

Описание процессов,
обеспечивающих поддержание
жизненного цикла
ПО «OpenAPI-микросервисы»

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ.....	3
1.1. НАЗНАЧЕНИЕ.....	3
1.2. ПОРЯДОК ДЕЙСТВИЯ	3
1.3. ТЕРМИНЫ И СОКРАЩЕНИЯ.....	3
2. ОБЩЕЕ ОПИСАНИЕ СИСТЕМЫ OPENAPI.....	4
2.1. ОРГАНИЗАЦИОННАЯ СТРУКТУРА ПОСТРОЕНИЯ СИСТЕМЫ OPENAPI	5
2.2. ОРГАНИЗАЦИОННАЯ СТРУКТУРА УПРАВЛЕНИЯ СИСТЕМЫ OPENAPI	5
2.2.1. Обязанности Пользователей системы OpenAPI	5
2.2.2. Обязанности Администраторов системы OpenAPI.....	5
2.3. ДОКУМЕНТАЛЬНОЕ ОБЕСПЕЧЕНИЕ ЭКСПЛУАТАЦИИ СИСТЕМЫ OPENAPI.....	6
2.4. ПЕРЕЧЕНЬ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В СИСТЕМЕ OPENAPI	6
3. ДОПУСК ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИОННЫМ РЕСУРСАМ СИСТЕМЫ OPENAPI	6
3.2. РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЯ	7
3.3. ИЗМЕНЕНИЕ ПРАВ ДОСТУПА ПОЛЬЗОВАТЕЛЯ.....	7
3.4. ПРЕКРАЩЕНИЕ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЯ	7
4. ВНЕСЕНИЕ ИЗМЕНЕНИЙ В СИСТЕМУ OPENAPI.....	7
4.1. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ	7
4.1.1. Модернизация системы OpenAPI включает:	7
4.1.2. Порядок подготовки к внесению изменений.	7
4.1.3. Порядок переноса изменений в рабочую схему.	8
5. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ И ОРГАНИЗАЦИИ НЕПРЕРЫВНОСТИ РАБОТЫ СИСТЕМЫ OPENAPI.....	8
5.1. ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ РАБОТЫ СИСТЕМЫ	8
5.2. ОБЕСПЕЧЕНИЕ РЕЗЕРВНОГО КОПИРОВАНИЯ	8
6. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	9

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение

Настоящий Документ определяет порядок осуществления деятельности должностных лиц Банка с использованием системы «OpenAPI-микросервисы» (далее – OpenAPI).

Настоящий Документ регламентирует права, обязанности и ответственность всех должностных лиц Банка, включая должностных лиц филиалов и других структурных подразделений, непосредственно использующих систему OpenAPI в процессе реализации своих должностных обязанностей.

Настоящий Документ относится к технологиям, системам и средствам обработки, передачи и хранения информации, используемым в рамках системы OpenAPI.

1.2. Порядок действия

Настоящий Документ, а также изменения и дополнения в него утверждаются уполномоченным органом Банка и вводятся в действие приказом по основной деятельности Банка.

В случае изменения действующего законодательства Российской Федерации, Устава Банка и до приведения настоящего Документа в соответствие таким изменениям, Документ считается действующим в части, им не противоречащей.

Настоящий Документ является внутренним документом Банка.

Настоящий Документ выступает основополагающим нормативным документом для всех внутренних нормативных документов Банка, касающихся функционирования системы OpenAPI и имеющих ссылку на настоящий Документ.

1.3. Термины и сокращения

«Банк» – ПАО «Совкомбанк», включая филиалы и внутренние структурные подразделения.

«Система OpenAPI» – Программно-аппаратный комплекс, предназначенный для предоставления внешним и внутренним потребителям унифицированного программного интерфейса (API) к банковским сервисам и данным.

«Документ» – настоящий Документ.

«Администратор системы» - привилегированный пользователь – сотрудник Банка, имеющий право настроек приложения, а также обладающий доступом ко всем информационным ресурсам системы OpenAPI.

«Пользователь (Разработчик API/Потребитель API)» – внутренний сотрудник или внешний интегратор, который получает доступ к системе OpenAPI через процедуру регистрации и использует API для интеграции с банковскими системами.

«Тестировщик» – специалист, занимающийся тестированием API-эндпоинтов, их функциональности, безопасности и производительности.

«Процедура регистрации» - последовательность действий, выполняемая Пользователем (Разработчиком/Интегратором) в целях получения ключей доступа (API-ключей) к ресурсам системы OpenAPI.

«Права доступа» – совокупность прав Пользователя на вызов определенных API-методов (эндпоинтов), объем, состав и период действия которых определяется на основании заявки в Системе регистрации заявок и политик безопасности.

«Система регистрации заявок» - программное обеспечение для регистрации заявок на внесение изменений в банковские системы, а также для фиксирования сообщений об ошибках, обнаруженных пользователями при работе в банковских информационных системах.

«Владелец продукта (Product Owner) API» - ответственное лицо из бизнес-подразделения, определяющее требования к API и приоритеты его развития.

2. ОБЩЕЕ ОПИСАНИЕ системы OpenAPI

Система OpenAPI предназначена:

Предоставить безопасный, стандартизированный и документированный интерфейс для интеграции внешних партнеров и внутренних систем с сервисами Банка.

Централизовать управление доступом, мониторингом и аналитикой использования API.

Обеспечить соблюдение политик безопасности, включая аутентификацию, авторизацию, ограничение частоты запросов (rate limiting) и шифрование трафика.

Ускорить процесс интеграции за счет предоставления документации и тестовой среды.

Абстрагировать внутреннюю сложность банковских систем от внешних потребителей.

В составе системы OpenAPI используется следующий набор компонентов:

API Gateway: Единая точка входа для всех API-запросов, отвечающая за маршрутизацию, трансформацию, безопасность и мониторинг.

Сервис проверки API-ключей по стандарту OAuth 2.0

Сервис мониторинга и аналитики: Сбор метрик использования, производительности и ошибок.

Бэкенд-сервисы (Backend Services): Фактические банковские системы (АБС, Фронт-ЮЛ и др.), к которым предоставляется доступ через API.

2.1. Организационная структура построения системы OpenAPI

Система допускает работу двух категорий пользователей: Администраторов и Пользователей.

Администраторы управляют системой и выполняют следующие действия:

- Регистрация и управление приложениями (клиентами API).
- Настройка политик безопасности на API Gateway (аутентификация, rate limiting).
- Публикация и версионирование документации API.
- Мониторинг состояния системы, просмотр логов и метрик.
- Управление жизненным циклом API-ключей и сертификатов.
- Проверка API-ключей (токенов).

Пользователи осуществляют вызовы API в соответствии со спецификацией.

2.2. Организационная структура управления системы OpenAPI

Организационная структура системы OpenAPI основана на четком разделении участников на привилегированных пользователей и Пользователей.

Привилегированными пользователями системы OpenAPI являются Администраторы системы. Остальные участники системы OpenAPI являются Пользователями (Разработчиками/Интеграторами).

2.2.1. Обязанности Пользователей системы OpenAPI

Использование API строго в соответствии с предоставленной документацией и условиями соглашения.

Обеспечение конфиденциальности полученных API-ключей и учетных данных.

Своевременное обновление интеграций при депрекации (устаревании) версий API.

Информирование Администратора системы о выявленных ошибках или уязвимостях через Систему регистрации заявок.

2.2.2. Обязанности Администраторов системы OpenAPI

Сопровождение и поддержание работоспособности API Gateway и смежных сервисов.

Настройка и конфигурация политик безопасности, маршрутизации и трансформации запросов.

Мониторинг производительности и доступности системы, реагирование на инциденты.

Публикация актуальной документации.

Участие в тестировании изменений после обновлений.

Взаимодействие с Департаментом информационной безопасности по вопросам защиты API.

2.3. Документальное обеспечение эксплуатации системы OpenAPI

Для обеспечения Пользователей инструктивными материалами, методологические подразделения банка выполняют разработку и утверждение:

Технических регламентов по использованию конкретных API.

Руководств по интеграции.

Политик использования API.

Эксплуатация OpenAPI выполняется в соответствии с регламентом на каждом рабочем месте Участника.

2.4. Перечень информации, обрабатываемой в системе OpenAPI

В рамках функционала системы обрабатываются:

Учетные данные и ключи доступа Пользователей (API-ключи).

Данные, передаваемые в запросах и ответах API, которые могут включать персональные данные клиентов Банка и сведения, относящиеся к банковской тайне (в зависимости от конкретного API).

Метрики и логи всех транзакций (время, эндпоинт, статус, идентификатор клиента).

3. ДОПУСК ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИОННЫМ РЕСУРСАМ системы OpenAPI

3.1. Получение прав Пользователя

Для получения доступа к API необходимо:

Регистрация (для внешних партнеров) или подача внутренней заявки (для сотрудников Банка).

Создание "Приложения" (Application) и получение пары ключей (Client ID / Client Secret).

Выбор необходимых API-продуктов (наборов эндпоинтов) и получение согласия на условия использования.

3.2. Регистрация Пользователя

Процедура регистрации инициируется Пользователем. Для внутренних сотрудников процедура инициируется руководителем подразделения через заявку в Системе регистрации заявок.

Администратор системы (или автоматизированный процесс) выполняет верификацию заявки, создает учетную запись и предоставляет доступы в соответствии с утвержденными политиками.

Заявка исполняется в срок, определенный регламентом (например, до 2 рабочих дней для внутренних заявок).

3.3. Изменение прав доступа Пользователя

В случае необходимости изменения набора доступных API (добавление/удаление эндпоинтов) или увеличения квот (rate limits) Пользователь/руководитель инициирует заявку в Системе регистрации заявок. Процедура аналогична процедуре регистрации.

3.4. Прекращение полномочий пользователя

Основанием для прекращения доступа является:

Заявка на отзыв доступа.

Нарушение условий использования API (политики безопасности, несанкционированная активность).

Прекращение договора с внешним партнером.

Администратор системы блокирует API-ключи и удаляет доступ приложения в системе.

4. ВНЕСЕНИЕ ИЗМЕНЕНИЙ В СИСТЕМУ OpenAPI

Доработка системы OpenAPI проводится для устранения ошибок, улучшения производительности, добавления новых API-методов или в связи с изменениями в бэкенд-системах.

4.1. Порядок внесения изменений

4.1.1. Модернизация системы OpenAPI включает:

Добавление новых или изменение существующих API-эндпоинтов.

Обновление документации.

Изменение политик безопасности или конфигурации API Gateway.

Реализация требований информационной безопасности.

4.1.2. Порядок подготовки к внесению изменений.

Владелец продукта API или бизнес-подразделение формирует заявку в «Системе регистрации заявок» на доработку.

Разработчики вносят изменения в код бэкенд-сервисов и/или конфигурацию API Gateway.

Изменения развертываются в тестовой среде (Sandbox).

Тестировщик совместно со специалистом функционального подразделения проводит тестирование: функциональное, интеграционное, нагрузочное и на безопасность.

Результаты тестирования фиксируются в заявке.

4.1.3. Порядок переноса изменений в рабочую схему.

После успешного тестирования Администратор системы планирует выкатку (deployment) в продуктивную среду.

Изменения переносятся в соответствии с утвержденным планом релиза, часто с использованием CI/CD пайплайнов.

Администратор проверяет работоспособность системы после обновления.

Публикуется обновленная документация.

Все заинтересованные Пользователи уведомляются об изменениях, особенно в случае депрекации старых версий API.

5. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ И ОРГАНИЗАЦИИ НЕПРЕРЫВНОСТИ РАБОТЫ СИСТЕМЫ OPENAPI

5.1. Обеспечение непрерывности работы системы

Непрерывность работы обеспечивается:

Отказоустойчивой архитектурой API Gateway (кластеризация, активный-активный режим).

Наличием резервной площадки (DR-сайта).

Использованием балансировщиков нагрузки (Load Balancer).

5.2. Обеспечение резервного копирования

Резервному копированию подлежат:

Конфигурации API Gateway.

Базы данных управления ключами и аналитики.

Документация.

Периодичность и порядок копирования осуществляются в соответствии с корпоративным положением об резервном копировании.

6. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Все пользователи обязаны соблюдать требования информационной безопасности:

Использовать только безопасные методы аутентификации (OAuth 2.0, JWT).

Никогда не передавать API-ключи в клиентский код или публичные репозитории.

Использовать HTTPS для всех вызовов API.

Следовать принципу минимальных привилегий при назначении прав доступа к API.

При обнаружении утечки ключа или подозрительной активности Пользователь обязан немедленно сообщить Администратору системы и в Департамент информационной безопасности. Ключи будут немедленно отозваны, а учетная запись заблокирована для расследования.