NAICE (ru)

Содержание

Администрирование

Администраторы

Раздел "Администраторы" предназначен для управления учётными данными администраторов NAICE.

Просмотр учетных записей администраторов

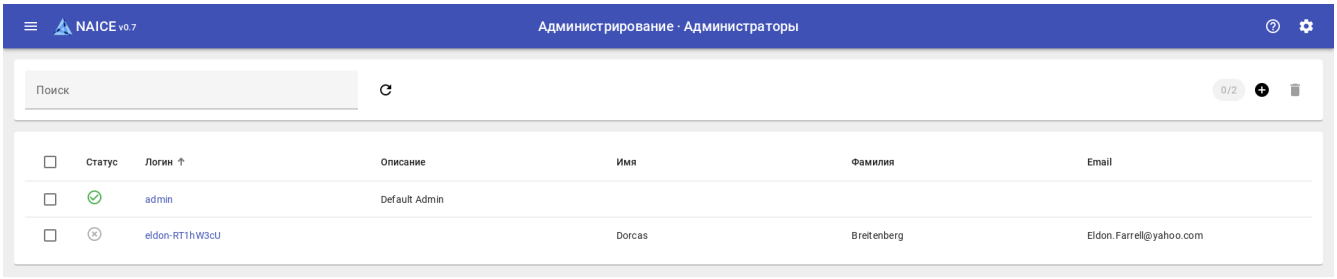

Рисунок 1. Таблица с перечнем администраторов на странице просмотра

На данной странице содержится таблица со списком всех администраторов системы.

Таблица содержит следующую информацию об администраторах системы:

- `Статус` - управляет разрешением на вход в систему: выключенный администратор не сможет авторизоваться;
- `Логин` - логин администратора (должен быть уникальным);
- `Описание` - произвольное описание;
- `Имя` - имя администратора;
- `Фамилия` - фамилия администратора;
- `Email` - адрес электронной почты администратора.

Допускается сортировка в прямом и обратном порядке по всем колонкам таблицы. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по колонке "Логин".

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - Обновить данные таблицы.
- `0/1` - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
-

☐ - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Добавление учетной записи администратора

Для добавления учетной записи администратора нажмите ⊕ на панели действий, расположенной над таблицей.

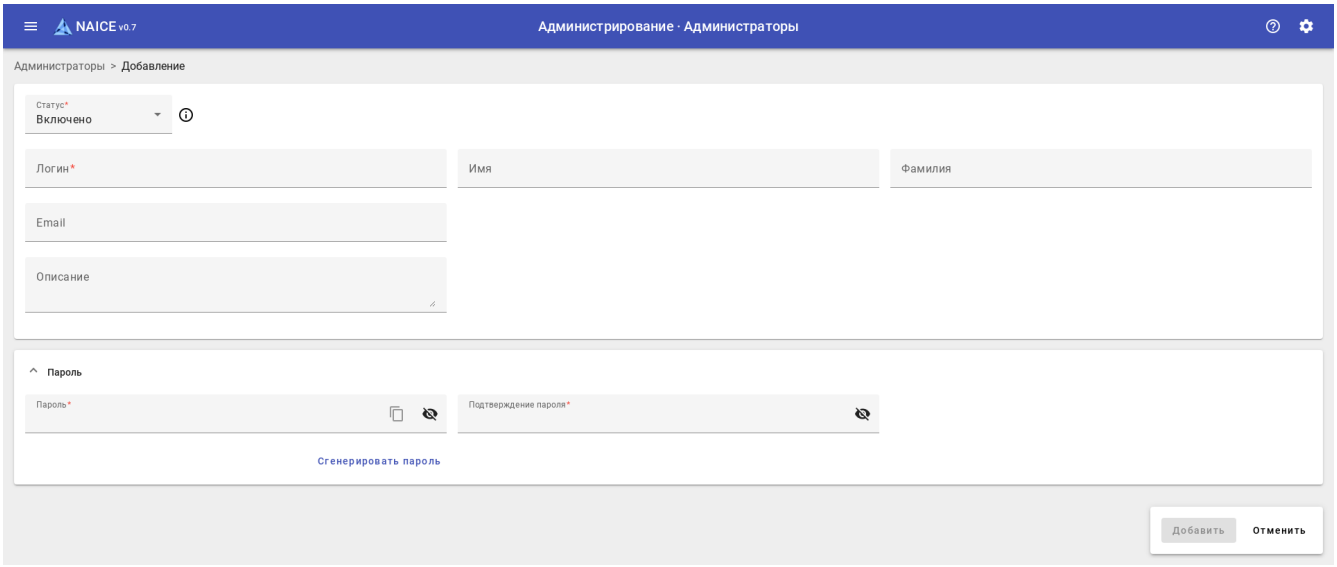

Рисунок 2. Страница добавления администратора

Форма добавления администратора включает в себя следующие поля:

- `Статус` * - включение или выключение возможности авторизации в системе данной учетной записи;
- `Логин` * (максимальная длина - 100 символов);
- `Имя` (максимальная длина - 100 символов);
- `Фамилия` (максимальная длина - 100 символов);
- `Email` (максимальная длина - 100 символов);
- `Описание` (максимальная длина - 250 символов);
- `Пароль` (максимальная длина - 100 символов);
- `Подтверждение пароля` (максимальная длина - 100 символов).

* - поля, обязательные для заполнения.

Пароль для входа в учетную запись администратора можно сгенерировать, нажав на кнопку **"Сгенерировать пароль"**, либо указать вручную. Сгенерированный пароль помещается в поля "Пароль" и "Подтверждение пароля", его можно скопировать по клику на ⧉ .

После ввода необходимых данных нажмите кнопку **"Добавить"**.

Редактирование учетной записи администратора

Для редактирования учетной записи администратора необходимо на странице со списком нажать на его логин:

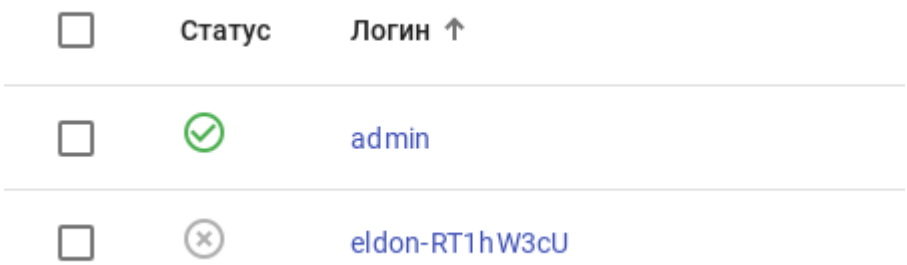

Рисунок 3. Гиперссылка на страницу редактирования администратора

После этого откроется страница редактирования администратора, аналогичная странице добавления:

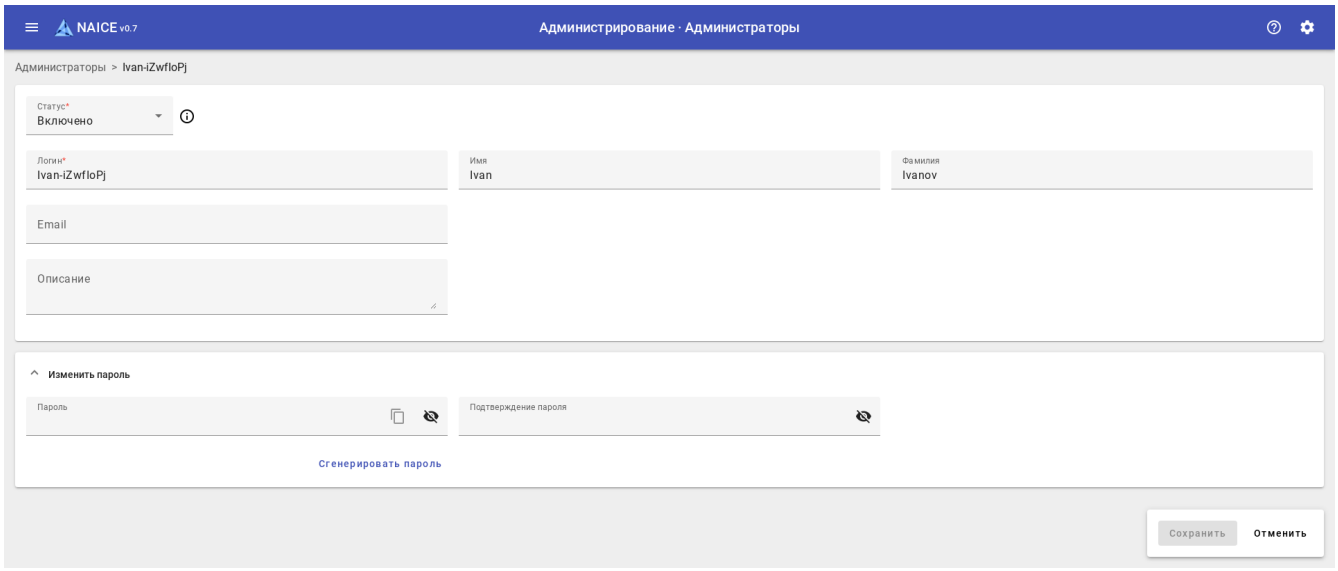

Рисунок 4. Страница изменения администратора

После редактирования нажать на кнопку **"Сохранить"**. Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

Удаление учетной записи администраторов

Для удаления учетной записи администратора в окне со списком администраторов надо выделить чекбокс слева от учетных записей, которые требуется удалить:

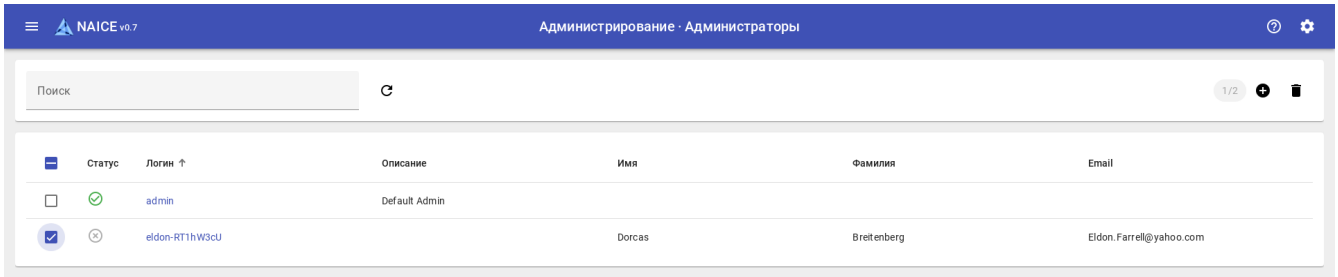

Рисунок 5. Выбор администраторов в таблице для удаления

и нажать кнопку  вверху справа.

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

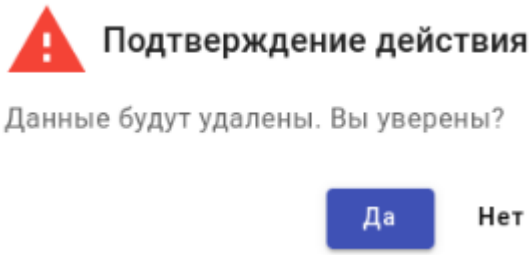

Рисунок 6. Модальный диалог подтверждения

Нельзя удалить учетную запись, под которой выполнен вход в систему.

Настройка аккаунта текущего администратора

Настройки аккаунта текущего администратора доступны на любой странице при нажатии на ⚙ в вернем правом углу окна в подменю **"Настройки аккаунта"**.

На данной странице доступен просмотр учетных данных текущего администратора (с учетной записью которого выполнен вход в систему), а также смена языка интерфейса. Поддержаны следующие языки: русский, английский.

Настройка часового пояса влияет на отображаемое время последней активности эндпоинта при мониторинге подключений.

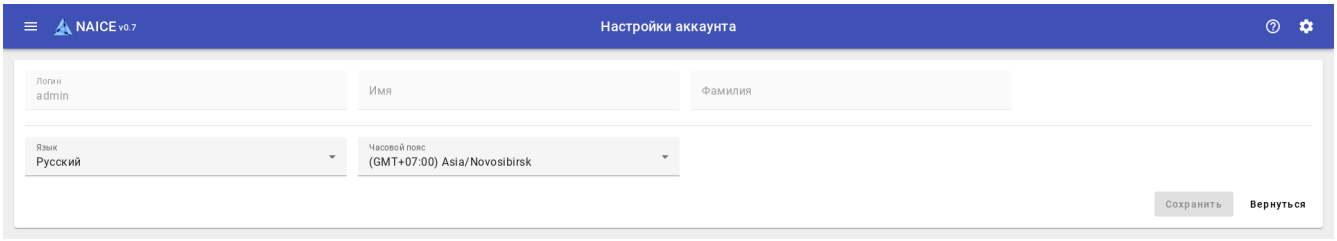

Рисунок 7. Настройка аккаунта текущего администратора

Кнопка **"Сохранить"** сохраняет внесенные в аккаунт изменения, кнопка **"Вернуться"** осуществляет возврат на страницу, с которой был выполнен переход в Настройки аккаунта.

Смена текущего администратора (выход из системы)

Для выхода из системы на любой странице необходимо нажать на ⚙ в вернем правом углу окна и выбрать подменю **"Выход"**.

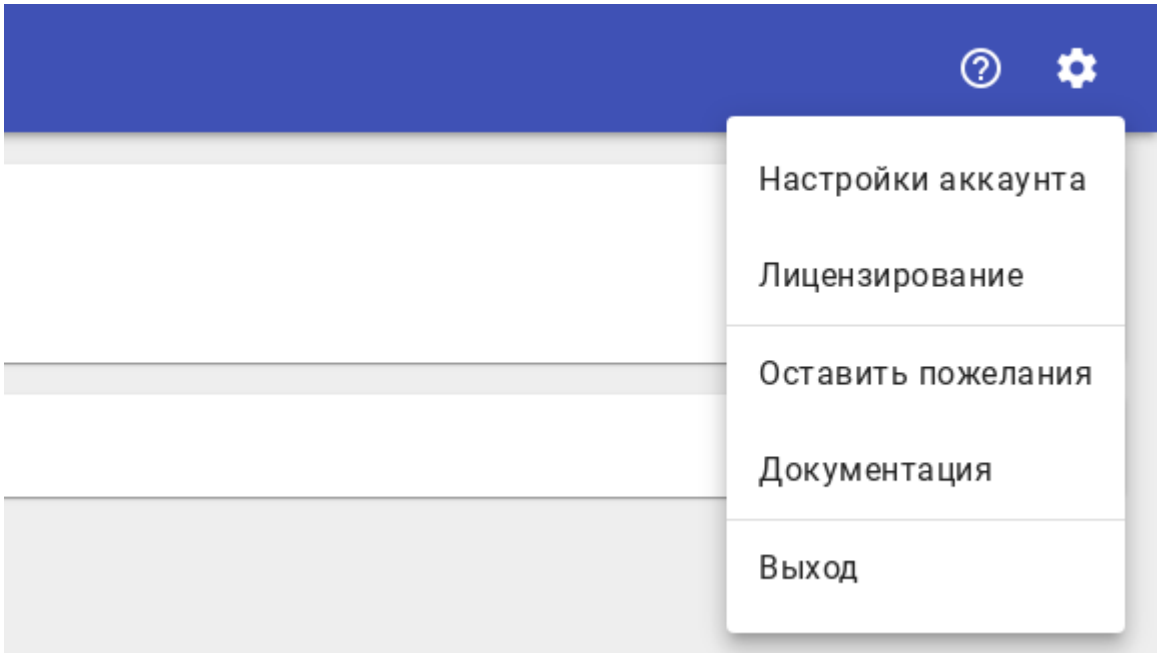

Рисунок 8. Пункт меню Выход

Далее необходимо подтвердить выход из системы, нажав на кнопку **"Выйти"**.

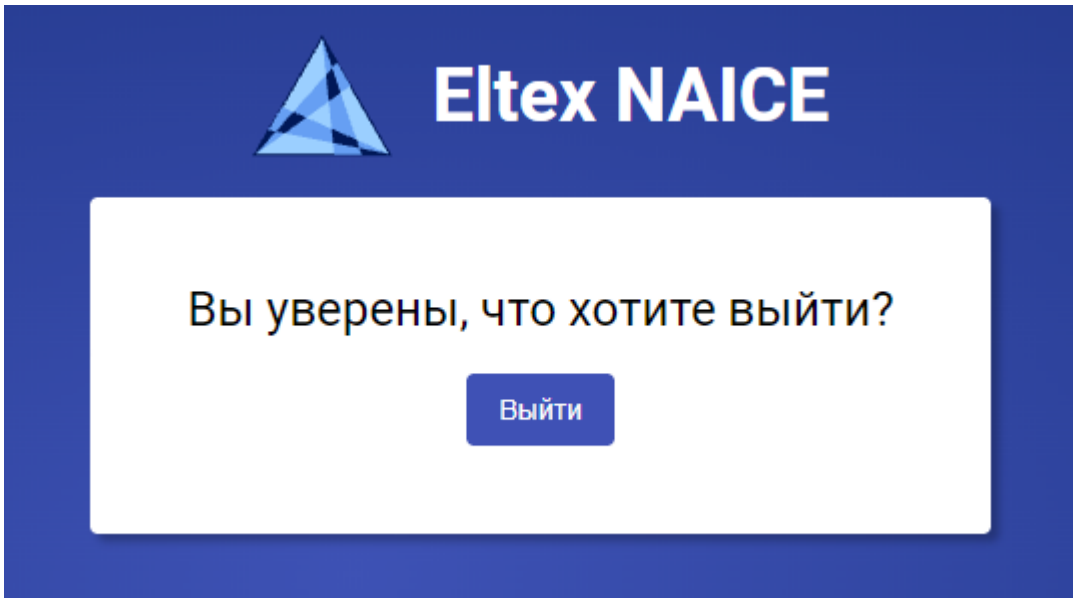

Рисунок 9. Страница подтверждения выхода из системы

После чего произойдет перенаправление на страницу авторизации.

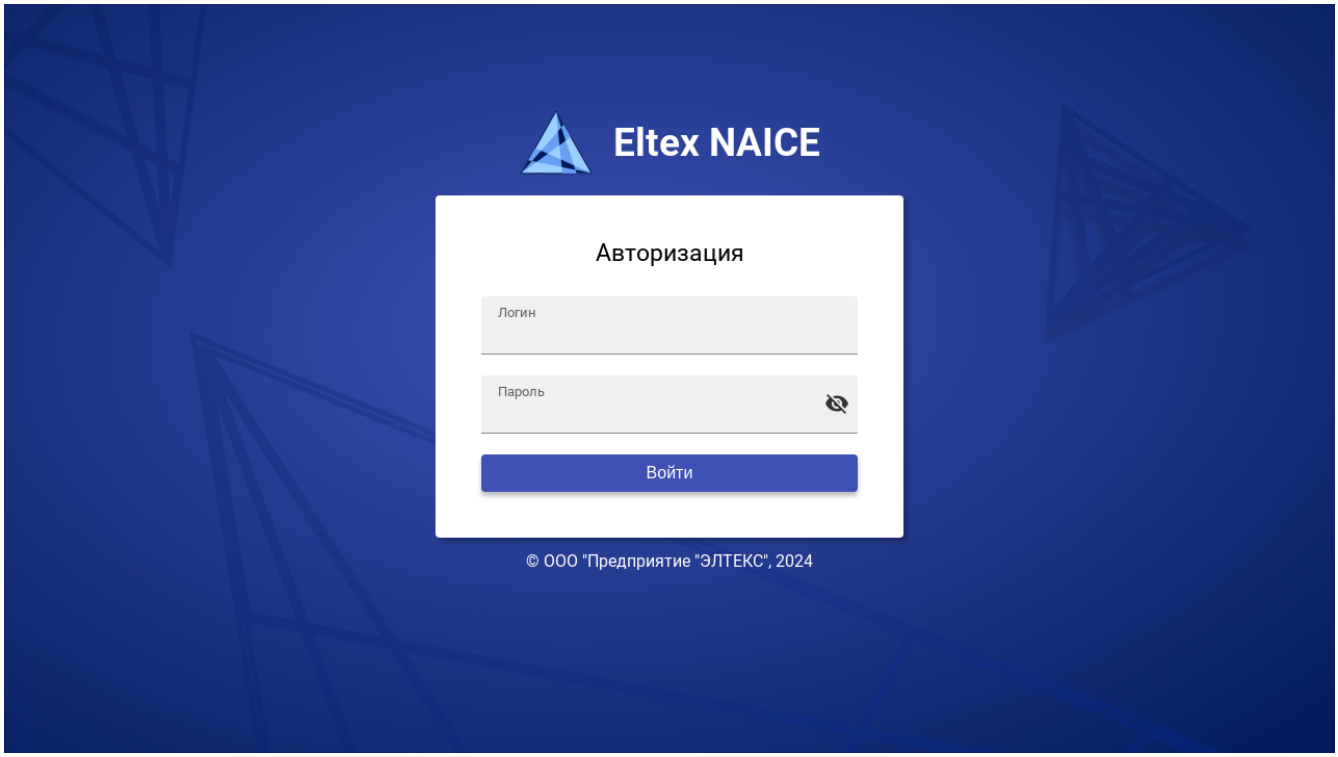

Рисунок 10. Страница авторизации в системе

Сетевые ресурсы

Сетевое устройство (authenticator, NAS - Network Attached Storage) - станционное устройство, обеспечивающее подключение клиентских устройств к сети и реализующее их аутентификацию с использованием протокола 802.1x, MAB или портальной авторизации.

Управление сетевыми устройствами выполняется в меню *"Администрирование"* → *"Сетевые ресурсы"*.

Содержит разделы:

- Устройства - раздел настроек взаимодействия с сетевыми устройствами;
- Группы устройств - раздел настроек групповых признаков, которые могут использоваться при настройке сетевых устройств;
- Профили устройств - профили, описывающие особенности взаимодействия сетевых устройств по протоколу RADIUS.

Устройства

Описание

Сетевое устройство (аутентификатор, NAS - Network Attached Storage) - станционное устройство, обеспечивающее подключение клиентских устройств к сети и реализующее их аутентификацию с использованием протокола 802.1x, MAB или других видов подключений.

Раздел "Устройства" отвечает за просмотр, добавление, удаление, редактирование сетевых устройств в системе NAICE.

Если устройство не было добавлено в систему, то запрос на авторизацию по RADIUS-протоколу от него не будет обработан!

Важно понимать — создание нового устройства невозможно без созданного профиля устройства.

Просмотр списка сетевых устройств

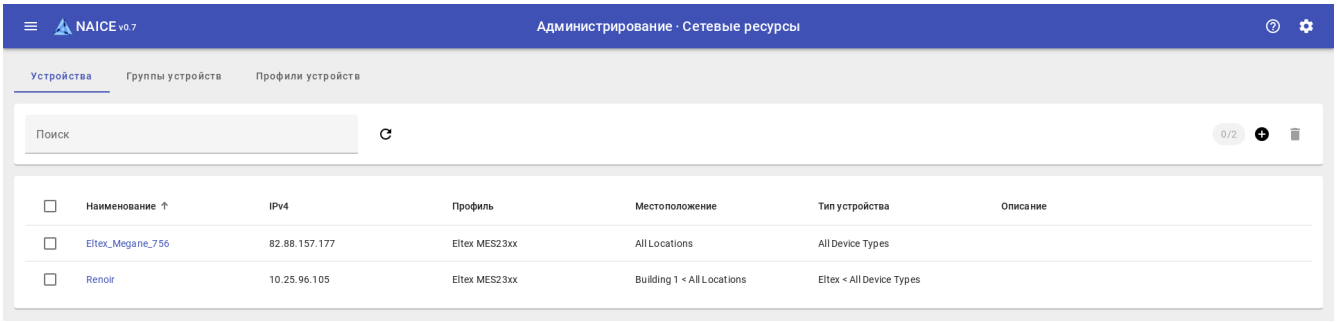

Рисунок 11. Таблица с перечнем сетевых устройств на странице просмотра

На данной странице содержится таблица со списком всех сетевых устройств, добавленных в систему.

Таблица содержит колонки:

- `Наименование` — наименование сетевого устройства.
- `IPv4` — IP-адрес, предназначенный для взаимодействия с устройством (IPv4).
- `Профиль` — назначенный профиль устройства.
- `Местоположение` — группа, определяющая местоположение устройства.
- `Тип устройства` — группа, определяющая тип устройства.
- `Описание` — произвольное описание устройства.

Возможна сортировка в прямом и обратном порядке по колонкам "Наименование", "IPv4", "Профиль". По умолчанию сортировка выполняется в прямом алфавитном порядке по колонке "Наименование".

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - Обновить данные таблицы.
- 0/1 - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

В данный момент IPv4 - единственный признак, по которому система определяет, с каким устройством идёт работа.
Доступно только полное совпадение по IP, а значит адреса всех устройств должны быть добавлены в систему явно.

Добавление сетевого устройства

Для добавления сетевого устройства нажмите  .

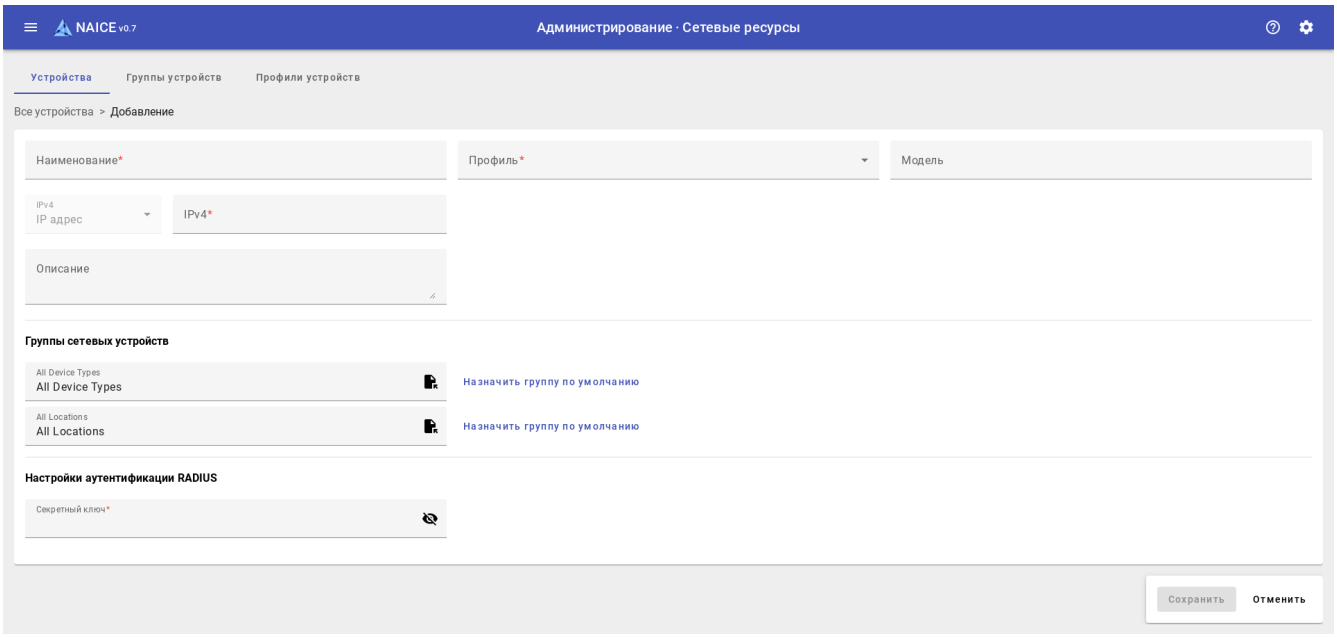

Рисунок 12. Страница добавления сетевого устройства

В открывшейся форме можно заполнить следующие параметры:

- `Наименование` * - наименование сетевого устройства; должно быть уникально в рамках списка сетевых устройств. Максимальная длина - 200 символов.
- `Профиль` * - выбор профиля сетевого устройства.
- `Модель` - модель сетевого устройства. Максимальная длина - 100 символов.
- `IPv4` * - IP-адрес сетевого устройства. Запись в виде четырех чисел от 0 до 255, разделенных точками.
- `Описание` - произвольное описание. Максимальная длина - 200 символов.

Группы сетевых устройств - выбор групп типа и локации сетевого устройства. Если выбор не сделать - будут назначены группы по умолчанию (т.е. корневые).

При создании новой корневой группы, как это описано в разделе Группы устройств, в списке *Группы сетевых устройств* они будут появляться автоматически.

Настройка аутентификации RADIUS содержит:

- Секретный ключ * для взаимодействия с сетевым устройством по протоколу RADIUS. Длина от 8 до 200 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После ввода необходимых данных нажмите кнопку **"Сохранить"**.

Редактирование сетевого устройства

Для редактирования сетевого устройства необходимо на странице со списком нажать на его имя.

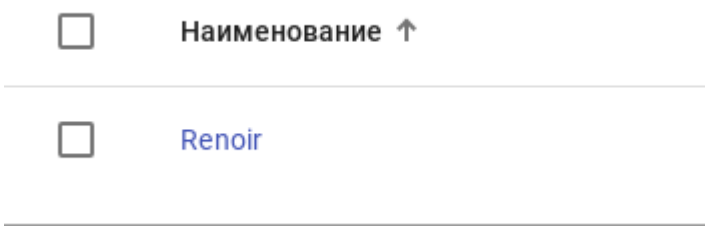

Рисунок 13. Гиперссылка на страницу редактирования устройства

После этого откроется окно редактирования, аналогичное странице добавления.

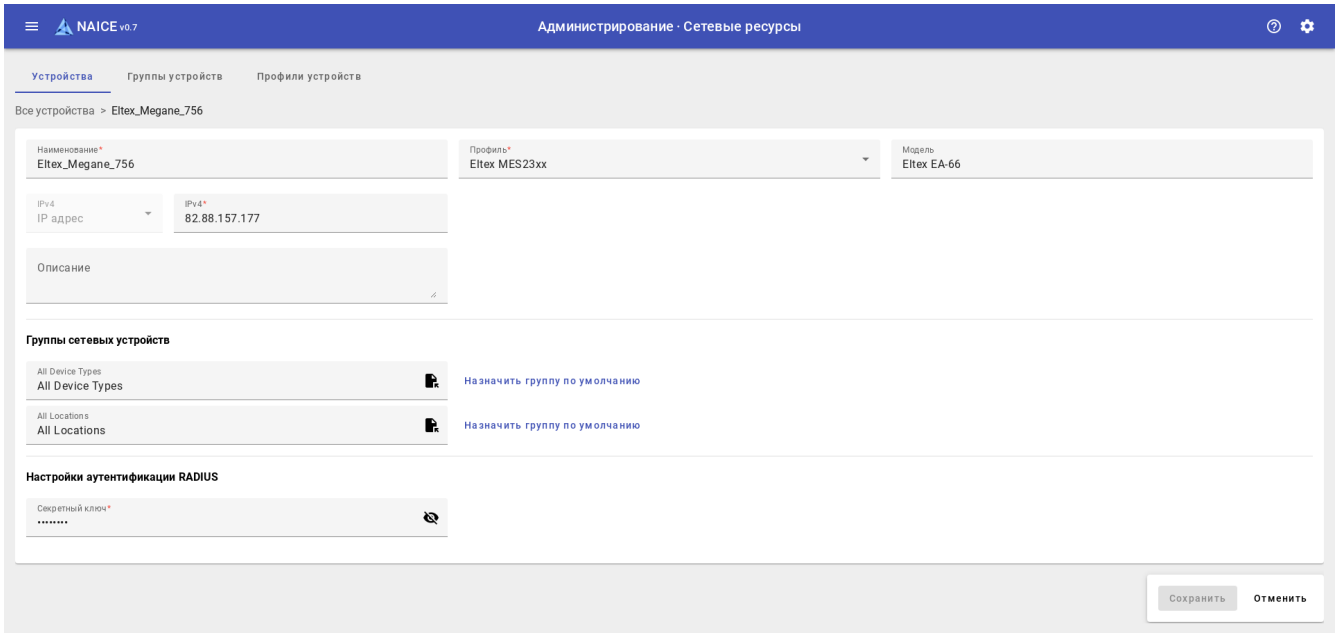

Рисунок 14. Страница редактирования устройства

RADIUS-сервер, находящийся в составе NAICE, кэширует сетевые устройства при их добавлении в систему. В случае ошибки при указании секретного ключа и последующем редактировании на корректный ключ эти данные в кэше не будут обновлены. В этом случае выполните рестарт docker-контейнера naice-radius для перечитывания новых данных из базы данных.

После редактирования нажать на кнопку **"Сохранить"**. Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

Удаление сетевого устройства

Для удаления в окне со списком надо выделить чекбокс слева от наименования сетевых устройств, которые требуется удалить, и нажать кнопку вверху справа.

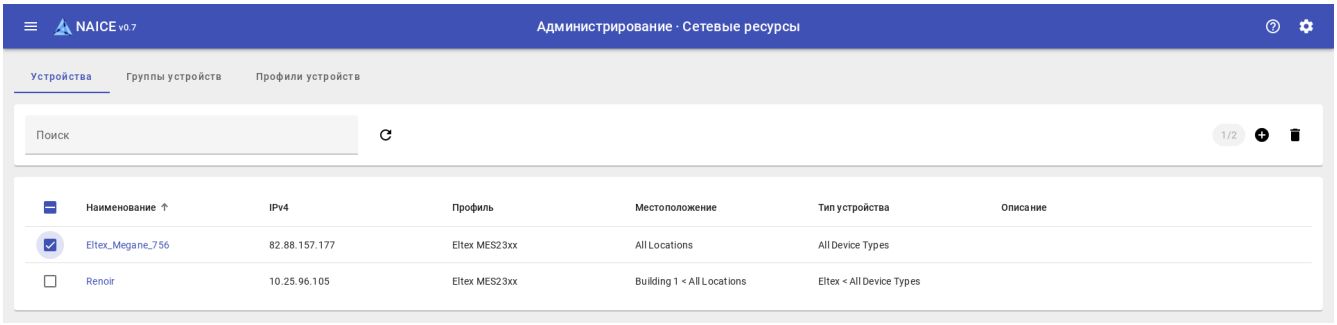

Рисунок 15. Выбор устройства в таблице для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

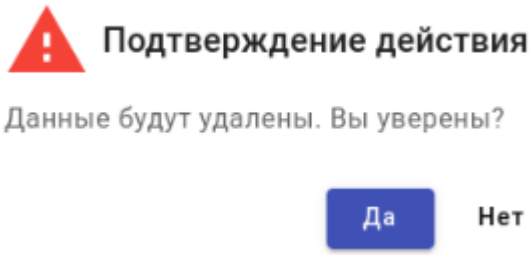

Рисунок 16. Модальный диалог подтверждения

Группы устройств

Описание

Группы устройств предназначены для агрегации сетевых устройств по различным признакам, с дальнейшей возможностью определения различных сценариев авторизации для разных групп в наборах политик.

Просмотр групп

На данной странице содержится таблица со списком всех групп.

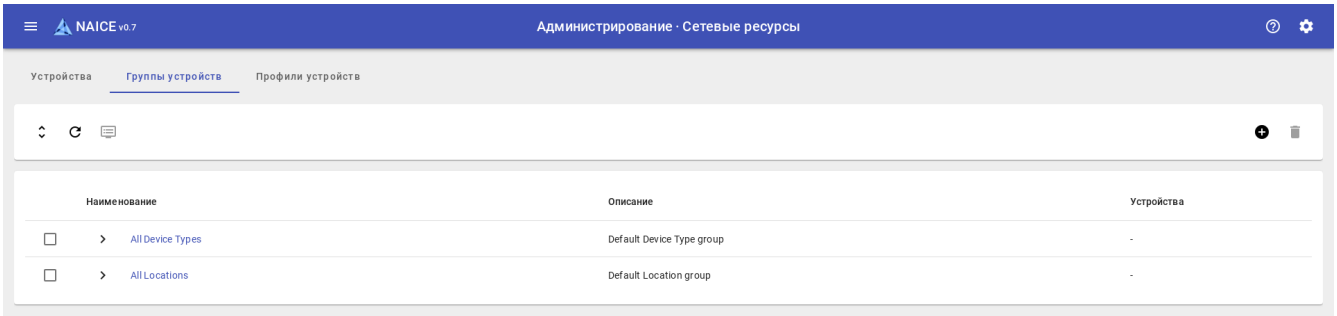

Рисунок 17. Странице просмотра списка групп

По умолчанию существуют две корневые группы:

- **All Device Types** - предназначена для формирования групп по признакам типа сетевых устройств
- **All Locations** - предназначена для формирования групп по признакам локации сетевых устройств.

Данные группы являются системными и не могут быть удалены или изменены.

При необходимости можно добавить новые пользовательские корневые группы. Таким образом администратор может создать любую иерархию устройств, группируя их по любым признакам, где *признак* выносится в Имя корневой группы, а *значения признака* в Имена дочерних групп.

Таблица содержит колонки:

- `Наименование` - наименование группы;
- `Описание` - произвольное описание группы;
- `Устройства` - количество устройств в группе; для корневых групп количество устройств не отображается.

Сортировка не предусмотрена.

Элементы управления:

- - раскрыть все группы.
- - обновить данные таблицы.
- - показать устройства группы и ее подгрупп (неактивно, пока не выбрана группа).
- - добавить группу.
- - удалить группу (неактивно, пока не выбрана группа).
- - раскрыть список подгрупп группы.
- - свернуть список подгрупп группы.
- - чекбокс для выделения группы (можно выбрать только одну группу).

Добавление группы

Добавление корневой группы

Для добавления корневой группы нажмите вверху справа от списка групп когда не выбрана ни одна группа.

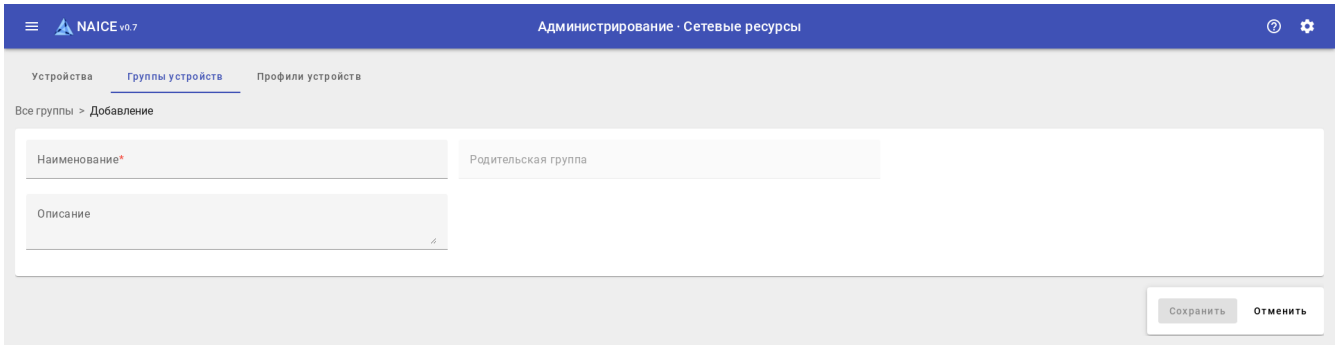

Рисунок 18. Страница добавление группы

В открывшемся окне можно заполнить:

- `Наименование` * - наименование группы. Максимальная длина - 100 символов.
- `Описание` - описание. Максимальная длина - 200 символов.

`Родительская группа` - заполняется автоматически, значение берется от группы для которой выполняется создание подгруппы. При создании корневой группы поле будет пустое.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После ввода необходимых данных нажмите кнопку **"Сохранить"**.

Добавление подгруппы в существующую группу

Для добавления группы в существующую группу необходимо выбрать её чекбоксом слева от наименования и нажать ⊕.

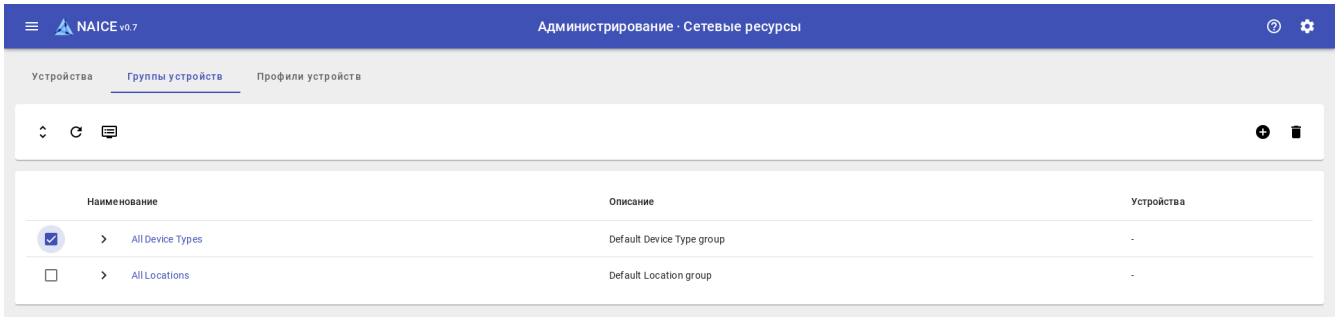

Рисунок 19. Страница с выбором корневой группы для добавления дочерней группы

При добавлении подгруппы в поле "Родительская группа" отображается наименование и ID родительской группы. Данное поле не может быть изменено.

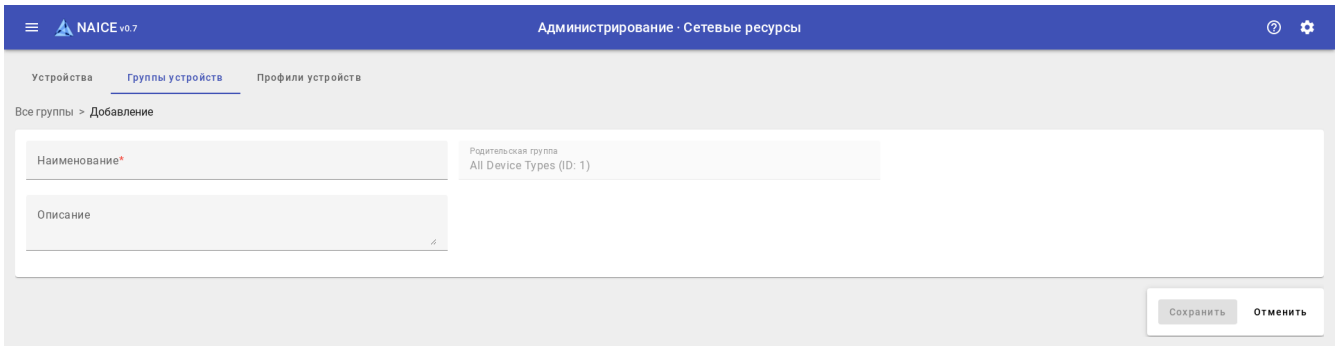

Рисунок 20. Страница с добавлением дочерней группы

Редактирование группы

Для редактирования группы необходимо нажать на её наименование.

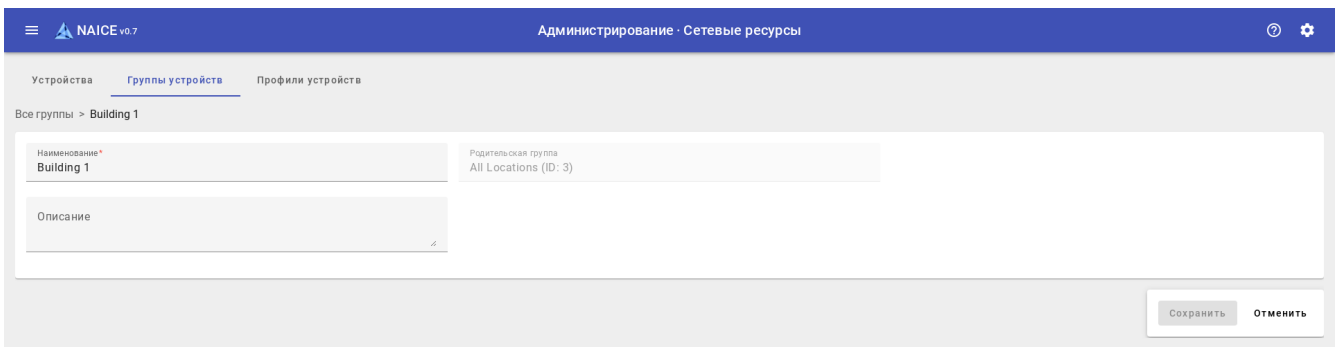

Рисунок 21. Страница редактирования группы

После редактирования нажать на кнопку **"Сохранить"**. Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

Изменить "Родительскую группу" нельзя. Процедура перемещения подгруппы в другую родительскую не предусмотрена. Для её изменения надо удалить группу и создать ее в качестве подгруппы иной группы.

Удаление группы

Для удаления в окне со списком надо выделить чекбокс слева от наименования и нажать кнопку вверху справа.

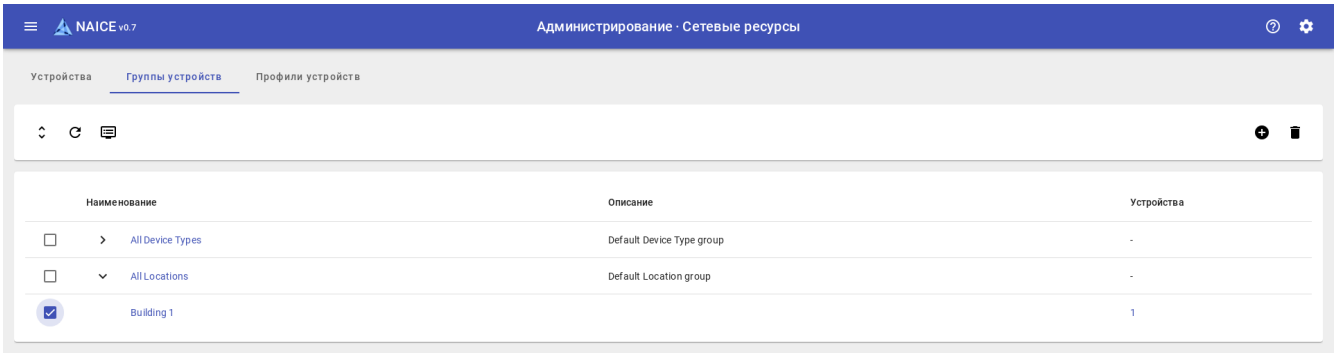

Рисунок 22. Страница с выделенной группой для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

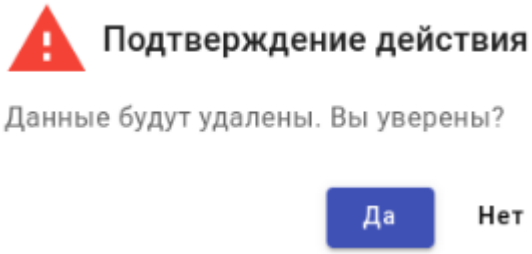

Рисунок 23. Модальный диалог подтверждения

Ограничения:

- нельзя выбрать и удалить несколько групп;
- нельзя удалить системные группы "All Device Types" и "All Locations";
- нельзя удалить группу содержащую подгруппы;
- нельзя удалить группу, которая назначена сетевому устройству.

Просмотр устройств в группе

Просмотр устройств в группе возможен двумя способами:

- просмотр устройств в группе и ее подгруппах через выбор группы и нажатие на ;
- просмотр устройств только этой группы через нажатие на счетчик напротив группы в колонке "Устройства".

В обоих случаях в правой части экрана будет открыта боковая панель с таблицей устройств в группе.

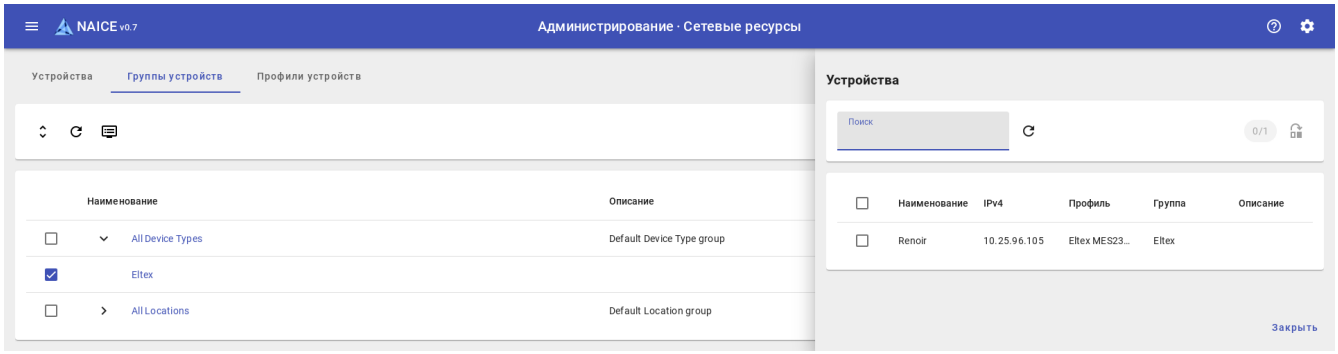

Рисунок 24. Панель просмотра устройств в группе

Таблица содержит колонки:

- `Наименование` - имя устройства;
- `IPv4` - IPv4-адрес устройства;
- `Профиль` - профиль устройства;
- `Группа` - подгруппа устройства в рамках данной корневой группы. Не отображается, если панель открыта при нажатии на счетчик устройств.
- `Описание` - произвольное описание устройства.

Сортировка доступна по колонкам "Наименование" и "IPv4".

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - Обновить данные таблицы.
- 0/1 - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Перемещение устройства в другую группу

После нажатия на кнопку перемещения устройства откроется окно с выбором группы для перемещения *в рамках этой же корневой группы*.

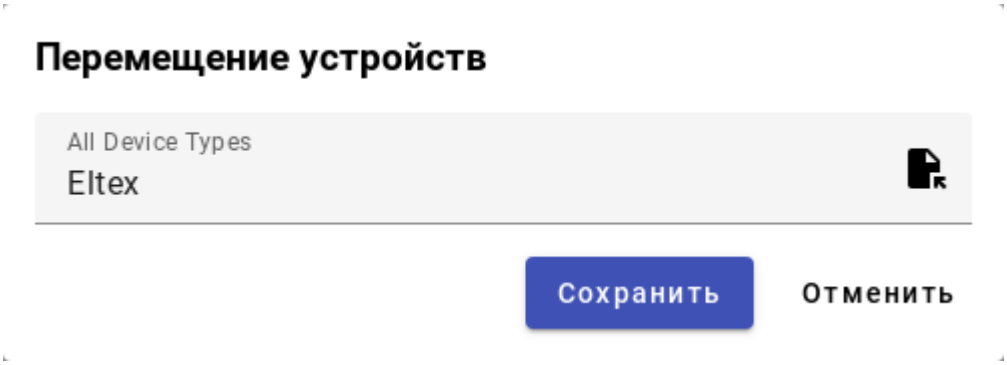

Рисунок 25. Панель перемещения устройств в группу

Группа выбирается из списка, открывающегося по нажатию на .

Профили устройств

Описание

Профили устройств предназначены для обобщения настроек похожих сетевых устройств. Как правило похожие настройки имеют устройства одного производителя и/или одного семейства.

Основными настройками в профилях устройств являются:

- *условия определения типа подключения* - при получении каких RADIUS-атрибутов подключение пользователя будет определено, например, как проводное MAB или беспроводной 802.1x. На основании типа подключения можно настраивать политики доступа. Например, для пользователя, подключающегося проводным способом, можно выдавать один VLAN, а для того же пользователя, подключающегося беспроводным способом - другой.
- *настройка MAB* - возможность авторизации подключенных к этому устройству клиентов по MAB и настройка особенностей этого подключения.
- *разрешения* - настройка возможности и RADIUS-атрибутов для выдачи VLAN и/или ACL для подключенных к этому устройству клиентов.

Просмотр списка профилей устройств

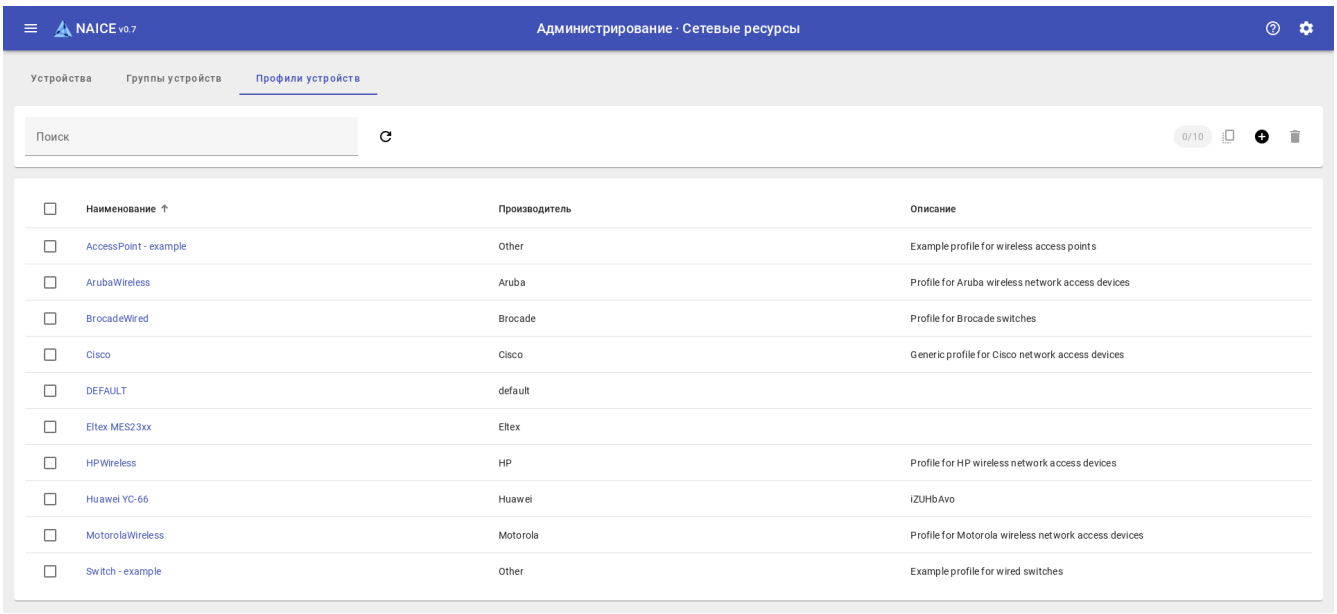

Рисунок 26. Таблица с перечнем профилей сетевых устройств

На данной странице содержится таблица со списком профилей устройств.

Таблица содержит колонки:

- `Наименование` - наименование профиля;
- `Производитель` - наименование вендора устройств;
- `Описание` - произвольное описание профиля.

Доступна сортировка по колонкам `Наименование`, `Производитель`.

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
-  - Обновить данные таблицы.
-  - Счетчик выбранных чекбоксом элементов / общего количества элементов.
-  - Добавить новый элемент.
-  - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  - Изменить текущий порядок сортировки.
-  - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Добавление профиля устройства

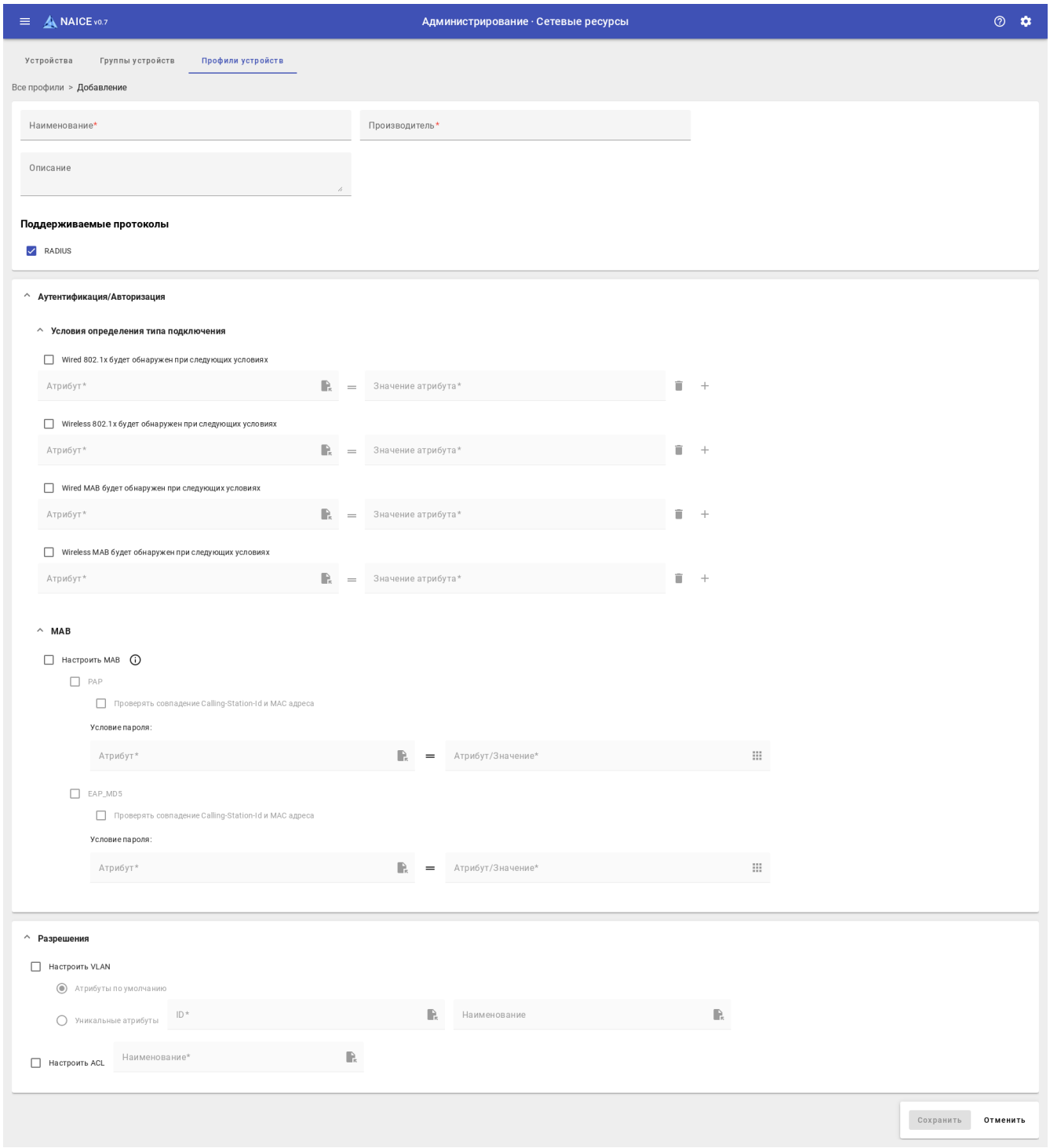

Рисунок 27. Страница добавления сетевого профиля устройств

Для добавления профиля устройства нажмите ⊕.

В открывшемся окне необходимо заполнить следующие параметры:

- `Наименование` * - наименование профиля устройства. Максимальная длина - 100 символов.
- `Производитель` * - наименование производителя сетевого устройства. Максимальная длина - 100 символов.
- `Описание` - произвольное описание. Максимальная длина - 200 символов.

`Поддерживаемые протоколы` - протоколы, который используется для взаимодействия с сетевым устройством. По умолчанию включен протокол RADIUS.

Аутентификация/Авторизация - блок настройки, отвечающий за определение типа подключения клиентского устройства.

- `Wired 802.1x / Wireless 802.1x / Wired MAB / Wireless MAB будет обнаружен при следующих условиях` - включение настройки определения одного из типов подключения.
- `Атрибут` - RADIUS-атрибут, используемый в условии.
- = означает что условие будет выполнено при равенстве атрибута указанному значению. При клике на иконку можно сменить условие на неравенство.
- `Значение атрибута` - значение RADIUS-атрибута, используемое в условии.
- - удалить условие.
- добавить условие.

При включении определения какого-либо типа подключения атрибуты заполнятся стандартными значениями. Их можно отредактировать или оставить без изменений.

Если используется несколько RADIUS-атрибутов в условии - они объединяются логическим "И". Если тип подключения не включен или не был определен - пользователь продолжает авторизацию, его тип подключения считается неопределенным.

MAB - блок настройки, отвечающий за разрешение и конфигурацию особенностей MAB авторизации.

- `Настроить MAB` - включение разрешения MAB авторизации на устройстве.
- `PAP / EAP_MD5` - включение разрешения MAB авторизации по указанным протоколам.
- `Проверять совпадение Calling-Station-Id и MAC адреса` - включение разрешения авторизации только тех устройств, в запросе которых RADIUS-атрибут Calling-Station-Id совпадает с MAC адресом в имени пользователя.
- `Условие пароля` - условие, при котором пароль будет считаться корректным. По умолчанию задано условие равенства пароля логину пользователя.

Разрешения - блок настройки, определяющий возможность упрощенной выдачи пользователю дополнительных атрибутов после авторизации.

- `Настроить VLAN` - включить возможность упрощенной выдачи VLAN в RADIUS-атрибутах.
  - `Атрибуты по умолчанию` - использовать стандартные IETF RADIUS-атрибуты для выдачи VLAN.
  - `Уникальные атрибуты` - использовать vendor-specific RADIUS-атрибуты для выдачи VLAN.
    - `ID` - vendor-specific RADIUS-атрибут для выдачи VLAN в формате числа от 1-4094.
    - `Наименование` - vendor-specific RADIUS-атрибут для выдачи VLAN в формате строки.

`Настроить ACL` - включить возможность упрощенной выдачи имени статической ACL в RADIUS-атрибутах.

- `Наименование` - vendor-specific RADIUS-атрибут для выдачи имени ACL в формате строки.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

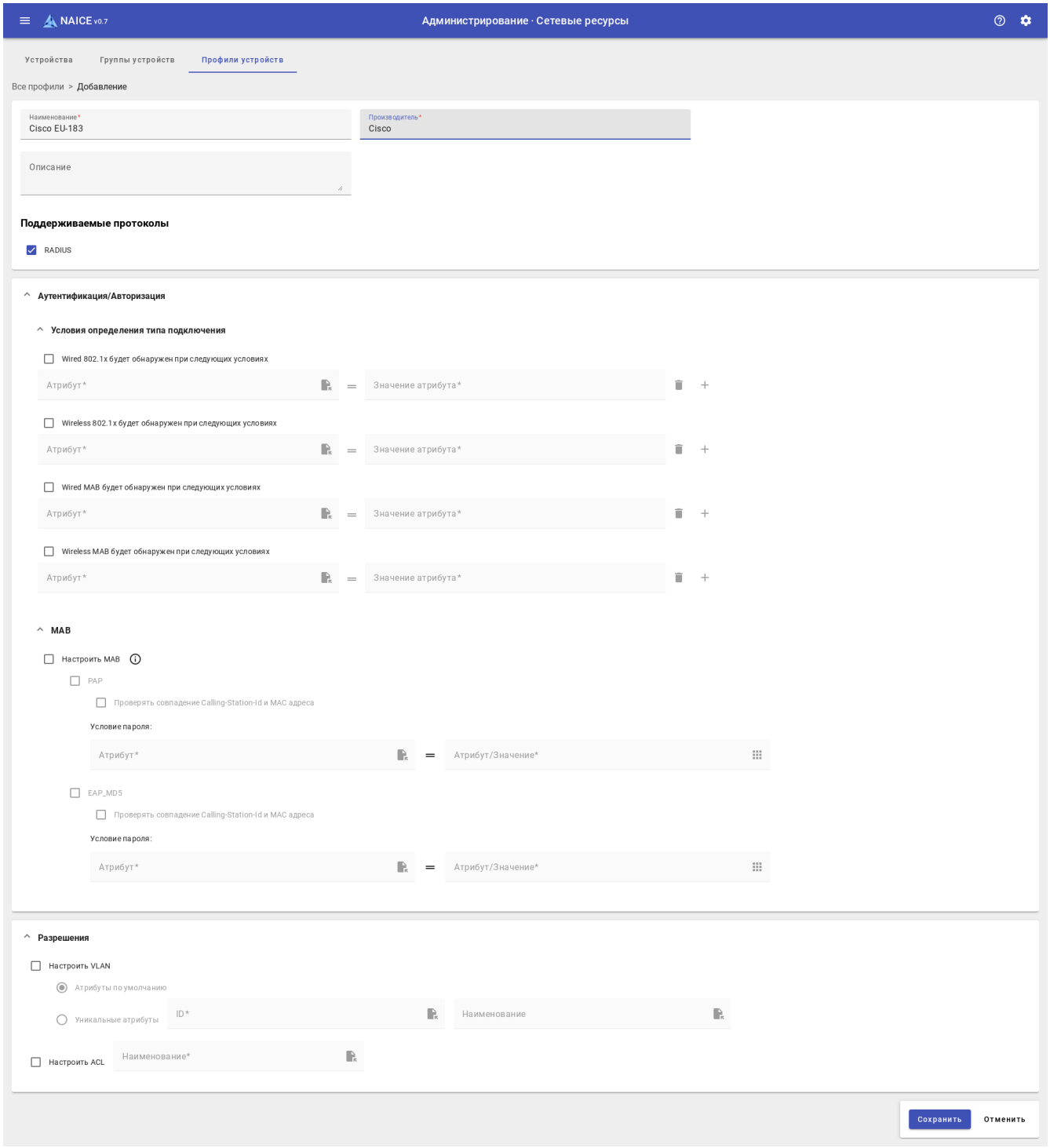

Рисунок 28. Страница с заполненными параметрами профиля устройств

После ввода необходимых данных нажмите кнопку **"Сохранить"**.

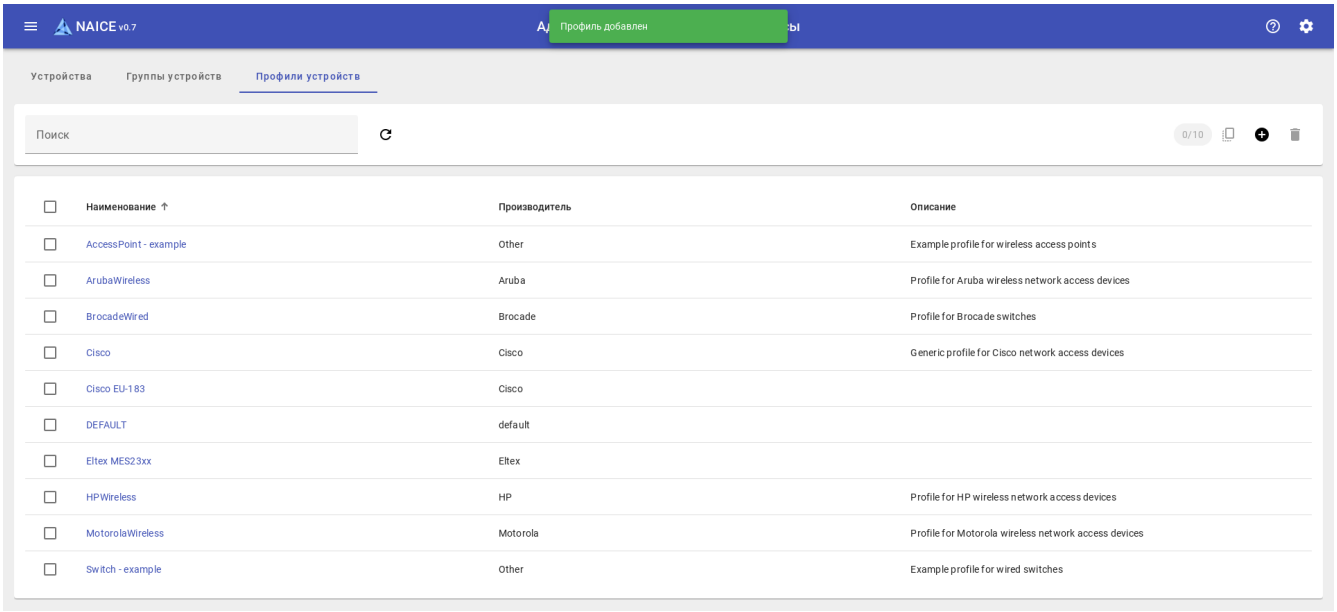

Рисунок 29. Страница успешного создания профиля сетевых устройств

Редактирование профиля устройства

Для редактирования профиля устройства необходимо на странице со списком нажать на его имя, после чего откроется окно редактирования, аналогичное окну добавления.

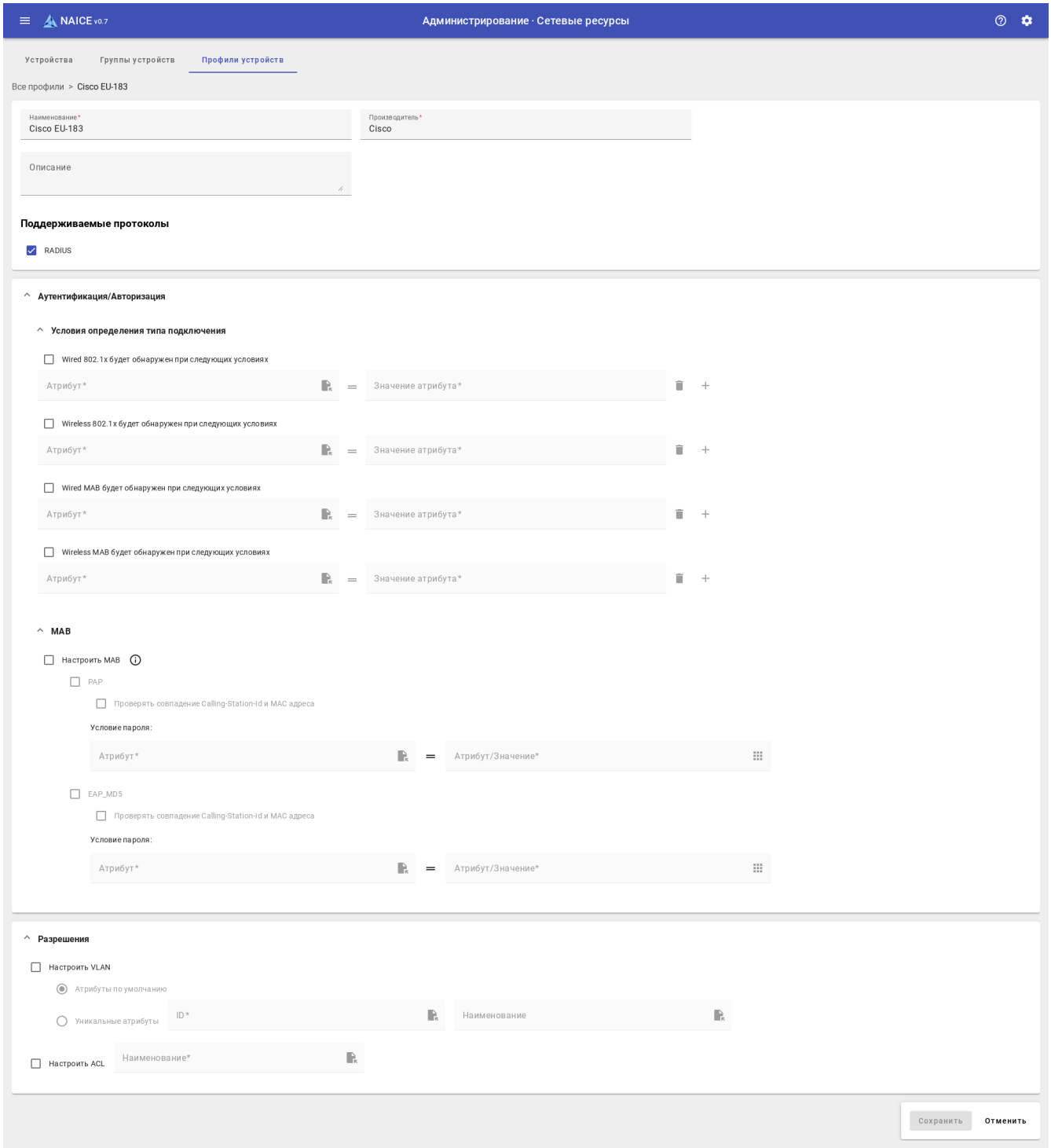

Рисунок 30. Страница редактирования профиля сетевых устройств

После редактирования нажать на кнопку **"Сохранить"**. Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

Удаление профиля устройства

Для удаления профиля выберите его чекбоксом и нажмите кнопку 🗑 в правой части панели над таблицей.

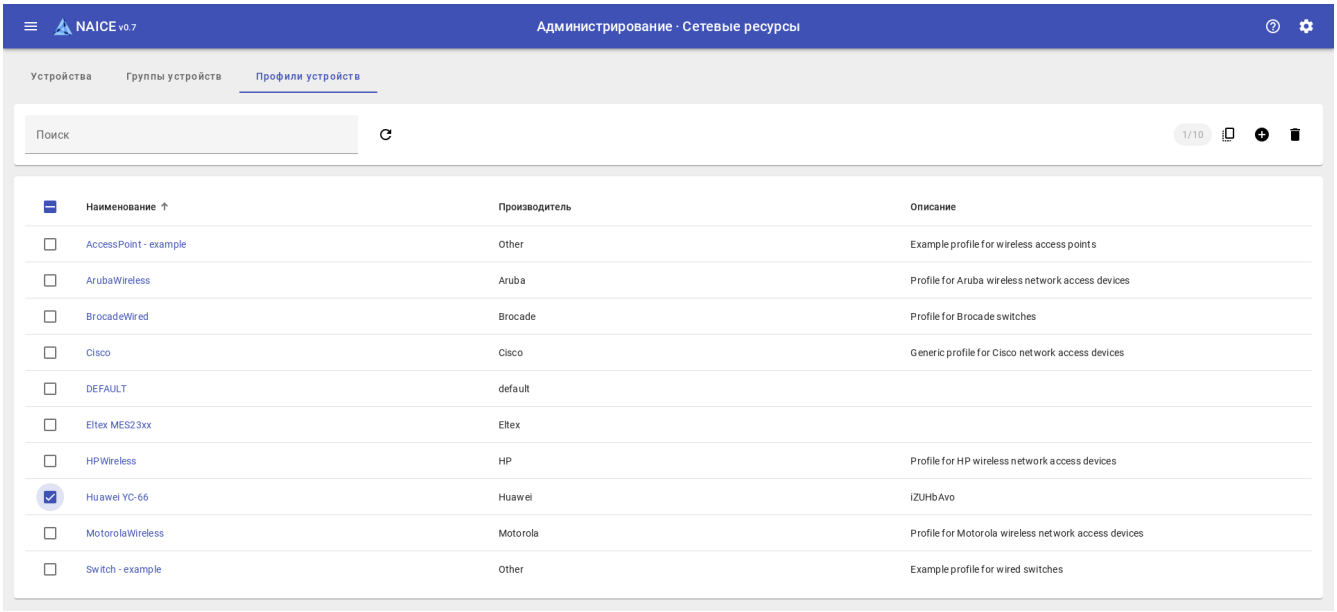

Рисунок 31. Страница с выбранным для удаления профилем устройств

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

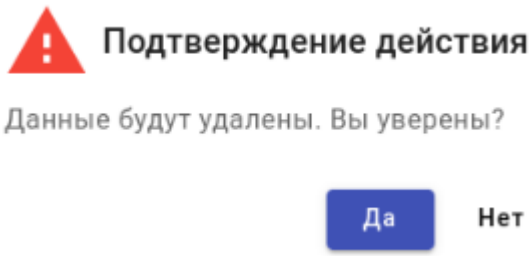

Рисунок 32. Модальный диалог подтверждения

После удаления произойдет переход на страницу просмотра списка профилей устройств.

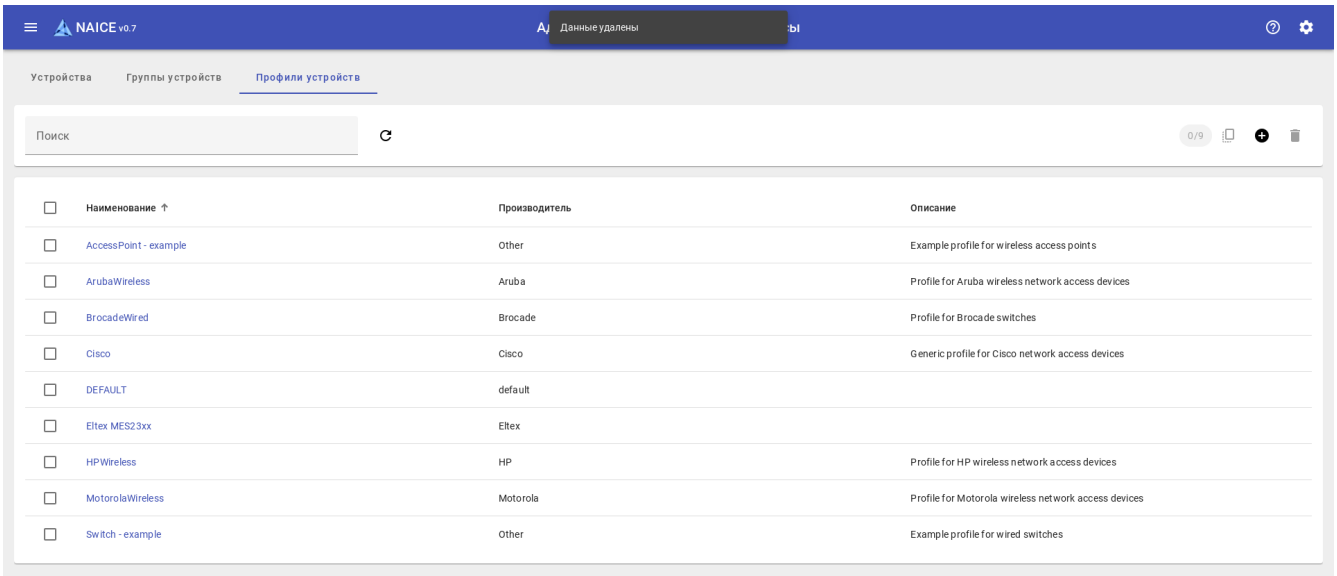

Рисунок 33. Страница просмотра списка профилей устройств после удаления

Ограничения:

- нельзя удалить профиль, который уже назначен какому-то устройству.
- нельзя удалить профиль, который используется в каком-либо профиле авторизации.

Управление идентификацией

Управление пользователями (супликантами) выполняется в меню "Администрирование" → "Управление идентификацией".

В качестве источника данных, используемого для аутентификации пользователей может использоваться внутренний список клиентов (их настройка рассматривается в Пользователи сети) и подключение к внешнему источнику идентификации данных о клиентах Active Directory или LDAP. Здесь же осуществляется работа с конечными устройствами (эндпоинтами).

Меню содержит разделы:

- Пользователи сети - раздел управления учетными данными пользователей, с которыми производится авторизация на устройствах.
- Группы пользователей сети - раздел настроек, позволяющий создать сущности для группировки пользователей.
- Эндпоинты - раздел для работы со списком конечных устройств, которые подключаются к сетевой инфраструктуре.
- Группы эндпоинтов - раздел для работы с группами конечных устройств.
- Внешние источники идентификации - раздел управления внешними источниками идентификации.
- Цепочки идентификаций - раздел настроек, позволяющий составить списки источников учетных данных пользователей.

Пользователи сети

Описание

Раздел "Пользователи сети" предназначен для управления учётными данными пользователей, с которыми производится авторизация на устройствах.

Просмотр пользователей сети

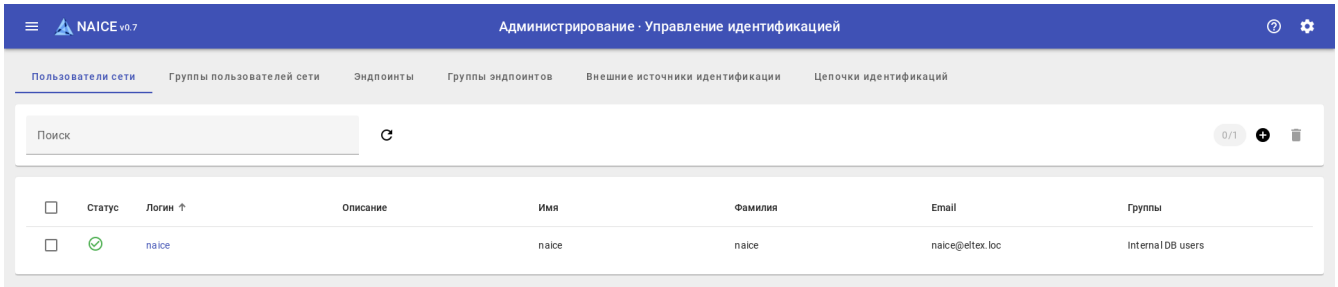

Рисунок 34. Таблица с перечнем пользователей сети на странице просмотра

На данной странице содержится таблица со списком учетных данных пользователей.

Таблица содержит колонки:

- `Статус` - статус пользователя (выключено или включено);
- `Логин` - логин пользователя (должен быть уникальным);
- `Описание` - произвольное описание пользователя;
- `Имя` - имя пользователя;
- `Фамилия` - фамилия пользователя;
- `Email` - адрес электронной почты пользователя;
- `Группы` - группы, в которых состоит пользователь.

Возможна сортировка в прямом и обратном порядке по колонкам "Статус", "Логин", "Описание", "Имя", "Фамилия", "Email" (по всем колонкам, кроме "Группы"). По умолчанию сортировка выполняется в прямом (алфавитном) порядке по полю "Логин".

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
-  - Обновить данные таблицы.
- 0/1 - Счетчик выбранных чекбоксом элементов / общего количества элементов.
-  - Добавить новый элемент.
-  - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  - Изменить текущий порядок сортировки.
-  - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Добавление пользователя

Для добавления пользователя нажмите  в правой части поля над таблицей.

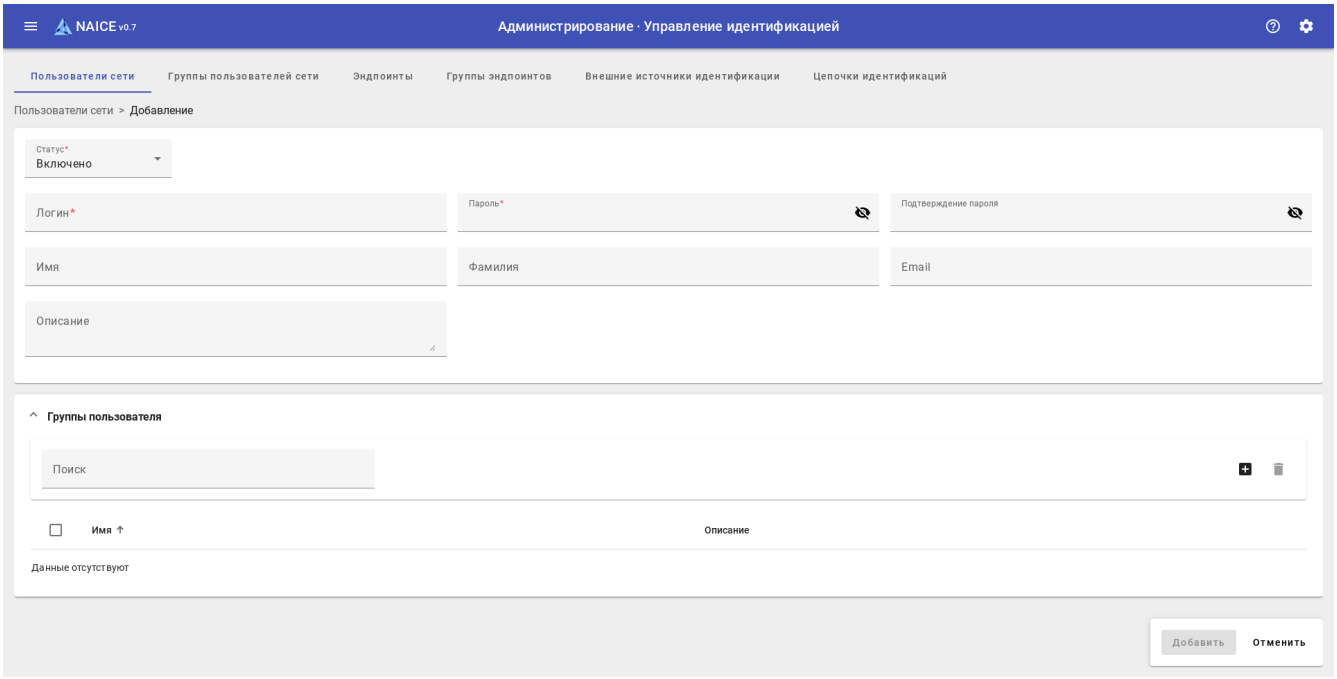

Рисунок 35. Страница добавления пользователя

В открывшейся странице представлены следующие параметры:

- `Статус` * - статус пользователя, может принимать значения "включено" или "выключено". Аутентификация по выключенным учетным данным запрещена.
- `Логин` * - логин пользователя. Максимальная длина логина - 200 символов.
- `Пароль` * - пароль пользователя. Минимальная длина пароля - 8 символов, максимальная - 200 символов. По нажатию на можно включить отображение вводимого пароля, по-умолчанию текст скрыт.
- `Подтверждение пароля` * - поле подтверждения пароля пользователя, должно совпадать со значением из `Пароль`. По нажатию на можно включить отображение вводимого пароля, по-умолчанию текст скрыт.
- `Имя` - имя пользователя. Максимальная длина - 200 символов.
- `Фамилия` - фамилия пользователя. Максимальная длина - 200 символов.
- `Email` - адрес электронной почты пользователя. Должно соответствовать определенному формату (например, naice@eltex.loc) и не превышать 200 символов.
- `Описание` - произвольное описание пользователя. Максимальная длина - 1000 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Также на данной странице находится таблица **Группы пользователя**, в которые входит данный пользователь.

Элементы управления:

- `Поиск` - регистронезависимая фильтрация по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
-

- удалить пользователя из выбранных чекбоксом групп (неактивно, пока не выбрана хоть одна группа).

- - изменить текущий порядок сортировки.
- - чекбокс, который отвечает за выбор групп для выполнения дальнейших действий (например, удаления пользователя из группы).
- - добавить пользователя в группы.

По нажатию появляется окно **Добавление пользователя в группы**, в котором необходимо выбрать группы, куда нужно добавить пользователей.

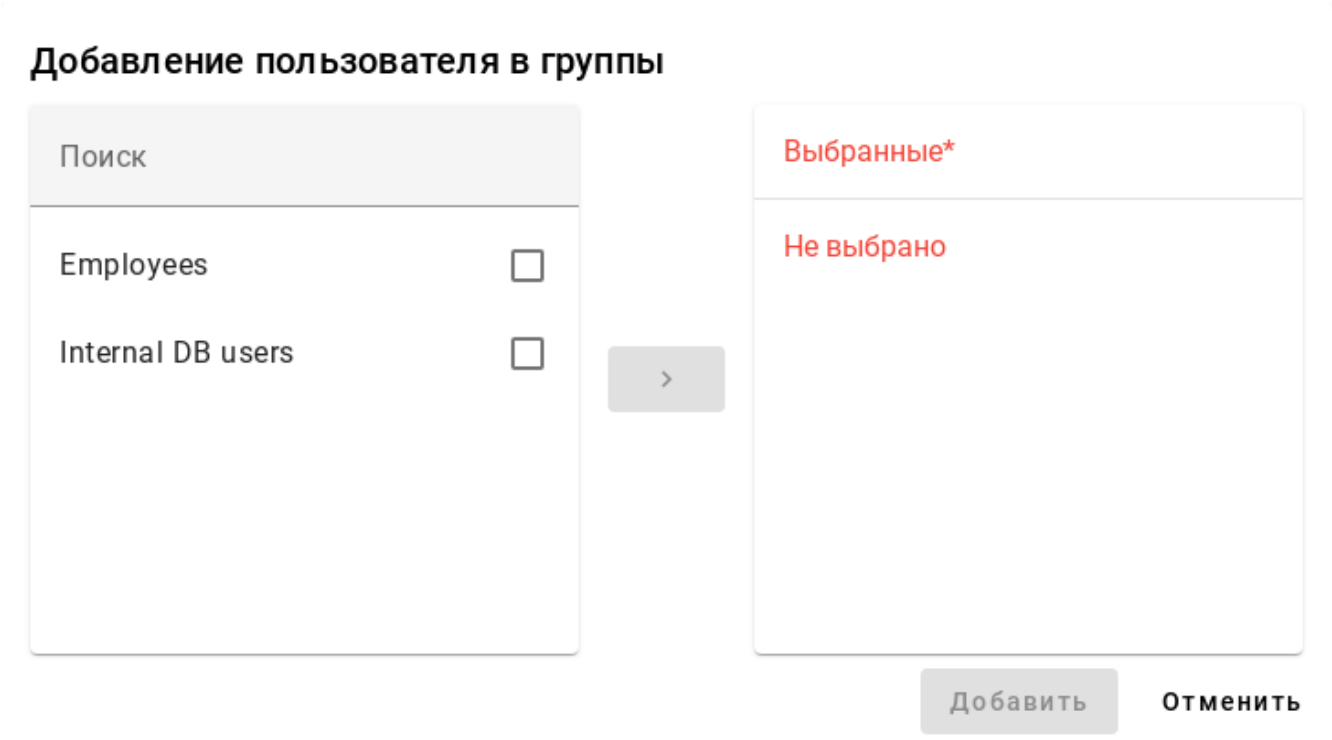

Рисунок 36. Страница добавления пользователя в группы

Элементы управления:

- `Поиск` - регистронезависимый поиск среди пользовательских групп: отображаются только группы, удовлетворяющие условию фильтрации.
- - чекбокс, который отвечает за выбор групп, для назначения пользователю (отображается только для доступных групп).
- - назначить выбранные группы пользователю.
- - удалить группу из списка выбранных для назначения (отображается только для выбранных групп).
- `Добавить` - применить изменения (активна только если что-либо было изменено).
- `Отменить` - отменить изменения.

Для добавления пользователя в список не забудьте нажать `Добавить`. Для сброса изменений и возврата на страницу просмотра нажмите на `Отменить`.

Редактирование пользователя

Для редактирования ранее добавленного пользователя на странице просмотра нажмите на логин в таблице.

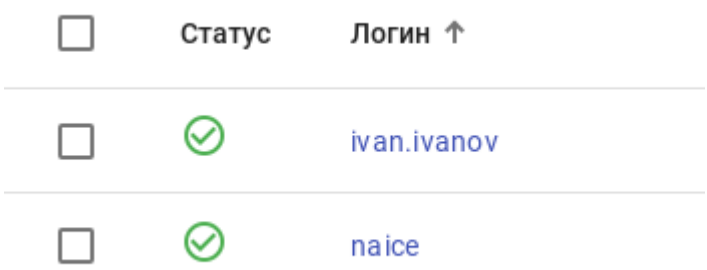

Рисунок 37. Гиперссылка на страницу редактирования пользователя

Откроется страница редактирования.

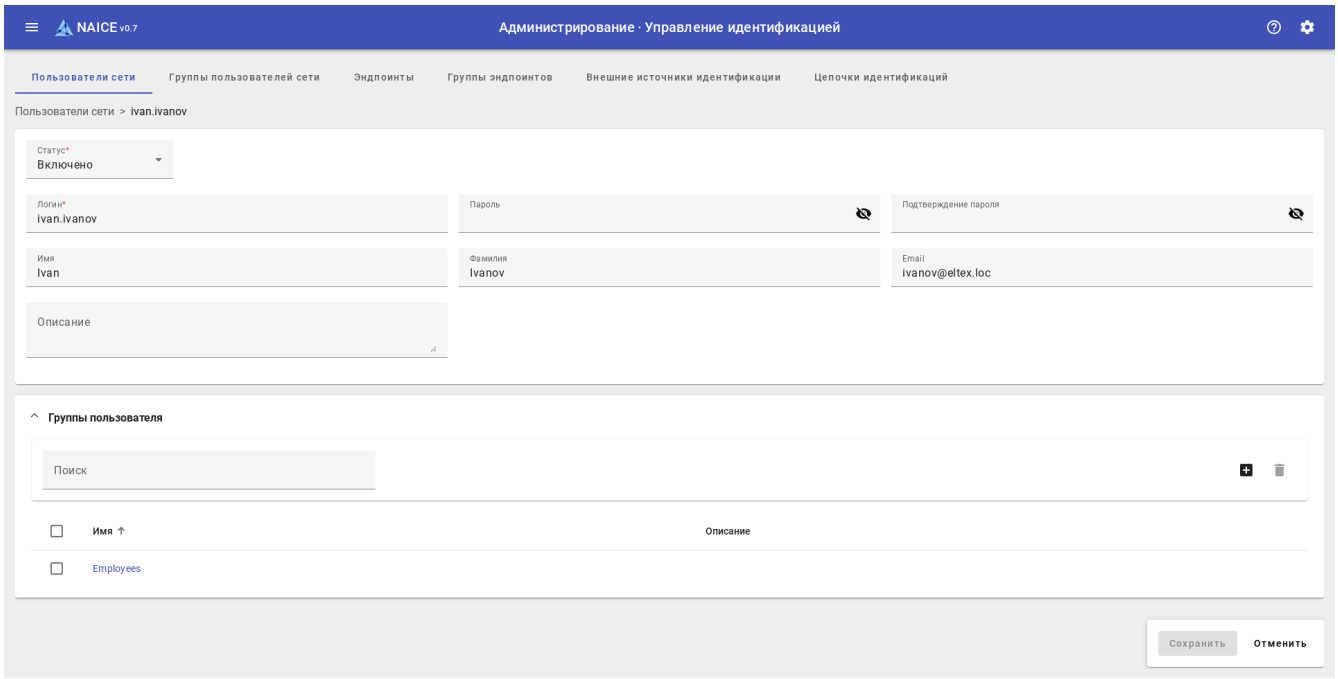

Рисунок 38. Страница редактирования пользователя

Старый пароль пользователя не отображается на странице редактирования!
Если вы не хотите изменять пароль пользователя, то оставьте поля "Пароль" и "Подтверждение пароля" пустыми.

После редактирования нажмите на `Сохранить`. Кнопка будет неактивной пока не изменено хотя бы одно поле.

Удаление пользователя

Для удаления пользователей необходимо на странице просмотра, используя чекбокс ☐, выбрать необходимых пользователей и в правом верхнем углу над таблицей нажать на 🗑.

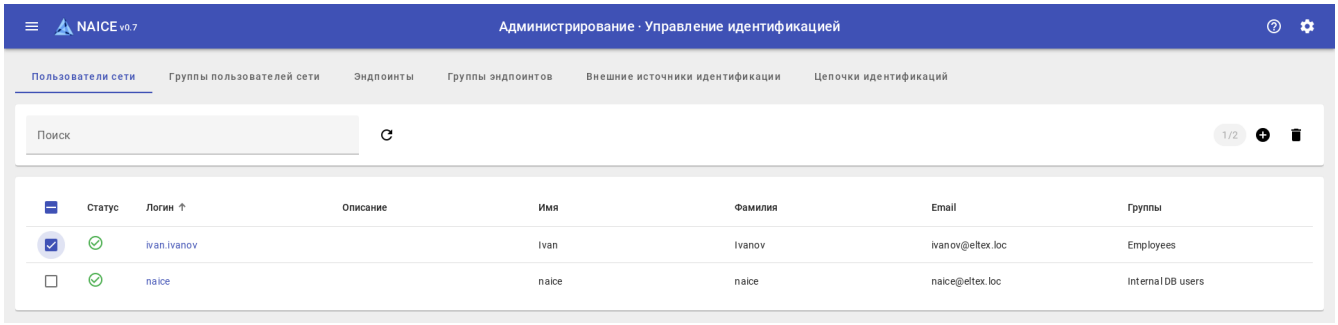

Рисунок 39. Выбор пользователей в таблице для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

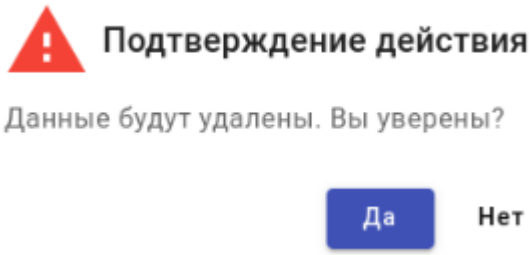

Рисунок 40. Модальный диалог подтверждения

Группы пользователей сети

Описание

Существует возможность объединять пользователей сети в *группы* и использовать в дальнейшем признак принадлежности пользователя к группе при настройке политик доступа.

Раздел "Группы пользователей сети" отвечает за создание, редактирование, удаление и просмотр данных групп.

Просмотр групп пользователей сети

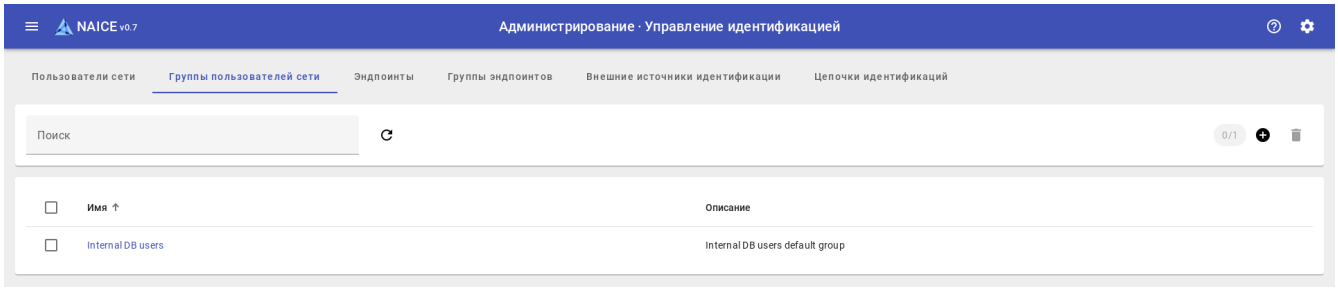

Рисунок 41. Таблица с перечнем групп пользователей сети на странице просмотра

На данной странице содержится таблица со списком всех групп пользователей сети.

Таблица содержит колонки:

- `Имя` - название группы.
- `Описание` - произвольное описание группы.

Возможна сортировка в прямом и обратном порядке по всем колонкам. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по полю "Имя".

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - Обновить данные таблицы.
- `0/1` - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Добавление группы пользователей

Для добавления группы пользователей нажмите в правой части поля над таблицей, откроется страница **Добавление**:

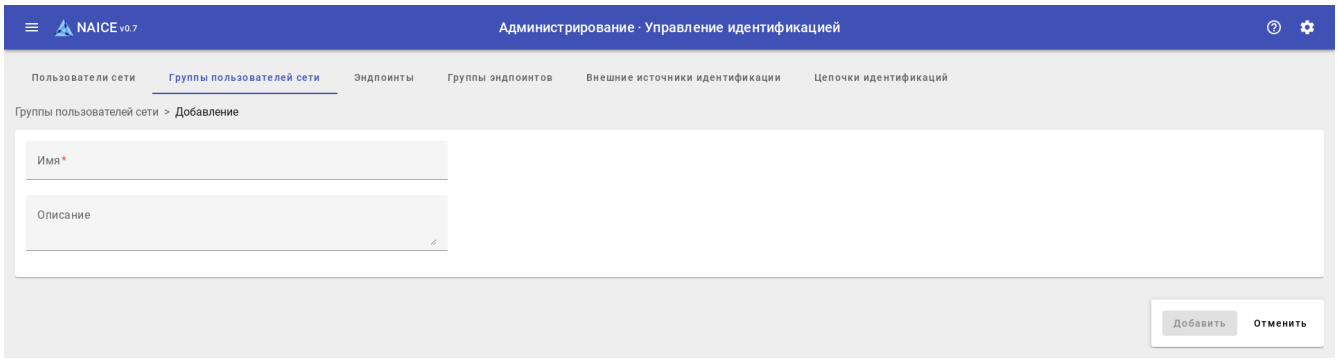

Рисунок 42. Страница добавления группы пользователей

Для заполнения доступны следующие параметры:

- `Имя` * - название группы. Максимальная длина - 200 символов.
- `Описание` - произвольное описание группы. Максимальная длина - 200 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

> Добавление пользователей в группу доступно на странице редактирования ранее добавленной группы.
> На этапе создания группы добавить в нее пользователей нельзя.

Для добавления группы в список групп пользователей не забудьте нажать `Добавить`. Для сброса изменений и выхода на страницу просмотра нажмите на `Отменить`.

Редактирование группы пользователей

Для редактирования ранее добавленной группы на странице просмотра групп пользователей нажмите на имя группы в таблице.

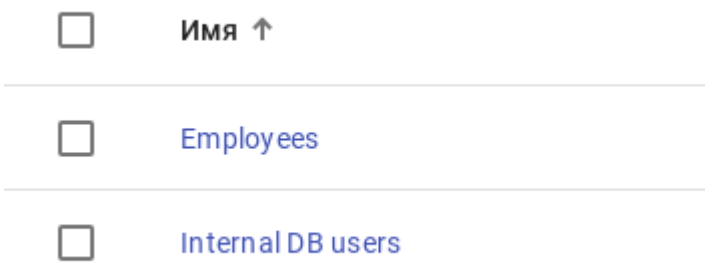

Рисунок 43. Гиперссылка на страницу редактирования группы пользователей

Откроется страница редактирования с возможностью добавления пользователей в группу.

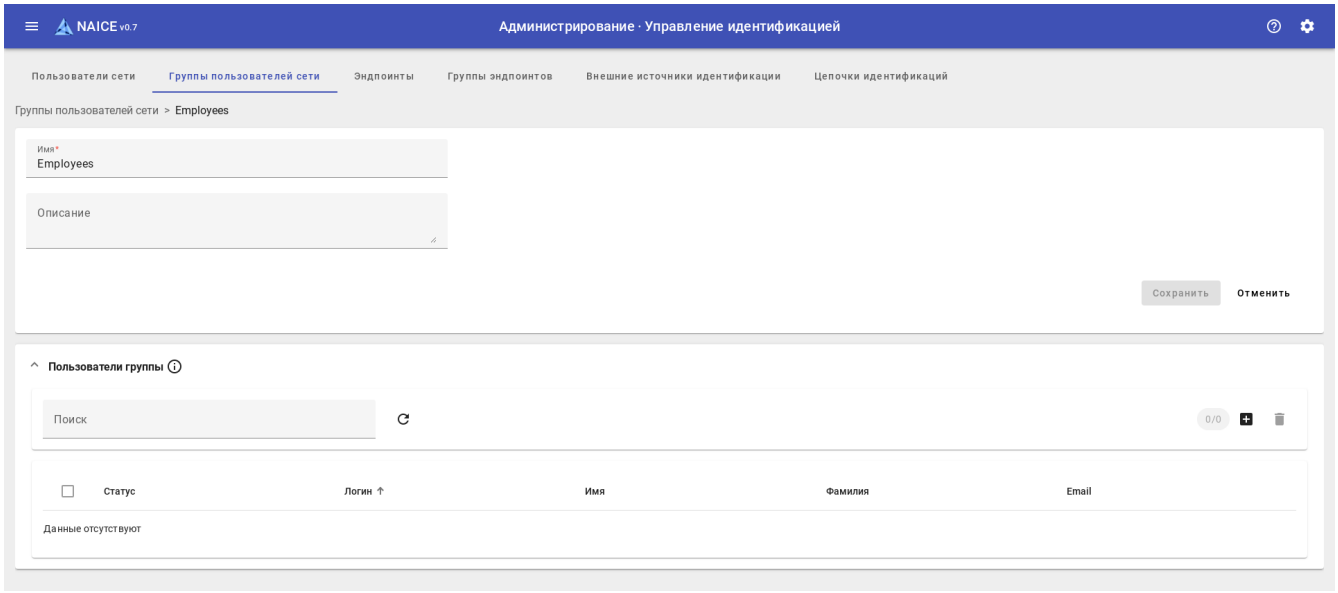

Рисунок 44. Страница изменения группы пользователей

Элементы управления в таблице **Пользователи группы**:

- `Поиск` - регистронезависимая фильтрация по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- 🗑 - удалить выбранных чекбоксом пользователей из группы (неактивно, пока не выбран хоть один пользователь).
- ↑ - изменить текущий порядок сортировки.
- ☐ - чекбокс, который отвечает за выбор пользователей для выполнения дальнейших действий (например, удаления пользователя из группы).
- `0/1` - счетчик выбранных чекбоксом элементов / общего количества элементов.
- ⊞ - добавить пользователей в группу.

По нажатию ⊞ появляется окно **Добавление пользователей в группу**, в котором необходимо выбрать пользователей для добавления в группу.

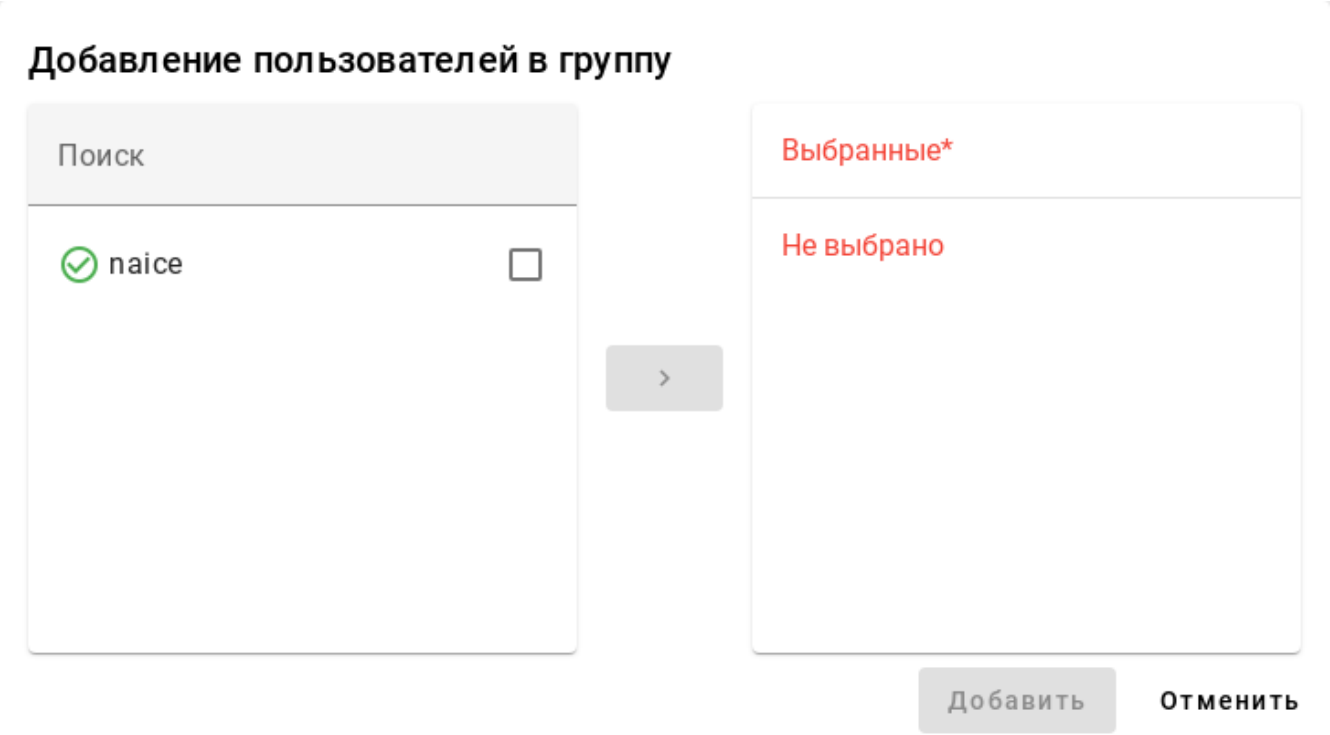

Рисунок 45. Окно добавления пользователей в группу

Элементы управления:

- `Поиск` - регистронезависимый поиск среди пользователей: отображаются только пользователи, удовлетворяющие условию фильтрации.
- ☐ - чекбокс, который отвечает за выбор пользователя для добавления (отображается только в левой колонке).
- › - переместить пользователей, выбранных чекбоксом из доступных, в список выбранных.
- 🗑 - удалить пользователя из списка выбранных (отображается только в правой колонке).
- `Добавить` - применить изменения (активна только если есть изменения).
- `Отменить` - отменить изменения.

> ⚠ Если при редактировании группы изменены только пользователи (имя и описание группы остались прежними), то кнопка `Сохранить` останется неактивной, так как изменения в списке пользователей группы сохраняются автоматически.
> Просто выйдете из режима редактирования по кнопке `Отменить`.

Удаление группы пользователей

Для удаления групп необходимо на странице просмотра, используя чекбокс ☐, выбрать необходимые группы и в правом верхнем углу над таблицей нажать на 🗑.

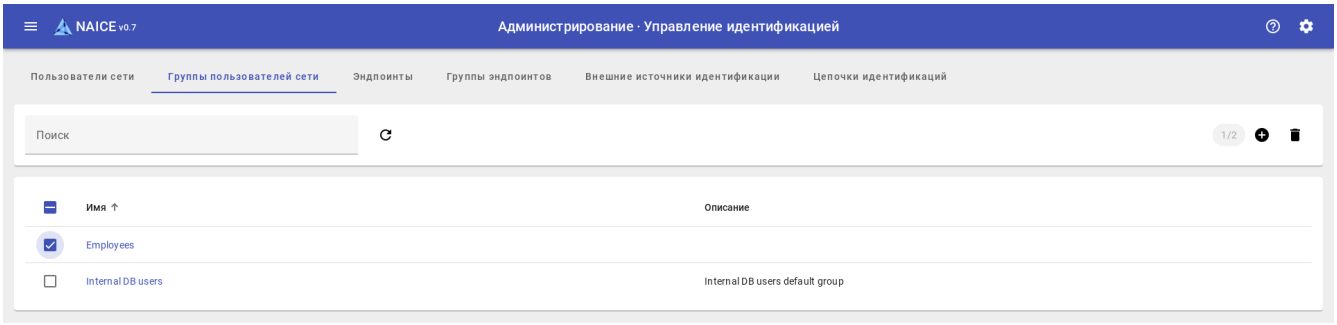

Рисунок 46. Выбор групп пользователей в таблице для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

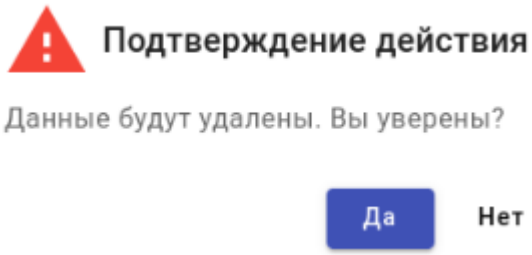

Рисунок 47. Модальный диалог подтверждения

Ограничения:

- нельзя удалить группу, в которой состоят пользователи. В этом случае необходимо сначала удалить из группы всех пользователей, затем удалить пустую группу.
- нельзя удалить группу, которая используется в каком-либо логическом условии.

Эндпоинты

Описание

Эндпоинты - это любые конечные устройства, которые подключаются к сетевой инфраструктуре через устройства-аутентификаторы (такие, как коммутаторы или точки доступа с аутентификацией по протоколу 802.1x или MAB), например - персональные компьютеры, мобильные и IP-телефоны, принтеры, IoT-устройства и другие.

Система NAICE позволяет отслеживать эндпоинты в сети, группировать их по определенным признакам автоматически или вручную, и на основе получаемых в процессе профилирования параметров и политик доступа разрешать или запрещать доступ к сети.

Заполнение таблицы эндпоинтов

Заполнение таблицы эндпоинтов происходит в автоматическом и ручном режиме.

- *в ручном режиме*: добавление эндпоинтов выполняется администратором системы по аналогии с добавлением других сущностей.
-

в автоматическом режиме: добавление эндпоинтов происходит при получении RADIUS-запросов от аутентификаторов в ходе подключения клиентов.

Для определения MAC-адреса добавляемого эндпоинта используется значение атрибута "Calling-Station-Id" RADIUS-запроса.

Случайно сгенерированные MAC-адреса (randomized MAC address) не будут добавлены в качестве эндпоинтов автоматически. При необходимости добавьте такие эндпоинты в ручном режиме.

Просмотр списка эндпоинтов

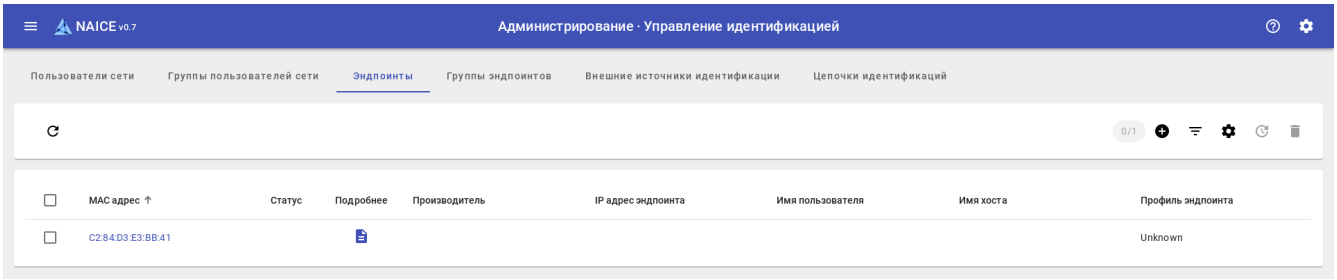

Рисунок 48. Просмотр списка эндпоинтов

На данной странице содержится таблица со списком всех вручную или автоматически добавленных эндпоинтов.

Таблица по умолчанию содержит колонки:

- `MAC адрес` - MAC адрес эндпоинта в формате "XX:XX:XX:XX:XX:XX".
- `Статус` - текущее состояние подключения эндпоинта. Статус отображается после первой попытки аутентификации эндпоинта и может принимать следующие значения:
  - Подключено - устройство успешно прошло аутентификацию и авторизацию и получило доступ к сети;
  - Отклонено - устройство не прошло аутентификацию и не получило доступ к сети;
  - Отключено - устройство отключено от сети.
- `Подробнее` - переход на страницу детальной информации об атрибутах эндпоинта и его последних событий аутентификации.
- `Производитель` - производитель конечного устройства, определенный по первым трем октетам MAC-адреса (MAC OUI).
- `IP адрес эндпоинта` - IP-адрес эндпоинта, информация о котором была получена в ходе профилирования. Для получения данных требуются настройки профилирования.
- `Имя пользователя` - имя пользователя, с которым эндпоинт проходил аутентификацию в последний раз.
- `Имя хоста` - имя хоста эндпоинта, информация о котором была получена в ходе профилирования. Для получения данных требуются настройки профилирования.
- `Профиль эндпоинта` - результат профилирования эндпоинта.

Дополнительно при нажатии на  возможно настроить отображение следующих колонок:

- `Причина ошибки аутентификации` - причина ошибки в ходе подключения клиента.
- `Политика аутентификации` - название правила политики аутентификации, которое было применено в рамках данной сессии;
- `Политика авторизации` - название правила политики авторизации, которое было применено в рамках данной сессии;
- `Протокол аутентификации` - протокол, по которому проходила аутентификация (например, PAP).
- `Тип подключения` - тип подключения, который был определен исходя из настроек профиля сетевого устройства.
- `Тип эндпоинта` - логический профиль, которому принадлежит устройство в результате профилирования.
- `Дата последней активности` - дата, когда последний раз была предпринята попытка подключения клиента (успешная или неуспешная).
- `Группа эндпоинта` - группа, в которою автоматически или вручную был помещен эндпоинт.
- `Имя NAS` - имя устройства-аутентификатора.

Возможна сортировка в прямом и обратном порядке по колонкам `MAC адрес`, `Статус`, `Производитель`, `IP адрес эндпоинта`, `Имя пользователя`, `Профиль эндпоинта`, `Дата последней активности` (по умолчанию), `Группа эндпоинта`.

Страница содержит следующие элементы управления:

-  - Обновить данные таблицы.
-  - Счетчик выбранных чекбоксом элементов / общего количества элементов.
-  - Добавить новый элемент.
-  - Открыть окно настройки фильтрации данных по таблице.
-  - Настроить отображение колонок таблицы.
-  - Запустить процесс перепрофилирования выбранных эндпоинтов (неактивно, пока не выбран хоть один элемент).
-  - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  - Изменить текущий порядок сортировки.
-  - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Фильтрация данных в таблице настраивается в следующем окне:

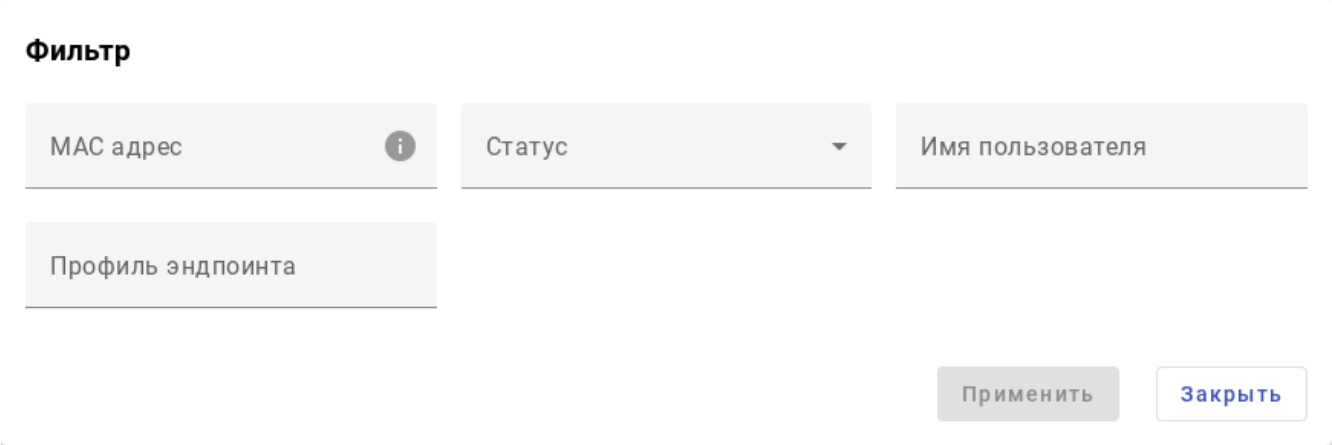

Рисунок 49. Настройка фильтрации данных в таблице

Фильтрация доступна по параметрам `Профиль эндпоинта`, `MAC адрес`, `Статус` и `Имя пользователя`.

В настройках таблицы можно сменить состав отображаемых колонок.

Кнопка выбирает или снимает выбор всех колонок для отображения.

Кнопка предназначена для сброса настроенных колонок к состоянию по умолчанию (неактивно, пока состоянию по умолчанию не изменено).

Добавление эндпоинта

Эндпоинты добавляются в систему автоматически в ходе попыток аутентификации. При необходимости можно добавить эндпоинт вручную. Для добавления эндпоинта нажмите в правой части поля над таблицей.

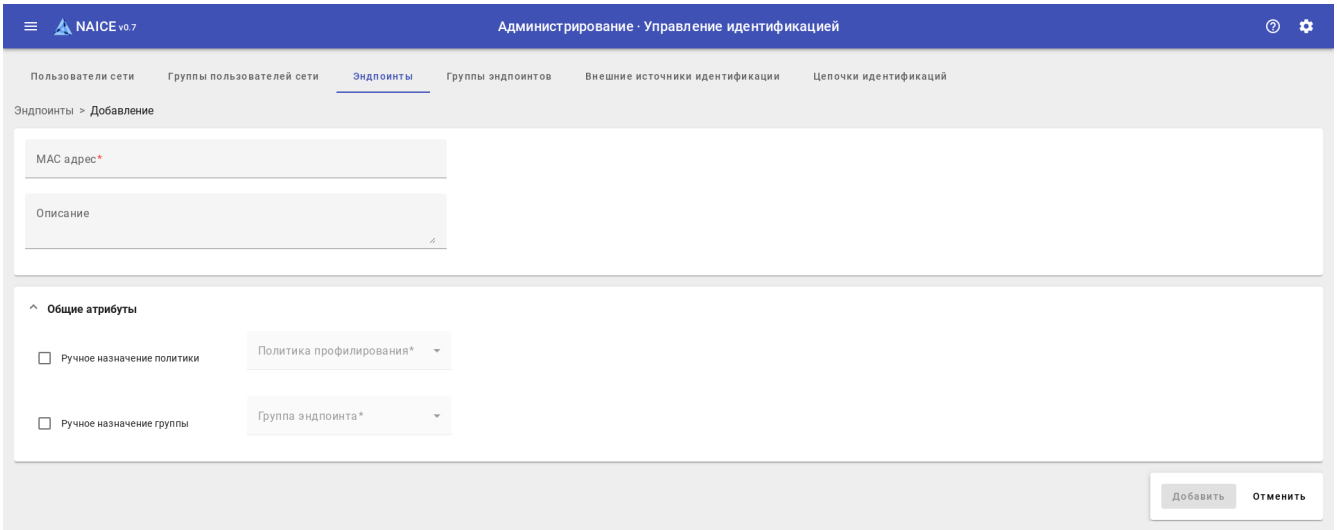

Рисунок 50. Добавление эндпоинта

На открывшейся странице представлены следующие параметры:

- `MAC адрес` * - MAC адрес эндпоинта.
- `Описание` - произвольное описание длиной до 200 символов.
- `Ручное назначение политики` - назначить для данного эндпоинта политику профилирования вручную. Данное значение не будет перезаписано в результате профилирования.

`Ручное назначение группы` - назначить для данного эндпоинта группу вручную. Данное значение не будет перезаписано в результате профилирования.

Параметры, отмеченные символом *, обязательны для заполнения.

Для добавления эндпоинта в список эндпоинтов не забудьте нажать **Добавить**. Для сброса изменений и возврата на страницу просмотра нажмите на **Отменить**.

Редактирование эндпоинта

Для редактирования ранее добавленного эндпоинта на странице просмотра нажмите на MAC адрес эндпоинта в таблице.

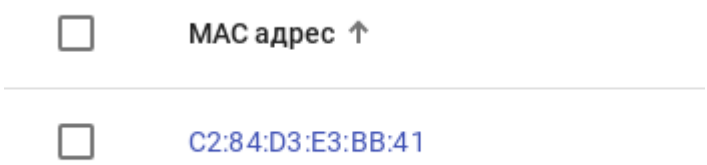

Рисунок 51. Гиперссылка на страницу редактирования эндпоинта

Откроется страница редактирования, аналогичная странице добавления.

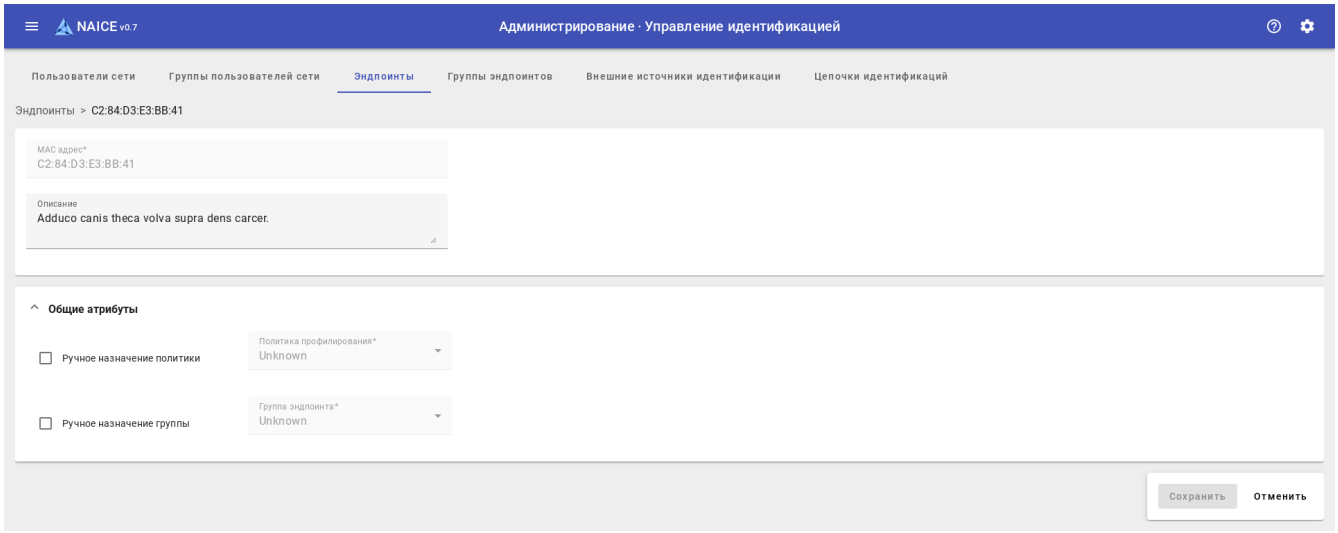

Рисунок 52. Редактирование эндпоинта

Редактирование MAC адреса эндпоинта недоступно.
Если необходимо отредактировать адрес, то удалите и создайте эндпоинт заново.

После редактирования нажмите на **Сохранить**. Кнопка останется неактивной пока не будет изменено хотя бы одно поле.

Просмотр детальной информации об эндпоинте

Для просмотра детальной информации об эндпоинте нажмите на  в колонке `Подробнее` в таблице. В браузере будет открыта новая вкладка с нужной страницей.

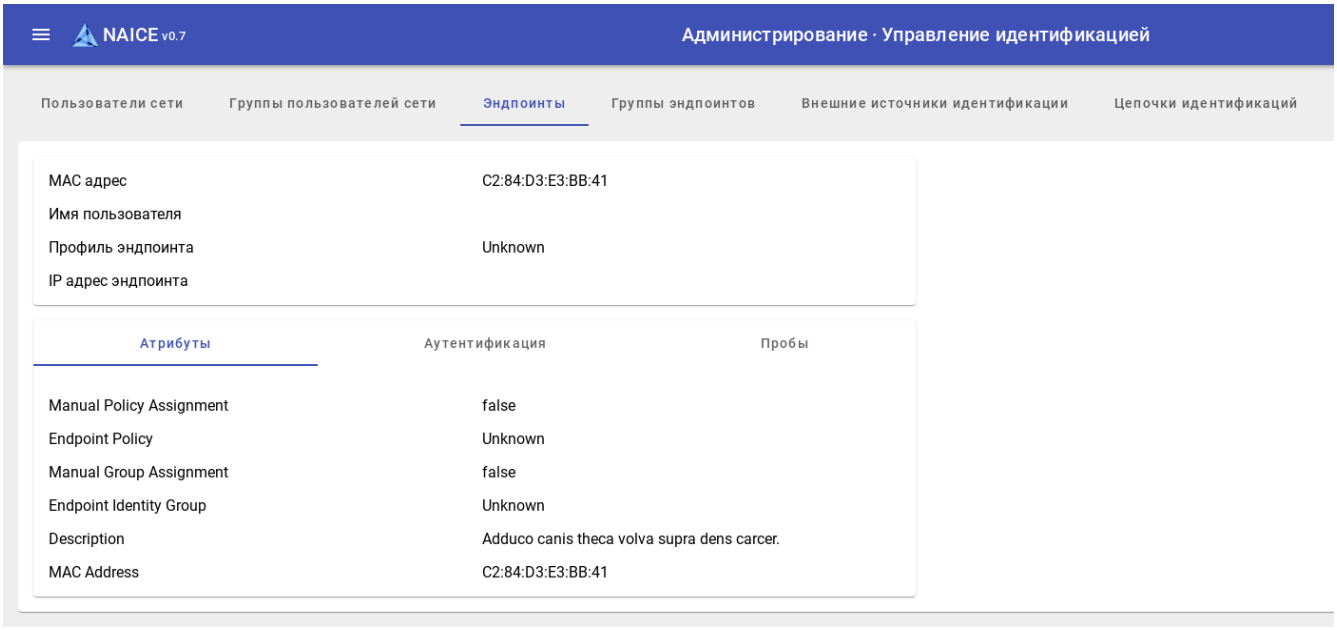

Рисунок 53. Просмотр детальной информации об эндпоинте

Информация на странице разделена на 4 блока:

- Краткая и наиболее важная информация об эндпоинте;
- **Атрибуты** - атрибуты эндпоинта, которые были получены в результате профилирования или заданы администратором;
- **Аутентификация** - данные о последней аутентификации эндпоинта:
  - `Общая информация` - краткая информация о результатах последнего подключения эндпоинта, отображается только если были попытки подключения;
  - `Детали аутентификации` - детальная информация, которая может быть полезна для отладки;
  - `Прочие атрибуты` - содержание пакета, полученного NAICE от RADIUS-сервера;
  - `Результат` - список атрибутов, которыми был обогащен ответ клиенту в результате авторизации (например, атрибуты для выдачи VLAN или ACL). Если выдача дополнительных атрибутов не настроена в профиле авторизации, то список будет пуст.
- **Пробы** - данные, которые могут быть использованы в настройках условий профилирования.

До окончания профилирования и до первой аутентификации страница может быть практически пуста. В таком случае вернитесь на страницу через некоторое время.

Удаление эндпоинта

Таблица эндпоинтов заполняется автоматически в процессе нормальной работы NAICE в ходе попыток подключения эндпоинтов. При удалении эндпоинта он будет повторно изучен при следующей попытке подключения. Отключить автоизучение эндпоинтов нельзя.

Для удаления эндпоинта необходимо на странице просмотра, используя чекбокс ☐, выбрать необходимые эндпоинты и в правом верхнем углу над таблицей нажать на 🗑.

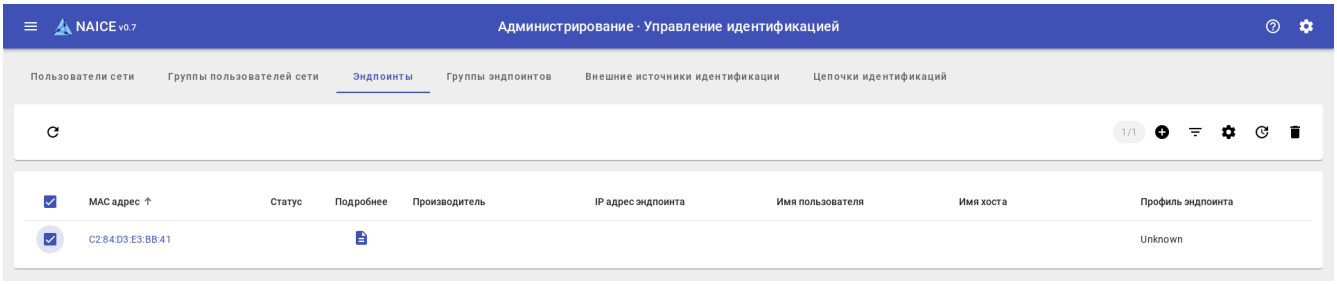

Рисунок 54. Выбор эндпоинтов в таблице для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

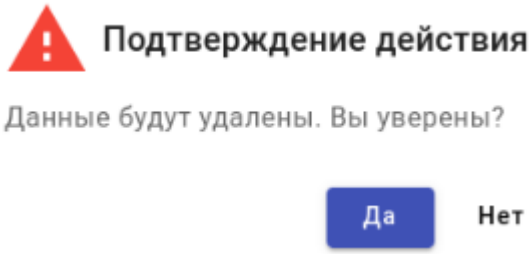

Рисунок 55. Модальный диалог подтверждения

Группы эндпоинтов

Описание

Группы эндпоинтов - это совокупность эндпоинтов, объеденных в группы по логическому признаку.

Система NAICE позволяет отслеживать эндпоинты в сети, группировать их вручную или автоматически, на основе получаемых в процессе профилирования параметров.

Просмотр всех групп

При переходе на вкладку "Группы эндпоинтов", открывается панель просмотра всех групп.

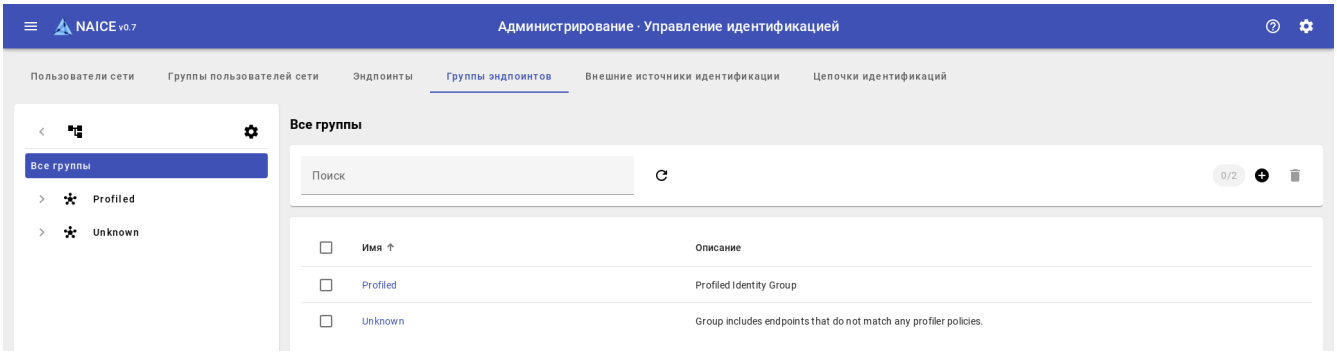

Рисунок 56. Просмотр списка групп эндпоинтов

Таблица содержит колонки:

- `Имя` - Имя группы
- `Описание` - Полное описание группы

Элементы управления:

`Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.

- - Обновить данные таблицы.
- `0/1` - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

В левой стороне располагается панель быстрого просмотра в виде дерева или списка

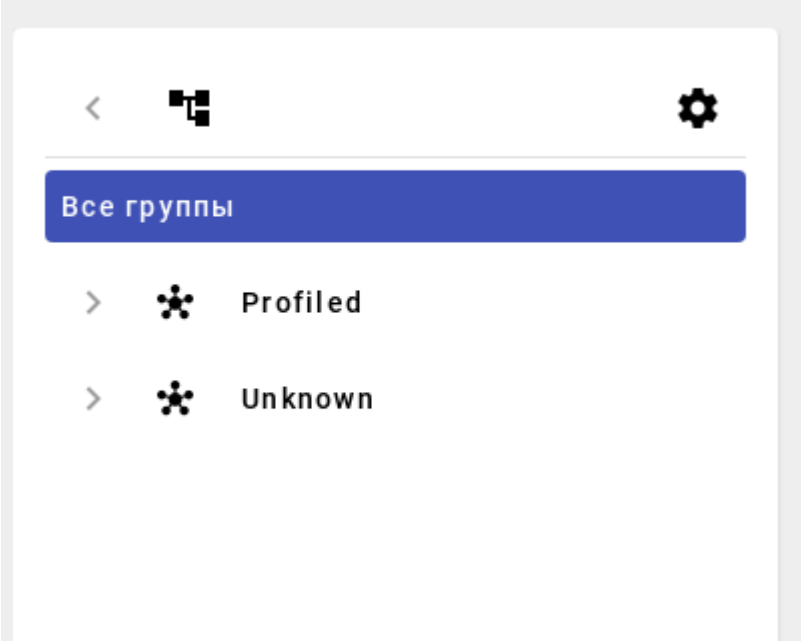

Рисунок 57. Меню навигации по дереву групп эндпоинтов

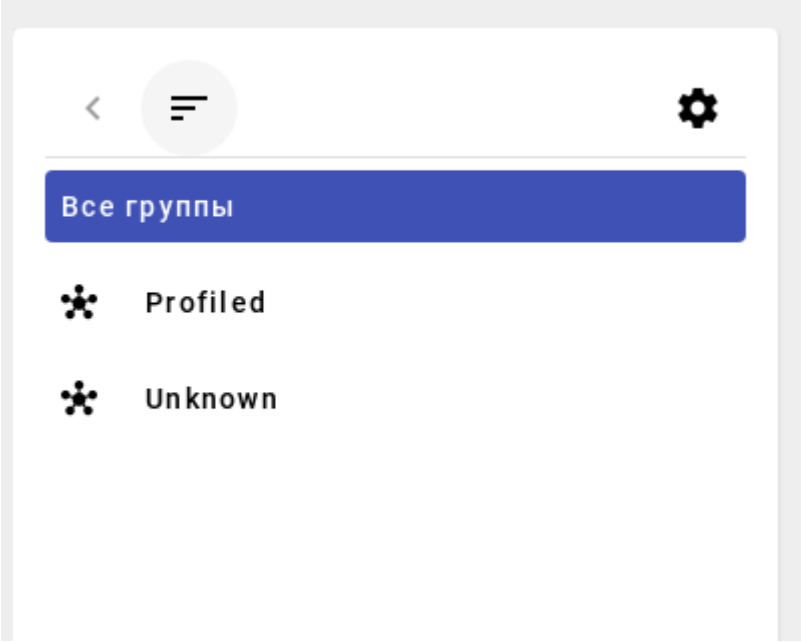

Рисунок 58. Вид Меню навигации в режиме списка

Содержит следующие элементы управления:

- `Все группы` - открыть таблицу с просмотром и администрированием всех групп
- ⚙ - Выбор доступных действий (зависит от выбранного элемента в дереве):
  - `Добавить корневую группу`
  - `Добавить дочернюю группу`
  - `Удалить группу`
- - включен режим отображения в виде дерева
- - включен режим отображения в виде списка
- - переход на уровень выше (активно только в режиме списка).
- - в режиме дерева отображается слева от наименования групп, имеющих дочерние элементы, если список закрыт. В режиме списка отображается справа от наименования групп, имеющих дочерние элементы.

Добавление группы

Для добавления группы нажмите ⊕ в правой части поля над таблицей, откроется страница **Добавление**:

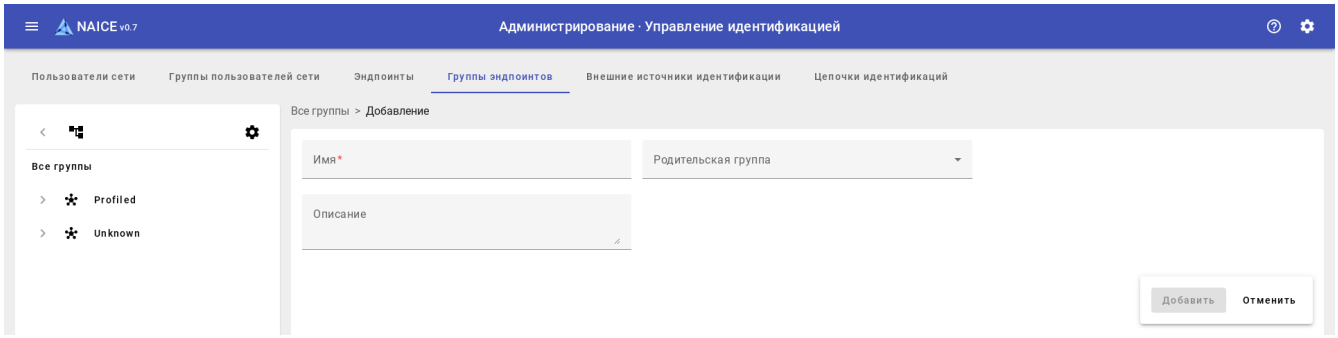

Рисунок 59. Форма добавления группы эндпоинтов

Для заполнения доступны следующие параметры:

- `Имя` * - название группы. Максимальная длина - 100 символов.
- `Родительская группа` - выбор родительской группы из списка. Настройка родительской группы доступна только в момент создания группы по кнопке ⊕.
- `Описание` - произвольное описание группы. Максимальная длина - 200 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Также создать группу можно по кнопке ⚙ на панели навигации по дереву групп - `Добавить корневую группу`, `Добавить дочернюю группу`

Перемещение групп (смена родительской группы) после создания не предусмотрены.

Редактирование группы

Для редактирования ранее добавленной группы на странице просмотра нажмите на имя группы в таблице или дереве.

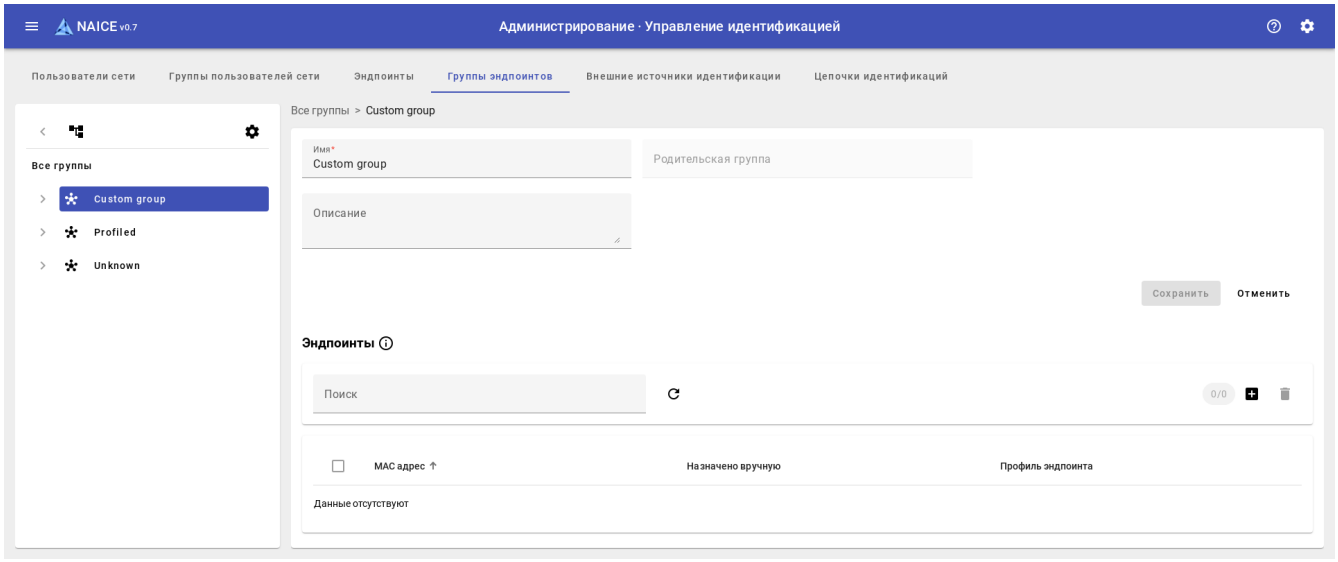

Рисунок 60. Форма редактирование группы эндпоинтов

Для изменения доступны:

- `Имя` * - название группы. Максимальная длина - 100 символов.
- `Описание` - произвольное описание группы. Максимальная длина - 200 символов.

После редактирования нажмите на **Сохранить**. Кнопка останется неактивной пока не будет изменено хотя бы одно поле.

Добавление эндпоинтов в группу

На странице редактирования группы в нижней части располагается таблица **Эндпоинты**.

Таблица содержит колонки:

- `MAC адрес` - MAC-адрес эндпоинта;
- `Назначено вручную` - признак добавления эндпоинта в группу вручную;
- `Профиль эндпоинта` - профиль, назначенный эндпоинту.

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - Обновить данные таблицы.
- 0/1 - Счетчик выбранных чекбоксом элементов / общего количества элементов.

- Добавить новый элемент.

- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

При удалении эндпоинта из группы ему автоматически назначается группа **"Unknown"**.

Для добавления эндпоинта в группу нажмите на . Откроется всплывающее окно, в котором необходимо выбрать эндпоинты для добавления в группу с помощью чекбоксов и перенести в список "Выбранные" по кнопке .

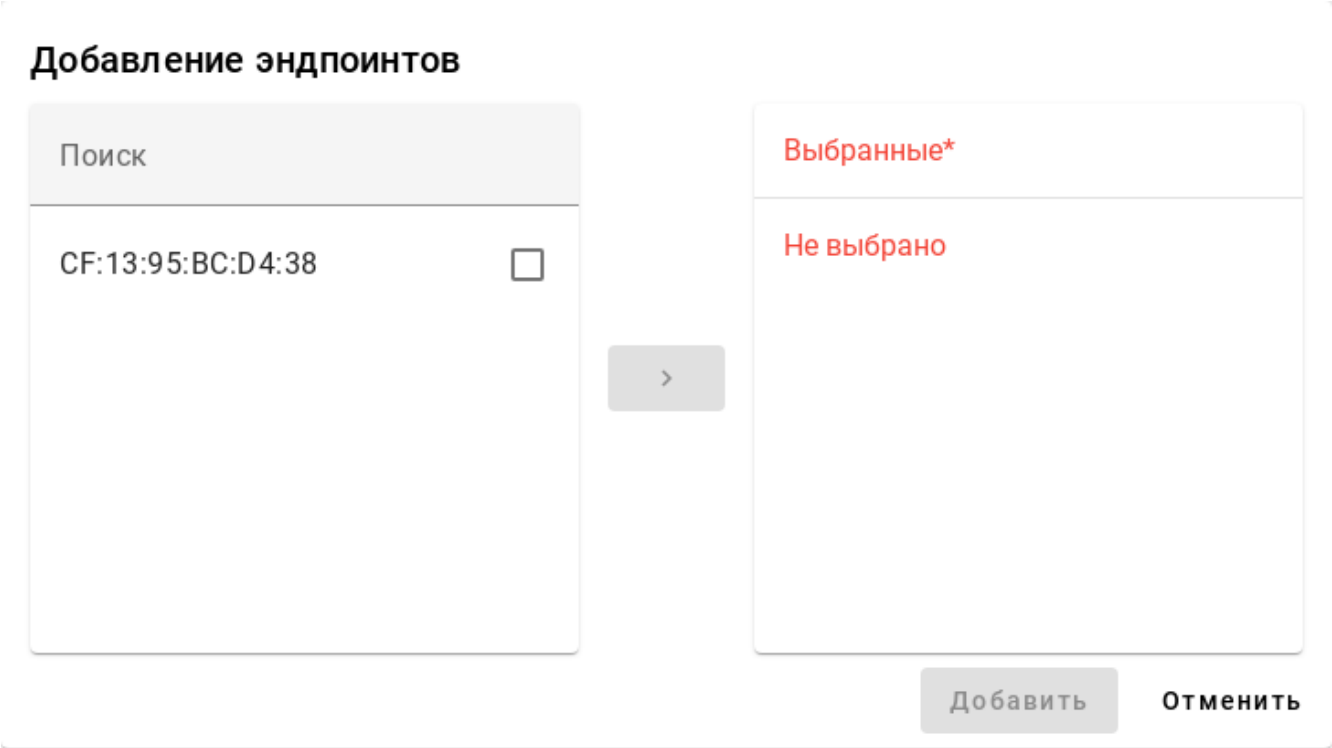

Рисунок 61. Модальный диалог добавления эндпоинтов

После выбора всех необходимых эндпоинтов нажмите на **Добавить**. Кнопка останется неактивной пока не будет выбран хотя бы один эндпоинт.

Все изменения в таблице **Эндпоинты** применяются автоматически и не требуют нажатия кнопки **Сохранить**. Действие кнопки сохранения распространяются на параметры группы.

Удаление группы

Для удаления групп необходимо на странице просмотра, используя чекбокс , выбрать необходимые группы и в верхней правой части таблицы нажать на .

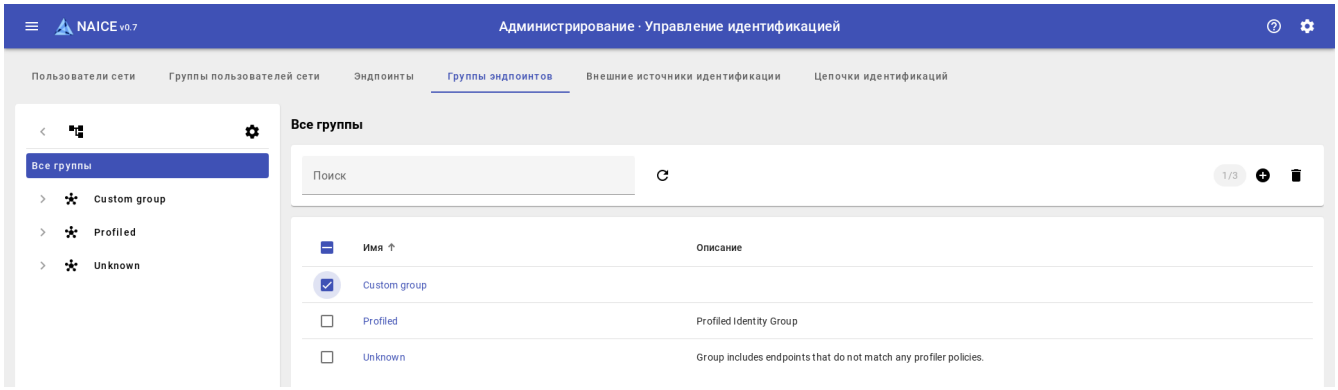

Рисунок 62. Выбор групп для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

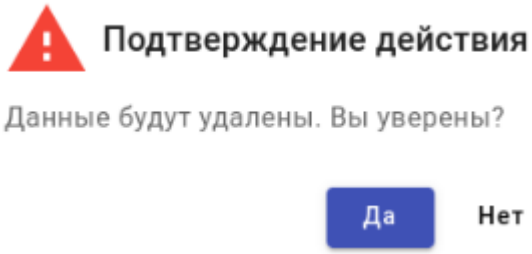

Рисунок 63. Модальный диалог подтверждения

Ограничения:

- нельзя удалить группу, которая имеет дочернюю группу;
- нельзя удалить группу в которой есть эндпоинты;
- нельзя удалить системные группы Profiled и Unknown.

Внешние источники идентификации

Описание

В качестве источника данных, используемого для аутентификации пользователей, помимо внутренней базы пользователей могут использоваться внешние источники идентификации данных о клиентах такие как MS Active Directory или LDAP.

В данном разделе производится настройка подключения к внешним источникам и добавление групп пользователей и/или атрибутов, которые в дальнейшем могут быть использованы при настройке политик доступа.

Просмотр внешних источников идентификации

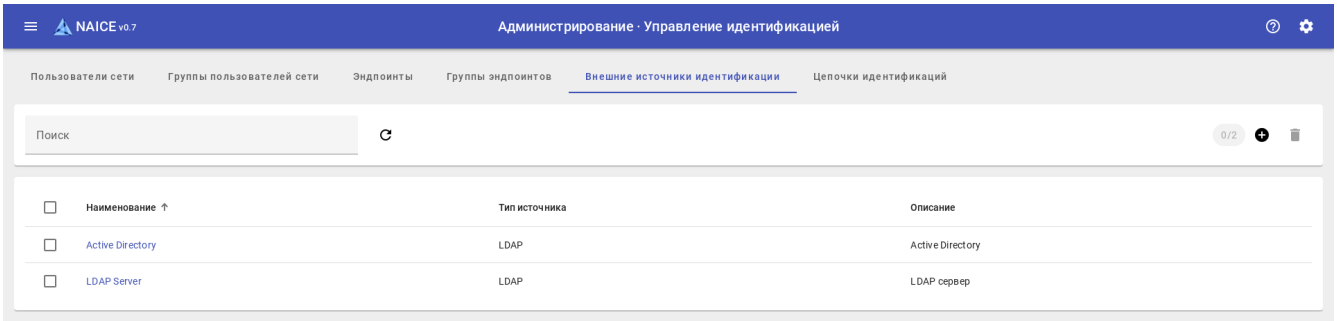

Рисунок 64. Просмотр внешних источников идентификации

На данной странице содержится таблица со списком внешних источников идентификации.

Таблица содержит колонки:

- `Наименование` - наименование источника.
- `Тип источника` - тип источника.
- `Описание` - произвольное описание источника.

Возможна сортировка в прямом и обратном порядке по колонкам `Наименование`, `Описание`. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по полю `Наименование`.

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - Обновить данные таблицы.
- 0/1 - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

> Поддержано взаимодействие с источниками идентификации типа "MicroSoft Active Directory" и "LDAP".
> Для каждого источника идентификации существуют определенные условия настройки и ограничения.

Настройка взаимодействия с каждым типом источника идентификации далее рассматривается отдельно.

Добавление источника идентификации типа Active Directory

Требования

В Active Directory должен быть заведен пользователь для взаимодействия с Eltex-NAICE, имеющий права:

- Выполнять поиск в Active Directory
- Добавлять компьютер в Active Directory
- Получать информацию о всех пользователях и группах домена

Также настройках пользователя необходимо отключить опцию "требовать смену пароля при первом подключении" (включена по умолчанию)

DNS-сервер, который будет использоваться хостом с установленным Eltex-NAICE, должен разрешать полное имя домена, в котором будет работать Eltex-NAICE, и полное имя контроллера AD.

Обращение Eltex-NAICE к Active Directory выполняется по портам:

Протокол	Порт	Назначение	Примечание
UDP	53	DNS	Сервер, отвечающий за разрешение доменных имен может быть отдельным от сервера Active Directory
TCP/UDP	88	Kerberos	
TCP/UDP	389	LDAP/CLDAP	
TCP/UDP	445	SMB	
TCP/UDP	3268	LDAP/CLDAP	Можно использовать вместо порта 389, если нет леса деревьев
TCP/UDP	49152-65535	RPC Dynamic Port Range	

Настройка подключения

В настройках переменных Ansible необходимо указать параметры взаимодействия с "Active Directory" и повторно выполнить плейбук "common-freeradius.yml" (если это не было сделано ранее).

В плейбуке Ansible в файле "ansible/group_vars/all.yml" необходимо отредактировать параметры:

```
# Включить интеграцию с MS AD:
use_ms_ad: true

# Указать IP адрес сервера "Active Directory":
radius_ms_ad_ip: '172.16.4.115'

# Указать логин подключения к серверу:
radius_kerberos_ad_user_login: 'fill_login'

# Указать пароль подключения к серверу:
radius_kerberos_ad_user_password: 'fill_password'

# Все доменный имена указывать заглавными буквами!
# Указать домен рабочей группы, в которой будет происходить авторизация:
radius_kerberos_workgroup: 'WS'

# Указать полностью домен:
radius_kerberos_kdc: 'WS.LOC'

# Указать полный адрес сервера Microsoft Active Directory {имя MS Windows Server}.{Домен MS
AD} например LABMS - имя сервера, WS.LOC домен MS AD
radius_kerberos_admin_server: 'LABMS.WS.LOC'

# Если необходимо поместить компьютер в нестандартый OU в MS AD, то укажите его полную
структуру от корня (например, "Building1/Cabinet1").
# Если необходимо оставить поведение по умолчанию, то оставьте значение переменной без
изменения.
radius_samba_ou_structure: 'Computers'
```

После этого повторно выполнить плейбук установки NAICE:

```
ansible-playbook --ask-become-pass common-naice-services.yml
```

После выполнения плейбука необходимо убедиться, что сервер с Eltex-NAICE появился в списке "Computers" "Active Directory" или в другой структуре, настроенной в `radius_samba_ou_structure`:

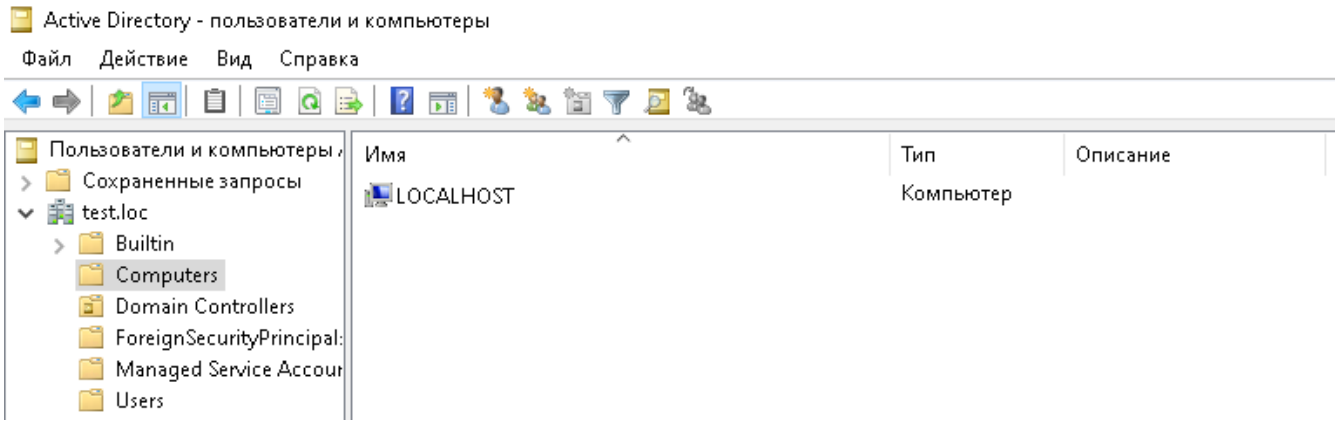

Рисунок 65. Active Directory - пользователи и компьютеры

В качестве имени компьютера будет выступать имя сервера с Eltex-NAICE.

На сервере с Eltex-NAICE для проверки корректности включения в "Active Directory" можно выполнить команду:

```
sudo net ads testjoin -U <логин подключения к серверу>
Join is OK
```

В случае возникновения проблем с подключением к "Active Directory" следует внимательно проверить настройки плейбука и повторить его выполнение.

Добавление источника идентификации

Для добавления источника идентификации нажмите  в правой части поля над таблицей, откроется следующая страница.

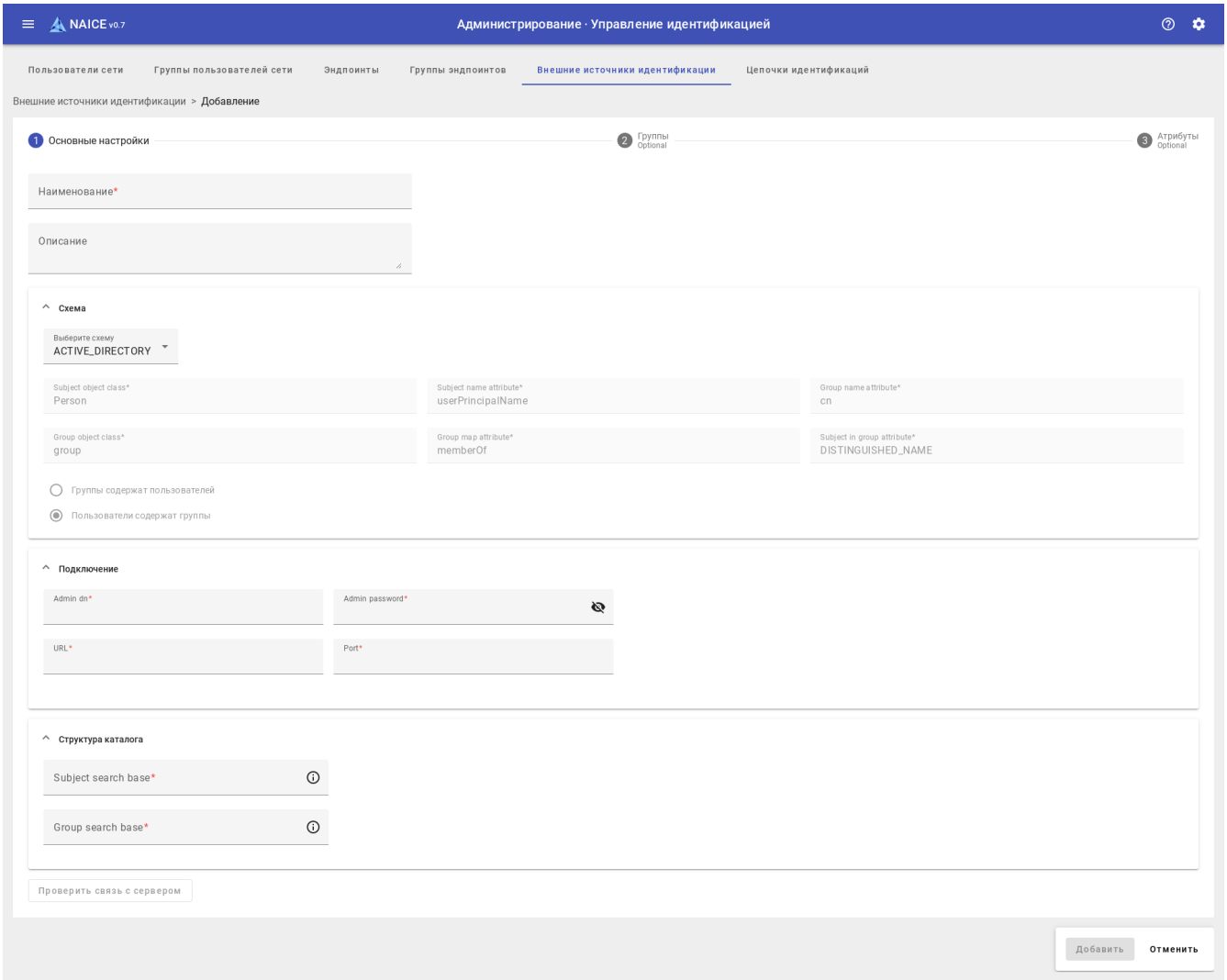

Рисунок 66. Окно добавления источника идентификации

В данной форме представлены следующие параметры:

- Блок **Основные настройки**:
  - `Наименование` * - наименование источника идентификации.
  - `Описание` - описание.
- Блок **Схема**:

- `Выберите схему` * - схема атрибутов источника идентификации. По умолчанию выбрана "ACTIVE_DIRECTORY", для данной схемы значение атрибутов предустановлено и не может быть изменено.

- Блок **Подключение**:
  - `Admin dn` * - данные административного пользователя для взаимодействия с Active Directory (в формате <пользователь>@<домен>).
  - `Admin password` * - пароль административного пользователя. По умолчанию не отображается, для просмотра требуется нажать  .
  - `URL` * - IP-адрес или доменное имя сервера Active Directory.
  - `Port` * - порт подключения (как правило используется TCP:389).
- Блок **Структура каталога**:
  - `Subject search base` * - контекст для поиска атрибутов записей службы каталогов.
  - `Group search base` * - контекст для поиска групп службы каталогов.
    Оба поля имеют формат вида перечисления через запятую атрибут=значение, например dc=test,dc=loc или ou=naice test,dc=test,dc=loc. Подробнее о формате вводимых в этом поле данных можно узнать при наведении на  или в подсказке ниже.
- `Проверить связь с сервером` - проверить корректность настроек и связь с сервером Active Directory.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Максимальная длина поля `Наименование` - 64 знаков. У остальных полей - 200 знаков.

Допустимые символы при вводе параметров Subject search base и Group search base:

- пробел,
- двойные кавычки (""),
- знак равенства (=),
- запятая (,),
- дефис (-),
- латинские буквы (a-z)(A-Z),
- русские буквы (а-я)(А-Я),
- цифры (0-9).

Ввод других элементов запрещен.

Система при сохранении автоматически удаляет пробелы возле знака равенства (=) и запятой (,), значение с пробелом берется в двойные кавычки. Значение атрибута, введенное слева от знака равенства (=), переводится в нижний регистр.

Пример:

Введённое значение	Сохранённое значение
ou=naice test, dc = test ,dc = loc	ou="naice test",dc=test,dc=loc
ou="naice test",dc = test,dc=loc	ou="naice test",dc=test,dc=loc

После заполнения всех необходимых данных станет активна кнопка **Добавить** и **Проверить связь с сервером**.

Кнопка **Добавить** становится активной при условии добавления всех параметров и не зависит от успешности проверки связи с сервером.

При успешной проверки связи с сервером появится сообщение вида:

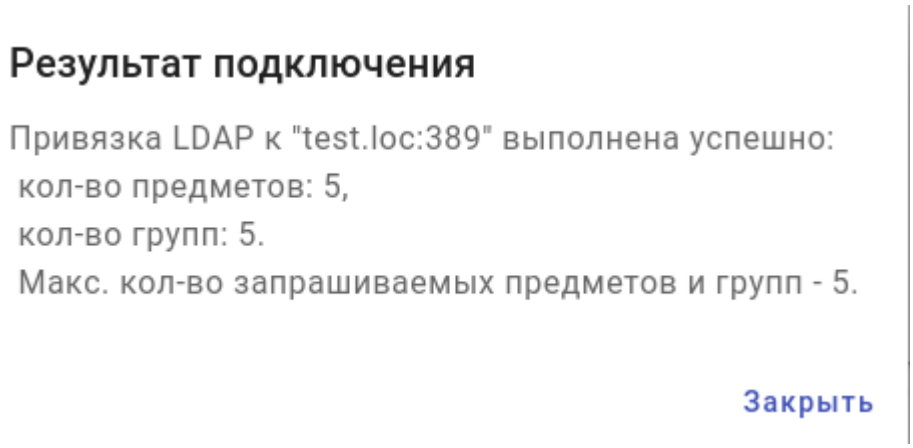

Рисунок 67. Привязка к LDAP выполнена успешно

При проверке соединения запрашивается не более 5 предметов и групп, что бы не вызывать лишнюю нагрузку на сервер, поэтому если реальных пользователей или групп больше все равно будет показано число "5" - это не свидетельствует о проблеме.

Добавление групп пользователей

Для возможности аутентификации через внешний источник идентификации добавление групп не является обязательным. Группы можно использовать в политиках авторизации пользователей.

После добавления источника идентификации кнопка **Добавить** примет значение **Далее**. Так же можно выполнить переход нажав на надпись **(2) Группы**, откроется страница:

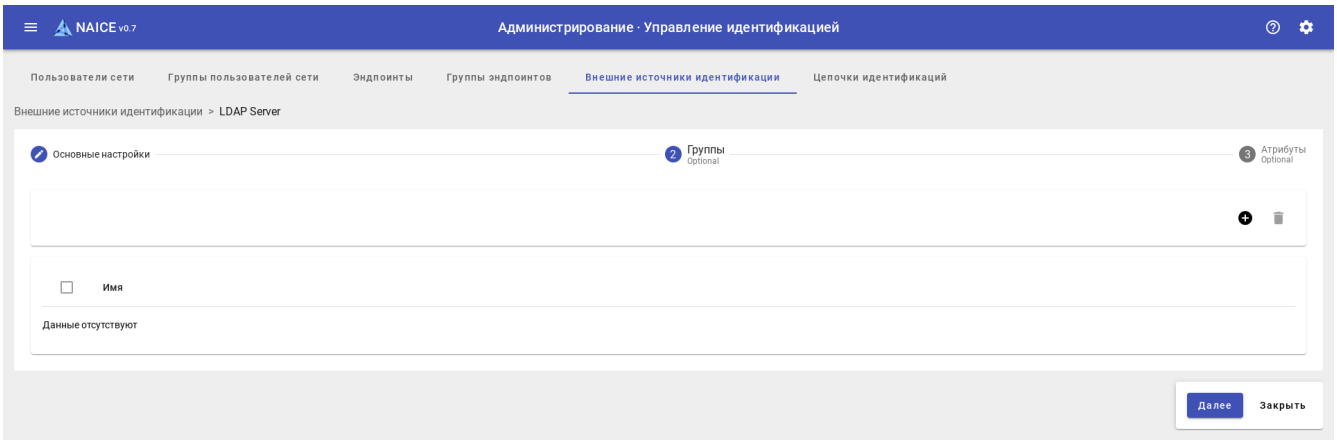

Рисунок 68. Пустая таблица групп

Таблица содержит колонки:

- "Имя" - имя группы

Элементы управления:

- - добавить группу.
- - удалить выбранные чекбоксом группы (неактивно, пока не выбран хоть одна группа).
- - редактировать группу (не отображается, пока не добавлена хотя бы одна группа).
- - сохранить группу после редактирования (не отображается, пока не начато редактирование группы).

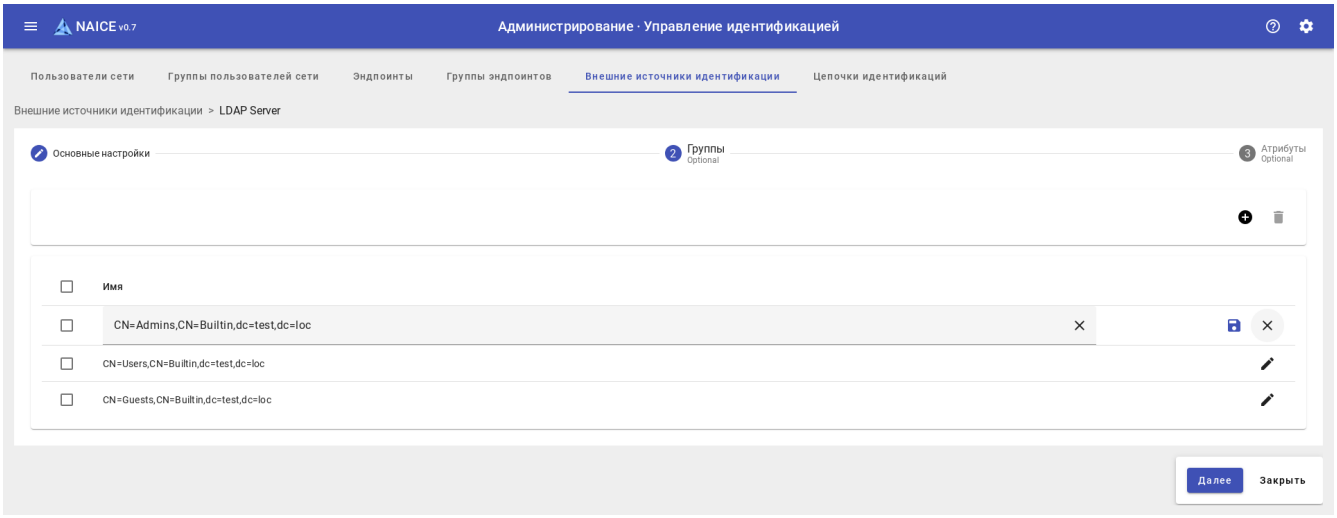

Рисунок 69. Таблица групп в режиме редактирования

После нажатия на кнопку ⊕ откроется меню:

- `Добавить новую группу` - создать произвольную новую группу.
- `Выбрать группы из службы каталогов` - добавить группы из источника идентификации.

Добавить новую группу

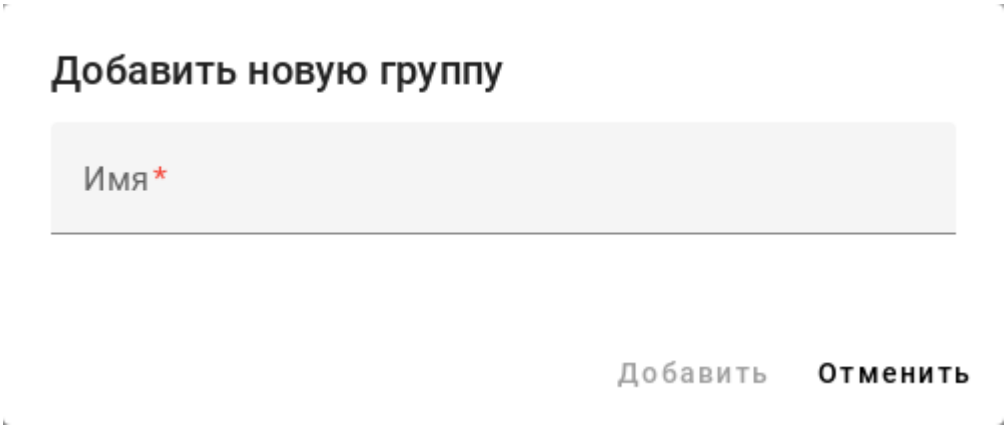

Рисунок 70. Добавить новую группу

В данном окне представлен следующий параметр:

- `Имя` * - произвольное имя группы.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После заполнения имени группы станет активна кнопка **Добавить**. Требуется нажать её для добавления группы.

Выбрать группы из службы каталогов

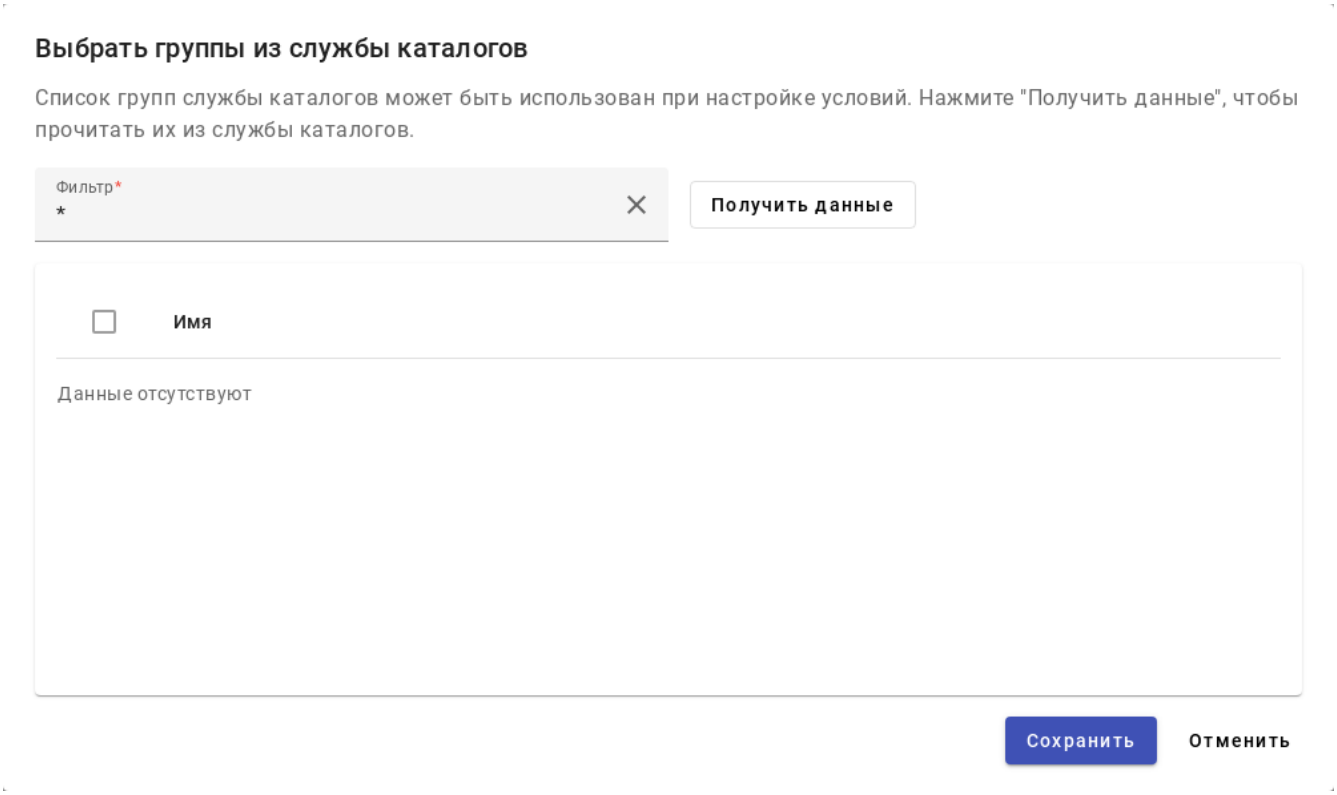

Рисунок 71. Окно выбора групп

В данном окне представлен следующие параметры:

- `Фильтр` - **фильтр для поиска групп, по умолчанию "**", можно ввести название группы.
- `Получить данные` - получить данные с учетом фильтра

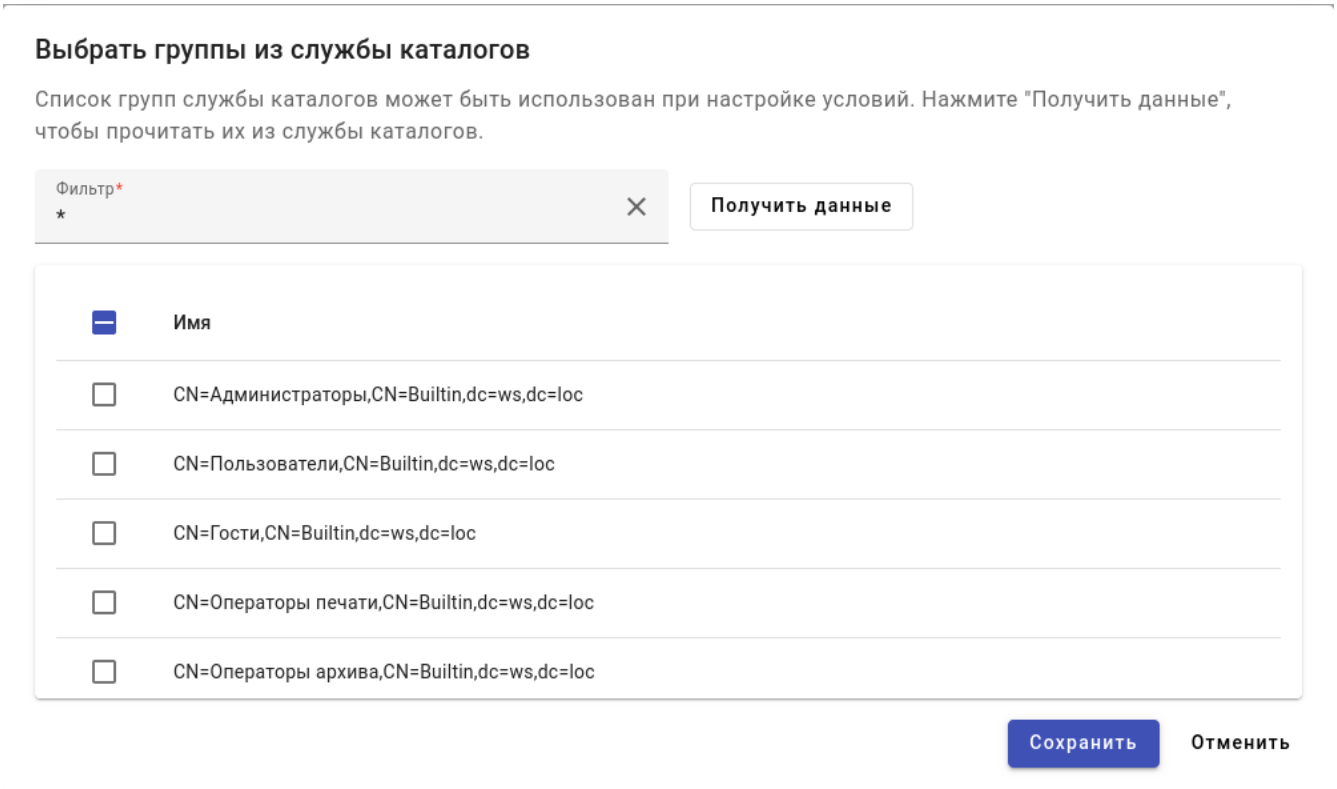

Рисунок 72. Окно выбора групп после получения данных

Требуется выбрать чекбоксом ☐ слева требуемые группы и нажать кнопку **Сохранить**.

Ранее сохранённые группы, которые не были повторно выбраны в списке поиска, будут удалены при повторном сохранении других выбранных групп!

Добавление атрибутов

Для возможности аутентификации через внешний источник идентификации добавление атрибутов не является обязательным.
Атрибуты можно использовать в политиках и профилях авторизации пользователей.

После добавления групп можно нажать кнопку "Далее" внизу справа экрана. Так же можно выполнить переход нажав на надпись **(3) Атрибуты**, откроется страница:

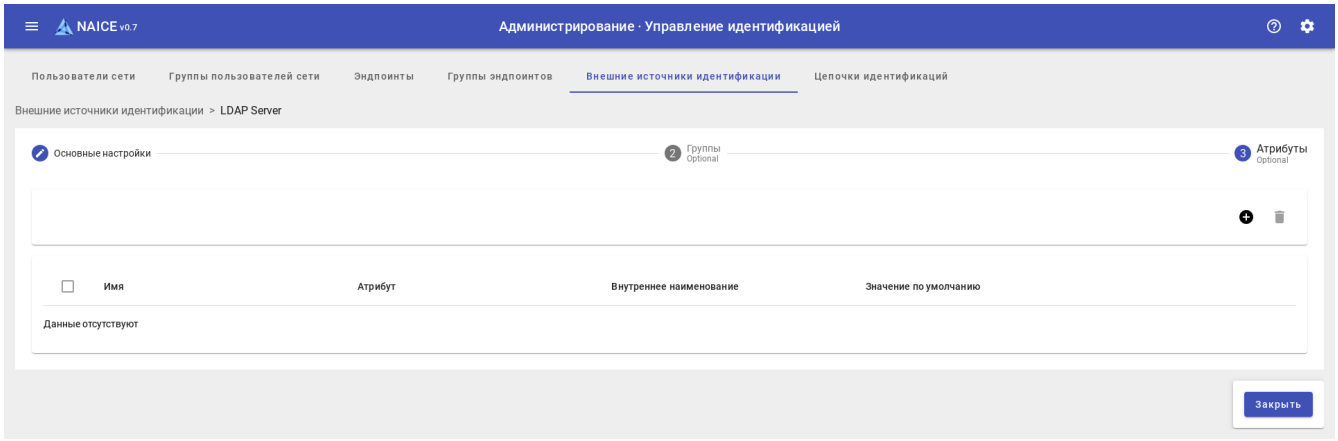

Рисунок 73. Добавление атрибутов

Таблица содержит колонки:

- `Имя` - имя атрибута, которое будет отображаться в словаре LDAP и использоваться при настройке логических условий и профилей авторизации. Можно указать произвольное, для удобства использования.
- `Тип` - тип атрибута, возможные значения:
  - `INTEGER` - числовой,
  - `IP_4_ADDR` - адрес IPv4,
  - `STRING` - строковый.
- `Внутренне наименование` - наименование атрибута в схеме Active Directory.
- `Значение по умолчанию` - значение атрибута, которое будет использоваться, если оно не получено от Active Directory.

Элементы управления:

- ⊕ - добавить атрибуты.
- 🗑 - удалить выбранные чекбоксом атрибуты (неактивно, пока не выбран хоть один атрибут).
- ✎ - редактировать атрибуты (не отображается, пока не добавлен хотя бы один).

- сохранить атрибут после редактирования (не отображается, пока не начато редактирование).

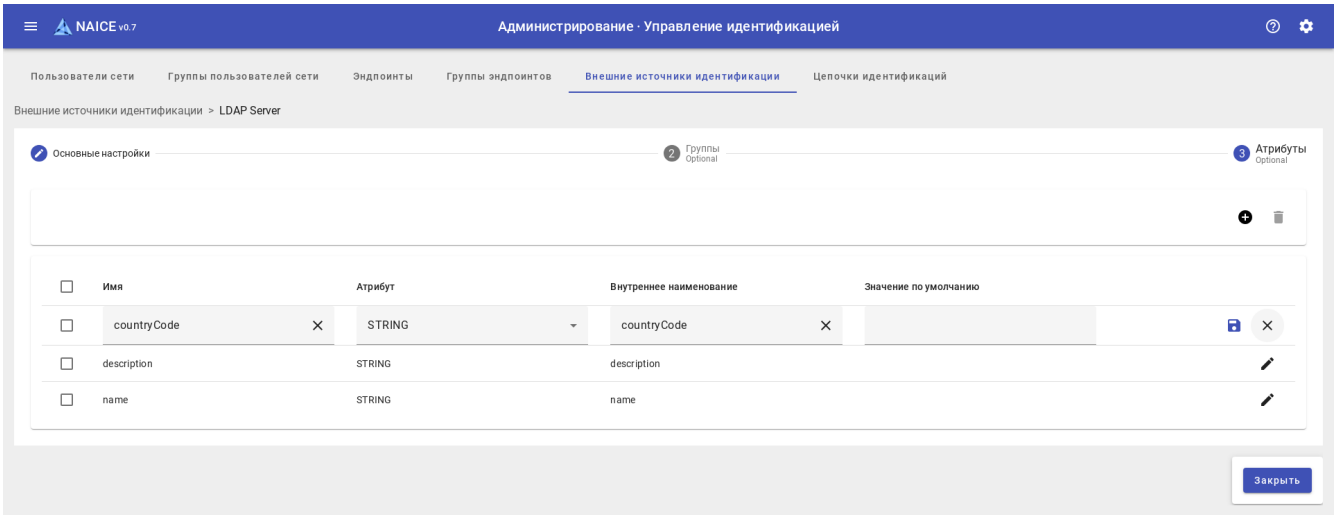

Рисунок 74. Таблица атрибутов в режиме редактирования

После нажатия на кнопку ⊕ откроется меню:

- `Добавить новый атрибут` - создать произвольный новый атрибут.
- `Выбрать атрибут из службы каталогов` - добавить атрибут из источника идентификации.

Добавить новый атрибут

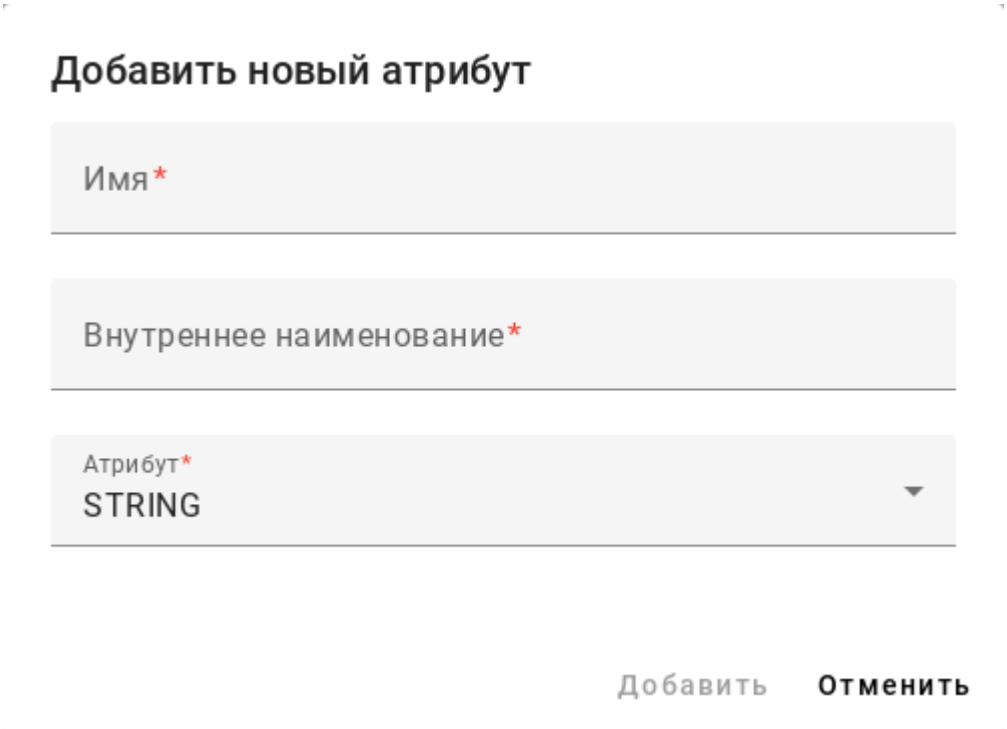

Рисунок 75. Добавить новый атрибут

В данном окне представлены следующие параметры:

- `Имя` * - произвольное имя атрибута, которое будет отображаться в словаре.
- `Внутреннее наименование` * - имя атрибута из источника идентификации.

`Тип` * - тип атрибута. Возможные значения:

- `INTEGER` - числовой,
- `IP_4_ADDR` - адрес IPv4,
- `STRING` - строковый (по умолчанию).

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После заполнения необходимых параметров станет активна кнопка **Добавить**. Требуется нажать её для добавления атрибута.

Выбрать атрибут из службы каталогов

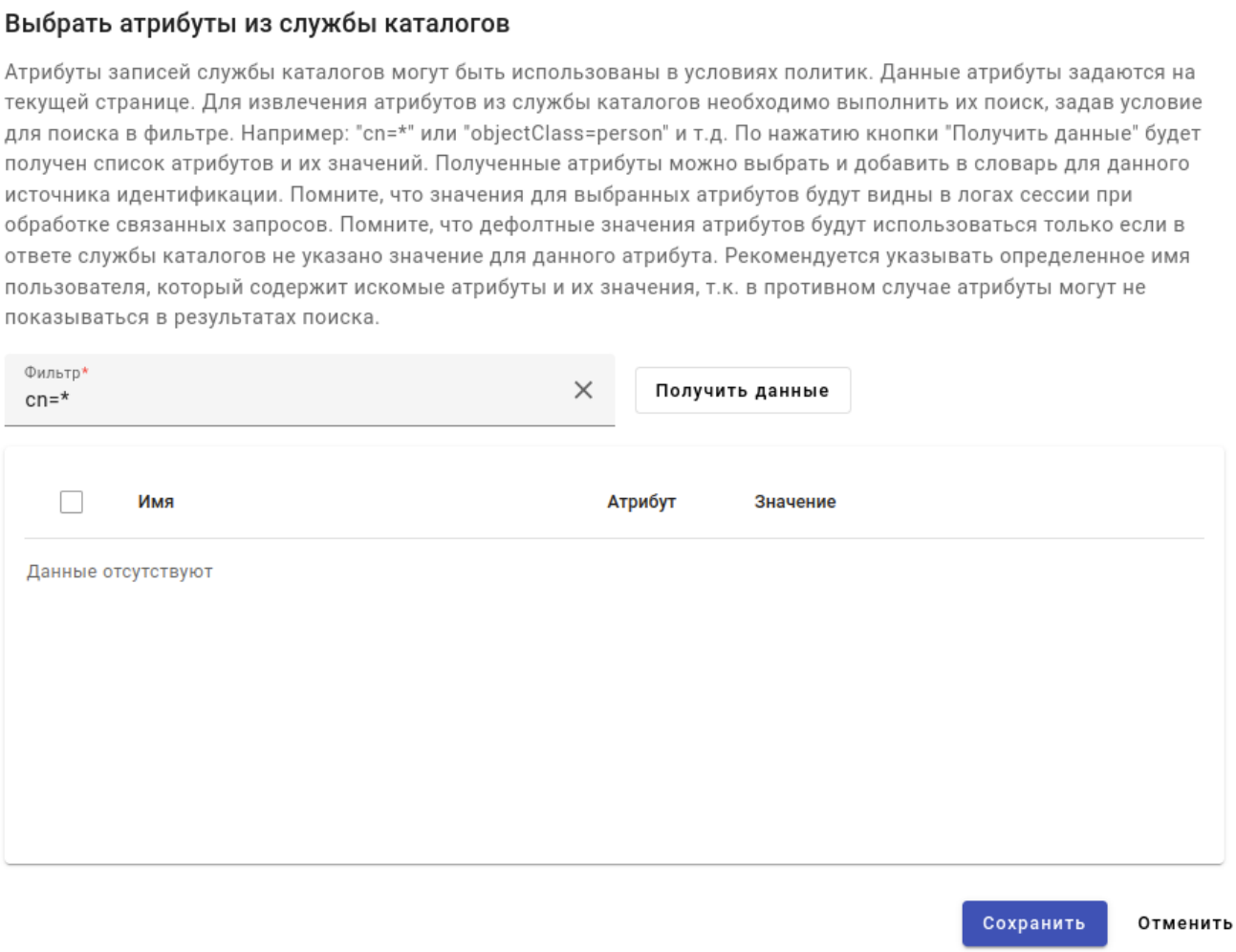

Рисунок 76. Выбор атрибутов из службы каталогов

В данном окне представлен следующие параметры:

- `Фильтр` * - фильтр для поиска атрибутов, по умолчанию `cn=*`. В качестве фильтра можно использовать выражения `<Атрибут>=<значение>`, если значение не важно надо указать `*`. Если у атрибута есть несколько значений - отображается только первое найденное.
- `Получить данные` - получить данные с учетом фильтра.

Как правило, дополнительные атрибуты пользователя добавляются после того, как им будут заданы значения, и до этого их вычитать нельзя.
При импорте атрибутов рекомендуется указать `cn=<логин пользователя>`: указанный пользователь должен содержать значения атрибутов, которые планируется импортировать.

После получения данных по атрибутам:

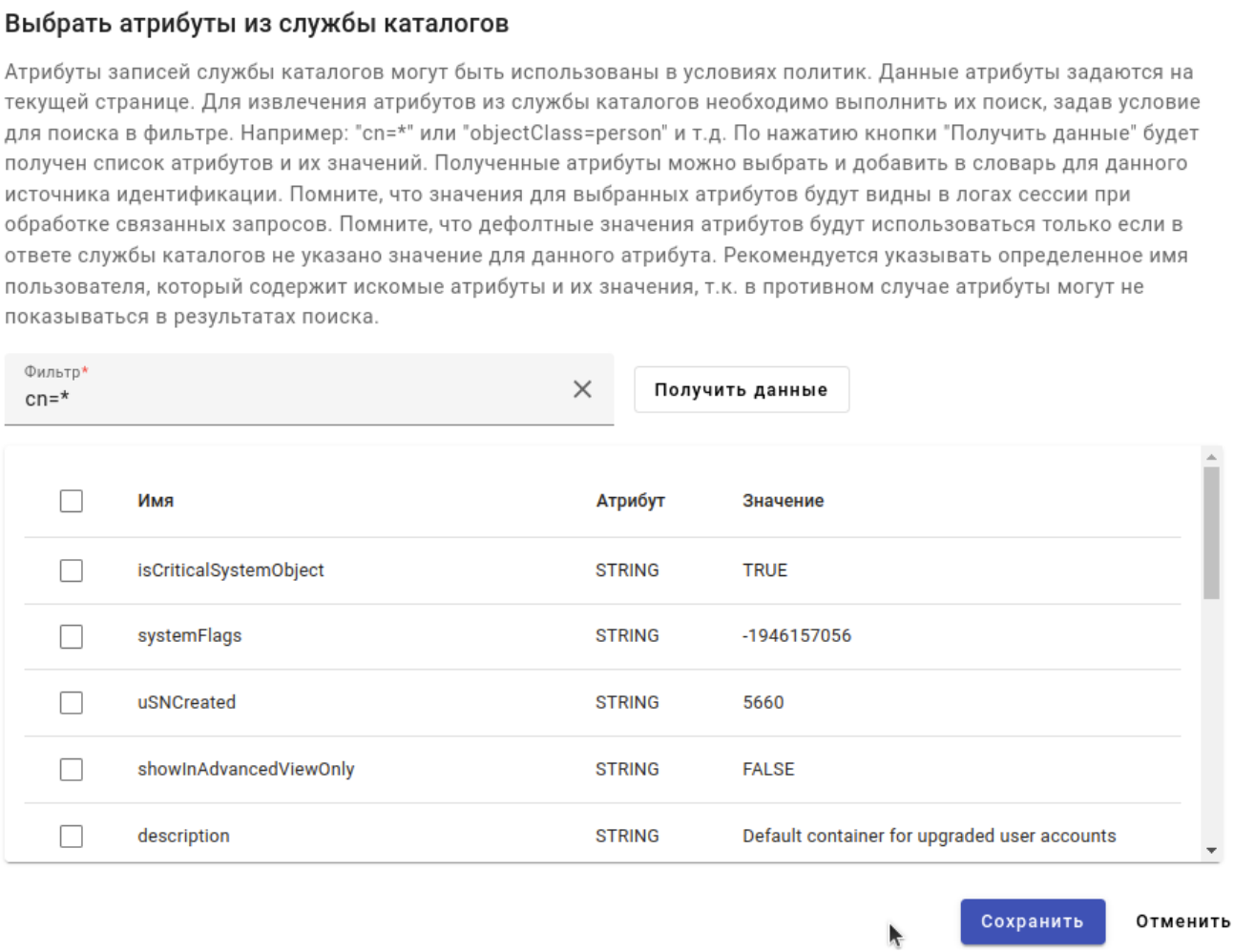

Рисунок 77. Окно выбора атрибутов после получения данных

Требуется выбрать чекбоксом слева требуемые атрибуты и нажать кнопку **Сохранить**.

Ранее сохранённые атрибуты, которые не были повторно выбраны в списке поиска, будут удалены при повторном сохранении других выбранных атрибутов!

Ограничения реализации

Есть следующие ограничения реализации взаимодействия с Active Directory:

- Возможно использовать пользователей, их атрибуты и группы только в рамках определенного домена.
- Имя пользователя на клиентском устройстве требуется вводить без домена.
- В именах пользователей и их паролях допускаются только латинские символы, цифры, знаки препинания.

Возможна авторизация только с использованием протокола MS-CHAPv2 или EAP-MS-CHAPv2.

Добавление источника идентификации типа Custom

Данный тип источника идентификации предназначен для интеграции с LDAP сервером, который может иметь произвольную схему.

Добавление источника идентификации

Для добавления источника идентификации нажмите в правой части поля над таблицей, откроется следующая страница, на которой надо будет выбрать схему `CUSTOM`:

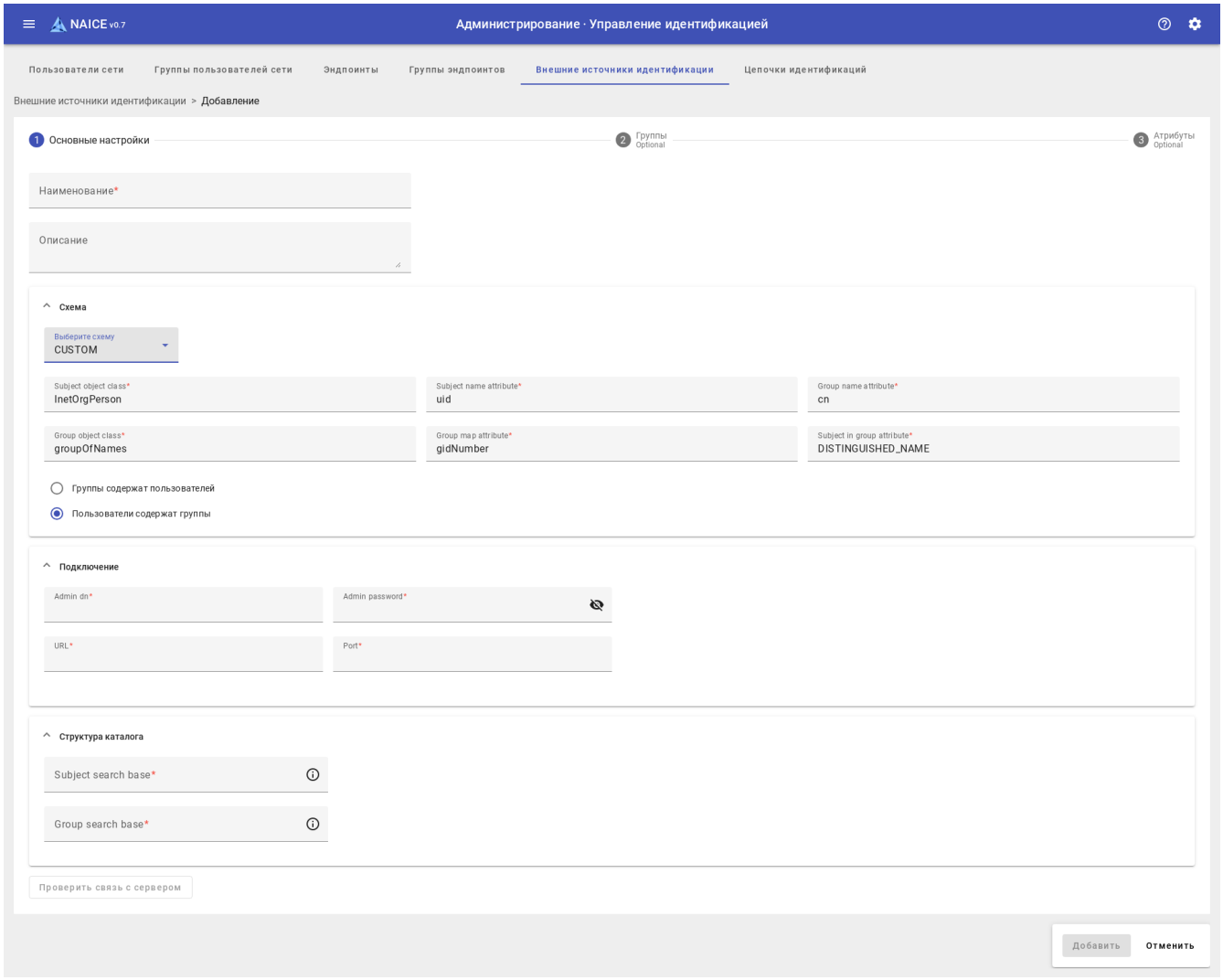

Рисунок 78. Окно добавления источника идентификации

В данной форме представлены следующие параметры:

- Блок **Основные настройки**:
  - `Наименование` * - наименование источника идентификации. (Максимальная длина поля - 64 знаков)
  - `Описание` - описание.
- Блок **Схема**:
  - `Выберите схему` * - схема атрибутов источника идентификации. По умолчанию выбрана `ACTIVE_DIRECTORY` требуется сменить на `CUSTOM`, что бы выбор значений атрибутов схемы стал

доступным.

- `Subject object class` * - атрибут, определяющий класс пользователей.
- `Subject name attribute` * - атрибут, определяющий имя пользователя, которое он будет использовать в качестве логина на клиентском устройстве.
- `Group name attribute` * - атрибут, определяющий имя группы пользователя.
- `Group object class` * - атрибут, определяющий класс групп.
- `Group map attribute` * - атрибут, определяющий принадлежность к группе.
- `Subject in group attribute` - атрибут, значение которого используется в значении атрибута "Group map attribute" при проверке принадлежности пользователя группе.
- `Группы содержат пользователей` * - выберите, если атрибут принадлежности пользователя к группе находится в атрибутах группы.
- `Пользователи содержат группы` * - выберите, если атрибут принадлежности пользователя к группе находится в атрибутах пользователя.

- Блок **Подключение**:
  - `Admin dn` * - данные административного пользователя для взаимодействия с LDAP (в формате "cn=admin,dc=example,dc=org").
  - `Admin password` * - пароль административного пользователя. По умолчанию не отображается, для просмотра требуется нажать .
  - `URL` * - IP-адрес или доменное имя сервера LDAP.
  - `Port` * - порт подключения (как правило, используется 389).
- Блок **Структура каталогов**:
  - `Subject search base` * - контекст для поиска атрибутов записей службы каталогов.
  - `Group search base` * - контекст для поиска групп службы каталогов.

Оба поля имеют формат вида перечисления через запятую атрибут=значение, например dc=test,dc=loc или ou=naice test,dc=test,dc=loc.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Максимальная длина поля `Наименование` - 64 знаков. У остальных полей - 200 знаков.

Допустимые символы при вводе параметров Subject search base и Group search base:

- пробел,
- двойные кавычки (""),
- знак равенства (=),
- запятая (,),
- дефис (-),
- латинские буквы (a-z)(A-Z),
- русские буквы (а-я)(А-Я),
- цифры (0-9).

Ввод других элементов запрещен.

Система при сохранении автоматически удаляет пробелы возле знака равенства (=) и запятой (,), значение с пробелом берется в двойные кавычки. Значение атрибута, введенное слева от знака равенства (=), переводится в нижний регистр.

Пример:

Введённое значение	Сохранённое значение
ou=naice test, dc = test ,dc = loc	ou="naice test",dc=test,dc=loc
ou="naice test",dc = test,dc=loc	ou="naice test",dc=test,dc=loc

После заполнения всех необходимых данных станет активна кнопка **Добавить** и **Проверить связь с сервером**.

Кнопка **Добавить** становится активной при условии добавления всех параметров и не зависит от успешности проверки связи с сервером.

При успешной проверки связи с сервером появится сообщение вида:

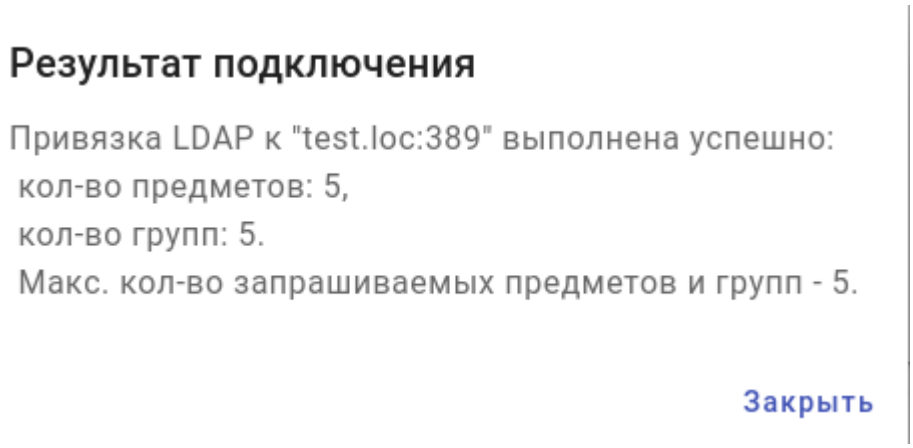

Рисунок 79. Привязка к LDAP выполнена успешно

При проверке соединения запрашивается не более 5 предметов и групп, что бы не вызывать лишнюю нагрузку на сервер, поэтому если реальных пользователей или групп больше будет показано число "5" - это не свидетельствует о проблеме.

Добавление групп пользователей

Для возможности аутентификации через внешний источник идентификации добавление групп не является обязательным. Группы можно использовать в политиках авторизации пользователей.

После добавления источника идентификации кнопка **Добавить** примет значение "Далее". Так же можно выполнить переход нажав на надпись **(2) Группы**, откроется страница:

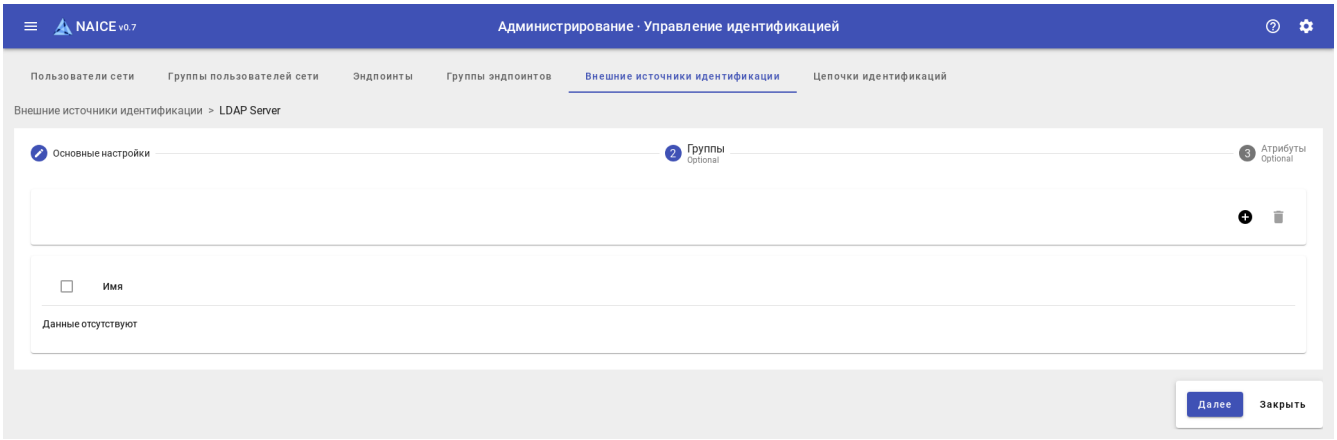

Рисунок 80. Пустая таблица групп

Элементы управления:

-  - добавить группу.
-  - удалить выбранные чекбоксом группы (неактивно, пока не выбрана хоть одна группа).

После нажатия на кнопку  откроется меню:

- `Добавить новую группу` - создать произвольную новую группу.
- `Выбрать группы из службы каталогов` - добавить группы из источника идентификации.

Добавить новую группу

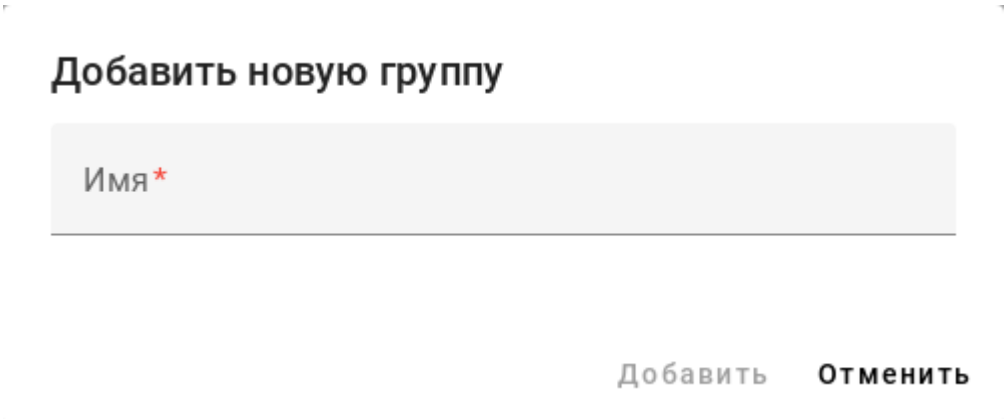

Рисунок 81. Добавить новую группу

В данном окне представлен следующий параметр:

- `Имя` * - произвольное имя группы.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После заполнения имени группы станет активна кнопка **Добавить**. Требуется нажать её для добавления группы.

Выбрать группы из службы каталогов

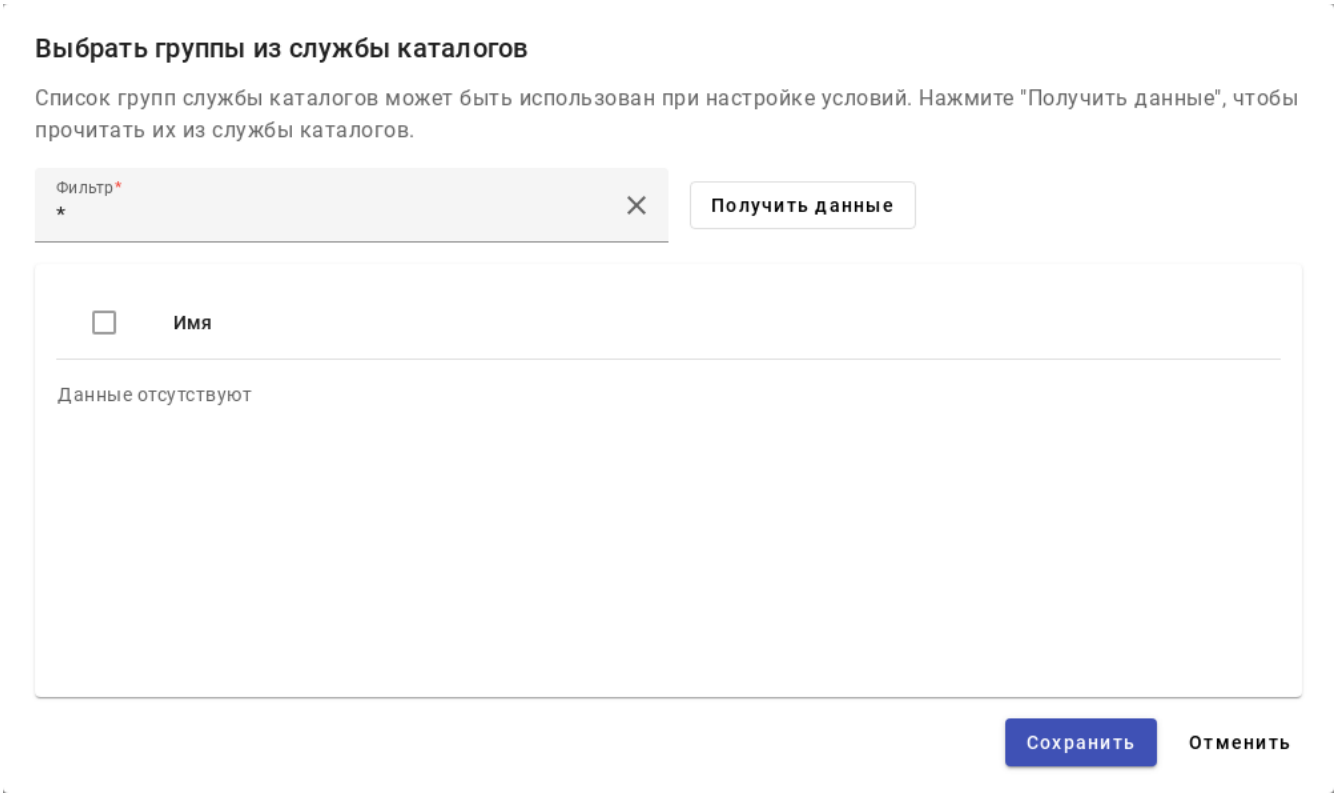

Рисунок 82. Окно выбора групп

В данном окне представлен следующие параметры:

- `Фильтр` * - фильтр для поиска групп, по умолчанию *, можно ввести название группы.
- `Получить данные` - получить данные с учетом фильтра.

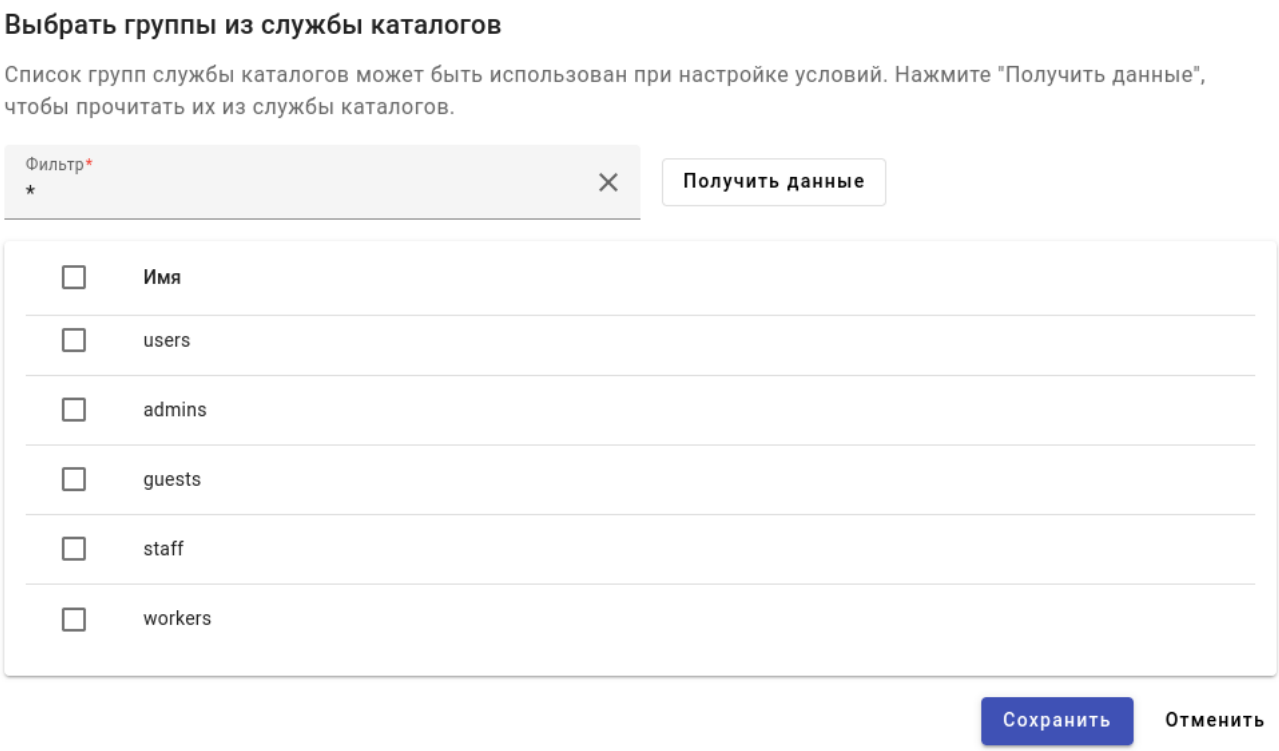

Рисунок 83. Окно выбора групп после получения данных

Требуется выбрать чекбоксом ☐ слева требуемые группы и нажать кнопку **Сохранить**.

Ранее сохранённые группы, которые не были повторно выбраны в списке поиска, будут удалены при повторном сохранении других выбранных групп!

Добавление атрибутов

Для возможности аутентификации через внешний источник идентификации добавление атрибутов не является обязательным. Атрибуты можно использовать в политиках и профилях авторизации пользователей.

После добавления групп можно нажать кнопку **Далее** внизу справа экрана. Так же можно выполнить переход нажав на надпись **(3) Атрибуты**, откроется страница:

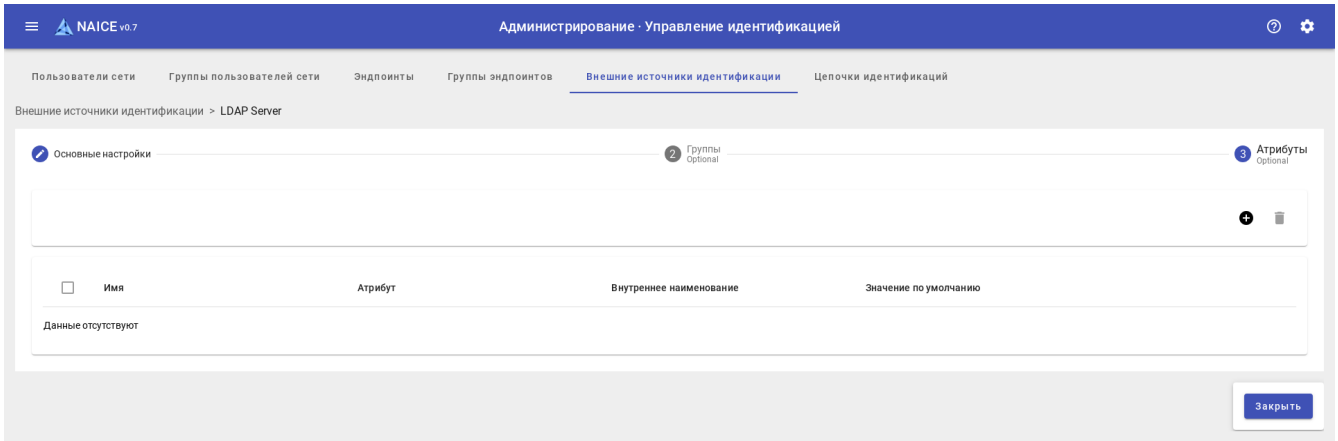

Рисунок 84. Добавление атрибутов

Элементы управления:

- добавить атрибуты.
- - удалить выбранные чекбоксом атрибуты (неактивно, пока не выбран хоть один атрибут).

После нажатия на кнопку откроется меню:

- `Добавить новый атрибут` - создать произвольный новый атрибут.
- `Выбрать атрибут из службы каталогов` - добавить атрибут из источника идентификации.

Добавить новый атрибут

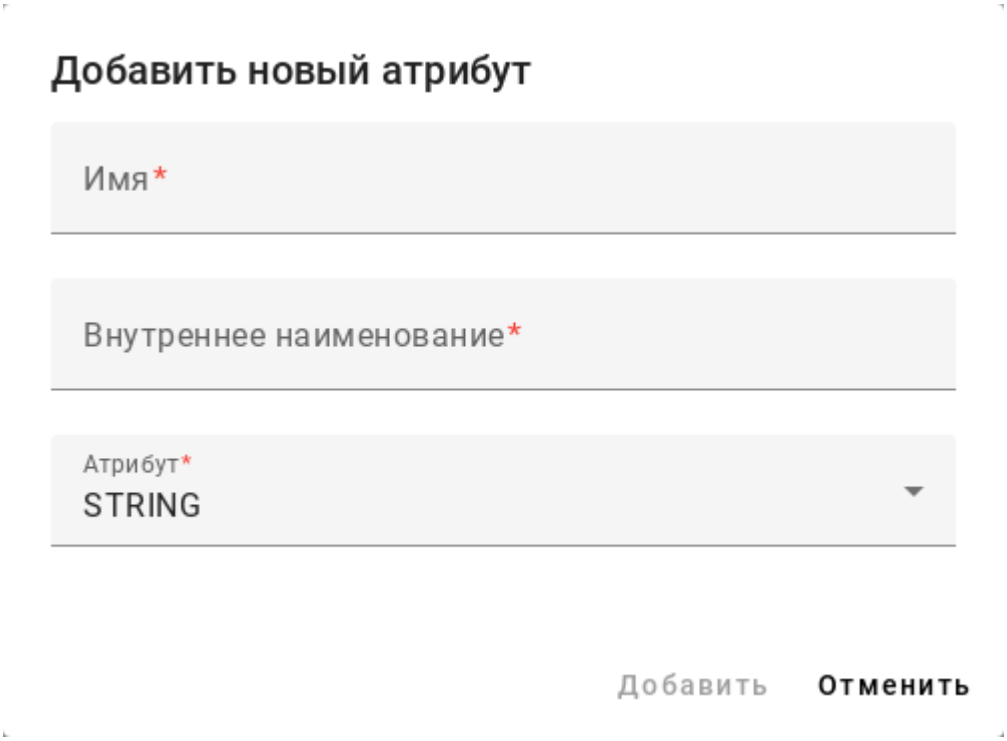

Рисунок 85. Добавить новый атрибут

В данном окне представлены следующие параметры:

- `Имя` * - произвольное имя атрибута, которое будет отображаться в словаре.
- `Внутреннее наименование` * - имя атрибута из источника идентификации.
- `Тип` * - тип атрибута. Возможные значения:
  - `INTEGER` - числовой,
  - `IP_4_ADDR` - адрес IPv4,
  - `STRING` - строковый (по умолчанию).

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После заполнения необходимых параметров станет активна кнопка **Добавить**. Требуется нажать её для добавления атрибута.

Выбрать атрибут из службы каталогов

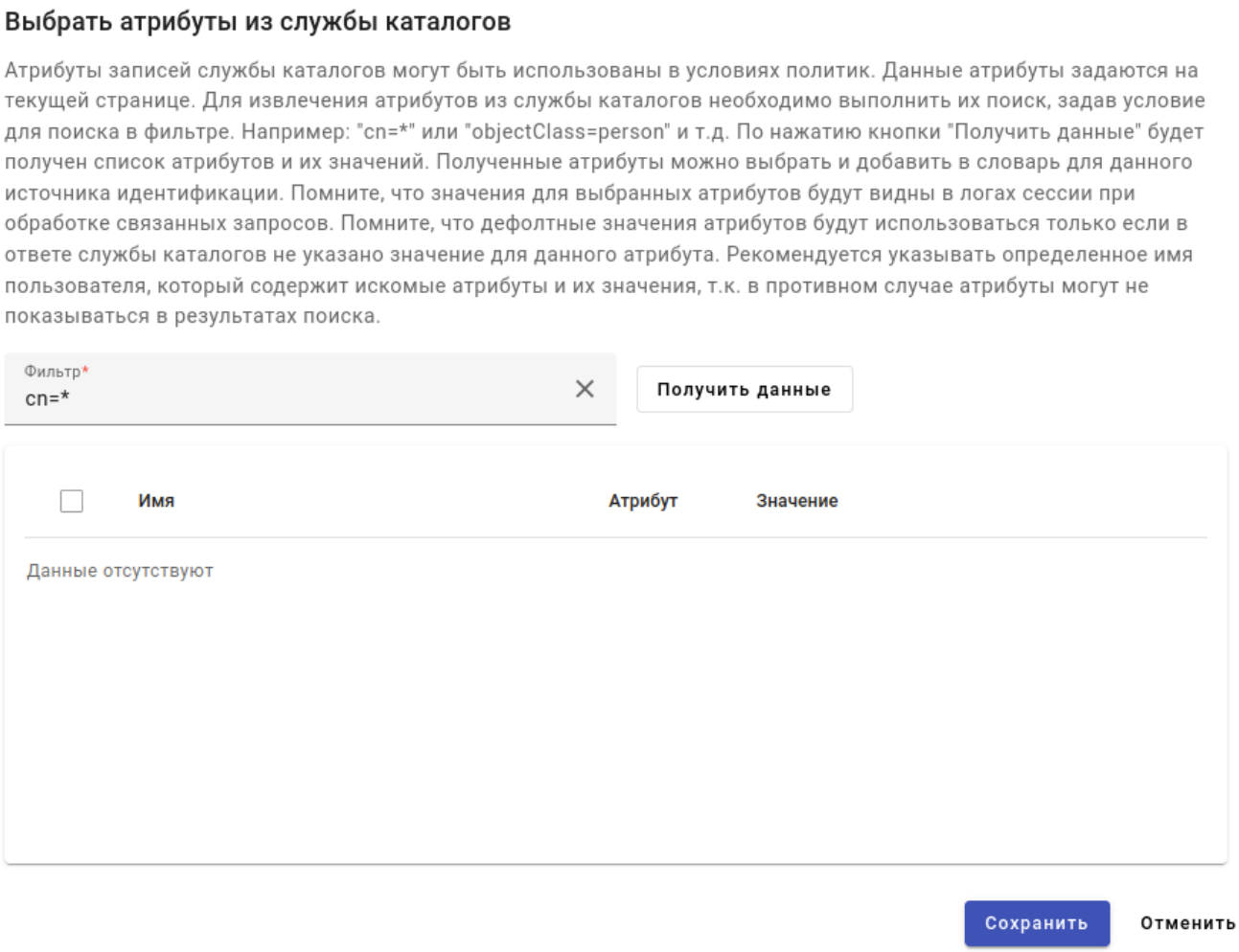

Рисунок 86. Выбор атрибутов из службы каталогов

В данном окне представлен следующие параметры:

- `Фильтр` * - фильтр для поиска атрибутов, по умолчанию `cn=*`. В качестве фильтра можно использовать выражения `<Атрибут>=<значение>`, если значение не важно надо указать `*`. Если у атрибута есть несколько значений - отображается только первое найденное. При выполнении поиска в LDAP, как правило, можно указать `uid=*` или `givenName=*`.
- `Получить данные` - получить данные с учетом фильтра.

После получения данных по атрибутам:

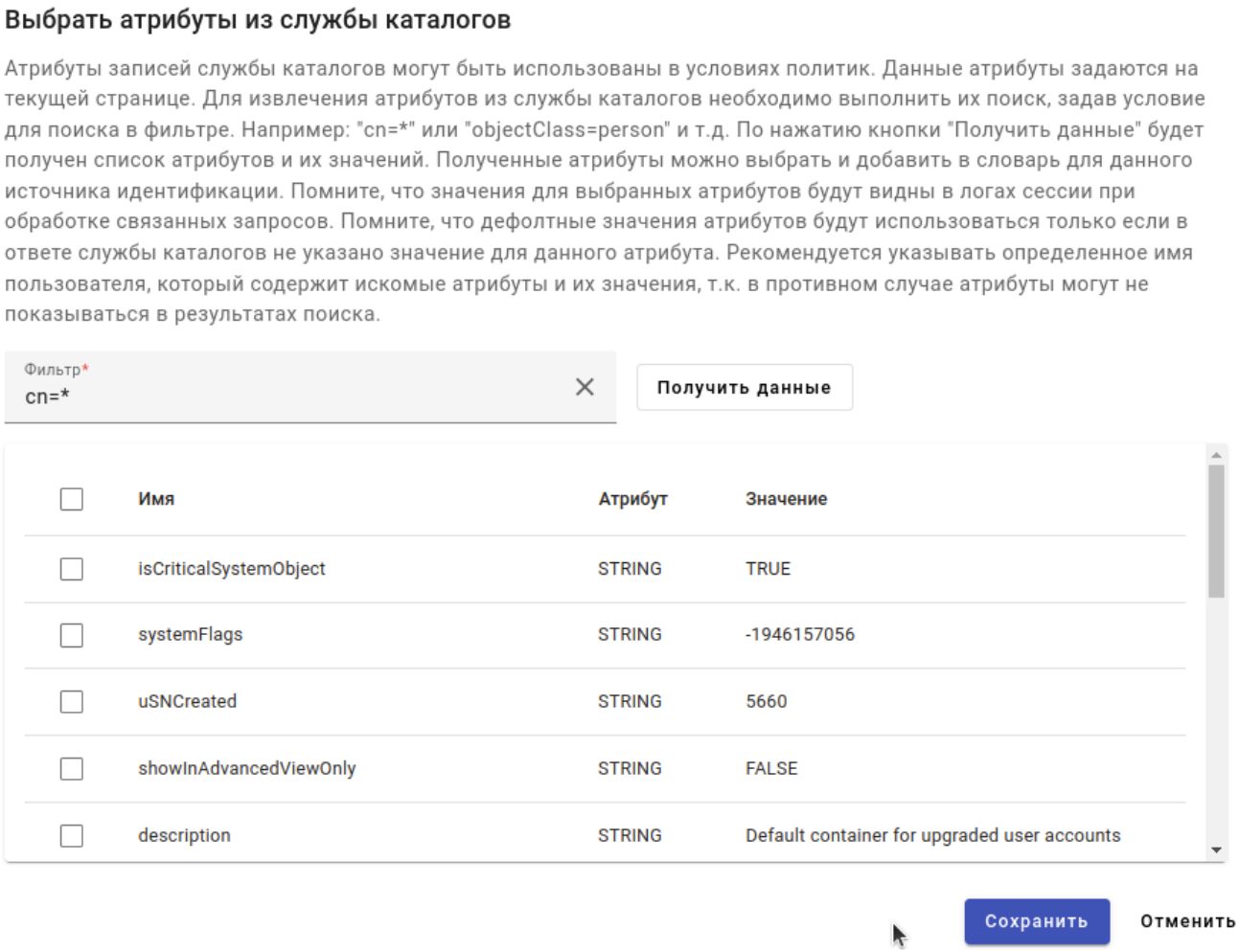

Рисунок 87. Окно выбора атрибутов после получения данных

Требуется выбрать чекбоксом слева требуемые атрибуты и нажать кнопку **Сохранить**.

Ранее сохранённые атрибуты, которые не были повторно выбраны в списке поиска, будут удалены при повторном сохранении других выбранных атрибутов!

Ограничения реализации

Есть следующие ограничения реализации взаимодействия с LDAP:

- Пароль пользователя должен хранится в ClearText.
- В именах пользователей и их паролях допускаются только латинские символы, цифры, знаки препинания.

Редактирование источника идентификации

Для редактирования ранее добавленного источника идентификации на странице просмотра нажмите на наименование источника в таблице.

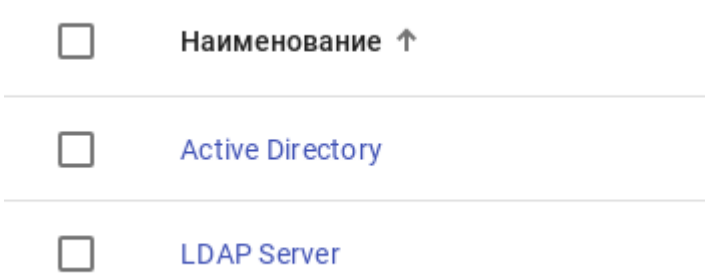

Рисунок 88. Колонка наименование

Откроется страница редактирования:

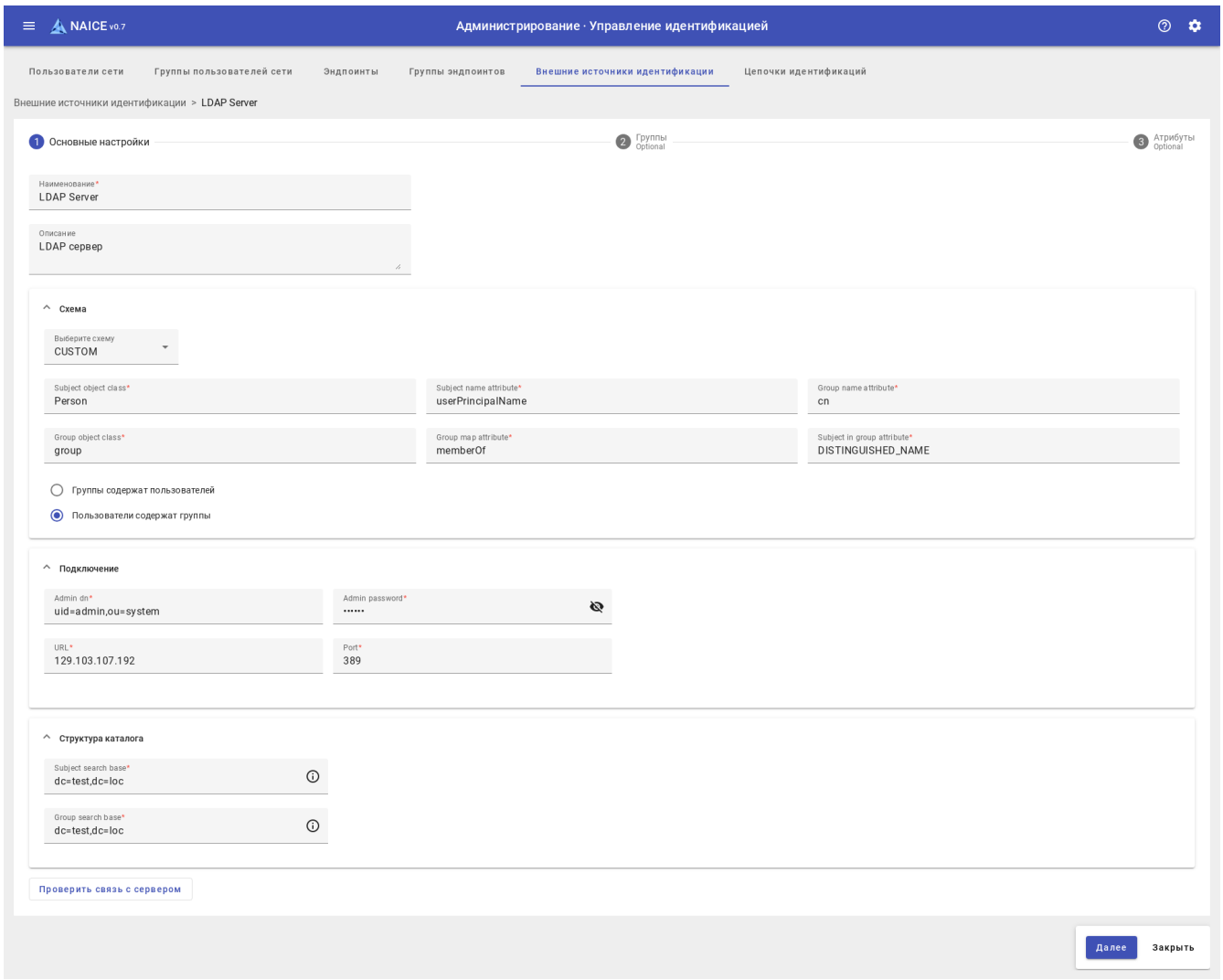

Рисунок 89. Страница редактирования источника

После редактирования нажмите на кнопку **Сохранить**. Кнопка будет неактивной пока не будет изменено хотя бы одно поле.

Удаление источника идентификации

Для удаления одного или нескольких источников идентификации необходимо на странице просмотра через чекбокс ☐ выбрать необходимые источники и в правом верхнем углу над таблицей нажать на 🗑 .

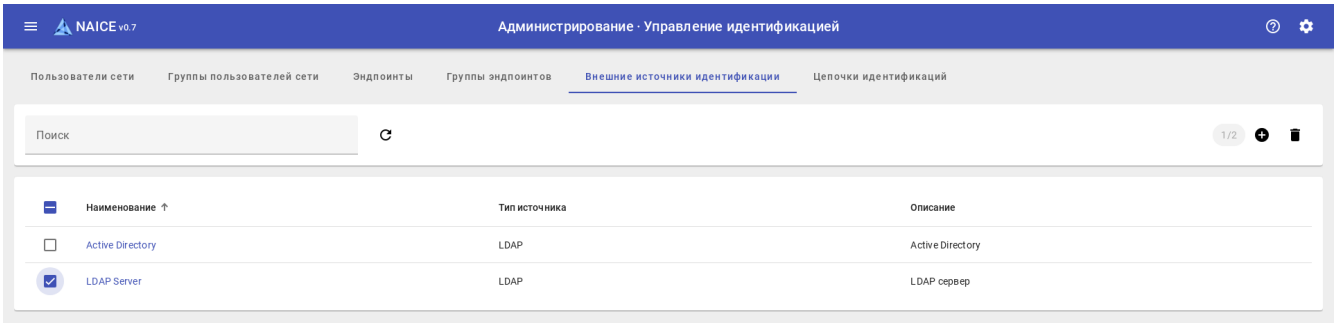

Рисунок 90. Выбор источников для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

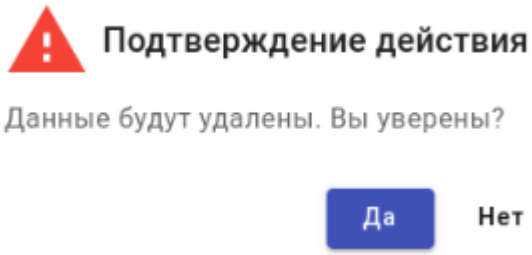

Рисунок 91. Модальный диалог подтверждения

Цепочки идентификаций

Описание

Цепочки идентификаций (цепочки источников идентификаций) используются в политиках аутентификации при настройке политик доступа. Они определяют, в каких источниках и в каком их порядке искать пользователей при аутентификации. В качестве источников пользователей поддержаны внутренняя база данных пользователей и внешние источники идентификации, такие как MS AD и OpenLDAP.

Просмотр цепочек идентификаций

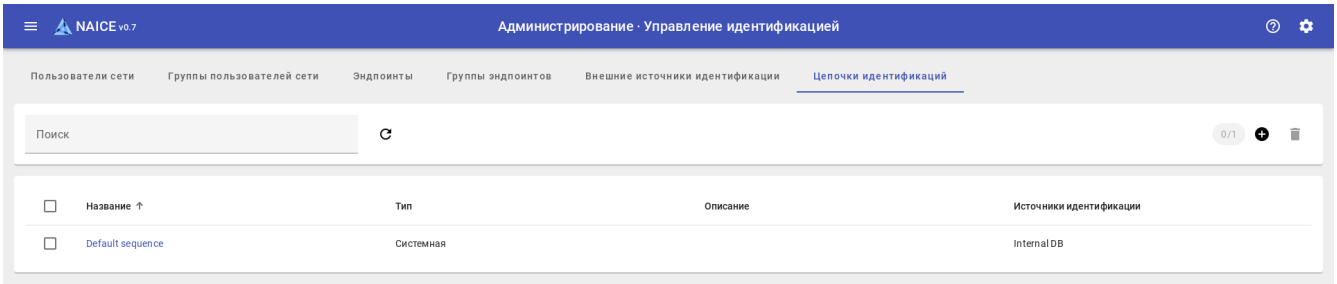

Рисунок 92. Просмотр цепочек идентификации

На данной странице содержится таблица со списком всех цепочек идентификаций.

Таблица содержит колонки:

- `Название` - название цепочки.
- `Тип` - тип цепочки идентификации. Возможны значения "Создана администратором" или "Системная".
- `Описание` - произвольное описание цепочки.

`Источники идентификации` - список источников учетных данных пользователей, которые настроены в данной цепочке.

Возможна сортировка в прямом и обратном порядке по колонкам `Название` и `Описание`. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по полю `Название`.

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - Обновить данные таблицы.
- 0/1 - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

> Нельзя переименовать или удалить системные цепочки идентификации: "[Default sequence]"

Добавление цепочки идентификаций

Для добавления цепочки идентификаций в правой части поля над таблицей страницы просмотра, откроется следующая страница:

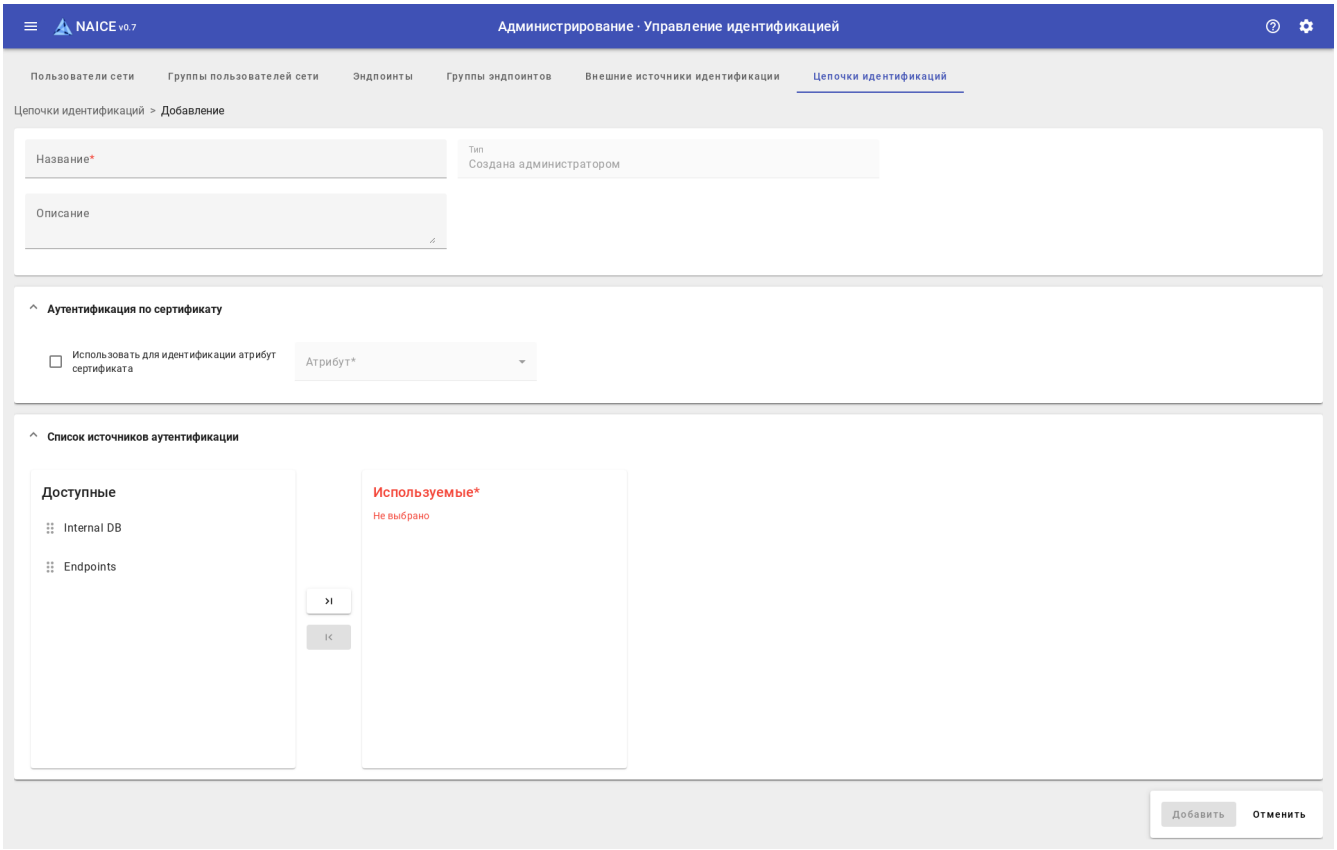

Рисунок 93. Страница добавления цепочки

Для заполнения доступны следующие параметры:

- `Название` * - название цепочки. Максимальная длина - 100 символов.
- `Тип` - тип цепочки идентификации. Все вручную созданные цепочки идентификации имеют значение "Создана администратором", изменить его нельзя.
- `Описание` - произвольное описание цепочки. Максимальная длина - 200 символов.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Аутентификация по сертификату

Данная настройка может быть использована только при аутентификации пользователя по протоколу EAP-TLS.

В данном разделе настраивается проверка соответствия выбранного поля сертификата пользователя атрибуту в источнике идентификации. Выбранное значение атрибута из сертификата пользователя сравнивается с атрибутом пользователя, указанным в поле "Subject Name Attribute" во внешнем источнике идентификации. В случае использования внутреннего источника идентификации (Internal DB) сравнение выполняется со значением указанным в поле "Логин" пользователя.

`Использовать для идентификации атрибут сертификата` - включает возможность выбора атрибута, который будет использоваться для проверки в качестве имени пользователя. При отключенной настройке используется значение атрибута User-Name из RADIUS-запроса аутентификации пользователя.

После включения настройки станет доступным поле `Атрибут`.

- `Атрибут` - поле в сертификате, содержащее данные для идентификации пользователя.

Поле может принимать следующие значения:

- `Subject - Common Name`
- `Subject - Serial Number`
- `Subject`
- `Subject Alternative Name - Email`
- `Subject Alternative Name - DNS`

Список источников идентификации

В этом разделе выбираются источники аутентификации, которые будут использоваться.

- `Доступные` - список всех источников, доступных для выбора.
- `Используемые` - список источников, которые будут применяться для аутентификации.

Для выбора источника учетных данных пользователей захватите его курсором мышки за поле ⠿ и переместите его из левой колонки "Доступные" в правую "Используемые".

Элементы управления:

- ⏭ - выбрать все доступные источники аутентификации.
- ⏮ - удалить все выбранные источники аутентификации.

Поиск пользователя по логину выполняется во всех доступных источниках, указанных в "Используемые". Поиск выполняется сверху вниз по списку. Поиск завершается как только совпадающий логин пользователя будет найдет в источнике.

Редактирование цепочки идентификаций

Для редактирования нажмите на название цепочки идентификаций в таблице.

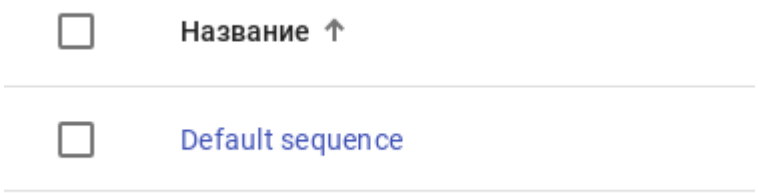

Рисунок 94. Гиперссылка на страницу редактирования цепочки идентификации

Откроется страница редактирования.

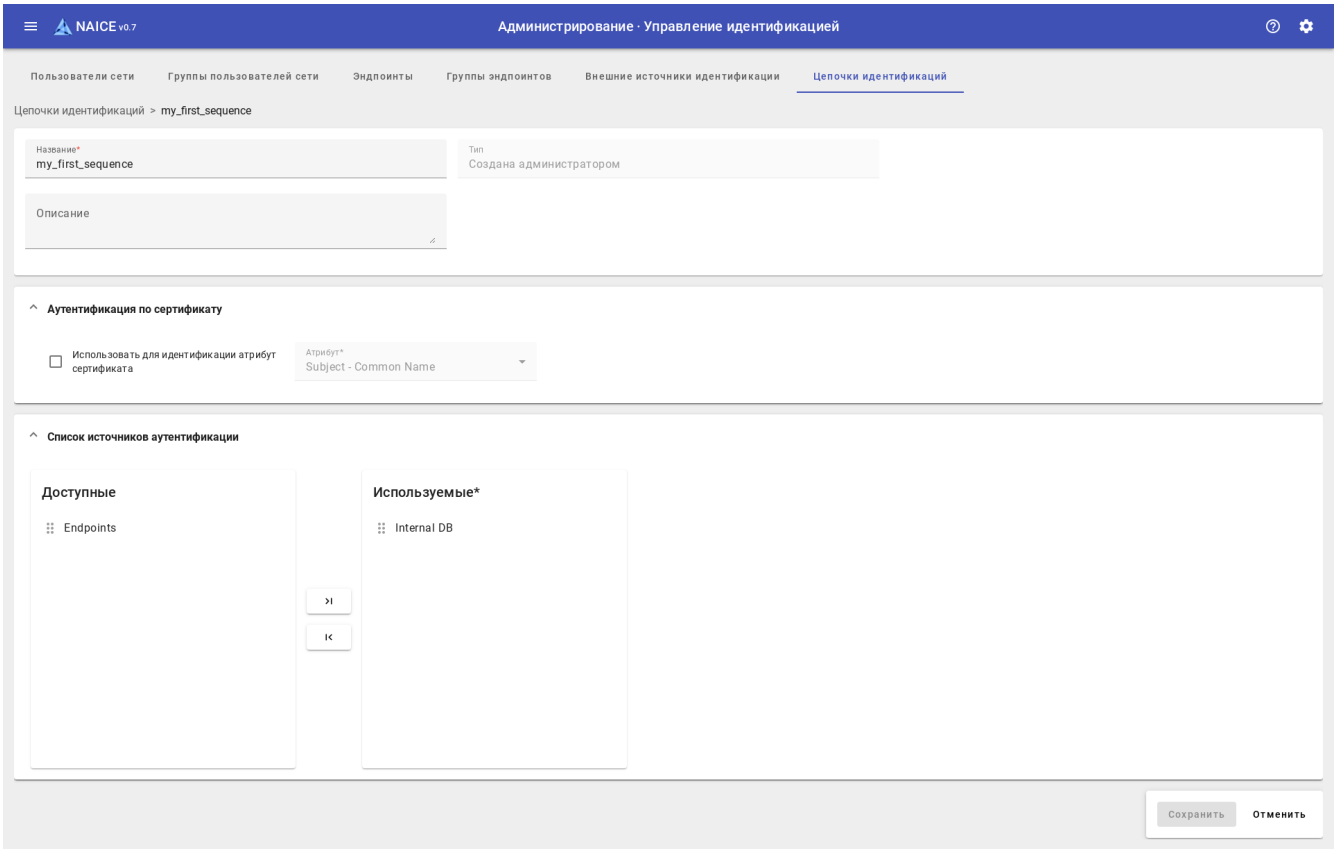

Рисунок 95. Страница редактирования цепочки идентификации

После редактирования нажмите **Сохранить**. Кнопка будет неактивной пока не будет внесено хотя бы одно изменение.

Удаление цепочки идентификаций

Для удаления одной или нескольких цепочек идентификации необходимо выбрать их через чекбокс ☐ и в правом верхнем углу над таблицей нажать на 🗑.

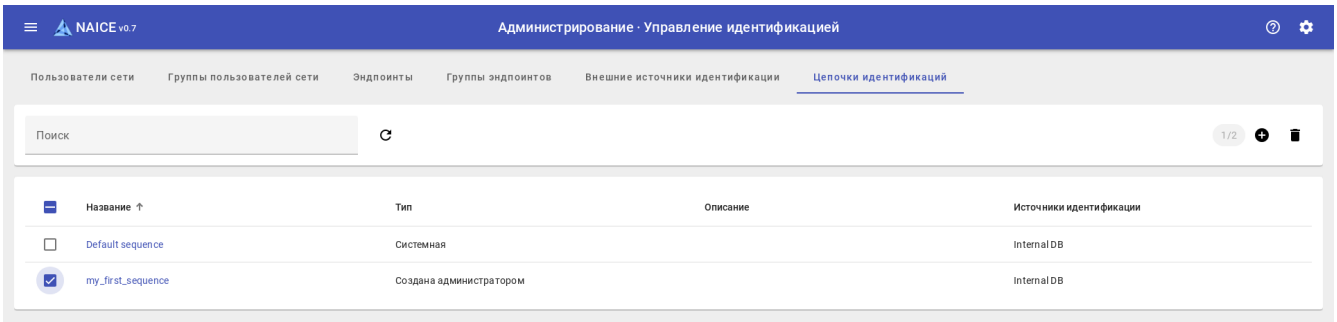

Рисунок 96. Выбор цепочек для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

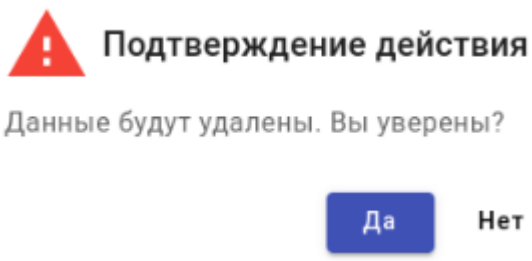

Рисунок 97. Модальный диалог подтверждения

Вы не сможете удалить цепочку, которая используется в политиках аутентификации какого-либо набора политик.
Для удаления цепочки необходимо сначала удалить ее из политики аутентификации, а затем удалить саму цепочку.

Политика

Элементы

Словари

Описание

Базовым элементом при настройке логического условия являются атрибуты, сгруппированные по словарям. Помимо базовых и vendor-specific атрибутов RADIUS в NAICE доступно использование Не-RADIUS атрибутов, таких как параметры сетевого устройства (словарь DEVICE) или пользователя (словарь IDENTITY).

Словари и атрибуты доступны для просмотра на отдельной странице. Добавление новых словарей или редактирование существующих недоступно.

Если необходимый Вам словарь не добавлен в систему, обратитесь к нам при помощи кнопки "Оставить пожелание", доступной из навигационного меню или меню  в верхней правой части окна.

Просмотр словарей

В левой части окна (с заголовком "Словари") находится список доступных словарей, в правой части - содержание выбранного словаря (по умолчанию - содержание словаря RADIUS).

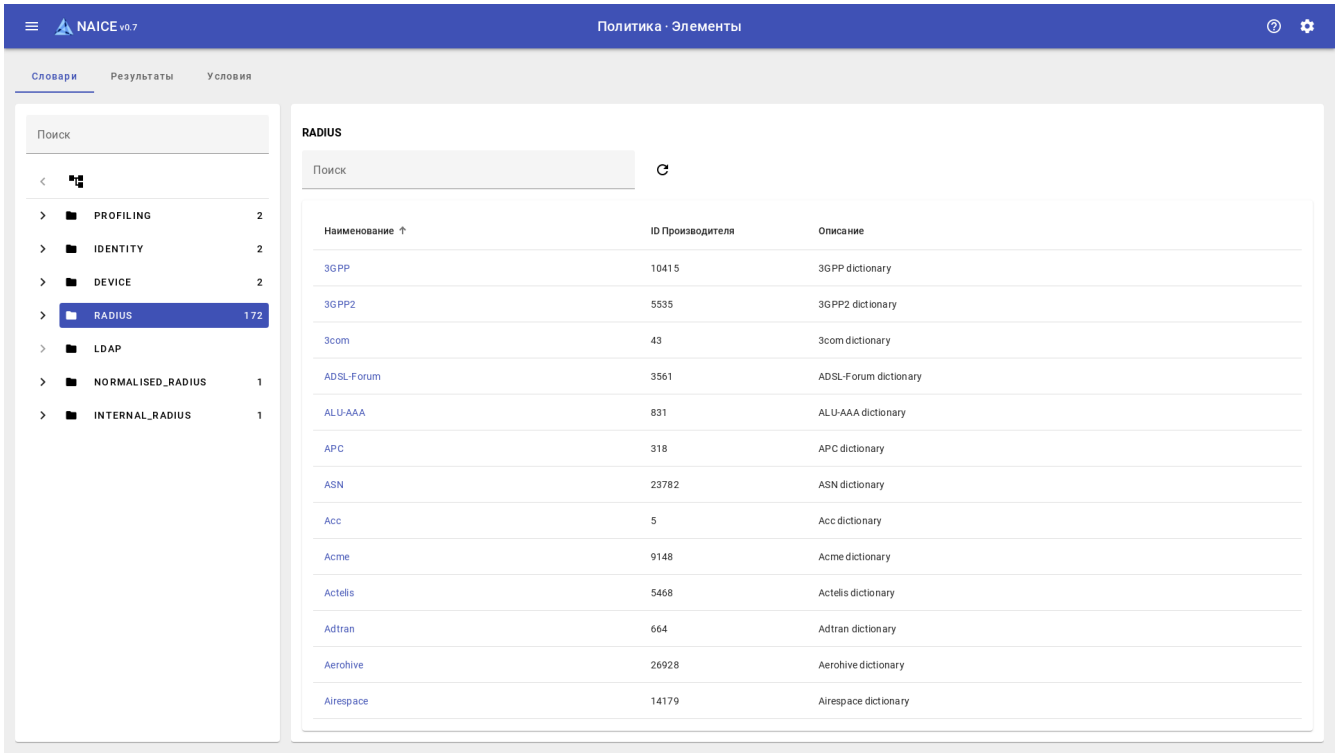

Рисунок 98. Просмотр словарей

Элементы управления:

-  - раскрыть список вложенных словарей.
- `"Словари. Поиск"` - фильтрация по имени словаря.

- `"RADIUS. Поиск"` - фильтрация по вложенным словарям и атрибутам.
- - обновить данные.
- Переключение варианта отображения меню навигации по словарям:
  - - меню навигации в виде дерева.
  - - меню навигации в виде списка.

Просмотр вложенных словарей и атрибутов

Для просмотра атрибутов словаря требуется выбрать необходимый словарь в списке и нажать на его имя:

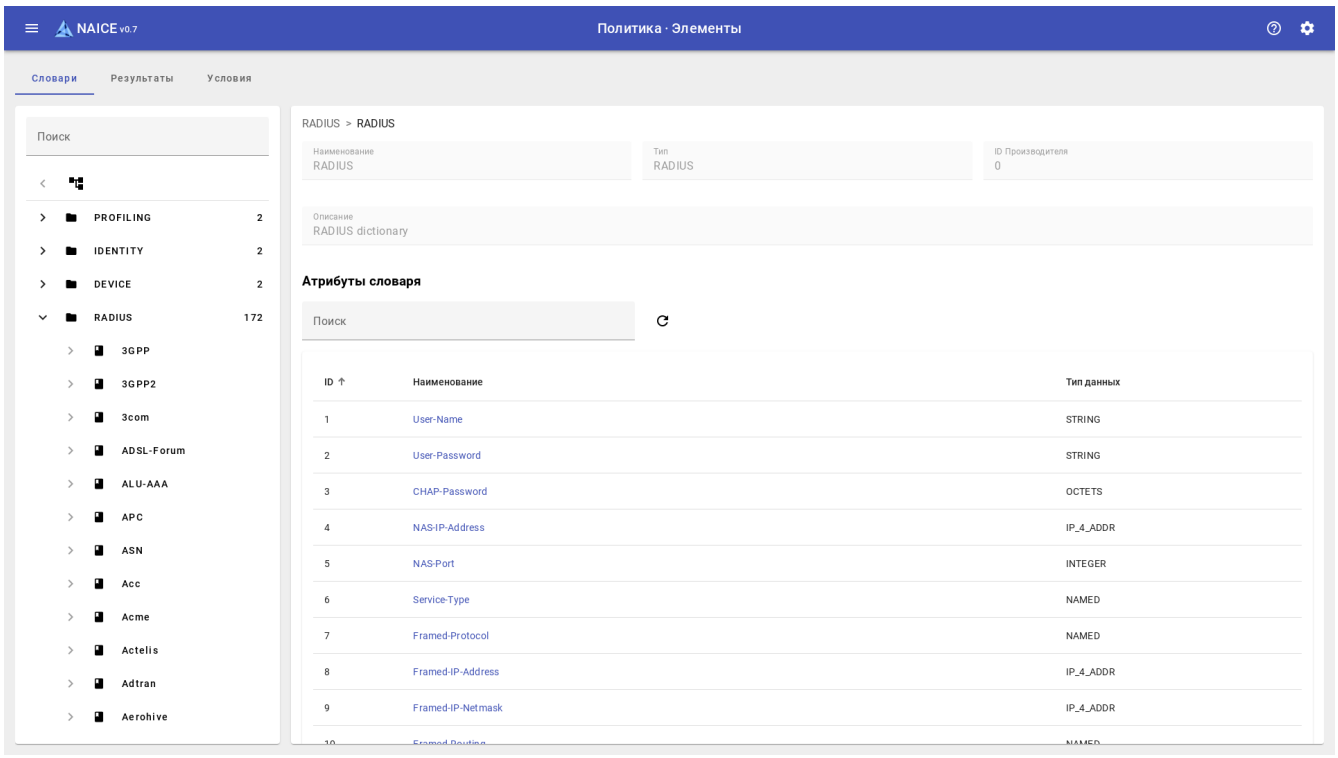

Рисунок 99. Просмотр атрибутов словаря

Для просмотра информации об атрибуте требуется нажать на имя атрибута в списке атрибутов:

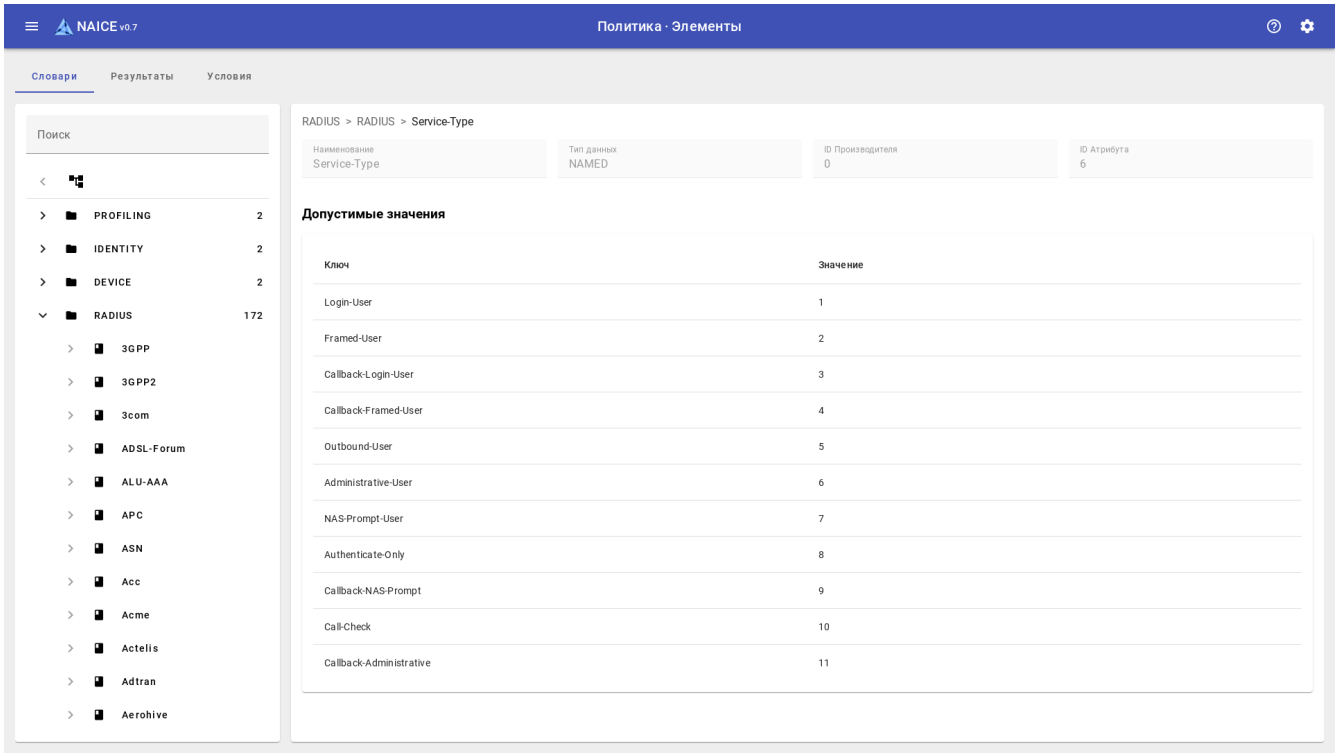

Рисунок 100. Просмотр информации об атрибуте

Для атрибутов, предполагающих конечный список допустимых значений, на данной странице будет перечислен список этих значений.

Результаты

Доступные протоколы

Описание

Управление протоколами аутентификации позволяет разрешить или запретить использование определенных протоколов или методов авторизации при аутентификации клиентского устройства. Существует возможность настройки нескольких списков разрешенных протоколов, что позволяет гибко настраивать разрешенные протоколы в наборах политик для каждого пользовательского сценария.

В данный момент поддерживаются следующие протоколы: PAP, MS-CHAPv2, EAP-PEAP, EAP-TLS.

Доступна настройка разрешения или запрета MAB авторизации.

Просмотр списка служб доступных протоколов

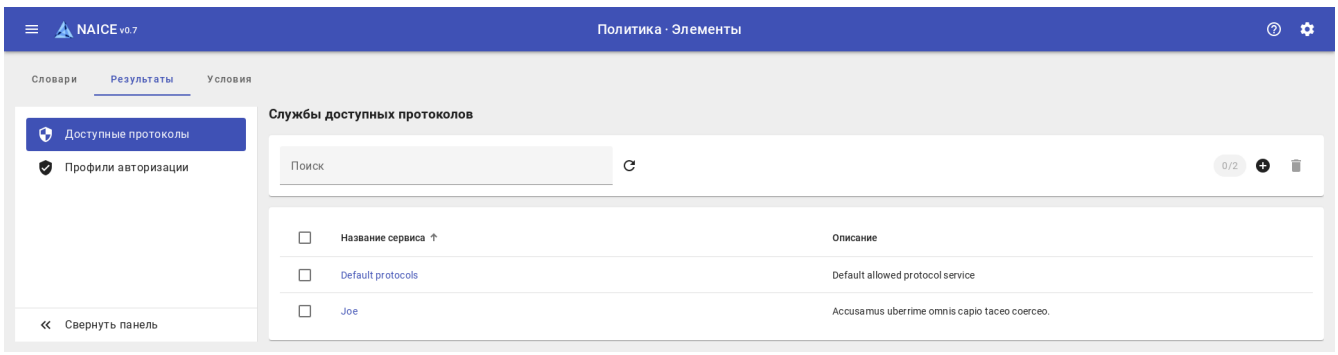

Рисунок 101. Таблица с перечнем служб доступных протоколов на странице просмотра

Слева расположена панель переключения между страницами результатов авторизации. Панель можно развернуть или свернуть при нажатии на соответствующую область в ее нижней части.

Справа расположена таблица со списком, которая содержит колонки:

- `Название сервиса` - название перечня доступных протоколов.
- `Описание` - произвольное описание.

Возможна сортировка в прямом и обратном порядке по любой колонке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по колонке "Название сервиса".

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - Обновить данные таблицы.
- 0/1 - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Добавление перечня доступных протоколов

Для добавления перечня доступных протоколов нажмите , после чего откроется окно:

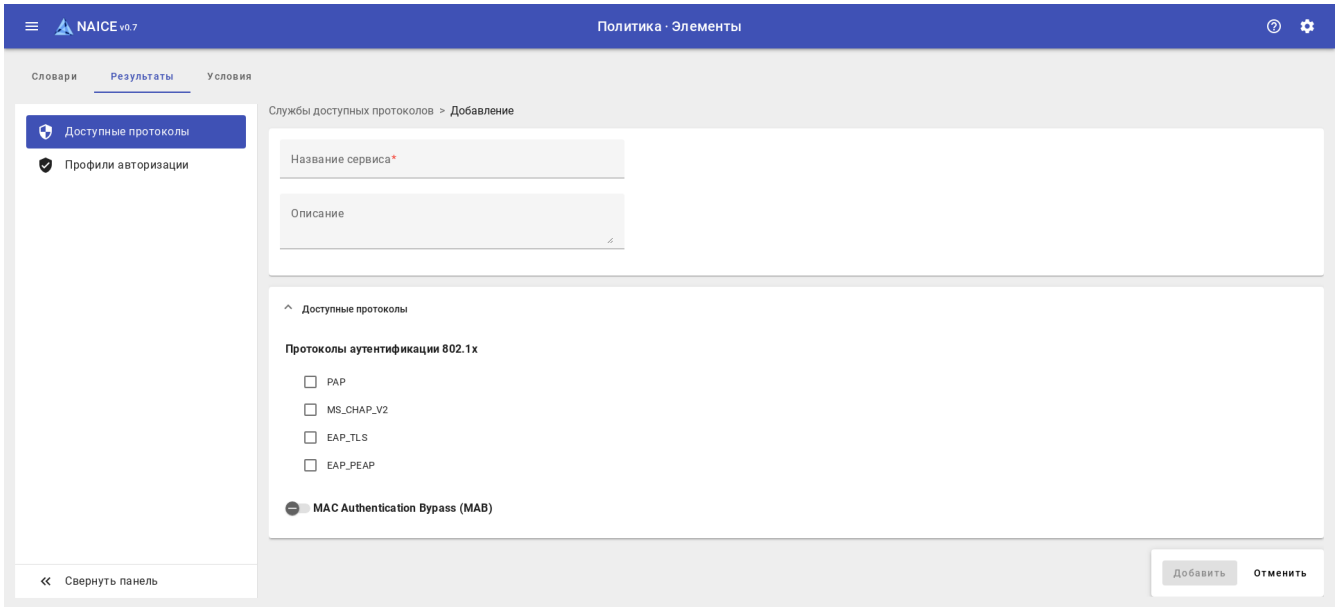

Рисунок 102. Окно добавления перечня доступных протоколов

- `Наименование сервиса` * - наименование, должно быть уникально. Максимальная длина - 100 символов.

`Описание` - произвольное описание. Максимальная длина - 200 символов.

- `Доступные протоколы` - выбор доступных протоколов аутентификации. По умолчанию все протоколы отключены.
  - `PAP` - выбрать протокол PAP (password authentication protocol), предусматривающий отправку логина и пароля на сервер аутентификации открытым текстом.
  - `MS_CHAP_V2` - выбрать протокол MS-CHAPv2 (Microsoft challenge handshake authentication protocol версии 2).
  - `EAP_TLS` - выбрать протокол EAP-TLS (Extensible Authentication Protocol Transport Layer Security).
  - `EAP_PEAP` - выбрать протокол EAP-PEAP (Protected Extensible Authentication Protocol), который инкапсулирует EAP (Extensible Authentication Protocol) внутрь TLS-туннеля (Transport Layer Security).
  - `MAC Authentication Bypass (MAB)` - разрешить аутентификацию конечных устройств по MAC адресу.

* - поля, обязательные для заполнения.

После ввода необходимых данных и выбора доступных протоколов нажмите кнопку **"Добавить"**.

Редактирование списка доступных протоколов

Для редактирования списка доступных протоколов необходимо на странице со списком нажать на его наименование.

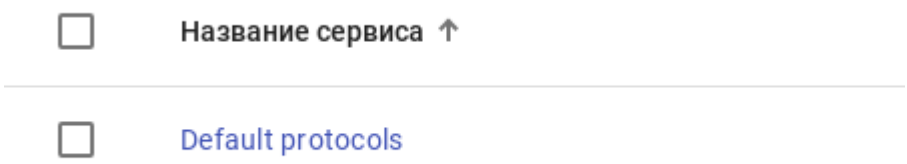

Рисунок 103. Гиперссылка на страницу редактирования перечня доступных протоколов

После этого откроется окно редактирования, аналогичное окну добавления.

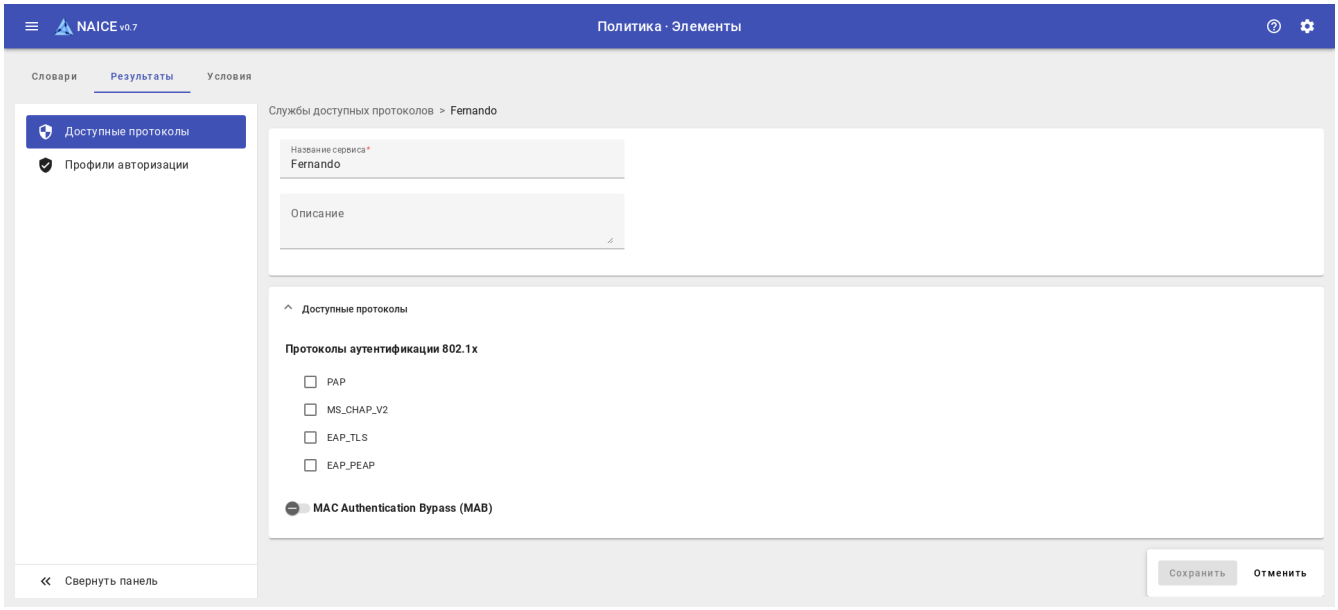

Рисунок 104. Окно редактирования перечня доступных протоколов

После редактирования нажать на кнопку **"Сохранить"**. Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

Удаление списка доступных протоколов

Для удаления в окне со списком надо выделить чекбокс слева от списка доступных протоколов, которые требуется удалить, и нажать кнопку  вверху справа.

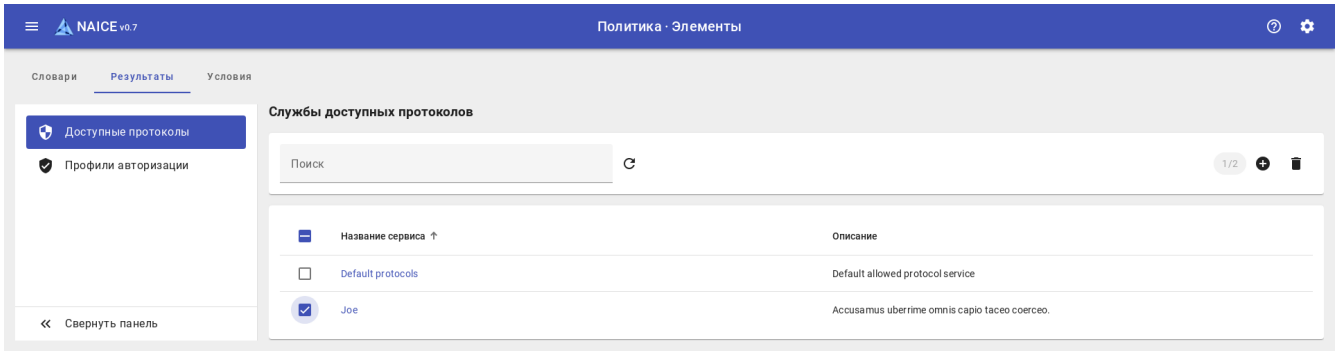

Рисунок 105. Выбор служб доступных протоколов в таблице для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

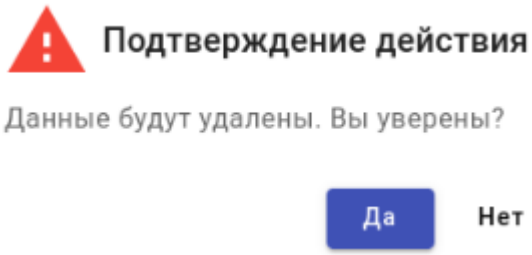

Рисунок 106. Модальный диалог подтверждения

Ограничения:

- нельзя удалить службу разрешенных протоколов, которая используется в каком-либо наборе политик.

Профили авторизации

Описание

Профили авторизации позволяют определить действия, которые необходимо выполнить после аутентификации пользователя. Доступно как разрешение доступа (ACCESS-ACCEPT), так и его запрет (ACCESS_REJECT).

Поддержано добавление в ответ ACCESS-ACCEPT после аутентификации клиента атрибутов:

- Динамически назначаемый VLAN клиента, с использованием стандартных IETF атрибутов (Tunnel-Medium-Type: IEEE-802, Tunnel-Type: VLAN, Tunnel-Private-Group-Id: <VLAN ID>) или атрибутов, настроенных в профиле устройства.
- Имя ACL, которую необходимо назначить клиенту (ACL с данным именем должна быть настроена на сетевом оборудовании).
- Любой другой RADIUS-атрибут через Расширенные настройки атрибутов.

Просмотр списка доступных профилей авторизации

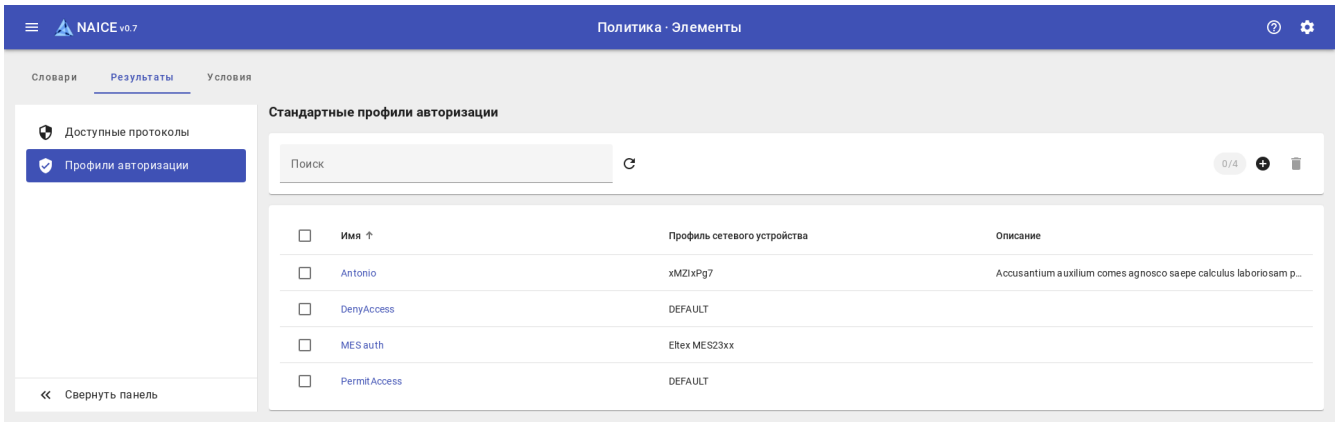

Рисунок 107. Таблица с перечнем профилей авторизации на странице просмотра

В левой части страницы расположена панель переключения между страницами результатов авторизации.

Панель можно свернуть или раскрыть в нижней ее области.

- « Свернуть панель
- » Развернуть

Основной компонент страницы - таблица профилей авторизации, которая содержит колонки:

- `Имя` - название профиля авторизации.
- `Профиль сетевого устройства` - выбранный профиль сетевого устройства.
- `Описание` - произвольное описание.

Возможна сортировка в прямом и обратном порядке по любой колонке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по колонке "Имя".

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - Обновить данные таблицы.
- 0/1 - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Добавление профиля авторизации

Для добавления профиля авторизации нажмите , откроется окно добавления профиля авторизации.

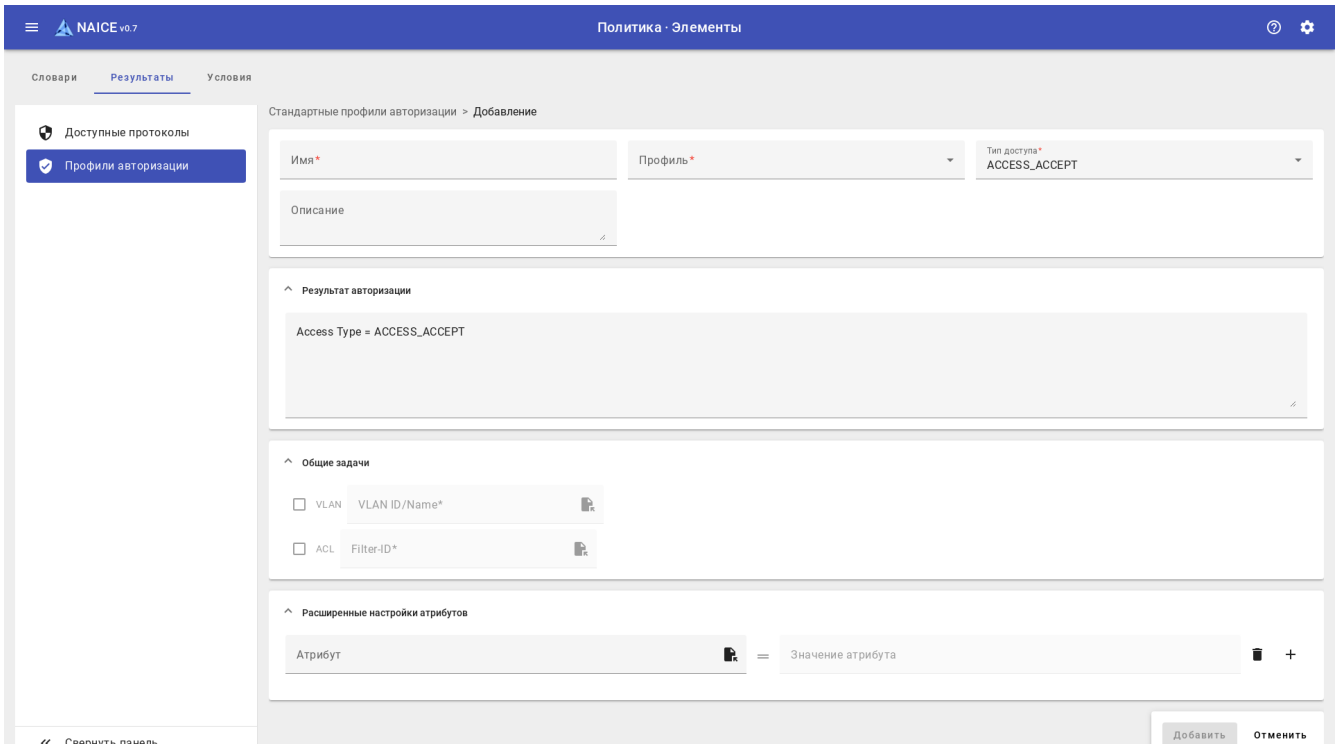

Рисунок 108. Окно добавления профиля авторизации

- `Имя` * - название, должно быть уникально. Максимальная длина - 100 символов.
- `Профиль` * - профиль сетевого устройства. В профиле сетевого устройства настраивается разрешение на выдачу клиентского VLAN и ACL, а также какие для этого использовать RADIUS-атрибуты.
-

`Тип доступа` * - тип доступа, при котором будет применяться профиль авторизации. Выпадающий список из двух элементов: `ACCESS_ACCEPT` (по умолчанию) и `ACCESS_REJECT`.

- `Описание` - произвольное описание. Максимальная длина - 200 символов.
- `Результат авторизации` - визуализация атрибутов в результирующем RADIUS-пакете на основе настроек "Типа доступа", "Общих задач" и "Расширенных настроек атрибутов".
- `Общие задачи` - включение и настройка распространенных сценариев при авторизации пользователя. Сценарии объединяют под собой один или несколько атрибутов. По умолчанию все сценарии отключены.
  - `VLAN` - включить динамическое назначение VLAN пользователю.
    - `VLAN ID/Name` - номер или имя VLAN, выдаваемое в атрибуте "Tunnel-Private-Group-Id" или другом атрибуте, настроенном в профиле устройства.
  - `ACL` - включить выдачу имени списка доступа пользователю.
    - `Filter-ID` - наименование списка доступа, назначаемое пользователю. Должно быть настроено с соответствующим наименованием на сетевом оборудовании, к которому подключается пользователь.
- `Расширенные настройки атрибутов` - ручная настройка выдачи RADIUS-атрибутов. Рекомендуется только в том случае, когда для определенного результата авторизации не доступен сценарий из списка `Общих задач`.

* - поля, обязательные для заполнения.

Для динамического назначения пользователю при авторизации VLAN и ACL необходимо, чтобы данные действия были включены в профиле сетевого устройства, который используется в профиле авторизации. В противном случае их настройка будет недоступна.

После ввода необходимых данных и выбора доступных протоколов нажмите кнопку **"Добавить"**.

Редактирование профиля авторизации

Для редактирования профиля авторизации необходимо на странице со списком нажать на его наименование.

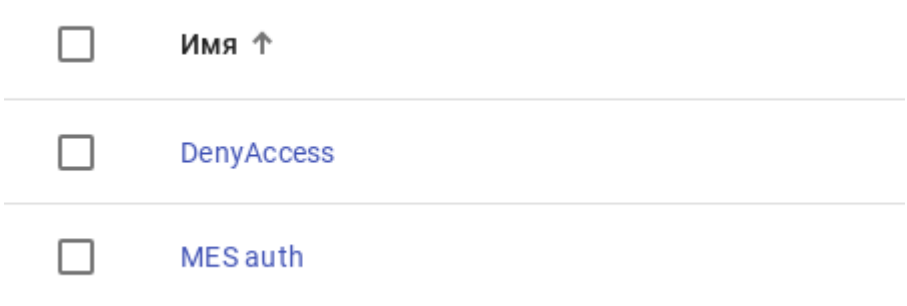

Рисунок 109. Гиперссылка на страницу редактирования профиля авторизации

После этого откроется окно редактирования, аналогичное окну добавления.

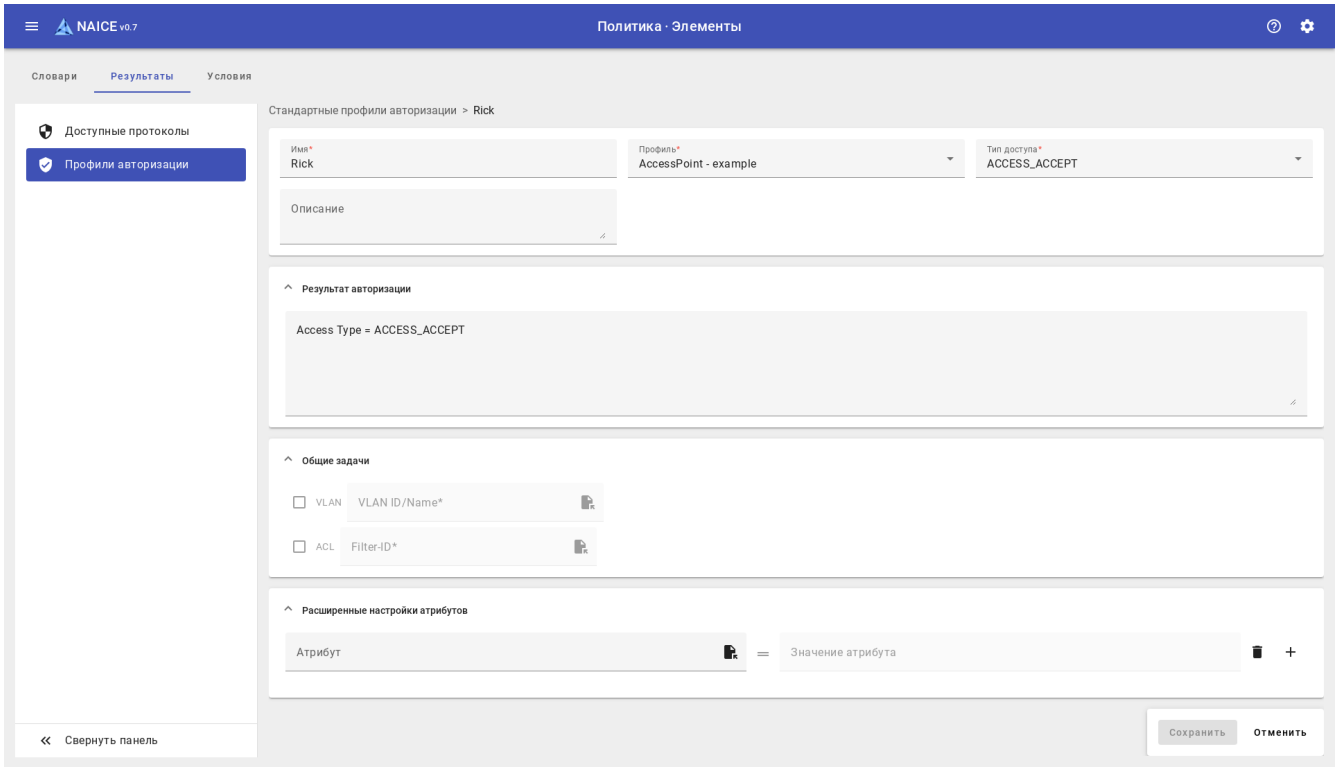

Рисунок 110. Окно редактирования профиля авторизации

После редактирования нажать на кнопку **"Сохранить"**. Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

Удаление профиля авторизации

Для удаления в окне со списком необходимо выделить чекбокс слева от профилей авторизации, которые требуется удалить, и нажать кнопку вверху справа.

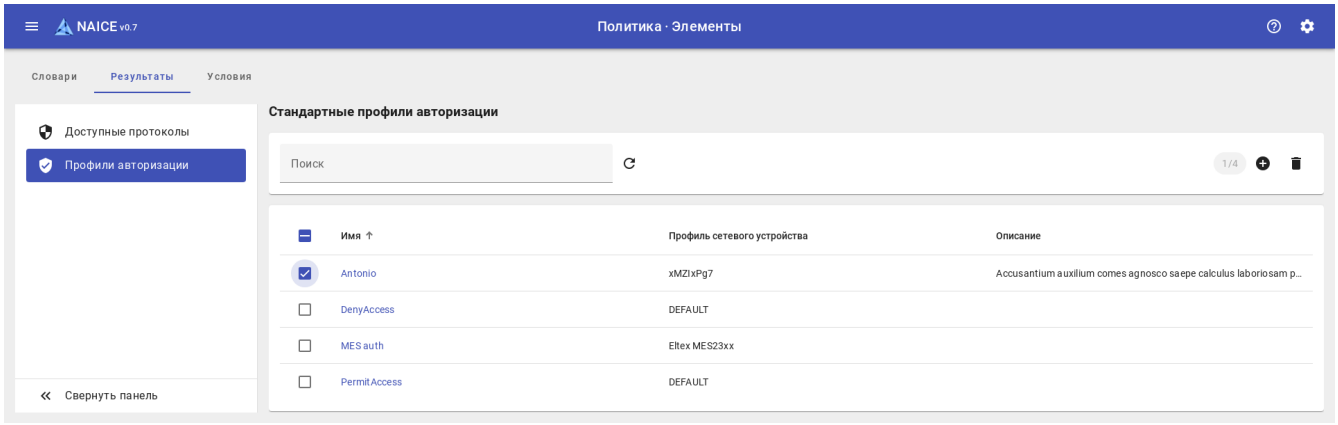

Рисунок 111. Выбор профиля авторизации в таблице для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

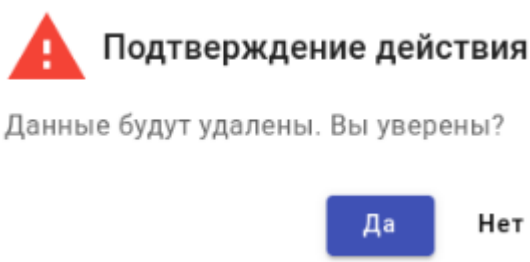

Рисунок 112. Модальный диалог подтверждения

Ограничения:

- нельзя удалить профиль авторизации, который используется в какой-либо политике авторизации.

Условия

Описание

Логические условия являются основным элементом политик аутентификации и авторизации, которые отвечают за формирование критериев, определяющих может ли пользователь пройти аутентификацию и какие действия должны быть к нему применены при выполнении авторизации.

В основе создания и обработки логического условия лежит алгебра логики. Результатом выполнения условия является "Истина" или "Ложь". Результат может быть инвертирован. Условие может быть простым и сложным. В простом условии в качестве критерия проверки выступает только один атрибут. В сложном условии можно использовать несколько различных атрибутов, объединив их логическими операциями "И" или "ИЛИ".

Просмотр списка логических условий

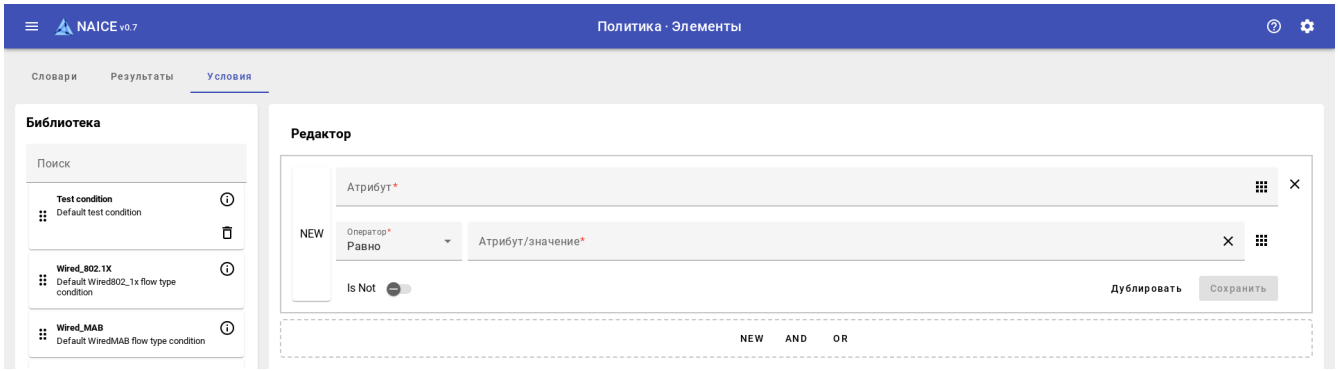

Рисунок 113. Библиотека логических условий

В левой части страницы расположена **Библиотека** логических условий.

Основной компонент страницы - **Редактор** логических условий:

- `Атрибут` * - атрибут логического условия.
- `Оператор` * - выбранный оператор логического условия. Может принимать значения (в зависимости от типа значения атрибута):
  - "Больше или равно" / "Меньше или равно"
  - "Больше чем" / "Меньше чем"
  - "Равно" / "Не равно"
  - "Равно NULL" / "Не равно NULL"
  - "Начинается на" / "Не начинается на"
  - "Заканчивается на" / "Не заканчивается на"

- "Содержит" / "Не содержит"
- "Соответствует" (*полное* соответствие строки с учетом регистра)

- `Атрибут/значение` * - атрибут/значение, которые используются для сопоставления с атрибутом логического условия в соответствие с выбранным оператором. Для атрибута, предполагающего предопределенные значения, выбор значения производится из списка.
- `Is Not` - выбор инвертирования результата выполнения условия (по умолчанию условие "Соблюдается", при включении настройки условие будет считаться "Не соблюдается")
- `NEW` - добавление нового логического условия в существующую иерархию на одном уровне с текущим.
- `AND` - добавление нового логического условия в качестве "дочернего" для существующего с логическим оператором "И".
- `OR` - добавление нового логического условия в качестве "дочернего" для существующего с логическим оператором "ИЛИ".

* - поля, обязательные для заполнения.

Элементы управления:

- `"Поиск"` - Выполняется регистронезависимая фильтрация по библиотеке логических условий по имени и описанию.
-  - Предпросмотр содержания логического условия.
-  - Удаление логического условия.
-  - Открыть словарь для добавления элемента.
-  - Удалить элемент из редактора. Действие зависит от расположения:
  - нажатие справа от поля "Атрибут" очистит соответствующее поле;
  - нажатие справа от поля "Атрибут/значение" очистит соответствующее поле;
  - нажатие справа от логического условия удалит данное условие.
- `"Сохранить"` - Сохранить соответствующее логическое условие.

Меню выбора атрибута

Для выбора атрибута, который будет использоваться в условии, необходимо нажать  - раскроется меню выбора атрибута.

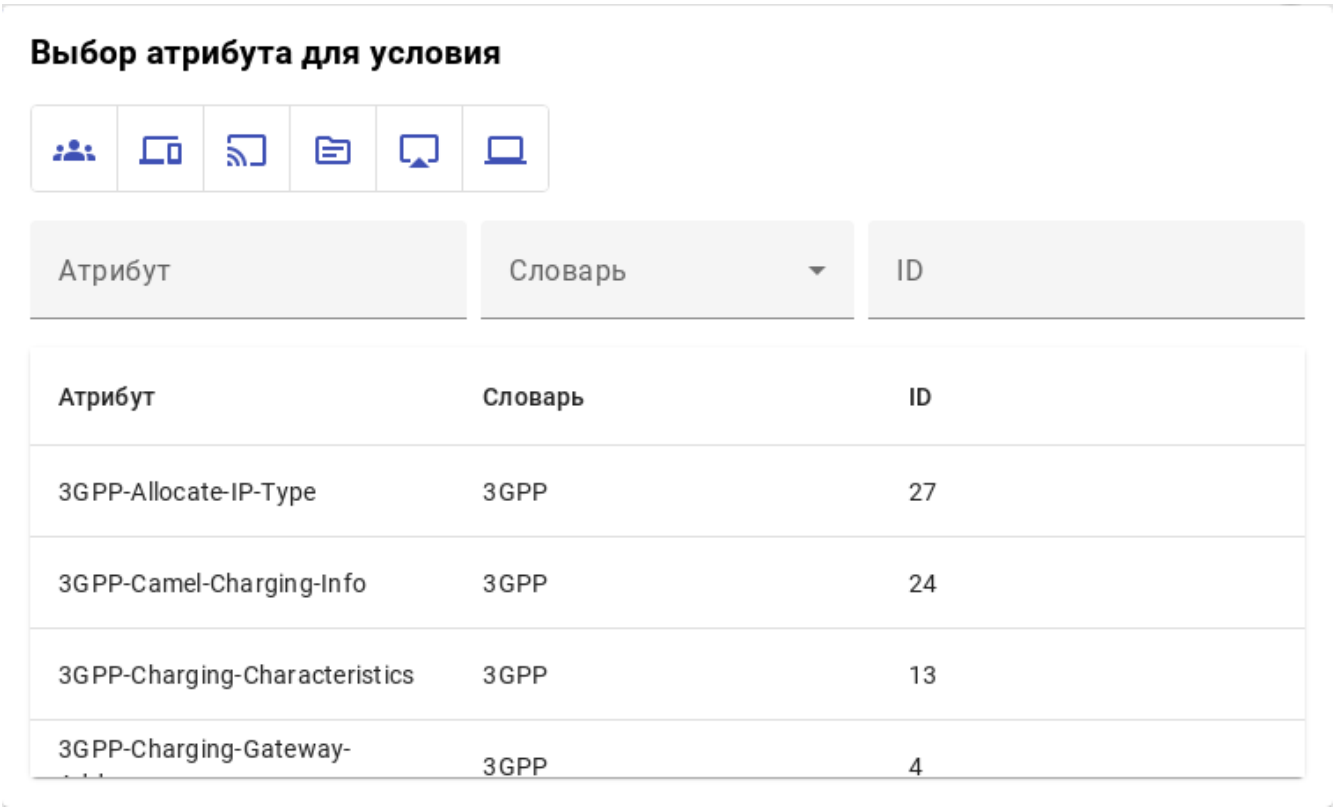

Рисунок 114. Меню выбора атрибута

Вверху находится список, позволяющий выполнить фильтрацию по типам словарей. Может быть выбран только один тип.

Типы словарей:

- `RADIUS` - словари RADIUS-атрибутов, в том числе vendor-specific.
- `NORMALISED_RADIUS` - системные атрибуты, формируемые на основе RADIUS-атрибутов, например - тип подключения.
- `INTERNAL_RADIUS` - служебный словарь с системными с атрибутами, как правило не используется.
- `DEVICE` - атрибуты на основе параметров устройства, например - тип устройства.
- `IDENTITY` - атрибуты пользователей и эндпоинтов.
- `LDAP` - атрибуты из внешних источников идентификации.

Ниже находятся колонки для фильтрации атрибутов.

- "Атрибут" - регистронезависимая фильтрация по наименованию атрибута.
- "Словарь" - меню выбора словаря. Для использования должен быть выбран тип словаря.
- "ID" - фильтрация по номеру атрибута.

Создание логических условий

Создание простого логического условия

Создание логического условия выполняется в **Редакторе**.

Рисунок 115. Исходное состояние редактора условия

После нажатия на ⠿ в правой части поля "Атрибут" раскроется меню выбора атрибута.

Для поиска нужного атрибута можно воспользоваться фильтрацией по наименованию атрибута. Либо выбрать тип словаря и в нем, выбрав необходимый словарь путем прокрутки выпадающего списка, определить необходимый атрибут.

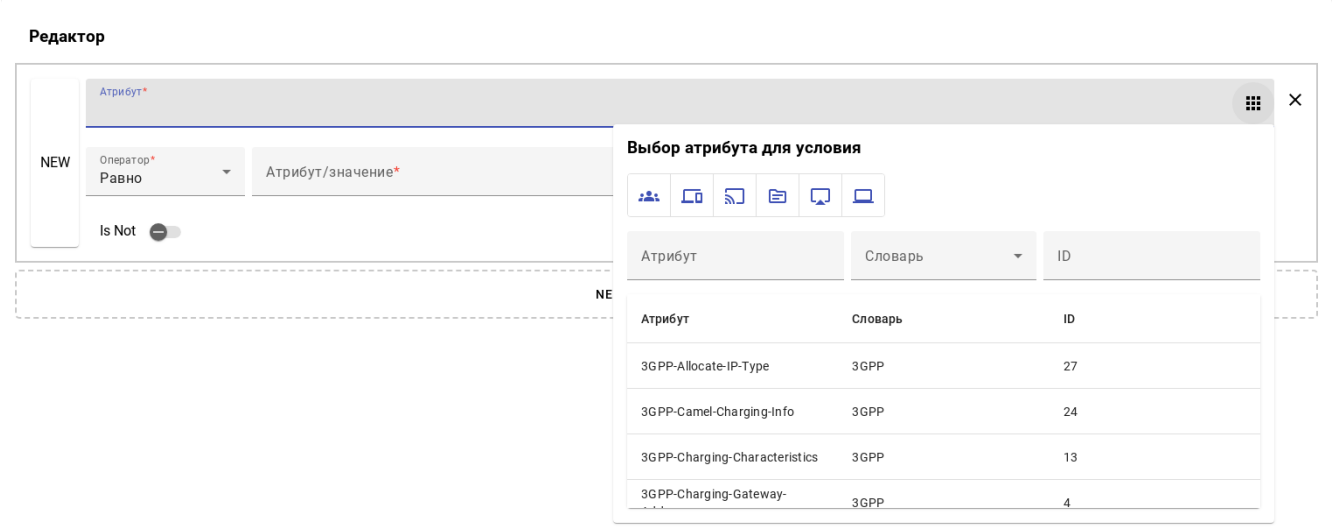

Рисунок 116. Выбор атрибута

После выбора атрибута необходимо кликнуть на него и он попадет в поле "Атрибут".

Далее необходимо выбрать оператор для сравнения значения атрибута (по умолчанию подставляется "Равно"). Список операторов зависит от типа данных используемых в значении выбранного атрибута.

Тип данных атрибута	Поддерживаемые операторы
Строка	Соответствует, Оканчивается на, Не оканчивается на, Начинается с, Не начинается с, Содержит, Не содержит, Равно, Не равно, Равно NULL, Не равно NULL
Число	Больше или равно, Больше чем, Меньше или равно, Меньше чем, Равно, Не равно, Равно NULL, Не равно NULL
IPv4 адрес	Равно, Не равно, Равно NULL, Не равно NULL
MAC адрес	Равно, Не равно, Равно NULL, Не равно NULL, Начинается на, Не начинается на, Заканчивается на, Не заканчивается на, Содержит, Не содержит,
Наименование	Равно, Не равно, Равно NULL, Не равно NULL
Последовательность байт	Равно NULL, Не равно NULL

Затем в поле *Атрибут/значение* выбирается атрибут или вводится его значение.

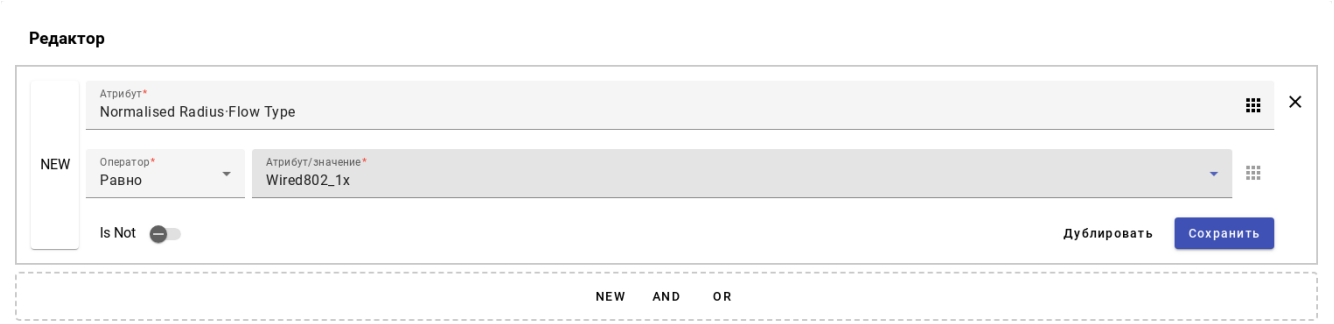

Рисунок 117. Условие, в котором заполнены все параметры

Для сохранения условия в библиотеку условий нужно нажать кнопку **"Сохранить"**. Можно заменить существующее условие в библиотеке или сохранить новое.

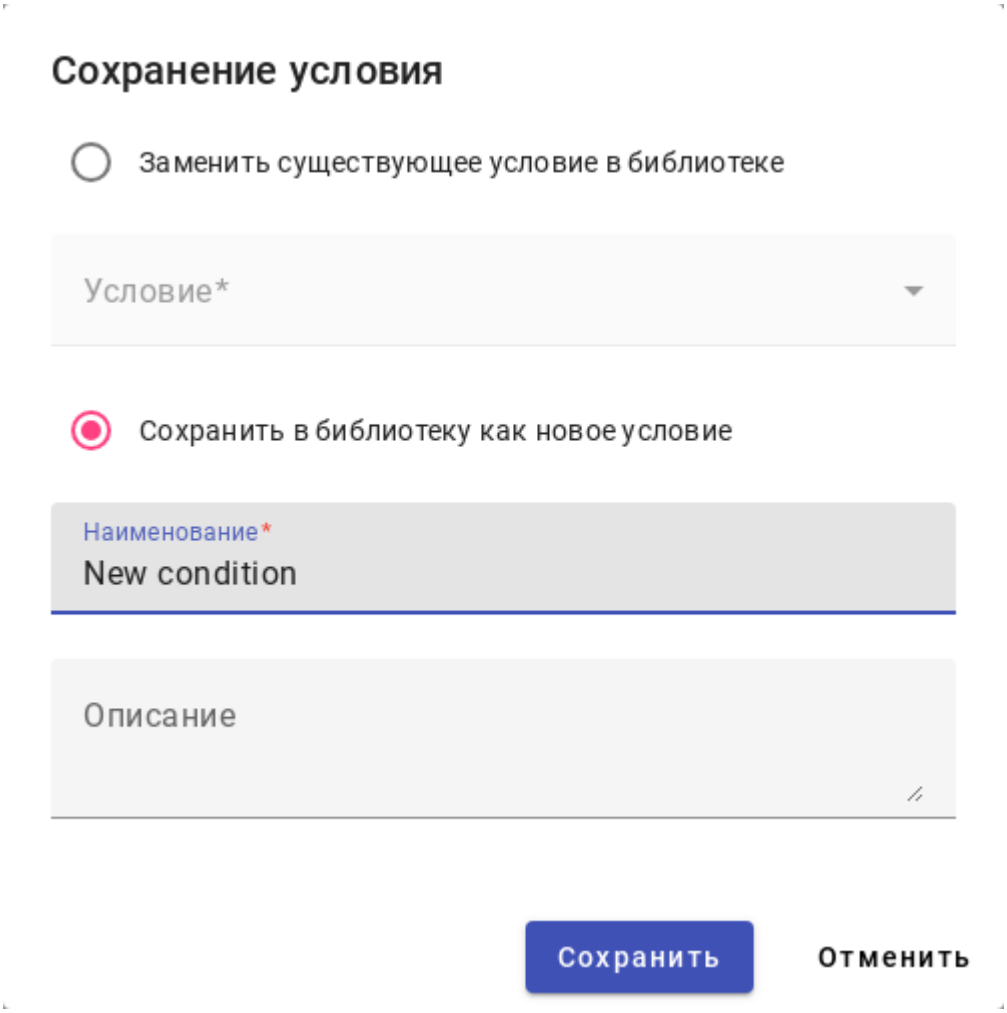

Рисунок 118. Диалог сохранения условия в библиотеку

По умолчанию действие предполагает сохранение нового условия:

- "Наименование" * - наименование условия. Максимальная длина - 100 символов.
- "Описание" - произвольное описание. Максимальная длина - 200 символов.

* - поля, обязательные для заполнения.

После нажать кнопку "Сохранить".

Для сохранения с заменой существующего условия в библиотеке необходимо выбрать *"Заменить существующее условие в библиотеке"* и выбрать условие в выпадающем списке. При необходимости можно выполнить фильтрацию по наименованию, введя соответствующий текст в поле перед списком.

После нажать кнопку "Сохранить".

Кнопка "Сохранить" всегда активна, чтобы иметь возможность сохранить существующее условие под другим именем.

Создание сложного логического условия

Для создания сложного логического условия из простого используется панель под логическим условием.

Рисунок 119. Панель для добавления дополнительного условия

- `New` - добавить логическое условие на одном уровне с существующим.
- `AND` - добавить дочернее условие с логическим "И".
- `OR` - добавить дочернее условие с логическим "ИЛИ".

При нажатии "New" в редакторе появится дополнительное правило на одном уровне с существующим, объеденные логическим "И".

Рисунок 120. Условие, состоящее из двух условий, объеденные логическим "И"

- Логическое "И", объединяющее правила, можно изменить на "ИЛИ".
- Есть возможность сохранить каждое условие отдельно кнопкой "Сохранить" в его окне или все вместе, кнопкой "Сохранить" внизу.
- Для удаления условия надо нажать на ✕ справа вверху в окне условия.
- Для полной очистки всех условий в редакторе надо нажать ✕ вверху справа редактора, расположенный за окнами отдельных условий.

При нажатии "AND" или "OR" появится новое окно, в котором можно будет доступно новое меню, далее можно добавить условия на новом уровне или создать дочерние условия. Ограничение на вложенность условий нет.

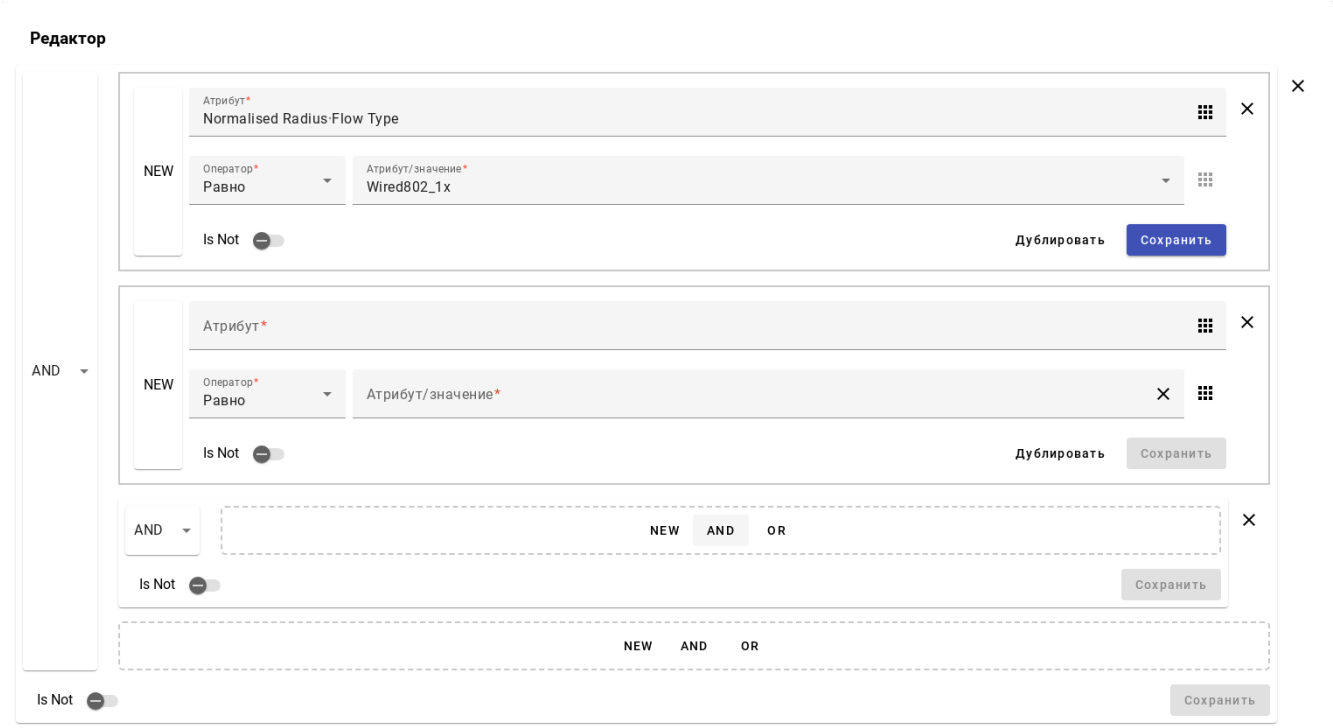

Рисунок 121. Условие, содержащее вложенные правила

Для сохранения всех условий надо нажать кнопку "Сохранить" в нижнем правом углу.

Редактирование логического условия

Для редактирования логического условия необходимо его захватить курсором в библиотеке и перенести в поле редактора.

Рисунок 122. Редактирование логического условия

Для редактирования условия нажать кнопку "Изменить". После редактирования нажать кнопку "Сохранить". Так как условие ранее было сохранено в библиотеке - по умолчанию будет предложено сохранить его с тем же названием. При необходимости можно выбрать другое условие, которое будет перезаписано или выбрать "Сохранить в библиотеку как новое условие". Нажать кнопку "Сохранить".

Так же в ходе редактирования можно перетаскивать условия из библиотеки в поле редактора дочернего условия.

Удаление логического условия

Для удаления логического условия надо найти его в библиотеке и нажать кнопку справа от имени условия.

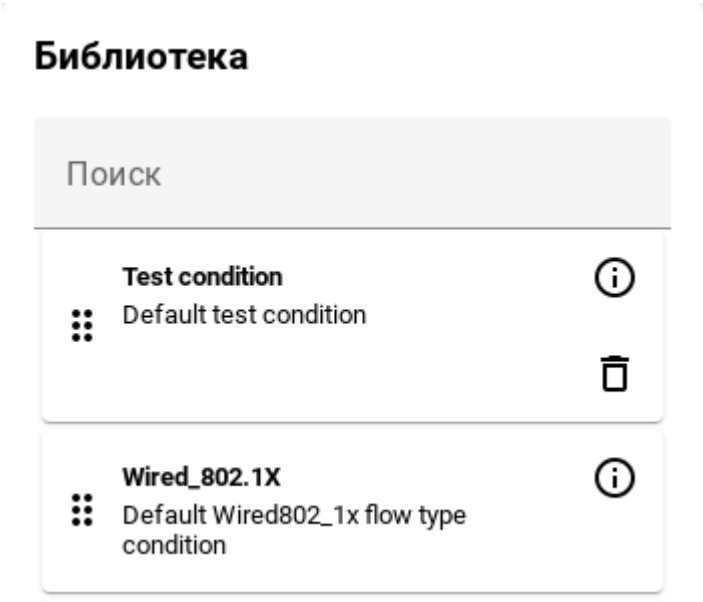

Рисунок 123. Выбор условия для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

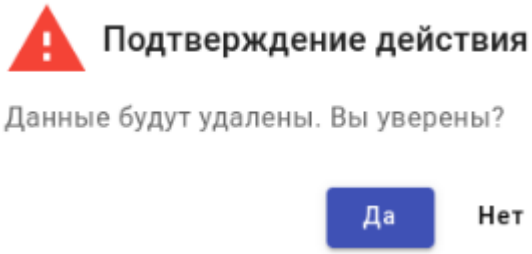

Рисунок 124. Модальный диалог подтверждения

Ограничения:

- нельзя удалить некоторые системные логические условия;
- нельзя удалить логические условия, которые используются в других сложных логических условиях;
- нельзя удалить логические условия, которые используются в каком-либо наборе политик.

Наборы политик

Описание

Политики аутентификации и авторизации определяют действия, которые необходимо выполнить при получении запросов на аутентификацию пользователей от сетевых устройств по протоколу RADIUS и действия при авторизации пользователей.

Порядок обработки запросов

Порядок обработки запросов аутентификации/авторизации от пользователей, передаваемых сетевыми устройствами, следующий:

Первоначальная проверка данных сетевого устройства:

- Входящий RADIUS-запрос анализируется на наличие атрибута `NAS-IP-Address` - в случае отсутствия пакет отбрасывается, никакой ответ не возвращается.
- Полученный `NAS-IP-Address` ищется среди записей о сетевых устройствах - в случае отсутствия пакет отбрасывается, никакой ответ не возвращается.
- Проверяется корректность secret в RADIUS-запросе - если секретный ключ неверен возвращается `ACCESS-REJECT`.

2. Обработка в таблице набора политик.
   - Выполняется проверка соответствия RADIUS-пакета логическим условиям, используемым в наборах политик.
   - Проверка выполняется последовательно сверху вниз. Отключенные наборы политик не участвуют в проверке.
   - При обнаружении подходящего набора политик дальнейший их перебор прекращается и продолжается проверка в рамках этого набора.
   - Если набор политик с подходящим условием не будет найден - сетевому устройству будет отправлен ответ в рамках политики `Default`. По-умолчанию в данном наборе политик в политике авторизации настроен профиль авторизации **DenyAccess**, согласно которому сетевому устройству будет отправлен `ACCESS-REJECT`. Данное поведение можно изменить, отредактировав политики в `Default`.
3. Обработка в рамках найденного набора политик:
   - Проверяется используемый протокол аутентификации и сравнивается с доступными в выбранном списке протоколов. Если совпадений не обнаружено - сетевому устройству будет отправлен `ACCESS-REJECT`.
   - В правилах политики аутентификации выполняется проверка сверху вниз, пока не будет найдено совпадающее условие. Если не будет найдено ни одного правила с совпадающим условием, то будет применено правило `Default` - по умолчанию сетевому устройству будет отправлен `ACCESS-REJECT`.
   - Выполняется поиск пользователя в выбранной цепочки источников идентификации. Если пользователь найден, то продолжается авторизация, если не найден - будет отправлен `ACCESS-REJECT`.
   - В политиках авторизации выполняется проверка правил сверху вниз, пока не будет найдено совпадающее условие. Если не будет найдено ни одного правила с совпадающим условием - сетевому устройству будет отправлен `ACCESS-REJECT` по правилу `Default`. Дефолтное поведение может быть перенастроено.
   - После определения правила политики авторизации выполняется проверка пароля пользователя. Если он не совпадает - сетевому устройству будет отправлен `ACCESS-REJECT`.
   - После успешной проверки логина/пароля пользователя выполнятся добавление в ответ атрибутов, предполагаемых по используемому профилю авторизации, и отправка ответа сетевому устройству. В профиле авторизации может быть настроен как `ACCESS-ACCEPT`, так и `ACCESS-REJECT` ответ.

Просмотр списка наборов политик

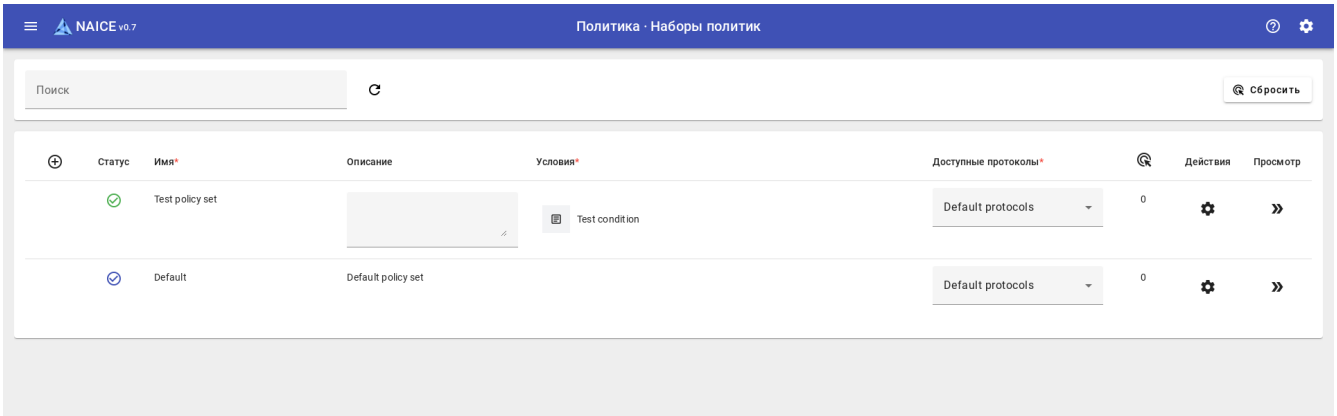

Рисунок 125. Просмотр всех наборов политик.

В таблице отображаются наборы политик, в соответствии с которыми проводится обработка запросов на аутентификацию/авторизацию.

> Последний набор политик с именем `Default` не может быть удален, у него нельзя изменить имя или условие.
> Он всегда будет последней в списке, ниже которой расположить другие политики нельзя.

Описание колонок таблицы:

- `Статус` - статус набора политик.
- `Имя` * - наименование набора политик.
- `Описание` - произвольное описание.
- `Условия` * - используемые логические условия. Если используется библиотечное условие - отображается его имя. Если используется не библиотечное условие - отображается его структура.
- `Доступные протоколы` * - выбранный список доступных протоколов.
- - количество попыток авторизации, подпадающих под указанные Условия.
- `Действия` - действия по добавлению/удалению набора политик.
- `Просмотр` - переход к просмотру и редактированию политик аутентификации/авторизации выбранного набора политик.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Элементы управления:

- `Поиск` - регистронезависимый поиск по имени набора политик (найденные совпадения будут подсвечены желтым цветом).
- - обновить данные.
- **Сбросить** - сбросить счетчики количества срабатываний всех наборов политик.
- - добавить политику (политика будет добавлена первой в списке).

- количество попыток авторизации, подпадающих под указанные Условия. При нажатии на число срабатываний счетчик можно **Сбросить**.

- - действия:
  - `Добавить сверху` - добавить набор политик *До* выбранного;
  - `Добавить снизу` - добавить набор политик *После* выбранного;
  - `Удалить` - удалить выбранный набор политик.
- » - перейти к управлению политиками аутентификации/авторизации текущего набора политик.
- `Сохранить` - сохранить изменения.
- `Отменить` - отменить изменения.

Все наборы политик проверяются по порядку, как на экране - сверху вниз. Потому на странице отображаются ВСЕ наборы политик сразу, а `Поиск` не скрывает записи из списка, а лишь подсвечивает их желтым цветом.

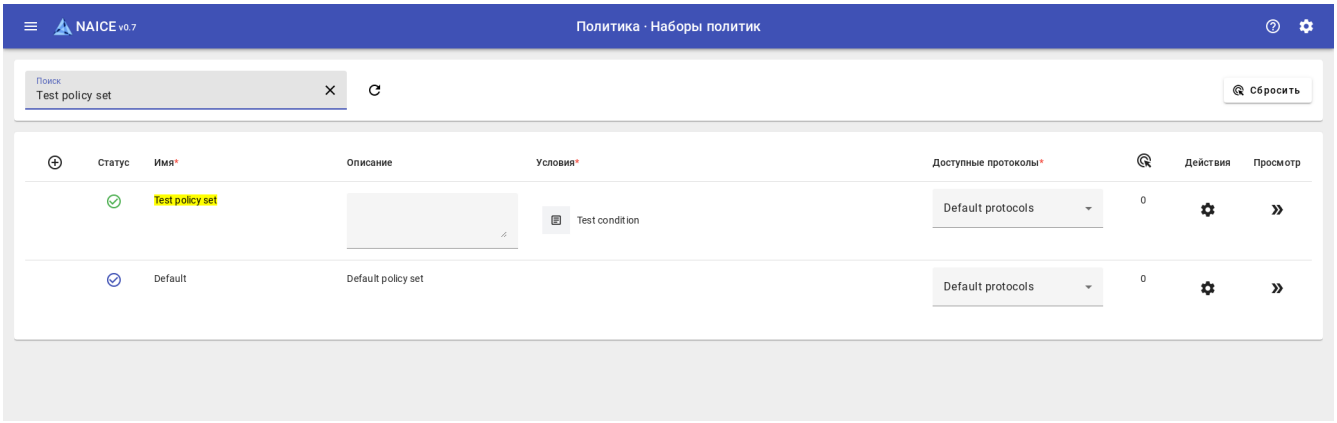

Рисунок 126. Поиск набора политик

Для изменения порядка перетащите политику за элемент в колонке (становится видимым при наведении в эту область).

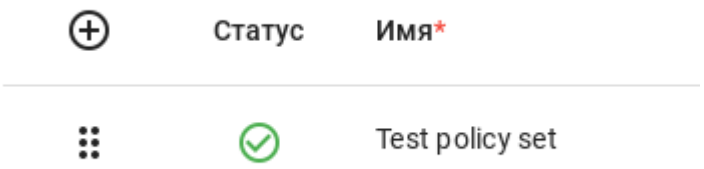

Рисунок 127. Иконка перетаскивания набора политик

После изменения порядка политик не забывайте нажать кнопку `Сохранить`, иначе изменения не вступят в силу.

Для просмотра списка политик аутентификации и авторизации необходимо в колонке `Просмотр` нажать » справа от выбранного набора политик.

Редактирование набора политик

Для добавления набора политик в окне списка наборов политик можно нажать вверху слева кнопку ⊕ - новый набор будет добавлен первый в списке.

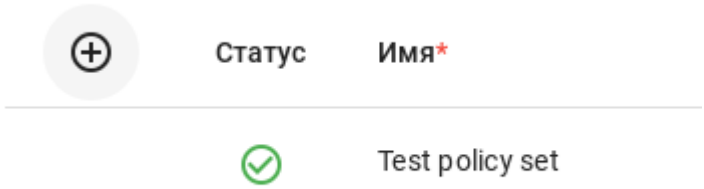

Рисунок 128. Иконка добавления набора политик

При необходимости добавить набор политик в произвольное место необходимо нажать на кнопку ⚙ справа от выбранного набора политик и в выпадающем меню выбрать `Добавить сверху` или `Добавить снизу`.

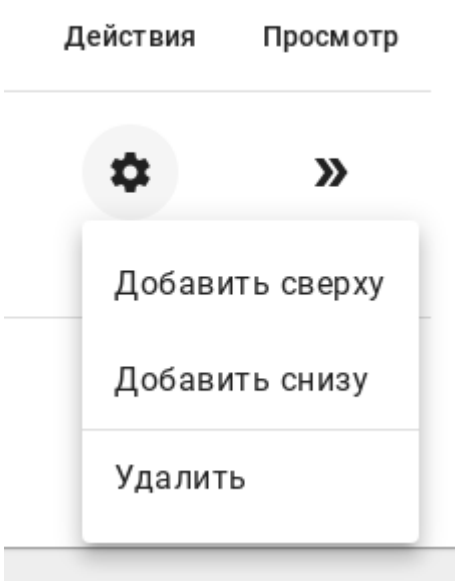

Рисунок 129. Отображение политики. Выпадающие меню с действиями.

Информация по `Статусу`:

- `Включено` - разрешается обрабатывать запросы;
- `Выключено` - исключить из обработки, не проверять Условие, не обрабатывать запросы;
- `Монитор` - разрешается проверять Условие (и инкрементировать счётчик срабатываний), обрабатывать запросы - нет;
- `По умолчанию` - используется только для политики по умолчанию `Default`.

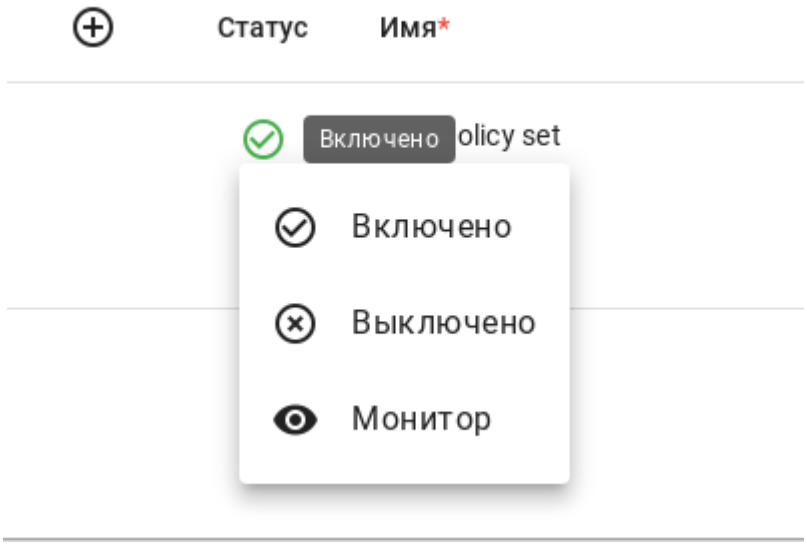

Рисунок 130. Изменение статуса политики.

Во вновь созданном наборе политик в поле `Имя` ввести наименование набора политик или оставить неизменным автоматически сформированное название.

Рисунок 131. Отображение записи новой политики. Элементы обязательные для заполнения.

Для редактирования условия необходимо нажать + и откроется редактор условий.

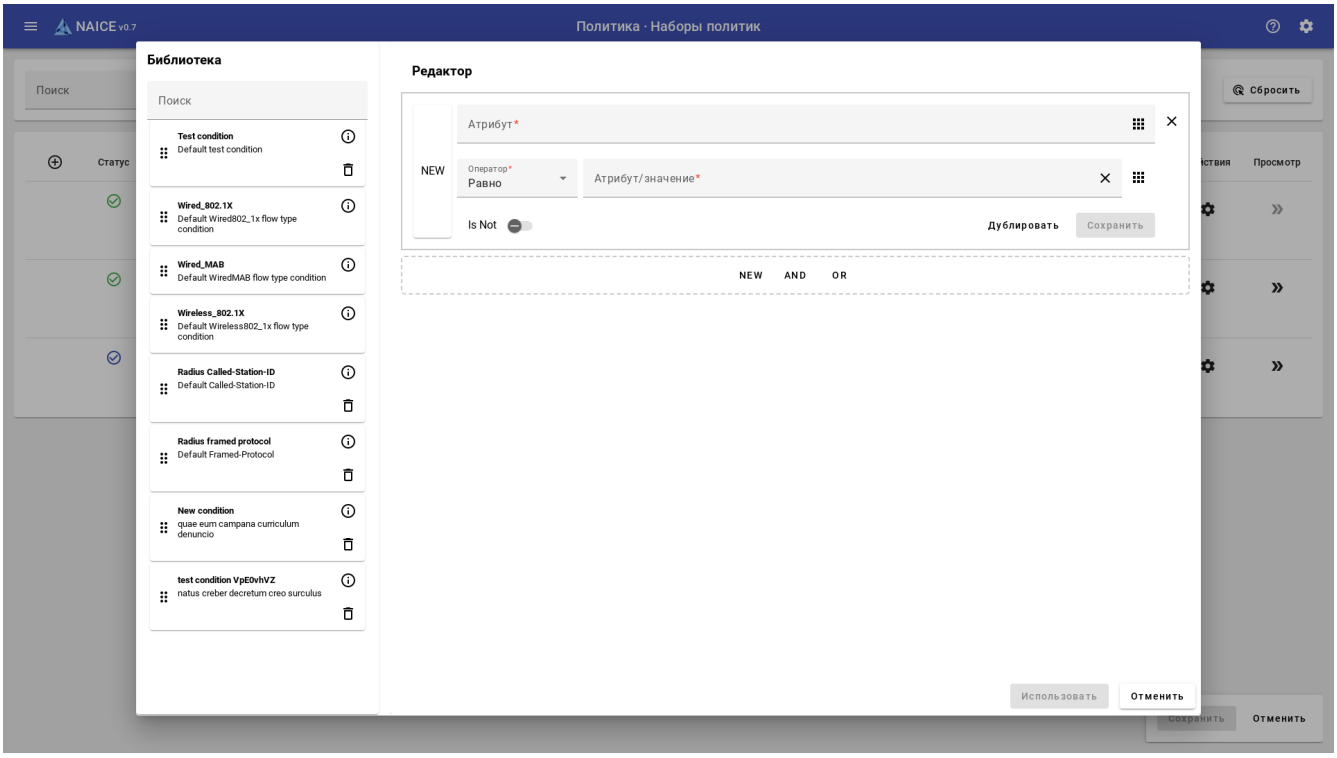

Рисунок 132. Редактор условий.

Редактирование условий выполняется способом, аналогичным описанному в условиях.

При настройке условия набора политик есть ограничение по используемым типам словарей. Можно использовать словари: `DEVICE`, `RADIUS`, `NORMALISED_RADIUS`, `INTERNAL_RADIUS`. Это связано с тем, какая информация о клиентском подключении может быть получена к моменту проверки набора политик, а какая еще нет.

При редактировании условий непосредственно в политике добавляется возможность использовать настроенное условие без сохранения его в **Библиотеке**. Для этого надо после настройки, не сохраняя условие, нажать кнопку `Использовать`.

После этого в колонке `Доступные протоколы` выбрать необходимый список.

По нажатию кнопки **Сохранить** изменения будут сохранены.

После создания новой политики необходимо настроить для нее политики аутентификации и авторизации, без этого все попытки подключения пользователей, попавшие под логическое условие данной политики, будут отклонены по правилам по умолчанию `Default`!
Для настройки перейти в Политики аутентификации и авторизации.

Удаление набора политик

Удаление набора политик доступно в меню `Действия`. Доступно удаление только одного набора политик за раз.

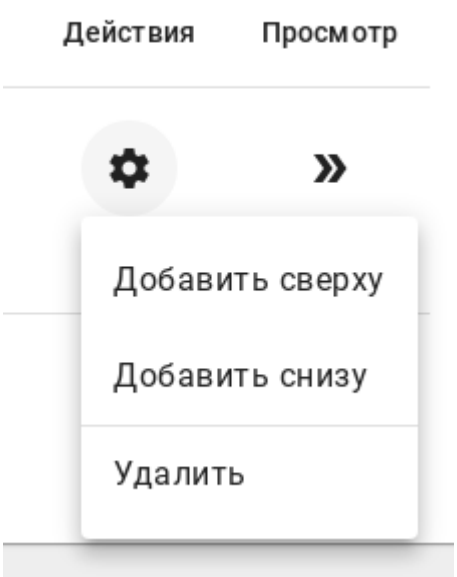

Рисунок 133. Выпадающие меню для удаления набора политик

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

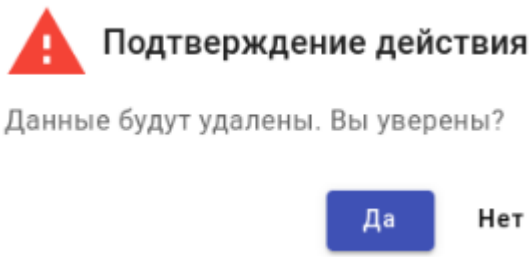

Рисунок 134. Модальный диалог подтверждения

Количество срабатываний политики

Счётчики в колонке показывают, сколько попыток авторизации было обработано с использованием этой политики. Изменения значений свидетельствует о том, что `Условие` срабатывает; нулевые значения, наоборот, говорят о несоответствии получаемых RADIUS-запросов отслеживаемому условию.

Используя статус `Монитор` и наблюдая за счётчиками срабатывания, можно сначала подобрать и отладить условие, а лишь потом включать политику в работу, переведя её в статус `Включено`.

Политики аутентификации и авторизации

Просмотр списка политик аутентификации и авторизации в выбранном наборе политик

Для просмотра списка политик аутентификации и авторизации необходимо в колонке `Просмотр` нажать справа от выбранного набора политик. Откроется детальная страница по изменению правил политик аутентификации и авторизации.

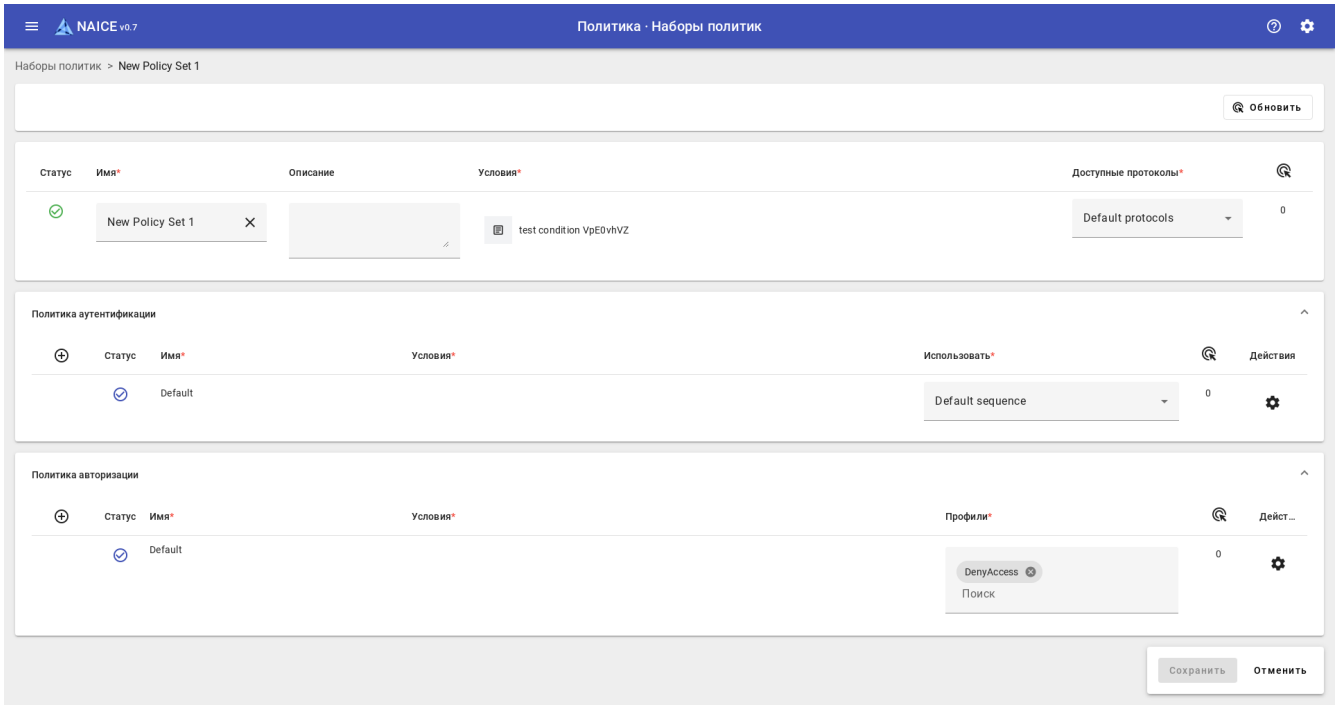

Рисунок 135. Страница просмотра и редактирования набора политик

Последние правила политик аутентификации и авторизации с именем `Default` нельзя переименовать или изменить им условие срабатывания.
Они всегда будут последние в списке, ниже расположить другие правила нельзя.
Данные правила предназначены для определения поведения по умолчания, когда другие правила не подходят.

Форма просмотра отдельного набора политик разбита на блоки:

- Блок, отвечающий за управление набором политик, который отображает содержимое выбранного набора политик в формате аналогичном используемому на странице Наборы политик.
- **Политика аутентификации** - управление аутентификацией пользователей.
- **Политика авторизации** - управление авторизацией пользователей.

Элементы управления:

- `Обновить` - запрос актуального количества срабатываний политик.
- `Статус` - включить/выключить/поставить на мониторинг соответствующую политику.
- `Имя` * - наименование политики.
- `Описание` - произвольное описание.
- `Условия` * - используемые логические условия. Если используется библиотечное условие - отображается его имя. Если используется не библиотечное условие - отображается его структура.
- `Доступные протоколы` * - выбранный список доступных протоколов.
- `Использовать` * - выбранная цепочка источников идентификации.
- `Профили` * - выбор доступных профилей авторизации.
- - количество попыток авторизации, подпадающих под указанные Условия. При нажатии на число срабатываний счетчик можно **Сбросить**.
- `Сохранить` - сохранить изменения.
- `Отменить` - отменить изменения.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Для изменения порядка Политик Аутентификации и Авторизации перетащите политику за элемент в колонке (становится видимым при наведении в эту область) аналогично разделу Наборы политик.

Редактирование политик аутентификации и авторизации

Для редактирования необходимо нажать справа от выбранного набора политик.

Требуется настроить как минимум одну политику аутентификации и одну политику авторизации для возможности успешного подключения клиента с использованием данного набора политик, или перенастроить запрещающее правило по умолчанию `Default`.

Политику по умолчанию `Default` можно отредактировать, настроив другое поведение, однако для безопасности рекомендуется настраивать собственные правила с более узкой областью действия, а поведение по умолчанию оставить запрещающим.

Политика аутентификации

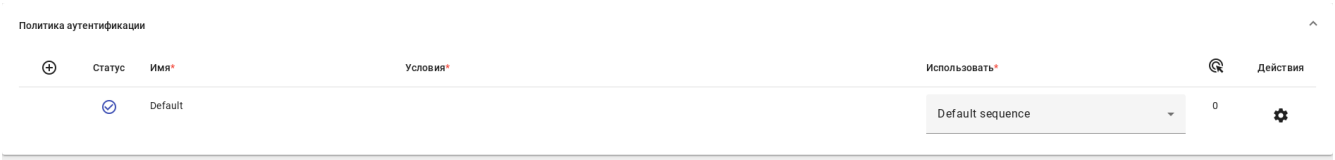

Рисунок 136. Панель политик "Аутентификации".

Для настройки политики аутентификации в блоке **Политика аутентификации** необходимо нажать кнопку ⊕. Появится новое правило.

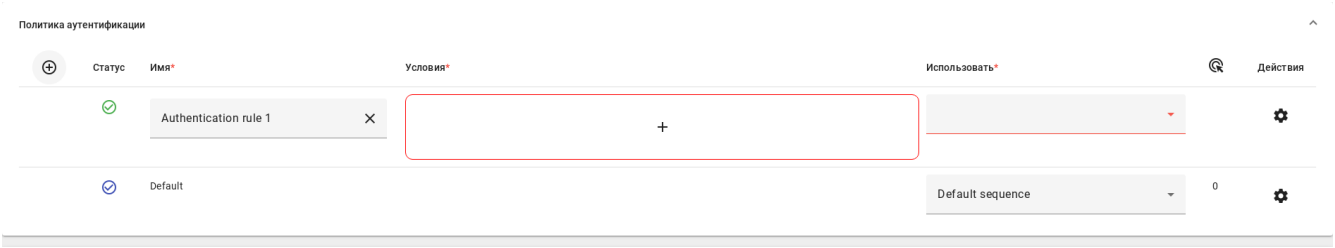

Рисунок 137. Новая политика "Аутентификации".

В поле `Имя` ввести наименование политики.

Для редактирования условия необходимо нажать + - откроется редактор условий.

Редактирование условий выполняется аналогично описанному в Условия.

При настройке политики аутентификации есть ограничение по используемым типам словарей. Можно использовать словари: `DEVICE`, `RADIUS`, `NORMALISED_RADIUS`, `INTERNAL_RADIUS`.

При редактировании условий непосредственно в политике добавляется возможность использовать настроенное условие без сохранения его в Библиотеке условий. Для этого надо после настройки не сохраняя условие нажать кнопку `Использовать`.

Выбрать в выпадающем меню `Использовать` цепочку идентификаций.

Кнопкой ⚙ справа от политики можно добавить новое правило выше или ниже, либо удалить текущее.

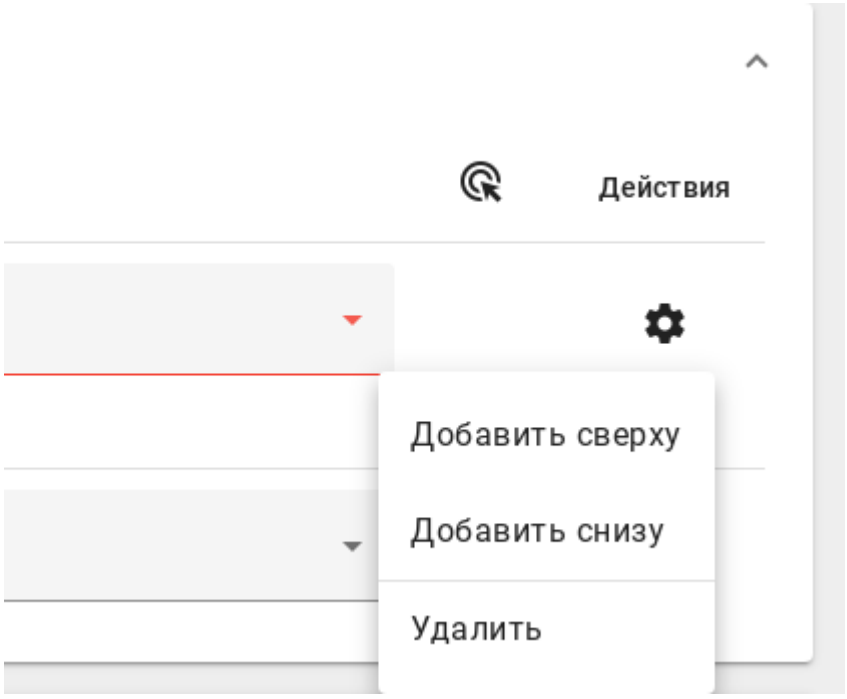

Рисунок 138. Политика аутентификации. Выпадающие меню. Действия.

Также можно изменить статус политики аналогично статусам в наборах политик.

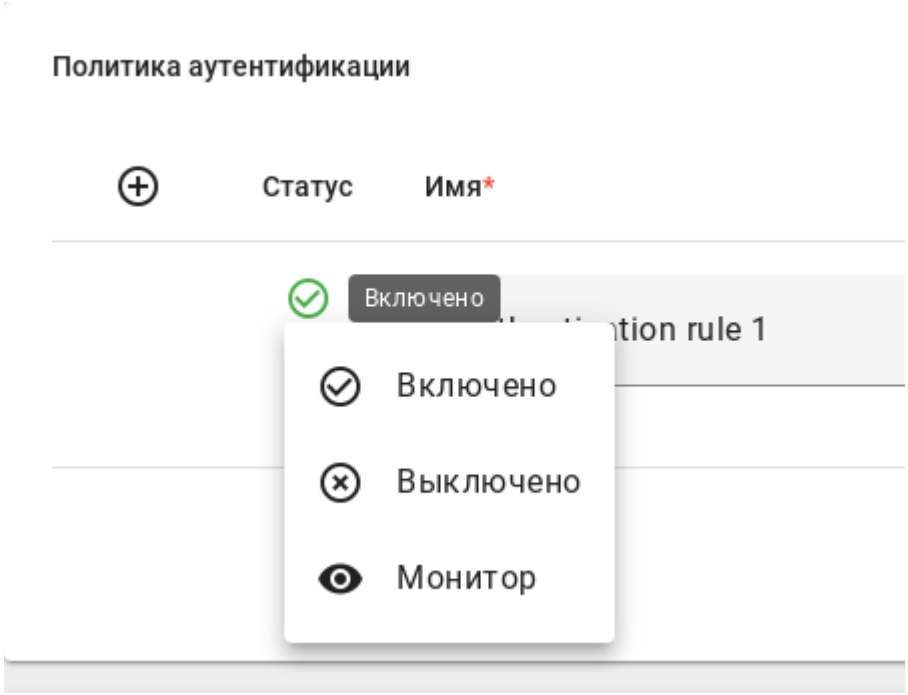

Рисунок 139. Политика аутентификации. Изменение статуса политики.

Политика авторизации

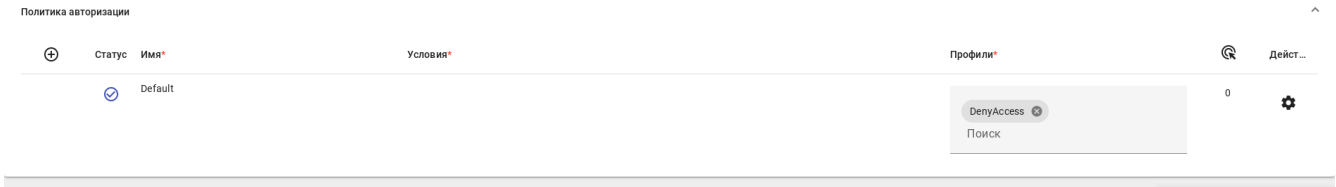

Рисунок 140. Панель политик "Авторизации".

Для настройки правила политики авторизации в блоке **Политики авторизации** нажать ⊕. Появится новое правило.

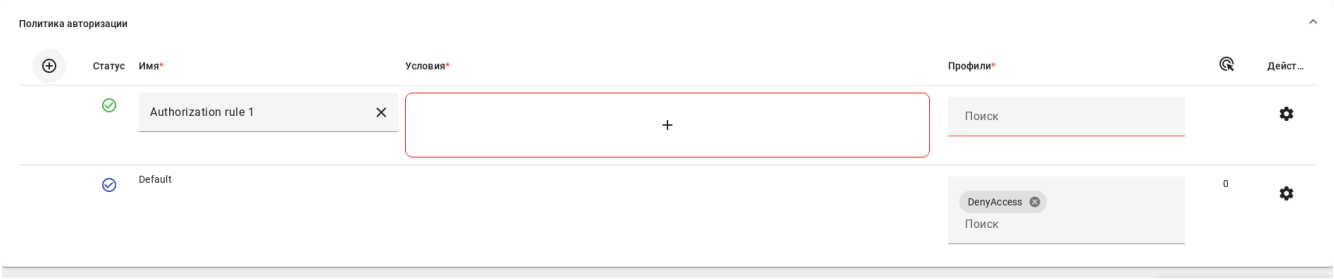

Рисунок 141. Новая политика "Авторизации".

В поле `Имя` ввести наименование правила политики.

Для редактирования условия необходимо нажать + - откроется редактор условий.

Редактирование условий выполняется аналогично описанному в Условия.

При настройке политики авторизации можно использовать все типы словарей без ограничений.

При редактировании условий непосредственно в политике добавляется возможность использовать настроенное условие без сохранения его в Библиотеке. Для этого надо после настройки не сохраняя условие нажать кнопку `Использовать`.

Выбрать в выпадающем меню **Профили** необходимый профиль авторизации. Можно при необходимости добавить несколько профилей, их не конфликтующие настройки будут просуммированы.

К одной Политика авторизации можно привязать несколько Профилей авторизации.
Однако при обработке запроса будут учитываться только те, которые соответствуют текущему Профилю устройства.

Кнопкой ⚙ справа от политики можно добавить новое правило выше или ниже, либо удалить текущее.

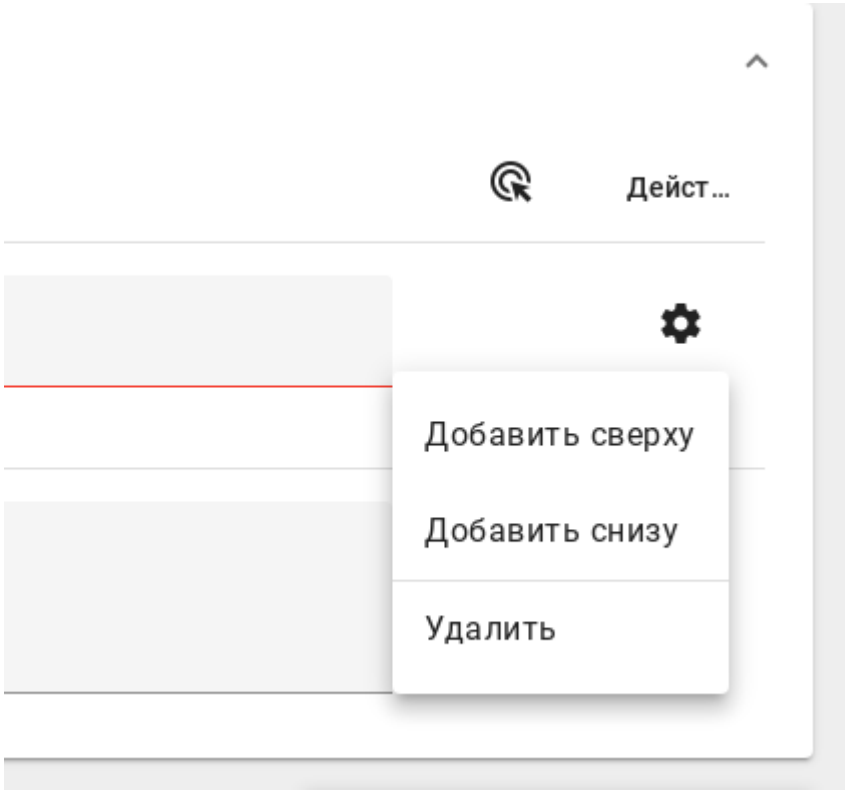

Рисунок 142. Политика авторизации. Выпадающие меню. Действия.

Также можно изменить статус политики аналогично статусам в наборах политик.

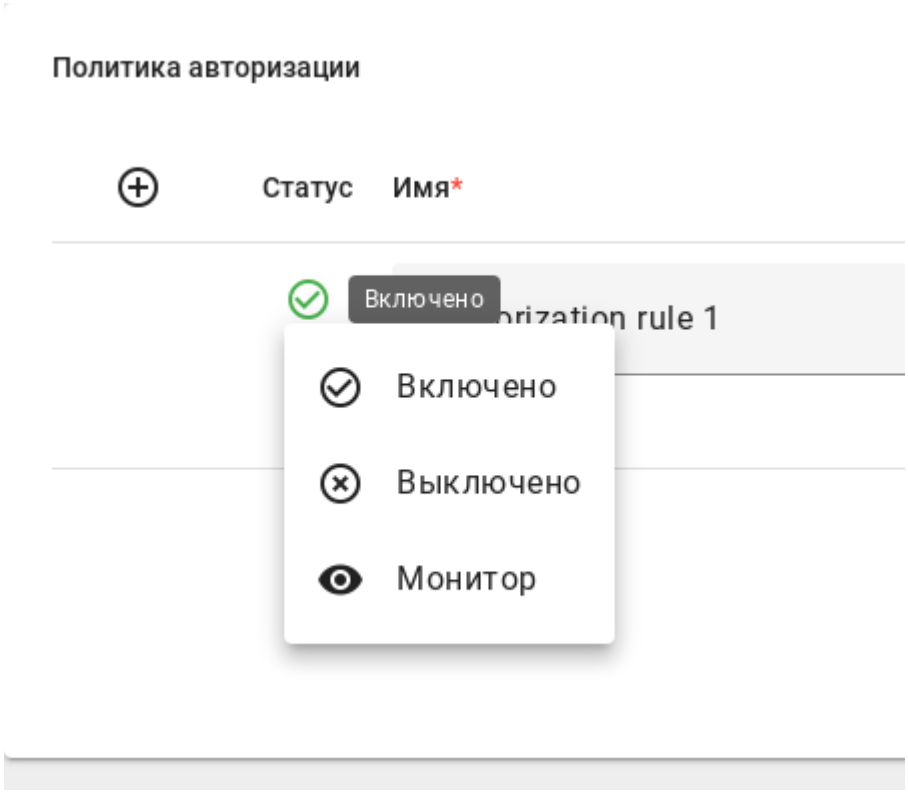

Рисунок 143. Политика авторизации. Изменение статуса политики.

Кнопка `Сохранить` станет доступна только после добавления хотя бы одной, полностью настроенной, политики аутентификации и политики авторизации.

Нажать кнопку `Сохранить`.

Редактирование правил политик

Редактирование политик выполняется путем нажатия кнопкой мыши на поле соответствующей настройки.

После этого необходимо нажать кнопку `Сохранить`.

Удаление правил политик

Удаление выполняется нажатием на кнопку ⚙ и выбором действия **Удалить**.

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

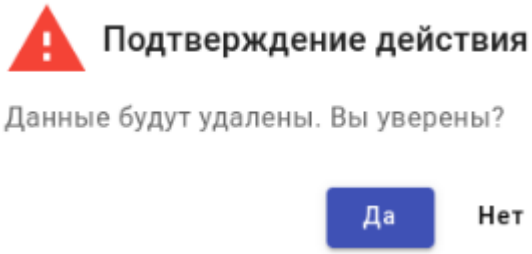

Рисунок 144. Модальный диалог подтверждения

Профилирование

Профилирование - процесс динамического обнаружения и классификации эндпоинтов на основе атрибутов, получаемых из различных источников (проб). В ходе профилирования собранные атрибуты сопоставляются с заранее созданными или заданными пользователем условиями, которые затем сопоставляются с профилями для их присвоения эндпоинту.

Меню содержит разделы:

- Условия профилирования - условия, определяющие как собранные атрибуты должны быть интерпретированы для классификации эндпоинта;
- Политики профилирования - набор правил, которые используются для автоматической классификации и управления доступом эндпоинтов на основе результатов профилирования;
- Логические профили - объединение определенных политик профилирования в логическую группу для более удобного использования в политиках доступа.

Условия профилирования

Описание

Условия профилирования являются основными элементами, используемыми в политиках профилирования. Они определяют, соответствует ли эндпоинт определенному признаку, на основе которого можно сделать вывод о его типе, модели, производителе, операционной системе и другим атрибутам.

В основе создания и обработки логического условия профилирования лежит алгебра логики. Результатом выполнения условия является "Истина" или "Ложь". Каждое условие профилирования может содержать только один атрибут.

Просмотр списка условий профилирования

На данной странице содержится таблица со списком всех условий профилирования.

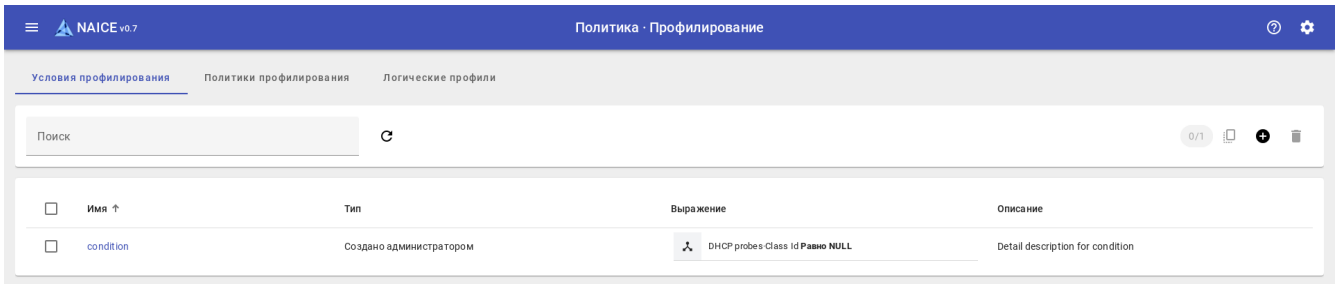

Рисунок 145. Таблица условий профилирования

Таблица содержит колонки:

- `Имя` - наименование условия профилирования.
- `Тип` - тип условия профилирования. Может быть "Системное" или "Создано администратором". Системные условия предустановлены и не могут быть удалены или изменены.
- `Выражение` - логическое условие, описывающее критерий по которому будет выполнено профилирование.
- `Описание` - произвольное описание условия профилирования.

Сортировка возможна только по полю "Имя" в прямом и обратном порядке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке.

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - Обновить данные таблицы.
- 0/1 - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
- - Чекбокс, который отвечает за копирование выбранного элемента. Становится активным, если выбран только один элемент в списке.

Добавление условия профилирования

Для добавления условия профилирования нажмите в правой верхней части поля над таблицей.

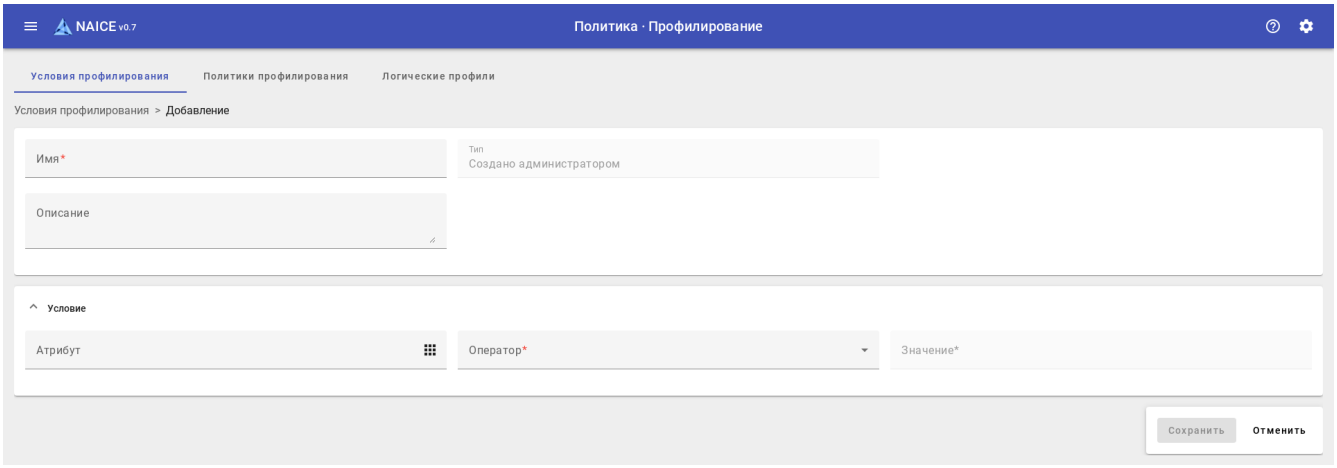

Рисунок 146. Форма добавления условия профилирования

В открывшейся странице представлены следующие параметры:

- `Имя` * - наименование условия профилирования. Максимальная длина - 100 символов.
- `Тип` - тип условия профилирования. Не может быть задано и всегда имеет значение "Создано администратором".
- `Описание` - произвольное описание условия профилирования. Максимальная длина - 200 символов.

Условие - блок, отвечающий за настройку условия профилирования.

- `Атрибут` * - по нажатию на кнопку слева в поле откроется словарь для добавления атрибута.
- `Оператор` * - выбранный оператор логического условия. Может принимать значения (в зависимости от типа значения атрибута):
  - "Начинается с" / "Не начинается с"
  - "Оканчивается на" / "Не оканчивается на"
  - "Равно" / "Не равно"
  - "Равно NULL" / "Не равно NULL"
  - "Содержит" / "Не содержит"
  - "Соответствует" (*полное* соответствие строки с учетом регистра)
- `Значение` * - значение, которые используются для сопоставления с атрибутом логического условия в соответствие с выбранным оператором. Для атрибута, предполагающего предопределенные значения, выбор значения производится из списка.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Меню выбора атрибута

Для выбора атрибута, который будет использоваться в условии, необходимо нажать - раскроется меню выбора атрибута.

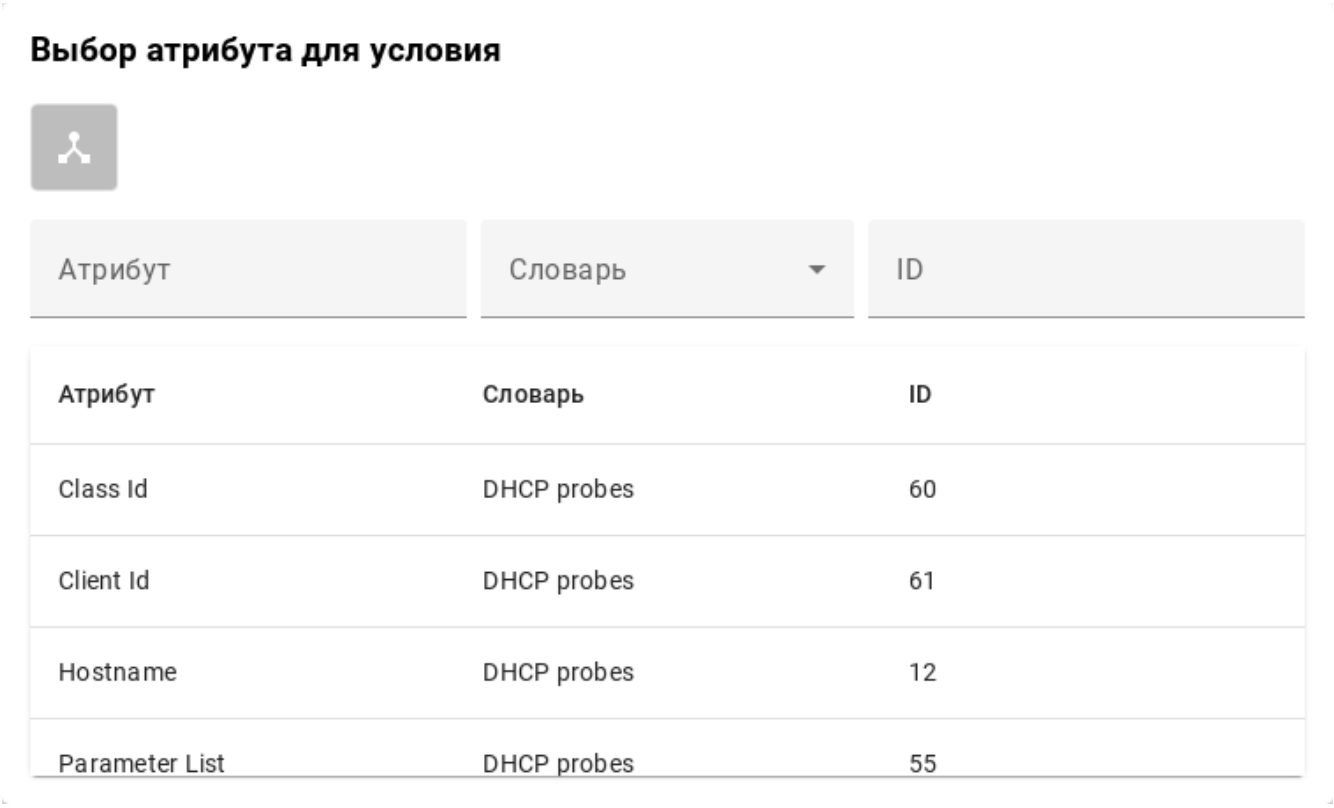

Рисунок 147. Меню выбора атрибута

Для выбора доступны только атрибуты словарей типа "PROFILING". Данный тип словарей обозначен иконкой .

Сверху находится список, позволяющий выполнить фильтрацию атрибутов:

- `Атрибут` - наименование атрибута.
- `Словарь` - наименование словаря, выполненное в форме выпадающего списка. Доступны для выбора словари "DHCP probes" и "MAC". Так же доступно для выбора "Не выбрано", если требуется отказаться от фильтрации.
- `ID` - идентификатор атрибута (числовое значение).

Редактирование условия профилирования

Для редактирования условия профилирования необходимо на странице со списком нажать на его имя.

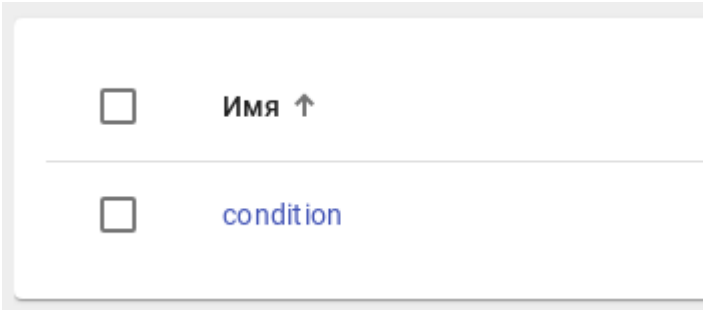

Рисунок 148. Гиперссылка на страницу редактирования условия

После этого откроется окно редактирования.

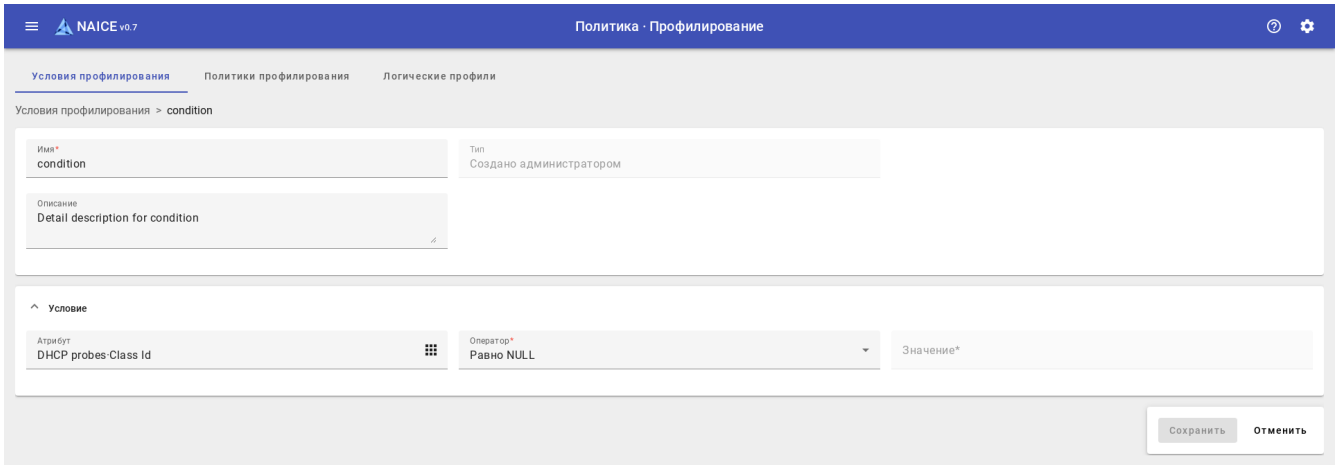

Рисунок 149. Форма редактирования условия профилирования

После редактирования нажать на кнопку "Сохранить". Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

Копирование условия профилирования

Новое условие профилирования можно создать на основе уже существующего.

Для этого выберите одно из существующих условий с помощью чекбокса и нажмите на . В открывшемся окне добавления условия все поля заполнены значениями из выбранного условия. По умолчанию к значению в поле `Имя` добавляется "_copy". Можно выбрать любое другое имя, которое еще не используется в системе.

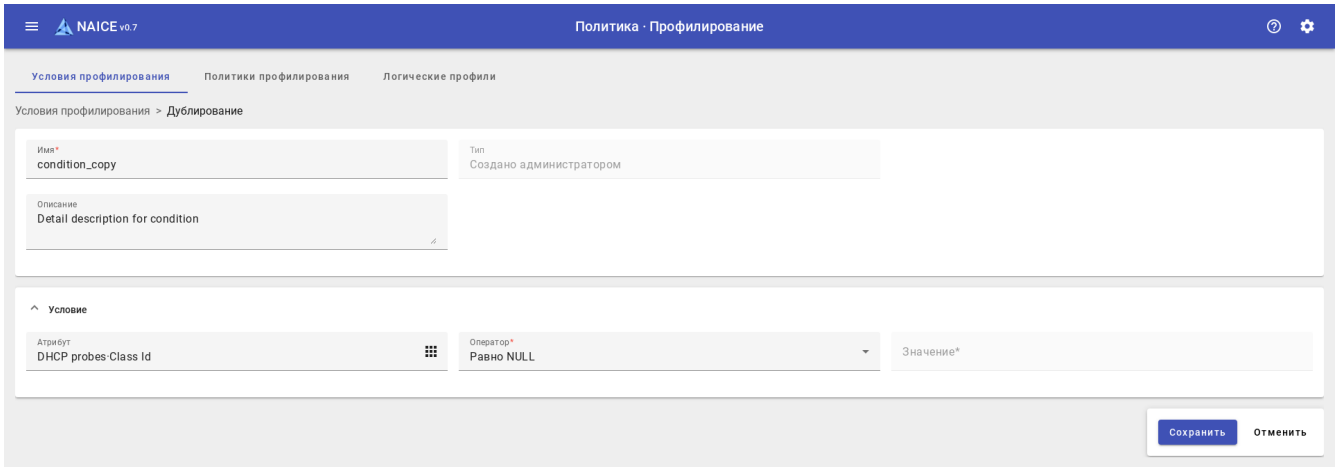

Рисунок 150. Форма копирования условия профилирования

После копирования условие не имеет никакой связи с исходным условием. Существуют и работают эти условия независимо друг от друга. Это всего лишь заполнение полей на момент добавления.

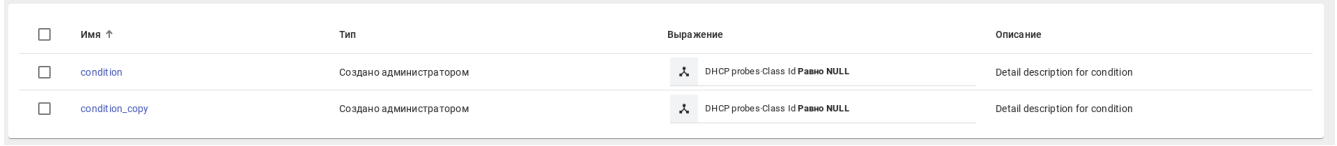

Рисунок 151. Таблица условий профилирования после копирования условия

Удаление условий профилирования

Для удаления в окне со списком надо выделить чекбокс слева от наименования условий профилирования, которые требуется удалить, и нажать кнопку вверху справа.

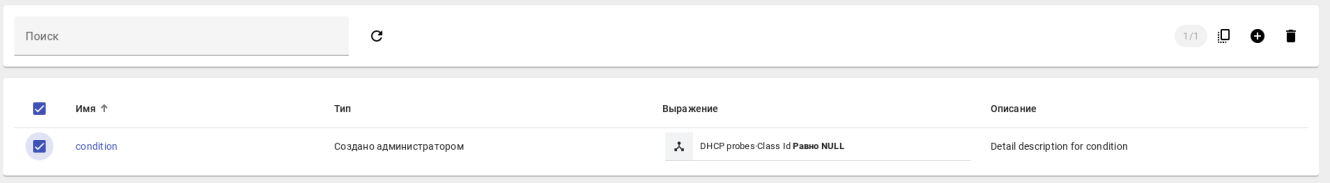

Рисунок 152. Выбор условий для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

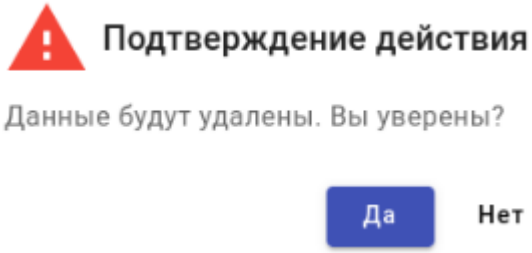

Рисунок 153. Модальный диалог подтверждения

Ограничения:

Нельзя удалить условие профилирования, которое уже назначено какой-либо политике профилирования.

Политики профилирования

Описание

Политики профилирования предназначены для динамической классификации новых и существующих эндпоинтов, подключенных к сети. Для классификации используются условия профилирования, на основании которых выполняется определение и назначение эндпоинту политики профилирования. Она может использоваться в условиях политик авторизации для предоставления доступа в соответствие с определенной политикой. Также на основании политики профилирования эндпоинт помещается в выбранную группу эндпоинтов.

Например, на основании условий профилирования можно определить эндпоинт как устройство определенного типа и производителя (например, IP-телефон Eltex), и настроить политику авторизации для выдачи этим устройствам определенных VLAN и ACL.

Процесс определения и назначения эндпоинту политики профилирования в соответствии с определенными для него в политике условиями называется "Профилирование эндпоинта".

Для эндпоинтов, имеющих вручную назначенные "Политику профилирования" или "Группу эндпоинта", эти параметры не могут быть измены по результатам выполнения профилирования.

Просмотр политик профилирования

На данной странице доступен просмотр и управление политиками профилирования. Политики профилирования имеют иерархическую структуру, которая необходима для группировки эндпоинтов.

В левой части окна содержится дерево политик профилирования, в котором осуществляется выбор политики для просмотра или редактирования.

В правой части окна отображается форма создания/редактирования политики профилирования. Если в дереве выбран элемент `Все политики`, то в правой части окна отображается таблица со списком всех политик профилирования.

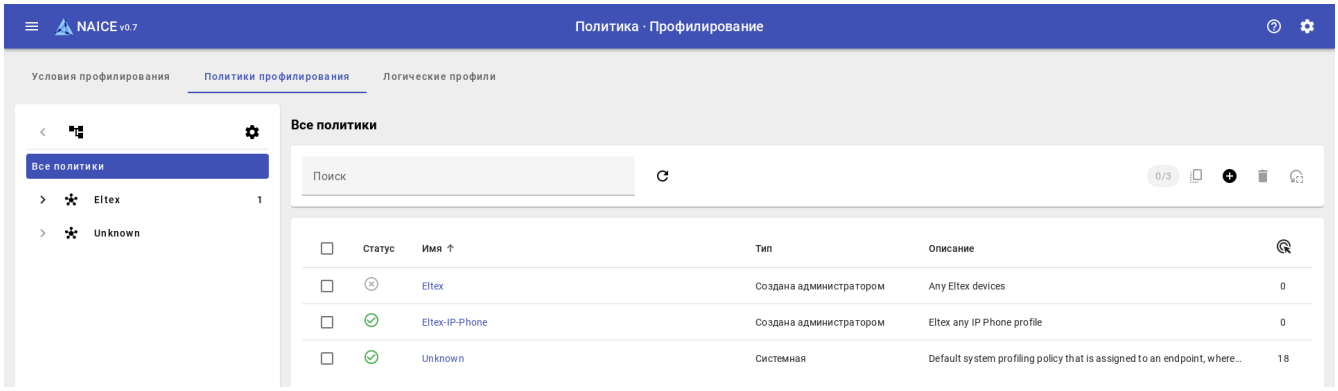

Рисунок 154. Просмотр политик профилирования.

Просмотр дерева или списка политик профилирования

Дерево политик профилирования расположено в левой части и отображает список политик профилирования в виде древовидной структуры или в виде списка дочерних политики профилирования выбранного узла - способ отображения можно переключать, по умолчанию используется отображение в виде древовидной структуры.

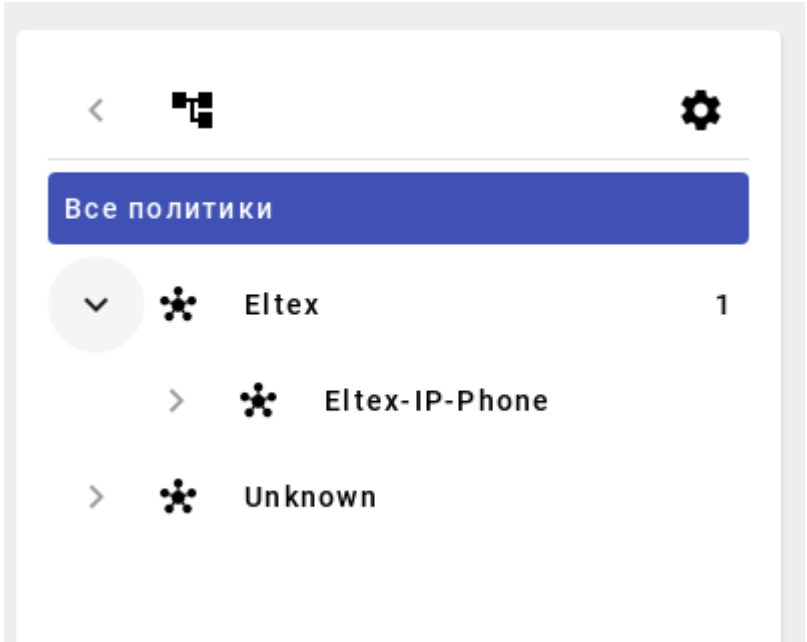

Рисунок 155. Дерево политик профилирования.

Содержит следующие элементы управления:

- - включен режим отображения в виде древовидной структуры политик профилирования (для переключения режима на противоположный необходимо нажать на иконку).
- - включен режим отображения в виде списка дочерних политик профилирования (для переключения режима на противоположный необходимо нажать на иконку).

- добавление/дублирование/удаление политики. Выбор доступных действий зависит от выбранного элемента в дереве политик.

- - переход на уровень выше от текущей политики (активно только в режиме списка дочерних политик, при нахождении в дочерней политике).
- - в режиме древовидной структуры отображается слева от наименования политик профилирования, если список закрыт. Неактивна, если нет дочерних элементов. В режиме списка отображается справа наименования политик профилирования, имеющих дочерние элементы.
- - в режиме древовидной структуры отображается слева от наименования политик профилирования имеющих дочерние элементы, если список раскрыт.
- - элемент для обозначения политики профилирования.

`Все политики` - заголовок списка политик. При выборе данного элемента в правой части окна будет отображаться "плоский" список всех политик профилирования. Выбирается по умолчанию при переходе на страницу политик профилирования.

`Unknown` - системная политика профилирования, которая используется для профилирования эндпоинтов, не попавших под другие политики профилирования. Не может быть отредактирована. Так же для неё нельзя создать дочерние политики.

Просмотр списка политик профилирования

Список всех политик профилирования отображается в правой части страницы в виде таблицы, если в дереве политик профилирования выбран элемент `Все политики`.

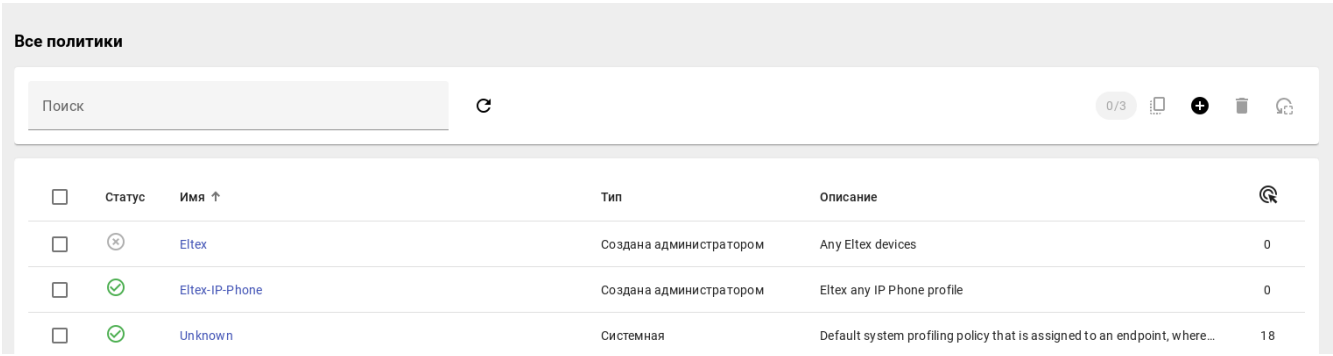

Рисунок 156. Таблица со списком всех политик профилирования.

Таблица содержит колонки:

- `Статус` - текущий статус политики профилирования: может принимать значения (включено) или (выключено).
- `Имя` - наименование политики профилирования.
- `Тип` - тип политики профилирования. Возможны значения "Создана администратором" или "Системная".
- `Описание` - описание политики профилирования.
- - количество проверок на соответствие эндпоинта политике профилирования.

Сортировка возможна по полям "Статус" и "Имя" в прямом и обратном порядке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке по полю "Имя".

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
-  - Обновить данные таблицы.
- 0/1 - Счетчик выбранных чекбоксом элементов / общего количества элементов.
-  - Добавить новый элемент.
-  - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
-  - Изменить текущий порядок сортировки.
-  - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).
-  - Копировать выбранный элемента. Становится активным, если выбран только один элемент в списке.
-  - Сбросить счётчик попаданий в политику профилирования. Становится активным, если выбран хотя бы один элемент в списке и количество срабатываний политики больше 0.

Порядок политик профилирования крайне важен!
Обращение к политикам профилирования для проверки соответствия эндпоинта политике профилирования происходит сверху вниз списка.

Добавление политики профилирования

Добавление политики профилирования возможно двумя способами:

- через дерево политик профилирования: нажать иконку  над деревом и выбрать "Добавить корневую политику", если выбран элемент "Все политики", или "Добавить дочернюю политику" если выбрана политика профилирования.

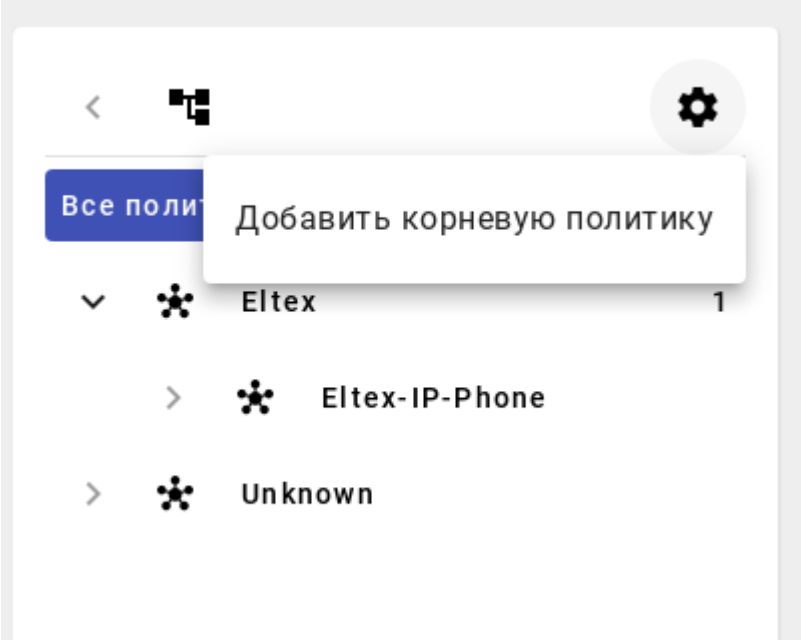

Рисунок 157. Добавление политики профилирования. Действия.

- через таблицу политик профилирования: нажать иконку ⊕ в правой верхней части поля над таблицей.

> ⚠ Для системной политики профилирования "Unknown" добавление дочерних политик запрещено.

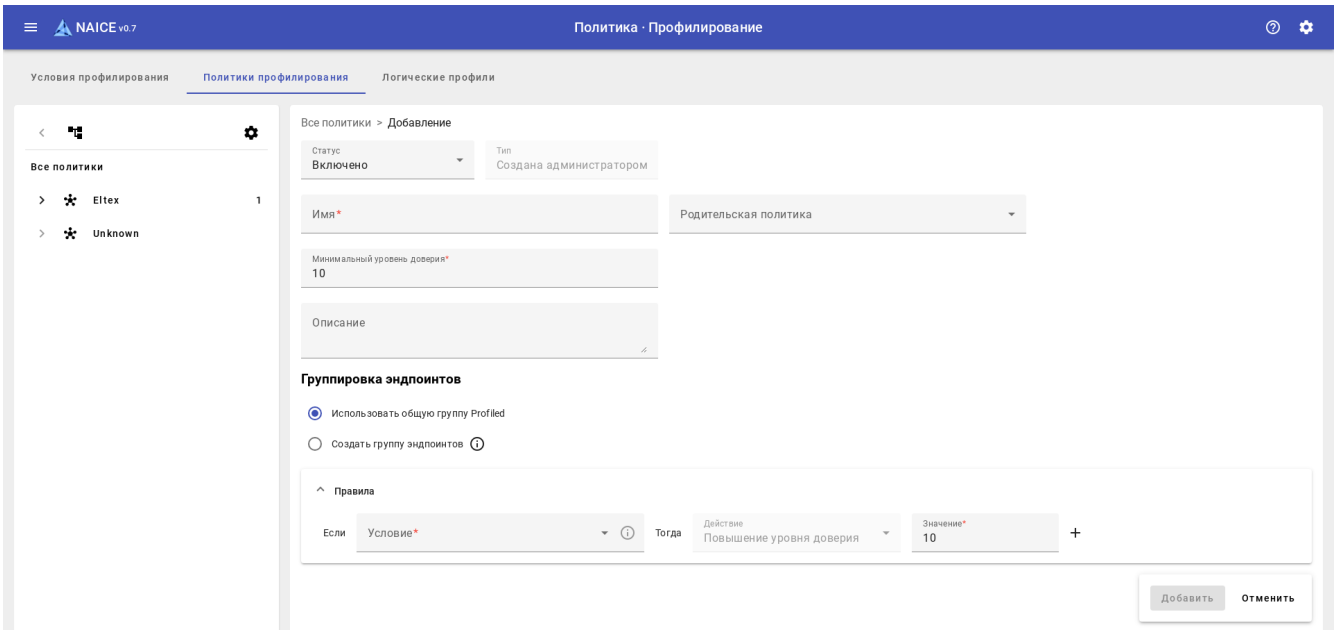

Рисунок 158. Добавление политики профилирования.

В результате в правой части страницы откроется раздел добавления политик, содержащий следующие параметры:

- `Статус` - статус политик профилирования. Может принимать значения "Включено" и "Выключено". По умолчанию значение "Включено".
- `Тип` - тип политики профилирования. Все вручную созданные политики профилирования имеют значение "Создана администратором", изменить его нельзя.

`Имя` * - наименование политики профилирования. Максимальная длина - 100 символов.

- `Родительская политика` - родительская политика профилирования. Можно выбрать родительскую политику профилирования в выпадающем списке или не выбирать ничего для создания корневой политики профилирования. При создании политики профилирования из дерева политик путем выбора меню "Добавить дочернюю политику" будет автоматически подставлена выбранная в дереве политика профилирования. При необходимости можно выбрать и другую `Родительскую политику`.
- `Минимальный уровень доверия` * - минимальное количество баллов, которое нужно получить в правилах, чтобы политика считалась подходящей для назначения эндпоинту. Не может быть больше, чем сумма значений всех уровней доверия, настроенных в разделе "Правила". Может принимать значения от 1 до 65535.
- `Описание` - произвольное описание условия политики профилирования. Максимальная длина - 200 символов.
- **Группировка эндпоинтов** - раздел, определяющий принцип группировки эндпоинтов.
  Доступен выбор следующих значений:
  - `Использовать общую группу Profiled` - данный выбор доступен и отображается только для корневой политики профилирования. Эндпоинты, классифицированные как принадлежащие данной политике профилирования, будут помещены в системную группу эндпоинтов "Profiled".
  - `Использовать группу эндпоинтов родительской политики` - данный выбор доступен и отображается только для дочерней политики профилирования. Эндпоинты, классифицированные как принадлежащие данной политике профилирования, будут помещены в указанную в родительской политике группу. Если для родительских политик не указаны группы - эндпоинты будут помещены в группу "Profiled".
  - `Создать группу эндпоинтов` - автоматически создать группу эндпоинтов с использованием наименования политики профилирования. Эндпоинты, классифицированные как принадлежащие данной политике профилирования, будут помещены в эту группу.
- **Правила** - раздел правил, отвечающий за настройку классификации эндпоинтов с использованием условий профилирования. Содержит параметры:
  - `Условие` * - меню выбора условия профилирования.
  - `Значение` * - количество баллов, которое будет назначено эндпоинту в случае совпадения условия профилирования.
  - `+` - иконка расположена справа от условия профилирования. При нажатии данной иконки ниже будет добавлено новое условие профилирования.

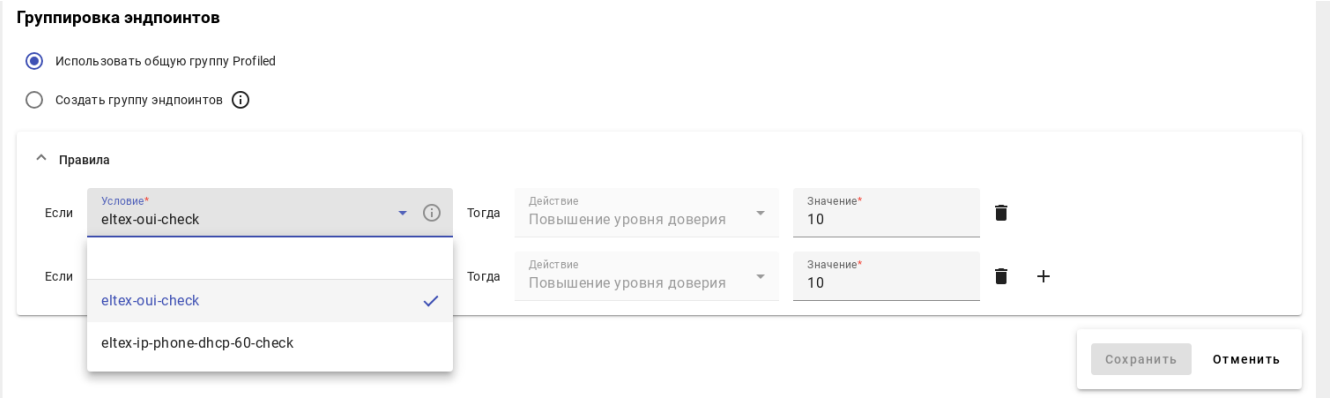

Рисунок 159. Добавление правил в политику профилирования.

Параметры, отмеченные звездочкой *, обязательны для заполнения.

Политика профилирования должна содержать минимум одно правило.

Для одной политики профилирования может быть добавлено несколько правил.

Запрещено добавлять одно и тоже условие профилирования в политику несколько раз.

Для добавления политики нажмите кнопку `Добавить`. Кнопка станет активной после заполнения всех необходимых полей политики профилирования.

Принцип проверки соответствия эндпоинта политике профилирования

При профилировании эндпоинта выполняются следующие действия:

- Для первого условия профилирования, указанного в правилах политики профилирования, выполняется проверка на соответствие эндпоинта указанному условию:
  - Если эндпоинт соответствует условию профилированию, то к текущему уровню доверия прибавляется соответствующее правилу значение;
  - Если эндпоинт не соответствует условию, то уровень доверия остается неизменным.
- Действие повторяется для каждого правила в политике.
- Когда эндпоинт был проверен на соответствие всем правилам политики, суммарный уровень доверия сравнивается с минимальным уровнем доверия политики:
  - Если суммарный уровень доверия равен или больше минимального, то эндпоинт соответствует политике профилирования;
  - Если суммарный уровень доверия меньше минимального, то эндпоинт не соответствует политике профилирования.
- Так как политики вложены друг в друга, работает обход дерева вглубь:
  - Обнаруживается первая совпавшая корневая политика.
  - Если у корневой политики есть дочерние, то происходит их обход на предмет совпадения.

Возвращается самая "глубокая" политика из дерева.

- Как только одна из политик текущего уровня подошла, обход этого уровня прекращается, поиск продолжается только среди дочерних политик.

Редактирование политики профилирования

Редактирование политики профилирования возможно двумя способами:

- Выбрать политику профилирования в дереве политик слева и нажать на нее - в правой части откроется форма редактирования.
- В списке всех политик в колонке "Имя" нажать на наименование политики - произойдет переход на форму редактирования данной политики.

После добавления политики профилирования внутри ее детальной информации добавляется поле `Количество срабатываний политики` и элемент управления `Сбросить счётчик`.

- `Количество срабатываний политики` - количество проверок на соответствие эндпоинта политике профилирования.
-  - сбросить счётчик попаданий в политику профилирования. Становится активным, если количество срабатываний политики больше 0.

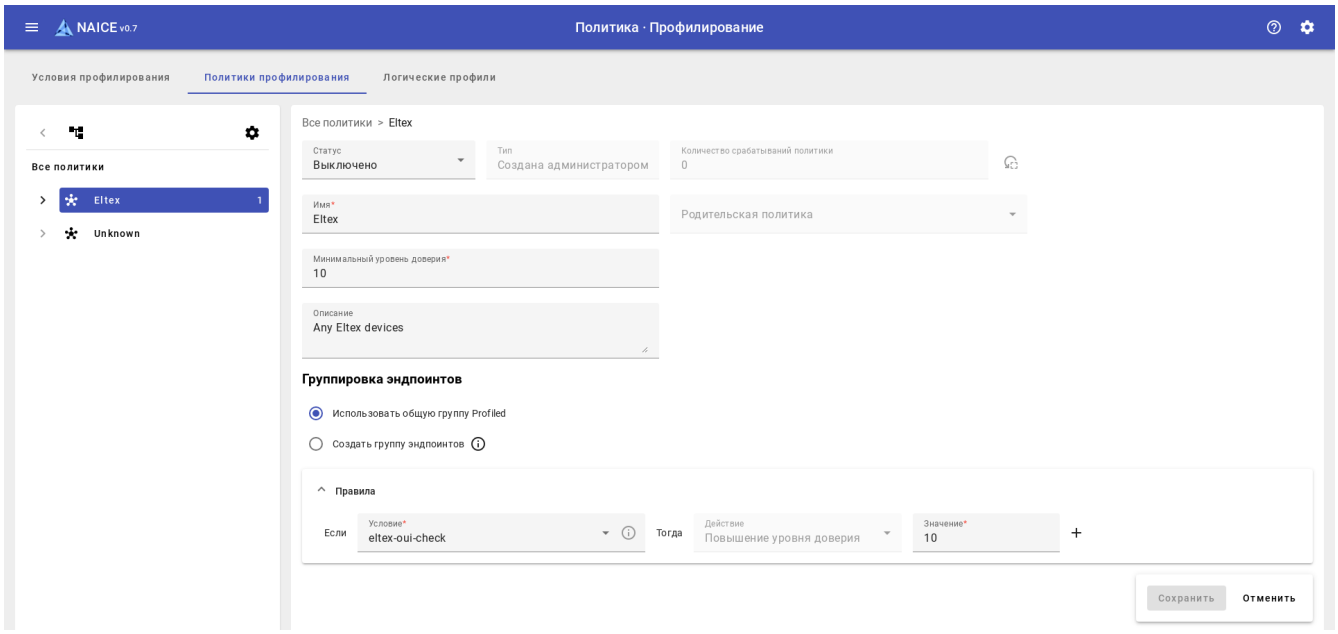

Рисунок 160. Редактирование политики профилирования.

Редактирование системной политики профилирования "Unknown" недоступно.

После редактирования нажать на кнопку "Сохранить". Кнопка остается неактивной, пока не будет изменено хотя бы одно поле.

Копирование политик профилирования

Новая политика профилирования может быть создана на основе существующей. Это можно сделать двумя способами:

В дереве политик выбрать одну из существующих политик профилирования и нажать иконку . В списке доступных действий выбрать меню "Дублировать политику".

- В списке всех политик выбрать одну из существующих политик профилирования и нажать иконку .

> Действие недоступно, если выбрано более одной политики или "Unknown".

Откроется форма, аналогичная форме добавления политик, где все поля будут заполнены значениями из выбранной политики. По умолчанию к значению в поле `Имя` добавляется "_copy". Можно выбрать любое другое имя, которое еще не используется в системе.

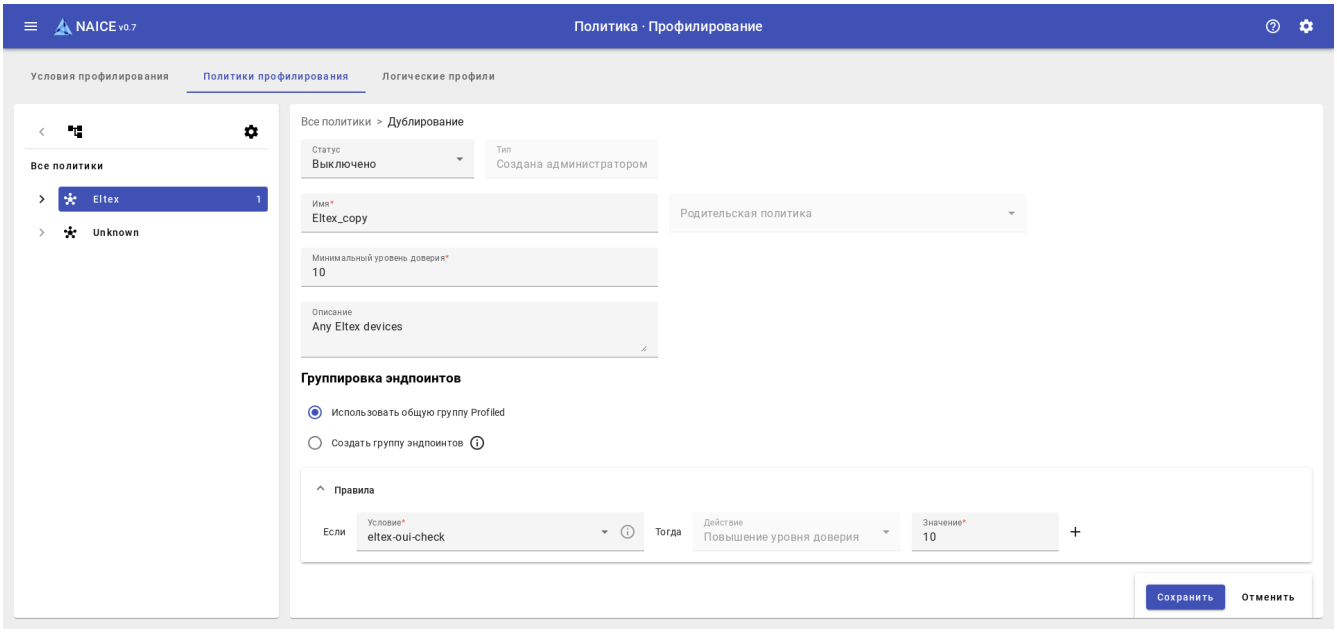

Рисунок 161. Дублирование политики профилирования.

После копирования политика профилирования не имеет никакой связи с исходной. Существуют и работают эти политики профилирования независимо друг от друга - исходная используется для заполнения полей новой на момент добавления.

Удаление политик профилирования

Удаление политик профилирования возможно двумя способами:

- через дерево политик профилирования: необходимо выделить политику и нажать на иконку . В списке доступных действий выбрать меню "Удалить политику". В дереве политик можно выполнять удаление только по одной политике профилирования.
- через таблицу политик профилирования: необходимо выделить чекбокс слева от наименования политик профилирования, которые требуется удалить, и нажать кнопку вверху справа. Можно выделить несколько политик профилирования для удаления.

> Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

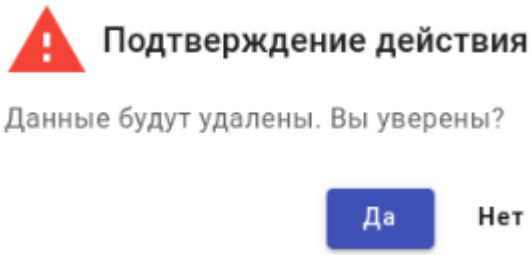

Рисунок 162. Модальный диалог подтверждения

Ограничения:

- Нельзя удалить политику профилирования, которая используется в каком-либо логическом профиле.
- Нельзя удалить политику профилирования, которая используется в каком-либо логическом условии или условии политики авторизации.
- Нельзя удалить системную политику профилирования "Unknown".

Логические профили

Описание

Логические профили предназначены для объединения определенных политик профилирования в логическую группу, которая может быть использована в настройках политик авторизации, что позволяет упростить структуру и уменьшить количество правил в политике. Например, логический профиль "Принтеры" может объединять в себе политики профилирования "Принтеры HP", "Принтеры Xerox", и "Принтеры Canon". Одна политика профилирования может быть членом нескольких различных логических профилей.

Просмотр логических профилей

На данной странице содержится таблица со списком всех логических профилей.

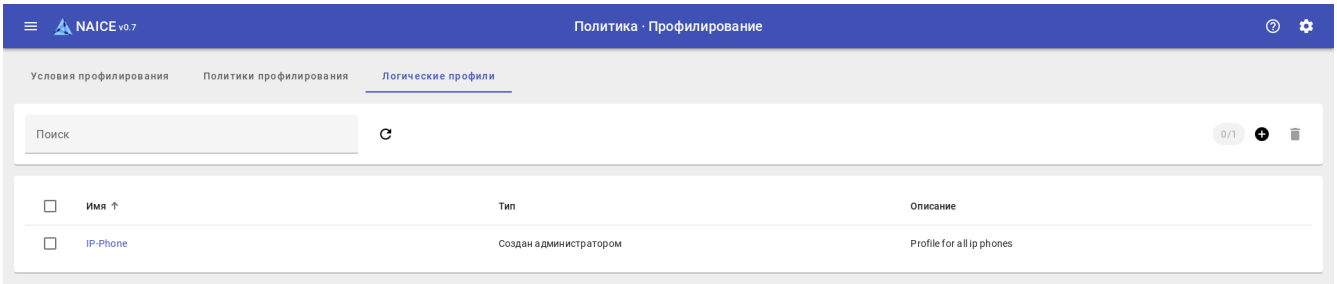

Рисунок 163. Таблица логических профилей

Таблица содержит колонки:

- `Имя` - наименование логического профиля.
- `Тип` - тип логического профиля. Может быть "Системное" или "Создано администратором". Системные условия предустановлены и не могут быть удалены или изменены.
- `Описание` - произвольное описание логического профиля.

Сортировка возможна только по полю "Имя" в прямом и обратном порядке. По умолчанию сортировка выполняется в прямом (алфавитном) порядке.

Элементы управления:

- `Поиск` - Выполняет регистронезависимую фильтрацию по всем колонкам: отображаются только записи, удовлетворяющие условию фильтрации.
- - Обновить данные таблицы.
- `0/1` - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- - Добавить новый элемент.
- - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- - Изменить текущий порядок сортировки.
- - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Добавление логического профиля

Для добавления логического профиля нажмите в правой верхней части поля над таблицей.

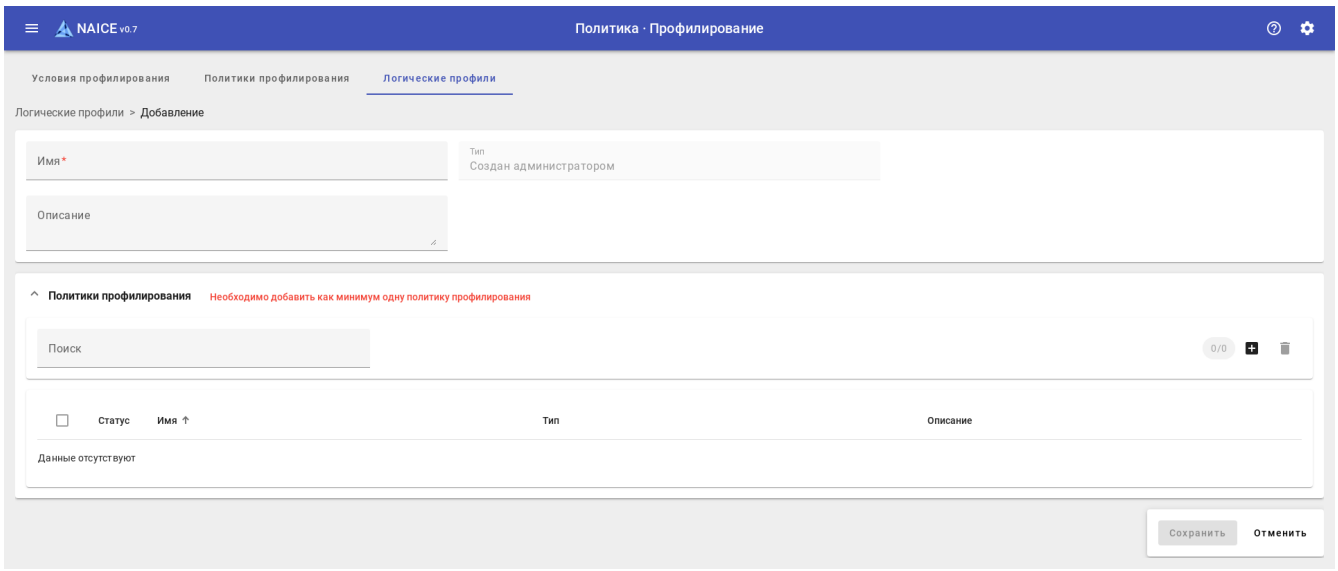

Рисунок 164. Форма добавления логического профиля

В открывшейся странице представлены следующие параметры:

- `Имя` * - наименование условия профилирования. Максимальная длина - 100 символов.
- `Тип` - тип условия профилирования. Не может быть задано и всегда имеет значение "Создано администратором".
- `Описание` - произвольное описание условия профилирования. Максимальная длина - 200 символов.

Политика профилирования - блок отвечающий за добавление/удаление политик профилирования. Для удобства конфигурирования ниже в табличной форме отображается список назначенных политик профилирования. Таблица содержит колонки:

-

`Поиск` - Выполняет регистронезависимую фильтрацию по колонкам `Имя` и `Описание`: отображаются только записи, удовлетворяющие условию фильтрации.

- 0/1 - Счетчик выбранных чекбоксом элементов / общего количества элементов.
- ⊞ - Добавить новый элемент.
- 🗑 - Удалить выбранные элементы (неактивно, пока не выбран хоть один элемент).
- ↑ - Изменить текущий порядок сортировки.
- ☐ - Чекбокс, который отвечает за выбор элементов для выполнения дальнейших действий (например, удаления).

Параметры, отмеченные звездочкой *, обязательны для заполнения.

После добавления необходимых политик логический профиль необходимо сохранить.

⚠ Логический профиль должен содержать хотя бы одну политику профилирования. Кнопка "Сохранить" будет неактивна, пока список политик профилирования будет пустой, или не заполнены другие обязательные параметры.

Добавление политик профилирования в логический профиль

Для добавления политик профилирования в логический профиль требуется нажать на иконку ⊞ справа вверху над таблицей раздела **Политики профилирования**.

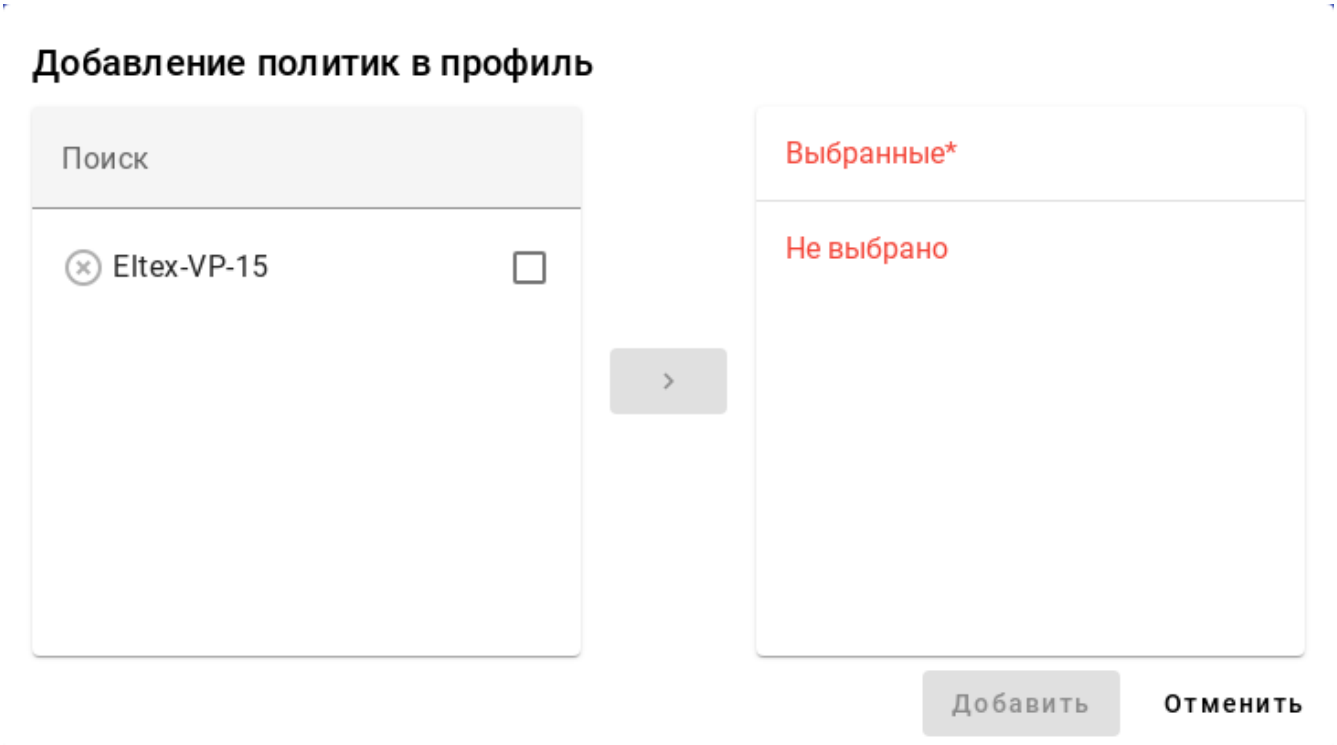

Рисунок 165. Модальный диалог добавления политик профилирования

В левой части открывшегося модальном окне выбрать чекбокс ☐ для политик профилирования, которые необходимо добавить в профиль. Для поиска нужной политики можно ввести ее имя в строке `Поиск`.

После выбора нужных политик нажать иконку ›. Отмеченные чекбоксом политики профилирования переместятся в правую часть модального окна. При необходимости политики профилирования в правой части модального окна можно удалить, нажав на иконку 🗑 справа от наименования. Когда все нужные политики выбраны, нажать кнопку `Добавить`, чтобы применить изменения.

Добавленные политики профилирования начнут отображаться в таблице раздела **Политики профилирования**. Порядок следования политик никакого значения не имеет. Все они проверяются независимо друг от друга.

Системную политику профилирования `Unknown` нельзя использовать в логическом профиле.

Редактирование логического профиля

Для редактирования логического профиля необходимо на странице со списком нажать на его имя.

После этого откроется окно редактирования.

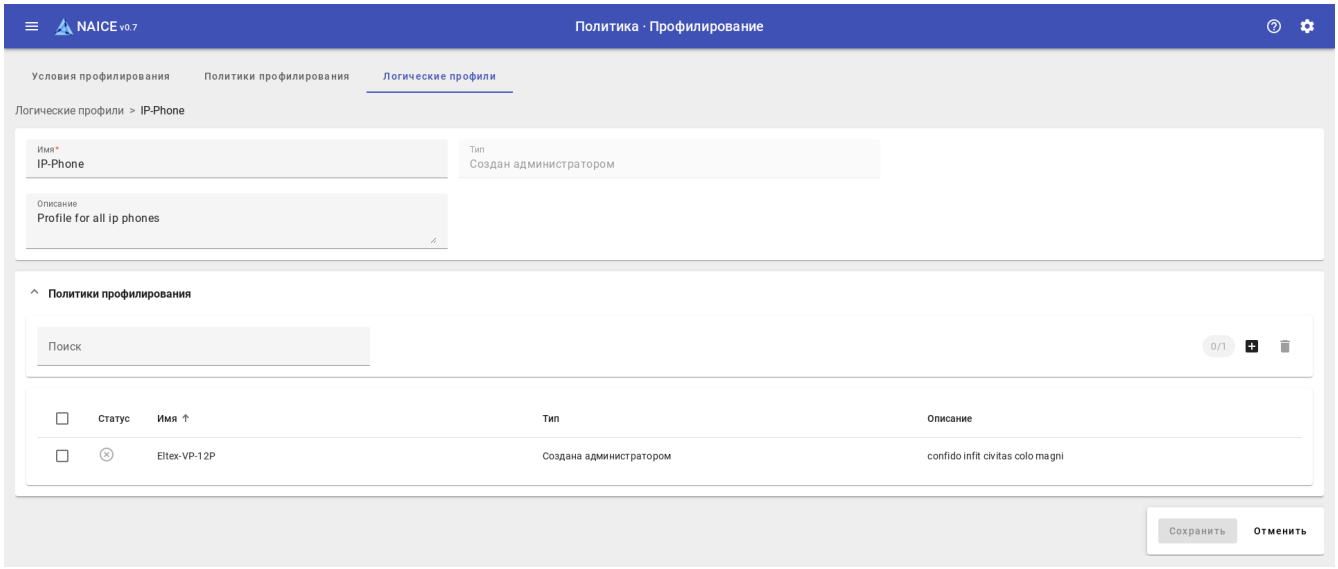

Рисунок 166. Форма редактирования логического профиля

После редактирования нажать на кнопку "Сохранить". Кнопка остается неактивной, пока не будет изменено хотя бы одно поле или изменен набор политик профилирования.

Удаление логического профиля

Для удаления в окне со списком необходимо выделить чекбокс слева от наименования логических профилей, которые требуется удалить, и нажать кнопку 🗑 вверху справа.

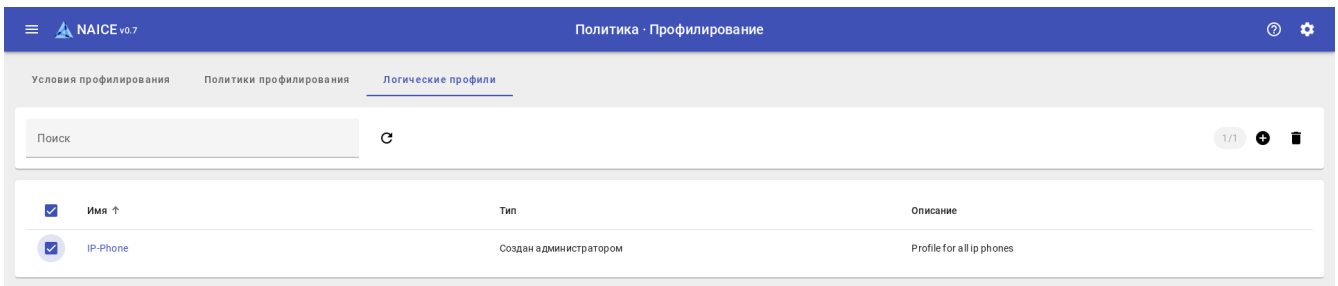

Рисунок 167. Выбор логических профилей для удаления

Удаление требует Подтверждения действия, для чего откроется модальный диалог. После явного подтверждения выбранные элементы будут удалены.

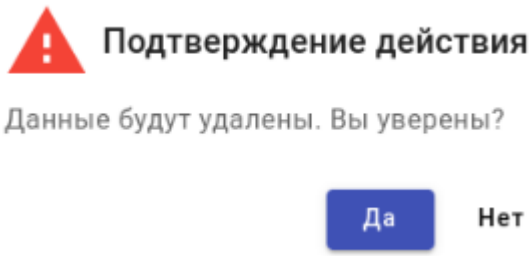

Рисунок 168. Модальный диалог подтверждения

Ограничения:

- Нельзя удалить логический профиль, который используется в какой-либо политике авторизации.

Мониторинг

RADIUS

Пользовательские сессии

Описание

Мониторинг пользовательских сессий позволяет просматривать подключения пользователей за определенный период времени, производить фильтрацию для поиска необходимых записей и анализировать детальную информацию об определенной сессии.

Просмотр списка пользовательских сессий

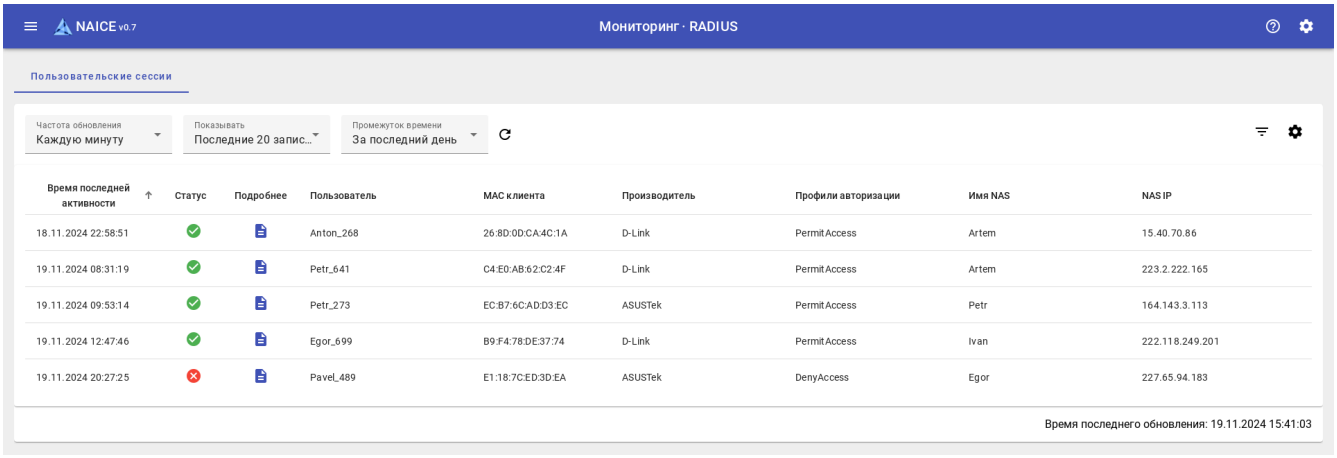

Рисунок 169. Таблица со списком сессий пользователей

Таблица по умолчанию содержит колонки:

- `Время последней активности` - время, когда в рамках данной сессии был получен последний RADIUS-пакет.
- `Статус` - статус сессии, может принимать значения:
  -  - CREATED - сессия была создана, однако по какой-то причине авторизация не была завершена;
  -  - ACCEPTED - авторизация была пройдена успешно;
  -  - REJECTED - авторизация была отклонена;
  -  - EXPIRED - сессия была завершена по истечении определенного времени.
- `Подробнее`  - ссылка для открытия детальной страницы сессии, на которой содержится подробная информация о сессии.
- `Пользователь` - логин пользователя, с которым проходила авторизация.
- `MAC клиента` - идентификатор авторизуемого клиента, который указан в RADIUS-атрибуте Calling-Station-Id.
- `Производитель` - имя организации, которое произвело устройство, проходившее авторизацию.
-

`Профили авторизации` - список профилей авторизации, которые были применены по результатам авторизации клиента.

- `Имя NAS` - имя NAS-устройства в системе.
- `NAS IP` - IP-адрес NAS-устройства, получаемый из RADIUS-атрибута NAS-IP-Address.
- `ID сессии` - идентификатор сессии из RADIUS-атрибута Acct-Session-Id.

Также доступны дополнительные колонки, настраиваемые в ⚙ в шапке таблицы:

- `Политика аутентификации` - название правила политики аутентификации, которое было применено в рамках данной сессии;
- `Политика авторизации` - название правила политики авторизации, которое было применено в рамках данной сессии;
- `Причина ошибки подключения`.
- `Тип подключения` - тип подключения, который был определен исходя из настроек профиля сетевого устройства.
- `Протокол аутентификации` - протокол, по которому проходила авторизация (например, PAP).

Элементы управления:

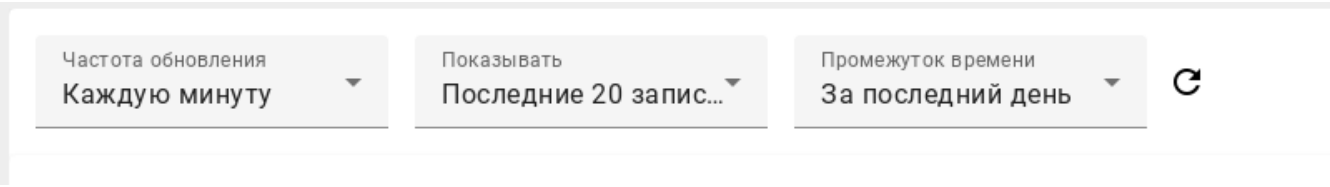

Рисунок 170. Настройки отображения активности пользователей

- `Частота обновления` - настройка частоты автоматического перечитывания пользовательских сессий.
- `Показывать` - настройка количества записей для отображения в таблице.
- `Промежуток времени` - выбор временного периода, в который происходила активность по пользовательским сессиям для отображения.
- ↻ - обновить данные таблицы вручную.
- ⚌ - открыть окно настройки фильтрации.
- ⚙ - открыть окно настройки отображаемых колонок таблицы.

Фильтрация настраивается в следующем окне:

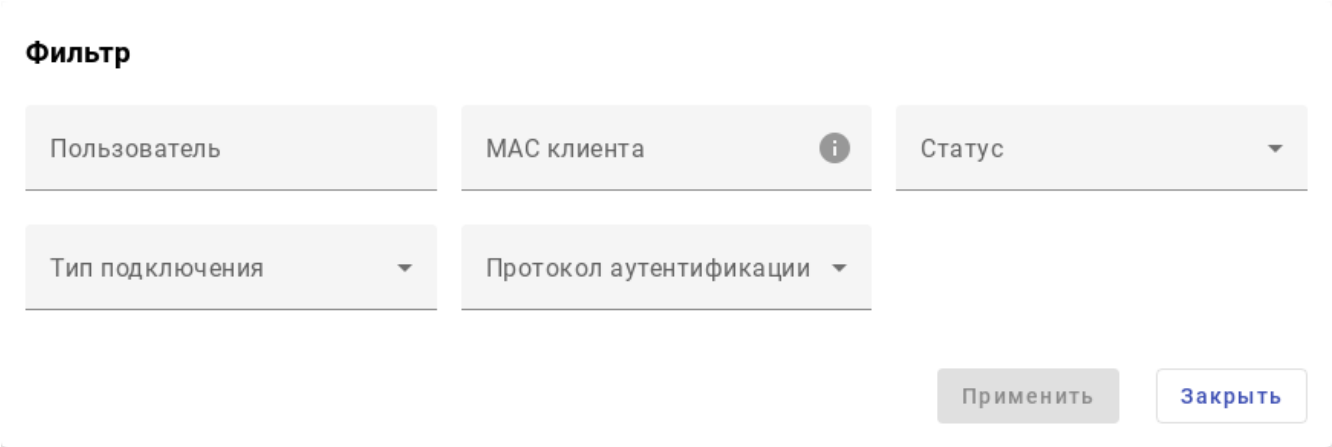

Рисунок 171. Окно настройки фильтрации записей

Фильтрация записей доступна по параметрам "MAC клиента", "Пользователь", "Статус", "Тип подключения" и "Протокол аутентификации".

В поле ввода MAC-адреса клиента доступен ввод только цифр 16-ичной системы счисления. Разделители октетов (двоеточия) вводятся автоматически.

Доступен поиск по частичному совпадению байтового представления.

Для поиска по части MAC-адреса необходимо, чтобы все доступные для поиска октеты адреса были указаны полностью.
Например, поиск по запросу "AA:BB:CC" возможен, по запросу "A:BB:C" - нет.

Кнопка "**Сбросить все**" предназначена для сброса настроенных параметров поиска.

В настройках таблицы  можно сменить состав отображаемых колонок.

Кнопка  выбирает или снимает выбор всех колонок для отображения.

Кнопка  предназначена для сброса настроенных колонок к состоянию по умолчанию (неактивно, пока состоянию по умолчанию не изменено).

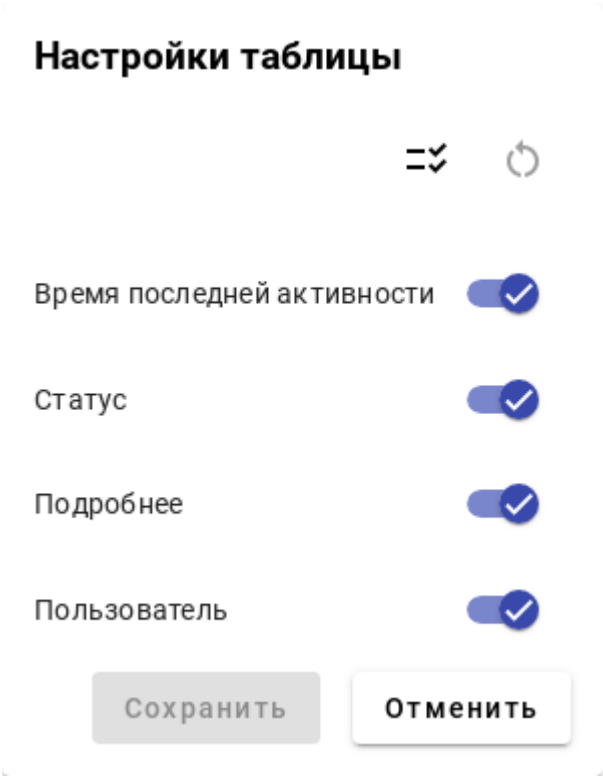

Рисунок 172. Окно настройки отображаемых колонок в таблице

Просмотр детальной информации о сессии

Для просмотра детальной информации о сессии из таблицы со всеми сессиями необходимо кликнуть на в колонке "Подробнее" для выбранной сессии.

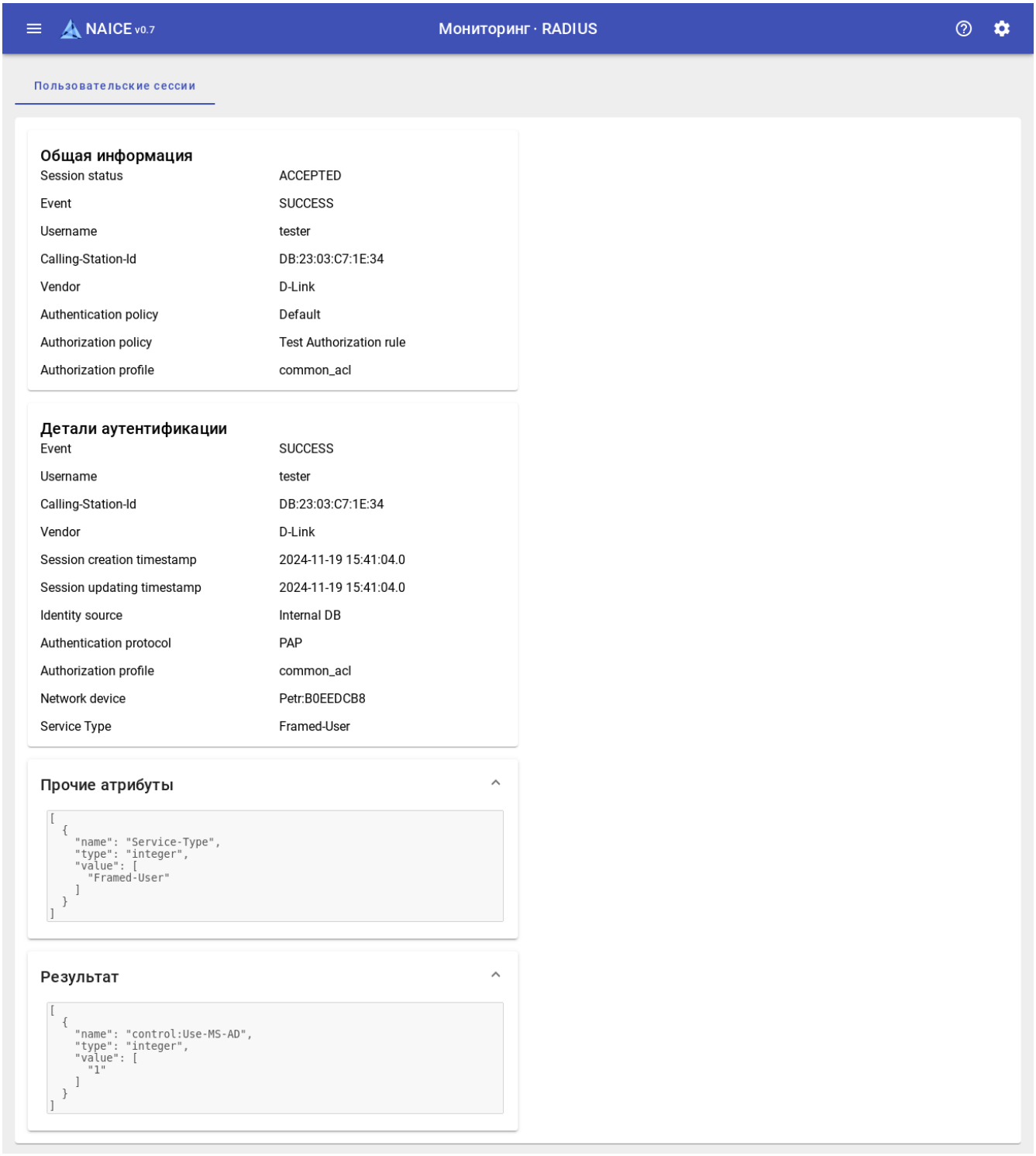

Рисунок 173. Детальная информация о сессии

Информация на странице разделена на 4 блока:

- `Общая информация` - краткая и наиболее важная информация о сессии;
- `Детали аутентификации` - детальная информация, которая может быть полезная для отладки;
- `Прочие атрибуты` - содержание пакета, полученного NAICE от RADIUS-сервера;
- `Результат` - список атрибутов, которыми был обогащен ответ клиенту в результате авторизации (например, атрибуты для выдачи VLAN или ACL). Если выдача дополнительных атрибутов не настроена в профиле авторизации, то список будет пуст.

Лицензирование

Описание

Лицензирование NAICE обеспечивается с помощью сервера лицензий **Eltex License Manager** (далее - **ELM**), осуществляющего функцию лицензирования программных и аппаратных продуктов компании «Элтекс». Для лицензирования может использоваться сервер ELM компании «Элтекс» (далее - Online ELM) или сервер ELM, установленный на стороне клиента (далее - Offline ELM). В обоих случаях адрес ELM сервера указывается при установке NAICE и на момент активации лицензии он должен быть доступен.

При приобретении доступа к продукту с определенным уровнем лицензирования генерируется *файл активации лицензии*, уникальный для каждого экземпляра NAICE. Для разблокировки NAICE данный файл необходимо загрузить в систему при первом входе в нее.

После успешной загрузки файла активации будет предоставлен доступ к функционалу продукта, соответствующий уровню лицензирования.

Уровни лицензии и лицензируемый функционал

В текущей версии реализован единственный уровень лицензирования **BASIC**. На этом уровне предоставляется доступ к основной услуге - авторизации эндпоинтов. Лицензируемым параметром является **количество успешно авторизованных уникальных конечных устройств за сутки**. Данное количество согласовывается на этапе приобретения лицензии и зависит от числа клиентских устройств в сети.

Пример расчета количества конечных устройств в сети

В организации "А" работает 1000 сотрудников, каждый из которых имеет ноутбук для работы. Сотрудники компании "А" не подключаются с личных устройств. В компании также к сети подключены 10 камер, 5 принтеров и 2 телевизора. Все эти устройства необходимо авторизовывать в NAC-системе.

Расчет количества уникальных конечных точек в сети: 1000 * 1 (количество устройств 1 сотрудника) + 10 (камеры) + 5 (принтеры) + 2 (телевизоры) = 1017 шт – уникальных устройств в компании.

Рекомендуется приобретать лицензии на большее число эндпоинтов, чем рассчитано уникальных устройств.

При необходимости количество эндпоинтов в лицензии можно увеличить. Для этого обратитесь к вашему менеджеру или отправьте запрос на нашу электронную почту eltex@eltex-co.ru.

Лицензии любого уровня могут быть выданы сроком на 1, 3, 5 лет или бессрочно.

По вопросам получения демо-лицензии для тестирования обращайтесь на нашу электронную почту eltex@eltex-co.ru.

Первичная активация лицензии

Для активации лицензии необходимо иметь *файл активации*, полученный от Вашего менеджера при приобретении системы.

Формат имени файла активации - **NICENNNNNNN.txt**, например - NICE1111111.txt.

После установки NAICE и первого входа систему отобразится страница "Лицензирование".

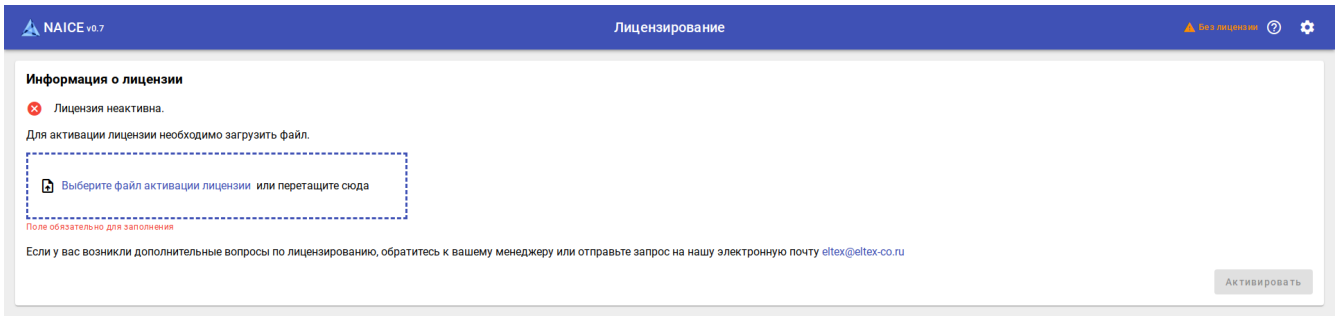

Рисунок 174. Первичная активация лицензии

Страница в состоянии "Без лицензии" содержит следующие элементы управления:

- `Без лицензии` - текущее состояние NAICE.
- `Лицензия неактивна` - текущий статус лицензии.
- Поле для загрузки файла активации лицензии. Файл активации лицензии можно выбрать из проводника или перетащить в данное поле.
- `Активировать` - кнопка для активации лицензии из загруженного файла активации.

Для загрузки лицензии перетащите файл в поле активации лицензии или выберите его в проводнике при клике на "*Выберите файл активации лицензии*". При необходимости до нажатия на кнопку `Активировать` файл можно заменить, кликнув на ↻ в правой части поля загрузки.

Рисунок 175. Загрузка файла активации

Валидный файл активации лицензии не может быть пустым или иметь размер более 1 Мб.

Для активации лицензии нажмите кнопку `Активировать`.

Активация лицензии может занять до нескольких минут. Не предпринимайте никаких действий до завершения процесса.

Успешная активация лицензии

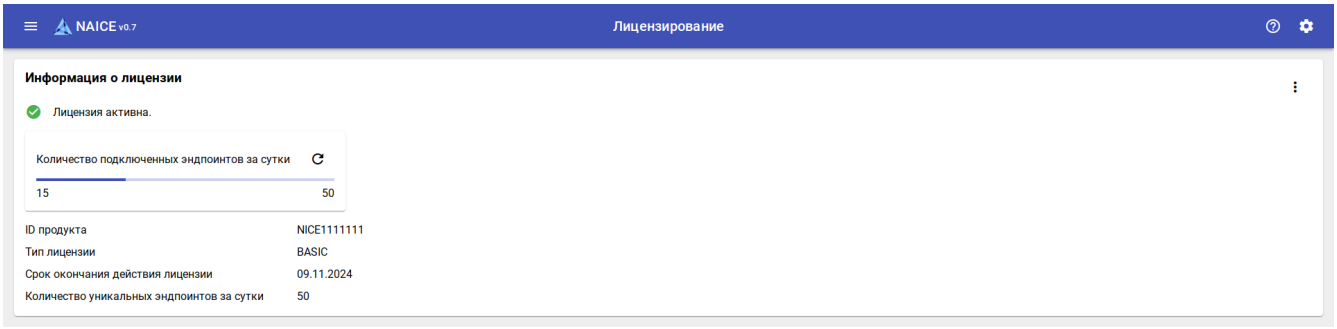

Рисунок 176. Лицензия активна

При успешной активации статус лицензии сменится на  `Лицензия активна` и отобразятся параметры текущей лицензии. Подробнее о параметрах лицензии описано далее.

Ошибки при активации лицензии

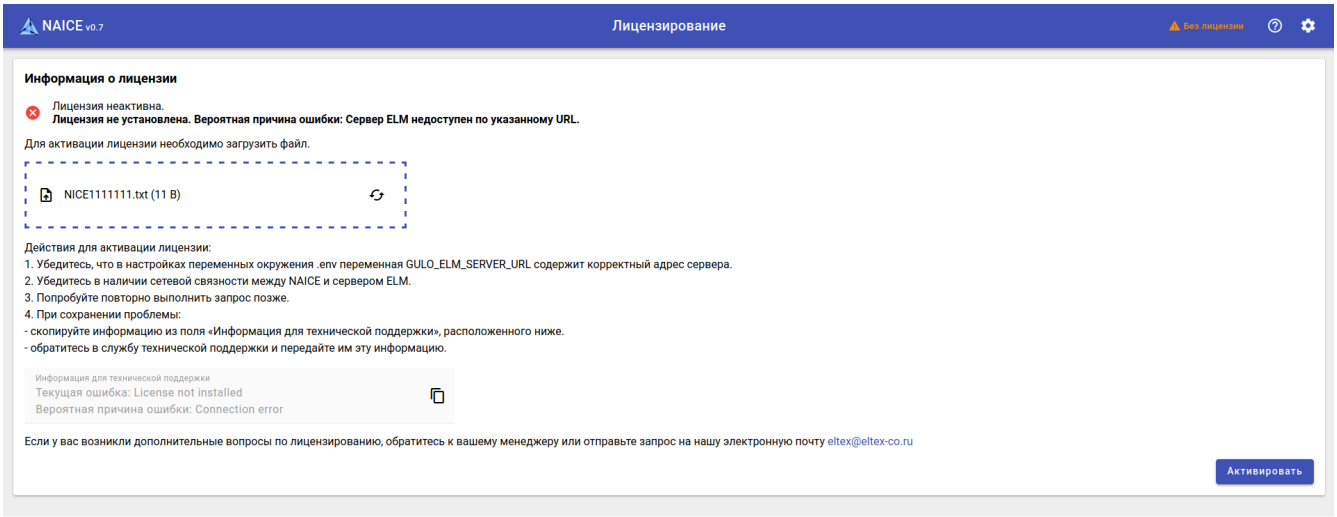

Рисунок 177. Ошибка при активации лицензии

При возникновении ошибок при активации лицензии на странице под статусом лицензии отобразится ошибка, возникшая в процессе активации. Как правило, ошибки при активации лицензии связаны либо с проблемами с доступом к серверу ELM (некорректный адрес ELM в конфигурации NAICE, отсутствие сетевой связности и т.п.), либо с ошибками самой лицензии (не наступивший или истекший срок лицензии).

Под полем для загрузки файла активации указаны рекомендации для устранения возникшей ошибки. В случае, если предложенные действия не оказали нужного воздействия, обратитесь в службу технической поддержки, приложив информацию из поля «Информация для технической поддержки» под рекомендациями.

Не рекомендуется выполнять действия, отличные от обозначенных в рекомендациях или указанных технической поддержкой. В некоторых ситуациях это может привести к блокировке экземпляра NAICE в ELM.

На данном этапе при необходимости файл активации лицензии можно заменить. Для этого нужно кликнуть на  в правой части поля загрузки файла активации и нажать на кнопку `Активировать`.

Мониторинг состояния лицензии

После успешной активации лицензии ее состояние можно отслеживать на странице *Лицензирование*. Для перехода на страницу из любого раздела NAICE в правом верхнем углу необходимо выбрать ⚙, в открывшемся меню выбрать "Лицензирование".

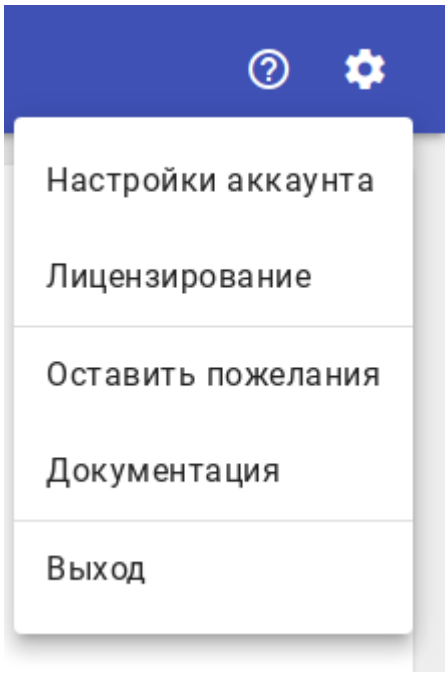

Рисунок 178. Меню системных настроек

После этого откроется страница с информацией о лицензии.

Информация о лицензии

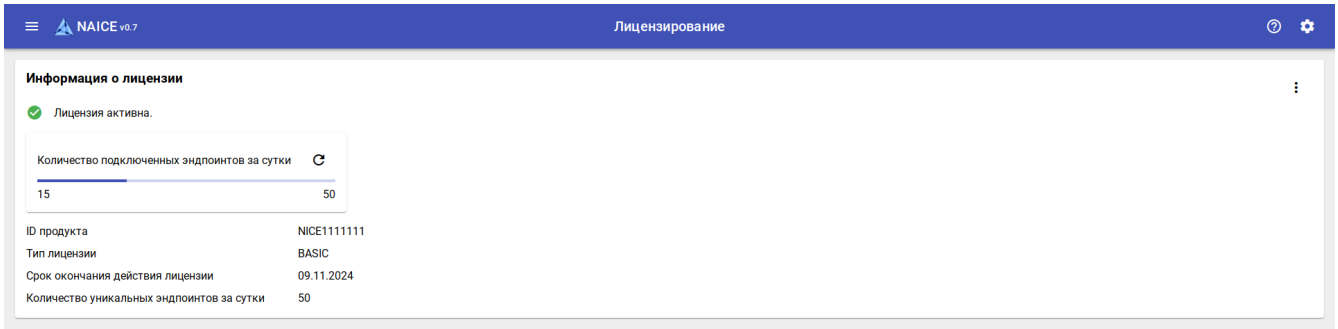

Рисунок 179. Информация о лицензии

Страница содержит следующие элементы:

- ✅ `Лицензия активна` - текущий статус лицензии.
- Счетчик текущего количества подключенных эндпоинтов за сутки. Автоматически обновляется раз в 5 минут.
- 🔄 - ручное обновление счетчика.
- Параметры лицензии:
  - `ID продукта` - уникальный идентификатор экземпляра NAICE.
  - `Тип лицензии` соответствует уровню лицензирования.

- `Срок окончания действия лицензии` - дата, при наступлении которой текущая срочная лицензия истекает. Не распространяется на бессрочную лицензию.

> При истечении срока действия лицензии лицензируемый функционал NAICE будет заблокирован, **в том числе авторизация конечных устройств**. Продлевайте лицензию заранее при появлении предупреждения для избежания таких ситуаций.

- `Количество уникальных эндпоинтов за сутки` - лимит по количеству подключенных эндпоинтов за сутки, предусмотренный лицензией.

> При достижении лимита по количеству подключенных эндпоинтов за сутки конечные устройства сверх этого лимита авторизованы не будут. Ранее авторизованные в последние сутки устройства будут успешно переавторизованы.

- ⋮ - меню, за которым находятся кнопки `Обновить лицензию` и `Заменить файл активации`. Подробнее об этих действиях описано далее.

Особенности подсчета количества подключенных устройств за сутки

- Счетчик подключенных эндпоинтов увеличивается только при подключении *уникального* эндпоинта, то есть эндпоинта, который не был успешно авторизован NAICE в последние 24 часа.
- Для определения уникальности эндпоинта необходимо, чтобы в RADIUS-запросе передавался RADIUS-атрибут `Calling-Station-Id`, содержащий MAC-адрес конечного устройства.
- Устройство считается активным ровно 24 часа с момента последнего подключения. При переавторизации в эти сутки время отсчета 24 часов обновляется.

> Пример.
>
> Эндпоинт был авторизован 10 июня в 13:31:10. "Освободит место" в лицензируемом лимите эндпоинт 11 июня в 13:31:11.
>
> Если конечное устройство было переавторизовано 10 июня в 20:20:10, то время сдвинется до 11 июня в 20:20:11.

Предупреждения о достижении лимитов

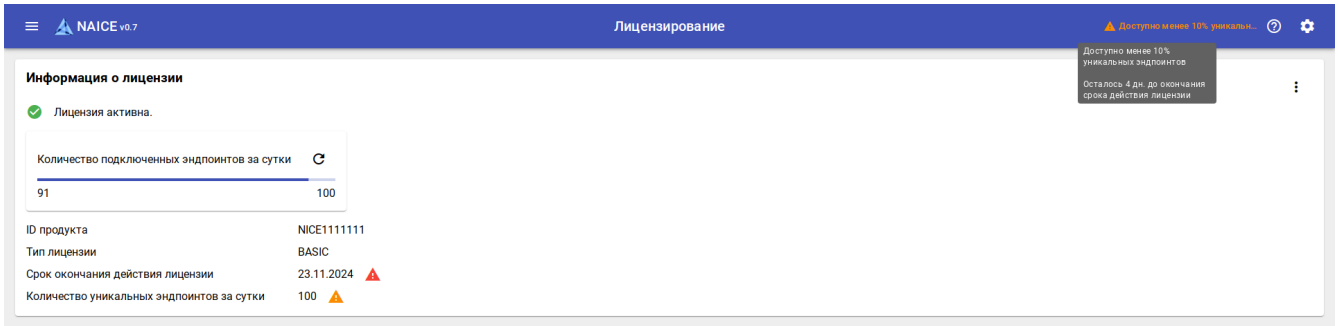

Рисунок 180. Предупреждения о достижении лимитов

При приближении к лимиту лицензии по количеству подключенных эндпоинтов или при приближении к дате истечения лицензии в верхней правой части любой страницы NAICE будут

отображаться предупреждения о приближении или достижении лимитов. При клике на предупреждение осуществляется переход на страницу Лицензирования.

Предупреждение о лимите по эндпоинтам начинает отображаться при достижении счетчиком значения в 90% от лицензируемого лимита.

Предупреждение о приближении даты окончания действия лицензии начинает отображаться за 90 дней до этого срока.

Помимо отображения в верхней части страниц, данные предупреждения отображаются на странице Лицензирование напротив соответствующего параметра в виде ⚠.

Недоступность сервера ELM

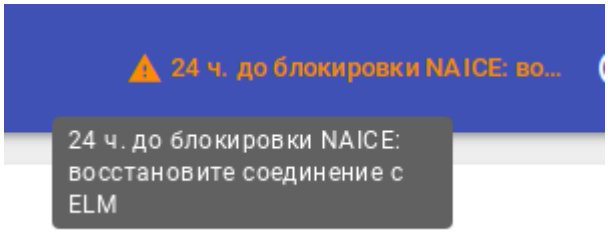

Рисунок 181. Предупреждение о недоступности ELM

NAICE периодически должен актуализировать параметры текущей лицензии на сервере ELM. В случае, если при очередной актуализации NAICE не смог получить параметры, то с этого времени стартует обратный отсчет до блокировки NAICE. Обратный отсчет отображается в верхней правой части страницы аналогично предупреждениям о достижении лимитов.

Если доступ до ELM не будет восстановлен в течение **72 часов**, то лицензируемый функционал NAICE будет заблокирован и лицензия будет сброшена.

Для проверки доступности сервера ELM можно воспользоваться следующей командой:

```
$ curl -k https://<IP адрес ELM>:<порт ELM>/elm/Hello
```

Если сервер ELM доступен, то вывод команды будет иметь вид:

```
{"server-info":
{"version":"1.4","build":"10","root":true,"serverType":"elm","daemonMode":"server","serverMode":"r
type":"elm","protocol-supported":2,"protocol-actual":4},"status":2,"result":"OK"}
```

Обновление параметров лицензии

Выполняйте ручное обновление параметров лицензии только в случаях, когда это действительно необходимо - например, если был изменен уровень лицензирования и необходимо ускорить процесс применения новых параметров.

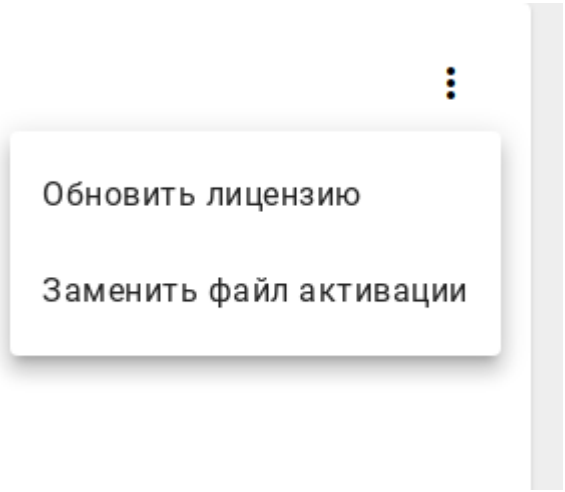

Рисунок 182. Меню дополнительных действий

Как было указано выше, NAICE периодически актуализирует параметры текущей лицензии на сервере ELM. В случае, если необходимо вручную обновить параметры лицензии, не дожидаясь автоматического обновления, то на странице Лицензирования нажмите на ⋮ и выберите `Обновить лицензию` в меню. Появится уведомление вида:

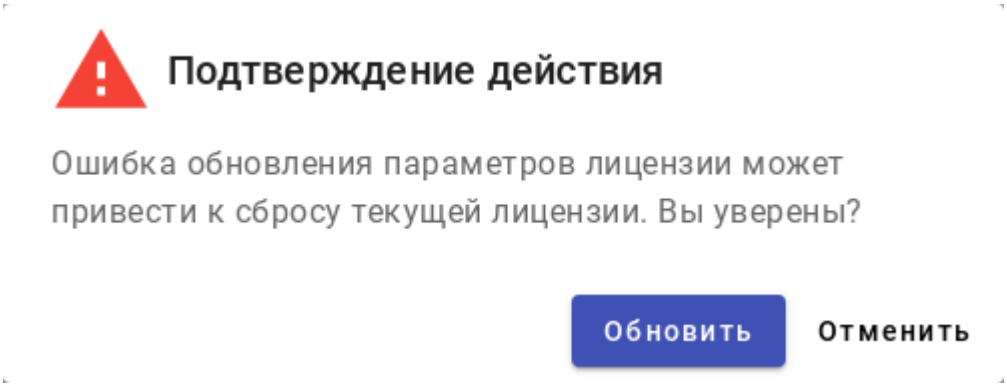

Рисунок 183. Подтверждение обновления параметров лицензии

Нажмите `Обновить`.

В случае успешного обновления параметров лицензии на странице отобразятся соответствующее уведомление и новые параметры лицензии.

Ручное обновление параметров доступно раз в 30 секунд. До истечения 30-секундной паузы кнопка будет заблокирована.

Замена лицензии

Одному экземпляру NAICE соответствует одна лицензия. При необходимости изменения лицензии правки вносятся сотрудниками «Элтекс» в *текущую* лицензию, после чего ее параметры автоматически обновляются. Замена лицензии действительно необходима в редких случаях. Выполняйте замену лицензии **только** по указанию технической поддержки или вашего менеджера.

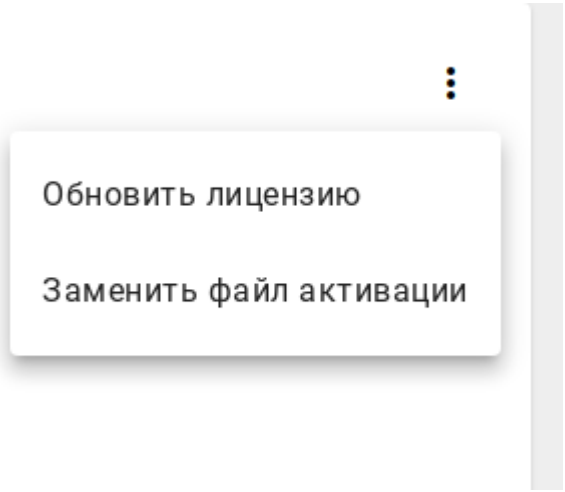

Рисунок 184. Меню дополнительных действий

Для замены файла активации на странице Лицензирования в правом верхнем углу страницы нажмите на ⋮ и выберите `Заменить файл активации` в меню.

Рисунок 185. Замена файла активации лицензии

В открывшемся окне выберите через проводник или перетащите в поле загрузки новый файл активации и нажмите `Заменить`.

При успешной замене файла откроется страница Лицензирование с параметрами новой лицензии.

При ошибках замены файла предыдущая лицензия будет сброшена, а возникшая ошибка отобразиться на странице. Для устранения ошибок следуйте рекомендациям по активации лицензии, указанным на странице.