Руководство по эксплуатации Magnus ID

Оглавление

1. Введение

Magnus ID — это система аутентификации пользователей в части предоставления возможности использования второго фактора. Многофакторная аутентификация (MFA) представляет собой механизм усиления безопасности системы аутентификации путем добавления дополнительных уровней проверки подлинности пользователя.

1.1 Краткое описание структуры

Принцип работы заключается в том, что Magnus ID выступает промежуточным звеном между пользователем и защищаемыми приложениями. Когда пользователь пытается получить доступ к защищенному ресурсу, система блокирует вход пользователя до ввода 2FA. Также, после успешной проверки 2FA, система выдает специальный токен, который позволяет пользователю получать доступ к различным сервисам без повторной авторизации.

Архитектурно система представляет собой программный комплекс, который может быть интегрирован с существующими системами аутентификации и предоставляет API для взаимодействия с клиентскими приложениями.

Программный комплекс Magnus ID разделён на несколько модулей:

- Magnus Core – центральная консоль управления;
- Magnus Auth – модуль мультифакторной аутентификации.

2. Описание архитектуры программного обеспечения

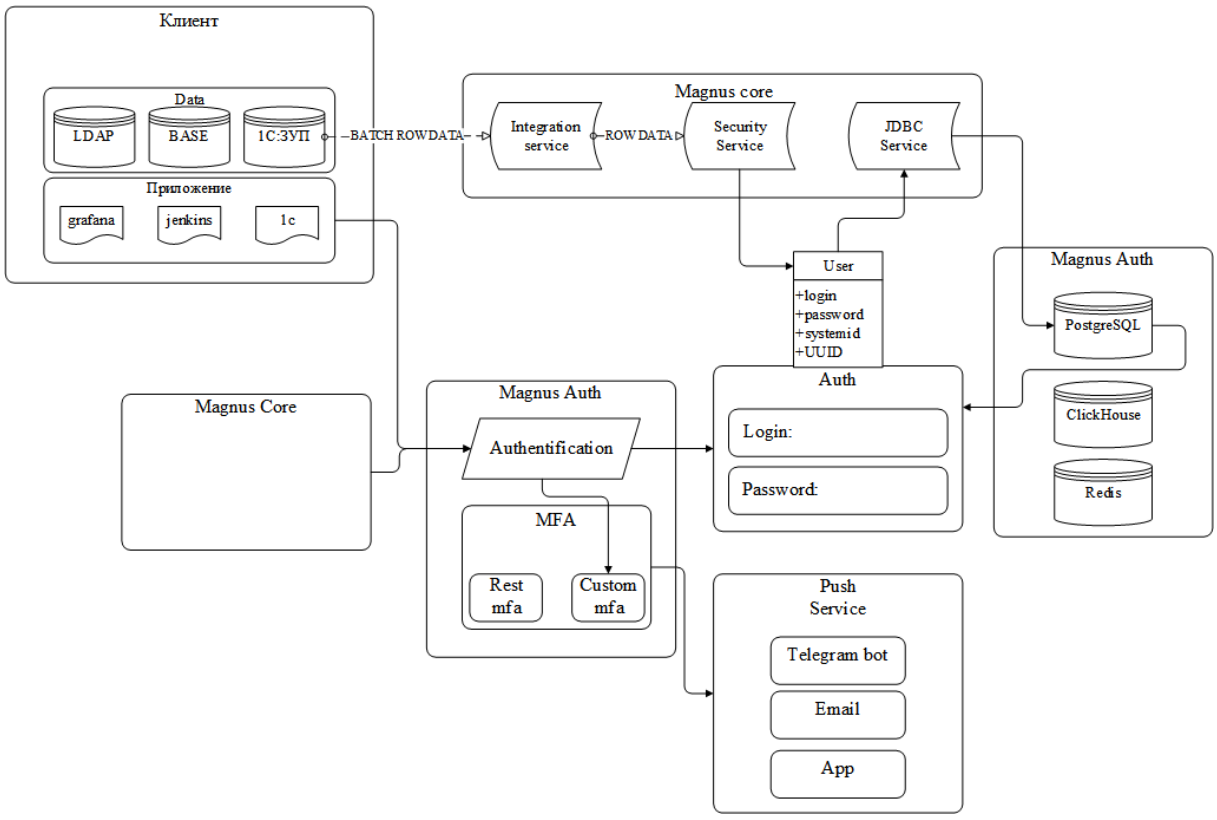
Принцип работы заключается в том, что Magnus ID выступает промежуточным звеном между пользователем и защищаемыми приложениями. Когда пользователь пытается получить доступ к защищенному ресурсу, система блокирует вход пользователя до ввода 2FA. Также, после успешной проверки 2FA, система выдает специальный тикет, который позволяет пользователю получать доступ к различным сервисам без повторной авторизации.

Архитектурно система представляет собой сервер, который может быть интегрирован с существующими системами аутентификации и предоставляет API для взаимодействия с клиентскими приложениями.

Программный комплекс Magnus ID разделён на несколько модулей:

- Magnus Core – Центральная консоль управления;
- Magnus Auth – модуль мультифакторной аутентификации.

Схема взаимодействия модулей отображены на схеме ниже:



С помощью Magnus ID организации получают надёжный инструмент использования второго фактора.

3. Обзор интерфейса

3.1 Авторизация

3.1.1 Первичная авторизация

Для использования сервиса необходимо авторизоваться в системе, для этого необходимо ввести в поля «Логин» и «Пароль» данные учётной записи. Логином является корпоративный адрес электронной почты, без домена. Экран авторизации представлен на рисунке 1.

Для входа в систему Magnus ID необходима учётная запись, добавленная администратором системы. Тестовая учётная запись для авторизации на сервисе:

- Логин: Superadmin
- Пароль: MagnusTech!1

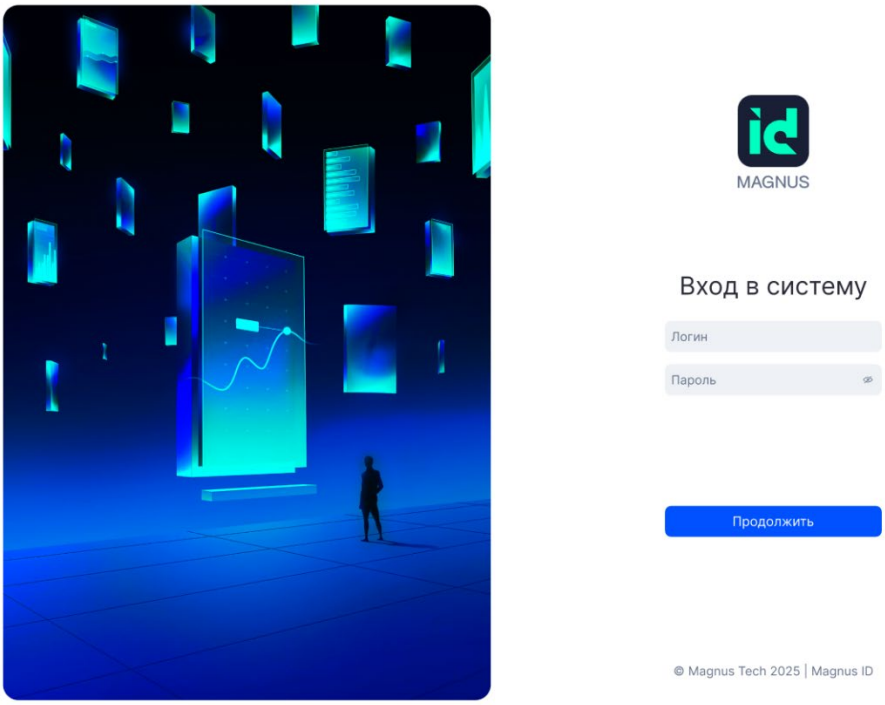


Рисунок 1

Первый вход в систему осуществляется без дополнительной проверки безопасности. После входа в систему пользователю необходимо перейти в раздел «Настройки безопасности», пункт 3.5 текущего документа, и подключить двухфакторную аутентификацию.

3.1.2 Авторизация с подключенным методом многофакторной аутентификации

Авторизация с подключенным методом многофакторной аутентификации отличается тем, что после введения данных учётной записи, пользователю необходимо ввести TOTP-код для подтверждения личности. Для прохождения аутентификации необходимо ввести TOTP-код из приложения «Яндекс Ключ».

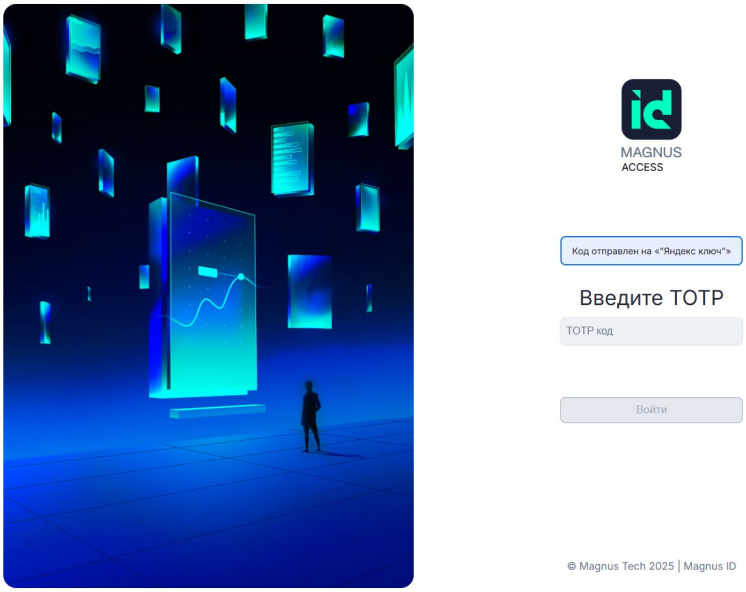


Рисунок 2

После успешного ввода TOTP-кода пользователь успешно проходит авторизацию и попадает в систему Magnus ID.

3.2 Менеджмент

3.2.1 Роли

Раздел «Роли» является ключевым инструментом IDM-портала для централизованного управления настройками доступа в организации. Вся работа с ролями сосредоточена в едином интерфейсе, список ролей позволяет находить и анализировать существующие роли.

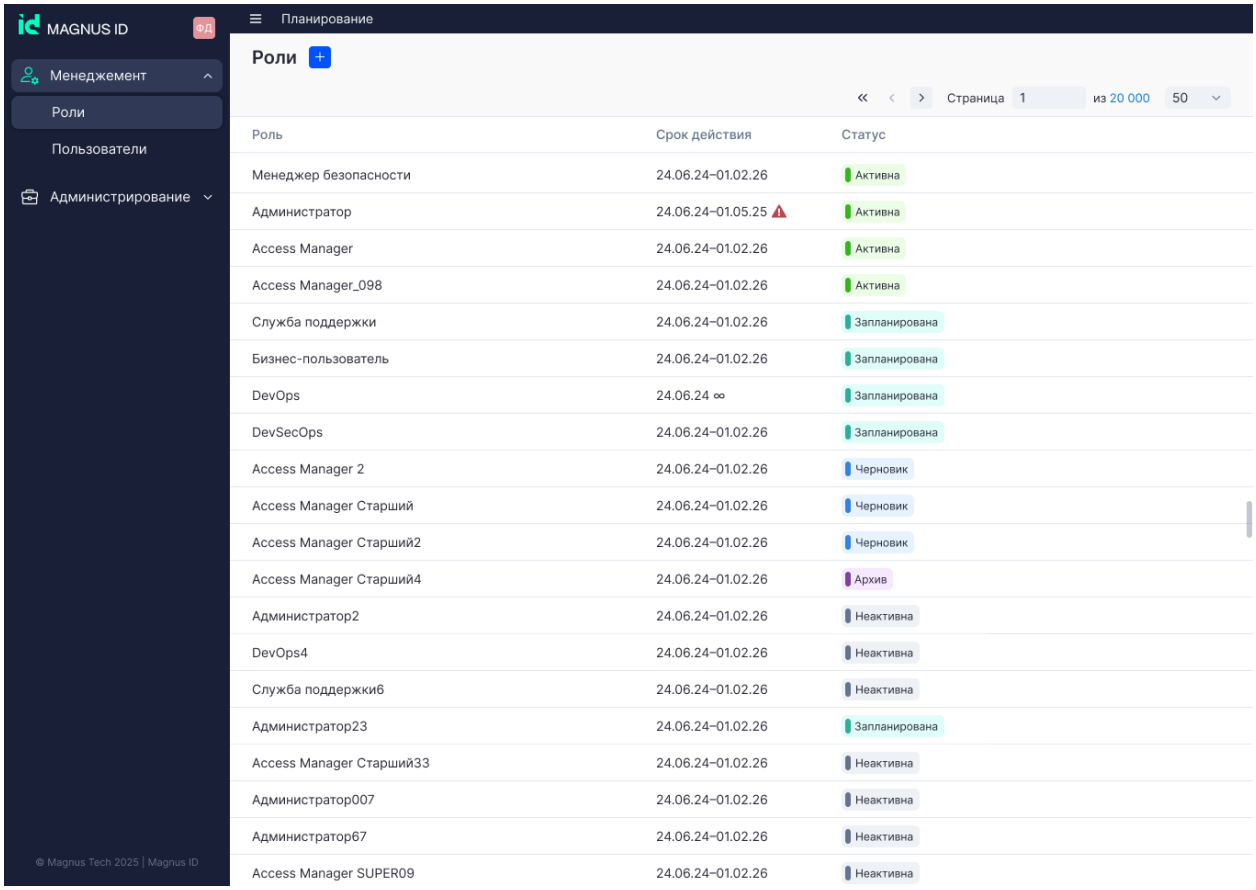


Рисунок 3

Дополнительно в данном разделе у пользователя есть возможность открыть карточку роли, которая предоставляет полную информацию о статусе и содержании роли.

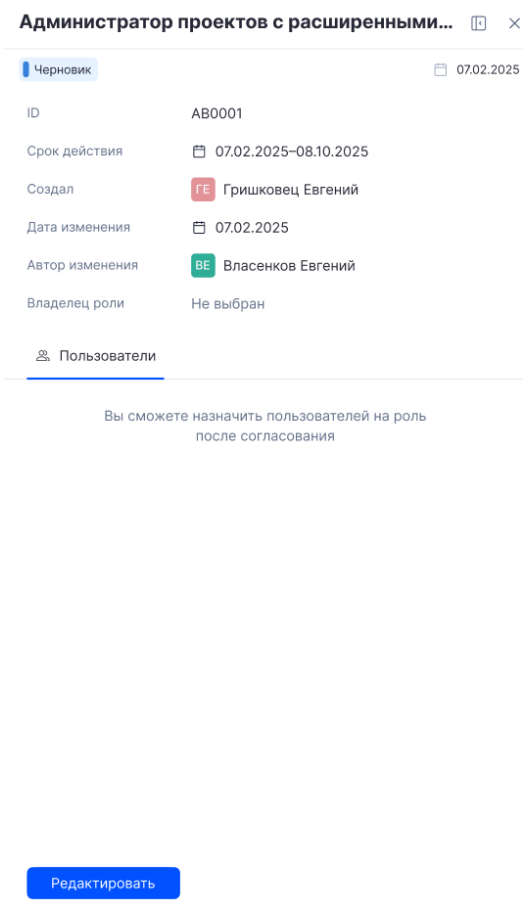


Рисунок 4

3.2.2 Пользователи

Раздел «Пользователи» обеспечивает централизованное и эффективное управление учетными записями сотрудников организации. Раздел представляет собой список пользователей.

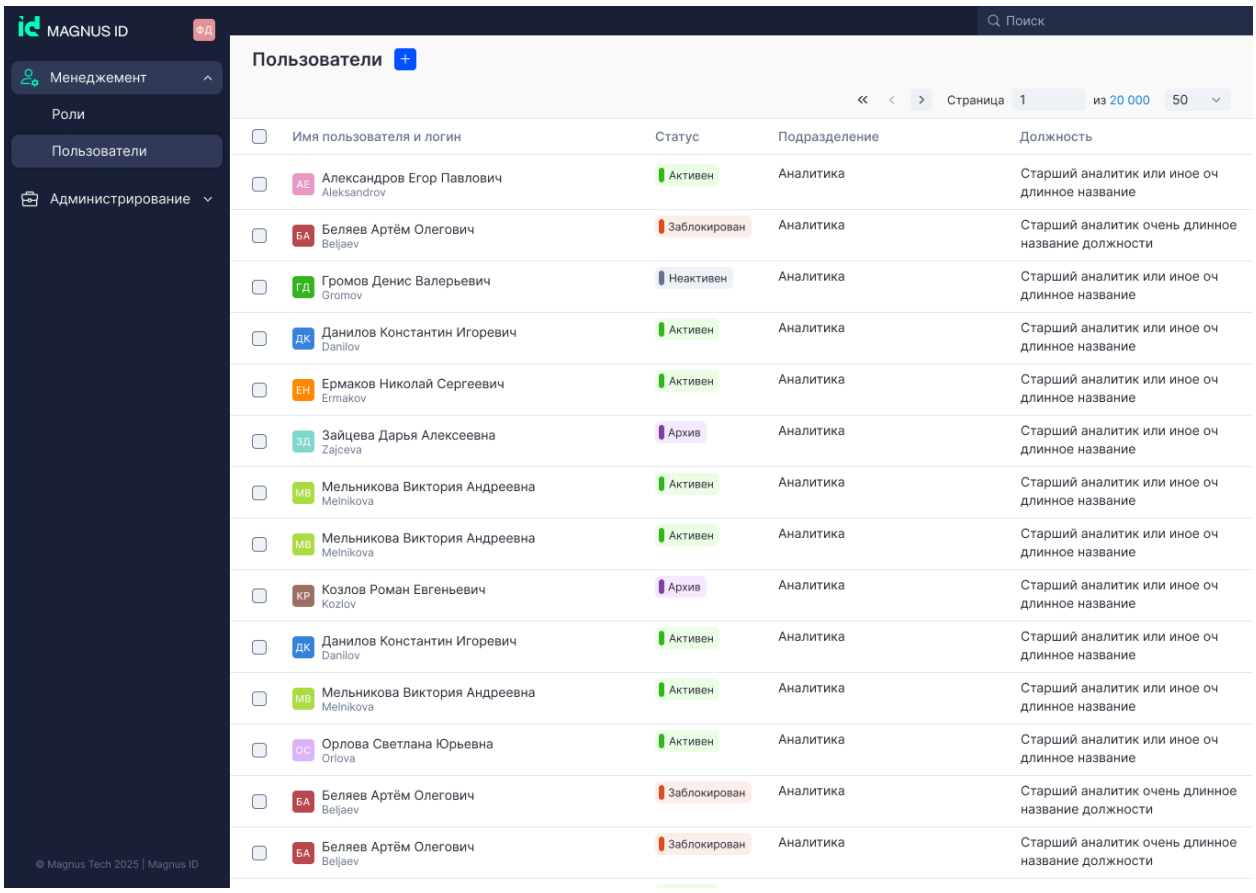


Рисунок 5

Дополнительно в данном разделе у пользователя есть возможность открыть карточку пользователя, которая предоставляет общую информацию о пользователе:

- Логин;
- Почта;
- Телефон;
- Дата рождения.

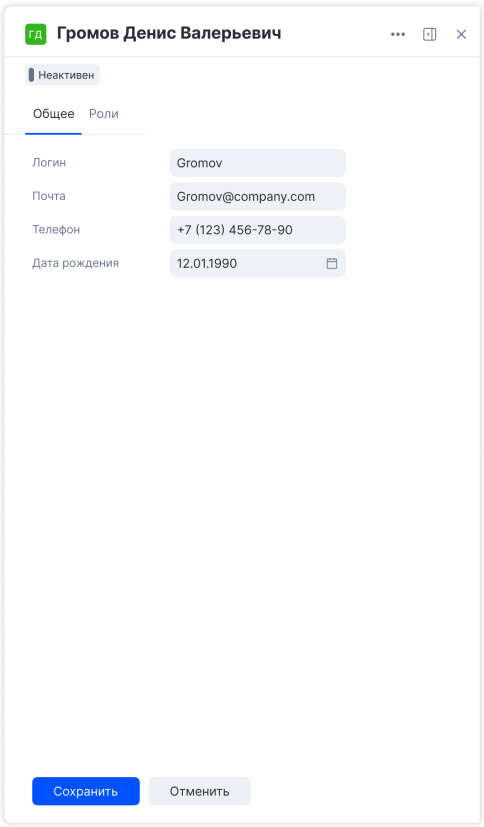


Рисунок 6

Также карточка содержит информацию о ролях пользователя.

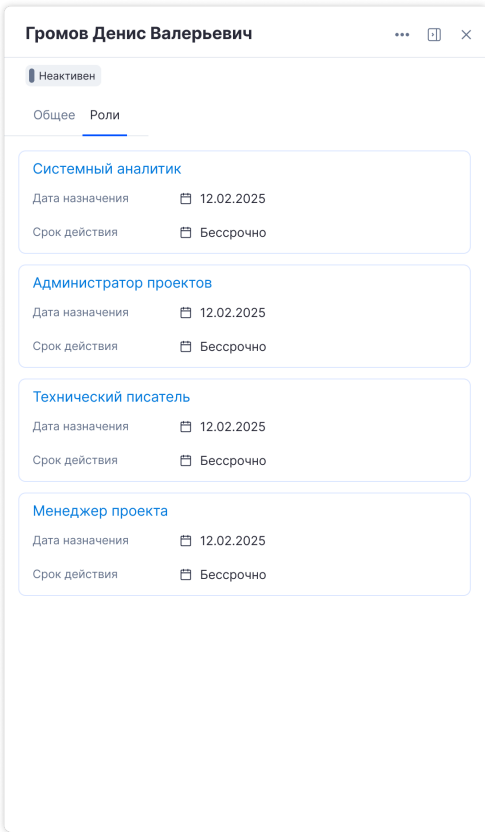


Рисунок 7

Данный раздел позволяет пользователю выбрать несколько пользователей, используя чекбоксы, находящиеся в списке пользователей для массового изменения статусов.

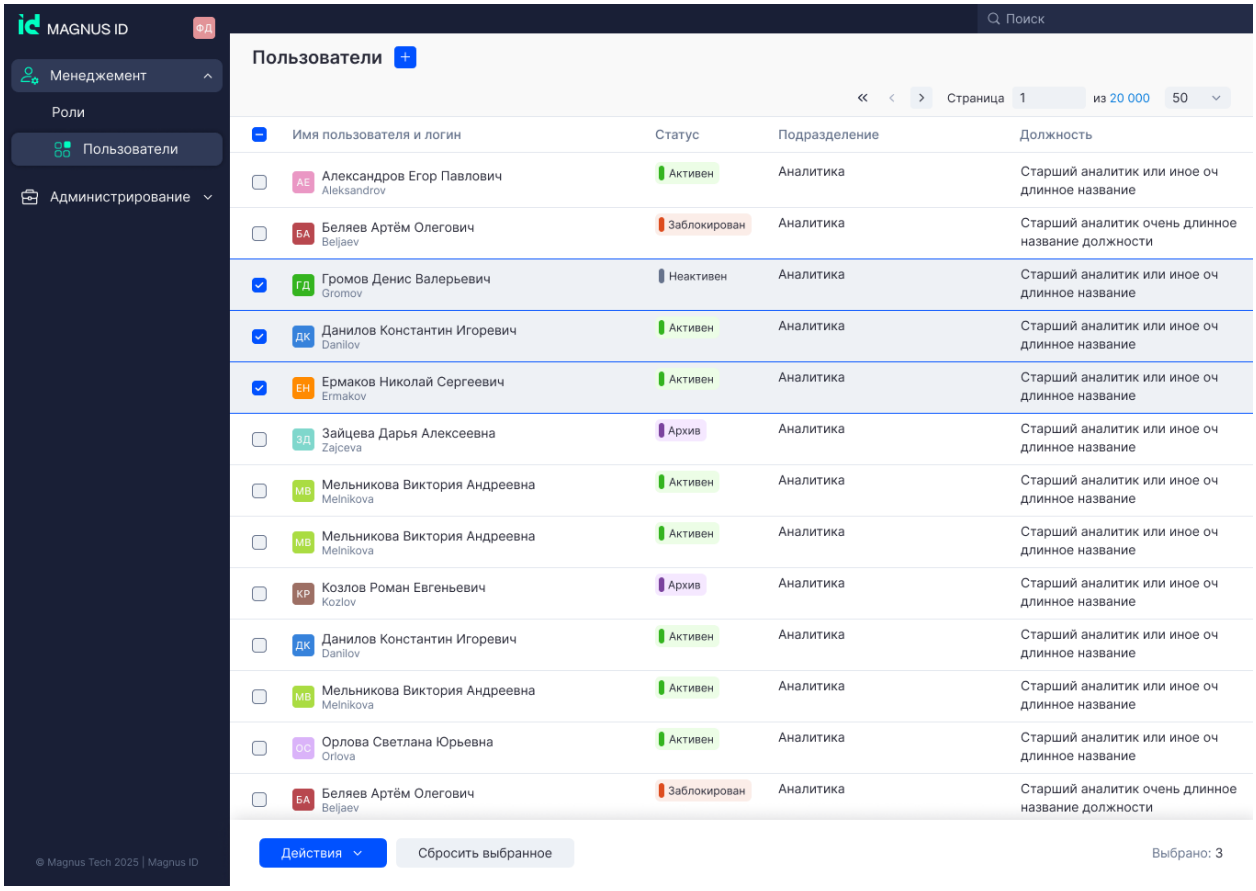


Рисунок 8

Для изменения статусов администратору необходимо нажать кнопку «Действия», после чего выбрать статус, который необходимо задать для выбранных пользователей.

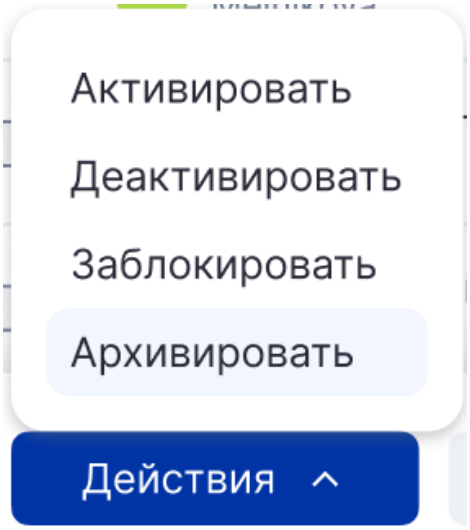


Рисунок 9

3.4 Профиль

3.4.1 Профиль пользователя

Пользователь может перейти в настройки профиля, для этого необходимо воспользоваться значком в верхней части экрана, содержащий инициалы пользователя, как показано на рисунке 10, кнопка 1.

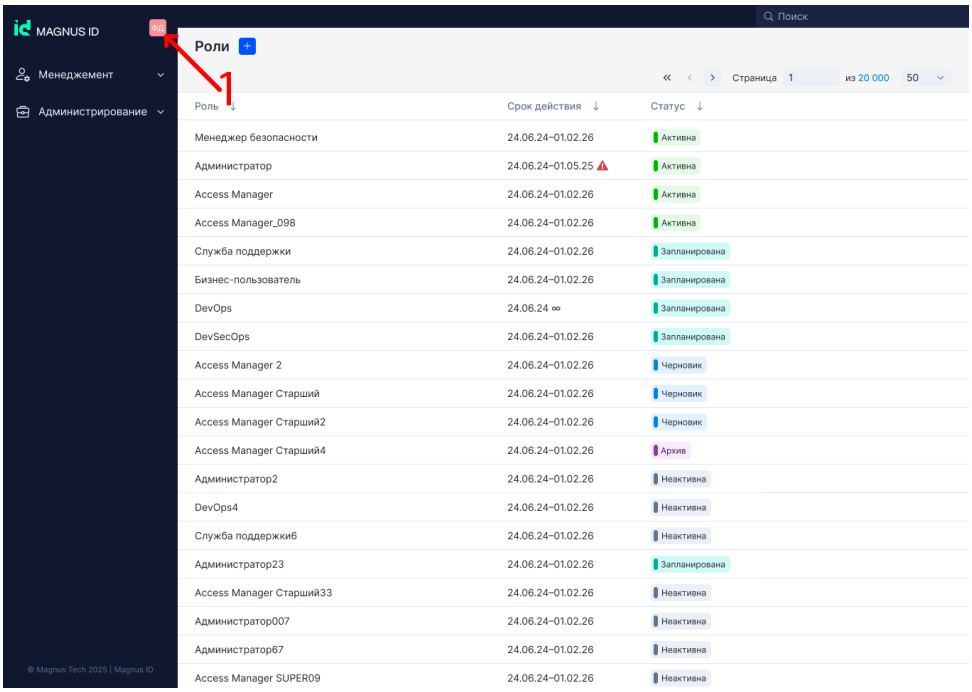


Рисунок 10

В открывшемся окне пользователю необходимо выбрать раздел «Профиль» для дальнейшего перехода в профиль пользователя.

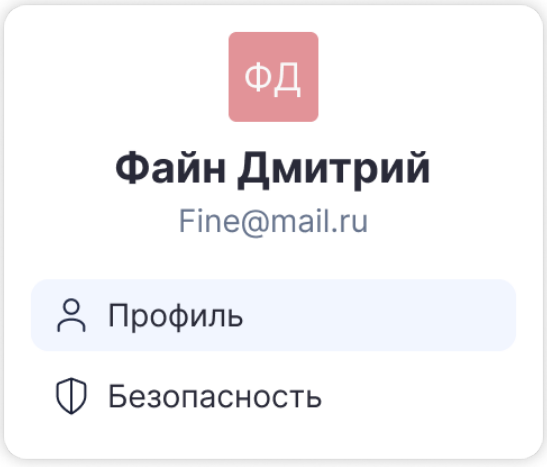


Рисунок 11

Раздел «Профиль пользователя» включает в себя:

- личные данные пользователя:
    - Фамилия и Имя;
    - Отчество (если есть);
    - Имя пользователя;
    - Дату рождения.
- контакты пользователя:
    - Почта;
    - Контактный номер телефона;
    - Дату приёма на работу.
- документы пользователя:
    - Табельный номер.

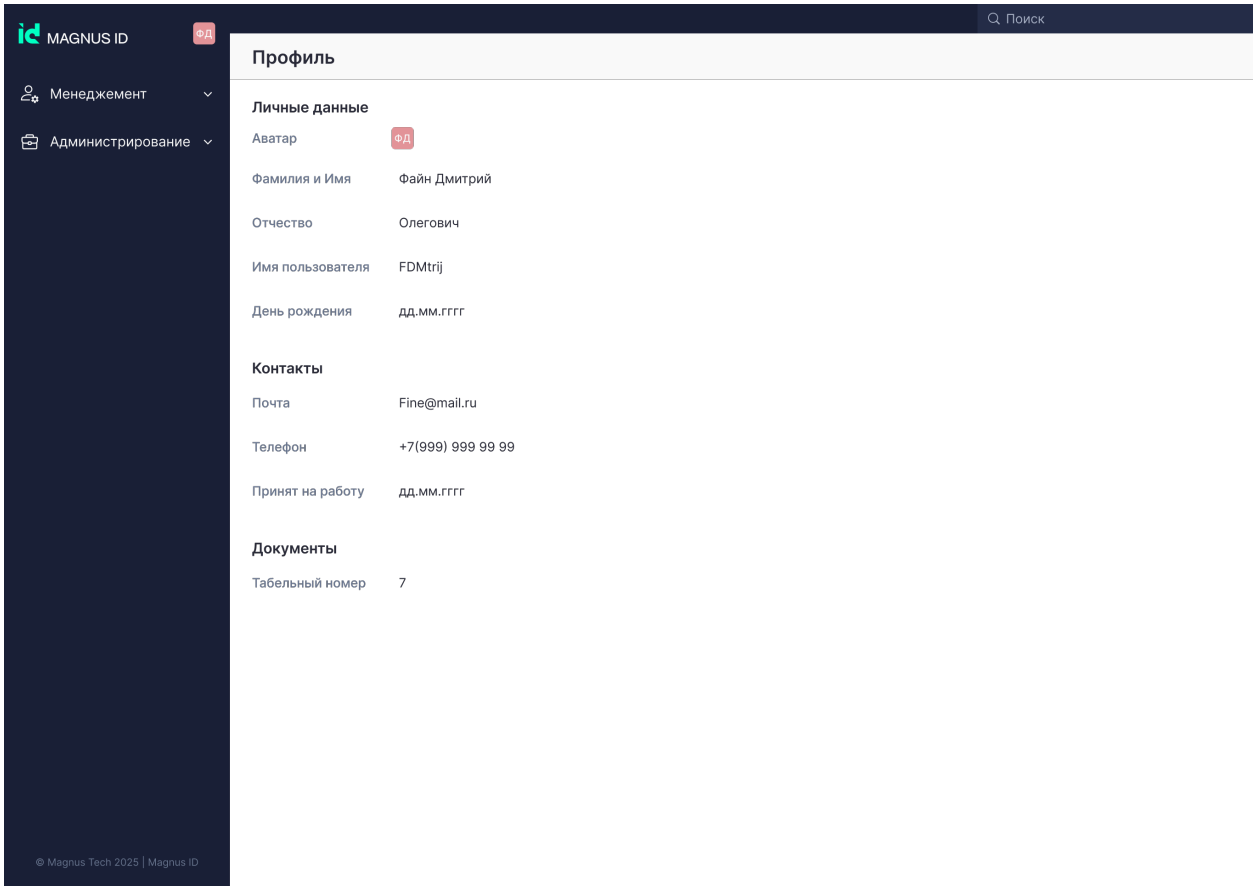


Рисунок 8

3.5 Настройки безопасности

Раздел «Безопасность» содержит в себе настройки двухфакторной аутентификации.

Пользователь может перейти в настройки безопасности аккаунта пользователя, для этого необходимо воспользоваться значком с инициалами пользователя в верхней части экрана, содержащий инициалы пользователя, как показано на рисунке 13.

В открывшемся окне пользователю необходимо выбрать раздел «Безопасность» для дальнейшего перехода.

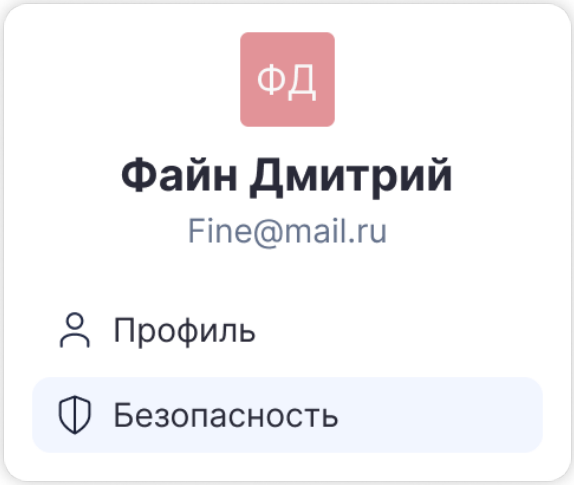


Рисунок 9

После чего пользователь попадёт на экран раздела «Безопасность».

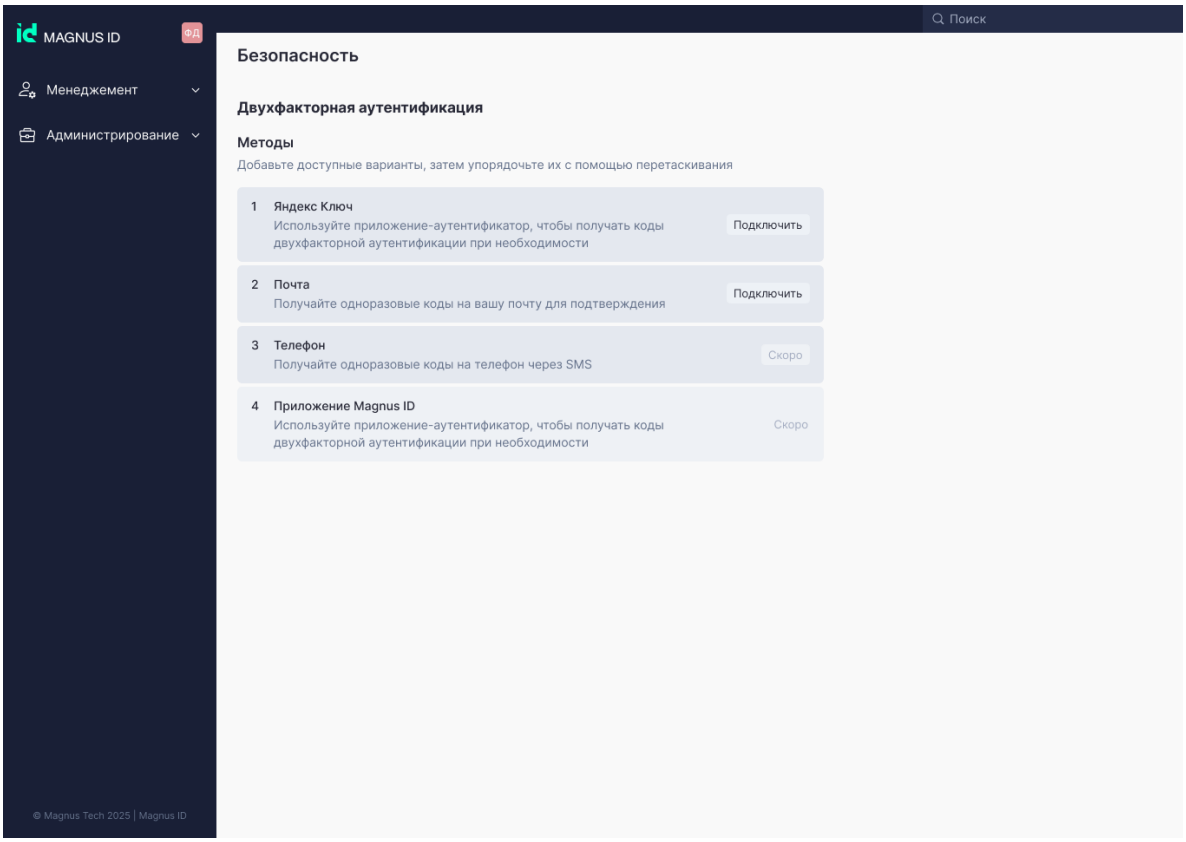


Рисунок 14

3.5.1 Двухфакторная аутентификация

В разделе «Двухфакторная аутентификация» представлены методы аутентификации второго фактора. Данный раздел позволяет пользователю подключать, изменять и упорядочивать методы двухфакторной аутентификации.

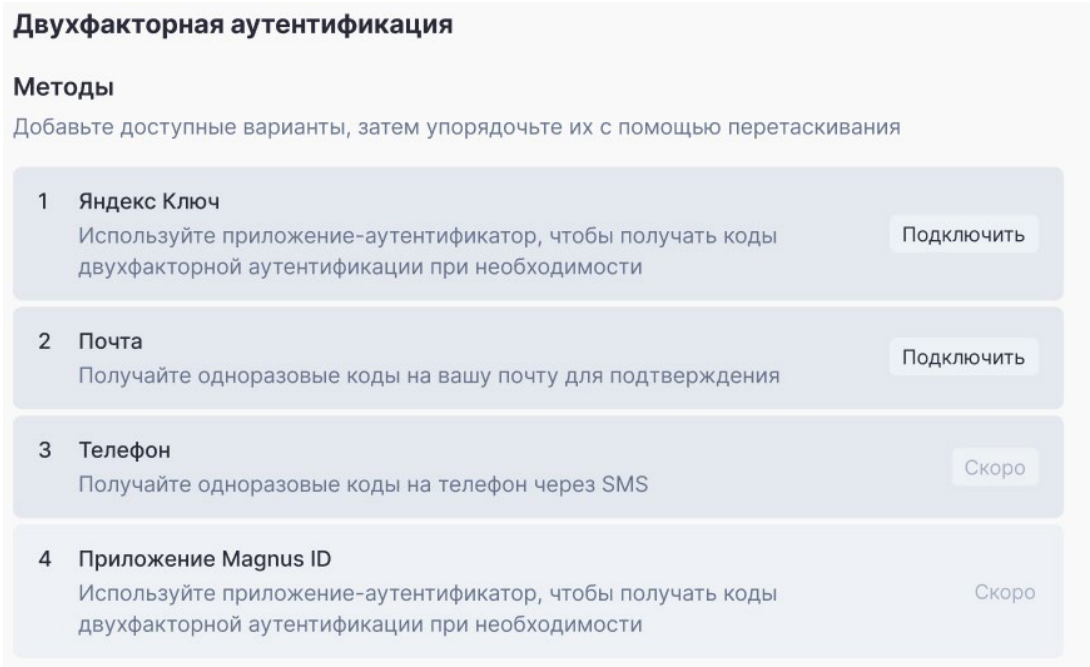


Рисунок 15

Почта является методов двухфакторной авторизации по умолчанию и подключена у каждого пользователя автоматически.

3.5.2.1 Яндекс Ключ

Пользователю доступно подключение двухфакторной аутентификации по методу Яндекс ключ. Для этого пользователю необходимо нажать кнопку «Подключить».

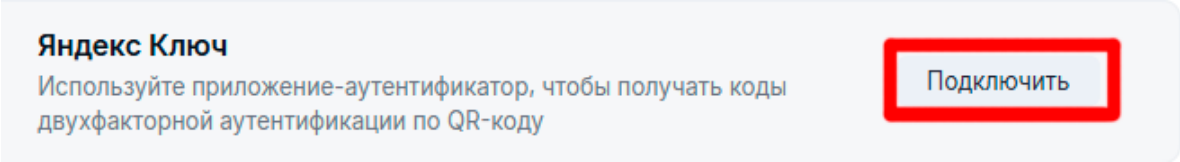


Рисунок 16

При нажатии этой кнопки появится диалоговое окно с пошаговым подключением приложения Яндекс Ключ. На первом шаге представлена рекомендация по установке приложения. Для перехода к следующему шагу пользователю необходимо нажать кнопку «Далее».

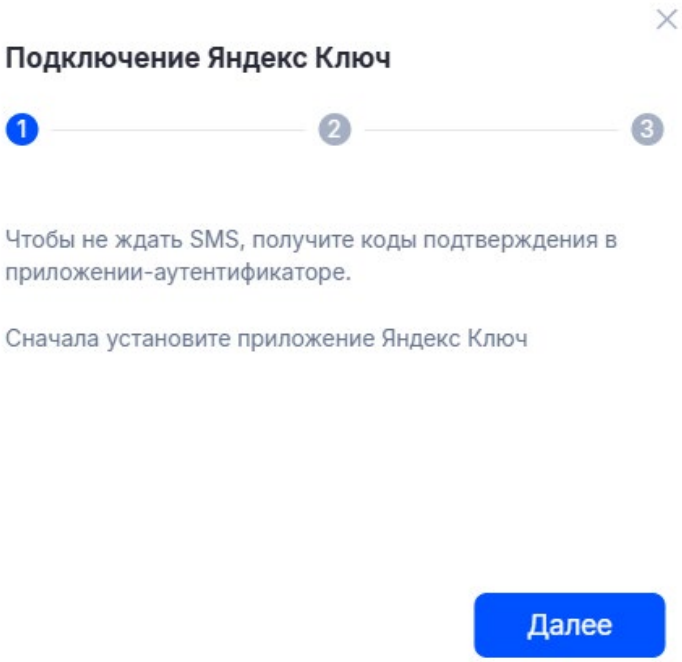


Рисунок 17

После этого отобразится второй шаг подключения приложения Яндекс Ключ через QR-код. Пользователю для подключения необходимо отсканировать код с помощью приложения Яндекс ключ, после чего в приложении будет отображаться TOTP-код для дальнейшей двухфакторной аутентификации по данному методу. Для перехода к третьему этапу необходимо нажать «Далее».

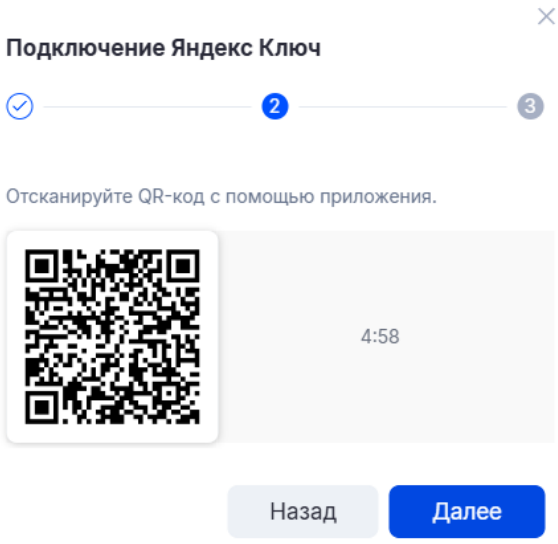


Рисунок 18

На третьем этапе подключения двухфакторной аутентификации с использованием приложения Яндекс Ключ пользователю необходимо ввести TOTP-код, отображаемый в приложении.

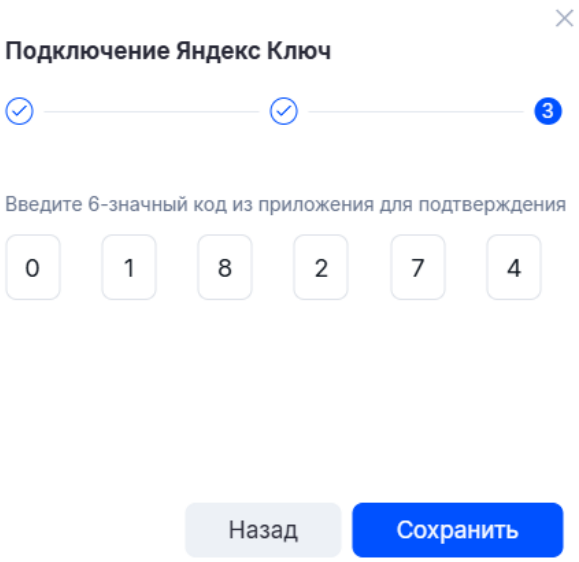


Рисунок 19

После введения TOTP-кода пользователю необходимо нажать кнопку «Сохранить». При успешном подключении пользователю отобразится подключенным метод двухфакторной аутентификации через приложение Яндекс Ключа.

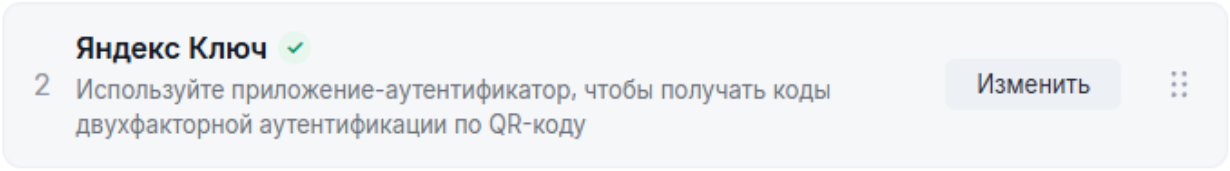


Рисунок 20

3.5.2.2 Упорядочивание методов аутентификации

Данный функционал позволяет пользователю выбирать приоритетный метод двухфакторной аутентификации пользователя методом перетаскивания карточки метода. Эта возможность доступна только для подключенных методов аутентификации. Для того, чтобы изменить приоритет метода аутентификации необходимо воспользоваться значками 1 на рисунке 21.

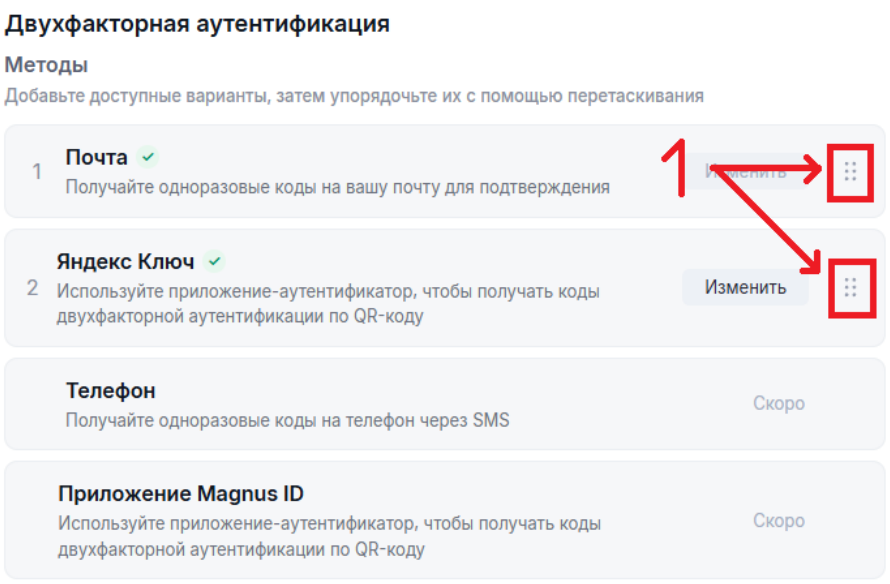


Рисунок 21

После изменения приоритета двухфакторной аутентификации пользователь получит уведомление об успешном сохранении нового порядка приоритета методов.

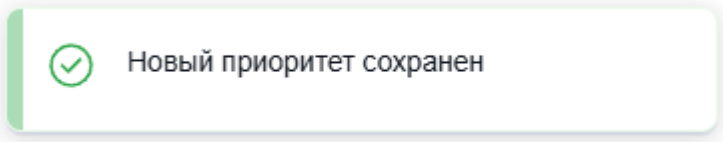


Рисунок 22

3.6 Настройки почты

Раздел «Настройка почты» обеспечивает централизованную настройку параметров отправки почтовых уведомлений из системы IDM.

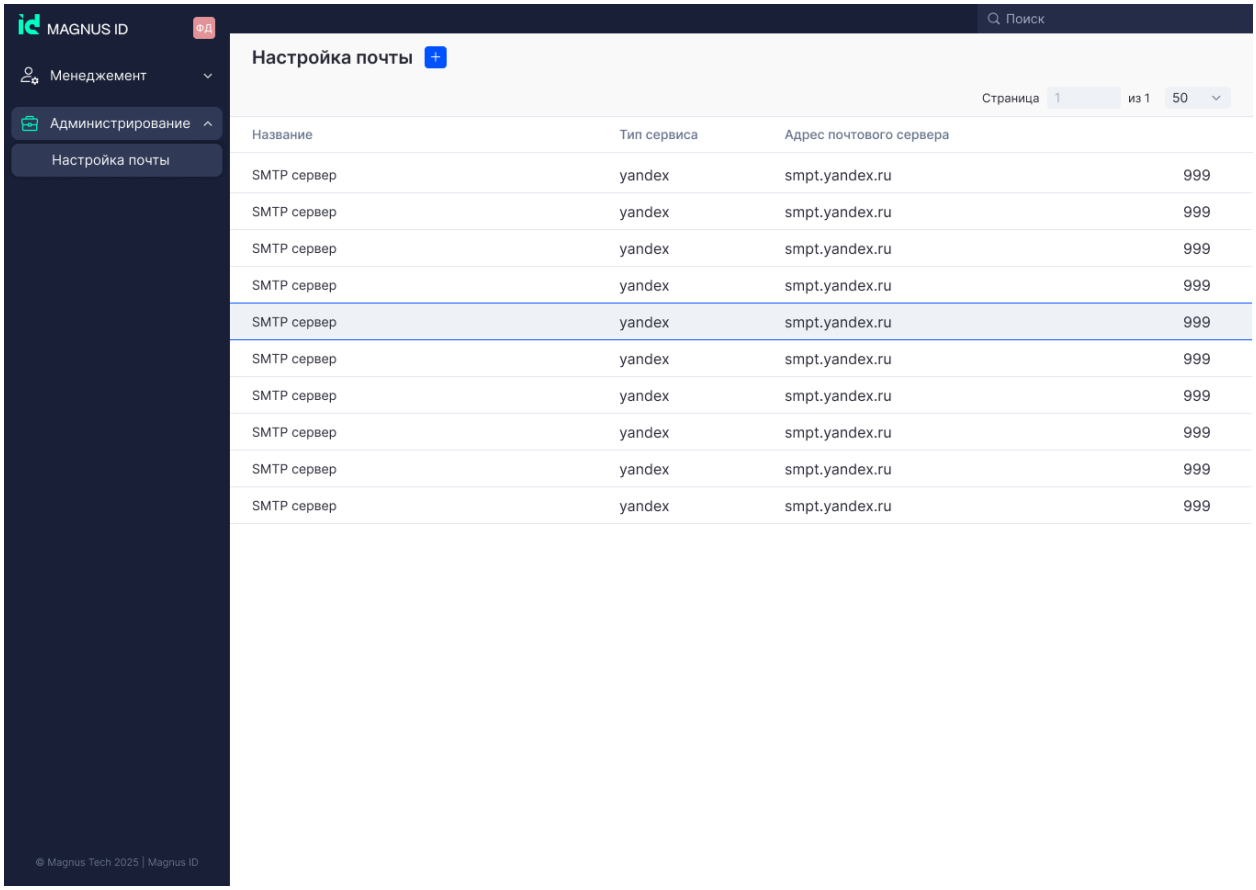


Рисунок 23

Данный раздел обеспечивает администраторам системы IDM возможность централизованной настройки и управления параметрами SMTP-сервера для отправки почтовых уведомлений, включая:

- Конфигурацию подключения (хост, порт, аутентификация).
- Безопасное хранение учетных данных (шифрование пароля).

3.6.1 Новая настройка почты

Для создания нового почтового сервера, администратору необходимо воспользоваться значком «+» в верхней части экрана, после этого будет открыто модальное окно, в котором пользователю необходимо заполнить соответствующие поля:

- Название;
- Тип сервиса;

- Адрес почтового сервера;
- Логин;
- Пароль;
- Порт.

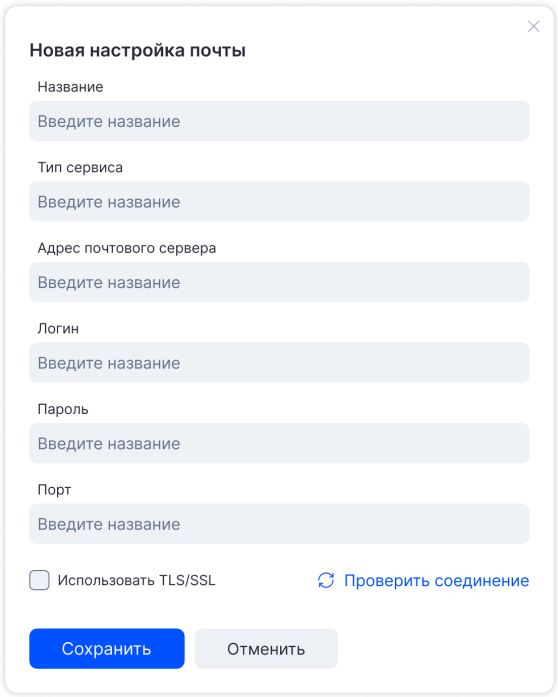


Рисунок 104

После заполнения полей администратору необходимо нажать кнопку «Проверить соединение».

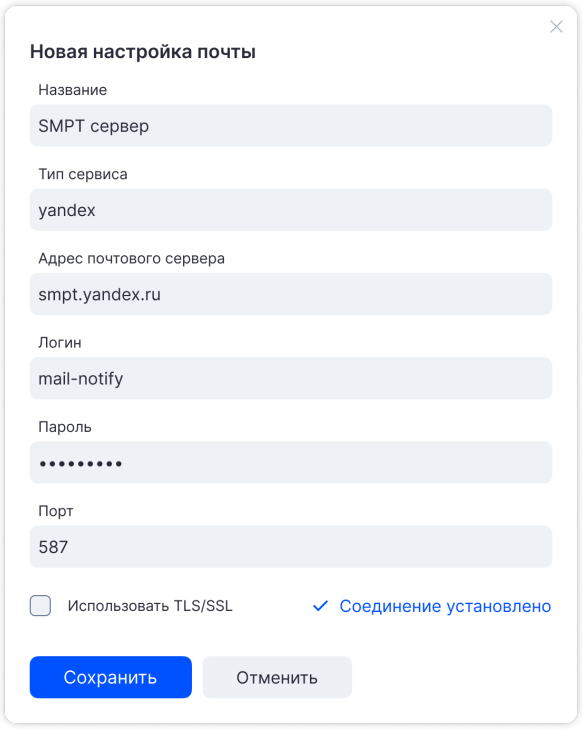


Рисунок 25

После проверки соединения, администратору необходимо нажать кнопку «Сохранить». В случае успешного сохранения нового сервера, он будет отображен в общем списке SMTP-серверов.

3.6.2 Карточка SMTP сервера

Раздел «Настройка почты» предоставляет администратору открыть карточку сервера, которая содержит подробную информацию о подключении.

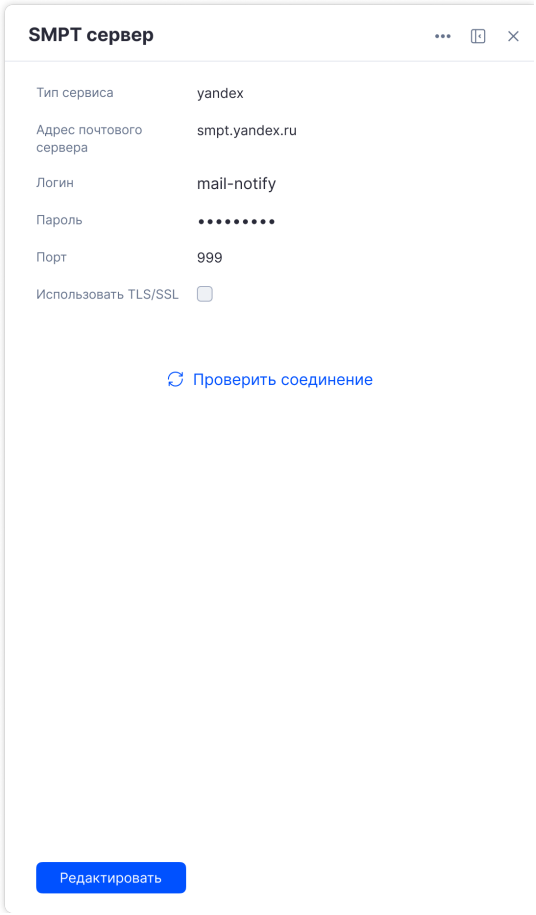


Рисунок 26

Для перехода в режим редактирования, пользователю необходимо нажать на кнопку «Редактировать», после чего карточка SMTP сервера станет доступной для редактирования.

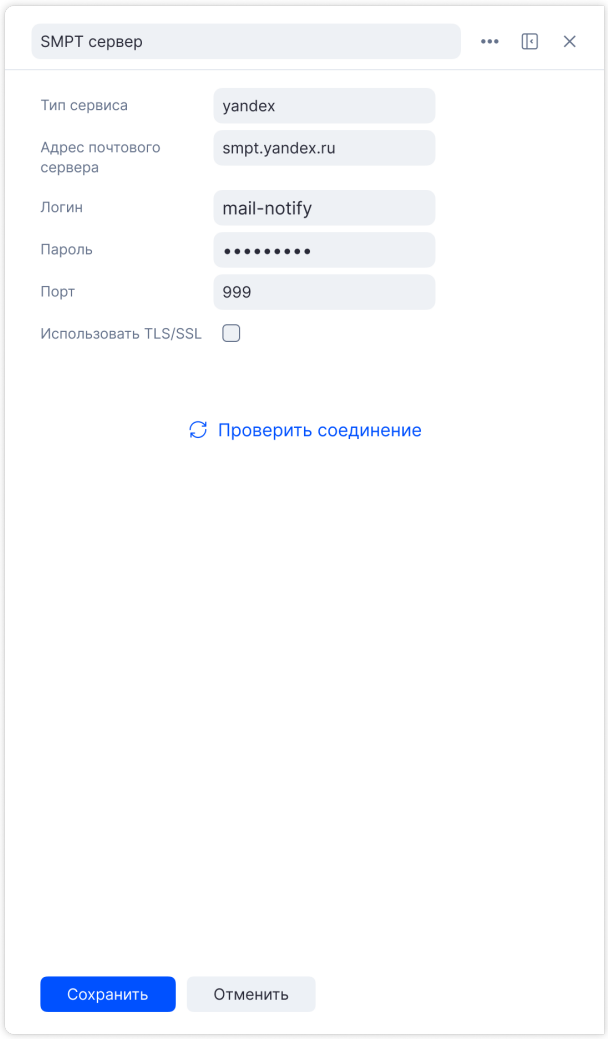


Рисунок 27

Для сохранения изменений администратору необходимо нажать кнопку «Сохранить».

4. Контактная информация

Компания ООО «МАГНУС ТЕХ» (ОГРН 1217700002959).

Адрес: 105082, г. Москва, ул. Большая Почтовая, д 36 стр. 1

Контакты:

По вопросам поддержки обращайтесь:

- На официальный сайт: Magnus-tech.ru
- На электронную почту: support@Magnus-tech.ru
- По телефону: +7(800)550-27-84

Отзыв по документации:

Если вы нашли ошибки в документации или у Вас есть предложения, свяжитесь с нами по адресу support@Magnus-tech.ru.

5. Информация о компании

Magnus Tech - специализируется на разработке инновационных систем и комплексных решений для эффективного управления бизнес-процессами в современных условиях. В основе деятельности компании лежит активное внедрение передовых технологий, с особым акцентом на вопросах безопасности и защиты данных.

Одним из направлений работы является создание надежного программного обеспечения для защищенного файлового обмена и организации совместной работы. Такие решения становятся важным элементом успешной цифровой трансформации рабочего пространства, что позволяет предлагать партнерам высококачественные продукты, соответствующие самым строгим требованиям информационной безопасности.

Разработки компании не только решают сложные бизнес-задачи, но и обеспечивают полную сохранность данных, становясь незаменимыми инструментами в стратегии цифровизации рабочих процессов. Постоянное совершенствование продуктов позволяет соответствовать актуальным потребностям рынка и обеспечивать максимальную эффективность работы партнеров.