Руководство администратора

по настройке и администрированию АльтерОфис Веб 2026.1.0.0

Страниц 185

ООО «АЛМИ Партнер»
апрель 2026 г.

Оглавление

1.Введение

1.1. Назначение документа

Настоящий документ предназначен для администраторов системы и описывает порядок настройки и администрирования **АльтерОфис Веб**.

Документ содержит информацию о структуре системы, её компонентах, механизмах интеграции с внешними службами (LDAP, почтовыми серверами), а также описание процедур обеспечения безопасности и мониторинга.

Документ служит:

- Руководством при первичной настройке и конфигурации системы;
- Методическим пособием по сопровождению и обновлению;
- Основанием для проверки соответствия настроек корпоративным требованиям.

1.2. Область применения

Руководство применяется при настройке и администрировании **АльтерОфис Веб** в организациях, использующих систему для:

- совместного доступа к файлам и документам;
- совместной работы над документами с использованием веб-версий офисных редакторов;
- организации защищённого обмена данными между пользователями и филиалами;
- подключения внешних каталогов пользователей (LDAP/Active Directory).

Документ может использоваться:

- системными администраторами;
- специалистами по информационной безопасности;
- инженерами по DevOps/инфраструктуре.

1.3. Перечень программной и эксплуатационной документации

При эксплуатации системы **АльтерОфис Веб** администраторам системы могут потребоваться следующие документы:

- «Руководство администратора по развертыванию системы АльтерОфис Веб».
- «Руководство администратора по настройке и администрированию АльтерОфис Веб» (настоящий документ).
- «Руководство пользователя по АльтерОфис Веб».
- «Руководство пользователя по АльтерОфис Редакторы».

2.Общие сведения о системе

2.1. Назначение системы

Система **АльтерОфис Веб** предназначена для организации корпоративного хранилища данных с возможностью совместного доступа, синхронизации, редактирования документов и интеграции с другими ИТ-сервисами.

АльтерОфис Веб обеспечивает:

- хранение файлов и управление версиями;
- контроль доступа на уровне пользователей и групп;
- совместную работу с документами через веб-интерфейс;
- интеграцию с LDAP/AD, почтовыми серверами и офисными редакторами.

2.2. Основные функции и возможности

- Управление пользователями и группами;
- Контроль прав доступа к файлам и папкам;
- Совместное редактирование документов в режиме реального времени;
- Настройка уведомлений и интеграция с почтовыми сервисами;
- Поддержка федеративного обмена между организациями;
- Аудит, журналирование и мониторинг событий безопасности.

2.3. Поддерживаемые платформы и требования

Перечень рекомендаций к аппаратному и программному обеспечениям см. в документе:

- «Руководство администратора по развертыванию системы АльтерОфис Веб»

2.4. Уровень подготовки пользователей (администраторов системы)

Функциональные обязанности администратора включают:

- Управление общесистемным и дополнительным программным обеспечением, установленным в инфраструктуре АльтерОфис Веб;
- Управление правами доступа и привилегиями пользователей:
  - Создание и управление группами пользователей, определение ролей и прав доступа на уровне групп;
  - Распределение полномочий и прав доступа к файлам, папкам и другим ресурсам системы между отдельными пользователями;
  - Контроль соблюдения политики безопасности при предоставлении доступа.

Требования к квалификации администратора:

- Практический опыт установки, настройки и администрирования программных средств;

- Опыт работы с LDAP/Active Directory, настройкой единого входа (SSO/SAML/OAuth2), сертификатами и HTTPS;
- Понимание механизмов управления пользователями и группами, прав доступа и ведения системного журнала (логирования) безопасности.

3.Начало работы с АльтерОфис Веб

При установке Системы, создается учетная запись пользователя **admin** и задается пароль администратора. Рекомендуется создавать пароль с учетом политики безопасности организации (например: длина не менее 12 символов, наличие букв, цифр и специальных символов).

При необходимости, заданный при установке пароль для пользователя **admin** может быть изменен.

3.1. Вход в систему

Для входа в Систему необходимо открыть веб-браузер и ввести в адресной строке ссылку[1] на Систему, которая была получена при развертывании Системы.

Откроется страница входа в Систему.

На форме входа введите логин администратора и временный пароль.

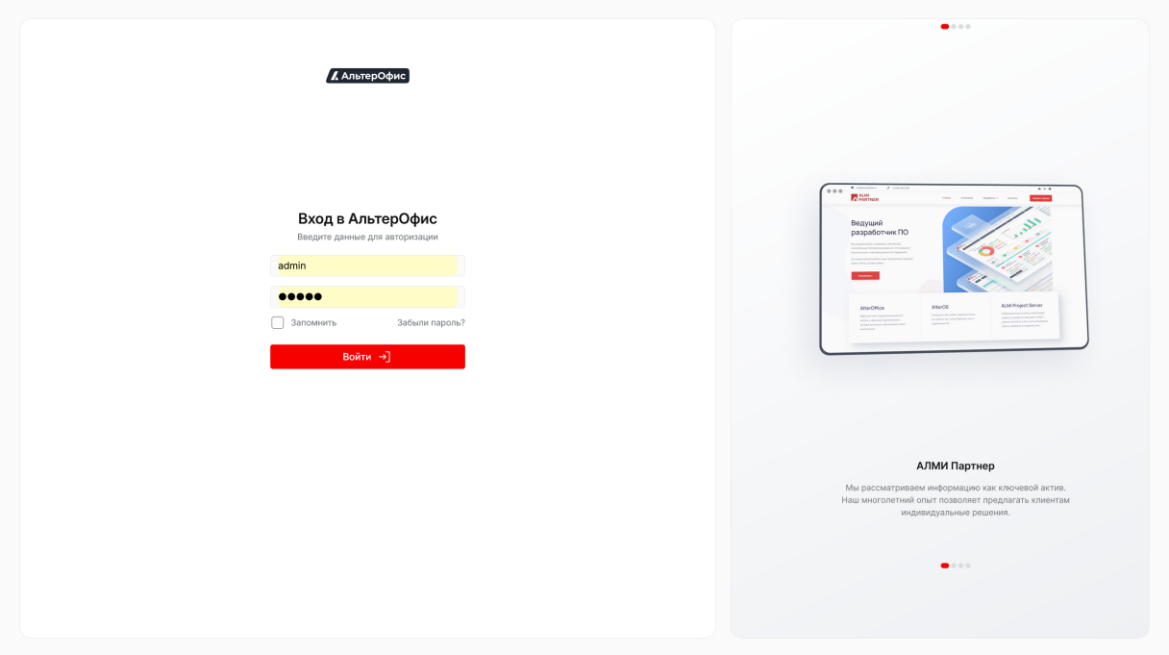


Рисунок 1. Форма авторизации администратора

Нажмите **Войти**.

При успешном входе в Систему откроется приветственная страница.

[1] Обычно адрес ссылки выглядит следующим образом: https://web2025.alteroffice.ru

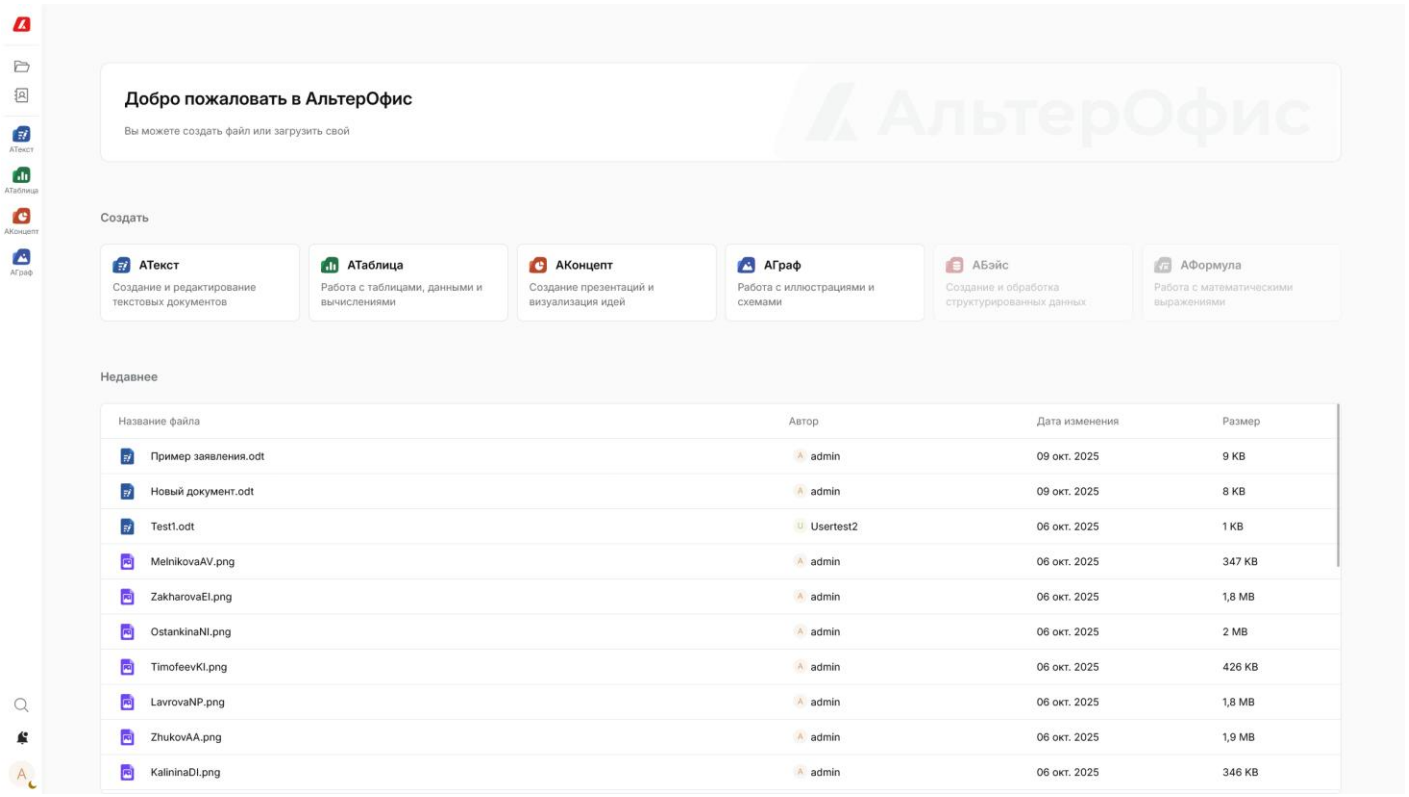


Рисунок 2. Приветственная страница администратора

3.2. Смена временного пароля

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт «Учетные записи».

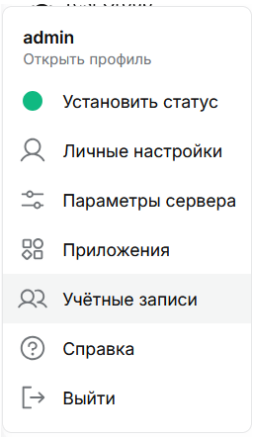


Рисунок 3. Меню администратора

Откроется страница со списком пользователей.

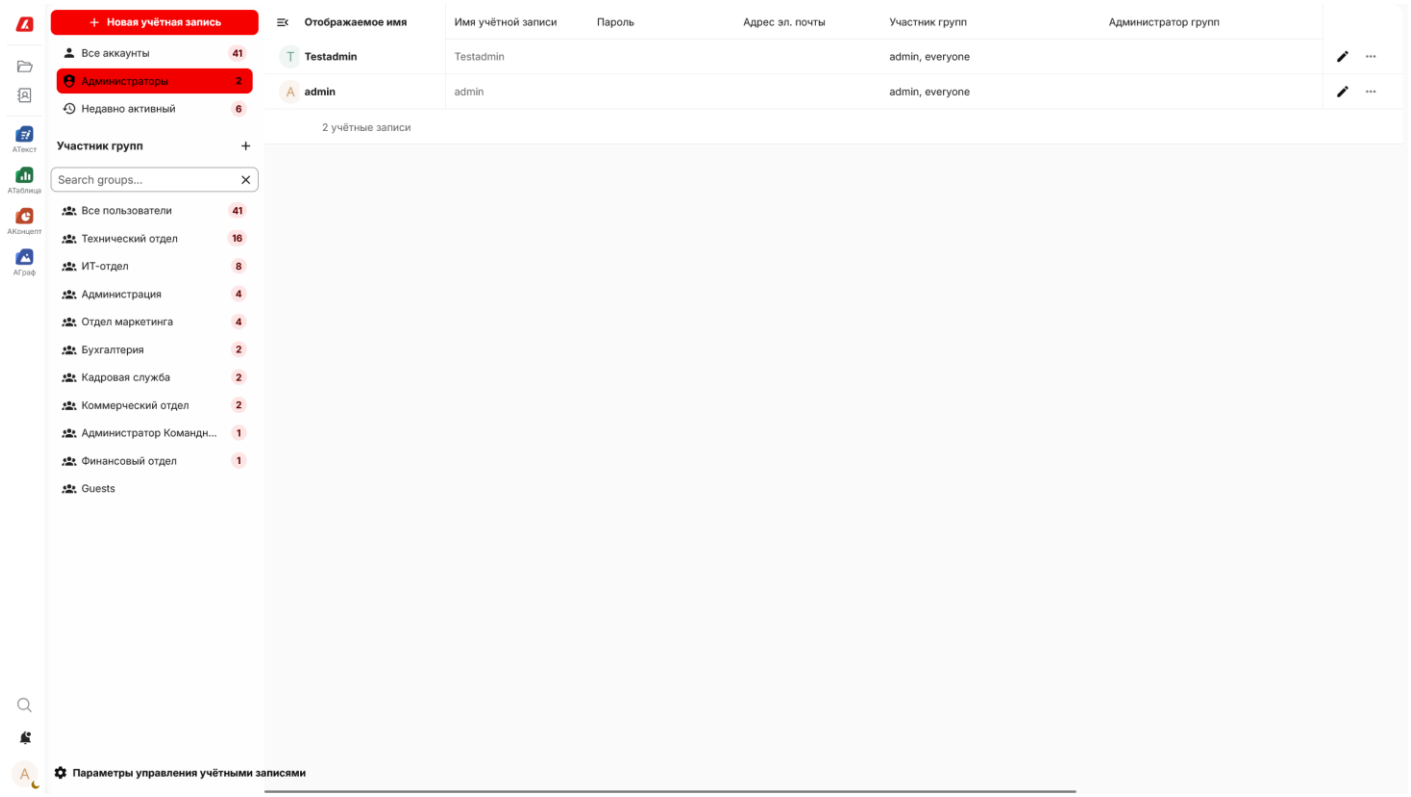


Рисунок 4. Список пользователей

Нажмите на иконку «Карандаш» справа от пользователя **admin**.

Введите новый пароль в поле **Пароль**.

Нажмите на иконку для подтверждения пароля.

> СОВЕТ
>
> - Пароль должен соответствовать политике безопасности организации (например: длина не менее 12 символов, наличие букв, цифр и специальных символов).

3.3. Порядок проверки работоспособности

Система **АльтерОфис Веб** считается работоспособной при выполнении следующих условий:

- Доступ к веб-интерфейсу осуществляется по HTTPS без ошибок;
- Авторизация под учетной записью администратора проходит успешно;
- Смена временного пароля выполняется корректно;
- Интерфейс открывает разделы «Файлы» и «Пользователи» без ошибок.

3.4. Возможные ошибки и рекомендации

Ошибка	Причина	Рекомендации
Невозможно войти	Неправильный логин или пароль	Проверьте корректность введённых данных; убедитесь, что пароль введён с учётом регистра символов

Ошибка	Причина	Рекомендации
Страница недоступна	Проблемы с HTTPS или DNS	Проверьте работу веб-сервера и доступность порта 443
Пароль не соответствует требованиям	Политика безопасности не соблюдена	Используйте пароль длиной не менее 12 символов с буквами, цифрами и спецсимволами

4.Описание операций

4.1. Работы по настройке системы

Для начала работы пользователей организации с системой **АльтерОфис Веб** рекомендуется выполнить следующие действия:

1) Настройка почтового сервера. См. «Настройка почтового сервера для рассылки уведомлений».
2) Настройка параметров предоставления общего доступа. См. «Настройка параметров предоставления пользователями общего доступа».
3) Настройка хранилища и внешних источников. См. «Управление внешними хранилищами».
4) Настройка аутентификации. См. «Аутентификация и безопасность» и «Интеграция с каталогами пользователей».
5) Настройка групп пользователей. См. «Настройка пользователей и групп».
6) Настройка пользователей. См. «Настройка пользователей и групп».

4.2. Настройка почтового сервера для рассылки уведомлений

Настройка почтового сервера в **АльтерОфис Веб** позволяет системе автоматически отправлять уведомления пользователям — о совместном доступе к файлам, изменениях документов, запросах на регистрацию, сбросе паролей и других событиях. Пользователи сами выбирают, какие уведомления они хотят получать.

ПРИМЕЧАНИЕ

- Для отправки писем необходимо иметь работающий почтовый сервер.
- Настройки почтового сервера можно настроить через веб-интерфейс или конфигурационный файл (config.php).

Когда использовать

- При необходимости отправки уведомлений пользователям о событиях в системе (приглашения, уведомления, напоминания).
- Для восстановления пароля через электронную почту.
- В корпоративных средах с централизованной почтовой инфраструктурой (SMTP/STARTTLS/SMTPS).

Шаги выполнения

1. Откройте раздел «Основные параметры»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт **«Параметры сервера»**.

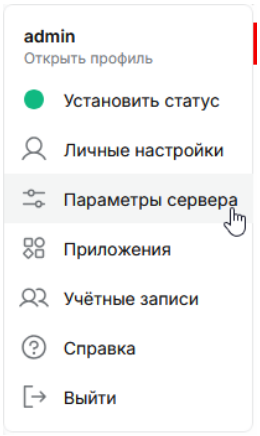


Рисунок 5. Меню администратора

В разделе **«Параметры сервера»** выберите пункт **«Основные параметры»**.

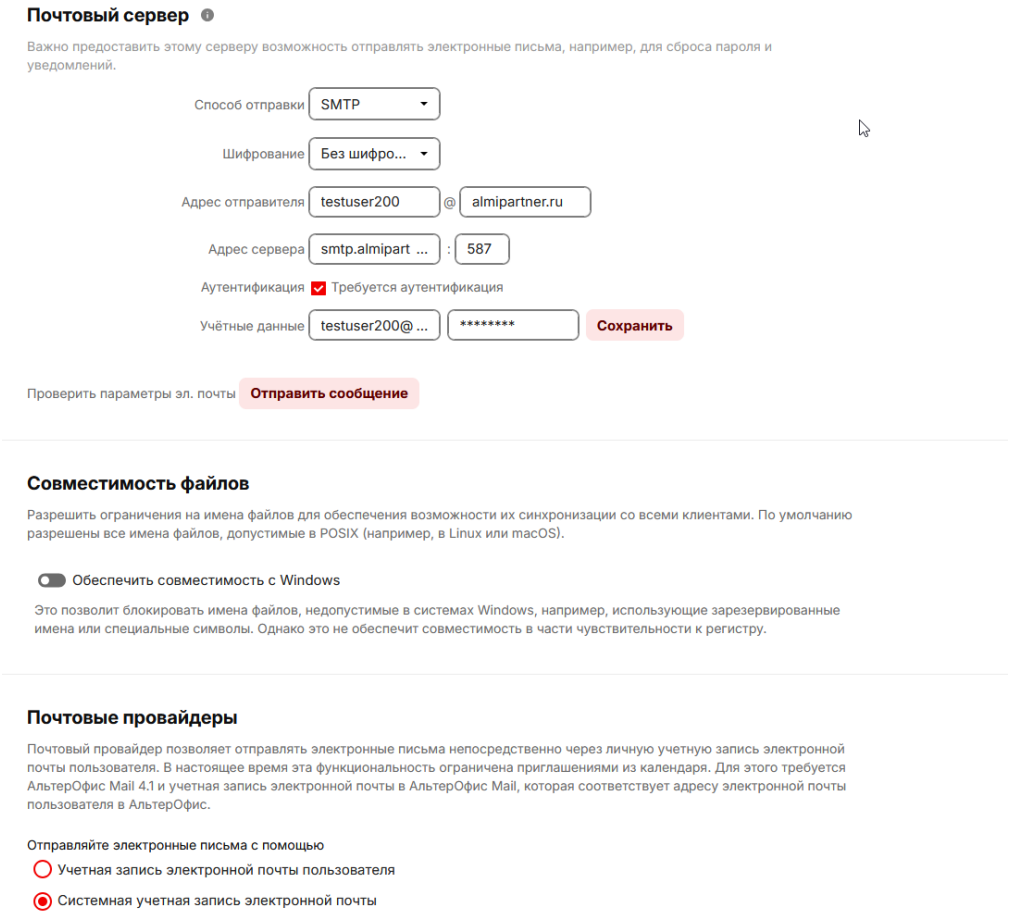


Рисунок 6. Настройка подключения к почтовому серверу

2. Переход к настройкам почтового сервера

Пролистайте страницу до раздела **«Почтовый сервер»**.

3. Настройка параметров SMTP-сервера

В разделе «Почтовый сервер» введите следующие данные:

Поле	Описание	Пример
Способ отправки	Режим отправки почты	SMTP
Шифрование	Выберите **SSL** или **Без шифрования/STARTTLS**. При выборе **Без шифрования/STARTTLS**, STARTTLS будет использоваться автоматически, если почтовый сервер его поддерживает.	Без шифрования/STARTTLS
Адрес отправителя	Адрес отправителя, от имени которого будут уходить уведомления. Адрес отправителя (до @)	aow
	Домен исходящей почты	almipartner.ru
Адрес сервера	Доменное имя или IP сервера	smtp.almipartner.ru
Порт	**465** для SMTPS или **587** STARTTLS. Если используется нестандартный порт, укажите его.	587
Аутентификация	Необходимость аутентификации.	Да
Учетные данные	Имя пользователя SMTP	aow@almipartner.ru
	Пароль пользователя SMTP	aow_password

Для сохранения настроек нажмите кнопку **Сохранить**.

4. Проверка отправки сообщений

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт **«Личные настройки»**.

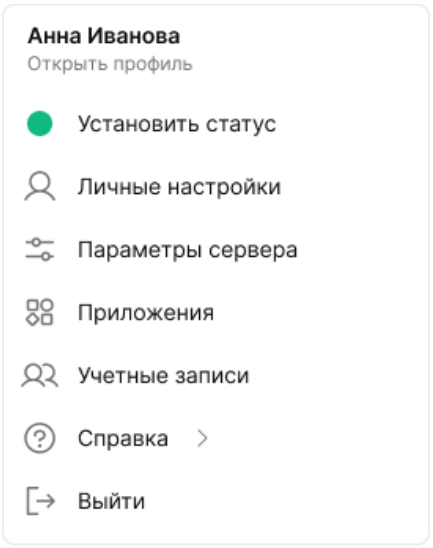


Рисунок 7. Меню администратора

В разделе **«Параметры пользователя** в подразделе **«Личная информация»** укажите адрес электронной почты на который придет проверочное письмо.

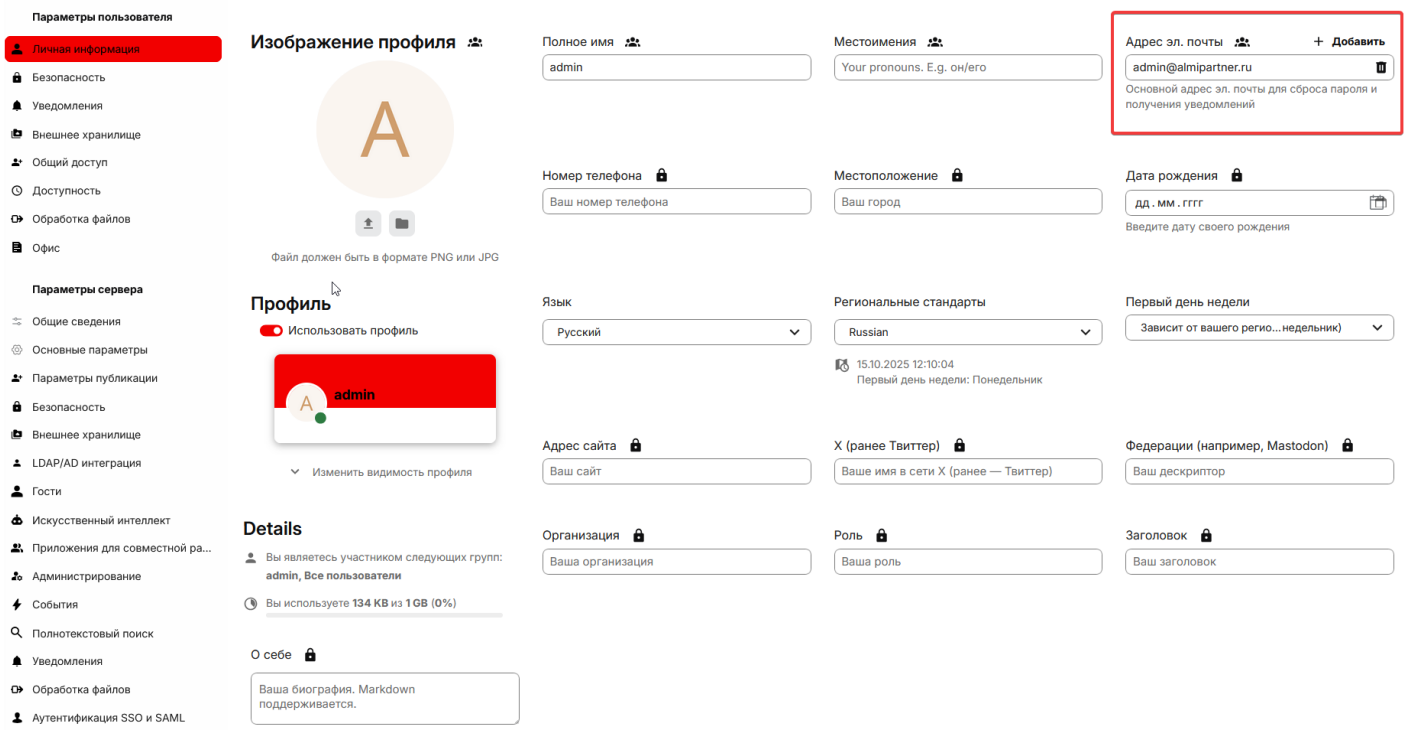


Рисунок 8. Личные настройки пользователя

Для проверки настроенной конфигурации и отправки тестового письма нажмите кнопку **«Отправить сообщение»**.

Письмо будет отправлено от имени пользователя, указанного в настройках, на адрес электронной почты, указанный в настройках пользователя, от имени которого вы работаете в системе.

Убедитесь, что сообщение успешно доставлено на указанный адрес.

Пример конфигурации SMTP (config.php)

```php
/**
 * Режим работы почтового сервера.
 * Возможные значения:
 * - 'smtp' — использование внешнего SMTP-сервера;
 */
'mail_smtpmode' => 'smtp',

/**
 * Хост почтового сервера (доменное имя или IP-адрес).
 * Например: 'smtp.example.ru'
 */
'mail_smtphost' => 'smtp.almipartner.ru',

/**
 * Порт для подключения к SMTP-серверу.
 * Рекомендуемые значения:
 * - 465 — для SSL/TLS
 * - 587 — для STARTTLS
 * - 25  — без шифрования (не рекомендуется)
 */
'mail_smtpport' => 587,

/**
 * Метод шифрования при подключении к серверу.
 * Возможные значения:
 * - 'ssl' — защищённое соединение SSL/TLS (обычно порт 465);
 * - 'tls' — STARTTLS (рекомендуется, порт 587);
 * - '' (пусто) — без шифрования (не рекомендуется).
 */
'mail_smtpsecure' => 'tls',

/**
 * Необходимость аутентификации на SMTP-сервере.
 * 1 — требуется логин/пароль;
 * 0 — без аутентификации.
 */
'mail_smtpauth' => 1,

/**
 * Имя пользователя для SMTP-аутентификации.
 * Обычно это полный адрес отправителя или имя почтового аккаунта.
 */
'mail_smtpname' => 'aow@almipartner.ru',

/**
 * Пароль от почтового аккаунта.
 * Рекомендуется хранить в защищённом месте или использовать
 * внешние механизмы хранения секретов.
 */
'mail_smtppassword' => 'aow_password',

/**
```

```
     * Адрес отправителя по умолчанию (часть до @).
     * Пример: если указано 'no-reply', а mail_domain = 'example.ru',
     * то адрес отправителя будет no-reply@example.ru.
     */
    'mail_from_address' => 'aow',

    /**
     * Домен отправителя (часть после @).
     */
    'mail_domain' => 'almipartner.ru',

    /**
     * Адрес электронной почты для получения системных уведомлений,
     * отчётов и ошибок (опционально).
     */
    'mail_smtpdebug' => false,  // включить отладку (true для диагностики)
```

4.3. Настройка параметров предоставления пользователями общего доступа

Настройка параметров предоставления пользователями общего доступа к файлам и папкам в **АльтерОфис Веб** позволяет пользователям делиться файлами и папками с другими пользователями, группами или внешними контактами.

Администратор системы может централизованно управлять параметрами общего доступа, ограничивая или разрешая конкретные сценарии обмена — для повышения безопасности и контроля над данными.

> ПРИМЕЧАНИЕ
>
> Настройки общего доступа определяют:
>
> - возможность обмена файлами между пользователями внутри системы;
> - разрешение или запрет внешнего общего доступа по ссылке;
> - необходимость пароля, срока действия или прав доступа (только чтение / редактирование);
> - доступность обмена с группами, по почте или через федерацию.

Когда использовать

Рекомендуется настраивать параметры общего доступа:

- **при первичной установке системы**, чтобы определить корпоративную политику безопасности;
- **при подключении внешних пользователей**, чтобы предотвратить утечку данных;
- **в организациях с повышенными требованиями к защите информации**, где необходимо ограничить возможность обмена файлами вне периметра сети.

Шаги выполнения

1. Проверьте доступность модуля File sharing

Перед началом настройки, убедитесь, что модуль **File sharing** для настройки общего доступа к файлам и папкам активирован.

> СМ. ТАКЖЕ
>
> - Подробнее см. в разделе «Управление приложениями (модулями) системы».

2. Откройте раздел «Параметры публикации»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт **«Параметры сервера»**.

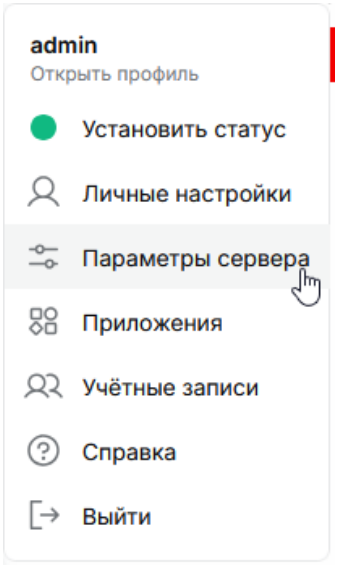


Рисунок 9. Меню администратора

В разделе **«Параметры сервера»** выберите пункт **«Параметры публикации»**.

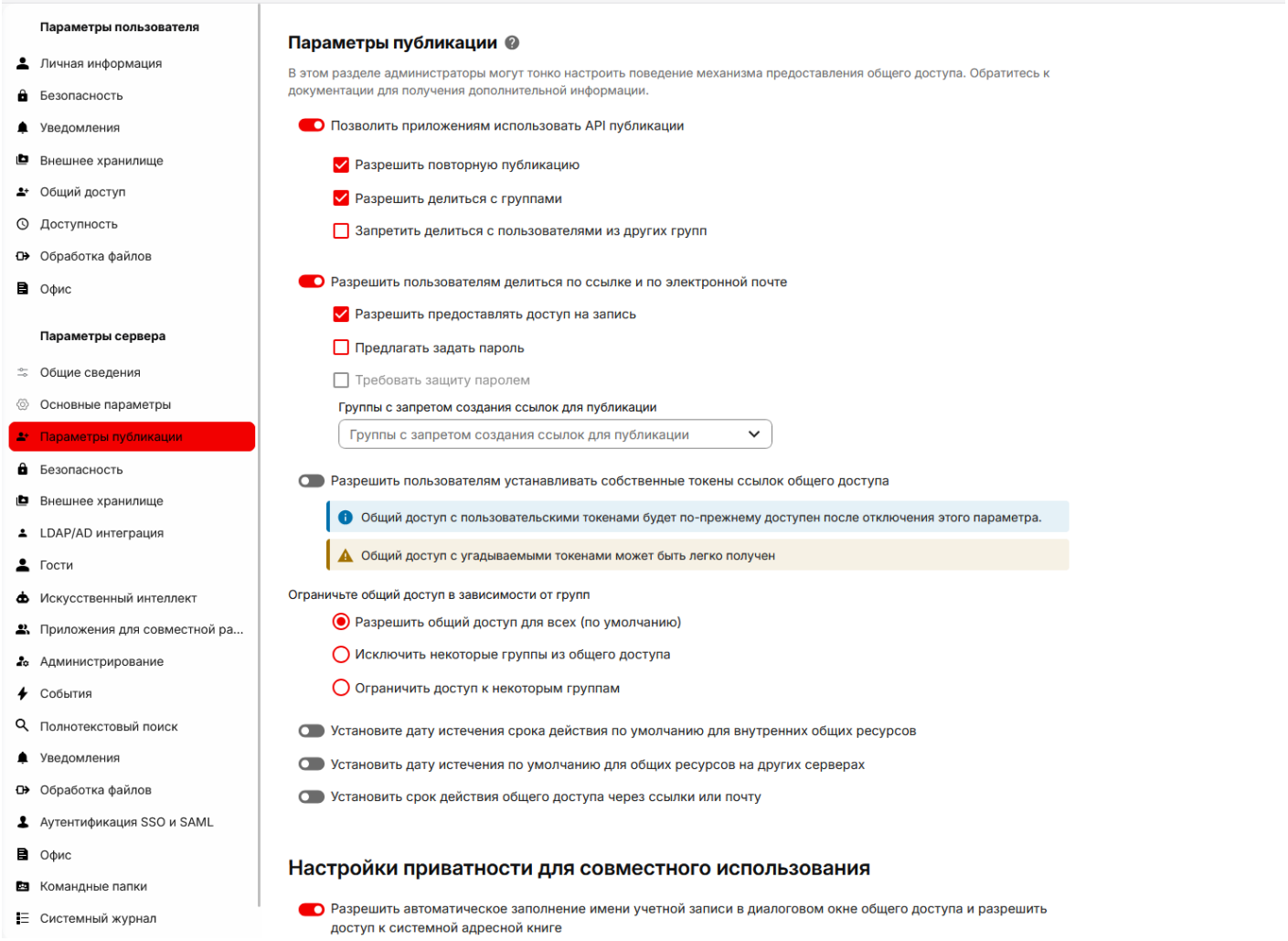
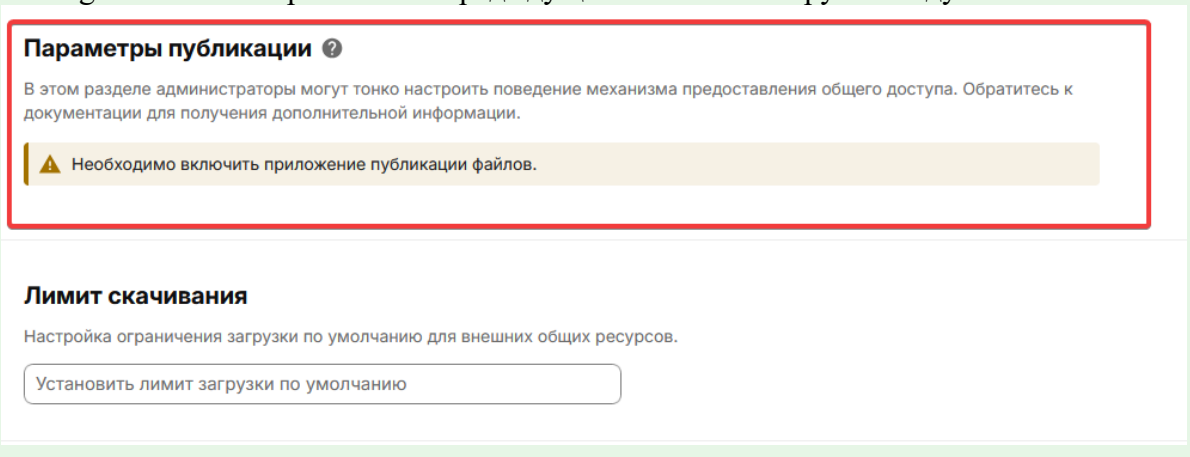


Рисунок 10. Параметры публикации

ПРИМЕЧАНИЕ

Если раздел **«Параметры публикации»** отображается как на рисунке ниже, значит модуль File sharing отключен. Вернитесь на предыдущий шаг и активируйте модуль.



Настройки модуля предоставления общего доступа

3. Настройка параметров общего доступа

Настройте параметры использования общего доступа пользователями на основе принятой в организации политики.

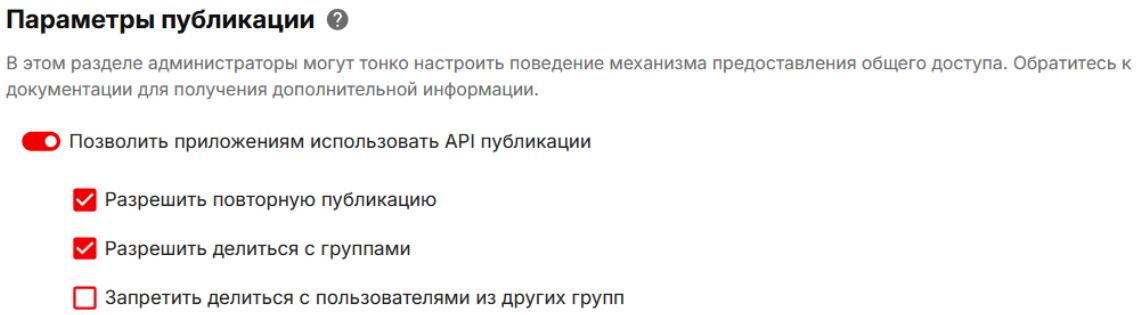


Рисунок 11. Настройка политики предоставления общего доступа

- Установите флажок **Позволить приложениям использовать API публикации**, чтобы разрешить пользователям обмениваться файлами. Если этот флажок не установлен, пользователи не смогут создавать общие папки.

Параметр	Назначение
Позволить приложениям использовать API публикации	Включает возможность пользователям обмениваться файлами, а также разрешает модулям системы использовать внутренний API для создания и управления общим доступом к файлам.

- Установите флажок **Разрешить повторную публикацию**, чтобы пользователи могли повторно делиться файлами, которыми поделились с ними. Если этот флажок не установлен, пользователи не смогут предоставлять доступ другим пользователям и группам к таким данным. Используйте данную настройку, если в организации допускается делегирование доступа к общим данным.

Параметр	Назначение
Разрешить повторную публикацию	Позволяет пользователям повторно делиться файлами, которые были им предоставлены другими пользователями.

- Установите флажок **Разрешить делиться с группами**, чтобы пользователи могли делиться данными с группами. Используйте данную настройку, если в организации используется групповая работа проектных команд или отделов.

Параметр	Назначение
Разрешить делиться с группами	Разрешает пользователям делиться файлами с целыми группами пользователей.

- Установите флажок **Запретить делиться с пользователями из других групп**, чтобы пользователи могли делиться файлами и папками исключительно внутри своей группы.

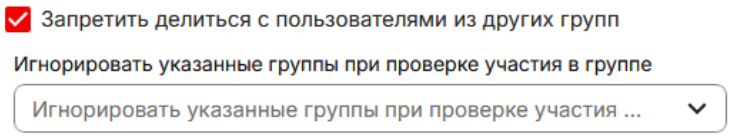


Рисунок 12. Настройка запрета делиться с пользователями из других групп

Параметр	Назначение
Запретить делиться с пользователями из других групп	Ограничивает возможность общего доступа только пользователями внутри одной группы.
Игнорировать указанные группы при проверке участия в группе	Исключает указанные группы из проверки групповой принадлежности при применении ограничений.

Если вы установите флажок **Запретить делиться с пользователями из других групп**, появится дополнительный раскрывающийся список **Игнорировать указанные группы при проверке участия в группе** для указания игнорируемых групп.

- Выберите группы, которые будут игнорироваться при проверке. Это значит, что члены указанных групп могут делиться файлами с другими группами вне зависимости от основной настройки.

ПРИМЕР

- В системе настроены три группы («Администраторы», «Бухгалтерия», «Финансовый отдел»).
- Группа «Администраторы» указана в поле **Игнорировать указанные группы при проверке участия в группе**.
- Пользователи группы «Бухгалтерия» не смогут делиться файлами с группой «Финансовый отдел» и «Администраторы».
- Пользователи группы «Администраторы» смогут делиться как с группой «Бухгалтерия», так и с группой «Финансовый отдел».

- Установите флажок **Разрешить пользователям делиться по ссылке и по электронной почте**, чтобы пользователи могли формировать публичные ссылки и отправлять их по электронной почте, людям которые не являются пользователями **АльтерОфис Веб**.

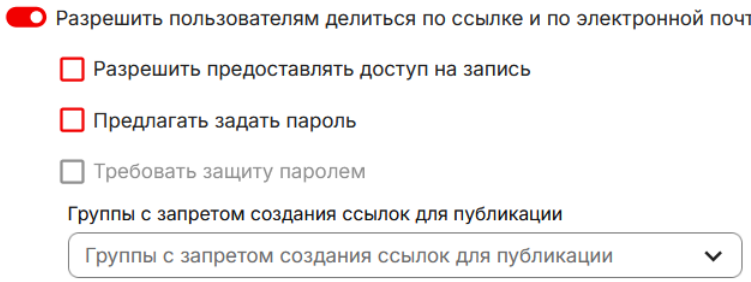


Рисунок 13. Настройка политики предоставления общего доступа (продолжение)

Параметр	Назначение
Разрешить пользователям делиться по ссылке	Включает возможность создания общих ссылок и

Параметр	Назначение
и по электронной почте	отправки приглашений по электронной почте.

Настройка **Разрешить пользователям делиться по ссылке и по электронной почте** должна быть включена, если требуется обеспечивать внешний доступ к данным (например, для партнёров).

- Установите флажок **Разрешить предоставлять доступ на запись**, чтобы пользователи, получившие доступ по ссылке, могли не только просматривать файлы, но и вносить изменения или загружать новые файлы в папку.

Параметр	Назначение
Разрешить предоставлять доступ на запись	Позволяет внешним пользователям загружать файлы при получении доступа через публичную ссылку. Используется, когда необходимо получать файлы от клиентов или подрядчиков без учётных записей.

- Установите флажок **Предлагать задать пароль**, чтобы при предоставлении общего доступа система предлагала пользователю установить пароль для создаваемых ссылок.

Параметр	Назначение
Предлагать задать пароль	При создании общей ссылки система всегда предлагает задать пароль. Используется для усиления безопасности при ручном создании ссылок пользователями.

- Установите флажок **Требовать защиту паролем**, чтобы при предоставлении общего доступа система требовала от пользователя задавать пароль для каждой создаваемой ссылки.

Параметр	Назначение
Требовать защиту паролем	Обязывает пользователей устанавливать пароль для всех публичных ссылок. Параметр становится доступным для редактирования, если установлен флажок **Требовать защиту паролем**. Включение параметра **Требовать защиту паролем** не влияет на локальные ссылки пользователей и групп.

Настройки **Предлагать задать пароль** и **Требовать защиту паролем** должны быть включены, если в организации повышенные требования к защите данных.

- Выберите в поле **Группы с запретом создания ссылок для публикации** список групп, которым будет запрещено создавать публичные ссылки на файлы.

Параметр	Назначение
Группы с запретом создания ссылок для публикации	Запрещает определённым группам создавать общие ссылки.

ПРИМЕР

- В системе настроены множество групп, включая группу «Стажёры».
- Группа «Стажёры» указана в поле **Группы с запретом создания ссылок для публикации**.
- Пользователи группы «Стажёры» не смогут создавать публичные ссылки на файлы и делиться ими с людьми, не являющимися пользователями системы.

- Установите флажок **Разрешить пользователям устанавливать собственные токены ссылок общего доступа**, чтобы пользователи могли использовать как автоматически созданный системой токен, но и задавать свой собственный. Если флажок **Разрешить пользователям устанавливать собственные токены ссылок общего доступа** отключен, то доступна опция автоматического системного токена.

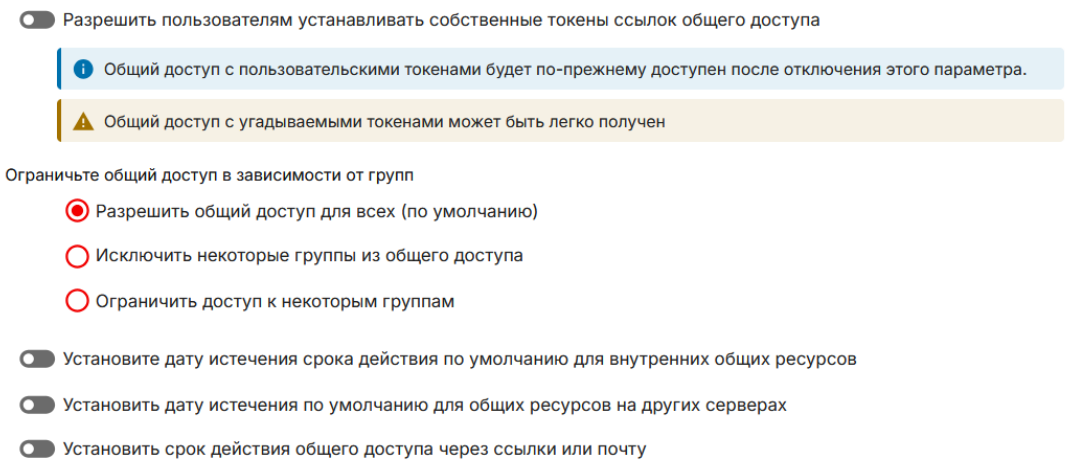


Рисунок 14. Настройка политики предоставления общего доступа (продолжение)

Параметр	Назначение
Разрешить пользователям устанавливать собственные токены ссылок общего доступа	Позволяет пользователю вручную изменить автоматически сгенерированный токен.

Настройка **Разрешить пользователям устанавливать собственные токены ссылок общего доступа** должна быть выключена, если в организации повышенные требования к защите данных.

- Выберите одну из опций в пункте **Ограничьте общий доступ в зависимости от групп**.
  - Если все пользователи системы могут делиться ресурсами оставьте значение **Разрешить общий доступ для всех (по умолчанию)**.
  - Если нужно ограничить возможность определенным группам делиться ресурсами, выберите опцию **Исключить некоторые группы из общего доступа**.
  - Если нужно определить список групп, которые могут делиться ресурсами, выберите опцию **Ограничить доступ к некоторым группам**.

Параметр	Назначение
Разрешить общий доступ для всех (по умолчанию)	Эта опция устанавливает доступ к ресурсам для всех пользователей без каких-либо ограничений

Параметр	Назначение
	по группам
Исключить некоторые группы из общего доступа	При выборе этой опции можно указать группы пользователей, которым запрещено предоставлять доступ и создавать общие ресурсы.
Ограничить доступ к некоторым группам	Настройка позволяет выбрать только определённые группы, которые будут иметь доступ к созданию и управлению общими ресурсами

При выборе опции **Исключить некоторые группы из общего доступа** в поле **Группы, которым запрещена публикация** перечислите группы, участники которых не будут видеть кнопку «Поделиться». Пользователи таких групп смогут пользоваться общедоступными ресурсами, но не смогут сами их создавать или делиться ими.

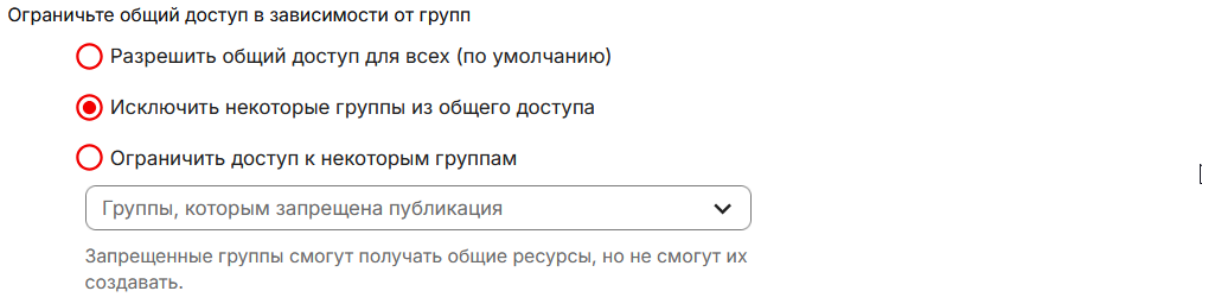


Рисунок 15. Настройка запрета на предоставление общего доступа для групп

При выборе опции **Ограничить доступ к некоторым группам** в поле **Группы, которым разрешена публикация** перечислите группы, участники которых будут иметь возможность создавать и делиться ресурсами. Другие группы, не включённые в этот список, не смогут создавать доступные для других ресурсы, но смогут пользоваться теми, что созданы другими.

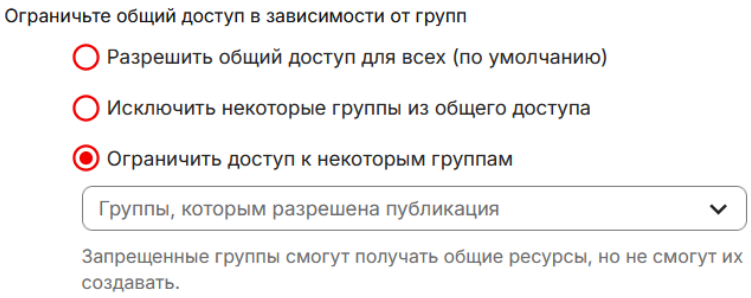


Рисунок 16. Настройка разрешения на предоставления общего доступа для групп

- Установите флажок **Установите дату истечения срока действия по умолчанию для внутренних общих ресурсов**, чтобы автоматически ограничивать длительность совместного доступа для внутренних общих ресурсов.

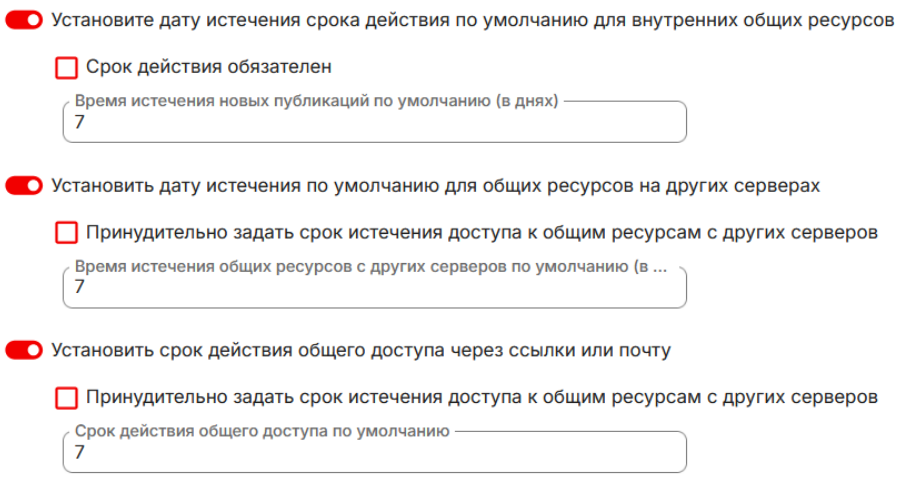


Рисунок 17. Настройка срока действия ссылок общего доступа

Параметр	Назначение
Установите дату истечения срока действия по умолчанию для внутренних общих ресурсов	Устанавливает срок действия общего доступа по умолчанию.

Если вы установите флажок **Установите дату истечения срока действия по умолчанию для внутренних общих ресурсов**, появятся дополнительные поля **Срок действия обязателен** и **Время истечения новых публикаций по умолчанию (в днях)**.

Если параметр **Установите дату истечения срока действия по умолчанию для внутренних общих ресурсов** выключен, то ограничение срока не применяется для ресурсов, которые предоставляются пользователям внутри системы.

- Установите флажок **Срок действия обязателен**, если системе необходимо проверять наличие установленного срока действия для внутренних ресурсов. Если эта опция активирована, при создании внутреннего общего доступа указывается обязательный срок действия. Без активации этой опции срок действия будет применяться только по умолчанию, но его можно изменить или убрать.
- В поле **Время истечения новых публикаций по умолчанию (в днях)** укажите количество дней, через которые общий доступ автоматически прекращается. Число «7» на рисунке означает, что внутренние ссылки на ресурсы будут действовать 7 дней с момента их создания, если не указано иное.

СОВЕТ

- Используйте данные настройки на основе принятой в организации политики ограничения времени доступа к данным.

- Установите флажок **Установите дату истечения по умолчанию для общих ресурсов на других серверах**, чтобы автоматически ограничивать срок действия общего доступа к ресурсам, размещенных на разных серверах АльтерОфис Веб.

Параметр	Назначение

Параметр	Назначение
Установите дату истечения по умолчанию для общих ресурсов на других серверах	Устанавливает срок действия общего доступа по умолчанию.

Если вы установите флажок **Установите дату истечения по умолчанию для общих ресурсов на других серверах**, появятся дополнительные поля **Принудительно задать срок истечения доступа к общим ресурсам на других серверах** и **Время истечения общих ресурсов с других серверов по умолчанию (в днях)**.

Если параметр **Установите дату истечения по умолчанию для общих ресурсов на других серверах** выключен, то ограничение срока не применяется.

- Установите флажок **Принудительно задать срок истечения доступа к общим ресурсам на других серверах**, чтобы пользователь не мог убрать или изменить дату.
- В поле **Время истечения общих ресурсов с других серверов по умолчанию (в днях)** укажите количество дней, через которые общий доступ автоматически прекращается. При создании общего доступа система автоматически подставит дату окончания (к текущей дате прибавит установленное количество дней).
- Установите флажок **Установите срок действия общего доступа через ссылки или почту**, чтобы задать автоматическое ограничение срока действия публичной ссылки отправленной по почте.

Параметр	Назначение
Установите срок действия общего доступа через ссылки или почту	Определяет срок действия общих ссылок или email-доступа по умолчанию.

Если вы установите флажок **Установите срок действия общего доступа через ссылки или почту**, появятся дополнительные поля **Принудительно задать срок истечения доступа к общим ресурсам с других серверов** и **Срок действия общего доступа по умолчанию**.

Если параметр **Установите срок действия общего доступа через ссылки или почту** выключен, то ограничение срока не применяется.

- Установите флажок **Принудительно задать срок истечения доступа к общим ресурсам с других серверов**, чтобы обязать пользователей задавать срок действия для ссылок и email-доступа.
- В поле **Срок действия общего доступа по умолчанию** укажите количество дней, через которые общий доступ автоматически прекращается.

> СОВЕТ
>
> - Используйте данные настройки для предотвращения бесконтрольного распространения публичных ссылок.

4. Настройки приватности для совместного использования

- Включите параметр **Разрешить автоматическое заполнение имени учетной записи в диалоговом окне общего доступа и разрешить доступ к системной адресной книге**, чтобы разрешить автозаполнение имён пользователей и использование системной адресной книги.

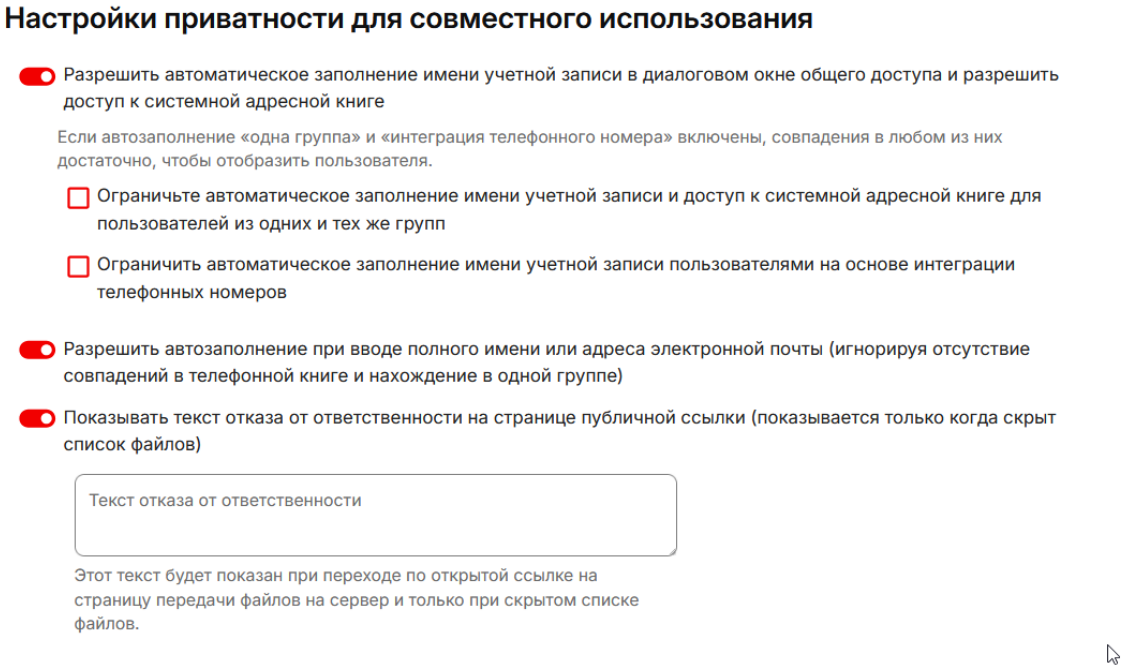


Рисунок 18. Настройки приватности для совместного использования

Параметр	Назначение
Разрешить автоматическое заполнение имени учетной записи в диалоговом окне общего доступа и разрешить доступ к системной адресной книге	Разрешает подстановку имён пользователей и использование системной адресной книги.

- Установите флажок **Ограничьте автоматическое заполнение имени учетной записи и доступ к системной адресной книге для пользователей из одних и тех же групп**, чтобы автозаполнение имени пользователя было доступно только пользователям из тех же групп, что и владелец общего доступа.

Параметр	Назначение
Ограничьте автоматическое заполнение имени учетной записи и доступ к системной адресной книге для пользователей из одних и тех же групп	Ограничивает автоматическую подстановку и адресную книгу пользователями внутри одной группы.

> СОВЕТ
>
> - Используйте настройку для разграничения видимости сотрудников разных подразделений.

- Установите флажок **Показывать текст отказа от ответственности на странице публичной ссылки (показывается только когда скрыт список файлов)**, чтобы установить и отобразить текст с отказом от ответственности в общедоступных ссылках со скрытыми списками файлов.

Параметр	Назначение
Показывать текст отказа от ответственности на странице публичной ссылки (показывается только когда скрыт список файлов)	Включает возможность ввода текста с отказом от ответственности.

Заполните поле **Текст отказа от ответственности**.

5. Настройки прав общего доступа по умолчанию

- В разделе **Права общего доступа по умолчанию** определите права, предоставляемые по умолчанию при создании общего доступа (создание, изменение, удаление и т.д.).

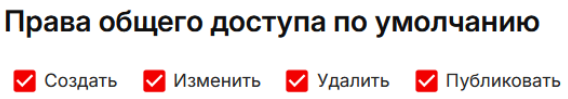


Рисунок 19. Права общего доступа по умолчанию

6. Настройки лимитов на скачивание общих ресурсов

- В разделе **Лимит скачивания** определите допустимое количество скачиваний по умолчанию. При предоставлении общего доступа пользователь сможет переопределить значение по умолчанию.

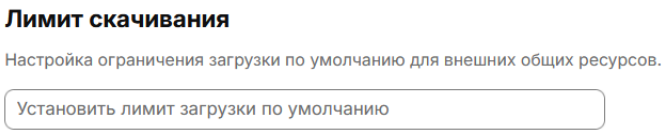


Рисунок 20. Лимит скачивания

7. Настройки предоставления доступа по почте

- В разделе **Поделиться по почте** настройте возможность предоставить доступ внешним пользователям (вне АльтерОфис Веб) без необходимости создания учётных записей. Удобно для одноразового обмена документами.

Раздел **Поделиться по почте** доступен, если активен модуль **Share by mail**.

> СМ. ТАКЖЕ
>
> - Подробнее см. в разделе «Управление приложениями (модулями) системы».

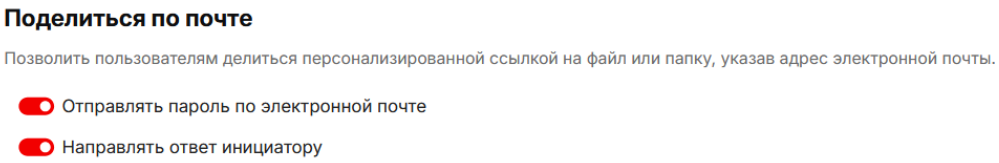


Рисунок 21. Поделиться по почте

Параметр	Назначение
Отправлять пароль по электронной почте	Отправляет пароль для защищённой ссылки на тот же адрес электронной почты, на который отправлена ссылка. Это упрощает получение доступа получателю, но снижает уровень безопасности (пароль и ссылка передаются через один канал). Ссылка и пароль рассылаются разными письмами.
Направлять ответ инициатору	Добавляет в письма обратный адрес (Reply-To) пользователя, создавшего общий доступ. Это позволяет получателям ответить напрямую отправителю.

4.4. Настройка командных папок

Использование модуля командных папок в АльтерОфис Веб позволяет администратору системы создавать папки, которые автоматически монтируются в домашнюю директорию определённым группам пользователей. В отличие от обычных пользовательских папок, командные папки управляются централизованно администратором и позволяют задавать права доступа, квоты и политику общего использования.

ПРИМЕЧАНИЕ

- В системе должны быть созданы необходимые группы пользователей или получены из LDAP / AD.

Когда использовать

- При необходимости общего доступа к папке для команды или отдела.
- Если нужно разграничить доступ между отделами (например, HR, IT, Финансы).

Шаги выполнения

1. Проверьте доступность модуля работы с командными папками

Перед началом настройки, убедитесь, что модуль **Team folders** для работы с командными папками активирован.

СМ. ТАКЖЕ

- Подробнее см. в разделе «Управление приложениями (модулями) системы».

2. Откройте раздел «Командные папки»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт **«Параметры сервера»**.

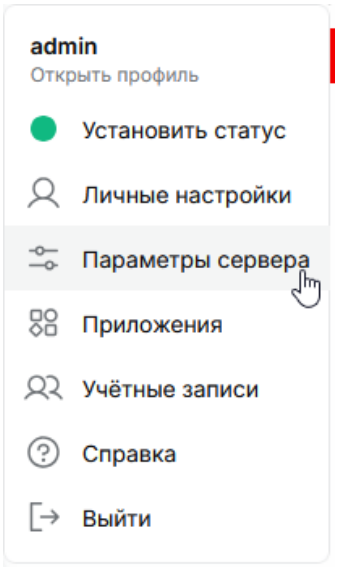


Рисунок 22. Меню администратора

В разделе **«Параметры сервера»** выберите пункт **«Командные папки»**.

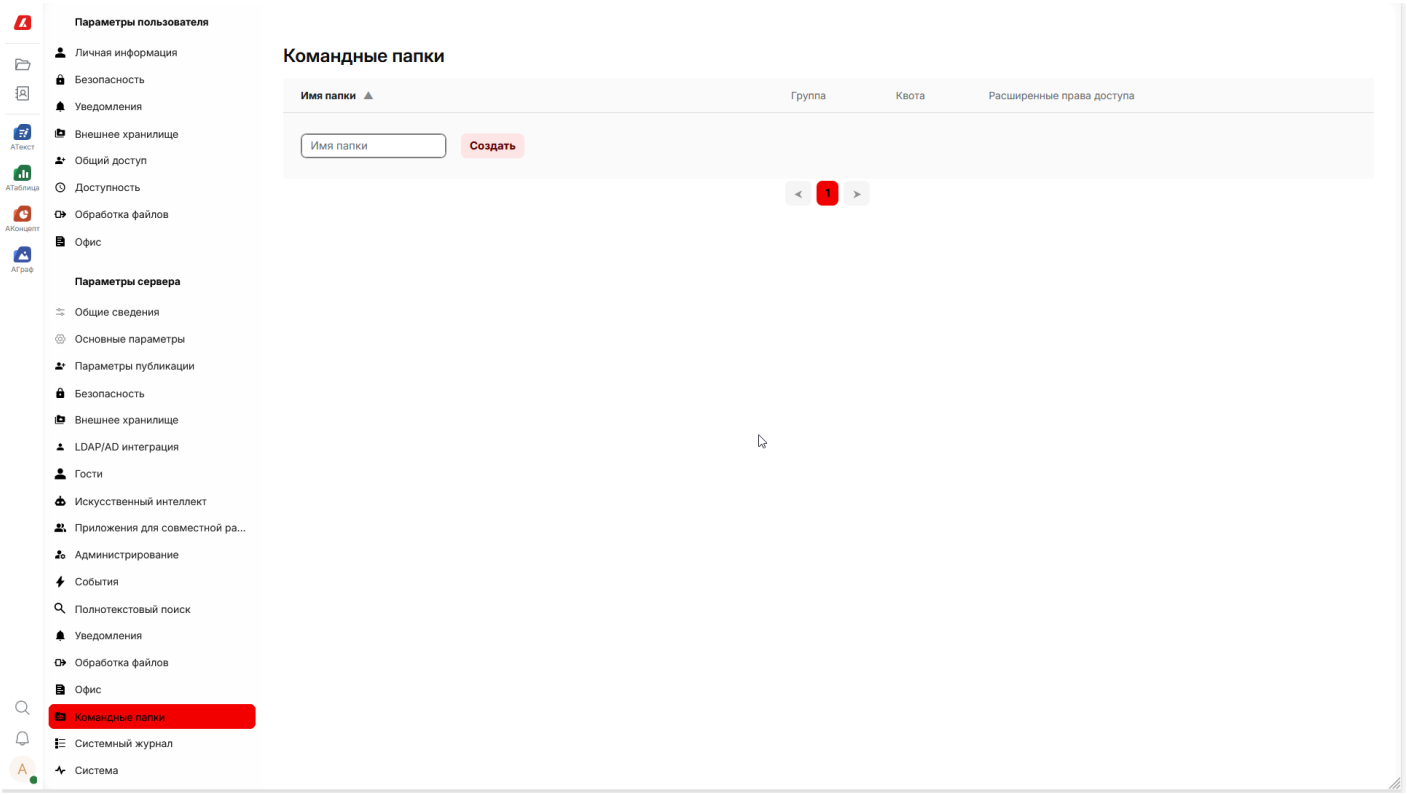


Рисунок 23. Настройка командных папок

3. Структура раздела «Командные папки»

Панель управления командными папками отображается в виде таблицы.

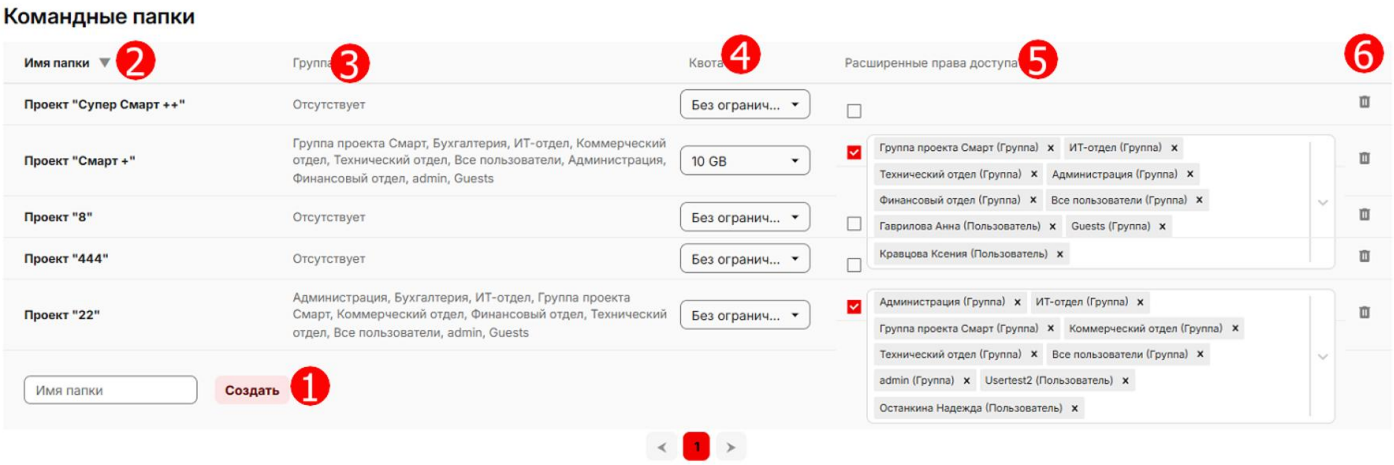


Рисунок 24. Структура раздела «Командные папки»

№	Элемент	Описание элемента
1	Кнопка **Создать**	Функция создания новой командной папки
	Поле **Имя папки**	Текстовое поле для ввода имени
2	Колонка **Имя папки**	Имя командной папки.
3	Колонка **Группа**	Список групп пользователей, у которых есть доступ к командной папке.
4	Колонка **Квота**	Допустимый объем дискового пространства для командной папки.
5	Колонка **Расширенные права доступа**	Определяет пользователей / группы пользователей и их права по администрированию выбранной командной папки.
6	Кнопка **Удалить**	Функция удаления выделенной командной папки

ПРИМЕЧАНИЕ

- Командные папки создаются и управляются **только администратором**.
- Администраторы групп могут настраивать структуру папок и права доступа внутри командных папок.
- Пользователи не могут самостоятельно удалять папки или изменять структуру прав.

4. Создание командной папки

Введите название новой командной папки в поле **Имя папки**.

Нажмите кнопку **Создать**.

Рисунок 25. Создание командной папки

При создании папки может потребоваться подтверждение выполняемой операции.

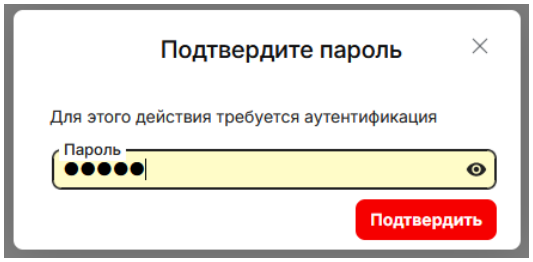


Рисунок 26. Подтверждение операции

Нажмите на кнопку **Подтвердить**.

В результате будет создана корневая командная папка, видимая пользователям.

5. Назначение групп доступа

Изначально пользователи не видят созданные командные папки. Чтобы они появились в интерфейсе пользователей, необходимо назначить права доступа.

Доступ групп к командной папке настраивается в поле **Группа**.

Выберите нужную командную папку и справа от поля **Группа** нажмите на иконку **Карандаш**.

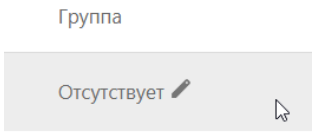


Рисунок 27. Редактирование настроек командных папок

Откроется раскрывающийся список в котором доступен выбор групп и назначение прав доступа.

При раскрытии список отображает все доступные для выбора группы (группы, созданные в разделе **Учетные записи**).

В поле **Добавить группу** выберите группы пользователей, которые должны иметь доступ к командной папке.

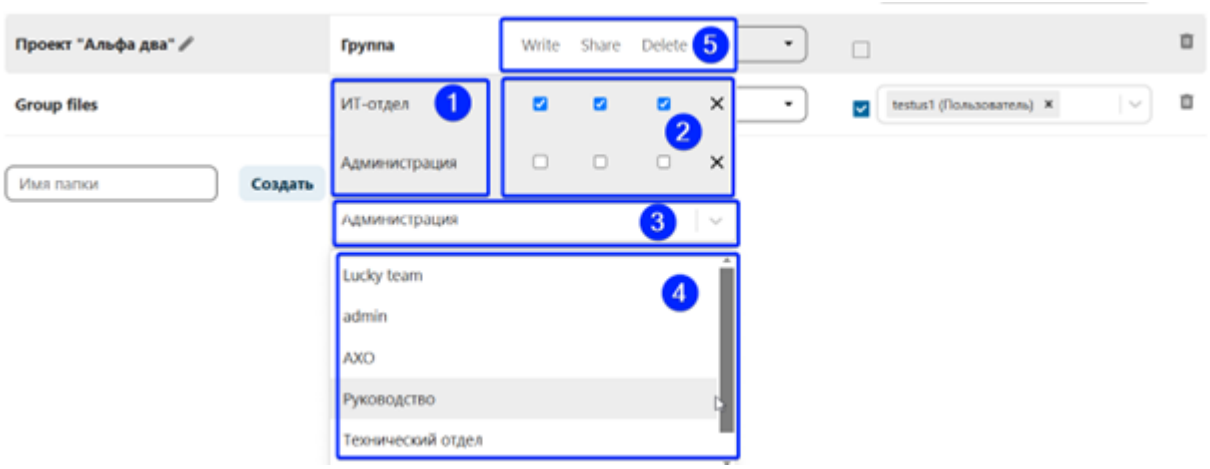


Рисунок 28. Настройка доступа к командным папкам

Элемент	Описание
Настроенный список групп пользователей (1)	Список групп пользователей, которым назначены права доступа к командной папке.
Флажки прав доступа (2)	Настройка уровней доступа. Для каждой группы можно задать права (5): только просмотр, редактирование, возможность делиться, удаление.
Поле поиска (3)	Поле для поиска группы пользователей.
Список групп пользователей (4)	Раскрывающийся список пользователей. В список выводятся только те группы, которые еще не выбраны (не отображаются в (1)).

Права доступа назначаются **по группам**, а не по отдельным пользователям.

Для выбранных групп назначьте права в таблице групп.

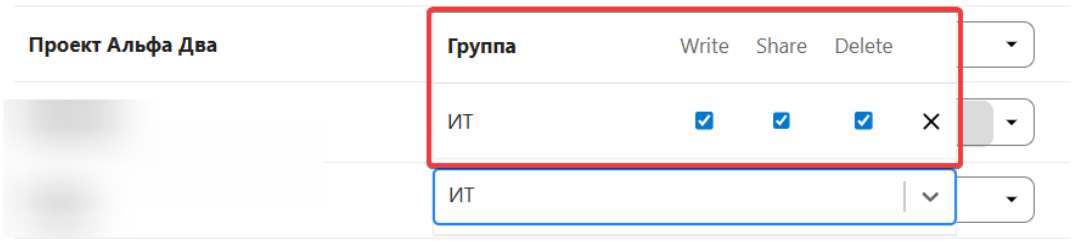


Рисунок 29. Настройка прав доступа к командным папкам

Вид командной папки после настройки доступа:

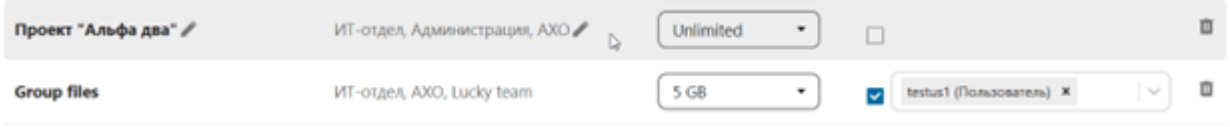


Рисунок 30. Настройка доступа к командным папкам

6. Управление квотами командных папок

При необходимости вы можете задать **квоту** (максимальный объем) на использование дискового пространства командной папкой. Использование квот позволяет предотвратить переполнение дискового пространства.

Квота задается для каждой групповой папки.

В поле **Квота** выберите одно из значений.

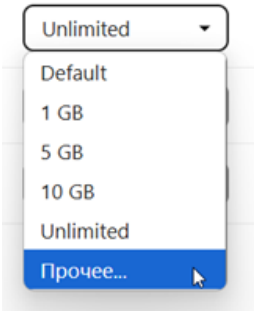


Рисунок 31. Установка квоты

Если нужно задать иной вариант, выберите **Прочее…**, после чего задайте объем.

ПРИМЕЧАНИЕ

- Объём задается в KB, MB, GB. Например: 1GB.

7. Настройка расширенных прав доступа

Включение флажка в поле **Расширенные права доступа** открывает поле **Расширенные права доступа** для выбора пользователя или группы пользователей, которые будут иметь возможность администрировать выбранную командную папку. Расширенные права могут применяться к пользователям и / или группам пользователей.

Администраторы папок могут выполнять функции администрирования:

- Добавлять в избранное.
- Предоставлять общий доступ другим группам и пользователям с настройкой прав (чтение, запись, создать, удалить, публикация).
- Копировать.
- Устанавливать напоминания.
- Скачивать.

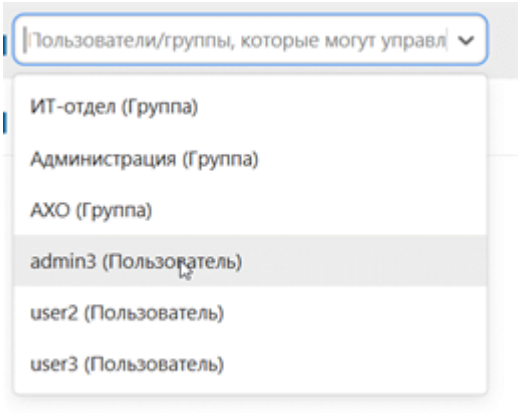


Рисунок 32. Настройка расширенных прав доступа

8. Удаление командной папки

Для удаления командной папки нажмите на кнопку **Удалить**, отобразится форма подтверждения действия.

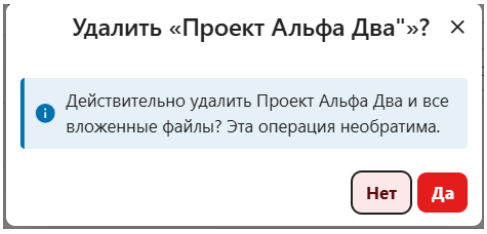


Рисунок 33. Удаление командной папки

Нажмите кнопку **Да**, чтобы удалить выбранную командную папку.

При нажатии кнопки **Нет** - форма закрывается без удаления папки.

> СОВЕТ
>
> - Удаление является безвозвратным действием.
> - Перед удалением, убедитесь, что командная папка не содержит нужной информации. При необходимости, выполните резервное копирование данных.

4.5. Аутентификация и безопасность

4.5.1. Двухфакторная аутентификация (2FA)

Двухфакторная аутентификация обеспечивает дополнительный уровень безопасности для учётных записей пользователей. При входе в систему пользователю, кроме ввода пароля, необходимо подтвердить свою личность с помощью второго фактора.

> СОВЕТ
>
> Рекомендуется включать 2FA для пользователей, работающих с конфиденциальной информацией.

Когда использовать

Рекомендуется настраивать параметры безопасности:

- **при первичной установке системы**, чтобы определить корпоративную политику безопасности;
- для **предотвращения несанкционированного доступа** даже при компрометации пароля пользователя.
- для **защиты административных аккаунтов** (имеющих доступ к конфигурации или управлению пользователями).

4.5.1.1. Поддерживаемые провайдеры 2FA

В системе поддерживается несколько провайдеров для реализации различных методов двухфакторной аутентификации:

Модуль 2FA	Описание
электронная почта	Способ, использующий отправку одноразового кода на электронную почту, связанную с учётной записью.
приложение TOTP	Способ, использующий одноразовые коды (например, через приложение **Я Ключ**).
резервные коды	Резервные коды, которые можно использовать при потере доступа к электронной почте или приложению TOTP.
разовый код пользователя	Возможность администратора сгенерировать аварийный код для восстановления доступа.

Включение или отключение модулей зависит от принятой в организации политики безопасности.

4.5.1.2. Включение обязательной двухфакторной аутентификации в АльтерОфис Веб

При установке системы двухфакторная аутентификация по умолчанию выключена. Рекомендуется включить двухфакторную аутентификацию и настроить группы пользователей, которые будут обязаны использовать 2FA.

1. Проверьте доступность провайдеров 2FA

Перед началом настройки, убедитесь, что активированы модули:

- **Two-Factor Email** провайдер для отправки одноразового кода на электронную почту;
- **Two-Factor TOTP Provider** провайдер для отправки одноразового кода через приложение TOTP;
- **Two-Factor Admin Support** генерация разового кода для определенного пользователя.

> СМ. ТАКЖЕ
>
> - Подробнее см. в разделе «Управление приложениями (модулями) системы».

2. Откройте раздел «Безопасность»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт **«Параметры сервера»**.

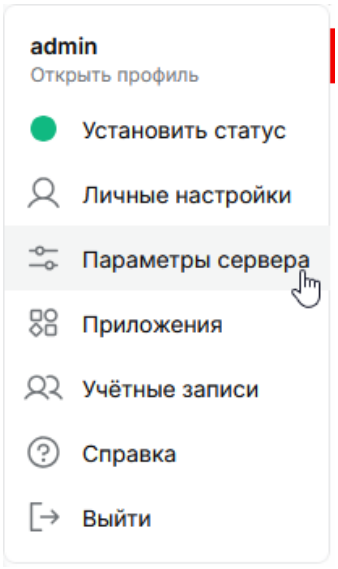


Рисунок 34. Меню администратора

В разделе **«Параметры сервера»** выберите пункт **«Безопасность»**.

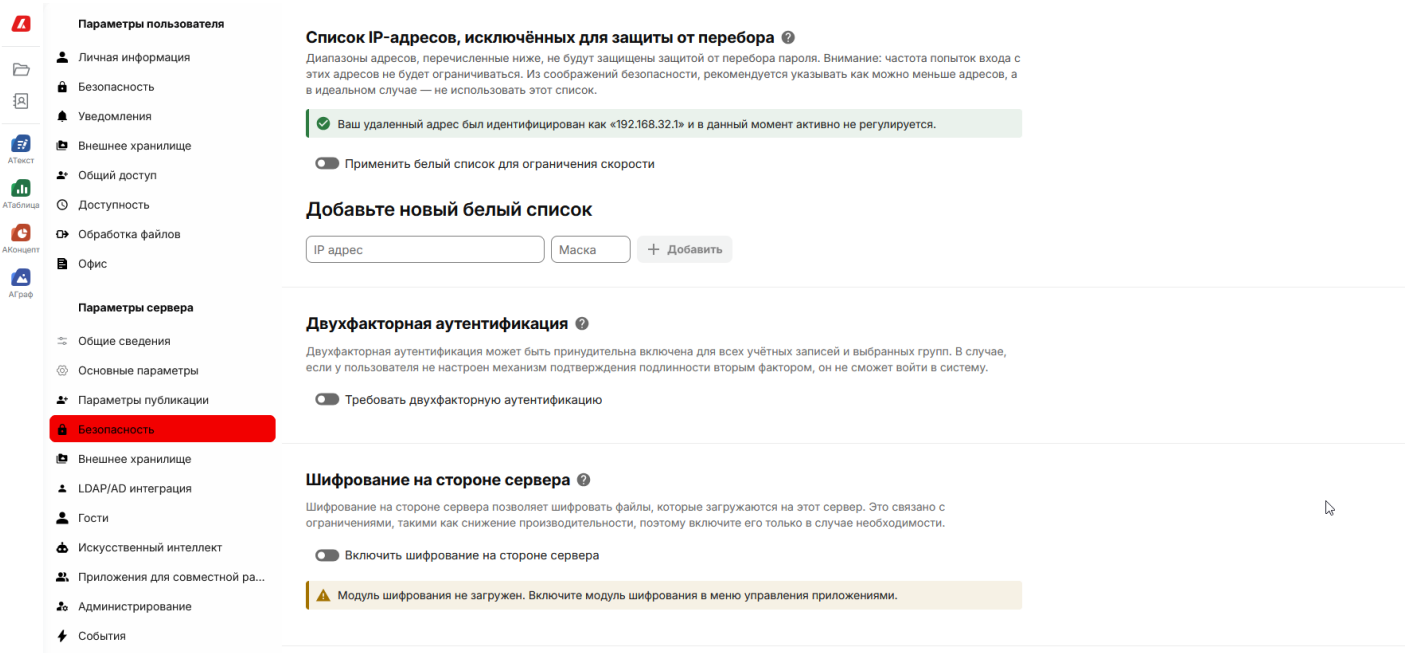


Рисунок 35. Настройки безопасности

3. Включение двухфакторной аутентификации

Для принудительного включения двухфакторной аутентификации нажмите переключатель **Требовать двухфакторную аутентификацию**.

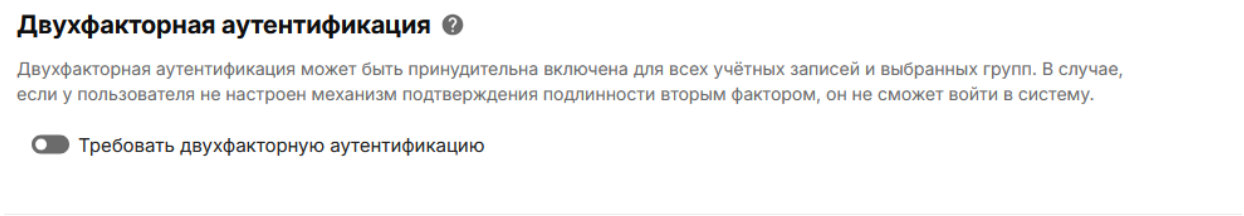


Рисунок 36. Двухфакторная аутентификация отключена

При включении двухфакторной аутентификации в разделе **Двухфакторная аутентификация** открываются дополнительные настройки **Разрешить использование только участникам этих групп**.

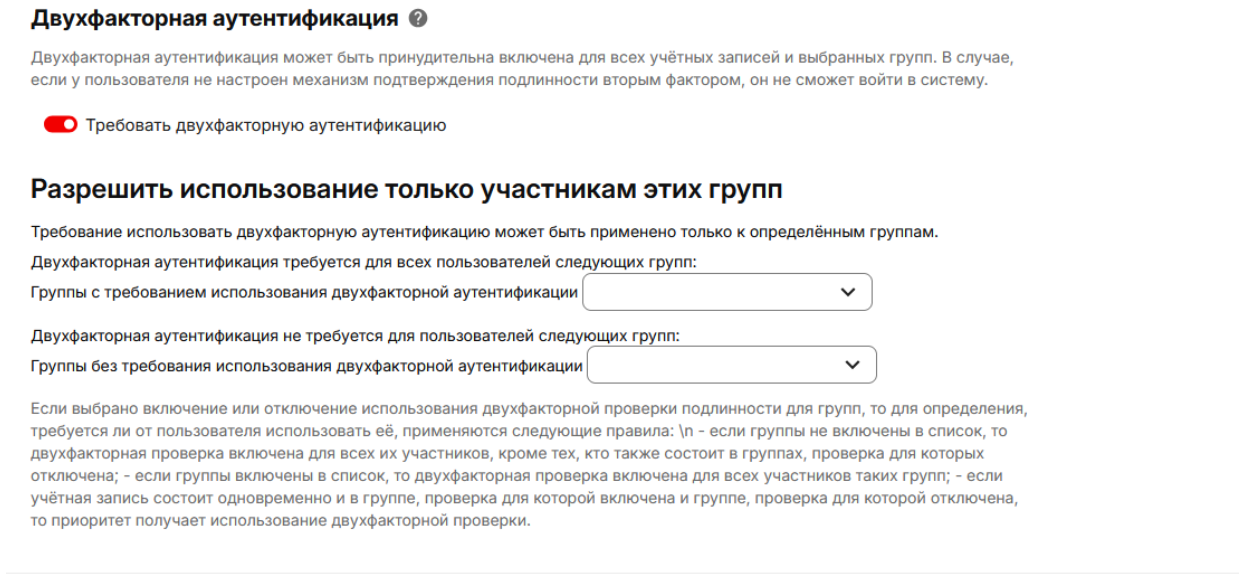


Рисунок 37. Двухфакторная аутентификация включена

4.5.1.3. Применение двухфакторной аутентификации к определённым группам

Администратор системы может принудительно включить 2FA для определенных групп пользователей или для всех пользователей.
Также Администратор может определить группу пользователей, от которой АльтерОфис Веб не будет требовать использование 2FA.

При настройке групп в полях **Двухфакторная аутентификация требуется для всех пользователей следующих групп** и **Двухфакторная аутентификация не требуется для пользователей следующих групп** применяются следующие правила:

Двухфакторная аутентификация требуется для всех пользователей следующих групп	Двухфакторная аутентификация не требуется для пользователей следующих групп	Правило применения
-	-	2FA включена для всех

Двухфакторная аутентификация требуется для всех пользователей следующих групп	Двухфакторная аутентификация не требуется для пользователей следующих групп	Правило применения
		пользователей системы
Группа А	-	2FA включена для пользователей, входящих в «Группу А». Другие пользователи могут входить в систему без использования второго фактора.
-	Группа Б	2FA включена для всех пользователей системы, кроме пользователей, входящих в «Группу Б»
Группа В	Группа В	2FA включена для всех пользователей системы, включая пользователей, входящих в «Группу В»

Выполните настройки в полях **Двухфакторная аутентификация требуется для всех пользователей следующих групп** и **Двухфакторная аутентификация не требуется для пользователей следующих групп** - выберите необходимые группы из раскрывающегося списка.

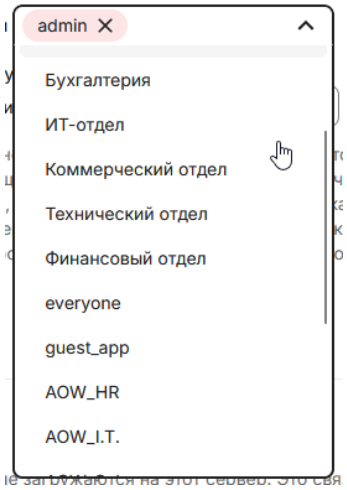


Рисунок 38. Список групп

Поле	**Описание**	**Пример**
Двухфакторная аутентификация требуется для всех пользователей следующих групп	Список групп, которые должны обязательно использовать 2FA.	admin

Поле	Описание	Пример
Двухфакторная аутентификация не требуется для пользователей следующих групп	Список групп, которым не обязательно использовать 2FA.	AlterOfficeWeb

Нажмите кнопку **Сохранить изменения** для применения и сохранения выполненных настроек.

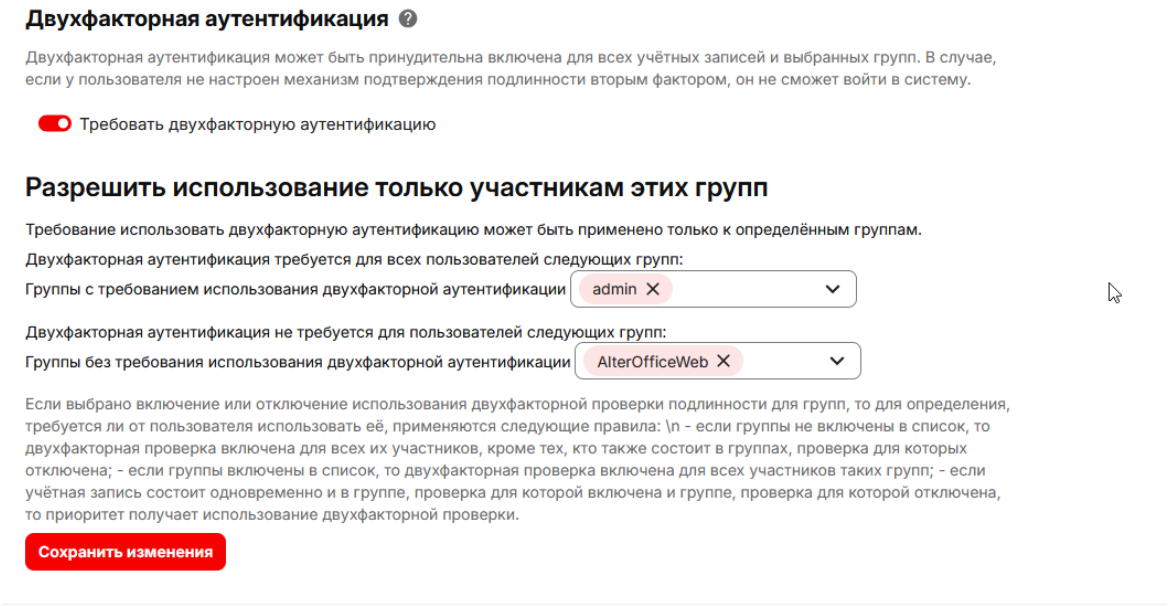


Рисунок 39. Применение двухфакторной аутентификации к определённым группам

После нажатия на кнопку **Сохранить изменения** настройки применятся и начнут действовать.

4.5.1.4. Настройка двухфакторной аутентификации для учетной записи администратора

Чтобы не потерять доступ к системе, администратор должен включить хотя бы одного провайдера услуг двухфакторной аутентификации для своей учетной записи.

1. Откройте раздел «Безопасность» в параметрах пользователя

Выберите пункт **Безопасность** в параметрах пользователя и пролистайте до раздела **Двухфакторная аутентификация**.

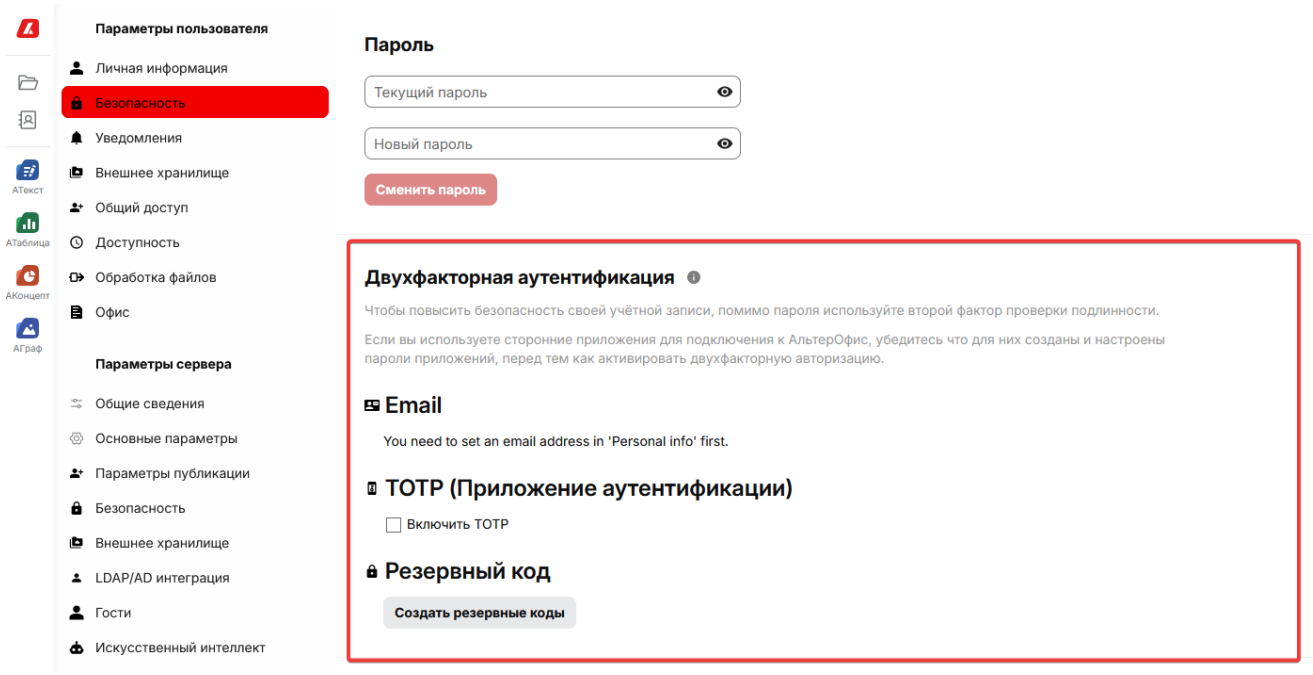


Рисунок 40. Двухфакторная аутентификация

2. Включение 2FA по электронной почте

В настройках пользователя введите адрес электронной почты, после этого появляется возможность включить 2FA по электронной почте.

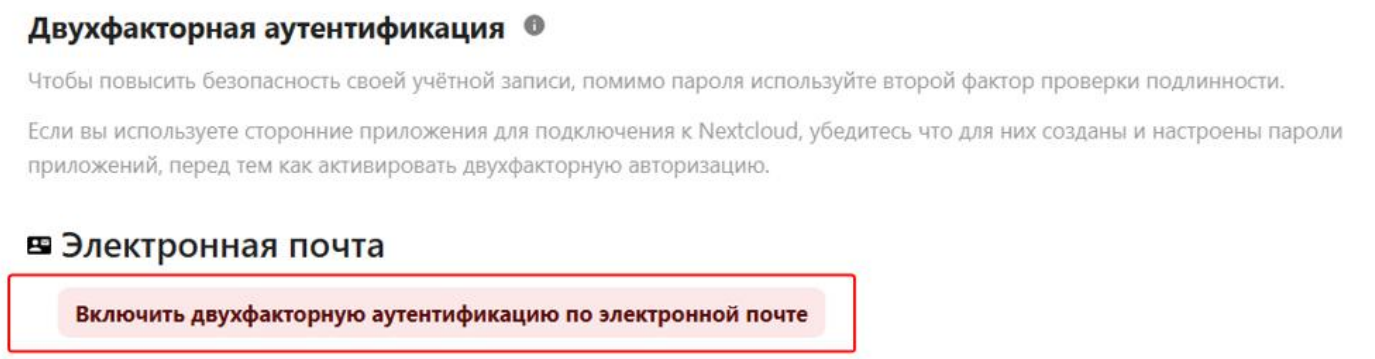


Рисунок 41. Двухфакторная аутентификация - электронная почта

Нажмите на кнопку **Включить двухфакторную аутентификацию по электронной почте**.

При нажатии на кнопку система отправляет письмо с кодом на указанный в настройках пользователя адрес электронной почты. Дождитесь письма с кодом и введите полученный код в поле.

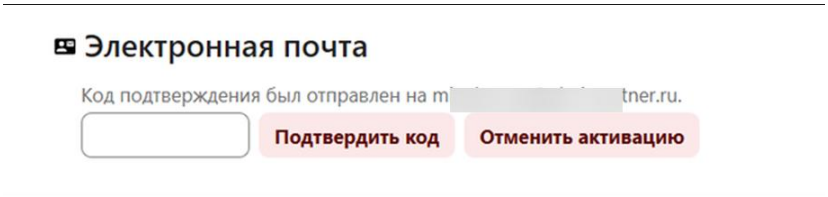


Рисунок 42. Двухфакторная аутентификация - подтверждение настроек

Для подтверждения активации двухфакторной аутентификации с использованием электронной почты нажмите кнопку **Подтвердить код**.

Раздел **Электронная почта** примет вид:

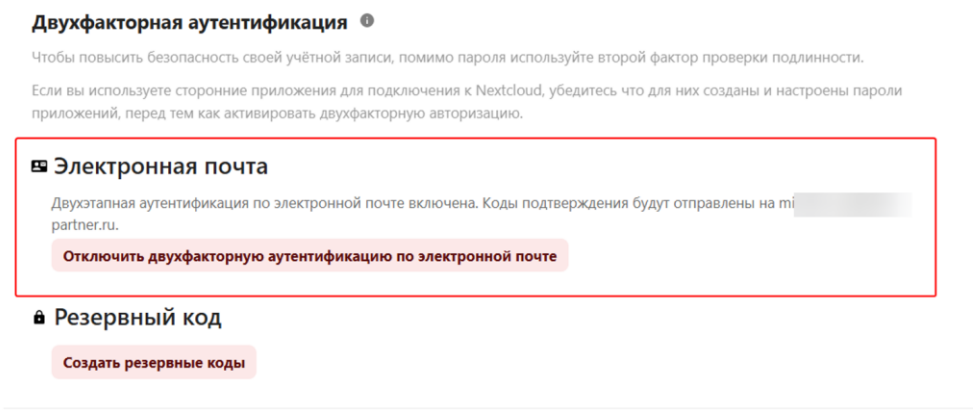


Рисунок 43. Настройка двухфакторной аутентификации по электронной почте завершена

3. Включение 2FA через приложение TOTP

TOTP – метод двухфакторной аутентификации (2FA), при котором пользователь получает временный одноразовый пароль, генерируемый с помощью специального приложения на основе текущего времени. Для получения второго фактора могут использоваться разные приложения, например приложение **Я Ключ**, **Google Authenticator**.

В параметрах пользователя выберите пункт **Безопасность**. В открывшейся форме найдите раздел **Двухфакторная аутентификация** и подраздел **TOTP (Приложение аутентификации)**.

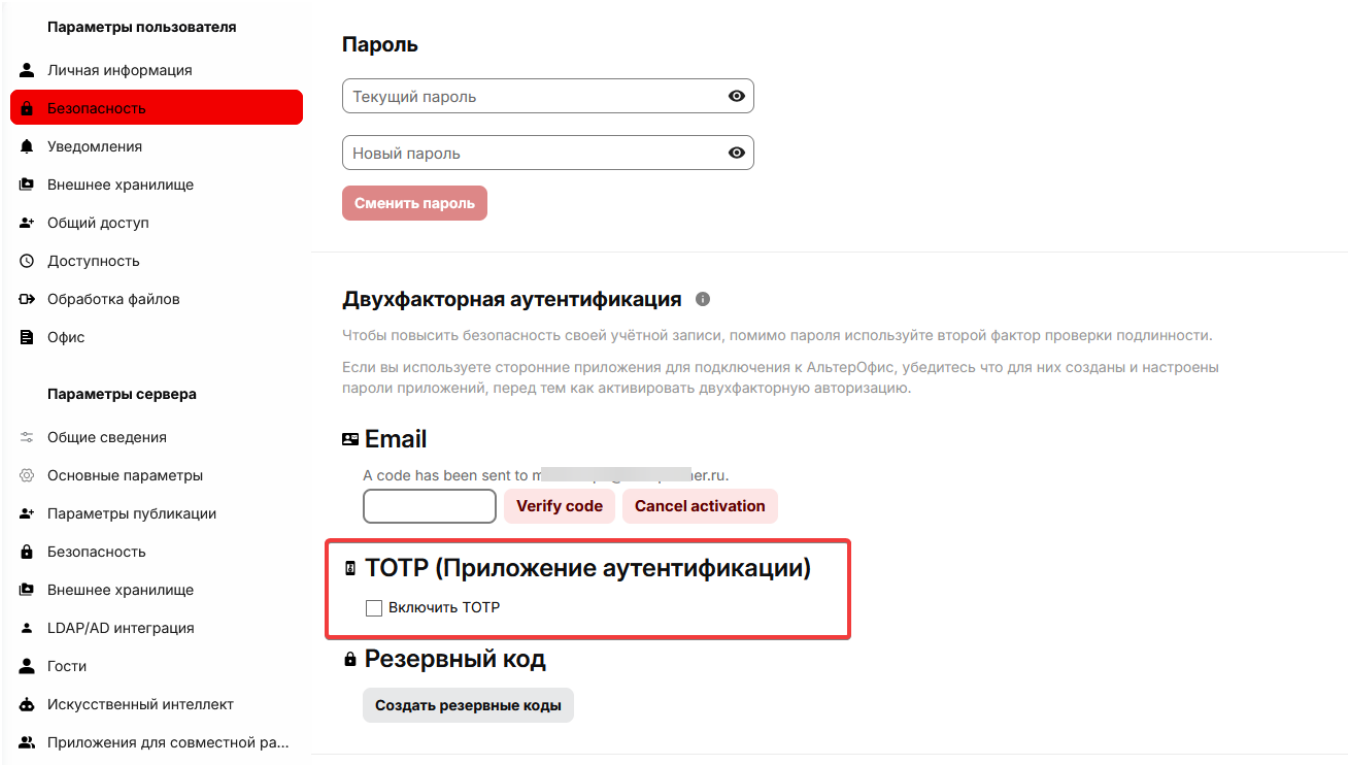


Рисунок 44. Двухфакторная аутентификация - TOTP

Активируйте опцию **Включить TOTP** в подразделе **TOTP (Приложение аутентификации)**. Это запустит процесс настройки аутентификации TOTP.

Система сгенерирует и отобразит QR-код. Используйте приложение TOTP, например **Я Ключ** или **Google Authenticator**, на своём телефоне, чтобы отсканировать его.

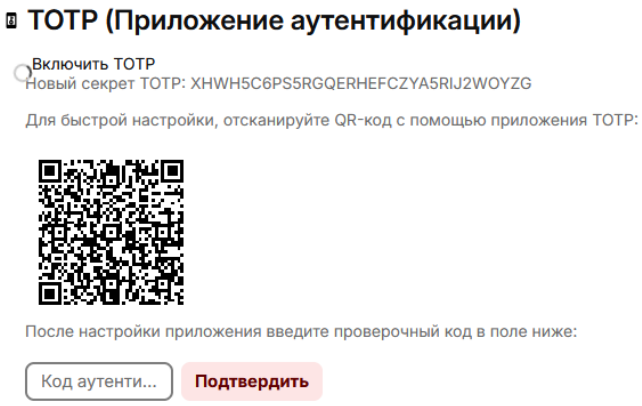


Рисунок 45. Двухфакторная аутентификация - подключение TOTP

Введите полученный через приложение разовый код в поле **Код аутентификации** и нажмите кнопку **Подтвердить**.

Это позволит связать вашу учётную запись АльтерОфис Веб с приложением для аутентификации.

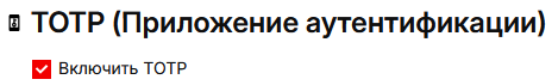


Рисунок 46. Двухфакторная аутентификация - TOTP подключен

После привязки ваше приложение TOTP будет генерировать уникальные коды, которые нужно использовать в качестве второго фактора при входе в систему.

4. Создание резервных кодов

После включения двухфакторной аутентификации создайте резервные коды и храните их в надёжном месте. Эти коды можно использовать для доступа к аккаунту, если вы потеряете доступ к телефону или приложению для аутентификации.

В параметрах пользователя выберите пункт **Безопасность**. В открывшейся форме найдите раздел **Двухфакторная аутентификация** и подраздел **Резервный код**.

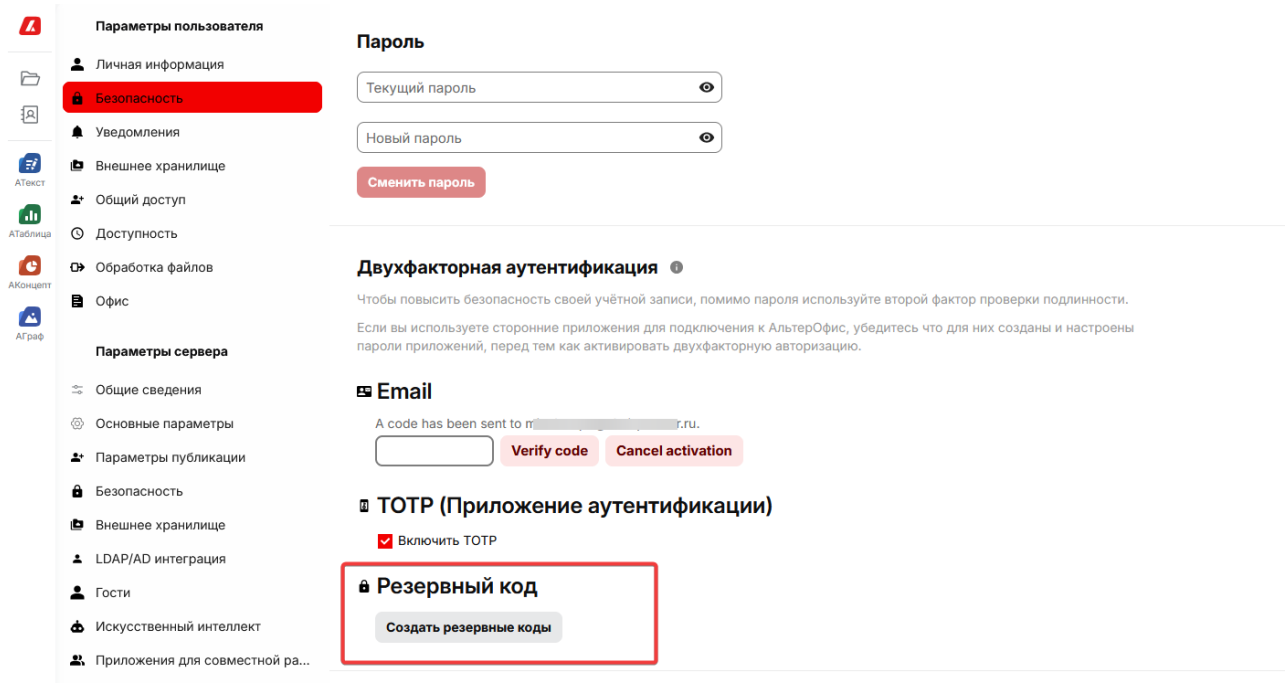


Рисунок 47. Двухфакторная аутентификация - резервные коды

Нажмите кнопку **Создать резервные коды**.

Система сгенерирует и отобразит резервные коды.

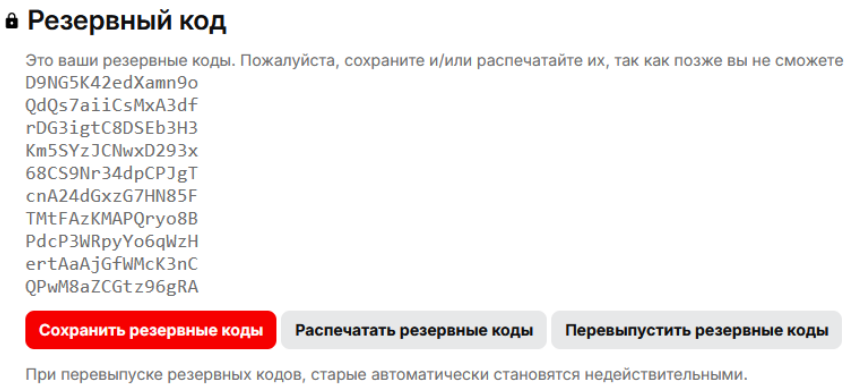


Рисунок 48. Двухфакторная аутентификация - сгенерированные резервные коды

Нажмите кнопку **Сохранить резервные коды** для сохранения кодов в текстовый файл.

Для печати сгенерированных кодов нажмите кнопку **Распечатать резервные коды**.

Для генерации новых кодов нажмите кнопку **Перевыпустить резервные коды**.

4.5.1.5. Генерация второго фактора администратором

Администратор системы может генерировать одноразовые коды для входа пользователей в учётную запись, защищённую 2FA. Это полезно в ситуациях, когда пользователи потеряли доступ к другим методам 2FA или к обязательной 2FA без предварительно включенного поставщика 2FA.

1. Откройте раздел «Безопасность» в параметрах сервера

Выберите пункт **Безопасность** в параметрах сервера и пролистайте до раздела **Двухфакторное администрирование**.

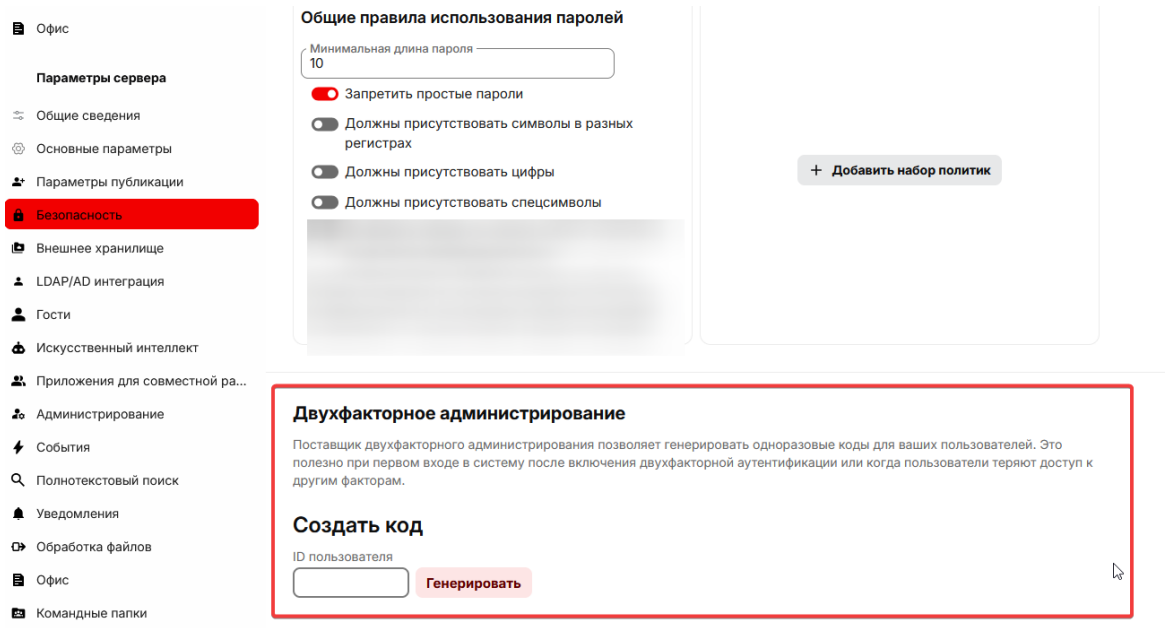


Рисунок 49. Двухфакторное администрирование

2. Генерация разового кода для пользователя

Введите в поле **ID пользователя** имя учётной записи пользователя.

ПРИМЕЧАНИЕ

- Имя учетной записи берется из списка пользователей и может быть как в виде *AbramovNS* (для локальных пользователей), так и в виде *DECB9B68-EE23-45CA-B02B-6F2B28C9B1E4* (для пользователей импортируемых из LDAP / AD).

Нажмите на кнопку **Генерировать**.

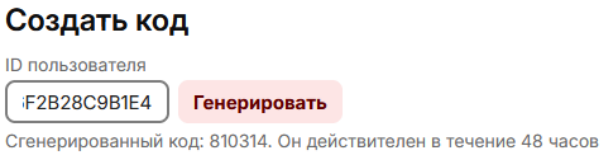


Рисунок 50. Генерация разового кода пользователя

После генерации кода, передайте код пользователю, запросившему разовый код.

СОВЕТ

- Поскольку код можно использовать только один раз, пользователю нужно убедиться, что двухфакторная аутентификация для его учетной записи настроена правильно. В противном случае он не сможет войти в систему повторно.

4.5.2. Политика безопасности паролей

Политика безопасности паролей предназначена для повышения уровня безопасности учетных записей пользователей путем задания административных требований к сложности и сроку действия паролей.

СОВЕТ

- Политика безопасности паролей должна балансировать между безопасностью и удобством пользователей.

Когда использовать

Политику безопасности паролей необходимо использовать всегда при наличии любой системы аутентификации, но особенно критично она требуется в следующих случаях:

- Первичной настройке системы или подключении новых пользователей.
- При хранении конфиденциальных данных (персональные данные, финансовые документы, коммерческая тайна).
- При доступе извне защищенной сети (удаленные сотрудники).
- Для привилегированных учетных записей (администраторы, руководители).
- Для всех пользователей по умолчанию как базовая мера защиты.

4.5.2.1. Поддерживаемые настройки политики паролей

Система позволяет задать минимальную длину пароля, обязательное использование символов разных типов (букв, цифр, специальных символов), а также включить проверку на использование слабых или ранее скомпрометированных паролей.

Настройка	Описание
Минимальная длина пароля	Определяет минимальное количество символов, допустимое при создании пароля.
Запретить простые пароли	Проверяет, не входит ли выбранный пароль в список часто используемых и слабых паролей.
Должны присутствовать символы в разных регистрах	Требует обязательного наличия заглавных букв (A–Z) и строчных букв (a–z).
Должны присутствовать цифры	Требует обязательного наличия хотя бы одной цифры в пароле.
Должны присутствовать спецсимволы	Требует наличие хотя бы одного специального символа (например, !@#$%^&*).
Размер истории паролей	Запрещает повторное использование предыдущих паролей. Количество предыдущих паролей задаётся параметром.
Максимальное количество попыток входа в систему	Количество попыток входа до блокировки учетной записи, снимаемой вручную (0 — без ограничений)
Количество дней до истечения действия пароля	Устанавливает срок действия пароля в днях, после чего пользователю будет предложено сменить пароль.

Настройки опций зависят от принятой в организации политики безопасности паролей.

4.5.2.2. Настройка политики безопасности паролей

1. Проверьте доступность модуля

Перед началом настройки, убедитесь, что активирован модуль **Password policy**.

> СМ. ТАКЖЕ
>
> - Подробнее см. в разделе «Управление приложениями (модулями) системы».

2. Откройте раздел «Безопасность»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя и в открывшемся меню выберите пункт **«Параметры сервера»**.

В разделе **«Параметры сервера»** выберите пункт **«Безопасность»**.

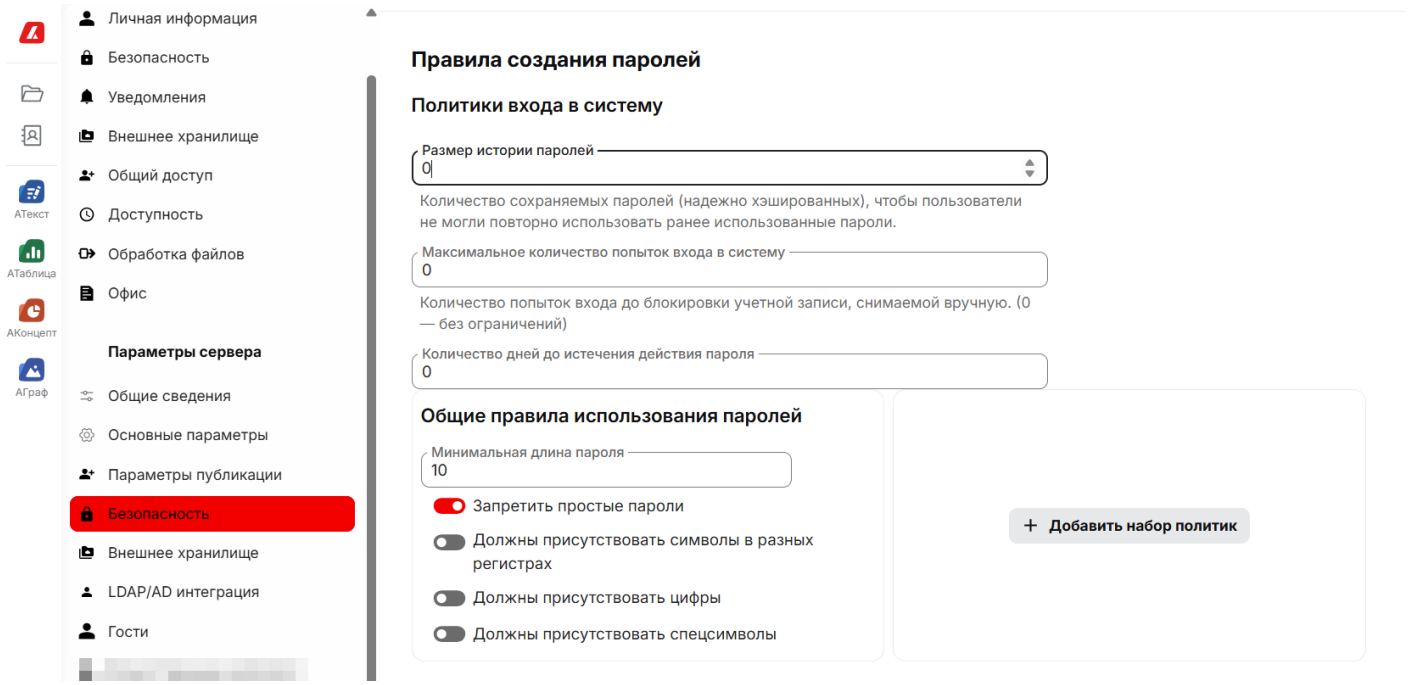


Рисунок 51. Настройка политики безопасности паролей

3. Настройте правила создания паролей

Задайте необходимые значения параметров:

- Минимальная длина пароля;
- Требование к использованию цифр, заглавных и строчных букв;
- Обязательное наличие специальных символов;
- Ограничение срока действия пароля.

Сохраните изменения и уведомите пользователей о новых правилах.

4.5.3. Настройка и управление защитой от перебора

Система имеет механизм защиты (**Brute-force protection**), который автоматически ограничивает количество попыток входа и подозрительных запросов с одного IP-адреса, защищая учетные записи от подбора паролей, DDoS-подобных действий и аномальной активности клиентов.

Когда подозрительная активность превышает заданные пороги, сервер может замедлять ответы, ограничивать доступ или временно полностью блокировать IP-адрес до 30 минут.

Когда использовать

- Если пользователи сообщают о временных блокировках после нескольких попыток входа.
- При подозрении на автоматический подбор пароля или резкое увеличение количества запросов от одного клиента.
- В инфраструктурах, использующих балансировщики, прокси или NAT.

4.5.3.1. Настройка параметров защиты от перебора

1. Проверьте доступность модуля

Перед началом настройки, убедитесь, что активирован модуль **Brute-force settings**.

> СМ. ТАКЖЕ
>
> - Подробнее см. в разделе «Управление приложениями (модулями) системы».

2. Откройте раздел «Безопасность»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя и в открывшемся меню выберите пункт **«Параметры сервера»**.

В разделе **«Параметры сервера»** выберите пункт **«Безопасность»**.

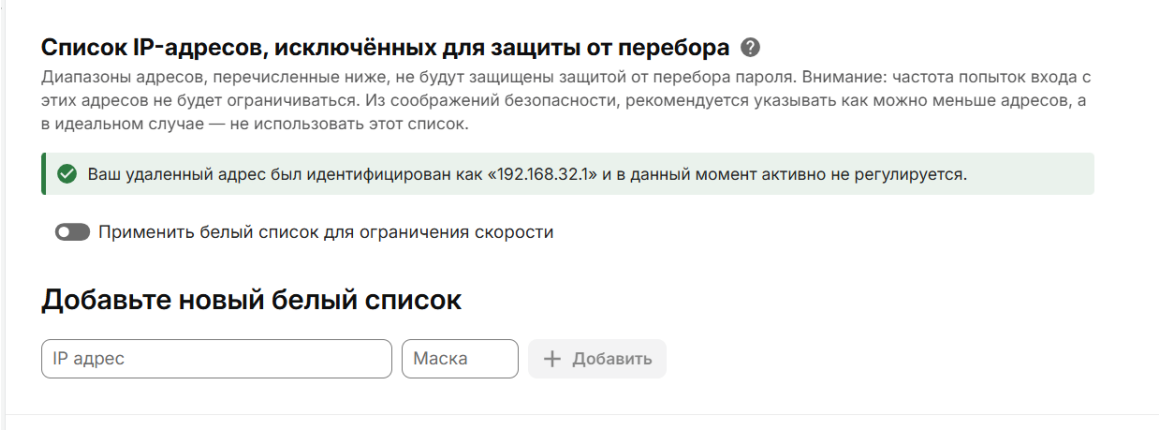


Рисунок 52. Настройка защиты от перебора паролей

3. Настройте «белый» список

Защита от перебора включена в системе по умолчанию. Если требуется разрешить неограниченный доступ для определённого IP-адреса или подсети (например, для служебных систем или доверенных сетей), их необходимо добавить в список исключений («белый список»).

В разделе **Параметры сервера** найдите заголовок **Список IP-адресов, исключённых для защиты от перебора**.

Активируйте переключатель **Применить белый список для ограничения скорости**.

Добавьте IP адрес и маску сети в разделе **Добавьте новый белый список**.

> СОВЕТ
>
> - Подходите ответственно к включению IP адресов в «белый список». Добавление адресов в «белый список» полностью отключает для них механизмы защиты от перебора, позволяя злоумышленнику выполнять неограниченное количество попыток подбора паролей, токенов и кодов двухфакторной аутентификации без замедления или блокировки.

4.6. Управление внешними хранилищами

Функциональность внешних хранилищ позволяет **администратору системы** подключать внешние сервисы и устройства хранения данных в качестве дополнительных устройств хранения данных к АльтерОфис Веб.

В системе используется два уровня подключения хранилищ.

Уровень	Описание
Системный уровень - настраивается администратором системы для всех пользователей	- Доступ к корпоративным облачным хранилищам. - Подключение общих сетевых ресурсов (FTP, SFTP, WebDAV).
Пользовательский уровень - настраивается индивидуально каждым пользователем	- Личные облачные аккаунты. - Персональные внешние диски и сетевые ресурсы.

> СОВЕТ
>
> Не смешивайте корпоративные и личные хранилища. Сначала настройте все общие хранилища, которые нужны командам, и только потом решите — разрешать ли сотрудникам подключать их личные диски.

Когда использовать

Подключение внешних хранилищ требуется в следующих случаях:

- Для расширения дискового пространства АльтерОфис Веб без физического добавления дисков на сервер.
- Для предоставления доступа к данным на специализированном сервере (например, SFTP) через удобный веб-интерфейс АльтерОфис Веб.

4.6.1. Поддерживаемые провайдеры

В системе поддерживается несколько провайдеров подключения внешних хранилищ:

Провайдер	Описание
Локальный	Подключение папок, расположенных на том же сервере, где установлена система, но вне его стандартной структуры каталогов.
SMB/CIFS	Доступ к сетевым папкам и общим ресурсам в локальной сети через протокол Windows.
SFTP	Безопасное подключение к файловым серверам через зашифрованное SSH-соединение.
FTP	Подключение к файловым серверам по стандартному протоколу передачи файлов.
WebDAV	Интеграция с веб-ресурсами и другими облачными сервисами, поддерживающими этот

Провайдер	Описание
	протокол.
Хранилище объектов OpenStack	Работа с объектными хранилищами, совместимыми с OpenStack Swift.
АльтерОфис	Подключение к другим серверам АльтерОфис Веб (федерация).

4.6.2. Настройка локальных хранилищ

Провайдер «Локальное хранилище» позволяет подключить к системе АльтерОфис Веб директорию (папку), которая физически находится на том же сервере, что и сама система, но за пределами его стандартного каталога данных (data/). Данная функциональность позволяет предоставлять доступ к уже существующим на сервере файлам или для использования отдельного диска/раздела без изменения структуры данных АльтерОфис Веб.

ПРИМЕЧАНИЕ

Подключение к локальному хранилищу может использоваться:

- Для использования отдельного смонтированного диска (например, большого HDD или SSD) без переноса туда данных пользователей.
- Если необходимо разделить данные приложений (в стандартной папке data/) и общие файлы компании (на отдельном диске).
- Для организации сложной структуры хранения, когда разные папки находятся на разных физических носителях.

1. Подготовьте директорию на сервере

Убедитесь, что папка, которую вы хотите подключить, существует и на нее есть права доступа у пользователя, от имени которого работает веб-сервер.

2. Проверьте доступность модуля

Перед началом настройки, убедитесь, что активирован модуль **External storage support**.

СМ. ТАКЖЕ

- Подробнее см. в разделе «Управление приложениями (модулями) системы».

3. Откройте раздел «Внешнее хранилище»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя и в открывшемся меню выберите пункт **«Параметры сервера»**.

В разделе **«Параметры сервера»** выберите пункт **«Внешнее хранилище»**.

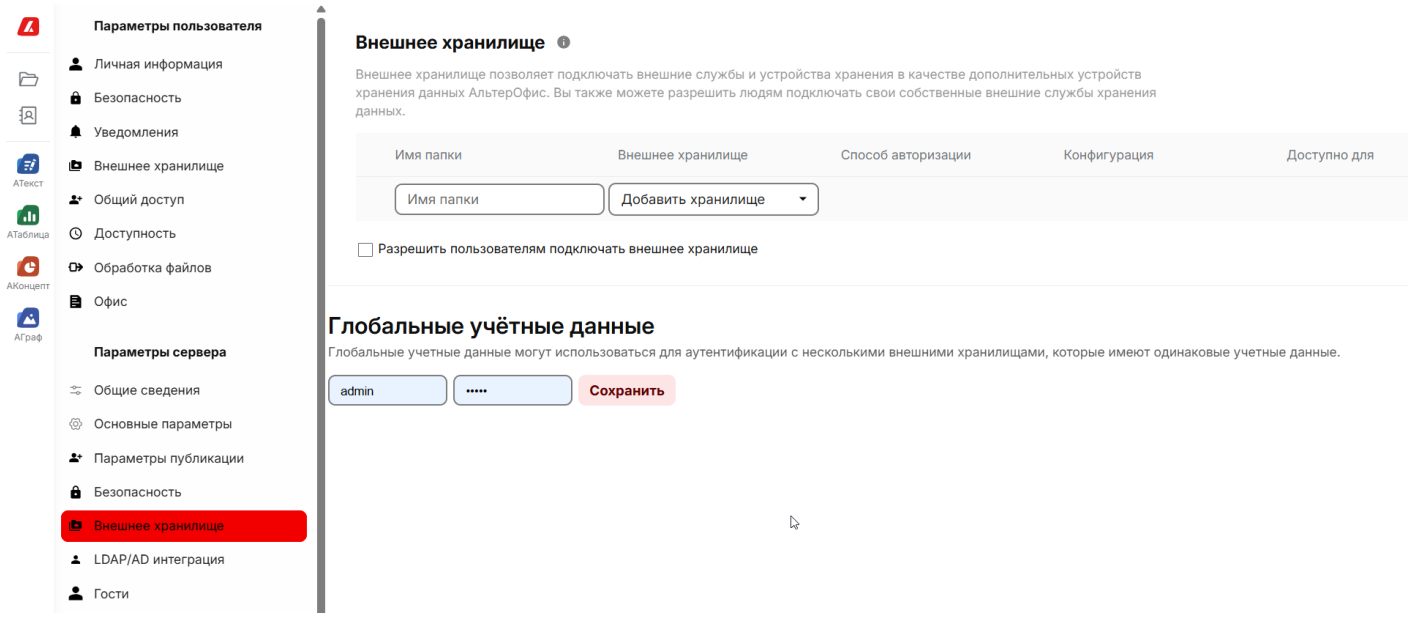


Рисунок 53. Внешнее хранилище

4. Настройте подключение к локальному хранилищу

На странице **«Внешнее хранилище»** заполните поля:

Поле	Описание	Пример
Имя папки	Введите имя, под которым хранилище будет отображаться у пользователей.	Общие документы
Внешнее хранилище	В выпадающем списке выберите «Локально».	Локально
Способ авторизации	Оставьте без изменений	Отсутствует
Конфигурация	В поле «Расположение каталога» укажите абсолютный путь к подготовленной папке на сервере.	/mnt/big_storage
Доступно для	Выберите пользователя или группу, которым будет доступно это хранилище. Чтобы сделать его доступным для всех, выберите «Все».	Все

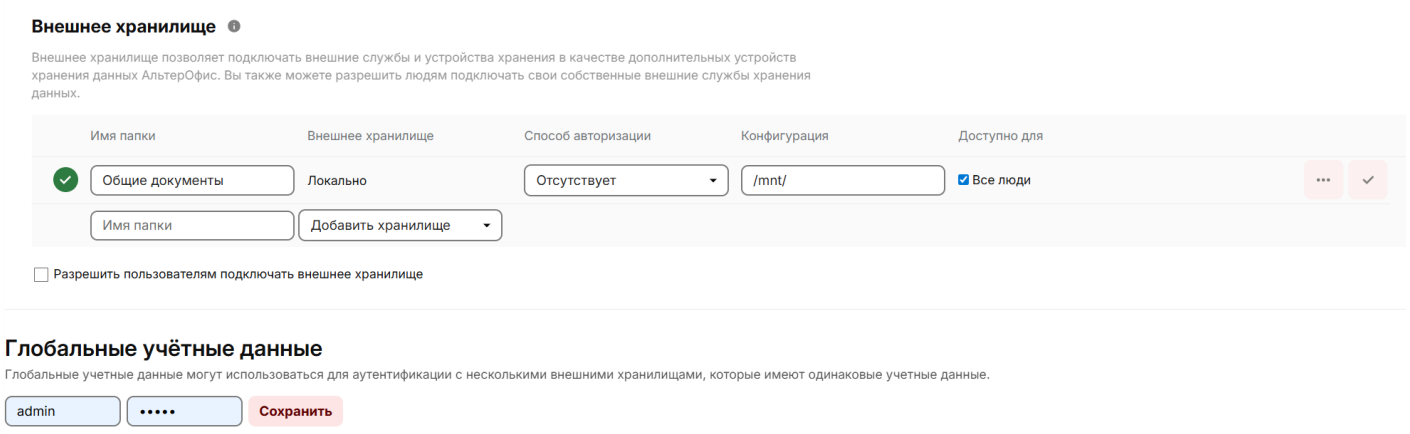


Рисунок 54. Форма настройки локального хранилища

5. Сохраните конфигурацию

Нажмите на кнопку с галочкой справа от формы.

Проверка подключения:

- Если конфигурация верна, слева от названия папки появится зеленая иконка, означающая успешное подключение.
- Красный крестик вместо галочки означает ошибку. Наведите на него курсор, чтобы увидеть описание проблемы (чаще всего — неверный путь или недостаточно прав).

4.6.3. Подключение сетевых дисков

Использование провайдера «SMB/CIFS» позволяет подключить к АльтерОфис Веб файловые ресурсы из вашей локальной сети.

> ПРИМЕЧАНИЕ
>
> Подключение внешнего хранилища по протоколу SMB/CIFS может использоваться:
>
> - В вашей локальной сети есть файловый сервер, к данным которого нужно получать из интерфейса АльтерОфис Веб.
> - Вам нужно предоставить доступ к общим сетевым папкам компании.

1. Предварительные условия для подключения хранилища SMB/CIFS

- Для работы SMB/CIFS на сервере АльтерОфис Веб должен быть установлен пакет *smbclient*.
- Убедитесь, что сервер доступен с хоста АльтерОфис Веб.
- Убедитесь, что имя пользователя и пароль для доступа к общему ресурсу действительны.

2. Проверьте доступность модуля

Перед началом настройки, убедитесь, что активирован модуль **External storage support**.

> СМ. ТАКЖЕ

- Подробнее см. в разделе «Управление приложениями (модулями) системы».

3. Откройте раздел «Внешнее хранилище»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя и в открывшемся меню выберите пункт **«Параметры сервера»**.

В разделе **«Параметры сервера»** выберите пункт **«Внешнее хранилище»**.

3. Настройте подключение к серверному хранилищу

На странице **«Внешнее хранилище»** заполните поля:

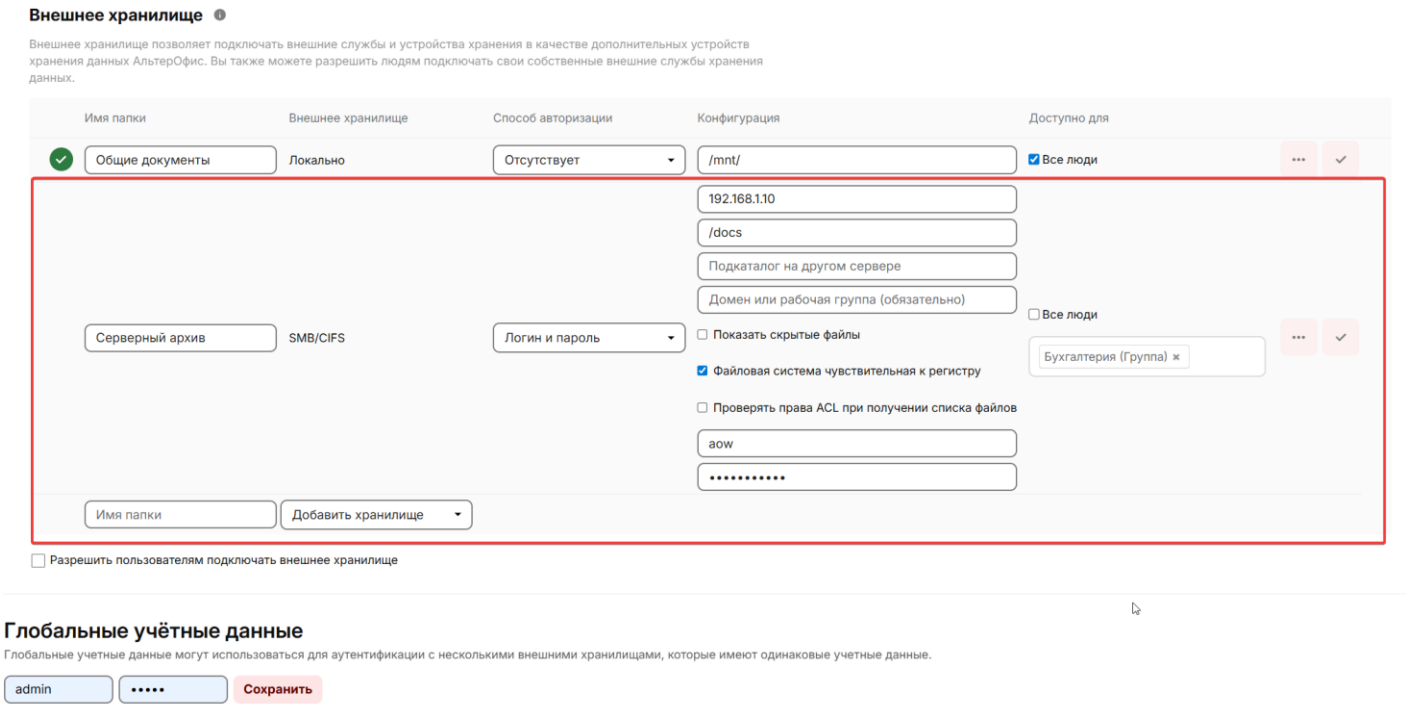


Рисунок 55. Форма настройки хранилища по SMB/CIFS

Поле	Описание	Пример
Имя папки	Введите имя, под которым хранилище будет отображаться у пользователей.	Серверный архив
Внешнее хранилище	В выпадающем списке выберите «SMB/CIFS».	SMB/CIFS
Способ авторизации	В выпадающем списке выберите способ авторизации.	Логин и пароль
Конфигурация / Имя или адрес сервера	IP-адрес или сетевое имя сервера (например, 192.168.1.10 или \fileserver)	192.168.1.10
Конфигурация / Общий ресурс	Удалённая папка	/docs

Поле	Описание	Пример
Конфигурация / Файловая система чувствительная к регистру	Если файловая система различает файлы с именами, которые отличаются только заглавными и строчными буквами, считая «File.txt» и «file.txt» двумя разными файлами, активируйте опцию.	Да
Имя пользователя	Учетные данные для доступа к этому серверу.	aow
Пароль		****
Доступно для	Выберите пользователя или группу, которым будет доступно это хранилище.	Бухгалтерия (Группа)

4. Сохраните конфигурацию

Нажмите на кнопку с галочкой  справа от формы.

4.6.4. Подключение WebDAV-хранилищ

Использование провайдера «WebDAV» позволяет подключить к АльтерОфис Веб сторонние облачные сервисы, создавая единое рабочее пространство для пользователей.

ПРИМЕЧАНИЕ

Используйте подключение по WebDAV, когда:

- Вам нужно подключить другое облако или хостинг, которое поддерживает WebDAV.
- Вы хотите объединить два разных сервера АльтерОфис Веб.

1. Проверьте доступность модуля

Перед началом настройки, убедитесь, что активирован модуль **External storage support**.

СМ. ТАКЖЕ

- Подробнее см. в разделе «Управление приложениями (модулями) системы».

2. Откройте раздел «Внешнее хранилище»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя и в открывшемся меню выберите пункт **«Параметры сервера»**.

В разделе **«Параметры сервера»** выберите пункт **«Внешнее хранилище»**.

3. Настройте подключение к WebDAV-хранилищу

На странице **«Внешнее хранилище»** заполните поля:

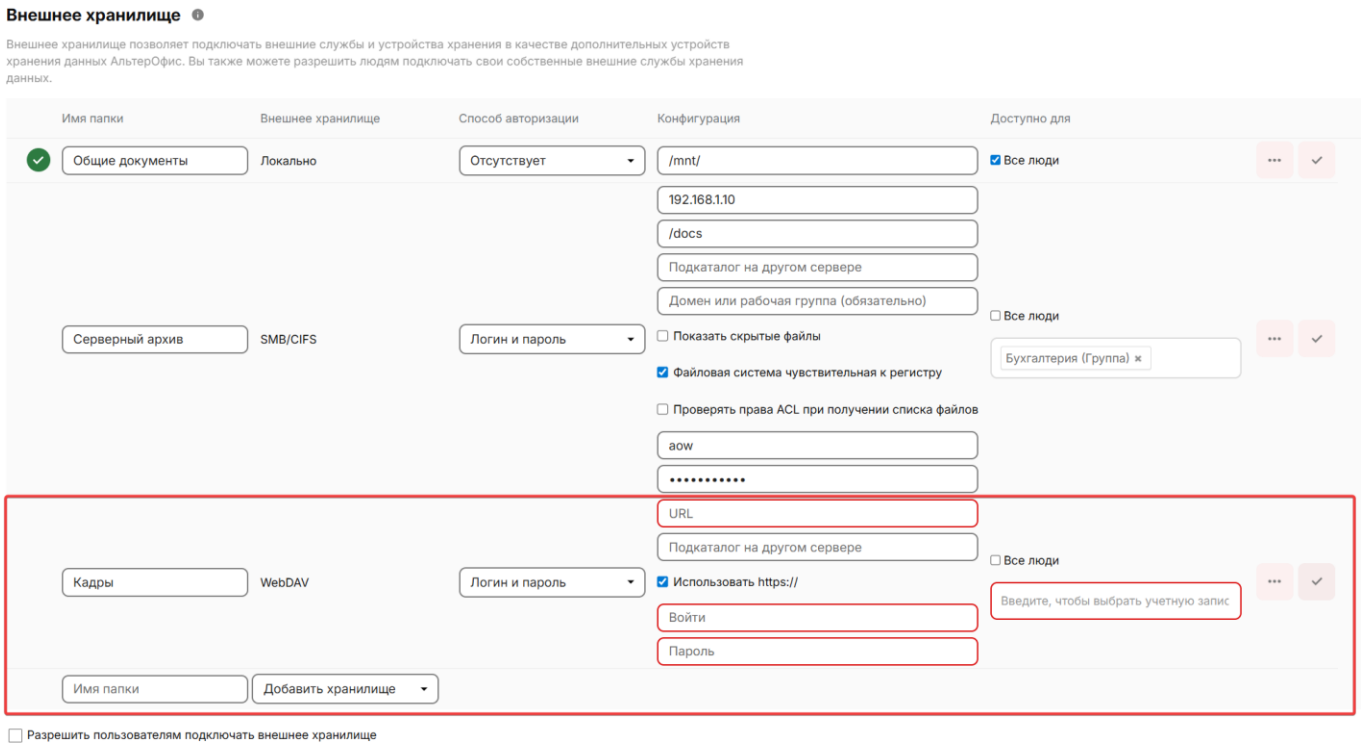


Рисунок 56. Форма настройки хранилища по WebDAV

Поле	**Описание**	**Пример**
Имя папки	Введите имя, под которым хранилище будет отображаться у пользователей.	Кадры
Внешнее хранилище	В выпадающем списке выберите «WebDAV».	WebDAV
Способ авторизации	В выпадающем списке выберите способ авторизации.	Логин и пароль
Конфигурация / URL	Точный URL (например, https://cloud.almipartner.ru/remote.php/dav/files/admin/)	https://cloud.almipartner.ru/remote.php/dav/files/admin/
Конфигурация / Использовать https://	Использовать защищенный протокол. Активируйте опцию, если используется https, а не http	Да
Имя пользователя	Учетные данные для доступа к этому серверу.	aow
Пароль		****
Доступно для	Выберите пользователя или группу, которым будет	Все пользователи (Группа)

Поле	Описание	Пример
	доступно это хранилище.	

4. Сохраните конфигурацию

Нажмите на кнопку с галочкой  справа от формы.

4.6.5. Решение проблемы загрузки файлов во внешнее хранилище по протоколу WebDAV

При подключении внешних хранилищ через провайдер «WebDAV» к другому экземпляру **АльтерОфис Веб** может возникать ошибка загрузки файлов: процесс выполняется аномально медленно и завершается сбоем.

Причины возникновения проблемы

Проблема возникает из-за особенностей механизма обработки временных файлов (`.part`-файлов) в АльтерОфис Веб. Для управления используется системная настройка `part_file_in_storage = true` (значение по умолчанию), которая предполагает:

1. Создание временного файла `filename.part` в целевом хранилище.
2. Загрузку данных в этот временный файл.
3. Атомарное переименование `.part` → `filename` после успешной загрузки.

При работе с **WebDAV-хранилищами** этот механизм вызывает конфликт:

- Протокол WebDAV имеет ограничения в обработке операций переименования файлов.
- Атомарная операция `MOVE` на удалённом сервере не поддерживается в полной мере.
- В результате возникает таймаут или ошибка целостности данных.

ПРЕДУПРЕЖДЕНИЕ

Данное подключение является нестандартным решением. Не рекомендуется для использования в рабочих средах.

Подключение одного экземпляра АльтерОфис Веб к другому через провайдер **«WebDAV»** вместо специализированного провайдера **«АльтерОфис»** нарушает архитектурные принципы платформы и может привести к:

- Потере данных при обрыве соединения.
- Некорректной работе версионирования файлов.
- Ошибкам при обработке комментариев и активности.
- Нестабильной работе приложений, зависящих от файловой системы.

ВНИМАНИЕ

- **Рекомендуемое решение:** Используйте провайдер **«АльтерОфис»** для подключения к другим экземплярам АльтерОфис Веб. Он обеспечивает полную совместимость, поддержку всех функций платформы и надёжную передачу данных.

Решение (временный обходной путь)

> ВНИМАНИЕ
>
> - Данное решение является **временным обходным путём** и применяется только в том случае, если использование провайдера «АльтерОфис» невозможно.

Для устранения проблемы нужно отключить использование временных файлов в целевом хранилище. Для этого изменяется значение настройки `part_file_in_storage` на `false`. Шаги выполнения:

Шаг 1: Подключение к контейнеру.

Подключитесь по `ssh` к серверу, где установлен АльтерОфис Веб.

Используя CLI на хосте с системой выполните команду:

```
docker exec -it <CONTAINER_NAME> ./occ config:system:set part_file_in_storage --type=bool --value=false`
```

В команде замените `<CONTAINER_NAME>` на фактическое имя вашего контейнера.

Пример:

```
docker exec -it demo03-app-1 ./occ config:system:set part_file_in_storage --type=bool --value=false`
```

Шаг 2: Проверка результата

После применения настройки выполните проверочную команду:

```
docker exec -it <CONTAINER_NAME> ./occ config:system:get part_file_in_storage
```

Ожидаемый результат:

```
false
```

После проверки, повторите попытку загрузки файла в внешнее **WebDAV-хранилище**. Он должен успешно загрузиться и быть доступен для работы.

4.7. Интеграция с каталогами пользователей

Для централизованного управления пользователями и их учетными записями в **АльтерОфис Веб** реализована возможность подключения к корпоративным каталогам LDAP или AD. Такой подход позволяет пользователям **АльтерОфис Веб** использовать для входа в систему свои доменные логины без необходимости создавать отдельные учетные записи.

Интеграцию АльтерОфис Веб с LDAP/AD следует использовать, когда в организации уже развернут каталог пользователей (например, FreeIPA или Active Directory).

Интеграция решает следующие задачи:

- Первичная загрузка данных о пользователях из домена.
- Поддержка актуальности данных о пользователях при их изменении в домене.

- Загрузка информации о членстве пользователей в группах.
- Вход пользователей в **АльтерОфис Веб** под корпоративными (доменными) логинами и паролями.
- Централизованное управление учетными записями и правами доступа.

Настройка должна быть выполнена как на стороне серверов (FreeIPA или Active Directory), так и на стороне АльтерОфис Веб.

АльтерОфис Веб может быть настроен на одновременную работу с несколькими доменами, в качестве которых будут выступать несколько LDAP-каталогов (FreeIPA, РЕД АДМ, Active Directory и другие службы каталогов).

4.7.1. Активация модуля LDAP/AD

Перед началом настройки, убедитесь, что модуль **LDAP user and group backend** для работы с пользователями и группами LDAP активирован.

ПРИМЕЧАНИЕ

- Подробнее см. в разделе «Управление приложениями (модулями) системы».
- Проверьте доступность LDAP-сервера: порт 389 (LDAP) или 636 (LDAPS).

Предварительная требования:

- Для работы **LDAP user and group backend** требуется модуль PHP LDAP.
- Для работы серверной части необходима неблокирующая (permissive) или правильно настроенная система SELinux.

4.7.2. Интеграция АльтерОфис Веб с FreeIPA

4.7.2.1. Настройка на стороне FreeIPA

1. Создайте служебную учетную запись в FreeIPA.

Создайте служебную учетную запись, добавьте ее в группу системных пользователей и задайте пароль.

Заполните поля:

Поле	Описание	Пример
Имя учётной записи пользователя	Идентификатор пользователя	aow_admin
Имя	Имя пользователя. Обязательное поле.	aow
Фамилия	Фамилия пользователя. Обязательное поле.	admin
Без личной группы	Отключает автоматическое	Да

Поле	Описание	Пример
	создание персональной группы с тем же именем при создании пользователя в FreeIPA.	
ID группы	Идентификатор группы. Выбрать группу, права которой достаточны для чтения данных из каталога.	1969000000
Новый пароль	Пароль учетной записи	`<password>`
Проверить пароль	Пароль учетной записи	`<password>`

Созданная учетная запись будет использоваться в АльтерОфис Веб для получения данных из каталога FreeIPA.

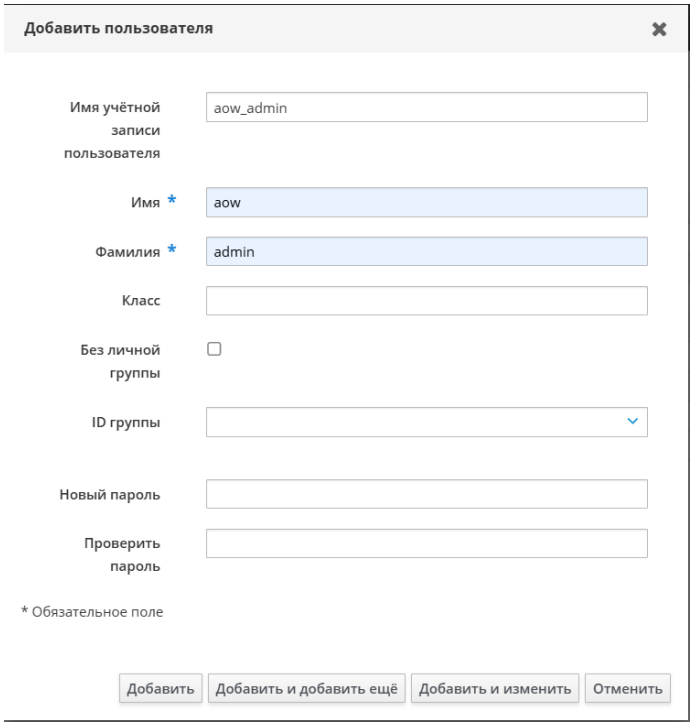


Рисунок 57. Добавление служебной учетной записи

2. Определите Base DN

Чтобы определить Base DN, на сервере FreeIPA выполните команду:

```
cat /etc/ipa/default.conf
```

Поле	Описание	Пример
basedn	BaseDN (Base Distinguished Name, базовое отличительное имя) — это отправная точка в иерархии каталога LDAP, с	`dc=aos,dc=loc`

Поле	Описание	Пример
	которой начинаются все операции поиска.	

Результат выполнения команды:

```
[global]
host = ipa-server.aos.loc
basedn = dc=aos,dc=loc
...
domain = aos.loc
...
```

3. Определите значение IP-адреса или DNS-имя сервера FreeIPA

Имя хоста может быть получено из файла `/etc/ipa/default.conf`, IP адрес с помощью команды:

```
ip a
```

4. Проверьте наличие групп пользователей и пользователей, которые необходимо передавать в АльтерОфис Веб

Пример списка групп пользователей FreeIPA:

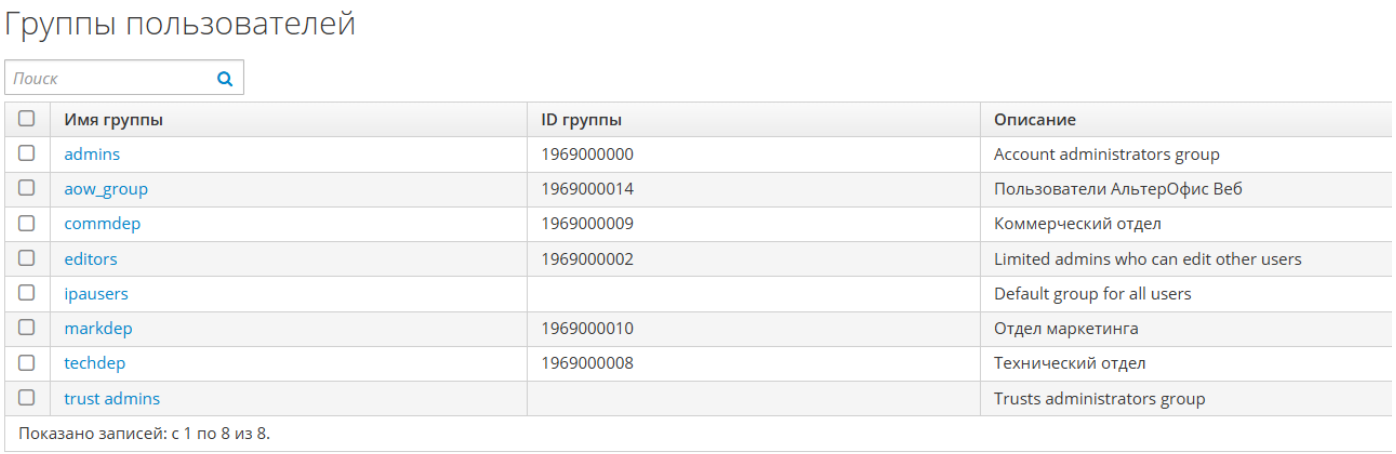


Рисунок 58. Группы пользователей в FreeIPA

Пример списка пользователей FreeIPA:

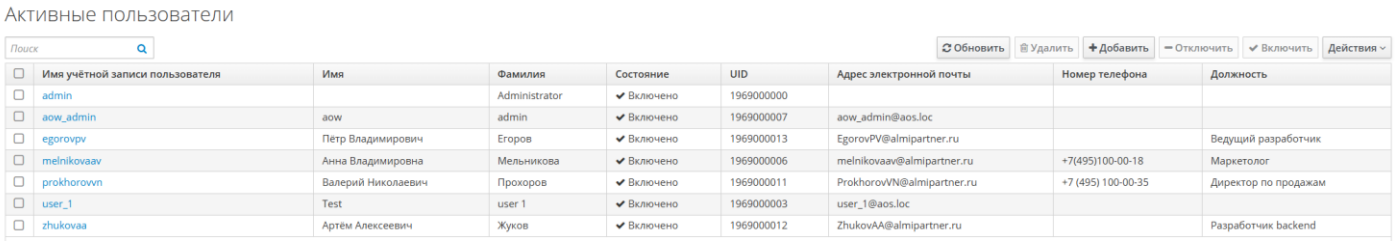


Рисунок 59. Пользователи в FreeIPA

ПРИМЕР

- В FreeIPA настроены группы («aow_group», «commdep», «markdep», «techdep»).
- Пользователи распределены по группам.

4.7.2.2. Настройка на стороне АльтерОфис Веб

1. Откройте раздел «LDAP/AD интеграция»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт **«Параметры сервера»**.

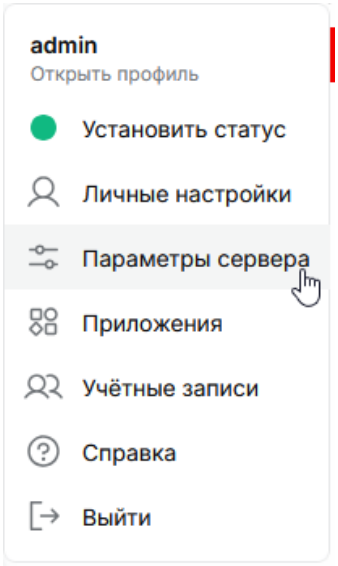


Рисунок 60. Меню администратора

В разделе **«Параметры сервера»** выберите пункт **«LDAP/AD интеграция»**.

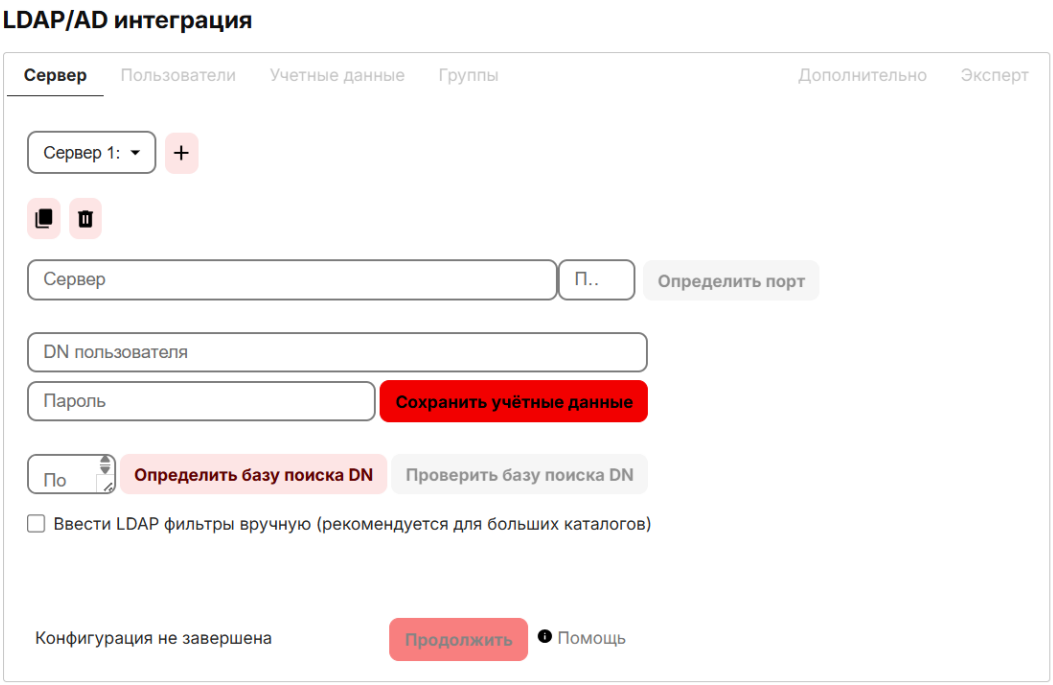


Рисунок 61. Настройка LDAP

Настройка LDAP осуществляется путем последовательного заполнения полей формы на шести вкладках: «Сервер», «Пользователи», «Учетные данные», «Группы», «Дополнительно» и «Эксперт».

2. Выполните настройки на вкладке «Сервер»

Настройка начинается с вкладки «Сервер», для доступа к другим вкладкам необходимо правильно заполнить первую вкладку («Сервер»). Если конфигурация выполнена правильно, загорается зеленый индикатор.

На вкладке **«Сервер»** заполните поля:

Поле	**Описание**	**Пример**
Сервер	IP-адрес или DNS имя контроллера домена FreeIPA.	ipa-server.aos.loc
Порт	Порт подключения к LDAP-каталогу.	389
DN пользователя	Имя пользователя домена, от имени которого АльтерОфис Веб будет опрашивать LDAP.	uid=aow_admin,cn=users,cn=accounts,dc=aos,dc=loc
Пароль	Пароль пользователя домена.	`<aow_admin_password>`

ПРИМЕЧАНИЕ

- Если используется протокол LDAPS и нужно, чтобы соединение с самоподписанным сертификатом не проверялось, выполните действия:
- Перейдите на вкладку **Дополнительно**.

- Проверьте настройку параметра «Отключить проверку сертификата SSL» (для отключения проверки нужно активировать параметр).
- Требования к указанию учётной записи пользователя в поле «DN пользователя» может отличаться для разных реализаций LDAP.

После ввода имени пользователя и пароля нажмите кнопку **«Сохранить учётные данные»**.

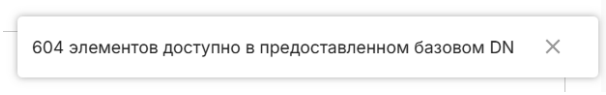
Для определения базы поиска пользователей и групп нажмите кнопку «Определить базу поиска DN».

При необходимости введите значение вручную.

Поле	Описание	Пример
Base DN	Объект каталога, начиная с которого производится поиск. Это поле обязательно для заполнения.	dc=aos,dc=loc

Нажмите кнопку **«Проверить базу поиска DN»**.

При успешной проверке отобразится:

- информация 

,
- внизу загорится зеленый индикатор *Конфигурация в порядке*.

Установите флаг **«Ввести LDAP фильтры вручную (рекомендуется для больших каталогов)»**.

Нажмите кнопку **«Продолжить»**.

3. Выполните настройки на вкладке «Пользователи»

На вкладке **«Пользователи»** определите, какие пользователи LDAP должны быть указаны в качестве пользователей **АльтерОфис Веб**.

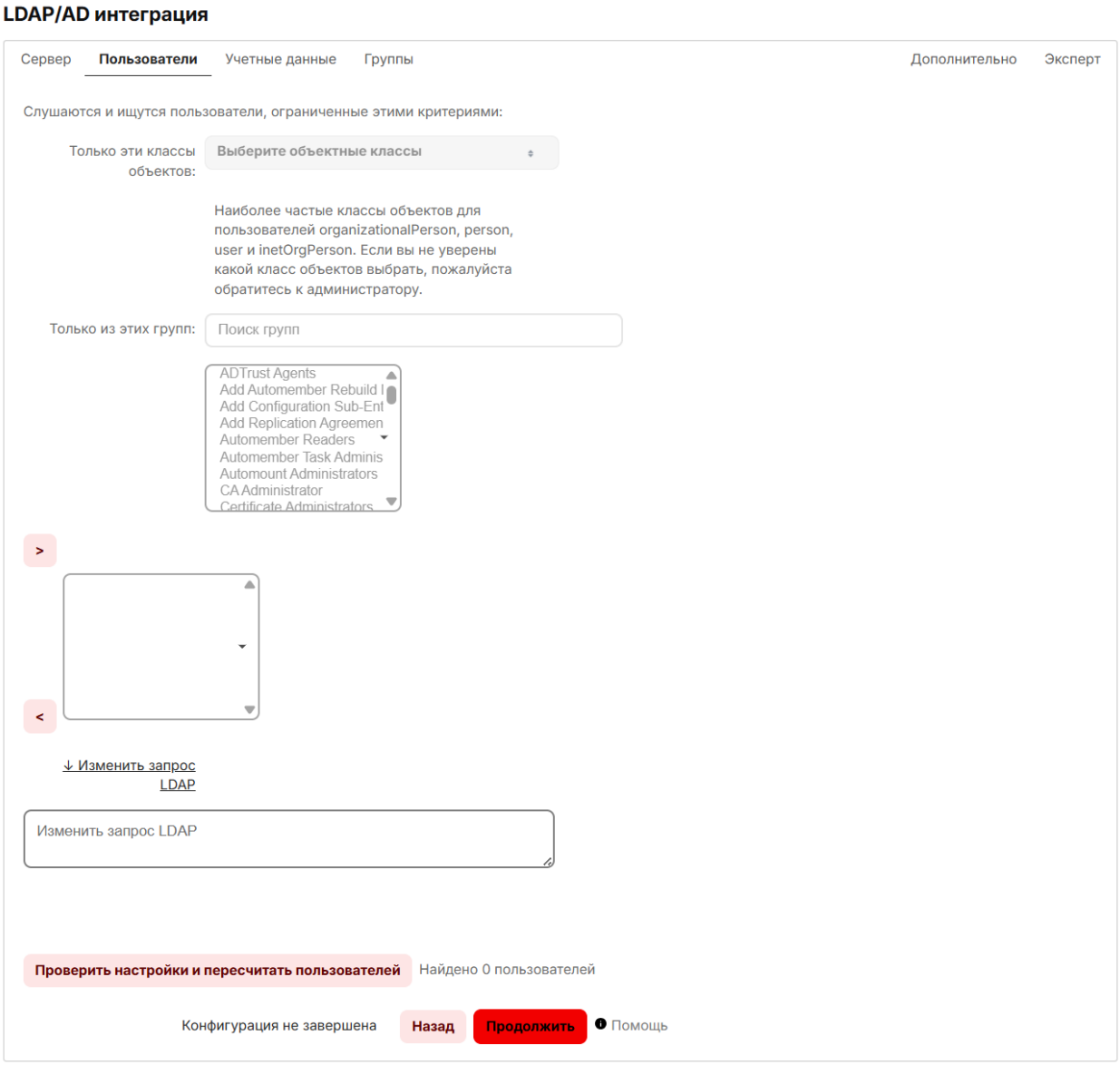


Рисунок 62. Настройка LDAP, вкладка «Пользователи»

Для определения списка пользователей используйте LDAP-фильтр.

LDAP-фильтр может быть задан с помощью мастера или в явном виде.

Для использования мастера, нажмите на ссылку **Изменить запрос LDAP**. Включится режим, при котором можно определить классы объектов и группы, из которых необходимо фильтровать пользователей, путем выбора из списков.

Укажите фильтр поиска пользователей:

Поле	Описание	Пример
Изменить запрос LDAP	Фильтр LDAP для поиска пользователей.	`(|(objectclass=inetorgperson)(objectclass=person))`

Нажмите кнопку **«Проверить настройки и пересчитать пользователей»**. Будет отображено количество найденных пользователей, входящих в настроенный фильтр.

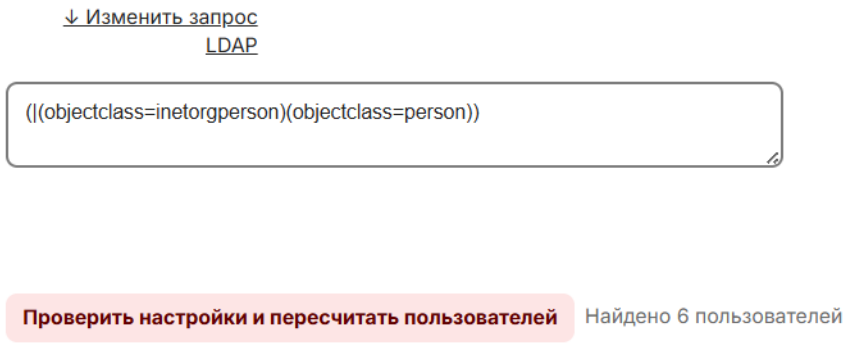


Рисунок 63. Настройка фильтра LDAP для поиска пользователей

Убедитесь, что с использованным фильтром пользователи найдены.

Нажмите кнопку **«Продолжить»**.

4. Выполните настройки на вкладке «Учетные данные»

На вкладке **«Учетные данные»** определите, какие пользователи LDAP могут входить в систему **АльтерОфис Веб** и по какому атрибуту или атрибутам сопоставляется указанное имя для входа (например, имя пользователя LDAP/AD, адрес электронной почты).

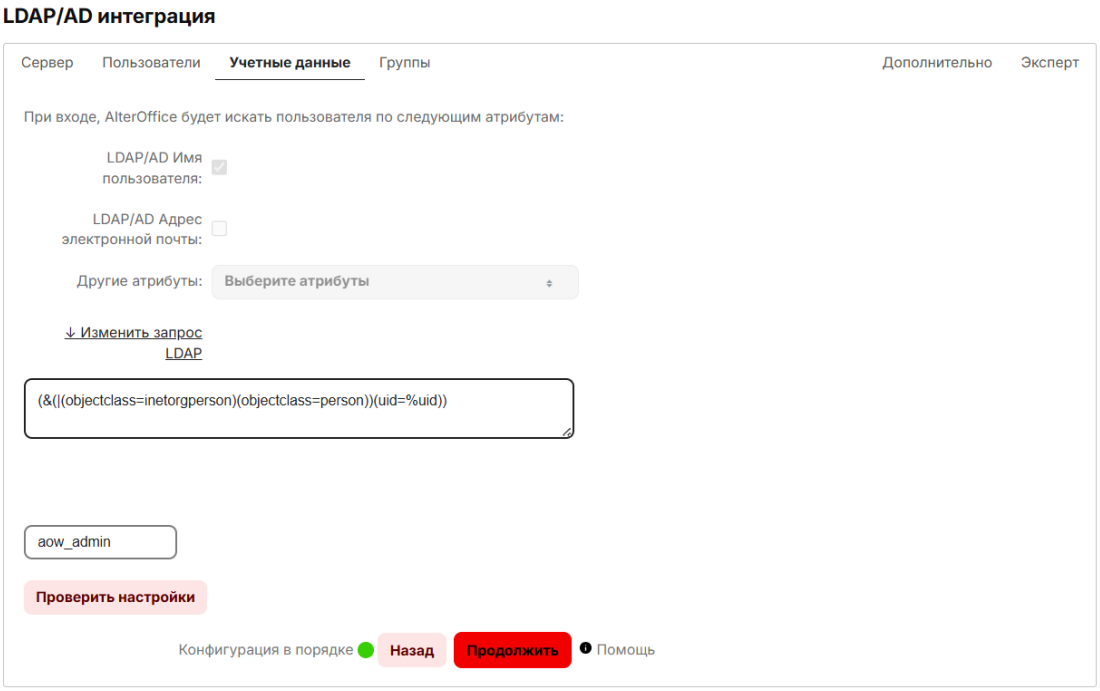


Рисунок 64. Настройка LDAP, вкладка «Учетные данные»

Укажите фильтр LDAP вручную или воспользуйтесь режимом выбора атрибутов.

Поле	Описание	Пример

Поле	Описание	Пример
Изменить запрос LDAP	Фильтр для определения атрибутов, которые будут использоваться в качестве логина пользователя.	`(&(|(objectclass=inetorgperson)(objectclass=person))(uid=%uid))`

Фильтр определяет атрибуты для входа в систему:

- `(&(|(objectclass=person))(|(uid=%uid)(|(mailPrimaryAddress=%uid)(mail=%uid))))` — в качестве логина можно использовать имя пользователя или адрес электронной почты;
- `(&(|(objectclass=inetorgperson)(objectclass=person))(uid=%uid))` — в качестве логина можно использовать имя пользователя.

В поле **«Проверить логин»** введите имя существующего пользователя в FreeIPA, например `aow_admin`.

Нажмите кнопку **«Проверить настройки»**. При успешной проверке выведется сообщение «Пользователь найден и настройки проверены».

После успешной проверки, нажмите кнопку **«Продолжить»**.

5. Выполните настройки на вкладке «Группы»

На вкладке **«Группы»** определите, какие группы LDAP должны быть доступны в **АльтерОфис Веб**.

Настройте поля:

Поле	Описание	Пример
Только эти классы объектов	В списке отображены только те классы объектов, которые возвращают хотя бы один групповой объект. Вы можете выбрать несколько классов объектов.	ipausergroup

Из раскрывающегося списка выберите необходимые классы объектов.

Выберите нужную группу в поле **«Только из этих групп»**, чтобы переместить группу в список выбранных групп, нажмите >.

Поле	Описание	Пример
Только из этих групп	Выбрать группы, которым будет предоставлен доступ к АльтерОфис Веб.	commdep, markdep, techdep

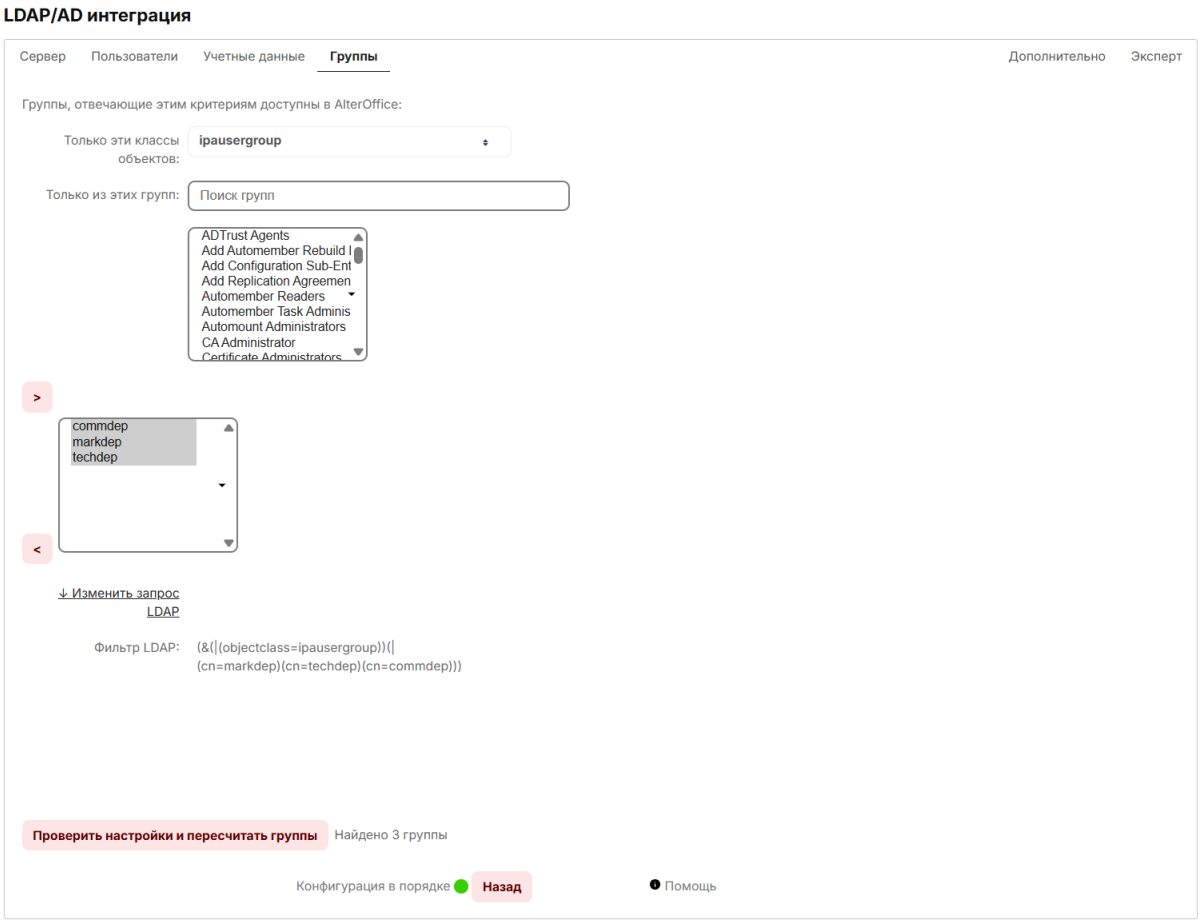


Рисунок 65. Настройка LDAP, вкладка «Группы»

Нажмите кнопку **«Проверить настройки и пересчитать группы»**. Будет отображено количество найденных групп, входящих в настроенный фильтр.

6. Выполните настройки на вкладке «Дополнительно»

На вкладке можно настроить импортируемые атрибуты пользователя из FreeIPA.

Например, если в поле «Поле отображаемого имени пользователя» указать значение `givenName`, то в качестве отображаемого имени пользователя в АльтерОфис Веб будет загружено имя пользователя.

Пример допустимых атрибутов:

Атрибут	Значение	Пример значения
displayName	ФИО	Петров Иван Сергеевич
givenName	Имя	Иван Иван Сергеевич
uid	Имя входа пользователя	petrovIS
gidNumber	Идентификатор группы	1969000010

Атрибут	Значение	Пример значения
cn	Код группы	markdep
description	Описание группы	Отдел маркетинга

Исчерпывающий перечень доступных для загрузки атрибутов содержится в документации на FreeIPA.

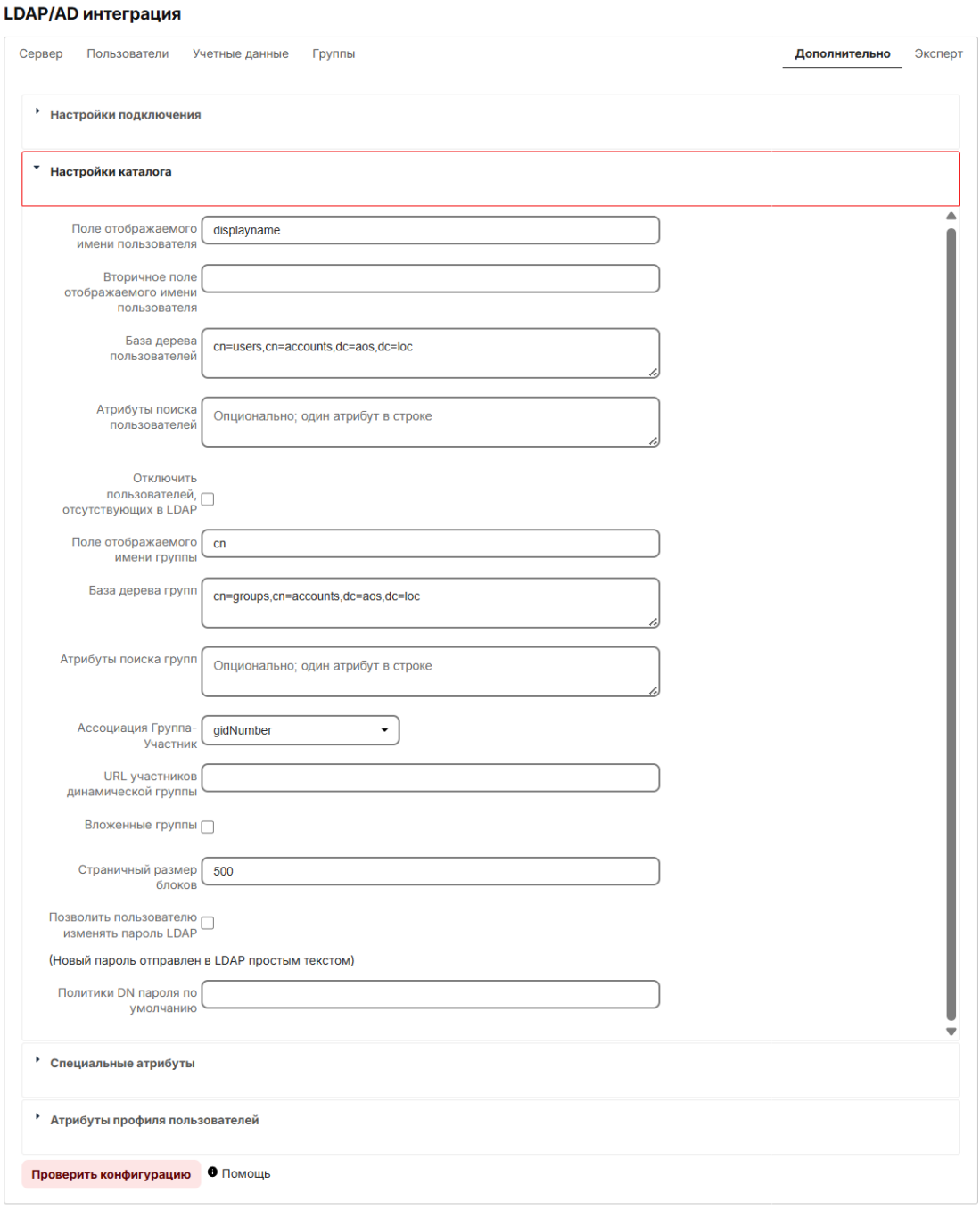


Рисунок 66. Настройка LDAP, вкладка «Дополнительно»

Заполните поля в разделе «Настройки каталога»:

Поле	**Описание**	**Пример**
Поле отображаемого имени	Атрибут для определения	`displayname`

Поле	Описание	Пример
пользователя	выводимого имени пользователя	
База дерева пользователей	Путь поиска атрибута для пользователей	`cn=users,cn=accounts,dc=aos,dc=loc`
Поле отображаемого имени группы	Атрибут для определения выводимого названия группы	`cn`
База дерева групп	Путь поиска атрибута для групп	`cn=groups,cn=accounts,dc=aos,dc=loc`

7. Выполните настройки на вкладке «Эксперт»

На вкладке можно определить на основе какого атрибута будет создаваться внутреннее имя пользователя при импорте данных из FreeIPA. Внутреннее имя пользователя используется для внутренней идентификации пользователя. Оно также является именем по умолчанию для домашней папки пользователя. Оно также является частью удалённых URL-адресов, например, для всех служб DAV.

ПРИМЕР

- Если в поле «Атрибут для внутреннего имени» указать значение `gidNumber`, то при импорте данных из FreeIPA создастся пользователь, у которого в качестве имени будет идентификатор `1969000008`.

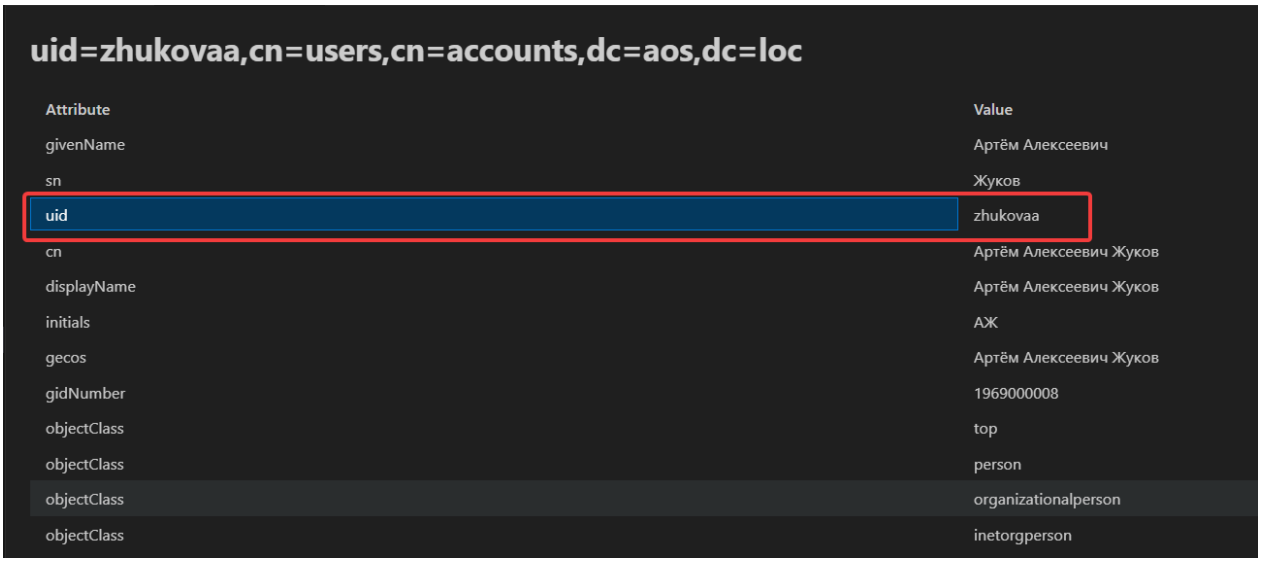


Рисунок 67. Параметры учетной записи в каталоге

Если предполагается, что учетные записи из FreeIPA не будут пересекаться с именами пользователей, созданные вручную в системе, то можно использовать атрибут `uid`, и папки пользователей будут иметь вид `zhukovaa`.

При использовании нескольких доменов для аутентификации пользователей, необходимо продумать именование внутренних имен пользователей, чтобы исключить пересечения имен.

8. Завершение

Настройка LDAP в АльтерОфис Веб успешно завершена, если на вкладках **«Сервер»**, **«Пользователи»**, **«Учетные данные»**, **«Группы»** отображается индикатор **Конфигурация в порядке**.

Рисунок 68. Конфигурация в порядке

Откройте раздел «Учетные записи» и убедитесь, что отображаются пользователи из каталога FreeIPA и пользователи корректно отнесены к группам.

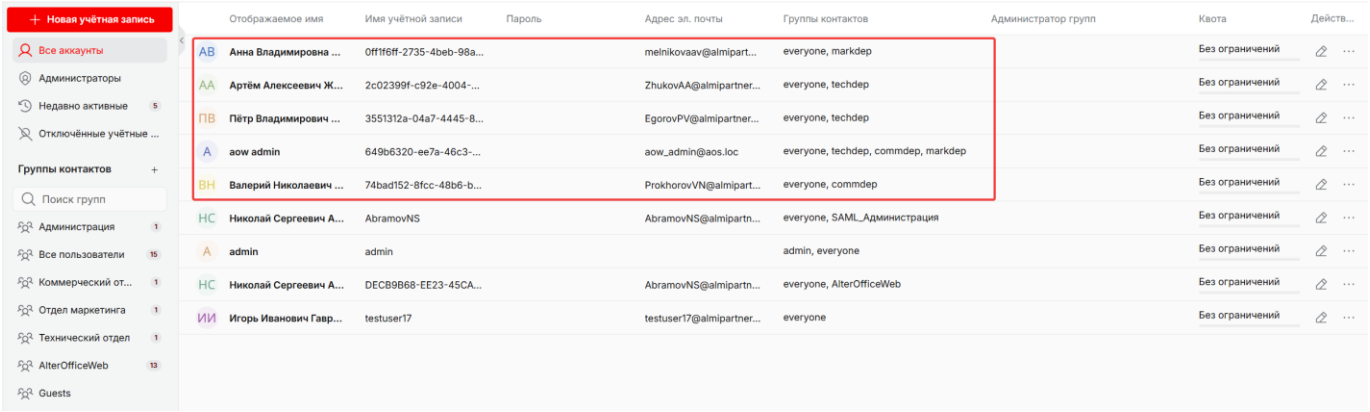


Рисунок 69. Учетные записи пользователей

4.7.3. Интеграция АльтерОфис Веб с РЕД АДМ

4.7.3.1. Настройка на стороне РЕД АДМ

1. Создайте служебную учетную запись в РЕД АДМ.

Создайте служебную учетную запись для получения данных (чтения) из каталога РЕД АДМ.

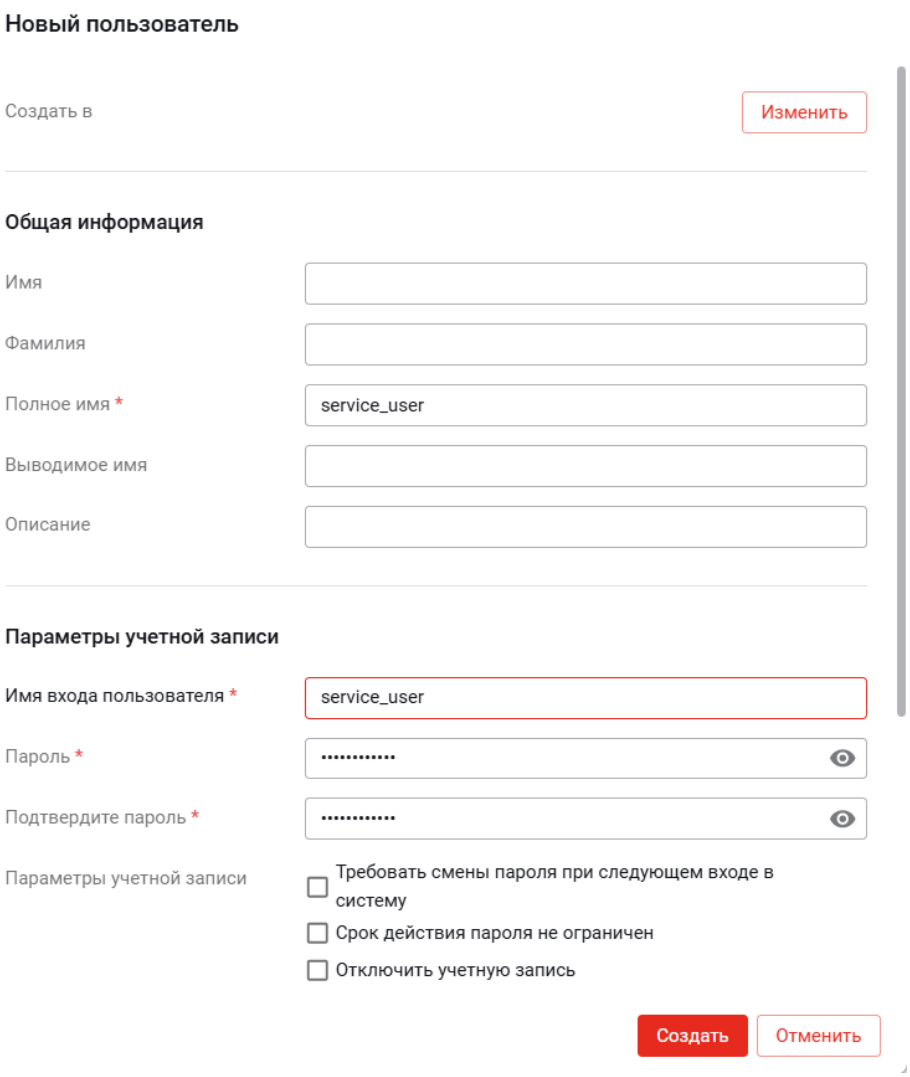


Рисунок 70. Добавление служебной учетной записи

Заполните поля:

Поле	**Описание**	**Пример**
Полное имя	Отображаемое имя пользователя. Обязательное поле.	service_user
Имя входа пользователя	Идентификатор пользователя	service_user
Пароль	Пароль учетной записи	`<password>`
Подтвердите пароль	Пароль учетной записи	`<password>`

Назначьте пользователю права, достаточные для получения (чтения) данных из каталога РЕД АДМ.

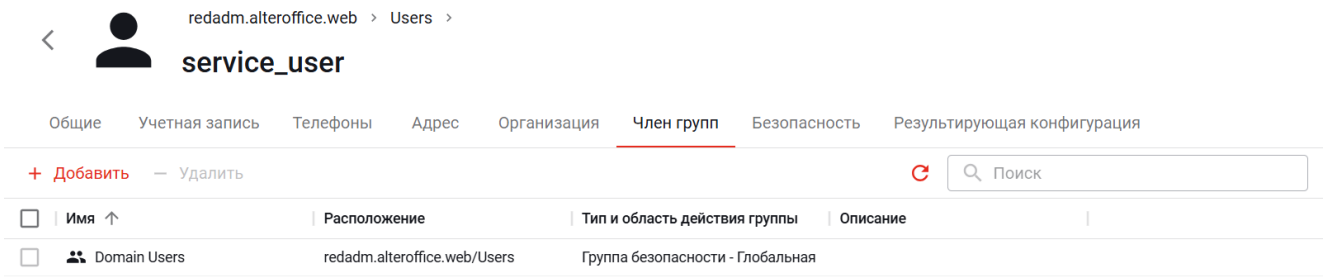


Рисунок 71. Настройка членства в группе

Созданная учетная запись будет использоваться в АльтерОфис Веб для получения данных из каталога РЕД АДМ.

2. Определите Base DN

Для настройки интеграции необходимо значение Base DN.

Определите любым удобным способом. Например через веб-интерфейс РЕД АДМ.

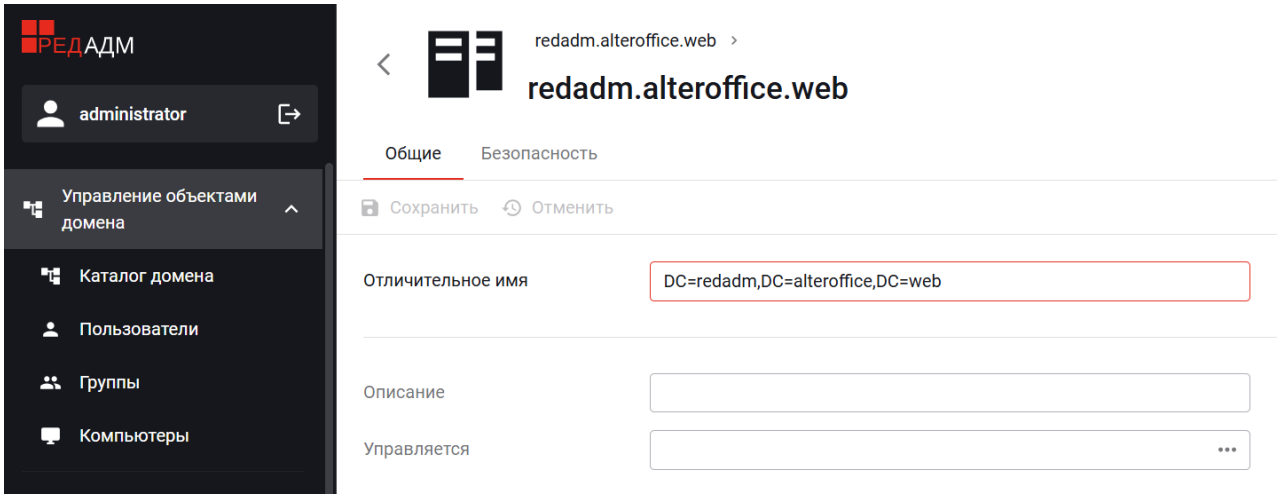


Рисунок 72. Определение базового отличительного имени

Поле	Описание	Пример
basedn	BaseDN (Base Distinguished Name, базовое отличительное имя) — это отправная точка в иерархии каталога LDAP, с которой начинаются все операции поиска.	`DC=redadm,DC=alteroffice,DC=web`

3. Определите значение IP-адреса или DNS-имя сервера РЕД АДМ

IP адрес сервера РЕД АДМ определите, например с помощью команды:

```
ip a
```

4. Проверьте наличие групп пользователей и пользователей, которые необходимо передавать в АльтерОфис Веб

Пример списка групп пользователей РЕД АДМ:

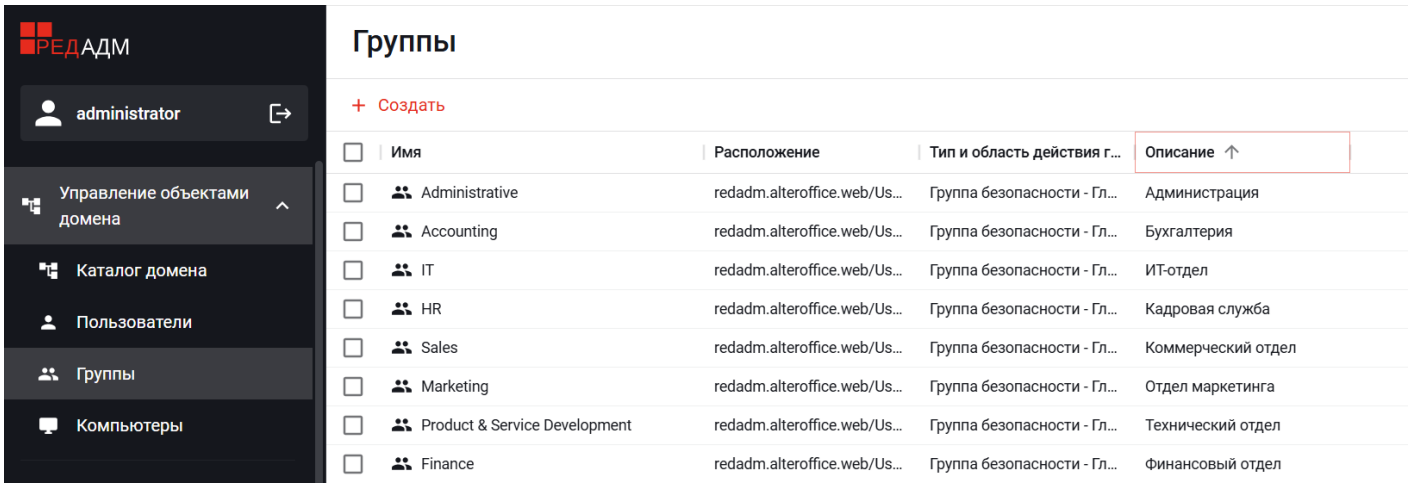


Рисунок 73. Группы пользователей в РЕД АДМ

Пример списка пользователей РЕД АДМ:

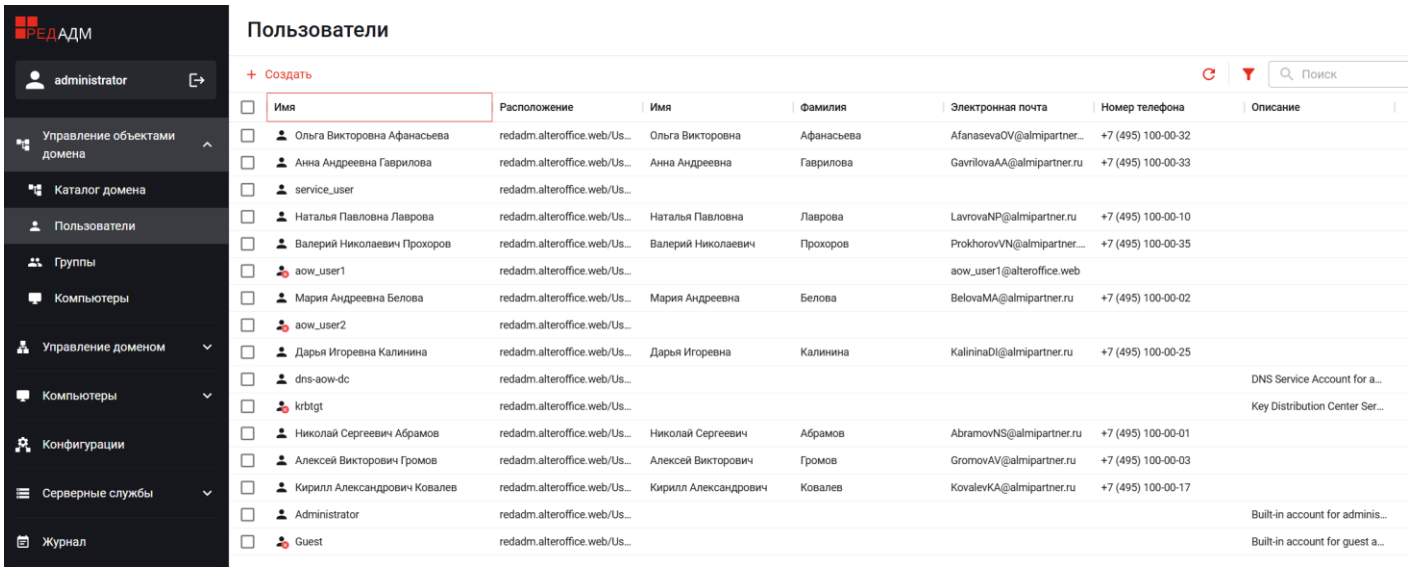


Рисунок 74. Пользователи в РЕД АДМ

Для удобства администрирования, может быть создана отдельная группа, в которую будут входить пользователи, работающие с АльтерОфис Веб.

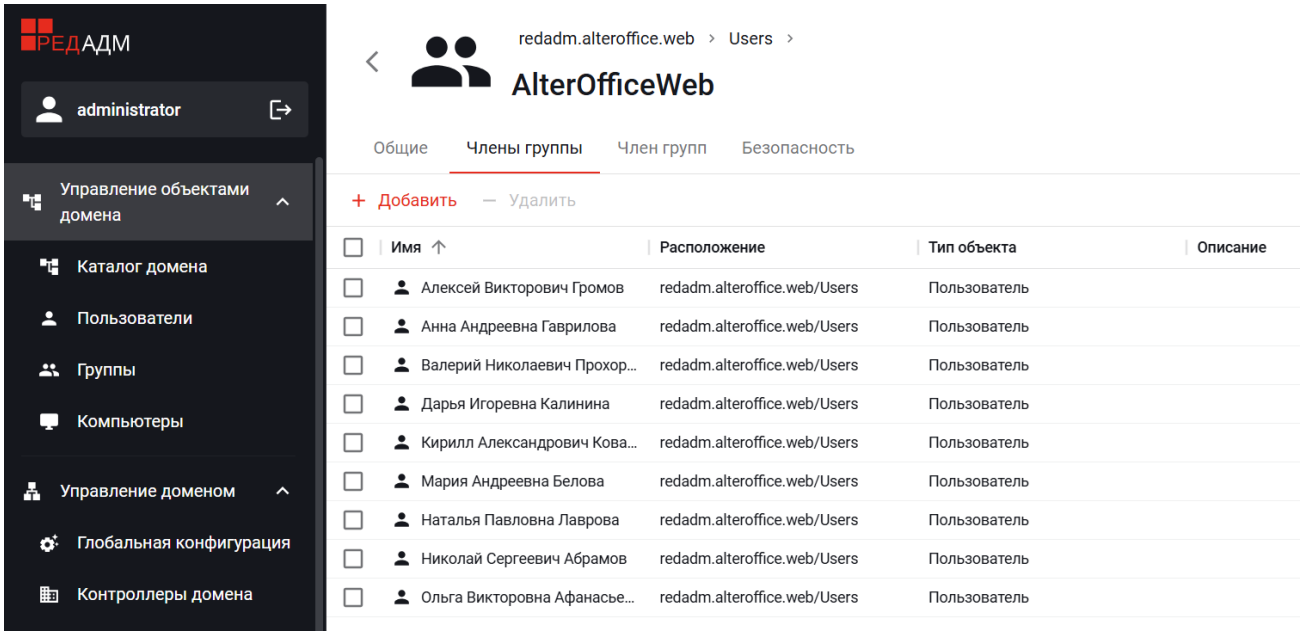


Рисунок 75. Пользователи группы AlterOfficeWeb

4.7.3.2. Настройка на стороне АльтерОфис Веб

1. Откройте раздел «LDAP/AD интеграция»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт **«Параметры сервера»**.

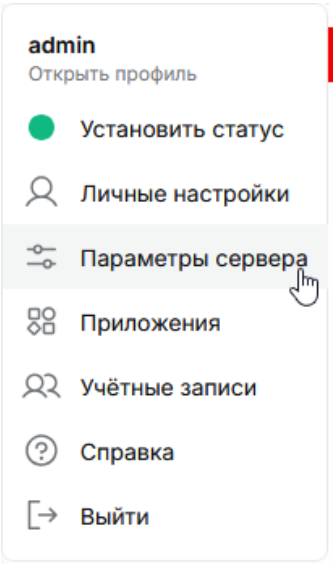


Рисунок 76. Меню администратора

В разделе **«Параметры сервера»** выберите пункт **«LDAP/AD интеграция»**.

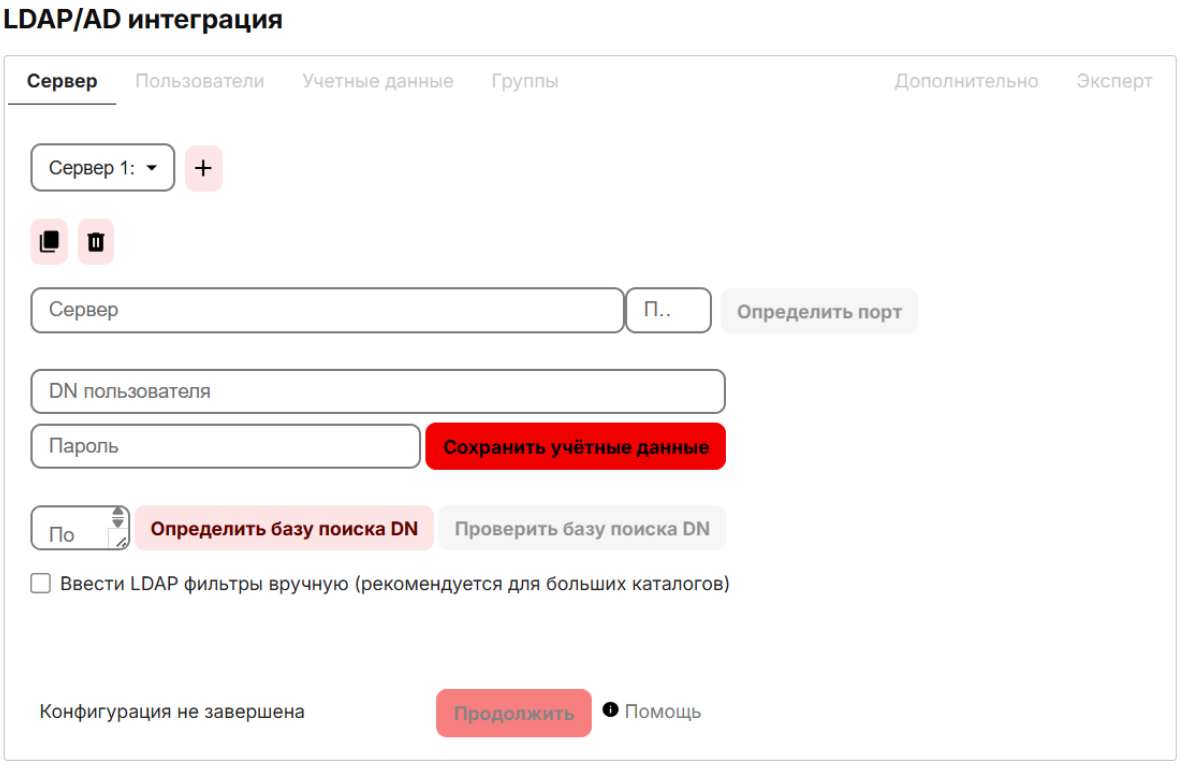


Рисунок 77. Настройка LDAP

Настройка LDAP осуществляется путем последовательного заполнения полей формы на шести вкладках: «Сервер», «Пользователи», «Учетные данные», «Группы», «Дополнительно» и «Эксперт».

2. Выполните настройки на вкладке «Сервер»

Настройка начинается с вкладки «Сервер», для доступа к другим вкладкам необходимо правильно заполнить первую вкладку («Сервер»). Если конфигурация выполнена правильно, загорается зеленый индикатор.

На вкладке **«Сервер»** заполните поля:

Поле	**Описание**	**Пример**
Сервер	IP-адрес или DNS имя контроллера домена РЕД АДМ.	172.20.3.14
Порт	Порт, через который осуществляется подключение к серверу LDAP.	389
DN пользователя	Имя пользователя домена, от имени которого АльтерОфис Веб будет опрашивать LDAP.	CN=service_user,CN=Users,DC=redadm,DC=alteroffice,DC=web
Пароль	Пароль пользователя домена.	`<service_user_password>`

ПРИМЕЧАНИЕ

- Требования к указанию учётной записи пользователя в поле «DN пользователя» может отличаться для разных реализаций LDAP.
- Сервер может быть указан в виде URI, например `ldaps://172.20.3.14:636`

После ввода имени пользователя и пароля нажмите кнопку **«Сохранить учётные данные»**.

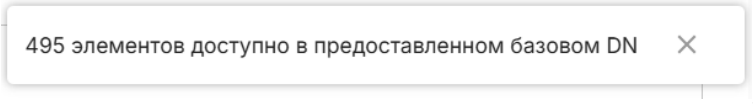
Для определения базы поиска пользователей и групп нажмите кнопку «Определить базу поиска DN».

При необходимости введите значение вручную.

Поле	Описание	Пример
Base DN	Объект каталога, начиная с которого производится поиск. Это поле обязательно для заполнения.	DC=redadm,DC=alteroffice,DC=web

Нажмите кнопку **«Проверить базу поиска DN»**.

При успешной проверке отобразится:

- информация 

,
- внизу загорится зеленый индикатор *Конфигурация в порядке*.

Установите флаг **«Ввести LDAP фильтры вручную (рекомендуется для больших каталогов)»**.

Нажмите кнопку **«Продолжить»**.

3. Выполните настройки на вкладке «Пользователи»

На вкладке **«Пользователи»** определите, какие пользователи LDAP должны быть указаны в качестве пользователей **АльтерОфис Веб**.

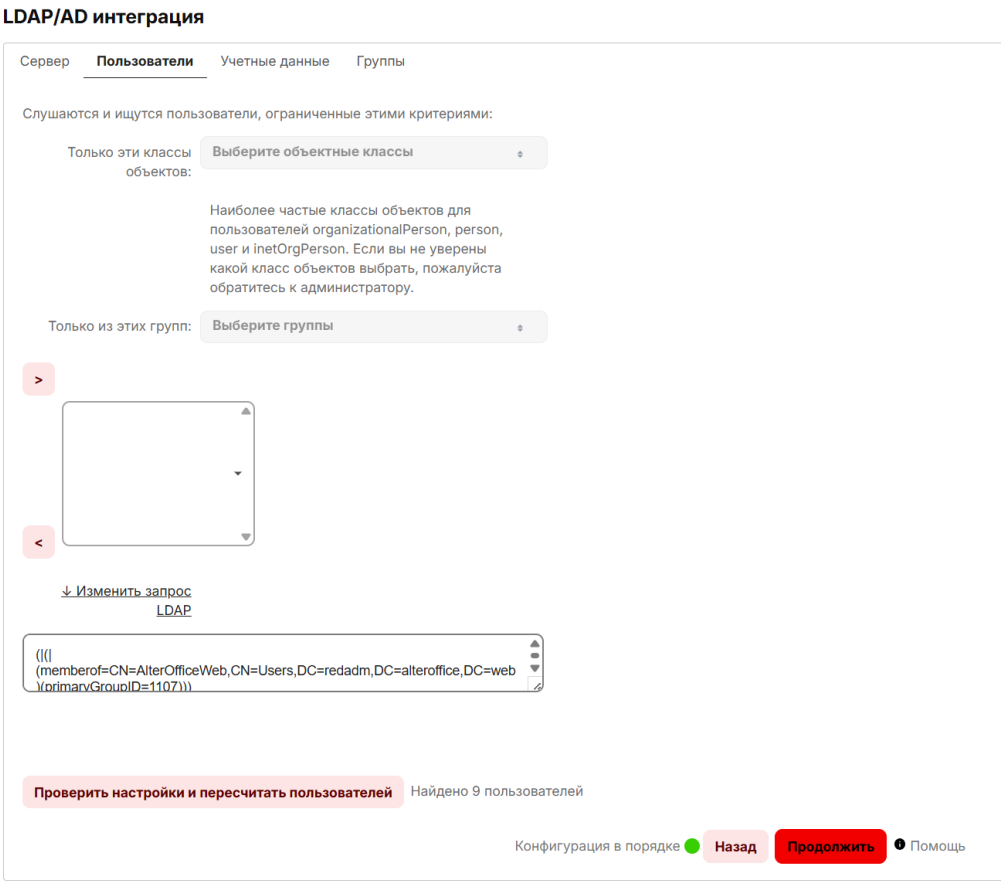


Рисунок 78. Настройка LDAP, вкладка «Пользователи»

Для определения списка пользователей используйте LDAP-фильтр.

LDAP-фильтр может быть задан с помощью мастера или в явном виде.

Для использования мастера, нажмите на ссылку **Изменить запрос LDAP**. Включится режим, при котором можно определить классы объектов и группы, из которых необходимо фильтровать пользователей, путем выбора из списков.

Укажите фильтр поиска пользователей:

Поле	**Описание**	**Пример**
Изменить запрос LDAP	Фильтр LDAP для поиска пользователей.	`(|(|(memberof=CN=AlterOfficeWeb,CN=Users,DC=redadm,DC=alteroffice,DC=web)(primaryGroupID=1107)))`

Нажмите кнопку **«Проверить настройки и пересчитать пользователей»**. Будет отображено количество найденных пользователей, входящих в настроенный фильтр.

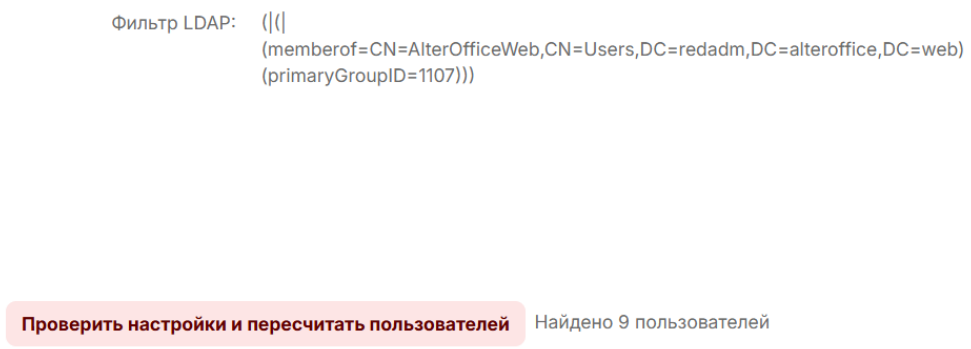


Рисунок 79. Настройка фильтра LDAP для поиска пользователей

Убедитесь, что с использованным фильтром пользователи найдены.

Нажмите кнопку **«Продолжить»**.

4. Выполните настройки на вкладке «Учетные данные»

На вкладке **«Учетные данные»** определите, какие пользователи LDAP могут входить в систему **АльтерОфис Веб** и по какому атрибуту или атрибутам сопоставляется указанное имя для входа (например, имя пользователя LDAP/AD, адрес электронной почты).

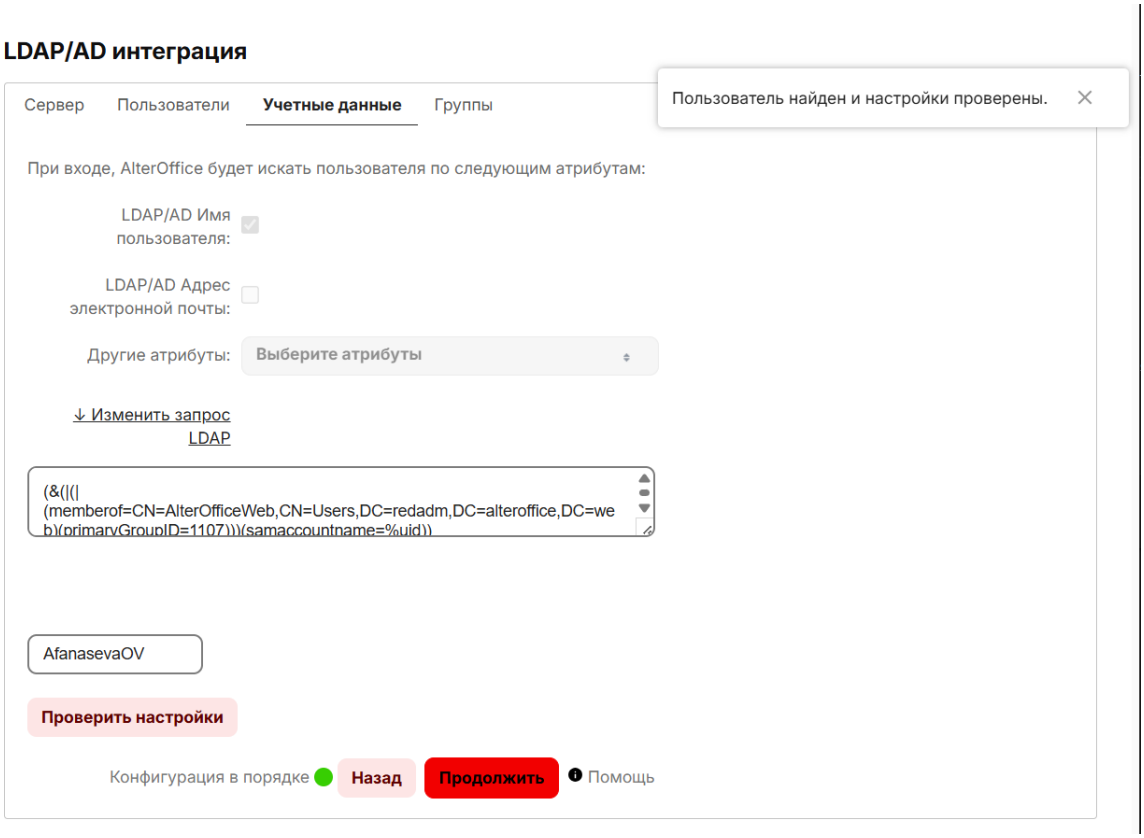


Рисунок 80. Настройка LDAP, вкладка «Учетные данные»

Укажите фильтр LDAP вручную или воспользуйтесь режимом выбора атрибутов.

Поле	Описание	Пример
Изменить запрос LDAP	Фильтр для определения атрибутов, которые будут использоваться в качестве логина пользователя.	`(&(|(|(memberof=CN=AlterOfficeWeb,CN=Users,DC=redadm,DC=alteroffice,DC=web)(primaryGroupID=1107)))(samaccountname=%uid))`

В поле **«Проверить логин»** введите имя существующего пользователя в РЕД АДМ, например `AfanasevaOV`.

Нажмите кнопку **«Проверить настройки»**. При успешной проверке выведется сообщение «Пользователь найден и настройки проверены».

После успешной проверки, нажмите кнопку **«Продолжить»**.

5. Выполните настройки на вкладке «Группы»

На вкладке **«Группы»** определите, какие группы из РЕД АДМ должны быть доступны в **АльтерОфис Веб**.

Настройте поля:

Поле	Описание	Пример
Только эти классы объектов	В списке отображены только те классы объектов, которые возвращают хотя бы один групповой объект. Вы можете выбрать несколько классов объектов.	group

Из раскрывающегося списка выберите необходимые классы объектов.

Выберите нужную группу в поле **«Только из этих групп»**, чтобы переместить группу в список выбранных групп, нажмите >.

Поле	Описание	Пример
Только из этих групп	Выбрать группы, которым будет предоставлен доступ к АльтерОфис Веб.	Administrative, Accounting, IT, HR, Sales, Marketing, Product & Service Development, Finance

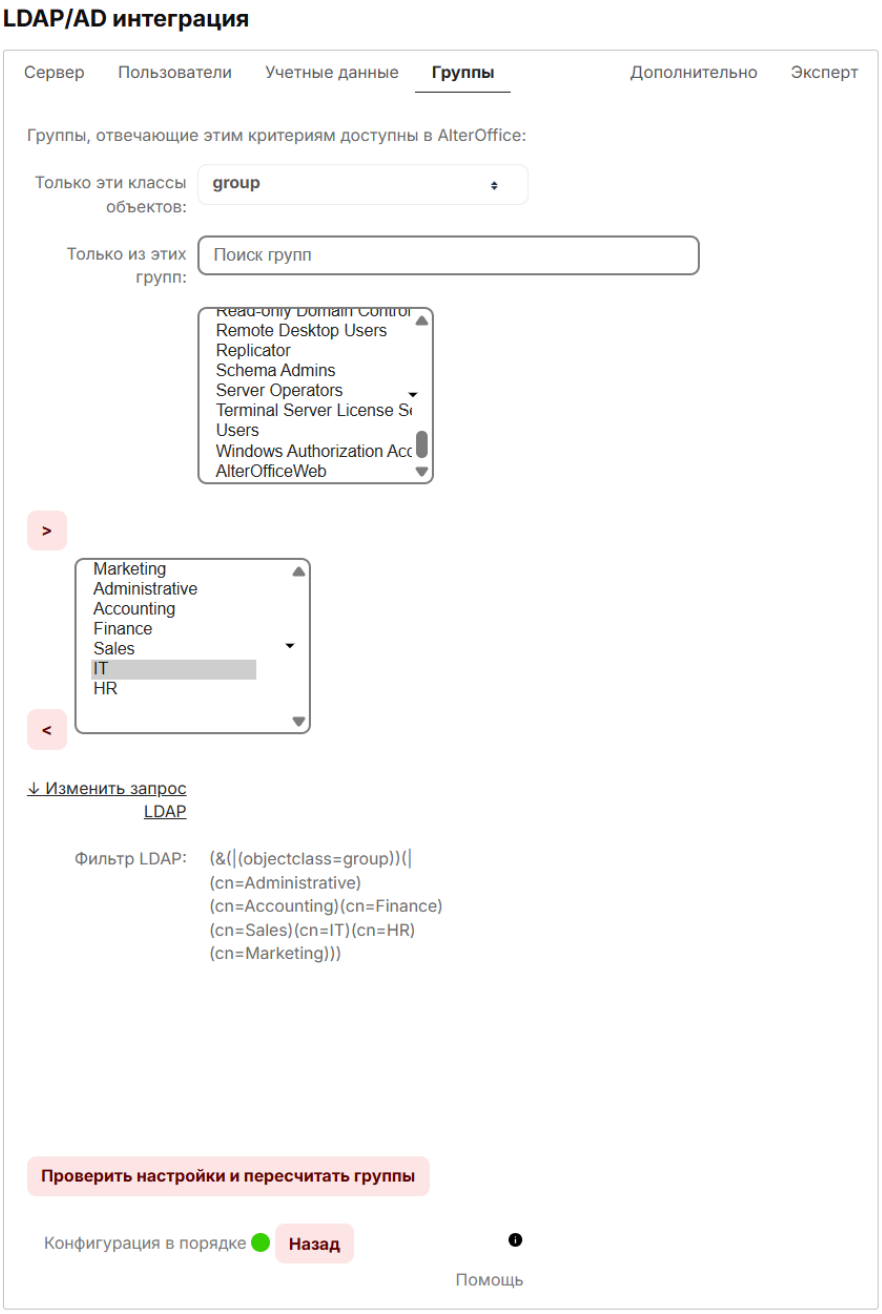


Рисунок 81. Настройка LDAP, вкладка «Группы»

Нажмите кнопку **«Проверить настройки и пересчитать группы»**. Будет отображено количество найденных групп, входящих в настроенный фильтр.

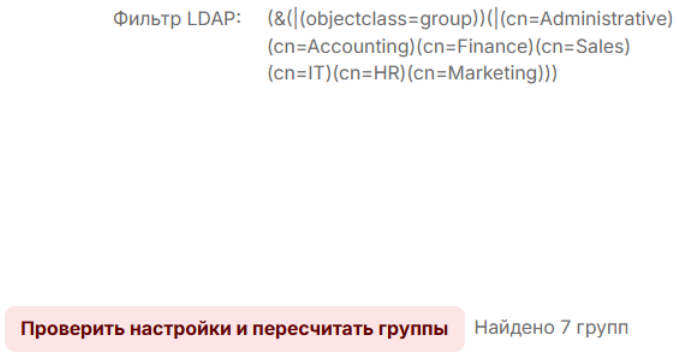


Рисунок 82. Настройка фильтра LDAP для поиска групп

6. Выполните настройки на вкладке «Дополнительно»

На вкладке можно настроить импортируемые атрибуты пользователя из РЕД АДМ.

Например, если в поле «Поле отображаемого имени пользователя» указать значение `displayName`, то в качестве отображаемого имени пользователя в АльтерОфис Веб будет загружено полное имя (ФИО) пользователя.

Пример допустимых атрибутов:

Атрибут	Значение	Пример значения
displayName	Отображаемое имя	Дарья Игоревна Калинина
cn	Основное имя объекта (пользователь)	Дарья Игоревна Калинина
givenName	Имя	Дарья Игоревна
sAMAccountName	Имя учетной записи	KalininaDI
mail	Адрес электронной почты	KalininaDI@almipartner.ru
cn	Основное имя объекта (группа)	IT
description	Описание объекта (группы)	ИТ-отдел

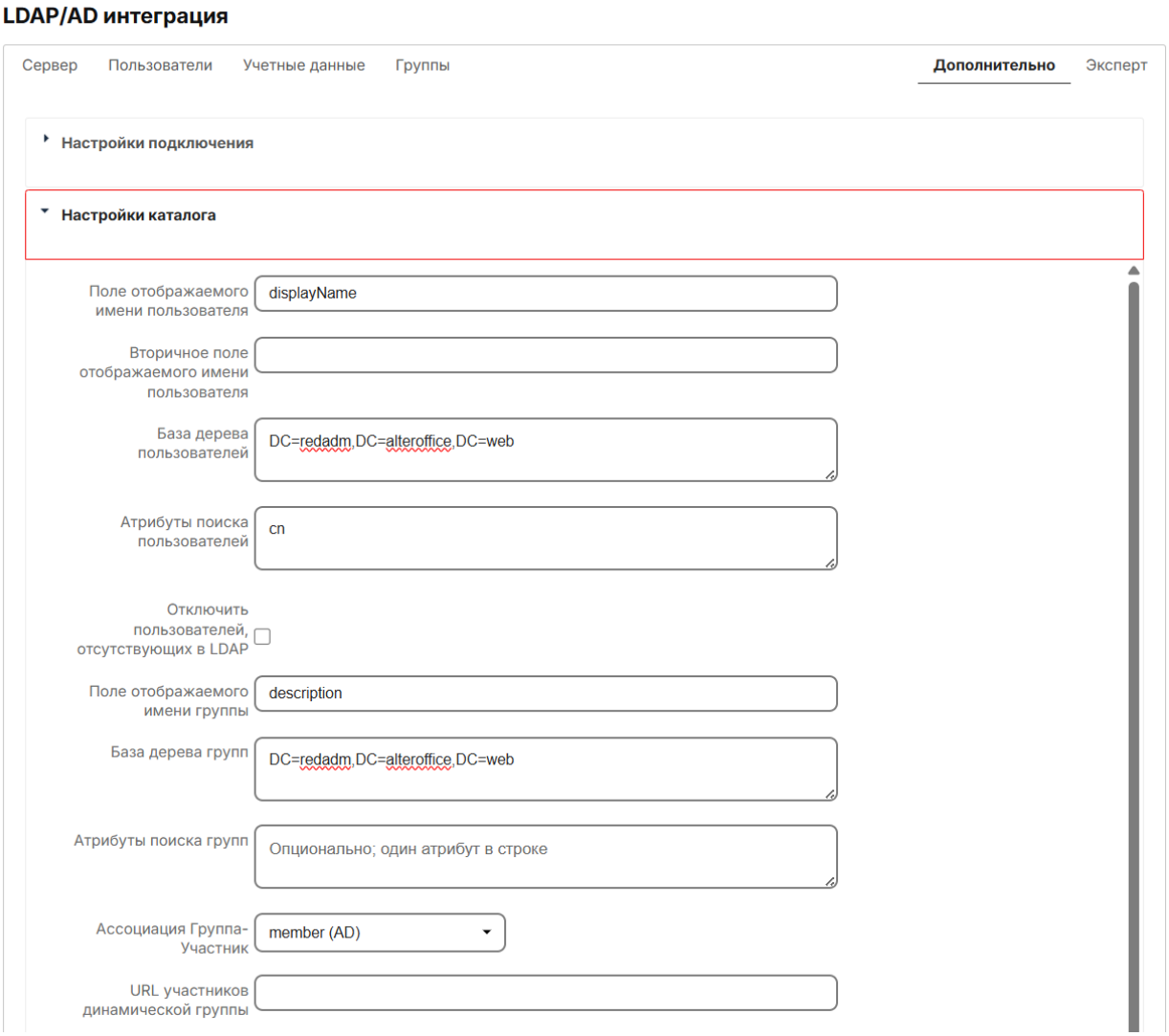


Рисунок 83. Настройка LDAP, вкладка «Дополнительно»

Заполните поля в разделе «Настройки каталога»:

Поле	Описание	Пример
Поле отображаемого имени пользователя	Атрибут для определения выводимого имени пользователя	`displayName`
База дерева пользователей	Путь поиска атрибута для пользователей	`DC=redadm,DC=alteroffice,DC=web`
Поле отображаемого имени группы	Атрибут для определения выводимого названия группы	`description`
База дерева групп	Путь поиска атрибута для групп	`cn=groups,cn=accounts,dc=aos,dc=loc`

Заполните поля в разделе «Специальные атрибуты»:

Поле	Описание	Пример

Поле	Описание	Пример
Поле адреса email	Адрес электронной почты	`mail`

Выполнение настроек на вкладке «Дополнительно» влияет на варианты загрузки данных из LDAP в АльтерОфис Веб.

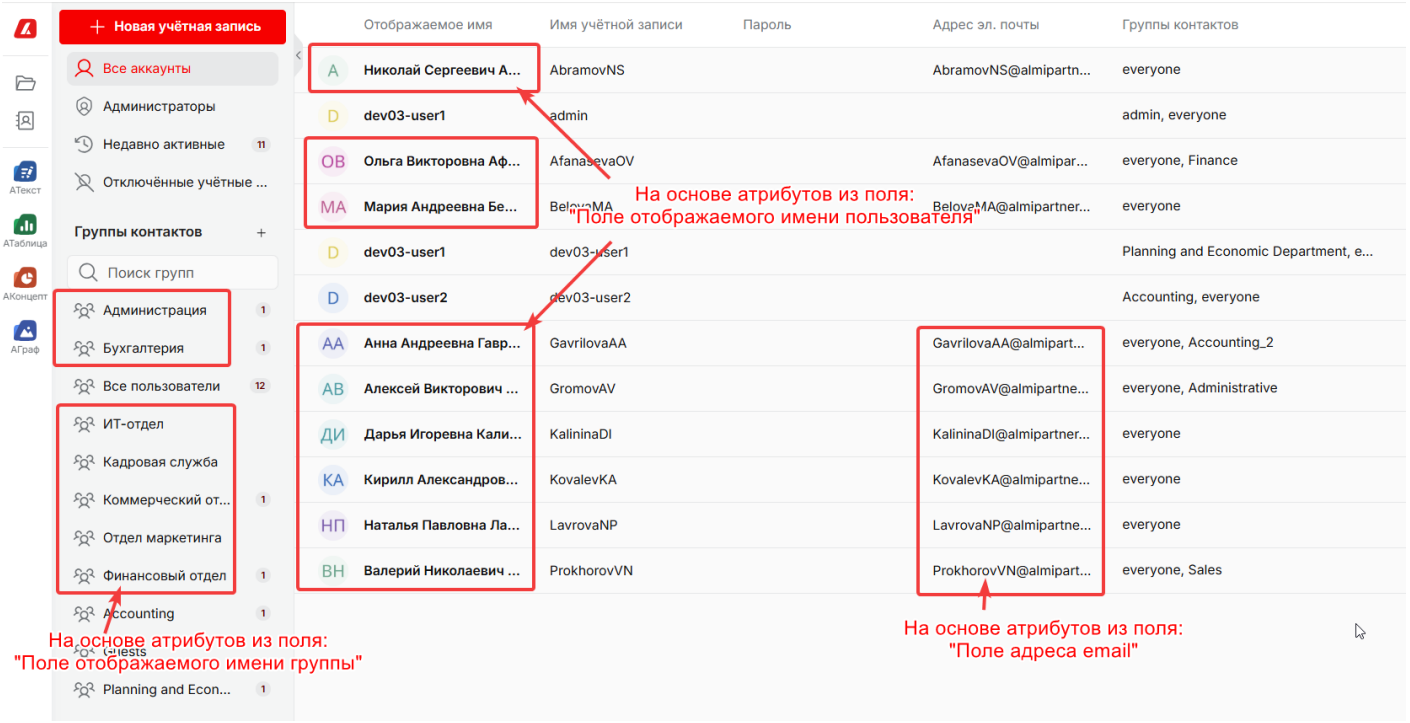


Рисунок 84. Учетные записи в АльтерОфис Веб

7. Выполните настройки на вкладке «Эксперт»

На вкладке можно определить на основе какого атрибута будет создаваться внутреннее имя пользователя при импорте данных из РЕД АДМ.

Внутреннее имя пользователя используется:

- для внутренней идентификации пользователя.
- для имени домашней папки пользователя.
- при формировании удалённых URL-адресов, например, для служб DAV, федеративного доступа.

Заполните поля в разделе «Внутреннее имя пользователя»:

Поле	Описание	Пример
Атрибут для внутреннего имени	На основе какого атрибута будет создано внутреннее имя пользователя	`sAMAccountName`

Выполнение настроек в разделе «Внутреннее имя пользователя» влияет на варианты загрузки данных из LDAP в АльтерОфис Веб.

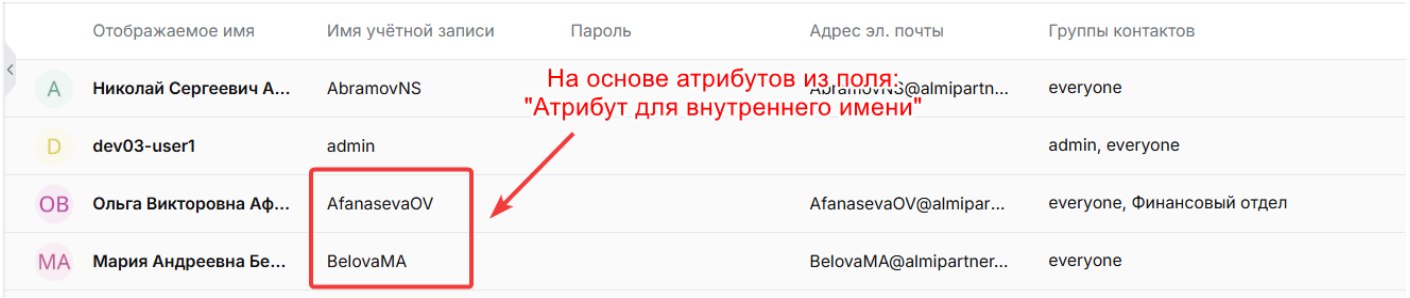


Рисунок 85. Учетные записи в АльтерОфис Веб

8. Завершение

Настройка LDAP в АльтерОфис Веб успешно завершена, если на вкладках **«Сервер»**, **«Пользователи»**, **«Учетные данные»**, **«Группы»** отображается индикатор **Конфигурация в порядке**.

Рисунок 86. Конфигурация в порядке

Откройте раздел «Учетные записи» и убедитесь, что отображаются пользователи из РЕД АДМ и пользователи корректно отнесены к группам.

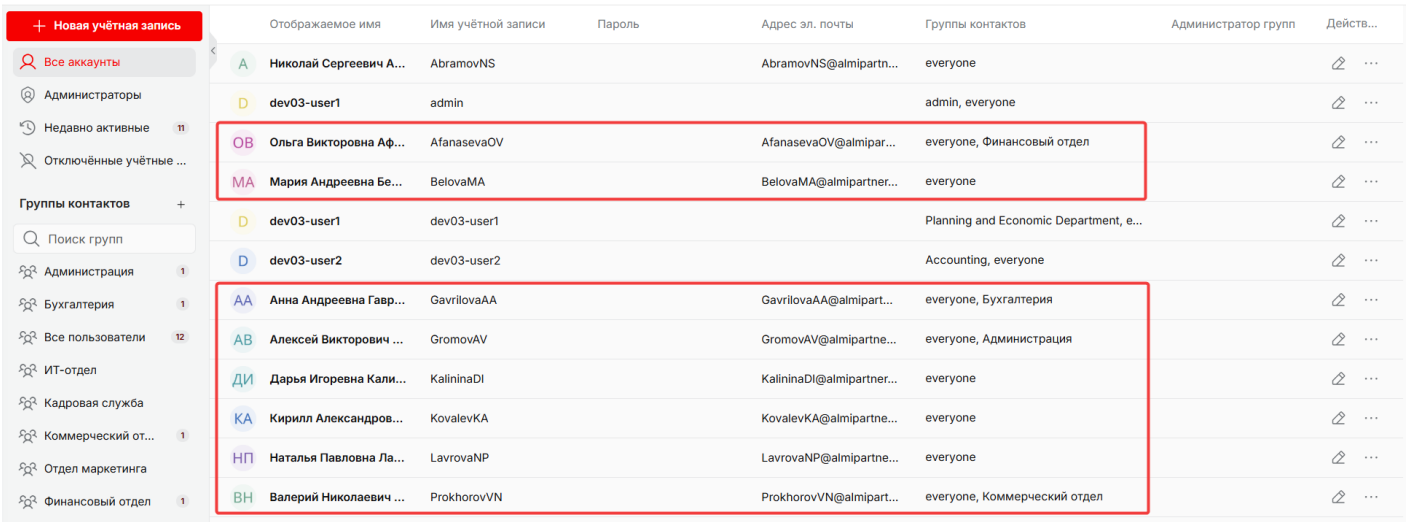


Рисунок 87. Учетные записи пользователей

4.7.4. Интеграция АльтерОфис Веб с Active Directory

1. Откройте раздел «LDAP/AD интеграция»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт **«Параметры сервера»**.

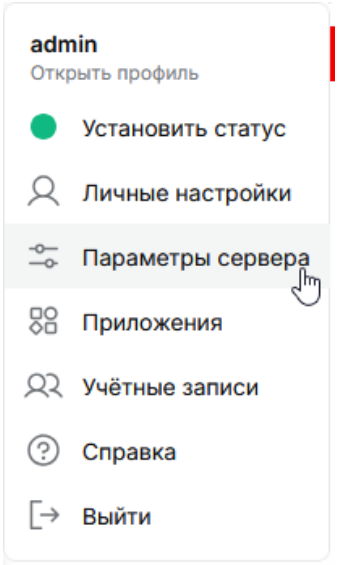


Рисунок 88. Меню администратора

В разделе **«Параметры сервера»** выберите пункт **«LDAP/AD интеграция»**.

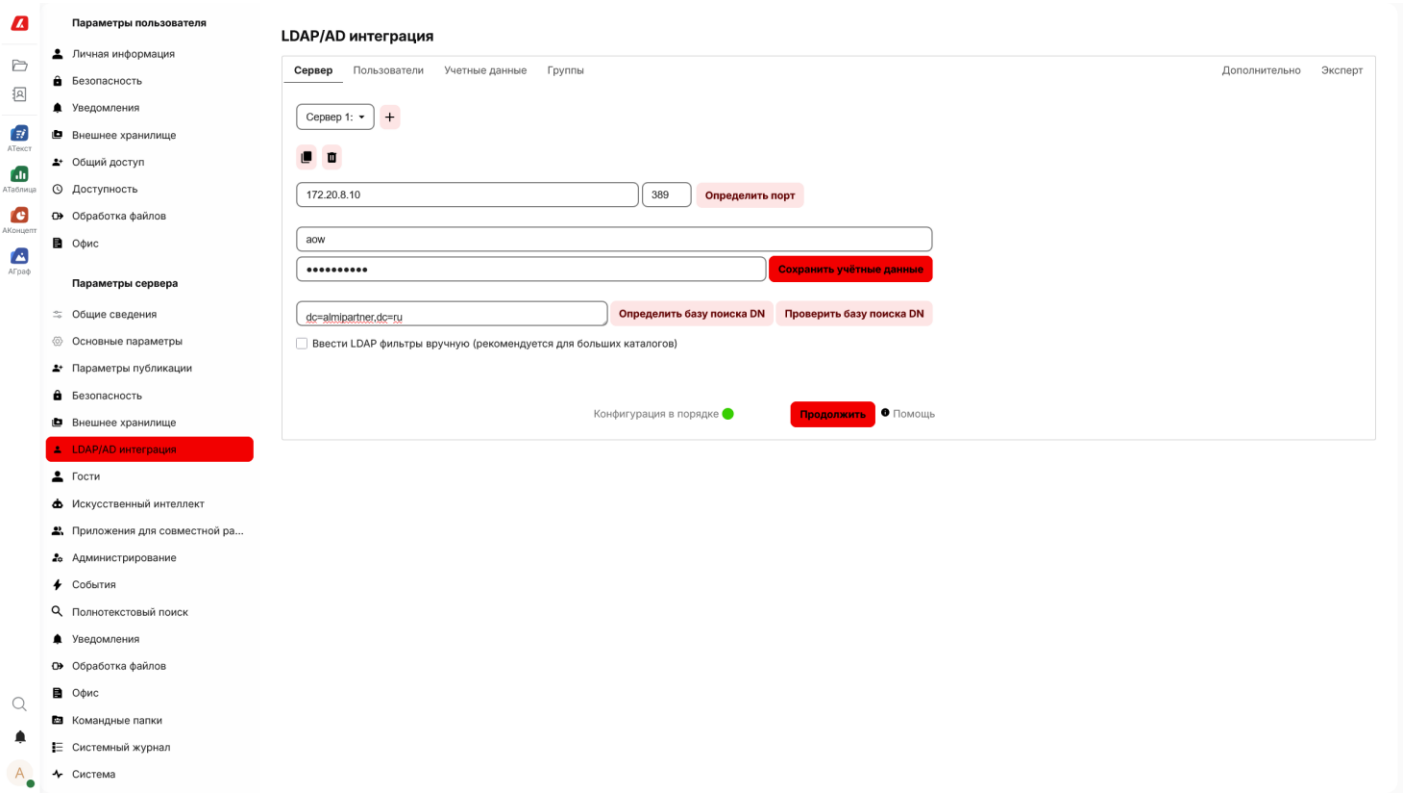


Рисунок 89. Настройка LDAP

2. Выполните настройки на вкладке «Сервер»

Панель настройки LDAP состоит из нескольких вкладок. Для доступа к другим вкладкам необходимо правильно заполнить первую вкладку («Сервер»). Если конфигурация выполнена правильно, загорается зеленый индикатор.

На вкладке **«Сервер»** заполните поля:

Поле	Описание	Пример
Сервер	IP-адрес контроллера домена.	172.20.8.10

Нажмите кнопку **Определить порт**. Если сервер LDAP работает на стандартном порту, он будет определен автоматически. Если это не удастся, вам придется ввести номер порта вручную.

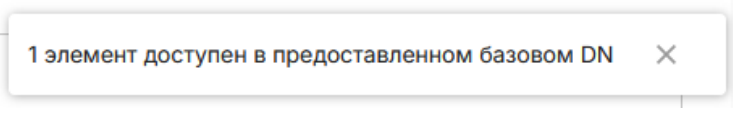
Поле	Описание	Пример
Порт	Порт, через который осуществляется подключение к серверу LDAP.	389
DN пользователя	Имя пользователя домена, от имени которого АльтерОфис Веб будет опрашивать LDAP. Рекомендуется использовать специального системного пользователя LDAP.	aow
Пароль	Пароль пользователя домена.	aow_password

После ввода имени пользователя и пароля нажмите кнопку **«Сохранить учётные данные»**.

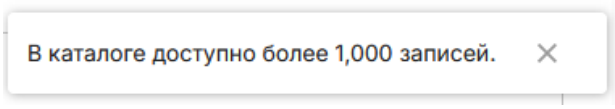
Поле	Описание	Пример
Base DN	Корневой каталог для поиска. Это поле обязательно для заполнения.	dc=almipartner,dc=ru

Нажмите кнопку **«Определить базу поиска DN»**, чтобы АльтерОфис Веб попробовал определить базовый DN на основе введенного DN пользователя или хоста. Если АльтерОфис Веб не может его определить, нужно ввести его вручную и нажать кнопку **«Проверить базу поиска DN»**.

При успешной проверке отобразится:

- информация 

,

- индикатор, который показывает, сколько примерно пользователей будет отображаться в АльтерОфис Веб 

,
- внизу загорится зеленый индикатор *Конфигурация в порядке*.

Установите флаг **«Ввести LDAP фильтры вручную (рекомендуется для больших каталогов)»**.

Нажмите кнопку **«Продолжить»**.

3. Выполните настройки на вкладке «Пользователи»

На вкладке **«Пользователи»** определите, какие пользователи LDAP должны быть указаны в качестве пользователей **АльтерОфис Веб**.

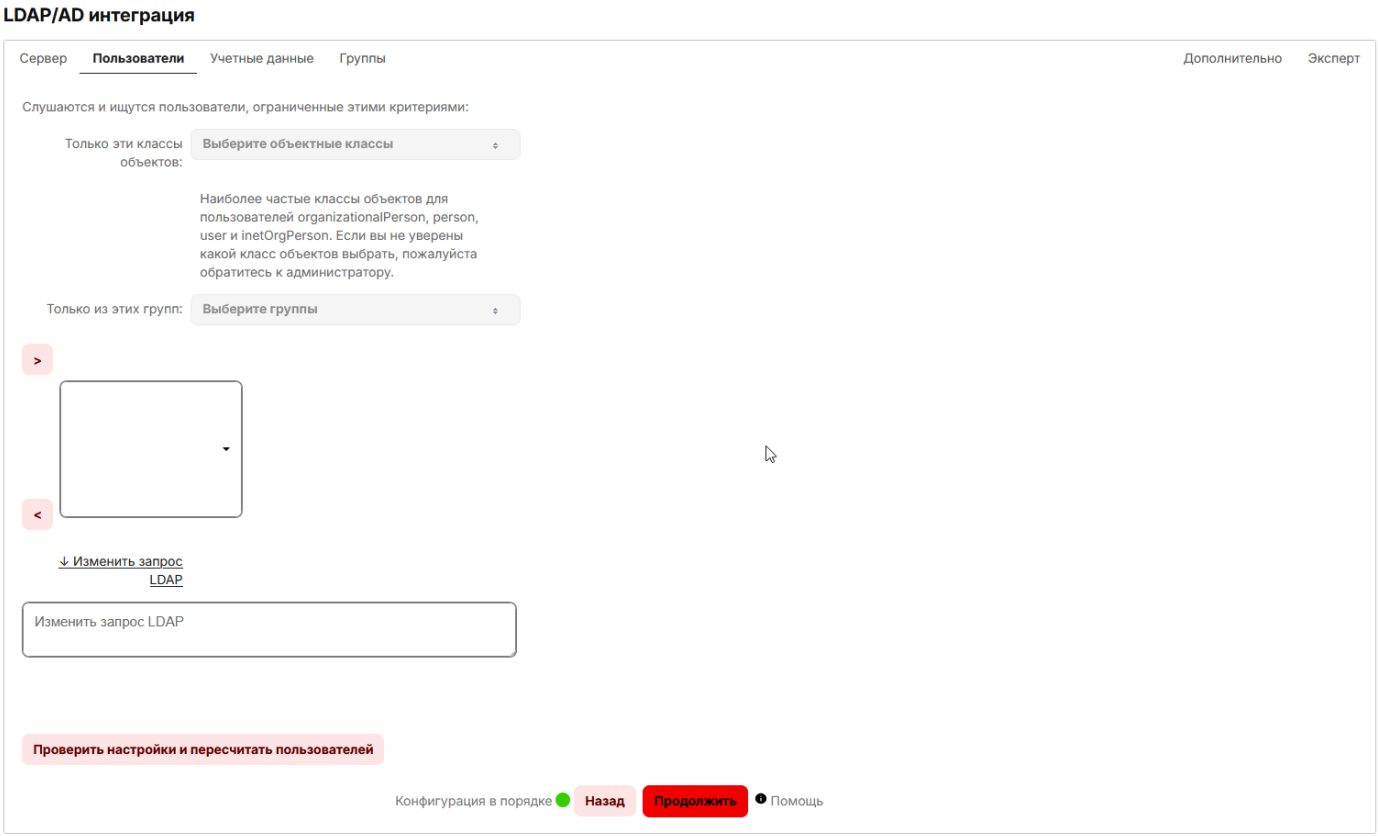


Рисунок 90. Настройка LDAP, вкладка «Пользователи»

Нажмите на ссылку **Изменить запрос LDAP**. При нажатии на этот текст включится режим, при котором можно определить классы объектов и группы, из которых необходимо фильтровать пользователей, путем выбора из списков.

Нажмите **«Да»** для включения режима.

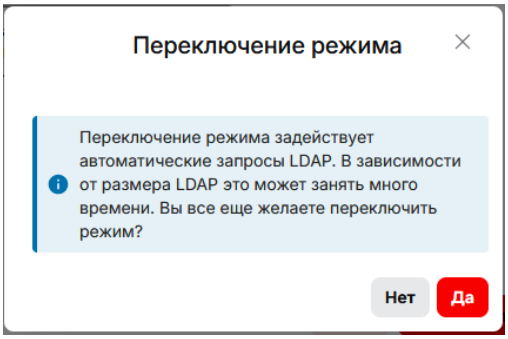


Рисунок 91. Настройка LDAP, включение режима опроса LDAP

Настройте поля:

Поле	Описание	Пример
Только эти классы объектов	Указать класс объектов.	person

Из раскрывающегося списка выберите необходимые классы объектов.

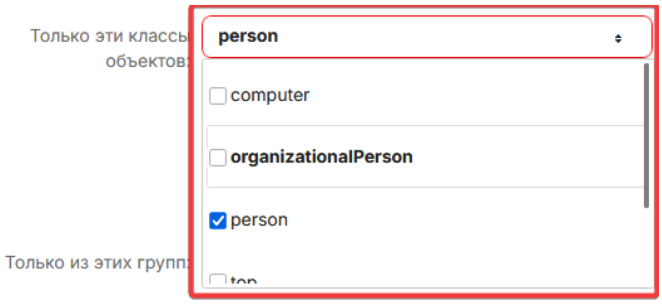


Рисунок 92. Выбор классов объектов

Поле	Описание	Пример
Только из этих групп	Выбрать группу из которой будут импортироваться учетные записи.	AlterOfficeWeb

Выберите нужную группу в списке, чтобы переместить группу в список выбранных групп, нажмите >.

Для включения еще одной группы повторите действия.

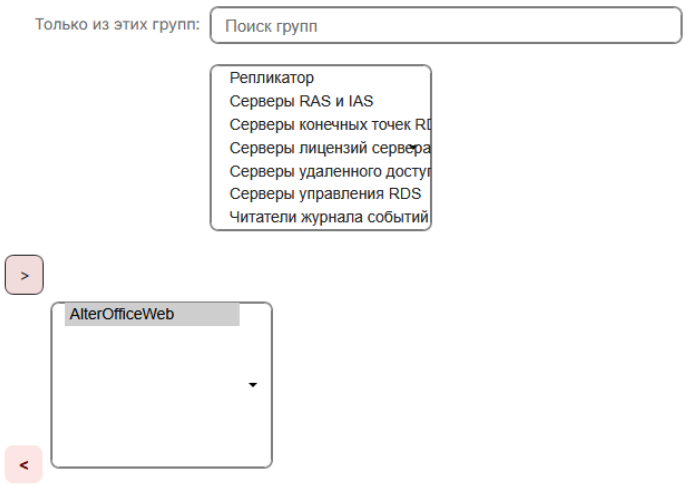


Рисунок 93. Выбор групп

> ПРИМЕЧАНИЕ
>
> Фильтр LDAP может быть задан в необработанном виде:

```
(&(|(objectclass=person))(|(|(memberof=CN=AlterOfficeWeb,CN=Users,DC=almipartner,DC=ru)(primaryGroupID=11427))))
```

> Для этого нажмите на ссылку **Изменить запрос LDAP** и введите фильтр в необработанном виде.

Нажмите кнопку **«Проверить настройки и пересчитать пользователей»**. Будет отображено количество найденных пользователей, входящих в настроенный фильтр.

Нажмите кнопку **«Продолжить»**.

4. Выполните настройки на вкладке «Учетные данные»

На вкладке **«Учетные данные»** определите, какие пользователи LDAP могут входить в систему **АльтерОфис Веб** и по какому атрибуту или атрибутам сопоставляется указанное имя для входа (например, имя пользователя LDAP/AD, адрес электронной почты).

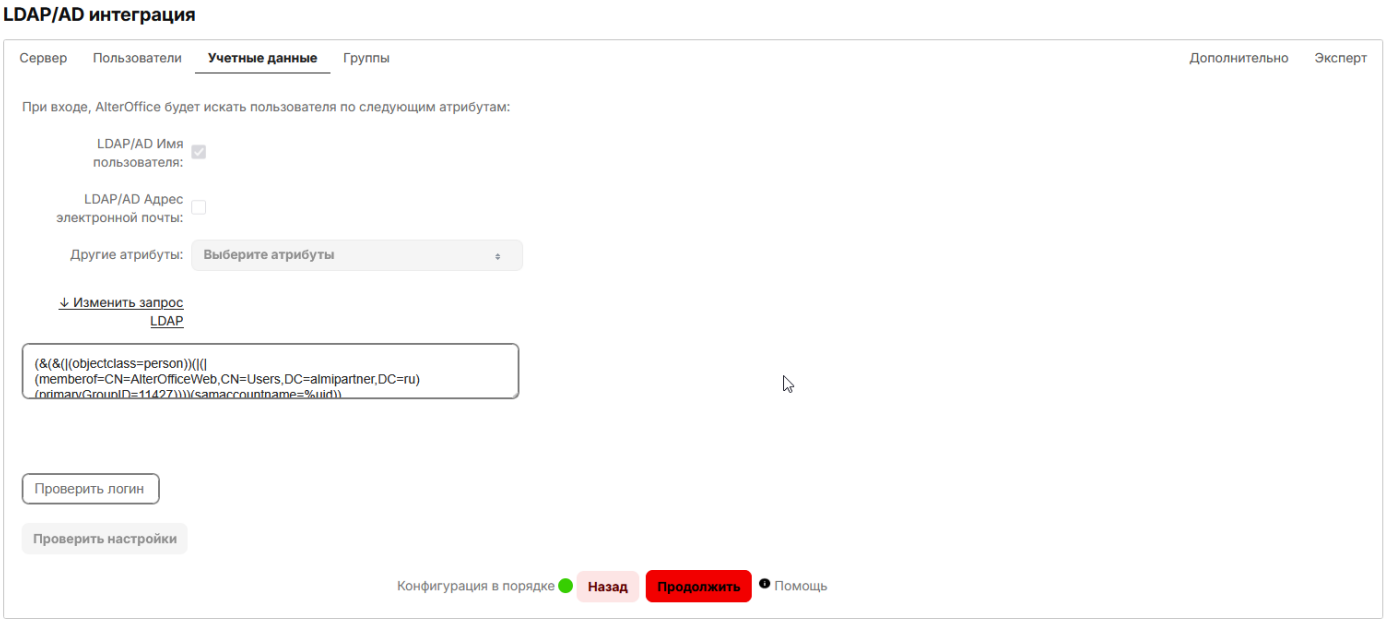


Рисунок 94. Настройка LDAP, вкладка «Учетные данные»

Нажмите на ссылку **Изменить запрос LDAP**. При нажатии на этот текст включится режим, при котором можно выполнить настройки путем выбора из списка и выставлением флагов.

Нажмите **«Да»** для включения режима.

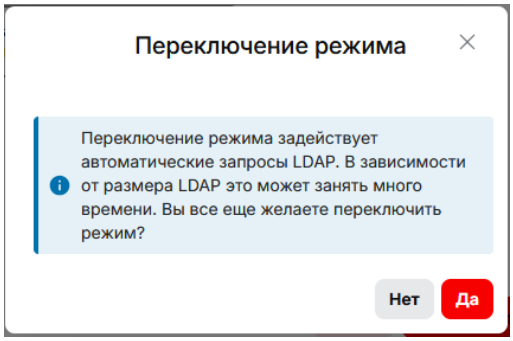


Рисунок 95. Настройка LDAP, включение режима опроса LDAP

Настройте поля:

Поле	Описание	Пример
LDAP/AD Имя пользователя	При включении параметра, значение для входа будет сравниваться с именем пользователя в каталоге LDAP.	Да
LDAP/AD Адрес электронной почты	При включении параметра, значение для входа будет сравниваться с адресом электронной почты в каталоге LDAP.	Нет

Поле	Описание	Пример
Другие атрибуты	При необходимости укажите атрибуты для сравнения. Список автоматически формируется на основе атрибутов пользовательского объекта на вашем сервере LDAP.	sAMAccountName

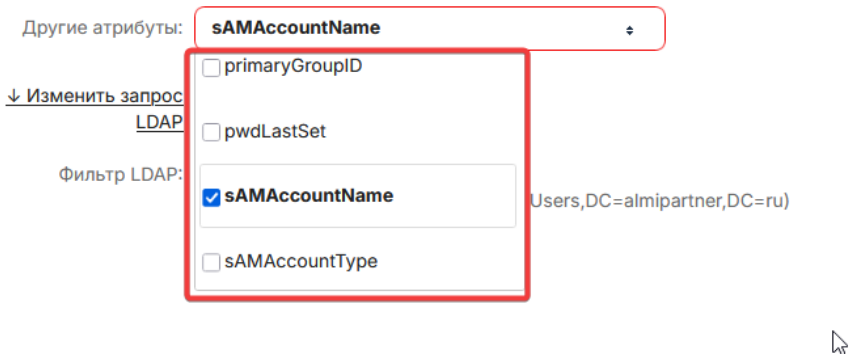


Рисунок 96. Выбор атрибутов

> ПРИМЕЧАНИЕ
>
> Фильтр LDAP может быть задан в необработанном виде:

```
(&(&(|(objectclass=person))(|(|(memberof=CN=AlterOfficeWeb,CN=Users,DC=almipartner
,DC=ru)(primaryGroupID=11427)))))(|(samaccountname=%uid)(|(sAMAccountName=%uid))))
```

> Для этого нажмите на ссылку **Изменить запрос LDAP** и введите фильтр в необработанном виде.

Введите в поле **«Проверить логин»** имя учетной записи для проверки настроек и нажмите **«Проверить настройки»**.

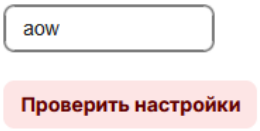
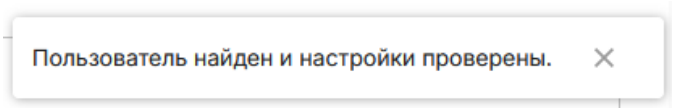


Рисунок 97. Проверка настроек

При правильной настройке отобразится сообщение **«Пользователь найден и настройки проверены»**.



Нажмите кнопку **«Продолжить»**.

5. Выполните настройки на вкладке «Группы»

На вкладке **«Группы»** определите, какие группы LDAP должны быть доступны в **АльтерОфис Веб**.

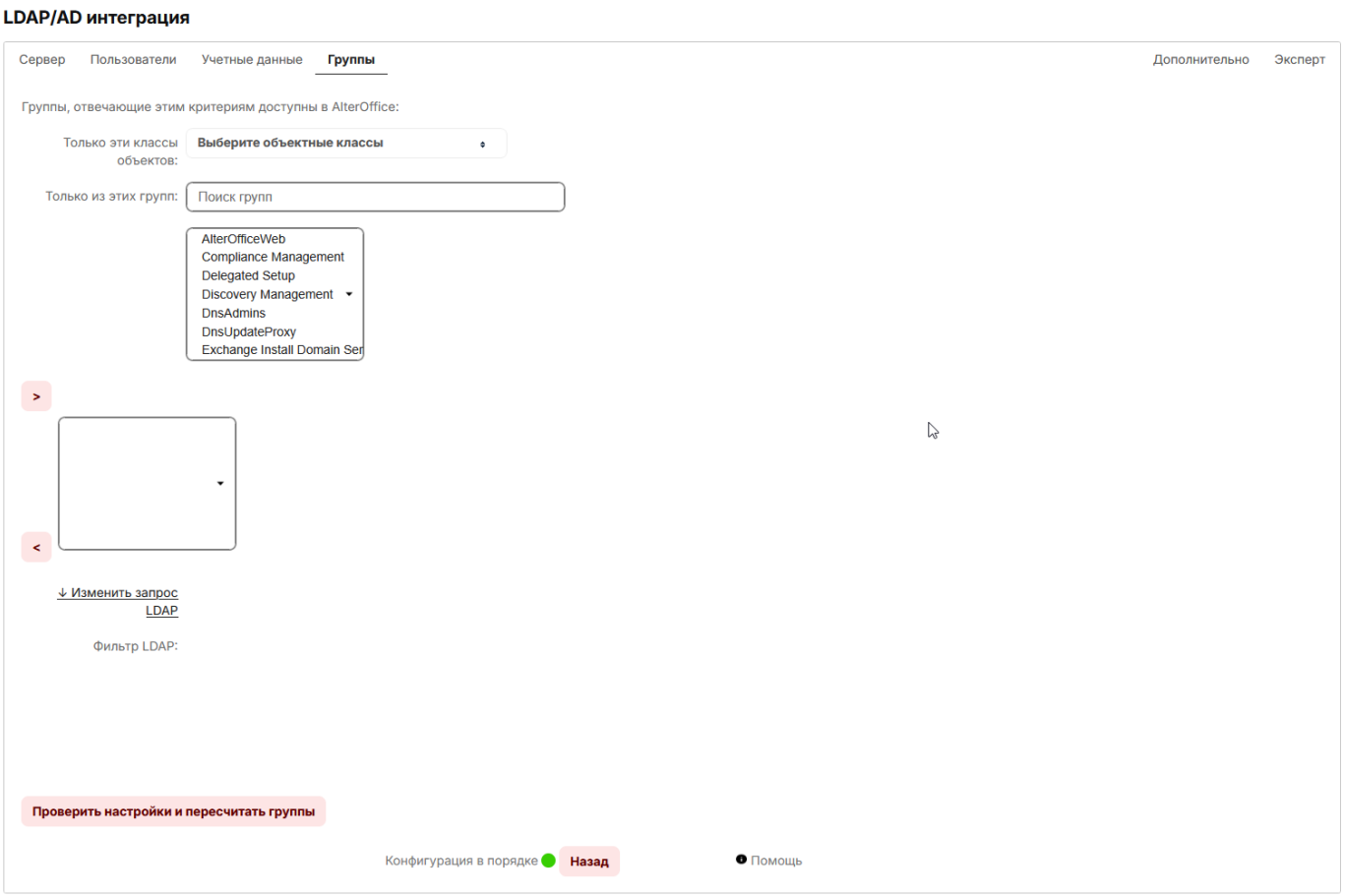


Рисунок 98. Настройка LDAP, вкладка «Группы»

Нажмите на ссылку **Изменить запрос LDAP**. При нажатии на этот текст включится режим, при котором можно определить классы объектов и группы путем выбора из списков.

Нажмите **«Да»** для включения режима.

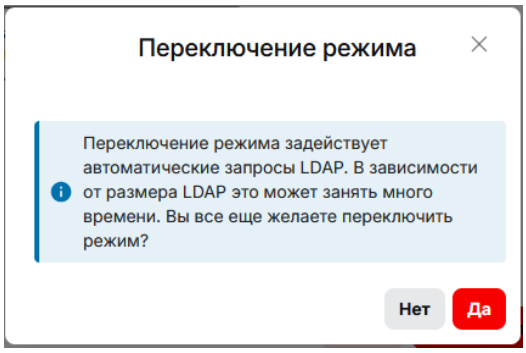


Рисунок 99. Настройка LDAP, включение режима опроса LDAP

Настройте поля:

Поле	Описание	Пример
Только эти классы объектов	В списке отображены только те	group

Поле	Описание	Пример
	классы объектов, которые возвращают хотя бы один групповой объект. Вы можете выбрать несколько классов объектов.	

Из раскрывающегося списка выберите необходимые классы объектов.

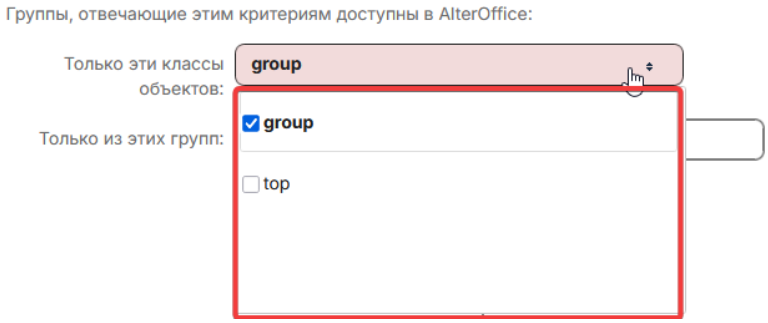


Рисунок 100. Выбор классов объектов

Выберите нужную группу в поле **«Только из этих групп»**, чтобы переместить группу в список выбранных групп, нажмите >.

Поле	Описание	Пример
Только из этих групп	Выбрать группы, которым будет предоставлен доступ к АльтерОфис Веб.	AlterOfficeWeb

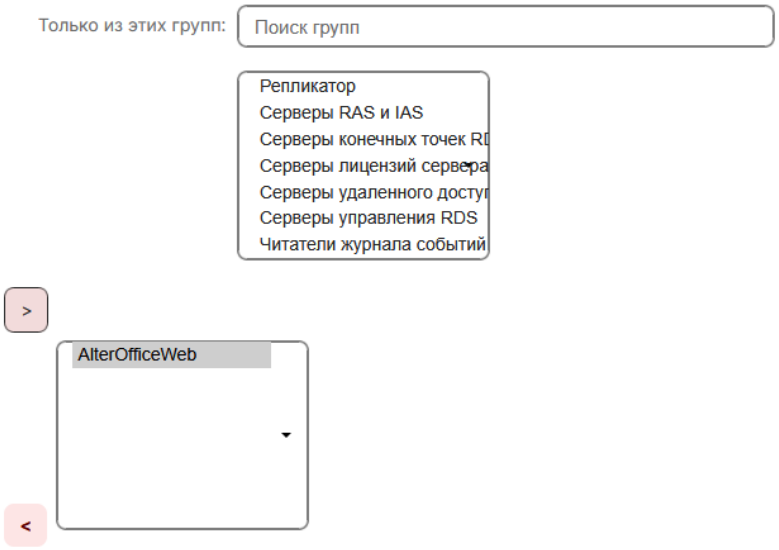


Рисунок 101. Выбор групп

ПРИМЕЧАНИЕ

Фильтр LDAP может быть задан в необработанном виде:

```
(&(|(objectclass=group)(objectclass=top))(|(cn=AlterOfficeWeb)(cn=AOW_Accounting)(cn=AOW_Administrative)(cn=AOW_Finance)(cn=AOW_HR)(cn=AOW_I.T.)(cn=AOW_Marketing)(cn=AOW_Product/Service Development)(cn=AOW_Sales)))
```

Для этого нажмите на ссылку **Изменить запрос LDAP** и введите фильтр в необработанном виде.

Нажмите кнопку **«Проверить настройки и пересчитать группы»**. Будет отображено количество найденных групп, входящих в настроенный фильтр.

6. Завершение

Настройка LDAP в АльтерОфис Веб успешно завершена, если на вкладках **«Сервер»**, **«Пользователи»**, **«Учетные данные»**, **«Группы»** отображается индикатор **Конфигурация в порядке**.

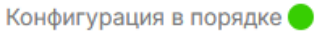


Рисунок 102. Конфигурация в порядке

ВОЗМОЖНЫЕ ОШИБКИ

- **Не удаётся подключиться к серверу LDAP** — Неверно указан адрес сервера (ldap:// или ldaps://) или порт (389 / 636).
- **Ошибка SSL/TLS при подключении** - Неправильный сертификат, самоподписанный сертификат, устаревший протокол.
- **Base DN не найден** - Ошибка в указании базы поиска.
- **Тайм-аут подключения** - Межсетевой экран или SELinux блокирует соединение.
- **Не отображаются пользователи LDAP** - Неверный фильтр поиска пользователей.
- **Не найдены группы** - Неверный Base DN для групп.

4.7.5. Создание нового профиля настроек на основе существующего

В **АльтерОфис Веб** может быть настроено несколько профилей настроек подключения к LDAP / AD.

Для создания копии настроек выполните действия, описанные ниже.

1. Выберите конфигурацию, которую необходимо скопировать.

Перейдите на вкладку **«Сервер»**.

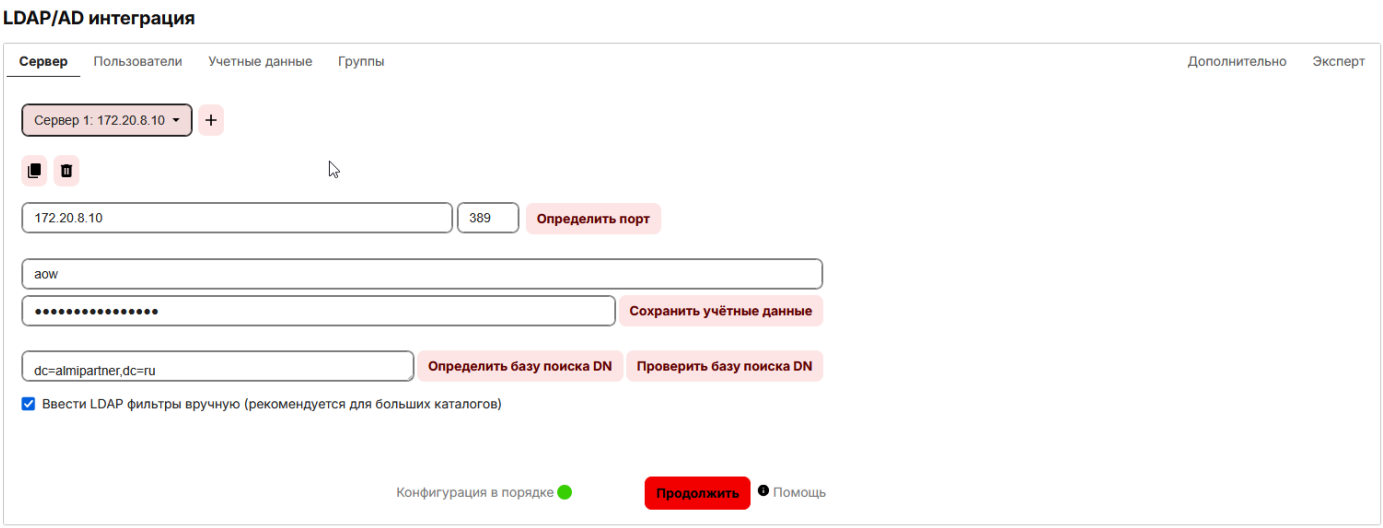


Рисунок 103. Выбор конфигурации

На вкладке **«Сервер»** выберите нужную конфигурацию.

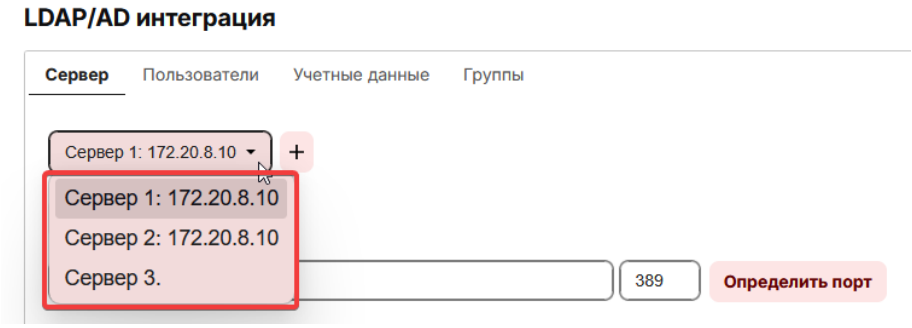


Рисунок 104. Выбор конфигурации

2. Копирование конфигурации.

Нажмите кнопку **«Копировать текущую конфигурацию…»** .

Будет создана новая конфигурация.

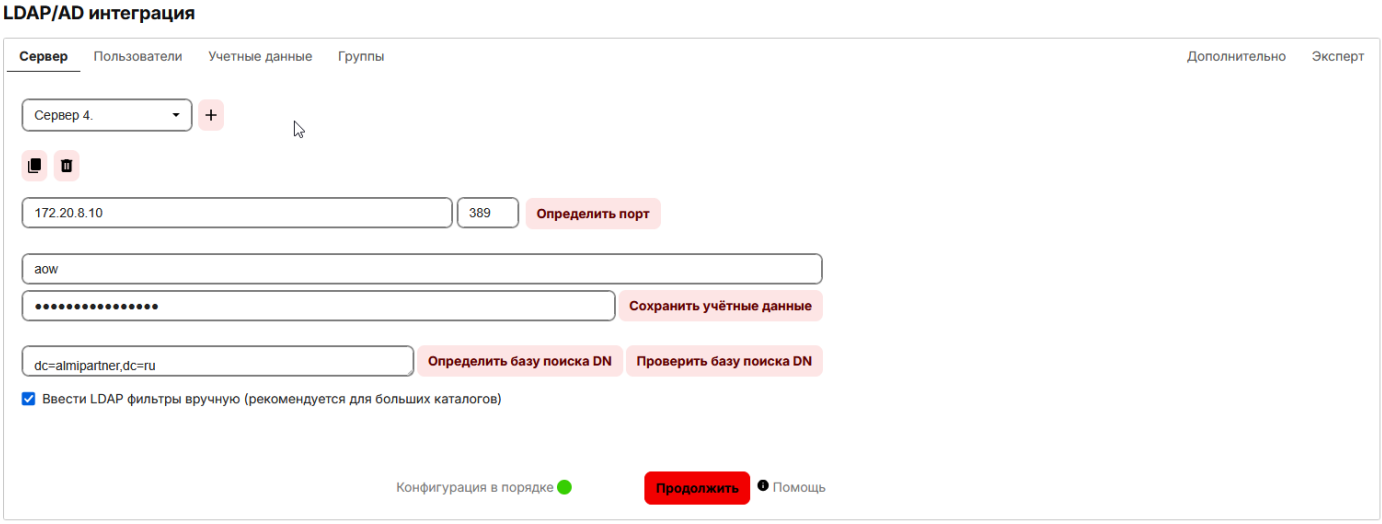


Рисунок 105. Выбор конфигурации

3. Изменение скопированной конфигурации.

Внесите изменения в настройки конфигурации на вкладках **«Сервер»**, **«Пользователи»**, **«Учетные данные»**, **«Группы»**. Убедитесь, что на всех вкладках отображается индикатор **Конфигурация в порядке**.

Рисунок 106. Конфигурация в порядке

4.7.6. Удаление профиля настроек

Для удаление ненужной конфигурации настроек подключения к LDAP / AD выполните действия, описанные ниже.

1. Выберите конфигурацию, которую необходимо удалить.

Перейдите на вкладку **«Сервер»**.

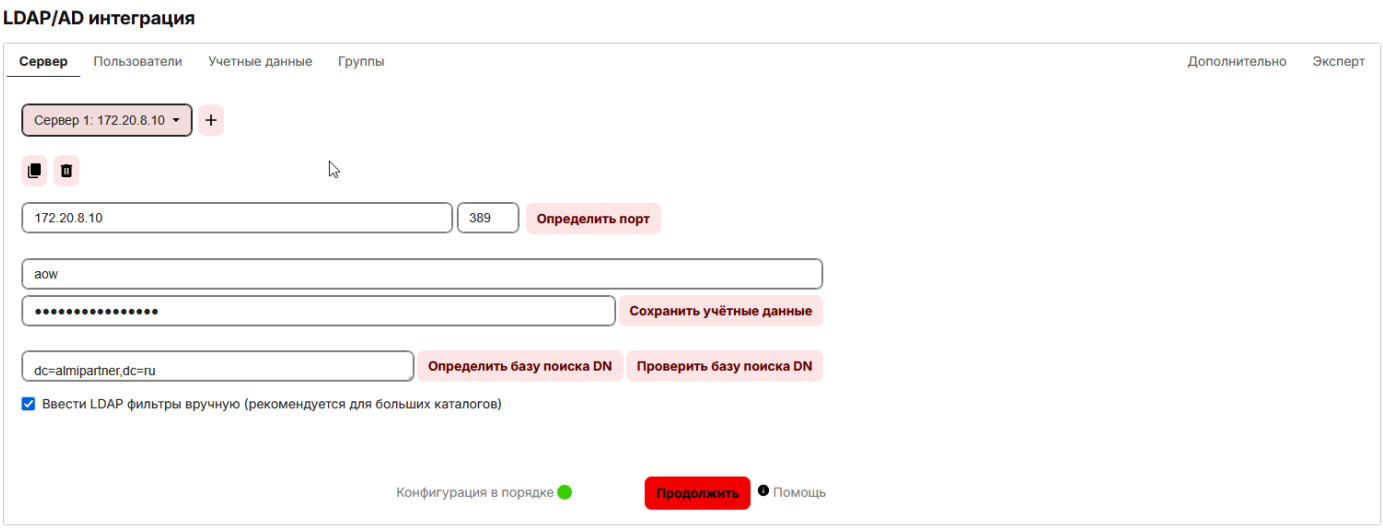


Рисунок 107. Выбор конфигурации

На вкладке **«Сервер»** выберите нужную конфигурацию.

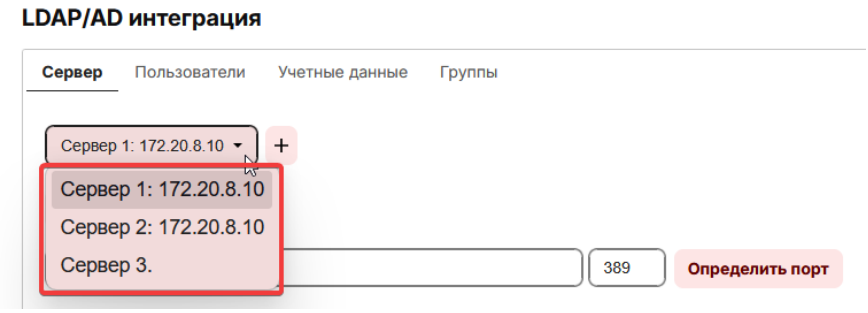


Рисунок 108. Выбор конфигурации

2. Удаление конфигурации.

Нажмите кнопку **«Удалить текущую конфигурацию»** .

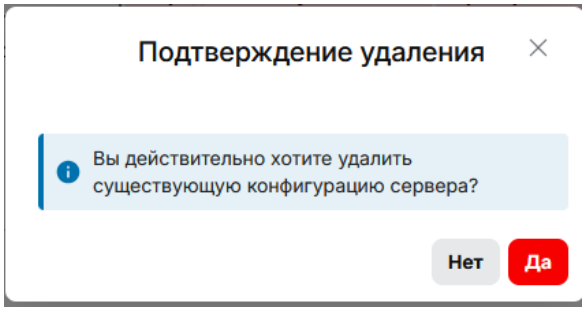


Рисунок 109. Подтверждение удаления настроек

Нажмите **«Да»** для подтверждения удаления.

Будет удалена текущая конфигурация.

4.7.7. Просмотр пользователей и групп полученных из LDAP / AD

В результате настроек подключения к LDAP / AD и настройки фильтрации групп и пользователей в **«АльтерОфис Веб»** добавляются группы и пользователи из LDAP / AD.

1. Откройте раздел «Учетные записи»**.**

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт **«Учетные записи»**.

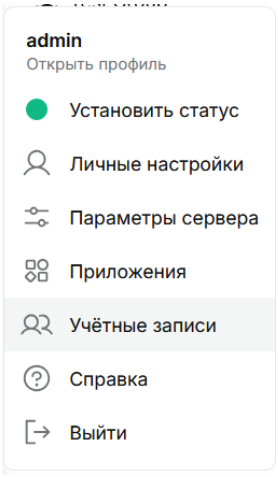


Рисунок 110. Меню администратора

Откроется страница со списком пользователей.

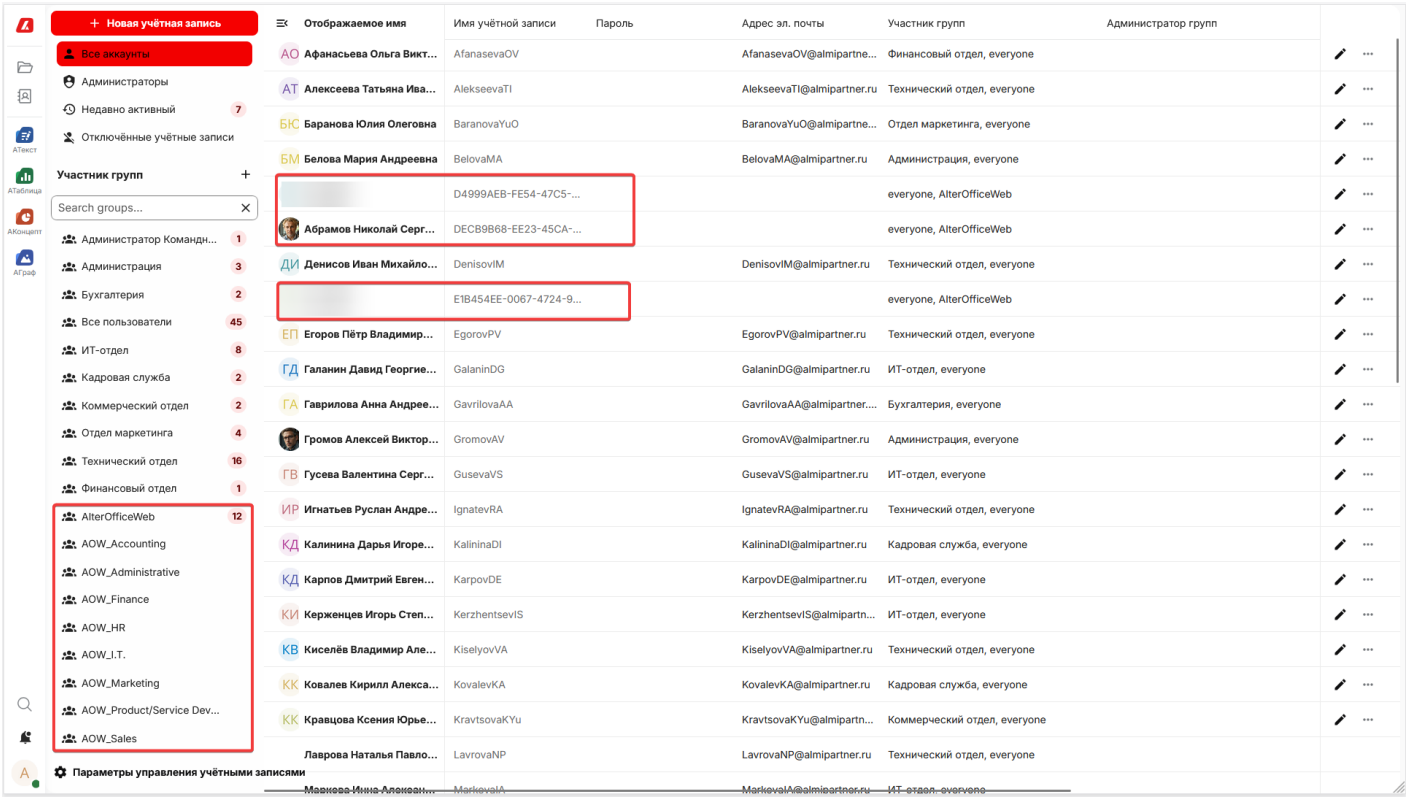


Рисунок 111. Список пользователей

2. Просмотр добавленных групп из LDAP / AD.

Слева в разделе «Участник групп» выведены группы, добавленные из LDAP / AD.

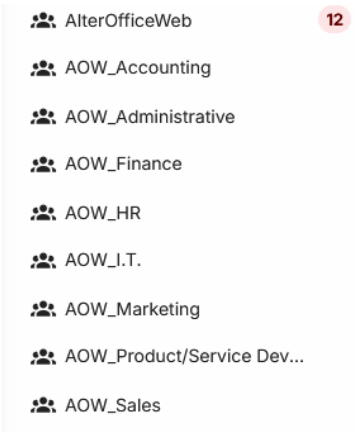


Рисунок 112. Группы пользователей из LDAP / AD

3. Просмотр добавленных пользователей из LDAP / AD.

В списке пользователей отображаются пользователи, добавленные из LDAP / AD.

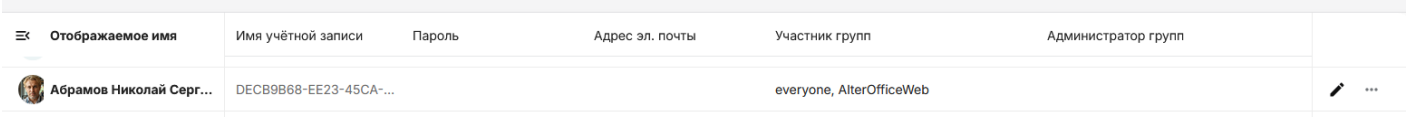


Рисунок 113. Пользователи из LDAP / AD

ПРИМЕЧАНИЕ

- Для пользователей загруженных из LDAP / AD имя учётной записи выглядит в виде идентификатора **uid**.
- После настройки интеграции с LDAP / AD, пользователи домена могут проходить авторизацию со своим доменным логином и паролем.
- Настройка доступа к папкам и файлам для пользователей LDAP / AD, выполняется также как и для пользователей с локальной учетной записью «АльтерОфис Веб».

4.8. Настройка пользователей и групп

Определение групп пользователей и распределение пользователей по группам, является важным шагом в настройке прав доступа к системе. Работа с пользователями осуществляется в разделе **Учетные записи**.

4.8.1. Общий вид интерфейса раздела управления учетными записями

Раздел **Учетные записи** представляет собой таблицу с данными по всем существующим пользователям.

1. Общий вид интерфейса

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт **«Учетные записи»**.

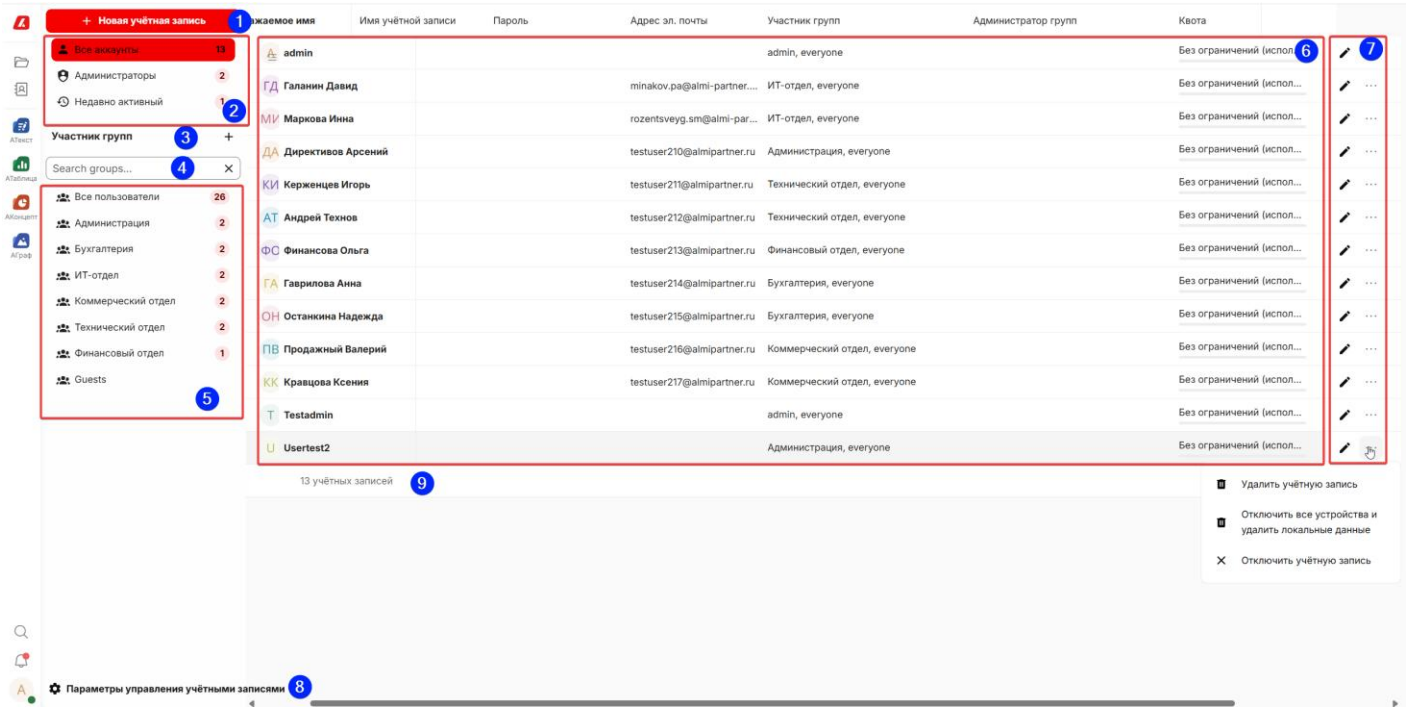


Рисунок 114. Раздел «Учетные записи»

Информацию на странице можно разделить на блоки:

Элемент	Описание
(1) Кнопка **Новая учетная запись**	Функция создания новой учетной записи.
(2) Быстрые фильтры	Блок быстрых фильтров.
(3) Участник групп	Заголовок подраздела и функциональная кнопка для создания групп пользователей.
(4) Поиск групп	Окно поиска по группам.
(5) Группы	Блок списка групп пользователей.
(6) Пользователи	Блок с информацией о пользователях.
(7) Действия	Функции для работы с пользователями.
(8) Параметры	Дополнительные параметры вывода сведений о пользователях, дополнительные настройки.
(9) Счетчик учетных записей	Кол-во учетных записей в списке.

В модуле управления пользователями доступны функции:

- Просмотр списка пользователей.
- Создание новых пользователей.
- Фильтрация пользователей по группам.
- Изменение отображаемого имена пользователя и пароля.
- Просмотр и установка квот.
- Активация и деактивация учетных записей.
- Удаление пользователей.

2. Быстрые фильтры и поиск

В левой боковой панели доступны **быстрые фильтры** (2):

Элемент	Описание
Все аккаунты	Полный список учетных записей.
Администраторы	Пользователи с правами администратора.
Недавно активный	Пользователи, недавно заходившие в систему.
Отключенные учетные записи.	Неактивные или заблокированные пользователи.

Справа от фильтра отображено количество пользователей, входящих в эту группу.

Ниже быстрых фильтров расположены **группы пользователей** (5) с указанием количества участников в каждой из групп.

Доступен поиск по группам через строку **Поиск групп…** (4). Для поиска группы начните вводить её название - система отобразит список групп, соответствующий введенному тексту.

3. Просмотр пользователей группы

Чтобы получить список пользователей, входящих в группу, в разделе **Участник групп** выберите нужную группу.

В рабочей области отобразится список пользователей, входящих в выбранную группу.

4.8.2. Параметры управления учетными записями

В разделе **Учетные записи** по умолчанию отображается основная информация о пользователях системы:

Поле	Описание	Пример 1	Пример 2
Отображаемое имя	Имя пользователя, которое отображается в общих папках, веб-интерфейсе и электронных письмах. Если полное имя не указано, по умолчанию используется имя для входа.	admin	Абрамов Николай Сергеевич
Имя учетной записи	Уникальный идентификатор пользователя, который нельзя изменить.	admin	DECB9B68-EE23-45CA-B02B-6F2B28C9B1E4
Пароль	Поле с зашифрованным значением пароля или возможностью его изменения	-	-
Адрес эл. почты	Адрес электронной почты, указанный в профиле учетной записи. Этот адрес можно использовать для запроса на сброс пароля.	-	AbramovNS@almipartner.ru
Участник групп	Список групп, в которых состоит учетная запись.	admin, everyone	everyone, AlterOfficeWeb, Администрация
Администратор групп	Администраторы групп получают административные права в определённых группах и могут добавлять и удалять пользователей из своих групп. Администраторы групп могут изменять имя пользователя, пароль, адрес электронной почты, квоту	-	Администрация

Поле	Описание	Пример 1	Пример 2
	и т. д. участников группы. Администраторам групп не разрешается добавлять в свои группы существующих пользователей.		
Квота	Установленный лимит дискового пространства (неограниченно или указанное значение), выделенное для каждого пользователя. Пользователь, превысивший квоту, не сможет загружать данные.	Без ограничений	5 GB
Руководитель	Пользователю может быть задан линейный руководитель. На основе данных о руководителях формируется организационная структура в системной адресной книге пользователя. Назначение руководителя не изменяет прав доступа пользователя или его руководителя.	-	-

Для изменения отображения информации, в разделе **Учетные записи** нажмите на кнопку **Параметры управления учётными записями**.

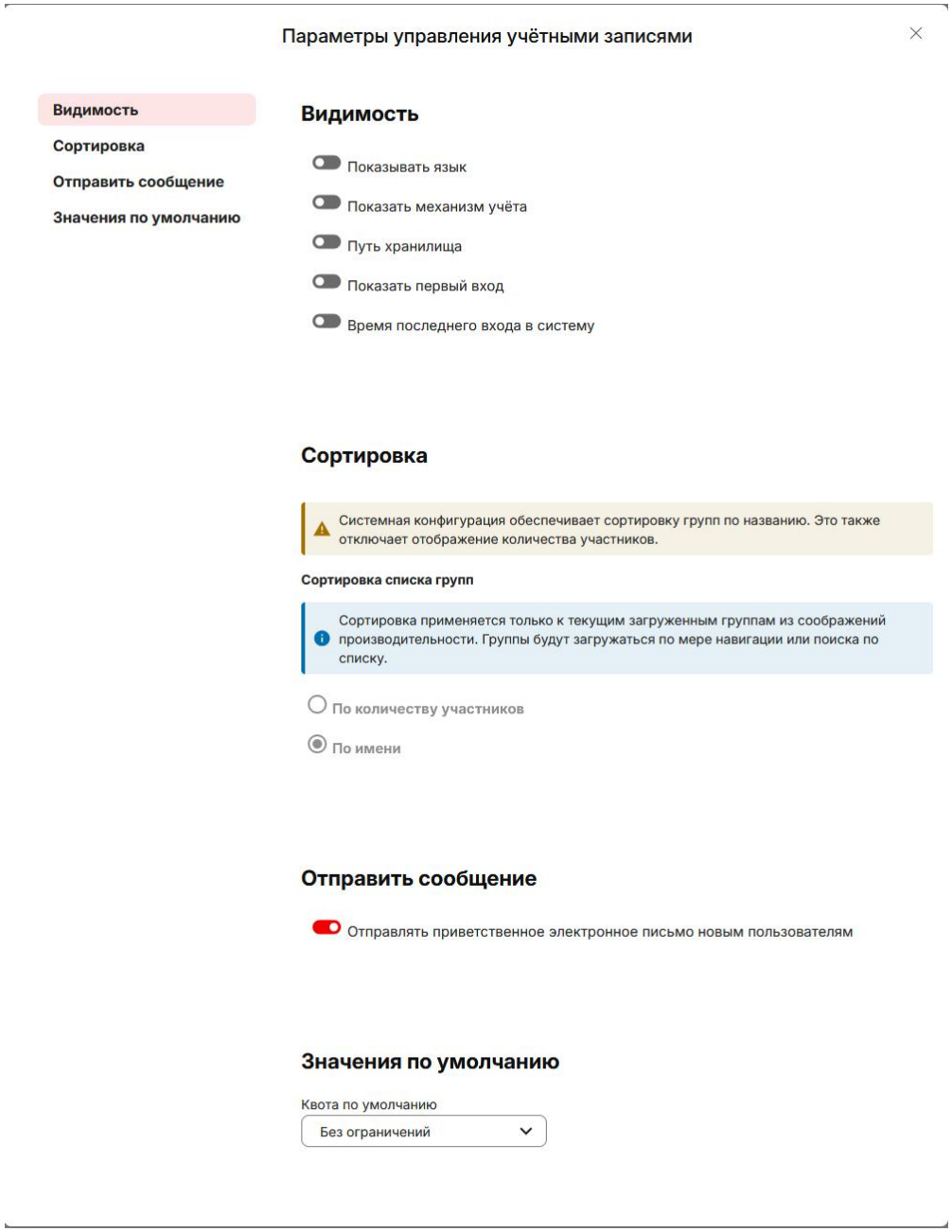


Рисунок 115. Параметры управления учётными записями

Параметры управления позволяют:

- Установить квоту хранилища для пользователей по умолчанию;
- Отобразить дополнительные поля:
  - Показать место хранения данных,
  - Показать время первого и последнего входа в систему,
  - Показать используемый метод входа в систему,
- Настроить отправку электронных писем новым пользователям.

Включите дополнительные параметры отображения сведений о пользователях в параметрах. В интерфейсе отобразятся поля:

Поле	Описание	Пример 1	Пример 2
Язык	Язык интерфейса пользователя	Русский	Русский
Механизм учёта	Источник учетных записей. Локальные пользователи, пользователи загруженные из LDAP / AD	Database	LDAP
Расположение хранилища	Расположение хранилища у пользователя	/var/www/html/data/admin	/var/www/html/data/DECB9B68-EE23-45CA-B02B-6F2B28C9B1E4
Первый вход	Дата и время первого входа	17.10.2025, 15:20	20.10.2025, 15:06
Последний вход	Время последнего входа в систему	час назад	2 дня назад

В поле **Квота по умолчанию** выберите или введите значение квоты по умолчанию для пользователей.

ПРЕДУПРЕЖДЕНИЕ

- При изменении квоты по умолчанию в настройках, также изменится квота в настройках пользователей у которых не настроена индивидуальная квота.
- Если квота по умолчанию будет указана меньше, чем пользователем занято в файловом хранилище, то у пользователя будет превышен лимит и он не сможет загружать файлы.

Активируйте опцию **Отправлять приветственное электронное письмо новым пользователям** для рассылки письма новым пользователям.

ПРИМЕЧАНИЕ

- Для отправки писем необходимо иметь работающий почтовый сервер.
- Письмо отправляется на адрес электронной почты, указанный в профиле учетной записи.

4.8.3. Управление группами

4.8.3.1. Создание группы пользователей

Для создания новой группы рядом с заголовком **Участник групп** нажмите на кнопку **+**.

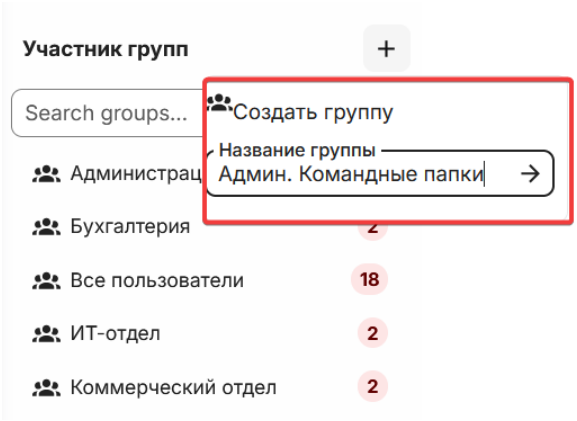


Рисунок 116. Создание новой группы

В открывшемся всплывающем окне в поле **Название группы** введите название новой группы.

Нажмите кнопку → .

Новая группа появится в списке.

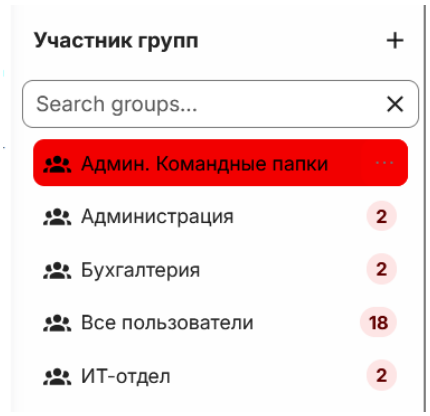


Рисунок 117. Созданная группа

4.8.3.2. Переименование группы пользователей

Выберите группу, которую нужно переименовать.

Справа от названия группы нажмите на кнопку **…**.

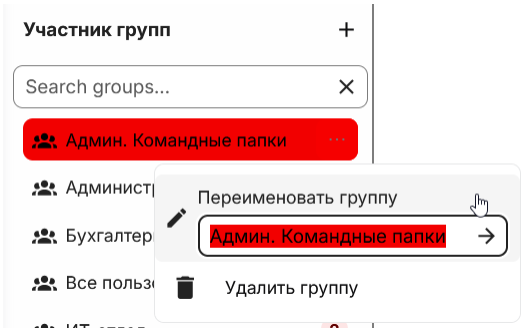


Рисунок 118. Переименование группы

В поле **Переименовать группу** введите новое название группы.

Нажмите кнопку → .

Группе присвоено новое название.

4.8.3.3. Удаление группы

Выберите группу, которую нужно удалить.

Справа от названия группы нажмите на кнопку ….

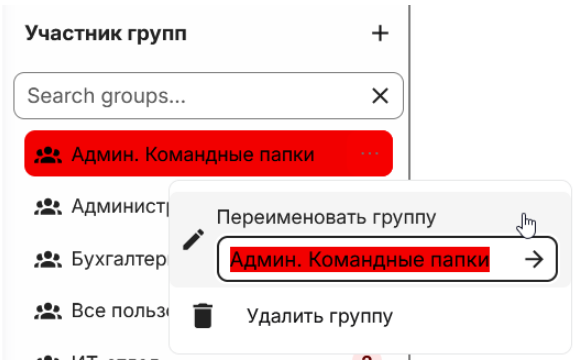


Рисунок 119. Удаление группы

Нажмите на кнопку **Удалить группу**.

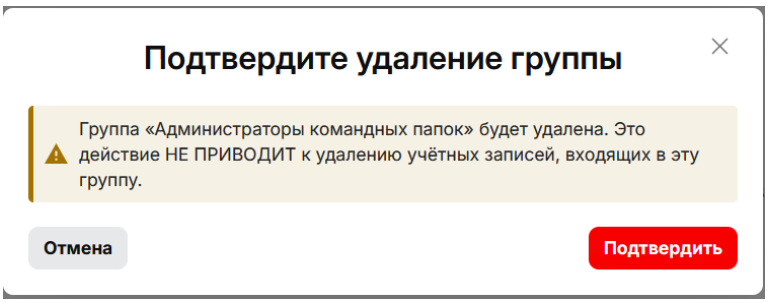


Рисунок 120. Подтверждение удаления группы

В открывшемся окне **Подтвердите удаление группы** нажмите на кнопку **Подтвердить** для согласия на удаление группы.

ПРИМЕЧАНИЕ

- Нельзя удалить группы пользователей, созданные при импорте из LDAP / AD. См. «Интеграция с каталогами пользователей»
- Нельзя удалить системные группы пользователей **Гости** и **Все пользователи**.

4.8.4. Управление пользователями

4.8.4.1. Создание нового пользователя

Для создания нового пользователя нажмите на кнопку + **Новая учетная запись**.

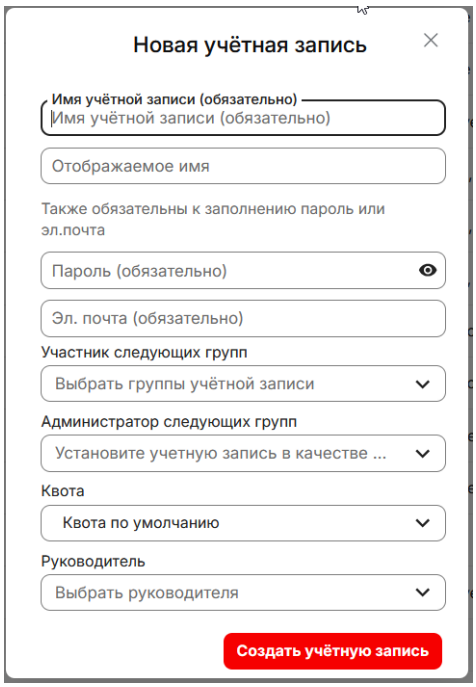


Рисунок 121. Форма «Новая учетная запись»

В открывшейся форме **Новая учетная запись**, введите следующие данные:

Поле	Описание	Пример
Имя учетной записи (обязательное поле)	Уникальный идентификатор пользователя. Имена пользователей могут содержать буквы (`a-z`, `A-Z`), цифры (`0-9`), дефисы (`-`), символы подчеркивания (`_`), точки (`.`), пробелы () и знаки @ (`@`). После создания пользователя вы можете указать его полное имя, если оно отличается от имени пользователя, или оставить поле пустым, чтобы пользователь заполнил его самостоятельно.	GromovAV
Отображаемое имя	Необязательное поле. Если не указать, примет значение из **Имя учетной записи**	Громов Алексей Викторович
Пароль (обязательное поле)	Пароль нового пользователя. Справа от поля расположен значок **глаз**, который выполняет функцию маскировки пароля	*****
Электронная почта (обязательное поле)	Адрес электронной почты на который будет выслано	GromovAV@almipartner.ru

Поле	Описание	Пример
	приветственное письмо	

Укажите группы, к которым будет относиться новая учетная запись, в поле **Участник следующих групп**. Поле может быть заполнено позже.

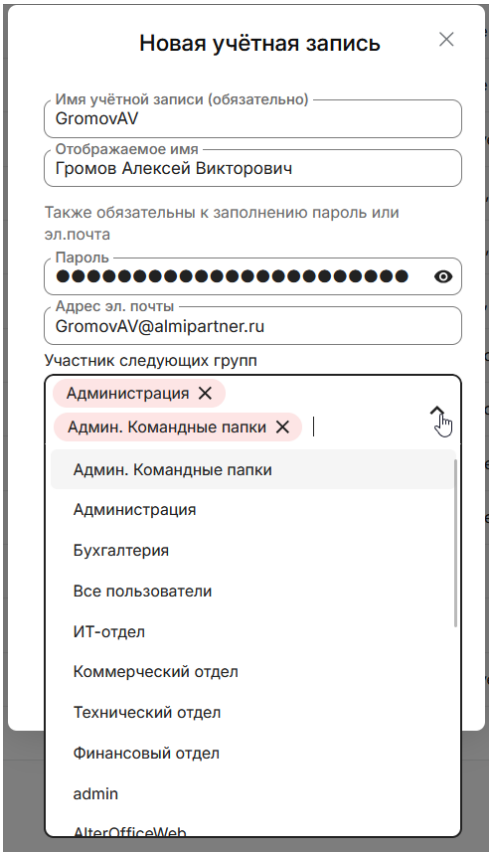


Рисунок 122. Назначение пользователю групп пользователей

Выбранные группы отображаются в виде тегов с названием и крестиком для удаления.

ПРИМЕЧАНИЕ

- Системная группа **Все пользователи** не может быть назначена пользователю вручную, в нее по умолчанию добавляются все пользователи системы автоматически.

В поле **Администратор следующих групп** установите группы, в которых пользователь будет Администратором групп.

В поле **Квота** укажите лимит объема доступного хранилища или оставьте без изменения, чтобы было использовано значение по умолчанию.

В поле **Руководитель** укажите линейного руководителя пользователя. Для идентификации руководителя используйте значение поля **Имя учетной записи**.

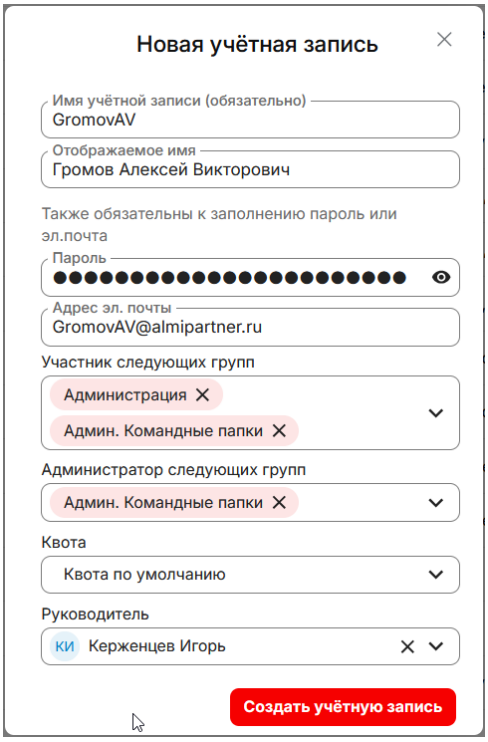


Рисунок 123. Создание нового пользователя

Для создания пользователя нажмите кнопку **Создать учётную запись**.

Учетная запись будет создана в системе и отобразится в списке пользователей.

ПРИМЕЧАНИЕ

- Для успешного создания учетной записи необходимо заполнить все обязательные поля (имя, пароль и электронная почта).
- Если в параметрах управления учётными записями активирована опция **Отправлять приветственное электронное письмо новым пользователям**, система автоматически отправит новому пользователю уведомление.

4.8.4.2. Редактирование учетных записей пользователей

Для перехода в режим редактирования учетной записи нажмите на иконку **Карандаш**.

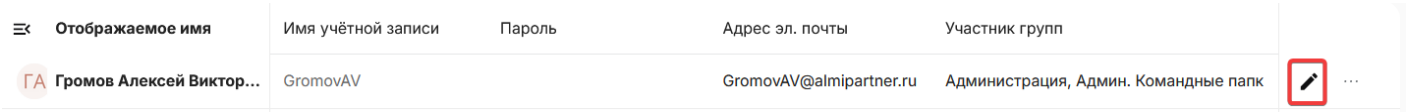


Рисунок 124. Редактирование учетной записи

Открывается режим редактирования с возможностью:

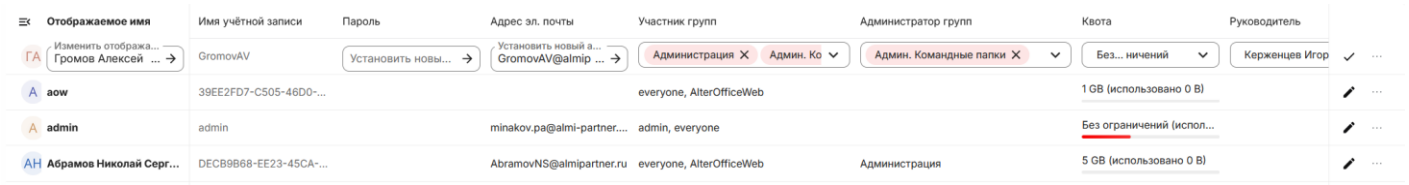


Рисунок 125. Режим редактирования учетной записи

- **Изменить отображаемое имя** пользователя в текстовом поле.
- **Установить новый пароль** пользователя.
- **Установить новый адрес электронной почты**.
- **Изменить участие в группах** - добавить или ограничить участие в группах (для удаления нажмите на крестик в метке).
- **Назначение администратора группы** - назначить права для администрирования в группе.
- **Изменение квоты хранилища**.
- **Назначение руководителя** - выбор из списка доступных пользователей.

1. Сброс пароля пользователя

Чтобы установить новый пароль пользователя выполните действия:

- Перейдите в режим редактирования - нажмите на иконку **Карандаш**.
- Установите курсор в поле **Пароль**.
- Введите новый пароль пользователя в поле для ввода пароля и не забудьте сообщить пользователю его пароль.

Для применения изменений нажмите на иконку .

После нажатия изменения сохраняются в системе.

2. Переименование пользователя

У каждого пользователя системы есть два имени: уникальное имя для входа, используемое для аутентификации, и полное имя, которое отображается в профиле. Вы можете изменить отображаемое имя пользователя, но не можете изменить имя для входа.

Чтобы изменить отображаемое имя пользователя выполните действия:

- Перейдите в режим редактирования - нажмите на иконку **Карандаш**.
- Установите курсор в поле **Отображаемое имя**.
- Введите новое отображаемое имя пользователя.

Для применения изменений нажмите на иконку .

После нажатия изменения сохраняются в системе.

3. Предоставление пользователю прав администратора

В системе есть два типа администраторов:

- Администраторы системы;
- Администраторы групп.

Администраторы групп **имеют право** в назначенных им группах:

- создавать пользователей;
- редактировать пользователей;
- удалять пользователей.

Администраторы групп **не могут**:

- получать доступ к настройкам системы;
- добавлять или изменять пользователей в группах, для которых они не являются администраторами групп.

Чтобы настроить **права администратора группы** выполните действия:

- Перейдите в режим редактирования - нажмите на иконку **Карандаш**.
- Установите курсор в поле **Администратор групп**.
- Выберите нужные группы из раскрывающегося списка, чтобы назначить права администратора для выбранных групп.

Администраторы системы имеют полные права доступа через веб-интерфейс системы и могут:

- просматривать настройки системы;
- изменять настройки системы;
- назначать другим пользователям права **администратора системы**.

Чтобы назначить пользователю права **администратора системы** выполните действия:

- Добавьте пользователю системную группу **admin**.

Для применения изменений нажмите на иконку  .

После нажатия изменения сохраняются в системе.

4.8.4.3. Активация и деактивация учетных записей пользователей

При необходимости пользователь может быть временно заблокирован в системе (пользователь будет отключен, настройки и файлы пользователя будут храниться в системе). Активировать пользователя можно в любое время без потери настроек и данных.

ПРИМЕР

- В организации принято, что при нахождении пользователя в отпуске, информационные ресурсы блокируются для пользователя.
- При возвращении из отпуска, доступ восстанавливается.

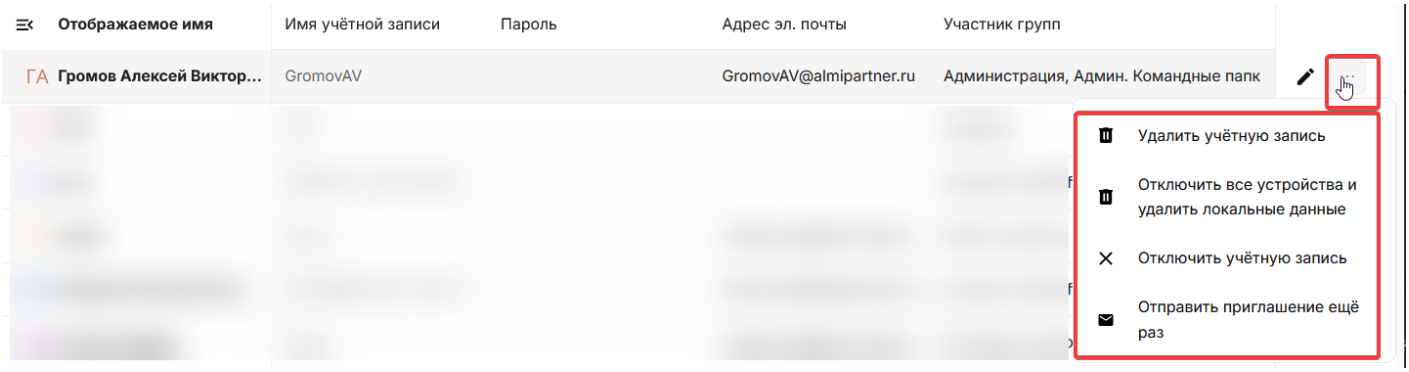


Рисунок 126. Дополнительные действия над учетной записью пользователя

Чтобы **заблокировать пользователя** в системе выполните действия:

- Нажмите на иконку **….**
- В открывшемся меню выберите пункт **Отключить учётную запись**.
- Система заблокирует вход для пользователя.

Учетная запись переместится из раздела **Все аккаунты** в **Отключённые учётные записи**.

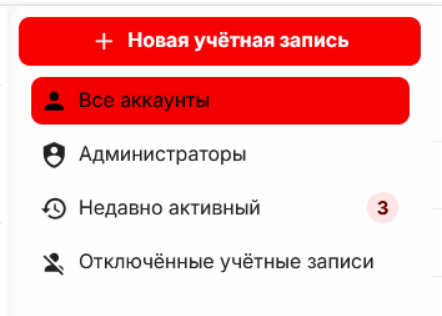


Рисунок 127. Блок быстрых фильтров

ПРИМЕЧАНИЕ

Пользователь больше не сможет получить доступ к системе, пока его учетная запись не будет активирована. Кроме того, будут недоступны все внешние ссылки и уведомления по электронной почте. Внутренние ссылки будут работать, чтобы другие пользователи системы могли продолжать работу.

Для **активации пользователя**:

- Перейдите в раздел **Отключённые учётные записи** и выберите пользователя.
- Нажмите на меню **…** и выберите пункт **Включить учётную запись**.

4.8.4.4. Удаление пользователей

Чтобы **удалить пользователя** в системе выполните действия:

- Нажмите на иконку **….**
- В открывшемся меню выберите пункт **Удалить учётную запись**.
- В открывшемся окне **Удаление учётной записи** подтвердите удаление выбранного пользователя.
- Система удалит пользователя со всеми его данными.

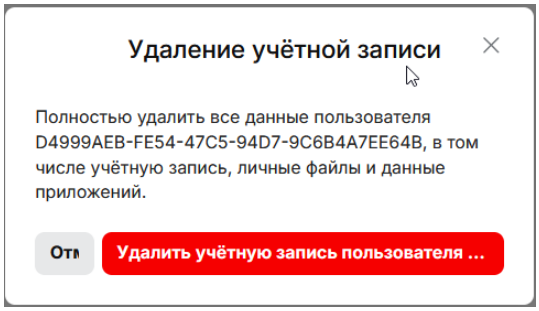


Рисунок 128. Подтверждение удаления пользователя

Все файлы, принадлежащие пользователю, также удаляются, в том числе все файлы, которыми он поделился с другими пользователями.

4.9. Управление ролями пользователей

Определение ролей доступа к системе является важным шагом в настройке АльтерОфис Веб, поскольку оно позволяет реализовать принцип минимальных привилегий и обеспечить безопасность данных.

4.9.1. Роли доступа в системе

Система позволяет управлять доступом к данным и функциям, в зависимости от того, к какой группе и / или роли принадлежит пользователь.
Пользователи объединяются в группы (например, «ИТ-отдел», «Администрация»).

Роль – это комбинация настроек:

- Групп пользователей;
- Настройка доступа к групповым папкам;
- Ограничения по приложениям.

В зависимости от группы и роли, пользователю разрешается или запрещается:

- просматривать файлы,
- редактировать документы,
- делиться папками,
- настраивать приложения,
- видеть определённые разделы интерфейса и т.д.

4.9.1.1. Базовые роли доступа

В системе реализована ролевая модель, включающая следующие базовые роли: **администратор системы**, **пользователь**, **все пользователи** и **гость**.

Роль	Права и полномочия	Уровень доступа
Администратор системы [2]	- Доступ ко всем настройкам системы - Управление пользователями и группами - Включение и настройка приложений - Назначение ролей администраторов групп - Управление политиками безопасности - Делегирование функций администрирования **Ограничения:** Отсутствуют	Системный
Пользователь	- Доступ к личному хранилищу файлов - Использование разрешенных приложений - Создание и участие в группах - Работа с общими ресурсами **Ограничения:** - Запрет на доступ к системным настройкам	Пользовательский
Все пользователи [3]	- Автоматически применяется ко всем существующим и будущим пользователям системы - Применяется при настройке общего доступа к ресурсам для всей организации **Особенности и ограничения:** - Действует для всех пользователей независимо от их основных ролей - Автоматически распространяется на новых пользователей - Не включает гостевые учетные записи - Не отменяет индивидуальные настройки прав для конкретных пользователей	Системный
Гость [4]	- Доступ только к явно предоставленным ресурсам - Скачивание разрешенных файлов **Ограничения:** - Отсутствие личного хранилища - Запрет на создание общих ресурсов - Запрет на использование большинства приложений	Ограниченный

[2] Системная роль, с идентификатором группы **`admin`**.

[3] Специальная системная роль, с идентификатором группы **`everyone`**, которая автоматически включает всех зарегистрированных пользователей системы, включая вновь создаваемые учетные записи.

[4] Специальная системная роль, с идентификатором группы **`guests`**, предназначена для краткосрочного сотрудничества без предоставления полномочий постоянного пользователя.

4.9.1.2. Делегированные роли

Система позволяет администраторам делегировать полномочия другим пользователям, не предоставляя им полные права администратора (и не делая их членами группы **`admin`**).

Для этого администратор системы создает группы, которым делегирует определенные права доступа и включает в группу пользователей.

Примерами таких групп могут быть:

Роль	Права и полномочия	Уровень доступа	Область действия
Администратор группы	- Создание новых пользователей в пределах своей группы - Назначение пользователей в свою группу - Управление правами доступа пользователей группы - Настройка квот хранилища для пользователей группы **Ограничения:** - Запрет на управление другими группами - Запрет на назначение роли администратора системы - Запрет на доступ к системным настройкам	Групповой	В рамках назначенной группы
Администратор безопасности	- Аудит назначенных прав и привилегий - Просмотр логов безопасности и аудита - Проверка безопасности и параметров	Системный (с ограничениями)	Безопасность и контроль доступа

4.9.2. Назначение ролей

4.9.2.1. Назначение роли администратора системы

По умолчанию только члены группы `admin` могут получить доступ к настройкам администрирования. Вы можете создать дополнительные группы пользователей (или использовать существующие), а затем предоставить этим группам доступ к определенным настройкам.

После входа в учётную запись, принадлежащую группе `admin`, нажмите на аватар пользователя и в открывшемся меню выберите пункт **«Учетные записи»**.

Шаги выполнения

1. Создание нового пользователя

Создайте нового пользователя.

СМ. ТАКЖЕ

- Подробнее см. в разделе «Создание нового пользователя».

Если пользователь уже создан, выберите его.

2. Добавьте пользователю группу admin

Откройте учетную запись на редактирование и назначьте пользователю группу `admin`.

ПРИМЕЧАНИЕ

- Рекомендуется ограничить количество пользователей с правами `admin`.
- Используйте системную учетную запись для первичного создания пользователей с правами `admin`.
- Используйте именованные учетные записи с правами `admin` для повседневной работы.

4.9.2.2. Назначение роли администратора группы

Роль администратора группы позволяет управлять пользователями и ресурсами в рамках своей группы, без предоставления полного доступа к системе. Эта роль подходит для руководителей отделов и менеджеров проектов, которые могут самостоятельно управлять своими командами в рамках назначенных групп.

Администратор группы получает права на создание пользователей, управление квотами хранилища и контроль доступа к ресурсам своей группы, что снижает нагрузку на системного администратора.

ПРИМЕР

- В организации созданы группы пользователей по названию отделов: «Администрация», «ИТ-отдел», «Бухгалтерия»;
- За каждой группой закреплен сотрудник, который будет иметь возможность создавать пользователей в группе.

Шаги выполнения

Для делегирования прав выполните описанные ниже действия.

1. Выбор пользователя

Зайдите в раздел **«Учетные записи»** в правами `admin`.

Выберите пользователя, которому нужно назначить права, и откройте его учетную запись на редактирование.

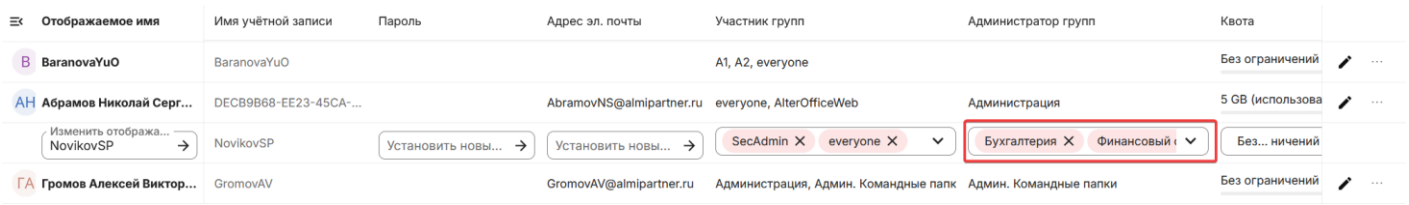


Рисунок 129. Редактирование учетной записи пользователя

2. Делегирование прав на администрирование групп

Добавьте выбранному пользователю в поле **Администратор групп** группы, в которых он будет администратором.

После настроек, пользователю с правами **администратора группы** станут доступны:

- Создание и управление пользователями в рамках назначенной группы.
- Назначение квот хранилища для пользователей своей группы.
- Управление членством в группе (добавление/удаление пользователей).

4.9.2.3. Делегирование прав на взаимодействие с модулями системы

Система позволяет **администраторам системы** предоставлять доступ к определенным модулям только пользователям, входящим в определённые группы.

ПРИМЕЧАНИЕ

- Делегирование прав на взаимодействие с модулями системы рассмотрено на примере **Share Review**. Данное приложение позволяет выполнять мониторинг предоставленных для общего доступа ресурсов.

Шаги выполнения

1. Создание группы

Создайте новую группу с названием **Мониторинг общего доступа**.

СМ. ТАКЖЕ

- Подробнее см. в разделе «Создание группы пользователей».

2. Проверьте доступность модуля Share Review

Убедитесь, что модуль **Share Review** активирован.

СМ. ТАКЖЕ

- Подробнее см. в разделе «Управление приложениями (модулями) системы».

3. Предоставьте доступ к модулю Share Review

Выберите приложение Share Review. Справа под описанием приложения активируйте опцию **Разрешить использование только участникам этих групп**.

В раскрывающемся списке выберите группы **Мониторинг общего доступа** и **admin**.

Обновите страницу приложений.

После настройки, пользователи входящие в группы **Мониторинг общего доступа** и **admin** будут иметь доступ к просмотру списка общих ресурсов системы.

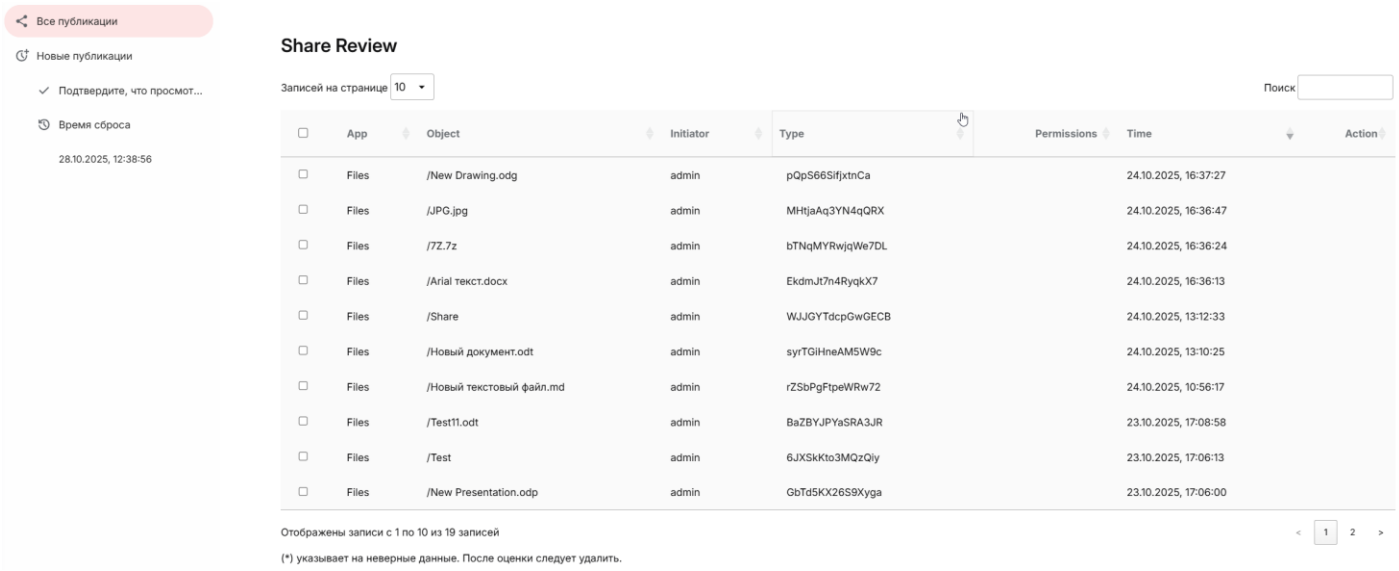


Рисунок 130. Ресурсы системы с общим доступом

4.9.2.4. Делегирование доступа к определенным разделам настроек администрирования

Администратор системы может делегировать доступ к некоторым разделам настроек системы.

Шаги выполнения

Для создания роли **администратора безопасности**, которая будет иметь доступ к настройкам и функциям, отвечающим за создание групп и пользователей, просмотр журнала системных событий и аудита пользовательских действий, настройкам предоставления общего доступа, выполните описанные ниже действия под пользователем, входящим в группу `admin`.

1. Создание группы

Создайте новую группу с названием **Администраторы безопасности**.

> СМ. ТАКЖЕ
>
> - Подробнее см. в разделе «Создание группы пользователей».

2. Настройка делегирования прав

Нажмите на аватар пользователя и в открывшемся меню выберите пункт «Параметры сервера».

В левой боковой панели в разделе **Параметры сервера** выберите пункт **Администрирование**.

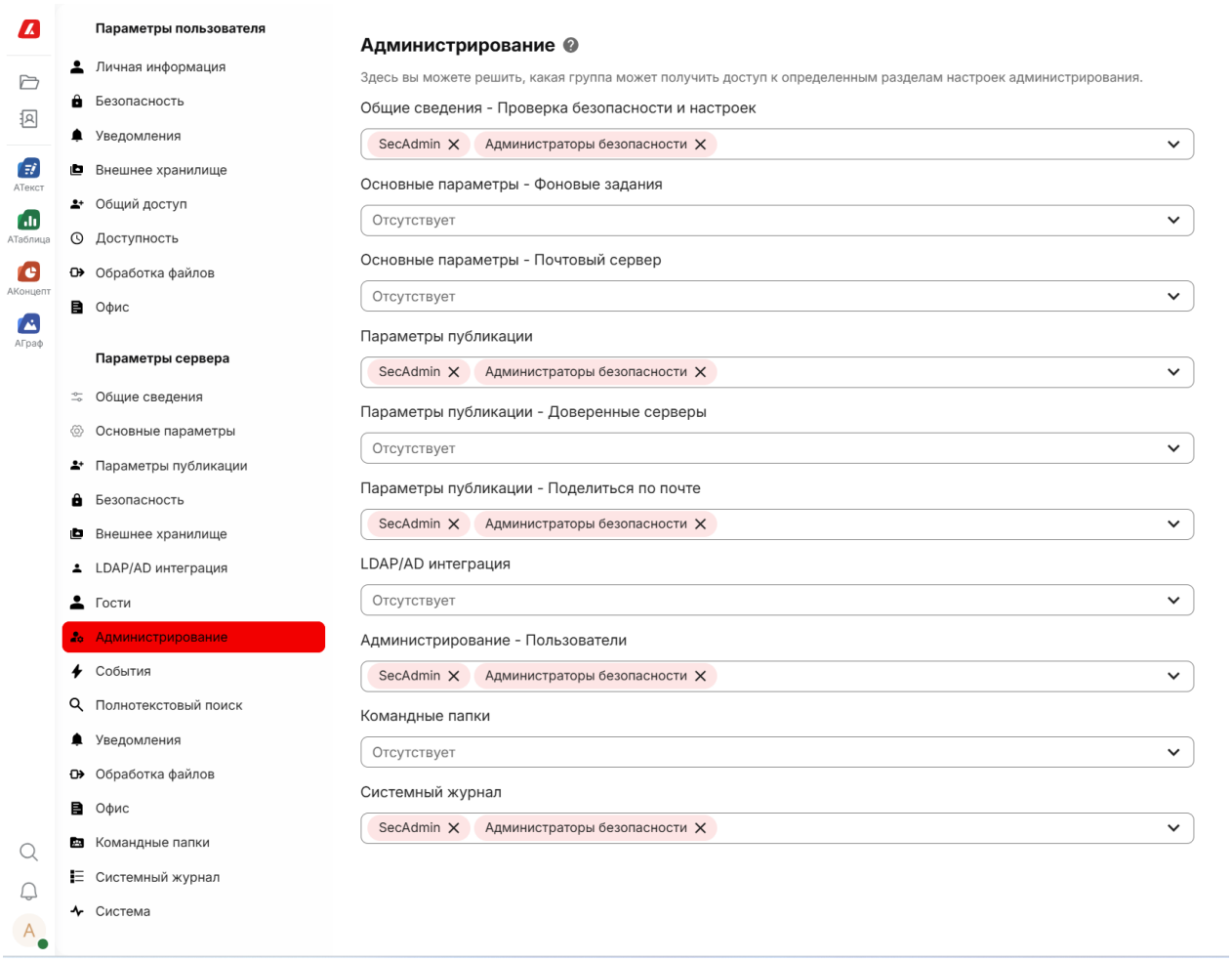


Рисунок 131. Делегирование разделов настроек

Добавьте группу **Администраторы безопасности** к разделам:

- Общие сведения - Проверка безопасности и настроек.
- Параметры публикации.
- Параметры публикации - Поделиться по почте.
- Администрирование - Пользователи.
- Системный журнал.

3. Назначение пользователям прав администратора безопасности

Нажмите на аватар пользователя и в открывшемся меню выберите пункт «Учетные записи».

Выберите пользователя, которому нужно назначить права, и откройте его учетную запись на редактирование.

В поле **Участник групп** укажите группу **Администраторы безопасности**.

4. Делегированный доступ

После выполненных действий, пользователь, входящий в группу **Администраторы безопасности** получает ограниченный доступ к системным настройкам.

- **Управление пользователями.** (пользователь с такими правами не может поднять привилегии до прав `admin`).
- **Проверка безопасности и настроек.**

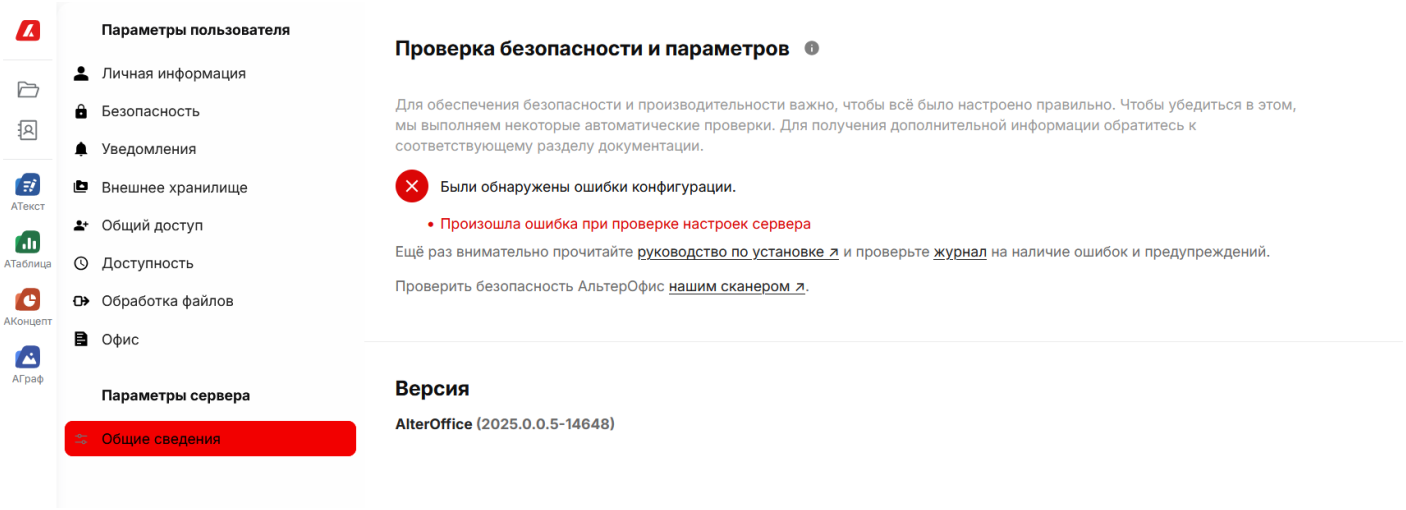


Рисунок 132. Проверка безопасности и настроек

- **Параметры публикации.**

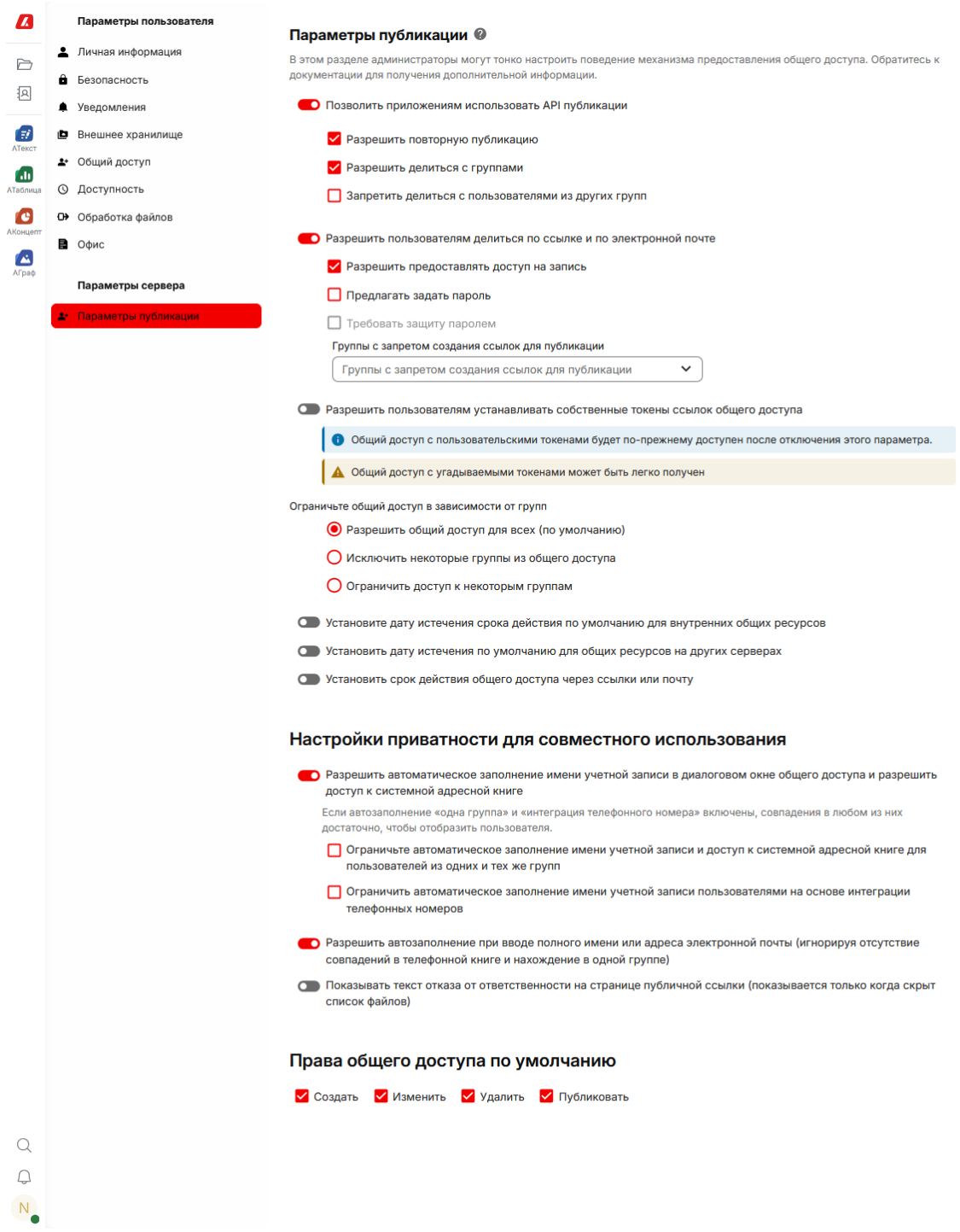


Рисунок 133. Параметры публикации

- **Предоставление доступа к ресурсам по почте.**

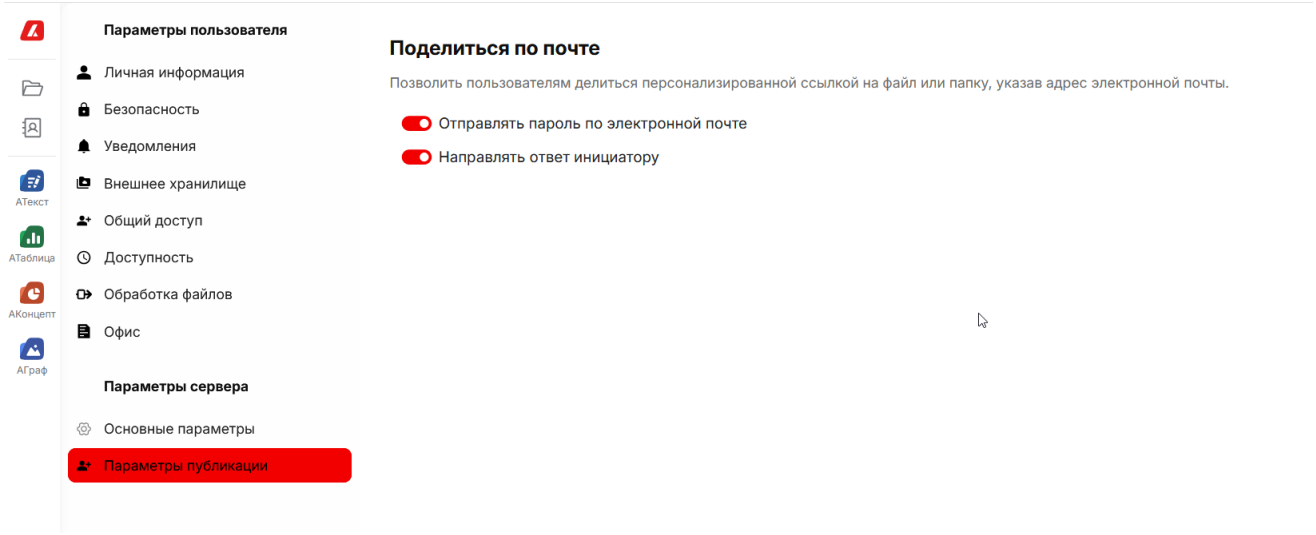


Рисунок 134. Поделиться по почте

- **Просмотр системного журнала.**

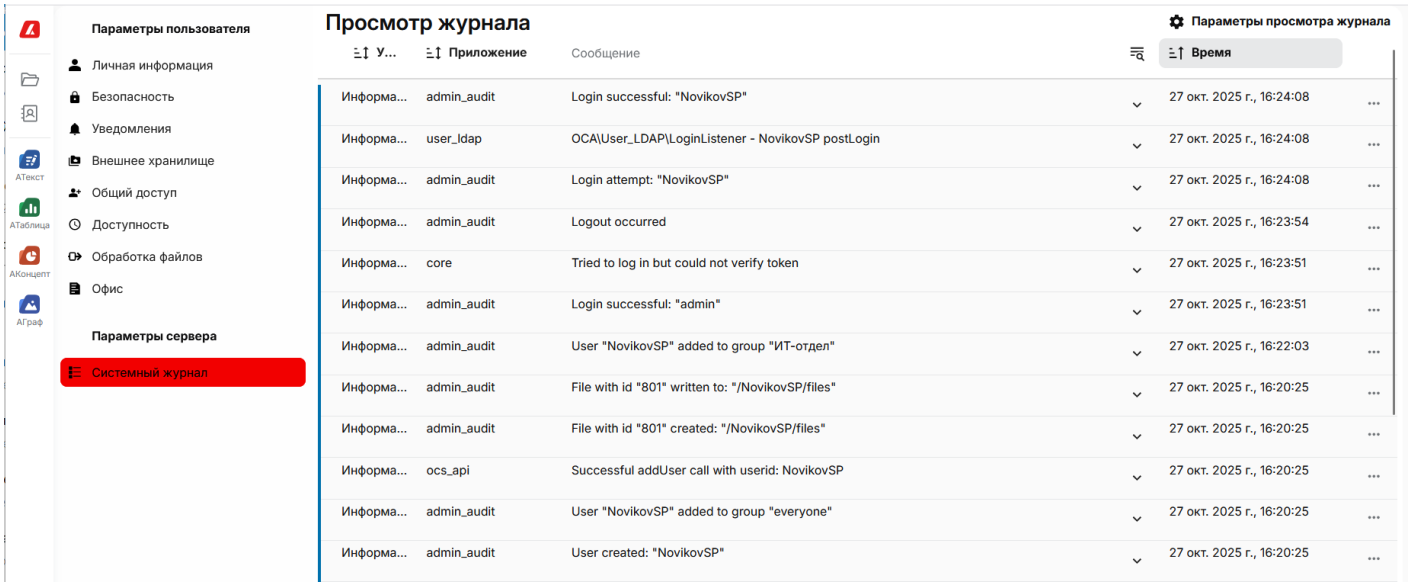
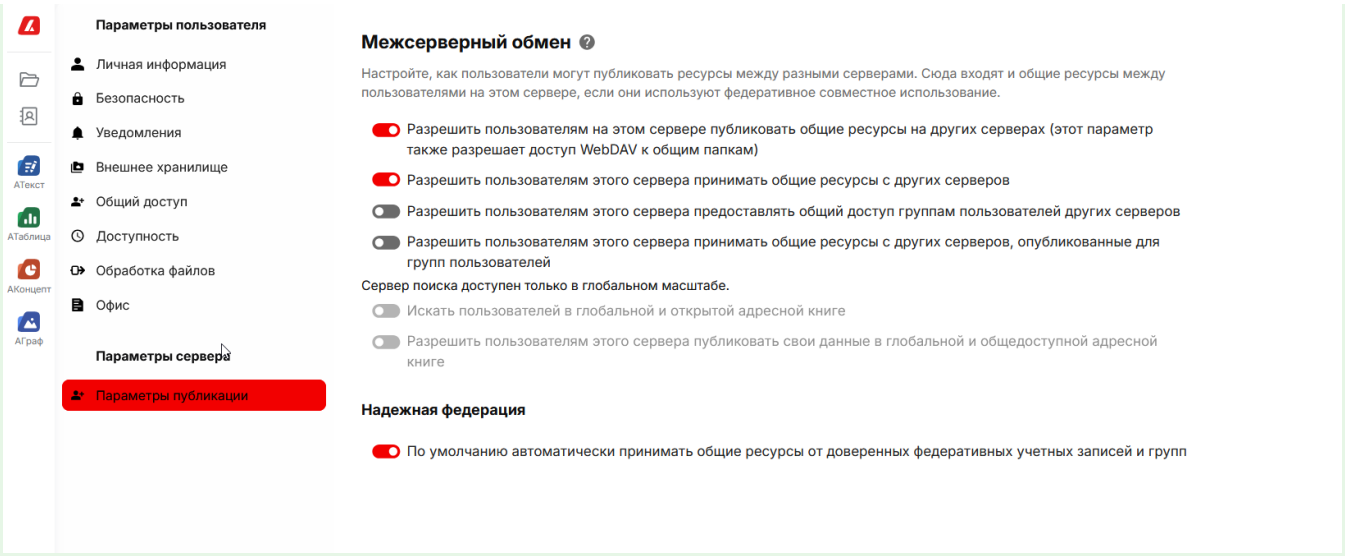


Рисунок 135. Системный журнал

ПРИМЕЧАНИЕ

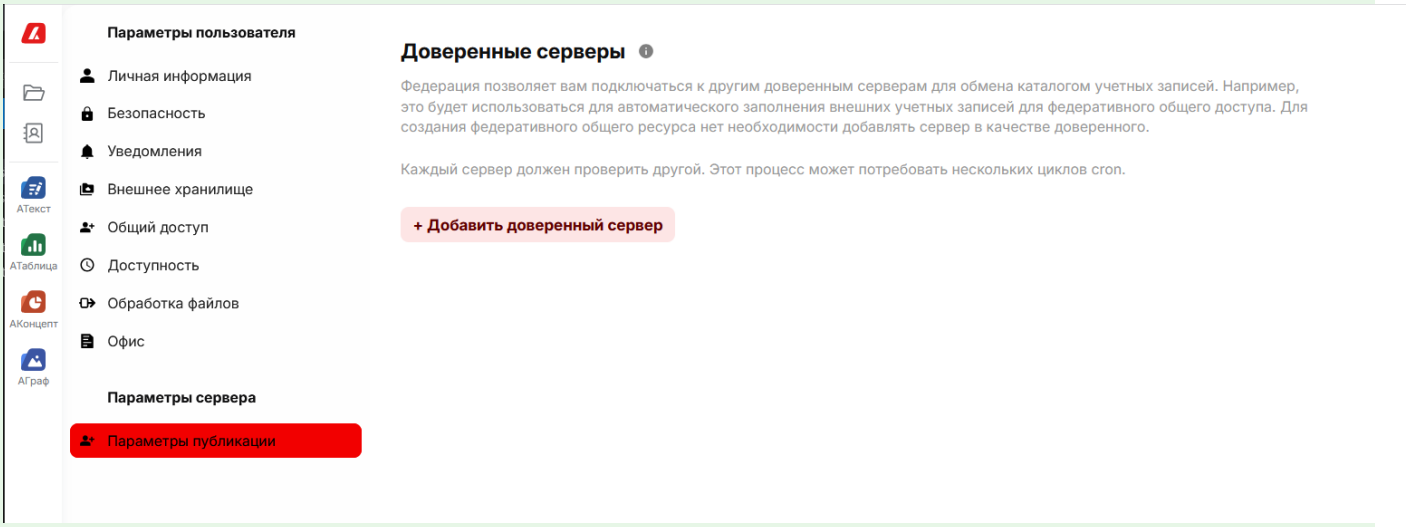
При необходимости, **администратор системы** может делегировать и другие настройки:

- **Настройку федеративного доступа.**



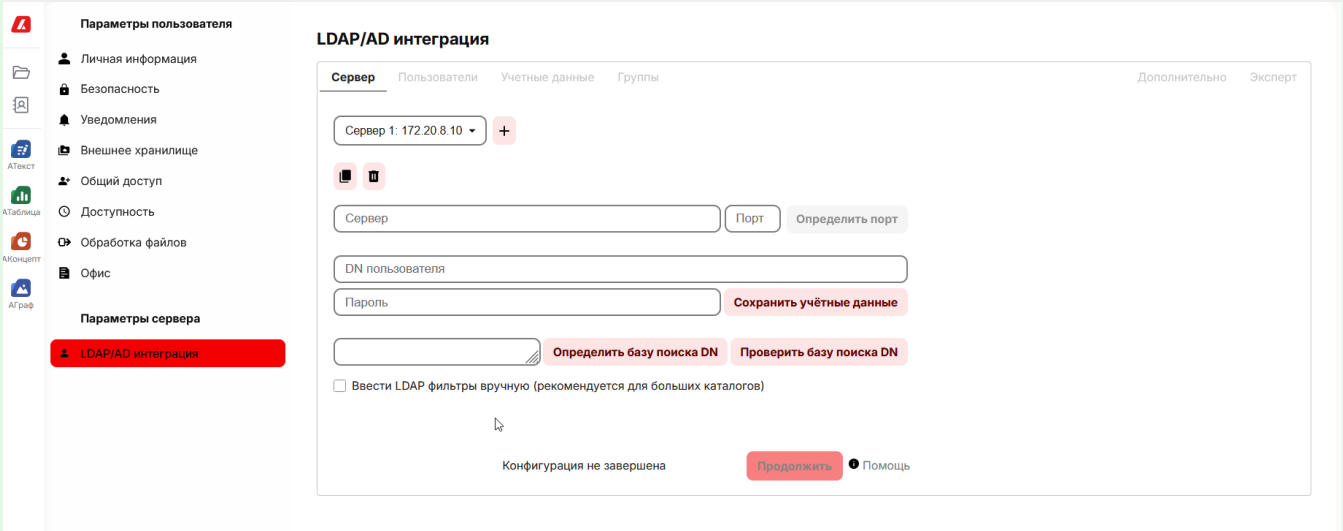
Межсерверный обмен

- **Настройку доверенных серверов.**



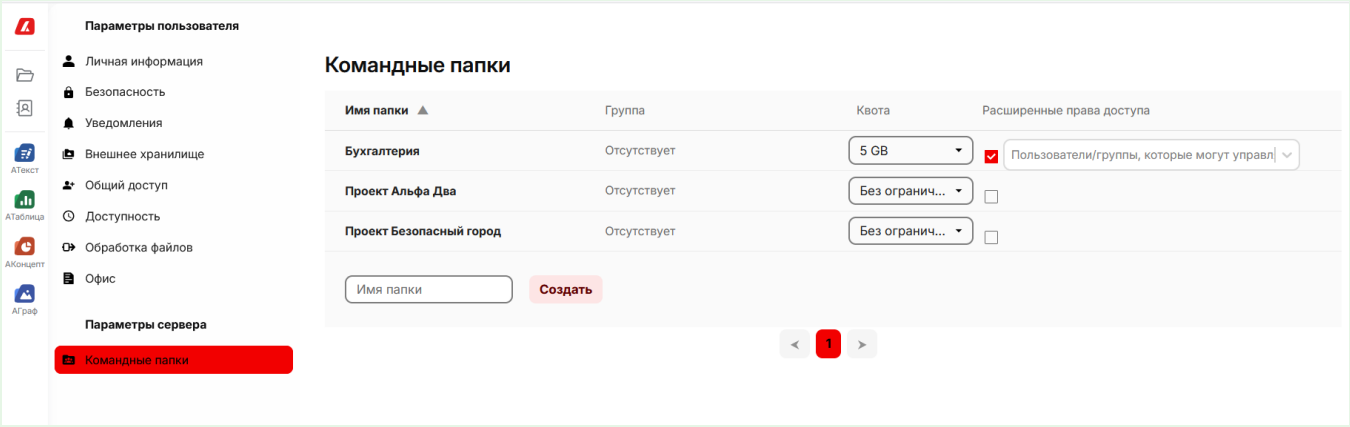
Доверенные сервера

- **Настройку LDAP / AD интеграция.**



LDAP / AD интеграция

- **Управление командными папками.**



Управление командными папками

4.10. Управление приложениями (модулями) системы

Функциональность системы сгруппирована в отдельные приложения (модули). Активируя и отключая модули, администратор системы может расширять или ограничивать возможности системы и пользователей.

Перед началом работы пользователей с системой, администратору системы нужно проверить и активировать необходимые модули.

ПРИМЕЧАНИЕ

- При установке системы приложения включаются по умолчанию.

4.10.1. Управление приложениями

Раздел **Приложения** представляет собой список с данными по приложениям (модулям) системы.

1. Общий вид интерфейса

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя  и в открывшемся меню выберите пункт **Приложения**.

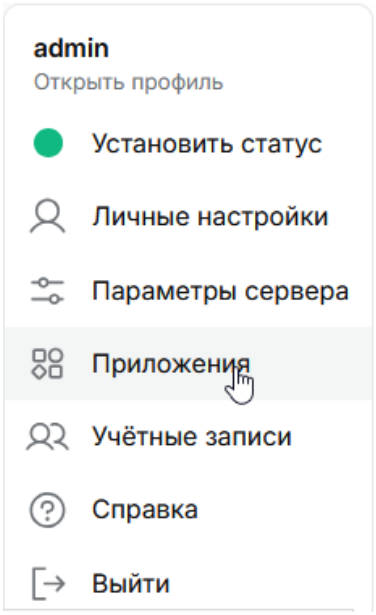


Рисунок 136. Меню администратора

Откроется страница со списком приложений (модулей).

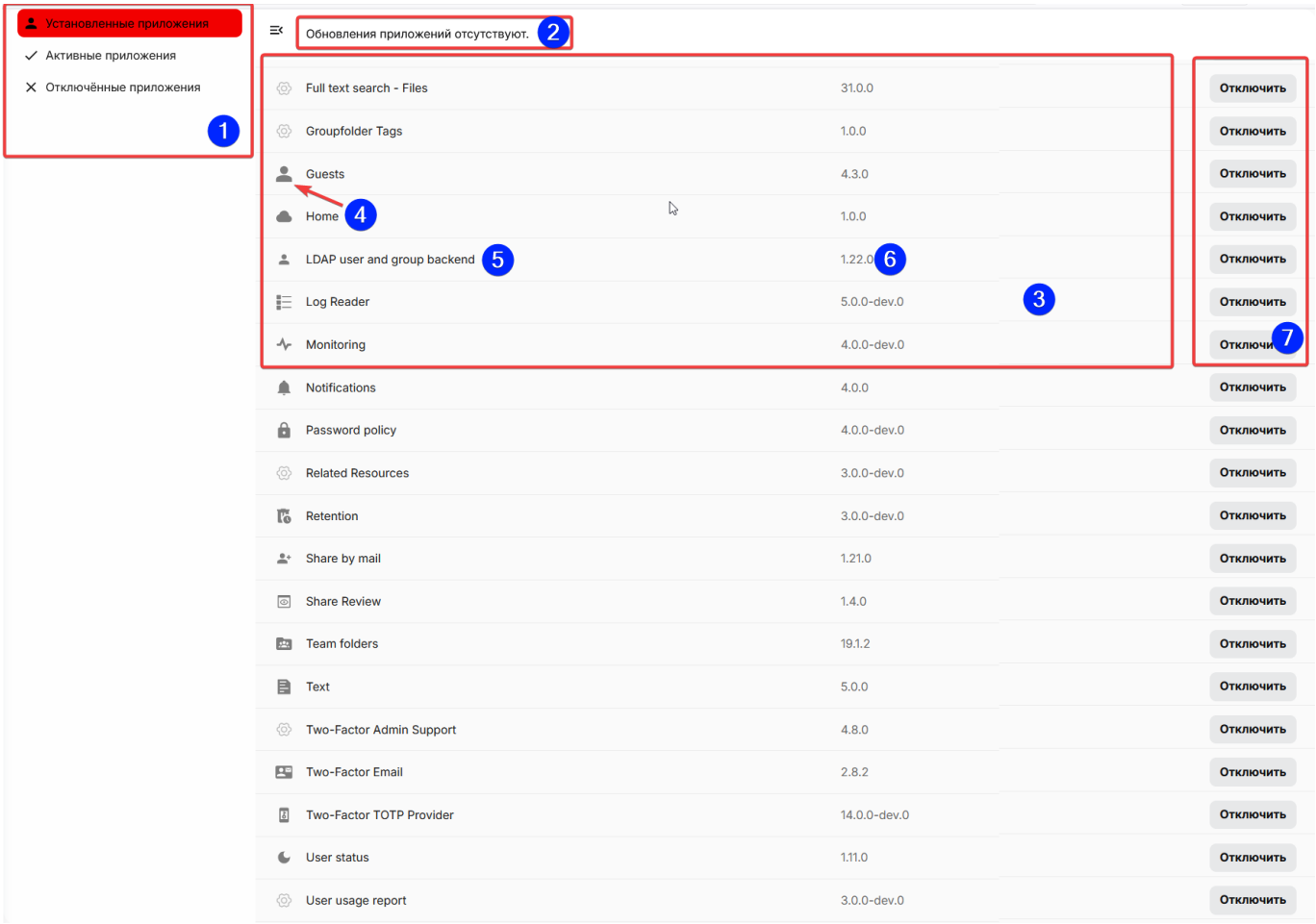


Рисунок 137. Список приложений

Информацию на странице поделена на блоки:

Элемент	Описание
(1) Блок **быстрых фильтров**	Позволяет просматривать список установленных, активных, отключённых приложений
(2) Индикация обновления приложений	При наличии новых версий приложений появляется значок, предупреждающий пользователя о возможных изменениях.
(3) Список приложений	Список приложений с учетов выбранного быстрого фильтра.
(4) Иконка приложения	Визуальный элемент.
(5) Название приложения	Название установленного приложения.
(6) Версия	Версия приложения.
(7) Кнопка	Функциональные кнопки.

2. Быстрые фильтры

В левой боковой панели доступны **быстрые фильтры** (1):

Элемент	Описание
Установленные приложения	Список всех приложений, которые установлены в системе. Здесь отображаются все добавленные приложения, независимо от того, активны они или нет. В этом разделе можно управлять приложениями – включать, отключать или удалять.
Активные приложения	Отображаются приложения, которые в данный момент включены (активированы) и работают в системе. Они обеспечивают текущую функциональность и доступны для использования пользователями.
Отключённые приложения	Здесь находятся приложения, которые установлены, но в данный момент отключены. Они не активны и не влияют на работу системы, т.е. функциональность этих приложений недоступна пользователям.

3. Отключение модулей

На странице **Приложения** можно включить или отключить приложения.

Для деактивации приложения выполните действия:

- В разделе **Установленные приложения** выберите приложение.
- Нажмите кнопку **Отключить**.
- Обновите страницу приложений.
- Убедитесь, что приложение переместилось в раздел **Отключённые приложения**.

> ПРЕДУПРЕЖДЕНИЕ
>
> Перед отключением приложения:
>
> - Убедитесь, что приложение не используется критическими процессами.
> - Уведомите пользователей о плановой деактивации приложения.
> - Создать резервную копию данных, если это необходимо.

4. Активация модулей

Для активации приложения выполните действия:

- В разделе **Отключённые приложения** выберите приложение.
- Нажмите кнопку **Включить**.
- Обновите страницу приложений.

- Убедитесь, что приложение переместилось в раздел **Активные приложения**.

5. Активация ограничения по группам

Доступ к некоторым приложениям может быть предоставлен только для определенных групп. Все остальные пользователи не увидят приложение в интерфейсе и не смогут его использовать.

Для определения групп, которые могут работать с модулем, выполните действия:

- В разделе **Установленные приложения** выберите приложение.
- Справа под описанием приложения активируйте опцию **Разрешить использование только участникам этих групп**.
- В раскрывающемся списке выберите нужные группы.
- Обновите страницу приложений.
- Убедитесь, что для приложения группы установлены корректно.

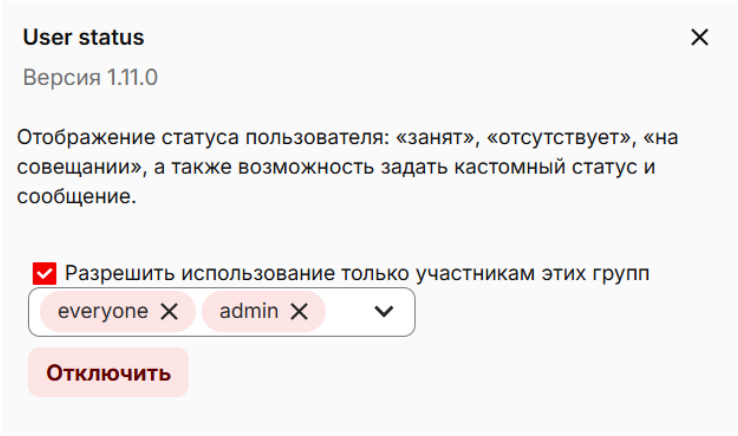


Рисунок 138. Активация доступа по группам

4.11. Системный журнал и аудит

Системный журнал – это инструмент для просмотра и мониторинга событий и ошибок, происходящих в системе (действия пользователей, ошибки приложений, системные события).

Журнал позволяет отслеживать аутентификацию, операции с файлами, изменения настроек и подключений, а также использовать данные для расследования инцидентов и анализа безопасности.

4.11.1. Просмотр системного журнала

Для просмотра системного журнала выполните действия:

- Нажмите на аватар пользователя и в открывшемся меню выберите пункт **Параметры сервера**.
- В левой боковой панели в разделе **Параметры сервера** выберите пункт **Системный журнал**.

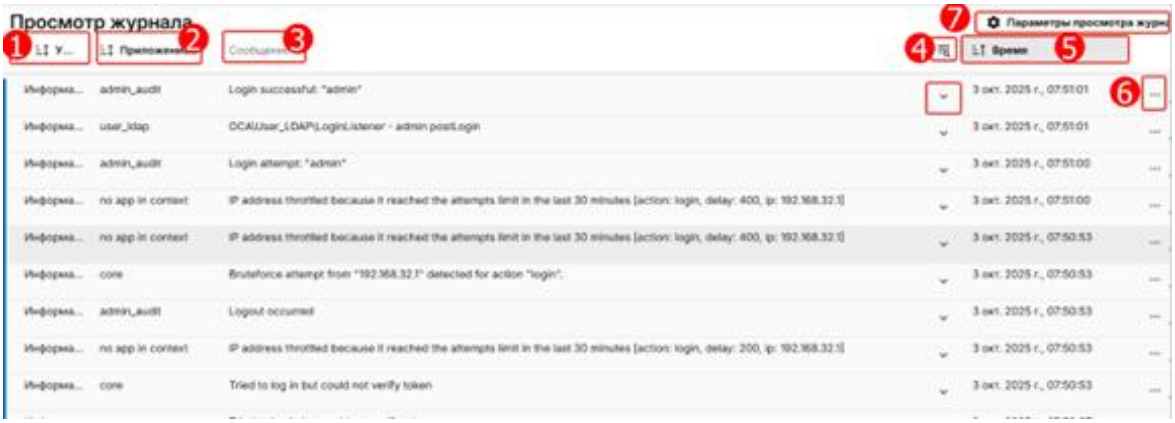


Рисунок 139. Системный журнал

Системный журнал представляет собой таблицу, в строках которой отображаются события.

Информацию на странице можно разделить на блоки:

Элемент	Описание
(1) Уровень	Поле **Уровень** определяет насколько детальными отображать записи на странице.
(2) Приложение	Поле **Приложение** – источник, который указывает на конкретный компонент или модуль системы, который сгенерировал запись в журнале.
(3) Сообщение	Поле **Сообщение** описывает произошедшее событие, ошибку или предупреждение.
(4) Поиск по логам	Возможен поиск по части слова, по слову, по фразе (не чувствителен к регистру), по цифрам.
(5) Время	Поле **Время** – временная метка журнала.
(6) Меню действий	Меню дополнительных действий.
(7) Параметры просмотра журнала	Раздел настройки журнала событий.

4.11.2. Настройка ведения и просмотра журнала событий

Нажмите на кнопку **Параметры просмотра журнала**.

Рисунок 140. Настройка системного журнала

В разделе **«Установить уровень ведения журнала»** выберите один из уровней логирования (детальное журналирование может влиять на производительность, особенно в режиме *Отладка*).

Доступные уровни:

Уровень	Описание
Отладка	Очень подробные сообщения для поиска ошибок. Записывает почти каждое действие.
Информация	Действия, такие как вход пользователя в систему и работа с файлами, а также предупреждения, ошибки и критические ошибки.
Предупреждение	Успешные, но потенциально проблемные ситуации, на которые стоит обратить внимание, а также ошибки и критические ошибки.
Ошибка	Ошибки в работе приложений, но не фатальные для всей системы, а также критические ошибки.
Критическая ошибка	Только самые серьезные ошибки, приводящие к неработоспособности сервера (сервер остановлен).

В разделе **«Фильтр по уровню логирования»** выберите уровни логирования (настройка фильтра) для отображения событий в веб-интерфейсе:

- **Отладка** - показывать все сообщения (включая самые детальные).
- **Информация** - показывать информационные сообщения и выше.

- **Предупреждение** - показывать предупреждения, ошибки и критические ошибки.
- **Ошибка** - показывать только ошибки и критические ошибки.
- **Критическая ошибка** - показывать только критические ошибки.

Раздел **«Просмотр в реальном времени»** активируйте опцию:

- При активации опции **Опрос** журнал обновляется в реальном времени (автоматически).
- Если опция отключена, то события в журнале обновляются только при повторном открытии страницы.

В разделе **«Формат времени»** определите в каком виде отображать дату в журнале.

Доступные форматы:

Формат	Описание
Сырые данные	Как хранится в системе 2025-10-02T15:18:47+00:00 (ISO формат).
Местное время	Переводит в часовой пояс пользователя (UTC+3 для Москвы).
Всемирное координированное время	Время по Гринвичу (без поправки на часовой пояс).
Относительно	Время в относительном формате (2 часа назад, вчера, 3 дня назад).

4.11.3. Поиск и просмотр событий

Для поиска записи, нажмите на кнопку поиска и в открывшемся окне введите запрос.

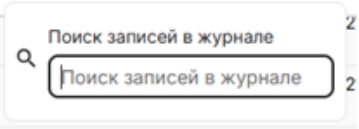


Рисунок 141. Поиск записей в журнале

ПРИМЕЧАНИЕ

- Возможен поиск по части слова, по слову, по фразе (не чувствителен к регистру), по цифрам.
- Хранит список последних поисковых запросов пользователя только во время текущей сессии. После закрытия приложения история очищается.

На основе введенного значения отобразится результат запроса.

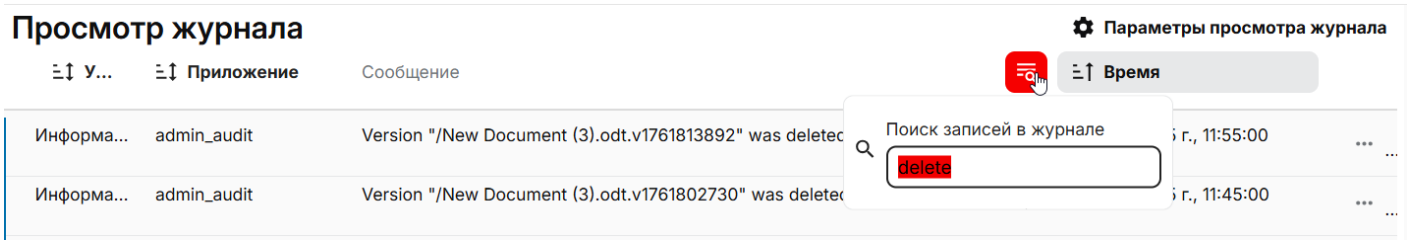


Рисунок 142. Найденные записи

Для просмотра или копирования сообщения, нажмите на кнопку **…** и выберите один из пунктов:

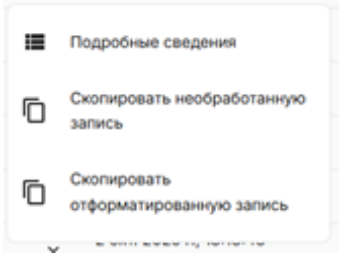


Рисунок 143. Дополнительное меню

- **Подробные сведения**. Отображает необработанную запись в журнале.

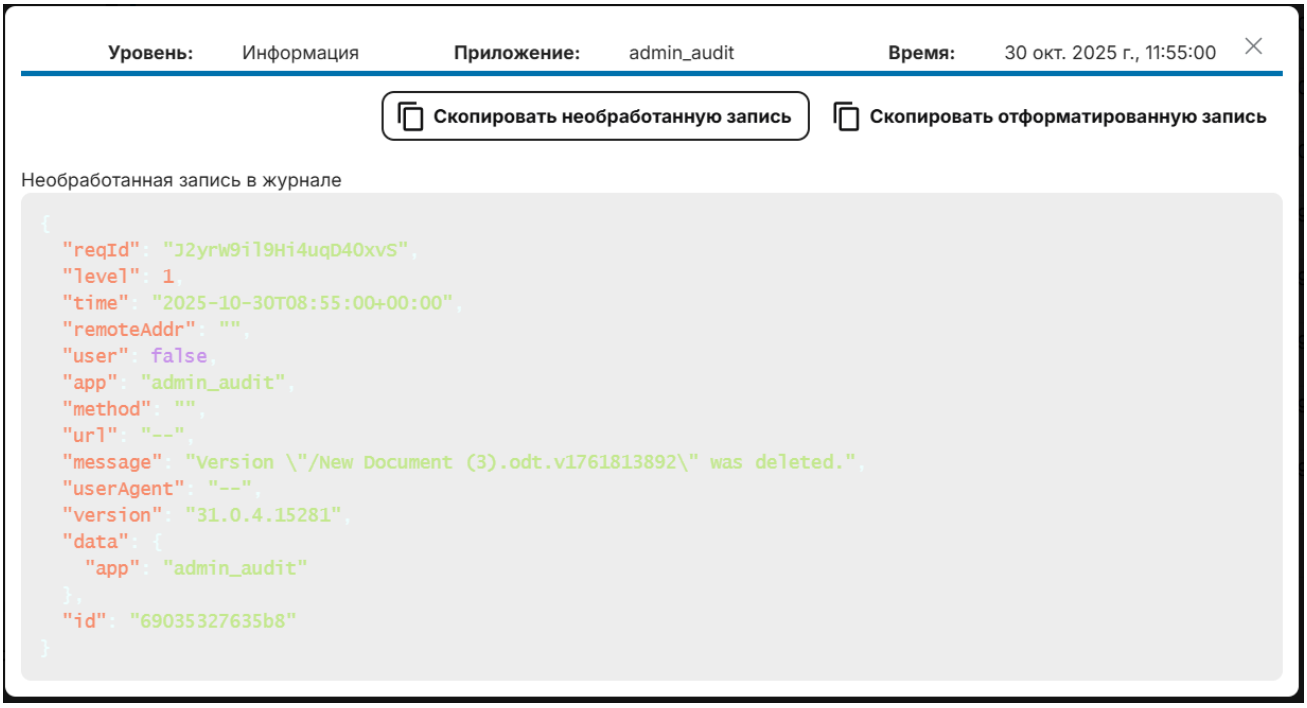


Рисунок 144. Подробные сведения

- **Скопировать необработанную запись**. Добавляет в буфер обмена JSON объект с выбранной записью.
- **Скопировать обработанную запись**. Добавляет в буфер обмена текстовую запись.

4.11.4. Скачивание журнала событий

Чтобы скачать системный журнал выполните действия:

- Нажмите на аватар пользователя и в открывшемся меню выберите пункт **Параметры сервера**.
- В левой боковой панели в разделе **Параметры сервера** выберите пункт **Системный журнал**.
- На странице **Просмотр журнала** нажмите на кнопку **Параметры просмотра журнала**.
- В открывшейся форме **Параметры просмотра журнала** нажмите на кнопку **Скачать журналы**.

4.11.5. Примеры событий

Вход пользователя в систему


```
{
  "reqId": "17xEP8jjtjtO0Z5PZ1lf",
  "level": 1,
  "time": "2025-07-25T10:48:36+00:00",
  "remoteAddr": "192.168.45.51",
  "user": "admin",
  "app": "admin_audit",
  "method": "POST",
  "url": "/login",
  "message": "Login successful: \"admin\"",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 Edg/138.0.0.0",
  "version": "31.0.4.1",
  "data": {
    "app": "admin_audit"
  },
  "id": "688cba18c96a8"
}
```


Загрузка новых файлов


```
{
  "reqId": "tE6ANcGFWZyrFvVIIOpO",
  "level": 1,
  "time": "2025-08-01T12:45:20+00:00",
  "remoteAddr": "192.168.45.51",
  "user": "admin3",
  "app": "admin_audit",
  "method": "PUT",
  "url": "/remote.php/dav/files/admin3/Documents/info.ru.fb2",
  "message": "File with id \"2157\" created:
\"/admin3/files/Documents/info.ru.fb2\"",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/134.0.0.0 YaBrowser/25.4.0.0 Safari/537.36",
  "version": "31.0.4.1",
  "data": {
    "app": "admin_audit"
  },
  "id": "688cb6eaa6f58"
}
```

Удаление файлов


```
{
  "reqId": "MlPzY9x7D9YYVFrOQCl6",
  "level": 1,
  "time": "2025-07-25T13:09:35+00:00",
  "remoteAddr": "192.168.45.51",
  "user": "admin3",
  "app": "admin_audit",
  "method": "DELETE",
  "url": "/remote.php/dav/files/admin3/Exml/Exml04.rtf",
  "message": "File with id \"542\" deleted: \"/admin3/files/Exml/Exml04.rtf\"",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/134.0.0.0 YaBrowser/25.4.0.0 Safari/537.36",
  "version": "31.0.4.1",
  "data": {
    "app": "admin_audit"
  },
  "id": "688cba18c86f2"
}
```


4.12. Шифрование данных в системе

Шифрование данных обеспечивает защиту информации как при хранении на сервере, так и во время передачи.

Передаваемые данные между клиентами и серверами должны быть защищены с использованием стандартного протокола TLS, обеспечивающий безопасную связь по протоколу HTTPS.

В зависимости от разработанной модели угроз в организации, данные в хранилище также могут быть защищены. Для этого в системе реализован модуль шифрования данных на стороне сервера. После его активации, создаваемые и загружаемые файлы автоматически шифруются перед записью в хранилище.

Шифрование файлов доступно как в **основном**, так и **внешнем подключаемом хранилище**.

Рекомендуется настраивать шифрование данных:

- **при первичной установке системы**, чтобы обеспечить защиту данных с самого начала их хранения;
- для **защиты конфиденциальных файлов** при использовании облачных или внешних хранилищ.

4.12.1. Сценарии шифрования в зависимости от функций аутентификации и типов хранилищ

В качестве **основного места хранения пользовательских данных** может выступать:

- **Локальное хранилище**: хранение файлов на дисках хоста, где развернута система.
- **Сетевое NFS хранилище**: хранение файлов на подключенном сетевом блочном хранилище.

- **S3 совместимое хранилище MinIO**: использование S3 совместимого хранилища, развернутого внутри защищенного контура организации.

В качестве **внешнего подключаемого хранилища** может выступать S3 совместимое хранилище, SMB/CIFS.

№	Аутентификация	Размещение данных	Основное хранилище	Внешнее хранилище	Шифрование	Описание
1	Логин-пароль	Основное хранилище	Локальное хранилище	-	Шифрование основного хранилища	Классическая установка на собственный сервер
2	AD/LDAP авторизация	Основное хранилище + Командные папки	Локальное хранилище/ Сетевое NFS хранилище / S3 совместимое хранилище MinIO	-	Шифрование основного хранилища	Интеграция в существующую ИТ-инфраструктуру
3	AD/LDAP авторизация, Гостевая учетная запись	Основное хранилище + Командные папки + Внешнее общее хранилище	Локальное хранилище/ S3 совместимое хранилище MinIO	-	Шифрование основного хранилища	Интеграция в существующую ИТ-инфраструктуру, возможность обмена файлами с внешними контрагентами
4	AD/LDAP авторизация, Гостевая учетная запись	Основное хранилище + Командные папки + Внешнее общее хранилище	Локальное хранилище/ S3 совместимое хранилище MinIO	S3 совместимое хранилище	Шифрование основного хранилища, шифрование удаленного хранилища	Расширение локального хранилища с помощью удаленного хранилища

4.12.2. Шифрование на стороне сервера

Шифрование выполняется по каждому отдельному файлу, с применением уникального ключа перед сохранением. Ключи файлов, в свою очередь, шифруются общим для сервера ключом.

При включении шифрования на стороне сервера, система начинает хранить **файлы в зашифрованном виде**, также на сервере хранятся все необходимые ключи. Названия файлов, а также структурных папок остаются открытыми.

- Ключи файлов и мастер-ключ никогда не покидают сервер.

4.12.2.1. Схема шифрования файлов

Когда активируется модуль шифрования в системе, выполняются следующие шаги:

1. В основном хранилище создается папка `/files_encryption`.
2. В папке `/files_encryption` создаётся папка с названием используемого модуля шифрования и набор ключей.

Пример структуры папки `/files_encryption`:

```
data/
├── files_encryption/                          # Хранилище системы шифрования
│   ├── <Используемый_модуль_шифрования>/      # Модуль шифрования по умолчанию
│   │   ├── master_<HASH>.privateKey           # Приватный (закрытый) мастер-ключ
│   │   ├── master_<HASH>.publicKey            # Публичный (открытый) мастер-ключ
│   │   ├── pubShare_<HASH>.privateKey         # Приватный ключ для общих файлов
│   │   └── pubShare_<HASH>.publicKey          # Публичный ключ для общих файлов
```

Назначение ключей:

Мастер-ключи (`master_<HASH>`) — управляют всеми файлами:

- `master_<HASH>.publicKey` — **Шифрует** индивидуальные ключи файлов.
- `master_<HASH>.privateKey` — **Расшифровывает** ключи файлов (хранится в защищенном виде).

Ключи общего доступа (`pubShare_<HASH>`) — управляют общими файлами:

- `pubShare_<HASH>.publicKey` — Шифрует ключи для файлов предоставленных в общий доступ.
- `pubShare_<HASH>.privateKey` — Расшифровывает общие ресурсы.

Когда пользователь создает/ загружает файл в хранилище, выполняются следующие шаги:

1. Для каждого создаваемого/ загружаемого файла генерируется **симметричный ключ** (AES), он шифрует содержимое файла.
2. Симметричный ключ файла **шифруется асимметричным ключом** (RSA) — публичным мастер-ключом `master_<HASH>.publicKey`.
3. Зашифрованный файл сохраняется в хранилище `/<Имя_пользователя>/files/`.

4. Зашифрованный ключ файла сохраняется в хранилище `/<Имя_пользователя>/files_encryption/`.

Пример структуры папки для пользователя `/<Имя_пользователя>`:

```
/data/<Имя_пользователя>/                          # Основное хранилище пользователя
├── files/                                         # Хранилище зашифрованных файлов
│   └─<Путь_к_файлам>/
│      ├── <Файл_1>
│      ├── <Файл_2>
│      ├── <...>
│      └── <Файл_N>
├── files_encryption/                              # Хранилище ключей пользовательских
файлов
│   └── keys/
│       └── files/
│           └─<Путь_к_файлам>/
│              ├── <Папка_файл_1>
│              │   └── <Используемый_модуль_шифрования>
│              │       └── master_<HASH>.shareKey
│              ├── <Папка_файл_2>
│              │   └── <Используемый_модуль_шифрования>
│              │       └── master_<HASH>.shareKey
│              ├── <...>
│              │   └── <Используемый_модуль_шифрования>
│              │       └── master_<HASH>.shareKey
│              └── <Папка_файл_N>
│                  └── <Используемый_модуль_шифрования>
│                      └── master_<HASH>.shareKey
```

При активации функции **Шифрование на стороне сервера** внутри пользовательского каталога данных (`/<Имя_пользователя>/`) создается системная папка `files_encryption`. Папка используется модулем шифрования для хранения **метаданных, ключей и вспомогательной информации**, необходимых для шифрования и расшифровки пользовательских файлов.

> СОВЕТ
>
> - Папку `files_encryption` **нельзя** удалять, перемещать или изменять вручную — это приведет к безвозвратной потере доступа ко всем зашифрованным файлам.

Когда пользователь открывает файл в хранилище, выполняются следующие шаги:

1. Система находит зашифрованный ключ файла.
2. Использует `master_<HASH>.privateKey` для его расшифровки.
3. Расшифровывает сам файл его личным ключом.

4.12.2.2. Настройка шифрования в системе

Перед включением шифрования необходимо определиться с тем, какие хранилища необходимо шифровать. Если в организации для защиты информации используются сторонние средства шифрования, то следует проработать сценарии резервного копирования данных.

Например, если в организации для шифрования дисков Linux используется технология LUKS, то использование дополнительного шифрования на стороне системы будет избыточным.

ПРИМЕЧАНИЕ

- При включении шифрования на стороне сервера, размер создаваемых и загружаемых файлов увеличивается.
- Также увеличивается потребление дискового пространства за счет хранения ключей и дополнительной информации.
- Если настроены квоты хранилищ для пользователей, то квоты пользователей рассчитываются на основе размера незашифрованных файлов, а не зашифрованных.
- Чтобы предотвратить безвозвратную потерю данных, необходимо регулярно создавать резервные копии всех ключей шифрования и зашифрованных данных.

1. Проверьте доступность модуля Default encryption module

Перед началом настройки, убедитесь, что модуль **Default encryption module** для шифрования активирован.

СМ. ТАКЖЕ

- Подробнее см. в разделе «Управление приложениями (модулями) системы».

После активации модуля шифрования, в системе будет отображаться сообщение:

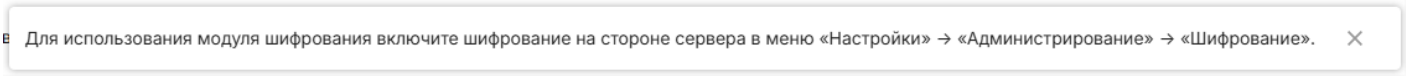


Рисунок 145. Активация модуля шифрования

2. Откройте раздел «Безопасность» и включите шифрование

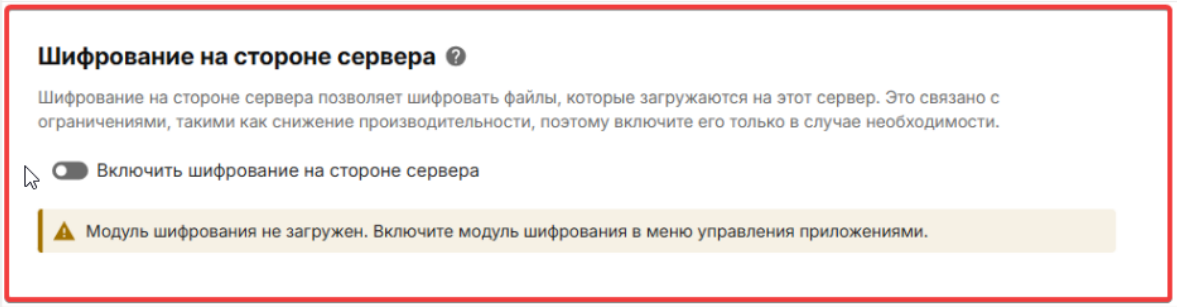
В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя и в открывшемся меню выберите пункт «**Параметры сервера**».

В разделе **«Параметры сервера»** выберите пункт **«Безопасность»**.

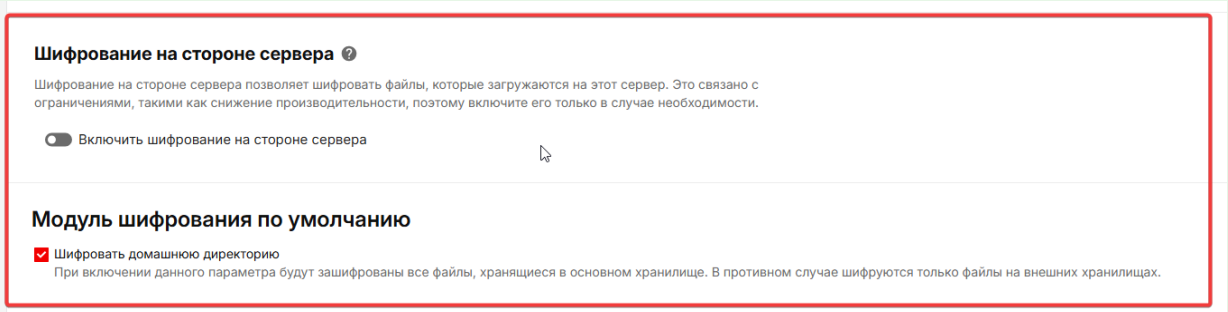
На открывшейся странице найдите раздел **Шифрование на стороне сервера**.

ПРИМЕЧАНИЕ

- Если видите сообщение, что *Модуль шифрования не загружен. Включите модуль шифрования в меню управления приложениями.*, то сначала нужно зайти в настройку приложений и активировать модуль *Default encryption module*.



- Если модуль шифрования активирован, раздел **Шифрование на стороне сервера** примет вид:



Если необходимо шифровать также домашнюю директорию пользователей, оставьте включенной опцию **Шифровать домашнюю директорию**.

Активируйте опцию **Включить шифрование на стороне сервера** для включения шифрования.

В окне **Подтвердите включение шифрования** ознакомьтесь с предупреждением.

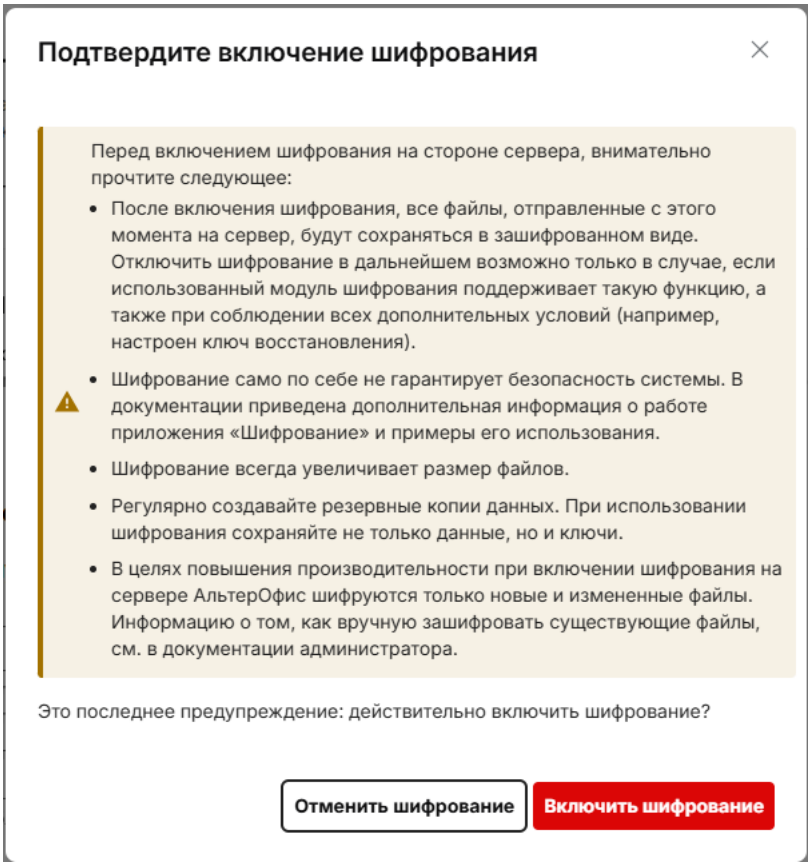


Рисунок 146. Активация шифрования на стороне сервера

Для включения шифрования, нажмите **Включить шифрование**.

Раздел **Шифрование на стороне сервера** примет вид:

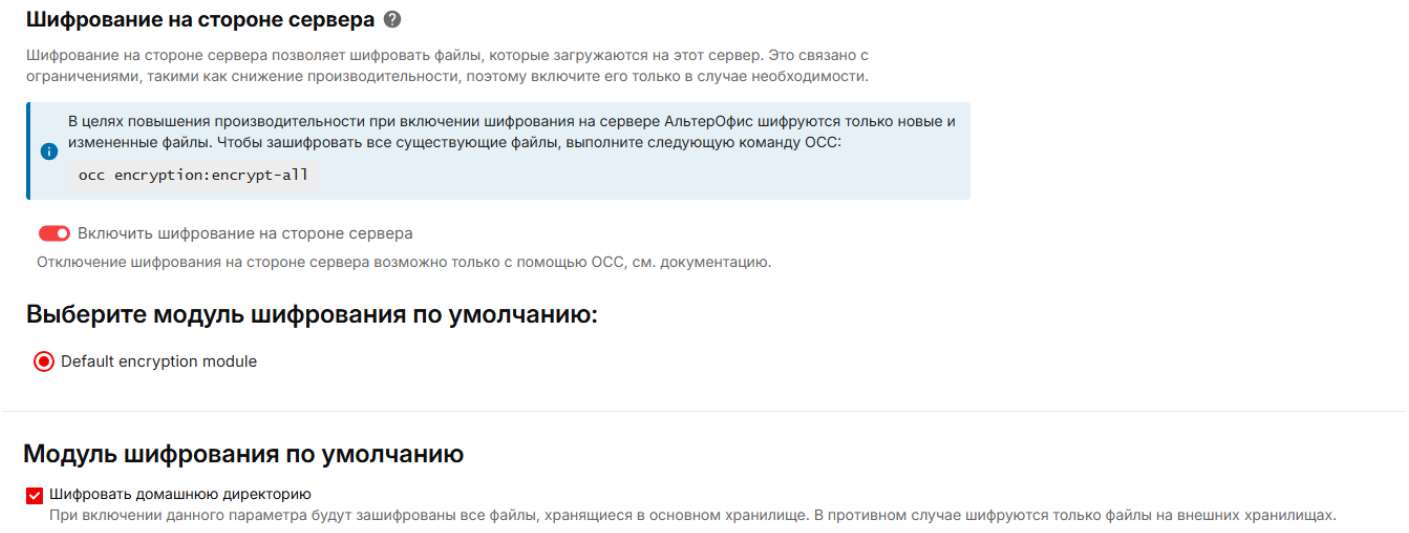


Рисунок 147. Шифрование на стороне сервера включено

С данного момента, все создаваемые и загружаемы файлы в хранилище будут шифроваться.

3. Загрузите файл в хранилище

Создайте новый документ, загрузите его на сервер хранилища **АльтерОфис Веб** с включенной опцией шифрования файлов.

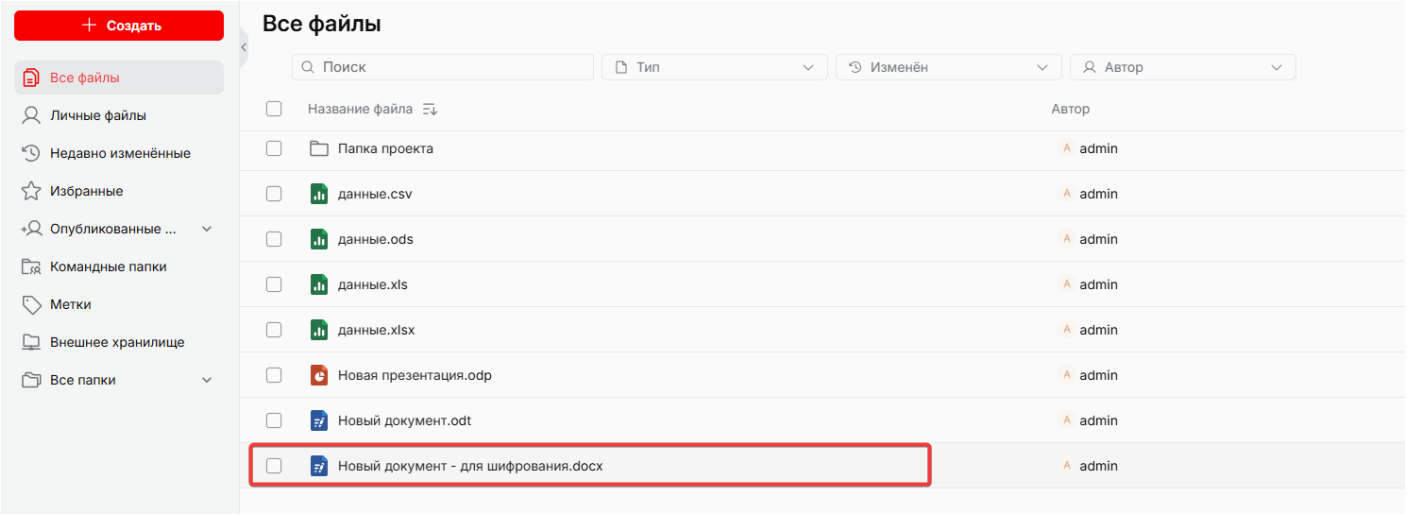


Рисунок 148. Загрузка зашифрованного файла

4. Проверьте открытие файла в онлайн редакторе

Файл должен корректно открыться.

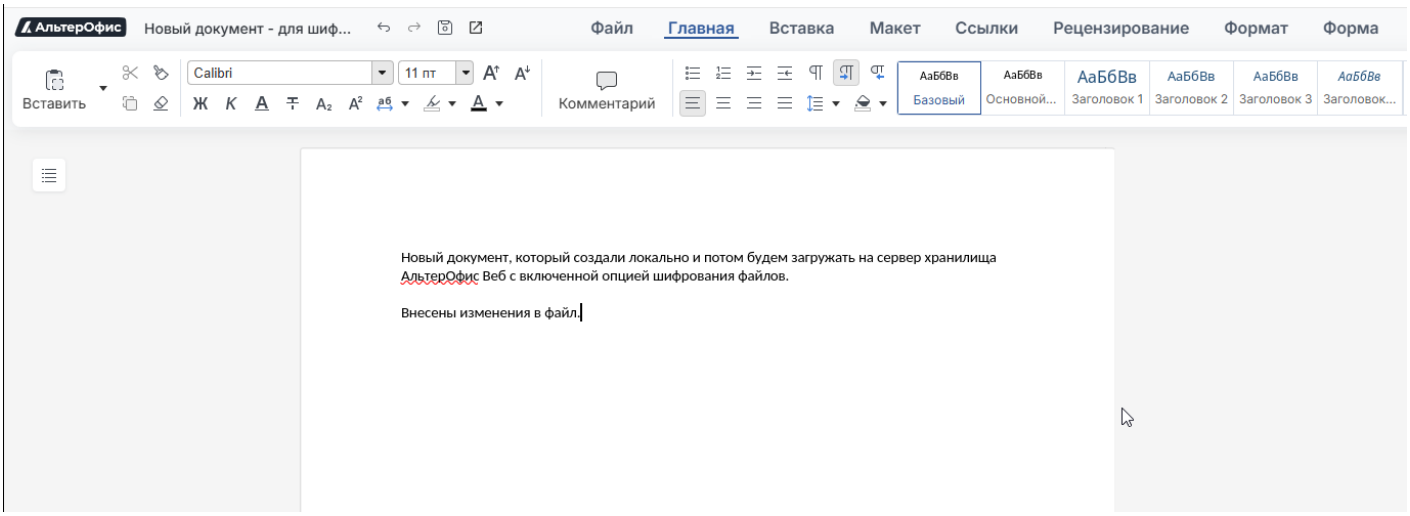


Рисунок 149. Открытие зашифрованного файла

Закройте файл.

5. Проверьте в файловом хранилище, что файл был зашифрован и ключи созданы

Любым удобным способом зайдите в хранилище файлов и откройте файл для просмотра, убедитесь что присутствует заголовок шифрования.

```
/data/<Имя_пользователя>/
├── files/
```

```
│    └─<Путь_к_файлам>/
│      ├── <Название_файла>
```

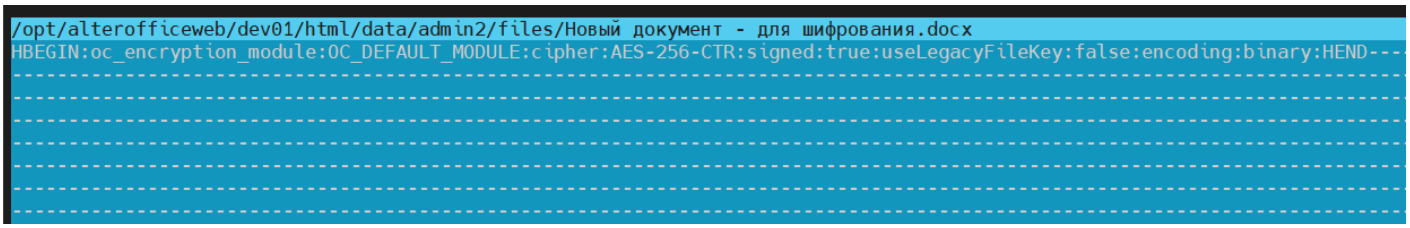


Рисунок 150. Файл зашифрован

Файл зашифрован. Закройте файл.

Убедитесь, что для файла создан ключ.

```
/data/<Имя_пользователя>/
├── files/
├── files_encryption/
│    └── keys/
│        └── files/
│            └─<Путь_к_файлам>/
│              ├── <Папка_название_файла>
│              │    └── <Используемый_модуль_шифрования>
│              │        └── master_<HASH>.shareKey
```

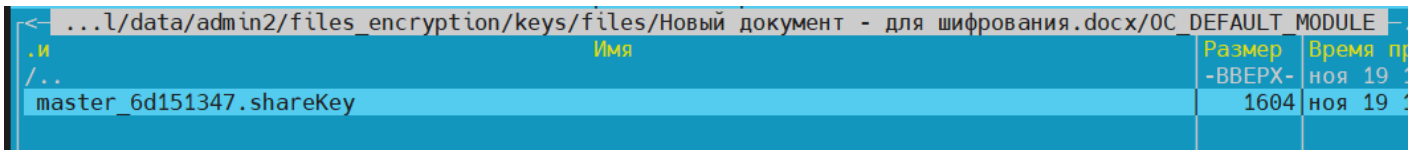


Рисунок 151. Ключ шифрования файла

Ключ шифрования создан и размещен в хранилище ключей.

6. Скачайте зашифрованный файл из хранилища на локальное устройство

При скачивании зашифрованного файла из хранилища АльтерОфис Веб на локальное устройство, файл скачивается в расшифрованном виде.

Скачайте и проверьте, что файл корректно открывается.

4.12.3. Сценарии по работе с шифрованием

Не все операции с **шифрованием на стороне сервера** можно выполнить через веб-интерфейс. Для выполнения некоторых требуется доступ к CLI.

- Ниже приведенные сценарии будут рассматриваться исходя из того, что у вас есть необходимые привилегии к контейнеру **app** (основное приложение).
- Будут рассмотрены команды из пространства `encryption` для **управления шифрованием на стороне сервера**, включая активацию, отключение, диагностику состояния системы шифрования. Для запуска команды будет использоваться OCC (OwnCloud Console) - интерфейс командной строки для управления АльтерОфис Веб.

4.12.3.1. Первоначальная настройка шифрования

1. Проверить статус

```
php /var/www/html/occ encryption:status
```

Команда показывает текущий статус: включено ли шифрование, какой модуль используется.

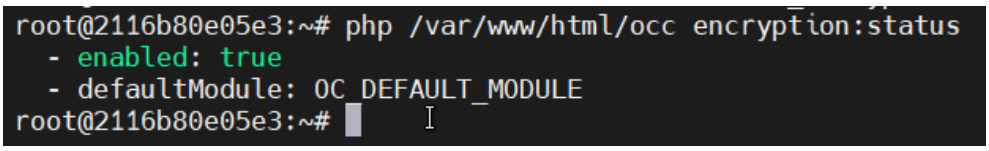


Рисунок 152. Настройка шифрования - статус

2. Проверить какие модули шифрования доступны

```
php /var/www/html/occ encryption:list-modules
```

Команда выводит список доступных модулей шифрования (например, `OC_DEFAULT_MODULE`).

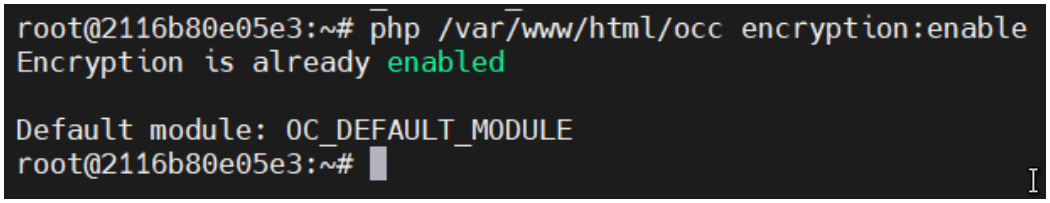


Рисунок 153. Настройка шифрования - активация

3. Включить шифрование

```
php /var/www/html/occ encryption:enable
```

Команда включает шифрование (Server-Side Encryption, SSE). После запуска создаются ключи пользователей и активируется модуль шифрования.

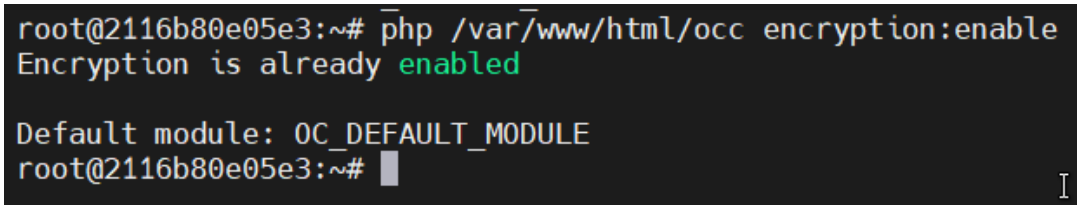


Рисунок 154. Настройка шифрования - активация

Данное действие можно выполнить также через веб-интерфейс.

4. Зашифровать существующие файлы

ПРИМЕЧАНИЕ

- Команды `encrypt-all` и `decrypt-all` могут долго выполняться. Их требуется выполнять в `maintenance mode`.
- Перед выполнением операций необходимо выполнять резервное копирование данных и настроек.

Переведите систему в режим обслуживания:

```
php /var/www/html/occ maintenance:mode --on
```

Выполните шифрование данных:

```
php /var/www/html/occ encryption:encrypt-all
```

Команда запускает процесс шифрования **всех существующих файлов** всех пользователей.

При запуске команды, будет задан вопрос, уверены ли вы в том, что нужно зашифровать данные. В случае утвердительного ответа, данные начнут шифроваться.

Так как команда включения `encryption:enable` не шифрует ранее загруженные в хранилище данные, то с использованием команды `encryption:encrypt-all` вы можете зашифровать данные перед началом использования системы с новыми настройками.

После завершения шифрования, выведите систему из режима обслуживания:

```
php /var/www/html/occ maintenance:mode --off
```

4.12.3.2. Отключение шифрования

1. Отключить шифрование (файлы остаются зашифрованными)

```
php /var/www/html/occ encryption:disable
```

Команда отключает шифрование на стороне сервера. После выполнения требуется расшифровать все данные с помощью команды `encryption:decrypt-all`.

2. Расшифровать все файлы

Переведите систему в режим обслуживания:

```
php /var/www/html/occ maintenance:mode --on
```

Выполните команду расшифровки файлов:

```
php /var/www/html/occ encryption:decrypt-all
```

По окончанию операции, выведите систему из режима обслуживания:

```
 php /var/www/html/occ maintenance:mode --off
```

3. Проверить, что шифрование отключено

```
php /var/www/html/occ encryption:status
```

Отобразится текущий статус.

- Никогда не удаляйте ключи шифрования.
- Перед любыми изменениями настроек системы выполняйте резервное копирование папки `files/` (локальное хранилище данных) и `files_encryption/` (хранилище ключей).

4.13. Интеграция с различными поставщиками удостоверений

4.13.1. Интеграция с Active Directory Federation Services (AD FS)

Если в организации используется доменная инфраструктура на базе Active Directory, возможна настройка доменной аутентификации пользователей АльтерОфис Веб с применением механизма единого входа (SSO). Для реализации данной интеграции необходимо выполнить конфигурацию как на стороне Active Directory Federation Services (AD FS), так и на стороне АльтерОфис Веб.

Внедрение SSO обеспечивает упрощённый доступ — пользователи проходят аутентификацию один раз и получают доступ к АльтерОфис Веб без повторного ввода пароля.

Интеграция реализуется на основе протокола SAML 2.0 и требует предварительной настройки доверительных отношений между АльтерОфис Веб (поставщик услуг, Service Provider) и AD FS (поставщик удостоверений, Identity Provider).

4.13.1.1. Установка роли службы федерации Active Directory

Зайдите на сервер на котором нужно настроить службы федерации Active Directory. Это может быть сервер, где установлен AD DS (**Active Directory Domain Service**) или другой сервер, который присоединен к домену Active Directory.

- Настройка AD FS описана на примере ОС Windows Server 2022 Datacenter, для других версий шаги могут отличаться.
- Перед установкой рекомендуется ознакомиться с официальной документацией производителя.

Проверьте, установлена ли роль службы федерации Active Directory. Для этого запустите PowerShell от имени администратора и выполните команду:

```
Get-WindowsFeature ADFS-Federation
```

Если роль не установлена, вернется сообщение:

```
Display Name                                            Name                       Install State
------------                                            ----                       -------------
[ ] Службы федерации Active Directory                   ADFS-Federation                Available
```

Или, если установлена:

```
Display Name                                            Name                       Install State
------------                                            ----                       -------------
[X] Службы федерации Active Directory                    ADFS-Federation                Installed
```

Для установки и последующей настройки вам понадобится действующий SSL-сертификат для использования в AD FS.

Роль AD FS в Windows Server может быть установлена с помощью **Диспетчера серверов** или с помощью PowerShell.

Установите службы федерации любым удобным способом.

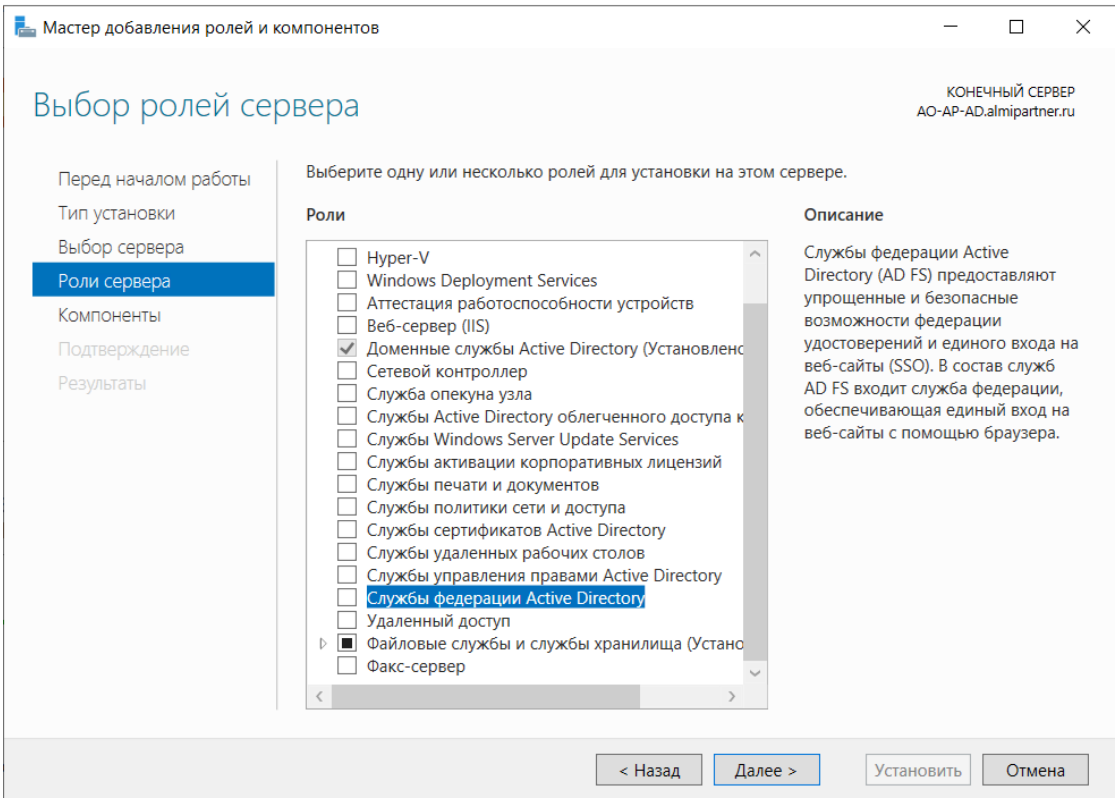


Рисунок 155. Добавление роли сервера.

После завершения установки роли AD FS, можно сразу приступить к настройке роли.

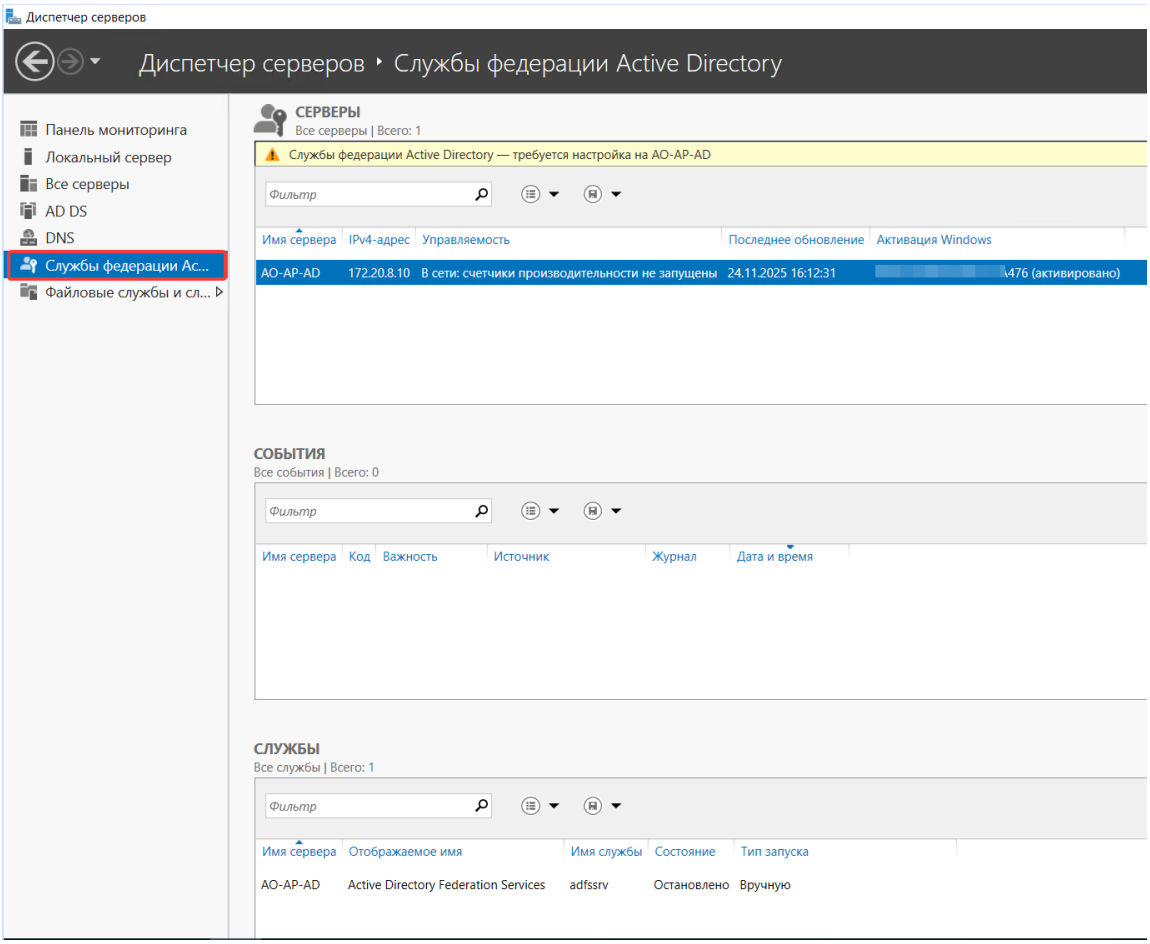


Рисунок 156. Службы федерации Active Directory установлены, требуется настройка.

4.13.1.2. Подготовка службы федерации Active Directory

Процесс настройки включает создание фермы серверов и настройку базы данных конфигурации.

Откройте **Диспетчер серверов**. Запустите мастер настройки службы, нажмите «Настроить службу федерации на этом сервере».

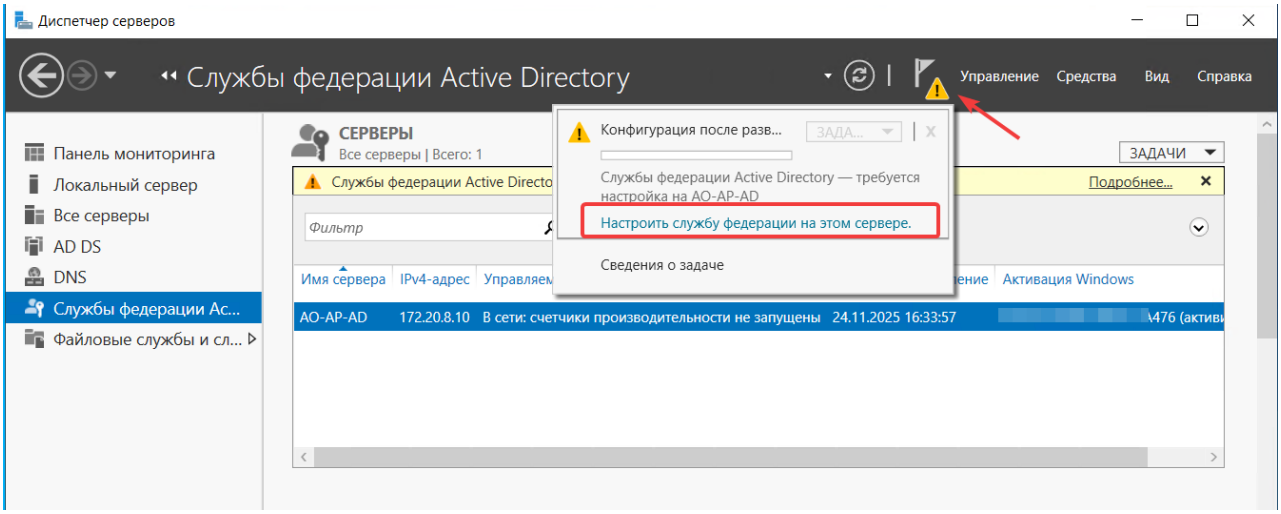


Рисунок 157. Запуск мастера настройки служб федерации.

В мастере настройки выберите «Создать первый сервер федерации в новой ферме». Нажмите «Далее».

На шаге «Подключение к AD DS» укажите учетную запись с правами администратора домена. Нажмите «Далее».

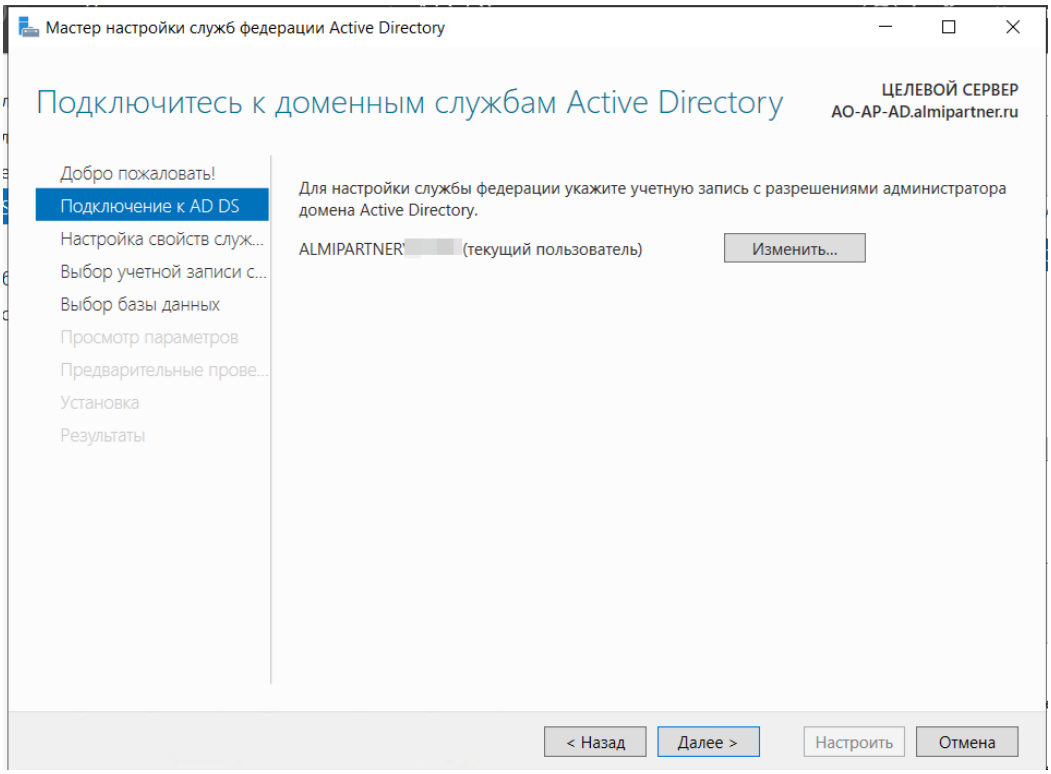


Рисунок 158. Подключение к доменным службам Active Directory.

На шаге «Настройка свойств службы» потребуется SSL-сертификат для вашего сервера AD FS.

Выберите подготовленный SSL-сертификат из списка доступных. Убедитесь, что сертификат соответствует полному доменному имени (FQDN) вашего сервера AD FS.

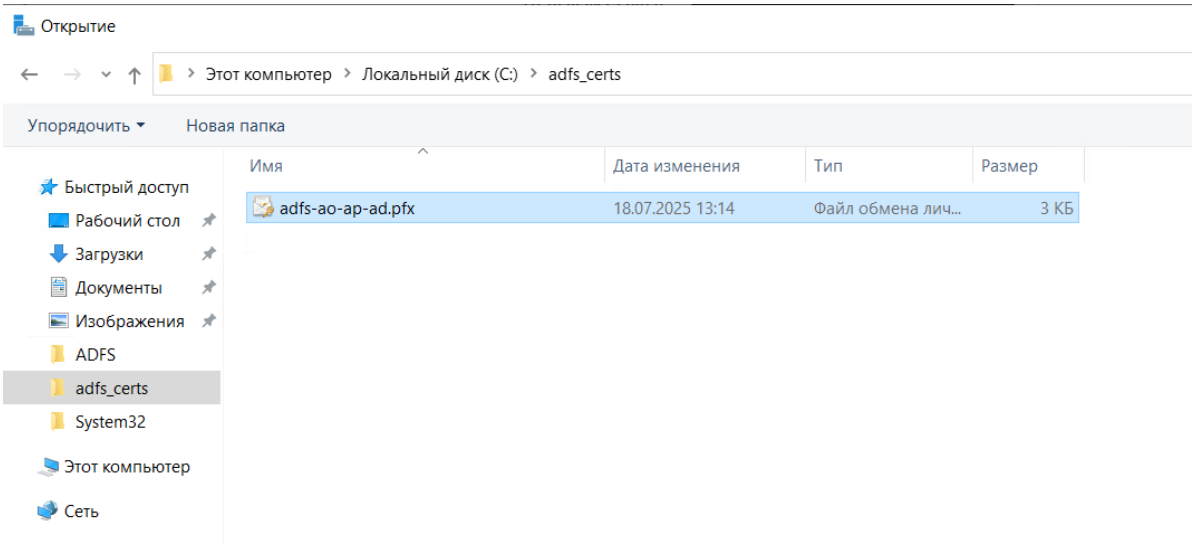


Рисунок 159. Импорт SSL-сертификата.

Выберите из раскрывающегося списка имя службы федерации.

В поле «Отображаемое имя службы» введите произвольное название.

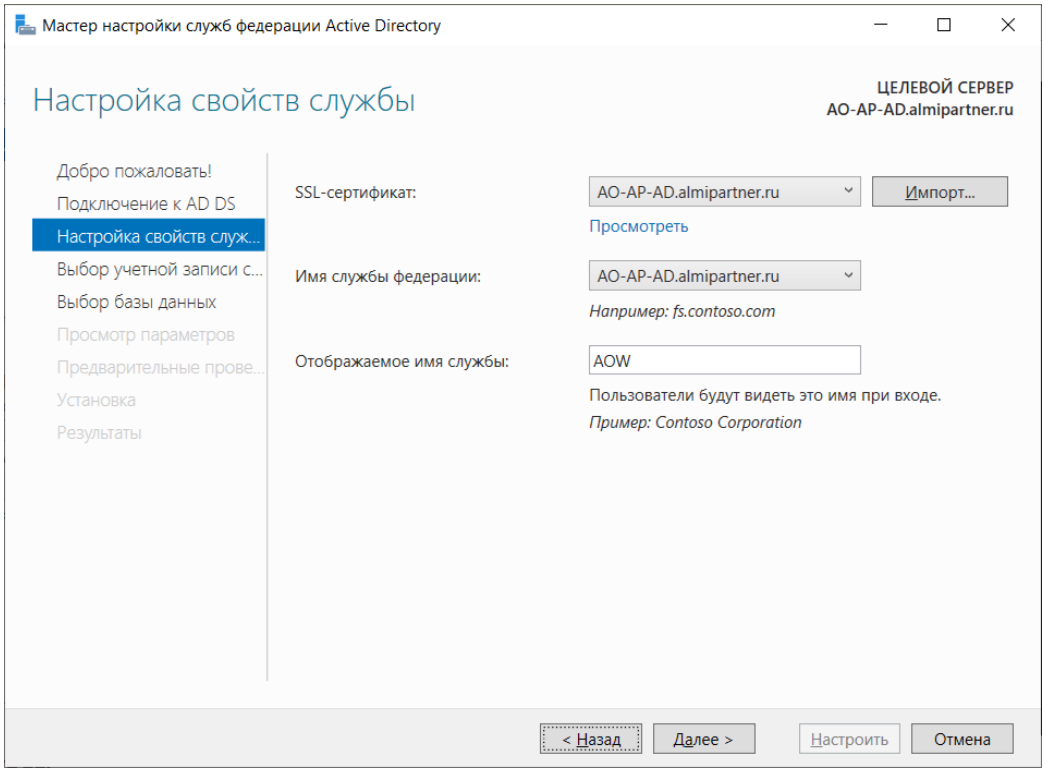


Рисунок 160. Настройка свойств службы.

Нажмите «Далее».

Укажите учётную запись для запуска службы. Нажмите «Далее».

На шаге настройки базы данных конфигурации, выберите тип базы данных:

- **Внутренняя база данных Windows** подходит для небольших организаций.
- **SQL Server** рекомендуется для крупных организаций с высокой нагрузкой.

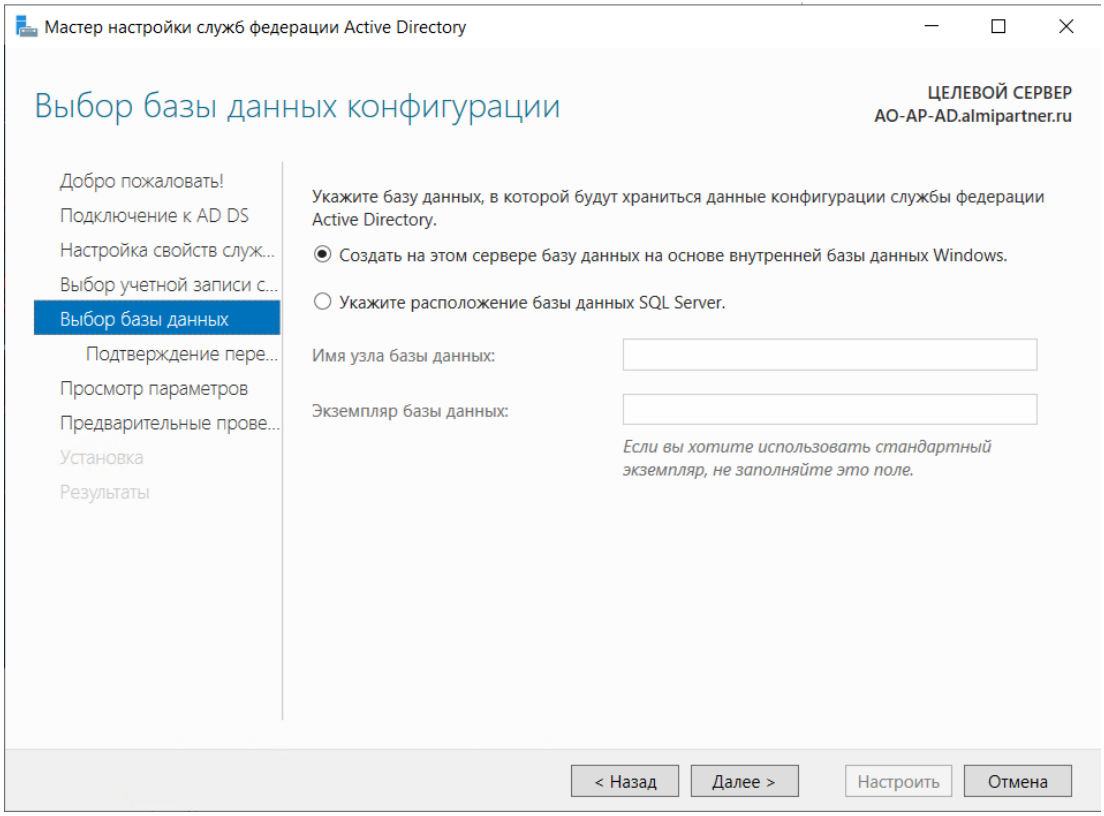


Рисунок 161. Настройка базы данных конфигурации.

Нажмите «Далее».

Перейдите к просмотру параметров и убедитесь, что проверки будут выполнены без ошибок. Нажмите «Настроить».

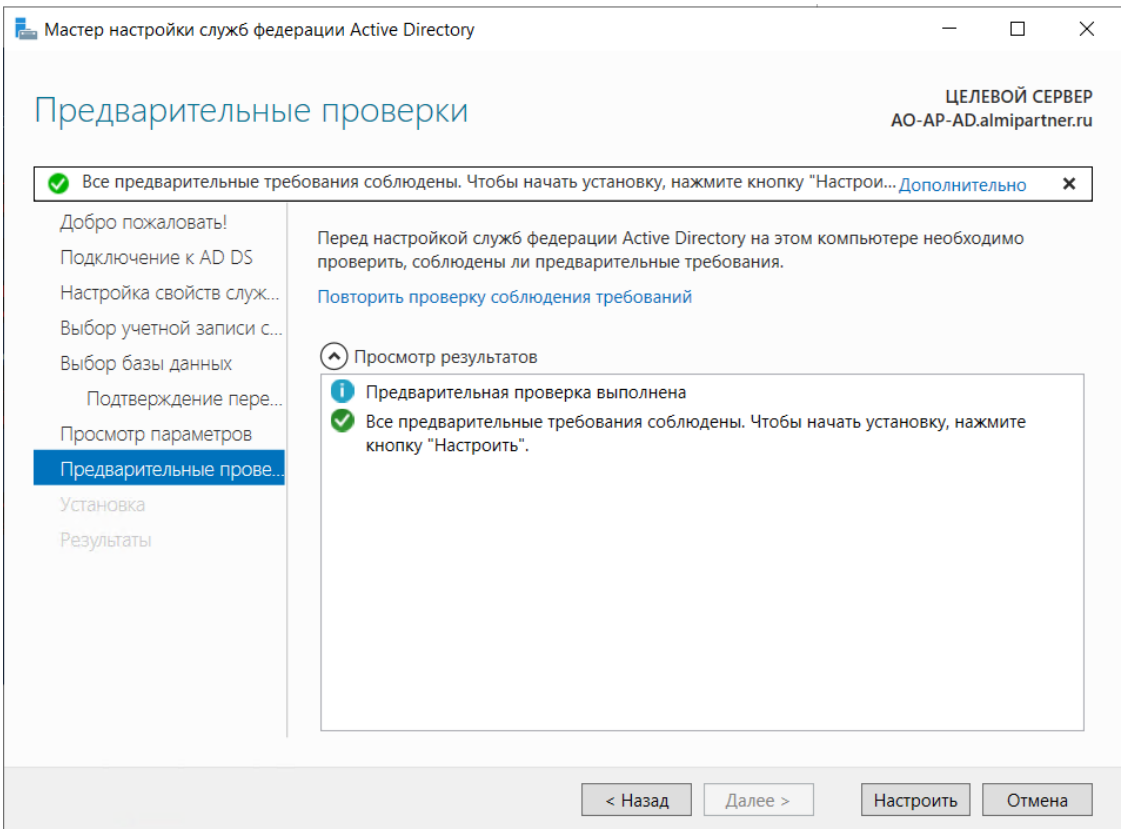


Рисунок 162. Результаты настройки.

Дождитесь, пока шаг установки будет завершён.

Перезагрузите сервер, если это потребуется.

4.13.1.3. Конфигурация службы федерации Active Directory

Теперь вы должны увидеть консоль настройки AD FS в меню «Пуск». Запустите её.

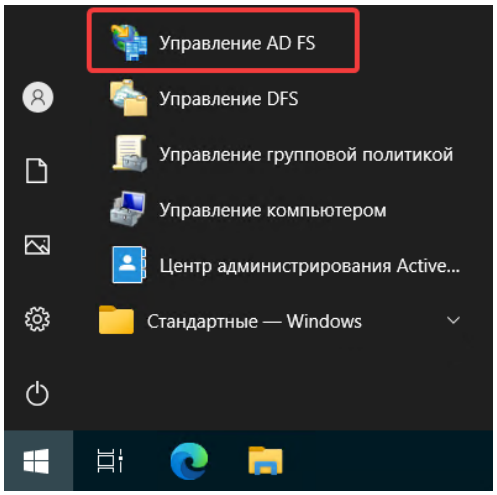


Рисунок 163. Оснастка «Управление AD FS».

1. Настройте методы проверки подлинности

Перейдите в раздел «Служба», подраздел «Методы проверки подлинности» и нажмите «Изменить».

Отключите все методы, кроме аутентификации по форме. Нажмите «ОК».

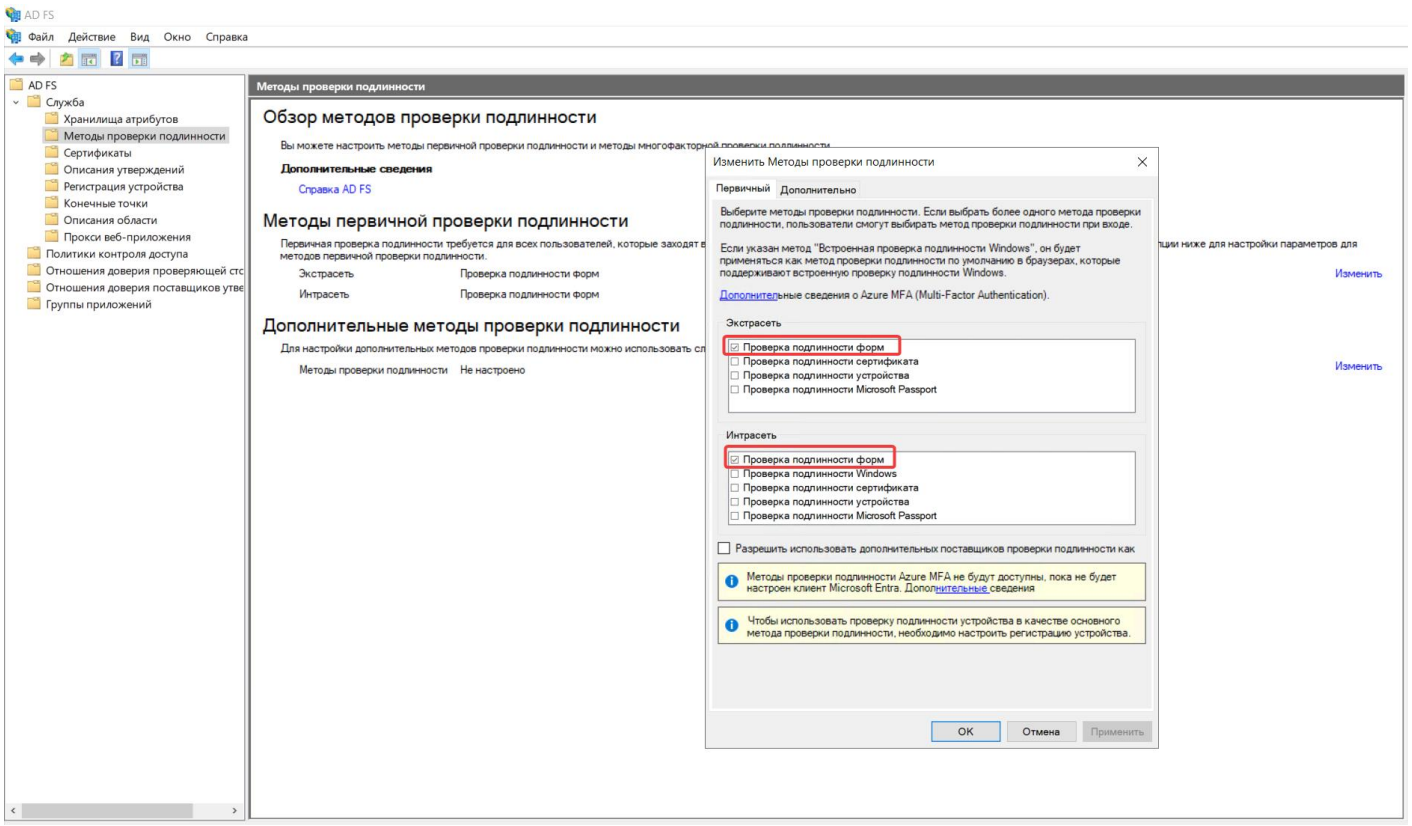


Рисунок 164. Методы проверки подлинности AD FS.

2. Получите конечную точку службы федераций

Перейдите в подраздел «Конечные точки» и убедитесь, что включена конечная точка типа «SAML 2.0/WS-Federation».

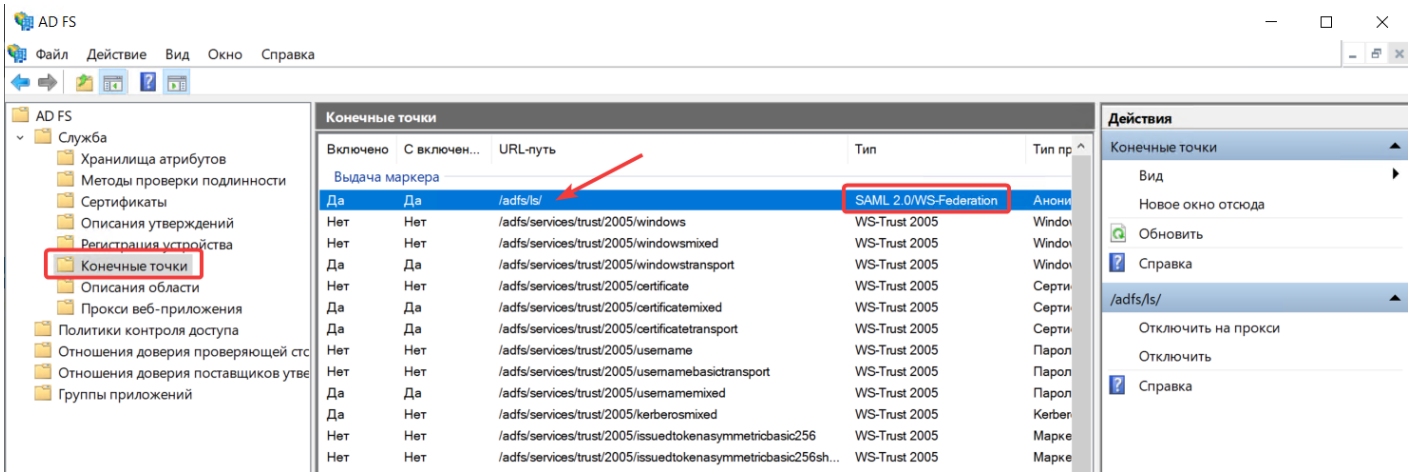


Рисунок 165. Конечная точка.

ПРИМЕЧАНИЕ

Чтобы пользователи могли входить в АльтерОфис Веб используя учетные данные Active Directory, необходимо настроить доверие между AD FS (поставщик удостоверений) и АльтерОфис Веб (проверяющая сторона).

Для настройки потребуется идентификатор АльтерОфис Веб и конечная точка (адрес для приема SAML-ответов), которые имеют вид:

- **Идентификатор:** `https://<FQDN>/apps/user_saml/saml/metadata`
- **Конечная точка:** `https://<FQDN>/apps/user_saml/saml/acs`

Где `<FQDN>` - полное доменное имя, например `test-web2025.alteroffice.ru`.

3. Настройте отношения доверия

Добавьте доверенную сторону с помощью PowerShell. Запустите PowerShell от имени администратора и выполните команды:

```
Add-AdfsRelyingPartyTrust -Name aow -Identifier "https://test-web2025.alteroffice.ru/apps/user_saml/saml/metadata" -ProtocolProfile SAML
Set-AdfsRelyingPartyTrust -Targetname aow -EncryptionCertificateRevocationCheck none -SigningCertificateRevocationCheck none
```

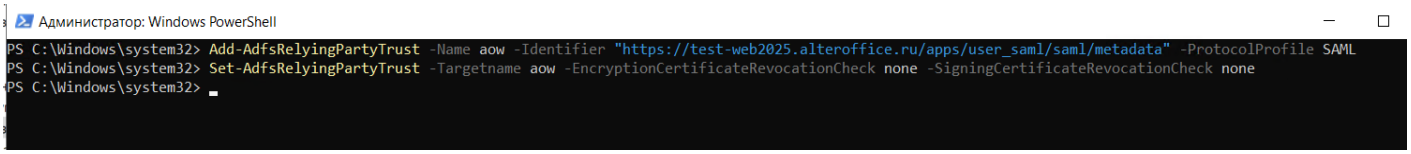


Рисунок 166. Добавление доверенной стороны с помощью PowerShell.

Перейдите в раздел «Отношения доверия проверяющей стороны», выберите созданную запись и откройте её на редактирование, дважды щёлкнув по ней.

На вкладке «Идентификаторы» просмотрите отображаемое имя и идентификатор, которые были добавлены с помощью PowerShell.

Перейдите на вкладку «Конечные точки» и нажмите кнопку **Добавить SAML…**.

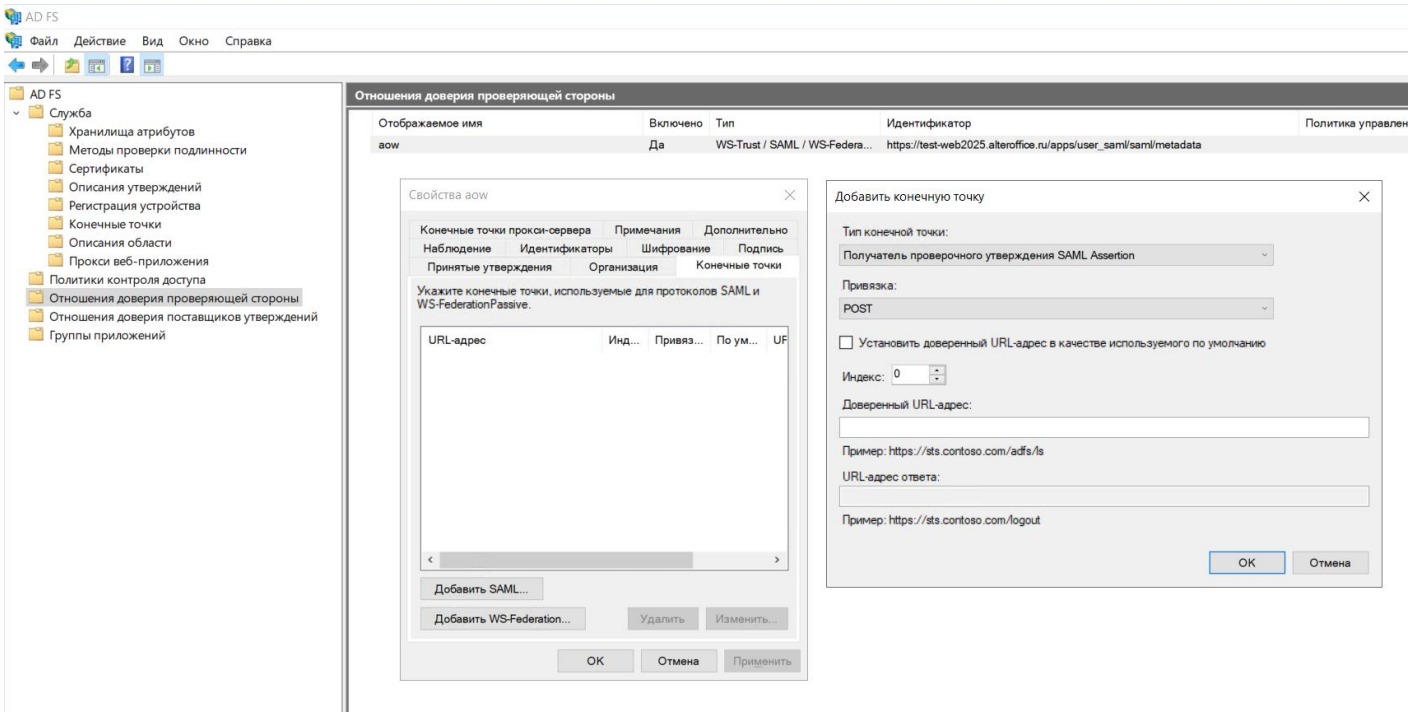


Рисунок 167. Отношения доверия проверяющей стороны.

В открывшейся форме «Добавить конечную точку» заполните поля:

Поле	**Пример**
Тип конечной точки	Получатель проверочного утверждения SAML Assertion
Привязка	POST
Установить доверенный URL-адрес в качестве используемого по умолчанию	Да
Доверенный URL-адрес	`https://test-web2025.alteroffice.ru/apps/user_saml/saml/acs`

Нажмите «ОК» и вернитесь в раздел «Отношения доверия проверяющей стороны».

4. Измените политику управления доступом

Выберите отредактированную запись и нажмите правую кнопку мыши, выберите пункт «Изменить политику подачи запросов…».

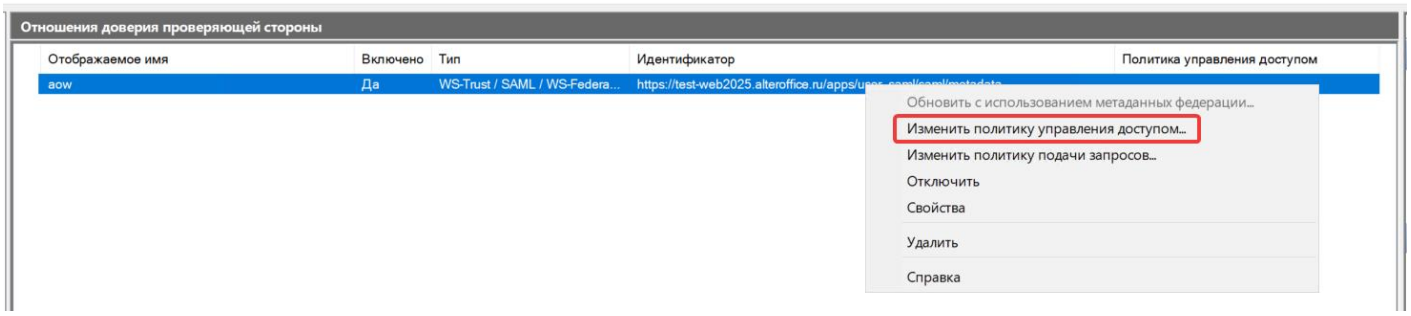


Рисунок 168. Изменение политики управления доступом.

Выберите политику управления доступом **Разрешение для каждого**, нажмите «Применить» и «ОК».

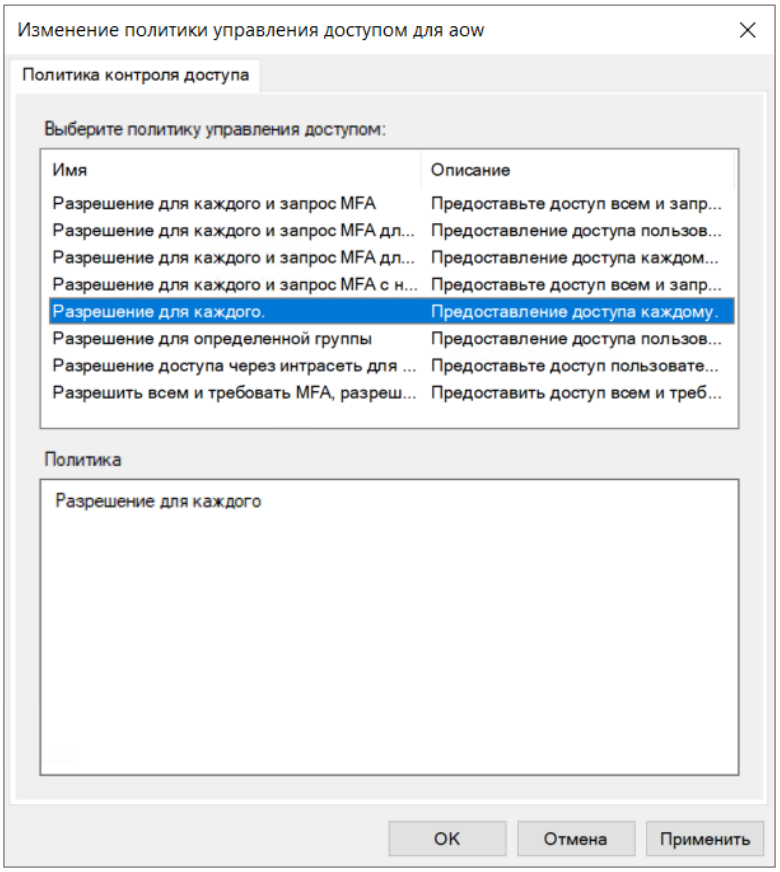


Рисунок 169. Изменение политики управления доступом.

Вернитесь в раздел «Отношения доверия проверяющей стороны».

5. Измените политику управления подачи запросов

Выберите отредактированную запись и нажмите правую кнопку мыши, выберите пункт «Изменить политику подачи запросов…».

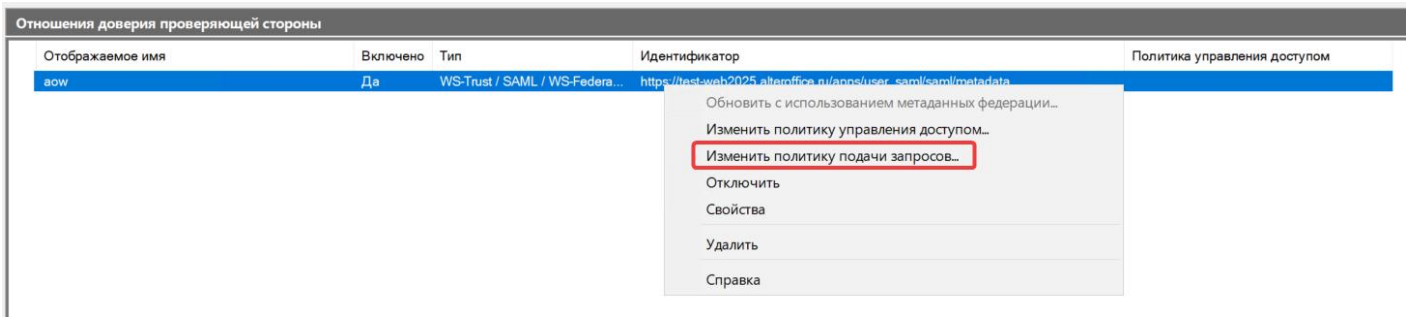


Рисунок 170. Изменение политики подачи запросов.

Здесь необходимо определить правила, как атрибуты пользователя передаются от поставщика удостоверений (IdP) к сервис-провайдеру (SP) во время аутентификации. Это важно для реализации технологии единого входа (SSO).

Для интеграции будут использоваться атрибуты:

- Уникальный идентификатор пользователя в домене.
- Отображаемое имя пользователя.
- Адрес электронной почты.
- Группа пользователей в домене.

В окне «Правила преобразования выдачи» нажмите кнопку **Добавить правило…**.

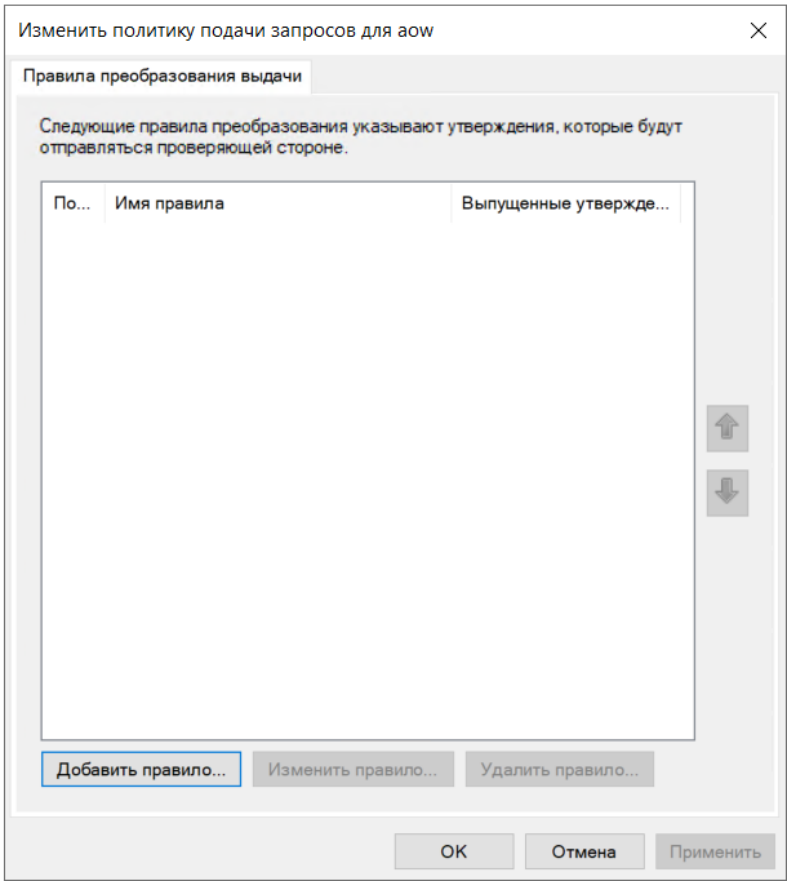


Рисунок 171. Правила преобразования выдачи.

Откроется мастер добавления правил.

На шаге «Выберите тип правила» в поле «Шаблон правила утверждения» выберите значение **Отправка атрибутов LDAP как утверждений**.

Нажмите «Далее».

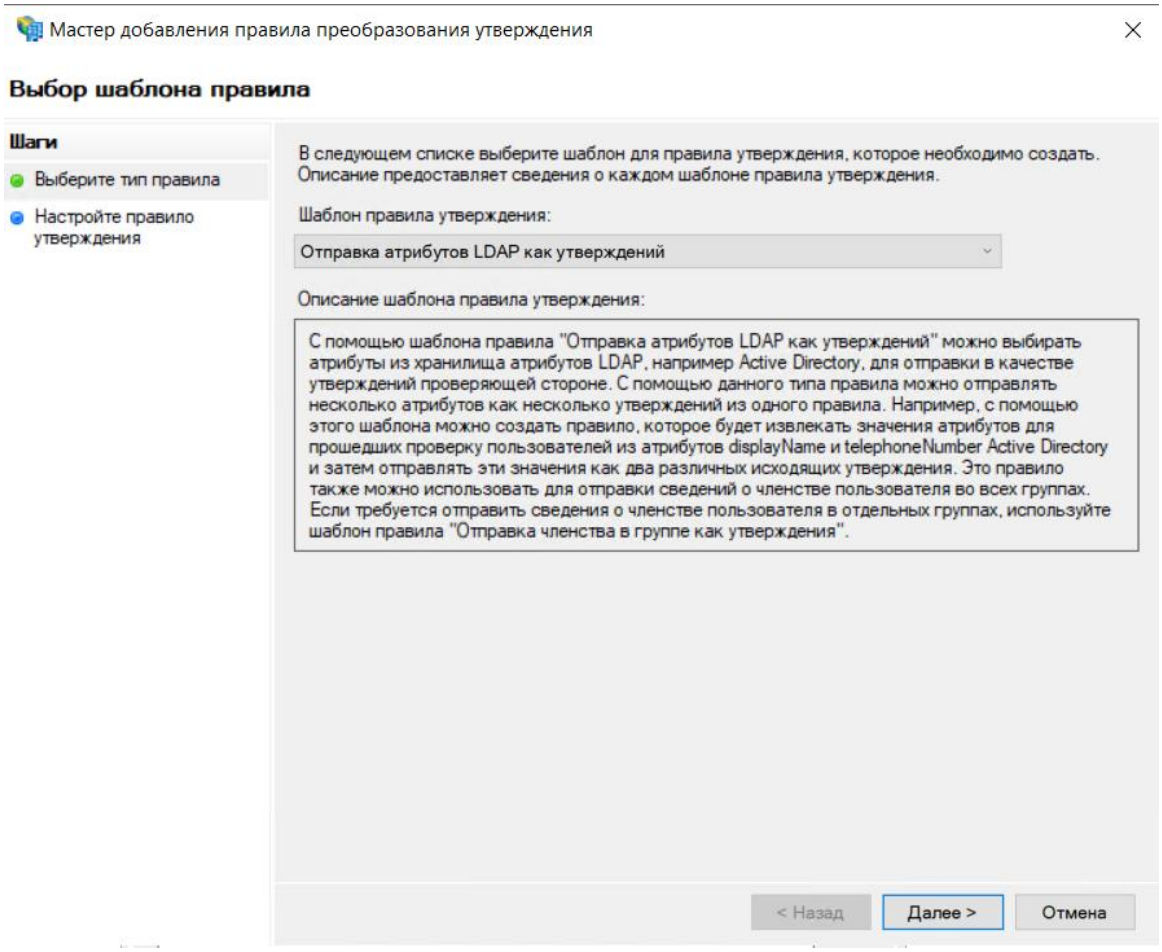


Рисунок 172. Выбор шаблона правила.

На шаге «Имя правила утверждения» заполните поля:

Поле	Описание	Пример
Имя правила утверждения	Введите произвольное имя.	AD mapping
Хранилище атрибутов	Выберите значение `Active Directory`	`Active Directory`

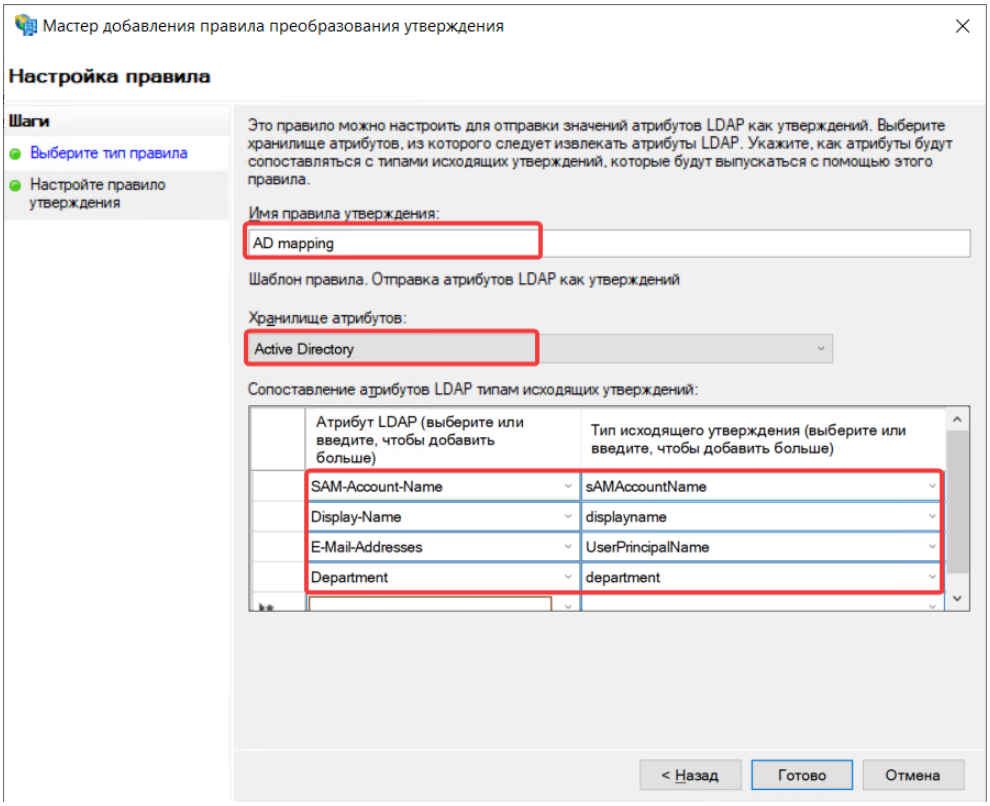


Рисунок 173. Правила утверждения.

Сопоставьте атрибуты LDAP с типами исходящих утверждений.

Пример:

Атрибут LDAP	**Тип исходящего утверждения**	**Описание**
SAM-Account-Name	sAMAccountName	Идентификатор пользователя
Display-Name	displayname	Отображаемое имя
E-Mail-Addresses	UserPrincipalName	Адрес электронной почты
Department	department	Группа

После применения этих правил АльтерОфис Веб будет получать в SAML-ответе:

- Уникальный идентификатор пользователя.
- Отображаемое имя для профиля пользователя.
- Электронный адрес для уведомлений.
- Информацию о группе.

На основе настроенных сопоставлений, учетные записи пользователей будут автоматически создаваться и обновляться в АльтерОфис Веб.

6. Получите открытый ключ

Перейдите в раздел «Служба», подраздел «Сертификаты» и выберите пункт «Для подписи маркера».

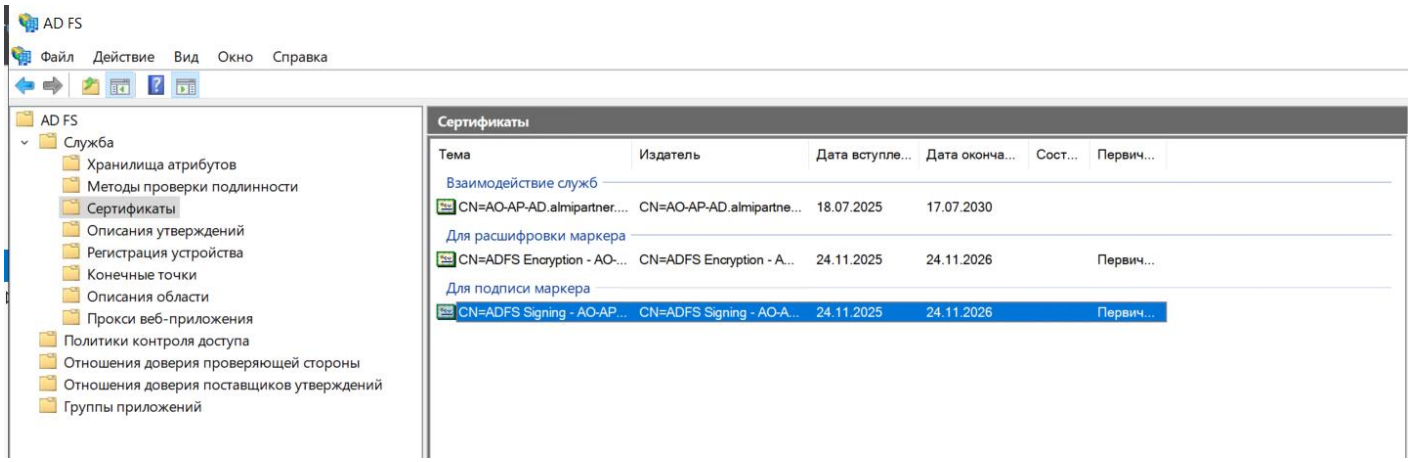


Рисунок 174. Сертификаты.

Откройте сертификат на просмотр, перейдите на вкладку «Состав».

Прокрутите список полей и найдите «Открытый ключ».

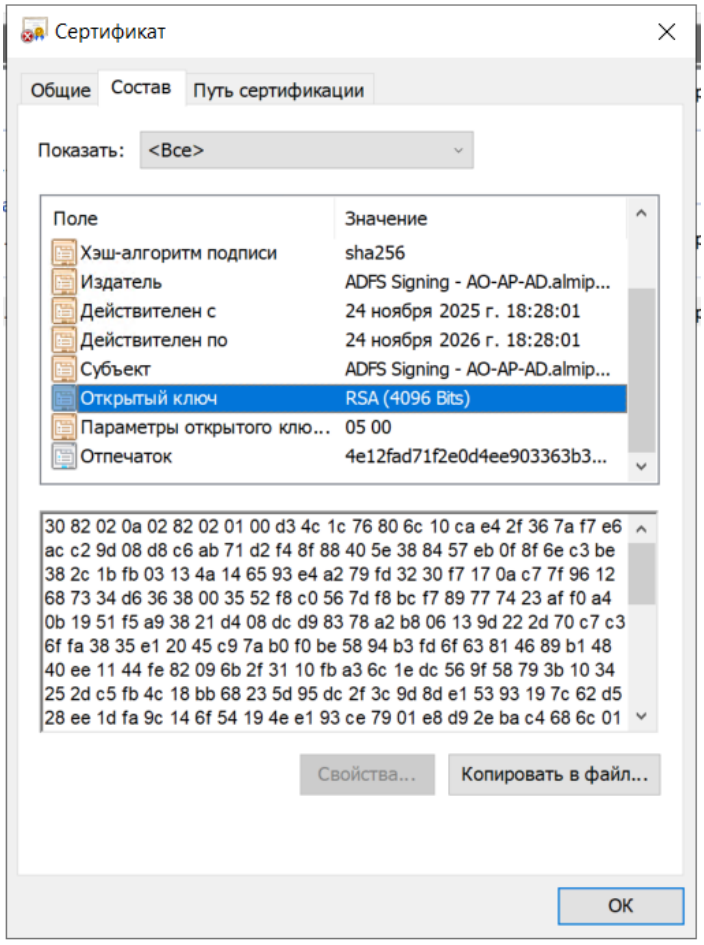


Рисунок 175. Открытый ключ.

Нажмите кнопку **Копировать в файл**, выберите формат файла для экспорта сертификата «Файлы X.509 (.CER) в кодировке Base-64».

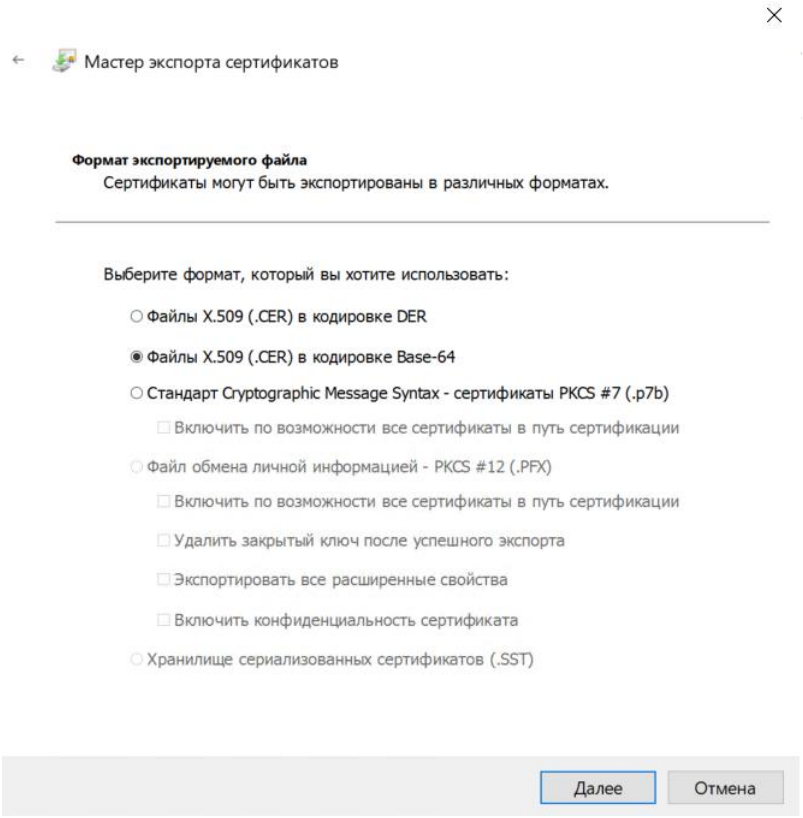


Рисунок 176. Формат экспорта сертификатов.

Нажмите «Далее».

Сохраните открытый ключ в файле (он потребуется при дальнейшей настройке).

4.13.1.4. Настройка SAML аутентификации в АльтерОфис Веб

1. Проверьте доступность модуля интеграции

Перед началом настройки, убедитесь, что активирован модуль **SSO & SAML authentication**.

> СМ. ТАКЖЕ
>
> - Подробнее см. в разделе «Управление приложениями (модулями) системы».

2. Откройте раздел «Аутентификация SSO и SAML»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя и в открывшемся меню выберите пункт **«Параметры сервера»**.

В разделе **«Параметры сервера»** выберите пункт **«Аутентификация SSO и SAML»**.

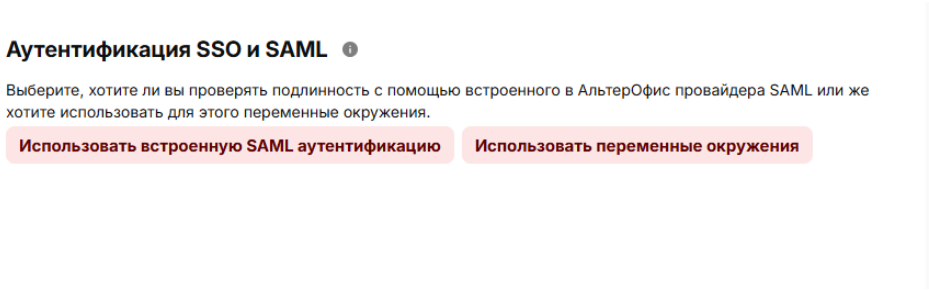


Рисунок 177. Настройка аутентификации SSO и SAML

3. Настройте встроенную SAML аутентификацию

На странице **Аутентификация SSO и SAML** нажмите кнопку **Использовать встроенную SAML аутентификацию**.

В разделе «Общие настройки» активируйте опцию **Разрешить использование нескольких пользовательских back-end (например, LDAP)**.

Включение данной опции позволит использовать параллельно другие методы аутентификации, такие как LDAP, локальные пользователи АльтерОфис Веб.

Нажмите кнопку **Добавить поставщика удостоверений**.

В разделе «Основные» укажите следующие параметры:

Поле	Описание	Пример
Атрибут для привязки UID	Атрибут, используемый в качестве внутреннего имени пользователя для АльтерОфис Веб	`sAMAccountName`
Дополнительное отображаемое имя поставщика удостоверений	Наименование провайдера, отображаемое на странице входа в АльтерОфис Веб (допускается ввести произвольное значение).	`Единый вход`

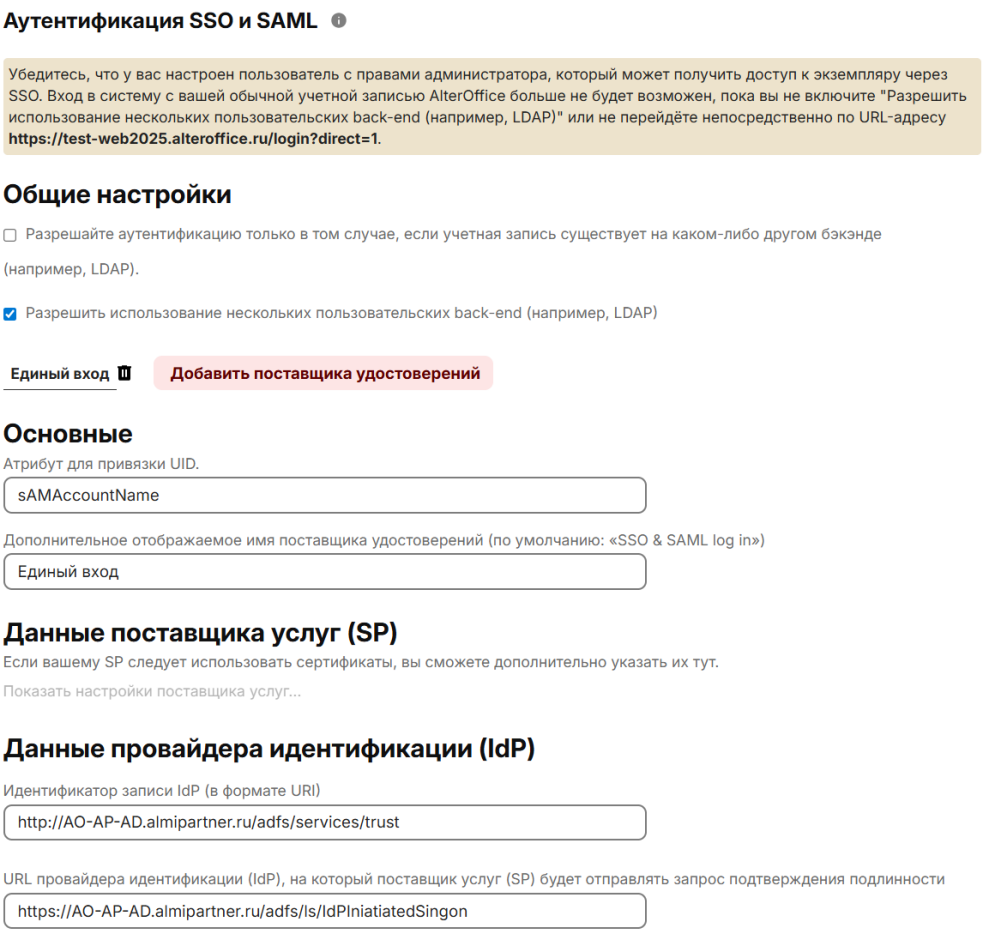


Рисунок 178. Настройка аутентификации SSO и SAML

В разделе «Данные провайдера идентификации (IdP)» укажите следующие параметры:

Поле	Описание	Пример
Идентификатор записи IdP (в формате URL)	Уникальный идентификатор IdP	`http://AO-AP-AD.almipartner.ru/adfs/services/trust`
URL провайдера идентификации (IdP)	Адрес для отправки поставщиком услуг (SP) запросов на аутентификацию	`https://AO-AP-AD.almipartner.ru/adfs/ls/IdPIniatiatedSingon`

- Идентификатор службы федерации указывается в формате `http://<FQDN ADFS сервера>/adfs/services/trust`
- URL провайдера идентификации: `https://<FQDN ADFS сервера>/adfs/ls/IdPInitiatedSignon`

Нажмите на ссылку «Показать дополнительные настройки провайдера идентификации», чтобы внести дополнительные данные.

Поле	Описание	Пример
URL адрес IdP, куда SP будет	Адрес для отправки	`https://AO-AP-`

Поле	Описание	Пример
оправлять запросы SLO	поставщиком услуг (SP) запроса на выход, когда пользователь инициирует завершение сеанса работы. Этот запрос сообщает IdP, что сессия пользователя должна быть закрыта	`AD.almipartner.ru/adfs/ls/?wa=wsignout1.0`
Открытый сертификат X.509 IdP	Сертификат проверки подписей SAML-сообщений в формате Base64. Используйте значение из ранее сохраненного файла.	`-----BEGIN CERTIFICATE----- MIIE6jCCAtKgAwIBAgIQFdrPnnQud6BEM5J1grbi5jANBgkqhkiG9w0BAQsFADAx...`

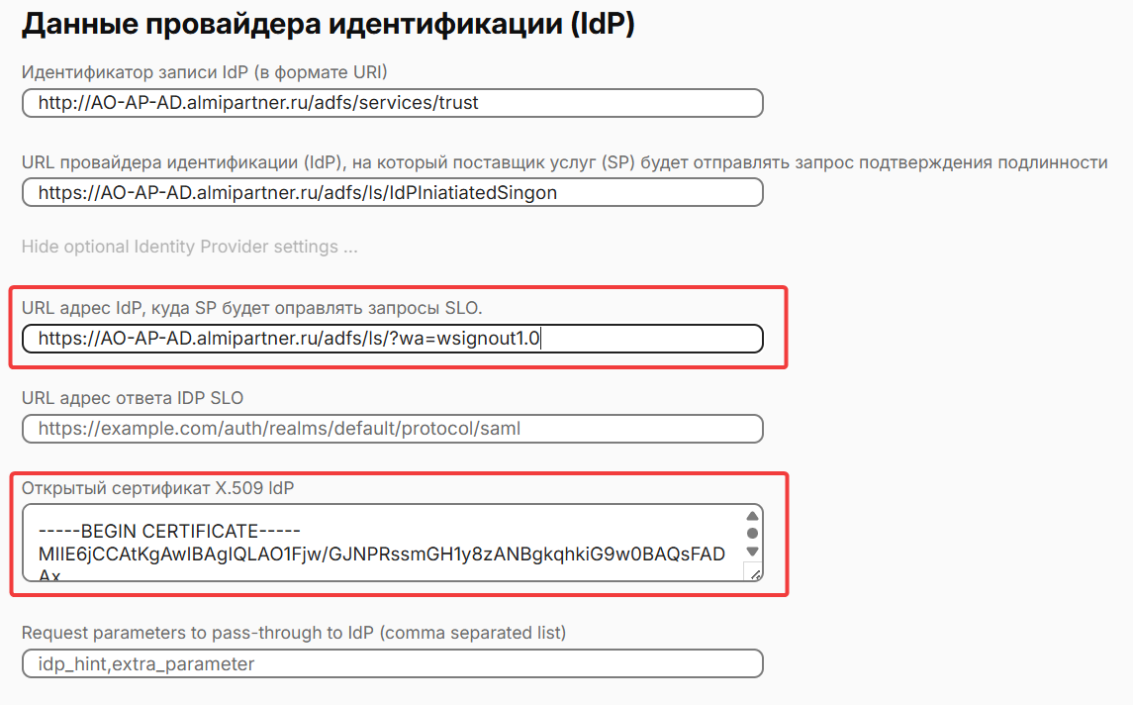


Рисунок 179. Настройка адреса запроса на выход и открытого ключа

В разделе «Привязка атрибутов» укажите следующие параметры:

Поле	Атрибут	Описание
Атрибут для привязки отображаемого имени	displayname	Отображаемое имя
Атрибут для привязки email	UserPrincipalName	Адрес электронной почты
Атрибут для отображения групп пользователей	department	Группа пользователей

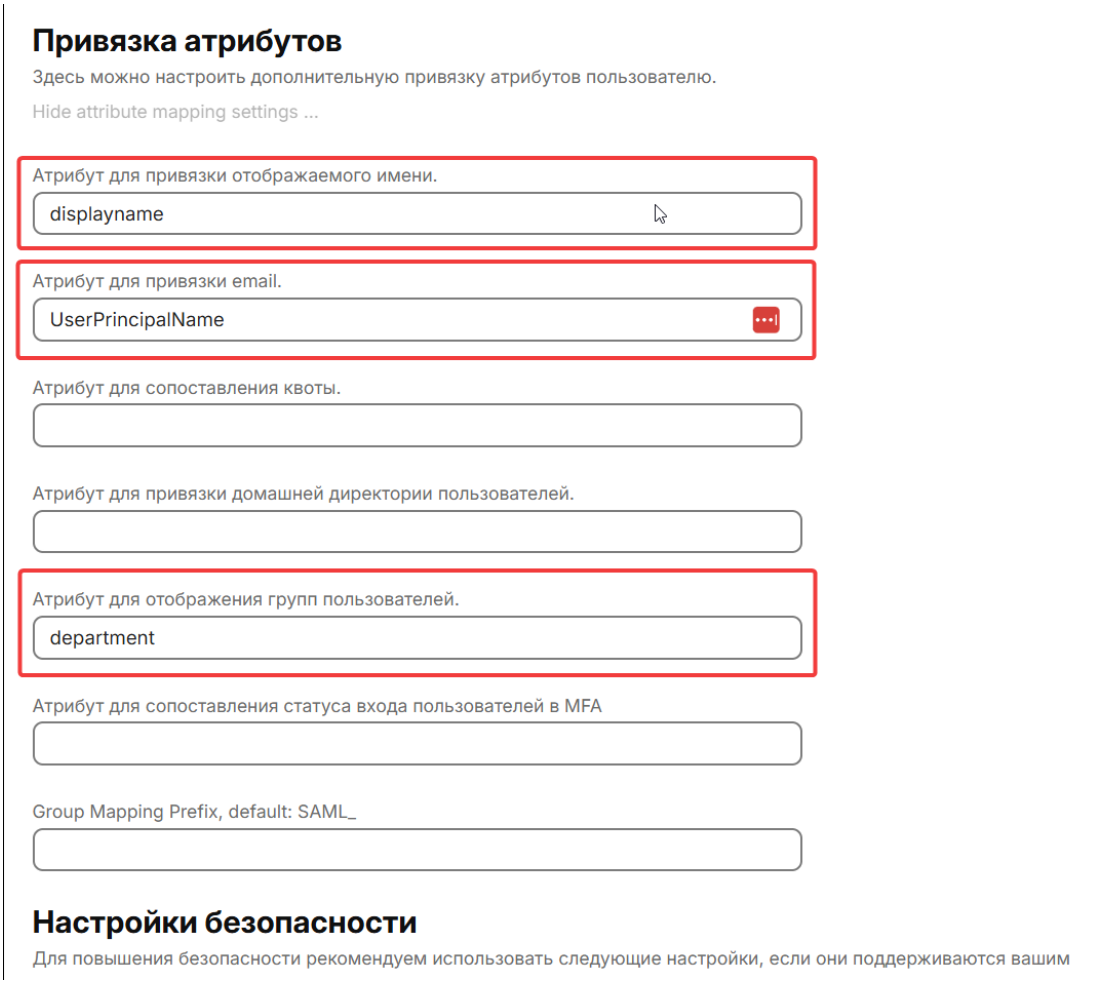


Рисунок 180. Настройка привязки атрибутов

Настройки сохраняются автоматически, внизу станицы отобразится сообщение «Метаданные верны», здесь же можно скачать данные в формате XML.

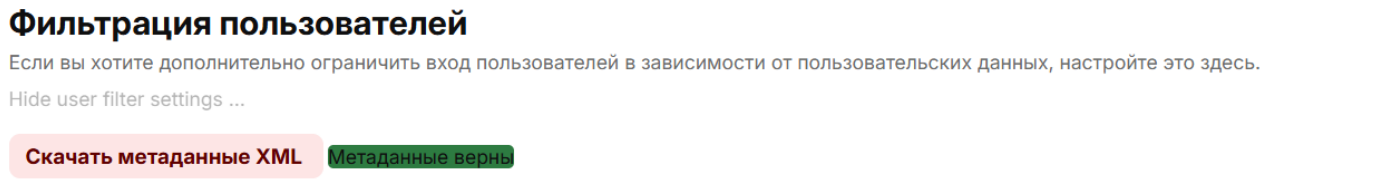


Рисунок 181. Получение метаданных XML.

4.13.1.5. Тестирование интеграции

Попробуйте войти в систему под учетной записью доменного пользователя, чтобы убедиться, что настройки работают корректно.

На приветственной странице выберите «Единый вход».

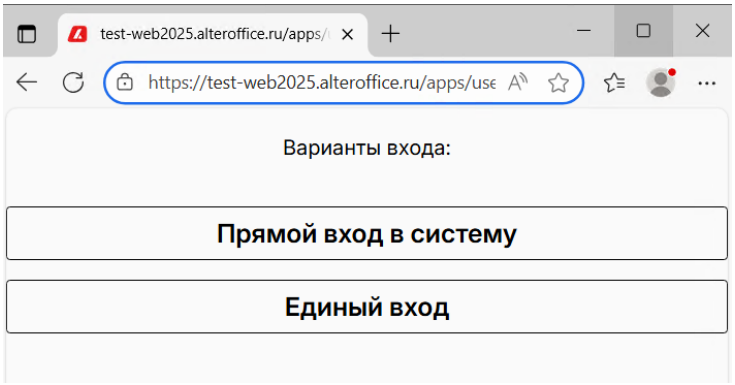


Рисунок 182. Варианты входа.

Значение «Единый вход» произвольное и настраивается на странице **Аутентификация SSO и SAML**.

Откроется форма для доменной аутентификации, введите данные.

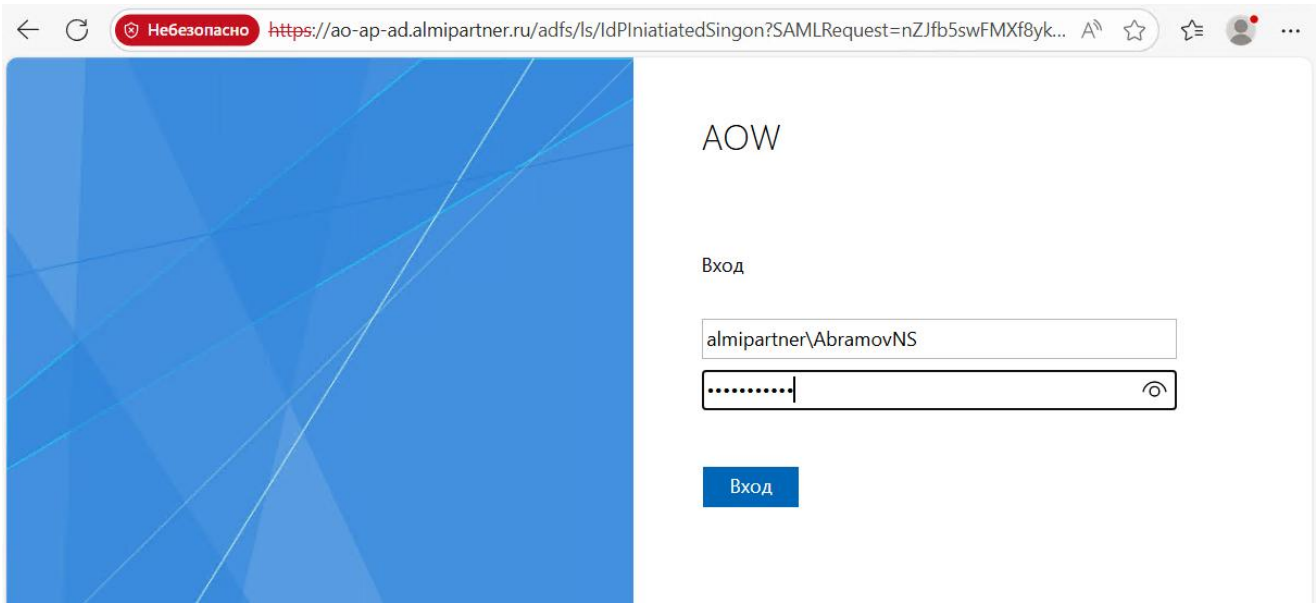


Рисунок 183. Аутентификация.

- SSO работает только с доверенными URL-адресами. Если используется самоподписанный сертификат, то ссылку на систему нужно включить в зону «Надёжные сайты» (Trusted sites).

Нажмите «Вход».

Пользователь авторизуется в системе и может посмотреть профиль, в котором будут отражены сведения, полученные из AD:

- Отображаемое имя.
- Адрес электронной почты.
- Группа пользователей.

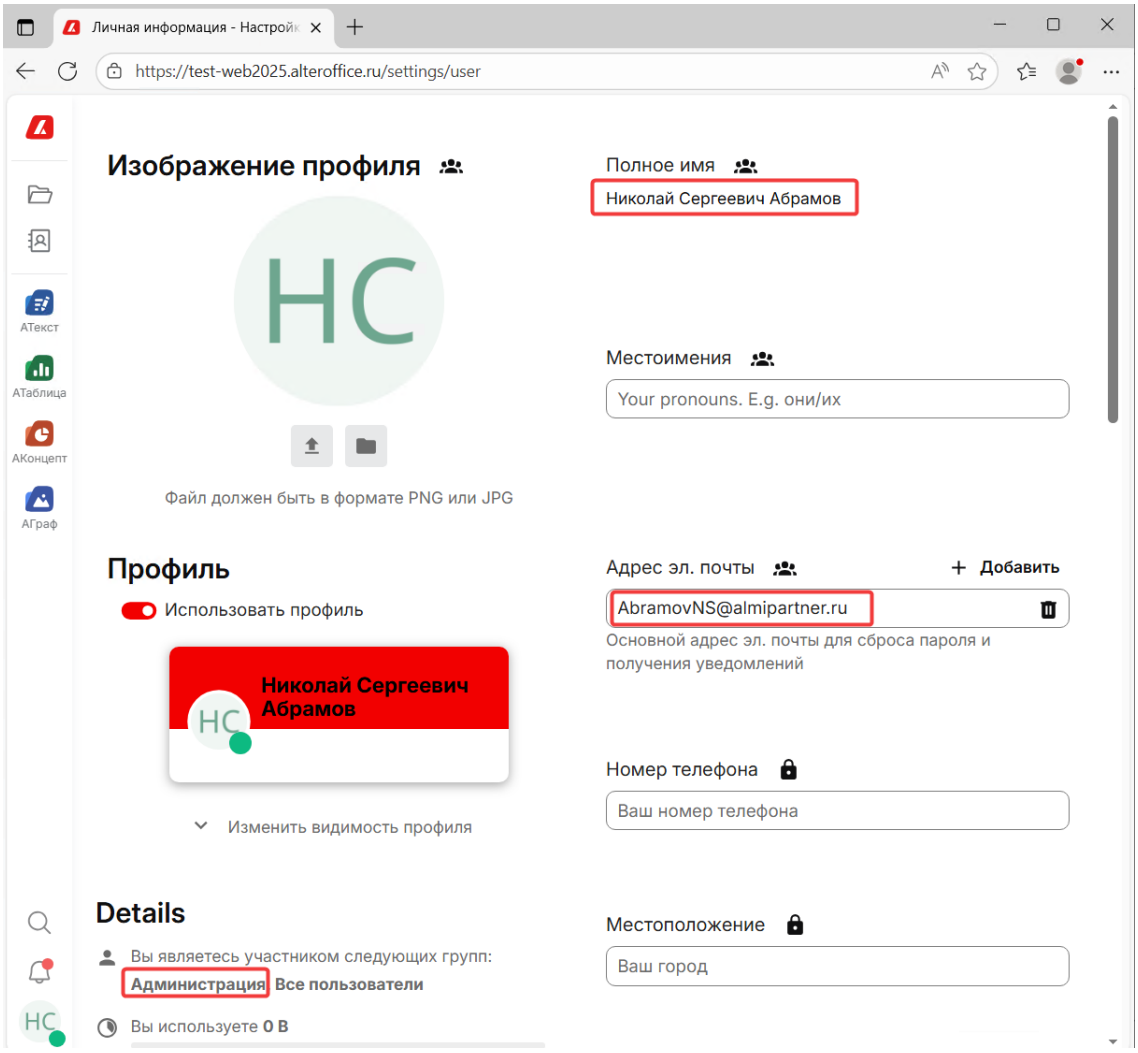


Рисунок 184. Сведения о пользователе.

Для выхода из системы нажмите на аватар и выберите «Выйти».

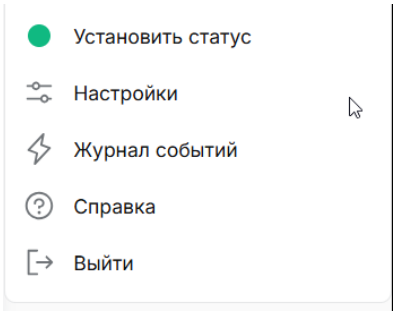


Рисунок 185. Выход из системы.

Откроется страница с информацией, что пользователь успешно вышел из системы.

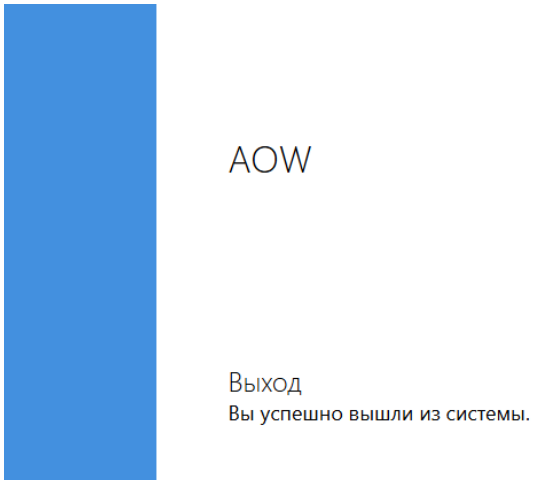


Рисунок 186. Пользователь успешно вышел из системы.

4.14. Настройка федеративного доступа

Между несколькими экземплярами АльтерОфис Веб может быть настроен федеративный доступ, реализованный на протоколе Open Cloud Mesh (OCM).

Каждый экземпляр функционирует автономно, но при необходимости пользователи могут обмениваться файлами и работать над документами совместно, как если бы они находились на одном сервере.

Федеративный доступ не является обязательным при установке системы и настраивается при необходимости. Настройки выполняются через командную строку (CLI) и через графический веб-интерфейс (WebUI).

В данном разделе описывается последовательность и настройки с использованием WebUI, настройки с использованием CLI описаны в документе «**Руководство администратора по развертыванию системы АльтерОфис Веб**».

4.14.1. Порядок выполнения операций для настройки федеративного доступа

Для успешной настройки рекомендуется соблюдать следующий порядок:

Настройка	**Вариант настройки**
Настройка сетевого взаимодействия	CLI
Проверка доступности	CLI
Активация приложения Federation	CLI
Разрешение доступа для изолированных серверов	CLI
Установка базовых URL	CLI
Настройка «белого» списка IP адресов	WebUI
Настройка межсерверного обмена	WebUI

Настройка	Вариант настройки
для пользователей	
Настройка доверенных серверов	WebUI
Синхронизация адресных книг для федеративного доступа	CLI
Настройка редакторов для совместной работы при федеративном доступе	CLI

4.14.2. Настройка сетевого взаимодействия

Для обеспечения корректного разрешения имен между серверами необходимо добавить статические записи в файл хостов внутри контейнера.

Настройка сетевого взаимодействия выполняется через CLI и описана в документе «**Руководство администратора по развертыванию системы АльтерОфис Веб**».

Выполните настройку для всех серверов, которые будут использоваться для организации федеративного доступа.

4.14.3. Проверка сетевой доступности

После настройки DNS-записей необходимо убедиться, что серверы могут взаимодействовать друг с другом без SSL-ошибок.

Выполните проверку доступности серверов через CLI, как описано в документе «**Руководство администратора по развертыванию системы АльтерОфис Веб**».

4.14.4. Активация приложения Federation

Выполните активацию приложения Federation через CLI, как описано в документе «**Руководство администратора по развертыванию системы АльтерОфис Веб**».

Также приложение может быть включено из WebUI, для этого убедитесь, что приложение **Federation** активировано.

> СМ. ТАКЖЕ
>
> - Подробнее см. в разделе «Управление приложениями (модулями) системы».

4.14.5. Разрешение доступа для изолированных серверов

По умолчанию АльтерОфис Веб разрешает федеративный обмен только с серверами, имеющими валидные публичные SSL-сертификаты. Для работы в изолированном контуре необходимо разрешить обмен с локальными серверами.

Выполните настройки для изолированных серверов через CLI, как описано в документе «**Руководство администратора по развертыванию системы АльтерОфис Веб**».

4.14.6. Установка базовых URL

Для корректной генерации абсолютных ссылок в системе (например, в уведомлениях по электронной почте или для внешних пользователей) необходимо явно задать базовый URL каждого сервера.

Выполните установка базовых URL через CLI, как описано в документе «**Руководство администратора по развертыванию системы АльтерОфис Веб**».

4.14.7. Настройка «белого» списка IP адресов

Для корректной работы серверов при организации федеративного доступа, необходимо IP адреса серверов добавить в «белый список».

Настройка «белого списка» выполняется через веб-интерфейс - подробнее см. «Настройка и управление защитой от перебора».

4.14.8. Настройка межсерверного обмена для пользователей

Настройте политики общего доступа к ресурсам для федеративного обмена как внутри сервера, так и между разными серверами.

1. Откройте раздел «Параметры публикации»

В веб-интерфейсе **АльтерОфис Веб** нажмите на аватар пользователя и в открывшемся меню выберите пункт **«Параметры сервера»**.

В разделе **«Параметры сервера»** выберите пункт **«Параметры публикации»**.

2. Настройка параметров межсерверного обмена

Найдите на открывшейся странице заголовок **Межсерверный обмен**.

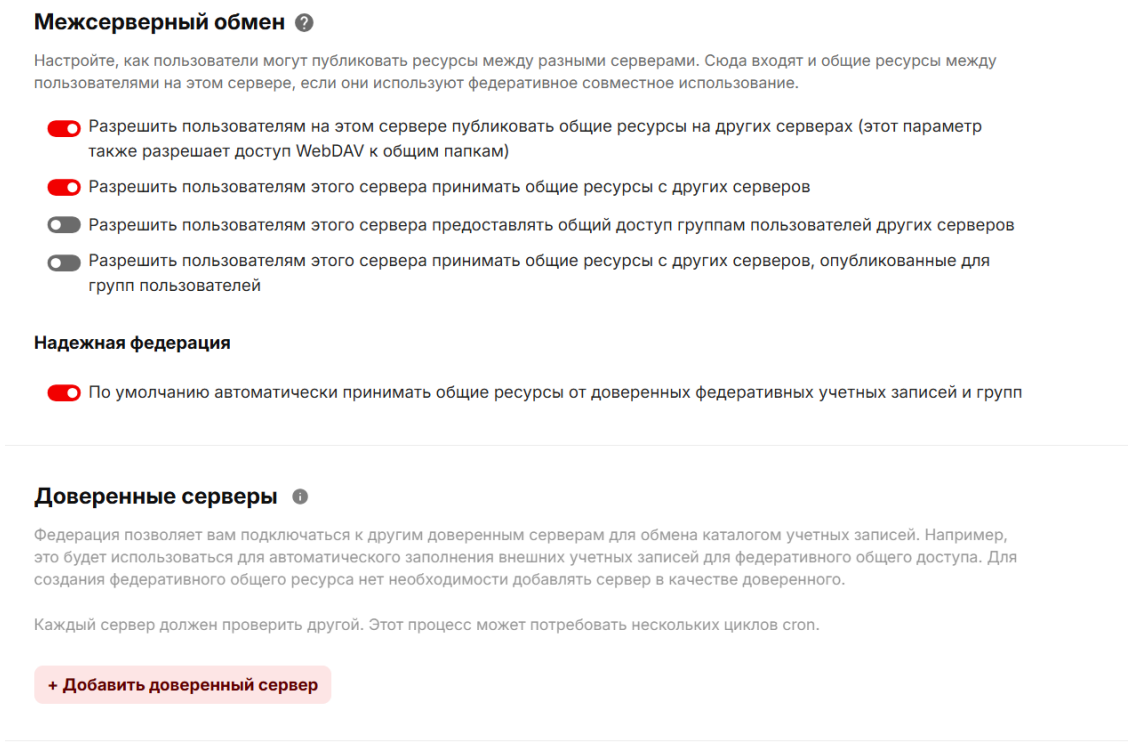


Рисунок 187. Настройка параметров публикации

Активируйте необходимые опции:

Параметр	Назначение	Примечание
Разрешить пользователям на этом сервере публиковать общие ресурсы на других серверах (этот параметр также разрешает доступ WebDAV к общим папкам)	Разрешает пользователям данного сервера предоставлять доступ к своим файлам и папкам пользователям на других (внешних) серверах.	Используйте, если требуется функционал совместной работы с внешними организациями или другими экземплярами АльтерОфис Веб.
Разрешить пользователям этого сервера принимать общие ресурсы с других серверов	Разрешает пользователям данного сервера получать и принимать файлы и папки, которыми с ними поделились пользователи внешних серверов.	Включите для полноценного двустороннего обмена. Обычно активируется вместе с предыдущей опцией.
Разрешить пользователям этого сервера предоставлять общий доступ группам пользователей других серверов	Позволяет пользователям этого сервера предоставлять доступ целым группам пользователей, существующим на внешнем сервере. Удобно для совместной работы с отделами или командами в другой организации.	Экспериментальная функция.

Параметр	Назначение	Примечание
Разрешить пользователям этого сервера принимать общие ресурсы с других серверов, опубликованные для групп пользователей	Разрешает группам пользователей на этом сервере получать общие ресурсы от пользователей внешних серверов. Все члены группы получат доступ к присланным файлам/папкам.	Экспериментальная функция.

В разделе **Надежная федерация** определите необходимость автоматического приёма общих ресурсов от доверенных федеративных учетных записей.

Параметр	**Назначение**	**Примечание**
По умолчанию автоматически принимать общие ресурсы от доверенных федеративных учетных записей и групп	Автоматически принимает входящие общие ресурсы от серверов и групп, добавленных в «доверенные» (Trusted Servers), без необходимости ручного подтверждения каждым пользователем.	Включайте только для серверов-партнёров с высоким уровнем доверия (например, внутри холдинга).

Настройку межсерверного доступа через CLI см. в документе «**Руководство администратора по развертыванию системы АльтерОфис Веб**».

4.14.9. Настройка доверенных серверов

Раздел **Доверенные серверы** позволяет создавать белый список серверов-партнеров для упрощенного и автоматизированного федеративного обмена. Ресурсы с доверенных серверов могут приниматься автоматически, минуя дополнительные подтверждения.

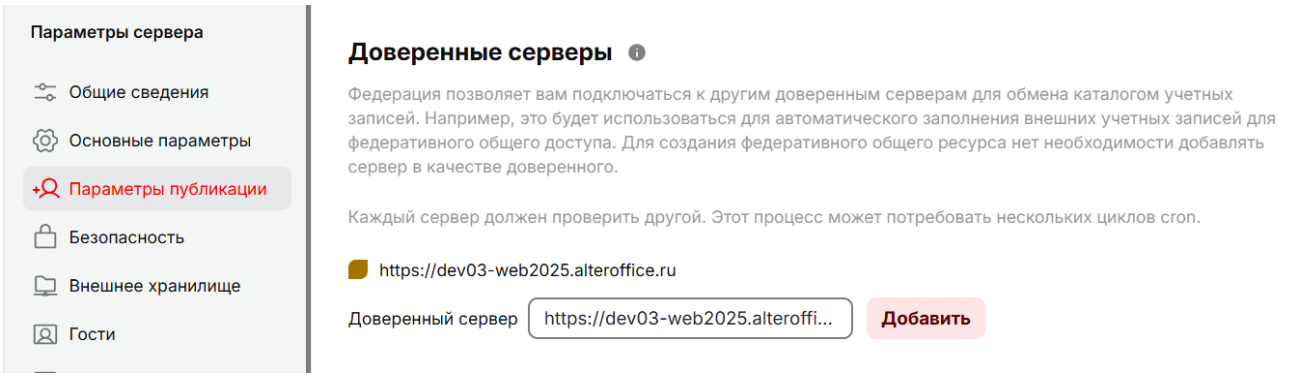


Рисунок 188. Настройка доверенных серверов

Нажмите кнопку **Добавить доверенный сервер**.

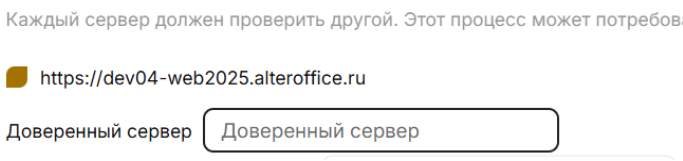


Рисунок 189. Добавление доверенного сервера

В поле **Доверенный сервер** укажите URL-адрес сервера-партнёра и нажмите Enter.

После добавления серверу присваивается индикатор состояния, который отображает результат проверки соединения:

- **Красный индикатор** означает, что подключение не удалось.
- **Жёлтый индикатор** указывает на успешное подключение без обмена именами пользователей.
- **Зелёный индикатор** указывает на успешное подключение с обменом именами пользователей.

Для получения зелёного статуса необходимо, чтобы доверенные серверы поддерживались на обоих взаимодействующих серверах.

Для достижения зелёного статуса необходимо выполнение двух обязательных условий на обоих серверах:

- Включена поддержка доверенных серверов в настройках федеративного обмена.
- Активны фоновые задания (`cron`) для синхронизации данных.

Для ускорения процесса добавления сервера в доверенные можно принудительно запустить фоновые задания.

Запуск фоновых заданий выполняется через CLI. Описание запуска фоновых заданий для настройки доверенных серверов см. в документе «**Руководство администратора по развертыванию системы АльтерОфис Веб**».

ПРИМЕЧАНИЕ

- Если **зелёный индикатор** не загорелся: проверьте, что серверы могут взаимодействовать друг с другом без SSL-ошибок, как описано в документе «**Руководство администратора по развертыванию системы АльтерОфис Веб**».

4.14.10. Синхронизация адресных книг для федеративного доступа

Синхронизация адресных книг обеспечивает автоматический обмен контактами между доверенными серверами, позволяя пользователям быстро находить коллег на партнёрских экземплярах АльтерОфис Веб при предоставлении общего доступа. Эта функция работает в фоновом режиме через `cron` задания и активируется при успешном установлении «зелёного» статуса соединения между серверами.

Для ускорения процесса синхронизации можно принудительно запустить фоновые задания.

Запуск фоновых заданий выполняется через CLI. Описание запуска фоновых заданий для синхронизации адресных книг см. в документе «**Руководство администратора по развертыванию системы АльтерОфис Веб**».

4.14.11. Настройка редакторов для совместной работы при федеративном доступе

Для корректного открытия офисных документов, к которым предоставлен федеративный доступ, необходимо выполнить настройки через CLI. Описание настройки редакторов для совместной работы при федеративном доступе см. в документе «**Руководство администратора по развертыванию системы АльтерОфис Веб**».

4.15. Управление сроком хранения версий файлов

Система автоматически удаляет устаревшие версии файлов, чтобы пользователи не могли превысить установленные квоты. Администратор может самостоятельно настроить правила хранения версий, чтобы оно соответствовало политике организации.

> ПРИМЕЧАНИЕ
>
> Если пользователь присвоил имя версии, то она не будет удаляться системой

4.15.1. Базовые правила хранения версий

> СОВЕТ
>
> **АльтерОфис Веб** не использует больше 50% квоты пользователя на свободное пространства при работе с версиями. Это правило является приоритетным, поэтому если сохраненные версии превышают этот лимит, то самые старые версии будут удалены автоматически, независимо от заданной настройки правила хранения версий.

По умолчанию действует следующий алгоритм хранения версий при работе с документом:

- В 1 секунду хранится одна версия.
- В первые 10 секунд **АльтерОфис Веб** хранит одну версию каждые 2 секунды.
- В первую минуту хранится одна версия файла каждые 10 секунд.
- В первый час хранится одна версия каждую минуту.
- В первые сутки хранится одна версия каждый час.
- В первые 30 дней хранится одна версия каждый день.
- После 30 дней хранится одна версия каждую неделю.

Важно понимать, что новая версия создается при изменении или сохранении файла. За счет алгоритма описанного выше обеспечивается приоритет новых версий над старыми, чем обеспечивается детальная история изменений для недавних правок. Система по умолчанию хранит не больше 15 версий файла.

> СОВЕТ
>
> - Схема пересчитывается каждый раз, когда создается новая версия.

4.15.2. Дополнительные правила хранения версий

АльтерОфис Веб предлагает дополнительные правила хранения версий. Для их применения внесите соответствующую запись в файл **config.php**.

Минимальный срок хранения в днях
Настройка сохраняет версию минимум **N** дней. Правила удаления применяются к версиям файла старше **N** дней.

```
'versions_retention_obligation' => 'N, auto',
```

Удаление версий старше определенного срока
Настройка удаляет все версии старше **N** дней. Остальные версии удаляются согласно правилу по умолчанию.

```
'versions_retention_obligation' => 'auto, N',
```

Задать диапазон хранения версий
Настройка позволяет хранить версии не менее **N1** дней и удалять их, когда исполнится более **N2** дней.

```
'versions_retention_obligation' => 'N1, N2',
```

Отключение автоматического удаления
Настройка позволяет отключить автоматическое удаление старых версий файла.

```
'versions_retention_obligation' => 'disabled',
```

- Не рекомендуется отключать автоматическое удаление старых версий файла, так как это может привести к переполнению хранилища пользователя.

4.15.3. Запуск фоновой задачи на удаление файлов

Для удаления устаревших версий файлов каждые 30 минут автоматически запускается фоновая задача.

Администратор может отключить автоматический запуск фоновой задачи и настроить системное расписание (cron), которое будет удалять старые версии с помощью команды occ.

Отключение фоновой задачи

```
occ config:app:set --value=no files_versions background_job_expire_versions
```

Включение фоновой задачи

```
occ config:app:delete files_versions background_job_expire_versions
```

Удаление вручную

```
occ versions:expire
```

В «тихом» режиме:

```
occ versions:expire --quiet
```

4.16. Настройка системы для работы с макросами

По умолчанию макросы в редакторах отключены в целях безопасности.

Работа с макросами не является обязательным при установке системы и настраивается при необходимости. Настройки выполняются через командную строку (см. описание в документе «**Руководство администратора по развертыванию системы**») и через графический веб-интерфейс (WebUI).

4.16.1. Порядок выполнения настроек для работы с макросами

Для успешной настройки рекомендуется соблюдать следующий порядок:

Настройка	**Вариант настройки**
Администратор системы настраивает контейнеры **app** и **editors** для работы с одним **VOLUME**, в который будут размещаться макросы.	CLI
Администратор системы подключает внешнее хранилище для размещения в нем макросов приложения через WebUI и которые будут доступны пользователям.	WebUI
Администратор системы создает новые макросы или загружает ранее созданные макросы в хранилище макросов.	WebUI
Пользователи АльтерОфис Веб используют настроенные администратором системы макросы для своей работы в офисных редакторах (АТекст, АТаблица, АКонцепт).	WebUI

Настройки через командную строку описаны в документе «**Руководство администратора по развертыванию системы**».

4.16.2. Подключение внешнего хранилища для работы с макросами.

Выполнение настроек для работы с макросами в системе «АльтерОфис Веб» будет рассмотрено на примере:

- **Экземпляр** имеет адрес `https://demo03-web2025.alteroffice.ru`

Шаг 1. Зайдите в систему с правами администратора системы по ссылке:

Пример: `https://demo03-web2025.alteroffice.ru`

Шаг 2. Настройте доступ к папке

В разделе **Аватар | Параметры сервера | Внешнее хранилище** настройте доступ к папке `/var/www/html/data/Scripts` внутри контейнера **app**.

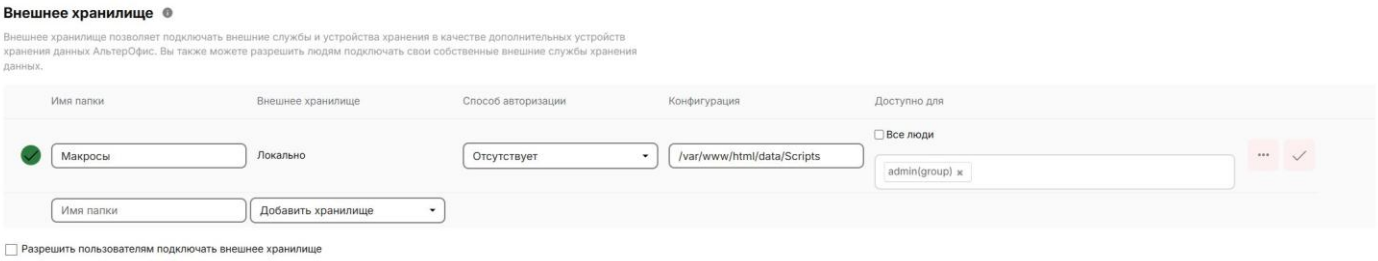


Рисунок 190. Настройка хранилища для макросов

Шаг 3. Проверьте корректность настройки

Убедитесь, что настройка подключения выполнена корректно - индикатор подключения «зеленый».

4.16.3. Загрузка и создание макросов.

После подключения хранилища для макросов, у администратора системы появляется в интерфейсе папка «Макросы» (зависит от того, какое название было указано в настройках на предыдущем этапе).

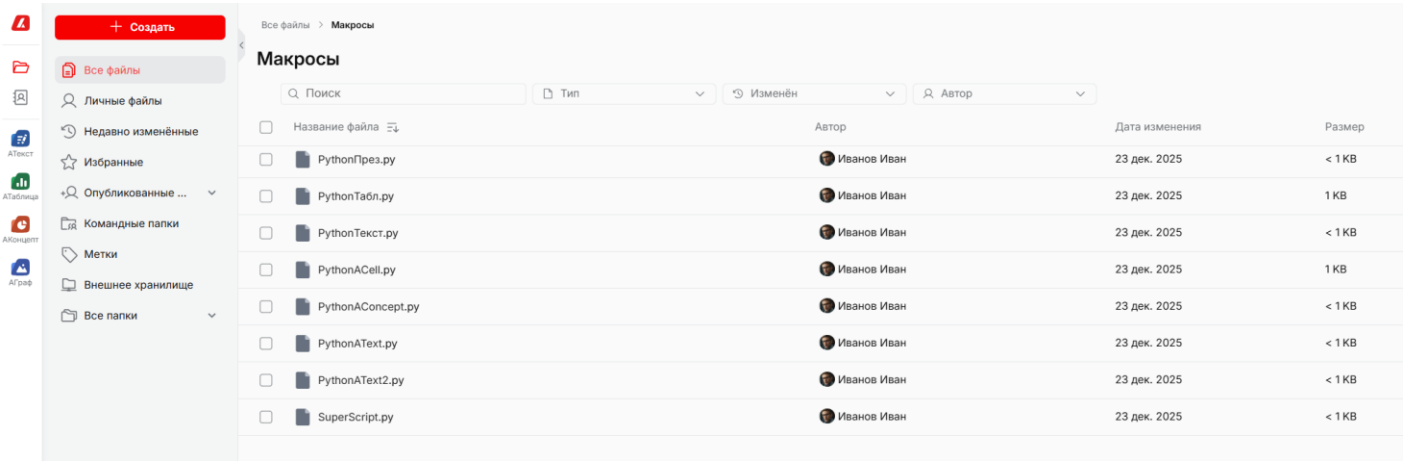


Рисунок 191. Список установленных макросов

В папку **Макросы** администратор системы может загружать макросы или создавать их используя текстовый редактор.

> ПРИМЕЧАНИЕ
>
> - Используйте в названиях макросов латинский алфавит.
> - Макросы не работают, если в названии есть кириллические символы.

Создайте и/или загрузите необходимые python макросы для работы в онлайн-редакторах.

После загрузки макросы становятся доступны спустя некоторое время (до 5-10 минут).

4.16.4. Работа пользователей с макросами приложения.

Шаг 1. Авторизуйтесь в системе под пользователем с ограниченными правами.

Шаг 2. Создайте новый документ в АТекст.

Шаг 3. Проверьте, что в интерфейсе появилась кнопка «Выполнить макрос».

Шаг 4. Проверьте, работу с макросами.

Нажмите на кнопку «Выполнить макрос».

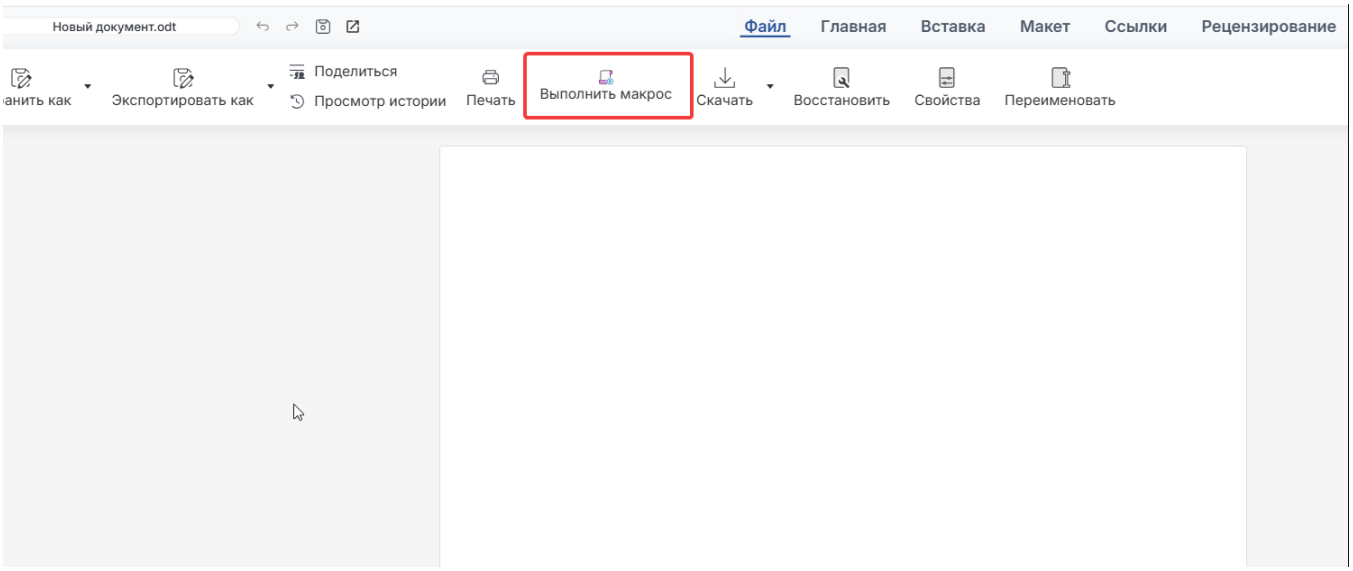


Рисунок 192. Новый документ

Убедитесь, что в разделе «Макросы приложения» отразился список загруженных макросов в папку **Макросы**.

Выберите требуемый макрос и запустите его.

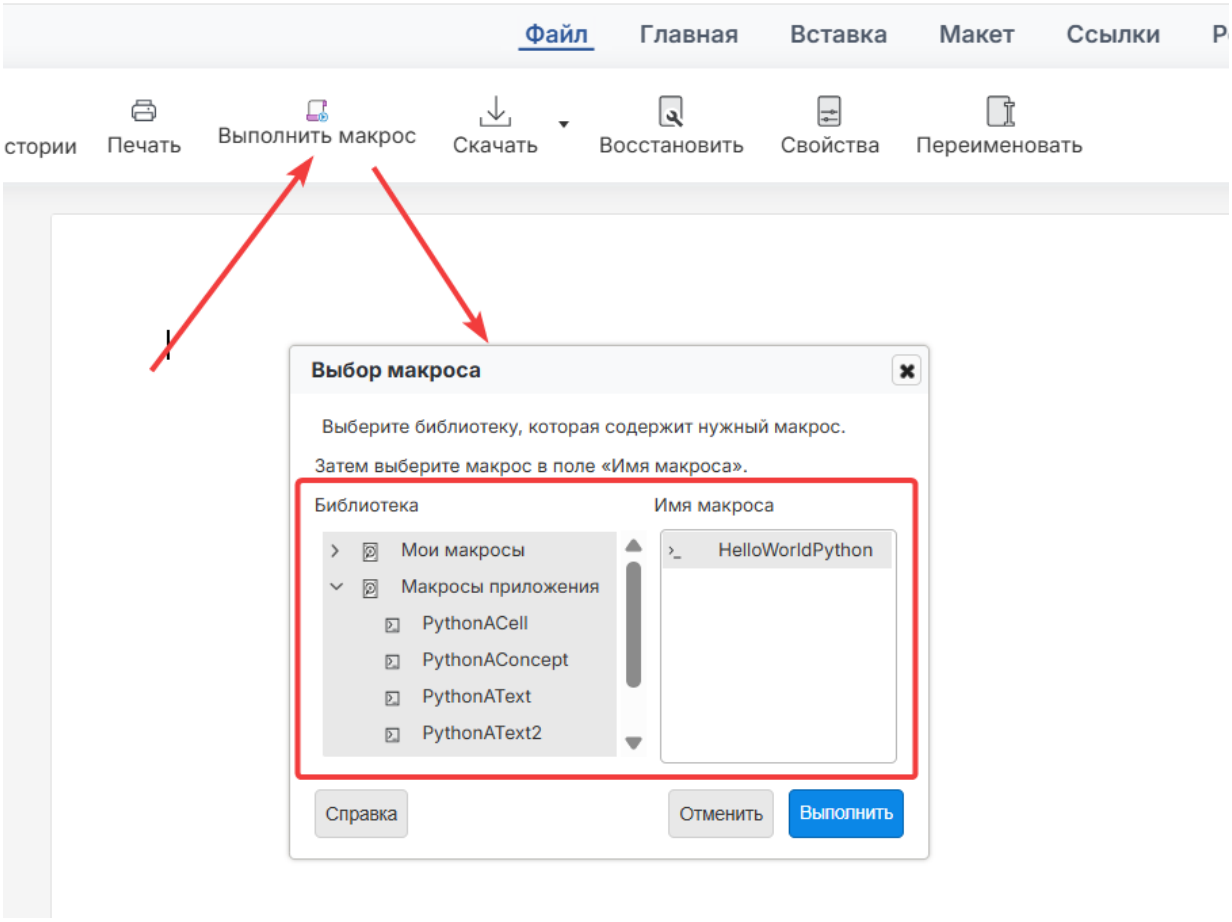


Рисунок 193. Запуск макросов приложения

Проверьте, что макрос отработал корректно.

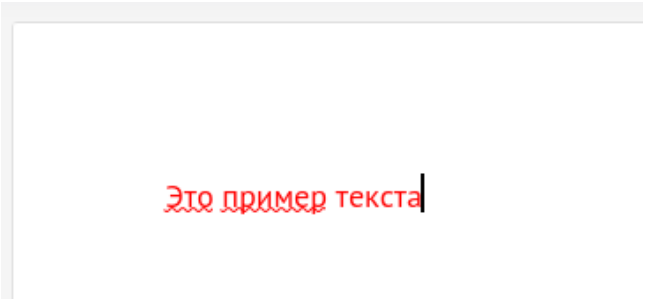


Рисунок 194. Запуск макросов приложения

На этом настройка для работы с макросами завершена. Обычные пользователи могут использовать загруженные администратором системы макросы.

5.Термины, обозначения и сокращения

В текст документа введены специальные сокращения на русском и английском языках. Определение терминов и расшифровка сокращений отражены в таблицах ниже.

5.1. Термины и определения

Термин	Определение
АльтерОфис Веб	Платформа для облачного хранения файлов и совместной работы пользователей (Система).
АТаблица	Приложение для работы с электронными таблицами, входящее в состав офисного пакета АльтерОфис.
Система	Совокупность элементов, объединенная связями между ними и обладающая определенной целостностью. В данном случае АльтерОфис Веб.
Пользователь	Учётная запись с базовым набором прав для работы с личными данными и ресурсами в рамках установленных политик доступа.
Логин	Имя учётной записи, используемое при входе в систему.
Пароль	Секретная комбинация символов для подтверждения личности при входе.
Двухфакторная аутентификация	(2ФА) Дополнительная защита при входе, требующая помимо пароля ввести ещё один код или подтвердить вход другим способом.
Одноразовый пароль	Код, действительный только один раз для подтверждения входа. Может быть получен по разным каналам (email, приложение).
Резервные коды	Набор заранее сгенерированных кодов для входа в систему, когда другие способы двухфакторной аутентификации недоступны.
Разовые коды администратора	Одноразовые коды для входа, выданные администратором пользователю в случае утери или недоступности других способов входа.
Корзина	Временное хранилище удалённых файлов и папок, из которого данные можно восстановить или удалить окончательно.
Папка общего доступа	Папка, доступ к которой предоставлен другим пользователям Системы или по публичной ссылке.
Публичная ссылка	Ссылка, позволяющая предоставить доступ к файлу или папке пользователям вне Системы. Может быть защищена паролем и сроком действия.
Метка (тег)	Ключевое слово, прикрепляемое к файлу или папке для упрощения поиска и организации данных.

Термин	Определение
Комментарий	Замечание или сообщение, оставляемое к файлу или папке для совместной работы.
Аутентификатор	Средство, используемое для подтверждения личности пользователя. Пользователь проходит аутентификацию в компьютерной системе или приложении, демонстрируя, что он владеет аутентификатором и контролирует его.
Роль	Набор прав доступа, назначаемый пользователю или группе пользователей.
Системная роль	Роль, определяющая глобальные права в рамках всей системы.
Администратор системы	Пользователь, обладающий неограниченными правами доступа ко всем функциям и ресурсам экземпляра
Администратор группы	Пользователь с делегированными правами администрирования в пределах назначенной группы.
Общий доступ	Механизм предоставления прав на отдельные ресурсы (файлы, папки).
Гость	Учётная запись с ограниченными правами доступа, предназначенная для временной работы внешних участников.
Политика безопасности паролей	Набор правил и требований, определяющих сложность, срок действия и условия обмена паролями для обеспечения защищенного доступа к системе.

5.2. Обозначения и сокращения

Сокращение	Расшифровка
OTP	One-Time Password — одноразовый пароль, который используется для подтверждения личности пользователя при входе в систему.
TOTP	Time-based One-Time Password — одноразовый пароль, действующий ограниченное время. Вариант OTP, генерируемый внешним приложением (например, «Я Ключ»).
2FA	Two Factor Authentication — двухфакторная аутентификация.
OTP	One-Time Password — одноразовый пароль.
OCM	Open Cloud Mesh – протокол объединения серверов, который используется для уведомления принимающей стороны о том, что ей предоставлен доступ к некоторому ресурсу.
WebDAV	Web Distributed Authoring and Versioning – протокол, который позволяет работать с файлами на сервере как с обычными файлами на локальном диске.

Сокращение	Расшифровка
ODF	Open Document Format — открытый стандарт для электронных документов, созданный как универсальное решение для хранения текстовых файлов, таблиц и презентаций. Формат включает текстовые файлы (.odt), электронные таблицы (.ods), презентации (.odp) и другие типы документов, например рисунки (.odg).
OOXML	Office Open XML — серия форматов файлов для хранения электронных документов пакетов офисных приложений (DOCX, XLSX, PPTX).
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
DNS	Domain Name System. Система доменных имён — механизм, посредством которого символьные доменные имена переводятся в IP-адреса и обратно.
HTTP	HyperText Transfer Protocol. Прикладной сетевой протокол, используемый для передачи гипертекстовых данных (веб-страниц) между клиентом и сервером.
HTTPS	HyperText Transfer Protocol Secure. Расширение HTTP, обеспечивающее шифрование соединения с помощью SSL/TLS, чтобы гарантировать конфиденциальность и целостность передаваемых данных.
SSL/TLS	Secure Sockets Layer / Transport Layer Security. Криптографические протоколы, обеспечивающие защищённую передачу данных в сетях TCP/IP. SSL — ранняя версия, заменена на TLS. Протокол гарантирует шифрование, целостность и аутентичность соединений.
IP	Internet Protocol. Сетевой протокол, определяющий правила адресации и маршрутизации пакетов данных между узлами в сетях TCP/IP.
LDAP	Lightweight Directory Access Protocol. Протокол прикладного уровня, предназначенный для доступа и управления распределёнными каталогами информации. Позволяет централизованно хранить и быстро получать данные о пользователях, группах, устройствах, сервисах и других объектах.
SMTP	Simple Mail Transfer Protocol. Протокол передачи электронной почты между серверами, используется для

Сокращение	Расшифровка
	доставки сообщений и уведомлений.
SSO	Single Sign-On. Механизм обеспечения единого входа: пользователь выполняет авторизацию один раз и получает доступ к множеству связанных приложений/сервисов без необходимости повторного ввода учётных данных.
TCP/IP	Transmission Control Protocol / Internet Protocol
AD	Active Directory. Служба каталогов и система управления доступом, разработанная Microsoft для централизованного управления ресурсами, такими как пользователи, компьютеры и принтеры, в корпоративной сети.
PHP-LDAP	Расширение для языка PHP, предоставляющее функции для взаимодействия веб-приложений с серверами каталогов, работающими по протоколу LDAP. С его помощью можно выполнять аутентификацию пользователей, осуществлять поиск и получение данных из централизованных каталогов (например, Active Directory), а также управлять записями, хранящимися в иерархической структуре каталога.
SMB/CIFS	SMB (Server Message Block) и его расширенная версия CIFS (Common Internet File System) — это сетевой протокол прикладного уровня, предназначенный для организации совместного доступа к файлам, принтерам и другим сетевым ресурсам в локальной вычислительной сети.
LUKS	Linux Unified Key Setup. Стандарт шифрования дисков в Linux, разработанный для безопасного хранения данных на физических и виртуальных носителях. Основная задача — защитить данные на диске от несанкционированного доступа, даже если диск был извлечён и подключён к другой системе.
CLI	Command Line Interface. Интерфейс командной строки. Это текстовый способ взаимодействия пользователя с компьютерной системой или программным обеспечением через командную строку.
AD FS	Active Directory Federation Services. Компонент операционной системы Windows Server, предоставляющий службы федерации идентификации и обеспечивающий единый вход (Single Sign-On, SSO) для аутентификации пользователей в распределенных средах. С помощью AD FS пользователи могут получать доступ к сторонним приложениям и сервисам (например, АльтерОфис Веб) с

Сокращение	Расшифровка
	использованием своих корпоративных учетных данных домена Active Directory, без необходимости повторного ввода пароля.
SAML	Security Assertion Markup Language. Открытый стандарт на основе XML, предназначенный для обмена данными аутентификации и авторизации между сторонами, в частности между поставщиком удостоверений (Identity Provider) и поставщиком услуг (Service Provider).
SSE	Server-Side Encryption. Метод шифрования данных, при котором процессы шифрования, расшифровывания и управления ключами выполняются исключительно на стороне сервера. Данные автоматически шифруются перед сохранением на диск и расшифровываются при авторизованном доступе, без активного участия клиентских приложений.
S3	Simple Storage Service. Сервис (и одновременно протокол) для хранения данных большого объёма. Для работы использует API поверх HTTP, который позволяет загружать или получать объекты из хранилища.