

Участники (Room 2):

- Барсуков Р3415
- Конкин Р3410
- Мальков Р3410
- Кобелев Р3412
- Шорников Р3411
- Ляшенко Р3409
- Аскарлов
- Таранов Р3419
- Эйдельман Р3414
- Кремпольская Р3420

Название системы: Облачное файловое хранилище (CloudDrive)

Шаг 1: определяем нашу систему

Предоставлять пользователям возможность загружать, хранить, скачивать, управлять и делиться файлами через веб-интерфейс или API.

Шаг 2: определяем акторов

Актор	Роль
Пользователь (End User)	Загружает, скачивает, просматривает, удаляет файлы. Может создавать папки, делиться файлами.
Администратор (Admin)	Управляет учетными записями, квотами, мониторингом, резервным копированием.
Внешний сервис авторизации (OAuth Provider)	Например, Google, GitHub — для входа пользователей.
Внешний сервис оплаты (Payment Gateway)	Если есть платные тарифы (Stripe, PayPal).
Система мониторинга / логирования (Monitoring System)	Собирает метрики и логи (например, Prometheus + Grafana).

Пользователь	Роль	Уровень доверия	Почему?
Конечный пользователь (End User)	Загружает, скачивает, делится файлами	Частичное доверие	Мы доверяем ему вводить свои данные, но не доверяем хранить чужие файлы без контроля. Нужна аутентификация и авторизация.
Администратор системы	Управляет пользователями, квотами, мониторингом	Высокое доверие	Имеет доступ к конфигурации, логам, данным. Должен быть строго ограничен (MFA, RBAC).
Внешние сервисы (OAuth, Payment)	Обеспечивают вход/платежи	Низкое доверие	Мы не контролируем их. Взаимодействие через API с токенами и подписями.

Шаг 3: определяем внешние системы

Внешняя система	Назначение
OAuth-провайдер (Google, Microsoft, etc.)	Аутентификация и авторизация пользователей.
Шлюз платежей (Stripe, YooKassa)	Обработка подписок и оплат.
Облачное хранилище объектов (AWS S3, Google Cloud Storage, MinIO)	Хранение самих файлов.
База данных (PostgreSQL, MySQL)	Хранение метаданных: пользователи, файлы, папки, права доступа.
Сервис отправки email (SendGrid, SMTP)	Уведомления о действиях (например, приглашения к файлам).
CDN (Cloudflare, Akamai)	Ускорение доставки файлов конечным пользователям.

Внешняя система	Назначение	Протокол / Механизм аутентификации	Безопасность
OAuth-провайдер (Google, GitHub)	Аутентификация пользователей	OAuth 2.0 / OpenID Connect	Токены JWT, HTTPS, PKCE для SPA
Payment Gateway (Stripe, YooKassa)	Обработка платежей	API Key + Signature / OAuth	Секретные ключи в переменных окружения, HTTPS, IP-whitelist
Object Storage (S3, MinIO)	Хранение файлов	AWS IAM / Access Key + Secret	Подписанные URL (presigned URLs), временные токены STS
Email Service (SendGrid)	Отправка уведомлений	API Key	Ограниченные права, HTTPS
CDN (Cloudflare)	Доставка контента	Token / Origin Pull	Защита от DDoS, WAF
Monitoring System (Prometheus)	Сбор метрик	Basic Auth / TLS Certificates	Изолированный сетевой доступ, TLS

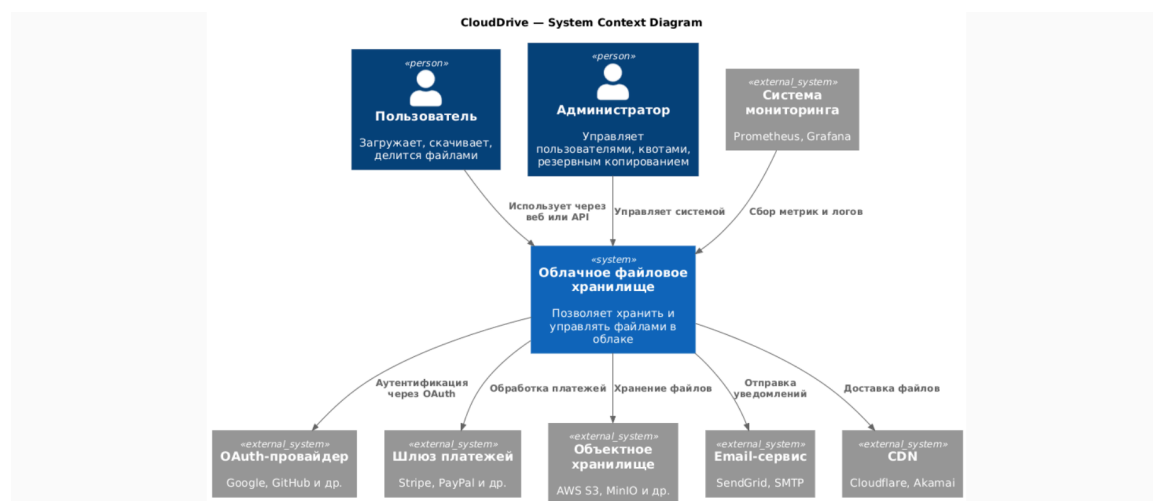
Все внешние интеграции должны использовать HTTPS, токены/ключи с минимальными привилегиями и временные учетные данные, где возможно

Контейнер → Контейнер	Протокол	Формат данных	Почему?
WebApp → API Gateway	HTTP/HTTPS	JSON (REST) или GraphQL	Стандартный веб-интерфейс, простой для фронтенда
API Gateway → Auth Service	gRPC / HTTP	JSON / Protobuf	Быстрая и надёжная внутренняя связь
API Gateway → File Service / User Service	HTTP/HTTPS	JSON	Гибкость, поддержка REST
File Service → Metadata DB	TCP/IP (PostgreSQL)	SQL	Надёжное хранение структурированных данных

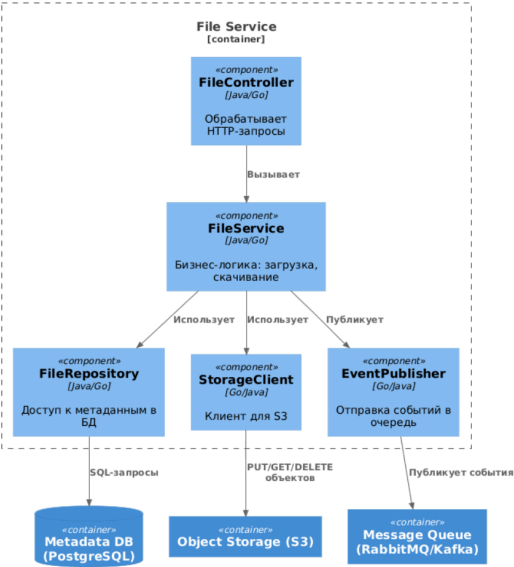
File Service → Message Queue	AMQP / Kafka Protocol	JSON	Асинхронная обработка задач (загрузка, резервное копирование)
Background Jobs → Storage Adapter	HTTP/HTTPS	S3 API	Совместимость с облачными хранилищами
Storage Adapter → Object Storage	S3 API	Binary / JSON	Стандартный протокол для объектного хранилища

Уровень	Что валидируется	Как
Frontend (WebApp)	Размер файла, тип MIME, расширение	JavaScript:file.type,file.name.endsWith('.jpg'), ограничение по размеру (например, 50 МБ)
API Gateway	Заголовки, токен авторизации, формат запроса	Проверка JWT, Content-Type, Content-Length, CORS
File Service (Controller/Service Layer)	Расширение, MIME-тип, сигнатура файла, антивирусный скан	Проверка через magic number(первые байты), вызов антивируса (ClamAV), блокировка.exe,.bat,.sh

Шаг 4: определяем взаимодействия



File Service — Component Diagram



CloudDrive — Container Diagram

