+Альянс
IT-КОМПАНИЯ

Бэкап Яндекс 360

Описание приложения

+Альянс
IT-КОМПАНИЯ

Оглавление

+Альянс
IT-КОМПАНИЯ

Описание продукта

Бэкап Яндекс 360 — это современное веб-приложение, созданное для автоматического резервного копирования данных из сервисов Яндекса в облачное хранилище S3.

Поддерживаемые сервисы:

- Яндекс Диск
- Яндекс Почта
- Яндекс Календарь
- Списки задач
- Контакты

Продукт обеспечивает надежное сохранение данных, их восстановление и бесперебойный доступ, защищая организации от потери информации в результате сбоев или непредвиденных ситуаций.
Приложение интегрируется с API Яндекса для извлечения данных и использует возможности S3 для масштабируемого и безопасного хранения, предоставляя организациям удобный инструмент управления резервными копиями сотрудников.

Целевая аудитория

Документация ориентирована на следующие категории пользователей:

- Администраторы организаций — специалисты, ответственные за подключение сервиса, настройку параметров резервного копирования и управление данными сотрудников.
- Руководители и владельцы бизнеса — лица, принимающие решения об использовании сервиса, подписок и общей стратегии использования приложения для защиты целостности и хранения данных.

+Альянс
IT-КОМПАНИЯ

Описание приложения

Приложение предназначено для автоматизированного резервного копирования данных из сервисов Яндекса (например, Яндекс.Диск, Яндекс.Почта, Яндекс.Календарь, Списки задач, Контакты) в облачное хранилище S3.

Облачное хранилище обеспечивает надежное хранение данных, позволяя пользователям и организациям защитить свои данные от потери, сбоев или непредвиденных ситуаций, реализовывая возможность бесперебойного доступа к данным, а также восстановления и скачивания в случае необходимости.

Приложение поддерживает гибкую настройку процесса резервного копирования, включая выбор данных для копирования, указания расписания выполнения задач, а также миграция данных.

Данные из сервисов Яндекса извлекаются через официальные API, после чего сохраняются в указанные администратором организации бакеты S3, с возможностью выбора приоритетов при копировании.

Функционал приложения

Приложение "Бэкап Яндекс 360" предоставляет следующие возможности для автоматизированного резервного копирования данных из сервисов Яндекса в облачное хранилище S3:

1. **Извлечение данных через API Яндекса**

- Поддерживается подключение к сервисам Яндекса (Диск, Почта, Календарь, Список задач, Контакты) через официальные API для получения данных сотрудников организации.

2. **Гибкая настройка резервного копирования**

- Выбор данных для копирования, с возможностью выбора как всех сервисов, так и определенных сценариев:
  - Диск
  - Почта
  - Календарь
  - Списки задач

  - Контакты
- Установка расписания выполнения задач (ежедневно, еженедельно и т. д.), в т. ч. групп пользователей.
  - Предоставляется возможность тонкой настройки резервного копирования:
    1. Указания через интерфейс дней недели для резервного копирования.
    2. Указание расписания с использованием CRON Expression, с возможностью дополнительного указания времени, с минимальной очередностью – ежедневно.
- Определение приоритетов выбора бакетов для выполнения копирования, в случае переполнения одного из хранилищ.

3. **Сохранение в S3**

- Передача данных в указанные администратором бакеты S3.
- Поддержка масштабируемого, в случае необходимого облачного хранилища.

4. **Миграция данных**

- Возможность переноса данных между сотрудниками Организации, с возможностью выбора отдельной папки для хранения данных.

5. **Дашборд для управления**

- Мониторинг статуса задач резервного копирования в реальном времени.
- Управление подписками и тарифами.
- Конфигурация параметров выполнения задач.
- Ручной запуск процесса копирования при необходимости.
- Выполнение миграций данных
- Просмотр информации о сохраненных данных внутри веб-интерфейса
- Статистика используемого места для резервных копий, с отображением отдельной информации по каждому пользователю, сервису и резервной копии, реализованный в виде таблицы и графиков

6. **Восстановление и доступ к данным**

- Обеспечение бесперебойного доступа к резервным копиям через интерфейс приложения.

- Функция восстановления данных из хранилища в случае потери или сбоя.
- Возможность скачивания резервных копий, а также отдельных сущностей для локального использования.

7. **Администрирование для организаций**

- Поддержка многопользовательской архитектуры для управления данными сотрудников.
- Назначение пользователей в качестве администратора тенанта, для делегирования управления и настройки сервисом

8. **Безопасность данных**

- Использование пары ключей шифрования для защиты данных при передаче и хранении.
- Соответствие требованиям конфиденциальности и защиты информации.

Функционал приложения адаптирован для удобства использования организациями, обеспечивая автоматизацию процессов резервного копирования, гибкость настройки и надежность хранения данных.

Безопасность и защита данных

Шифрование данных при передаче

Все взаимодействия между приложением, сервисами Яндекса и Amazon S3 осуществляются через защищённый протокол HTTPS (HTTP Secure) с использованием TLS (Transport Layer Security). Это исключает возможность перехвата данных третьими лицами во время передачи.

Отсутствие хранения данных внутри приложения

Приложение не сохраняет данные сотрудников или организаций на своих серверах. Оно выступает исключительно в роли посредника, извлекая данные из сервисов Яндекса через API и передавая их напрямую в указанные бакеты S3. После завершения процесса копирования данные о содержании файлов не остаётся в системе.

Симметричное и асимметричное шифрование

1. **AES-GCM**: для симметричного шифрования данных используется алгоритм AES (Advanced Encryption Standard) в режиме GCM (Galois/Counter Mode) с

длиной ключа 256 бит. Этот метод обеспечивает высокую скорость шифрования и дополнительную проверку целостности данных.

2. **RSA**: для асимметричного шифрования применяется алгоритм RSA с длиной ключа не менее 2048 бит. Он используется для безопасной передачи ключей шифрования между компонентами системы и аутентификации.

Ключи генерируются индивидуально для каждой организации (тенанта) и хранятся в защищённой среде, доступной только администратору.