Токены и API

Константин Башевой
Аналитик-разработчик, Яндекс

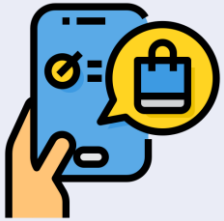
Почему данные API закрытые

API (application programming interface) – программный интерфейс приложения

Часто содержит конфиденциальные данные:

- данные о пользователях, их действиях
- данные о расходах и доходах проекта
- личные данные пользователя
- организация не хочет, чтобы ее данные быстро скачали

Запрос не обязательно от вас



Поиск
Ответы на любые вопросы

Картинки
Изображения всех цветов и размеров

Новости
Картина дня, созданная автоматически

Погода
Прогноз в вашем городе
и по всему миру

Почта
Электронный ящик без спама и вирусов

Маркет
Товары, сравнение цен,
отзывы покупателей

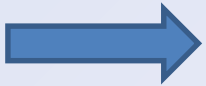
Афиша
Развлекательные мероприятия

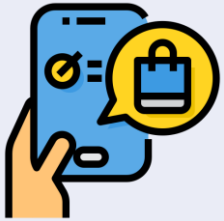
Такси
Свободные водители поблизости

Диск
Безопасное облако для ваших файлов

Недвижимость
Объявления о комнатах, квартирах
и домах

Запрос не обязательно от вас





Поиск
Ответы на любые вопросы

Картинки
Изображения всех цветов и размеров

Новости
Картина дня, созданная автоматически

Погода
Прогноз в вашем городе
и по всему миру

Почта
Электронный ящик без спама и вирусов

Маркет
Товары, сравнение цен,
отзывы покупателей

Афиша
Развлекательные мероприятия

Такси
Свободные водители поблизости

Диск
Безопасное облако для ваших файлов

Недвижимость
Объявления о комнатах, квартирах
и домах

Как защитить данные?

Использовать логин и пароль

Чем плохо:

- придется в запросе к системе передавать логин и пароль в открытом виде, видно чей он
- если приложение будет скомпрометировано, то придется много где менять пароль
- нельзя разделять права доступа на разные сценарии

Как защитить данные?

Использовать хэш от пароля

Что стало лучше:

- Хэш нельзя использовать для входа в аккаунт

Чем плохо:

- если приложение будет скомпрометировано, то придется много где менять этот хэш
- нельзя разделять права доступа на разные сценарии

Как делают на практике

Под каждую задачу – свое приложение

чтение статистики

загрузка фото

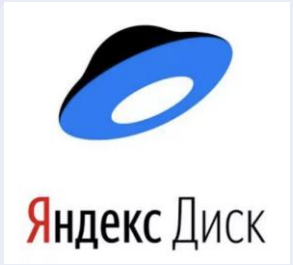
поиск организаций

Как делают на практике

Под каждую задачу – свое приложение

чтение статистики

загрузка фото



поиск организаций

Приложение может иметь сразу несколько разрешений

Набор приложений

Чем хорошо:

- **Каждое приложение будет иметь свой набор прав (чтение данных Метрики, загрузка файлов на Диск итд)**
- **В случае проблем доступы приложения можно обновить**
- **Каждое приложение имеет свои лимиты по запросам**
- **Доступы никак не задействуют ваш личный пароль**