

Инструкция по развертыванию ПК CL DATARK на ОС Альт Сервер 10 и Альт СП релиз 10

ООО «СайберЛимфа» <support@cyberlympha.com>, Мирдофатихов Роман

Version 1.19.0.1, 26.03.2024

Оглавление

1. Дистрибутивы	1
1.1. Состав и назначение дистрибутивов	1
1.2. Контрольные суммы файлов	1
2. Требования и рекомендации	2
2.1. Общие	2
2.2. ОС Альт Сервер 10 или Альт СП Сервер релиз 10	2
2.3. Рабочие станции ОС АЛЬТ на 10-й платформе	2
3. Предварительная подготовка	3
3.1. Обновление ОС АЛЬТ	3
3.2. Настройка NTP-сервера	3
3.2.1. Настройка openntpd на серверной ОС АЛЬТ	3
3.2.2. Проверка NTP-сервера локально	4
3.2.3. Проверка NTP-сервера с любой рабочей станции	4
4. Установка CL DATAPK	6
5. Запуск CL DATAPK	7
6. Первичная настройка CL DATAPK	9
7. Завершение работы	16

1. Дистрибутивы

- Файлы дистрибутива программного комплекса **CyberLympha DATAPK** (ПК **CL DATAPK**), перечисленные в следующем подразделе;
- Для развертывания ПК **CL DATAPK** потребуется ОС **Альт Сервер 10** (проверялось на дистрибутивах 10.0, 10.1 и 10.2) либо ОС **Альт СП Сервер релиз 10**;
- Для начальной настройки и дальнейшего управления ПК **CL DATAPK** потребуется ОС **Альт Рабочая станция 10** (проверялось на дистрибутивах 10.0, 10.1 и 10.2) либо ОС **Альт СП Рабочая станция релиз 10**;

1.1. Состав и назначение дистрибутивов

Название дистрибутива (файла)	Версия	Назначение
Альт СП Сервер (x86_64)	Релиз 10	для развертывания CL DATAPK
Альт Сервер (x86_64)	10.x	для развертывания CL DATAPK
Альт СП Рабочая станция (x86_64)	Релиз 10	для управления CL DATAPK
Альт Рабочая станция (x86_64)	10.x	для управления CL DATAPK
cl-datapk-*.rpm (noarch)	1.19.0.1	основной пакет CL DATAPK
cl-datapk-defconf-*.rpm (noarch)	1.19.0.1	конфигурация по умолчанию
datapk-*.tar.gz (x86_64)	1.19.0.1	базовые слои CL DATAPK
snmb_mibs.tar.gz (noarch)	1.19.0.1	архив SNMP MIBs

1.2. Контрольные суммы файлов

Название файла	Контрольная сумма MD5
alt-sp-server-20230529-x86_64.iso	0fc20c6767e4f920118b5175da448b79
alt-server-10.0-x86_64.iso	3cc064c3410e8763c2b7bbd8d0af4936
alt-server-10.1-x86_64.iso	80d02a4d1cf54a8ab5868615cabb4255
alt-server-10.2-x86_64.iso	28827cc95d0dc18c1fb7ecccf0ddcac8
alt-sp-workstation-20230528-x86_64.iso	a5fcb8fb1f3b0b3edf5903eb73932bee
alt-workstation-10.0-x86_64.iso	8e73289f12ab15ee71d07b82ac532ad3
alt-workstation-10.1-x86_64.iso	84605e6eb98ae4015da7a7d719235941
alt-workstation-10.2-x86_64.iso	5ad8a1e6472950d2bbf63d9981d043b5
cl-datapk-1.19.0.1-alt1.noarch.rpm	9fc253b5e269688993b1180be674087f
cl-datapk-defconf-1.19.0.1-alt1.noarch.rpm	0837f2205773f3cf7fec7802578e53ec
datapk-v1.19.0.1.tar.gz	c6dc6f136d73ad7c9a4fcd4c196f873f
snmb_mibs.tar.gz	f60dcaedee7b1066f3490b481baef50d

2. Требования и рекомендации

2.1. Общие

- В закрытом сетевом контуре АСУ ТП должен быть настроен, по меньшей мере, один NTP-сервер (рекомендуется 2-3 независимых NTP сервера);
- Из закрытого сетевого контура АСУ ТП необходимо обеспечить доступ к Интернет репозиторию для обновления пакетной базы ОС Альт либо, используя ЦУС, развернуть отдельный сервер с зеркалом репозитория, согласно [документации](#).

2.2. ОС Альт Сервер 10 или Альт СП Сервер релиз 10

- Сервер для развертывания ПК **CL DATAPK** должен иметь, как минимум, два сетевых интерфейса: один — для управления комплексом, второй — для прослушивания трафика с объектов защиты;
- Рекомендуемый объем ОЗУ для развертывания ПК **CL DATAPK** — не менее 32 ГБ;
- Рекомендуемый объем свободного места на диске — не менее 400 ГБ;
- Рекомендуемое число ядер ЦП — не менее 8;
- На новых серверах предпочтительно использовать UEFI загрузку;
- ОС **Альт Сервер 10** устанавливается с минимальным профилем;
- В процессе установки любой серверной ОС конфигурируется только один сетевой интерфейс — для управления комплексом, интерфейс для прослушивания трафика настраивать при установке ОС не требуется, при этом не следует менять используемую по умолчанию подсистему управления сетью [Etcnet](#).
- Для работы ПК **CL DATAPK** рекомендуется разбивать диск вручную с использованием LVM и файловой системы XFS, размещать все данные на одном разделе вместе с системой, место для SWAP-раздела также стоит предусмотреть.

2.3. Рабочие станции ОС Альт на 10-й платформе

- Рекомендуемый объем ОЗУ для управления ПК **CL DATAPK** — не менее 8 ГБ;
- Рекомендуемое разрешение экрана — не менее 1920x1080;
- Для работы с веб-интерфейсом Комплекса рабочие станции должны быть подключены к подсети управляющего контура Комплекса и поддерживать браузеры:
 - ОС **Альт СП Рабочая станция релиз 10**:
Mozilla Firefox ESR версии 102.11.0 и выше;
 - ОС **Альт Рабочая станция 10**:
Chromium версии 96.0.46 и выше либо Mozilla Firefox ESR версии 91.3 и выше.
Допустимо использовать другие веб-браузеры, базирующиеся на вышеуказанных.

3. Предварительная подготовка

3.1. Обновление ОС Альт

После установки ОС Альт должна быть обновлена до актуального состояния. [Инструкция по обновлению](#) сертифицированных ОС поставляется вместе с дистрибутивом, для остальных ОС выполните нижеперечисленные шаги:

1. Войдите под учетной записью **«root»**, введя ее имя и пароль;



При использовании удаленного доступа к серверу, можно зайти под созданной на этапе установки ОС учетной записью обычного пользователя, после чего ввести команду **su-** (обязательно с минусом на конце) и пароль от учетной записи **«root»**. Пароль при вводе никогда не отображается.

2. Выполните штатное обновление ОС Альт командой:

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

3. Выполните перезагрузку компьютера командой **reboot**;
4. После перезагрузки можно снова зайти под учетной записью **«root»**, удалить не нужные ядра командой **remove-old-kernels** и почистить кэш командой **apt-get clean**.

3.2. Настройка NTP-сервера

Для корректной работы ПК **CL DATAPK** на серверной ОС Альт должен быть поднят NTP-сервер, часы должны быть синхронизированы. ОС Альт поддерживает различные серверы времени, включая **openntpd**, **ntp** и **chrony**. Изначально все ОС Альт уже настроены на работу с **«pool.ntp.org»** через **openntpd**, что может подходить не всем.

3.2.1. Настройка openntpd на серверной ОС Альт

1. Используя текстовый редактор (уже установлены **vim**, **mcedit**, другие надо устанавливать), откройте файл **/etc/ntpd.conf**, например, так: **mcedit /etc/ntpd.conf**;
2. Замените **«pool.ntp.org»** на имя или IP-адрес своего локального NTP-сервера либо прокомментируйте все строки, которые начинаются со слова **«servers»**, и добавьте одну строку **«server <IP>»** для каждого NTP-сервера с адресом **<IP>**.
3. Сохраните и закройте файл;
4. Вручную синхронизируйте время с одним из ваших локальных NTP-серверов:

```
# ntpdate 10.20.19.11
15 Mar 10:23:12 ntpdate[3328]: adjust time server 10.20.19.11 offset +0.085952 sec
```

5. Сервер ПК **CL DATAPK** может выполнять роль NTP-сервера. По умолчанию он работает в режиме NTP-клиента. Для изменения этой настройки введите команду:

```
# control ntpd server
```

6. Проверку работы службы NTP можно выполнить уже после установки ПК и перезагрузки сервера. Если хотите проверить работу NTP сразу, сначала перезапустите службу точного времени командой: `service ntpd restart`.

3.2.2. Проверка NTP-сервера локально

Включите просмотр последних событий журнала и наблюдайте за процессом синхронизации времени:

```
# journalctl -f -u ntpd
Mar 15 10:23:19 datapk-alt ntpd[3334]: ntp engine ready
Mar 15 10:23:35 datapk-alt ntpd[3334]: reply from 10.20.19.11: offset 0.014736 delay
0.064452, next query 8s
Mar 15 10:23:43 datapk-alt ntpd[3334]: peer 10.20.19.11 now valid
...
Mar 15 10:24:38 datapk-alt ntpd[3333]: adjusting local clock by -0.180809s
Mar 15 10:24:38 datapk-alt ntpd[3333]: skipping very first adjtimex
...
Mar 15 10:32:26 datapk-alt ntpd[3333]: adjusting local clock by -0.375735s
Mar 15 10:32:26 datapk-alt ntpd[3333]: interval 467.938 olddelta 0.000 (delta - olddelta)
-0.376
Mar 15 10:32:26 datapk-alt ntpd[3333]: error_ppm -401.479 freq_delta -96910 tick_delta -4
Mar 15 10:32:26 datapk-alt ntpd[3334]: clock is now synced
```



Обратите внимание, что после первоначальной подстройки системных часов демон `openntpd` не сразу выполняет синхронизацию. Окончательная синхронизация зависит от количества и удаленности NTP-серверов, качества ЛВС и хода часов компьютера. При этом в журнале должно появиться сообщение: «**clock is now synced**».

Данный шаг выполнять необязательно, поскольку к этому времени системные часы компьютера уже должны быть синхронизированы вручную. Для завершения наблюдения нажмите **Ctrl-C**.

3.2.3. Проверка NTP-сервера с любой рабочей станции

Если планируется использовать CL DATAPK в качестве NTP-сервера, убедитесь, что с вашим новым сервером ПК **CL DATAPK** можно синхронизировать часы, используя IP-адрес его интерфейса управления, например, **10.51.203.213**:

```
$ su - -c 'ntpdate 10.51.203.213'
```

```
15 Mar 10:35:02 ntpdate[3328]: adjust time server 10.51.203.213 offset +0.157953 sec
```

При этом на сервере должен быть выполнен пункт **3.2.1.5** инструкции, **должно пройти достаточно времени**, чтобы сервер мог выступать в качестве надежного источника точного времени. Иначе вы получите сообщение: «**no server suitable for synchronization found**».

4. Установка CL DATAPK

1. Выполните установку RPM-пакетов для работы ПК CL DATAPK:

```
# cd /путь/к/файлам/дистрибутива/  
# apt-get install -y \  
  ./cl-datapk-1.19.0.1-alt1.noarch.rpm \  
  ./cl-datapk-<конфигурация>-1.19.0.1-alt1.noarch.rpm
```



Все файлы дистрибутива **CL DATAPK** должны быть предварительно сохранены в один каталог на сервере, например, в домашний каталог созданного на этапе установки обычного пользователя. Основной пакет должен устанавливаться одновременно с одной из возможных конфигураций, в зависимости от уровня, который занимает в иерархии настраиваемый комплекс **CL DATAPK** (ТК, Филиал или Предприятие).

2. Запустите пост-установочный скрипт, который выполнит конфигурирование комплекса и создаст файл окружения `/opt/datapk/.env`, описанный в разделах «Основные переменные файла env» и «Рекомендации по использованию переменных файла .env» Руководства по эксплуатации.

```
# datapk-postinstall.sh
```



Пост-установочный скрипт должен быть запущен из каталога с файлами дистрибутива. Если запуск без параметров не привел к успеху, воспользуйтесь встроенной подсказкой (`datapk-postinstall.sh --help`). Работа скрипта должна завершиться сообщением:

```
Success! CL DATAPACK prepared without any critical errors.  
Don't forget to reboot and run: 'cd /opt/datapk && docker-compose up -d'...
```

3. Выполните перезагрузку компьютера командой `reboot`.
4. Убедитесь, что сетевой интерфейс для сбора трафика перешел в неразборчивый режим (PROMISC MODE), выполнив команду `ip a`:

```
$ ip a show ens224  
3: ens224: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group  
default qlen 1000  
    link/ether 00:50:56:b7:02:c6 brd ff:ff:ff:ff:ff:ff
```

5. Убедитесь в корректности работы NTP — см. предыдущий раздел.

5. Запуск CL DATAPK

1. Запустите все сервисы ПК CL DATAPK и дождитесь окончания их запуска:

```
$ su - -c 'cd /opt/datapk && docker-compose up -d'
...
Creating logstash           ... done
Creating user_service       ... done
Creating host_data_collector ... done
Creating alerting          ... done
Creating auth_backend       ... done
Creating exporter          ... done
Creating report_generator   ... done
Creating api                ... done
Creating ngui               ... done
```

2. При помощи команды `docker ps` убедитесь, что все сервисы ПК CL DATAPK запущены — имеют статус «Up» и не имеют статуса «Restarting» в графе «STATUS»:

```
$ su - -c 'docker ps --format="table {{.ID}}\t{{.Names}}\t{{.Status}}"'
CONTAINER ID   NAMES                                STATUS
e619c12cdb67   ngui                                  Up 29 minutes
2bba865e27cc   api                                    Up 29 minutes
152d838defd8   exporter                              Up 29 minutes
...
d9024cb8db3a   db                                    Up 30 minutes
6d1dbb29a85b   sql_connector                         Up 30 minutes
ddc478f1b4ba   modbus_connector                     Up 30 minutes
8faf4052bef7   plc_config_connector                 Up 30 minutes
bb8acdbe92e3   opc_connector                        Up 30 minutes
28bd0f6249ee   node_exporter                       Up 30 minutes
1face9571f42   plc_connector                        Up 30 minutes
7707e3c1a2b2   terminal_connector                   Up 30 minutes
83d5a24753f2   nginx                                 Up 30 minutes
3c0f616d2a01   snmp_connector                       Up 30 minutes
f99d80acaa5c   pg                                    Up 30 minutes
```

3. Проверьте возможность подключения к ПК CL DATAPK по протоколу HTTPS. Для этого в ОС **Альт Рабочая станция 10** или **Альт СП Рабочая станция релиз 10** откройте браузер и введите IP-адрес интерфейса управления CL DATAPK, например: <https://10.51.203.213/>
4. Если в браузере появится предупреждение о незащищенном подключении (по причине того, что созданный серверный сертификат не является доверенным для браузера), нажмите на кнопку «Дополнительно...» (Рисунок 1):

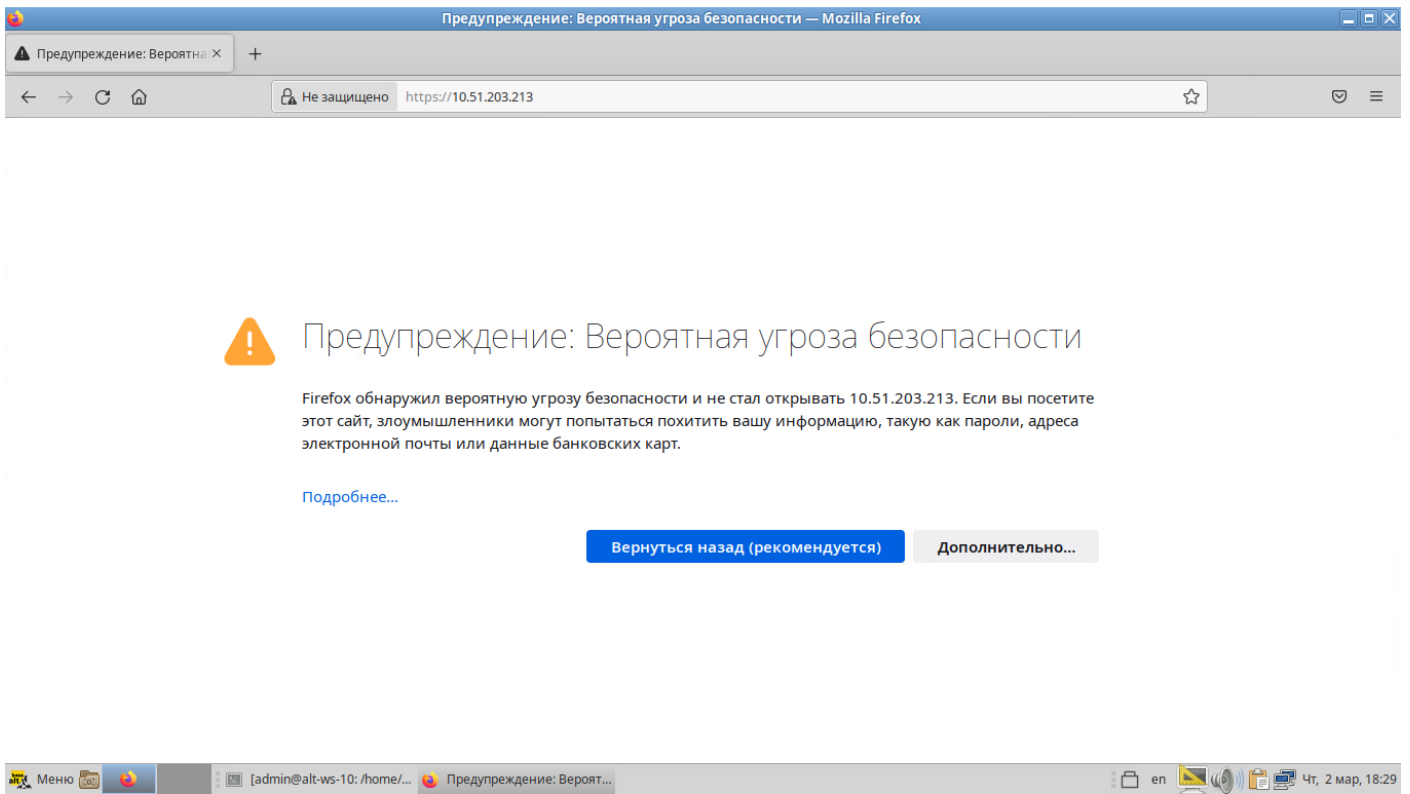


Рисунок 1 – Окно предупреждения о незащищенном подключении

5. Для продолжения подключения к CL DATAPK нажмите кнопку «Принять риск и продолжить» (Рисунок 2):

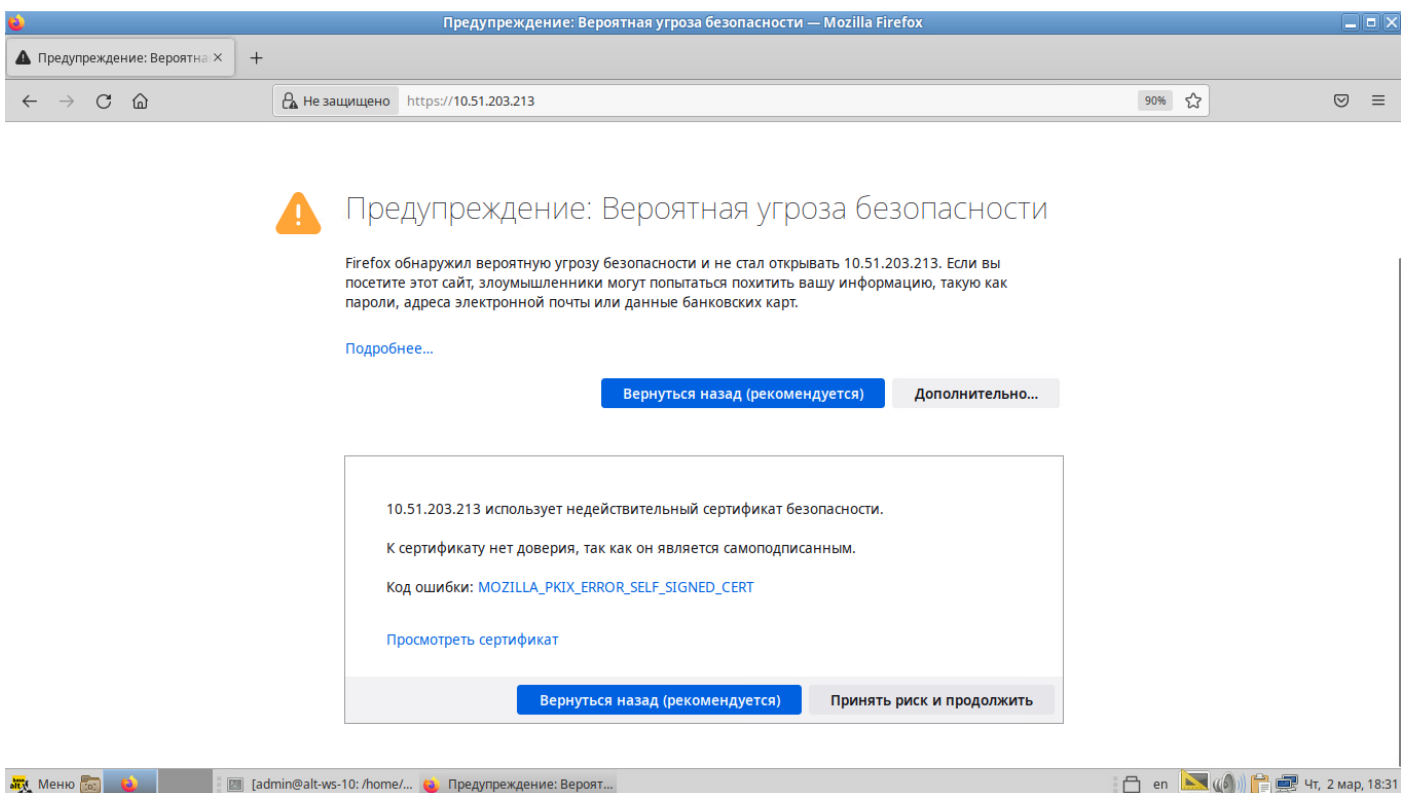


Рисунок 2 – Подключение к CL DATAPK по HTTPS

6. При успешном подключении к ПК CL DATAPK в браузере отобразится окно авторизации (Рисунок 3).

6. Первичная настройка CL DATAPK

1. Подключитесь к ПК CL DATAPK. Для этого:

1. Откройте браузер.
2. В адресной строке введите IP-адрес интерфейса управления ПК CL DATAPK.
3. В окне авторизации (Рисунок 3) в поля «Логин», «Пароль» введите имя и пароль учетной записи администратора ПК CL DATAPK (datapk/datapk):

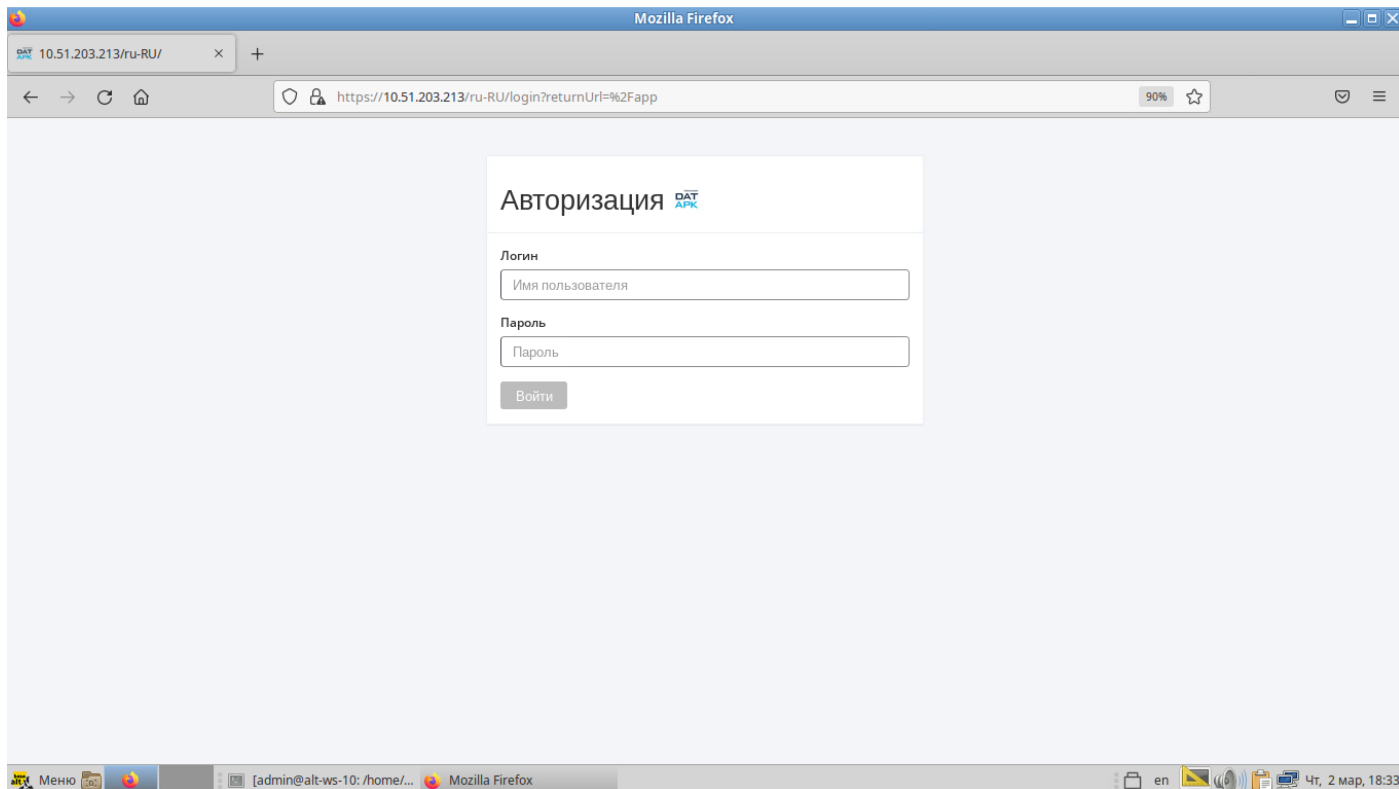


Рисунок 3 – Окно авторизации в ПК CL DATAPK

2. Пройдите по шагам первоначальной настройки комплекса:

1. примите лицензионное соглашение;
2. создайте новую учетную запись для входа в веб-интерфейс;
3. введите адрес домашней сети, в которой будет находиться ПК CL DATAPK (к примеру, это может быть подсеть, где находится интерфейс управления CL DATAPK);
4. импорт справочников пропустите и нажмите «Завершить»;
5. войдите созданной учетной записью.

3. Перейдите в подраздел управления комплексом «Основные настройки» (Рисунок 4).

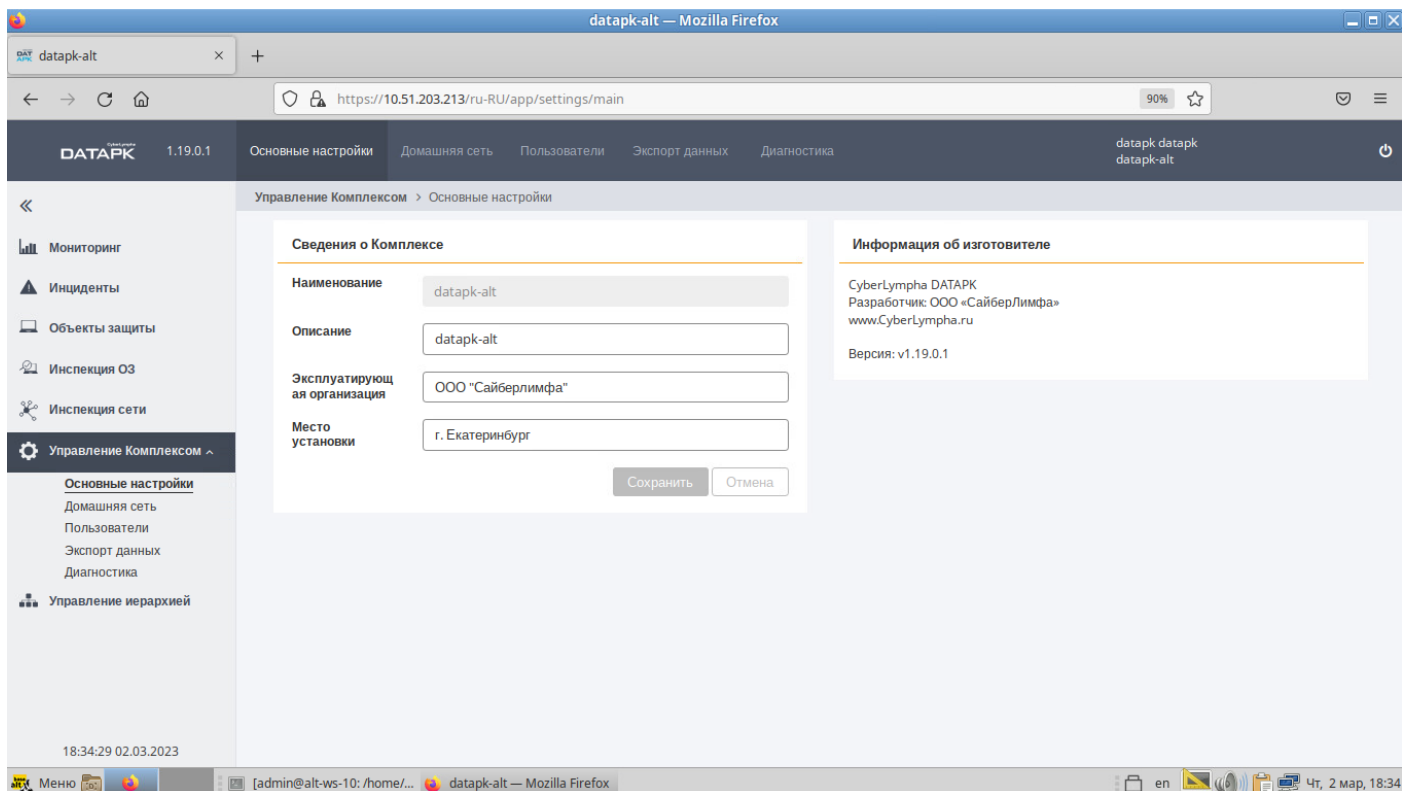


Рисунок 4 – Веб-интерфейс CL DATAPK, путь к странице «Основные настройки»

На панели «Описание DATAPK» в поле «Наименование» отображается сетевое имя (hostname) узловой машины, которое не подлежит редактированию (Рисунок 5).

4. Заполните все доступные поля области «Сведения о DATAPK» (Рисунок 5):

Сведения о Комплексе

Наименование

datapk-alt

Описание

datapk-alt

Эксплуатирующая организация

ООО "Сайберлимфа"

Место установки

г. Екатеринбург

Сохранить

Отмена

Рисунок 5 – Заполнение основных сведений о DATAPK

1. В поле «Описание» введите описание данного DATAPK;
2. В поле «Эксплуатирующая организация» введите название организации, на которой

будет установлен DATAPK.

3. В поле «Место установки» введите местоположение устройства.
4. Для подтверждения изменений нажмите кнопку «Сохранить».
5. Перейдите в подраздел управления «Домашняя сеть» (Рисунок 6).

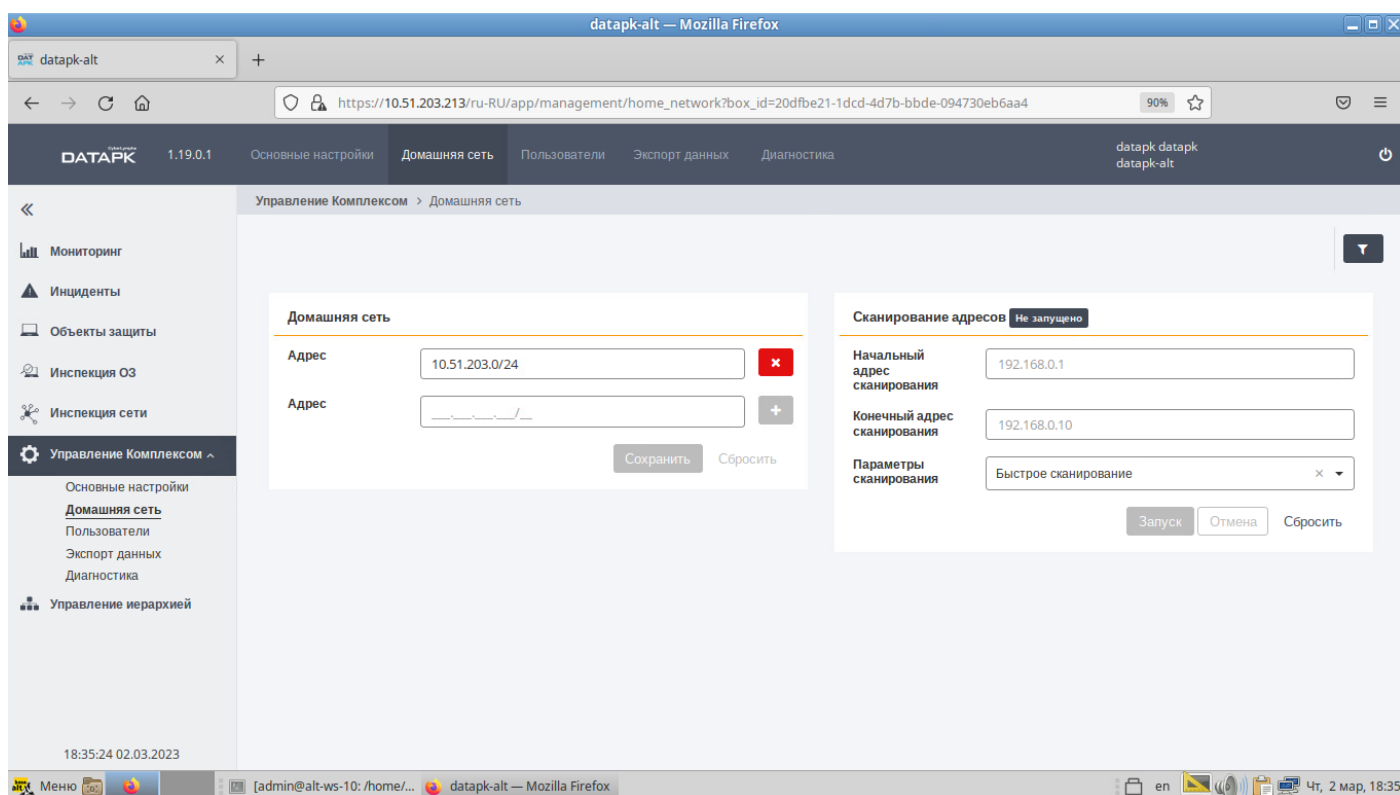


Рисунок 6 – Страница «Домашняя сеть»

6. В области «Домашняя сеть» введите IP-адрес домашней сети и маску подсети. Нажмите кнопку «Сохранить» (Рисунок 7).

Домашняя сеть

Адрес

Адрес

Рисунок 7 – Область «Домашняя сеть» на странице «Домашняя сеть» DATAPK

7. Создайте шаблон индекса. Для этого:
 1. Перейдите в веб-интерфейсе CL DATAPK в раздел мониторинга «События» (Рисунок 8). Нажмите «Создать шаблон индекса».

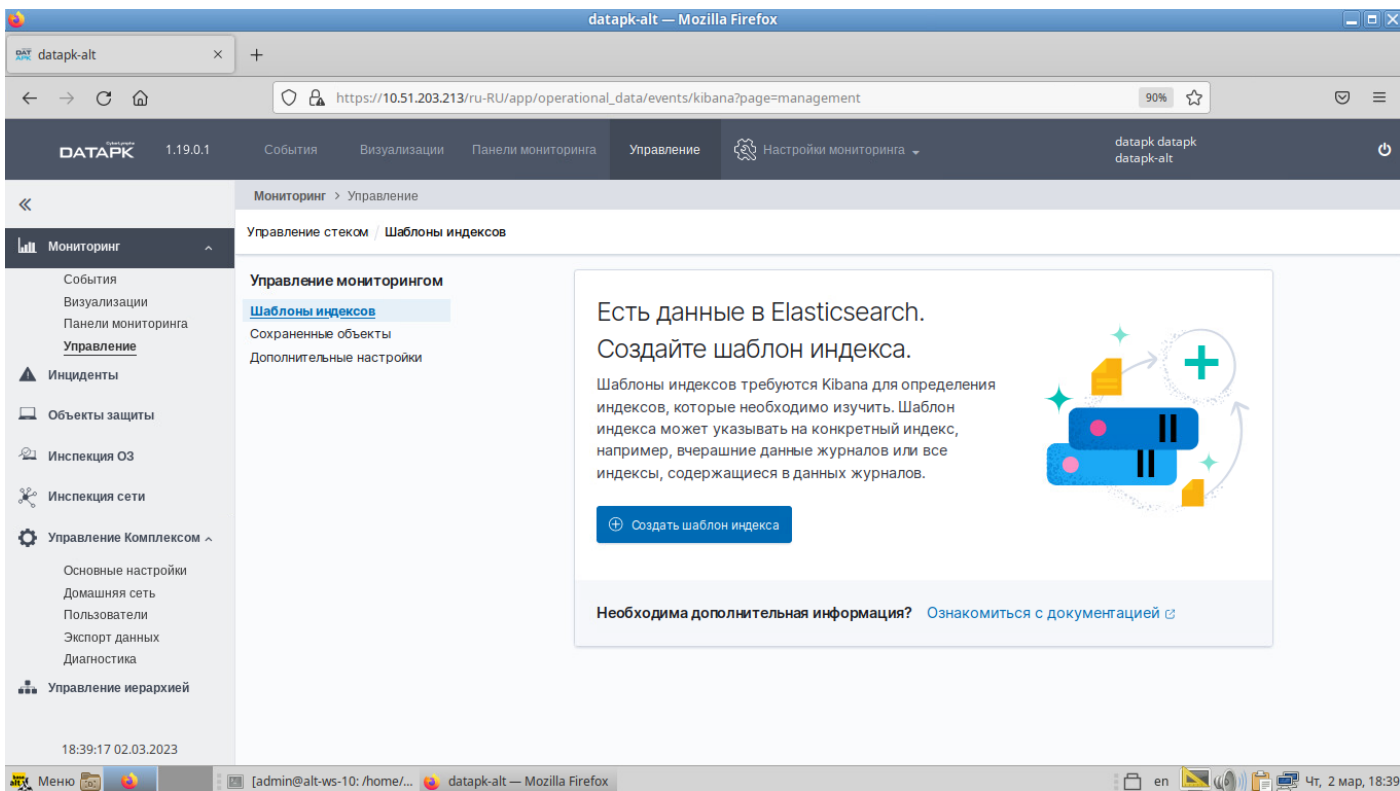


Рисунок 8 – Внешний вид интерфейса событий

- Создайте новый индекс шаблона. Для этого на странице «События» в поле «Шаблон индекса» введите название предустановленного в DATAPK шаблона «datapk-events-*» и нажмите кнопку «Далее» (Рисунок 9).

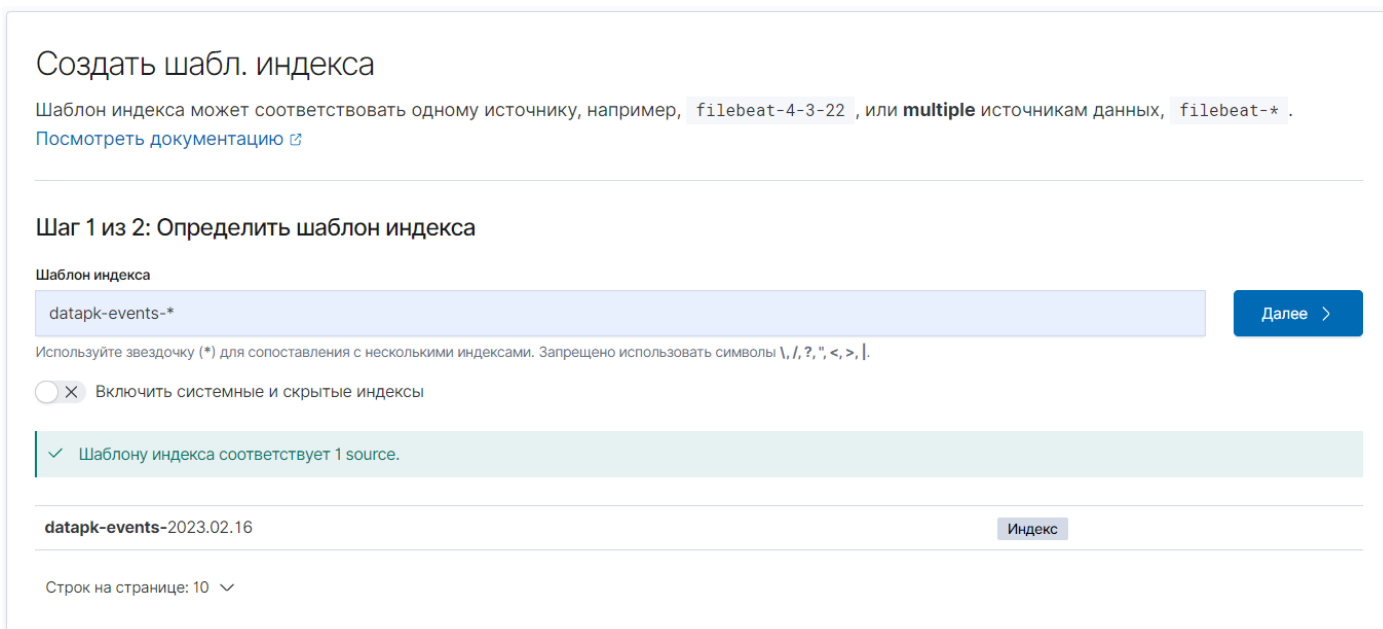


Рисунок 9 – Окно создания нового шаблона нормализации событий

- На следующем шаге выберите фильтр времени для событий (Рисунок 10). Для этого в поле «Поле времени» выберите из списка поле фильтра времени «create_time» (время создания события).

Создать шабл. индекса

Шаблон индекса может соответствовать одному источнику, например, `filebeat-4-3-22`, или **multiple** источникам данных, `filebeat-*`.
[Посмотреть документацию](#)

Шаг 2 из 2: Настройка параметров

Укажите параметры для `datapk-events-*` шаблона индекса.

Выберите основное поле для применения с глобальным фильтром времени.

Поле времени Обновить

create_time ▼

[Показать дополнительные настройки](#)

[Назад](#)

[Создать шаблон индекса](#)

Рисунок 10 – Окно настройки атрибута временного фильтра в интерфейсе визуализации

4. Нажмите кнопку «Создать шаблон индекса».

5. Обновите страницу «События» (Рисунок 11) и убедитесь, что в список полей «Доступные поля» были загружены поля из предустановленного шаблона.

The screenshot shows the DataPARK interface with the 'Events' page selected. The top navigation bar includes 'События', 'Визуализации', 'Панели мониторинга', 'Управление', and 'Настройки мониторинга'. The main content area displays a search bar with 'datapk-events-*' and a filter dropdown set to 'create_time'. Below the search bar is a bar chart showing event counts over time, with a peak around 12:27:00. The chart is titled '138 hits' and shows data for 'Feb 16, 2023 @ 12:18:55.877 - Feb 16, 2023 @ 12:33:55.877'. Below the chart is a table of events with columns for 'Time' and '_source'. The table contains several rows of event data, including fields like 'severity', 'target_port', '@version', 'target_mac', 'host_id', 'additional_information', 'protocol', '@timestamp', 'receive_time', 'hostname', 'datapk_alt user', 'datapk_event_id', 'request_id', 'description', 'post method for kibana', 'target_ip', 'justification', 'source', 'datapk_sensor', 'source_port', 'category', 'tags', 'MN', 'source_ip', 'source_id', 'action', 'POST', 'target_id', 'source_mac', 'target_hostname', and 'type'.

Рисунок 11 – Страница «События» интерфейса визуализации

8. Импортируйте панели мониторинга в CL DATAPK. Для этого:

1. Откройте подраздел мониторинга «Управление», затем выберите «Управление» → «Сохраненные Объекты» (Рисунок 12).

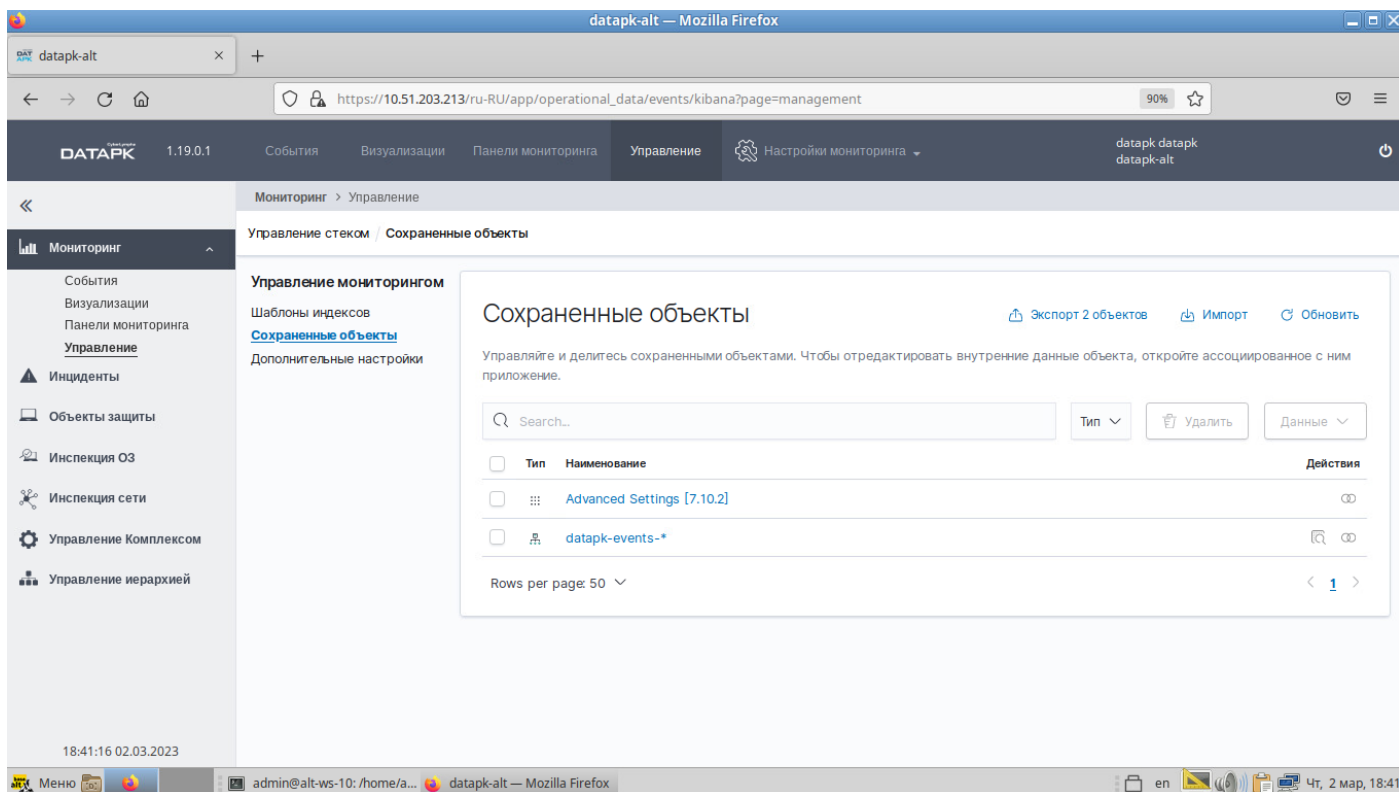


Рисунок 12 – Страница «Сохраненные объекты»

2. В верхней части страницы нажмите кнопку «Импорт».
Результат шага: появится окно импорта сохраненных объектов.
3. В открывшемся окне перетащите или выберите по нажатию на «Импорт» файл формата «*.ndjson» с объектами интерфейса визуализации (Рисунок 13).

Выберите файл для импорта

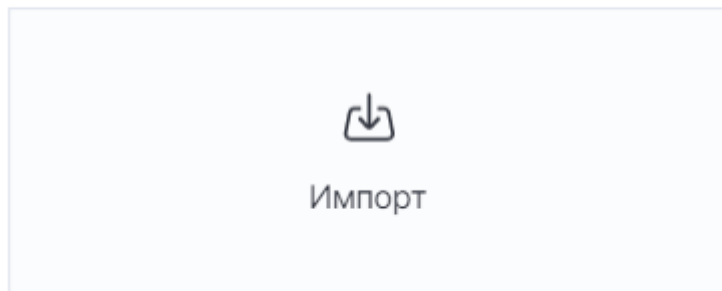


Рисунок 13 – Область выбора файла для импорта

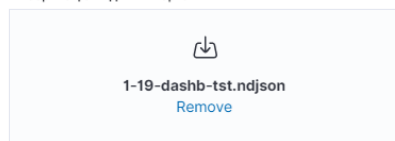


Оставьте включенным переключатель «Автоматически перезаписать все конфликты».

4. Нажмите «Импорт» (Рисунок 14).

Импортировать сохраненные объекты

Выберите файл для импорта



Опции импорта

Проверить, существуют ли объекты ⓘ

Автоматически перезаписывать конфликты

Действие при конфликте

Создавайте новые объекты со случайными ID ⓘ



Рисунок 14 – Окно импорта сохраненных объектов

5. При появлении окна «Конфликты паттерна индексирования» в столбце «Новый паттерн индексирования» в выпадающем списке выберите «datapk-events-*» и нажмите «Подтвердить все изменения» и нажать «Готово» (Рисунок 15).

Импортировать сохраненные объекты

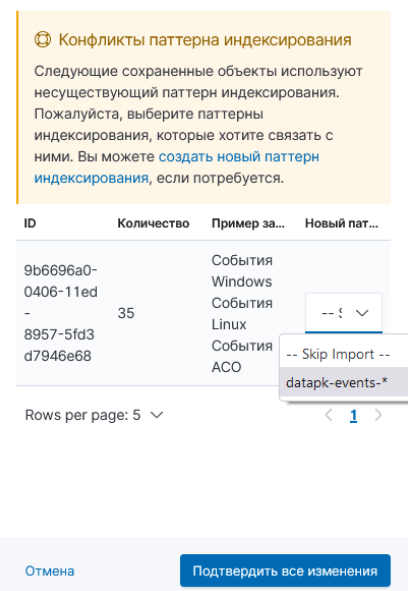


Рисунок 15 – Окно конфликтов паттерна индексирования

9. Загрузите прочий контент (политика корреляции, правила обнаружения вторжений, группы сканеров, группы OVAL-определений и пр.), выполните иные настройки в соответствии с документацией на CL DATAPK.

7. Завершение работы

Перед перезагрузкой или выключением комплекса на сервере, используйте для остановки всех сервисов ПК CL DATAPK команду:

```
$ su - -c 'cd /opt/datapk && docker-compose down'
```



Данная операция может занять до 5-7 минут.