Magnus Secure Cloud

Руководство администратора

MAGNUS TECH

Авторские права

Содержание

1. Введение 5
2. Конфигурирование 6
   2.1 Администрирование 6
      2.1.1 Общие настройки системы 6
      2.1.2 Управление пользователями 6
      2.1.3 Управление хранилищем 6
      2.1.4 Отчеты 6
   2.2 Пользовательский функционал 6
3. Вход в систему 7
   3.1 Доступ к системе 7
   3.2 Авторизация локального пользователя 7
   3.3 Авторизация через сервисы аутентификации/авторизации 7
      3.3.1 Авторизация LDAP 8
      3.3.2 Авторизация SSO 8
      3.3.3 Авторизация Active Directory 9
   3.4 Восстановление пароля локальной учетной записи 9
4. Администрирование системы 12
   4.1 Главный экран администратора 12
   4.2 Раздел «Администрирование» 12
      4.2.1 Общие настройки 13
      4.2.2 Настройка аутентификации 15
      4.2.3 Настройка LDAP 16
      4.2.4 Конфигурация SMTP сервера 18
      4.2.5 Управление API-токенами 18
      4.2.6 Настройка СЗИ 19
      4.2.7 Размер хранилища 19
      4.2.8 Лицензия 20
   4.3 Раздел «Управление пользователями» 21
      4.3.1 Историях входов 23
      4.3.2 Размер хранилища 23
      4.3.3 Деактивация учетной записи 24
      4.3.4 Удаление учетной записи 24
   4.4 Раздел «Управление пользовательскими квотами» 24
      4.4.1 История входов 25
      4.4.2 Размер хранилища 25
      4.4.3 Удалить запрос на квоту 26
   4.5 Отчеты 26
      4.5.1 Отчёт «Журнал действий» 26
      4.5.2 Отчёт «Журнал активности» 28

О компании 30

1. ВВЕДЕНИЕ

«Magnus Secure Cloud» (Далее MSC) – это продукт для организации корпоративной виртуальной рабочей среды, предоставляющий сервис совместной и безопасной работы с файлами.

Облачное хранение по принципу on-premise обеспечивает полный контроль доступа к данным и позволяет уменьшить риски потери коммерческой информации.

Обеспечение высокого уровня защиты информации с помощью современных технологий шифрования.

Обеспечение бесшовной интеграции с существующими системами, поддержка роста нагрузки для крупных организаций, а также управление размером хранилища с помощью пользовательских квот и объемов хранилища при исчерпании места.

Легкий доступ к файлам в любое время и из любого места.

Гибкие решения для хранения данных, которые адаптируются под нужды вашего бизнеса.

2. КОНФИГУРИРОВАНИЕ

2.1 Администрирование

2.1.1 Общие настройки системы

- Настройка доменных имен для локальной регистрации/авторизации;
- Настройка LDAP;
- Конфигурация SMTP-сервера;
- Управление лицензиями;
- Настройка количества дней неактивности пользователей для автоматической деактивации;
- Настройка параметров доступа для ссылок и общих папок.

2.1.2 Управление пользователями

- Изменение роли пользователя;
- Настройка квот для отдельных пользователей;
- Деактивация/активация учетных записей;
- Полное удаление учетных записей.

2.1.3 Управление хранилищем

- Настройка/изменение квот хранилища.

2.1.4 Отчеты

- Журнал активности пользователей;
- Журнал действий пользователей.

2.2 Пользовательский функционал

- Загрузка файлов;
- Загрузка папок;
- Операции с файлами и папками;
- Создание и управление ссылками;
- Управление общим доступом;
- Настройки языка и аккаунта.

3. ВХОД В СИСТЕМУ

3.1 Доступ к системе

Доступ к Системе для администраторов и пользователей осуществляется через веб-интерфейс с использованием веб-браузера. Система поддерживает работу со следующими браузерами:

- Microsoft Edge — версия 16 и выше;
- Google Chrome — версия 58 и выше;
- Mozilla — версия 55 и выше;
- Opera — версия 45 и выше;
- Яндекс.Браузер — версия 23 и выше;
- Safari — версия 12.2 и выше.

3.2 Авторизация локального пользователя

При первом доступе к облачному хранилищу Magnus Secure Cloud (MSC) необходимо запустить веб-браузер и перейти по URL-адресу на страницу MSC. Если система была только что развернута, необходимо войти под учетной записью Администратора, используя логин и пароль, указанный в Инструкции по установке (Рисунок 1).

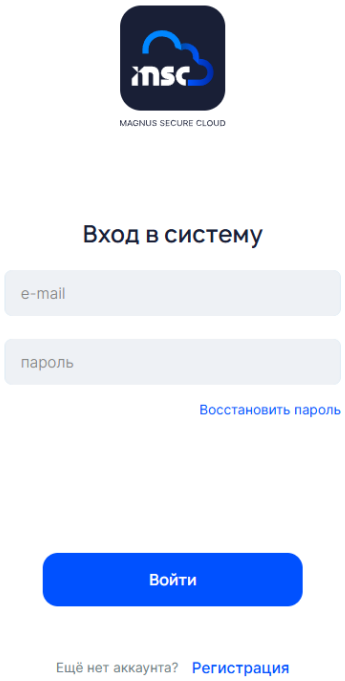

Рисунок 1

3.3 Авторизация через сервисы аутентификации/авторизации

Данные для входа с использованием сервисов аутентификации/авторизации указываются в конфигурационном файле при развертывании системы. Для авторизации

пользователей с помощью протокола LDAP настройки могут быть указаны в том числе в п. 4.2.3 настоящего руководства. При необходимости предоставления доступа внешним пользователям (контрагентам) в рамках локальной регистрации и авторизации необходимо настроить разрешенные доменные имена (см. п. 4.2.2).

При первом входе в систему с использованием любого из методов AD требуется установить пароль для взаимодействия с папками, защищенными сквозным (E2E) шифрованием. Для этого в появившемся окне необходимо ввести и повторить ввод пароля.

3.3.1 Авторизация LDAP

Для входа в систему с помощью LDAP, необходимо на странице авторизации ввести логин и пароль корпоративной учетной записи и нажать кнопку «Active Directory» (Рисунок 2), в случае успешной аутентификации будет осуществлено предоставление доступа к личному кабинету пользователя в MSC.

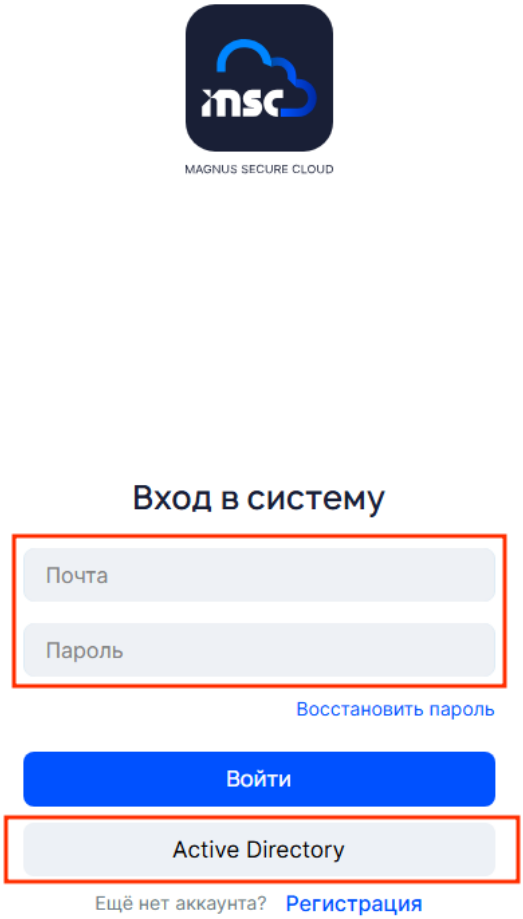

Рисунок 2

3.3.2 Авторизация SSO

Для входа в систему с помощью Single Sign-On (SSO), необходимо на странице авторизации нажать на кнопку «SSO», в открывшемся диалоговом окне ввести логин и пароль корпоративной учетной записи и нажать кнопку «Войти», в случае успешной

аутентификации будет осуществлено предоставление доступа к личному кабинету пользователя в MSC.

3.3.3 Авторизация Active Directory

Для входа в систему с помощью Active Directory, необходимо на странице авторизации нажать на кнопку «Active Directory» (Рисунок 3), в открывшемся диалоговом окне ввести логин и пароль корпоративной учетной записи и нажать кнопку «Войти», в случае успешной аутентификации будет осуществлено предоставление доступа к личному кабинету пользователя в MSC.

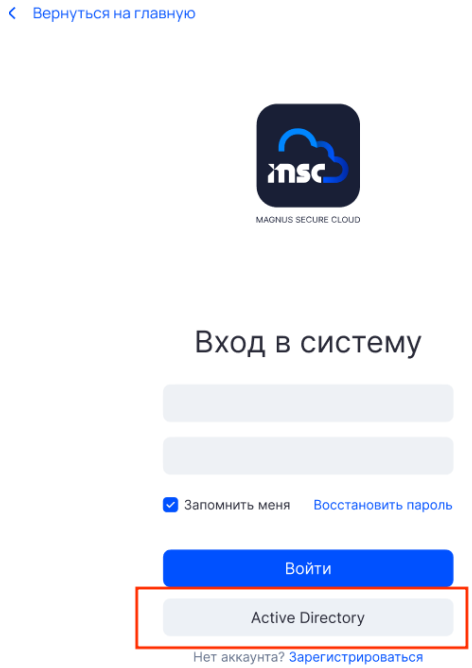

Рисунок 3

3.4 Восстановление пароля локальной учетной записи

В случае утраты пароля локальной учетной записи, при входе на портал необходимо выбрать опцию «Восстановить пароль» (Рисунок 1). Затем требуется ввести логин и нажать кнопку «Следующий шаг» (Рисунок 4).

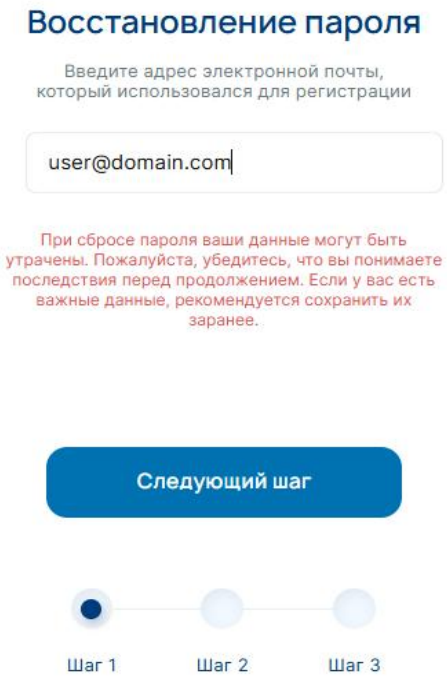

Рисунок 4

На электронную почту будет отправлено письмо с кодом и ссылкой для восстановления пароля. На следующем шаге потребуется ввести шестизначный код, полученный из этого письма (Рисунок 5).

Рисунок 5

На заключительном этапе, необходимо установить пароль, который соответствует установленным критериям сложности, включая требования к длине, регистру и используемым символам (Рисунок 6).

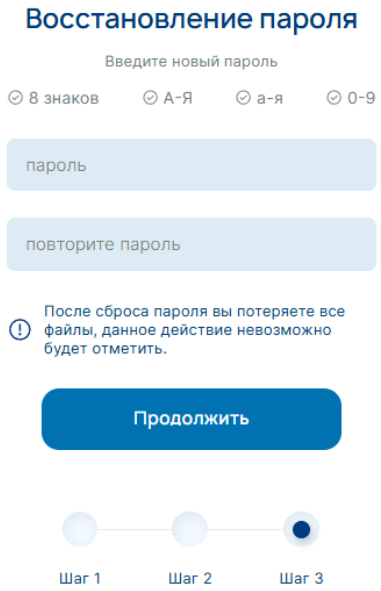

Рисунок 6

В любое время после авторизации имеется возможность сменить пароль локальной учетной записи, перейдя в раздел настройки на главном экране кликнув на иконку:  в правой верхней части экрана.

4. АДМИНИСТРИРОВАНИЕ СИСТЕМЫ

4.1 Главный экран администратора

На главном экране представлены ключевые функции интерфейса для работы с файлами, отображается корневая папка "Мой диск" пользователя, а также логин учетной записи (Рисунок 7). Чтобы перейти в настройки аккаунта пользователя, требуется кликнуть на иконку «шестеренки» в правом верхнем углу. Структуру отображения папок можно изменить на крупные значки, мелкие значки или таблицу, выбрав соответствующий элемент в правом верхнем углу экрана. Более подробная информация о работе с файловым хранилищем и пользовательскими функциями содержится в «Руководстве Пользователя».

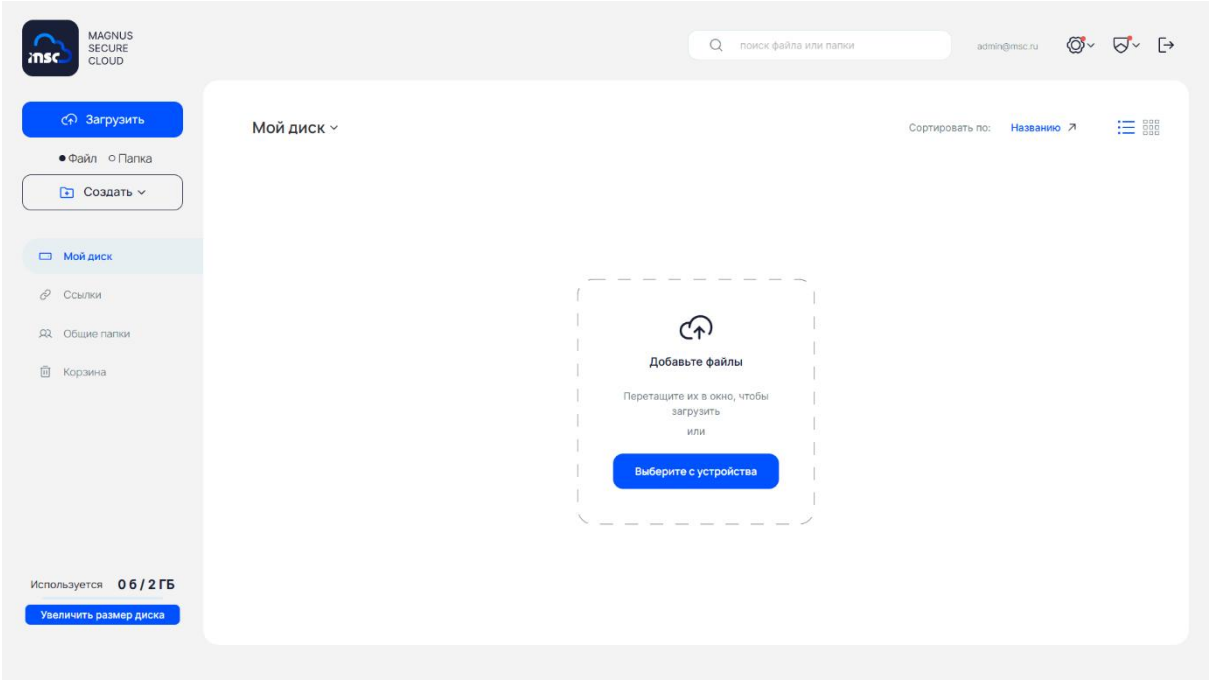

Рисунок 7

4.2 Раздел «Администрирование»

Для перехода в раздел администрирования пользователю с правами администратора необходимо воспользоваться иконкой «щит», расположенной в правом верхнем углу (Рисунок 8).

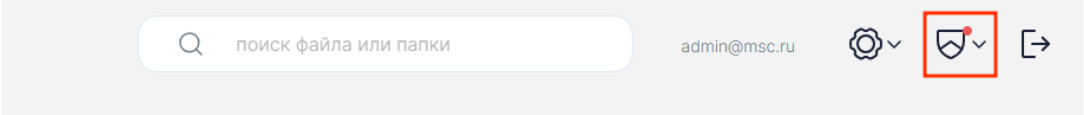

Рисунок 8

Затем, в выпадающем списке необходимо выбрать пункт «Администрирование» (Рисунок 9).

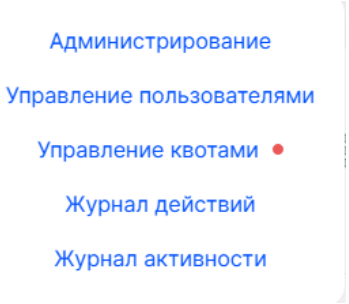

Рисунок 9

Откроется страница администрирования. (Рисунок 10).

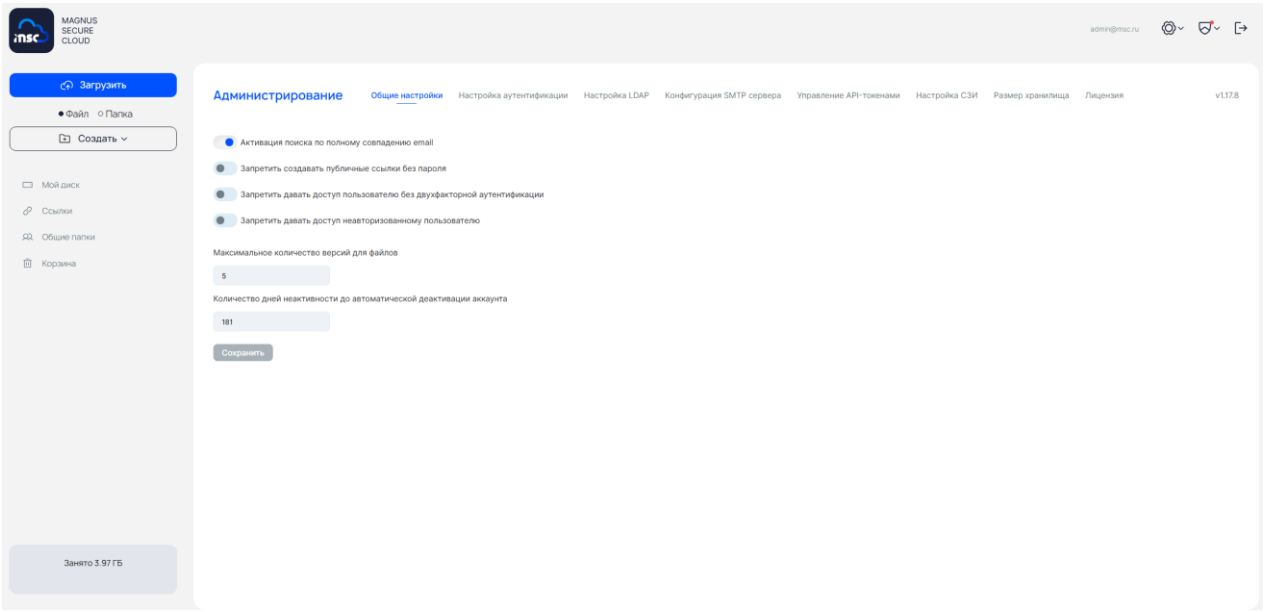

Рисунок 10

В разделе «Администрирование» пользователю доступны:

4.2.1 Общие настройки

В данном подразделе предусмотрена возможность активации следующих функций (Рисунок 12):

- Активация поиска по полному совпадению email. При включении этой функции поиск пользователей в системе — в разделах пользователей хранилища, отвечающих за предоставление доступа другим пользователям, создание групп и прочие действия, — будет выполняться только при вводе полного email-адреса (логина) пользователя. По умолчанию эта функция отключена, и поисковик отображает результаты после ввода первого символа.
- Запрет на создание публичных ссылок без пароля. При создании публичной ссылки система автоматически генерирует уникальный пароль, который владелец должен передать получателю для получения доступа к файлам или папкам;
- Запрет на предоставление доступа неавторизованному пользователю. Доступ к файлам/папкам по ссылке возможен только зарегистрированным в системе пользователям;
- Запрет на предоставление доступа пользователю без двухфакторной аутентификации (2FA).

Предоставление доступа к общим папкам владельца разрешено только зарегистрированным пользователям, у которых активирована 2FA.

При попытке предоставить доступ к папке или добавить пользователя без 2FA в группу, рядом с его email-адресом будет отображаться значок « », при наведении курсора мыши на этот значок появится сообщение: «Доступ можно предоставить только пользователям с включенной двухфакторной аутентификацией» (Рисунок 11), возможность предоставить доступ такому пользователю будет заблокирована;

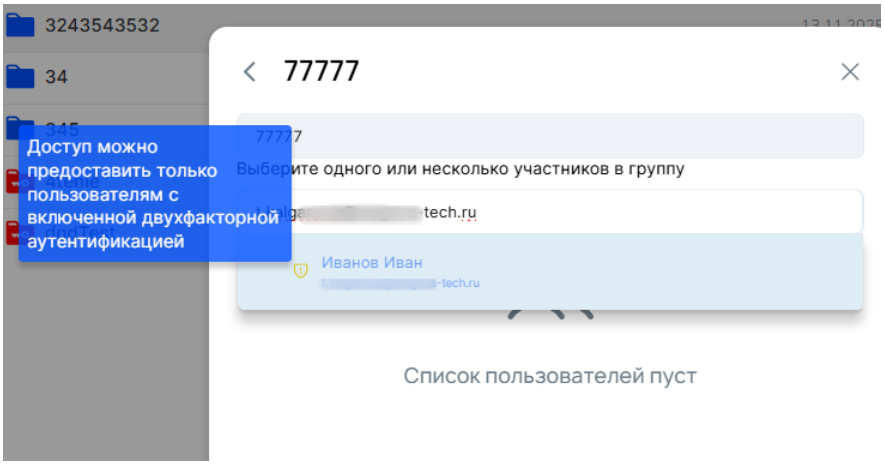

Рисунок 11

- Максимальное количество версий для файлов. Эта настройка определяет лимит версий для файлов пользователей в хранилище. При достижении максимального количества следующая новая версия документа автоматически перезапишет самую старую версию. Если новый лимит установлен ниже предыдущего и у пользователя есть файлы с количеством версий, превышающим этот лимит, старые версии будут удалены для соблюдения установленного максимума при сохранении новой версии файла.
- Количество дней неактивности до автоматической деактивации аккаунта. Эта настройка определяет, через сколько дней без входа в систему учетная запись пользователя будет автоматически деактивирована, если он не осуществлял авторизацию в течение установленного времени.

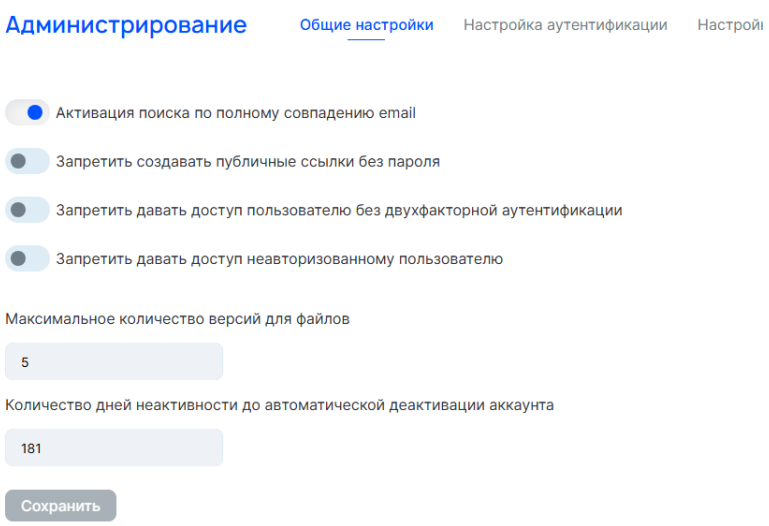

Рисунок 12

4.2.2 Настройка аутентификации

В данном подразделе предусмотрена возможность добавления доверенных доменных имен, а также активация и деактивация уже существующих доменных имен при локальной регистрации/авторизации в системе (Рисунок 13).

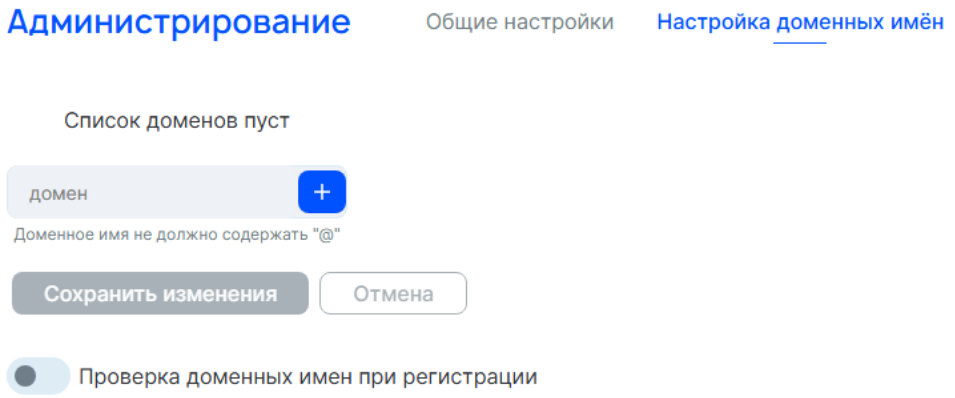

Рисунок 13

- Чтобы включить двухфакторную аутентификацию (2FA) для доверенного домена, необходимо ввести адрес домена, активировать переключатель напротив его имени и сохранить изменения.

В этом случае до момента активации 2FA пользователем, все действия с папками и файлами в хранилище будут заблокированы. В правом нижнем углу экрана будет отображаться сообщение об ошибке (Рисунок 14).

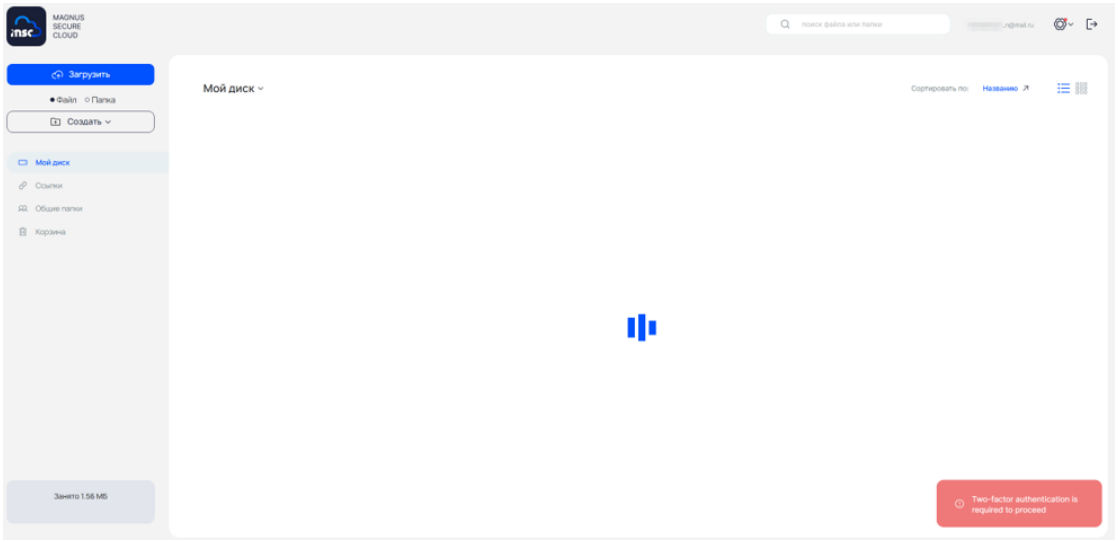

Рисунок 14

- Настройка проверки доменных имен при регистрации и авторизации. Эта функция позволяет пользователям регистрироваться и авторизоваться в системе только с доменов, указанных в списке доверенных доменов (Рисунок 14).
- Активация срока действия сессии. Эта настройка устанавливает срок жизни пользовательской сессии на 24 часа, после истечения которого происходит автоматический выход из системы.

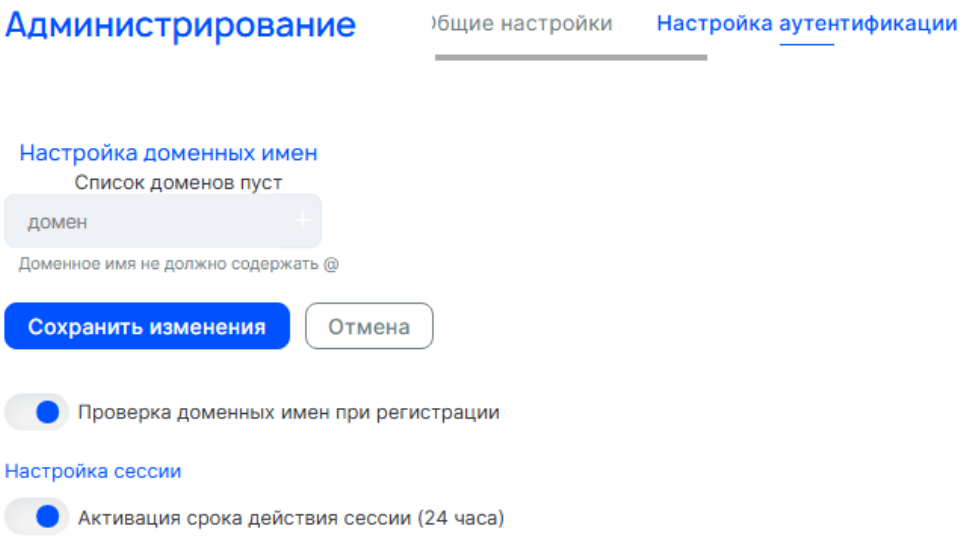

Рисунок 15

4.2.3 Настройка LDAP

В данном подразделе предусмотрены следующие параметры настройки интеграции с LDAP (Рисунок 16).

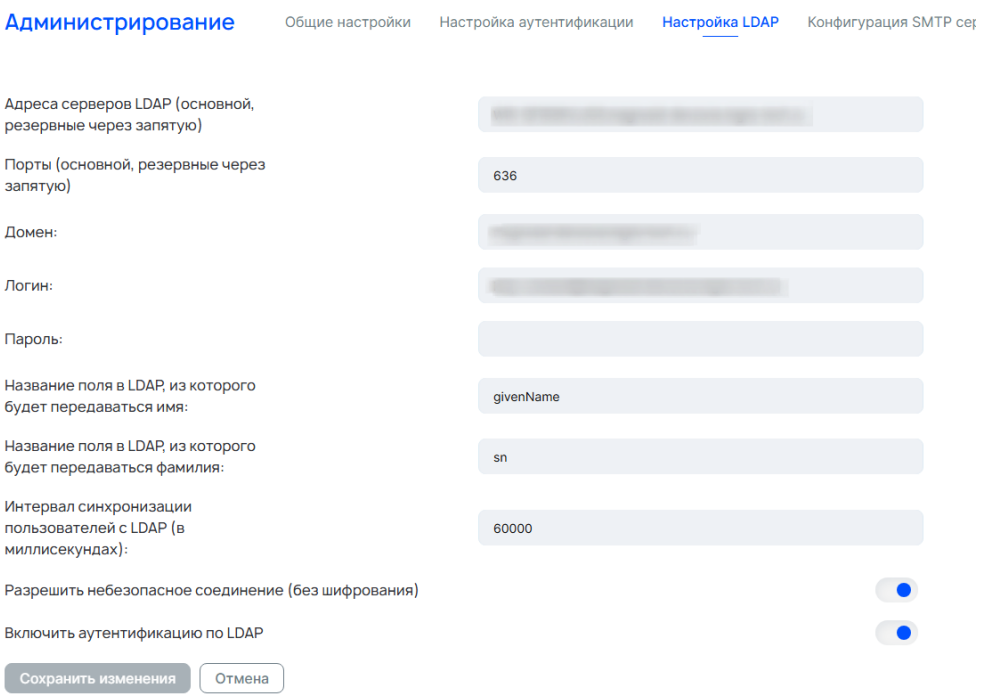

Рисунок 16

- Адреса серверов LDAP - IP-адрес или DNS-имя сервера LDAP, к которому будет подключаться система для синхронизации данных. Это поле обязательно для установления соединения с основным сервером, адреса резервных серверов указываются через запятую после основного и являются необязательными.
- Порты - номера портов для подключения к серверам LDAP. Это поле обязательно для установления соединения с основным сервером, резервные порты указываются через запятую после основного и являются необязательными.
- Домен - домен LDAP или Active Directory (например, example.com), который будет использоваться для поиска и аутентификации пользователей.
- Логин - имя пользователя (логин) с правами доступа к серверу LDAP.
- Пароль - пароль, соответствующий указанному логину. Пароль хранится в зашифрованном виде и необходим для безопасного доступа к LDAP-серверу.
- Название поля в LDAP, из которого будет передаваться имя - название атрибута в LDAP, содержащего имя пользователя (например, "givenName").
- Название поля в LDAP, из которого будет передаваться фамилия - название атрибута в LDAP, содержащего фамилию пользователя (например, "sn").
- Интервал синхронизации пользователей с LDAP (в миллисекундах) - периодичность автоматической синхронизации данных пользователей из LDAP (например, 3600000 мс для одного часа). Это определяет, как часто система будет обновлять информацию о пользователях.
- Разрешить небезопасное соединение (без шифрования) - включите эту опцию, если сервер LDAP не поддерживает шифрование (например, для тестирования). По умолчанию рекомендуется использовать безопасные соединения (LDAPS) для защиты данных.

• Включить аутентификацию по LDAP - активируйте эту настройку, чтобы разрешить пользователям входить в систему с использованием учетных данных из LDAP. При отключении аутентификация будет производиться через внутренние механизмы системы.

После заполнения всех полей необходимо нажать кнопку «Сохранить изменения».

4.2.4 Конфигурация SMTP сервера

В данном подразделе предусмотрена возможность внесения изменений в конфигурацию SMTP-сервера (Рисунок 17).

- SMTP сервер - адрес SMTP-сервера, который будет использоваться для отправки сообщений.
- Порт - номер порта для подключения к SMTP-серверу.
- SMTP логин - имя пользователя (логин) для аутентификации на SMTP-сервере.
- SMTP пароль - пароль, соответствующий логину для аутентификации на SMTP-сервере.
- Разрешить небезопасное соединение - включение или отключение опции для использования незащищенного соединения (без шифрования).
- Модифицированный автор сообщения - адрес электронной почты, который будет отображаться как отправитель сообщений (например, no-reply@example.com).

Для сохранения внесенных изменений необходимо нажать кнопку «Сохранить изменения».

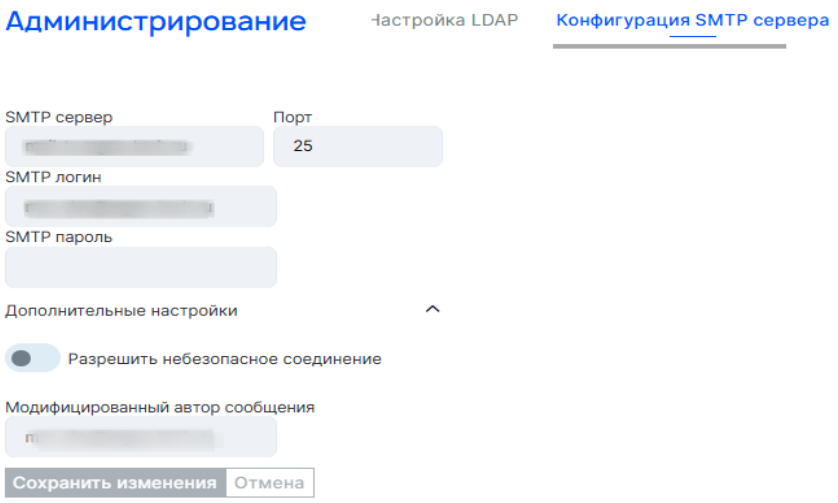

Рисунок 17

4.2.5 Управление API-токенами

API-токен предоставляет возможность отправлять запросы в хранилище с использованием Public API. Токен привязан к учетной записи администратора и обеспечивает аутентифицированный доступ к защищенным ресурсам.

Для генерации нового API-токена необходимо:

- Нажать кнопку «Сгенерировать новый токен». Система отобразит уникальный токен в виде строки символов (Рисунок 18).

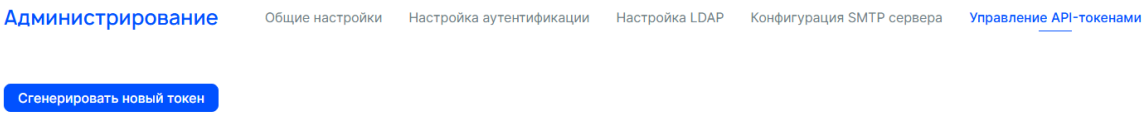

Рисунок 18

- Скопировать отобразившийся токен немедленно, так как он доступен только один раз при генерации и не будет показан повторно.

Для отправки запросов через Public API необходимо включить токен в заголовок HTTP-запроса, использовать формат: Authorization: Bearer <token>, где <token> — это скопированная строка токена, например, в инструментах: cURL или Postman добавить этот заголовок к каждому запросу.

Токен действует бессрочно до момента его удаления на странице генерации. Для удаления токена на странице управления API-токеном нажать кнопку "Удалить" (Рисунок 19).

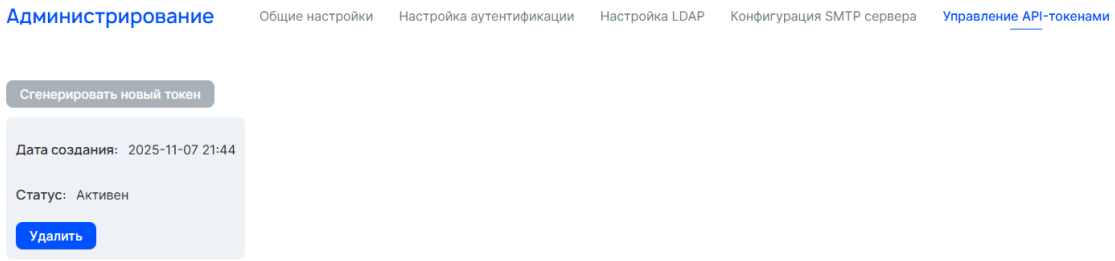

Рисунок 19

4.2.6 Настройка СЗИ

Если установленная версия системы включает антивирусную систему Kaspersky Endpoint Security (KES), то в данном подразделе предоставляется возможность включения функции загрузки файлов пользователями без проверки антивирусом если сервис KES не доступен.

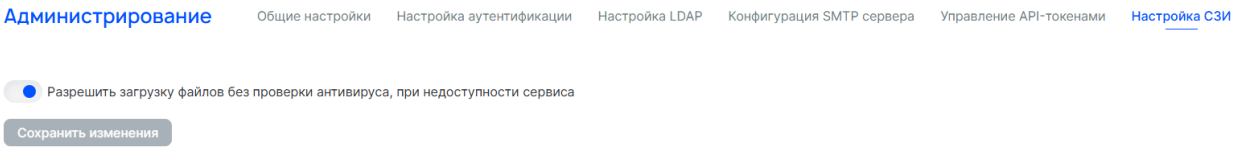

Рисунок 20

4.2.7 Размер хранилища

В данном подразделе предусмотрена возможность настройки объема дискового пространства в гигабайтах (ГБ), доступного для пользователей системы. При активации

опции "Безлимитное" размер хранилища становится неограниченным для всех пользователей (Рисунок 21).

Для установления конкретного размера хранилища (в ГБ) необходимо:

- Ввести числовое значение в соответствующем поле, нажать кнопку "Сохранить изменения" для применения настроек. Изменения вступят в силу немедленно, у пользователей в личном кабинете отобразится установленный размер хранилища.

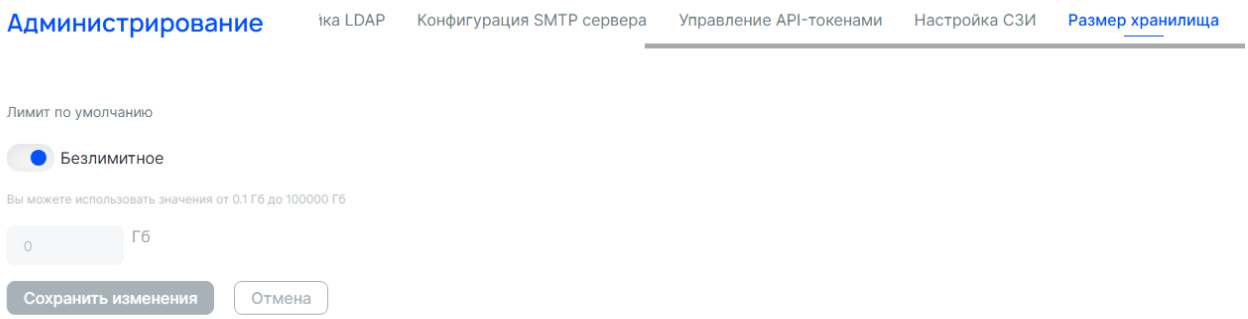

Рисунок 21

4.2.8 Лицензия

В данном подразделе представлена информация о действующей лицензии и ее параметрах (Рисунок 22).

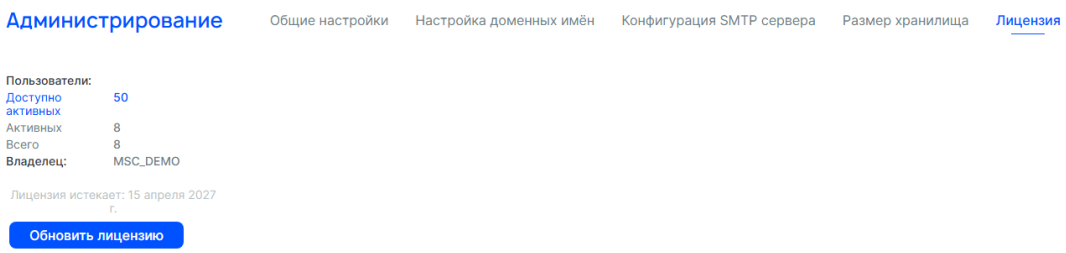

Рисунок 22

Для обновления лицензии необходимо выполнить следующие действия:

- Скачать лицензионный файл, предоставленный по одноразовой ссылке.
- Открыть файл и скопировать лицензионный ключ.
- На странице подраздела «Лицензии» нажать кнопку «Обновить лицензию» (Рисунок 23).

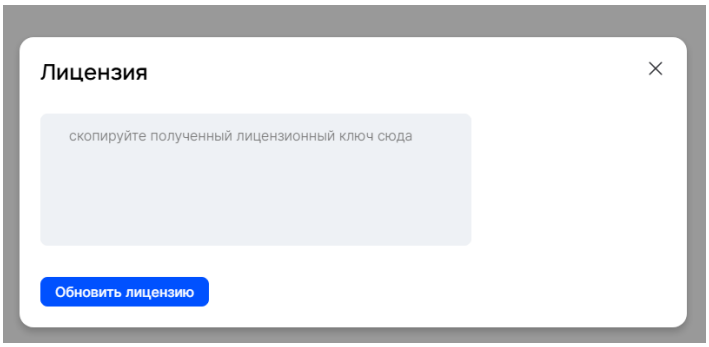

Рисунок 23

- В открывшемся диалоговом окне вставить скопированный лицензионный ключ (Рисунок 24) и нажать кнопку «Обновить лицензию».

Рисунок 24

4.3 Раздел «Управление пользователями»

Для перехода в раздел «Управления пользователями» необходимо выбрать соответствующий раздел нажав на иконку «».

Раздел «Управление пользователями» содержит информацию о пользователях (Рисунок 25):

- Логин – адрес электронной почты пользователя, используемый для входа в систему;
- ФИО – полное имя пользователя в формате «Фамилия Имя Отчество»;
- Активность – показывает текущий статус учетной записи пользователя;
- Последний вход – дата и время последней успешной авторизации пользователя в системе;
- Квота (Гб) – определяет максимальный размер персонального хранилища пользователя в гигабайтах. Если ограничения на размер хранилища отсутствуют, отображается значение «Безлимит»;
- Хранилище – показывает объем занятого пространства в персональном хранилище пользователя в гигабайтах или мегабайтах, значение рассчитывается на основе загруженных файлов;
- Файлы – указывается общее количество файлов, хранящихся в персональном хранилище пользователя, это включает все типы файлов (документы, изображения, видео и т.д.);

- 2FA – отображает статус подключения двухфакторной аутентификации (2FA) для учетной записи пользователя;
- Роль – указывается роль пользователя в системе, определяющая уровень доступа и полномочий («Администратор» или «Пользователь»).

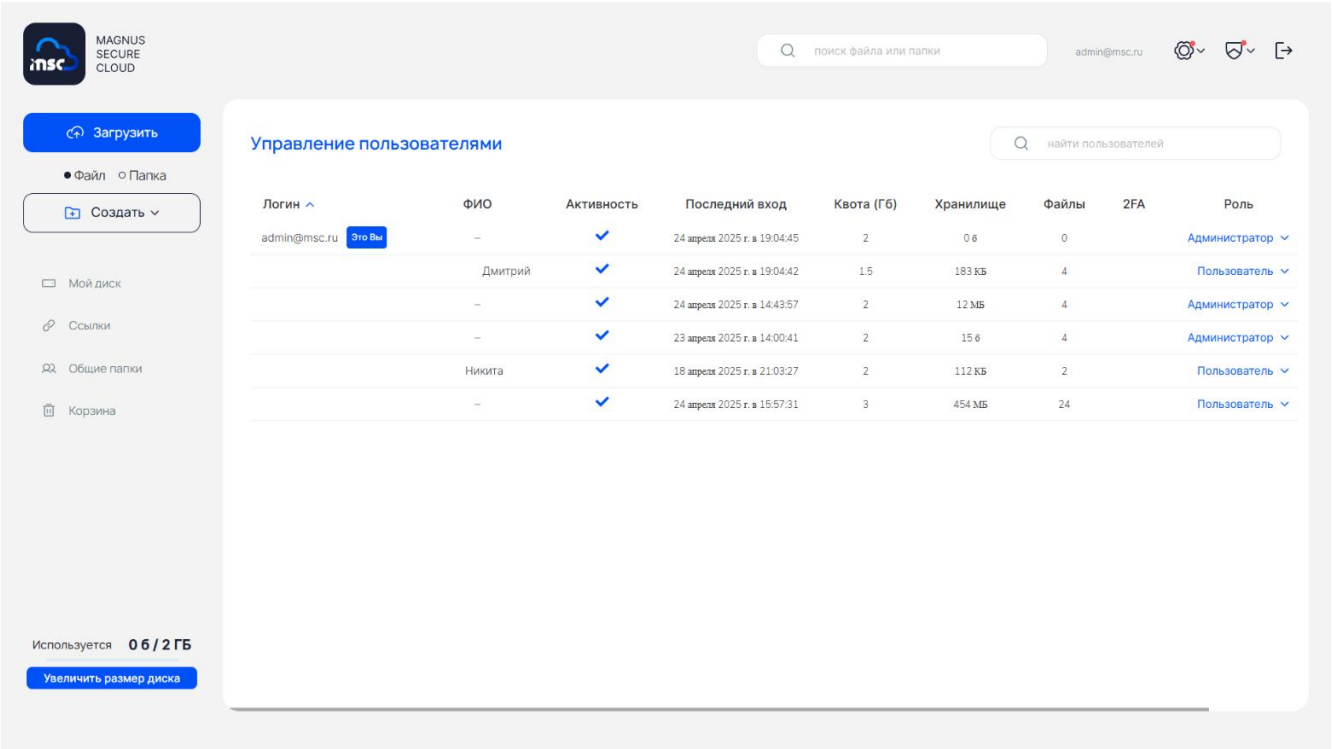

Рисунок 25

Администратор имеет возможность менять роль учётных записей, нажав на соответствующее поле (Рисунок 26).

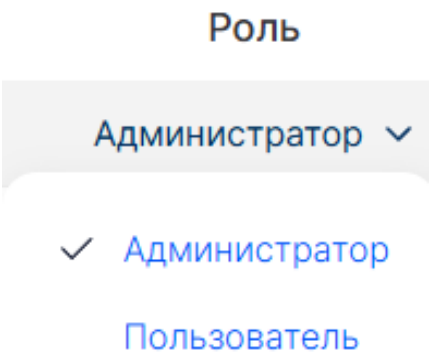

Рисунок 26

Также администратор имеет возможность взаимодействия с учётными записями с помощью меню действий (Рисунок 27).

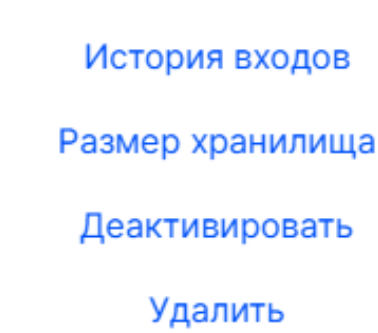

Рисунок 27

4.3.1 Историях входов

В данном подразделе хранится информация об активности пользователя (Рисунок 28).

Рисунок 28

4.3.2 Размер хранилища

В данном подразделе хранится информация о размере хранилища пользователя, в данном окне администратор может редактировать доступный размер хранилища пользователя (Рисунок 29).

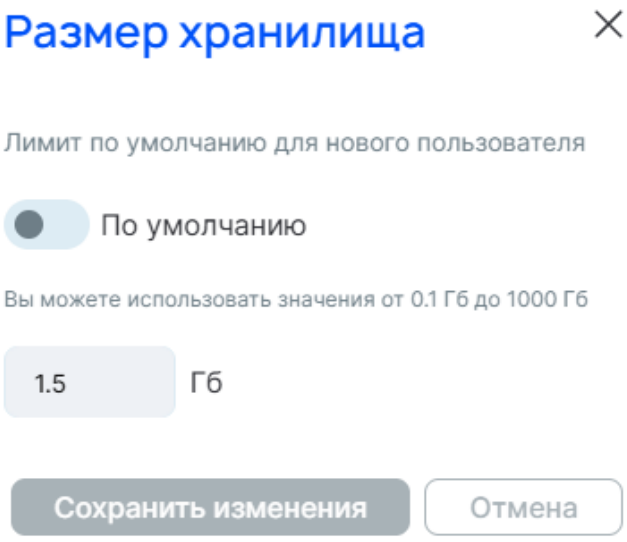

Рисунок 29

4.3.3 Деактивация учетной записи

Данная функция позволяет временно отключить учетную запись пользователя.
При этом:

- Содержимое хранилища не удаляется;
- Доступ к данным блокируется на время деактивации;
- Предусмотрена возможность восстановления доступа (активация);
- После активации все файлы и папки снова становятся доступными пользователю.

4.3.4 Удаление учетной записи

Данная функция позволяет удалить учётную запись пользователя.

4.4 Раздел «Управление пользовательскими квотами»

Данный раздел содержит в себе информацию о пользовательских заявках на увеличение объемов хранилища пользователями и данные о пользователе (Рисунок 30):

- Логин;
- ФИО;
- Активность;
- Последний вход;
- Квота (Гб);
- Хранилище;
- Файлы;
- Роль.

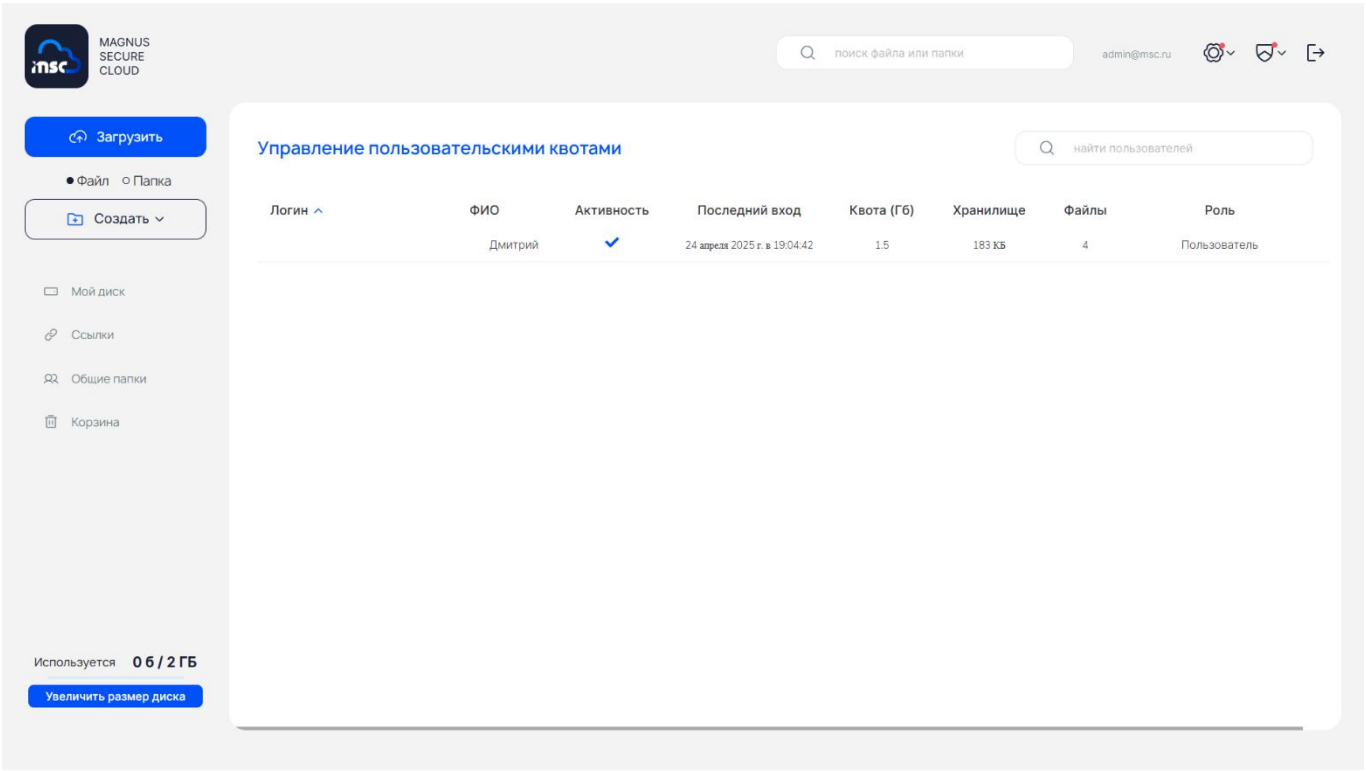

Рисунок 30

С помощью меню действий администратору доступны кнопки (Рисунок 31):

- История входов;
- Размер хранилища;
- Удалить запрос на квоту.

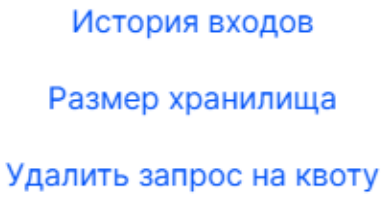

Рисунок 31

4.4.1 История входов

В данном подразделе хранится информация об активности пользователя (Рисунок 32), отображает дата и время последнего входа в систему и IP адрес компьютера, с которого был осуществлен вход.

Рисунок 32

4.4.2 Размер хранилища

В данном подразделе отображается информация о запрошенном пользователем новом размере хранилища.

Администратор может выполнить одно из следующих действий:

- Подтвердить увеличение лимита хранилища без изменения значения в поле «Гб», нажав кнопку «Сохранить изменения»;
- Ввести в поле ввода размера хранилища собственные значения и нажать кнопку «Сохранить изменения»;
- Закрыть запрос без изменений, нажав на иконку крестика (в этом случае запрос останется в списке необработанным (Рисунок 33).

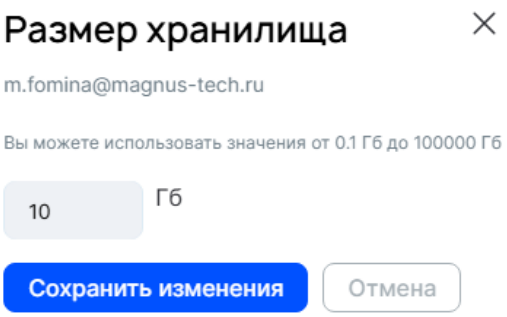

Рисунок 33

4.4.3 Удалить запрос на квоту

С помощью данной функции администратор может удалить заявку пользователя на увеличение квоты.

4.5 Отчеты

В системе доступно формирование отчетов:

- «Журнал действий»;
- «Журнал активности».

Для просмотра отчета необходимо в выпадающем списке при нажатии на иконку « » (щит) выбрать нужный отчет (Рисунок 34).

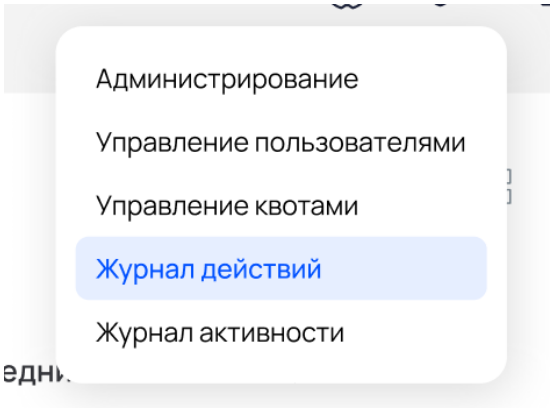

Рисунок 34

4.5.1 Отчёт «Журнал действий»

Содержит информацию о действиях пользователя в отношении файлов и папок. В данном отчёте отображаются все операции, связанные с созданием, изменением, переименованием, удалением, скачиванием и предпросмотром.

Отчёт представлен в табличном виде со следующими столбцами (Рисунок 35):

- Дата и время – дата и время выполнения события;
- Пользователь – ФИО пользователя, осуществившего действие;
- Логин – логин пользователя, осуществившего действие (адрес электронной почты, используемый для входа в систему);
- Тип объекта – тип элемента, с которым производились действия (например, «Файл» или «Папка»);

- Имя объекта – название элемента, с которым производились действия;
- Действие – действие, которое было применено;
- Владелец папки – ФИО пользователя — владельца папки, в отношении которой было осуществлено действие;
- Логин владельца – логин пользователя — владельца папки, в отношении которой было осуществлено действие (адрес электронной почты);
- Имя папки – название папки, в отношении которой было осуществлено действие;
- IP пользователя – IP–адрес устройства, с которого было выполнено действие.

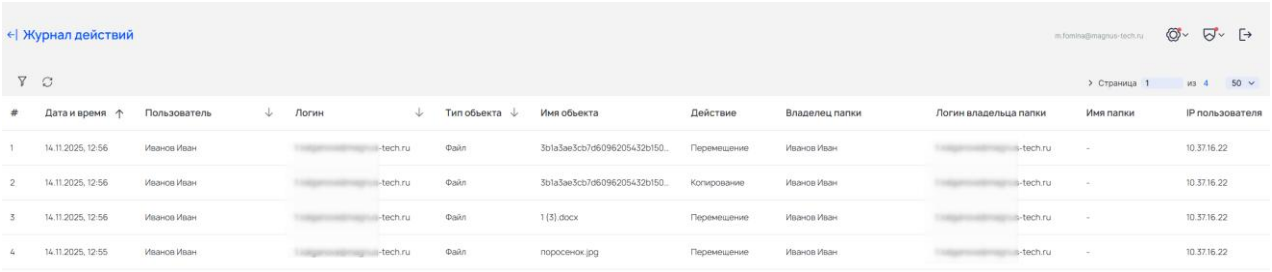

Рисунок 35

В левой верхней части страницы расположен фильтр, позволяющий сформировать отчёт по конкретному пользователю(-ям), по пользователю(-ям) — владельцу(-ам) папки, по типу объекта, по действию или за заданный период времени. Для применения фильтрации необходимо задать значения в соответствующих полях и нажать кнопку «Применить».

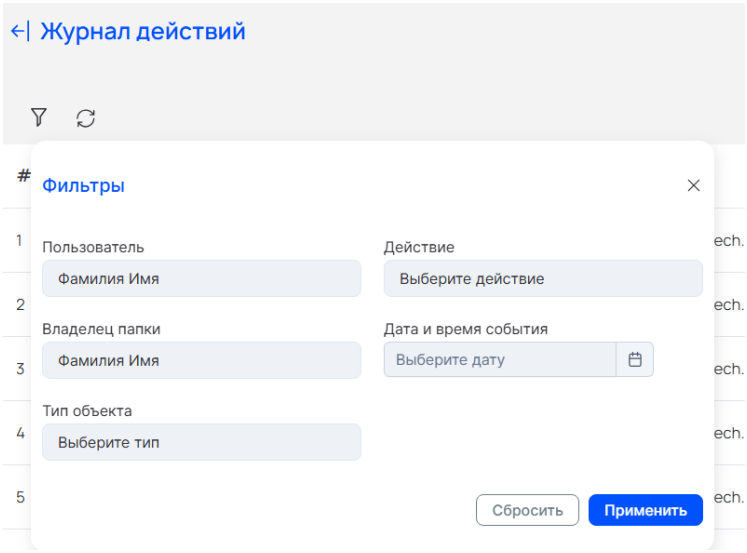

Рисунок 36

Сортировка записей по убыванию или возрастанию значений осуществляется нажатием на заголовок соответствующего столбца табличного представления. Последовательные нажатия на заголовок столбца изменяют порядок сортировки; индикатором служит пиктограмма стрелки:

- Стрелка вниз: упорядочивание записей по убыванию значений столбца.
- Стрелка вверх: упорядочивание записей по возрастанию значений столбца.

4.5.2 Отчёт «Журнал активности»

Предоставляет информацию о IP-адресах, времени входа и выхода из системы, типе авторизации, изменении роли пользователя, активации и деактивации пользователей. В данном отчёте отображаются операции, связанные с входом в систему, выходом из неё, а также административными действиями, такими как изменение ролей или статуса активности пользователей.

Отчёт представлен в табличном виде со следующими столбцами:

- Дата и время – дата и время осуществления действия в системе;
- Пользователь – ФИО пользователя, осуществившего действие (например, вход или выход из системы) либо в отношении которого было выполнено действие (например, изменение роли или установка статуса «Активен/Неактивен»);
- Логин – логин пользователя, осуществившего действие (адрес электронной почты, используемый для входа в систему) либо в отношении которого было выполнено действие (например, изменение роли или установка статуса «Активен/Неактивен»);
- Действие – действие, которое было осуществлено;
- Тип авторизации – тип авторизации пользователя в системе;
- IP пользователя – IP–адрес устройства, с которого было выполнено действие.
- OS – операционная система компьютера, с которого было выполнено действие.

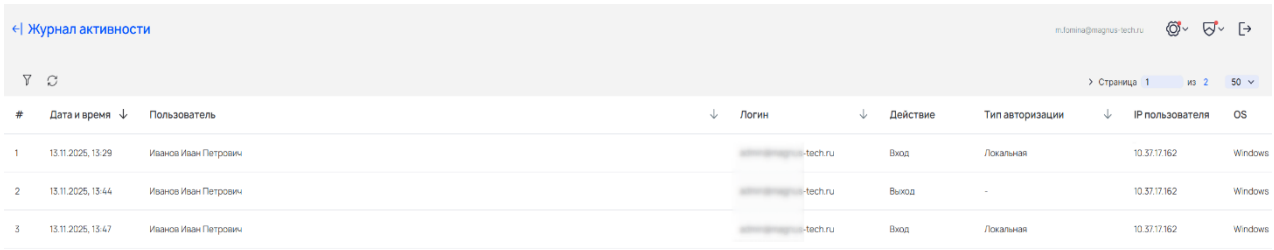

Рисунок 37

В левой верхней части страницы расположен фильтр, позволяющий сформировать отчёт по конкретному пользователю(-ям), по действию или за заданный период времени. Для применения фильтрации необходимо задать значения в соответствующих полях и нажать кнопку «Применить» (Рисунок 38).

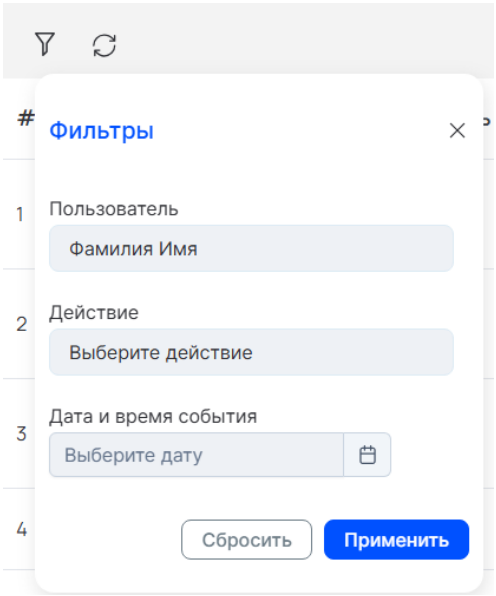

Рисунок 38

Сортировка записей по убыванию или возрастанию значений осуществляется нажатием на заголовок соответствующего столбца табличного представления. Последовательные нажатия на заголовок столбца изменяют порядок сортировки; индикатором служит пиктограмма стрелки:

- Стрелка вниз: упорядочивание записей по убыванию значений столбца.
- Стрелка вверх: упорядочивание записей по возрастанию значений столбца.

О КОМПАНИИ

ООО «МАГНУС ТЕХ» (ОГРН 1217700002959) - 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.

Связаться с нами:
Адрес: 105082, г. Москва, ул. Большая Почтовая, д 36 стр. 1
Тел: +7 499 350 66 15
e-mail: info@Magnus-tech.ru
Magnus-tech.ru