

ИНСТРУКЦИЯ ПО УСТАНОВКЕ  
ЭКЗЕМПЛЯРА ПО  
**FINIST GATEWAY OPERATIONS**

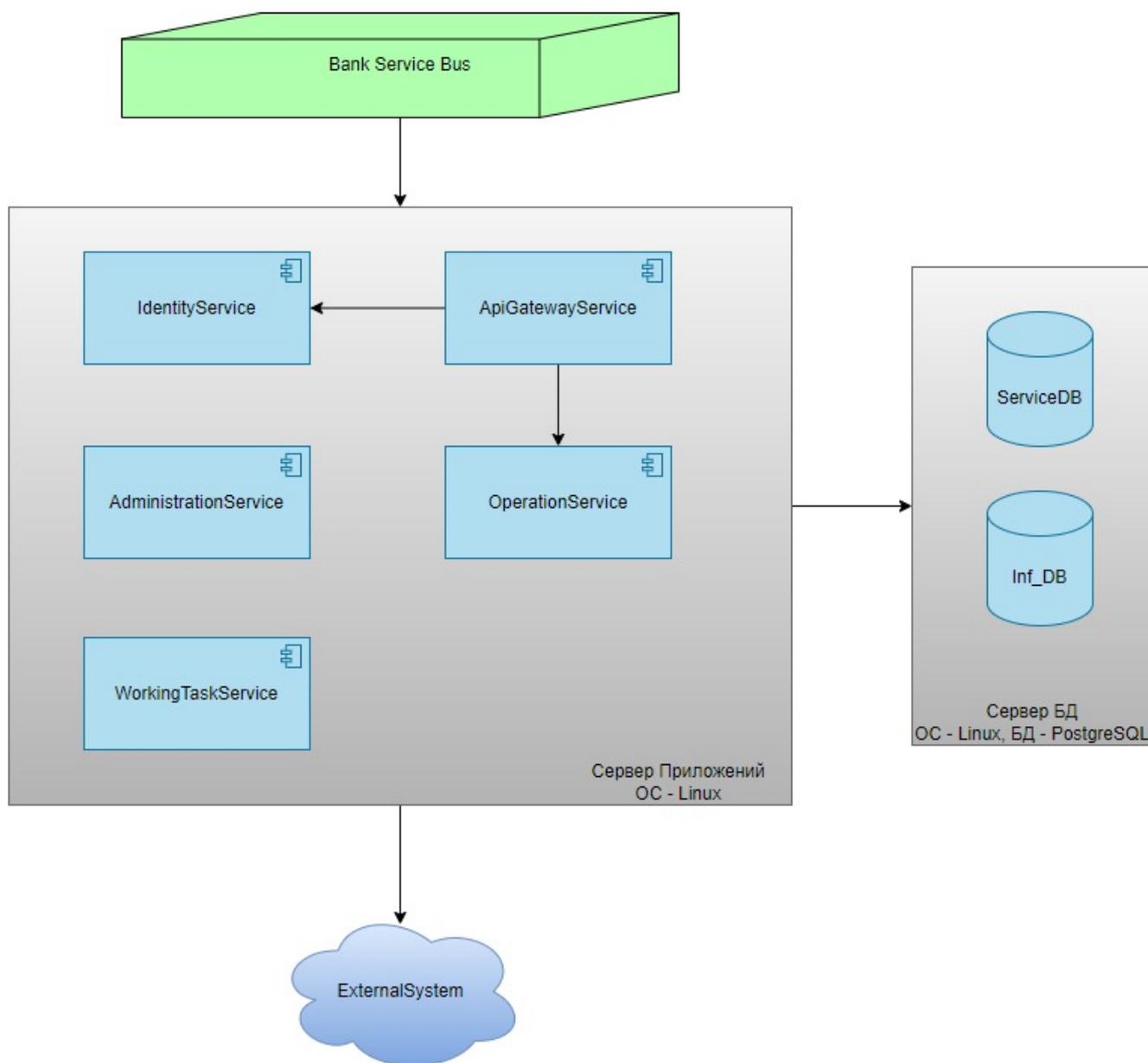
г. Казань, 2024

## Оглавление

Оглавление.....	2
1 Архитектура решения.....	3
2 Поставка.....	4
3 Предварительная настройка.....	4
4 Конфигурирование сервисов .....	4
4.1 Appsettings.json .....	4
4.1.1 HTTP/HTTPS .....	5
4.2 LDAP.....	7
4.3 Настройка веб-сервера, HTTPS.....	8
5 Проверка работоспособности .....	9
6 Проблемы, которые могут возникнуть .....	11
6.1 При авторизации по корректному логину/паролю ничего не происходит.....	11
6.2 При авторизации возникает ошибка 502 Bad gateway .....	11
6.3 При авторизации возникает ошибка 408 Request timeout.....	11
7 Технические требования .....	12
7.1 Требования к СУБД .....	12
7.1.1 Программное обеспечение СУБД .....	12
7.1.2 Аппаратное обеспечение сервера:.....	12
7.2 Требования к конфигурации сервера приложений .....	12
7.2.1 Программное обеспечение сервера .....	12
7.2.2 Аппаратное обеспечение сервера .....	12
7.3 Рабочая станция:.....	12
7.3.1 Программное обеспечение ОС рабочей станции.....	12
7.3.2 Аппаратное обеспечение рабочей станции .....	12

## 1 Архитектура решения

Finist gateway operations реализован на базе микросервисной архитектуры, с возможностью динамического подключения сервисов. Каждый из сервисов может быть горизонтально масштабирован для увеличения пропускной способности, а общий набор сервисов может быть масштабирован как вертикально, так и горизонтально для обеспечения отказоустойчивости и равномерного распределения возрастающей нагрузки.



**Архитектура Finist gateway operations (финансового шлюза) и взаимодействие с финансовыми и платежными системами**

## 2 Поставка

В поставке участвуют не менее пяти архивов:

- **APIGatewayService** – сервис динамической балансировки и маршрутизации сообщений.
- **WorkingTaskService** – сервис исполнения периодических задач.
- **OperationService** – сервис для интеграции с финансовыми и платежными системами. Например, Элекснет.
- **AdminService** – сервис для управления настройками и конфигурации интеграционного шлюза. Содержит в себе интерфейс администрирования (тонкий клиент).
- **IdentityService** – сервис для аутентификации и идентификации запросов, приходящих на APIGatewayService.

## 3 Предварительная настройка

Необходимо настроить учётные записи, под которыми будет осуществляться работа веб-приложения.

Учётная запись должна обладать правами уровня Администратора.

## 4 Конфигурирование сервисов

Каждым сервисом конфигурируется настройками в БД и файлом настроек *appsettings.json*.

### 4.1 Appsettings.json

```
{
  "AllowedHosts": "*",
  "Kestrel": {
    "EndpointDefaults": {
      "Protocols": "Http1AndHttp2"
    },
    "Endpoints": {
      "gRPC": {
        "Url": "https://localhost:5075",
        "Protocols": "Http1AndHttp2"
      }
    }
  },
  "MethodConfig": {
    "RetryMaxAttempts": 3,
    "MinDelayBackoff": 1,
    "MaxDelayBackoff": 5,
  }
}
```

```

    "BackoffMultiplier": 1.5
  },
  "JwtBearerTokenSettings": {
    "SecretKey": "secretKey@xxxxxxxxxxx@KJHA)UDYAS__",
    "Audience": "http://localhost:5143",
    "Issuer": "http://localhost:5143",
    "ExpiryTimeInSeconds": 360,
    "RefreshTokenExpiryInDays": 7
  },

  // Провайдер работы с БД. PsSQL - PostgreSQL; MsSQL - Microsoft SQL Server;
  "DatabaseProvider": "PsSQL",

  // InfrastructureDB - единая БД для работы с логами, метриками и настройками сервисов.
  "ConnectionStrings": {
    "InfrastructureDB":
    "Host=dev.domen.com;Port=5432;Database=Bank_InfrastructureDB;Username=postgres;Password=xxxxxx"
  }
}

```

Секция *AllowedHosts*:

Указываются адреса, с которых сервер принимает запросы.

Секция *Kestrel*:

*EndpointDefaults* – системная секция. Версия протокола общения gRPC.

*ServerOptions / Limits / MaxRequestBodySize* – Максимальный размер тела запроса, в байтах.

#### 4.1.1 HTTP/HTTPS

В секции *Endpoints* находятся настройки выставленных адресов для gRPC. **Url** – адрес, по которому будет осуществляться общение с сервером.

- **Http** – вариант адреса без сертификата.
- **Https** – вариант адреса с сертификатом. Настройки сертификата указываются в секции *Certificate*. В секции *Certificate* указывается путь (Параметр *Path*) до pfx-сертификата и пароль от сертификата (Параметр *Password*).

Секция *MethodConfig* – секция управления повторными вызовами при неуспешном обращении к другим сервисам.

- **RetryMaxAttempts** – Максимальное количество попыток вызова, включая исходную попытку
- **MinDelayBackoff** - Минимальное значение задержки
- **MaxDelayBackoff** - Максимальное значение задержки
- **BackoffMultiplier** - Задержка будет умножена на это значение после каждой повторной попытки и будет увеличиваться экспоненциально

Секция *JwtBearerTokenSettings* – секция настроек для обращения к IdentityService.

- **SecretKey** – секретный ключ на основе которого генерируется токен
- **Audience** - задает допустимое значение аудитории для полученного токена безопасности
- **Issuer** - строка, которая идентифицирует принципала, выдавшего JWT
- **ExpiryTimeInSeconds** – время жизни токена в секундах
- **RefreshTokenExpiryInDays** – Период обновления токена (в днях)

Секция *DatabaseProvider* – указывается тип провайдера для работы с БД.

Секция *ConnectionStrings* – указывается строка соединения с БД шлюза.

## 4.2 LDAP

В настройках, хранящихся в БД IdentityService есть возможность настроить LDAP сервер, для аутентификации пользователей через доменные учётные данные. LDAP серверов может быть несколько.

### Пример:

```
{
  "Ldap": {
    "Server": [
      {
        "GEstAuthentication": {
          "Bind": {
            "_dynamic": "true",
            "_dn": "uid=%%login%,ou=Users,dc=some_server,dc=com",
            "_password": "some_password"
          },
          "Search": {
            "_root": "dc=some_server,dc=com",
            "_filter": "(&(uid=%%login%)(objectClass=posixAccount))"
          }
        },
        "_key": "some_server",
        "_host": "some_server.com",
        "_port": "389",
        "_useSsl": "false",
        "_trustServerCertificate": "false",
        "_repeatedAuthenticationInterval": "0:10:0",
        "_authenticationType": "Basic",
        "_protocolVersion": "3",
        "_displayName": "Some server"
      },
      {
        "GEstAuthentication": {
          "Bind": {
            "_dynamic": "true",
            "_dn": "%%login%@domen.com"
          },
          "Search": {
            "_root": "dc=domen,dc=com",
            "_filter": "(&(sAMAccountName=%%login%)(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))"
          }
        },
        "_key": "finist",
        "_host": "bighead.domen.com",

```

```

        "_port": "389",
        "_useSsl": "false",
        "_trustServerCertificate": "false",
        "_repeatedAuthenticationInterval": "0:10:0",
        "_authenticationType": "Basic",
        "_protocolVersion": "3",
        "_displayName": "EsterDev (LDAP)"
    },
    {
        "GEstAuthentication": {
            "Bind": {
                "_dynamic": "true",
                "_dn": "uid=%login%,ou=Users,dc=ldaptest,dc=com"
            },
            "Search": {
                "_root": "dc=ldaptest,dc=com",
                "_filter": "(&(uid=%login%)(objectClass=posixAccount))"
            }
        },
        "_key": "ldaptest",
        "_host": "192.168.1.114",
        "_port": "389",
        "_useSsl": "false",
        "_trustServerCertificate": "false",
        "_repeatedAuthenticationInterval": "0:10:0",
        "_authenticationType": "Basic",
        "_protocolVersion": "3"
    }
}
]
}

```

### 4.3 Настройка веб-сервера, HTTPS

Для подписания веб-сайта сертификатом потребуется связка публичный сертификат и секретный ключ.

```

ssl_certificate      www.example.com.crt;
ssl_certificate_key  www.example.com.key;

```

Секретный ключ (`ssl_certificate_key`) необходимо хранить в файле с ограниченным доступом, но Nginx'у необходимы права для чтения на этот файл.

## 5 Проверка работоспособности

Открыть веб-браузер, ввести адрес машины/глобальный адрес машины, на которой развёрнут веб-сервер.

При корректной настройке веб-сервера/указания адреса – откроется стандартная форма логина. Вход в приложение можно осуществить при помощи связки логин (с доменом) + пароль, от windows-аккаунта, в случае, если настроен LDAP сервер.

Finist-Soft

Логин

Иванова.ТС

Пароль

\*\*\*\*\*

[Восстановить пароль](#)

[ВОЙТИ →](#)

[Нужна помощь?](#) [НАПИСАТЬ В ПОДДЕРЖКУ](#)

В форме указываем логин/пароль пользователя. Если всё настроено корректно, то откроется окно основной страницы приложения:

The screenshot displays the 'Parameters of the system' (Параметры системы) configuration page in the Finist-Soft application. The interface features a left-hand navigation menu and a main content area with three sections: 'Event Logs' (Журналы событий), 'Inter-service interaction' (Межсервисное взаимодействие), and 'Task parameters' (Настройки рабочих задач). A 'SAVE' (СОХРАНИТЬ) button is located at the bottom left, and a yellow warning box is positioned at the bottom center.

**Finist-Soft**

**Параметры системы**

- Главная
- Справочники
- Страница логов
- Просмотр метрик
- Параметры системы**
  - Управление состоянием сервисов
  - Параметры сервисов
  - Параметры рабочих задач
  - Параметры учетных записей
  - Настройки сервиса
  - Общие настройки шлюза**
- Сервисы
- Элекснет
- Компас+
- FinistRetail
- FinistABS
- ERetail
- История операций
- Редактирование системных ролей и прав
- Тест Тестович Тестов

**Журналы событий**

Уровень трассировки	Информация
Файловый лог	\\Users\gateway\eventlog
Строка подключения к БД	Host=pgserver;Port=5432;...

**Межсервисное взаимодействие**

Количество попыток запроса	3
Время ожидания ответа (в секундах)	30

**Настройки рабочих задач**

Период выполнения запросов типа Push (в секундах)	30
Период выполнения запросов типа Pull (в секундах)	30

**СОХРАНИТЬ**

**ВНИМАНИЕ!**  
Изменения вступят в силу после нажатия кнопки «СОХРАНИТЬ»

## **6 Проблемы, которые могут возникнуть**

### **6.1 При авторизации по корректному логину/паролю ничего не происходит.**

Если не возникло никаких дополнительных информационных сообщений, то, скорее всего, дело в том, что был добавлен новый логин для пользователя/пользователь. В таком случае, система безопасности не перезагружена и сервер-приложение не знает о новом логине пользователя.

### **6.2 При авторизации возникает ошибка 502 Bad gateway**

Одно из возможных решений - проверить настройку веб-сервера. Корректно ли он перенаправляет запросы.

Если запросы перенаправляются корректно, то, возможно, ошибка в настройке веб-приложения.

### **6.3 При авторизации возникает ошибка 408 Request timeout**

Необходимо убедиться, что веб-приложение корректно настроено на сервер-приложение. Так же, проверить, что сервер-приложение запущено и работает.

## 7 Технические требования

### 7.1 Требования к СУБД

#### 7.1.1 Программное обеспечение СУБД

- PostgreSQL - рекомендуется устанавливать только для ОС на базе Linux:
- PostgreSQL от версии 15;
- pgAdmin IV

#### 7.1.2 Аппаратное обеспечение сервера:

- Процессор: x86-совместимый 64-разрядный (Intel, AMD); 8 ядер с частотой от 2 ГГц.
- Оперативная память: 64ГБ.
- Дисковая подсистема: от 400 ГБ.

Канала связи: от 100 Mbit/sec, при кол-ве пользователей более 50 рекомендуется от 1000 Mbit/sec.

### 7.2 Требования к конфигурации сервера приложений

#### 7.2.1 Программное обеспечение сервера

- Linux, поддерживающий .Net 6.0:
- Nginx версия не ниже 1.12
- Необходимо установить пакеты libcsb-dev и libgdipplus
- .Net 6.0

#### 7.2.2 Аппаратное обеспечение сервера

- Основные требования к аппаратному обеспечению вытекают из требований используемой версии ОС и СУБД.
- Процессор: x86-совместимый 64-разрядный (Intel, AMD); 8 ядер с частотой от 2 ГГц.
- Оперативная память: 32ГБ.
- Дисковая подсистема: от 200 ГБ.

### 7.3 Рабочая станция:

#### 7.3.1 Программное обеспечение ОС рабочей станции

- Браузер (тонкий клиент) на базе платформы Chromium;

#### 7.3.2 Аппаратное обеспечение рабочей станции

Основные требования к аппаратному обеспечению вытекают из требований используемой версии ОС.

- Процессор: x86-совместимый 64-разрядный (Intel, AMD).

- Оперативная память: от 16Gb
- Разрешение монитора: 1920x1080 и выше

Для выполнения операций, требующих больших вычислительных ресурсов, таких как импорт / экспорт данных или получение сложных отчетных форм, рекомендуется использовать более мощные рабочие станции с характеристиками выше рекомендуемых.