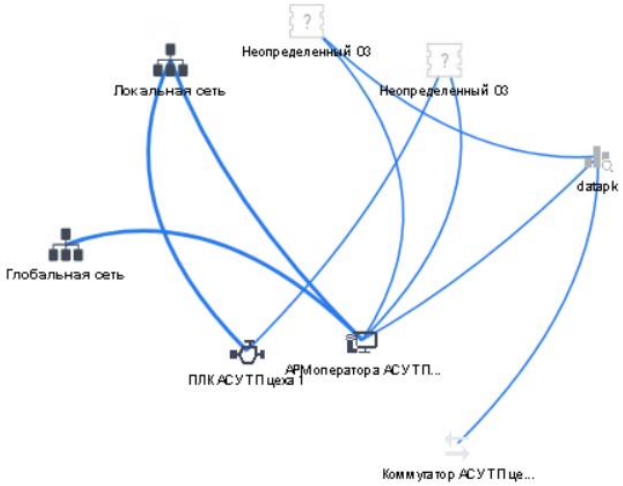


Рисунок 62 — Выделение нескольких активов на карте сети

Лабораторное задание 2.6. Обнаружение новых сетевых соединений. Просмотр сессий на карте сети предприятия

Цель: сформировать умение работы с потоками данных.

Ход работы:

Сессия — зарегистрированное взаимодействие между двумя узлами сети.

Режим обучения – режим работы правил сессий, при котором правила будут создаваться автоматически для всех обнаруженных сессий, такие сессии будут иметь статус «Не определен».

Для переключения режима необходимо перейти в раздел «Сенсоры», выбрать сенсор и в появившемся окне переключить «Автоматическое создание правил сессий» (режим обучения соответствует включенному переключателю) (***Рисунок 63***).

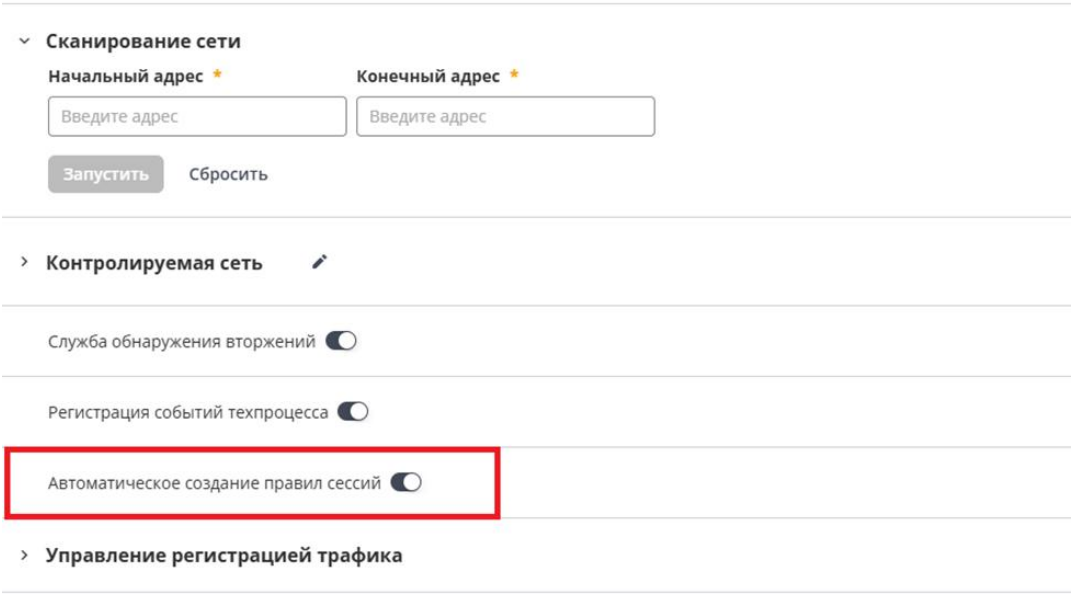


Рисунок 63 — Переключатель «Автоматическое создание правил сессий» в настройках сенсора

Просмотрите список обнаруженных сессий. Для этого перейдите на страницу «Инспекция сети» → «Сетевые соединения» (**Рисунок 64**). При необходимости сбросьте все фильтры вверху.

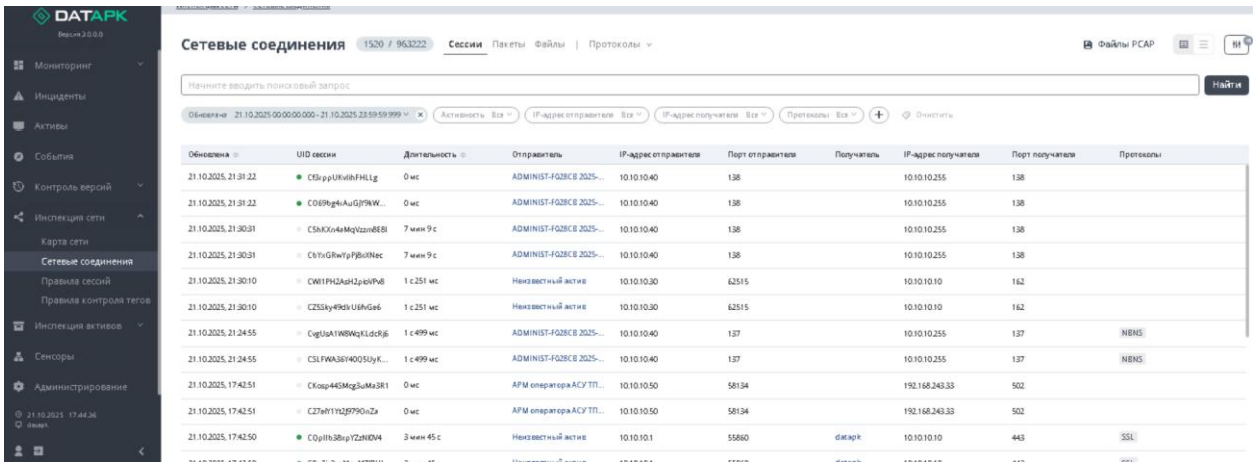


Рисунок 64 — Страница «Сетевые соединения»

Примечание:
Для генерации неподтвержденных сессий режим обучения должен быть выключен.

Посмотрите список неподтвержденных сессий. Для этого:

- В верхней части страницы нажмите на «+»;
- Добавьте фильтр «Статус»;
- в фильтре отметьте параметр «Не разрешена»;
- нажмите «Применить» (**Рисунок 65**).

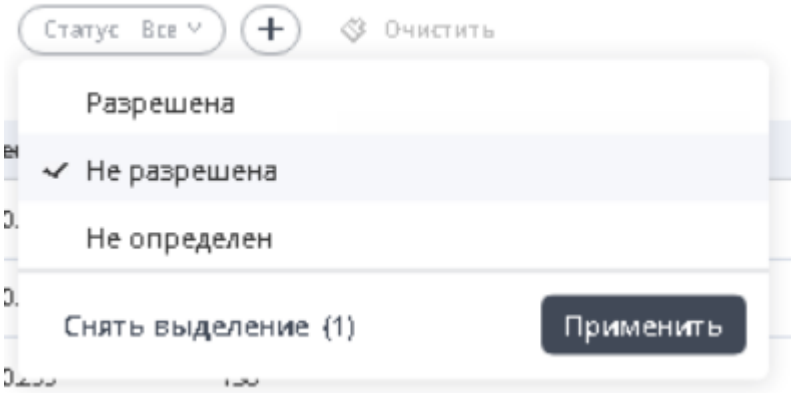


Рисунок 65 — Порядок фильтрации списка неподтвержденных сессий

Нажмите на сетевое соединение, чтобы просмотреть подробную информацию о нем (**Рисунок 66**).

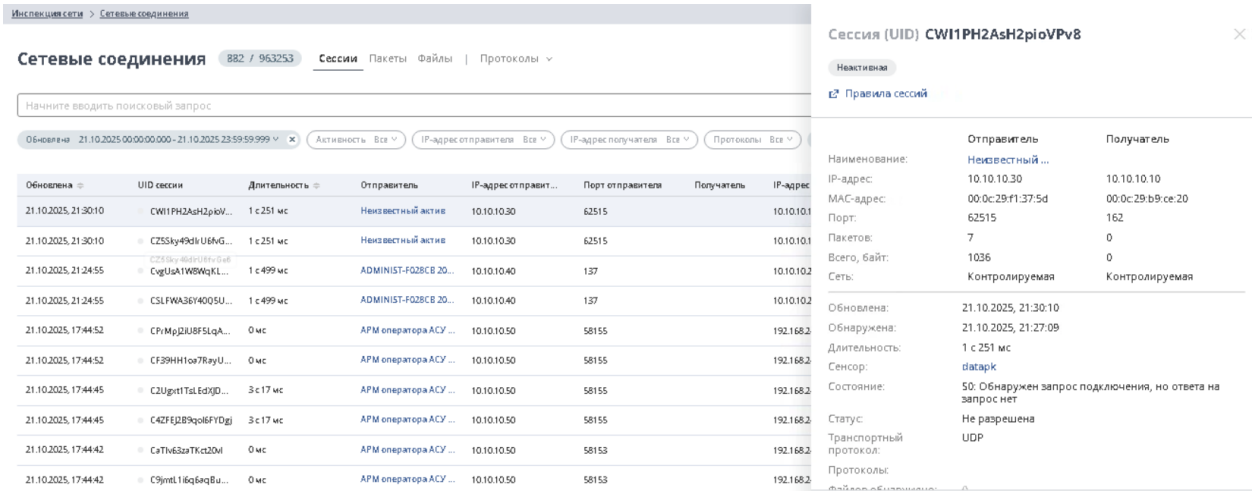


Рисунок 66 — Подробная информация о сетевом соединении

Для изменения отображаемых столбцов отмените параметр «UID сессии» в правом верхнем углу и просмотрите результат (**Рисунок 67**).

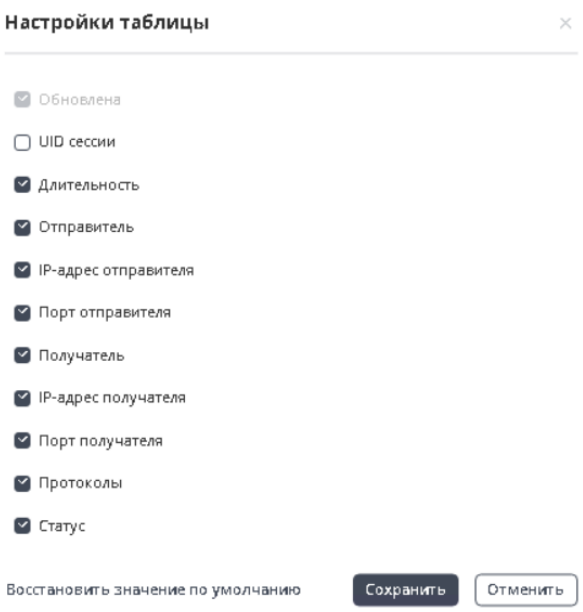


Рисунок 67 — Настройка отображаемых столбцов списка сессий, навигация по страницам списка

Сгенерируйте отправку эхо запросов с «АРМ оператора АСУ ТП цеха 1» на «ПЛК АСУ ТП цеха 1» при помощи команды ping.

Отфильтруйте информацию при помощи полей «IP-адрес отправителя» и «IP-адрес получателя». Через некоторое время информация о соединении появится на странице (***Рисунок 68***).

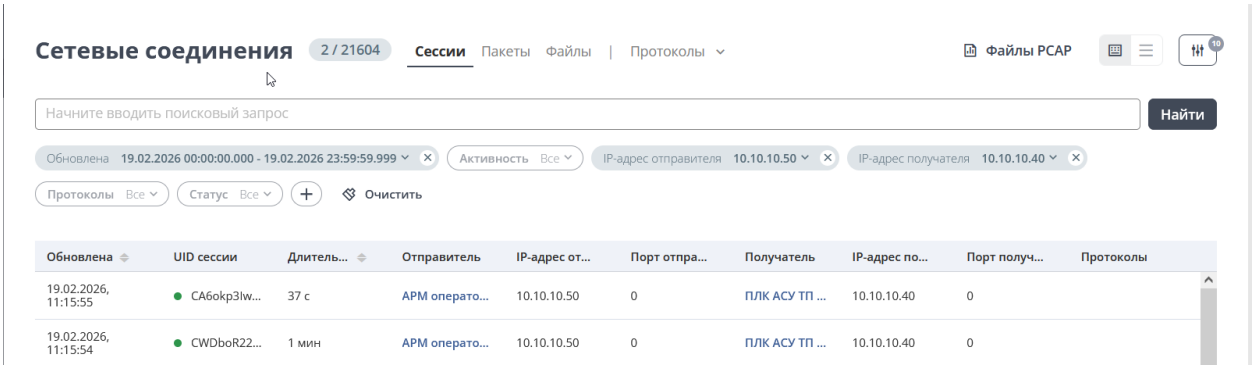


Рисунок 68 - Сетевые соединения

Перейдите в «Инспекция сети» - «Карты сети». Нажмите на соединение между «АРМ оператора АСУ ТП цеха 1» и «ПЛК АСУ ТП цеха 1». В открывшемся окне выберите «Подробнее о соединениях» (***Рисунок 69***).

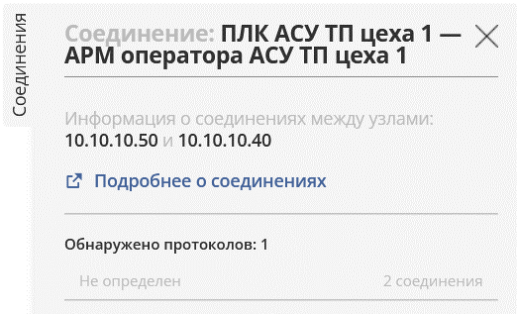


Рисунок 69 - Подробнее о соединениях

В результате вы перейдете на страницу с найденными соединениями между этими устройствами.

Лабораторное задание 2.7. Работа с правилами сессий

Цель: сформировать умение создания и проверки функционирования правил потоков.

Ход работы:

- правила применяются только для новых сессий;
- по умолчанию правила генерируются автоматически;
- если поток попал под правило, на следующие правила не проверяется.
- если поток не попал под правило и выключен режим обучения, то будет сгенерировано событие с типом - **session_control**

Для управления сессиями в интерфейсе Комплекса предусмотрены соответствующие правила. Они позволяют задать необходимые параметры (**Рисунок 70**) для автоматических действий по отношению к соединениям.

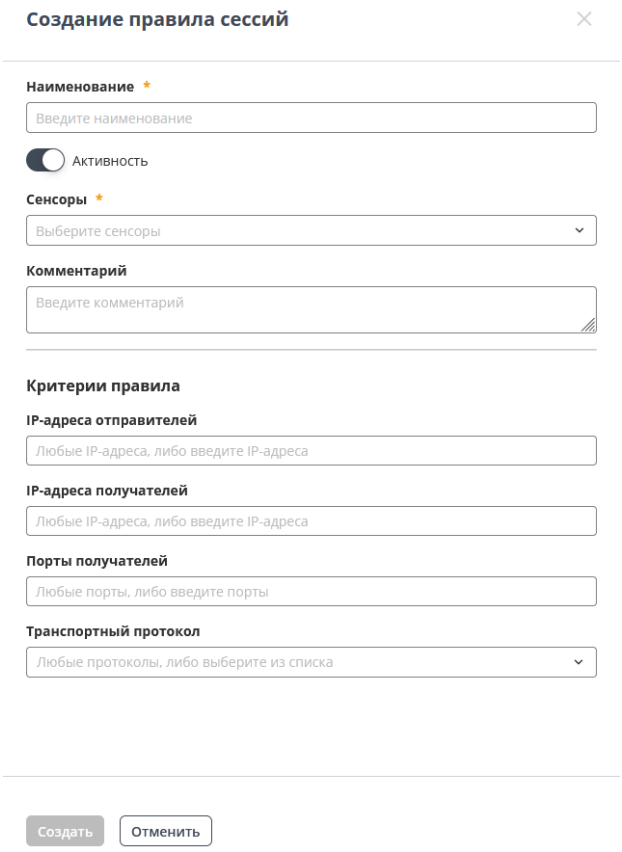


Рисунок 70 — Окно создания правила сессий

Подробное описание полей окна создания правил управления потоками данных приведено в таблице ниже (**Таблица 5**).

Таблица 5 – Поля окна создания сессий

Поле	Описание	Обязат.
Наименование	Название правила.	+
Активность	Чекбокс активности правила.	
Сенсоры	Используемый сенсор для обнаружения сессий	+

Поле	Описание	Обязат.
Комментарий	Обоснование, которое будет отображаться в результате выполнения правила.	
Блок «Критерии правила»		
IP-адреса получателей / отправителей	Один, несколько, или диапазон IP-адресов, попадающих под маску (префикс) IP-адреса (включая broadcast/multicast адреса). Если поле пустое, то под условие попадет любой IP-адрес. Один из основных фильтров. Рекомендуется применять его вместе с фильтром по портам.	
Порты получателей	Один, несколько или диапазон портов получателей. Возможны значения в диапазоне от 1 до 65535. Если поле пустое, то будет найден любой порт.	
Транспортный протокол	Транспортный протокол из списка, используемый для передачи данных.	

Перейдите в подраздел «Правила сессий» раздела «Инспекция сети» (**Рисунок 71**).

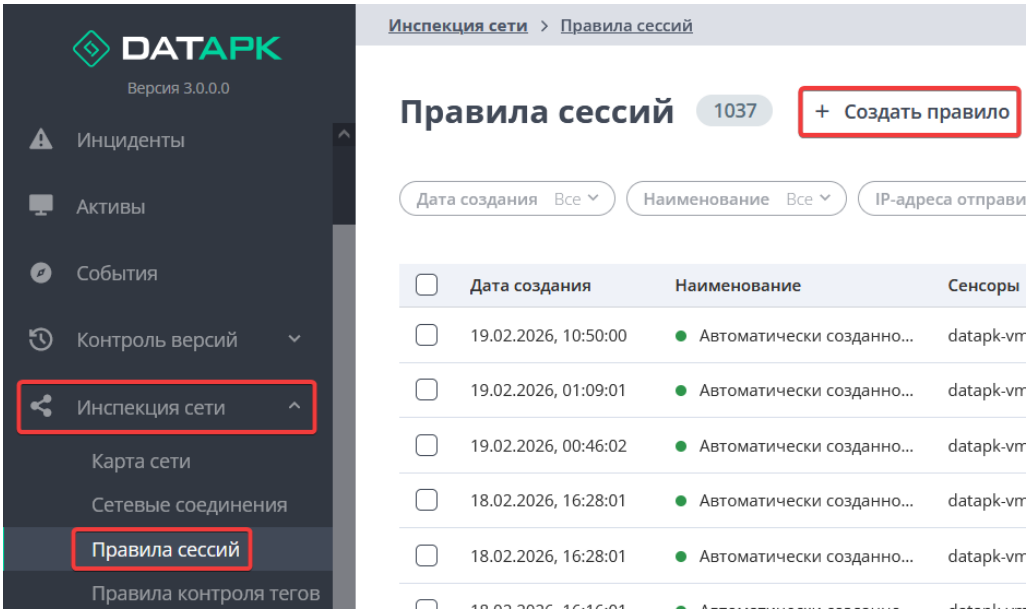


Рисунок 71 — Переход к правилам сессий

Используя полученные знания о полях окна создания правил сессий и их особенностях, создайте свои правила потоков:

Одобрите весь ICMP-трафик (**Рисунок 72**).

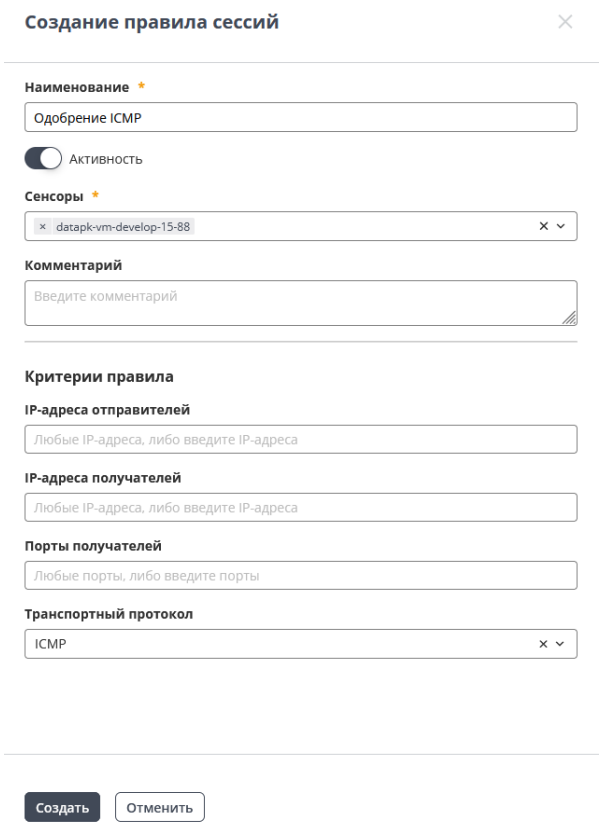


Рисунок 72 — Пример правила одобрения сессий ICMP

При помощи команды ping отправьте эхо-запросы с «АРМ оператора АСУ ТП цеха 1» на «ПЛК АСУ ТП цеха 1».

Выберите созданное правило сессии и в открывшемся окне нажмите на «Сессии» (**Рисунок 73**). Через некоторое время там появится информация об обнаруженном одобренном сетевом соединении.

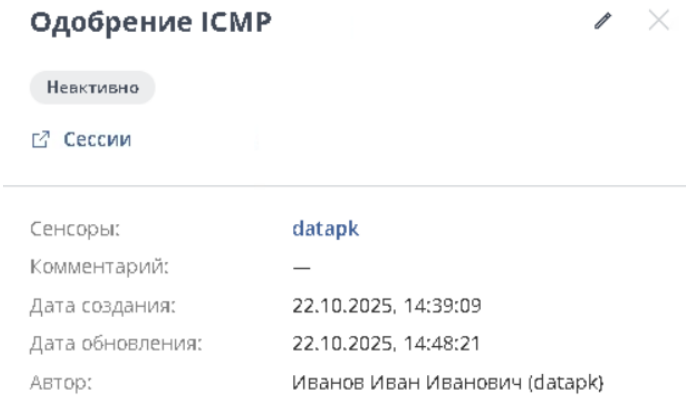


Рисунок 73 — Пример правила с временным одобрением потоков RDP

Вернитесь в «Инспекция сети» - «Правила сессий». Нажмите на чекбокс перед созданным вами правилом и выберите «Деактивировать» (**Рисунок 74**). Повторите отправку эхо-запросов.

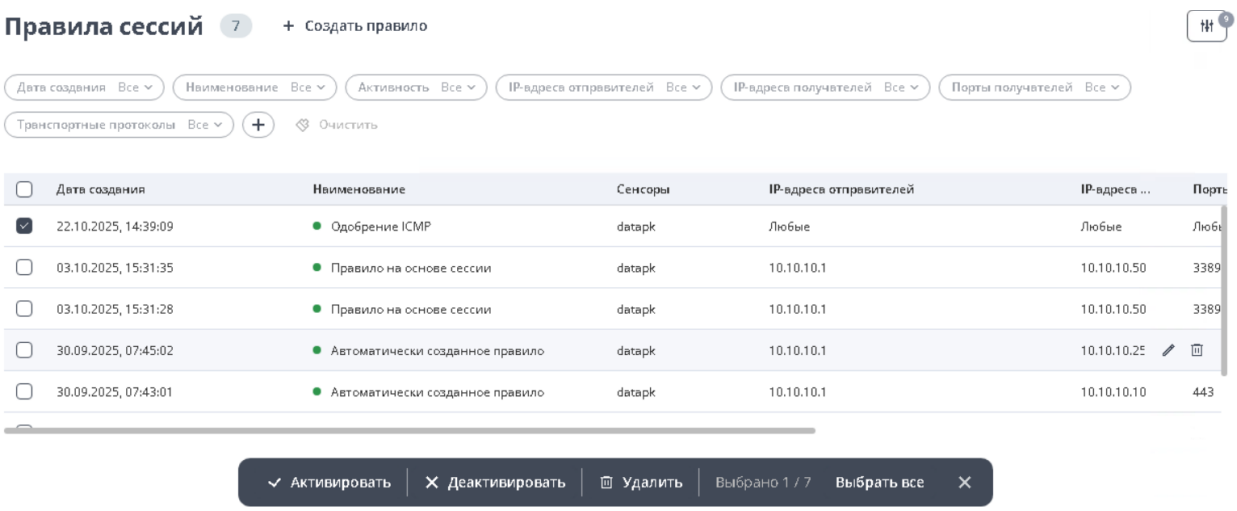


Рисунок 74 — Пример сессий, попавших под правила

В результате новая сессия получит статус «Не разрешена».

Также будет сгенерировано событие, у которого «Тип события» - **session_control** и «Код события» - **1270001**, найдите его в разделе «События», используя фильтры (***Рисунок 75***).

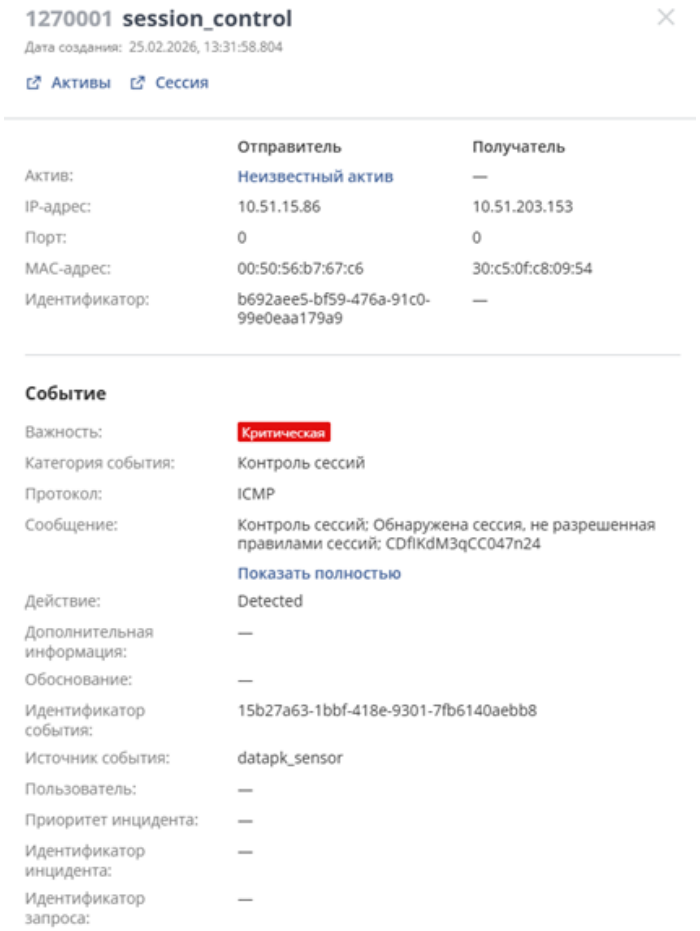


Рисунок 75 — Пример события неразрешенной сессии

В верхней части события будут переходы на сессию и активы, если найдены соответствующие данные, перейдите по ссылке «Сессия», в итоге должна появиться неразрешенная сессия (***Рисунок 76***).

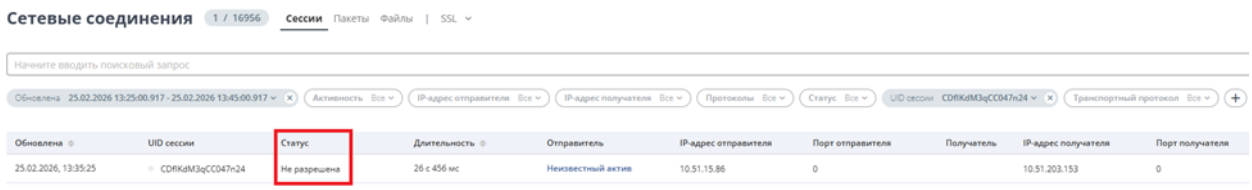


Рисунок 76 — Пример неразрешенной сессии после перехода

> **Примечание:**
> Переходы от события к сессии доступны для некоторых типов событий, например session_control, ids_event, dpi_notice и т.п.

Удалите созданное правило.

Лабораторное задание 2.8. Работа с правилами обнаружения вторжений

Цель: сформировать навыки настройки и импорта правил обнаружения вторжений, просмотра событий по результатам их работы.

Ход работы:

Создайте правило обнаружения вторжений. Для этого:

Откройте веб-интерфейс DATAPK.

Перейдите на страницу «Администрирование» → «Правила обнаружений» (**Рисунок 77**).

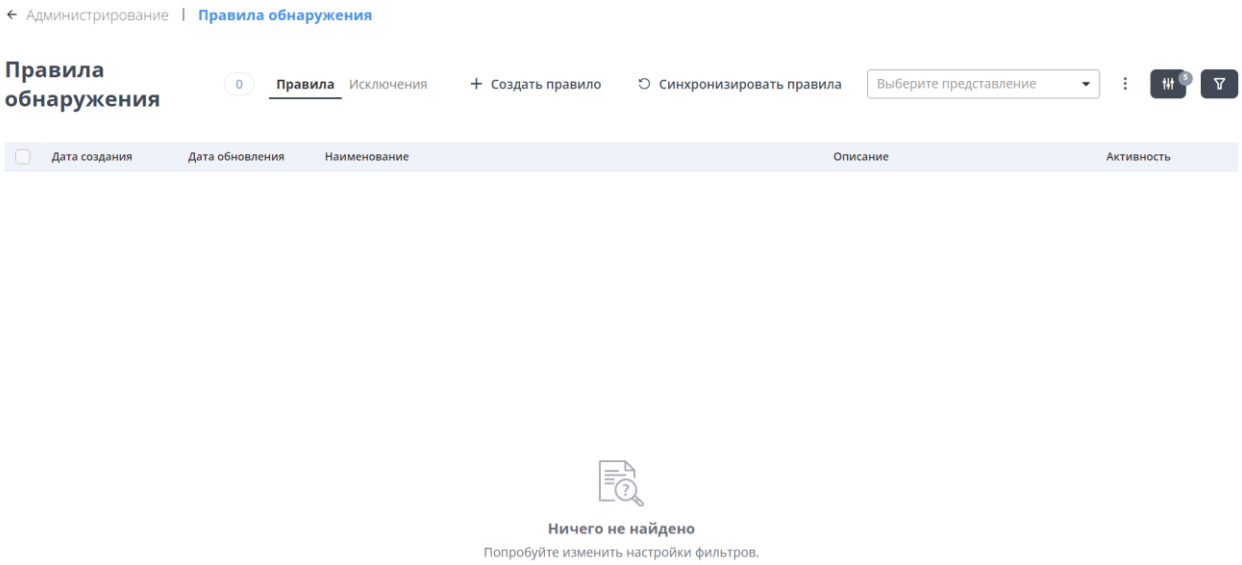


Рисунок 77 — Страница «Правила обнаружений»

Нажмите кнопку «Создать правило». В открывшемся окне (**Рисунок 78**) задайте параметры из таблицы (***Таблица 6***).

Таблица 6 — Параметры настройки правила для обнаружения отправки ICMP-трафика

Параметр	Значение
Наименование	ICMP-трафик
Описание	Правило обнаружения ICMP-трафика
Условие	**alert icmp any any -> any any (msg:"ICMP test detected"; GID:1; sid:11111111; rev:001; classtype:icmp-event;)**
Активность	Установить флаг «☑»

Нажмите кнопку «Создать» для подтверждения изменений.

Рисунок 78 — Создание правила обнаружения вторжений

Проверьте работу правила обнаружения ICMP-трафика. Для этого:

Смоделируйте ICMP-трафик на стенде. Для этого в командной строке Windows введите команду:

```
ping [IP-адрес актива, генерирующего ICMP-трафик]
```

Перейдите в раздел «События».

В фильтре «Тип события» введите «**ids_event**», выберите соответствующий пункт и нажмите «Применить».

Просмотрите полученное сообщение от службы обнаружения вторжений об обнаружении ICMP-трафика (***Рисунок 79***).

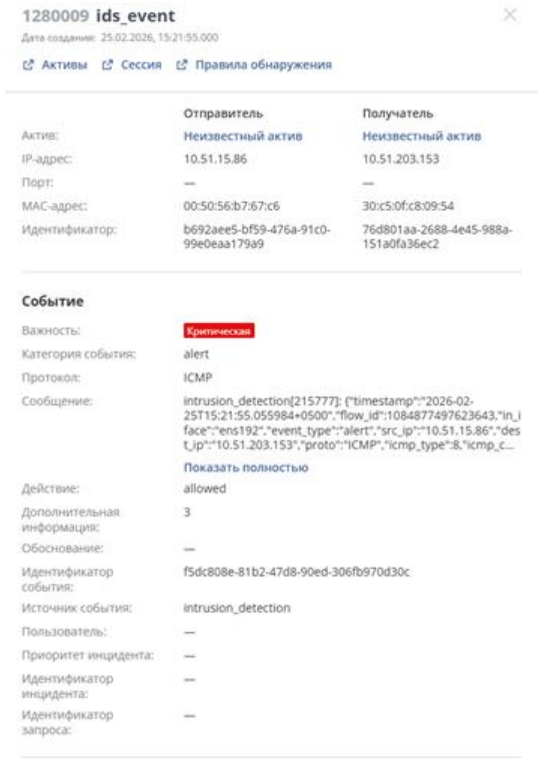
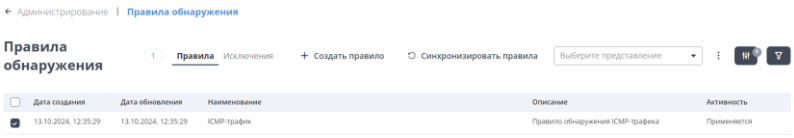


Рисунок 79 — Пример события от службы обнаружения вторжений

Примечание:
События IDS удобно фильтровать по полю **Тип события**. Оно равно **ids_event**. Также обратите внимание на остальные поля. В поле **Описание** пишется **msg** из правила suricata, в поля **IP-адрес Отправителя** / **IP-адрес Получателя** пишутся соответствующие IP-адреса пакета (в некоторых случаях – совокупности пакетов), который подпал под правило. Некоторые поля (**Порт Отправителя**, **Порт**

Отключите правило, обнаруживающее ICMP. Для этого на странице «Правила обнаружения» найдите созданное правило, поставьте рядом с ним «галочку». Как результат на экране появится меню действий с правилом. Нажмите на кнопку «Деактивировать» (**Рисунок 80**).



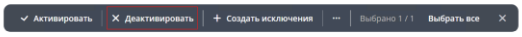


Рисунок 80 — Деактивация правила IDS

Импортируйте правила обнаружения вторжений. Для этого перейдите в подраздел управления «Администрирование» → «Импорт и экспорт» (**Рисунок 81**).

Загрузите правила обнаружения вторжений, подготовленные в Комплексе (**rules_datapk_IDS-3-0.json**).

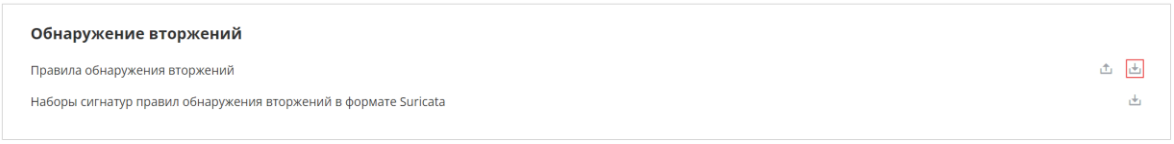


Рисунок 81 —Кнопка загрузки правил обнаружения вторжений

Дождитесь появления уведомления (**Рисунок 82**) об успешном импорте правил в правом верхнем углу.

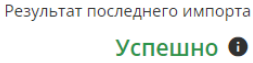


Рисунок 82 — Уведомление об успешной загрузке правил обнаружения вторжений

Примечание:
Правила после импорта применяются автоматически.

Импортируйте файл в формате Suricata («**test+eicar.rules**»). В данном файле закомментировано правило для обнаружения ICMP, а также правило для обнаружения EICAR.(Suricata – это система

обнаружения вторжений. EICAR – это специальный файл, который используется для проверок – работает ли антивирус.) (**Рисунок 83**).

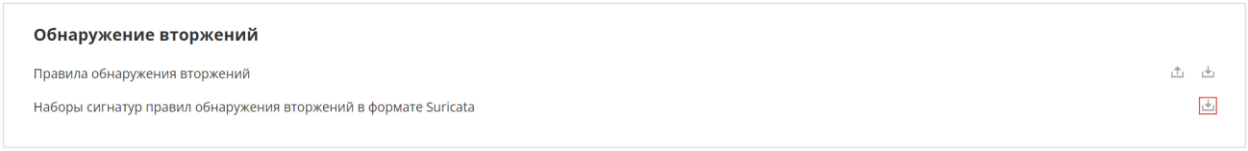


Рисунок 83 —Кнопка загрузки правил обнаружения вторжений в формате Suricata

Скопируйте файл **only_eicar.pcap** на операционную систему Комплекса.

Проиграйте трафик утилитой **tcpreplay** на слушающем интерфейсе Комплекса **(Рисунок 84).** Для этого введите команду:

```
tcpreplay -i dummy0 [путь к pcap-файлу]
```

```
[root@datapk-vm-develop-15-86 ~]# tcpreplay -i dummy0 only_eicar.pcap
Actual: 1 packets (238 bytes) sent in 0.000031 seconds
Rated: 7677419.3 Bps, 61.41 Mbps, 32258.06 pps
Flows: 1 flows, 32258.06 fps, 1 unique flow packets, 0 unique non-flow packets
Statistics for network device: dummy0
        Successful packets:        1
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

Рисунок 84 — Результат работы команды

Примечание:
Если на Комплексе не установлена утилита **tcpreplay**, то установите её командой: **sudo apt-get install tcpreplay**, предварительно переключив интерфейс управления Комплекса в сеть NAT.

Найдите событие по результатам сработки EICAR. Для этого:

Перейдите на страницу «События» и введите в фильтре «Описание» - **EICAR** (***Рисунок 85***).

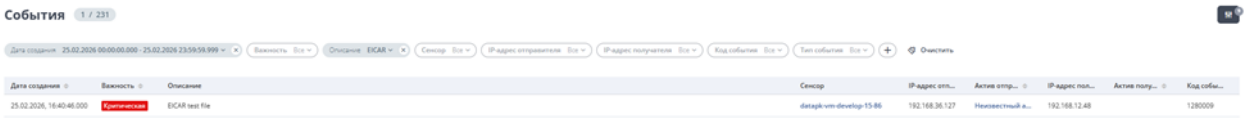


Рисунок 85 — Пример события от IDS для трафика EICAR

Примечание:
Для добавления исключений IDS можно создавать **pass** правила, которые является более приоритетными и останавливают анализ пакета, если он подошел под условия. Такие правила должны иметь **sid** из пользовательского диапазона (94000000-94999999) и не иметь в условиях конструкции вида: **threshold: type both, track by_dst, count 1, seconds 60;**

Создайте pass правило для EICAR. Для этого:

Найдите импортированное правило, кликнув по переходу «Правила обнаружения» в соответствующем событии (***Рисунок 86***).

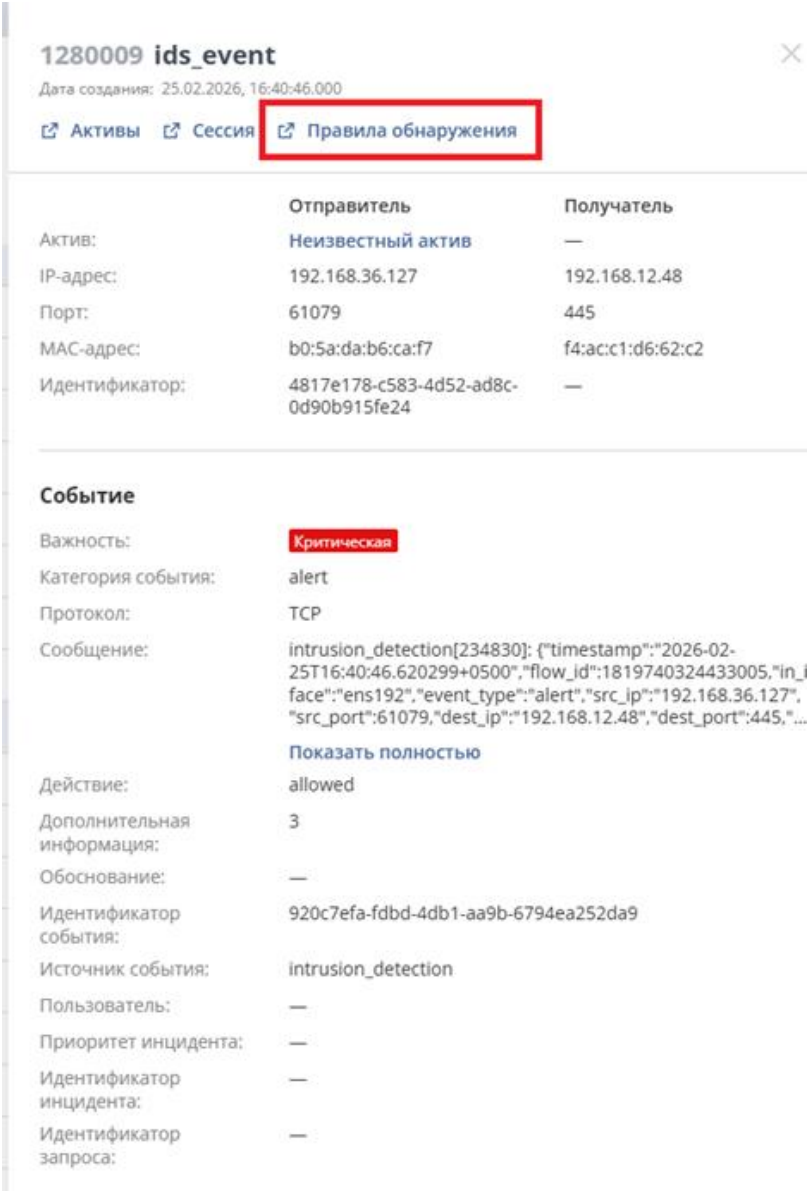


Рисунок 86 — Расположение перехода к правилу обнаружения в событии

Создайте копию найденного правила, заменив **alert** в самом начале на **pass** и **sid** на номер в пользовательском диапазоне, например 94000001 (***Рисунок 87***).

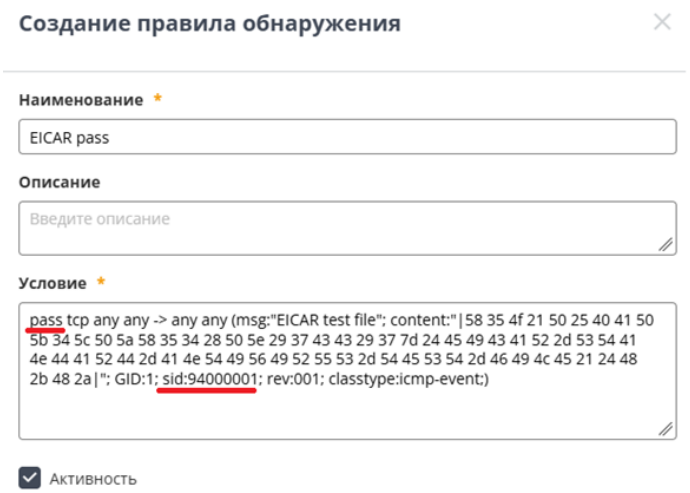


Рисунок 87 — Пример pass правила обнаружения EICAR

Проиграйте **only_eicar.pcap**, выполнив команду (событие не должно генерироваться):

```
tcpreplay -i dummy0 [путь к pcap-файлу]
```

Экспортируйте файл с правилами обнаружения вторжений. Для этого:

Перейдите в подраздел управления «Администрирование» → «Импорт и экспорт».

Найдите строку «Правила обнаружения вторжений, подготовленные в Комплексе» и нажмите напротив нее кнопку «» (**Рисунок 88**).

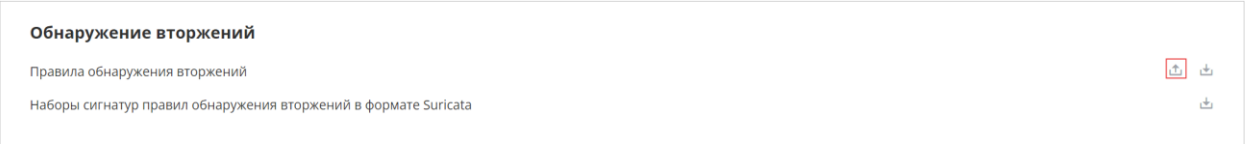


Рисунок 88 — Экспорт правил обнаружения вторжений

Результат шага: в файл запишутся все правила обнаружения вторжений с данного Комплекса. Потом этот json-файл можно загружать на другие Комплексы (**Рисунок 89**).

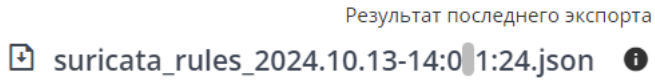


Рисунок 89 — Результат экспорта правил обнаружения вторжений

Примечания:
В продуктивных инсталляциях настоятельно рекомендуется проводить тюнинг правил IDS – отключать часто срабатывающие правила, создавать исключения с помощью pass правил для определенных IP-адресов, добавлять в исключения правила для определенного сенсора

Для корректного отображения событий в интерфейсе визуализации нужно обеспечить синхронизацию времени на ОС Комплекса и ОС оператора. Временные фильтры в интерфейсе визуализации привязываются к времени клиента.

События Комплекса отображаются в часовом поясе клиента, но хранятся на Комплексе

Лабораторное задание 2.9. Работа с правилами контроля тегов

Цель: сформировать навыки настройки контроля тегов, просмотра событий по результатам его работы.

Ход работы:

На основе трафика могут генерироваться различные событие, помимо уже рассмотренных **session_control** и **ids_event**, в эту группу входят события с типом:

- **dpi_notice** – соответствует сетевым атакам и критичным командам техпроцесса
- **ml_notice**– соответствует атакам обнаруженным ml-модулем
- **tag_control** – соответствуют событиям, связанными с контролем тегов

Для изменения перечня критичных функций необходимо изменить конфигурационный файл, который расположен в файле **/usr/share/udv/zeek-wrapper/configs/ics-function.dat** на уровне **Sensor**. Также можно отключить регистрацию события техпроцесса (критичных функций) с помощью переключателя в настройках сенсора (***Рисунок 90***).

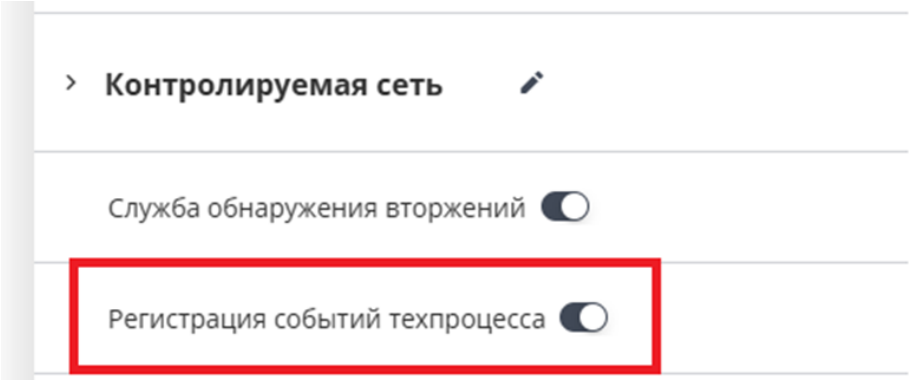


Рисунок 90 — Переключатель для управления регистрацией критичных функций

Белый список **dpi_notice** и **ml_notice** задается в файле **/usr/share/udv/zeek-wrapper/configs/general.dat** на уровне **Sensor**, процесс описан в соответствующем разделе официальной документации к Комплексу.

Для контроля тегов предусмотрены правила, которые позволяют задать разрешенные значения, при выходе из которых будет сформировано событие (***Рисунок 91***).

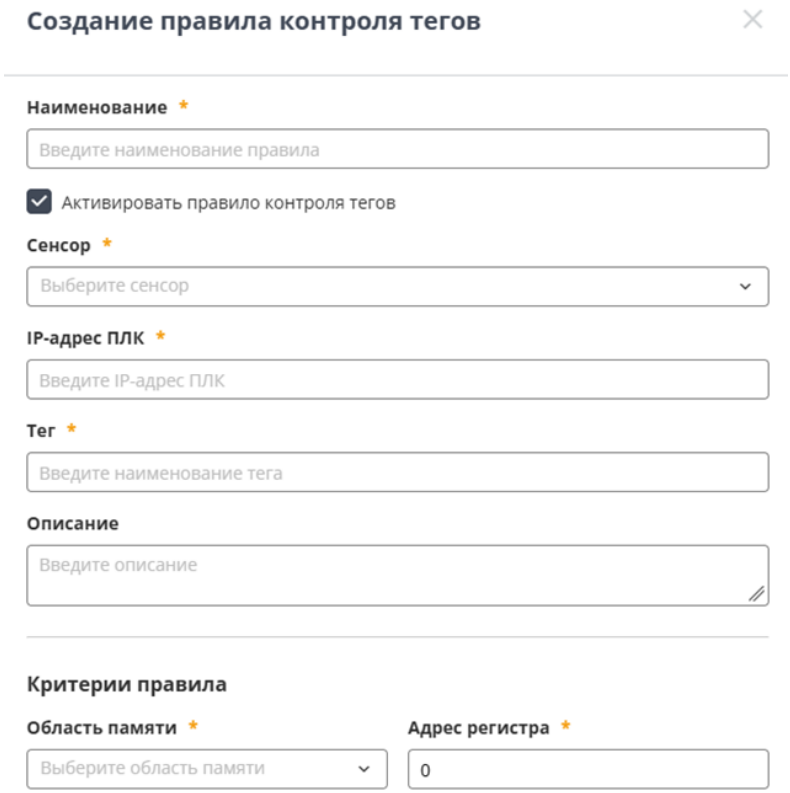


Рисунок 91 — Окно создания правила контроля тегов для протокола Modbus

Создайте правило контроля тегов для протокола Modbus. Для этого:

Откройте веб-интерфейс DATAPK.

Перейдите в подраздел «Правила контроля тегов» раздела «Инспекция сети»

Выберите вкладку «Modbus» и нажмите «Создать правило» (***Рисунок 92***).

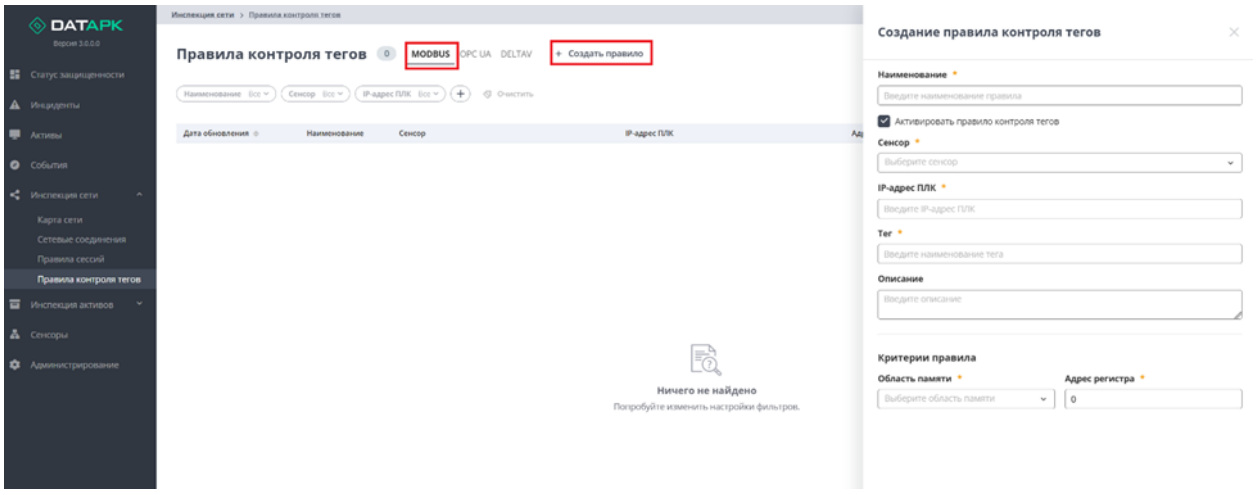


Рисунок 92 — Переход к созданию правила контроля тегов

В появившемся окне введите значения из таблицы (***Таблица 7***).

Таблица 7 — Параметры правила контроля тегов

Параметр	Значение
Наименование	Переполнение бака

Сенсор	Выбрать сенсор
IP-адрес ПЛК	192.168.0.3
Тег	Уровень воды
Область памяти	Регистры ввода
Адрес регистра	2
Тип данных	Int16
Условие	Меньше
Значение	1500

Нажмите кнопку «Создать» для подтверждения (***Рисунок 93***).

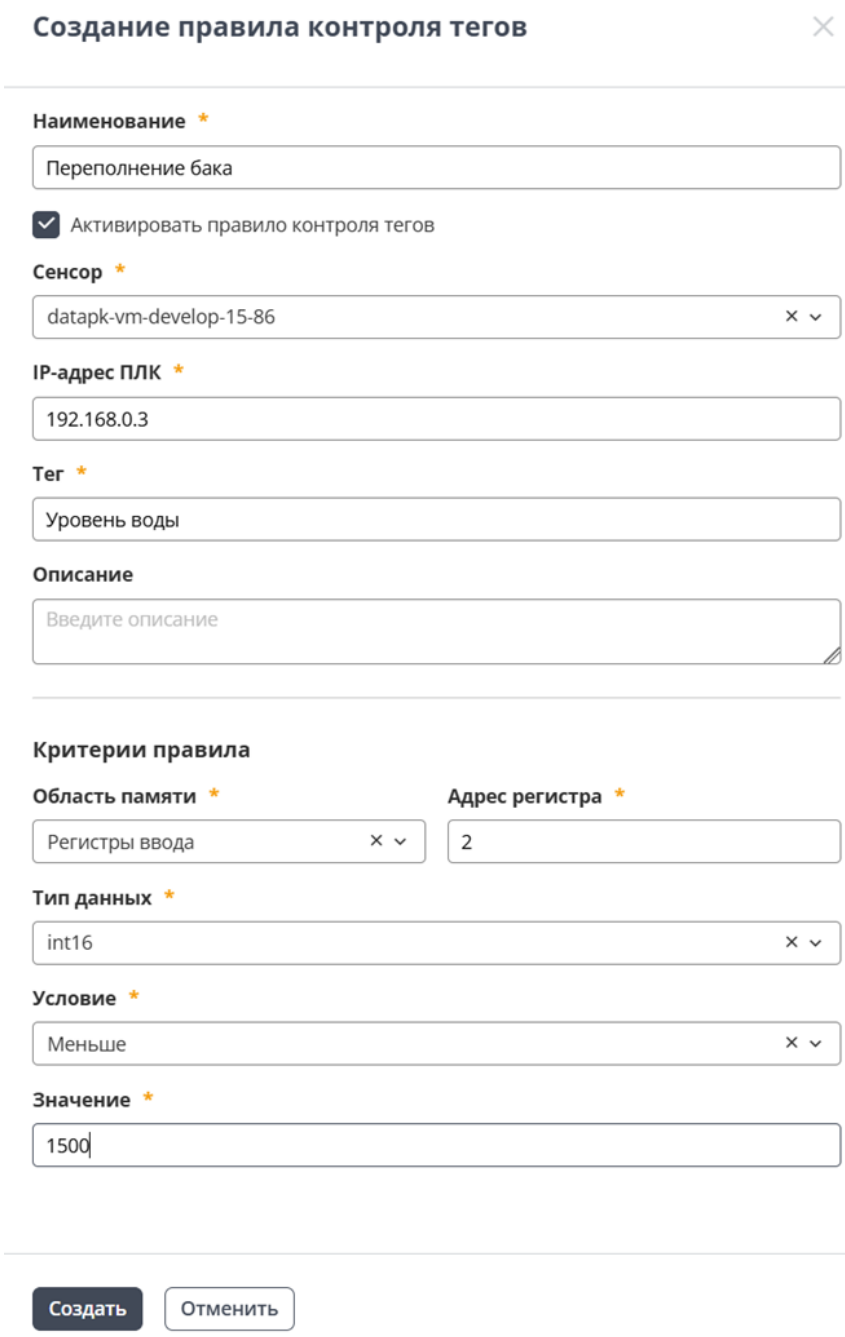


Рисунок 93 — Окно создания правил контроля тегов

Скопируйте файл **tags.pcap** на операционную систему Комплекса.
Проиграйте трафик утилитой **tcpreplay** на слушающем интерфейсе Комплекса (***Рисунок 94***). Для этого введите команду:

```
tcpreplay -i dummy0 [путь к pcap-файлу]
```

```
[root@datapk-vm-develop-15-86 ~]# tcpreplay -ti dummy0 slb.pcap
Actual: 11140 packets (833026 bytes) sent in 0.033893 seconds
Rated: 24578113.4 Bps, 196.62 Mbps, 328681.43 pps
Flows: 74 flows, 2183.34 fps, 11140 unique flow packets, 0 unique non-flow packets
Statistics for network device: dummy0
        Successful packets:        11140
        Failed packets:            0
        Truncated packets:         0
        Retried packets (ENOBUFS): 0
        Retried packets (EAGAIN):  0
```

Рисунок 94 — Результат работы команды

Примечания:
Новые события несоответствия значения тега не будут генерироваться, если его значение не пришло в норму (событие с кодом 1260002).

Перейдите в раздел «События».

В фильтре «Тип события» введите **tag_control**, выберите соответствующий пункт и нажмите «Применить».

Просмотрите события о несоответствии значения тега и о нормализации значения (**Рисунок 95**).

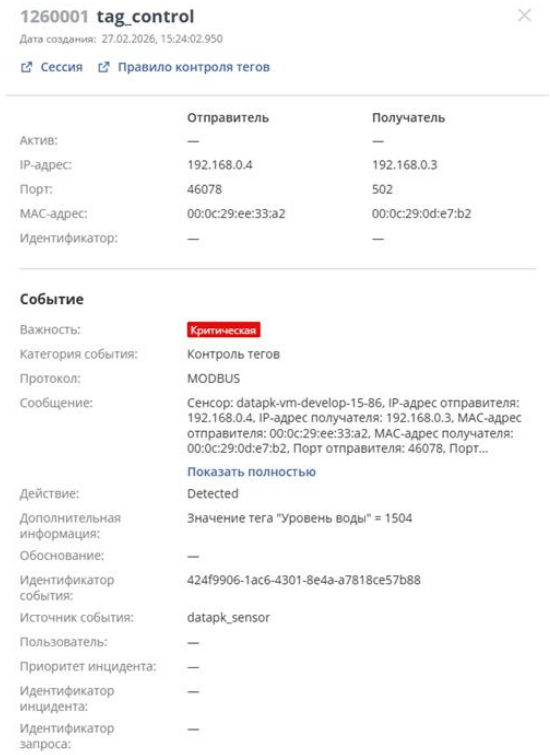


Рисунок 95 — Пример события о несоответствии значения тега

Удалите созданное правило контроля тегов

Лабораторное задание 2.10. Сохранение, изменение и удаление представлений

Цель: сформировать навык работы с представлениями.

Ход работы:

На странице Карта сети вы можете создавать, редактировать и удалять представления. Для этого вернитесь на страницу «Карта сети» выберите фильтры.

Примечание:

К сохранению в составе представлений доступны:

- фильтры;
- группировка узлов по количеству потоков («» - «Сгруппировать по количеству потоков»);
- расположение элементов на карте: «» - «Расположить на сетке», «» - «Расположить по кругу». В составе представлений не учитывается масштабирование, поиск и выделение по его результатам.

Измените необходимые параметры фильтров. Например, выберите типы активов «АРМ», «Коммутатор», «ПЛК». (**Рисунок 96**).

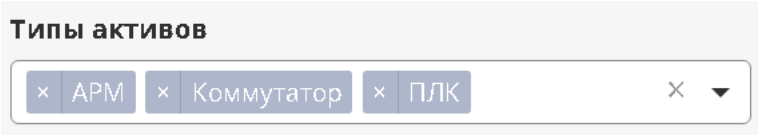


Рисунок 96 — Выбор типа отображаемых на карте активов

Измените параметры отображения узлов на карте. Например, выберите группировку по количеству узлов («», «Сгруппировать по количеству потоков»).

В верхней правой части страницы нажмите «».

В выпадающем меню выберите опцию «Сохранить как».

Результат шага: появится окно сохранения представления.

В окне сохранения представления:

- введите наименование;

Внимание: Имя не должно совпадать с существующим.

- выберите, будет ли представление доступно для использования другими пользователями.

Например, введите название «Подсеть управления» и выберите тип использования «Только для меня» (**Рисунок 97**).

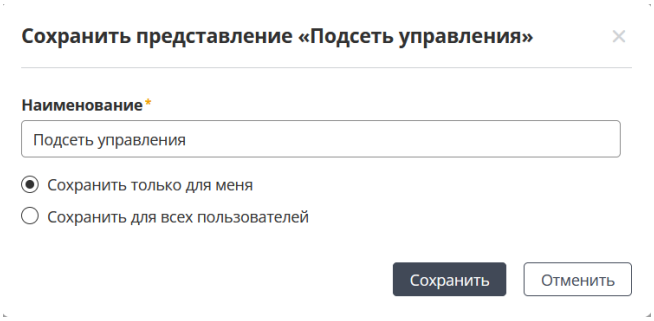


Рисунок 97 — Окно сохранения представления

Нажмите «Сохранить». Результат шага: Новое представление станет доступно для выбора.

В верхней части панели фильтров выберите из выпадающего списка только что созданное представление (**Рисунок 98**).

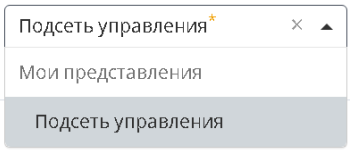


Рисунок 98 — Выпадающий список с доступными представлениями

Изменение представления. Для изменения представления:

- в верхней части панели представлений выберите из выпадающего списка представление, которое будет изменено;
- измените параметры представления;
- для пересохранения фильтра нажмите «Сохранить»;
- для сохранения измененного фильтра отдельно от созданного ранее, нажмите «⋮» в верхней части панели фильтров.

Результат шага: появится меню с кнопками управления представлениями.

В появившемся меню нажмите «Сохранить как» (**Рисунок 99**).

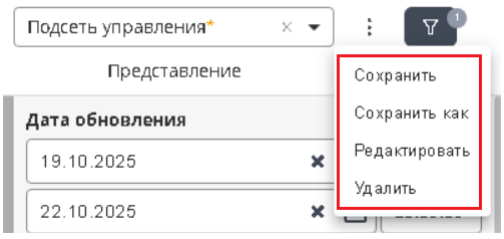


Рисунок 99 — Меню управления представлениями

Результат шага: появится окно сохранения представления.

В окне сохранения представления введите имя нового фильтра. Имя не должно совпадать с именем существующего представления, при попытке ввести существующее имя представления будет выведено соответствующее предупреждение. Выбрать доступно ли будет представление только для текущего пользователя или для всех (**Рисунок 100**).

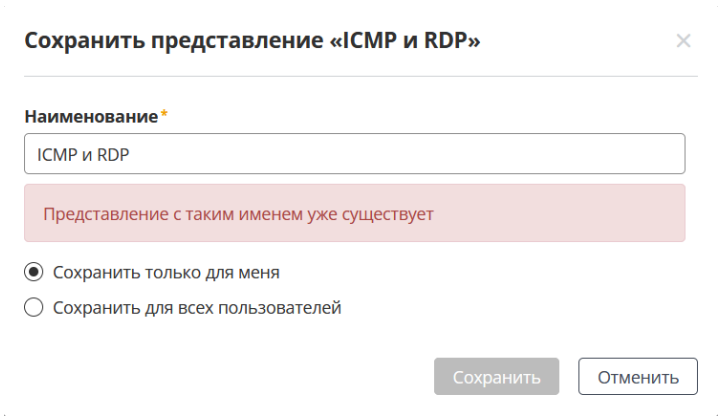


Рисунок 100 — Предупреждение в окне сохранения представления

Нажмите «Сохранить».

Переименование представления. Для переименования представления:

- нажмите «⋮» в верхней части панели представлений;

Результат шага: появится меню с кнопками управления представлениями.

- в появившемся меню нажмите «Редактировать»;

Результат шага: появится окно редактирования представления.

- в окне «Наименование» введите новое имя фильтра;
- нажмите «Сохранить».

Удаление представления.

Внимание! Удаление представления является невозвратной операцией.

Для удаления представления:

- нажмите «⋮» в верхней части панели представлений.

Результат шага: появится меню с кнопками управления представлением.

- в появившемся меню нажмите «Удалить»;

Результат шага: появится окно удаления представления.

- в окне «Удалить представление» нажмите «Удалить».

Результат шага: появится всплывающее уведомление «Представление удалено».

Лабораторная работа 3. Настройка подсистемы сбора конфигураций активов

Разделы документации

Разделы Руководства по эксплуатации:

- Настройка учетных данных активов;
- Управление и просмотр конфигураций активов;
- Рекомендации по настройке сбора данных и инфообмена;
- Документы из каталога «Настройка активов».

Документация по cron (из Интернета): https://ru.wikipedia.org/wiki/Cron

Тренажер по cron (из Интернета): https://crontab.guru

Справочная информация

В данной лабораторной работе описан процесс настройки активов с использованием скриптов вендора для автоматизации и ускорения процесса. Помимо этого, имеются полноценные руководства по настройке активов в ручном режиме. Доступ к этим руководствам предоставляется по запросу.

Не путайте тег и логин учетной записи! Тег — это служебное поле, которое используется в сканерах Комплекса для того, чтобы различать учетные записи, которые завел пользователь, между собой.Примеры нескольких тегов Комплекса:

- admin;
- cisco;
- cisco_en;
- eltex;
- sa;
- snmp3.

Какие теги использовать при сборе с актива, всегда можно узнать в официальной документации к Комплексу, в разделе «Реестр сканеров Комплекса».

Скрипты, загружаемые в datapk, должны иметь кодировку UTF-8 (без BOM). Для редактирования и просмотра скриптов в ОС Windows рекомендуется использовать Notepad++ или другие редакторы для работы с Python. Стандартный блокнот Windows не всегда корректно отображает файлы с UTF-8, а при сохранении меняет кодировку на UTF-8 с BOM (из-за чего скрипты не загружаются на DATAPK).

Для создания задачи потребуется:

- Создание группы сканеров;
- Создание группы активов или выбор конкретного актива;
- Создание задачи с группами сканеров и активов, с указанием расписания сбора данных.

Задачи должны создаваться на схожие активы, чтобы не возникло ситуации, когда сбор с актива осуществляется по протоколу, который актив не поддерживает.

Рекомендации по сбору данных:

- Сбор данных рекомендуется проводить в режиме ТО;
- Не рекомендуется опрашивать актив часто (чаще 2-4 раз в сутки);

- Рекомендуется разные активы опрашивать в разное время — не опрашивать в одно и то же время разные активы, разносить опрос разных активов по времени;
- Задачи рекомендуется объединять по принадлежности к активу и по протоколу сбора данных;
- Не рекомендуется создавать большие задачи сбора данных (более 10 сканеров).

Файлы для лабораторных работ

- **new-usr.bat** — скрипт создает пользователя с бесконечным паролем, добавляет его в группу локальных администраторов, параметры запрашиваются в диалоговом окне, работает на XP и новее, запускается скрипт от имени администратора;
- **datapk-winrm-https.ps1** — скрипт настраивает WMI и WinRM over HTTPS, работает на Windows 7 и новее, позволяет как импортировать сертификат Winrm, так и генерировать сертификат непосредственно на активе;
- **datapk-winrm-https.pfx** — сертификат для настройки активного сбора по WinRM over HTTPS.
- **datapk-xp-winexe.bat** — скрипт настраивает WMI и WinEXE, работает на Windows XP SP2/Server 2003 и новее (не предназначен для Windows 7 и новее, где настройка WinEXE не целесообразна в связи с наличием встроенного механизма WinRM).
- **Список пользователей (winrm https).py** — скрипт для сбора списка пользователей по протоколу winrm https.
- **Список устройств (winrm https).py** — скрипт для сбора списка устройств по протоколу winrm https.
- **datapk_script.crt** — сертификат для создания цифровой подписи скриптов.
- **datapk_script.key** — закрытый ключ для создания цифровой подписи скриптов.
- **Файл hosts (winrm https).py** — скрипт для сбора содержимого файла «hosts» по протоколу winrm https.
- **scripts_cisco.json** — набор скриптов и сканеров для сбора конфигураций с АСО Cisco.
- **scripts_configuration.json** — набор скриптов и сканеров для сбора данных с актива под управлением ОС Windows.
- **unix-ssh.json** — набор скриптов для сбора данных с unix-подобных систем и по протоколу SSH.
- **Файл hosts (winrm https).py** — некорректно работающий скрипт для сбора содержимого файла hosts.
- **папка Sign** — содержит в себе утилиту для генерации цифровой подписи скриптов в ОС Windows.
- **udv-terminal-connector.log** — файл с логами службы udv-terminal-connector, нужный для выполнения задания лабораторной работы.

Лабораторное задание 3.1. Настройка учетных записей на активах

Цель: сформировать умение настройки учетных записей на активах.

Ход работы:

Создайте пользователя на АРМ оператора АСУ ТП цеха 1 с правами локального администратора. Для этого:

Подключитесь к АРМ оператора АСУ ТП цеха 1.

Создайте учетную запись одним из предложенных способов: вручную (п. 1.3) или при помощи скрипта (п. 1.4).

Для создания учетной записи вручную:

Нажмите на кнопку «Пуск». Введите «Панель управления» и кликните по результату (**Рисунок 101**).

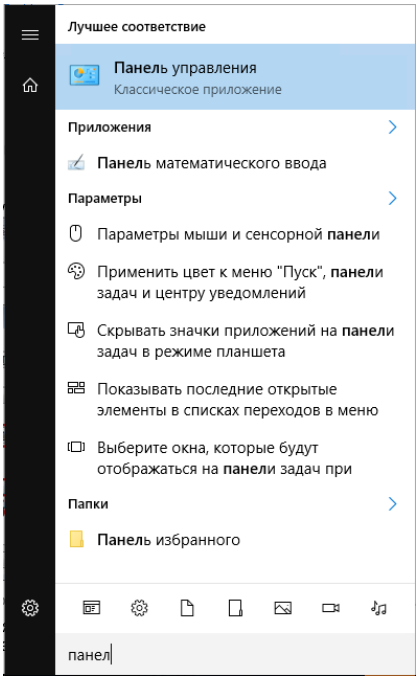


Рисунок 101 — Переход к панели управления в Windows 10

В панели управления выберите «Администрирование» → «Управление компьютером» (**Рисунок 102**).

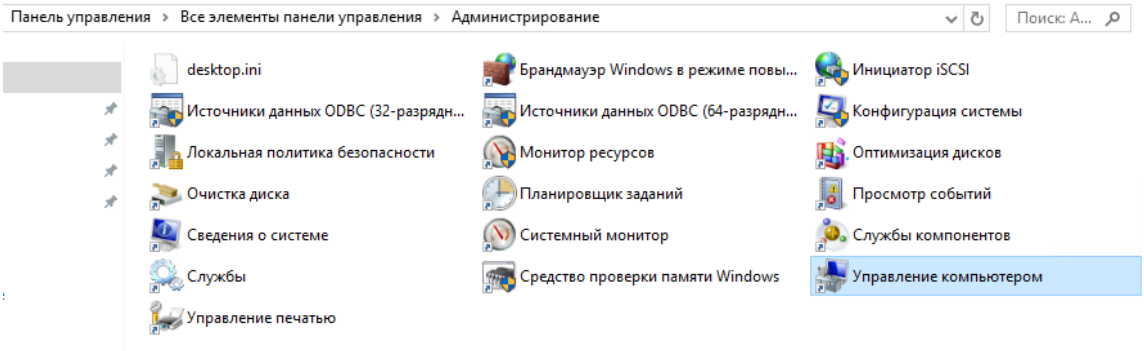


Рисунок 102 — Выбор пункта «Управление компьютером»

Результат шага: появится окно управления компьютером.

Раскройте пункт «Локальные пользователи и группы».

Наведите мышь на заголовок «Пользователи» и нажмите правую кнопку мыши.

Выберите в выпадающем меню «Новый пользователь» (**Рисунок 103**).

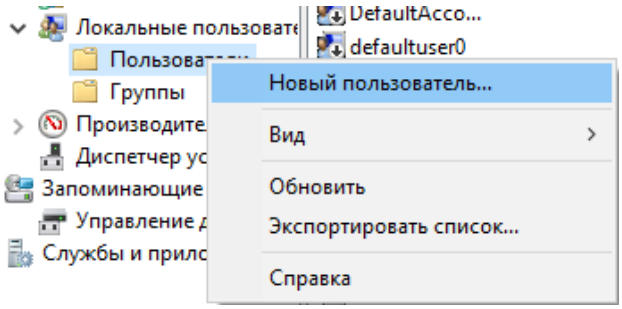


Рисунок 103 — Кнопка создания нового пользователя

Результат шага: появится окно добавления пользователя.

В открывшемся окне «Новый пользователь» задайте следующие параметры (**Рисунок 104**):

- в поле «Пользователь» введите «datapk»;
- в поле «Пароль» введите пароль учетной записи «P@ssw0rd»;
- в поле «Подтверждение» повторите ввод пароля;
- снимите галочку напротив параметра «Требовать смены пароля при следующем входе в систему»;
- установите чекбокс напротив параметра «Срок действия пароля не ограничен».

Нажмите на кнопку «Создать».

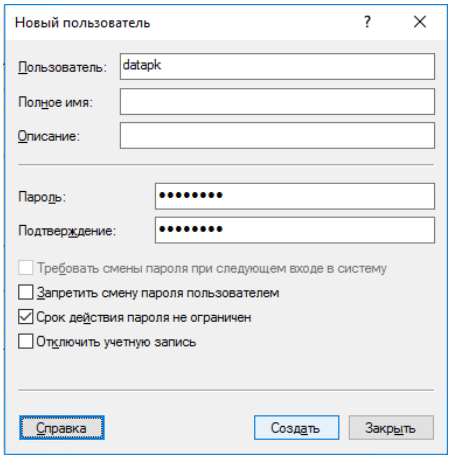


Рисунок 104 — Создание новой учетной записи пользователя

В обновленном списке дважды нажмите на пользователя datapk.

Результат шага: появится окно свойств пользователя (**Рисунок 105**).

В появившемся окне настройки свойств пользователя. Перейдите во вкладку «Членство в группах». Нажмите на кнопку «Добавить».

Результат шага: появится окно «Выбор: «Группы».

В окне «Выбор: «Группы»:

В поле «Введите имена выбираемых объектов» введите «Администраторы».

Нажмите на кнопку «Проверить имена».

Нажмите на кнопку «ОК» дважды, для закрытия двух окон.

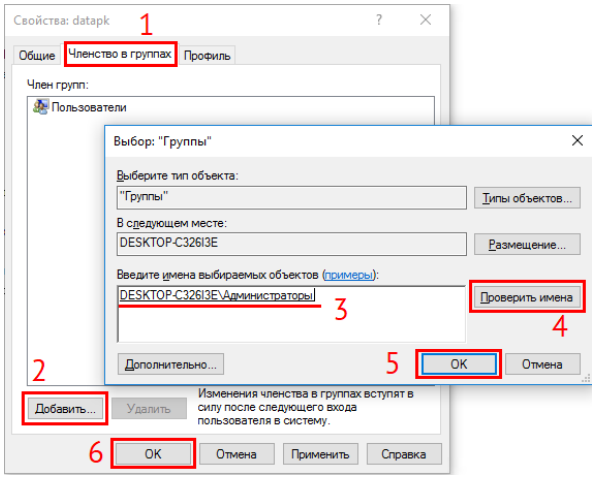


Рисунок 105 — Настройка новой учетной записи пользователя

Внимание! Если вы создали пользователя datapk вручную, то пропустите следующий шаг (1.4).

Для создания учетной записи при помощи скрипта:

Запустите скрипт для создания пользователя new-usr.bat от имени администратора (**Рисунок 106**).

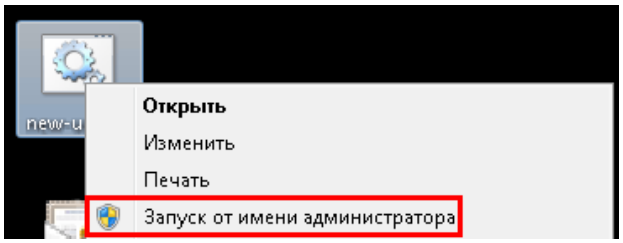


Рисунок 106 — Запуск файла от имени администратора

Введите следующие параметры (**Рисунок 107**):

- имя пользователя;
- пароль;
- подтверждение пароля.

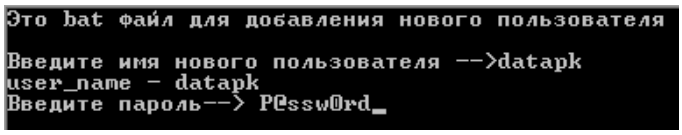


Рисунок 107 — Ввод имени и пароля для нового пользователя

Результат шага: появится сообщение (**Рисунок 108**) о том, что команда успешно выполнена.

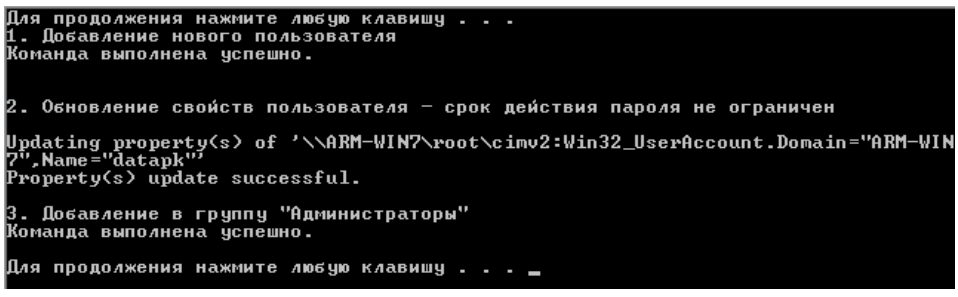


Рисунок 108 — Сообщение об успешном создании пользователя

Аналогичным образом создайте учетную запись datapk на активе «ПЛК АСУ ТП цеха 1».

Настройте протокол winrm https на активе. Для этого:

Ознакомьтесь с принципами работы скрипта в файле datapk-winrm-https.txt.

Подключитесь к АРМ оператора АСУ ТП цеха 1.

Скопируйте в папку **C://scripts файлы datapk-winrm-https.ps1 и datapk-winrm-https.pfx**.

Запустите приложение Windows PowerShell от имени администратора (**Рисунок 109**).

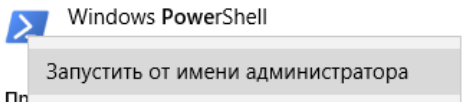


Рисунок 109 — Запуск Windows PowerShell от имени администратора

Перейдите в каталог с загруженными файлами при помощи команды:

```
cd "C:\scripts"
```

Запустите скрипт при помощи команды (**Рисунок 110**):

```
powershell -executionpolicy RemoteSigned -file .\datapk-winrm-https.ps1
"[Ваша подсеть]" "gen" | tee log.txt
```

Примечание:

В качестве аргумента [ваша подсеть] может использоваться как диапазон IP-адресов, так и отдельные IP-адреса через запятую или по одиночке. Примеры:

- "192.168.1.1" — один IP-адрес;
- "192.168.1.1,192.168.10.0/24" — несколько конкретных IP-адресов;
- "10.0.0.0/16" — все IP-адреса из подсети 10.0.[0-255].[0-255].

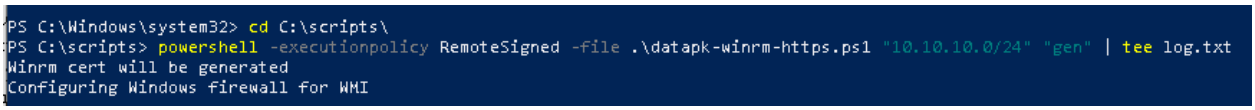


Рисунок 110 — Запуск скрипта для настройки winrm https

Результат шага: произойдет настройка протокола winrm https на заданных IP-адресах.

Ознакомьтесь с содержанием файла **log.txt**.

Обсудите с преподавателем и другими обучающимися содержание логов.

Настройте протокол winexe на активе под управлением Windows XP. Для этого:

Ознакомьтесь с принципами работы скрипта в файле datapk-xp-winexe.txt.

Подключитесь к ПЛК АСУ ТП цеха 1 с учётными данными из таблицы (Таблица 1).

Скопируйте файл datapk-xp-winexe.bat и откройте его.

Результат шага: скрипт настроит протокол winexe на активе (**Рисунок 111**).

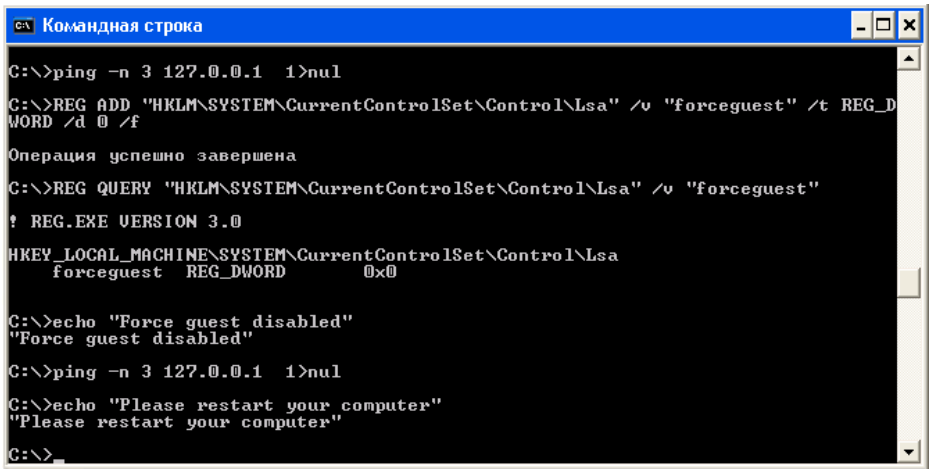


Рисунок 111 — Результат работы скрипта для настройки winexe

Перезапустите актив, чтобы изменения вступили в силу.

Настройте политику аудита безопасности. Для этого:

Нажмите комбинацию клавиш Win+R, введите secpol.msc и нажмите на кнопку ОК (**Рисунок 112**).

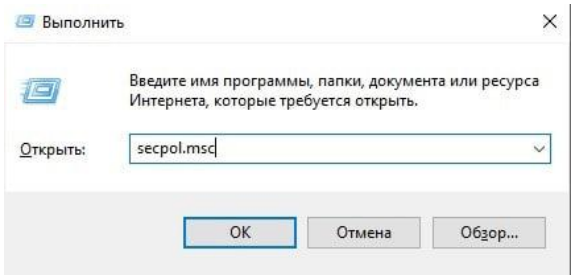


Рисунок 112 — Быстрый переход к настройкам локальной политики безопасности

> **Примечание:**
>
> Также можно перейти через панель управления («Пуск» → «Панель управления» → «Администрирование» → «Локальная политика безопасности»).

Результат шага: откроется окно «Локальная политика безопасности».

Перейдите в подраздел «Параметры безопасности» → «Локальные политики» → «Политика аудита».

Настройте политику в соответствии с таблицей (**Таблица 8**). Для этого:

Установите курсор на параметр безопасности, который хотите изменить.

Нажмите дважды левую кнопку мыши или однократно правую кнопку мыши и выберите в контекстном меню пункт «Свойства».

Измените значение параметра и нажмите «ОК».

Таблица 8 – Настройки политики аудита

Политика	**Параметр безопасности**
Аудит входа в систему	Успех, Отказ
Аудит доступа к объектам	Нет аудита

Политика	Параметр безопасности
Аудит доступа к службе каталогов	Нет аудита
Аудит изменения политики	Успех, Отказ
Аудит использования привилегий	Нет аудита
Аудит отслеживания процессов	Нет аудита
Аудит системных событий	Успех, Отказ
Аудит событий входа в систему	Успех, Отказ
Аудит управления учетными записями	Успех, Отказ

Результат шага: политика аудита будет настроена (**Рисунок 113**).

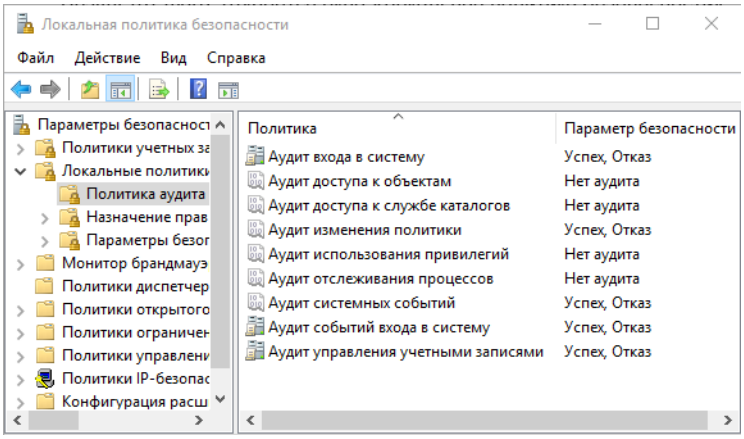


Рисунок 113 — Настроенная политика аудита

Настройте ротацию журналов. Для этого:

Нажмите комбинацию клавиш Win+R, введите eventvwr.msc и нажмите кнопку «ОК».

Примечание. Также можно перейти через панель управления («Пуск» → «Панель управления» → «Администрирование» → «Просмотр событий»).

Результат шага: откроется окно «Просмотр событий».

Настройте ротацию для журналов «Приложение», «Безопасность» и «Система». Для этого:

- Раскройте пункт меню «Журналы Windows».
- Выделите журнал, который ходите изменить.
- Нажмите правую кнопку мыши и в контекстном меню выберите пункт «Свойства» (**Рисунок 114**).

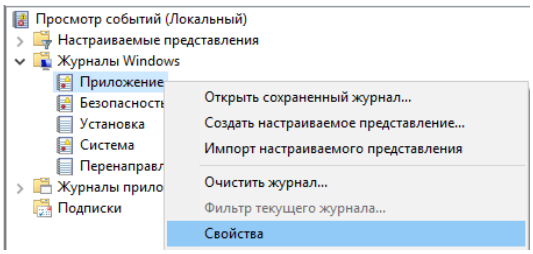


Рисунок 114 — Переход к настройкам журнала «Приложение»

Результат шага: появится окно свойств выбранного журнала (**Рисунок 115**).

Установите следующие свойства (**Рисунок 115**) журналам «Приложение», «Безопасность» и «Система»:

- Макс. размер журнала (КБ): 20480.
- При достижении максимального размера: «Переписывать события при необходимости (сначала старые события)».
- Нажмите кнопку «Применить».

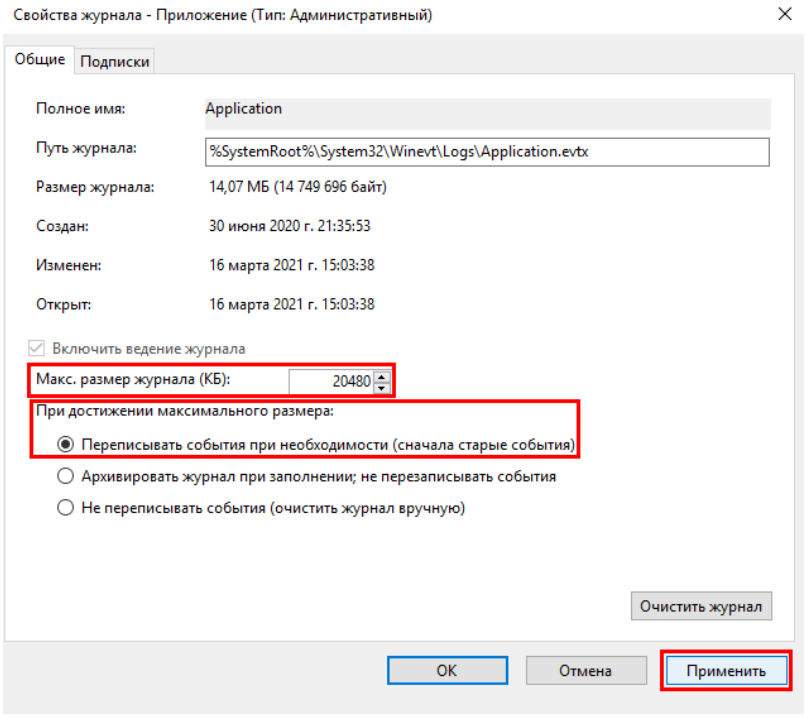


Рисунок 115 — Настройка журнала «Приложение»

> **Примечание:**
>
> Выше был описан процесс настройки активов с использованием скриптов вендора для автоматизации и ускорения процесса.
> Помимо этого, имеются полноценные руководства по настройке активов в ручном

Подключитесь к Комплексу. Для этого:

Откройте браузер.

В адресной строке введите IP-адрес ПК DATAPK, указанный в таблице (**Таблица 1**).

В окне авторизации (**Рисунок 116**) в полях «Логин» и «Пароль» введите логин и пароль учетной записи администратора Комплекса.

Рисунок 116 — Окно авторизации пользователя Комплекса

Добавьте учетные данные для подключения к активам. Для этого:

Перейдите в раздел «Администрирование» → «Учетные данные актива».

Нажмите на кнопку «Добавить учетные данные» (**Рисунок 117**).

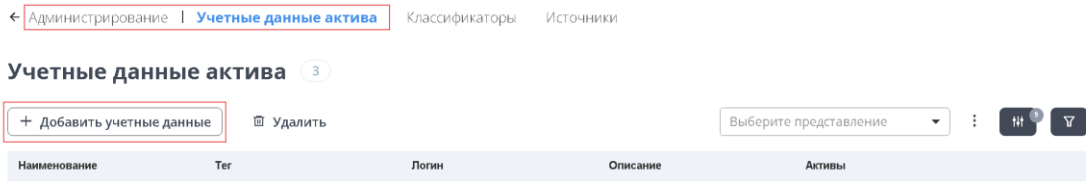


Рисунок 117 — Расположение кнопки «Добавить учетные данные»

В появившемся окне «Добавление учетных данных актива» (**Рисунок 118**) введите атрибуты учетной записи «Windows» в соответствии с таблицей (**Таблица 9**).

Таблица 9 – Учетные данные активов

Наименование	**Описание**	**Тег**	**Логин**	**Пароль**
Windows	Учетная запись ОС Windows для DATAPK	admin	datapk	P@ssw0rd
CISCO_ DATAPK	Учетная запись для коммутатора Cisco	cisco	cisco	cisco
cisco_enable	Учетная запись для привилегированного режима Cisco	cisco_en	cisco	cisco

Примечание:

Не путайте тег и логин учетной записи!
Тег — это служебное поле, которое используется в сканерах Комплекса для того, чтобы различать учетные записи, которые завел пользователь, между собой.
Примеры нескольких тегов Комплекса:

- admin;
- cisco;
- cisco_en;
- eltex;
- sa;
- snmp3

Какие теги использовать при сборе с актива, всегда можно узнать в официальной

Нажмите кнопку «Сохранить» (**Рисунок 118**).

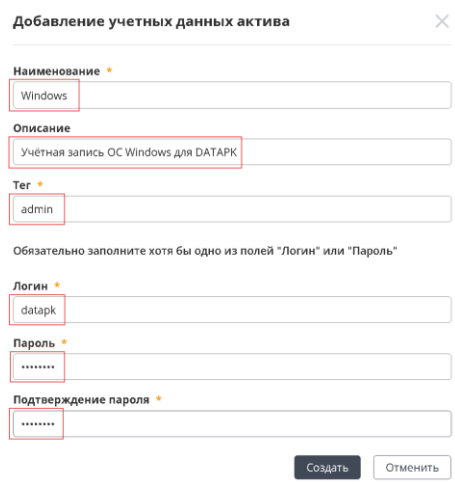


Рисунок 118 — Окно «Создание учетных данных актива»

Укажите активу учетные записи для подключения к активам. Для этого:

Перейдите в раздел «Активы» и перейдите к карточке актива АРМ оператора АСУ ТП цеха 1.

Нажмите « » напротив заголовка «Учётные данные актива».

Выберите учётные данные «Windows» и нажмите «Сохранить» (**Рисунок 119**).

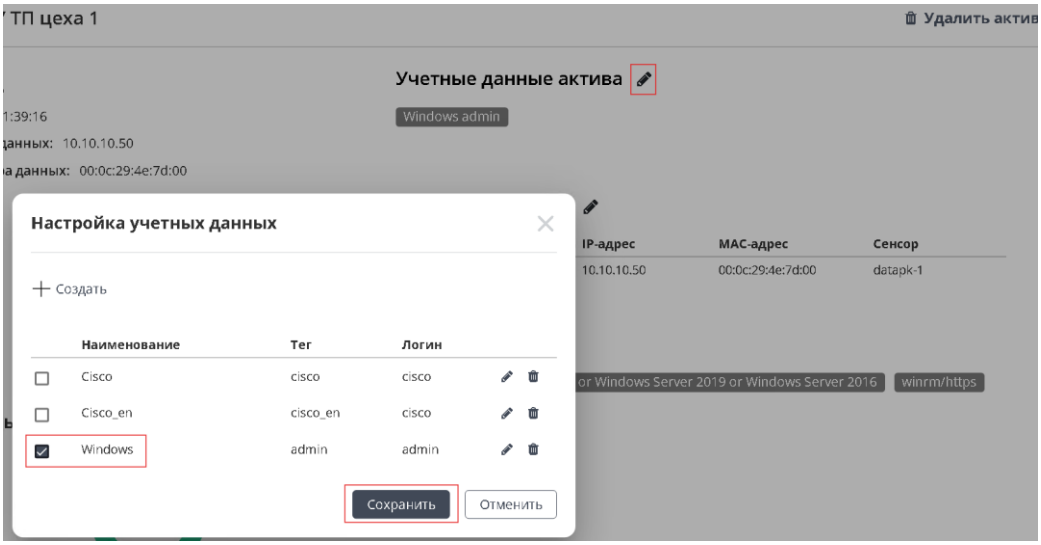


Рисунок 119 — Настройка учётных данных

Присвойте учётные данные к остальным активам.

Самостоятельное задание. Создайте две учетные записи для коммутатора в соответствии с таблицей (**Таблица 9**) и привяжите их к активу.

Лабораторное задание 3.2. Настройка сканеров. Создание конфигурационных файлов сканеров.

Цель: сформировать умение настройки сборщиков параметров (сканеров), формирования конфигурационных файлов сборщиков параметров (сканеров).

> **Примечание:**
>
> Скрипты, загружаемые в datapk, должны иметь кодировку UTF-8 (без BOM)
>
> Для редактирования и просмотра скриптов в ОС Windows рекомендуется использовать Notepad++ или другие редакторы для работы с Python. Стандартный блокнот Windows не всегда корректно отображает файлы с UTF-8, а при сохранении меняет кодировку на UTF-8 с BOM (из-за чего скрипты не загружаются на DATAPK).

Ход работы:

Создайте сканер для сбора списка пользователей ОС Windows.

Сканер — исполняемый скрипт сбора данных.

Найдите среди материалов к лабораторным работам скрипт сбора данных «**Список устройств (winrm https).py**».

Создайте цифровую подпись для скрипта сбора данных.

Перейдите на машину DATAPK. Создайте директорию с названием scripts-certs в домашнем каталоге пользователя datapk и перейдите во вновь созданную директорию следующей командой:

```
mkdir ~/scripts-certs && cd ~/scripts-certs
```

С помощью программы WinSCP скопируйте с хостовой ОС в директорию **/home/datapk/scripts-certs** на Комплексе следующие файлы:

- цифрового сертификата для подписи скриптов «**datapk_scripts.crt**»;
- ключа «**datapk_scripts.key**»;
- скрипта «**Список устройств (winrm https).py**» (**Рисунок 120**).

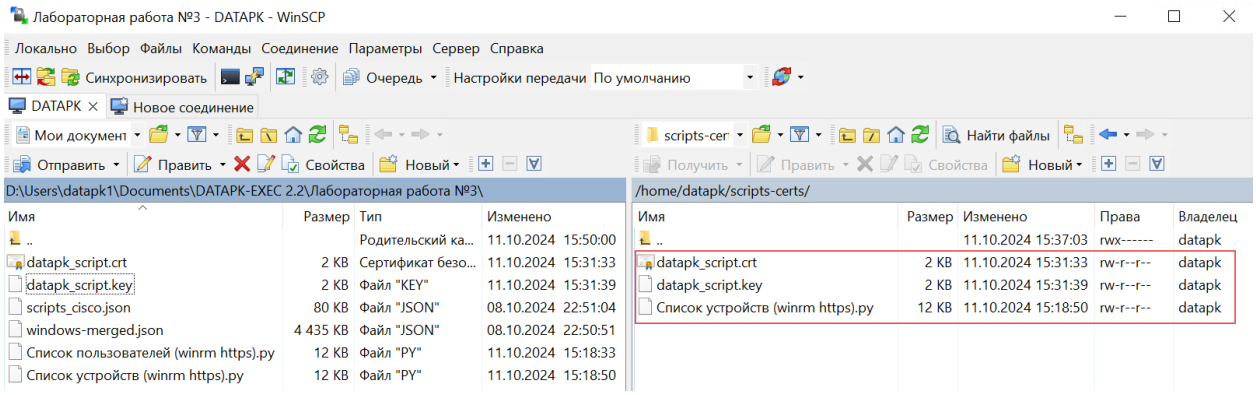


Рисунок 120 — Результат копирования файла «Список устройств (winrm https)» с помощью программы WinSCP

Убедитесь в наличии скопированных файлов с помощью команды (**Рисунок 121**):

```
ls -lA
```

```
[datapk@datapk-1 scripts-certs]$ ls -lA
итого 20
-rw-r--r-- 1 datapk datapk  1212 окт 11 15:31  datapk_script.crt
-rw-r--r-- 1 datapk datapk  1675 окт 11 15:31  datapk_script.key
-rw-r--r-- 1 datapk datapk 11743 окт 11 15:18 'Список устройств (winrm https).py'
[datapk@datapk-1 scripts-certs]$
```

Рисунок 121 — Сертификат и закрытый ключ для создания цифровой подписи скриптов

Создайте цифровую подпись для файла «Список устройств (winrm https).py», используя следующую команду:

```
openssl dgst -sha256 -sign datapk_script.key "Список устройств (winrm https).py" | openssl enc -base64 -in /dev/stdin
```

Результат выполнения команды (цифровая подпись в формате base64) будет выведена на экран (**Рисунок 122**).

```
[datapk@datapk-1 scripts-certs]$ openssl dgst -sha256 -sign datapk_script.key "Список устройств (winrm https).py" |
 openssl enc -base64 -in /dev/stdin
Kx6uBX7sbcztGFG9UN+UOW9kxfaMYEdhxK2ghR95Aq5MtUIOT1N3cjniBnbxbk3e
07ZsPtHGKH4XsLTVWGrCVT5YYA/6rtlDuGAhwwkJakMjRr2VjDtLEayo2yghPWLO
O03EMvfnl9WVt4nds6SNsavV9LZcLovuGRiDyGDW15it+Y3+HKK5QJyYJ6m+FBmT
CGeXXOZKPGQEAEa1nref0mf+W9f0RgHZf/NSvf47sR6gMBikUGfPveyeSDp+HB4y
ec9eLLbh0EDDfIUuAczll9cYzxfW6vBO9ndooBCGwLT5XJU1pqQeMWFtW/Hia4GN
LuYnJgCg3LsZqDBDxt8R5w==
[datapk@datapk-1 scripts-certs]$
```

Рисунок 122 — Результат создания цифровой подписи для файла «Список пользователей (winrm https).py»

Скопируйте полученную цифровую подпись в буфер обмена (или в текстовый файл).

Загрузите скрипт в веб-интерфейс Комплекса.

Откройте веб-интерфейс Комплекса.

Перейдите на страницу «Администрирование» → «Сканеры».

Нажмите на кнопку «Создать сканер» (**Рисунок 123**).

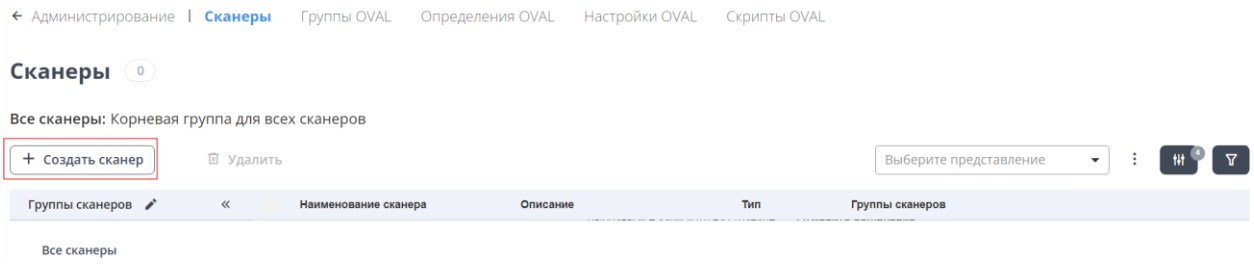


Рисунок 123 — Расположение кнопки «Создать сканер»

В открывшемся окне «Создание сканера» настройте следующие параметры (**Рисунок 124**):

- в поле «Наименование» введите «Список устройств (winrm https)»;
- в поле «Описание» введите «Сбор списка устройств ОС Windows»;
- в поле «Тип» оставьте «Конфигурации»;
- в поле «Цифровая подпись» вставьте из буфера обмена скопированную ранее цифровую подпись;
- нажмите кнопку «Импортировать». В открывшемся окне выберите файл Список устройств (winrm https).py и нажмите кнопку «Открыть».

Нажмите кнопку «Создать».

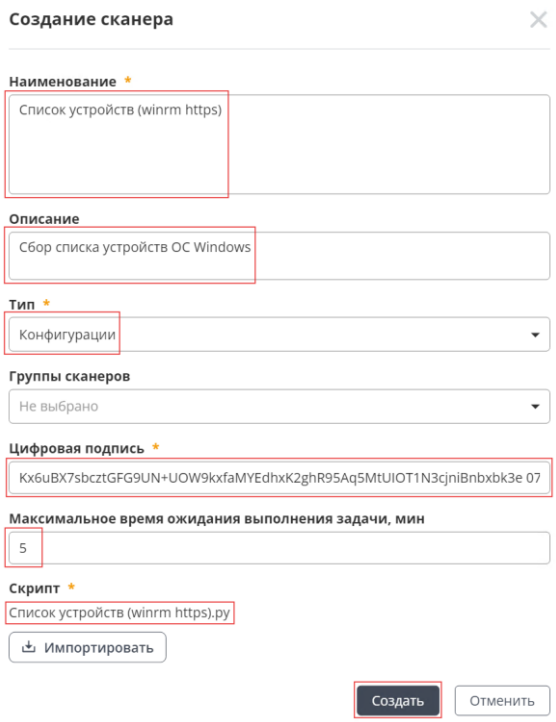


Рисунок 124 — Порядок создания скрипта в окне «Создание скрипта»

Если сканер прошел верификацию и был успешно загружен, он отобразится в списке на странице «Сканеры» (**Рисунок 125**).

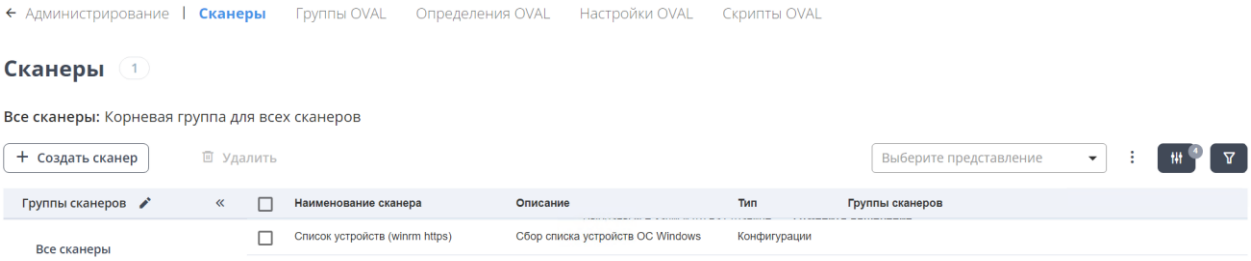


Рисунок 125 — Результат успешной загрузки сканера на странице «Скрипты»

Примечание. Если сканер не прошел верификацию, в верхнем правом углу страницы отобразится надпись: «Ошибка верификации сканера» с описанием ошибки (**Рисунок 126**).

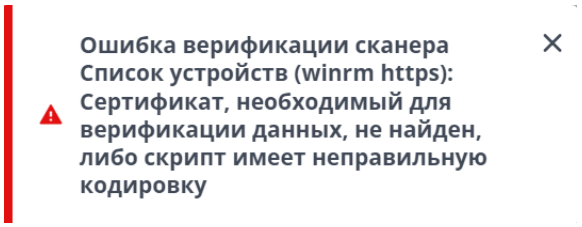


Рисунок 126 — Ошибка верификации сканера

Отредактируйте сканер. Для этого:

В списке сканеров в строке Список устройств (winrm https).py нажмите кнопку «  » («Редактировать», **Рисунок 127**).

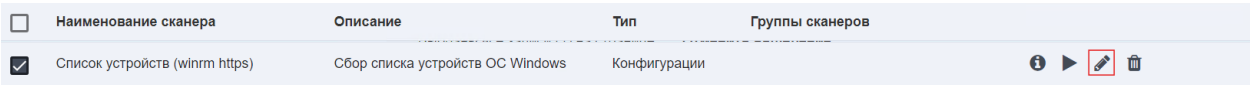


Рисунок 127 — Список сканеров и расположение кнопки «Редактировать»

В окне «Редактирование сканера» отредактируйте поле «Описание» (**Рисунок 128**).

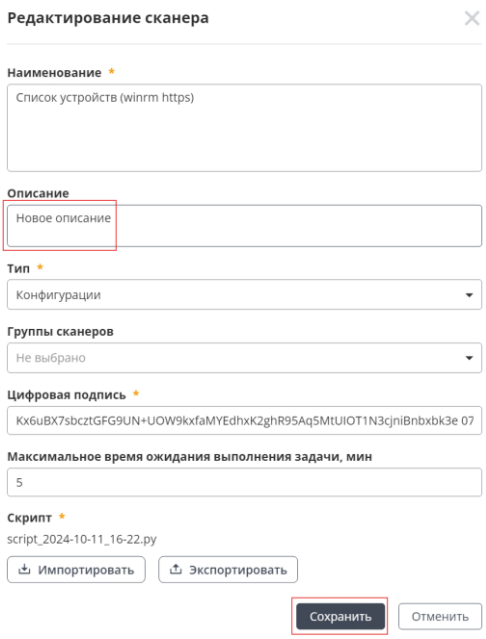


Рисунок 128 — Редактирование сканера

Нажмите кнопку «Сохранить».

Найдите скрипт в списке и убедитесь, что описание было отредактировано успешно.

Самостоятельное задание.

1. Откройте в текстовом редакторе сканер для сбора содержимого файла «hosts» в ОС Windows.
2. Используйте поиск по содержимому сканера и найдите строку, содержащую: «**command =»**
3. Добавьте в конец строки: «**hosts**» (**Рисунок 129**). Сохраните изменения и закройте файл сканера.

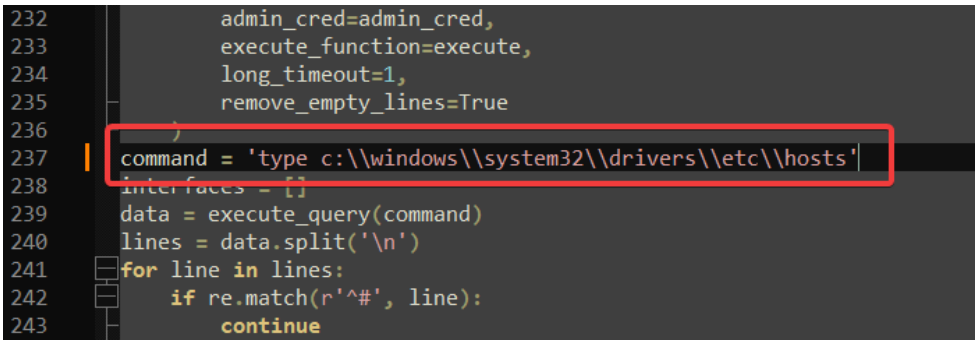


Рисунок 129 — Редактирование содержимого скрипта

4. Проделайте те же действия из данного раздела для загрузки данного сканера в Комплекс (цифровая подпись, создание сканера).
5. Соберите конфигурацию созданным сканером, удостоверьтесь, что не возникло ошибок в ходе сбора. Результат продемонстрируйте преподавателю.

Лабораторное задание 3.3. Настройка задачи сбора данных

Цель: сформировать умение настройки задач сбора данных.

Ход работы:

Задачи активного сбора позволяют запускать сразу несколько сканеров на несколько активов.

Для создания задачи потребуется:

- Создание группы сканеров;
- Создание группы активов или выбор конкретного актива;
- Создание задачи с группами сканеров и активов, с указанием расписания сбора данных.

Задачи должны создаваться на схожие активы, чтобы не возникло ситуации, когда сбор с актива осуществляется по протоколу, который актив не поддерживает.

Создание группы сканеров

Будет создана группа сканеров для сбора конфигураций по протоколу winrm https.

Перейдите на страницу «Администрирование» → «Сканеры» (**Рисунок 130**).

Нажмите рядом с надписью «Группа сканеров» кнопку для группы сканеров.

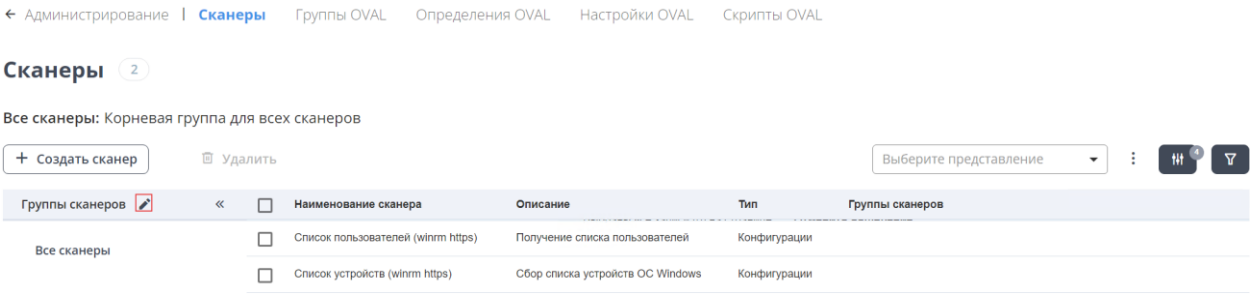


Рисунок 130 — Расположение кнопки «Редактировать» для групп сканеров

Нажмите кнопку «+» напротив группы, которая будет вышестоящей для создаваемой группы сканеров (**Рисунок 131**).

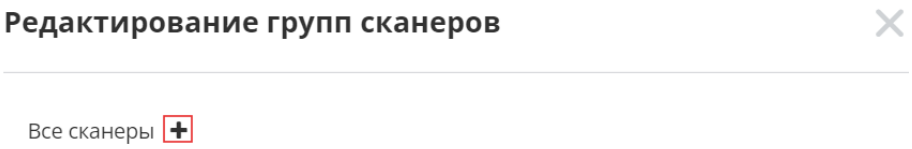


Рисунок 131 — Страница редактирования группы сканеров

В появившемся окне «Создание группы сканеров» введите следующие параметры (**Рисунок 132**):

- в поле «Наименование» введите «Сбор конфигураций по winrm https»;
- в поле «Описание» введите «Сканеры по winrm https»;
- в поле «Вышестоящая группа» выберите из списка группу «Все сканеры».

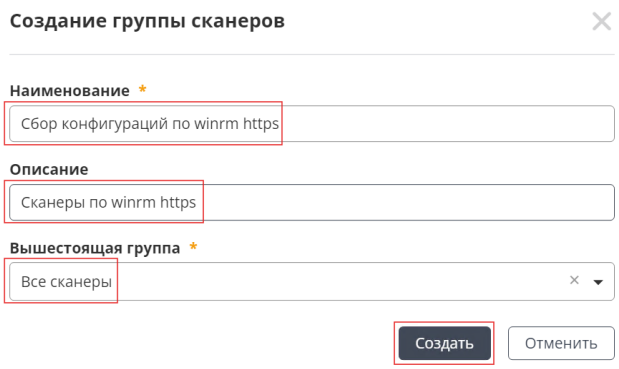


Рисунок 132 — Создание группы сканеров

В списке сканеров найдите сканер «Список пользователей (winrm https)». И нажмите на кнопку «  » (редактировать) (**Рисунок 133**).

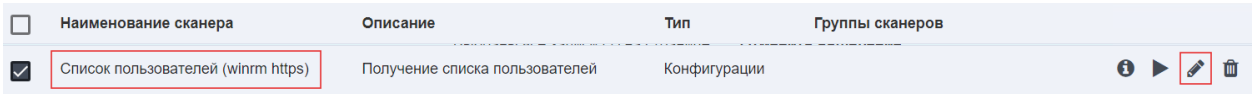


Рисунок 133 —Редактирование сканера

В поле «Группы сканеров» выберите ранее созданную группу сканеров и нажмите «Сохранить» (**Рисунок 134**).

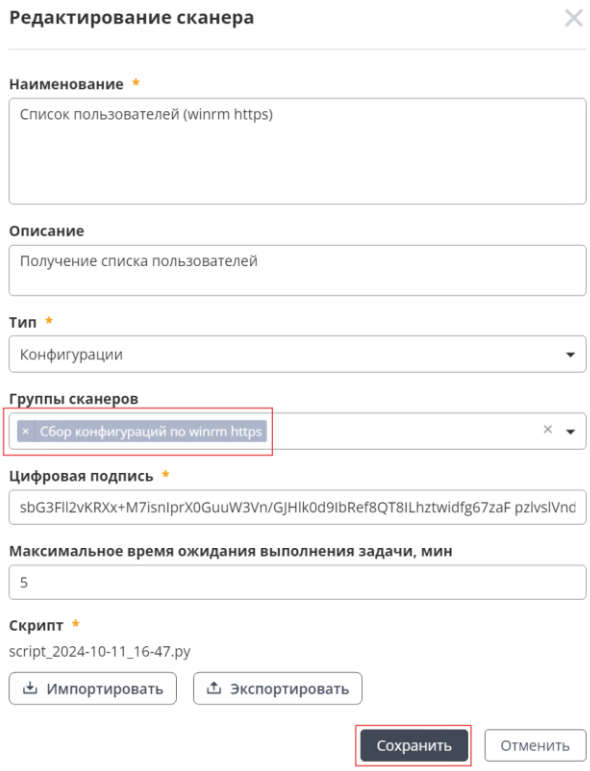


Рисунок 134 —Добавление сканера к группе сканеров

Для сканера «Сбор устройств (winrm https)» воспользуйтесь способом перетаскивания сканера:

- наведите курсор на сканер;
- зажмите левую кнопку мыши;
- перетащите сканер на ранее созданную группу сканеров;
- отпустите левую кнопку мыши.

Результат шага: отобразится окно подтверждения (**Рисунок 135**).

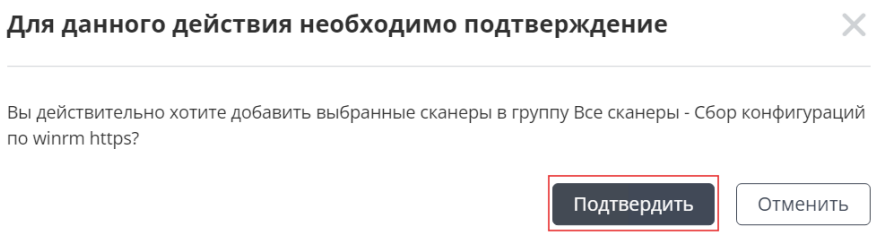


Рисунок 135 —Подтверждение добавления сканера в группу

Нажмите «Подтвердить».

Создание группы активов

Перейдите на страницу «Активы» и нажмите на кнопку  рядом с надписью «Группы активов» в левой части окна (**Рисунок 136**).

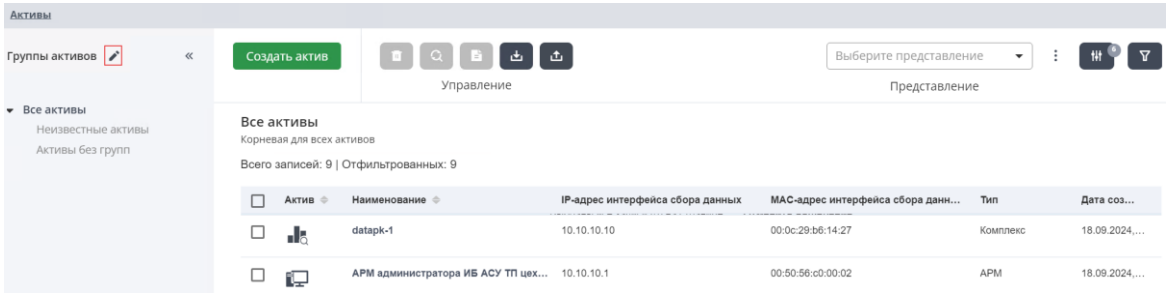


Рисунок 136 — Расположение кнопки «Редактировать» для групп активов

Нажмите кнопку «✚» напротив группы, которая будет вышестоящей для создаваемой группы активов (**Рисунок 137**).

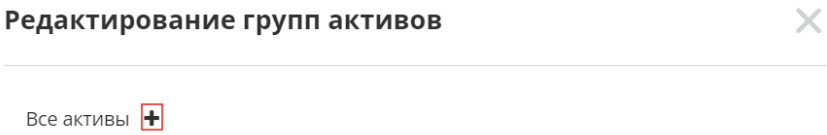


Рисунок 137 — Окно редактирования групп активов

В появившемся окне «Создание группы активов» введите следующие параметры (**Рисунок 138**):

- в поле «Наименование» введите «Windows 10»;
- в поле «Описание» введите «Активы с ОС Windows 10»;
- в поле «Вышестоящая группа» выберите из списка группу «Все активы».

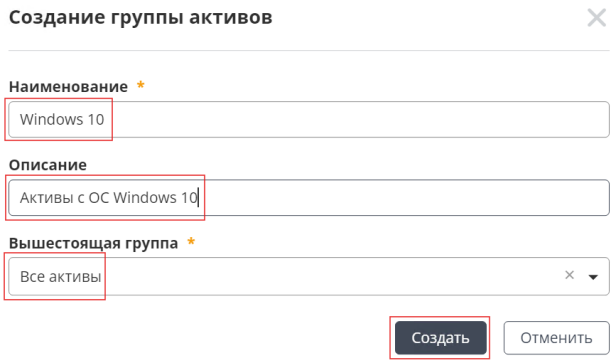


Рисунок 138 —Создание группы активов

Нажмите «Создать» и далее нажмите «Сохранить».

Добавьте актив «АРМ оператора АСУ ТП цеха 1» в созданную группу активов. Сделать это можно на вкладке «Описание актива» в настройках самого актива.

Создание задачи сбора

Будет создана задача сбора данных для сканера сбора списка устройств Windows. Для этого:

Перейдите на страницу «Инспекция активов» → «Задачи сбора».

Нажмите на кнопку «Создать задачу» (**Рисунок 139**).

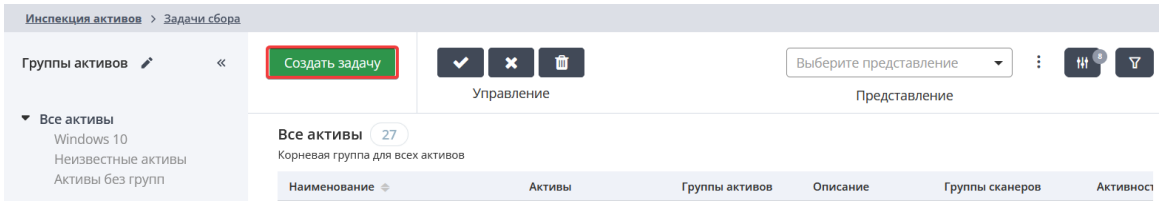


Рисунок 139 — Расположение кнопки «Создать задачу»

В появившемся окне «Создание задачи» введите следующие параметры задачи (**Рисунок 140**):

- в поле «Наименование» введите «Задача сбора конфигураций ОС Windows»;
- в поле «Описание» введите «Сбор конфигураций ОС Windows»;
- в поле «Активы» выберите «АРМ оператора АСУ ТП цеха 1»;
- в поле «Группы активов» выберите группу «Windows 10»;
- в поле «Группа сканеров» выберите из списка группу, в которую входят сканеры с наименованием «Список устройств (winrm https)» и «Список пользователей (winrm https)».

Нажмите кнопку «Создать».

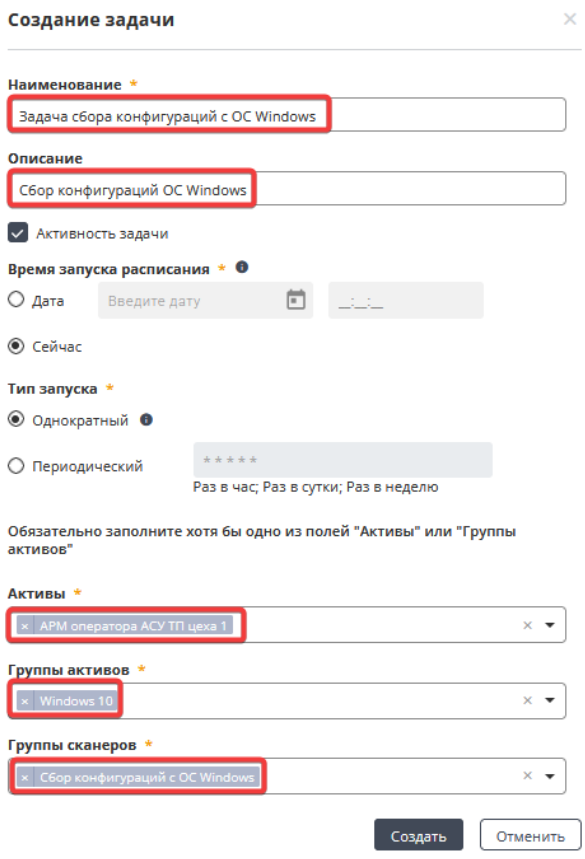


Рисунок 140 — Порядок создания задачи сбора данных

Проверьте статус задачи, созданной ранее (**Рисунок 141**).

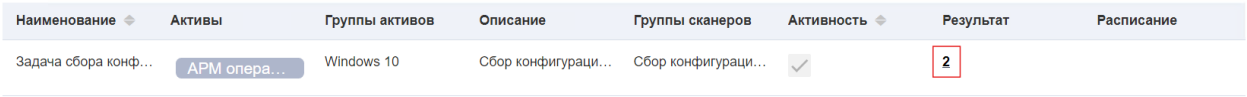


Рисунок 141 — Список задач с результатами выполнения

Импортируйте сканеры для оборудования производства компании Cisco Systems для этого:

- перейдите в раздел «Администрирование» → «Импорт и экспорт»;
- в блоке «Сбор данных» нажмите на кнопку рядом с надписью «Группа сканеров»;
- выберите файл sciprs-cisco.json;
- нажмите «Импортировать».

Создайте задачу для сбора конфигурации с ОС «Cisco IOS» по протоколу SSH. Для этого:

Отредактируйте сканеры «ECI_CISCO_IOS_SHOW_RUNNING_CONFIG (ssh-en)» и «ECI_CISCO_IOS_SHOW_STARTUP_CONFIG (ssh-en)» так, чтобы максимальное время ожидания выполнения задачи составляло 5 минут.

- Создайте задачу со следующими параметрами:
- наименование: «Сбор конфигурации с Cisco IOS»;
- описание: «Задача сбора конфигурации с Cisco IOS»;
- сканер: «ECI_CISCO_IOS_SHOW_RUNNING_CONFIG (ssh-en)» и «ECI_CISCO_IOS_SHOW_STARTUP_CONFIG (ssh-en)».

Нажмите кнопку «Сохранить».

Проверка доступности сетевых портов

В некоторых ситуациях может быть необходимо проверить сетевые порты актива на доступность. Для этого можно использовать системные утилиты ОС Альт Сервер СП. Ниже будут примеры команд, которые могут помочь проверить доступность 22 порта (SSH) на активе 192.168.0.3:

Проверка с помощью утилиты NC:

```
nc -zv 192.168.0.3 22
```

Примеры вывода успешной (**Рисунок 142**) и неуспешной (**Рисунок 143**) проверок ниже.

Рисунок 142 — Утилита NC, порт доступен

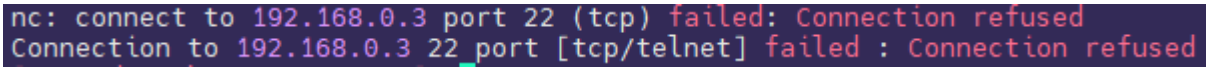


Рисунок 143 — Утилита NC, порт недоступен

Проверка с помощью утилиты NMAP:

```
nmap 192.168.0.3 -p 22
```

Примеры вывода успешной (**Рисунок 144**) и неуспешной (**Рисунок 145**) проверок ниже.

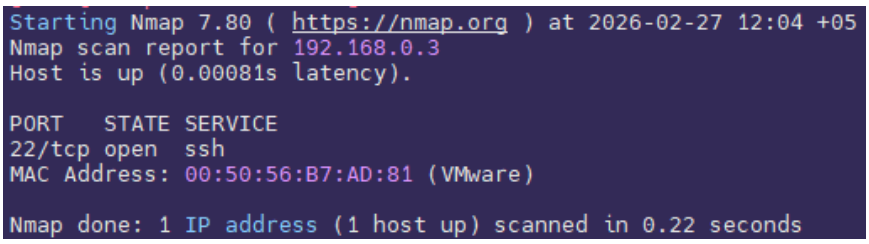


Рисунок 144 — Утилита NMAP, порт доступен

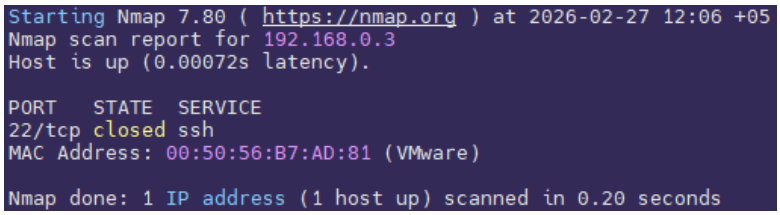


Рисунок 145 — Утилита NMAP, порт доступен

Проверка с помощью утилиты Curl:

```
curl -v http://192.168.0.3:22
```

Примеры вывода успешной (**Рисунок 146**) и неуспешной (**Рисунок 147**) проверок ниже.

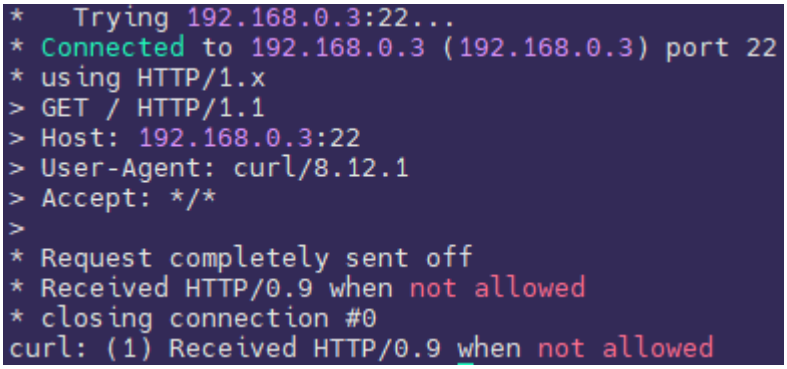


Рисунок 146 — Утилита Curl, порт доступен

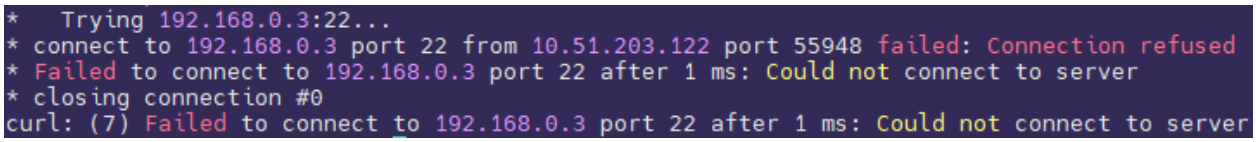


Рисунок 147 — Утилита Curl, порт недоступен

Сбор данных по устаревшим протоколам (SSHv1, Winexe 0.8, Winexe 1.0)

Данные протоколы являются устаревшими и небезопасными для использования, однако в некоторых инсталляциях по прежнему присутствуют в сети устройства, которые поддерживают только такие протоколы.

Для взаимодействия Комплекса с активами по данным протоколам:

1. Подключитесь к Комплексу по SSH учетной записью «user» и смените учетную запись на «root»:

```
su -
```

2. Выполните установку специального пакета:

```
apt-get install udv-terminal-connector-bins -y
```

Теперь Комплекс будет осуществлять сбор по устаревшим протоколам SSHv1, Winexe 0.8, Winexe 1.0.

Самостоятельное задание

Убедитесь, что пакет udv-terminal-connector-bins» был установлен или установите его.

Осуществите сбор конфигураций с актива «ПЛК», где установлена ОС Windows XP, по протоколу Winexe.

Результат сбора продемонстрируйте преподавателю.

Лабораторное задание 3.4. Работа с архивом изменений конфигурации актива

Цель: сформировать умение работы с архивом изменений конфигурации актива.

Для конфигураций актива доступны следующие действия:

- просмотр архива конфигураций;
- удаление конфигурации, в том числе групповое;
- выбор эталонной конфигурации;
- сравнение открытой конфигурации с эталонной.

Ход работы:

Просмотрите архив конфигураций. Для этого:

Перейдите в подраздел «Конфигурации» раздела «Инспекция активов» (**Рисунок 148**).

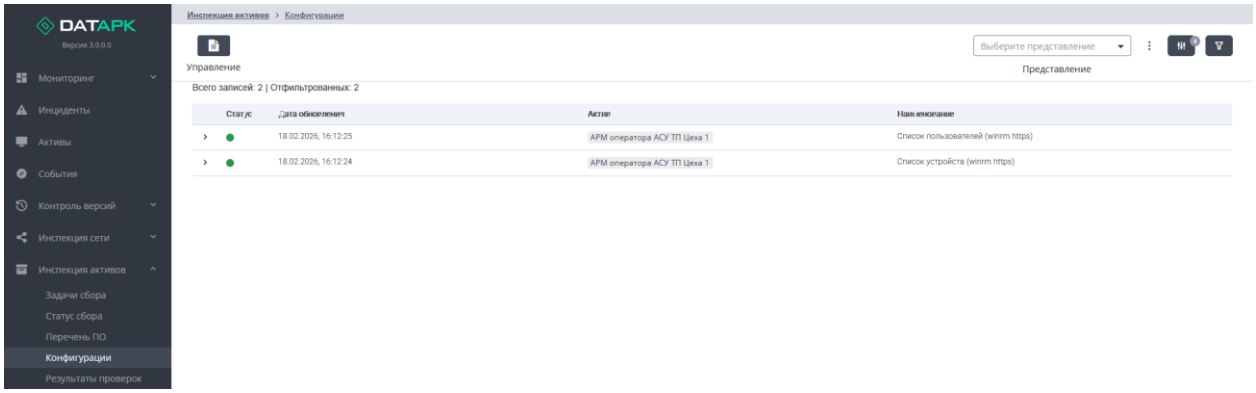


Рисунок 148 — Список конфигураций

Выберите конфигурацию «Список пользователей (winrm https)» (**Рисунок 149**).

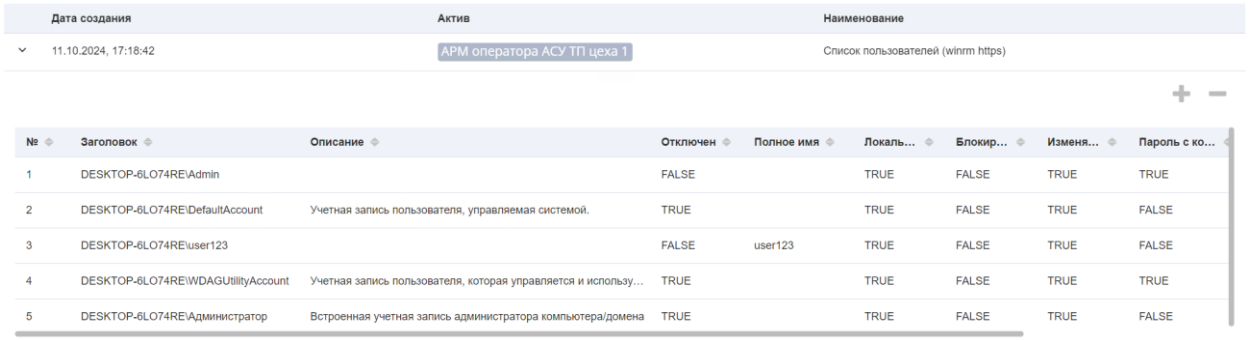


Рисунок 149 — Порядок просмотра конфигурации

Ознакомьтесь с представленным списком пользователей.

Измените состав пользователей на активе. Для этого:

Удаленно подключитесь к активу по RDP.

Подсказка. IP-адрес можно посмотреть в карточке актива.

Войдите в систему с логином «**admin**» и паролем «**P@ssw0rd**».

Создайте пользователя на активе. Для этого:

Перейдите в панель управления и в разделе «Учетные записи» нажмите «Управление учетными записями».

В открывшемся окне нажмите «Добавить» или «Создать» и введите имя «user-N», где «N» — номер вашего рабочего места. Пароль можно не задавать.

Запустите повторное сканирование списка пользователей из карточки актива АРМ оператора АСУ ТП цеха 1 со вкладки «Сбор данных» (**Рисунок 150**).

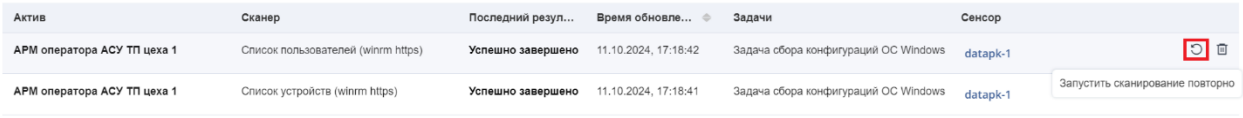


Рисунок 150 — Повторный запуск сканера

Ознакомьтесь с произведенными изменениями в веб-интерфейсе и примите новую конфигурацию за эталон. Для этого:

Перейдите в раздел «Мониторинг» → «Статус защищённости», здесь вы увидите оповещение об изменении конфигурации (**Рисунок 151**):

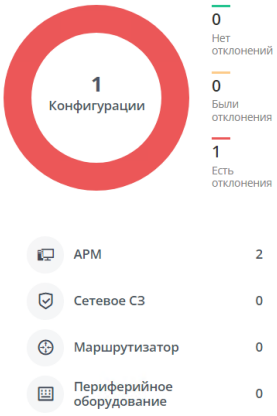


Рисунок 151 — Статус защищённости активов

Также можно увидеть изменение конфигурации на «Главном дашборде» на странице «Мониторинг» → «Панели мониторинга» (**Рисунок 152**).

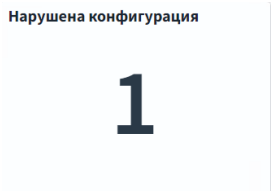


Рисунок 152 — Виджет количества зафиксированных изменений конфигураций

Нажмите на прямоугольный виджет количества зафиксированных изменений конфигураций (**Рисунок 153**).

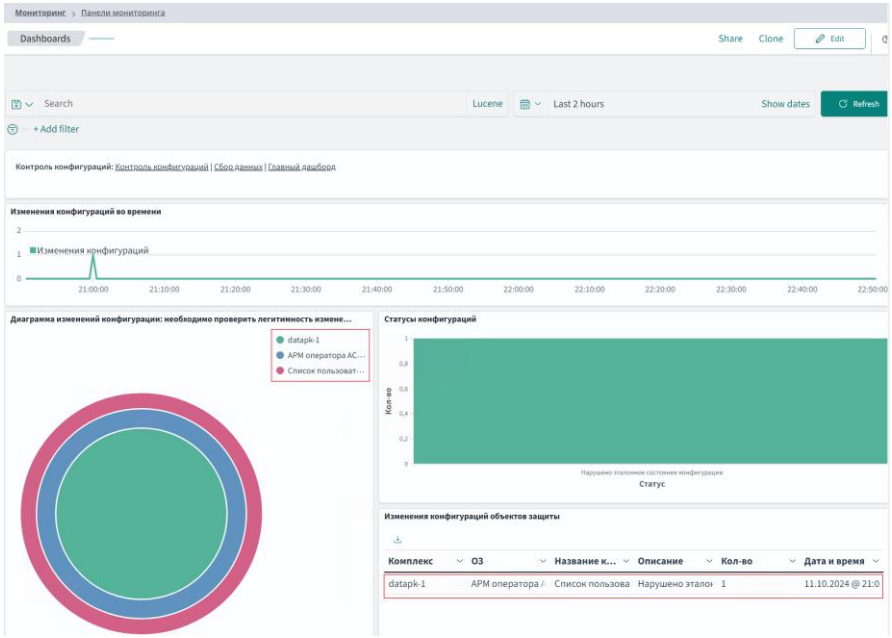


Рисунок 153 — Информация о нарушении конфигурации

Перейдите в раздел «Активы», иконка актива «АРМ оператора АСУ ТП цеха 1» будет выглядеть следующим образом  , что соответствует статусу проблемы с активом. В разделе «Конфигурации» карточки активы вы увидите также информацию о нарушении конфигурации актива (**Рисунок 154**).

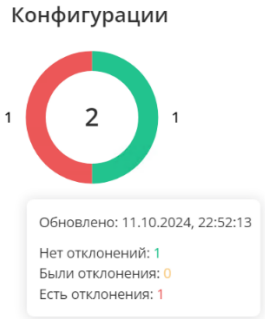


Рисунок 154 — Статусы конфигураций в карточке актива

В разделе «Связанные данные» актива нажмите на «Конфигурации» (**Рисунок 155**):

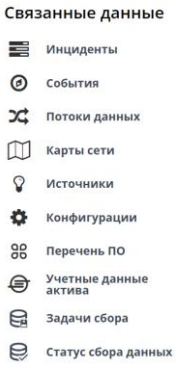


Рисунок 155 — Раздел «Связанные данные» карточки актива

Рядом с проблемной конфигурацией увидите восклицательный знак в жёлтом кружке (**Рисунок 156**).

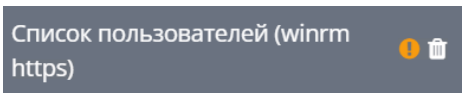


Рисунок 156 — Обозначение проблемной конфигурации

В списке конфигураций в верхней части страницы выберите новейшую конфигурацию, время сбора которой позже, чем было произведено создание пользователя на активе (**Рисунок 157**).

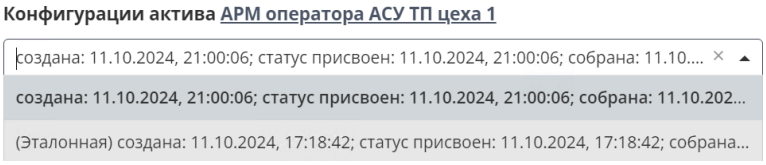


Рисунок 157 — Выбор конфигурации для просмотра

Выберите вкладку «Сравнение» для сравнения с эталонной конфигурацией (**Рисунок 158**).

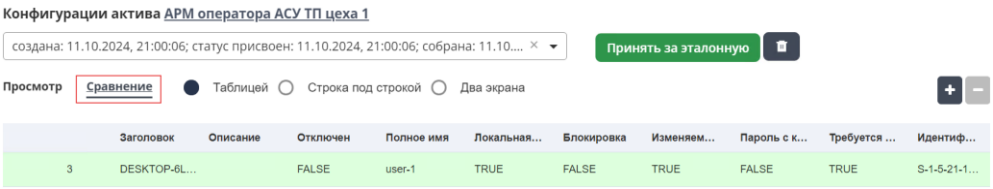


Рисунок 158 — Вкладка «Сравнить»

Выберите вариант представления «Строка под строкой» (**Рисунок 159**).

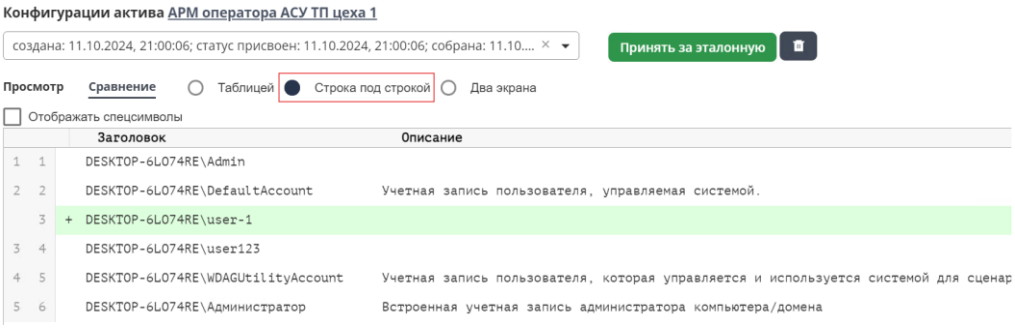


Рисунок 159 — Вариант представления «Строка под строкой»

Выберите вариант представления «Два экрана» (**Рисунок 160**).

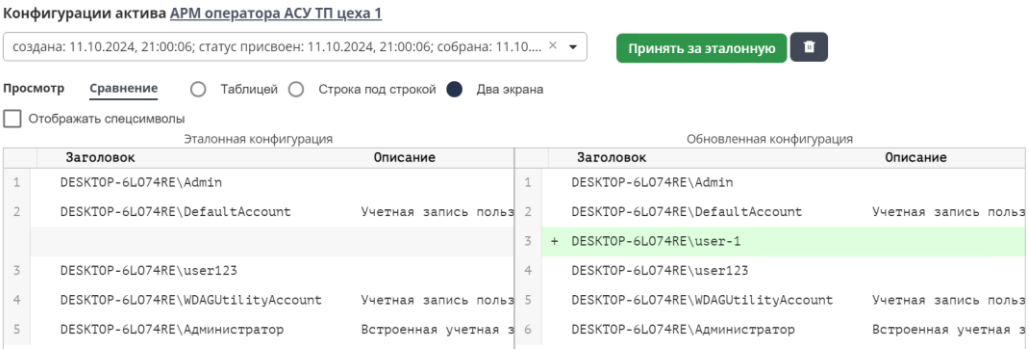


Рисунок 160 — Вариант представления «Два экрана»

Примечание. Зеленый цвет строки обозначает, что по сравнению с эталонной конфигурацией была добавлена строка.

Найдите в списке созданную вами учетную запись.

Включите отображение окружающих элементов собранной конфигурации. Для этого в представлении «Таблицей» нажмите на символ плюс справа («Показать еще по 5 окружающих строк», **Рисунок 161**).

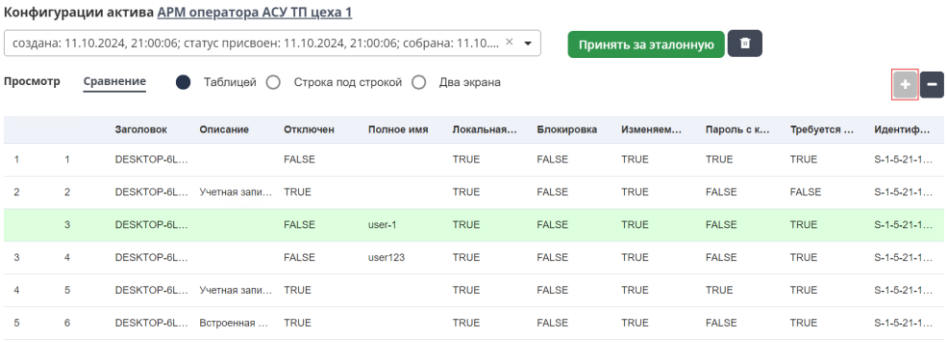


Рисунок 161 — Расширенное отображение сравнения конфигураций

Верните краткий режим отображения. Для этого нажмите «-» («Скрыть по 5 окружающих строк», **Рисунок 162**).

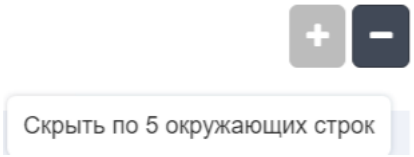


Рисунок 162 — Кнопка возвращения краткого режима отображения конфигураций

Примите конфигурацию за эталон. Для этого нажмите «Принять за эталонную» напротив новой конфигурации (**Рисунок 163**).

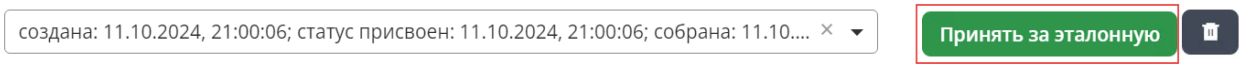


Рисунок 163 — Кнопка «Принять за эталонную»

Введите обоснование принятия конфигурации за эталон — «Администратором изменен состав пользователей».

Удалите конфигурацию. Для этого:

Выберите одну из конфигураций, не являющихся эталоном в верхней части страницы.

Примечание. Удаление эталонной конфигурации невозможно.

Нажмите «» напротив нее.

Результат шага: появится окно ввода обоснования.

Введите обоснование удаления конфигурации — «Ошибочная конфигурация».

Примечание. Обоснование удаления и других групповых операций фиксируется в событиях и может быть полезно при расследовании действий пользователей в интерфейсе DATAPK.

Ознакомьтесь с событиями по результатам изменения конфигураций. Для этого:

Перейдите в раздел «События».

Найдите в списке событие об удалении конфигурации (**Рисунок 164**).

Рисунок 164 — Событие об удалении конфигурации

Ознакомьтесь с изменениями конфигураций на панели мониторинга. Для этого:

перейдите на страницу «Мониторинг» → «Панели мониторинга» и выберите панель мониторинга «Контроль конфигураций» (**Рисунок 165**).

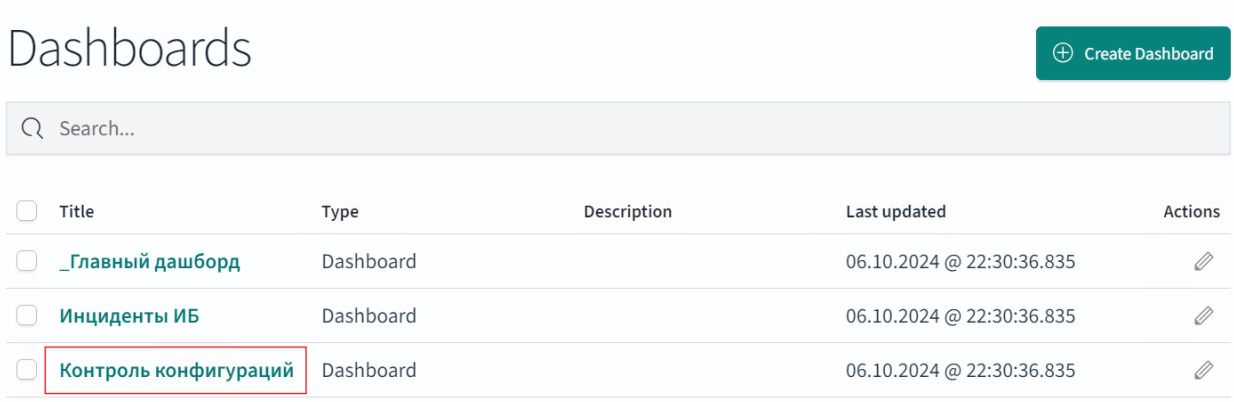


Рисунок 165 — Выбор панели мониторинга «Контроль конфигураций»

Ознакомьтесь со списком изменений конфигураций (**Рисунок 166**).

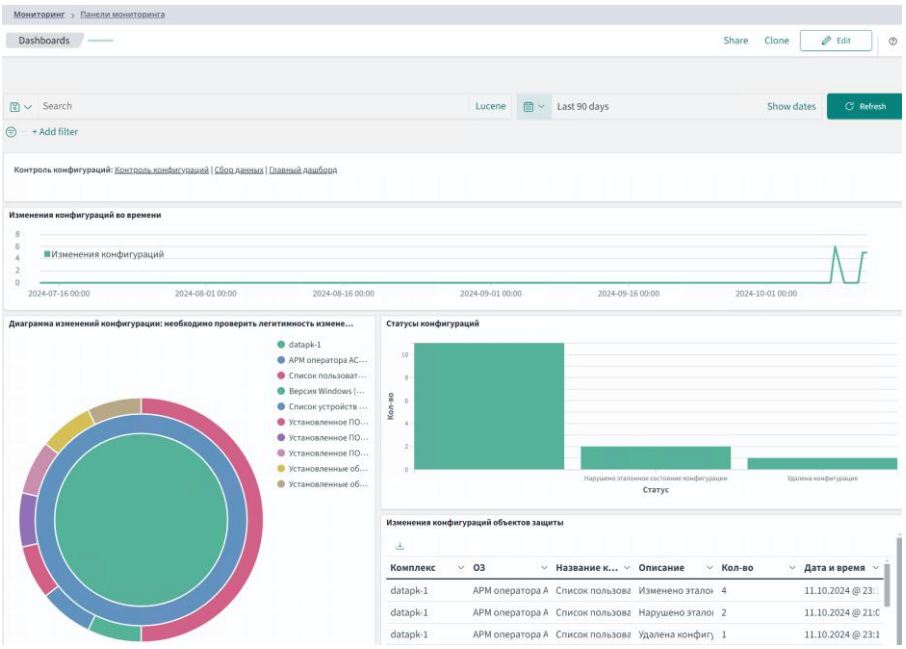


Рисунок 166 — Панель мониторинга «Контроль конфигураций»

Ознакомьтесь с примером настройки контроля целостности файлов на активе. Для этого:

На активе под управлением Windows 10 создайте тестовый каталог (**C:\testdir**).

Внутри каталога создайте два текстовых файла и заполните их произвольной информацией.

Откорректируйте скрипт «**Контрольные суммы файлов Win7+ (winrm https).py**» следующим образом: в переменную folders напишите в кавычках путь к каталогу **testdir**.

Примечание. Символ обратного слеша необходимо экранировать, поэтому ставятся 2 слеша подряд в пути к файлу.

Пример пути к каталогу:

```
folders = ["C:\\testdir"]
```

В массив **exception** запишите абсолютный путь к файлу, который не нужно проверять на целостность, например:

```
files = ["C:\\testdir\\file1.txt"]
```

Сохраните файл, подпишите скрипт, загрузите в DATAPK.

Соберите контрольные суммы, посмотрите результат.

Поменяйте содержимое одного или нескольких файлов.

Создайте в каталоге еще один файл.

Повторно запустите сбор конфигураций на проверку контрольных сумм.

Проанализируйте получившийся результат.

Лабораторное задание 3.5. Импорт группы сканеров

Цель: сформировать умение импорта и экспорта скриптов, сканеров, задач сбора данных.

Ход работы:

Перейдите в подраздел управления «Администрирование» → «Импорт и экспорт».

Напротив типа данных «Группы сканеров» нажмите (**Рисунок 167**).

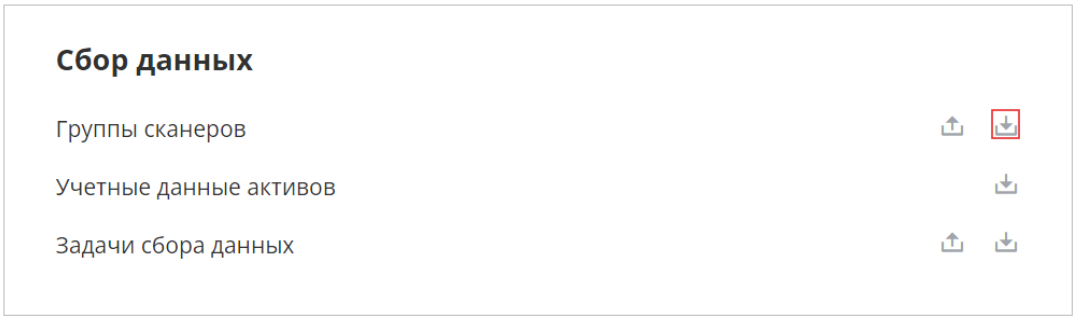


Рисунок 167 — Загрузка скриптов на странице «Обмен»

В диалоговом окне выберите файл Скрипты **scripts_configuration.json** — данные json-файлы содержат уже подписанные скрипты сбора данных.

Результат шага: появится окно «Импорт» (**Рисунок 168**), в котором предлагается выбор для разрешения конфликтов между загружаемыми (новыми) и уже загруженными (старыми) элементами справочника в DATAPK.

В диалоговом окне выберите «Оставить».

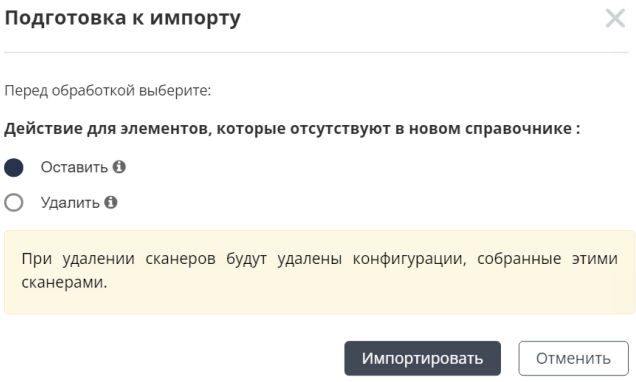


Рисунок 168 — Окно «Подготовка к импорту»

Создайте одну или несколько задач сбора данных из любых сканеров.

Экспортируйте группы сканеров и задачи со страницы «Импорт и экспорт» (**Рисунок 169**).

Рисунок 169 — Кнопка для экспорта задач, сканеров и групп сканеров на странице «Обмен»

Удалите созданную ранее задачу.

Импортируйте экспортированные ранее задачи и группы сканеров, убедитесь, что удаленные задачи появились снова.

Рекомендации по сбору данных

Сбор данных рекомендуется проводить в режиме ТО.

Не рекомендуется опрашивать актив часто (чаще 2-4 раз в сутки).

Рекомендуется разные активы опрашивать в разное время — не опрашивать в одно и то же время разные активы, разносить опрос разных активов по времени.

Задачи рекомендуется объединять по принадлежности к активу и по протоколу сбора данных.

Не рекомендуется создавать большие задачи сбора данных (более 10 сканеров).

Пример корректных задач

- конфигурации Windows (winrm/https) — состоит из сканеров, обращающихся к Windows по протоколу WinRM over HTTPS, сбор осуществляется 2 раза в сутки, при этом, время сбора не пересекается с другими задачами Комплекса.
- конфигурации Cisco (ssh, enable) — состоит из сканеров, собирающих данные с коммутаторов Cisco, используя пароль на привилегированный режим, сбор осуществляется 4 раза в сутки, при этом, время сбора не пересекается с другими задачами Комплекса.

Пример некорректных задач

Сканеры SSH — все возможные сканеры для сбора по ssh (вперемешку АСО, Linux,…) — будут ошибки сбора данных, т.к. скрипты под Cisco не выполнятся на Debian и пр., сбор осуществляется каждые 2 минуты.

События и конфигурации windows — состоит из всех возможных сканеров, собирающих данные с Windows по разным протоколам — большая + неэффективно переиспользуется соединение с активом (т.к. разные сканеры используют разные протоколы сбора). Также такая политика не универсальна — если часть активов работает по winrm/https +wmi, а другая — по winexe. Сбор осуществляется каждые 5 минут.

Частые ошибки при работе со скриптами для активного опроса

Ниже будут примеры частых ошибок, которые могут встретиться при запуске сканеров:

- **ошибка выполнения команды (No route to host)** — нет доступа (либо в принципе данный механизм сбора не применим к активу);
- **учетные данные для пользователя не найдены** — УЗ не привязана к активу/ УЗ не с тем тегом;
- **ошибка выполнения команды», «the specified credentials were rejected by the server»** — неверные учетные данные или не хватает прав на активе;
- **ошибка выполнения команды. Соединение неожиданно закрылось** — любая ошибка для протокола WinEXE (неверные УЗ, нехватка прав на активе и пр.);
- **превышено время ожидания выполнения задачи сбора событий» или «Превышено время ожидания выполнения задачи сбора данных / Превышено время ожидания, ошибка выполнения сканера, не удалось получить ожидаемое сообщение** — сканер сбора не успел выполниться за таймаут – проверить доступы, если ок – увеличить таймаут или переписать сканер (иногда из-за ошибок в регулярных выражениях возникает);
- **ошибка выполнения команды rpc_s_access_denied** — некорректные учетные данные или недостаточно прав для WMI/MS-EVEN запроса

Изменение уровня логирования (debug-режим)

Ошибки выполнения в ходе работы сканеров можно также отслеживать, если изменить уровень логирования на «DEBUG» на Сенсоре, который опрашивает активы. Уровень логирования «DEBUG» позволит увидеть выполняемые команды из скриптов для активного сбора, а также информацию, которую предоставляет актив.

Для этого:

1. Выполните подключение к Комплексу по SSH учетной записью «user» и повысьте привилегии до администратора:

```
su -
```

2. Остановите все службы Комплекса:

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

3. Откройте для редактирования файл с переменными Сенсора:

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

4. Найдите переменную «LOG_LEVEL» и установите ей значение «DEBUG» (по умолчанию значение «INFO»). Сохраните и закройте файл «sensor.env».
5. Выполните запуск служб Комплекса:

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

6. Запустите выполнение сканера на активе.
7. Проверьте логи службы «udv-terminal-connector»:

```
journalctl -eu udv-terminal-connector
```

8. Теперь вы можете видеть команды, которые выполняются при запуске скрипта, а также данные, которые актив предоставляет в результате выполнения команды из скрипта.

Пример логов Комплекса с уровнем логирования «INFO» (**Рисунок 170**):

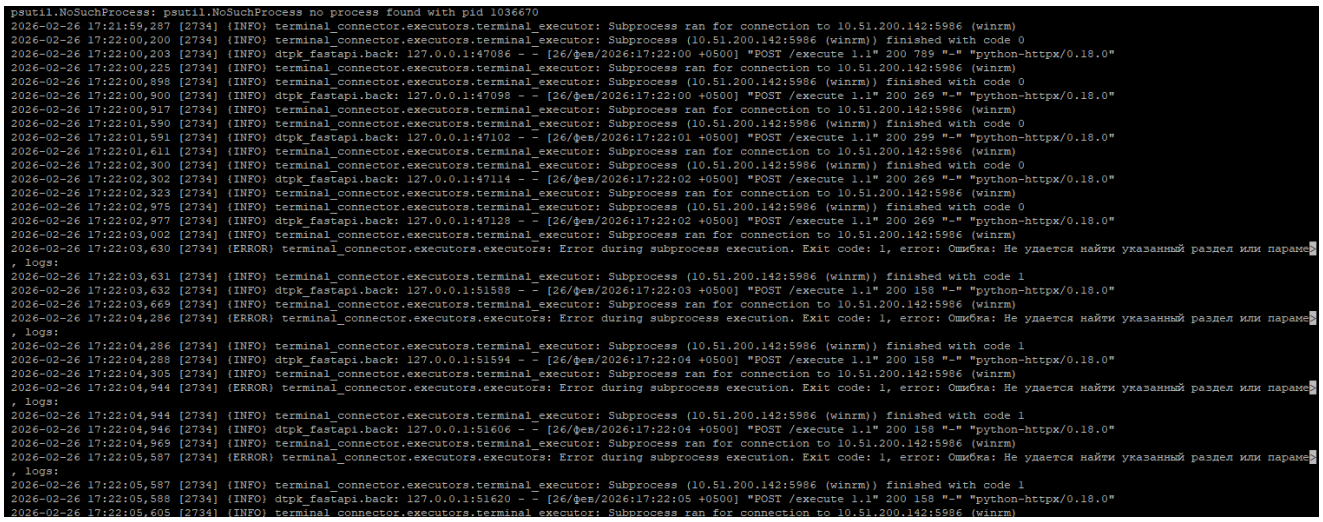


Рисунок 170 – Уровень логирования «INFO»

Пример логов Комплекса с уровнем логирования «DEBUG» (**Рисунок 171**):

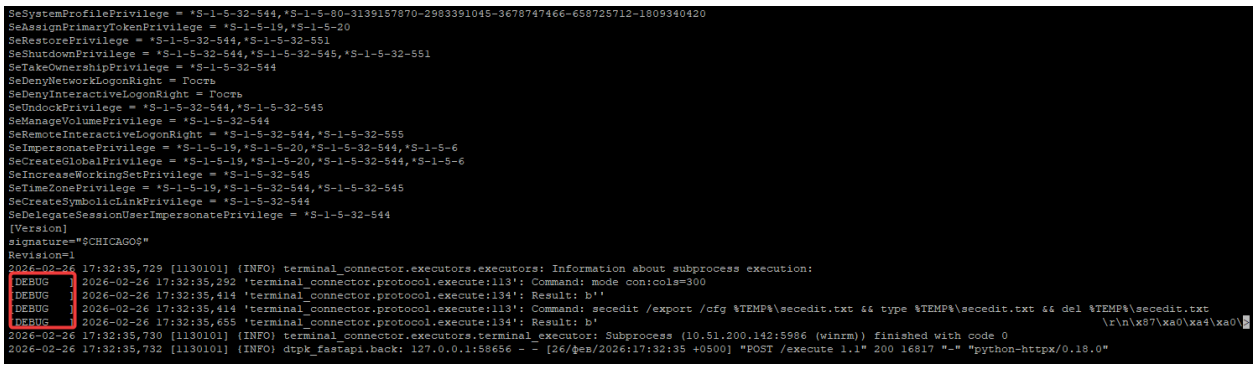


Рисунок 171 – Уровень логирования «DEBUG»

Самостоятельное задание

Проанализируйте лог службы «udv-terminal-connector.service» в файле «udv-terminal-connector.log»:

1. Откройте текстовым редактором файл «udv-terminal-connector.log».
2. В определенный момент был запущен сканер, собирающий информацию о пользователях ОС Windows. В выводе актив отдал список пользователей.
3. Найдите имена всех 5 пользователей, которые отдал актив.
4. Результаты сообщите преподавателю.

Лабораторная работа 4. Настройка подсистемы мониторинга событий

Разделы документации

- Мониторинг событий;
- Служба обнаружения вторжений;

Справочная информация

Без установленного модуля «Управление внешними событиями» сбор событий с активов не будет работать.

Внутренние события Комплекса могут отправляться во внешние системы по следующим протоколам:

- UDP;
- TCP 5424.

Для нормализации событий DATAPK использует стек «Opensearch».

По встроенным в DATAPK правилам нормализации события, полученные с активов, приводятся к нормализованному виду с использованием следующих полей событий (часть полей может отсутствовать, в зависимости от типа получаемых сообщений) – **@timestamp, @version, action, appliance_node_id, category, create_time, description, event_type, observer_id, observer_name, id, justification, message, protocol, receive_time, source_ip, source_mac, target_ip, target_mac, type, user**.

В настоящее время в комплексе используется source-based подход к нормализации событий. Это означает, что тип события (event_type) определяется в первую очередь на основе источника данных (IP-адреса), а не только по содержимому самого сообщения. Все события проходят через файл 04-event_type-translate-filter.conf, там они получают event_type = undefined.

Корреляция — способность системы выявлять неочевидные закономерности в событиях и формировать инциденты на их основе

В Комплексе так же имеются внутренние правила корреляции, которые работают независимо от установленного модуля «Управление внешними событиями». Для управления внутренними правилами корреляции в Комплексе предусмотрена возможность отключения отдельных внутренних правил корреляции.

Файлы для лабораторных работ

- **scripts_events.json** — скрипты для сбора событий из журналов ОС Windows.
- **rules_correlation_RU.json** — правила корреляции.
- **policy_correlation_RU.json** — политика корреляции.
- **schemes_correlation_RU.json** — схемы корреляции.
- **3-0-dashb.ndjson** — панели мониторинга.

Лабораторное задание 4.1. Установка модуля «Управление внешними событиями»

Цель: **сформировать навыки установки модуля EEM.**

Ход работы:

> **Примечание:**
> Без установленного модуля «Управление внешними событиями» сбор событий с активов не будет работать

Для установки модуля потребуется остановить комплекс:

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

Далее установить udv-external-events-system с помощью команды:

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

Удалить содержимое директории /var/lib/rabbitmq/:

```
rm -rf /var/lib/rabbitmq/*
```

Перезапустить комплекс

```
systemctl restart udv-* --all
```

Лабораторное задание 4.2. Настройка и редактирование сканеров сбора данных. Настройка параметров доступа в реквизитах активов

Цель: сформировать навыки настройки и редактирования сканеров сбора данных.

Ход работы:

В рамках лабораторного задания рассматриваются настройки сбора событий ОС Windows.

Настройте сбор событий из журналов MS Windows. Для этого:

Загрузите сканеры «windows-merged.json» в веб-интерфейс Комплекса, если это не было сделано ранее.

Создайте задачу на основе загруженных сканеров. Для этого:

Перейдите на страницу «Инспекция активов» → «Задачи сбора» (**Рисунок 172**).

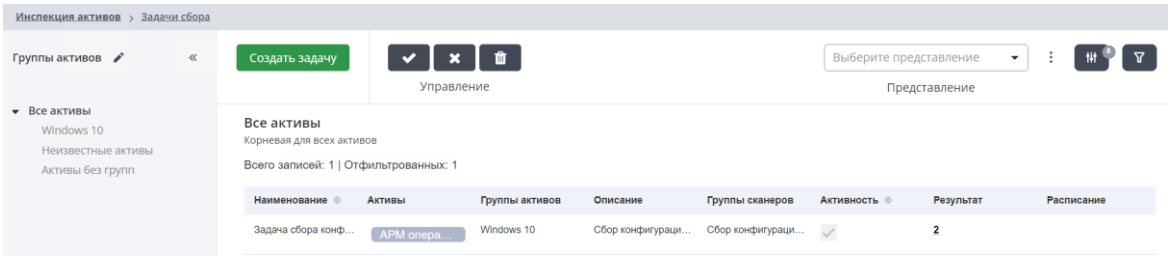


Рисунок 172 – Путь к разделу «Задачи сбора»

Нажмите кнопку «Создать задачу».

В появившемся окне «Создание задачи» введите следующие параметры задачи (**Рисунок 173**):

- в поле «Наименование» введите «Сбор событий Windows XP»;
- в поле «Описание» введите «Задача сбора событий Windows XP»;
- в поле «Активы» выбрать ПЛК АСУ ТП цеха 1;
- в поле «Группа сканеров» выберите группу сканеров, в которую входят сканеры:
  - События Windows Application Windows XP (mseven).
  - События Windows Security Windows XP (mseven).
  - События Windows System Windows XP (mseven).
- выберите «Тип запуска» - «Периодический» и введите расписание работы задачи «***/1 * * * ***» (раз в минуту, в формате расписания cron);

Внимание! Данное расписание работы задачи используется исключительно для целей обучения. В реальной АСУ ТП нужно выставлять расписания в соответствии с эксплуатационной документацией.

Обратите внимание, что сканеры, добавляемые в этой лабораторной работе, будут иметь тип «События». Это значит, что на их основе будут собираться не конфигурации, как в предыдущей лабораторной работе, а события.

Нажмите кнопку «Создать».

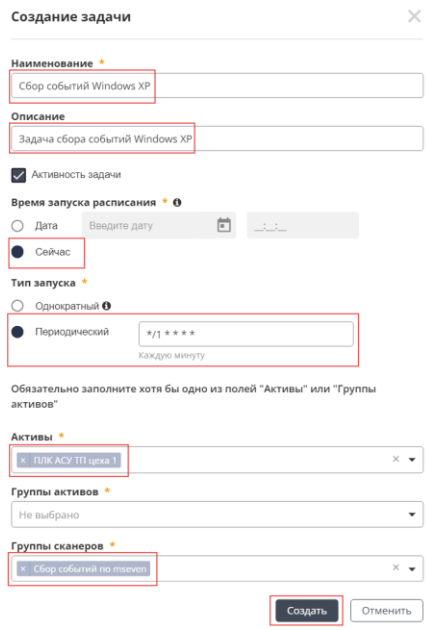


Рисунок 173 – Создание задачи сбора событий с Windows XP

Если сбор событий не сработал – проверьте наличие учетных данных в настройках актива и наличие самой учетной записи на активе.

Создайте еще одну задачу со следующими параметрами (**Рисунок 174**):

- в поле «Наименование» введите «Сбор событий Windows 10»;
- в поле «Описание» введите «Задача сбора событий Windows 10»;
- в поле «ОЗ» выбрать АРМ АСУ ТП цеха 1;
- в поле «Группа сканеров» выберите из списка группу сканеров, в которую входят следующие сканеры:
  - События Windows Application (winrm https).
  - События Windows Security (winrm https).
  - События Windows System (winrm https).
- выберите «Тип запуска» – «Периодический» и введите расписание работы задачи «***/1 * * * ***» (раз в минуту, в формате расписания cron).

Нажмите кнопку «Создать».

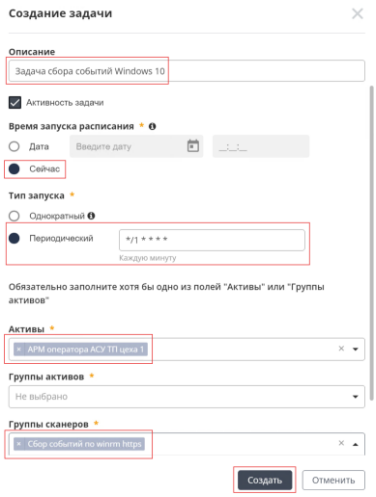


Рисунок 174 – Создание задачи сбора событий с Windows 10

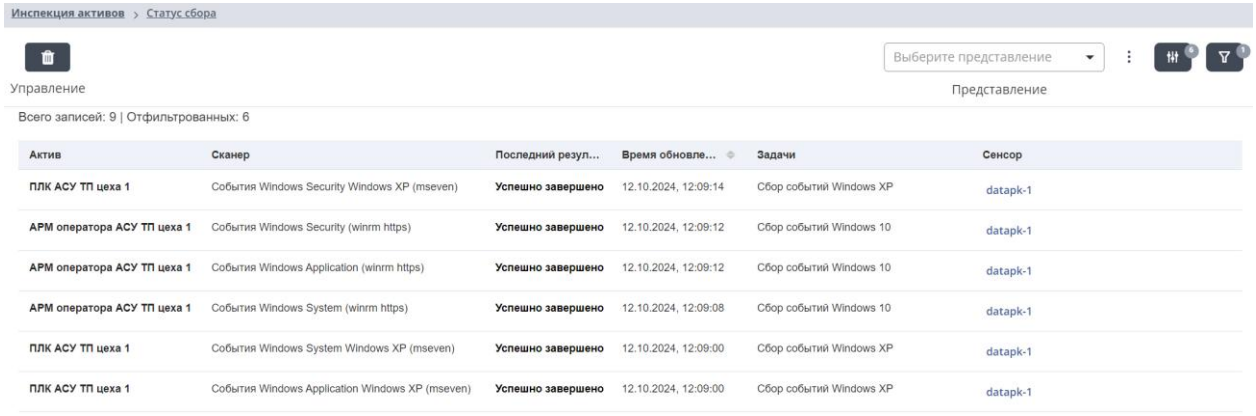


Рисунок 175 – Сообщения об успешном сборе событий

Просмотрите полученные события (**Рисунок 176**). Для этого:

Перейдите в «События» и далее в «Экспертный режим».

В поле контекстного поиска введите слово «События», чтобы найти события успешного сбора данных:

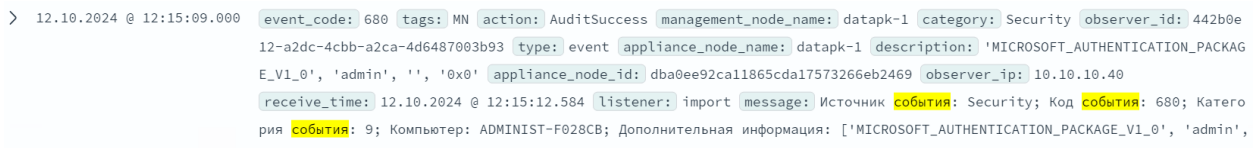


Рисунок 176 — Пример события о сборе данных сканером

Сгенерируйте и просмотрите событие на активе «АРМ оператора АСУ ТП цеха 1». Для этого:

- Откройте приложение «Удаленный рабочий стол».
- Войдите на актив
- Примечание. IP-адрес можно также посмотреть в карточке актива.
- Создайте пользователя («Панель управления» → «Учетные записи пользователей» → «Добавление и удаление учетных записей пользователей»).

Просмотрите событие о добавлении пользователя в журнале «Безопасность» ОС Windows. Для этого (**Рисунок 177**):

- В меню «Пуск» введите «Просмотр событий».
- Перейдите к журналу Windows «Безопасность».
- Найдите событие о создании пользователя.

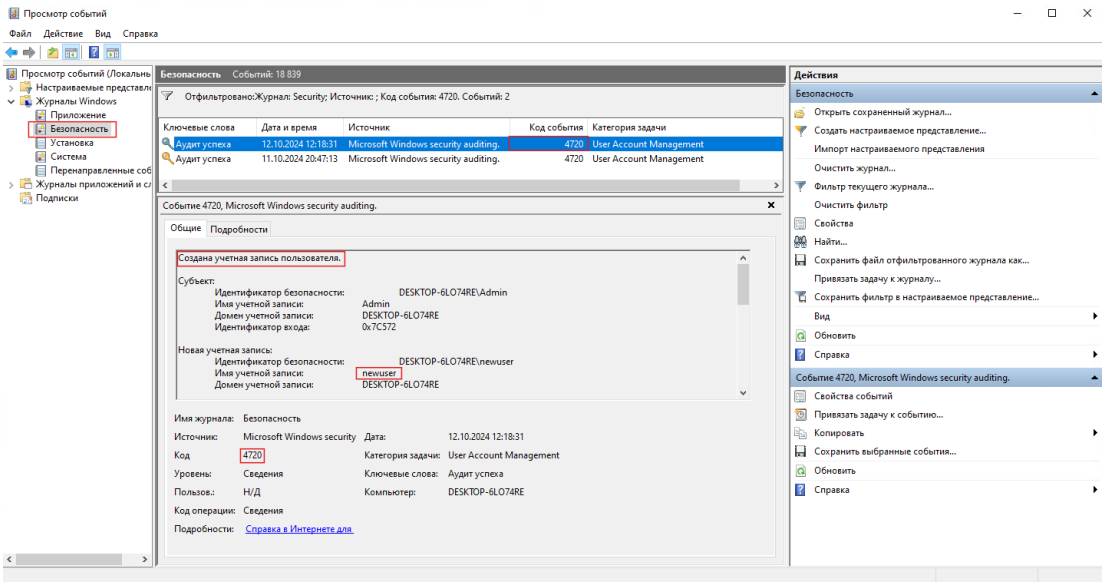


Рисунок 177 — Событие о создании учетной записи пользователя

Просмотрите событие о добавлении пользователя в веб-интерфейсе Комплекса. Для этого:

Перейдите в карточку актива.

Перейдите к событиям актива через его вкладку «Связанные данные» (**Рисунок 178**).

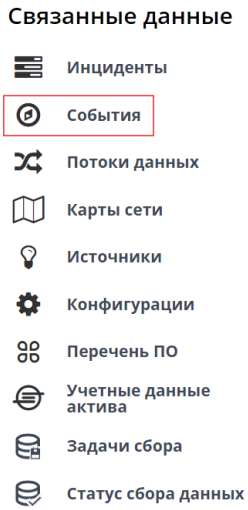


Рисунок 178 — Кнопка перехода к событиям актива на панели «Связанные данные»

Найдите событие «Создана учетная запись пользователя» (**Рисунок 179**).

event_code: 4720 tags: MN additional_information: Создана учетная запись пользователя (A user account was created) management_node_name: datapk-1 category: Security observer_id: ad847f21-261c-4f13-8a05-e9019d3d6024 type: event appliance_node_name: datapk-1 description: <Data Name="TargetUserName">newuser</Data> <Data Name="TargetDomainName">DESKTOP-6LO74RE</Data> <Data Name="TargetSid">S-1-5-21-1595977729-289706286-3462116362-1003</Data> <Data Name="SubjectUserSid">S-1-5-21-1595977729-289706286-3462116362-1000</Data> <Data Name="SubjectUserName">Admin</Data> <Data Name="SubjectDom

Рисунок 179 — Событие о создании учетной записи из журнала безопасности Windows

Примечание. Идентификатор события (event_code) в ОС Windows и веб-интерфейсе DATAPK совпадает.

Выполните завершение сеанса на активе и найдите событие (**Рисунок 180**) об этом в веб-интерфейсе DATAPK.

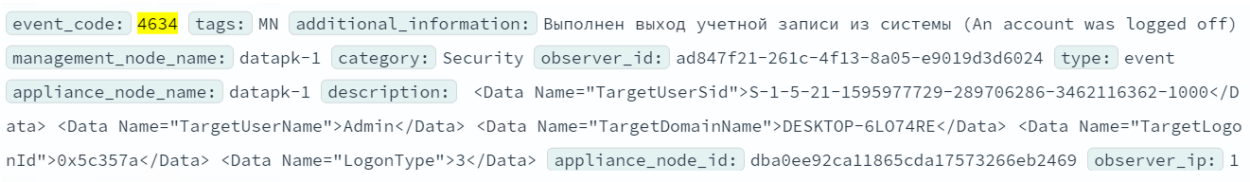


Рисунок 180 — Событие журнала Security о выходе из системы

Сгенерируйте события на активе «ПЛК АСУ ТП цеха 1» и просмотрите. Для этого:

Перейдите в карточку актива.

Убедитесь, что учетные данные привязаны.

При помощи удаленного доступа добавьте пользователя в операционной системе актива.

Запустите сбор событий журнала «Безопасность» на активе.

Перейдите в «События».

Воспользуйтесь фильтрами (например, event_code, category, event_type,) и найдите событие о добавлении пользователя.

Лабораторное задание 4.3. Настройка отправки внутренних событий во внешнюю систему

Цель: сформировать навыки настройки отправки внутренних событий во внешнюю систему.

Лабораторное задание 4.3.1. Отправка внутренних событий во внешнюю систему по протоколу Syslog 5424 без установленного модуля «Управление внешними событиями»

Данный пункт необязателен к выполннению.

Внутренние события Комплекса могут отправляться во внешние системы по следующим протоколам:

- транспорт UDP;
- транспорт TCP.

Отправка событий по протоколу UDP

Подключитесь к UDV DATAPK по протоколу SSH:

- откройте программу-клиент SSH и выполните подключение к Комплексу с учетной записью, созданной на этапе установки (например, «user»);
- в окне подключения введите пароль учетной записи и нажмите «Enter»;
- повысьте привилегии, выполнив команду для смены учетной записи на «root»:

```
su -
```

- введите пароль учетной записи «root» и нажмите клавишу «Enter».

Откройте на редактирование файл «manager.env» командой:

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

Установите следующие значения переменных:

```
EVENT_SYSLOG_SEND=true
EVENT_SYSLOG_PROTOCOL=UDP
```

Дополнительно настройте фильтрацию сообщений о передаче внутренних событий, установив требуемое значение переменной «EVENT_SYSLOG_SEVERITY».

Примечание:
При значении переменной INFORMATIONAL будут пересылаться все сообщения без исключений. При значении переменной CRITICAL будут пересылаться только критичные сообщения (сообщения от критичных источников)

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

Перезапустите сервис «udv-event-manager» командой:

```
systemctl restart udv-event-manager
```

Убедитесь, что новые события отправляются по Syslog. Для этого выполните команду:

```
tcpdump -i lo port 514 -s0 -v
```

Отправка событий по протоколу TCP 5424

Подключитесь к UDV DATAPK по протоколу SSH:

- откройте программу-клиент SSH и выполните подключение к Комплексу с учетной записью, созданной на этапе установки (например, «user»);
- в окне подключения введите пароль учетной записи и нажмите «Enter»;
- повысьте привилегии, выполнив команду для смены учетной записи на «root»:

```
su -
```

- введите пароль учетной записи «root» и нажмите клавишу «Enter».

Откройте на редактирование файл manager.env командой:

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

Установите следующие значения переменных:

```
EVENT_SYSLOG_SEND=true

EVENT_SYSLOG_PORT=515

EVENT_SYSLOG_PROTOCOL=TCP
```

Примечание:
При значении переменной INFORMATIONAL будут пересылаться все сообщения без исключений. При значении переменной CRITICAL будут пересылаться только критичные сообщения (сообщения от критичных источников)

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

Перезапустите сервис «udv-event-manager» командой:

```
systemctl restart udv-event-manager
```

Убедитесь, что новые события отправляются по Syslog. Для этого выполните команду:

```
tcpdump -i lo port 514 -s0 -v
```

Лабораторное задание 4.3.2. Настройка отправки событий во внешнюю систему по протоколу Syslog при установленном модуле «Управление внешними событиями»

Для отправки событий во внешнюю систему, например SIEM

Проверьте наличие файла «95-siem-output.conf» в директории «/etc/logstash/pipeline», выполнив команду:

```
ls /etc/logstash/pipeline
```

Если конфигурационный файл «95-siem-output.conf» отсутствует в директории «/etc/logstash/pipeline», создайте новый файл вручную, выполнив команду:

```
> 95-siem-output.conf
```

Примечание:
Данная команда должна выполняться не в директории /etc/logstash/pipeline

Откройте конфигурационный файл «95-siem-output.conf» для редактирования.

Если файл «95-siem-output.conf» пустой и был создан вручную, скопируйте в него следующий текст:

```
output {
    syslog {
        host => "1.1.1.1" # IP-адрес внешнего сервера
        port => 514 # порт получения на внешнем сервере, если он не стандартный
        codec => "json"
        protocol => "udp"
        facility => "loc0"
        severity => "informational"
        sourcehost => "${HOSTNAME}"
        appname => "datapk_event"
        rfc => "rfc5424"
    }
```

При необходимости измените в файле «95-siem-output.conf» следующие параметры:

- в поле host измените IP-адрес внешнего сервера, на который будет выполняться отправка событий;

- в поле port измените номер порта, если на внешнем сервере настроен другой порт для получения событий по Syslog UDP.

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

Поместите созданный файл в «/etc/logstash/pipeline» командой:

```
mv 95-siem-output.conf /etc/logstash/pipeline
```

Измените права на файл «95-siem-output.conf», выполнив команду:

```
chmod 777 /etc/logstash/pipeline/95-siem-output.conf
```

Перезапустите сервис «udv-logstash», выполнив команду:

```
systemctl restart udv-logstash.service
```

Убедитесь в отсутствии ошибок в журнале сообщений сервиса «udv-logstash», выполнив команду:

```
journalctl -u udv-logstash.service
```

Откройте веб-интерфейс Комплекса и убедитесь, что события генерируются.

Убедитесь, что сетевой трафик отправляется на внешний Syslog-сервер. Для этого перейдите в режим командной строки Комплекса и введите команду (***Рисунок 181***):

```
tcpdump -nn -i [наименование интерфейса для отправки событий] host
[адрес Syslog-сервера]
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp11s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:52:22.716156 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 1042
11:52:22.716391 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 872
11:52:22.716551 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 944
11:52:22.716721 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 744
11:52:22.717552 IP 10.51.201.130 > 10.51.202.39: ICMP 10.51.201.130 udp port 514
 unreachable, length 556
11:52:22.717605 IP 10.51.201.130 > 10.51.202.39: ICMP 10.51.201.130 udp port 514
 unreachable, length 556
11:52:22.717647 IP 10.51.201.130 > 10.51.202.39: ICMP 10.51.201.130 udp port 514
 unreachable, length 556
11:52:22.718272 IP 10.51.201.130 > 10.51.202.39: ICMP 10.51.201.130 udp port 514
 unreachable, length 556
11:52:22.949030 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 686
11:52:22.950098 IP 10.51.201.130 > 10.51.202.39: ICMP 10.51.201.130 udp port 514
 unreachable, length 556
11:52:23.006557 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 686
```

Рисунок 181 – Пример отправки сетевого трафика на внешний Syslog-сервер

Остановите просмотр сетевого трафика на интерфейсе, используя комбинацию клавиш Ctrl+C.

Остановка отправки событий во внешнюю систему по протоколу Syslog

Для остановки отправки событий во внешнюю систему по протоколу Syslog:

Удалите конфигурационный файл «95-siem-output.conf» из директории «/etc/logstash/pipeline», выполнив команду:

```
rm -f /etc/logstash/pipeline/95-siem-output.conf
```

Перезапустите сервис «udv-logstash», выполнив команду:

```
systemctl restart udv-logstash.service
```

Убедитесь в отсутствии ошибок в журнале сообщений сервиса «udv-logstash», выполнив команду:

```
journalctl -u udv-logstash.service
```

Лабораторное задание 4.4. Настройка правил нормализации событий

Цель: сформировать навыки настройки правил нормализации событий.

Ход работы:

Для нормализации событий DATAPK использует стек «Opensearch».

По встроенным в DATAPK правилам нормализации события, полученные с активов, приводятся к нормализованному виду с использованием следующих полей событий (часть полей может отсутствовать, в зависимости от типа получаемых сообщений) – **@timestamp, @version, action, appliance_node_id, category, create_time, description, event_type, observer_id, observer_name, id, justification, message, protocol, receive_time, source_ip, source_mac, target_ip, target_mac, type, user**.

Просмотрите предустановленные правила нормализации событий. Для этого:

Перейдите (**Рисунок 182**) на страницу «События» актива «АРМ оператора АСУ ТП цеха 1». Для этого:

Перейдите в карточку актива «АРМ оператора АСУ ТП цеха 1».

Перейдите на вкладку «Связанные данные» актива «АРМ оператора АСУ ТП цеха 1» нажмите на надпись «События» рядом с иконкой «».

Рисунок 182 – Путь к странице «События» для актива

В новой области найдите кнопку «+ Add filter» (**Рисунок 183**). В поле «Фильтр» из выпадающих меню выберите поле «target_hostname», оператора «is not», значение «имя вашего datapk.

Нажмите кнопку «Сохранить».

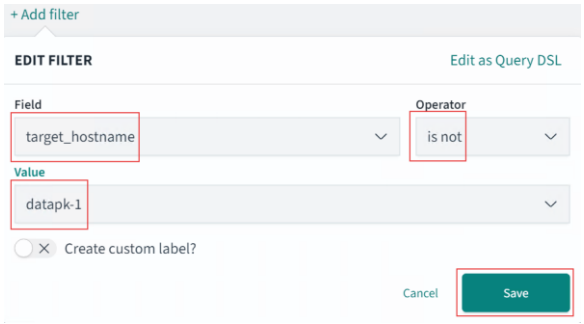


Рисунок 183 – Настройка фильтра на странице «События»

Если данные не отображаются – измените временной промежуток. Для этого нажмите « » (**Рисунок 184**) и выберите подходящий промежуток времени.

Результат шага: под поисковой строкой будут выведены результаты, удовлетворяющие фильтрам.

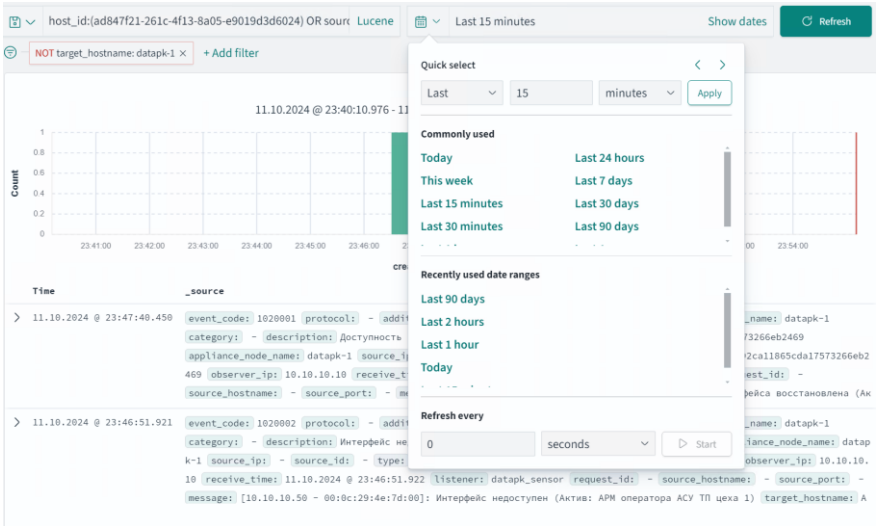


Рисунок 184 – Временной фильтр экспертного режима страницы «События»

Просмотрите правила нормализации событий, они располагаются в директории «**/etc/logstash/pipeline**». В данной директории располагается файл «**09-custom-filter.conf»**, в котором можно написать кастомные правила формата grok.

В настоящее время в комплексе используется source-based подход к нормализации событий. Это означает, что тип события (event_type) определяется в первую очередь на основе источника данных (IP-адреса), а не только по содержимому самого сообщения. Все события проходят через файл 04-event_type-translate-filter.conf, там они получают event_type = undefined.

В файле host-event_type-map.yaml можно задать список ip-адресов с заданным event_type для более точной сработки нормализации.

Далее получив event_type либо undefined либо какой-то другой из списка, событие проходит по остальным файлам конфигурации.

Самостоятельное задание.

Ознакомьтесь с содержанием других дочерних файлов в папке logstash элементов.

Лабораторное задание 4.5. Настройка механизма корреляции событий

Цель: сформировать навыки настройки механизма корреляции событий.

Ход работы:

Корреляция — способность системы выявлять неочевидные закономерности в событиях и формировать инциденты на их основе.

Отредактируйте правило обнаружения подбора паролей. Для этого:

Перейдите в раздел «Администрирование» → «Импорт и экспорт».

Найдите блок «Корреляция событий» и нажмите на рядом со строкой «Схема корреляции» и далее на рядом с «Правилами корреляции», либо сразу «Политику корреляции», так как она в себя включает уже правила и схему корреляции (**Рисунок 185**).

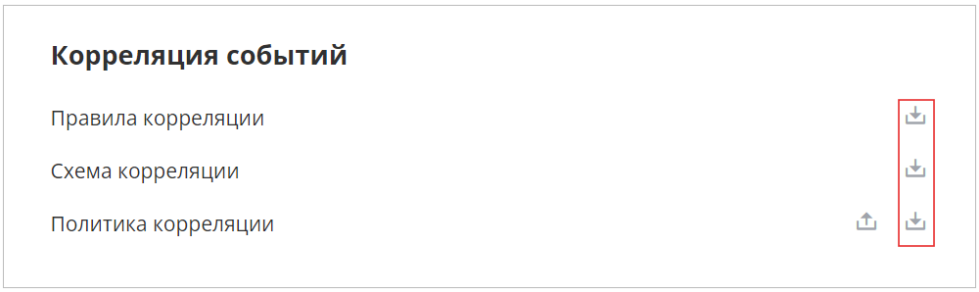


Рисунок 185 – Расположение кнопок

Найдите среди материалов к лабораторным работам файлы со схемой корреляции «schemes_correlation_RU.json» и с правилами корреляции «rules_correlation_RU.json» и выберите их для загрузки (или сразу загрузить политику корреляции «policy_correlation_RU.json» – файл содержит объединенные правила и схему).

Результат шага: появится окно подготовки к импорту.

В окне «Подготовка к импорту»:

- выберите «Оставить» уже существующие, но не пересекающиеся с загружаемыми элементы справочника (**Рисунок 186**);
- нажмите «Импортировать».

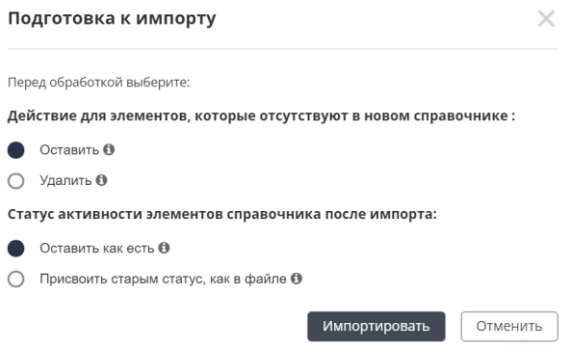


Рисунок 186 – Окно «Подготовка к импорту»

Перейдите в подраздел управления «Администрирование» → «Правила корреляции» (**Рисунок 187**).

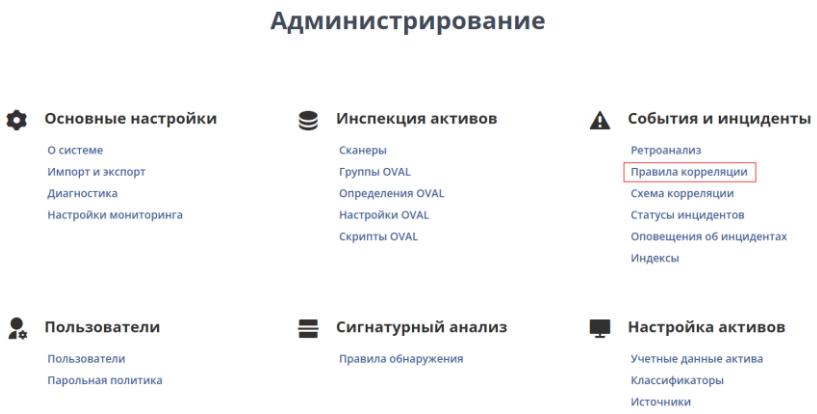


Рисунок 187 – Путь к разделу «Правила корреляции»

В меню фильтров, в поле «Наименование/Описание/Правило» введите название правила корреляции «Подбор пароля на активе с ОС Windows» и нажмите «Применить».

Отредактируйте найденное правило. Для этого:

Нажмите кнопку в правой части страницы (**Рисунок 188**).

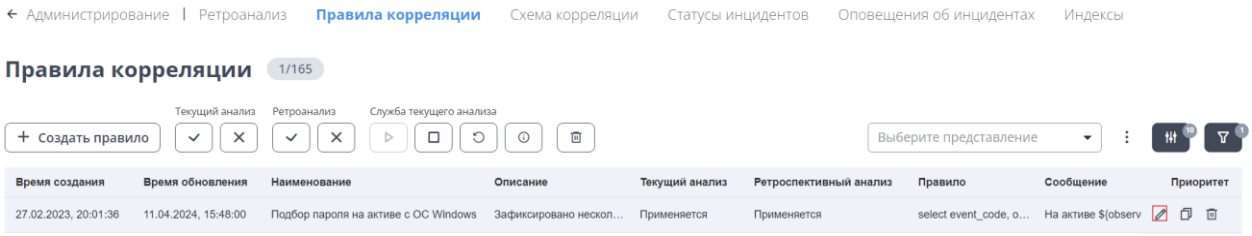


Рисунок 188 – Поиск правила корреляции

Результат шага: появится окно «Редактирование правила корреляции».

Измените параметры в соответствии с приведенными в таблице (**Таблица 10**), для уменьшения попыток входа.

Таблица 10 – Параметры настройки правила корреляции событий для обнаружения подбора паролей

Параметр	Значение
Наименование	Подбор пароля на активе с ОС Windows
Описание	Зафиксировано несколько неудачных попыток входа в ОС Windows за короткий интервал времени
Правило	**select event_code, id, observer_name, observer_id, window(id), user, observer_ip, appliance_node_id from windows_event(category="Security" and (event_code ="4625" or event_code ="529")).win:time(180 sec) group by observer_name having count(event_code) = 3**
Сообщение	На активе ${observer_name} (${observer_ip}) обнаружен подбор пароля к учетной записи пользователя ${user}
Приоритет	Очень высокий

Нажмите кнопку «Сохранить» (**Рисунок 189**).

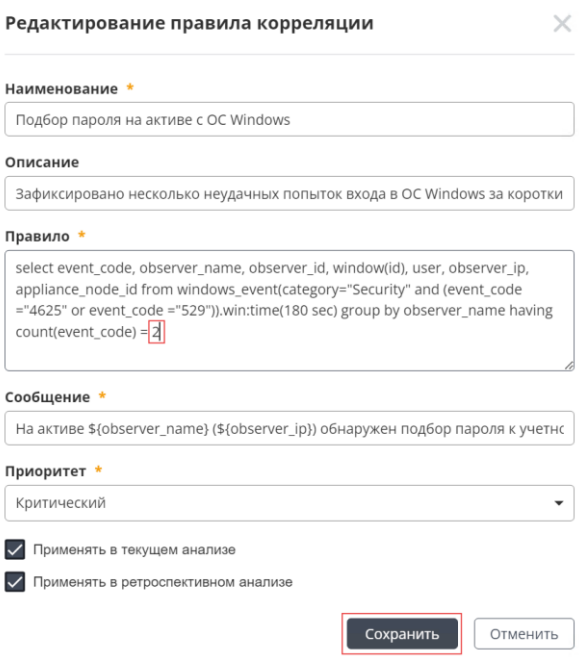


Рисунок 189 – Окно «Правило корреляции»

Убедитесь, что загруженное правило принято сервисом. Для этого:

Посмотрите количество активных правил корреляции на Комплексе, отфильтровав их в левой части страницы (если фильтры заполнены сначала нажмите «Сбросить») (**Рисунок 190**).

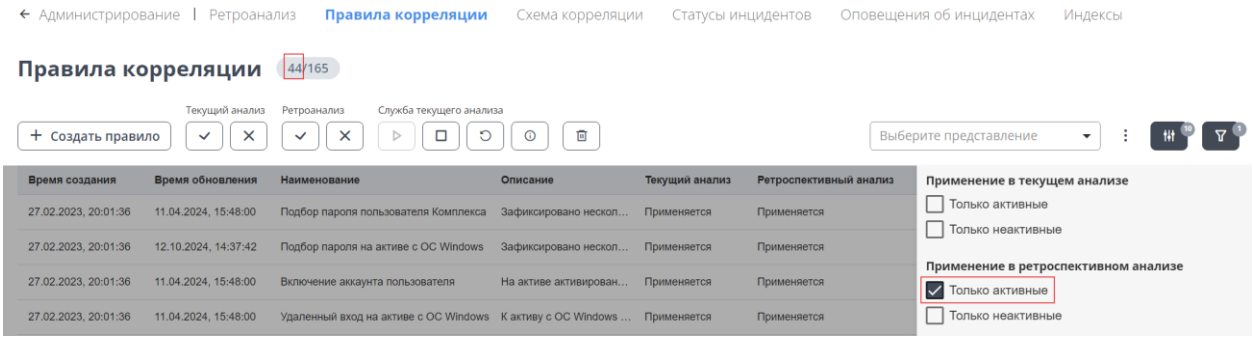


Рисунок 190 — Фильтр активности правил

На странице «Правила корреляции событий» (**Рисунок 191**) убедитесь в том, что служба корреляции событий запущена, нажав на кнопку «».

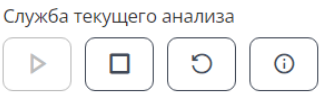


Рисунок 191 – Кнопки управления службой корреляции событий

Проверьте, что на активе «АРМ оператора АСУ ТП цеха 1» запущена задача сбора событий из журнала Windows.

Аналогично запустите задачу сбора событий из журнала Windows на активе «ПЛК АСУ ТП цеха 1». Убедитесь, что сбор событий выполняется успешно (на странице актива и на странице «События», а также «Мониторинг» → «Панели мониторинга» → «События активов»).

Проверьте работу правила обнаружения подбора паролей.

На активе «АРМ оператора АСУ ТП цеха 1» выйдите из системы и совершите не менее двух неудачных попыток входа.

На активе «ПЛК АСУ ТП цеха 1» выйдите из системы и совершите не менее двух неудачных попыток входа.

В веб-интерфейсе DATAPK перейдите подраздел оперативных данных «События и инциденты» → «События».

Выберите период отображения событий «Последний час». В поле поиска введите «Обнаружен инцидент» или **event_type:incident** и нажмите на кнопку поиска.

Результат шага: в поле просмотра событий отобразятся события, полученные от службы корреляции событий(**Рисунок 192**).

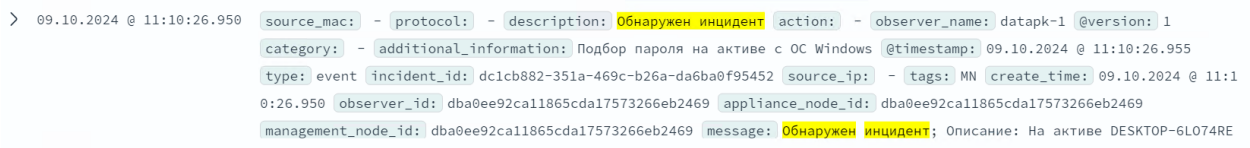


Рисунок 192 – Просмотр событий, полученных от службы корреляции событий

Сгенерируйте и просмотрите события о подборе пароля DATAPK. Для этого:

Найдите правило «Подбор пароля пользователя на DATAPK», измените «**count(description) = 2**» на 3 и примените его.

Введите неверный пароль в веб-интерфейс DATAPK для несуществующего пользователя больше трех раз.

Внимание! Не используйте основной аккаунт для проверки событий по подбору пароля, иначе ваш пользователь будет заблокирован на 15 минут. При необходимости создайте пользователя для проверки.

Просмотрите событие по результатам подбора пароля (**Рисунок 193**).

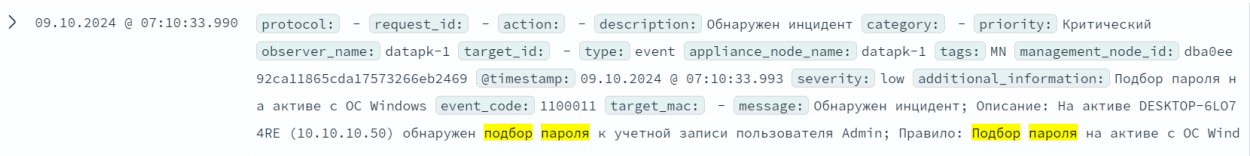


Рисунок 193 — Событие по результатам подбора пароля на DATAPK

Данная часть является ознакомительной, шаги можно выполнить только без установленного «Управление внешними событиями».

В Комплексе так же имеются внутренние правила корреляции, которые работают без установленного модуля «Управление внешними событиями». Для управления внутренними правилами корреляции в Комплексе предусмотрена возможность отключения отдельных внутренних правил корреляции.

Для отключения внутреннего правила корреляции:

Войдите в терминал Комплекса под учетной записью «root».

Откройте на редактирование файл «exceptions_rules.json», выполнив команду:

```
mcedit /usr/share/udv/event-correlator/exceptions_rules.json
```

Добавьте в файл номер правила, которое необходимо отключить в Комплексе. Если правил несколько, укажите их через запятую.

["0001","0004","0005"]

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

Перезагрузите службу корреляции внутренних событий, выполнив команду:

```
systemctl restart udv-event-correlator
```

Лабораторное задание 4.6. Работа с инцидентами

Цель: сформировать навыки работы с журналом событий Комплекса.

Ход работы:

Перейдите на страницу «Инциденты».

Найдите инцидент ИБ (**Рисунок 194**).

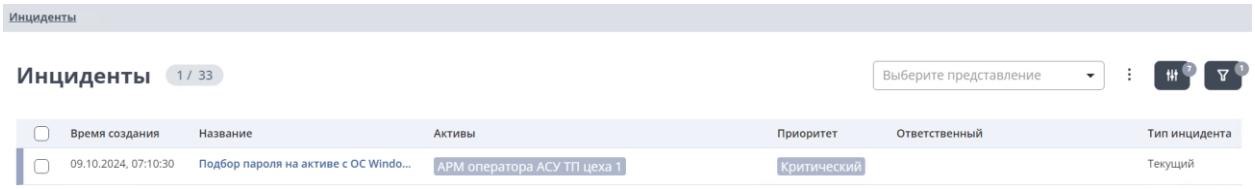


Рисунок 194 — Просмотр инцидентов

Откройте карточку инцидента нажав на название инцидента (**Рисунок 195**).

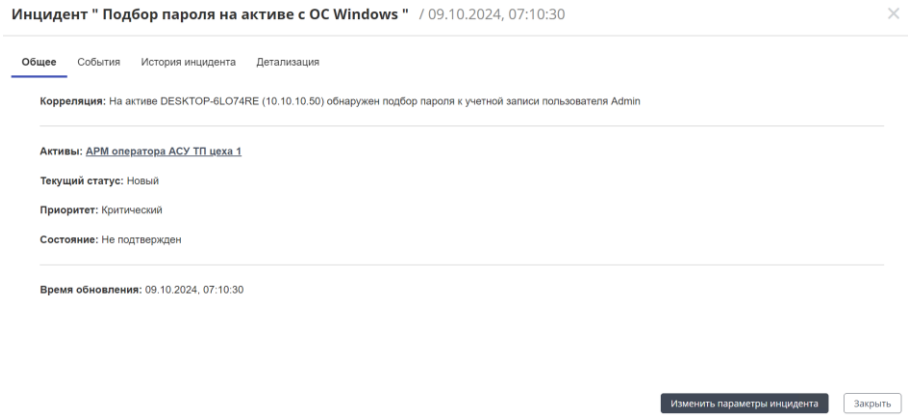


Рисунок 195 — Подробности инцидента

Перейдите на вкладку «События» карточки инцидента.

Нажмите «Подробнее» (**Рисунок 196**).

Результат шага: произойдет переход к событиям инцидента.

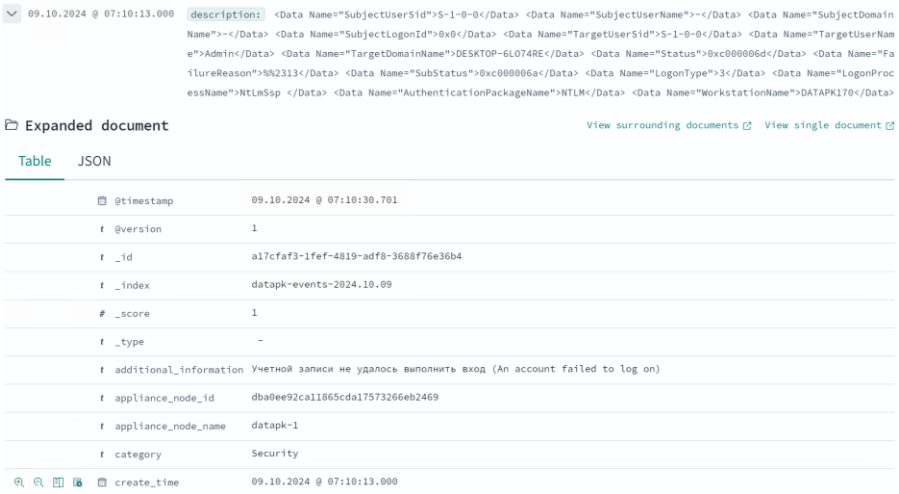


Рисунок 196 — Событие об инциденте на странице «События»

Измените статус инцидента. Для этого:

Вернитесь в карточку инцидента.

Нажмите «Изменить параметры инцидента» внизу карточки инцидента (**Рисунок 197**).

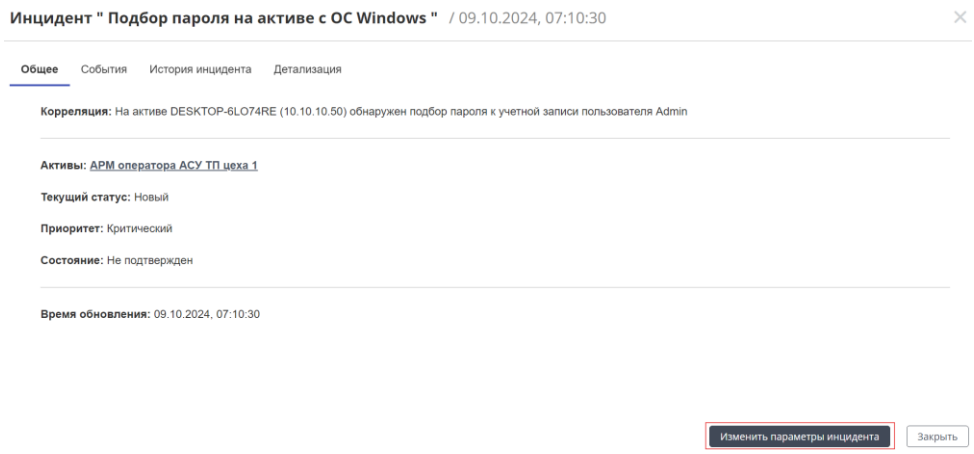


Рисунок 197 — Кнопка изменения параметров инцидента

Задайте статус инцидента «В работе. Проведен анализ» и укажите обоснование (**Рисунок 198**).

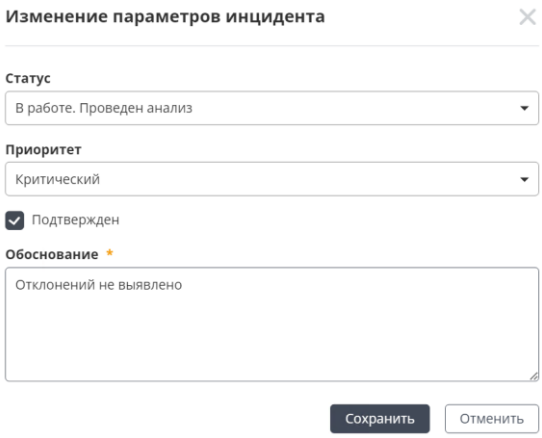


Рисунок 198 — Обновление статуса инцидента в ходе расследования

Убедитесь, что актив не был скомпрометирован и присвойте инциденту статус «Закрыт» (**Рисунок 199**).

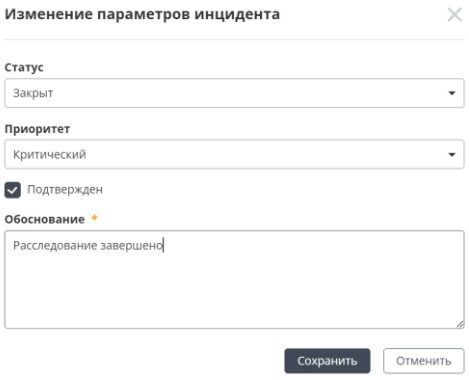


Рисунок 199 — Закрытие инцидента после расследования

Подключитесь к активу «Коммутатор АСУ ТП цеха 1» по ssh. Перейдите в привилегированный режим при помощи команды:

```
enable
```

Перейдите в режим конфигурирования при помощи команды:

```
configure terminal
```

Результат шага: коммутатор запросит ввод команд для настройки (**Рисунок 200**).

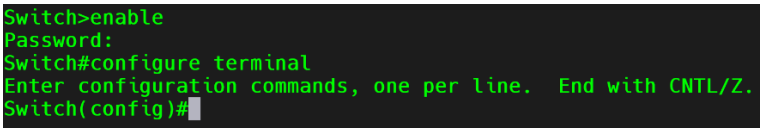


Рисунок 200 — Переход в режим конфигурирования

Включите логирование при помощи команды:

```
logging on
```

Настройте отправку событий в адрес DATAPK при помощи команды:

```
logging host [IP-адрес DATAPK]
```

Включите аудит успешных и неудачных попыток входа при помощи команд (последовательно):

Закройте режим конфигурирования при помощи команды:

```
login on-success log

login on-failure log
```

Примечание:
Если при подключении коммутатор не запрашивает связку логин-пароль, то события входа/выхода пользователей регистрироваться не будут.

```
exit
```

Сохраните конфигурацию при помощи команды:

```
copy run start
```

Подтвердите действие клавишей **Enter**.

Результат шага: конфигурация будет записана (**Рисунок 201**).

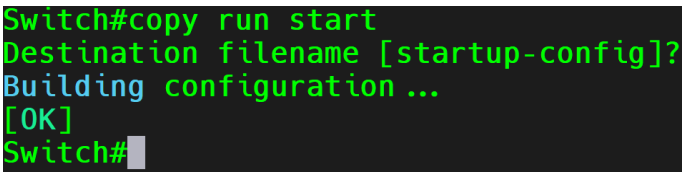


Рисунок 201 — Результат сохранения конфигурации

Создайте (**Рисунок 202**) нестрогий источник Syslog3164 для актива «Коммутатор АСУ ТП». Для этого перейдите в раздел «Администрирование» → «Источники» и нажмите «Создать источник».

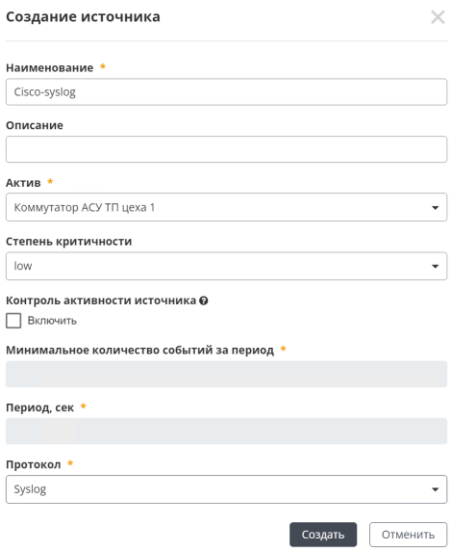


Рисунок 202 — Создание источника

> **Примечание:**
> На Комплексе не должно быть других известных локальных активов с IP-адресом коммутатора.

Сгенерируйте события на коммутаторе АСУ ТП. Например, выполните 3 неудачных попытки входа на коммутатор.

Примечание:

Настройки логирования на коммутаторе можно посмотреть командой **show logging** в привилегированном режиме.

В интерфейсе Комплекса перейдите к событиям коммутатора Cisco. При необходимости откорректируйте временное окно.

Ознакомьтесь (**Рисунок 203**) с событиями, полученными от коммутатора по Syslog **(source: syslog_rfc3164_sensor, event_type:cisco_event)**.

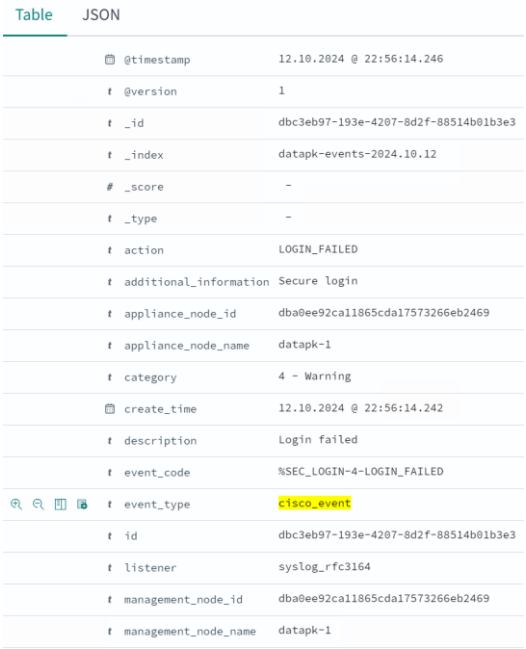


Рисунок 203 — События от коммутатора

Перейдите на страницу инцидентов.

Ознакомьтесь с инцидентом подбора пароля на коммутаторе Cisco (**Рисунок 204**).

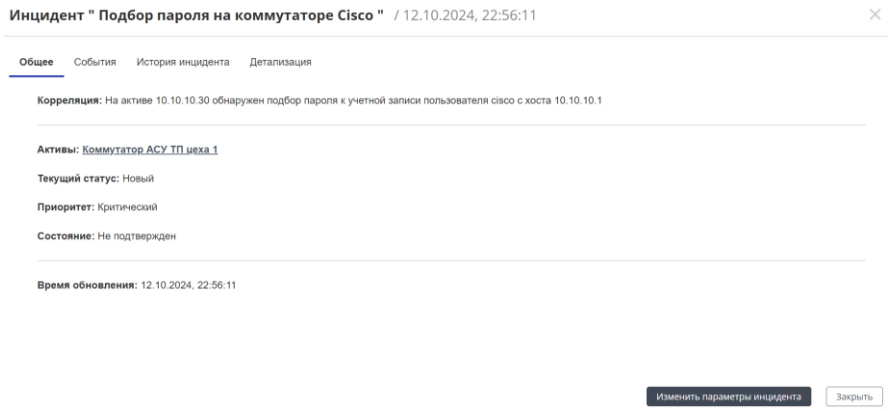


Рисунок 204 — Инцидент на основании события по подбору пароля

Посмотрите подробную информацию, перейдите к событиям службы корреляции, породившим данный инцидент.

Лабораторное задание 4.7. Работа с журналом событий Комплекса

Цель: сформировать навыки работы с журналом событий Комплекса.

Справочная информация

Страница «События» содержит следующие элементы:

- **строка поиска** – находится непосредственно под главным меню навигации, позволяет выполнить поиск по собранным сообщениям;
- **фильтр по времени (период времени)** – находится в правом верхнем углу. Используйте эту функцию для фильтрации событий на основе различных относительных и абсолютных временных диапазонов;
- **список полей** – находится слева, сразу под строкой поиска. Здесь можно выбирать поля для визуализации;
- **гистограмма** – график, который находится в центре страницы под строкой поиска. По умолчанию в нём отображается количество всех логов в зависимости от времени (ось X);
- **список событий** – находится под гистограммой, содержит события, нормализованные по полям. В случае, если поле не установлено, сообщение отображается полностью.

Ход работы:

Настройте работу с событиями. Для этого:

- Откройте веб-интерфейс Комплекса.
- Перейдите на страницу «События».
- Добавьте новые фильтры для отображения событий из журнала Windows.

В верхней части страницы «События» нажмите кнопку «+ Add filter», которая находится под строкой поиска, для создания нового фильтра (**Рисунок 205**).

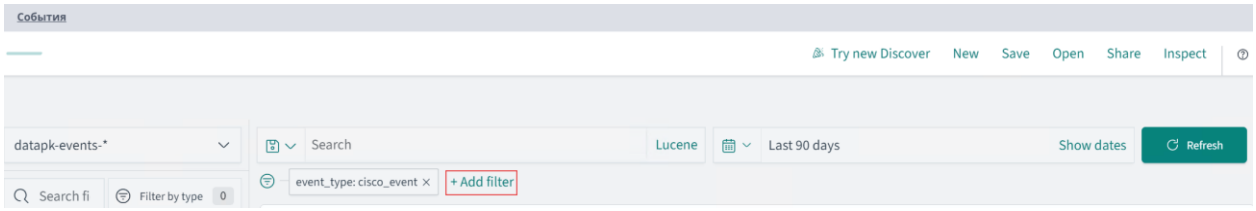


Рисунок 205 — Расположение кнопки «+ Add filter»

Результат шага: появится всплывающее окно редактирования фильтра.

Задайте следующие параметры (**Рисунок 206**) создаваемому фильтру:

- Поле — category.
- Оператор — is.
- Значение — Security.

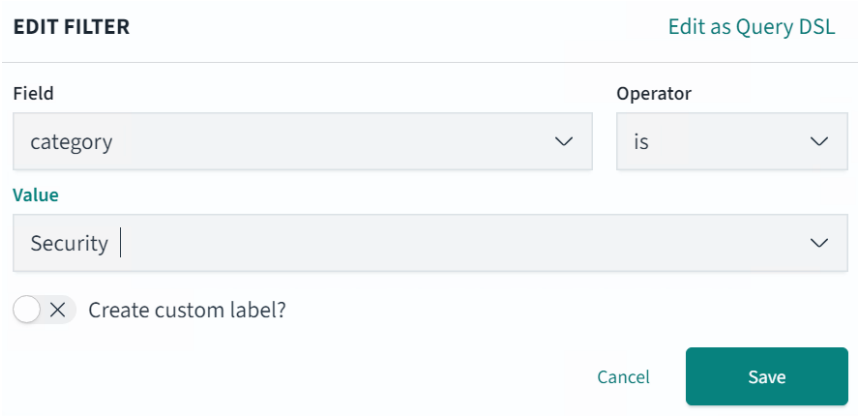


Рисунок 206 — Окно редактирования фильтра

Нажмите «Сохранить».

В отфильтрованном списке найдите событие «Вход с учетной записью выполнен успешно».

Создайте фильтр из режима просмотра события. Для этого найдите событие, отличное от «Задача сбора событий успешно выполнена, новых событий не обнаружено». Например «Вход с учетной записью выполнен успешно». Для этого:

Разверните событие. Нажмите « » рядом со строкой «event_code».

Примечание. Поле «event_code» содержит уникальный идентификатор типа события, совпадающий с тем, что есть в журнале «Безопасность» Windows.

Результат шага: страница обновится и в верхней части страницы появится выбранный фильтр (**Рисунок 207**).

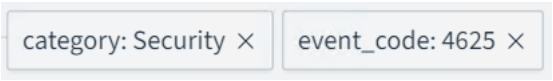


Рисунок 207 — Панель фильтров после добавления фильтров по категории и типу события

Повторите процедуру еще два раза, чтобы отображалось несколько видов событий. Например, **4625** — неудачная попытка входа.

Добавьте фильтры для событий Windows XP. Например, **528** — успешный и **529** — неуспешный вход. Сохраните фильтры. Для этого:

Нажмите кнопку «Сохранить» (**Рисунок 208**) в верхней части страницы.

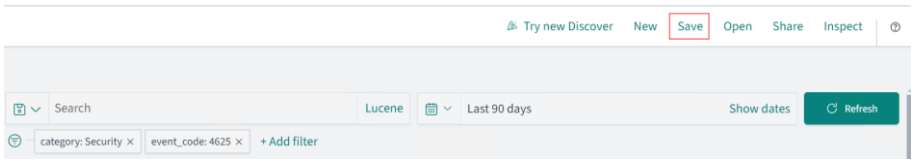


Рисунок 208 – Порядок сохранения фильтра на странице «События»

Результат шага: появится окно сохранения фильтров и поиска.

В окне «Сохранить: search» введите название фильтра «security_events».

Нажмите кнопку «Сохранить» (**Рисунок 209**).

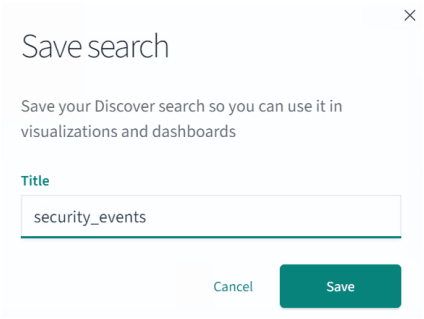


Рисунок 209 — Окно сохранения фильтров и поиска

Создайте вертикальные диаграммы, отображающие количество событий выбранного типа в ОС Windows за день. Для этого:

Перейдите на страницу «Виджеты» (**Рисунок 210**).

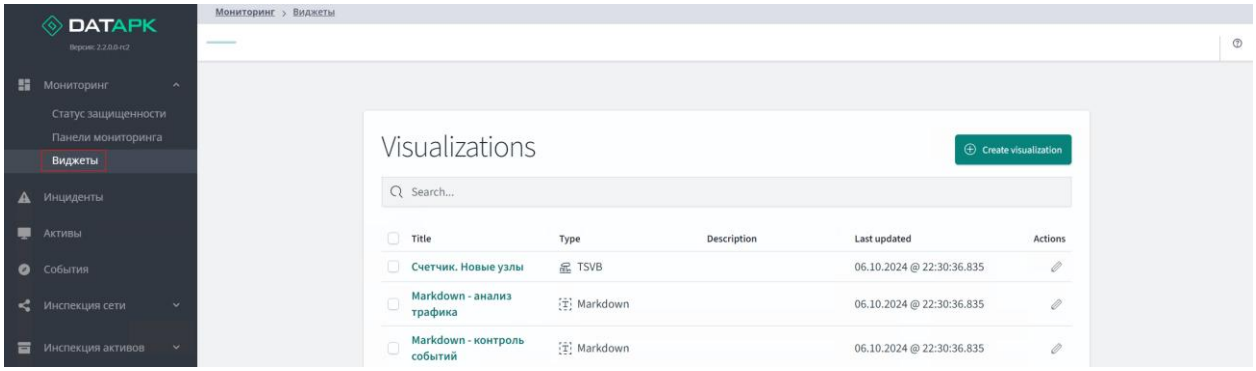


Рисунок 210 — Путь к странице «Виджеты»

Нажмите на кнопку «**Create visualization**».

Результат шага: появится окно «**New visualization**».

В появившемся окне выберите тип визуализации «**Vertical Bar**» (Гистограмма) (**Рисунок 211**).

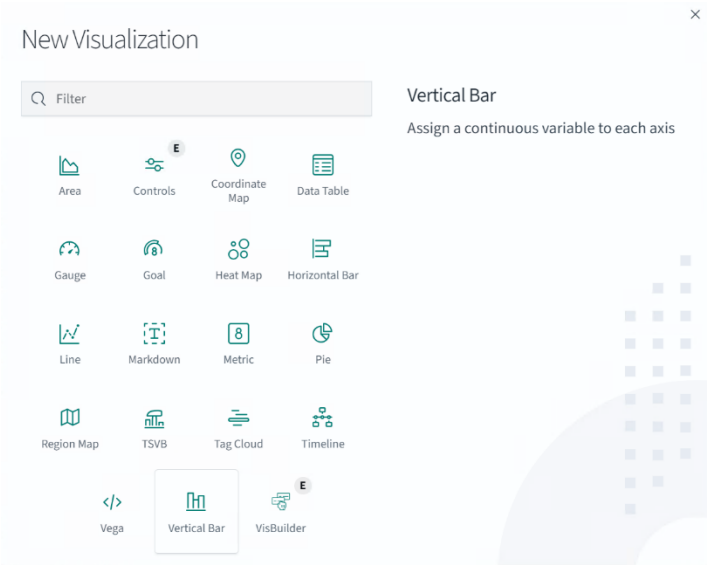


Рисунок 211 – Окно выбора типа визуализации

Введите и выберите сохраненный фильтр «**security_events**» (**Рисунок 212**).

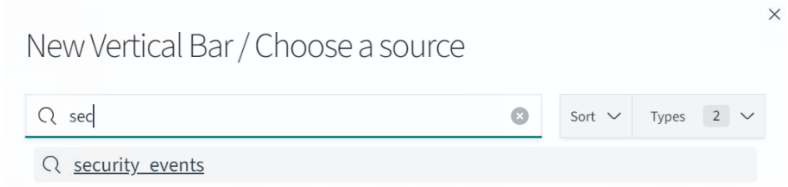


Рисунок 212 – Окно выбора источника поиска данных

В верхнем правом углу окна выберите период отображения «Today». На экране появится вертикальная диаграмма, состоящая только из оси Y, которая отображает количество событий (**Рисунок 213**).

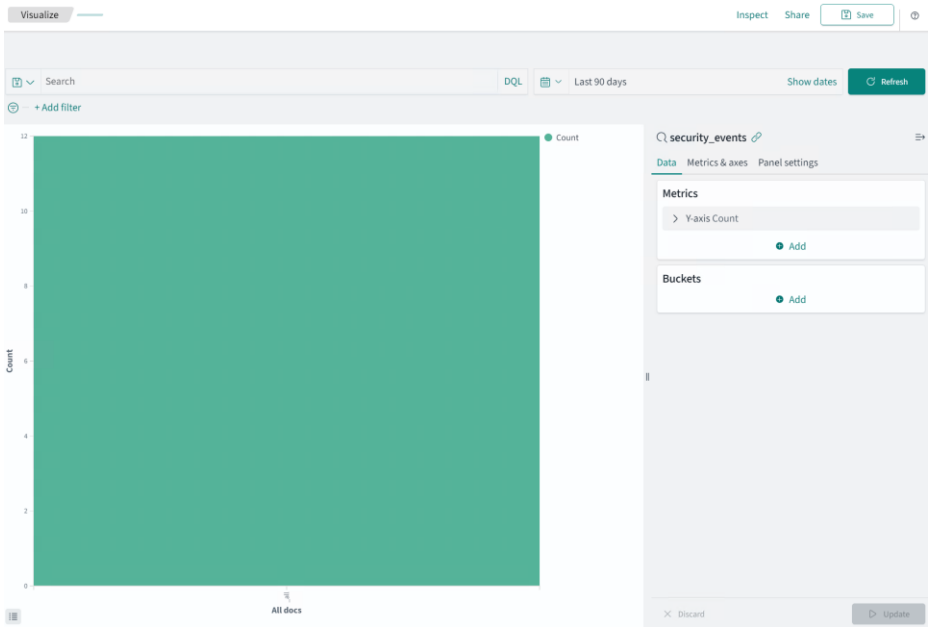


Рисунок 213 – Вертикальная диаграмма, отображающая количество событий неудачного входа в ОС Windows за текущий день

Настройте ось Y диаграммы (**Рисунок 214**).

В области «Метрика» раскройте поле «Ось Y». Для этого нажмите кнопку « » слева от названия поля (1).

В поле «Агрегация» выберите данные, которые будут отображаться по оси Y: «Количество» (количество событий, 2).

В поле «Особая метка» введите отображаемое наименование оси Y: «Количество» (3).

Для подтверждения изменений нажмите кнопку «Обновить» (4).

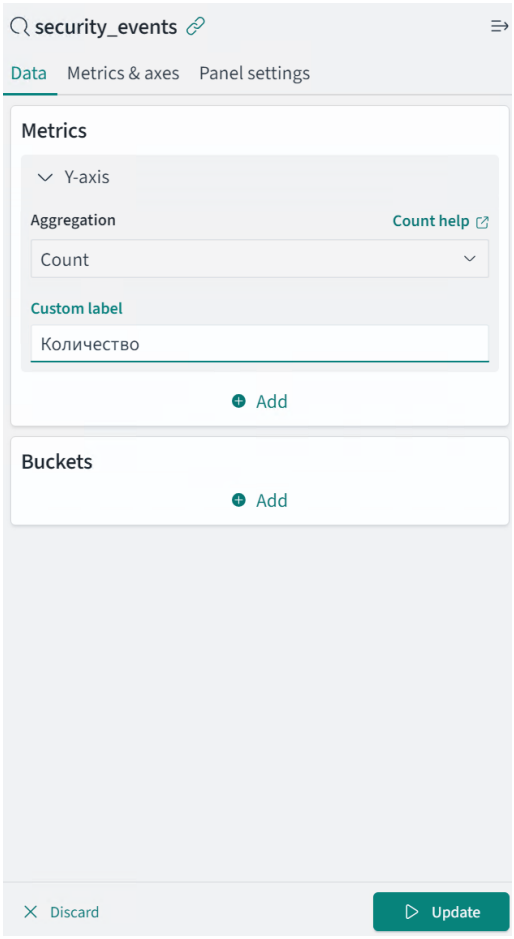


Рисунок 214 – Порядок настройки оси Y диаграммы

Настройте ось X диаграммы.

В области «Сегмент» нажмите «Добавить» и выберите «Ось X» (**Рисунок 215**).

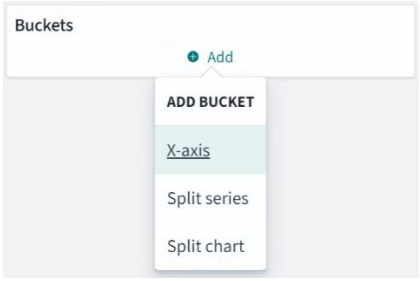


Рисунок 215 — Добавление оси X на диаграмму

Настройте ось X (**Рисунок 216**). Для этого:

В поле «Агрегация» (1) выберите из списка значение «Условия».

В поле «Поле» выберите из списка «hostname» (2) для отображения сетевых имен активов, с которых были получены события.

В поле «Сортировать по» выберите из списка «Метрика: Количество» (3) для сортировки событий по названию актива.

В поле «Сортировать» выберите из списка «По убыванию» (4).

В поле «Размер» (5) введите «10» (максимальное количество отображаемых активов на панели визуализации).

В поле «Особая метка» введите наименование оси X: «Наименование актива» (6).

Для подтверждения изменений нажмите кнопку «Обновить» (7).

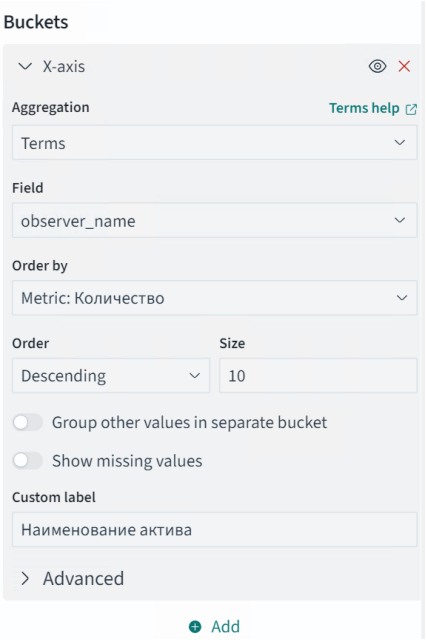


Рисунок 216 – Порядок настройки оси X диаграммы

Сверните настройки оси X и нажмите кнопку «Добавить» и выберите «Разделить серию» (**Рисунок 217**).

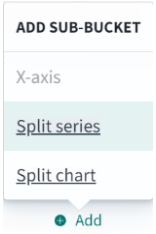


Рисунок 217 – Создание нового параметра типа «Разделённая серия»

Настройте параметры разделения событий (**Рисунок 218**). Для этого:

В поле «Субагрегация» выберите из списка «Условия».

В поле «Поле» выберите из списка «additional_information» для отображения описания событий.

В поле «Сортировать по» выберите из списка «Метрика: Количество».

В поле «Сортировать» выберите из списка «По убыванию».

В поле «Размер» введите «50».

В поле «Особая метка» введите наименование параметра «Событие».

Для подтверждения изменений нажмите кнопку «Обновить».

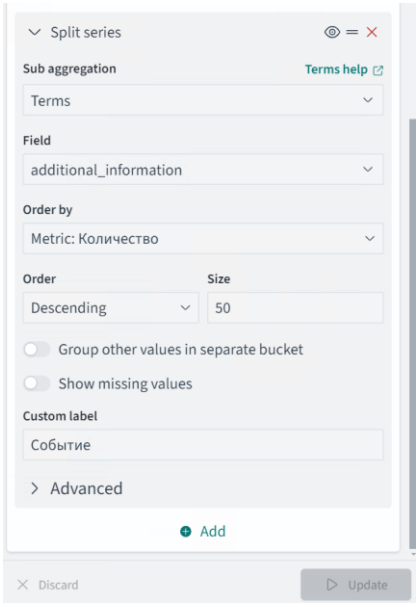


Рисунок 218 — Параметры разделения событий

Подведите указатель мыши на диаграмму для текстового отображения результатов построения диаграммы (**Рисунок 219**).

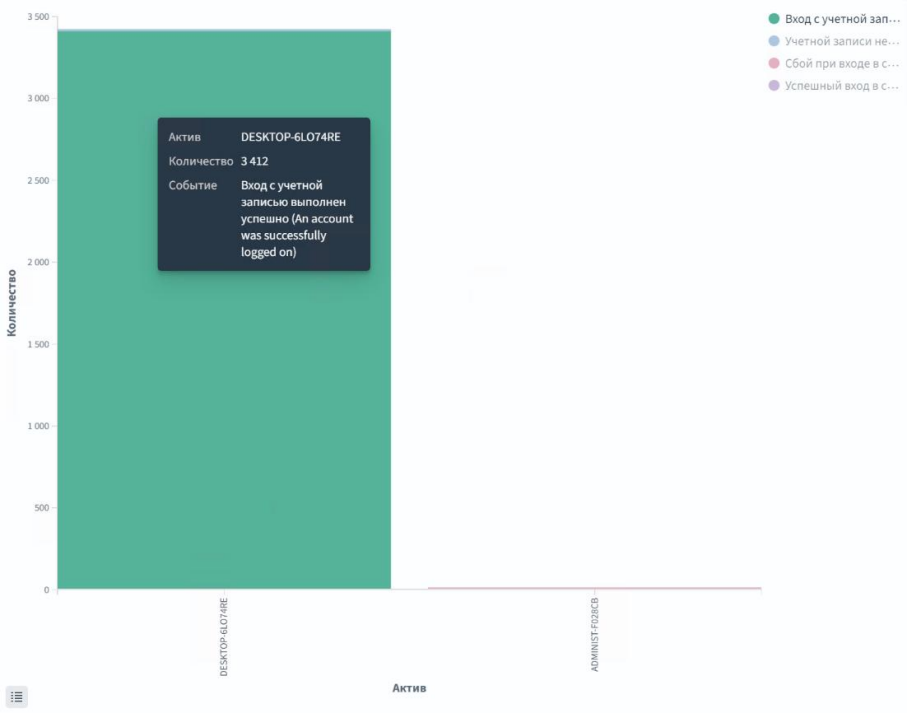


Рисунок 219 – Диаграмма с текстовым отображением результатов

Сохраните фильтры.

Нажмите кнопку «Save» в верхней части страницы (**Рисунок 220**).

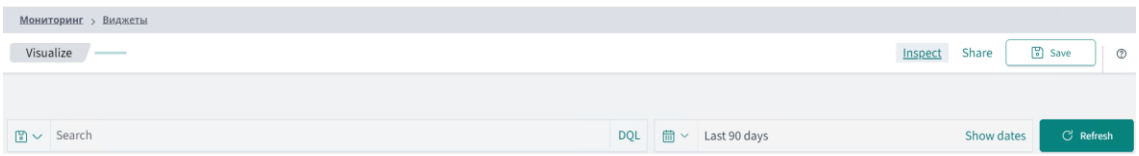


Рисунок 220 — Кнопка «Сохранить»

Результат шага: появится окно сохранения визуализации.

В поле «Title» введите название фильтра «События безопасности в ОС Windows». Введите подходящее название для выбранного вами типа событий.

Нажмите кнопку «Save» (**Рисунок 221**).

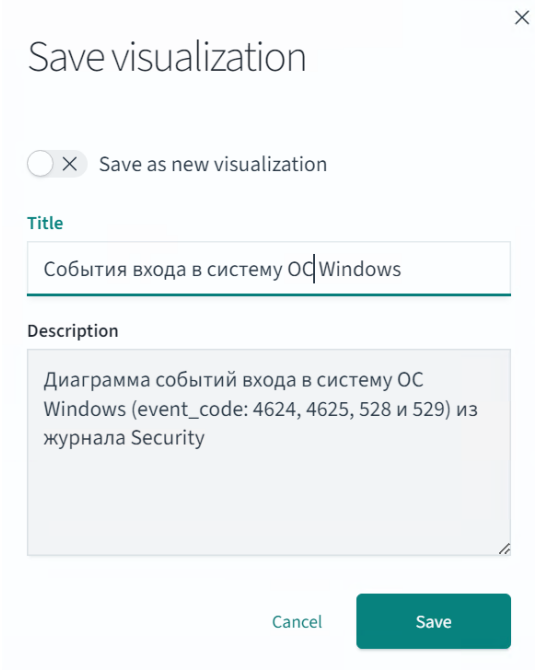


Рисунок 221 – Порядок сохранения визуализации

Результат шага: визуализация будет сохранена и отобразится на странице «Виджеты» (**Рисунок 222**).

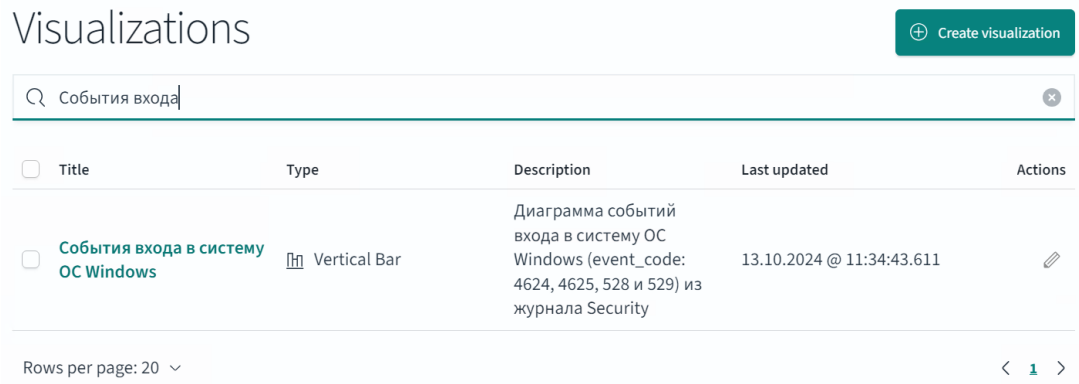


Рисунок 222 — Созданная визуализация на странице «Виджеты»

Лабораторное задание 4.8 Работа с панелями мониторинга

Цель: сформировать навык импорта панелей мониторинга и обнаружения событий на панелях мониторинга.

Ход работы:

Для импорта объектов раздела «Мониторинг» из файлов формата «*.ndjson»:

Перейдите на страницу «Администрирование» → «Основные настройки» → «Настройки мониторинга».

Выбрать вкладку «Saved Objects» (***Рисунок 223***).

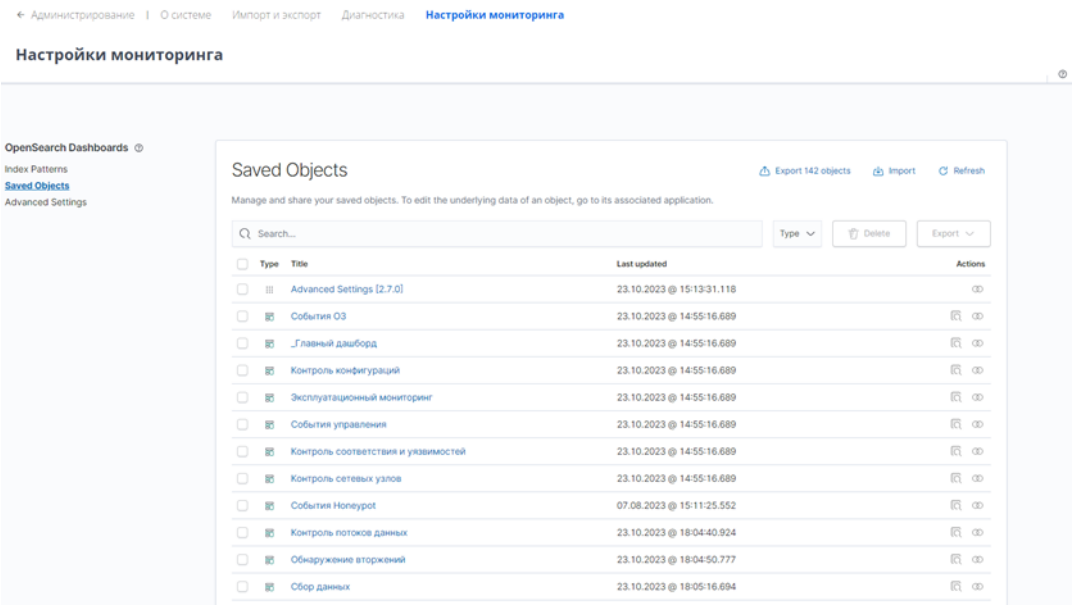


Рисунок 223 — Вкладка «Saved Objects»

Нажмите кнопку «Import».

Результат шага: появится окно импорта сохраненных объектов.

В открывшемся окне:

Оставьте активной настройку «Check for existing objects» → «Automatically overwrite conflicts» (***Рисунок 224***).

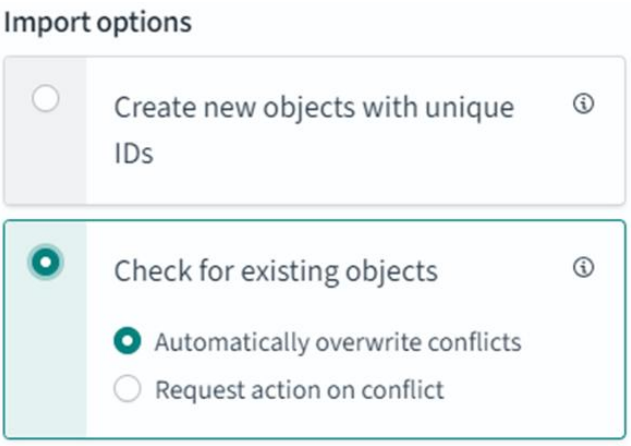


Рисунок 224 — Область настройки импорта

Перетащите или выберите по нажатию на «Import» файл формата «*.ndjson» с объектами раздела «Мониторинг» (***Рисунок 225***).

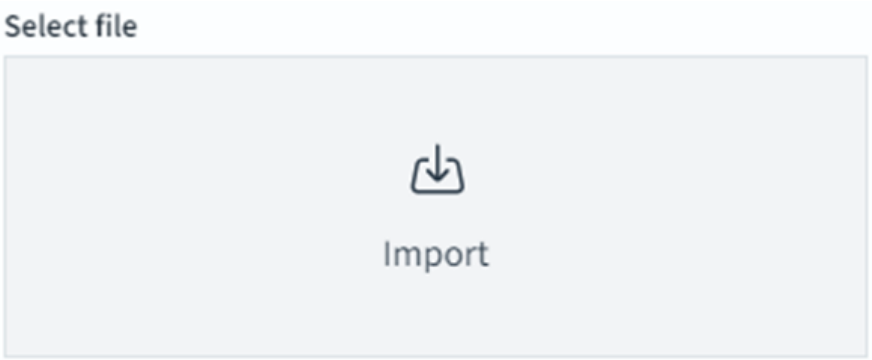


Рисунок 225 — Область выбора файла для импорта

Нажмите «Import» (***Рисунок 226***).

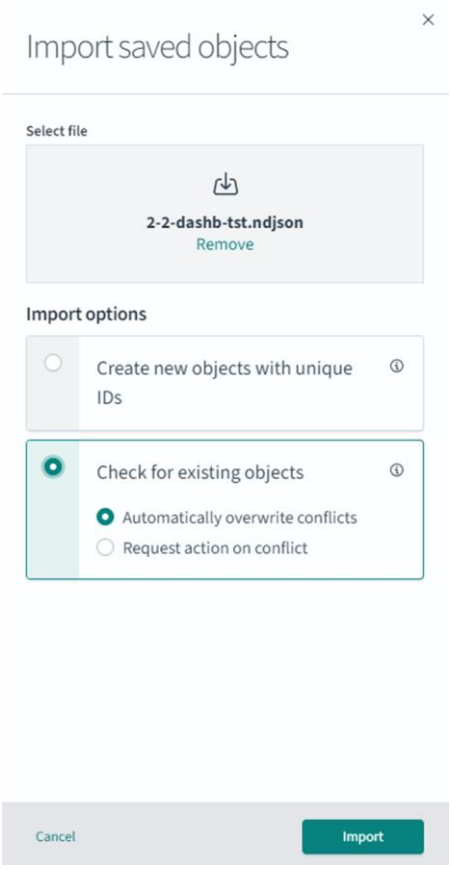


Рисунок 226 — Окно импорта сохраненных объектов

При отображении предупреждения «Index Pattern Conflicts. The following saved objects use index patterns that do not exist» выберите из выпадающего списка в столбце «New Index Pattern» наименование существующего шаблона индекса и нажмите кнопку «Confirm all changes» (***Рисунок 227***).

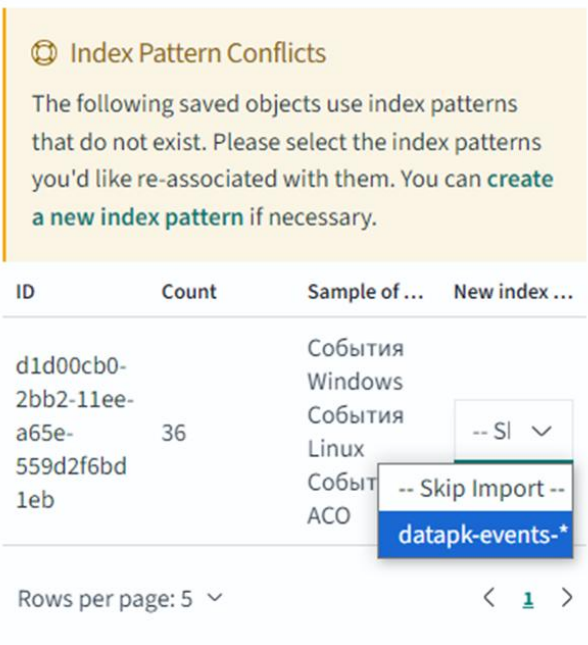


Рисунок 227 — Список шаблонов индекса в столбце «New Index Pattern»

В открывшемся окне с результатами импорта нажмите кнопку «Done».

Убедитесь, что на вкладке «Saved Objects» страницы «Настройки мониторинга» отобразились импортированные объекты.

Убедитесь, что панели мониторинга были импортированы. Для этого:

Перейдите в подраздел интерфейса визуализации «Панели мониторинга» (**Рисунок 228**).

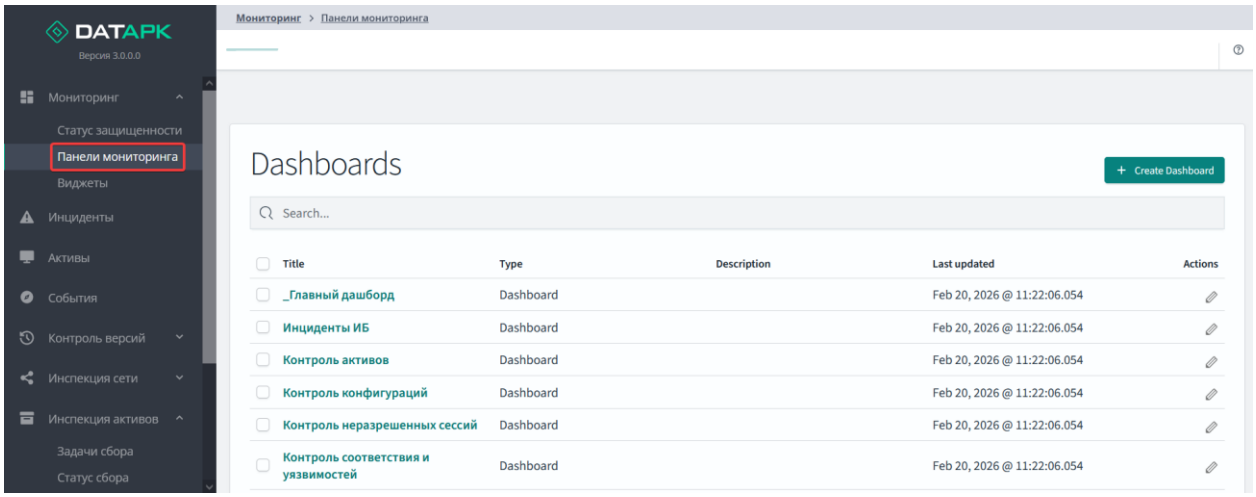


Рисунок 228 — Путь к странице «Панели мониторинга»

Просмотрите содержание страницы (**Рисунок 229**).

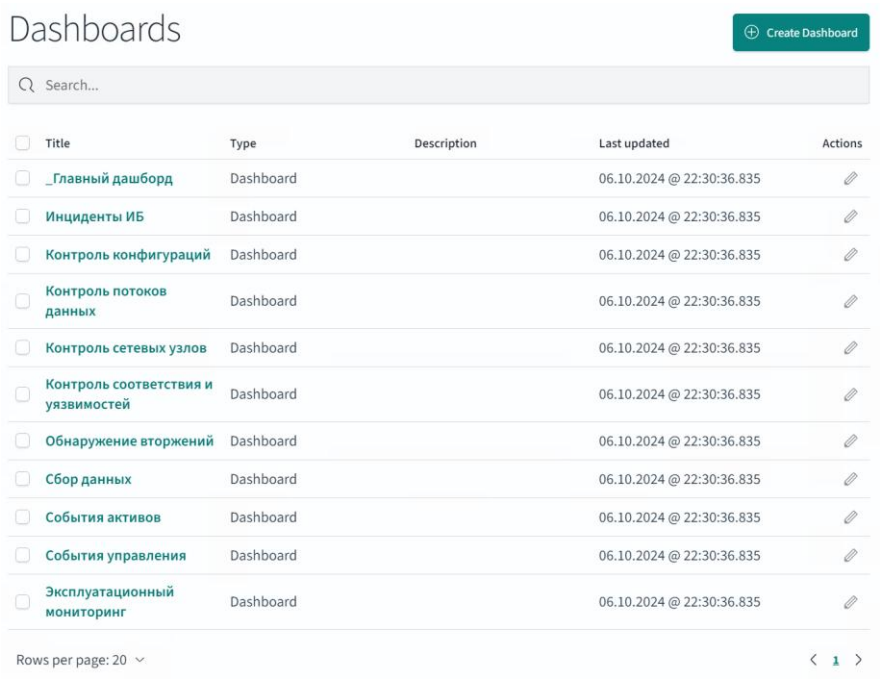


Рисунок 229 — Страница «Панели мониторинга»

Перейдите на главный дашборд. Для этого в разделе «Панели мониторинга» нажмите «_Главный дашборд» (**Рисунок 230**).

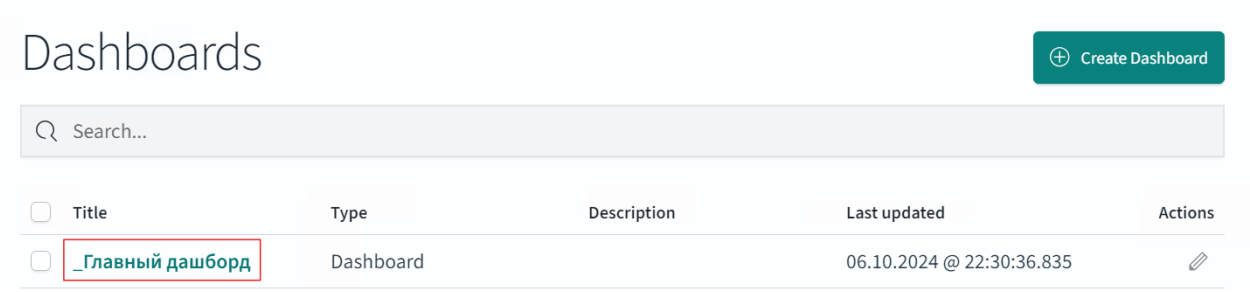


Рисунок 230 — Переход к главному дашборду

Установите временной промежуток получения событий величиной в одну неделю «(Last 7 days)».

Изучите представленные виджеты (**Рисунок 231**).

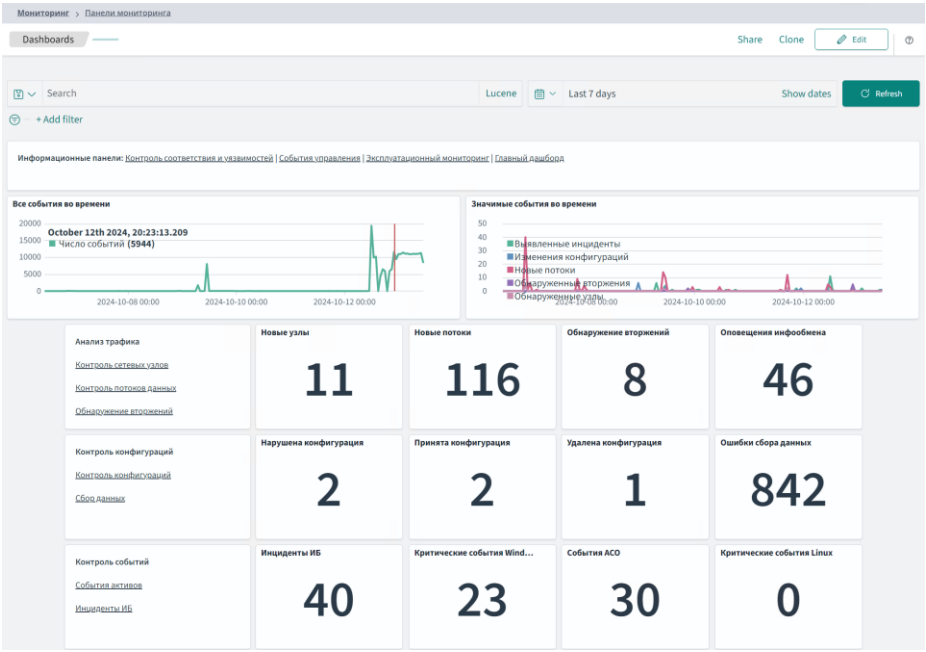


Рисунок 231 — Виджеты главного дашборда

Просмотрите изменения конфигураций за последнее время. Для этого:

Перейдите в панель мониторинга «Контроль конфигураций». Для этого нажмите ссылку на главном дашборде (**Рисунок 232**).

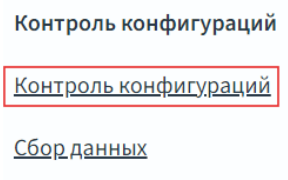


Рисунок 232 — Ссылка на панель мониторинга «Контроль конфигураций»

Просмотрите имеющиеся записи (**Рисунок 233**).

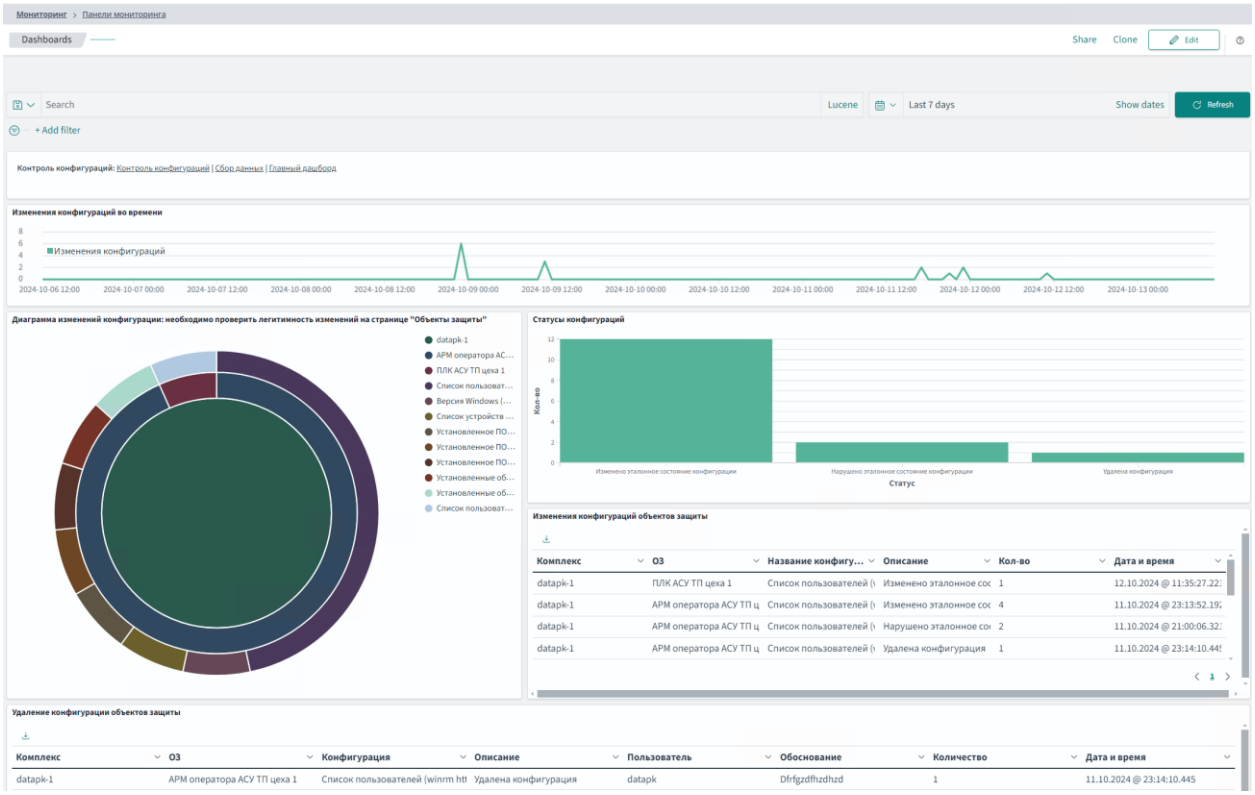


Рисунок 233 — Панель мониторинга «Контроль конфигураций»

На диаграмме изменений конфигурации на внешнем круге нажмите на один из типов изменений конфигурации, например, «Список пользователей (wmi)» (**Рисунок 234**).

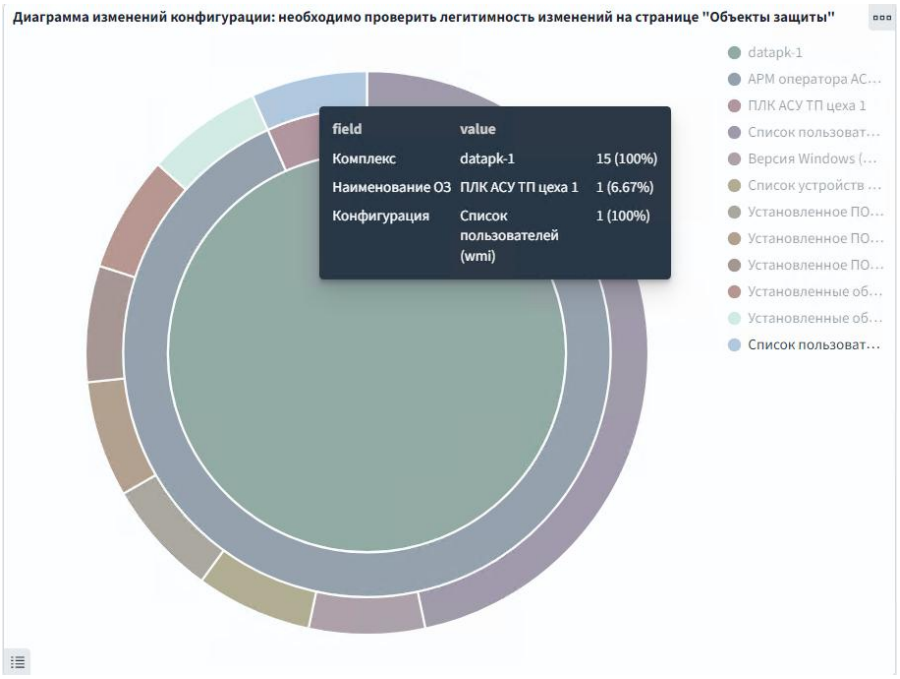


Рисунок 234 — Выбор типа изменений конфигурации

Результат шага: появится окно выбора фильтра.

В окне выбора фильтров нажмите «Apply» (**Рисунок 235**).

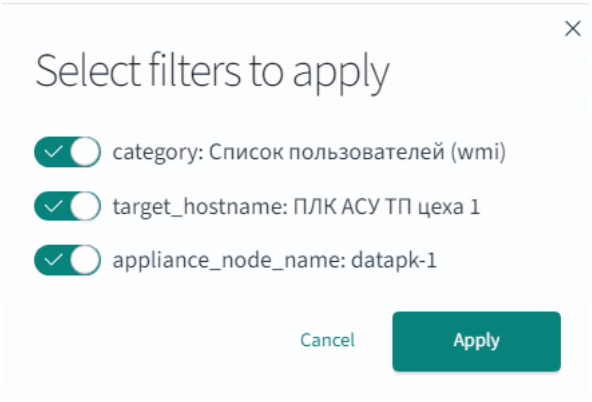


Рисунок 235 — Применение фильтров

Результат шага: страница обновится в соответствии с условиями.

Найдите знакомые записи о добавлении пользователя (**Рисунок 236**). Это еще один способ обнаружения изменений конфигурации.

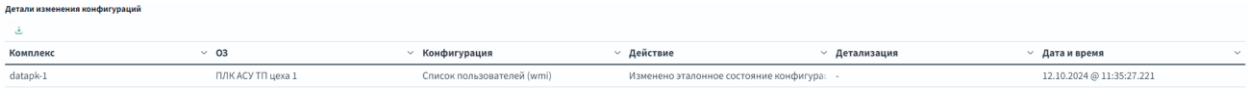


Рисунок 236 — Детали изменения конфигурации

Перейдите к конфигурациям актива и найдите эти же изменения в основном интерфейсе. Для этого:

- запомните название актива, изменения которого будете искать, а также время обнаружения конфигурации;
- Перейдите на страницу «Активы»;
- перейдите к конфигурациям актива;
- найдите искомую конфигурацию;
- примите решение о том, является ли она эталонной.

Найдите записи о новых потоках на панели мониторинга «Контроль сессий». Для этого:

Вернитесь на главный дашборд.

Перейдите к панели мониторинга «Контроль неразрешенных сессий» (**Рисунок 237**).

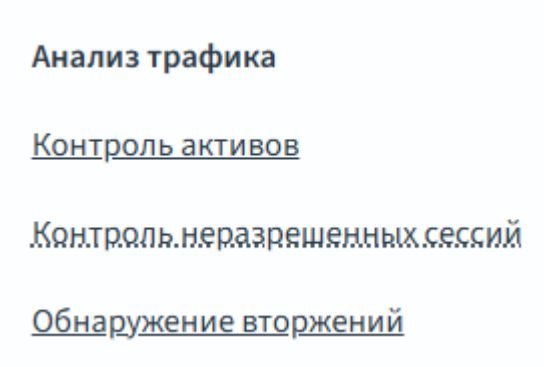


Рисунок 237 — Ссылка на панель мониторинга «Контроль сессий»

Просмотрите содержимое страницы (**Рисунок 238**).

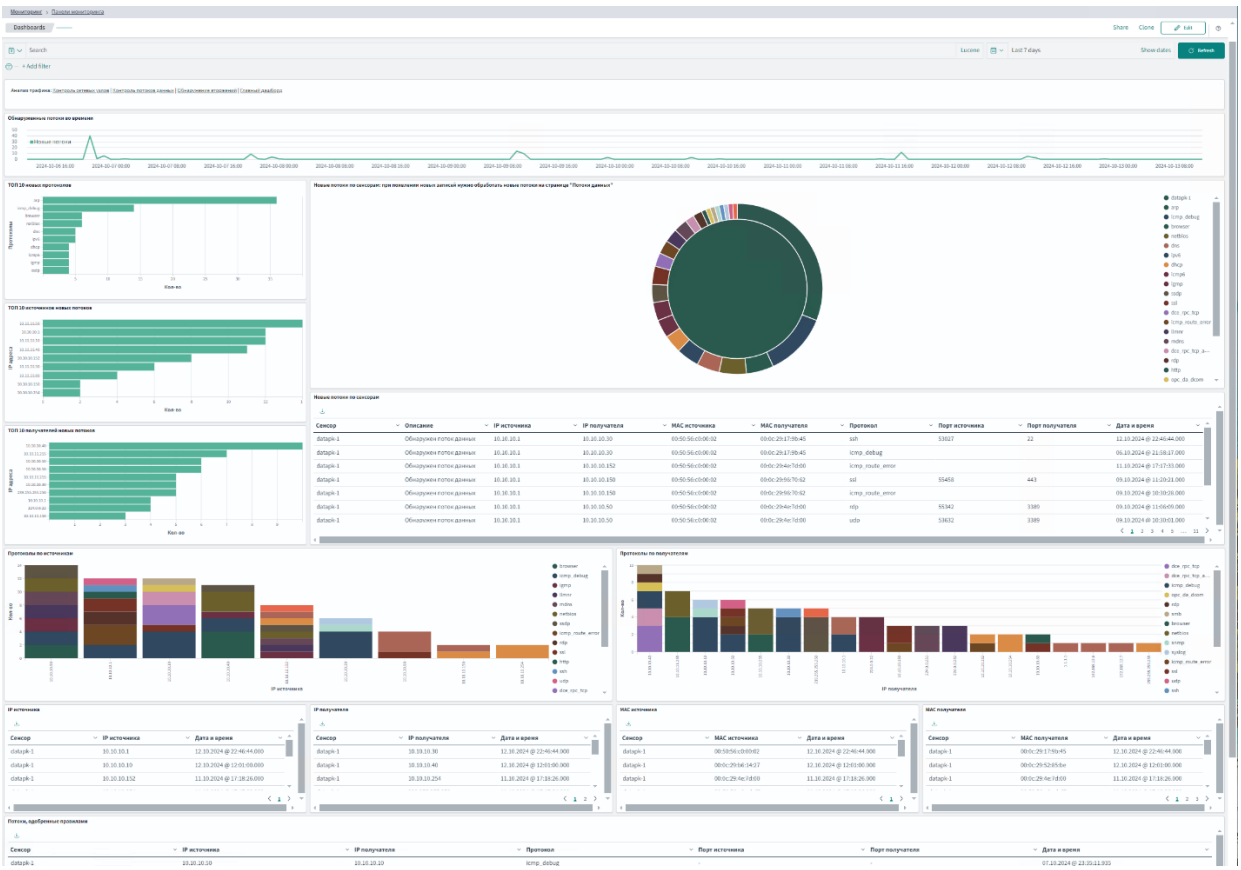


Рисунок 238 — Панель мониторинга «Контроль неразрешенных сессий»

Выберите одну из сессий и найдите её в основном интерфейсе Комплекса. Для этого:

Запомните данные сессии, по которым её можно будет найти (дата и время, IP-адрес, порт, протокол, **Рисунок 239**).

Сенсор	Описание	IP источника	IP получателя	MAC источника	MAC получат…	Протокол	Порт источн…	Порт получа…	Дата и время
datapk-1	Обнаружен поток	10.10.10.1	10.10.10.30	00:50:56:c0:00:02	00:0c:29:17:9b:45	ssh	53027	22	12.10.2024 @ 22:46

Рисунок 239 — Данные протокола, полезные при расследовании

Перейдите в подраздел «Сетевые соединения» в боковом меню.

Используйте фильтры на странице «Сетевые соединения», чтобы найти выбранную сессию.

Создайте правило для этой сессии.

Лабораторная работа 5. Настройка проверок на уязвимости и соответствие требованиям информационной безопасности

Разделы документации

- Поиск уязвимостей и проверка соответствия требованиям информационной безопасности.

Справочная информация

Комплекс имеет в своем составе сканеры, позволяющие проводить проверки на соответствие требованиям ИБ.

Данные сканеры работают по следующим протоколам: ssh, winrm http, winrm https. Целевыми активами для проверки могут быть хосты с ОС Windows и Linux. Все сканеры такого типа вы можете найти в каталогах по предоставленной вендором ссылке: windows security recomendations и linux security recomendations.

Сканеры для сбора списка установленного – это особый тип сканеров. Их можно найти на странице «Администрирование» → «Сканеры» с установленным фильтром «Тип» – «Установленное ПО».Доступные протоколы для сбора: ssh, wmi, winrm http, winrm https, winrm http (basic), winrm https (basic).

Для активов типа «ПЛК», поиск уязвимостей выполняется по версии прошивки, собираемой с помощью сканеров типа «Версия ОС».

Файлы для лабораторных работ

- **scripts_linux_security.json** — сканеры для сбора на соответствование требованиям ИБ (Linux);
- **scripts_windows_security_recommendations.json** — сканеры для сбора на соответствование требованиям ИБ (Windows);
- **scripts_os_soft.json** — сканеры для сбора версии ОС и установленного ПО;
- **vullist.xlsx** — БДУ ФСТЭК, выгруженная с официального сайта;
- **mappings_[date]_[version].tar.bz2** — файл сопоставления ПО и справочника CPE;
- **cve_cpe_db_[date].tar.bz2** — справочник ПО и уязвимостей.

Лабораторное задание 5.1. Проверка активов на соответствие требованиям ИБ

Цель: сформировать умение создавать, применять и интерпретировать результат проверки активов на соответствие требованиям ИБ.

Ход работы:

Комплекс имеет в своем составе сканеры, позволяющие проводить проверки на соответствие требованиям ИБ.

Данные сканеры работают по следующим протоколам: ssh, winrm http, winrm https. Целевыми активами для проверки могут быть хосты с ОС Windows и Linux.

Перейдите в раздел «Администрирование» → «Сканеры», выполните фильтрацию по полю «Наименование сканеры» введя в него «ФСТЭК» (**Рисунок 240**).

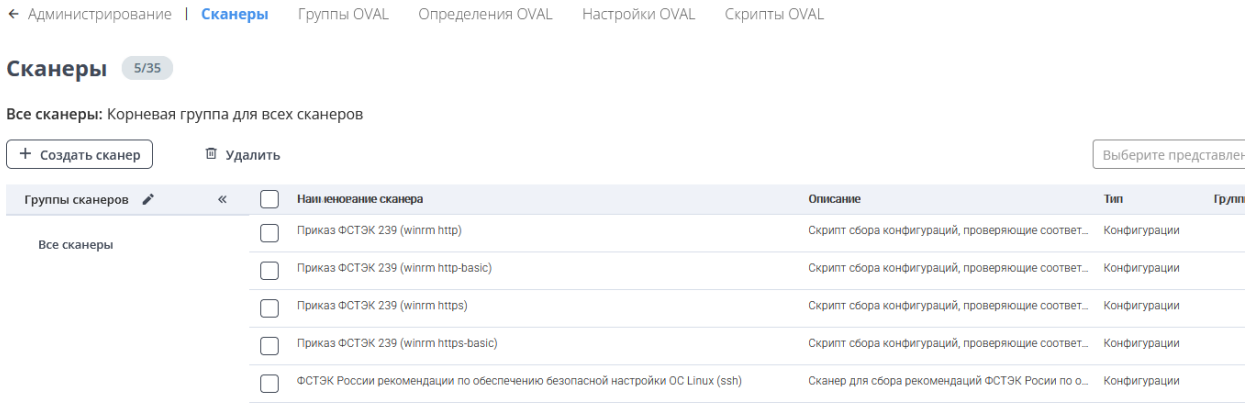


Рисунок 240. Сканеры для проверки на соответствие мерам ФСТЭК

Запустите сканер «Приказ ФСТЭК 239» на активе АРМ Оператора АСУ ТП, нажатием кнопки « ▶ » рядом в строке сканера. Дождитесь его выполнения (может занять некоторое время).

Перейдите в «Активы», откройте карточку актива АРМ Оператора АСУ ТП, в поле «Связанные данные» перейдите на страницу «Конфигурации» (**Рисунок 241**).

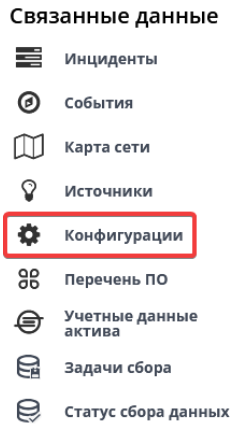


Рисунок 241. Переход в конфигурации актива

Ознакомьтесь с конфигурацией «Приказ ФСТЭК 239» (**Рисунок 242**).

Просмотр Сравнение

№	Название	Описание	Результат	Текущее
1	АВЗ.1_Реализация антивирусной защиты	Требуется установка антивируса Kaspersky https://w...	Соответствует	Установлен антивирус Kaspersky
2	АУД.3_Генерация временных меток и (или) синхрон...	Проверка, включен ли NTP сервер на хосте, в редак...	Соответствует	NTP сервер на хосте включен
3	АУД.4_Аудит входа в систему	Требуется проверить, включена ли регистрация соб...	Не соответствует	Значение политики "Аудит входа в систему" некор...
4	АУД.4_Регистрация событий входа в систему	Требуется проверить, включена ли регистрация соб...	Не соответствует	Значение политики "Аудит событий входа в систе...
5	АУД.4_Регистрация событий использования привил...	Требуется проверить, включена ли регистрация соб...	Не соответствует	Значение политики "Аудит использования привил...
6	АУД.4_Регистрация событий управления учетными ...	Требуется проверить, включена ли регистрация соб...	Соответствует	Установлены значения "Успех" и "Отказ" для поли...
7	ЗИС.7_Использование эмулятора среды функциони...	Требуется установка среды функционирования про...	Не соответствует	Не установлена среда функционирования програ...
8	ЗНИ.5_Контроль использования интерфейсов ввод...	Требуется заменить параметр Start на значение 4 в ...	Не соответствует	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet...
9	ИАФ.1_Идентификация и аутентификация пользова...	Требуется удалить параметр DefaultPassword в ред...	Соответствует	Параметр DefaultPassword удалён. Минимальная ...
10	ИАФ.2_Идентификация и аутентификация устройств	Идентификация и аутентификация устройств являе...	Соответствует	ОС принадлежит к семейству Windows
11	ИАФ.3_Управление идентификаторами	Управление идентификаторами является организац...	Соответствует	ОС принадлежит к семейству Windows
12	ИАФ.4_Максимальный срок действия пароля	Требуется установить менее 90 дн. (но не менее 1 д...	Не соответствует	Значение политики "Максимальный срок действи...
13	ИАФ.4_Минимальная длина пароля	Требуется установить значение 6 зн. для политики "...	Соответствует	Значение политики "Минимальная длина пароля" ...
14	ИАФ.4_Минимальный срок действия пароля	Требуется установить значение более 1 дн. для пол...	Соответствует	Значение политики "Минимальный срок действия...
15	ИАФ.4_Соответствие пароля требованиям сложнос...	Требуется включить политику "Пароль должен отве...	Не соответствует	Политика "Пароль должен отвечать требованиям ...
16	ИАФ.4_Соответствие требованиям журналирования...	Требуется установить значение больше или равное ...	Не соответствует	Значение политики "Вести журнал паролей" не со...
17	ИАФ.4_Соответствие требованиям шифрования пар...	Требуется отключить политику "Хранить пароли, ис...	Соответствует	Политика "Хранить пароли, используя обратимое ...
18	ИАФ.5_Идентификация и аутентификация внешних ...	Требуется проверить, что установлено значение не ...	Соответствует	Значение политики "Минимальная длина пароля" ...
19	ИАФ.7_Защита аутентификационной информации п...	Локальная политика безопасности. Клиент сети Mi...	Соответствует	"Клиент сети Microsoft: отправлять незашифрова...
20	ИАФ.7_Защита аутентификационной информации п...	Локальная политика безопасности. Сетевая безопа...	Не соответствует	Политика "Сетевая безопасность: минимальная с...
21	ИАФ.7_Защита аутентификационной информации п...	Локальная политика безопасности. Сетевая безопа...	Не соответствует	Политика "Сетевая безопасность: минимальная с...
22	ИАФ.7_Сетевой доступ: не разрешать хранение пар...	Проверка, сохраняет ли диспетчер учетных данных ...	Не соответствует	Отключено

Рисунок 242. Результаты проверки на соответствие мерам ФСТЭК

> **Примечание:**
> Мы рассмотрели не все сканеры, позволяющие осуществлять проверку на соответствие требованиям ИБ.
> Все сканеры такого типа вы можете найти в каталогах по предоставленной вендором ссылке: windows security recomendations и linux security recomendations

Самостоятельное задание

1. Перейдите в «Администрирование» → «Сканеры».

2. Найдите сканер для проверки настроек политики безопасности Windows.

3. Запустите данный сканер на активе АРМ Оператора АСУ ТП.

4. Перейдите в конфигурации актива АРМ Оператора АСУ ТП, ознакомьтесь с результатами работы сканера.

5. Подключитесь к активу АРМ Оператора АСУ ТП, нажмите комбинацию клавиш WIN+R и введите «secpol.msc».

6. В окне «Локальная политика безопасности» перейдите в «Политики учетных записей» → «Политика паролей».

7. Измените политику «Минимальная длина пароля» на «10 зн.» и сохраните изменения.

8. Повторно выполните запуск сканера с шага 2.

9. Повторно откройте собранную конфигурацию с актива АРМ Оператора АСУ ТП. Убедитесь в том, что конфигурация отличается от эталонной. Проверьте, какой параметр изменился и как?

10. Продемонстрируйте результат преподавателю.

Лабораторное задание 5.2. Проверка перечня ПО активов на уязвимости

Цель: сформировать умение выполнять проверку активов на уязвимости.

Ход работы:

1. Импорт справочников ПО и уязвимостей

Для импорта справочников CPE и CVE:

1.1. Перейдите на страницу «Администрирование» → «Основные настройки» → «Импорт и экспорт».
1.2. На панели «Обнаружение уязвимостей (CVE)» в строке «Справочники ПО и уязвимостей (CPE и CVE)» нажмите кнопку (Импортировать).
1.3. В открывшемся окне укажите расположение импортируемого файла cve_cpe_db_[дата].tar.bz и подтвердите выбор.

Результат шага: будет запущен процесс импорта: в правом верхнем углу появится уведомление «Запущен импорт справочника», а под заголовком «Результат последнего импорта» будет символ «-».

1.4. Дождитесь загрузки справочника и убедитесь, что файл был успешно загружен.

- Если файл импортирован успешно, в правом вернем углу под заголовком Результат последнего импорта появится уведомление: «Успешно».
- Если произошла ошибка, в правом верхнем углу под заголовком Результат последнего импорта появится уведомление «Ошибка». Для просмотра информации об ошибке нажмите ссылку Подробнее в подсказке рядом с уведомлением.

2. Для импорта файла сопоставления собранного сканерами ПО со справочником CPE:
2.1. Перейдите на страницу Администрирование → Основные настройки → Импорт и экспорт.
2.2. На панели Обнаружение уязвимостей (CVE) в строке Сопоставление собранного сканерами ПО со справочником CPE нажмите кнопку (Импортировать).
2.3. В открывшемся окне укажите расположение импортируемого файла mappings_[дата].tar.bz2 и подтвердите выбор.

Результат шага: будет запущен процесс импорта: в правом верхнем углу появится уведомление «Запущен импорт справочника», а под заголовком «Результат последнего импорта» будет символ «-».

2.4. Дождитесь загрузки справочника и убедитесь, что файл был успешно загружен.

- Если файл импортирован успешно, в правом вернем углу под заголовком Результат последнего импорта появится уведомление: «Успешно».
- Если произошла ошибка, в правом верхнем углу под заголовком Результат последнего импорта появится уведомление «Ошибка». Для просмотра информации об ошибке нажмите ссылку Подробнее в подсказке рядом с уведомлением.

3. Для импорта справочника БДУ ФСТЭК России:
3.1. Перейдите на страницу Администрирование → Основные настройки → Импорт и экспорт.
3.2. На панели Обнаружение уязвимостей (CVE) в строке Справочник БДУ ФСТЭК нажмите кнопку (Импортировать).
3.3. В открывшемся окне укажите расположение импортируемого файла формата *.xlsx и подтвердите выбор.

Результат шага: будет запущен процесс импорта: в правом верхнем углу появится уведомление «Запущен импорт справочника», а под заголовком «Результат последнего импорта» будет символ «-».

3.4. Дождитесь загрузки справочника и убедитесь, что файл был успешно загружен.

- Если файл импортирован успешно, в правом вернем углу под заголовком Результат последнего импорта появится уведомление: «Успешно».
- Если произошла ошибка, в правом верхнем углу под заголовком Результат последнего импорта появится уведомление «Ошибка». Для просмотра информации об ошибке нажмите ссылку Подробнее в подсказке рядом с уведомлением.

4. Осуществить сбор списка установленного ПО на активе одним из доступных сканеров, убедиться, что список ПО присутствует на странице «Перечень ПО».

Примечание:
Сканеры для сбора списка установленного – это особый тип сканеров. Их можно найти на странице «Администрирование» → «Сканеры» с установленным фильтром «Тип» – «Установленное ПО».
Доступные протоколы для сбора: ssh, wmi, winrm http, winrm https, winrm http (basic), winrm https (basic).
Для активов типа «ПЛК», поиск уязвимостей выполняется по версии прошивки,

5. Запуск поиска уязвимостей актива в базах CVE, CPE и БДУ ФСТЭК России (**Рисунок 243**):

5.1. Перейдите на страницу Активы.

5.2. При помощи чекбокса выберите актив.

5.3. Нажмите кнопку (Запустить поиск уязвимостей).

5.4. Результат шага: появится окно «Запуск поиска уязвимостей».

5.5. Нажмите «Запустить поиск».

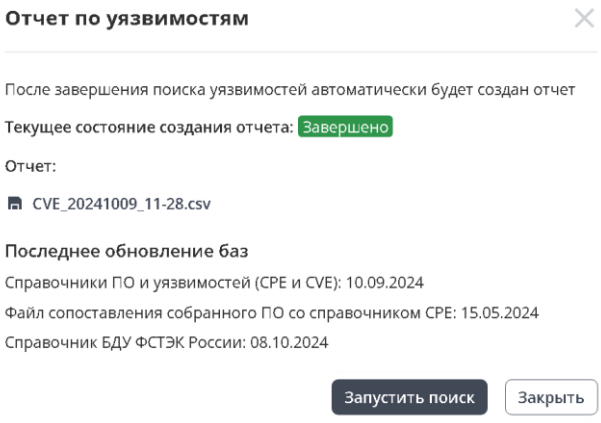


Рисунок 243. Окно «Запуск поиска уязвимостей»

5.6. Дождитесь завершения поиска.

Результат шага: в окне Запуск поиска уязвимостей отобразится текущее состояние создания отчета: «Завершено».

6. Для поиска уязвимостей нескольких активов:

6.1. Перейдите на страницу Активы.

6.2. При помощи чекбоксов выберите активы.

6.3. Нажмите кнопку (Запустить поиск уязвимостей).

Результат шага: появится окно Запуск поиска уязвимостей.

6.4. Нажмите «Запустить поиск».

Подсказка:

Поиск уязвимостей и создание отчета может занять продолжительное время. Вы можете безопасно закрыть окно — поиск продолжится в фоновом режиме. Для просмотра статуса поиска уязвимостей заново откройте окно Запуск поиска уязвимостей — для этого на странице Активы выберите любой актив и нажмите кнопку .

Вы также можете отменить поиск уязвимостей, нажав кнопку Остановить поиск в окне Запуск поиска уязвимостей

6.5. Дождитесь завершения поиска.

Результат шага: в окне Запуск поиска уязвимостей отобразится текущее состояние создания отчета: «Завершено».

7. Для просмотра уязвимостей и рекомендаций в карточке актива:

7.1. Перейдите в карточку актива и нажмите на круговую диаграмму Уязвимости, либо перейдите на страницу Активы и в строке с активом в столбце Уязвимости нажмите на его статус (**Рисунок 244**).

Результат шага: откроется окно Просмотр уязвимостей со списком уязвимостей, обнаруженных на активе.

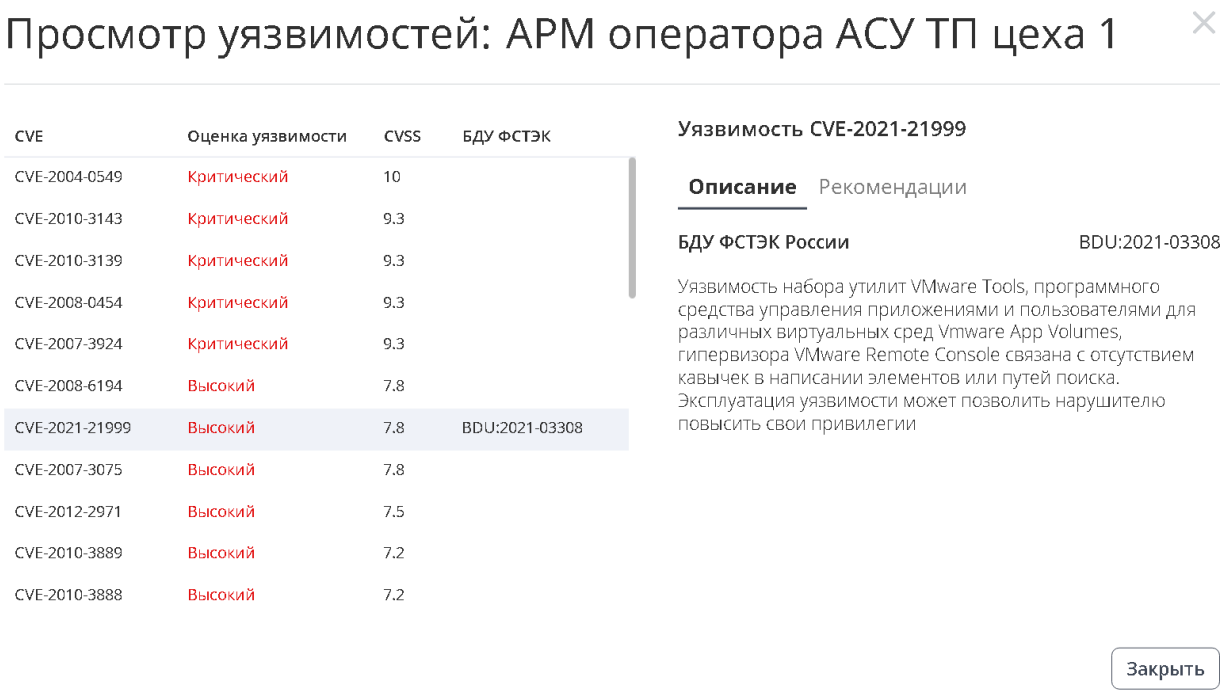


Рисунок 244 – Окно «Просмотр уязвимостей»

7.2. Выберите необходимую уязвимость из списка в окне «Просмотр уязвимостей» и откройте вкладку «Рекомендации» (**Рисунок 245**).

Результат шага: в данной вкладке будут отображаться ссылка на рекомендации производителя и кнопка Ссылка на источник, при нажатии которой откроется веб-страница с рекомендациями по устранению уязвимости.

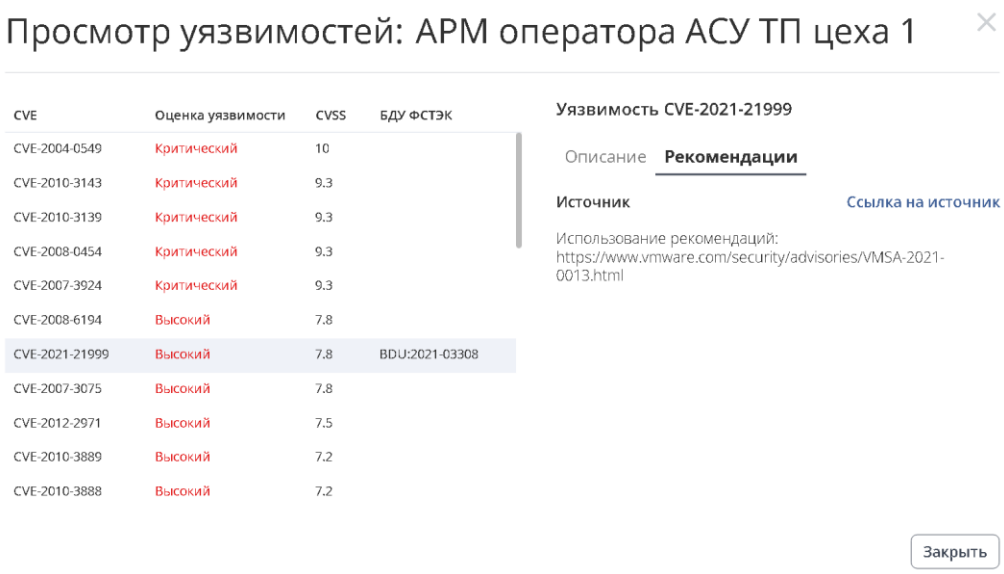


Рисунок 245 – Вкладка «Рекомендации»

2. Для просмотра уязвимостей в отчете в формате csv:

а. Перейдите в карточку актива, на котором выполнялся поиск уязвимостей, и откройте окно «Запуск поиска уязвимостей».

б. В открывшемся окне скачайте отчет формата *.csv.

Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE

Для экспорта отчета, содержащего результаты сопоставления собранного сканерами ПО и ОС со справочником CPE всех активов, для которых когда-либо выполнялся поиск уязвимостей:

Убедитесь, что поиск уязвимостей был выполнен на всех интересующих активах.

Перейдите в раздел «Инспекция активов» → «Перечень ПО» (**Рисунок 246**).

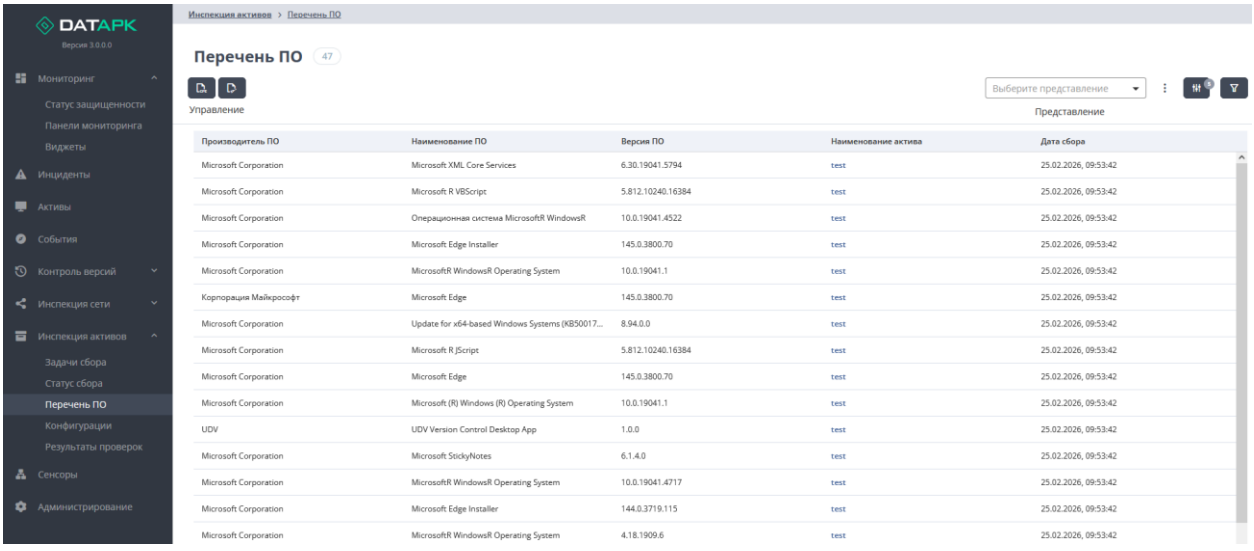


Рисунок 246 – Вкладка «Перечень ПО»

В верхней части окна нажмите кнопку «  » для экспорта отчета по результатам сопоставления собранного ПО со справочником CPE. Будет загружен файл в формате «.csv».

Заполните анкету для обращения в техническую поддержку, в анкете укажите список ПО, для которого необходимо уточнить CPE, и направьте анкету и файл в адрес технической поддержки Комплекса.

Лабораторная работа 6. Настройка системы управления доступом

Разделы документации

- Раздел «Управление пользователями» Руководства по эксплуатации.

Справочная информация

Ролевая модель DATAPK

С целью гибкого разграничения прав доступа пользователей к функциям ПК DATAPK реализована ролевая моделью — пользовательскими ролями и их разрешениями.

Каждая пользовательская роль связывается с набором разрешений. При создании пользователей и назначении им роли, пользователи станут обладать набором разрешений роли.

Файлы для лабораторных работ

—

Лабораторное задание 6.1. Работа с парольной политикой пользователей Комплекса

Цель: сформировать умение работы с парольной политикой пользователей Комплекса.

Ход работы:

Перейдите на страницу «Администрирование» → «Пользователи» → «Парольная политика» (**Рисунок 247**).

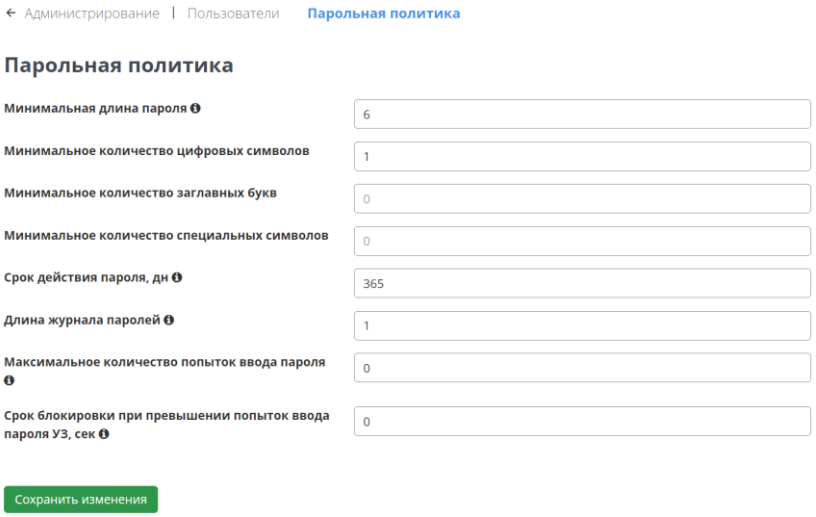


Рисунок 247 — Страница «Парольная политика»

На активной странице «Парольная политика» измените следующие параметры (**Рисунок 248**):

- в поле «Максимальная длина пароля» введите «8»;
- в поля «Минимальное количество цифровых символов (0-9)» введите «1»;
- в поле «Минимальное количество заглавных букв» введите «1»;
- в поле «Минимальное количество специальных символов» введите «1»;
- в поле «Срок действия пароля (в днях)» введите «365»;
- в поле «Длина журнала паролей (1-24)» введите «2»;

Нажмите клавишу «Сохранить изменения».

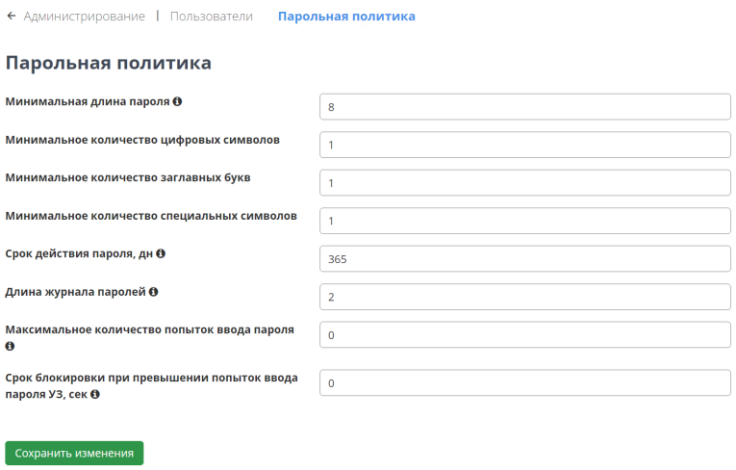


Рисунок 248 — Активная страница «Парольная политика»

Лабораторное задание 6.2. Управление пользователями

Цель: сформировать навык управления учетными записями пользователей.

Ход работы:

Создайте учётную запись. Для этого:

Перейдите на страницу «Управление Комплексом» → «Пользователи».

Нажмите кнопку «Создать учетную запись» (**Рисунок 249**).

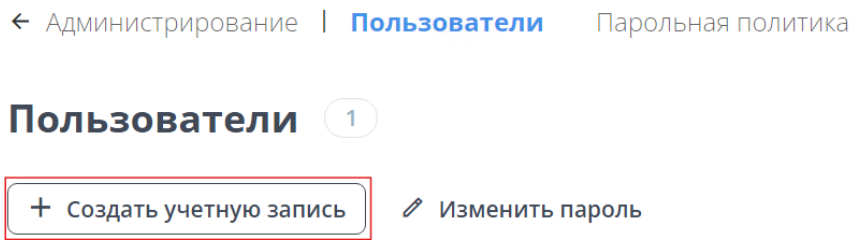


Рисунок 249 — Расположение кнопки «Создать учетную запись»

В появившемся окне «Создание учетной записи» введите значения (**Рисунок 250**):

- в поле «Тип учётной записи» выберите «Локальная»;
- в поле «Логин» введите логин учетной записи «test»;
- в поля «Пароль» и «Подтверждение пароля» введите пароль «aDd6El3m»;
- в поле «Фамилия» введите «Петров»;
- в поле «Имя» введите «Пётр»;
- в поле «Отчество» введите «Петрович»;
- в поле «Роли пользователя» выберите из списка роль «Просмотр веб-интерфейса»;
- в поле «Учетная запись пользователя активна» поставьте отметку «☑»;
- в поле «Сменить пароль при входе» снимите отметку «☑».

Нажмите кнопку «Создать».

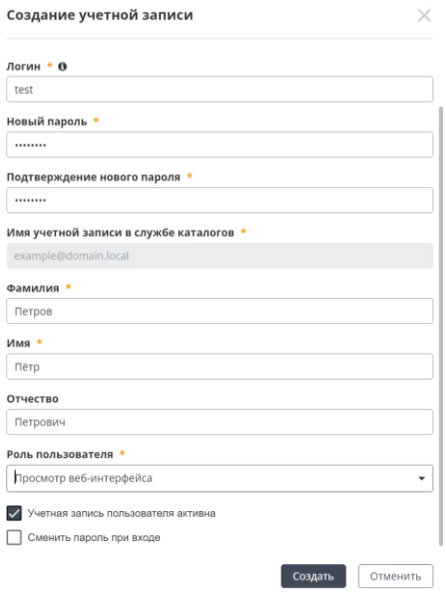


Рисунок 250 — Порядок создания учетной записи

Отредактируйте учетную запись.

Нажмите кнопку «» («Редактировать учетную запись») напротив учетной записи «Петров Пётр Петрович» (**Рисунок 251**).

Рисунок 251 — Расположение кнопки «Редактирование учетной записи»

В появившемся окне «Редактирование учетной записи» поставьте отметку «» у поля «Сменить пароль при входе».

Нажмите кнопку «Сохранить».

Осуществите вход под учётной записью «Иванов Иван Иванович». Для этого:

Нажмите на кнопку «» в левом нижнем углу страницы.

На странице «Авторизация» введите учётные данные «test/”созданный пароль”». Нажмите кнопку «Войти».

Результат шага: появится окно изменения пароли учетной записи пользователя.

На странице «Изменение пароля» введите новый пароль, удовлетворяющий парольной политике.

При вводе некорректного пароля система выведет предупреждение.

После ввода нового корректного пароля нажмите «Изменить пароль» (**Рисунок 252**).

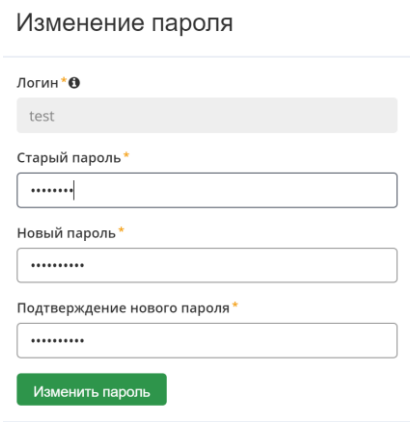


Рисунок 252 –Изменение пароля учетной записи

На странице «Авторизация» введите обновлённые учётные данные пользователя «test». Нажмите кнопку «Войти».

Проверьте работу роли, примененной к пользователю, переходя по страницам веб-интерфейса Комплекса.

Удалите созданного пользователя. Для этого:

Авторизуйтесь под учётной записью «datapk/P@ssw0rd».

Перейдите на страницу «Управление комплексом» → «Пользователи».

Нажмите кнопку «» («Удалить учетную запись») напротив учетной записи «Петров Пётр Петрович».

Рисунок 253 — Кнопка удаления пользователя

В появившемся окне «Подтверждение действия» введите обоснование действия (не менее 3 символов).

Нажмите кнопку «Подтвердить».

Лабораторное задание 6.3. Мониторинг действий пользователей

Цель: сформировать навык просмотра действий пользователей.

Ход работы:

Перейдите в панель мониторинга. Для этого:

Откройте браузер и в адресной строке введите IP-адрес Комплекса.

Авторизуйтесь.

Перейдите на страницу оперативных данных «Мониторинг» → «Панели мониторинга».

Выберите панель мониторинга «События управления» (**Рисунок 254**).

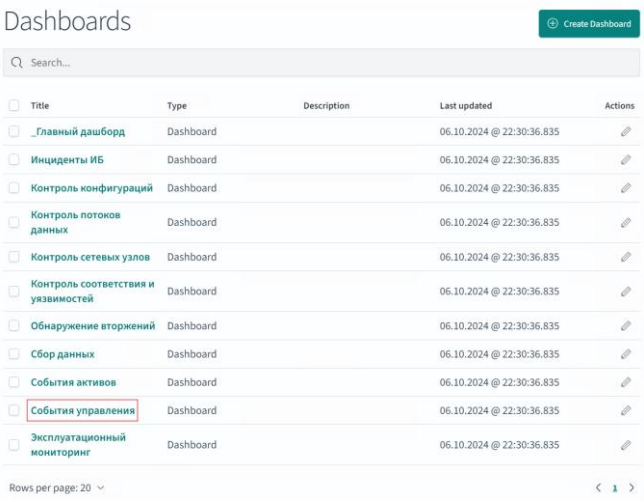
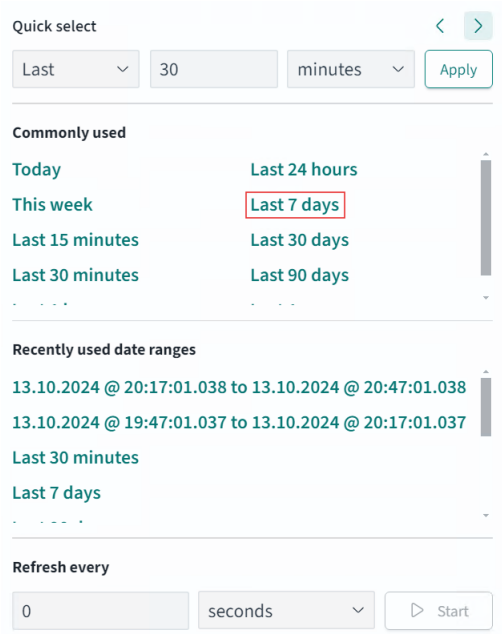
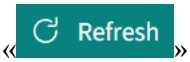


Рисунок 254 — Выбор панели мониторинга «События управления»

Выберите отображение событий за последние 7 дней. Для этого в верхней части страницы нажмите «  » и выберите «Last 7 days».



Нажмите « 

» (**Рисунок 255**).

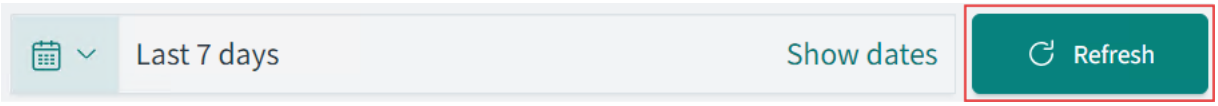


Рисунок 255 — Кнопка «Обновить»

Результат шага: появится список событий управления за последние 7 дней.

Ознакомьтесь с содержанием визуализаций (**Рисунок 256**).

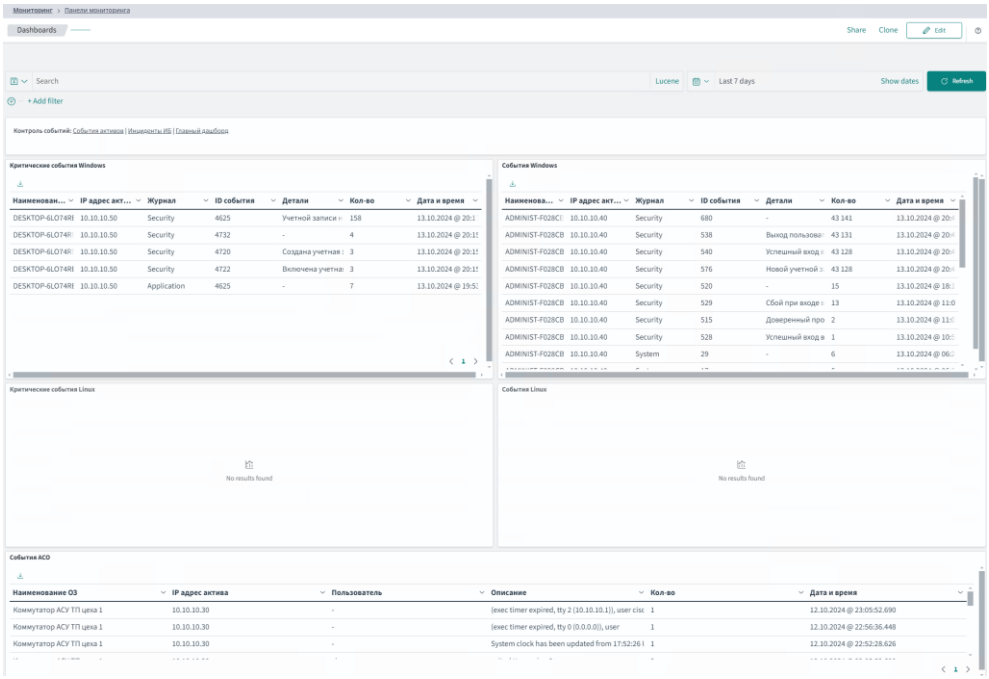


Рисунок 256 — Панель мониторинга «События управления»

Отфильтруйте только успешные попытки входа в систему. Для этого:

Наведите на ячейку, где есть успешный вход в систему.

Нажмите «🔍» во всплывающем элементе «Фильтр значений» (**Рисунок 257**).

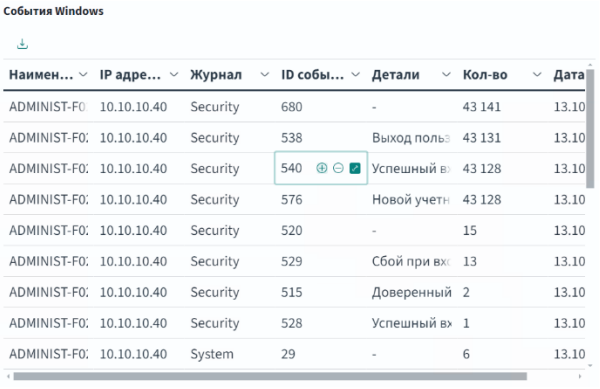


Рисунок 257 — Добавление фильтра по успешным входам в систему

Результат шага: на странице будет применен фильтр по успешным входам в систему (**Рисунок 258**).

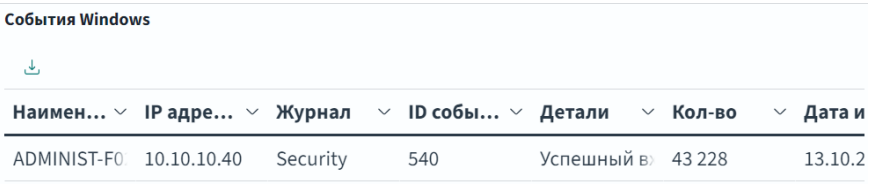


Рисунок 258 — Содержание таблицы «События Windows» после применения фильтра

Исключите вывод событий с успешным входом в систему. Для этого во всплывающем фильтре выберите «» или отредактируйте фильтр. Для этого:

Нажмите на фильтр «description: Успешный вход в систему».

Результат шага: появится контекстное меню фильтра.

Выберите «Исключить результаты» (**Рисунок 259**).

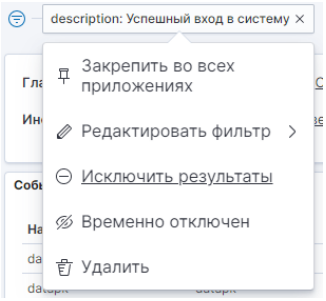


Рисунок 259 — Исключение попыток успешного входа в Комплексе

Отредактируйте фильтр. Для этого:

В контекстном меню фильтра выберите «Редактировать фильтр»;

Результат шага: появится окно редактирования фильтра.

Измените следующие параметры фильтра:

- Поле — user;
- Оператор — является;
- Значение — datapk.

Нажмите «Сохранить» (**Рисунок 260**).

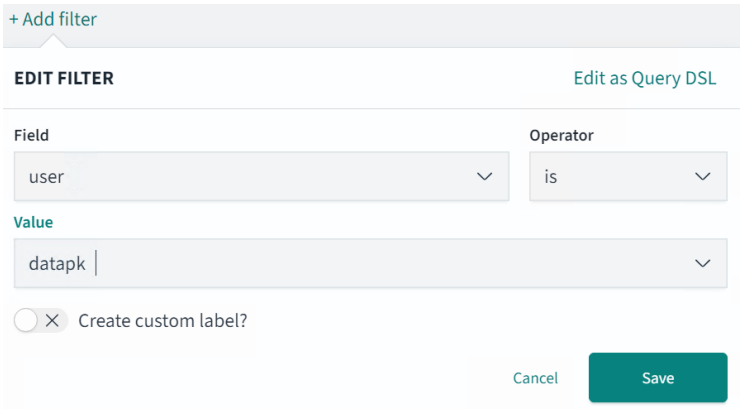


Рисунок 260 — Настройка параметров фильтра

Ознакомьтесь с результатом изменения фильтра.

Просмотрите все события по действиям пользователя datapk. Для этого:

- В контекстном меню фильтра выберите «Закрепить во всех приложениях».
- Перейдите в подраздел «События».
- Отфильтруйте результаты по полю «Описание». Для этого в левой части страницы нажмите «Добавить» напротив поля «description» (**Рисунок 261**).

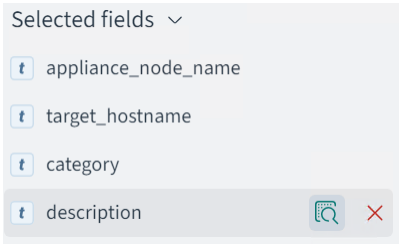


Рисунок 261 — Фильтрация событий по полю «description»

Ознакомьтесь со всеми событиями по действиям пользователя Комплекса (

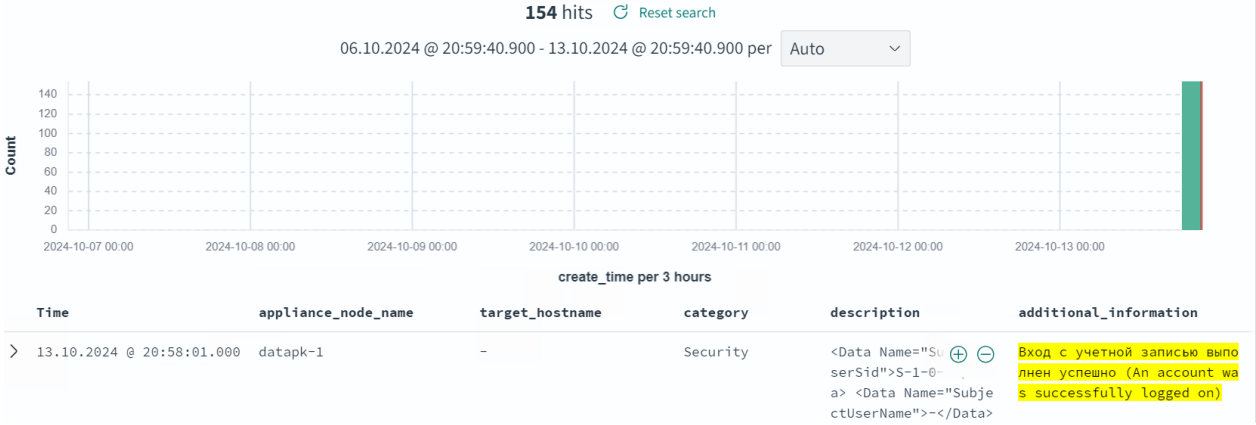


Рисунок 262).

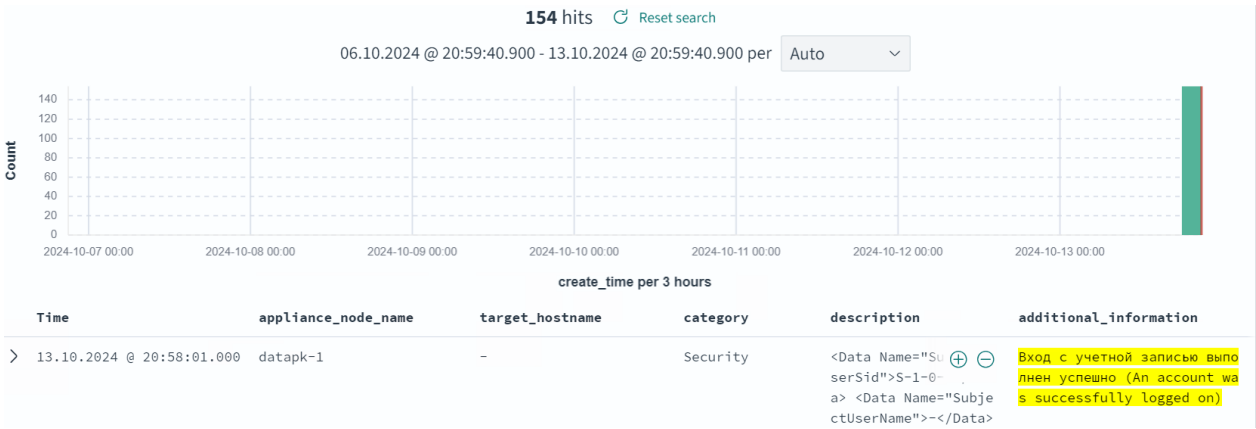


Рисунок 262 — Описание действий пользователя datapk за последнюю неделю

Лабораторная работа 7. Экспорт данных и работа с резервной копией. Отчеты.

Разделы документации

- Резервное копирование данных;
- Восстановление данных из резервных копий.

Справочная информация

Структура tar-архива с резервной копией:

- **data.tar.bz2** — архив включающий в себя данные модулей: «Управление уязвимостями», «Управление внешними событиями», «Анализ промышленного сетевого трафика», а также каталог «/usr/share/udv/datapk» со всем его содержимым;
- **repos_data.tar.bz2** — архив с репозиториями проектов ПЛК модуля «Управление проектами ПЛК»;
- **maria_db_dump.aes, postgres_db_dump.aes, redis_db_dump.aes** — шифрованные резервные копии баз данных (паролем, заданным в интерфейсе или в команде – ключ --password);
- **info.json** — метаданные, включая контрольные суммы.

Файл с резервной копией будет расположен в каталоге «/var/backups».

Файл /etc/machine-id — это уникальный идентификатор машины, который устанавливается в процессе развертывания Комплекса.

machine-id должен быть уникальным и не повторяться на других машинах, особенно в одной локальной сети.

Комплексы уровня Sensor не хранят данные, поэтому их резервное копирование заключается только в ручном сохранении некоторых локальных файлов

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:

- Резервное копирование данных;
- Проверка наличия резервной копии;
- Восстановление данных из резервной копии.

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.

Файлы для лабораторных работ

—

Лабораторное задание 7.1. Создание резервной копии Комплекса

Цель: сформировать навык по созданию резервной копии Комплекса.

Ход работы:

Резервное копирование данных Комплекса уровня Management

Модуль резервного копирования backup_manager локального Комплекса уровня Management сохраняет следующие данные в резервной копии:

- пользовательские конфигурационные файлы сервисов Комплекса;
- справочники уязвимостей (Common Platform Enumeration, Common Vulnerabilities and Exposures и Банк данных угроз безопасности информации ФСТЭК России) для поиска уязвимостей с помощью установленного модуля «Управление уязвимостями»;
- репозитории ПЛК, которые хранятся в модуле «Управление проектами ПЛК»;
- базы данных локального Комплекса, содержащие все накопленные данные.

Для выполнения резервного копирования рабочей директории и баз данных локального Комплекса уровня Management:

1. Подключитесь к Комплексу уровня Management по протоколу SSH с учетной записью «user» и повысьте привилегии до администратора:

```
su -
```

2. Убедитесь, что директория «/usr/share/udv/datapk» занимает менее 500 Мбайт:

```
du -h -d 1 /usr/share/udv/datapk | sort -h
```

3. Из любой директории выполните следующую команду для запуска резервного копирования (**Рисунок 263**):

```
python3 -m backup_manager create --include-nta [quick|full] --
justification 'Регламентные работы' --username 'datapk' --password
'1234567890' --db-username DB_USER --db-password DB_PASS
```

где:

--include-nta — параметр для создания в директории «/var/backups» отдельного архива с резервной копией базы данных clickhouse установленного модуля «Анализ промышленного сетевого трафика». Вместо [quick|full] укажите глубину создания резервной копии БД:

- quick — создание резервной копии оперативных данных БД;
- full — создание полной резервной копии БД.

Если модуль «Анализ промышленного сетевого трафика» не установлен, удалите параметр и его значение из команды.

--justification — комментарий к создаваемой резервной копии;
--username — имя пользователя, который создает резервную копию;
--password — пароль для архива резервной копии;
--db-username — логин пользователя базы данных, значение которого необходимо скопировать из переменной DB_USER конфигурационного файла «/usr/share/udv/datapk/manager.env»;
--db-password — пароль доступа к базе данных, значение которого необходимо скопировать из переменной DB_PASS конфигурационного файла «/usr/share/udv/datapk/manager.env».

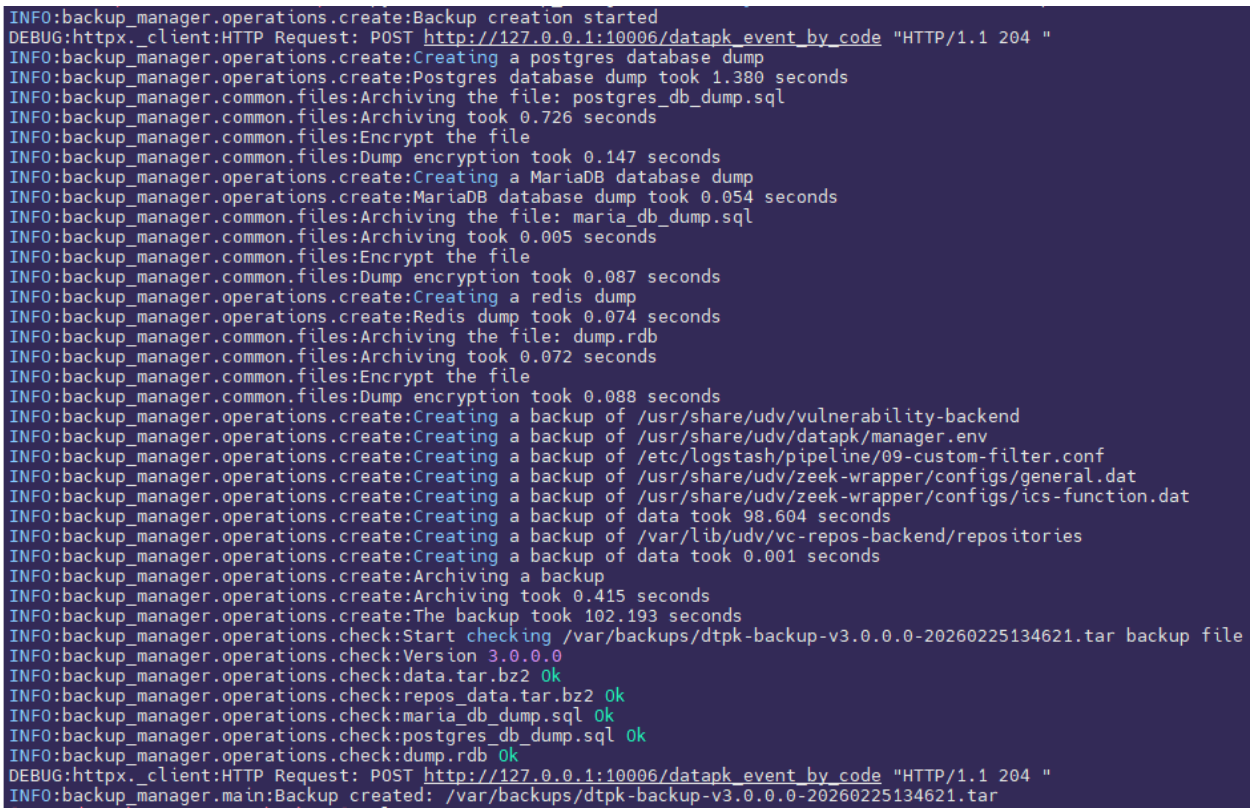


Рисунок 263 — Процесс создания резервной копии Комплекса

Файл с резервной копией будет расположен в каталоге «/var/backups».

Проверку созданной резервной копии можно с помощью команды (**Рисунок 264**):

```
python3 -m backup_manager check --file=dtpk-backup-[version]-
[YYYYmmddhhmmss].tar --password='1234567890'
```

где:

--file — название созданного ранее архива резервной копии, который нужно проверить на корректность;

--password — пароль от архива, заданного в одноименном ключе при запуске резервного копирования.

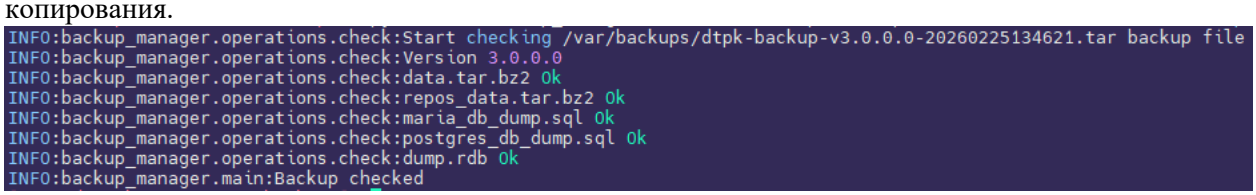


Рисунок 264 — Процесс проверки созданной резервной копии Комплекса

Резервное копирование данных Комплекса уровня Sensor

Комплексы уровня Sensor не хранят данные, поэтому их резервное копирование заключается только в ручном сохранении следующих локальных файлов сенсора:

- /etc/machine-id — идентификатор текущего сенсора;
- /usr/share/udv/datapk/sensor.env — конфигурационный файл сенсора.
- /usr/share/udv/zeek-wrapper/configs/general.dat и /usr/share/udv/zeek-wrapper/configs/ics-function.dat — конфигурационные файлы модуля «Анализ промышленного сетевого трафика» (если он установлен на сенсоре).

Примечание:
Файл /etc/machine-id — это уникальный идентификатор машины, который устанавливается в процессе развертывания Комплекса.
machine-id должен быть уникальным и не повторяться на других машинах, особенно в одной локальной сети.

Лабораторное задание 7.2. Экспорт данных Комплекса

Цель: сформировать навык по экспорту данных из Комплекса.

Ход работы:

Экспорт индексов событий

Перейдите в подраздел оперативных данных «Администрирование» → «События и инциденты» → «Индексы».

В верхней части страницы нажмите « Архивировать » (**Рисунок 265**).

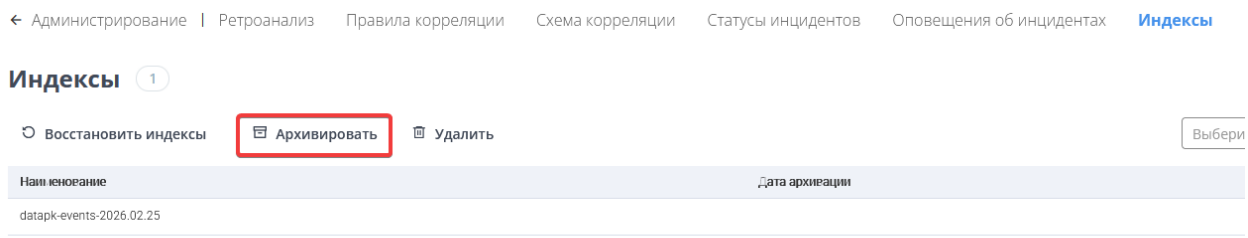


Рисунок 265 — Кнопка архивации индексов событий

> **Примечание:**
> При нажатии на кнопку «Архивировать», будут заархивированы все отфильтрованные индексы, которые отображаются на данной странице. Если нужно заархивировать индексы только за определенные даты, следует воспользоваться фильтром и указать

Сформированные индексы будут расположены в каталоге «/var/backups/elasticsearch/indices» и доступны для восстановления.

Обновите страницу и убедитесь, что дата создания резервной копии обновилась для всех индексов (**Рисунок 266**).

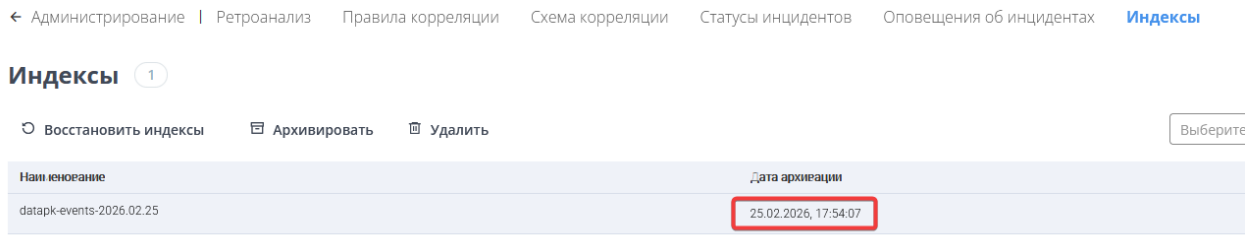


Рисунок 266 — Индексы событий с обновленной датой архивации

Экспорт справочников

Перейдите в подраздел управления «Администрирование» → «Импорт и экспорт».

Для экспорта конкретного справочника, нажмите кнопку экспорта в соответствующем поле (**Рисунок 267**):

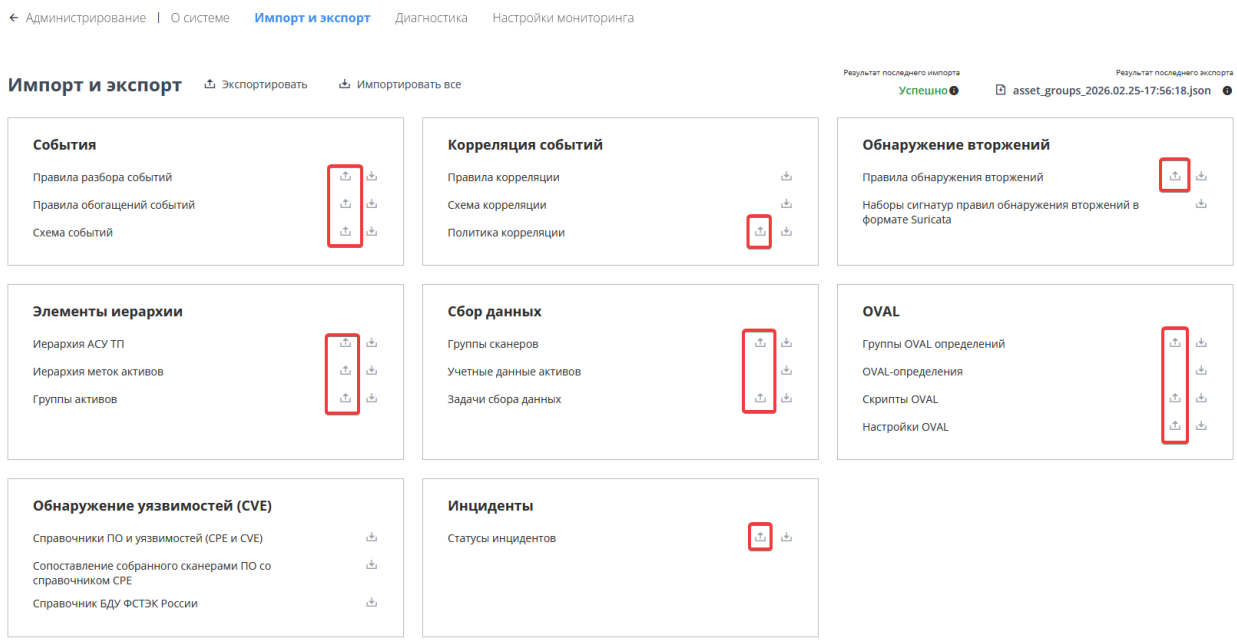


Рисунок 267 — Экспорт отдельных справочников

Для группового экспорта нескольких справочников нажмите в верхней части страницы «Экспортировать» (**Рисунок 268**).

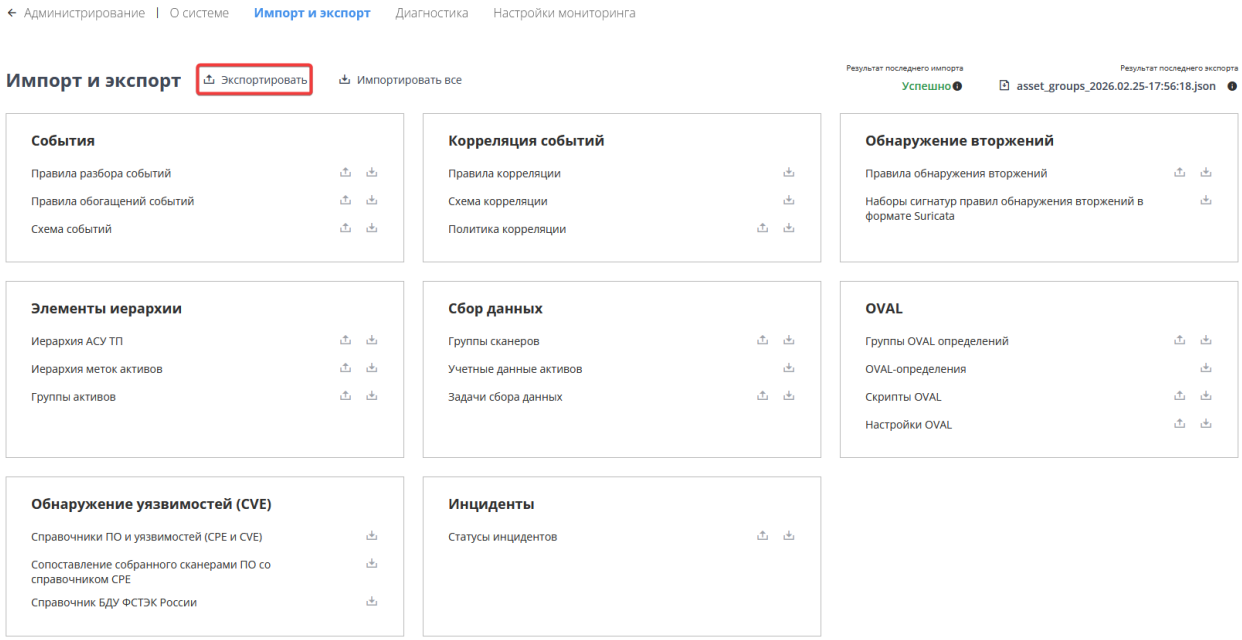


Рисунок 268 — Кнопка группового экспорта справочников

В появившемся окне выберите все справочники, кроме справочников OVAL (**Рисунок 269**).

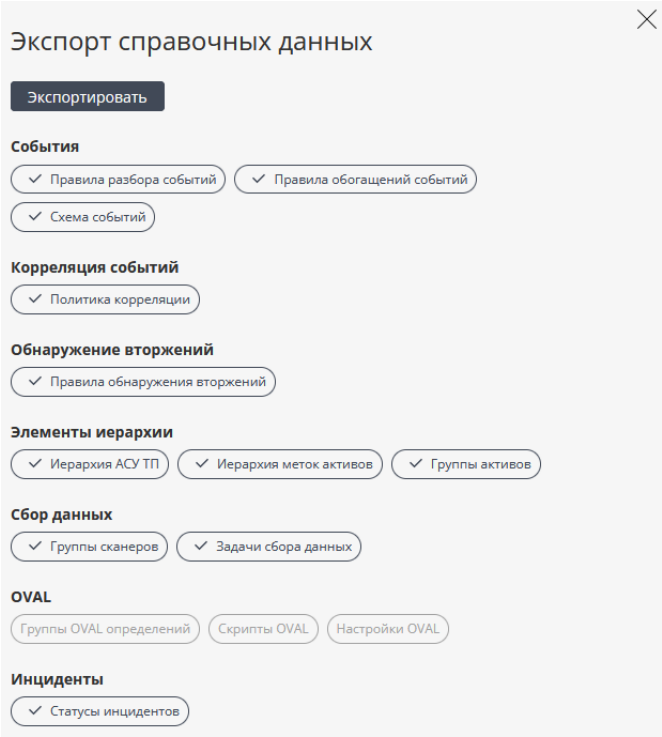


Рисунок 269 — Экспорт справочных данных

Нажмите «Экспортировать».

Появится уведомление об успешном экспорте данных с ссылкой на скачивание архива «.tar» с экспортированными справочниками (**Рисунок 270**).

Рисунок 270 — Результат экспорта справочников

Лабораторное задание 7.3. Восстановление Комплекса из резервной копии

Цель: сформировать навык восстановлению Комплекса из резервной копии.

Ход работы:

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:

- Резервное копирование данных.
- Проверка наличия резервной копии.
- 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».

> **Примечание:**
> 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

Восстановление данных Комплекса уровня Management и 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».

Подключитесь к Комплексу уровня Management по протоколу SSH с учетной записью «user» и повысьте привилегии до администратора:

```
su -
```

Убедитесь, что архив резервной копии **dtpk-backup-v3.0.[минорная_версия].[патч_версия]-{ГГГГММДДччммсс}.tar** расположен в директории «/var/backups».

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».

Проверьте целостность архива резервной копии так же, как в лабораторном задании 7.1 и убедитесь в отсутствии ошибок после окончания проверки резервной копии.

Остановите работу всех сервисов Комплекса:

```
/usr/bin/stop_services.sh
```

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
```

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).

Выполните восстановление внешних событий. Для этого поместите сохраненные ранее индексы событий в директорию «/var/backups/elasticsearch/uploads».

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».

После успешного восстановления перезагрузите Комплекс, выполнив команду:

```
shutdown -r now
```

Войдите в веб-интерфейс Комплекса под учетной записью администратора.
Перейдите в раздел «События» → «Экспертный режим».
Нажмите «Create index pattern».
В поле «Index pattern name» введите «datapk-events-*» и нажмите «Next step».
В поле «Time field» выберите «create_time» и нажмите «Create index pattern».
Перейдите в раздел «Администрирование» → «События и инциденты» → «Индексы».
Нажмите «Восстановить индексы».

Восстановление данных Комплекса уровня Sensor

Выполните развертывание Комплекса уровня Sensor в соответствии с разделом «Установка Комплекса уровня Sensor».

Замените файл «/etc/machine-id» на файл, сохраненный при резервном копировании.

Сохраните файл «machine-id» в директории «/var/lib/dbus».

Замените файл «/usr/share/udv/datapk/sensor.env» на файл, сохраненный при резервном копировании.

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.

Перезагрузите Комплекс, выполнив команду:

```
shutdown -r now
```

Войдите в веб-интерфейс Комплекса уровня Management, к которому подключен данный Комплекс уровня Sensor.

Перейдите в раздел Сенсоры и убедитесь, что Комплекс уровня Sensor успешно подключился к Комплексу уровня Management.

Лабораторное задание 7.4. Формирование отчетов

Цель: сформировать навыки по формированию отчетов о работе Комплекса.

Ход работы:

В таблице ниже будут представлены отчеты, формируемые Комплексом (**Таблица 11**):

Таблица 11 – Виды отчетов Комплекса

Страница	Содержание отчета	Формат отчета
Активы	Выбранные активы	html, xlsx
	Уязвимости последнего проверяемого актива	csv
Инциденты	Выбранные инциденты	html, xlsx
Конфигурации	Отфильтрованные конфигурации	html, xlsx
Перечень ПО	Результаты сопоставления собранного сканерами ПО и ОС со справочником CPE для актива, для которого в последний раз выполнялся поиск уязвимостей	csv
Результаты проверок	Отфильтрованные результаты проверок	html, xlsx

Самостоятельное задание

Выгрузите отчеты по активам и инцидентам за время прохождения лабораторных работ в формате «.xlsx».

Результат продемонстрируйте преподавателю.

Лабораторная работа 8. Обращение в техническую поддержку и сбор логов

Разделы документации

- Анкета при обращении в сервисный центр;
- Диагностика сервисов и иерархии;
- Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных.

Справочная информация

Полнота предоставленных данных значительно ускоряет процесс решения сервисных заявок.

Многие проблемы, возникающие в ходе работы Комплекса, описаны в документации, в разделе: «Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных». Перед созданием обращения в техническую поддержку, рекомендуется ознакомиться данным разделом документации.Многие проблемы, возникающие в ходе работы Комплекса, описаны в документации, в разделе: «Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных». Перед созданием обращения в техническую поддержку, рекомендуется ознакомиться данным разделом документации.Скрипт для сбора логов Комплекса периодически обновляется. Настоятельно рекомендуется загружать актуальную версию скрипта непосредственно перед сбором логов.

Ссылку на актуальную версию диагностического скрипта всегда можно запросить у технической поддержки.Скрипт для сбора логов Комплекса периодически обновляется. Настоятельно рекомендуется загружать актуальную версию скрипта непосредственно перед сбором логов.

Ссылку на актуальную версию диагностического скрипта всегда можно запросить у технической поддержки.

Диагностический скрипт собирает следующие данные:

- общая информация об аппаратных компонентах Комплекса;
- общая информация об ОС;
- общая информация о настройках сети;
- общая информация о сертификатах Комплекса;
- журналы служб Комплекса Management и Sensor;
- метрики некоторых служб Комплекса;
- некоторые конфигурационные файлы Комплекса;
- общая информация о базах данных Комплекса.

Файлы для лабораторных работ

- **dtpk_get_logs-3_0.bash —** диагностический скрипт для сбора логов Комплекса.

Лабораторное задание 8.1. Обращение в техническую поддержку

Цель: сформировать навык составления анкеты для обращения в техническую поддержку.

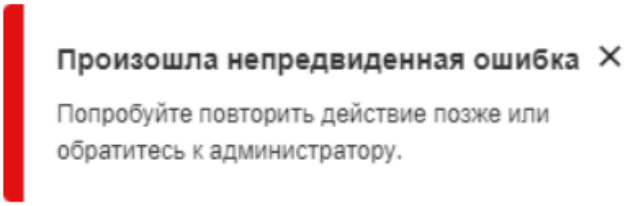
Ход работы:

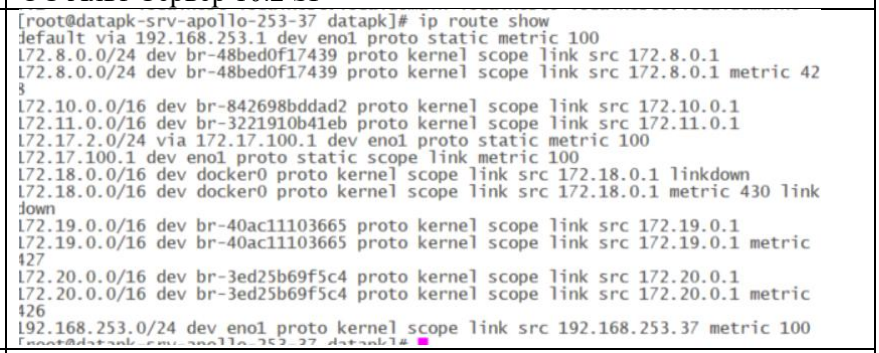
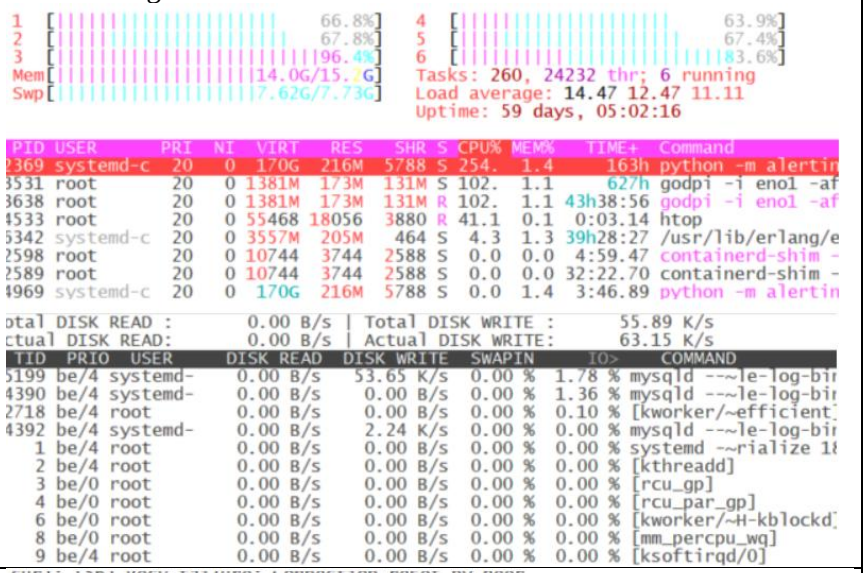
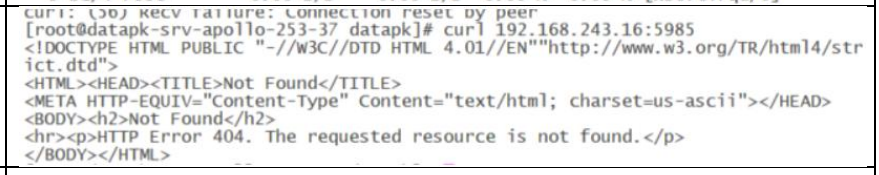
В случае нарушения корректной работы Комплекса или появления вопросов по его работе, контенту и пр. составляется анкета для обращения в техническую поддержку.

Ниже будет таблица с данными анкеты, которые требуется предоставить при обращении (**Таблица 12**):

Внимание!
Полнота предоставленных данных значительно ускоряет процесс решения сервисных заявок.

Таблица 12 – Анкета для обращения в техническую поддержку

Параметр	Пример
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 UDV DATAPK (включая полученные с сенсора)	150 активов, 300 тыс. сессий, 250 тыс. событий в сутки
Количество подчиненных UDV DATAPK уровня Sensor	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.
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 (см. раздел «Диагностика сервисов и иерархии»)	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)
Версия ОС	ОС Альт Сервер 10.2 SP
Вывод таблицы маршрутизации (**route -n** или **ip route show**)	
Свободное место на корневом разделе диска (**df -Th /**) Свободная оперативная память, текущий список процессов (**top**) Значение Load Average Загрузка диска (**iotop**)	Свободное место на корневом разделе: 2.5 ТБ Свободная оперативная память: 1 МБ Load Average: 14 
Наличие сетевых доступов до проблемного актива/UDV DATAPK (**curl [ip_addr]:[port_number]**)	
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

Заявки на создание сканеров сбора данных для отдельных активов

Список поддерживаемых устройств, с которых Комплекс может осуществлять активный сбор данных, постоянно расширяется.

Если в Вашей сети имеется устройство, для которого отсутствуют сканеры, то в таком случае оформляется запрос на разработку сканера.

Внимание!
Полнота предоставленных данных значительно ускоряет процесс разработки контента.

В таблице ниже будет пример анкеты, которая составляется для запроса на разработку сканера (**Таблица 13**):

Таблица 13 – Анкета на разработку сканера

Параметр	Пример
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
Сведения об активе (тип, производитель, модель, версия ОС, настроенные протоколы сбора данных)	Коммутатор Eltex MES1428, SSHv2
Тип собираемых данных (события/конфигурация)	Конфигурация
Описание того, какие данные планируется собирать	Планируется осуществлять сбор данных ARP-таблицы
Команды для получения нужных данных актива (в текстовом виде)	show arp
Вывод команд для получения нужных данных (в текстовом виде и на скриншотах), либо удаленный доступ к тестовому активу.	eltext-lab#show arp Total number of entries: 1 VLAN Interface IP address HW address status vlan 2522 gil/0/24 10.52.1.1 e4:5a:d4:c0:b0:c0 dynamic Текстовый файл с данным выводом во вложении

Результат рассмотрения заявки на поддержку типа актива отправляется в адрес заявителя в течение 14 календарных дней с момента регистрации заявки в сервисном центре производителя Комплекса посредством электронной почты.

Заявки на разработку нормализации для отдельных активов

Список поддерживаемых устройств, с которых Комплекс может получать события, постоянно расширяется.

Если в Вашей сети имеется устройство, нормализация для которого отсутствует в Комплексе, можно оформить запрос на разработку нормализации для конкретного актива, типа активов.

Внимание!
Полнота предоставленных данных значительно ускоряет процесс разработки контента.

В таблице ниже будет пример анкеты, которая составляется для запроса на разработку нормализации (**Таблица 14**):

Таблица 14 – Анкета на разработку нормализации

Параметр	Пример
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
Сведения об активе (тип, производитель, модель, версия ОС, настроенные протоколы сбора данных)	Коммутатор Eltex MES1428, Syslog
Тип собираемых данных (события/конфигурация)	События
Описание того, какие данные планируется собирать	Планируется осуществлять сбор событий любой критичности
Примеры событий (в текстовом виде), либо удаленный доступ к тестовому активу.	Примеры событий из DATAPK приложены в формате txt и json.

Результат рассмотрения заявки на поддержку типа актива отправляется в адрес заявителя в течение 14 календарных дней с момента регистрации заявки в сервисном центре производителя Комплекса посредством электронной почты.

Примечание:
Многие проблемы, возникающие в ходе работы Комплекса, описаны в документации, в разделе: «Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных». Перед созданием обращения в техническую поддержку, рекомендуется ознакомиться данным разделом документации.

Лабораторное задание 8.2. Сбор логов Комплекса

Цель: сформировать навык сбора диагностических данных Комплекса для технической поддержки.

Ход работы:

Большинство проблем, возникающих в ходе работы Комплекса, видно в диагностических логах. С помощью скрипта «dtpk_get_logs-3_0.bash» происходит однократный сбор состояния системы и журналов сервисов Комплекса уровней Management и Sensor на текущем сервере за указанный период времени в часах.

> **Примечание:**
> Скрипт для сбора логов Комплекса периодически обновляется. Настоятельно рекомендуется загружать актуальную версию скрипта непосредственно перед сбором логов.
> Ссылку на актуальную версию диагностического скрипта всегда можно запросить у ..

Для сбора диагностических логов выполните следующие действия:

1. Поместите скрипт «dtpk_get_logs-3_0.bash» в операционную систему Комплекса, к примеру, в директорию «/opt».
2. Подключитесь к выбранному Комплексу по SSH с учетной записью обычного пользователя и повысьте привилегии до администратора:

```
su -
```

3. Перейдите в директорию «/opt»:

```
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).

Чтобы собрать журналы за последние 6 часов, выполните команду:

```
bash dtpk_get_logs-3_0.bash 6
```

В текущей директории «/opt» будет создан архив «logs-[hostname]-[текущая_дата].tar.gz» с журналами сервисов текущего Комплекса за выбранный период времени.

Диагностический скрипт собирает следующие данные:

- общая информация об аппаратных компонентах Комплекса;
- общая информация об ОС;
- общая информация о настройках сети;
- общая информация о сертификатах Комплекса;
- журналы служб Комплекса Management и Sensor;
- метрики некоторых служб Комплекса;
- некоторые конфигурационные файлы Комплекса;
- общая информация о базах данных Комплекса.

Самостоятельное задание

Соберите логи Комплекса за 2 часа. Ознакомьтесь с содержимым сформированного архива.