Руководство пользователя

Централизованная система управления и мониторинга межсетевыми экранами «Аргос FW»

Версия 2.1.0

Обновлено: 26 мая 2026

СОДЕРЖАНИЕ

О ПРИЛОЖЕНИИ

Централизованная система управления и мониторинга межсетевыми экранами «Аргос FW» (далее - ЦСУМ МЭ «Аргос FW», или ЦСУМ) является инструментом, разработанным компанией ООО «ТехАргос», и предназначена для выполнения следующих функций:

- управление пользователями и их правами доступа к МЭ «Аргос FW»;
- управление контекстами и их настройками хранения данных МЭ «Аргос FW»;
- сбор и хранения метрик и логов безопасности контекстов с разграничением доступа по контекстам МЭ «Аргос FW»;
- графический вывод аналитики данных по собранным метрикам и логам с разграничением доступа по контекстам МЭ «Аргос FW»;
- просмотр информации о подключенных устройствах МЭ «Аргос FW» и их конфигурации;
- поиск L3/L4 сессии на одном из подключенных устройств МЭ «Аргос FW»;
- доступ к CLI системы управления устройствами МЭ «Аргос FW».

1. Архитектура ЦСУМ МЭ «Аргос FW»

ЦСУМ реализован набором микросервисов, оркестрируемых Docker Compose на отдельном сервере.

Список микросервисов и описание их функциональности приведено в таблице ниже.

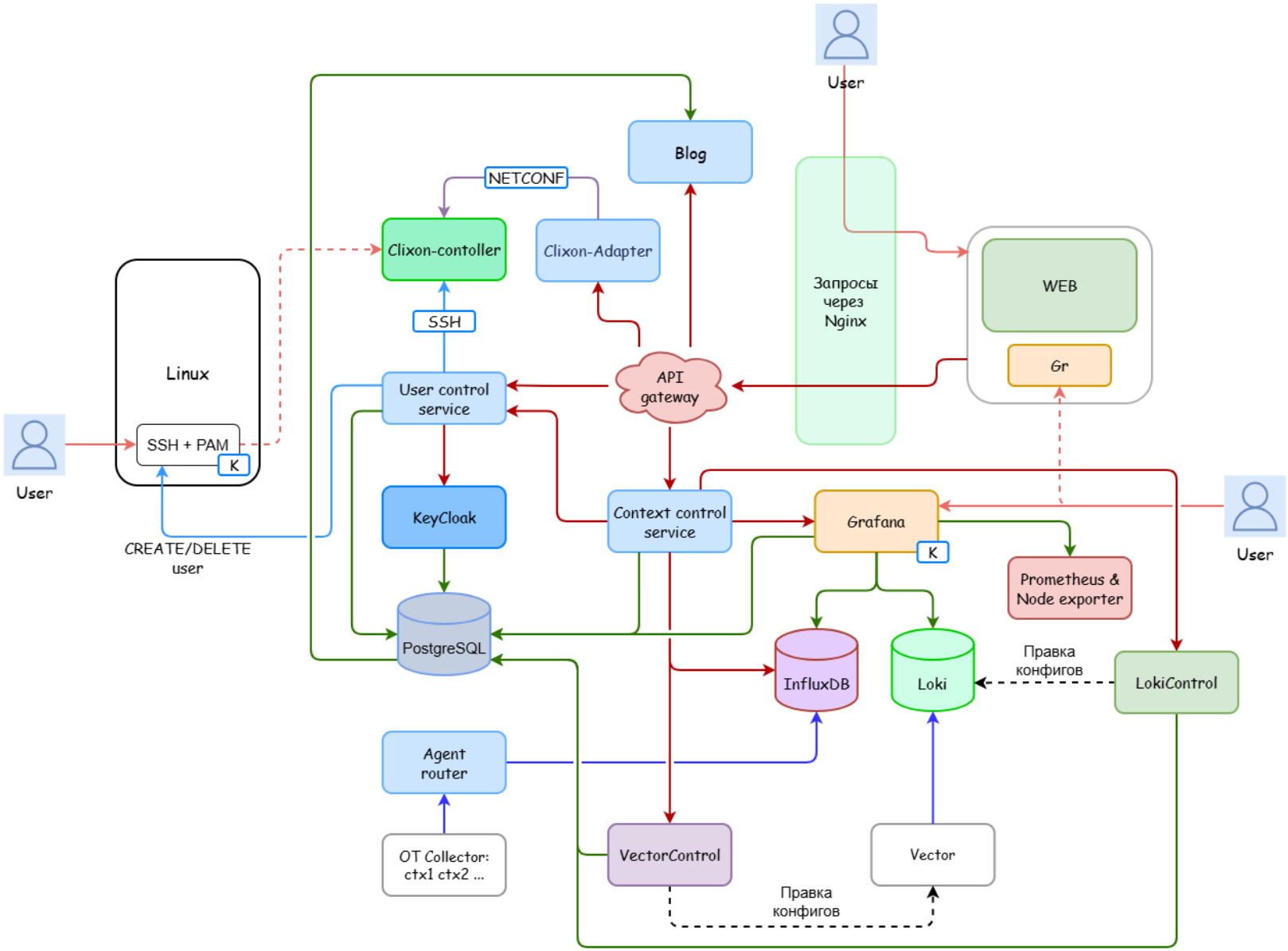
Микросервис	**Описание**
Agent Router	Маршрутизация OpenTelemetry (OT) данных от межсетевых экранов «Аргос FW» в отдельные bucket'ы базы данных InfluxDB, для каждого контекста свой bucket. Маршрутизация метрик от межсетевых экранов, на рисунке они показаны как OT Collector, основана на контексте сообщений от межсетевых экранов. Маршруты создаются автоматически после создания контекстов в ЦСУМ.
API Gateway	Внутренний шлюз для управления запросами к REST API сервисам компонент. Обеспечивает маршрутизацию и безопасность API-запросов между различными компонентами системы, включая Web, User Control, Context Control и Blog.
Blog	Сервис для управления бизнес-логами, логами действий пользователей в системе, с возможностью поиска, фильтрации и пагинации.
Clixon-controller	Централизованный CLI-интерфейс на базе Clixon. Менеджер конфигурации на основе YANG с интерактивным интерфейсом командной строки, а также интерфейсом RESTCONF для автоматизации внесения изменений в конфигурации подключенных межсетевых экранов «Аргос FW».
Clixon-Adapter	Микросервис в составе ЦСУМ, предназначен для получения информации о состоянии подключенных устройств по Netconf over SSH протоколу, их конфигураций, а также вызова разнообразных RPC-запросов, к примеру, вывода текущего состояния сессий и т.д.
Context Control Service	Управляет созданием, удалением и изменением контекстов. Реализует REST API управление подсистемами Grafana, InfluxDB, Elasticsearch, UserControl и Agent Router. Основная задача — создание необходимых для контекста ресурсов и ролей в ЦСУМ.
Grafana	Платформа для визуализации данных. Позволяет создавать и настраивать дашборды, обеспечивая наглядное представление данных производительности и других ключевых метрик.
InfluxDB	База данных для хранения временных рядов OpenTelemetry метрик, получаемых от межсетевых экранов.
KeyCloak	Система идентификации и управления доступом (Identity Provider). Обеспечивает единую точку входа, аутентификации и авторизации (SSO).
Loki	Используется для хранения и поиска данных о событиях информационной безопасности.
LokiControl	Сервис на Golang для управления конфигурациями Loki при создании/ удалении контекста.
PAM	Модуль аутентификации и авторизации SSH. Устанавливается на хост Linux машину и интегрируется с KeyCloak для разграничения доступа к CLI-контроллеру.
Prometheus&Node Exporter	Система сбора и хранения метрик ЦСУМ

PostgreSQL	СУБД для хранения конфигурации ЦСУМ и состояний отдельных сервисов. Также хранит информацию из Grafana и KeyCloak, включая данные и их текущую конфигурацию.
User Control Service	Управляет пользователями и ролями через интеграцию с Keycloak. Отвечает за автоматизацию создания и управления пользователями в Clixon-controller и обеспечивает взаимодействие с Identity Provider'ом (KeyCloak).
Vector	Агент сбора Syslog CEF логов и событий информационной безопасности. Принимает данные с межсетевых экранов, выполняет их предварительную обработку и передает на хранение в Loki.
VectorControl	Управление конфигурациями Vector при создании/удалении контекста.

Логическая архитектура ЦСУМ, набор компонент и их взаимодействие, отражены на рисунке 1. В таблице ниже указана цветовая маркировка стрелок и других элементов, применяемая на рисунке.

Элемент	**Цвет и маркировка**	**Обозначение**
	Красный сплошной	Взаимодействие посредством REST API
	Розовый сплошной	Взаимодействие пользователя с ЦСУМ
	Голубой сплошной	Взаимодействие посредством протокола NETCONF
	Синий сплошной	Получение в ЦСУМ внешних метрик и логов
	Зеленый сплошной	Обращение к реляционным (SQL) и нереляционным (Time Series и Log Databases) БД
	Черный пунктирный	Взаимодействие путем правки конфигурационного файла сервиса
	Буква "К" в голубом квадрате	Авторизация с использованием SSO KeyCloak

Рис. 1 – Логическая структура ЦСУМ МЭ «Аргос FW»



Пользовательский интерфейс, доступный пользователю, состоит из трех взаимно-дополняющих компонентов:

Пользовательский интерфейс	**Раздел**	**Описание**
WEB-интерфейс ЦСУМ	Авторизация	Веб-интерфейс для аутентификации пользователей в системе. Использует интеграцию с KeyCloak для обеспечения SSO. После успешной аутентификации пользователь перенаправляется на главную страницу.
	Dashboard	Главная веб-страница, которая предоставляет пользователю доступ к основным сервисам системы, таким как мониторинг производительности и логов (редирект на Web-страницу Grafana), управление пользователями, контекстами, устройствами, профилем и поиску активных L3/4 сессий.
	Управление пользователями	Веб-страница управления пользователями. Позволяет искать, создавать, редактировать пользователей и назначать им роли. Системный администратор управляет всеми пользователями, контекстный администратор — в рамках своего контекста. Остальным ролям эта страница недоступна.
	Управление контекстами	Веб-страница управления контекстами. Позволяет создавать, редактировать и удалять контексты. Доступна только Системному администратору.
	Управление устройствами	Веб-страница управления устройствами. Позволяет управлять подключением устройства, просматривать и обновлять конфигурацию с устройства, переходить в WEB-интерфейс устройства.
	Поиск сессий	Веб-страница поиска активных L3/4 сессий. Позволяет производить поиск сессий по заданным фильтрам и просматривать информацию о сессии.
	Управление профилем	Веб-страница управления профилем пользователя.
WEB-интерфейс Grafana	CEF Syslog	Сбор, фильтрация и анализ CEF Syslog событий информационной безопасности.
	Open Telemetry Metrics	Мониторинг производительности, графики и табличные значения счетчиков
CLI-интерфейс Clixon-контроллера	SSH-подключение	CLI-интерфейс, поддерживающий одновременное применение политик безопасности, сетевых конфигураций одновременно к нескольким устройствам межсетевого экранирования в транзакционном режиме (всё или ничего)

2. Политика доступа

В ЦСУМ МЭ «Аргос FW» реализована политика разграничения доступа по ролям и контекстам.

В системе предусмотрены три роли:

- системный администратор (SA);
- контекстный администратор (CA);
- контекстный оператор (CO).

Пользователь с ролью **системного администратора (SA)** имеет полный доступ, что подразумевает права на:

- управление пользователями (создание и редактирование пользователей);
- создание и редактирование контекстов;
- настройку системы аналитики метрик и логов;
- просмотр событий ИБ и метрик (статистической информации) любого из контекстов;
- управление устройствами и переход в WEB-интерфейс устройства;
- просмотр списка активных сессий и информации о сессии;
- полный доступ в CLI-интерфейсе Clixon-контроллера ко всем подключенным устройствам за исключением раздела управления пользователям. Управление пользователями возможно только через графический интерфейс ЦСУМ МЭ «Аргос FW».

Пользователь с ролью **контекстного администратора (CA)** имеет права на:

- управление пользователями контекста;
- редактирование контекста;
- настройку системы аналитики метрик и логов в рамках своего контекста;
- просмотр событий ИБ и метрик (статистической информации) контекста;
- управление устройствами и переход в WEB-интерфейс устройства;
- просмотр списка активных сессий и информации о сессии;
- доступ на просмотр, создание и изменение настроек контекста межсетевого экранирования в CLI-интерфейсе Clixon-контроллера.

Пользователь с ролью **контекстного оператора (CO)** имеет права на:

- формирование метрик и логов;
- редактирование своего профиля;
- управление устройствами и переход в WEB-интерфейс устройства;
- просмотр списка активных сессий и информации о сессии;
- просмотр событий ИБ и метрик (статистической информации) контекста;
- просмотр настроек контекста межсетевого экранирования в CLI-интерфейсе Clixon-контроллера.

Таким образом, разграничение прав доступа по контекстам подразумевает под собой, что настройки системы аналитики метрик и логов определенного контекста будут доступны пользователям с ролями системного администратора (SA) и администратора контекста (CA).

3. Работа с главной панелью WEB UI

3.1 Авторизация

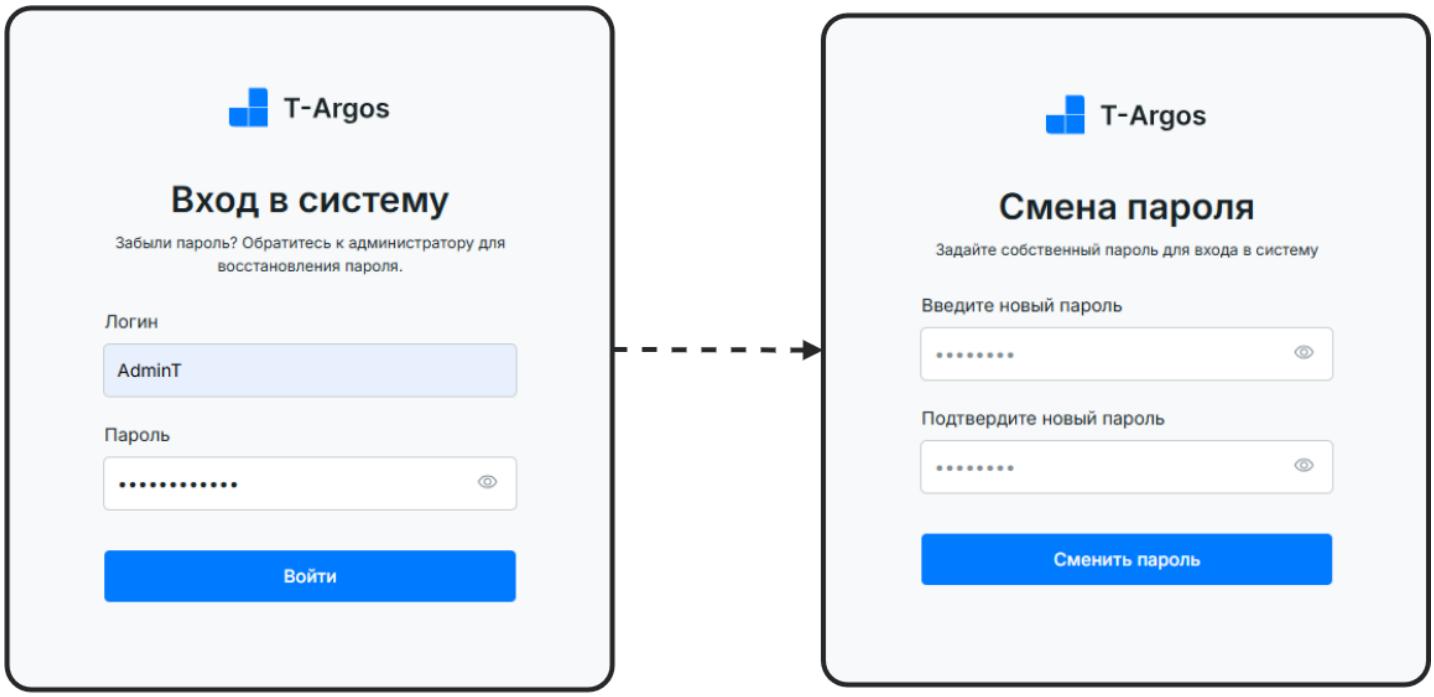
При начальном развертывании для доступа в систему через WEB-интерфейс используется пользователь с ролью системного администратора (SA). Для входа следует использовать логин/пароль: **admin/ admin**.

При первичной авторизации система потребует сменить пароль (см. рис. 2).

При переходе по адресу хоста, на котором развернут ЦСУМ, отобразится окно авторизации, в котором следует ввести логин и пароль.

При первичной авторизации вновь созданным пользователем вводится логин и пароль, выданный администратором. При этом система потребует сменить пароль на собственный, по которому будет осуществляться вход при последующих авторизациях.

Рис. 2 – Первичная авторизация пользователя



Требования к сложности пароля

Для успешной смены старого или временного пароля новый пароль должен удовлетворять следующим требованиям:

- длина пароля должна составлять не менее 8 символов;
- пароль должен содержать буквенные и числовые символы.

3.2 Главная страница

После авторизации пользователю откроется главная страница системы, на которой представлены различные функциональные возможности согласно матрице ролей.

Рис. 3 – Главная страница пользователей с ролями SA и CA

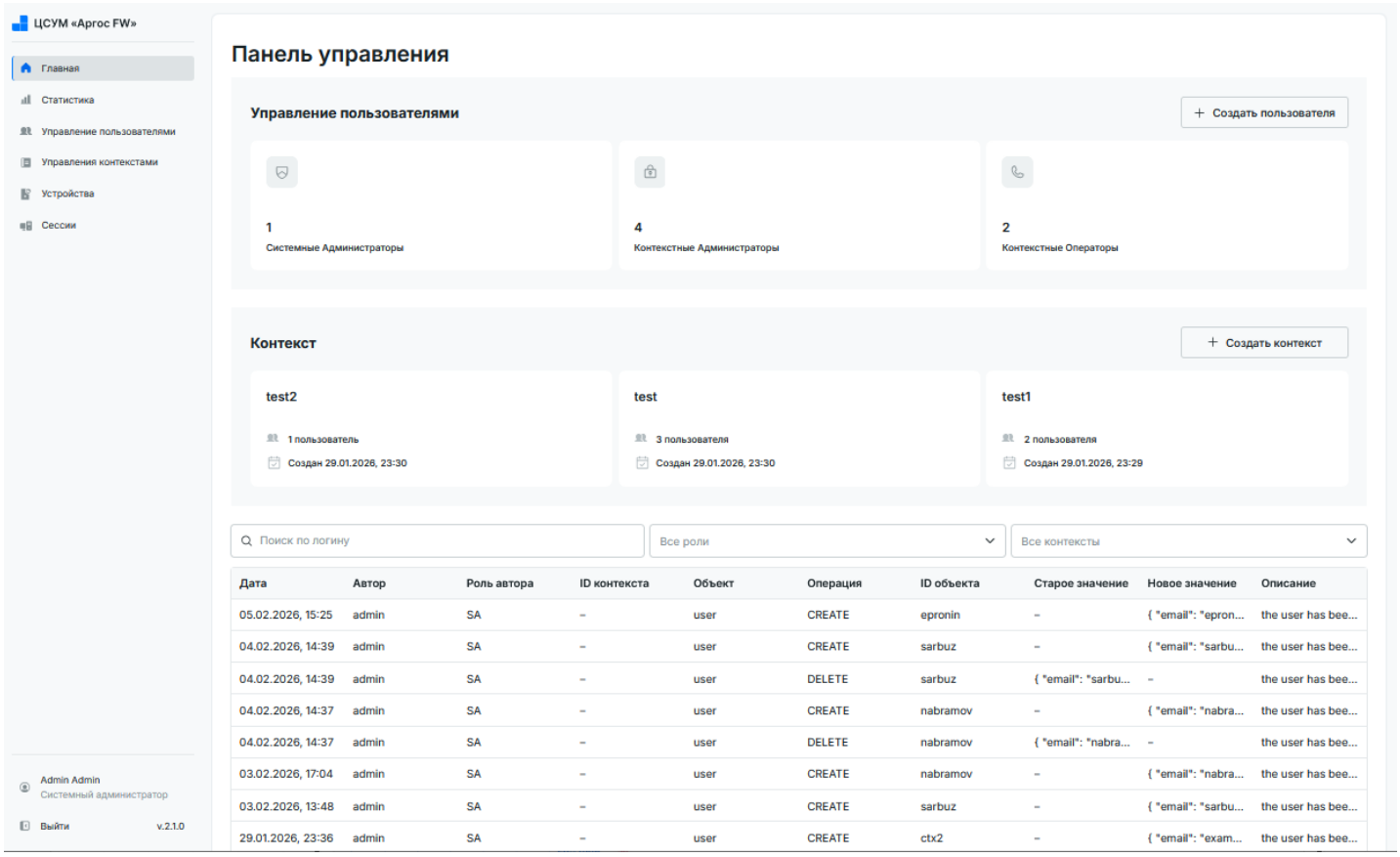
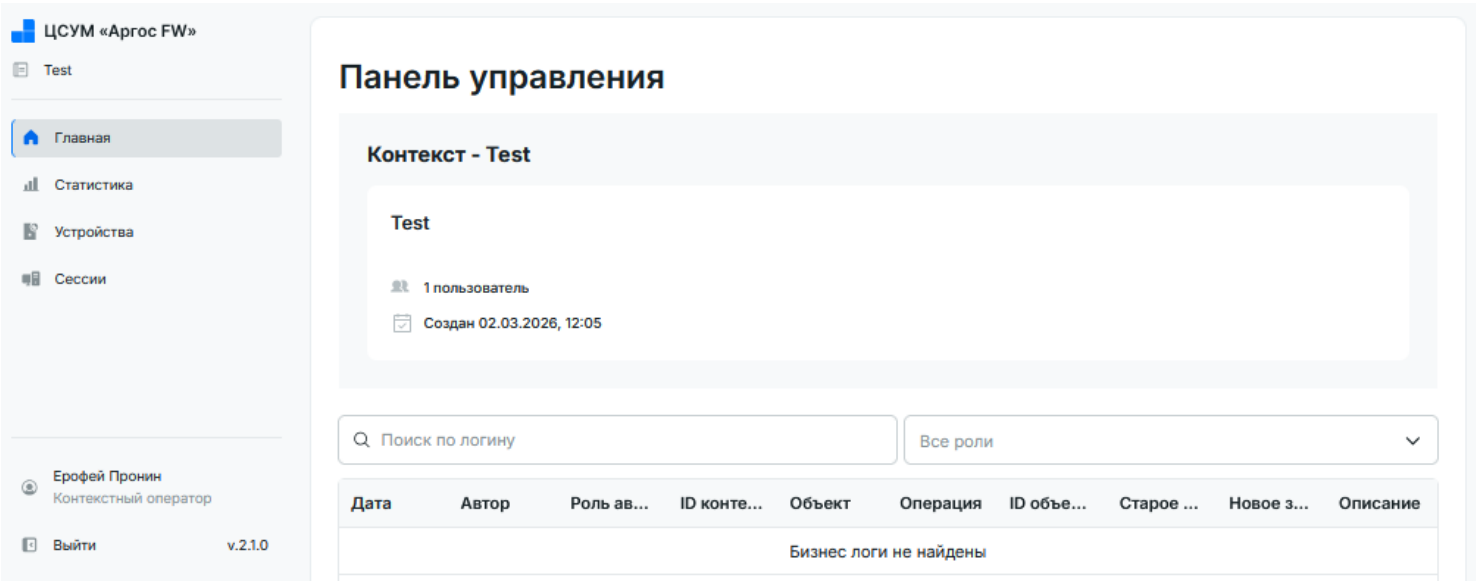


Рис. 4 – Главная страница пользователей с ролью СО



Бизнес-логи

Действия пользователей в ЦСУМ логируются и отображаются в таблице бизнес-логов, расположенной в нижней части главной страницы (см. рис. 5).

Для пользователей с ролью SA будут отображаться события всех контекстов и пользователей (пример таблицы логов для пользователя с правами системного администратора (SA) приведен на рисунке 5). Для пользователей с ролью CA будут отображаться события контекста. Для контекстного оператора будут видны только события, произошедшие в рамках его профиля.

В таблице отображаются следующие события:

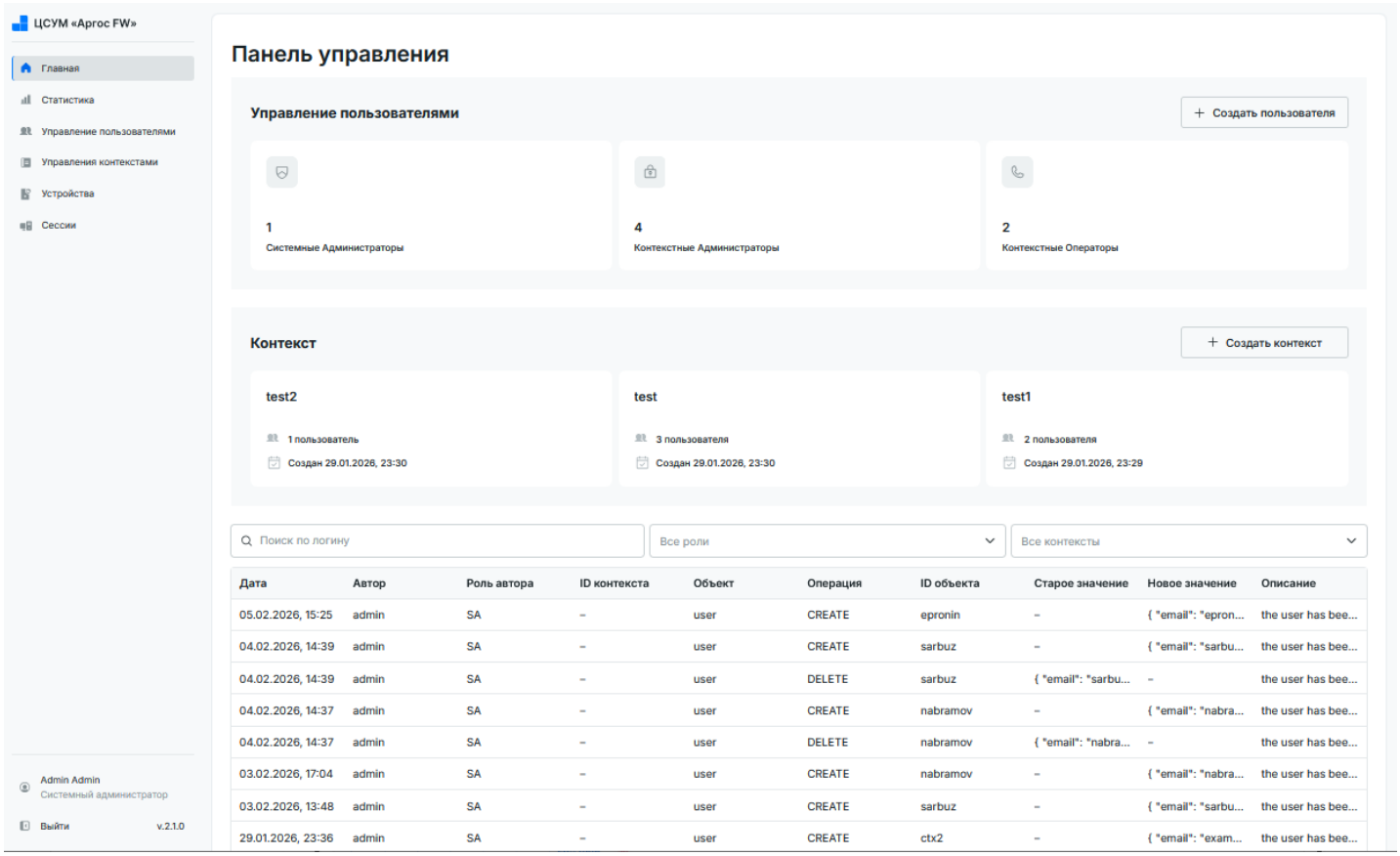
1. Управление пользователями:

- создание пользователя;
- удаление пользователя;
- обновление информации о пользователе.

2. Управление контекстами:

- создание контекста;
- удаление контекста;
- изменение конфигурации контекста.

Рис. 5 – Пример таблицы бизнес-логов для пользователя с ролью SA



Для каждого события в логе отображаются следующие поля:

- дата - дата и время события;
- автор - логин пользователя, совершившего событие;
- роль автора - роль пользователя, совершившего действие;
- ID контекста - ID контекста, в рамках которого произошло указанное событие;
- объект - пользователь или контекст, с которым произвелось действие;
- операция - наименование операции, совершенной пользователем. Возможные значения: CREATE, UPDATE, DELETE.
- ID объекта - логин пользователя или ID контекста, над которым произвелось действие;
- старое значение - информация о пользователе или конфигурация контекста до внесения изменений или удаления. В случае, если пользователя/контекст только что создали, значением данного поля будет символ прочерк «—».
- новое значение - скорректированная информация о пользователе/контексте. В случае удаления пользователя/контекста, значением данного поля будет символ прочерк «—».
- описание - текстовое описание произошедшего события.

При наведении курсора на ячейки полей «Старое значение» и «Новое значение», выводится всплывающее окно с информацией в формате json (см. рис. 6).

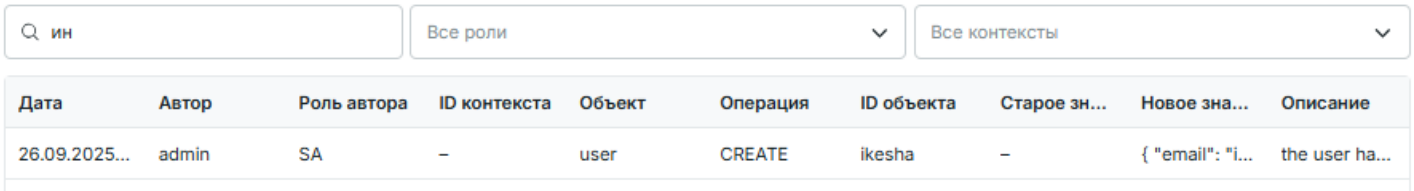
Рис. 6 – Пример значения ячейки полей «Старое значение» и «Новое значение»

```json
{
  "description": "Тестовый
контекст",
  "id": "TestC",
  "log_input_port": 9003,
  "log_input_transport": "tcp",
  "logs_retention": 7,
  "metric_retention": 7,
  "metrics_input_port": "6000",
  "name": "TestC"
}
```

В ЦСУМ предоставлена возможность фильтрации бизнес-логов по следующим параметрам:

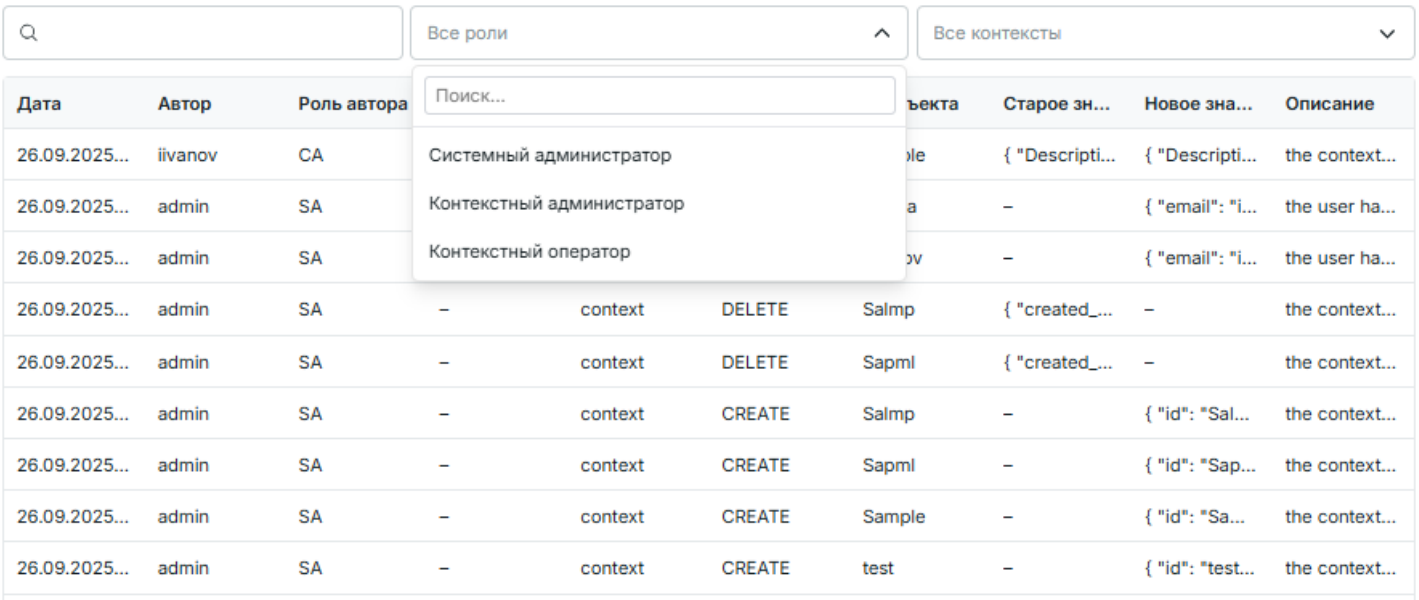
- Логин пользователя - фильтрация по логину пользователя в полях «Автор» и «ID объекта» (рис. 7).

Рис. 7 – Фильтрация по логину



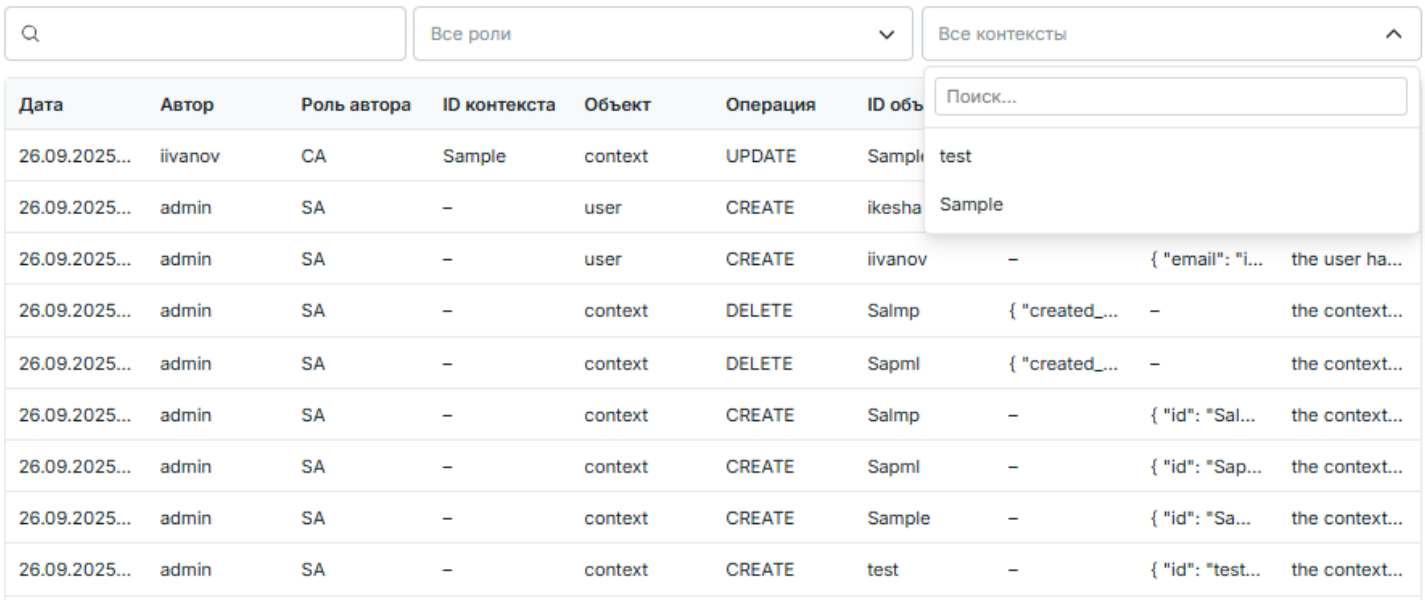
- Роли - фильтрация по ролям пользователей (рис. 8).

Рис. 8 – Фильтрация по ролям



- Контексты - фильтрация по контексту, в рамках которого произошло событие (рис. 9).

Рис. 9 – Фильтрация по контекстам



3.3 Управление контекстами

Под контекстом понимается множество изолированных друг от друга виртуальных межсетевых экранов, использующих общий ресурс физического устройства.

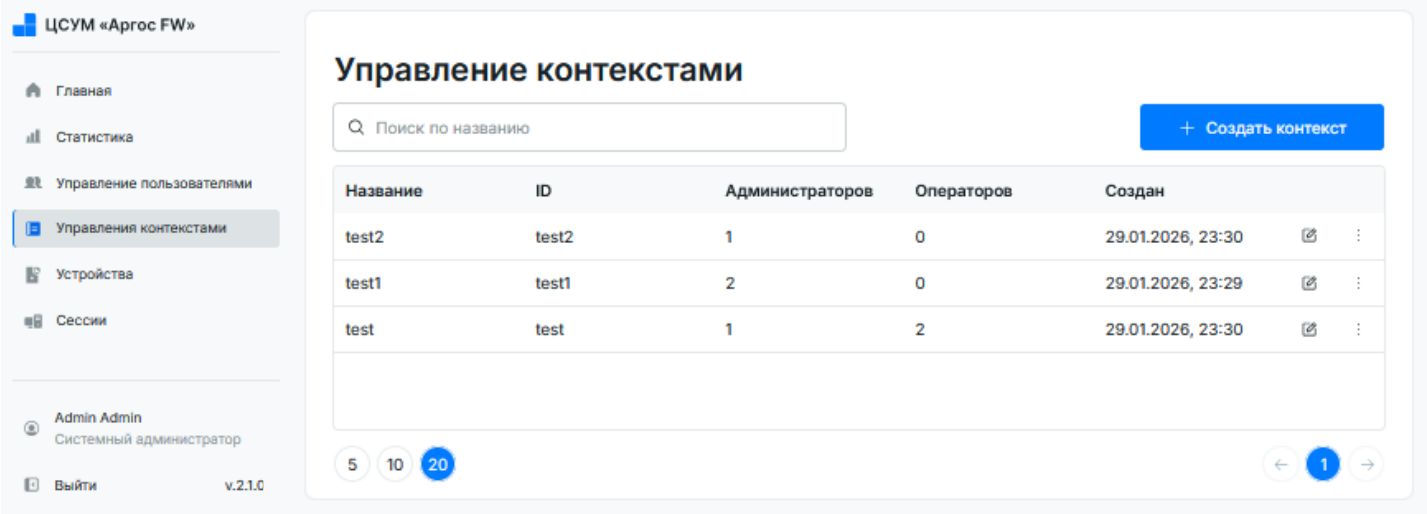
Функционал управления контекстами доступен только пользователям с правами системного администратора (SA) и контекстного администратора (CA) в рамках своего контекста.

Для перехода к управлению контекстами следует на сайдбаре выбрать вкладку «Управление контекстами». Откроется страница со списком контекстов, доступных пользователю. Для контекстного администратора (CA) будет доступно конфигурирование и просмотр только того контекста, которому он принадлежит.

Действия, доступные пользователям с ролью SA (рис. 10):

- создание контекста + Создать контекст;
- редактирование настроек контекста;
- просмотр информации о контексте (доступен при нажатии иконки ⋮, расположенной справа в строке информации о контексте);
- удаление контекста (доступно при нажатии иконки ⋮, расположенной справа в строке информации о контексте);
- поиск в списке контекстов по названию.

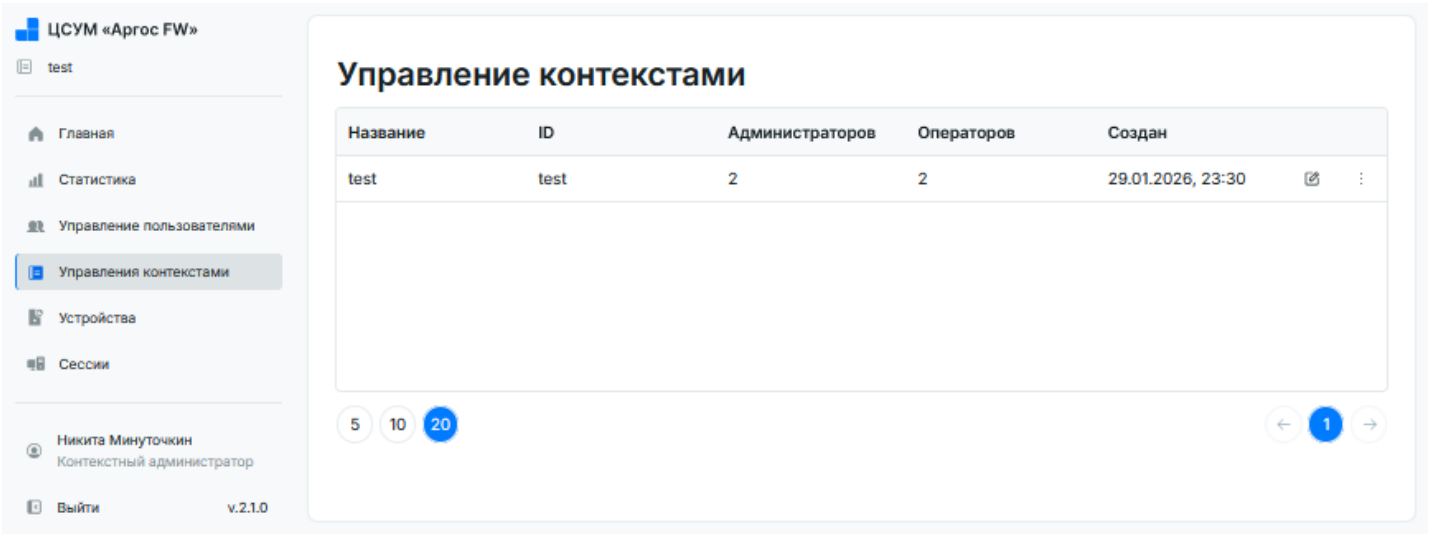
Рис. 10 – Страница управления контекстами системного администратора (SA)



Пользователям с ролью CA доступны следующие возможности работы с контекстом (рис. 11):

- редактирование настроек контекста ;
- просмотр информации о контексте (доступен при нажатии иконки , расположенной справа в строке информации о контексте).

Рис. 11 – Страница управления контекстами контекстного администратора (CA)



Создание контекста

После нажатия кнопки «Создать контекст», откроется окно создания контекста (рис. 12), в котором **на первом шаге** заполняется основная информация о контексте:

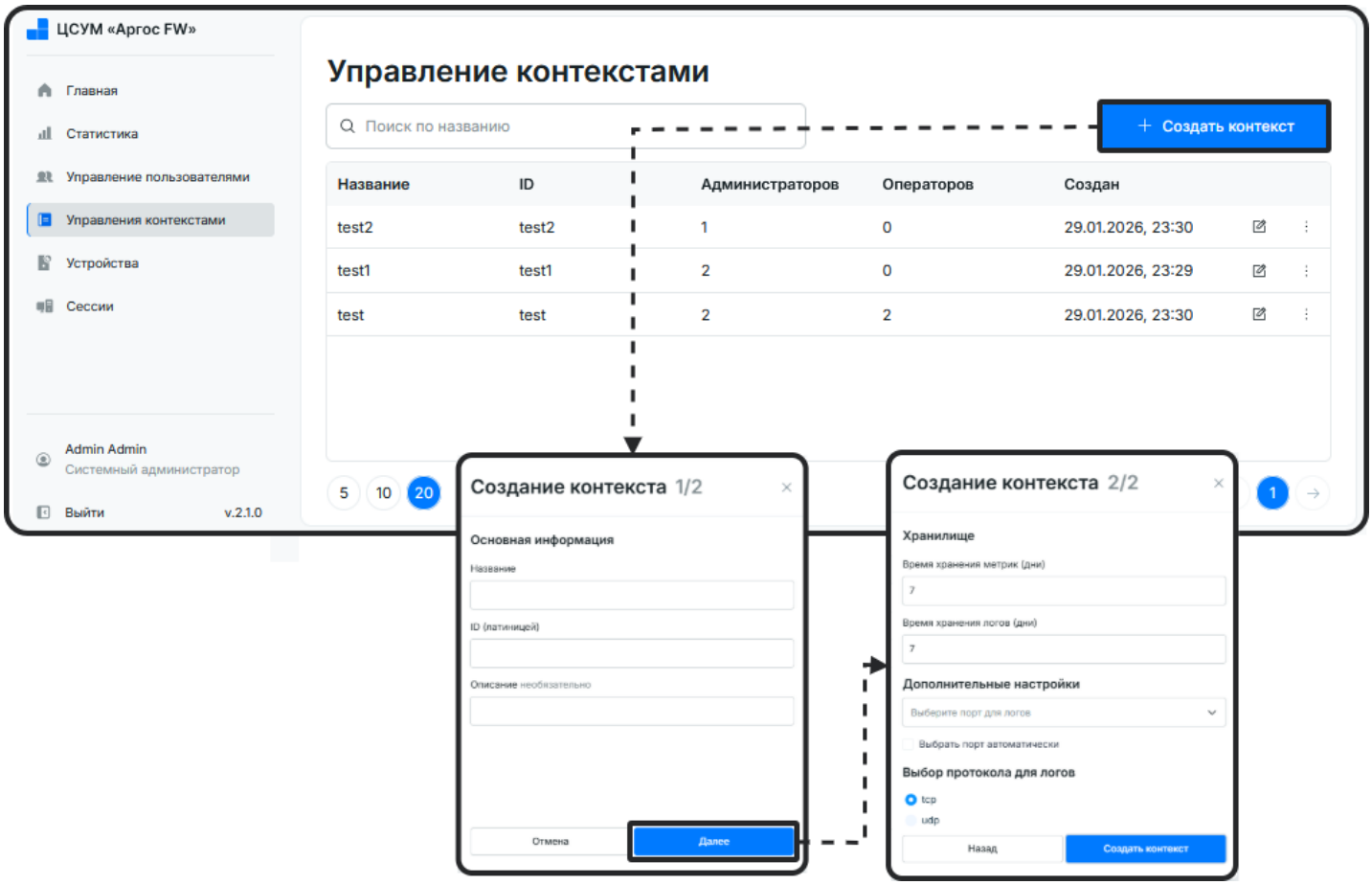
- название;
- ID;
- описание.

на втором:

- хранилище: время хранения метрик (от 1 дня), время хранения логов (от 1 дня);
- дополнительные настройки: выбор порта для логов или автоматический выбор порта;

- выбор протокола: TCP или UDP.

Рис. 12 – Создание контекста

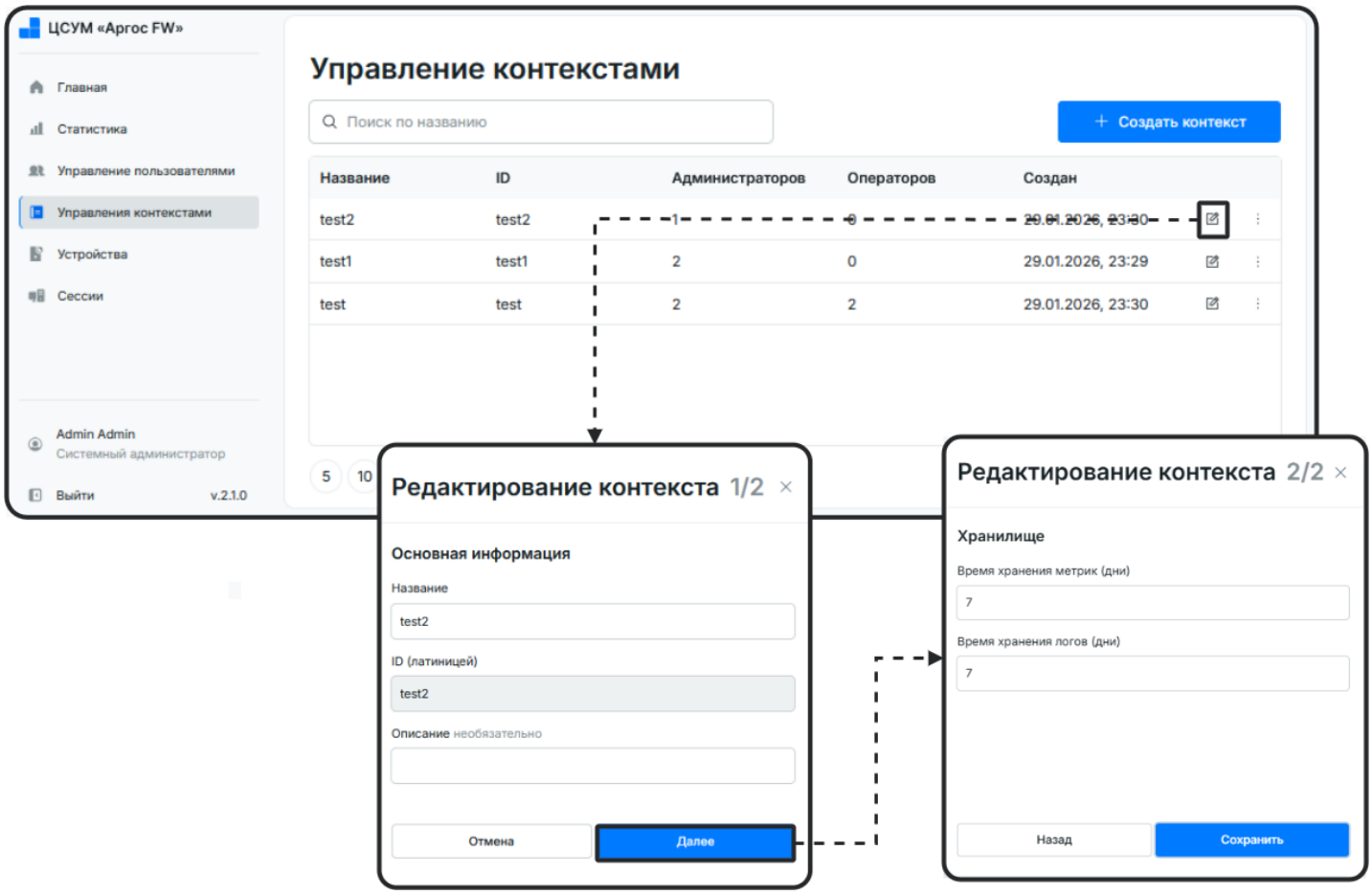


После корректного заполнения всех обязательных полей, созданный контекст отобразится в таблице контекстов.

Редактирование настроек контекста

Для редактирования настроек контекста необходимо нажать иконку  в строке нужного контекста. Откроется окно с последовательным внесением изменений в два шага (рис. 13).

Рис. 13 – Редактирование контекста



Удаление контекста и просмотр его настроек

Для просмотра информации о контексте следует нажать иконку ⋮, далее выбрать необходимое действие (рис. 15). Удаление контекста производится нажатием на иконку 🗑 (рис. 14).

Рис. 14 – Просмотр настроек контекста

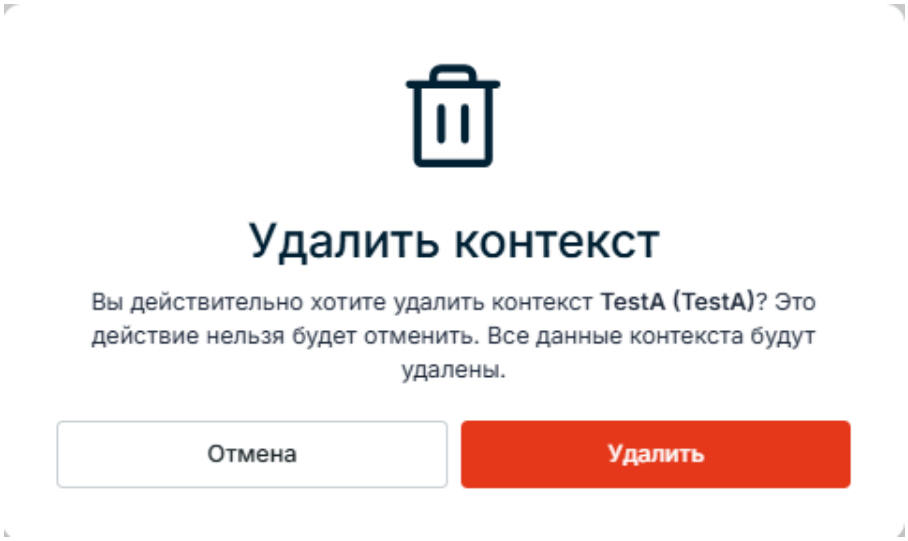
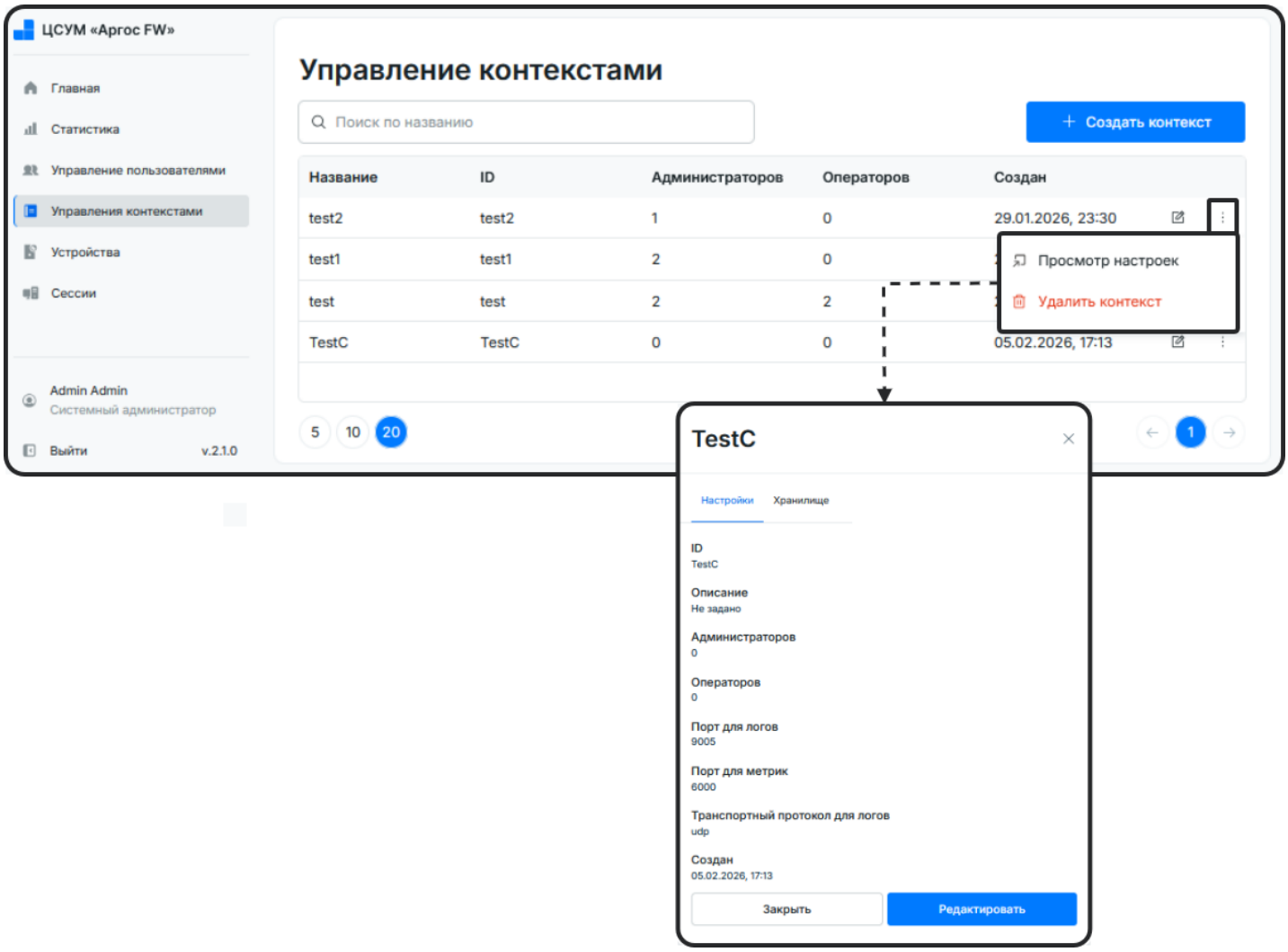


Рис. 15 – Просмотр настроек контекста

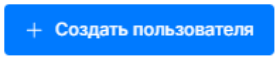


3.4 Управление пользователями

Функционал управления пользователями доступен только пользователям с правами системного администратора (SA) и контекстного администратора (CA). Для оператора контекста (CO) доступно только управление своим профилем.

Для перехода к управлению пользователями следует на сайдбаре выбрать вкладку «Управление пользователями». Откроется страница со списком пользователей, доступных к управлению. Для контекстного администратора (CA) будет доступно управление и просмотр только пользователей контекста, которому он принадлежит.

Действия, доступные пользователям с ролью SA и CA:

- создание пользователя 

;
- редактирование данных о пользователе  ;
- сброс пароля  (доступен при нажатии иконки , расположенной справа в строке информации о пользователе);

- удаление пользователя  (доступен при нажатии иконки ⋮, расположенной справа в строке информации о пользователе);
- фильтрация по ФИО, роли и контексту (для СА доступна фильтрация только по ФИО и роли пользователя).

Создание пользователя

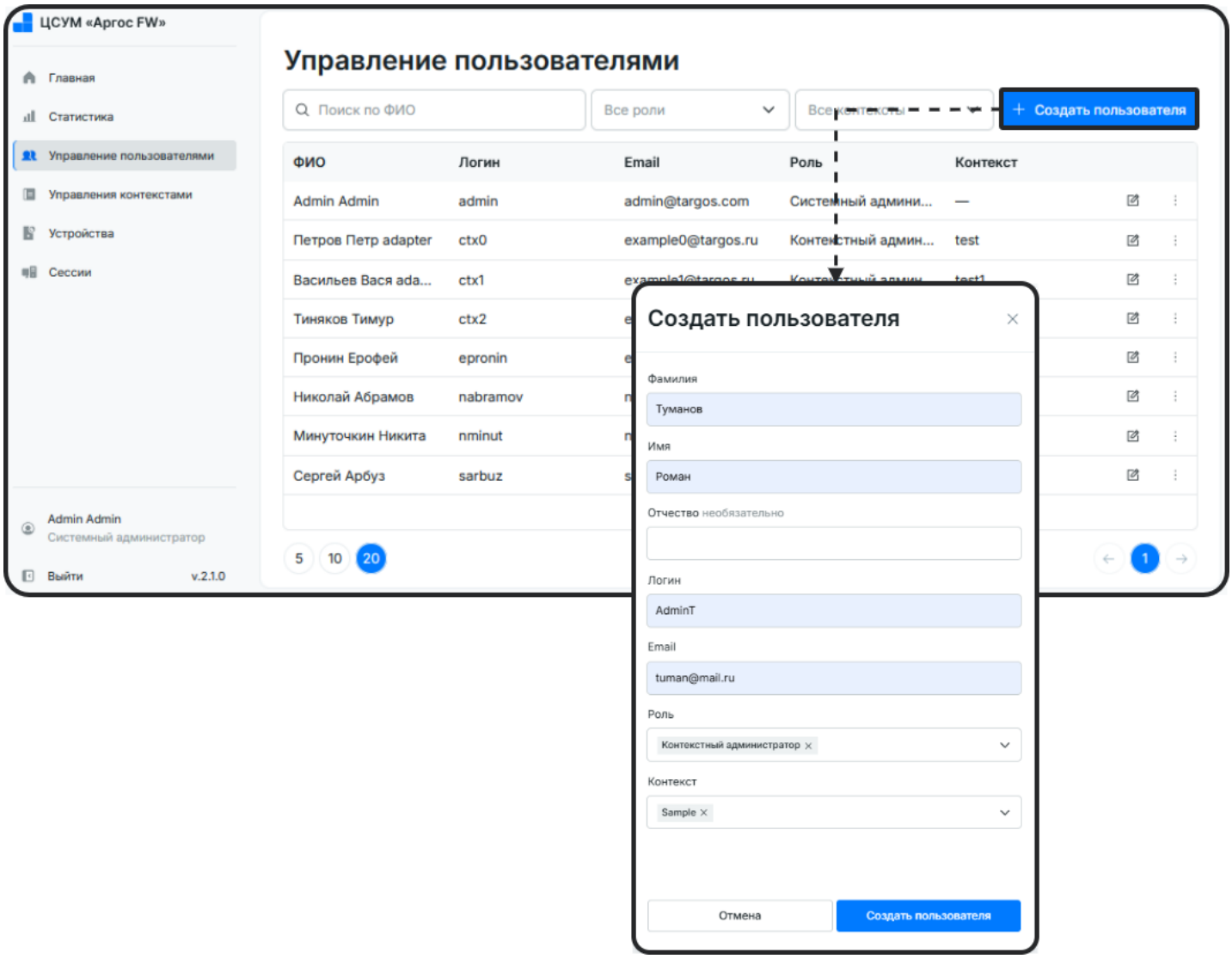
Для создания пользователя следует нажать кнопку «Создать пользователя».

Откроется окно создания пользователя (рис. 16), в котором будут присутствовать следующие поля:

- фамилия;
- имя;
- отчество;
- логин;
- Email;
- роль;
- контекст (поле отображается только в том случае, если выбрана роль СА или СО).

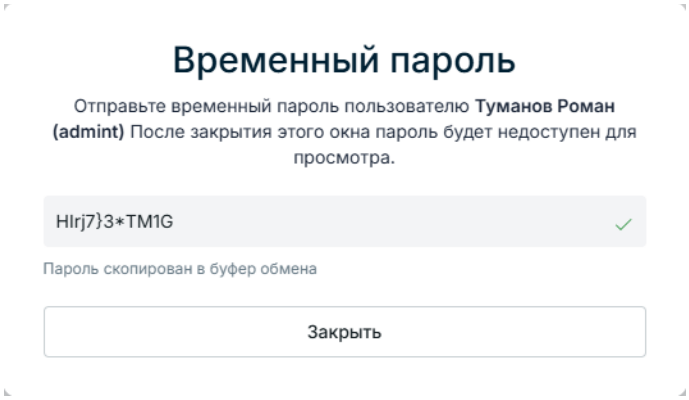
В случае если пользователя создает **контекстный администратор (СА)**, то в поле «Контекст» будет автоматически проставляться контекст, которому принадлежит сам контекстный администратор.

Рис. 16 – Создание пользователя



После подтверждения создания пользователя, откроется окно с временным паролем (рис. 17), который необходимо передать каким-либо внешним образом владельцу аккаунта для его первого входа в систему.

Рис. 17 – Окно временного пароля

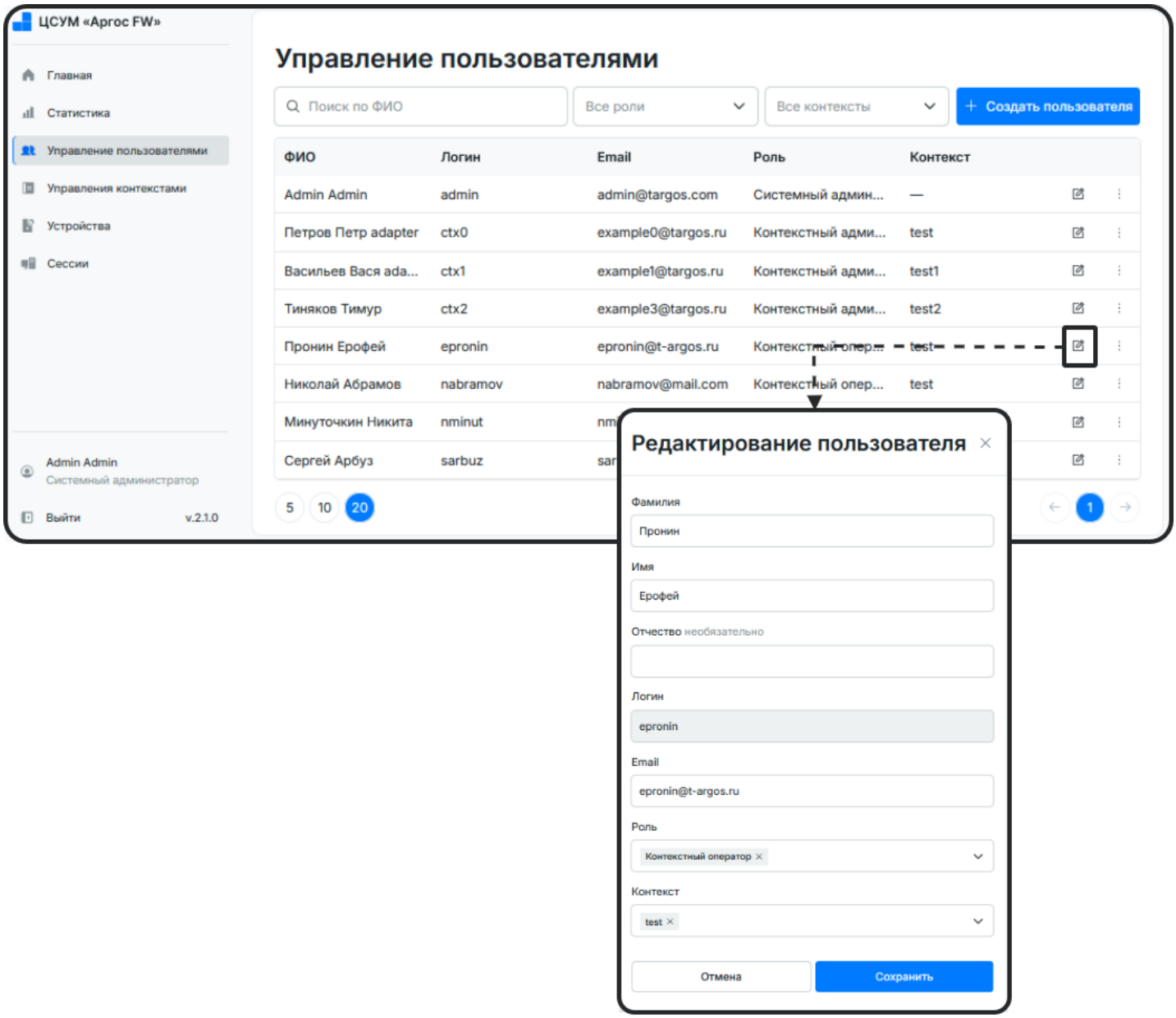


Редактирование данных о пользователе

Для редактирования данных о пользователе следует нажать иконку в строке таблицы пользователей.

Откроется окно редактирования (рис. 18).

Рис. 18 – Редактирование пользователя

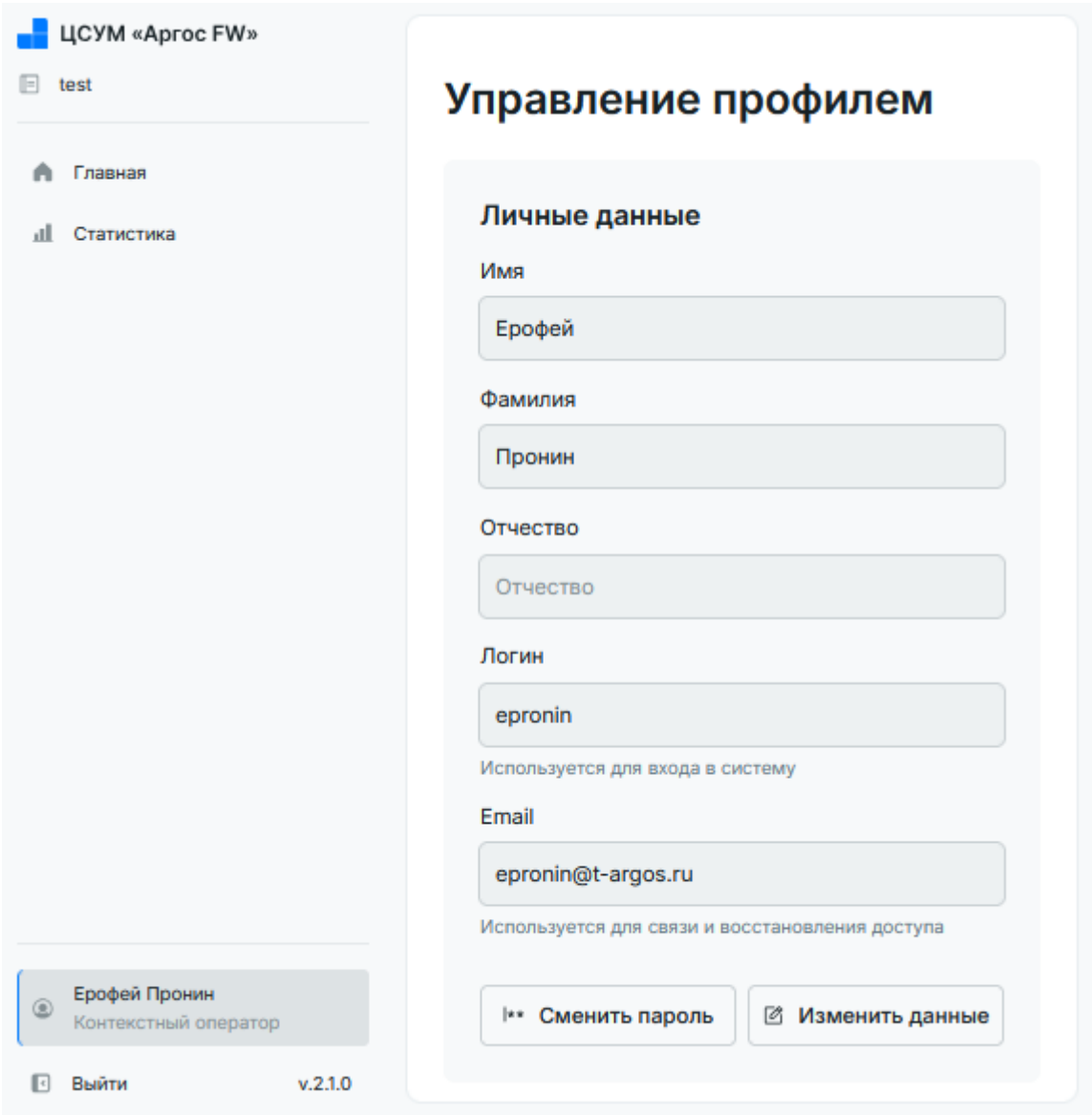


Управление профилем

Так же отредактировать собственные данные можно через управление профилем.

При нажатии на имя в левом нижнем углу WEB-страницы, откроется страница управления профилем (рис. 19).

Рис. 19 – Управление профилем



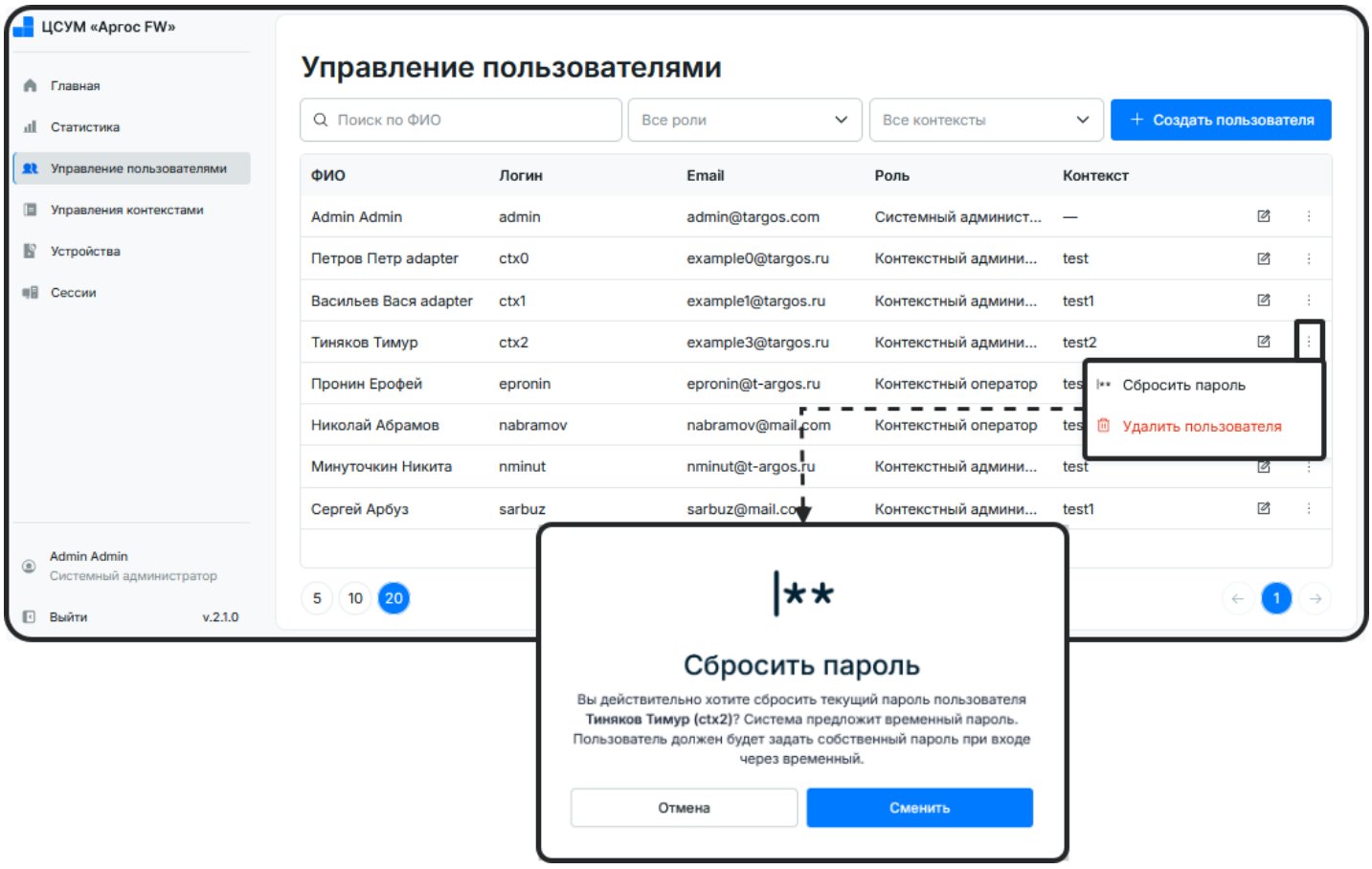
На данной странице пользователю предоставляется возможность сменить пароль Сменить пароль и изменить личные данные Изменить данные.

Сброс пароля и удаление пользователя

Сброс пароля и удаление пользователя доступны при нажатии иконки ⋮ (рис. 20) .

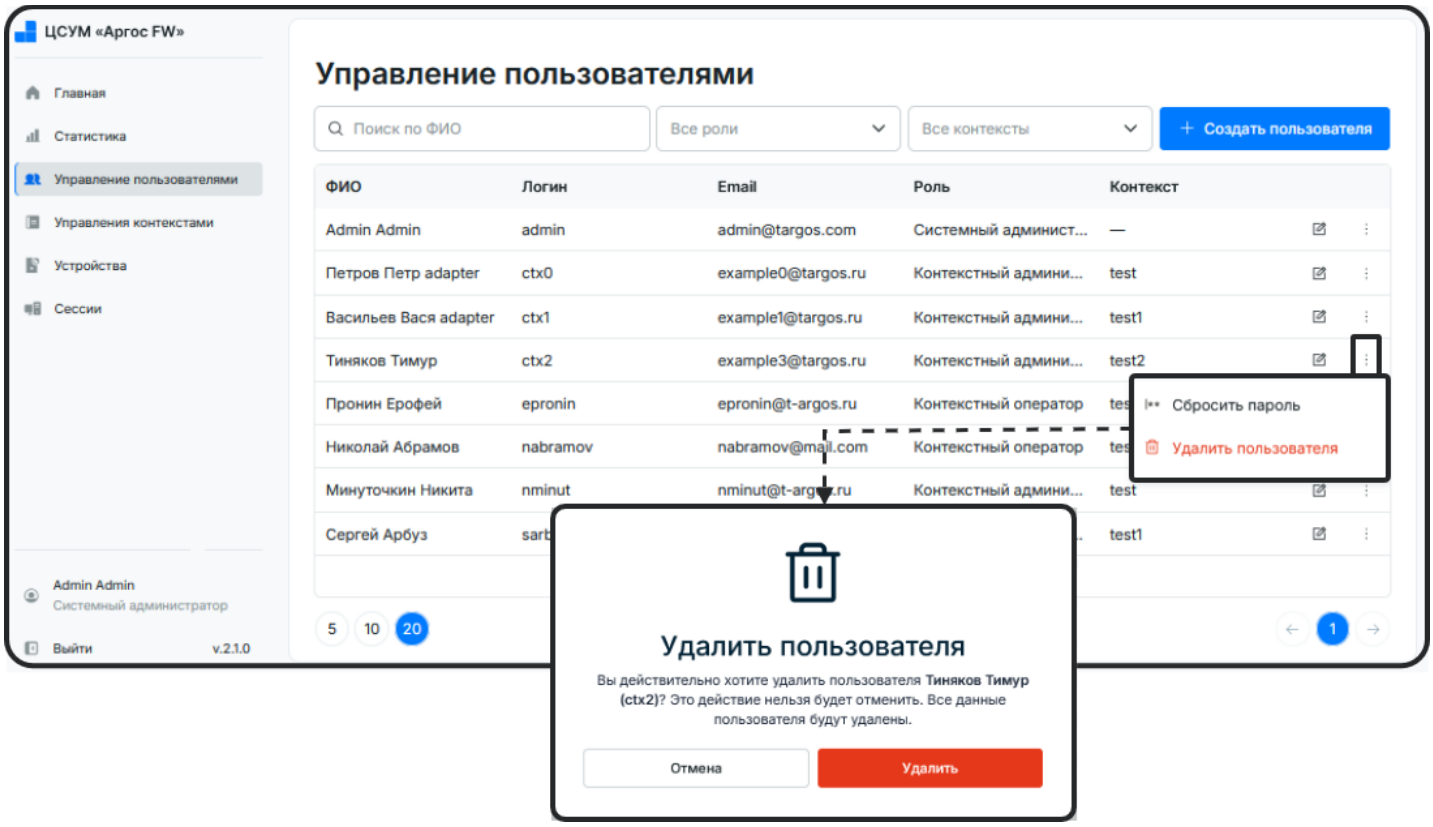
Пользователь с ролью контекстного администратора (CA) имеет право относительно пользователя с такой же ролью удалить его аккаунт и сбросить его пароль.

Рис. 20 – Сброс пароля



При удалении пользователя, откроется окно подтверждения действия (рис. 21).

Рис. 21 – Удаление пользователя



3.5 Устройства

Функционал управления устройствами доступен пользователям с любой ролью.

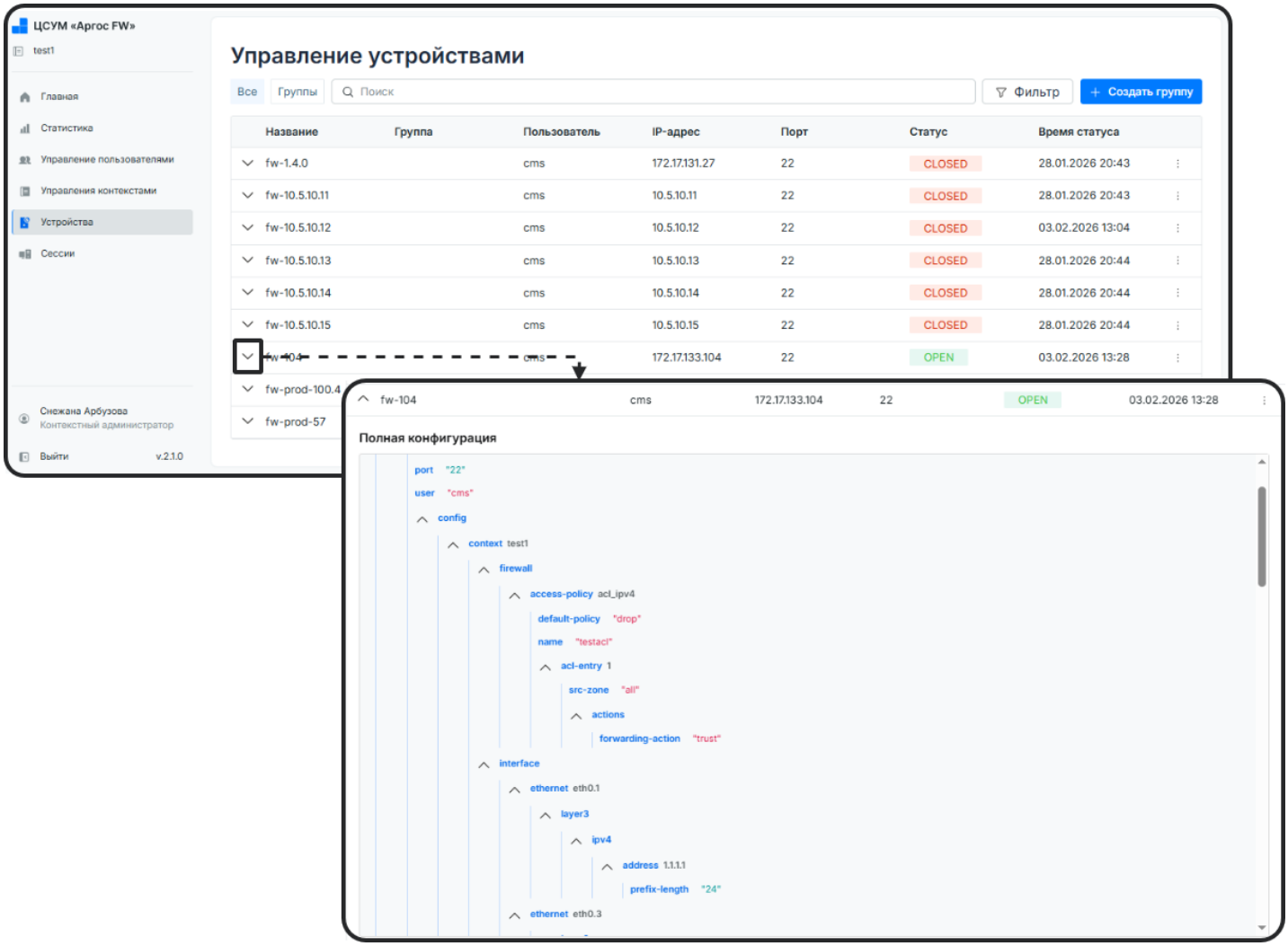
Для перехода к управлению устройствами следует на сайдбаре выбрать вкладку «Устройства». Откроется страница со списком всех устройств, доступных к управлению.

В текущем релизе пользователям доступны следующие действия с устройствами:

- просмотр конфигурации контекста на устройстве;
- подключение (connect) устройства;
- отключение (disconnect) устройства;
- переподключение (reconnect) устройства;
- обновление (pull) конфигурации с устройства;
- переход в WEB-интерфейс устройства.

Конфигурацию всех устройств и контекстов может просматривать только системный администратор (SA) (рис. 22). CA и CO могут просматривать конфигурацию только своего контекста, при этом они видят все подключенные устройства.

Рис. 22 – Просмотр конфигурации устройства



При нажатии на иконку ⋮ справа в строке с наименованием устройства откроется список возможных действий:

- для устройства в статусе «Closed»: подключение и переход в WEB-интерфейс (рис. 23);
- для устройства в статусе «Open»: отключение, переподключение, обновление, переход в WEB-интерфейс (рис. 24).

Рис. 23 – Действия с устройством в статусе «Close»

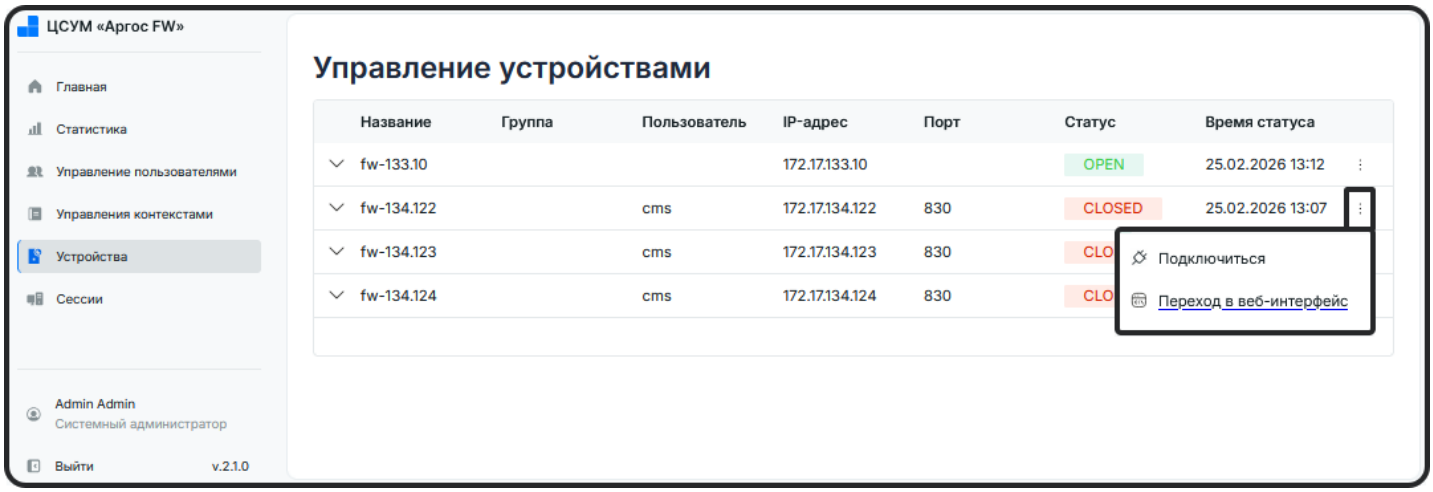
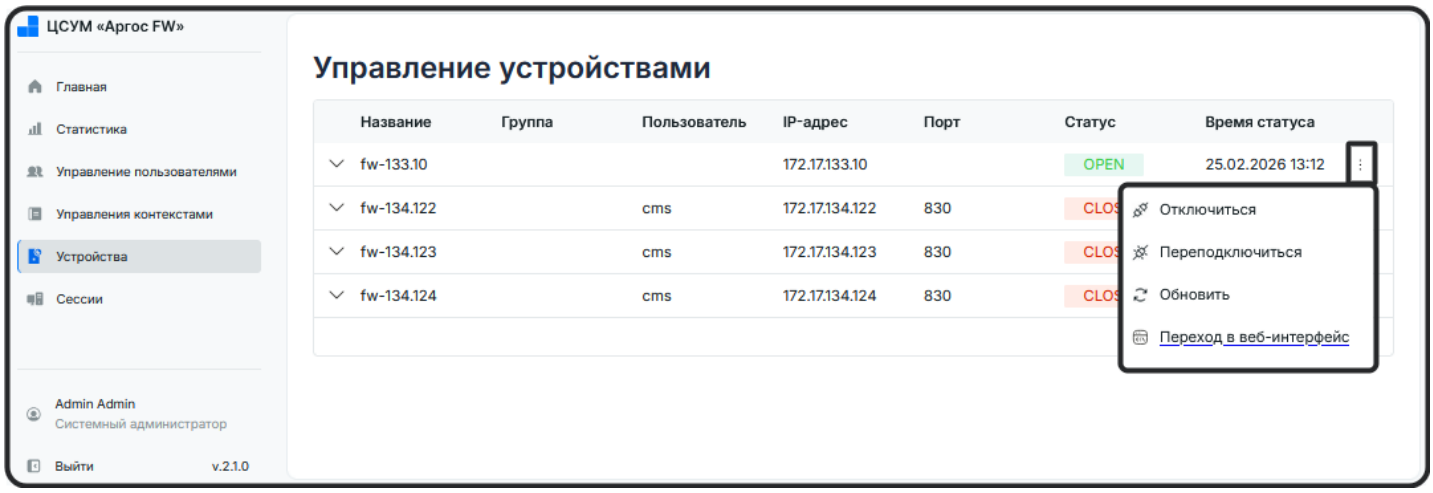


Рис. 24 – Действия с устройством в статусе «Open»



При выборе действия «Обновить» происходит pull-запрос конфигурации подключенного устройства и её перезапись в локальном хранилище Clixon-controller.

При выборе действия «Переход в веб-интерфейс», откроется окно авторизации для входа в WEB-интерфейс выбранного устройства (рис. 25).

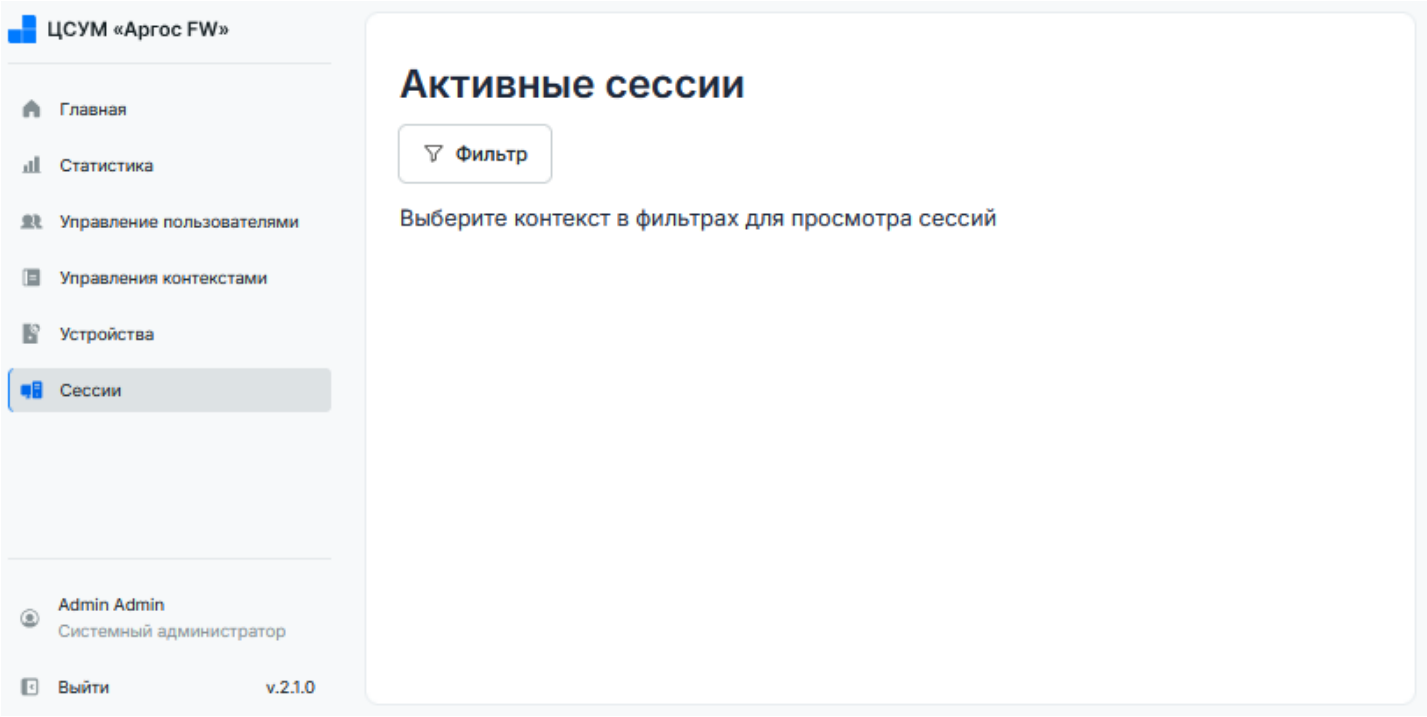
Рис. 25 – Переход в WEB-интерфейс устройства

3.6 Сессии

В системе реализована возможность поиска активных L3/4 сессий в рамках контекста по всем подключенным устройствам.

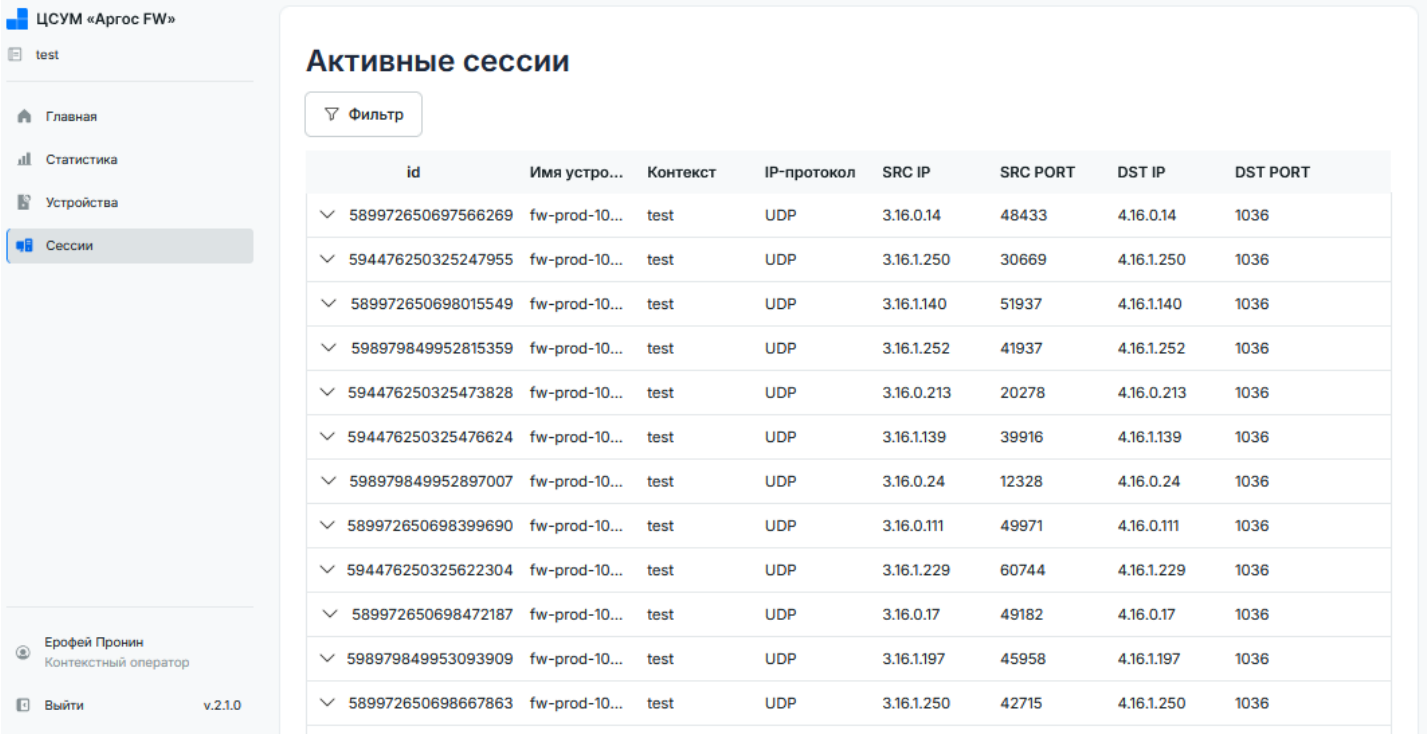
Для перехода на страницу поиска сессий следует выбрать на сайдбаре «Сессии». Для пользователя с ролью SA откроется страница с возможностью выставить в фильтре нужный контекст (рис. 26).

Рис. 26 – Страница отображения сессий для роли SA



Для ролей CA и CO откроется страница с отображенными сессиями соответствующего контекста.

Рис. 27 – Страница отображения сессий для ролей CA и CO



Поиск сессий

Для поиска сессий используется функционал фильтрации по задаваемым параметрам:

- Контекст — для SA предоставляется возможность фильтрации по контексту (рис. 28), для CA и CO контекст будет задан

Рис. 28 – Фильтрация сессий по контексту

- Имя устройства — выбор из подключенных устройств (рис. 29)

Рис. 29 – Фильтрация сессий по устройству

- IP-протокол — ID протокола в IP-заголовке
- IP-адрес назначения — задается в формате <x.x.x.x>
- TCP/UDP-порт назначения
- IP-адрес источника — задается в формате <x.x.x.x>
- TCP/UDP-порт источника
- Тип NAT-трансляции: ipv4-dnat-static, ipv4-snat-dynamic-ip-port, ipv4-snat-dynamic, ipv4-snat-static
- Входящий интерфейс (Ingress) — имя интерфейса в строковом формате
- Исходящий интерфейс (Egress) — имя интерфейса в строковом формате
- Минимальное время жизни сессии — в секундах
- Минимальный размер переданных данных — в килобайтах
- Количество выводимых найденных сессий — значение в диапазоне <1-10000>
- Вывод по порядковому номеру найденной сессии

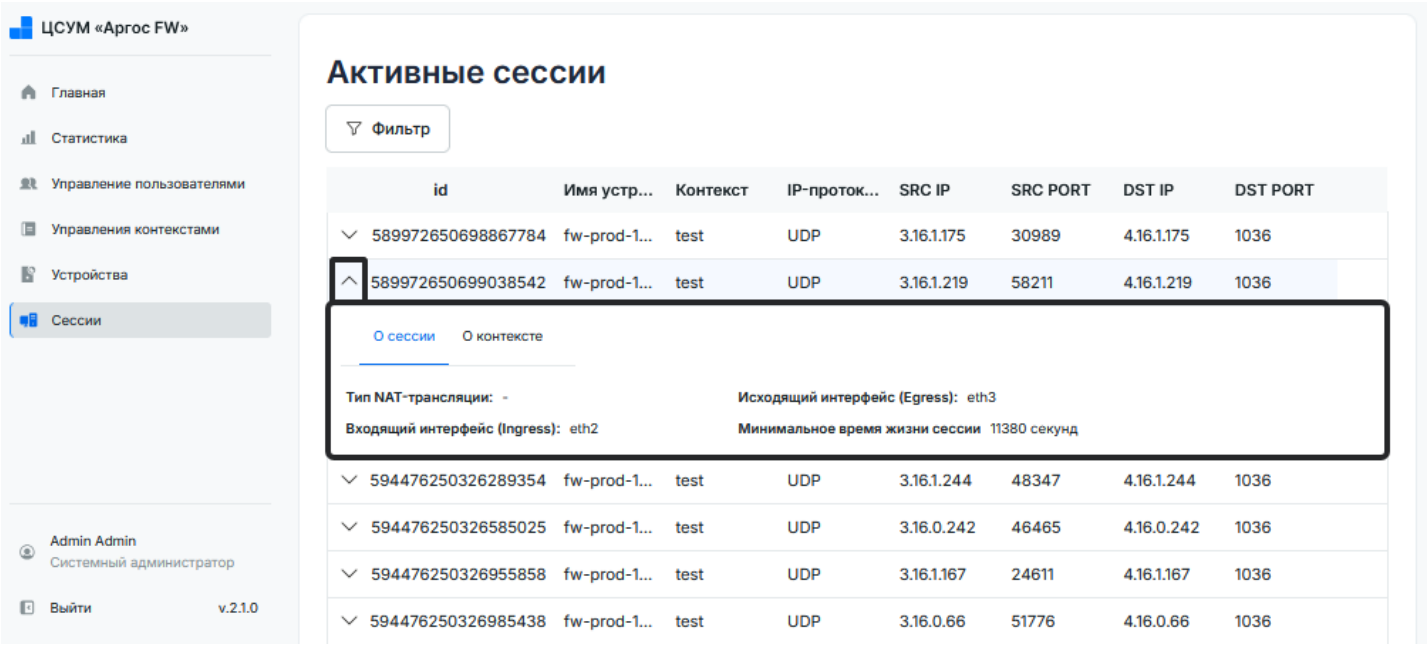
После заполнения необходимых полей следует нажать кнопку Показать, после чего система отобразит заданное количество сессий в таблице задаваемых фильтров.

О каждой сессии представлена информация (рис. 30), раскрывающаяся при нажатии на значок выпадающего списка ⌄ :

- Тип NAT-трансляции

- Входящий интерфейс (Ingress)
- Исходящий интерфейс (Egress)
- Минимальное время жизни сессий

Рис. 30 – Информация о сессии

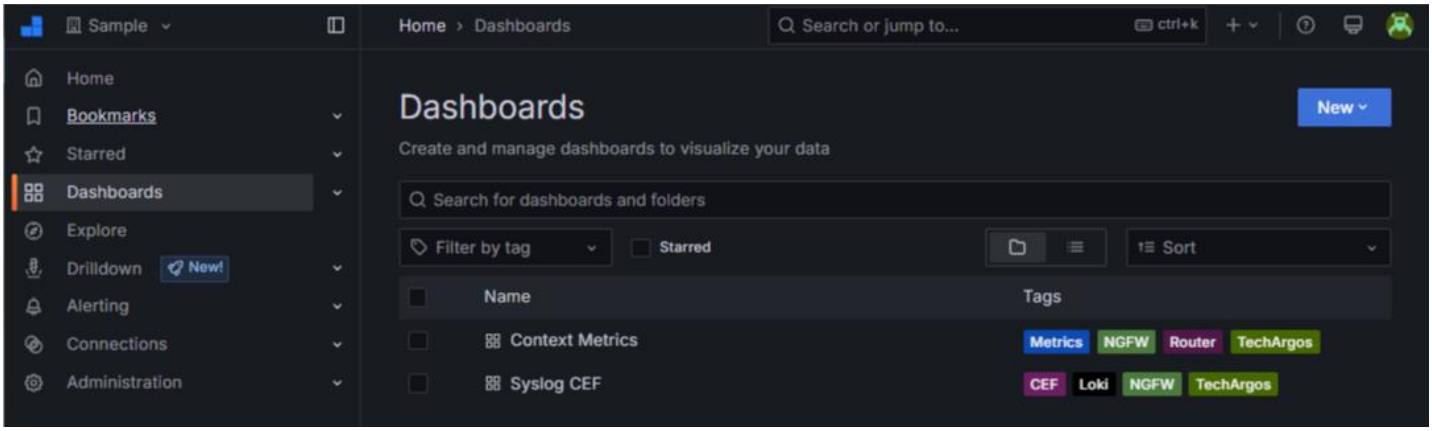


Так же во вкладке «О контексте» представлена информация о контексте, в рамках которого устанавливается сессия.

4. Работа с системой аналитики

Для перехода в систему аналитики метрик и логов следует на сайдбаре выбрать раздел «Статистика», после чего произойдет редирект на страницу системы Grafana с уже авторизованной сессией из панели управления ЦСУМ (рис. 31).

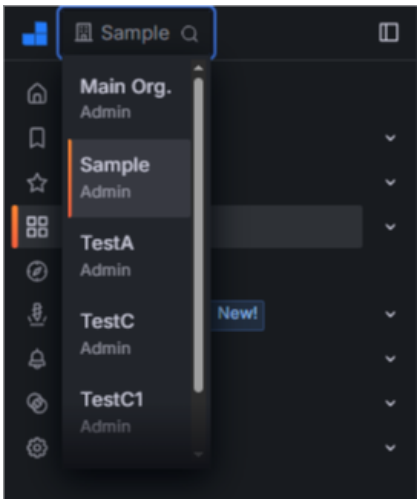
Рис. 31 – Переход в систему аналитики метрик и логов



Пользователи с ролью системного администратора (SA) имеют следующие возможности:

- переход между контекстами (рис. 32);
- доступ к системным (внеконтекстным) данным;
- доступ дашбордам, относящимся к аналитике компонентов ЦСУМ (рис. 33);
- создание и просмотр дашбордов в любом контексте.

Рис. 32 – Переход между контекстами

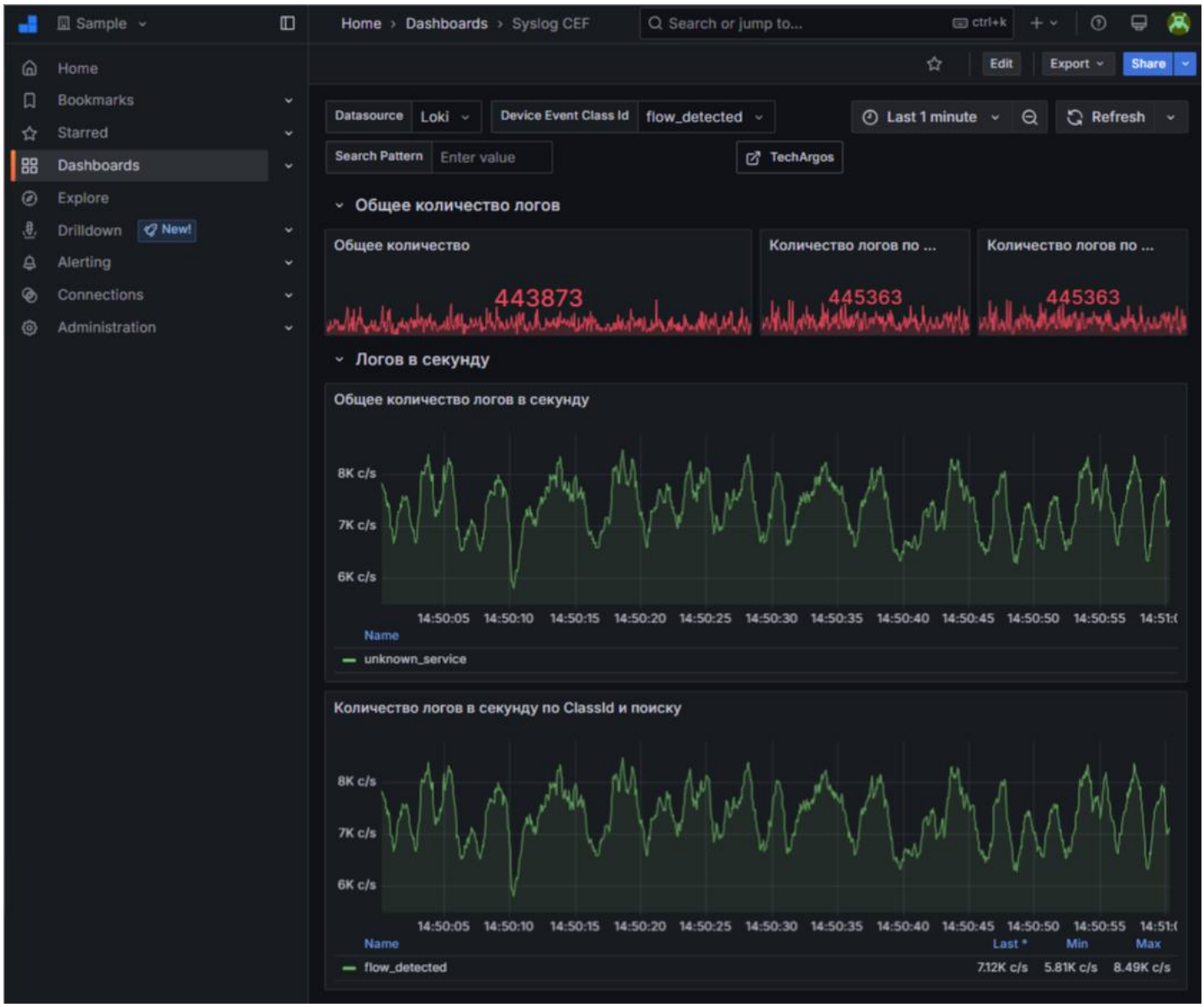


Пользователи с ролью контекстного администратора (CA) имеют следующие возможности:

- создание дашбордов в контексте;
- просмотр дашбордов контекста.

Пользователи с ролью контекстного оператора (CO) имеют право только на просмотр, созданных администраторами дашбордов.

Рис. 33 – Пример отображения статистики по событиям ИБ на дашбордах



5. Подключение и работа в CLI-интерфейсе

5.1 Авторизация

После создания пользователя в WEB-интерфейсе и смены его временного пароля на постоянный есть возможность подключиться по SSH к Clixon-контроллеру, входящему в состав ЦСУМ, для централизованного управления устройствами межсетевого экранирования посредством CLI-интерфейса.

Обратите внимание, что пароль с временного на постоянный можно сменить только посредством WEB-интерфейса.

Для подключения необходимо в пользовательском терминале ввести команду **ssh** <user>@<IP адрес ЦСУМ> и далее указать пароль пользователя. При успешной проверке пароля пользователь попадет в CLI-интерфейс Clixon-контроллера, где увидит приветствие командной строки **controller>**.

5.2 CLI-интерфейс

Здесь и далее доступны стандартные CLI-команды, сходные с такими в CLI-интерфейсе управления межсетевыми экранами «Аргос FW».

К примеру, символ «?» выводит контекстную подсказку по командам, доступным пользователю.

CLI-интерфейс имеет два режима: ***операционный*** и ***конфигурирования***. Ниже представлены приветствие '>' и набор команд в операционном режиме.

```
controller> ?
  configure             Change to configure mode
  connection            Change connection state of one or several devices
  exit                  Quit
  pull                  Pull config from one or multiple devices
  push                  Push config to one or multiple devices
  quit                  Quit
  rpc                   Send RPC to devices
  session               Client sessions
  show                  Show a particular state of the system
```

Для перехода в режим конфигурирования необходимо ввести команду **configure**. Ниже представлен набор команд доступных в режиме конфигурирования, [/] приветствие.

```
controller> configure
controller[/]# ?
  apply                 Apply template
  commit                Run services, commit and push to devices
  delete                Delete a configuration item
  discard               Discard edits (rollback 0)
  edit                  Edit specific datamodel level
  exit                  Change to operation mode
  lock                  Lock candidate datastore
  operation             Run operational commands
  quit                  Change to operation mode
  set                   Set a specific datamodel parameter
  show                  Show a particular state of the system
  top                   Go to the datamodel top
  unlock                Unlock candidate datastore
  up                    Go up one level in a datamodel
  update                Update private candidate from running configuration
  validate              Validate changes
```

Подключение устройств и локальное применение конфигурации

Для подключения межсетевого экрана «Аргос FW» к ЦСУМ необходимо в CLI-интерфейсе межсетевого экрана создать пользователя, к примеру, cmsacc с ролью **cms (сокращение от Central Management System)**, от имени которого ЦСУМ будет управлять устройством.

Ниже приведены настройки cmsacc пользователя на межсетевом экране «Аргос FW»

```
set system aaa authentication user cmsacc
set system aaa authentication user cmsacc role cms
```

Отметим, что после создания cmsacc пользователя на межсетевом экране необходимо задать ему публичный SSH-ключ из ключевой пары, созданной и хранящейся на ЦСУМ.

```
sysadmin@FW-S1-01:/> install crypto key cmsacc
Введите публичный SSH ключ: <здесь необходимо ввести rsa_id.pub ключ>
```

Также для разрешения Netconf_over_SSH доступа через Mgmt-интерфейс межсетевого экрана нужно явно указать этот протокол в списке разрешенных.

```
set system interface management mgmt0 allow-access protocol SSH-NETCONF
```

В ЦСУМ в режиме конфигурирования необходимо добавить межсетевой экран к пулу управляемых устройств по протоколу **Netconf over SSH** (стандартный ssh порт TCP/830).

Рассмотрим пример добавления устройства с именем **fw1**. Здесь важен параметр **ssh-stricthostkey: false**, благодаря которому контроллер автоматически добавит информацию об ssh-подключении к устройству в локальный файл **/root/.ssh/known_hosts**. Также обязательно использование опции **private-candidate: true** с устройствами «Аргос FW», согласование режима работы Netconf Private-candidate.

```
set devices device fw1
set devices device fw1 enabled true
set devices device fw1 user cmsacc
set devices device fw1 ssh-stricthostkey false
set devices device fw1 private-candidate true
set devices device fw1 port 830
set devices device fw1 addr <IP-адрес mgmt-интерфейса устройства>
```

После создания конфигурации необходимо применить ее локально на Clixon-контроллере командой **commit local**

```
controller[/]# commit local
controller[/]#
```

Управление подключенными устройствами разделяется на два домена:

- локальная конфигурация — информация о том, как подключиться к устройству;
- конфигурация самого подключенного устройства, скачиваемая (pull) с устройства.

Соответственно, «commit» операция разделяется на local и remote (push), где local соответствует изменению конфигурации, хранимой в Clixon-контроллере, а remote (push) – трансляции и применению изменений уже на самом подключенном устройстве.

```
controller[/]# commit ?
  <cr>
  diff                  Show the result of running the services but do not commit
  local                 Local commit, do not push to devices
  push                  Run services, commit and push to devices
```

После создания локальной конфигурации устройства необходимо подключиться к нему. Для этого используется команда **connection** из операционного режима и соответствующая **show** команда для определения состояния подключения.

```
controller> connection open fw1
controller>
controller> show connections fw1
Name                    State      Time                    Logmsg
=========================================================================
fw1                     OPEN       2025-09-30T19:54:59
```

Статус устройства «OPEN» означает, что устройство успешно подключено и получена (pull) его конфигурация. Теперь можно просмотреть конфигурацию данного устройства с помощью команды **show configuration** в CLI-интерфейсе контроллера.

```
controller> show configuration
set devices device fw1
set devices device fw1 enabled true
set devices device fw1 user cmsacc
set devices device fw1 ssh-stricthostkey false
set devices device fw1 private-candidate true
set devices device fw1 port 830
set devices device fw1 addr 172.17.133.104
set devices device fw1 config
set devices device fw1 config context test1
set devices device fw1 config context test1 interface ethernet eth0.1
set devices device fw1 config context test1 interface ethernet eth0.1 layer3 ipv4 address 1.1.1.1
set devices device fw1 config context test1 interface ethernet eth0.1 layer3 ipv4 address 1.1.1.1
prefix-length 24
set devices device fw1 config context test1 interface ethernet eth0.3
set devices device fw1 config context test1 interface ethernet eth0.3 layer3 ipv4 address 2.3.2.3
set devices device fw1 config context test1 interface ethernet eth0.3 layer3 ipv4 address 2.3.2.3
prefix-length 24
set devices device fw1 config context test1 network-zone all
set devices device fw1 config context test1 network-zone all interface eth0.1
……
```

Здесь мы видим, как локальные настройки устройства **fw1**, так и ниже по иерархии уровня **set devices device fw1 config**, в котором отображается конфигурация самого устройства.

Изменение конфигурации подключенных устройств

Для изменения конфигурации подключенного устройства необходимо в режиме конфигурирования контроллера выполнить соответствующую команду устройства с добавлением служебного префикса, включающего имя устройства, на котором должна быть применена команда.

К примеру, команда изменения описания интерфейса в CLI межсетевого экрана имеет вид **set context test1 interface ethernet eth0.1 layer3 description "test interface description"**

В случае же применения указанной конфигурации в CLI-контроллера ЦСУМ команда контроллера имеет вид ***set devices device fw1 config* context test1 interface ethernet eth0.1 layer3 description "test interface description"**

Обратите внимание, что в CLI контроллера работает tab-расширение, когда после каждого слова команды клавиша “Tab” выводит возможное продолжение команды согласно CLI-модели подключенных устройств.

```
controller> configure
controller[/]# set devices device fw1 config context test1 interface ethernet eth0.1 layer3
 description            ethernet               ipv4                   mtu                    rx-frag-
packets-allow
controller[/]# set devices device fw1 config context test1 interface ethernet eth0.1 layer3 des
 <description>
controller[/]# set devices device fw1 config context test1 interface ethernet eth0.1 layer3 description
"test interface description "
```

Одновременное применение конфигурации на контроллере и подключенном устройстве

Перед применением конфигурации посмотреть текущие изменения можно с помощью команды **commit diff** .

```
controller[/]# commit diff
fw1:
                  <config xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
-                 <description></description>
+                 <description>test interface description</description>
                  </config>
OK
```

Проверка применимости текущих изменений подключенным устройством осуществляется с помощью команды **validate push** .

```
controller[/]# validate push
OK
```

Непосредственное применение указанной конфигурации к устройству производится с помощью команды **commit push**. Изменение будет внесено как в конфигурацию подключенного устройства, так и в локальную копию конфигурации, хранимую в контроллере.

```
controller[/]# commit push
OK
```

Локальное применение конфигурации и последующее ее применение на подключенном устройстве

В системе присутствует возможность сначала применить изменения в локальную базу данных контроллера, содержащую конфигурацию подключенного устройства, с помощью команды **commit local**.

```
controller[/]# set devices device fw1 config context test1 interface ethernet eth0.1 layer3 description
"another test interface description"
controller[/]# commit local
controller[/]#
```

Затем в операционном режиме командой **push validate** проверяется, что изменение конфигурации может быть применено на подключенном устройстве. Либо сразу применяется изменение конфигурации устройства с помощью команды **push commit**. Ниже приведены примеры таких команд: применение локально сохраненной конфигурации на контроллере к устройству fw1.

```
controller> push fw1 validate
OK
controller> push fw1 commit
OK
```

Для получения конфигурации подключенного устройства и копирования в локальную базу данных CLI-контроллера следует использовать команду **pull**.

```
controller> pull fw1
OK
```

Одновременное применение конфигурации сразу к нескольким подключенным устройствам

Контроллер позволяет одновременно внести изменение в конфигурации нескольких устройств и транзакционно применить эти изменения. Транзакционность здесь означает, что конфигурация будет либо применена на всех четырех устройствах, либо не будет применена нигде.

К примеру, предположим, что у нас настроены четыре устройства «Аргос FW», подключенных к CLI-контроллеру под именами fw1, fw2, fw3, fw4. Для изменения конфигурации всех четырех устройств следует использовать шаблон на базе символа «*» (любая последовательность символов). Команда **commit push** позволяет транзакционно применить внесенные изменения.

```
controller[/]# set devices device fw* config context test1 interface ethernet eth0.1 layer3 description
"super interface"
controller[/]# commit push
OK
```

ООО «ТехАргос»
127015, г. Москва, ул. Новодмитровская, 2Б, ДЦ «Дмитровский»

Телефон: +7(495) 411-90-37
Web: https://t-argos.ru/
E-mail: mail@t-argos.ru