**NPP Analytics**

**Руководство пользователя**

Содержание

[1. Введение 3](#_Toc91606510)

[1.1. Полное наименование Системы и её условное обозначение 3](#_Toc91606511)

[1.2. Назначение и условия применения 3](#_Toc91606512)

[2. Интерфейс NPP Analytics 4](#_Toc91606513)

[2.1. Отчёты по событиям УОЭ 5](#_Toc91606514)

[2.1.1. Показатели: СНУ 8](#_Toc91606515)

[2.1.2. Показатели: Отклонения 9](#_Toc91606516)

[2.1.3. Показатели: Нарушения 9](#_Toc91606517)

[2.1.4. Показатели: Дефекты 10](#_Toc91606518)

[2.2. Отчёт «Кристаллизация знаний» 11](#_Toc91606519)

[2.3. Выход из интерфейса NPP Analytics 12](#_Toc91606520)

[3. NPP консоль настройки визуализации 13](#_Toc91606521)

[3.1. Создание своей первой панели управления 13](#_Toc91606522)

[3.1.1. Подключение к новой базе данных 13](#_Toc91606523)

[3.1.2. Регистрация новой таблицы 14](#_Toc91606524)

[3.1.3. Настройка свойств столбца 14](#_Toc91606525)

[3.1.4. Семантический слой 14](#_Toc91606526)

[3.1.5. Создание диаграмм в представлении «Обзор» 15](#_Toc91606527)

[3.1.6. Создание среза и панели управления 16](#_Toc91606528)

[3.1.7. Управление доступом к панелям управления 16](#_Toc91606529)

[3.2. Изучение данных 17](#_Toc91606530)

[3.2.1. Включение функции загрузки данных 17](#_Toc91606531)

[3.2.2. Загрузка данных CSV 17](#_Toc91606532)

[3.2.3. Визуализация таблицы 17](#_Toc91606533)

[3.2.4. Основы работы с панелью управления 18](#_Toc91606534)

[3.2.5. Сводная таблица 18](#_Toc91606535)

[3.2.6. Линейная диаграмма 19](#_Toc91606536)

[3.2.7. Разметка 20](#_Toc91606537)

[3.2.8. Поле фильтра 20](#_Toc91606538)

[3.2.9. Публикация панели управления 21](#_Toc91606539)

[3.2.10. Аннотации 21](#_Toc91606540)

[3.2.11. Расширенная аналитика 22](#_Toc91606541)

[3.2.12. Скользящее среднее 22](#_Toc91606542)

[3.2.13. Сравнение времени 22](#_Toc91606543)

[3.2.14. Повторная выборка данных 23](#_Toc91606544)

[4. NPP консоль управления правами 24](#_Toc91606545)

[4.1. Создание реалма и пользователя 24](#_Toc91606546)

[4.1.1. Реалм и пользователи 24](#_Toc91606547)

[4.1.2. Создание реалма 24](#_Toc91606548)

[4.1.3. Создание пользователя 25](#_Toc91606549)

[4.1.4. Вход в консоль учётной записи 25](#_Toc91606550)

[4.2. Управление сессией пользователя 26](#_Toc91606551)

[4.2.1. Администрирование сессий 26](#_Toc91606552)

[4.2.2. Политика отзыва 27](#_Toc91606553)

[4.2.3. Таймауты сессии и токена 27](#_Toc91606554)

[4.3. Объединение хранилищ пользователей 30](#_Toc91606555)

[4.3.1. Добавление поставщика 31](#_Toc91606556)

[4.3.2. Работа со сбоями поставщика 31](#_Toc91606557)

[4.3.3. LDAP и Active Directory 32](#_Toc91606558)

[4.4. Аудит и события 40](#_Toc91606559)

[4.4.1. События входа в систему 40](#_Toc91606560)

[4.4.2. События администратора 42](#_Toc91606561)

[4.5. Экспорт и импорт 42](#_Toc91606562)

[4.5.1. Экспорт и импорт 43](#_Toc91606563)

[4.6. Служба учётной записи пользователя 44](#_Toc91606564)

[4.6.1. Тематические 45](#_Toc91606565)

[4.7. Уменьшение рисков 45](#_Toc91606566)

[4.7.1. Угадывание пароля: атаки методом перебора 45](#_Toc91606567)

[4.7.2. Атрибуты пользователя только для чтения 48](#_Toc91606568)

# Введение

## Полное наименование Системы и её условное обозначение

Наименование: Программное обеспечение NPP Analytics

Условное обозначение и краткое наименование: NPP Analytics.

## Назначение и область применения

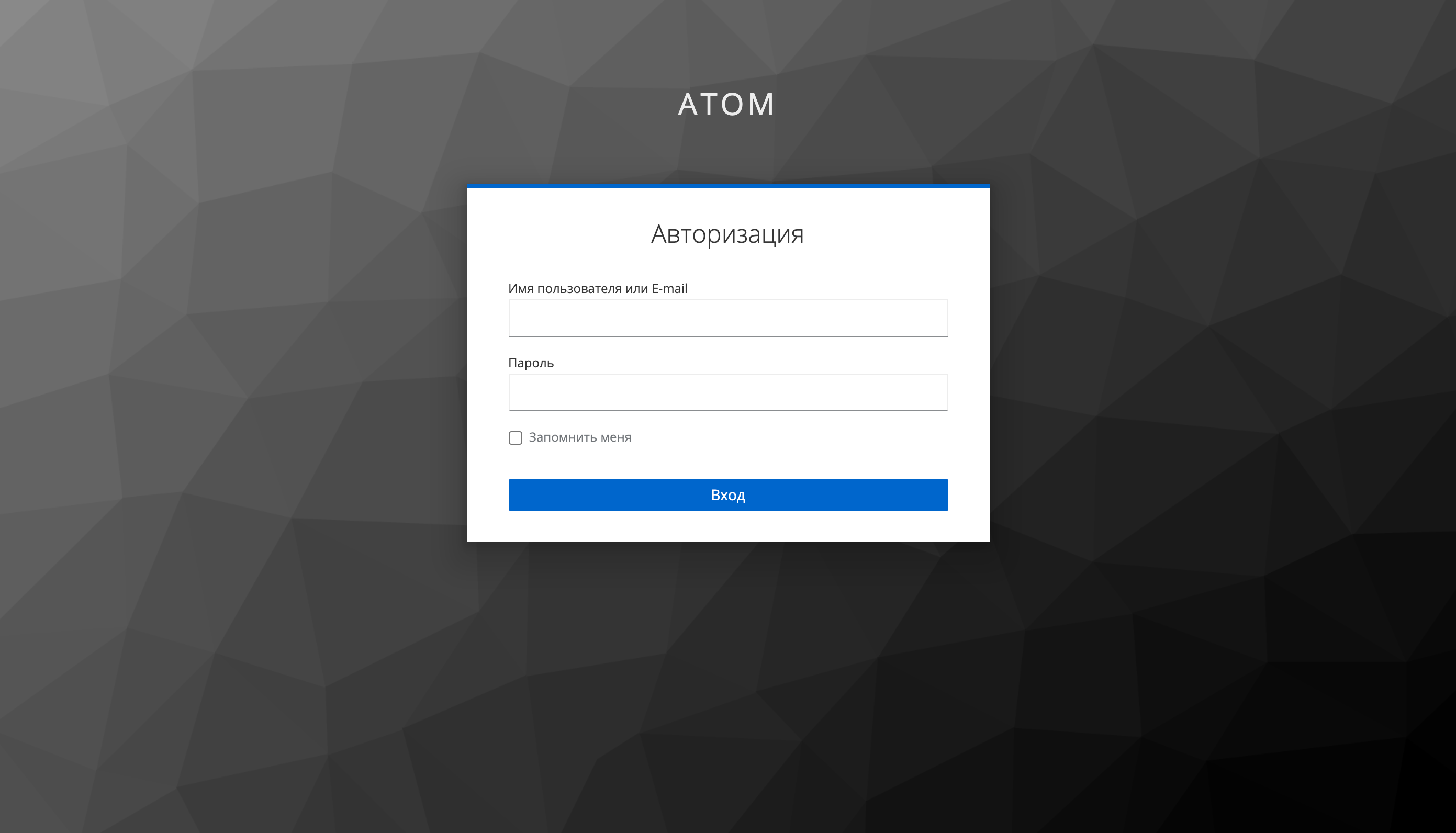
NPP Analytics предназначено для консолидации исторических и оперативных данных работы атомных электростанций (далее – АЭС) и крупных электрогенерирующих предприятий, для решения задач расследования и анализа причин событий на АЭС и крупных электрогенерирующих предприятиях, сквозного анализа данных учета опыта эксплуатации (далее – УОЭ) от событий низкого уровня до аномальных событий УОЭ с целью выявления причинно-следственных связей между событиями и определения трендов их развития.

Областью применения NPP Analytics является предоставление высокопроизводительных инструментов для решения аналитических задач по выявлению и прогнозированию аномальных событий на АЭС и крупных электрогенерирующих предприятиях.

# Интерфейс NPP Analytics

Для входа в систему введите в поле ввода адреса веб-браузера (рекомендуется использовать Google Chrome, Яндекс.Браузер или аналогичные актуальных версия) адрес расположения (URL) развернутой системы ЕААД NPP.

Введите логин и пароль для входа в ЕААД NPP (далее Система), откроется интерфейс Аналитической подсистемы в составе ЕААД NPP.



1. Окно входа

Выберите набор аналитических интерфейсов на вкладке «Отчёты», описание отчётов приведено в таблице.

Виды отчётов в системе.

|  |  |  |
| --- | --- | --- |
| Наименование |  | Описание |
| Показатели:  СНУ | Аналитический интерфейс анализа событий «СНУ на АЭС» |  |
| Показатели: Отклонения | Аналитический интерфейс анализа событий «Отклонения в работе АЭС» |  |
| Показатели: Нарушения | Аналитический интерфейс анализа событий «Нарушения в работе АЭС» |  |
| Показатели: Дефекты | Аналитический интерфейс анализа событий «Дефекты в работе АЭС» |  |
| Кристаллизация знаний | Аналитический интерфейс анализа упоминания единиц оборудования в материалах УОЭ |  |

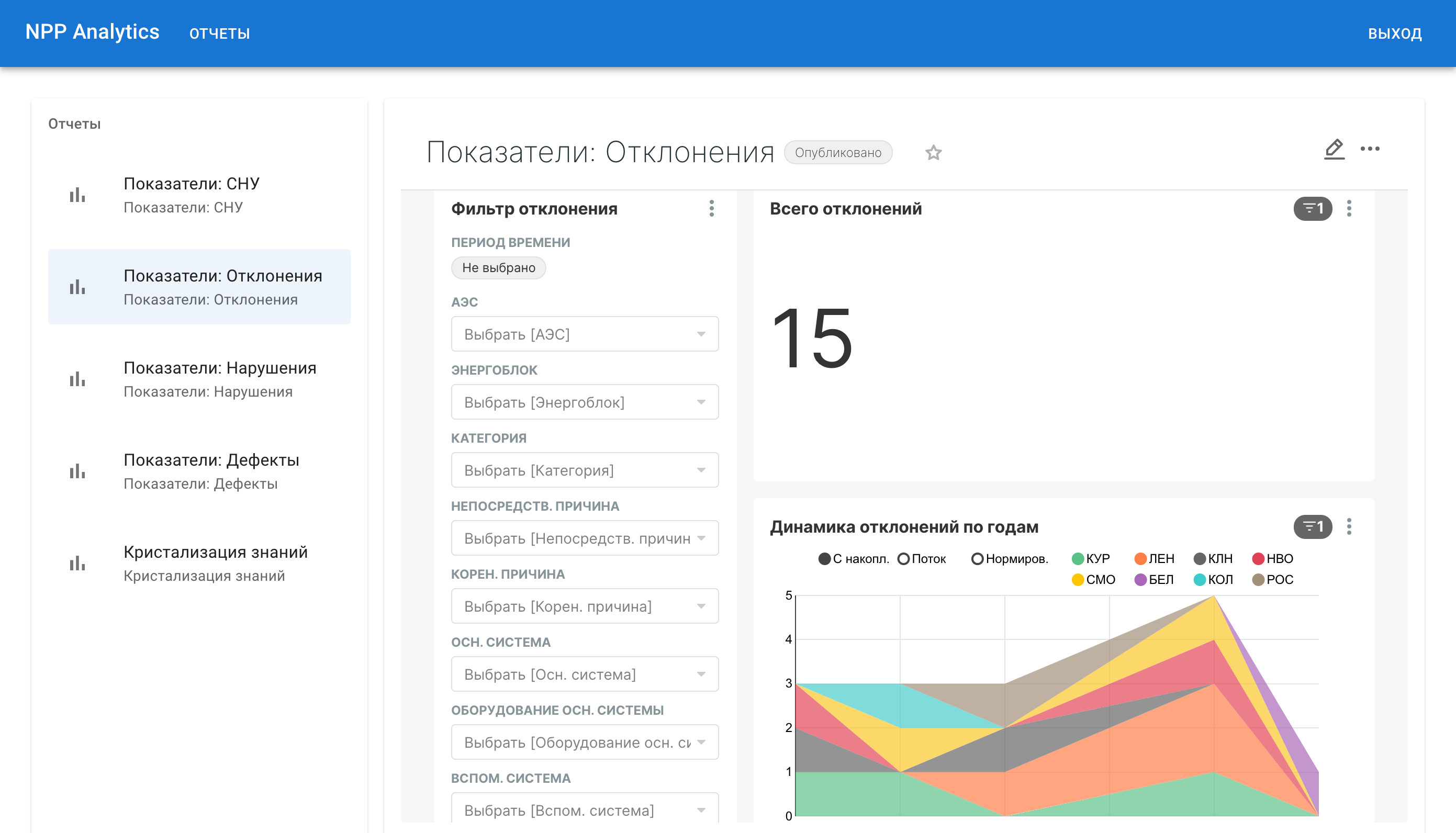
## Отчёты по событиям УОЭ

Для проведения анализа причин событий, трендов и тенденций, статистического анализа событий и анализа безопасности выберите на вкладке «Отчёты» аналитические интерфейсы общей статистики по событиям УОЭ:

* Показатели: СНУ;
* Показатели: Отклонения;
* Показатели: Нарушения;
* Показатели: Дефекты.

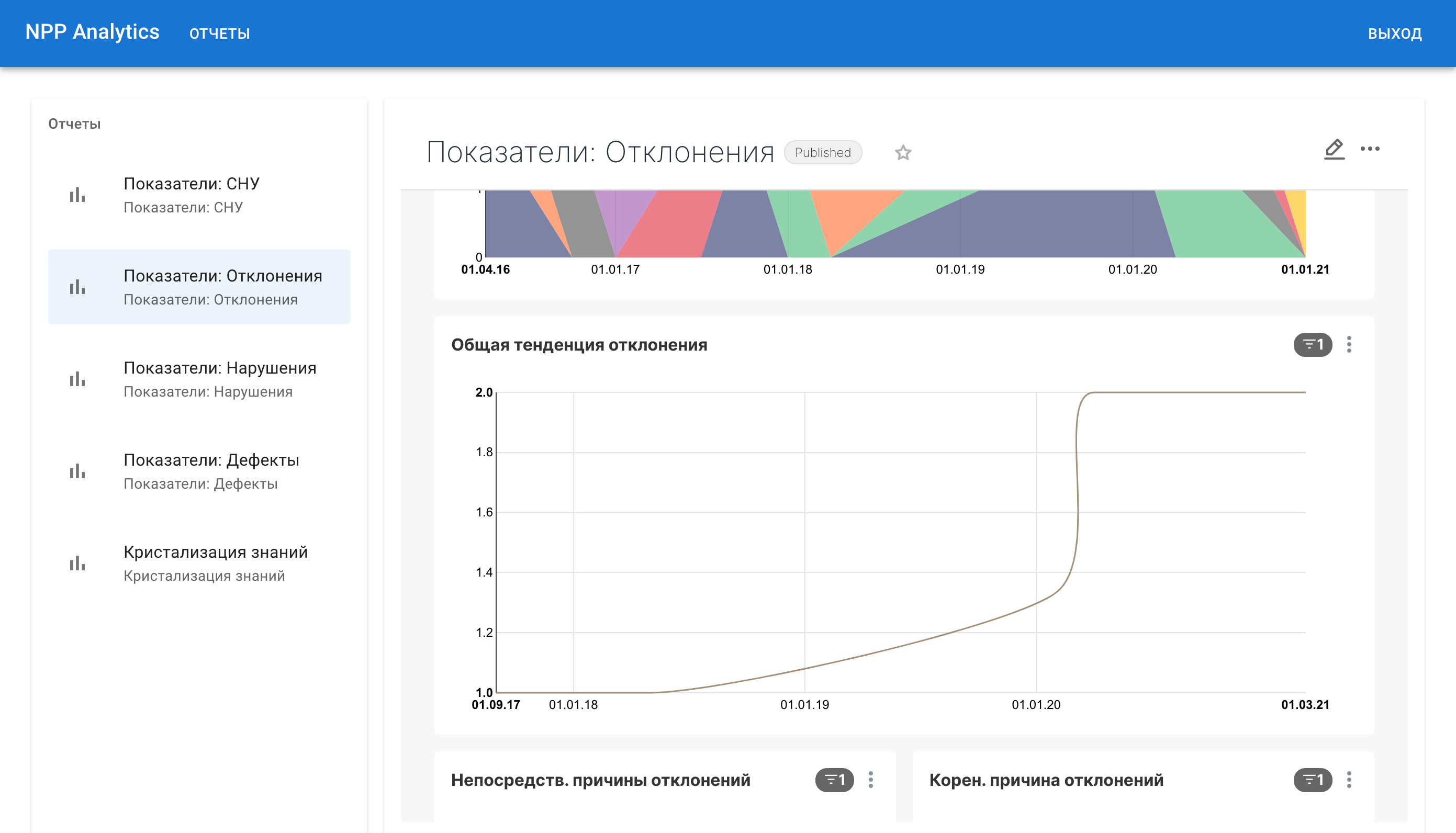
Аналитические интерфейсы, указанные выше, построены аналогично друг другу и содержат стандартный набор панелей, графиков и гистограмм:

* Панель фильтрации.
* Общее количество объектов отчёта.
* Динамика показателей за год/квартал/месяц.



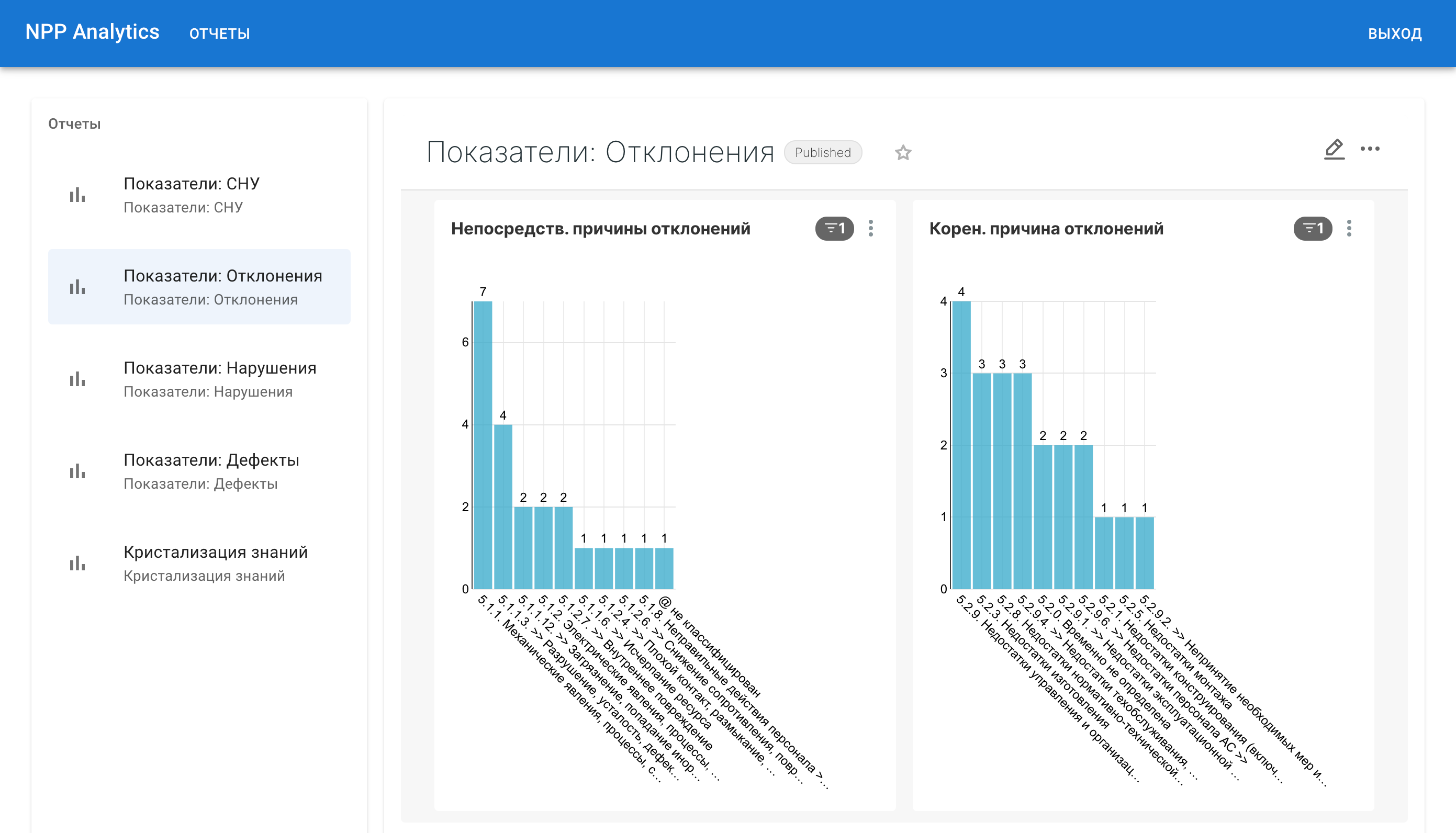
1. Панель фильтрации, общее количество объектов отчёта, динамика показателей

* Общая тенденция.



1. Общая тенденция

* Гистограмма специфичных показателей.



1. Гистограммы специфичных показателей

Для фильтрации всех графиков и гистограмм, представленных на открытом аналитическом интерфейсе, используйте панель фильтров. После установления соответствующих фильтров в правом верхнем углу появится общее число показателей, представленных на визуализациях.

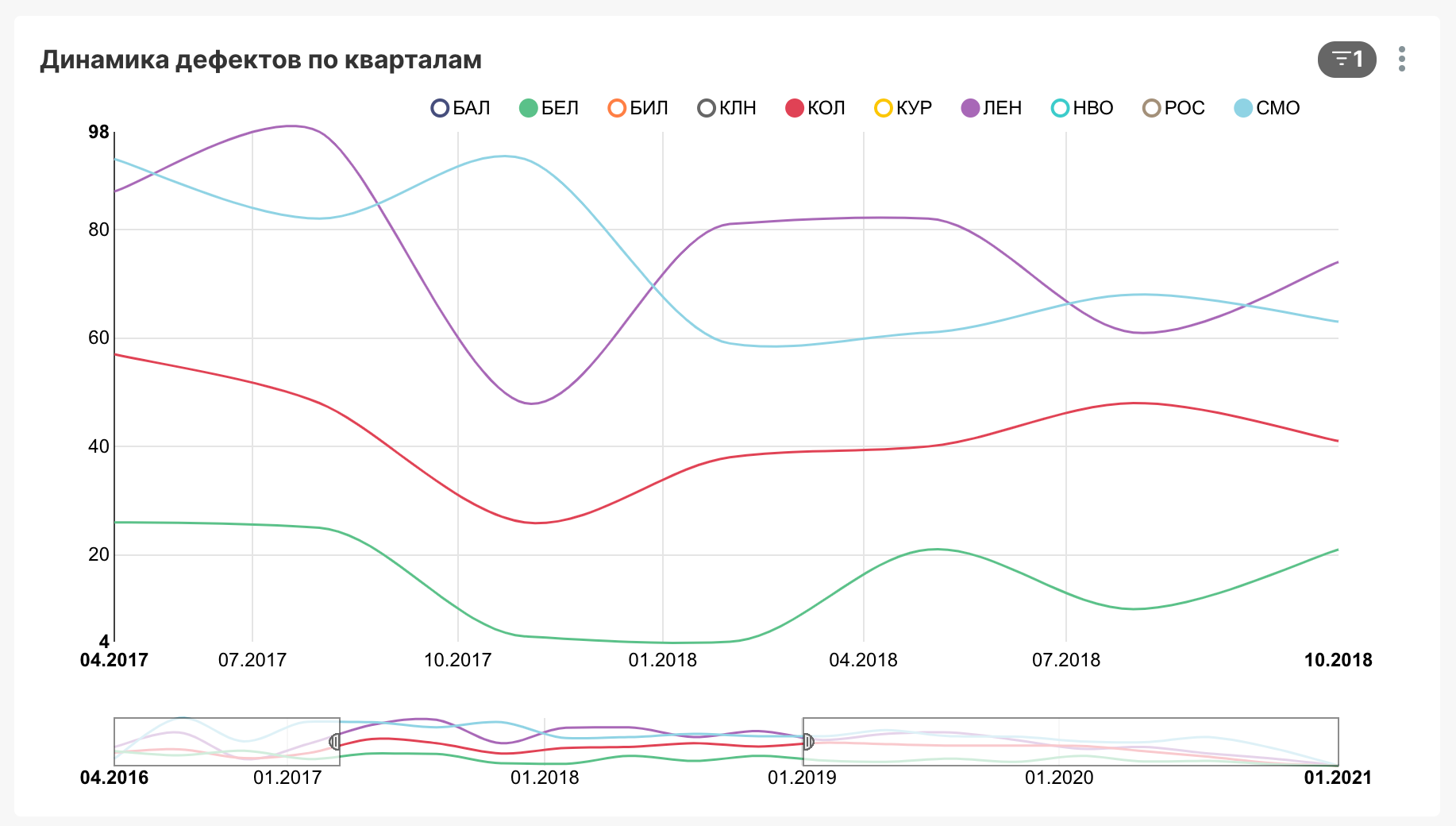
Для анализа динамики нарушений в работе АЭС на временной шкале откройте график областей с фильтрацией «Динамика нарушений». Присутствует возможность ограничить выборку, например, по АЭС с помощью панели фильтров или непосредственно на графике.

Для анализа тенденции изменений общего числа нарушений откройте график «Общая тенденция нарушений».

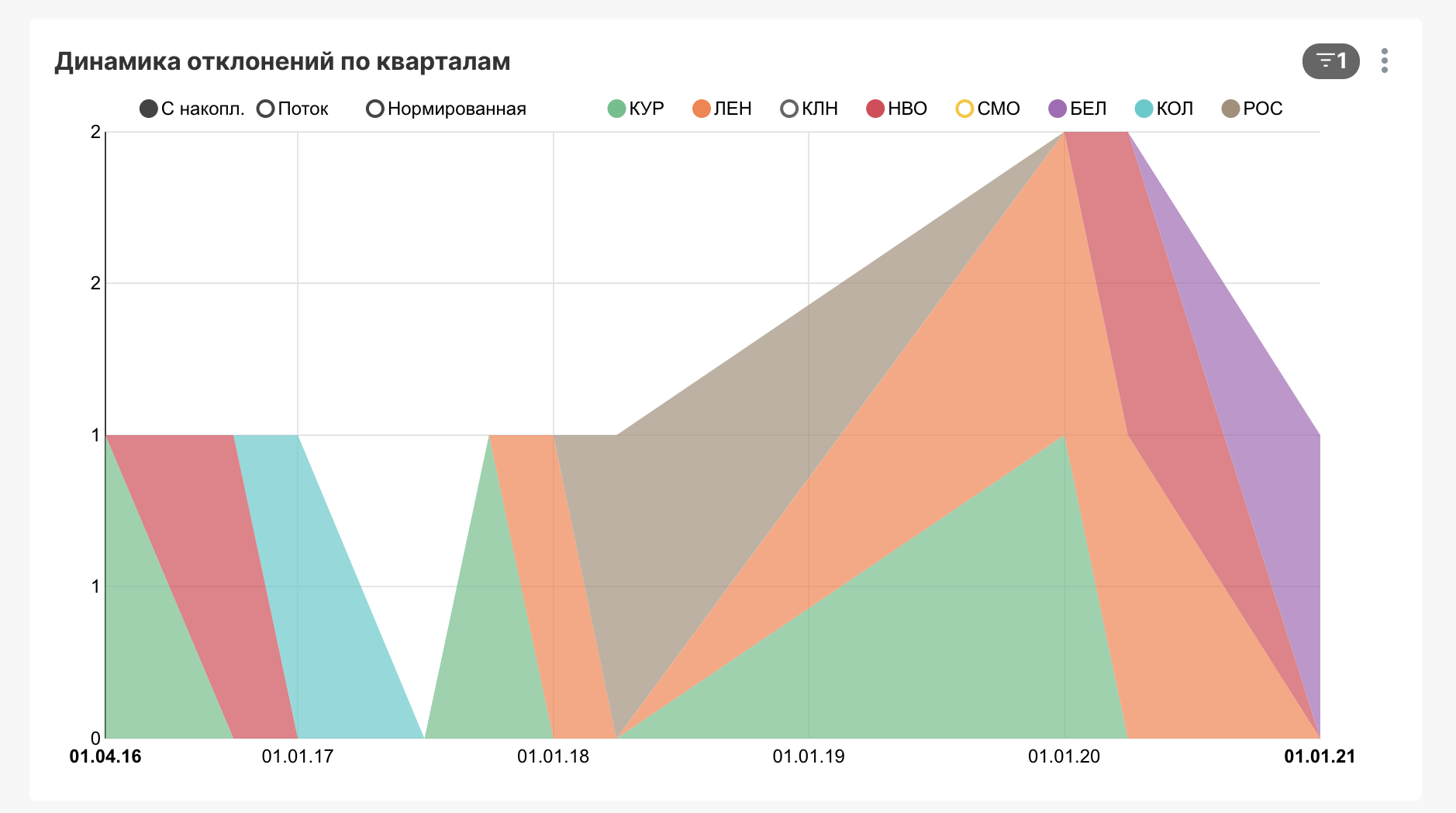
Отображение показателей в виде графиков осуществляется по умолчанию, изменить состав отображаемой информации можно на панели фильтров и с помощью фильтров, расположенных непосредственно на графиках.

На аналитических интерфейсах представлены графики следующих видов:

1. Простой линейный график — автоматически собираемый график, отображающий количество событий или расчётное значение в каждой точке времени заданного временного интервала. Данные, показанные на графике, зависят от того, что выбрано на панели фильтров. Наведите курсор на точку графика, чтобы узнать значение на конкретную дату. Нажимая на элементы в составе легенды, можно отключать их отображение. На дополнительной временной шкале под графиком можно уменьшать и увеличивать временной интервал. Для этого необходимо манипулятором мышь выделить область, которую можно изменять с помощью ползунков.



1. Общий линейный график или график областей с фильтрацией — автоматически собираемый график с возможностью отображения динамики изменения показателей по нескольким типам данных. Нажимая на элементы в составе легенды, можно отключать их отображение. Чтобы переключить режимы отображения: поток, с накоплением или посмотреть нормированную диаграмму, нужно нажать соответствующую кнопку над графиком.



### Показатели: СНУ

Содержит следующие фильтры:

1. Период времени. Выбор преднастроенных значений (за прошедший день, неделю, месяц и т.д.) или ввод произвольного диапазона.
2. АЭС. Выбор из списка.
3. Энергоблок. Выбор из списка.
4. Категория. Выбор из списка.
5. Вид безопасности. Выбор из списка.
6. Коренная причина. Выбор из списка.
7. Хаускипинг. Выбор из списка.
8. ПСС. Выбор из списка.
9. Оборудование. Выбор из списка.
10. Человеческий фактор. Выбор из списка.

Доступна следующая динамика показателей:

* по кварталам,
* по месяцам.

Специфичные графики:

* Категории СНУ.
* Оборудование.
* Виды безопасности.
* Основные причины.

### Показатели: Отклонения

Содержит следующие фильтры:

1. Период времени. Выбор преднастроенных значений (за прошедший день, неделю, месяц и т.д.) или ввод произвольного диапазона.
2. АЭС. Выбор из списка.
3. Энергоблок. Выбор из списка.
4. Категория. Выбор из списка.
5. Непосредственная причина. Выбор из списка.
6. Коренная причина. Выбор из списка.
7. Основная система. Выбор из списка.
8. Оборудование основной системы. Выбор из списка.
9. Вспомогательная система. Выбор из списка.
10. Оборудование вспомогательной системы. Выбор из списка.

Доступна следующая динамика показателей отклонений:

* по годам,
* по кварталам.

Специфичные графики:

* Непосредственные причины отклонений.
* Корневая причина отклонений.
* Основные системы отклонения.
* Оборудование основных систем отклонения.
* Вспомогательные системы отклонения.
* Оборудование вспомогательных систем отклонения.

### Показатели: Нарушения

Содержит следующие фильтры:

1. Период времени. Выбор преднастроенных значений (за прошедший день, неделю, месяц и т.д.) или ввод произвольного диапазона.
2. АЭС. Выбор из списка.
3. Энергоблок. Выбор из списка.
4. Категория. Выбор из списка.
5. Оценка по шкале ИНЕС. Выбор из списка.
6. Непосредственная причина. Выбор из списка.
7. Корневая причина. Выбор из списка.
8. Основная система. Выбор из списка.
9. Оборудование основной системы. Выбор из списка.
10. Вспомогательная система. Выбор из списка.
11. Оборудование вспомогательной системы. Выбор из списка.

Доступна следующая динамика показателей нарушений:

* по годам,
* по кварталам.

Специфичные графики:

* Непосредственные причины нарушений.
* Корневые причины нарушений.
* Основные системы нарушений.
* Оборудование основных систем нарушений.
* Вспомогательные системы нарушений.
* Оборудование вспомогательных систем нарушений.

### Показатели: Дефекты

Содержит следующие фильтры:

1. Период времени. Выбор преднастроенных значений (за прошедший день, неделю, месяц и т.д.) или ввод произвольного диапазона.
2. АЭС. Выбор из списка.
3. Энергоблок. Выбор из списка.
4. Тип оборудования. Выбор из списка.
5. Непосредственная причина. Выбор из списка.
6. Корневая причина. Выбор из списка.
7. Код технической системы. Выбор из списка.
8. Наименование технической системы. Выбор из списка.
9. Вспомогательная система. Выбор из списка.
10. Оборудование вспомогательной системы. Выбор из списка.

Доступна следующая динамика показателей дефектов:

* по кварталам,
* по месяцам.

Специфичные графики:

* Непосредственные причины дефектов.
* Корневые причины дефектов.
* Типы оборудования, где фиксируются дефекты.

## Отчёт «Кристаллизация знаний»

Чтобы провести анализ отказавшего оборудования и определить непосредственные и коренные причины отказа, откройте аналитический интерфейс «Кристаллизация знаний» для построения графа связей между событиями, произошедшими при упоминании одного и того же оборудования.

Отчёт «Кристаллизация знаний» содержит следующие элементы:

* панель ввода данных,
* информационную панель,
* граф связей,
* перечень отчётных документов со ссылками.

Для задания условий построения графа связей введите вручную или выберите из выпадающего списка данные на панели ввода данных, расположенной в левом верхнем углу аналитического интерфейса.

Выберите справочник по упоминанию оборудования для построения графа из выпадающего списка: «ТОИР» или «Дефекты». После чего установите типы событий в графе «Направление», выбирая направления связей. Затем введите станционный номер оборудования, по которому будет устанавливаться связь. Чтобы сформировать отчёт, нажмите «Применить».

После этого система отобразит в правом верхнем углу информационную панель, на которой будет информация по характеристикам выбранного для построения графа оборудования (отображение информационной панели производится системой только при выборе справочника «ТОИР»).

Одновременно с выводом данных на информационной панели в центральной части отчёта система формирует граф связей в виде окружностей, различающихся по цвету, и связей между ними, в зависимости от значений связанных показателей.

В нижней части отчёта содержится перечень отчётных документов по событиям всех направлений, выбранных на панели ввода данных и отображённых на визуализации графа связей. При необходимости можно получить более детальную информацию, кликнув по ссылке, указанной в первом столбце таблицы.

По ссылке откроется выбранный отчёт с цветовым выделением упоминания оборудования, по которому установлена связь.

## Выход из интерфейса NPP Analytics

Чтобы завершить работу с системой, нажмите «Выход» в левом верхнем углу экрана.

# NPP консоль настройки визуализации

## Создание личной пользовательской панели управления

Этот раздел ориентирован на конечных пользователей, которые будут использовать NPP консоль настройки визуализации для анализа и исследования данных (аналитики данных, бизнес-аналитики, специалисты по данным и т.д.).

Это руководство предназначено для тех, кому необходимо создавать диаграммы и информационные панели в NPP, консоли настройки визуализации. Пользователи имеют возможность подключить NPP консоль настройки визуализации к новой базе данных и настроить таблицу в этой базе данных для анализа, изучить предоставленные данные и добавить визуализацию на панель инструментов.

### Подключение к новой базе данных

Сама NPP консоль настройки визуализации не имеет уровня хранения для хранения ваших данных, а вместо этого работает в паре с вашей существующей базой данных или хранилищем данных, использующих язык SQL.

Прежде всего, необходимо добавить учётные данные для подключения к вашей базе данных, чтобы иметь возможность запрашивать и визуализировать данные из неё. Если вы используете NPP консоль настройки визуализации локально, вы можете пропустить этот шаг, потому что база данных Postgres включена и предварительно настроена в NPP консоль настройки визуализации за вас.

В меню «Данные» выберите параметр «Базы данных».

Затем нажмите зелёную кнопку «+ База данных» в правом верхнем углу.

В этом окне можно настроить ряд дополнительных параметров, но обязательно нужно указать только:

* имя базы данных,
* URI SQLAlchemy.

Как сообщается в тексте под URI, вам следует обратиться к документации SQLAlchemy по созданию новых URI подключения для вашей целевой базы данных.

Нажмите на кнопку «Проверить подключение», чтобы убедиться, что всё работает от начала до конца. Если соединение в порядке, сохраните конфигурацию, нажав кнопку «Добавить».

### Регистрация новой таблицы

Теперь вы можете выбрать определённые таблицы («наборы данных» в NPP консоль настройки визуализации), которые вы хотите отобразить в NPP консоли настройки визуализации для запроса.

Перейдите в «Данные» → «Наборы данных» и нажмите кнопку «Набор данных» в правом верхнем углу.

Откроется модальное окно. Выберите «База данных», «Схема», а также «Таблица», используя появившиеся раскрывающиеся списки. В следующем примере мы регистрируем таблицу cleaned\_sales\_data из базы данных.

Для завершения нажмите значок «Добавить» в правом нижнем углу. Теперь вы увидите свой набор данных в списке наборов данных.

### Настройка свойств столбца

Для настройки свойства столбца, отметьте необходимые чекбоксы:

* Временной.
* Фильтруемый.
* Размерный.

И укажите настройки формата данных, если это актуально для столбца.

### Семантический слой

NPP консоль настройки визуализации имеет тонкий семантический слой, который значительно унифицирует и облегчает процессы анализа данных. Семантический уровень может хранить 2 типа вычисленных данных:

1. Виртуальные метрики: вы имеете возможность формировать запросы SQL, которые собирают значения из нескольких столбцов (например, SUM (recovered) / SUM (confirmed) и делать их доступными в виде столбцов для визуализации (например, recovery\_rate) в «Обзоре». Для показателей разрешено и приветствуется использование агрегатных функций.

Вы также имеете возможность сертифицировать показатели, если хотите, чтобы ваша команда использовала это представление.

1. Виртуальные вычисляемые столбцы: вы имеете возможность формировать запросы SQL, которые настраивают внешний вид и поведение определённого столбца (например, CAST (recovery\_rate) as float). В вычисляемых столбцах нельзя использовать агрегатные функции.

### Создание диаграмм в представлении «Обзор»

Существует два основных интерфейса для исследования данных:

* «Обзор»: визуальный конструктор без программирования. Выберите набор данных, выберите диаграмму, настройте внешний вид и опубликуйте.
* SQL Lab: SQL IDE для очистки, объединения и подготовки данных для рабочего процесса «Обзора».

Представление «Обзор» предназначено для создания диаграмм. Чтобы начать рабочий процесс на вкладке «Наборы данных» нажмите на имя набора данных, который будет использоваться в вашей диаграмме.

Теперь вам доступен рабочий процесс для изучения данных и итераций на диаграммах.

* В представлении «Набор данных» слева есть список столбцов и показателей с привязкой к текущему выбранному вами набору данных.
* В области предварительного просмотра «Данные» под областью диаграммы также приводится полезный контекст данных.
* С помощью вкладок «Данные» и «Настроить» вы можете изменить тип визуализации, выбрать временной столбец, выбрать метрику для группировки и настроить внешний вид диаграммы.

При настройке диаграммы с помощью раскрывающихся меню нажмите на кнопку «Запустить», чтобы получить визуальную обратную связь.

### Создание среза и панели управления

Чтобы сохранить диаграмму, нажмите на кнопку «Сохранить». Вы также можете:

* Сохранить диаграмму и добавить её на существующую панель управления.
* Сохранить диаграмму и добавить её на новую панель управления.

Для публикации нажмите «Сохранить и перейти на панель управления».

NPP консоль настройки визуализации создаст срез и сохранит всю информацию, необходимую для создания вашей диаграммы, на своем тонком уровне данных (запрос, тип диаграммы, выбранные параметры, имя и т.д.).

Чтобы изменить размер диаграммы, нажмите на кнопку карандаша в правом верхнем углу.

Затем щёлкните по правому нижнему углу диаграммы и перетаскивайте его, пока макет диаграммы не встанет в нужное положение на основной сетке.

Нажмите «Сохранить», чтобы сохранить изменения.

### Управление доступом к панелям управления

Управление доступом к панелям управления осуществляется через их владельцев (пользователей, у которых есть права на редактирование панели управления).

Доступом для пользователей, не являющихся владельцами, можно управлять двумя способами:

1. Разрешения для набора данных. Если вы добавите к соответствующим ролям разрешения для наборов данных, это автоматически предоставит скрытый доступ ко всем панелям управления, которые используют эти разрешенные наборы данных.
2. Роли панели управления. Если вы установите флажок функции DASHBOARD\_RBAC, то сможете настраивать роли и их доступ к панели управления.

* Наличие доступа к панели управления неявно предоставляет доступ для чтения к связанным наборам данных, поэтому все диаграммы будут загружать свои данные, даже если флаг функции установлен и значение ролей установлено на «роли не назначены», значение доступа вернется к «Разрешения для набора данных».

## Изучение данных

В этой части руководства описаны ключевые концепции NPP консоли настройки визуализации.

### Включение функции загрузки данных

Возможно, вам потребуется включить функцию загрузки файла CSV или Excel в вашу базу данных. В следующем разделе объясняется, как это сделать.

В верхнем меню выберите «Данные» → «Базы данных». Найдите базу данных и нажмите на кнопку «Редактировать».

В появившемся модальном окне перейдите на вкладку «Дополнительно», установите флажок «Разрешить загрузку данных» и нажмите кнопку «Сохранить».

### Загрузка данных CSV

Загрузите набор данных CSV на свой компьютер. В меню NPP консоль настройки визуализации выберите «Данные» → «Загрузить CSV».

Затем введите название в поле «Имя таблицы» и выберите файл CSV на своём компьютере.

Далее введите текст «Дата поездки» в поле «Парсинг дат».

Оставьте для всех остальных параметров значения по умолчанию и выберите «Сохранить» внизу страницы.

### Визуализация таблицы

Теперь вы видите набор данных на вкладке «Наборы данных». Нажмите на запись, чтобы запустить рабочий процесс «Обзор» с использованием этого набора данных.

В этом разделе мы создадим визуализацию таблицы.

По умолчанию NPP консоль настройки визуализации Apache показывает данные только за последнюю неделю. Чтобы посмотреть все данные, откройте раздел «Время» → «Временной диапазон» и измените «Тип диапазона» на «Без фильтра».

Нажмите «Применить» для сохранения.

Теперь нужно указать строки в таблице, используя параметр «Группировать по». Затем можно указать метрики для отображения в таблице с помощью опции «Метрики».

* COUNT — количество строк в таблице.
* SUM (Cost) — общая сумма.

Выберите «Выполнить запрос», чтобы увидеть результаты в таблице.

Чтобы сохранить визуализацию, нажмите «Сохранить» в верхнем левом углу экрана. В следующем модальном меню:

* выберите опцию «Сохранить как» и введите имя диаграммы (вы сможете найти её снова на экране «Диаграммы», доступном через верхнее меню);
* выберите «Добавить на панель управления» и войдите в Учебную панель управления. Выберите «Сохранить и перейти на панель управления».

### Основы работы с панелью управления

Откройте интерфейс панели управления, выбрав «Панели управления» в верхнем меню, а затем «Учебную панель управления» из списка панелей управления.

На этой панели управления вы увидите таблицу, созданную в предыдущем разделе. Выберите «Редактировать панель управления», а затем наведите курсор на таблицу. Потянув правый нижний угол таблицы, вы можете изменить размер таблицы.

Сохраните изменения.

### Сводная таблица

В этом разделе описан расширенный анализ с помощью более сложной визуализации — сводной таблицы.

Создайте новую диаграмму, выбрав «+» → «Диаграмма» в правом верхнем углу. Снова выберите источник данных, затем щёлкните тип визуализации для перехода в меню визуализации. Выберите «Сводная таблица» (вы можете фильтровать список, вводя текст в поле поиска), а затем «Создать новую диаграмму».

В разделе «Время» оставьте столбец времени, затем выберите месяц в качестве параметра «Детализации времени», так как ежедневные данные будут слишком подробными, чтобы увидеть закономерности. Затем выберите временной диапазон.

Далее в разделе «Запрос» удалите COUNT по умолчанию и добавьте Cost, сохранив агрегат SUM по умолчанию. Обратите внимание, что NPP консоль настройки визуализации Apache будет обозначать тип метрики символом в левом столбце списка (ABC для строки, # для числа, циферблат для времени и т.д.).

В опции «Группировать по» выберите «Время»: это приведёт к автоматическому использованию выбора столбца времени и детализации времени.

Выберите столбцы и нажмите «Выполнить запрос», чтобы увидеть данные.

### Линейная диаграмма

В этом разделе описано создание линейной диаграммы.

В разделе «Время» оставьте столбец времени, а в «Детализации времени» — месяц, но на этот раз в качестве «Временного диапазона» выберите «Без фильтра» (No filter), чтобы просмотреть весь набор данных.

В Метриках удалите метрику по умолчанию COUNT и вместо этого добавьте AVG (Cost), чтобы показать среднее значение.

Далее выберите «Выполнить запрос» для отображения данных на графике.

Перейдите на вкладку «Настройка» на левой панели и измените цветовую схему, удалив фильтр диапазона, выбрав «Нет» в раскрывающемся списке «Показать фильтр диапазона» и добавив несколько меток с помощью метки оси X и метки оси Y.

Когда закончите, опубликуйте диаграмму на своей учебной панели управления.

### Разметка

В этом разделе описано, как добавить текст на панель управления. Откройте «Панели управления» в верхнем меню, а затем «Учебную панель управления» из списка. Перейдите в режим редактирования, выбрав «Редактировать панель управления».

На панели «Вставить компоненты» перетащите поле Markdown на панель управления. Обратите внимание на синие линии, обозначающие точку привязки, в которую будет помещено поле.

Теперь, чтобы отредактировать текст, установите флажок. Вы можете ввести текст в формате Markdown. Вы можете переключаться между редактированием и предварительным просмотром, используя меню в верхней части окна.

Для выхода выберите любую другую часть панели инструментов.

### Поле фильтра

В этом разделе описано, как добавить фильтр на панель управления.

Визуализацию поля фильтров можно создать, как и любую другую визуализацию, выбрав «+» → «Диаграмма», а потом источник данных и «Поле фильтра» как тип визуализации.

В разделе «Время» очистите фильтры из списка «Временной диапазон».

Далее в «Конфигурации фильтров» сначала добавьте новый фильтр, нажав значок плюса, а затем отредактируйте вновь созданный фильтр, нажав на значок карандаша.

Выберите столбец и нажмите «Выполнить запрос». Это позволяет предварительно просматривать результаты фильтрации.

Затем удалите фильтр и нажмите «Сохранить».

Назовите диаграмму «Учебный фильтр», добавьте её на существующую панель управления «Учебная панель управления», а затем нажмите «Сохранить и перейти на панель управления». Оказавшись на приборной управления, попробуйте использовать фильтр. Фильтр применится ко всем другим визуализациям на панели управления.

### Публикация панели управления

Вы можете переставить элементы панели управления, выбрав «Редактировать панель управления» и перетащив элементы.

Если вы хотите сделать свою панель управления доступной для других пользователей, выберите «Черновик» рядом с заголовком панели инструментов в левом верхнем углу, чтобы изменить её состояние на «Опубликована». Вы можете добавить эту панель в избранное, нажав на звёздочку.

### Аннотации

Аннотации позволяют добавить к вашей диаграмме дополнительный контекст.

Добавьте слой аннотации, перейдя в «Управление» → «Слои аннотации». Добавьте новый слой аннотаций, нажав на зелёный знак плюса. Введите название и сохраните его. Этот слой можно использовать для ссылки на ряд различных аннотаций.

Затем добавьте аннотацию, перейдя в «Управление» → «Аннотации», а затем создайте новую аннотацию, нажав на зелёный знак плюса. Затем выберите только что созданный слой и добавьте краткое описание.

Затем перейдите к линейной диаграмме, открыв в «Диаграммы» и выбрав «Учебная линейная диаграмма» из списка.

Затем перейдите в раздел «Аннотации и слои» и выберите «Добавить слой аннотации». В этом диалоговом окне:

* Назовите слой.
* Измените тип слоя аннотации на «Событие».
* Задайте источник аннотации как аннотацию NPP консоли настройки визуализации.
* Укажите в качестве слоя аннотации созданный слой.

Нажмите Применить, чтобы увидеть свою аннотацию на диаграмме.

При желании вы можете настроить внешний вид аннотации, изменив настройки в разделе «Настройка отображения». В противном случае нажмите ОК и «Сохранить», чтобы сохранить график. Если вы оставите выбор по умолчанию для перезаписи диаграммы, ваша аннотация будет сохранена в диаграмме и также автоматически появится на Учебной панели управления.

### Расширенная аналитика

Функция «Расширенная аналитика» позволяет применять дополнительные преобразования к данным.

#### Настройка базовой диаграммы

Создайте новую диаграмму, используя тот же источник данных и тип визуализации «Линейная диаграмма».

Выберите «Выполнить запрос», чтобы показать диаграмму.

Вы увидите общие данные за каждый месяц.

Сохраните визуализацию как «Учебная аналитическая основа», добавив её в «Учебную панель управления».

### Скользящее среднее

Если данные довольно сильно различаются, это затрудняет выявление тенденции. Один из подходов, который можно использовать, — это показать вместо этого скользящее среднее временного ряда. Для этого в подразделе «Скользящее среднее» раздела «Расширенная аналитика», выберите среднее в поле «Скользящее» и введя 7 в поля «Периоды» и «Минимальные периоды». Период — это длина скользящего периода, кратная детализации времени. В нашем примере детализация времени — это день, поэтому скользящий период составляет 7 дней. Указав в поле «Минимальные периоды» значение 7, мы гарантируем, что среднее значение всегда будет рассчитываться за 7 дней, и избегаем любого периода нарастания.

После отображения диаграммы, выбрав «Выполнить запрос», вы увидите, что данные менее изменчивы и что серия начинается позже, поскольку период нарастания исключён.

Сохраните диаграмму как «Учебное скользящее среднее» и добавьте его на «Учебную панель управления».

### Сравнение времени

В этом разделе мы сравним значения в нашем временном ряду со значением за неделю до этого. Сначала откройте диаграмму «Учебная расширенная аналитическая основа», перейдя в «Диаграммы» в верхнем меню, а затем выберите имя визуализации в списке (можно также найти диаграмму на «Учебной панели инструментов» и выбрать «Обзор диаграммы» в меню этой визуализации).

Затем в подразделе «Сравнение времени» раздела «Расширенная аналитика», укажите сдвиг по времени «минус 1 неделя» (обратите внимание, что это поле принимает ввод данных на естественном языке). Выполните запрос, чтобы увидеть новую диаграмму, на которой есть дополнительные ряды с теми же значениями, сдвинутыми на неделю назад во времени.

Затем измените «Тип расчета» на «Абсолютная разница и выберите «Выполнить запрос». Теперь снова видно только одну серию, на этот раз показывающую разницу между двумя сериями, которые мы видели ранее.

Сохраните диаграмму как «Учебное сравнение времени» и добавьте её на «Учебную панель управления».

### Повторная выборка данных

В этом разделе изменим выборку данных, чтобы вместо ежедневных данных получить еженедельные данные. Как и в предыдущем разделе, снова откройте диаграмму «Учебная расширенная аналитическая основа».

Затем в подразделе «Функции Python» раздела «Расширенная аналитика» введите 7D, что соответствует семи дням, в «Правиле» и медиане в качестве «Метода» и отобразите диаграмму, выбрав «Выполнить запрос».

Обратите внимание, что теперь есть одна точка данных каждые 7 дней. В этом случае показанное значение соответствует среднему значению в пределах семи дневных точек данных.

Сохраните диаграмму как «Учебная повторная выборка» и добавьте её на «Учебную панель управления». Перейдите на «Учебную панель управления», чтобы увидеть четыре диаграммы рядом и сравнить разные результаты.

# NPP консоль управления правами

## Создание реалма и пользователя

Чтобы начать работать с консолью управления правами, создайте реалм и администратора в этом реалме. Войдите в созданный реалм, используя логин и пароль администратора, и откройте встроенную консоль учётной записи, к которой имеют доступ все пользователи.

### Реалм и пользователи

Когда вы входите в консоль администратора, вы работаете в реалме, который представляет собой пространство, где вы управляете объектами.

Существуют два типа реалмов:

* Главный реалм — этот реалм был создан, когда вы впервые запустили NPP консоль управления правами. Он содержит учётную запись администратора, которую вы создали при первом входе в систему. Вы используете этот реалм только для создания других реалмов.
* Другие реалмы — эти реалмы создаются администратором в главном реалме. В этих реалмах администраторы создают пользователей и приложения. Приложения принадлежат пользователям.

### Создание реалма

Как администратор в главном реалме, вы можете создать реалмы, в которых администраторы создают пользователей и приложения. Для этого:

1. Войдите в консоль администратора NPP консоли управления правами, используя учётную запись администратора.
2. В меню главного реалма нажмите «Добавить реалм». После входа в главный реалм в этом меню будет перечислены все остальные реалмы.
3. Заполните название реалма. Обратите внимание, что поле чувствительно к регистру.
4. Нажмите «Создать». Откроется главная страница административной консоли.
5. Переключайтесь между управлением главным реалмом и реалмом, который вы только что создали, с помощью списка «Выбрать реалм».

### Создание пользователя

Чтобы создать пользователя:

1. Откройте пункт меню «Пользователи» и нажмите кнопку «Добавить пользователя».
2. Введите имя в поле «Имя пользователя».
3. Переключите переключатель «Электронная почта подтверждена» в положение «Вкл.» и нажмите «Сохранить». Откроется страница управления для нового пользователя.
4. Нажмите на вкладке «Учётные данные», чтобы установить временный пароль для нового пользователя.
5. Введите новый пароль и подтвердите его.
6. Нажмите «Установить пароль».

Этот пароль является временным, и пользователю потребуется изменить его при первом входе в систему. Если вы хотите создать постоянный пароль, переведите переключатель «Временный» в положение «Выкл.» и нажмите «Установить пароль».

### Вход в консоль учётной записи

Каждый пользователь в реалме имеет доступ к консоли учётной записи. В этой консоли можно обновлять информацию профиля и изменения учётных данных. Теперь вы можете протестировать вход в систему с этим пользователем в созданном вами реалме.

1. Выйдите из консоли администратора, открыв меню пользователя и выбрав «Выход».
2. Перейдите по адресу консоли и войдите в свой демонстрационный реалм как пользователь, которого вы только что создали.
3. Введите новый пароль. Откроется консоль учётной записи.
4. Заполните обязательные поля.

## Управление сессией пользователя

Когда пользователь входит в реалм, NPP консоль управления правами поддерживает для него сессию пользователя и запоминает каждого клиента, которого он посетил в течение сессии.

В пользовательских сессиях администраторы реалма могут:

* просматривать статистику входа в систему для всего реалма,
* детально просматривать сведения о каждом клиенте, чтобы увидеть, кто и где вошел в систему.

Администраторы могут завершить сессию пользователя или группы пользователей. Они могут отзывать токены и устанавливать все таймауты токенов и сессий.

### Администрирование сессий

В пункте меню «Сессии» вы увидите список клиентов и количество активных сессий для этого клиента в настоящее время. Вы можете вывести из системы всех пользователей в реалме, нажав кнопку «Разлогинить все сессии» в правой части этого списка.

#### Детализация приложения

На странице «Сессии» вы можете подробно просмотреть каждого клиента, открыв вкладку «Сессии» этого клиента. Нажав кнопку «Показать сессии», вы увидите, какие пользователи вошли в это приложение.

#### Детализация пользователей

Информацию о сессии можно посмотреть на вкладке «Сессии» отдельного пользователя.

### Политика отзыва

Если вашу систему взломали, вы можете завершить все сессии и отозвать токены доступа. Для этого перейдите на вкладку «Отзыв» на экране «Сессии».

Установите дату, когда ваша система была взломана, и все токены, выпущенные до этого времени, а также все сессии, начатые до этого времени, станут недействительными.

Команда «Установить на сейчас» установит текущее время и дату.

### Таймауты сессии и токена

NPP консоль управления правами предоставляет вам возможность контроля таймаутов сессии, файлов cookie и токенов. Настроить их можно на вкладке «Токены» в пункте «Настройки реалма».

* Алгоритм подписи по умолчанию — алгоритм, который используется для назначения токенов этому реалму.
* Отзыв токена обновления — дДля клиентов, которые выполняют процедуру обновления токенов, эта опция, если она отмечена, отменит этот токен обновления и выдаст другой токен с запросом, который нужно использовать клиенту. В результате каждый токен обновления используется только один раз.
* Бездействие в сессии единого входа (SSO) — если пользователь неактивен дольше этого времени, сессия пользователя будет закрыта. Таймаут бездействия сбрасывается клиентом, запрашивающим аутентификацию, или запросом на обновление токена. Существует небольшое временное окно, которое всегда добавляется к таймауту бездействия, прежде чем сессия будет закрыта.
* Максимальное количество сессий единого входа (SSO) — максимальное время, по истечении которого срок сессии пользователя истечёт и он станет недействительным. Этот параметр определяет максимальное время, в течение которого сессия пользователя может оставаться активной, независимо от активности пользователя.
* Бездействие в сессии единого входа (SSO) «Запомнить меня» — то же, что и стандартная конфигурация бездействия в сессии единого входа (SSO), но касающаяся конкретно входа в систему с включённой функцией «Запомнить меня». Она позволяет указать более длительные таймауты бездействия в сессии, когда во время входа в систему выбрано «Запомнить меня». Это необязательная конфигурация, и если не установлено значение больше 0, используется тот же таймаут простоя, который установлен в конфигурации ожидания сессии единого входа.
* Максимальное количество сессий единого входа «Запомнить меня» — то же, что и стандартное максимальное количество сессий единого входа (SSO), но только для учётных записей с включённой функцией «Запомнить меня». Эта опция позволяет указывать более длительные сессии, когда во время входа в систему выбрано «Запомнить меня». Это необязательная конфигурация, и если не задано значение больше 0, используется тот же срок существования сессии, который задан в конфигурации параметра «Максимум сессии единого входа (SSO).
* Бездействие в автономной сессии — для автономного доступа это время, в течение которого сессии разрешено оставаться в режиме ожидания до того, как токен автономного режима будет отозван. Существует небольшое временное окно, которое всегда добавляется к таймауту бездействия, прежде чем сессия будет закрыта.
* Максимальное количество автономных сессий ограничено — при автономном доступе, если установлена отметка этой опции, включается параметр «Максимум автономной сессии» для управления максимальным временем, в течение которого токен автономного режима может оставаться активным, независимо от активности пользователя. Также включены параметры «Бездействие в автономной сессии клиента» и «Максимум автономной сессии клиента».
* Максимум автономной сессии — при автономном доступе это максимальное время, по истечении которого соответствующий токен автономного режима будет отозван. Этот параметр определяет максимальное время, в течение которого токен автономного режима может оставаться активным, независимо от активности пользователя.
* Бездействие в автономной сессии клиента — при автономном доступе, если пользователь неактивен дольше этого времени, запросы токенов автономного режима увеличат таймаут бездействия. Это позволяет указать более короткий таймаут бездействия для токена автономного режима, чем таймаут бездействия в автономной сессии. Однако его можно переопределить для отдельных клиентов. Это необязательная конфигурация, и если не установлено значение больше 0, используется тот же таймаут простоя, который установлен в конфигурации бездействия автономной сессии.
* Максимум автономной сессии клиента — при автономном доступе это максимальное время, по истечении которого срок токена автономного режима истечёт и токен станет недействительным. Это позволяет указать более короткий таймаут токена автономного режима, чем таймаут автономной сессии. Однако его можно переопределить для отдельных клиентов. Это необязательная конфигурация, и если не установлено значение больше 0, используется тот же таймаут простоя, который установлен в конфигурации максимума автономной сессии.
* Бездействие в клиентскую сессию — если пользователь неактивен дольше этого времени, запросы токенов обновления увеличат таймаут простоя. Это позволяет указать более короткий таймаут бездействия токена обновления, чем таймаут бездействия сессии. И его можно переопределить для отдельных клиентов. Это необязательная конфигурация, и если не установлено значение больше 0, используется тот же таймаут простоя, который установлен в конфигурации бездействия сессии единого входа (SSO).
* Максимум клиентской сессии — максимальное время, по истечении которого токен обновления истечёт и станет недействительным. Это позволяет указать более короткий таймаут токена обновления, чем таймаут бездействия сессии. И его можно переопределить для отдельных клиентов. Это необязательная конфигурация, и если не установлено значение больше 0, используется тот же таймаут простоя, который установлен в конфигурации максимума сессии единого входа (SSO).
* Срок действия токена доступа — когда создаётся токен доступа OIDC, это значение влияет на срок действия.
* Срок службы токена доступа для неявного потока — при использовании неявного потока токен обновления не предоставляется. По этой причине существует отдельный таймаут для токенов доступа, созданных с помощью неявного потока.
* Таймаут входа клиента — максимальное время, в течение которого клиент должен завершить поток с кодом подтверждения в OIDC.
* Таймаут входа в систему — общее время, необходимое для входа в систему. Если аутентификация занимает больше времени, чем указанное время, пользователю придется начать процесс аутентификации заново.
* Таймаут действия входа в систему — максимальное время, которое пользователь может провести на любой странице в процессе аутентификации.
* Продолжительность действия, инициированного пользователем — максимальное время до истечения срока действия разрешения на действие, отправленное пользователем (например, электронное письмо о забытом пароле). Рекомендуется, чтобы это значение было небольшим, поскольку ожидается, что пользователь быстро отреагирует на самостоятельно созданное действие.
* Продолжительность действия по умолчанию, инициированного администратором — максимальное время до истечения срока действия разрешения на действие, отправленного пользователю администратором. Рекомендуется, чтобы это значение было большим, чтобы администраторы могли отправлять электронные письма пользователям, которые в настоящее время не подключены к интернету. Таймаут по умолчанию можно изменить прямо перед выпуском токена.
* Переопределить продолжительность действия, инициированного пользователем — позволяет иметь независимые таймауты для каждой операции (например, проверка электронной почты, забытый пароль, действия пользователя и проверка электронной почты поставщика удостоверений). Это поле необязательно для заполнения. Если ничего не указано, по умолчанию используется значение, настроенное в поле «Продолжительность действия, инициированного пользователем».

Для таймаутов бездействия существует небольшое временное окно (2 минуты), в течение которого срок сессии не истекает. Например, если у вас установлен таймаут 30 минут, фактически до истечения сессии будет 32 минуты.

## Объединение хранилищ пользователей

У многих компаний есть базы данных пользователей, в которых хранится информация о пользователях и их паролях или других учётных данных. Во многих случаях невозможно перейти с этих существующих хранилищ на чистое развертывание NPP консоли управления правами. Но NPP консоль управления правами может объединять существующие внешние пользовательские базы данных. По умолчанию поддерживается LDAP и Active Directory, но вы также можете создать собственное расширение для любой пользовательской базы данных.

Это работает так: когда пользователь входит в систему, NPP консоль управления правами просматривает собственное внутреннее хранилище пользователей, чтобы найти пользователя. Если она не может найти его там, она будет перебирать всех поставщиков хранилища пользователей, которые вы настроили для реалма, пока не найдёт совпадение. Данные из внешнего хранилища собираются в общую пользовательскую модель, которая используется средой выполнения NPP консоли управления правами. Затем эту общую пользовательскую модель можно сопоставить с токенами и атрибутами SAML.

Внешние пользовательские базы данных редко содержат все данные, необходимые для поддержки всех функций NPP консоли управления правами. Таким образом, поставщик пользовательского хранилища может выбрать локальное сохранение некоторых объектов в пользовательском хранилище NPP консоли управления правами. Некоторые поставщики даже импортируют пользователя локально и периодически синхронизируют с внешним хранилищем. Такой подход зависит от возможностей поставщика и того, как он настроен. Например, ваше внешнее хранилище пользователей может не поддерживать OTP. В зависимости от поставщика этот OTP может обрабатываться и храниться NPP консолью управления правами.

### Добавление поставщика

Чтобы добавить поставщика хранилища, перейдите в пункт левого меню «Федерация пользователей» в консоли администратора.

Из выпадающего списка «Добавить поставщика» выберите тип поставщика, откроется страница конфигурации этого поставщика.

### Работа со сбоями поставщика

Если у поставщика хранилища пользователей происходит сбой (например, ваш сервер LDAP не работает), у вас могут возникнуть проблемы со входом в систему, и вы не сможете просматривать пользователей в консоли администратора. NPP консоль управления правами не обнаружит сбой при использовании поставщика хранилища для поиска пользователя, и это прервет вызов. Таким образом, если у вас есть поставщик хранилища с более высоким приоритетом, который не работает во время поиска пользователя, вход в систему или запрос пользователя полностью завершится с исключением и прервётся. Он не перейдёт к следующему настроенному поставщику.

Сначала всегда просматривается локальная база данных пользователей NPP консоли управления правами, а затем в LDAP или у настраиваемого поставщика хранилища пользователей.

Возможно, вы захотите создать учётную запись администратора, которая хранится в локальной базе данных пользователей NPP консоли управления правами, на случай, если возникнут какие-либо проблемы при подключении к вашему LDAP и настраиваемым серверам.

У каждого LDAP и настраиваемого поставщика хранилища пользователей есть переключатель «включить» на странице консоли администратора.

Отключение поставщика хранилища пользователей приведёт к пропуску поставщика при выполнении пользовательских запросов, чтобы вы могли просматривать пользователей, которые могут храниться у другого поставщика с более низким приоритетом, и входить в систему с их помощью.

Если ваш поставщик использует стратегию импорта и вы отключите её, импортированные пользователи по-прежнему будут доступны для поиска, но в режиме только для чтения. Вы не сможете изменить этих пользователей, пока снова не включите поставщика.

Причина, по которой NPP консоль управления правами не переключается при сбое при поиске поставщика хранилища, заключается в том, что пользовательские базы данных часто имеют повторяющиеся имена пользователей или одинаковые электронные почты. Это может вызвать проблемы с безопасностью и непредвиденные проблемы, поскольку пользователь может быть загружен из одного внешнего хранилища, когда администратор ожидает загрузки пользователя из другого.

### LDAP и Active Directory

NPP консоль управления правами поставляется со встроенным поставщиком LDAP/AD. Можно объединить несколько разных серверов LDAP в один и тот же реалм NPP консоли управления правами. Вы можете отобразить атрибуты пользователя LDAP в общей пользовательской модели NPP консоли управления правами. По умолчанию она хранит имя пользователя, адрес электронной почты, имя и фамилию, но вы можете настроить дополнительные поля. Поставщик LDAP также поддерживает проверку пароля через протоколы LDAP/AD и различные режимы хранения, редактирования и синхронизации.

Чтобы настроить объединенное хранилище LDAP, перейдите в консоль администратора. Нажмите на пункт «Федерация пользователей» в левом меню. Откроется страница со списком «Добавить поставщика». Выберите ldap, откроется страница конфигурации LDAP.

#### Режим хранилища

По умолчанию NPP консоль управления правами импортирует пользователей из LDAP в свою локальную базу данных пользователей. Эта копия пользователя синхронизируется либо по запросу, либо с помощью периодического выполнения фоновой задачи. Единственное исключение — синхронизация паролей. Пароли никогда не импортируются. Их проверка всегда делегируется серверу LDAP. Преимущества этого подхода в том, что все функции NPP консоли управления правами будут работать, поскольку любые дополнительные необходимые данные для каждого пользователя могут храниться локально. Недостатком этого подхода является то, что каждый раз, когда конкретный пользователь запрашивается в первый раз, выполняется соответствующая вставка в базу данных NPP консоли управления правами. Импорт также может потребовать синхронизацию с вашим сервером LDAP. Однако синхронизация импорта не требуется, если мапперы LDAP сконфигурированы так, чтобы всегда считывать определённые атрибуты из LDAP, а не из базы данных.

Кроме того, вы можете отказаться от импорта пользователей в базу данных пользователей NPP консоли управления правами. В этом случае стандартная пользовательская модель, которую использует среда выполнения NPP консоли управления правами, поддерживается только сервером LDAP. Это означает, что если LDAP не поддерживает часть данных, которая нужна функции NPP консоли управления правами, эта функция не будет работать. Преимущество этого подхода заключается в том, что у вас не возникает непроизводительных издержек на импорт и синхронизацию копии пользователя LDAP в базу данных пользователей NPP консоли управления правами.

Этот режим хранения контролируется переключателем «Импортировать пользователей». Для импорта установите его в положение «Вкл.».

Если импорт пользователей отключён, вы не можете сохранять атрибуты профиля пользователя в базе данных NPP консоли управления правами. Также вы не можете сохранять метаданные, за исключением метаданных профиля пользователя, которые сопоставлены LDAP. Сюда могут входить сопоставления ролей, сопоставления групп и другие метаданные на основе конфигурации ваших мапперов LDAP. Когда вы попытаетесь изменить некоторые данные пользователя, не сопоставленные с LDAP, обновление пользователя будет невозможно. Например, вы не сможете отключить сопоставленного пользователя LDAP, если включённый флаг пользователя сопоставляется с некоторым атрибутом LDAP (что обычно не так).

#### Режим редактирования

Пользователи с помощью службы учётной записи пользователя, а администраторы с помощью консоли администратора могут изменять метаданные пользователя. В зависимости от ваших настроек вы можете иметь или не иметь права на обновление LDAP. В режиме редактирования параметр конфигурации определяет политику редактирования вашего хранилища LDAP. Варианты режимов:

* Только чтение. Имя пользователя, адрес электронной почты, имя, фамилия и другие сопоставленные атрибуты нельзя будет изменить. NPP консоль управления правами будет показывать ошибку каждый раз, когда кто-нибудь попытается изменить эти поля. Также не будет поддерживаться изменение паролей.
* Режим редактирования. Имя пользователя, адрес электронной почты, имя, фамилия и другие сопоставленные атрибуты и пароли могут быть обновлены и будут автоматически синхронизированы с вашим хранилищем LDAP.
* Без синхронизации. Любые изменения имени пользователя, электронной почты, имени, фамилии и паролей будут храниться в локальном хранилище NPP консоли управления правами. Вы сами решаете, как выполнить синхронизацию с LDAP. Это позволяет развертываниям NPP консоли управления правами поддерживать обновления пользовательских метаданных на сервере LDAP только для чтения. Этот параметр применяется только при импорте пользователей из LDAP в локальную базу данных пользователей NPP консоли управления правами.

Когда создается поставщик LDAP, также создаётся набор начальных мапперов LDAP. Мапперы настраиваются по принципу «максимальных усилий» на основе выбранной комбинации переключателей «Поставщик», «Режим редактирования», а также «Импортировать пользователей». Например, в случае с режимом редактирования «без синхронизации» мапперы предварительно сконфигурированы таким образом, что определённый пользовательский атрибут в предпочтительном порядке считывается из базы данных, а не из LDAP. Однако, когда вы позже измените режим редактирования, конфигурация мапперов не изменится, так как сложно определить, были ли они изменены вручную за это время. Это означает, что НЕ рекомендуется изменять положение переключателя «Режим редактирования», а лучше всегда выбирать «Режим редактирования» при создании поставщика LDAP. Это относится также к переключателю «Импортировать пользователей».

#### Другие параметры конфигурации

* Имя в консоли — имя, используемое, когда этот поставщик упоминается в консоли администратора.
* Приоритет — приоритет этого поставщика при поиске или добавлении пользователя.
* Синхронизация регистраций — если ваш LDAP поддерживает добавление новых пользователей, нажмите на этот переключатель, чтобы новые пользователи, созданные NPP консолью управления правами в консоли администратора или на странице регистрации, добавлялись в LDAP.

#### Подключение к LDAP через SSL

Когда вы настраиваете защищенный URL-адрес подключения к вашему хранилищу LDAP, NPP консоль управления правами будет использовать SSL для связи с сервером LDAP. Важно правильно настроить хранилище доверенных сертификатов на стороне сервера NPP консоли управления правами, иначе консоль не сможет доверять SSL-соединению с LDAP.

Глобальное хранилище доверенных сертификатов для NPP консоли управления правами можно настроить с помощью Truststore SPI. Если вы не укажете SPI хранилища доверенных сертификатов, хранилище доверенных сертификатов будет использовать механизм по умолчанию, предоставляемый Java (либо файл, предоставленный системным свойством javax.net.ssl.trustStore либо файл cacerts из JDK, если системное свойство не установлено).

В конфигурации есть свойство «Использовать Truststore SPI», где вы можете выбрать, будет ли использоваться Truststore SPI. По умолчанию это значение «Только для ldaps», что подходит для большинства развёртываний. SPI хранилища доверенных сертификатов будет использоваться только в том случае, если URL-адрес подключения к LDAP начинается с ldaps.

#### Синхронизация пользователей LDAP с NPP консоли управления правами

Если вы включите опцию «Импортировать пользователей», поставщик LDAP автоматически синхронизирует (импортирует) необходимых пользователей LDAP в локальную базу данных NPP консоли управления правами. Когда пользователи входят в систему, поставщик LDAP импортирует пользователя LDAP в базу данных NPP консоли управления правами, а затем аутентифицируется по паролю LDAP. Это единственный раз, когда импортируются пользователи. Если вы перейдёте в меню «Пользователи» и нажмёте «Просмотреть всех пользователей», то увидите только тех пользователей LDAP, которые хотя бы один раз прошли аутентификацию с помощью NPP консоли управления правами. Это реализовано таким образом, что эта операция не запускает импорт всей базы данных пользователей LDAP.

Если вы хотите синхронизировать всех пользователей LDAP с базой данных NPP консоли управления правами, вы можете настроить и включить настройки синхронизации на странице конфигурации поставщика LDAP.

Существует два типа синхронизации:

* Периодическая полная синхронизация.
* Этот тип синхронизирует всех пользователей LDAP с базой данных NPP консоли управления правами. Те пользователи LDAP, которые уже существуют в NPP консоли управления правами и были изменены непосредственно в LDAP, будут обновлены в базе данных консоли.
* Синхронизация периодически изменяемых пользователей.
* При синхронизации будут обновлены или импортированы только те пользователи, которые были созданы или обновлены после последней синхронизации.

Лучший способ выполнить синхронизацию — нажать кнопку «Синхронизировать всех пользователей» при первом создании поставщика LDAP, а затем настроить периодическую синхронизацию изменённых пользователей.

#### Мапперы LDAP

Мапперы LDAP — это «слушатели», которые запускаются поставщиком LDAP в различных точках и обеспечивают ещё одну точку расширения для интеграции LDAP. Они запускаются, когда пользователь входит в систему через LDAP и должен быть импортирован, когда NPP консоль управления правами инициирует регистрацию или когда пользователя запрашивают из консоли администратора. Когда вы создаёте поставщика объединения LDAP, NPP консоль управления правами автоматически предоставит набор встроенных мапперов для этого поставщика. Вы можете изменить этот набор и создать новый маппер, а также обновить или удалить существующие.

* Маппер атрибутов пользователя.
* Он позволяет указать, какой атрибут LDAP сопоставлен с каким атрибутом пользователя NPP консоли управления правами. Так, например, вы можете настроить сопоставления атрибута LDAP «почта» (mail) c атрибутом эл. почта (email) в базе данных NPP консоли управления правами. Для этой реализации маппера всегда существует сопоставление «один-к-одному» (один атрибут LDAP сопоставляется с одним атрибутом NPP консоли управления правами).
* Маппер FullName (Полное имя).
* Он позволяет указать, что полное имя пользователя, которое сохраняется в каком-либо атрибуте LDAP (обычно cn), будет сопоставлено с атрибутами firstName и lastname в базе данных NPP консоли управления правами. Наличие полного имени пользователя в cn часто встречается в некоторых развертываниях LDAP.
* При регистрации новых пользователей в NPP консоли управления правами и включённом параметре «Синхронизация регистраций» для поставщика LDAP, маппер fullName допускает возможность возврата к имени пользователя. Этот резервный вариант особенно полезен в случае с Microsoft Active Directory. Обычная настройка MSAD — настроить атрибут LDAP cn как fullName и в то же время cn обычно используется как атрибут RDN LDAP в конфигурации поставщика LDAP. При такой настройке будет использоваться возврат к имени пользователя. Например, когда вы создаёте пользователя «john123» в NPP консоли управления правами и оставляете поля firstName и lastName пустыми, тогда маппер полного имени сохранит «john123» в качестве значения cn в LDAP. Когда вы позже введёте «John Doe» в качестве firstName и lastName, маппер полного имени обновит LDAP. cn на значение «John Doe», поскольку резервный вариант имени пользователя больше не потребуется.
* Маппер жёстко заданных атрибутов.
* Этот маппер добавляет жёстко заданное значение атрибута каждому пользователю NPP консоли управления правами, связанному с LDAP.
* Этот маппер также может принудительно установить значения для свойств пользователя «включено» (enabled) или «почта подтверждена» (emailVerified).
* Маппер ролей.
* Он позволяет настраивать сопоставления ролей из LDAP в качестве сопоставления ролей NPP консоли управления правами. Один маппер ролей может использоваться для сопоставления ролей LDAP (обычно групп из определенной ветви дерева LDAP) и преобразования их в роли, соответствующие либо ролям реалма, либо ролям клиента. Можно настроить несколько мапперов ролей для одного и того же поставщика LDAP. Так, например, вы можете указать, что сопоставления ролей из групп в ou=main, dc=example, dc=org будут сопоставлены сопоставлениям ролей реалма и сопоставления ролей из групп ниже ou=finance, dc=example, dc=org будут сопоставлены с сопоставлениями ролей клиента finance.
* Маппер жёстко заданных ролей.
* Этот маппер предоставляет указанную роль NPP консоли управления правами каждому пользователю консоли от поставщика LDAP.
* Маппер групп.
* Этот маппер позволяет сопоставлять группы LDAP из определённой ветви дерева LDAP с группами в NPP консоли управления правами. Он также будет распространять сопоставления групп пользователей из LDAP в сопоставления групп пользователей в NPP консоли управления правами.
* Маппер учётных записей пользователей MSAD.
* Этот маппер используется только с Microsoft Active Directory (MSAD). Он может тесно связать состояние учётной записи пользователя MSAD с состоянием учётной записи NPP консоли управления правами (учётная запись включена, срок действия пароля истёк и т.д.). Он использует userAccountControl и атрибуты LDAP wdLastSet, которые специфичны для MSAD и не являются стандартом LDAP. Например, если pwdLastSet равен 0, пользователь NPP консоли управления правами должен обновить свой пароль, и для этого пользователя будет добавлено обязательное действие UPDATE\_PASSWORD. Если userAccountControl равен 514 (отключённая учётная запись), пользователь NPP консоли управления правами также отключён.
* Маппер сертификатов.
* Этот маппер предназначен для сопоставления сертификатов X.509. Обычно он используется вместе с аутентификацией X.509 и Полным сертификатом в формате PEM как источником удостоверения. Он ведёт себя так же, как и маппер атрибутов пользователя, но позволяет NPP консоли управления правами фильтровать атрибут LDAP, который хранит сертификат в формате PEM или DER. Обычно рекомендуется включать параметр «Всегда считывать значение из LDAP» (Always Read Value From LDAP) с этим маппером.

По умолчанию существуют мапперы атрибутов пользователя, которые сопоставляют основные атрибуты пользователя NPP консоли управления правами, такие как имя пользователя, имя, фамилия и адрес электронной почты, с соответствующими атрибутами LDAP. Вы можете расширить их и предоставить дополнительные сопоставления атрибутов. В консоли администратора есть всплывающие подсказки, которые помогут настроить соответствующие мапперы.

#### Хеширование паролей

Когда пароль пользователя обновляется из NPP консоли управления правами и отправляется в LDAP, он всегда отправляется в виде обычного текста, в отличие от обновления пароля во встроенной базе данных NPP консоли управления правами, когда к паролю перед отправкой в базу данных применяется хеширование и обработка. В случае LDAP NPP консоль управления правами использует сервер LDAP для обеспечения хеширования и обработки паролей.

Серверы LDAP, такие как Microsoft Active Directory, RHDS или FreeIPA, делают это по умолчанию. Другие, такие как OpenLDAP или ApacheDS, могут хранить пароли в виде обычного текста по умолчанию, если вы не используете LDAPv3 Password Modify Extended Operation согласно RFC3062. Расширенная операция изменения пароля LDAPv3 должна быть явно включена на странице конфигурации LDAP. Сверьтесь с документацией к вашему серверу LDAP для получения более подробной информации.

Всегда проверяйте, что пароли пользователей правильно хешированы и не хранятся в виде открытого текста. Для этого проверяйте изменённую запись каталога с помощью ldapsearch и декодирование значения атрибута userPassword с помощью base64.

## Аудит и события

NPP консоль управления правами предоставляет богатый набор возможностей аудита. Каждое действие входа в систему может быть записано, сохранено в базе данных и просмотрено в консоли администратора. Все действия администратора также можно записывать и просматривать. Существует также слушатель SPI, с помощью которого плагины могут прослушивать эти события и выполнять некоторые действия. Встроенные слушатели включают в себя простой файл журнала и возможность отправлять электронное письмо в случае возникновения события.

### События входа в систему

События входа в систему происходят, например, когда пользователь успешно входит в систему, когда кто-то вводит неверный пароль или когда учётная запись пользователя обновляется. Каждое событие, которое происходит с пользователем, можно записать и просмотреть. По умолчанию никакие события не сохраняются и не просматриваются в консоли администратора. В консоли и файле журнала сервера регистрируются только события ошибок. Чтобы начать сохранение, вам нужно включить хранилище. Перейдите в раздел меню «События» и выберите вкладку Конфигурация.

Чтобы начать сохранять события, вам нужно включить переключатель «Сохранять события» под Настройками событий входа в систему.

В пункте «Сохраняемые типы» можно указать, какие типы событий вы хотите сохранить в хранилище событий. Кнопка «Удалить события» позволяет удалить все события из базы данных. В поле «Истечение срока действия» можно указать, как долго вы хотите хранить события. После того как вы включили хранение событий входа в систему и определились с настройками, нажмите «Сохранить».

Для просмотра событий перейдите на вкладку «События входа в систему».

Как видите, сохраняется много информации, и, если вы сохраняете каждое событие, для каждого действия входа в систему будет сохраняться множество событий. Кнопка «Фильтр» на этой странице позволяет вам отфильтровать события.

#### Типы событий

События входа в систему:

* Вход — пользователь вошел в систему.
* Регистрация — пользователь зарегистрировался.
* Выход — пользователь вышел из системы.
* Код в токен — приложение/клиент обменял(-о) код на токен.
* Обновить токен — приложение/клиент обновил(-о) токен.

События учётной записи:

* Привязка соцсети — учётная запись была привязана к поставщику соцсети.
* Удалить привязку к соцсети — поставщик соцсети удалён из учётной записи.
* Обновить адрес электронной почты — адрес электронной почты учётной записи изменён.
* Обновить профиль — профиль учётной записи изменён.
* Отправить запрос на сброс пароля — отправлено электронное письмо для сброса пароля.
* Обновить пароль — пароль учётной записи изменён.
* Обновить TOTP — настройки TOTP для учётной записи изменены.
* Удалить TOTP — TOTP удалён из учётной записи.
* Отправить электронное письмо с подтверждением — было отправлено электронное письмо с подтверждением.
* Подтвердить электронную почту — адрес электронной почты учётной записи подтверждён.

Для всех событий существует соответствующее событие ошибки.

### События администратора

Любое действие, выполняемое администратором в консоли администратора, может быть записано для целей аудита.

Чтобы включить аудит действий администратора, перейдите в пункт «События» в левом меню и выберите вкладку «Конфигурация».

В разделе «Настройки событий администратора» включите переключатель «Сохранить события».

Переключатель «Включить представление» позволяет вам увидеть, что сделал администратор, но может привести к хранению большого количества информации в базе данных.

Кнопка «Удалить события администратора» позволяет стереть текущую сохранённую информацию.

Для просмотра событий администратора перейдите на вкладку «События администратора».

Если в столбце «Подробности» есть поле «Представление», вы можете нажать на него, чтобы просмотреть JSON, который был отправлен с этой операцией.

Вы также можете отфильтровать интересующие вас события, нажав кнопку «Фильтр».

## Экспорт и импорт

NPP консоль управления правами может экспортировать и импортировать всю базу данных. Это может быть особенно полезно, если вы хотите перенести всю базу данных NPP консоли управления правами из одной среды в другую или перейти в другую базу данных (например, из MySQL в Oracle). Экспорт и импорт запускаются во время загрузки сервера, а его параметры передаются через системные свойства Java. Важно отметить, что поскольку импорт и экспорт происходят при запуске сервера, никакие другие действия не должны предприниматься на сервере или в базе данных, пока это происходит.

Вы можете экспортировать и импортировать свою базу данных в каталог в локальной файловой системе или в один файл JSON в вашей файловой системе.

При импорте с использованием стратегии каталога обратите внимание, что файлы должны соответствовать правилам наименования, указанным ниже. Если вы импортируете файлы, которые были ранее экспортированы, файлы уже соответствуют этим правилам.

Если вы экспортируете в каталог, вы также можете указать количество пользователей, которые будут храниться в каждом файле JSON.

Если в вашей базе данных много пользователей (500 или больше), настоятельно рекомендуется экспортировать в каталог, а не в один файл. Экспорт в один файл может привести к созданию очень большого файла. Также поставщик каталога использует отдельную транзакцию для каждой «страницы» (файла с пользователями), что приводит к гораздо лучшей работе. По умолчанию количество пользователей на файл (и транзакцию) составляет 50, что показало нам лучшую производительность, но у вас есть возможность переопределить его (см. ниже). При экспорте в один файл используется одна транзакция для всего экспорта и одна транзакция для всего импорта, что приводит к снижению производительности при большом количестве пользователей.

### Экспорт и импорт

Импорт и экспорт большинства ресурсов может быть выполнен из консоли администратора. Экспорт пользователей не поддерживается.

Атрибуты, содержащие конфиденциальную информацию, будут замаскированы в файле экспорта. Таким образом, файлы экспорта, полученные через консоль администратора, не подходят для резервного копирования или передачи данных между серверами. Для этого подходит только экспорт во время загрузки.

Файлы, созданные во время «загрузочного» экспорта, также можно использовать для импорта из пользовательского интерфейса администратора. Таким образом, вы можете экспортировать данные из одного реалма и импортировать их в другой реалм. Или вы можете экспортировать данные с одного сервера и импортировать на другой.

Экспорт-импорт консоли администратора позволяет использовать только один реалм для каждого файла.

Импорт консоли администратора позволяет вам «перезаписывать» ресурсы, если вы этого захотите. Используйте эту функцию с осторожностью, особенно в производственной системе. Экспорт файлов JSON из консоли администратора с помощью операции экспорта обычно не подходит для импорта данных, поскольку они содержат конфиденциальную информацию.

Экспорт консоли администратора позволяет экспортировать клиентов, группы и роли. Если в вашем реалме много любых из этих ресурсов, операция может занять много времени. В это время сервер может не отвечать на запросы пользователей. Используйте эту функцию с осторожностью, особенно в производственной системе.

## Служба учётной записи пользователя

В NPP консоли управления правами есть встроенная служба учётных записей пользователей, к которой имеет доступ каждый пользователь. Эта служба позволяет пользователям управлять своей учётной записью, изменять свои учётные данные, обновлять свой профиль и просматривать сессии входа в систему. URL-адрес этой службы: <server-root>/auth/realms/{realm-name}/account.

Начальная страница — это профиль пользователя, который открывается в пункте меню «Учётная запись». Здесь пользователи указывают основные данные о себе. Этот экран можно настроить, чтобы пользователь смог управлять дополнительными атрибутами.

В пункте «Пароль» в левом меню пользователь может изменить свой пароль.

В пункте меню «Аутентификатор» пользователь может по желанию задать одноразовый пароль (OTP). Он будет отображаться только в том случае, если OTP является допустимым механизмом аутентификации в вашем реалме.

Пункт «Объединенное удостоверение» позволяет пользователю связать свою учётную запись с брокером удостоверений (обычно это используется для связывания учётных записей социальных сетей друг с другом). Будет показан список внешних поставщиков удостоверений, которых вы настроили для своего реалма.

Объединенное удостоверение

1. Объединенное удостоверение

В пункте меню «Сессии» пользователь может увидеть, какие устройства вошли в систему и откуда, и управлять такими устройствами. Он также может выполнить выход из этих сессий с этого экрана.

В пункте меню «Приложения» пользователи могут увидеть, к каким приложениям у них есть доступ.

### Тематические

Как и все пользовательские интерфейсы в NPP консоли управления правами, служба учётных записей пользователей полностью адаптируется к теме и интернационализируется.

## Уменьшение рисков

В этой главе обсуждаются возможные уязвимости системы безопасности, которые может иметь любой сервер аутентификации, и то, как NPP консоль управления правами устраняет эти уязвимости.

### Угадывание пароля: атаки методом перебора

Атака методом перебора происходит, когда злоумышленник пытается угадать пароль пользователя. NPP консоль управления правами имеет некоторые ограниченные возможности обнаружения атаки методом перебора. Если этот параметр включён, учётная запись пользователя будет временно отключена при достижении порога неудачных попыток входа в систему. Чтобы включить эту функцию, перейдите в пункт «Настройки реалма» в меню, нажмите на вкладку «Средства безопасности», затем дополнительно перейдите на вкладку «Обнаружение перебора».

Обнаружение взлома методом перебора по умолчанию отключено. Включение этой функции настоятельно рекомендуется для защиты от атак этого типа.

Есть две разные конфигурации для обнаружения атаки методом перебора: постоянная блокировка и временная блокировка.

Постоянная блокировка отключит учётную запись пользователя после обнаружения атаки; учётная запись будет отключена до тех пор, пока администратор повторно не активирует ее. Временная блокировка отключит учётную запись пользователя на время после обнаружения атаки; период времени, на который учётная запись отключена, увеличивается в зависимости от того, чем дольше продолжается атака.

Когда пользователь временно заблокирован и пытается войти в систему, отображается сообщение об ошибке по умолчанию «Неправильное имя пользователя или пароль». Это то же сообщение об ошибке, что и сообщение, отображаемое при вводе неверного имени пользователя или неверного пароля. Это сделано намеренно, поскольку мы не хотим сообщать злоумышленнику о том, что пользователь временно отключён.

Обычные параметры:

* Максимальное количество неудачных попыток входа в систему.
* Максимально допустимое количество неудачных попыток входа в систему. Значение по умолчанию равно 30.
* Интервал проверки быстрого входа в систему в миллисекундах.
* Минимальное время между попытками входа в систему. По умолчанию равно 1000.
* Минимальное время ожидания быстрого входа.
* Минимальное время, на которое пользователь будет временно отключён, если попытки входа в систему будут быстрее, чем значение «Интервал проверки быстрого входа в систему в миллисекундах». По умолчанию равно 1 минуте.

Параметры временной блокировки:

* Приращение ожидания.
* Время, добавляемое к времени отключению пользователя каждый раз после достижении значения «Максимальное количество неудачных попыток входа в систему». По умолчанию равно 1 минуте.
* Максимальное ожидание.
* Максимальное время, на которое пользователь будет временно отключён. По умолчанию равно 15 минут.
* Время сброса отказа.
* Время, по истечении которого счётчик отказов будет сброшен; таймер запускается с момента последнего неудачного входа в систему. По умолчанию равно 12 часам.

Алгоритм постоянной блокировки:

1. При успешном входе
   * Сброс счётчика
2. При неудачном входе в систему
   * Приращение счётчика
   * Если значение на счётчике больше «Максимального количества неудачных попыток входа в систему»
     + Отключить пользователя навсегда
   * В противном случае, если время между этим и последним отказом меньше, чем «Интервал проверки быстрого входа в систему в миллисекундах»
     + Временно отключить у пользователя «Минимальное время ожидания быстрого входа».

Когда пользователь отключён, он не может войти в систему, пока администратор не включит пользователя, включив счётчик сброса учётной записи.

Алгоритм временной блокировки:

1. При успешном входе
   * Сброс счётчика
2. При неудачном входе в систему
   * Если время между этим и последним отказом больше, чем «Время сброса отказа»
     + Сброс счётчика
   * Приращение счётчика
   * Рассчитать ожидание с использованием ожидание приращения (счётчик / «Максимальное количество неудачных попыток входа в систему»). Деление является целочисленным, поэтому всегда округляется до целого числа.
   * Если счётчик равен 0, а время между этим и последним отказом меньше, чем значение «Интервал проверки быстрого входа в систему в миллисекундах», то ожидание устанавливается вместо этого на «Минимальное время ожидания быстрого входа».
     + Временно отключить пользователя при меньшем значении ожидания и значении «Максимального ожидания» в секундах.

Ошибки входа в систему, когда пользователь временно отключён, не увеличивают счётчик.

Недостатком обнаружения взлома методом NPP консолью управления правами является то, что сервер становится уязвимым для атак типа «отказ в обслуживании». Злоумышленник может просто попытаться угадать пароли для любых учётных записей, которые ему известны, и эта учётная запись будет отключена. Со временем мы расширим эту функциональность, чтобы учитывать IP-адрес клиента при принятии решения о блокировке пользователя.

Лучшим вариантом может быть такой инструмент, как Fail2Ban. Вы можете указать эту службу в файле журнала сервера NPP консоли управления правами. NPP консоли управления правами регистрирует каждый сбой входа и IP-адрес клиента, на котором произошел сбой. Fail2Ban может использоваться для модификации брандмауэров после обнаружения атаки для блокировки соединений с определённых IP-адресов.

#### Политика в отношении паролей

Для предотвращения подбора пароля необходимо иметь достаточно сложную политику паролей или настроить сервер на использование одноразового пароля (OTP).

### Атрибуты пользователя только для чтения

Типичные пользователи, хранящиеся в NPP консоли управления правами, имеют различные атрибуты, связанные с их профилями пользователей. К таким атрибутам относятся адрес электронной почты, имя или фамилия.

Однако у пользователя могут быть атрибуты, которые не являются типичными данными профиля, а скорее метаданными. Атрибуты метаданных обычно должны быть доступны пользователям только для чтения, и у обычных пользователей никогда не должно быть возможности обновить эти атрибуты из пользовательского интерфейса NPP консоли управления правами.

Атрибуты метаданных обычно являются атрибутами из этих групп:

* Различные ссылки или метаданные, относящиеся к поставщикам пользовательских хранилищ. Например, в случае интеграции атрибут LDAP LDAP\_ID содержит идентификатор пользователя на сервере LDAP.
* Метаданные, предоставленные пользовательским хранилищем. Например createdTimestamp, предоставленный из LDAP, должен всегда быть доступен только для чтения пользователем или администратором.
* Метаданные, относящиеся к различным аутентификаторам. Например атрибут KERBEROS\_PRINCIPAL может содержать основное имя Kerberos конкретного пользователя. Аналогичным образом атрибут usercertificate может содержать метаданные, связанные с привязкой пользователя к данным из сертификата X.509, который обычно используется, когда включена аутентификация сертификата X.509.
* Метаданные, относящиеся к идентификатору пользователей приложениями или клиентами. Например, saml.persistent.name.id.for.my\_app может содержать SAML NameID, который будет использоваться клиентским приложением my\_app как идентификатор пользователя.
* Метаданные, относящиеся к политикам авторизации, которые используются для управления доступом на основе атрибутов (ABAC). Значения этих атрибутов могут использоваться для решений об авторизации. Следовательно, важно, чтобы пользователи не могли обновлять эти атрибуты.