Нейроключ — Руководство по установке и настройке

Содержание

1. Обзор системы
2. Аппаратные требования
3. Требования к установке
4. Этапы установки
5. Настройка и проверка

1. Общие сведения

1.1 Назначение документа

Настоящий документ представляет собой руководство по установке и настройке аппаратурно-программного комплекса **Нейроключ** (комплексы **G2R Data Handling Gateway**, фотовитрин распознавания лиц и прочих комплексов с ОСнСр компонентом, использующих распознавание лиц).

1.2 Архитектура решения

Интегрированная платформа состоит из двух основных подсистем:

- **Нейроключ** — серверная часть на базе фреймворка Promtech на Ruby 2.6, Sinatra (на Rubyfox Pure65, PostgreSQL, Redis)
- **G2R Data Handling Gateway** — прокси-сервер для аппаратно-программных комплексов, разворачиваемый на двух аппаратных платформах:

Аппаратная платформа 1:

- **Контур В (доверенный)** — Astra Linux Common Edition, обработка запросов, взаимодействует только с Нейроключом и СУП приложением;
- **Контур Г (шлюзовый)** — Astra Linux Special Edition с ограниченным сетевым стеком. Перехватывает данные обращающиеся только внутри этого контура.

Аппаратная платформа 2:

- **Контур Д (изолированный)** — Astra Linux Special Edition, обработка запросов, взаимодействует только с Нейроключом и СУП приложением.
- **Контур Е (шлюзовый)** — Astra Linux Special Edition, прокси-сервер, разворачивается на двух аппаратных платформах

1.3 Технологический стек

Компонент	Версия	Назначение
Nginx	1.20.1	Обратный прокси, SSL-терминация
Puma	6.4.0	Ruby-сервер приложений
Sinatra	2.2.4	Веб-фреймворк
Ruby	2.6.10	Интерпретатор
PostgreSQL	9.6	Основная база данных
Redis	7.0.11	Кэш, очереди задач
Sidekiq	6.5.12	Фоновые задачи
Sidekiq-cron	1.2	Расписание задач
Sidekiq-unique-jobs	7.1.29	Уникальные задачи
Sidekiq-pro	5.0.2	Расширенные возможности Sidekiq
Sidekiq-ent	1.0.0	Enterprise-функции Sidekiq
Sidekiq-cron-ui	0.4.0	Веб-интерфейс для cron-задач
Sidekiq-unique-jobs-web	7.1.29	Веб-интерфейс уникальных задач
Sidekiq-pro-web	5.0.2	Веб-интерфейс Sidekiq Pro
Sidekiq-ent-web	1.0.0	Веб-интерфейс Sidekiq Enterprise
Sinatra-contrib	2.2.4	Расширения Sinatra
Sinatra-cookies	0.1.0	Работа с cookies
Sinatra-cookies-ui	0.1.0	Веб-интерфейс для cookies
Sinatra-sessions	0.3.0	Сессии
Sinatra-sessions-ui	0.3.0	Веб-интерфейс для сессий
Sinatra-activerecord	5.3.0	ORM для Sinatra
Sinatra-activerecord-ui	0.1.0	Веб-интерфейс для ORM
Sinatra-cache	0.4.1.2	Кэширование
Sinatra-cache-ui	0.1.0	Веб-интерфейс кэша
Sinatra-cache-redis	0.4.1.2	Redis-кэш
Sinatra-cache-redis-ui	0.1.0	Веб-интерфейс Redis-кэша
Sinatra-cache-memcache	0.4.1.2	Memcached-кэш
Sinatra-cache-memcache-ui	0.1.0	Веб-интерфейс Memcached
Sinatra-cache-memcache-kit	0.1.0	Утилиты Memcached
Sinatra-cache-memcache-kit-ui	0.1.0	Веб-интерфейс утилит Memcached
Sinatra-cache-memcache-multi	0.1.0	Multi-Memcached
Sinatra-cache-memcache-multi-ui	0.1.0	Веб-интерфейс Multi-Memcached
Sinatra-cache-memcache-multi-kit	0.1.0	Утилиты Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui	0.1.0	Веб-интерфейс утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui-ui	0.1.0	Веб-интерфейс веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса веб-интерфейса утилит Multi-Memcached
Sinatra-cache-memcache-multi-kit-ui

Latency LLM	Gateway	Время ответа LLM-провайдера (p50 / p95 / p99)
PII обнаружено	Gateway	Количество обнаруженных PII по типам сущностей
Запросы заблокированы	Gateway	Количество запросов, отклонённых политикой BLOCK
Кредиты	Нейроключ	Потребление кредитов по организациям
Redis Memory	Redis	Использование памяти (protected и operational)
Kafka Lag	Apache Kafka	Отставание потребителей от продюсеров
Error Rate	Все сервисы	Процент ошибочных ответов (5xx)

Рекомендуемые пороги алертов

Алерт	Условие	Уровень
High Error Rate	error_rate > 5% за 5 мин	Critical
High Latency	p99 latency > 5s за 5 мин	Warning
NER Service Down	Все экземпляры NER недоступны	Critical
Redis Memory	Использование > 80%	Warning
Kafka Lag	Consumer lag > 10000	Warning
Low Credits	Баланс организации < 10%	Info

5.4 Устранение неполадок при установке

Проблема: NER-сервис не запускается или OOM Killed

Симптомы: контейнер NER-сервиса завершается с кодом 137 (OOM) или не может загрузить модель.

Причина: недостаточно оперативной памяти. Каждый экземпляр NER-сервиса требует **минимум 5 ГБ RAM** для загрузки модели DeepPavlov.

Решение:

```
# Проверить лимиты памяти контейнера
docker stats ner-service-1

# Увеличить лимит в docker-compose.yml:
# services:
#   ner-service:
#     deploy:
#       resources:
#         limits:
#           memory: 6G
#         reservations:
#           memory: 5G

# Если RAM на сервере ограничена — уменьшить число реплик до 1
```

Проблема: Redis — ошибка подключения

Симптомы: `RedisConnectionException: Unable to connect to Redis` в логах Gateway.

Решение:

```
# 1. Проверить, что Redis запущен
docker ps | grep redis

# 2. Проверить доступность
docker exec -it redis-protected redis-cli -a <password> ping
# Ожидаемый ответ: PONG

# 3. Проверить переменные окружения
# REDIS_HOST, REDIS_PORT, REDIS_PASSWORD должны совпадать

# 4. Проверить сетевую связность (Docker network)
docker network inspect <network-name>
```

Проблема: mTLS — ошибка рукопожатия

Симптомы: `SSLHandshakeException` при обращении External Gateway к Internal Gateway.

Решение:

```
# 1. Проверить сертификаты
openssl s_client -connect internal-gateway:8443 \
  -cert client-cert.pem -key client-key.pem -CAfile ca-cert.pem

# 2. Убедиться, что:
#    - Клиентский сертификат подписан тем же CA
#    - CN клиентского сертификата совпадает с ожидаемым
#    - Сертификаты не истекли
openssl x509 -in client-cert.pem -noout -dates
openssl x509 -in server-cert.pem -noout -dates

# 3. Проверить формат хранилища ключей (PKCS12)
keytool -list -keystore keystore.p12 -storetype PKCS12
```

Проблема: Gateway — 502 Bad Gateway

Симптомы: NGINX возвращает 502 при обращении к Gateway.

Решение:

```
# 1. Проверить, что External Gateway запущен
docker ps | grep external-gateway

# 2. Проверить health endpoint
curl -s http://localhost:8080/actuator/health | jq .

# 3. Проверить логи на ошибки
docker logs external-gateway --tail 100

# 4. Проверить конфигурацию NGINX upstream
# nginx.conf: proxy_pass http://external-gateway:8080;
```

Проблема: LLM не отвечает или таймаут

Симптомы: запросы к LLM завершаются таймаутом (`504 Gateway Timeout`).

Решение:

```
# 1. Проверить исходящий доступ к LLM-провайдерам
curl -s https://openrouter.ai/api/v1/models | head -c 200

# 2. Проверить API-ключ
curl -s https://openrouter.ai/api/v1/models \
  -H "Authorization: Bearer sk-or-..." | jq '.data | length'

# 3. Увеличить таймауты в конфигурации Gateway
# GATEWAY_LLM_TIMEOUT=120s (по умолчанию 60s)

# 4. Проверить firewall / proxy для исходящих подключений
```

Проблема: Маскирование не работает

Симптомы: персональные данные передаются в LLM без маскирования.

Решение:

```
# 1. Проверить, что Internal Gateway доступен
curl -sk https://internal-gateway:8443/actuator/health | jq .

# 2. Проверить, что NER-сервис работает
curl -s http://ner-service-1:8090/health | jq .

# 3. Тестировать NER напрямую
curl -X POST http://ner-service-1:8090/ner \
  -H "Content-Type: application/json" \
  -d '{"text": "Иванов Пётр, СНИЛС 123-456-789 00"}'

# 4. Проверить политики маскирования
curl -s http://localhost:8080/admin/policies \
  -H "Authorization: Bearer <admin-token>" | jq .

# 5. Проверить, что запросы от Нейроключа идут через Gateway
# (OPENROUTER_API_BASE_URL должен указывать на Gateway)
```

Проблема: Kafka — ошибка продюсера

Симптомы: `KafkaProducerException` в логах External Gateway.

Решение:

```
# 1. Проверить статус Kafka
docker logs kafka --tail 50

# 2. Проверить топики
docker exec -it kafka kafka-topics.sh --bootstrap-server localhost:9092 --list

# 3. При необходимости пересоздать топики
docker exec -it kafka kafka-topics.sh --bootstrap-server localhost:9092 \
  --create --topic masking-events --partitions 3 --replication-factor 1
```

Проблема: PostgreSQL — нехватка подключений

Симптомы: `FATAL: too many connections` в логах PostgreSQL.

Решение:

```
# 1. Проверить текущее число подключений
docker exec -it neurokey-postgres psql -U neurokey -c \
  "SELECT count(*) FROM pg_stat_activity;"

# 2. Увеличить max_connections
# В postgresql.conf или через переменную окружения:
# POSTGRES_MAX_CONNECTIONS=200

# 3. Настроить connection pooling (PgBouncer)
```

5.5 Расположение логов

Компонент	Расположение логов	Команда просмотра
Нейроключ Backend	stdout контейнера	`docker logs neurokey-backend -f`
Нейроключ Frontend	stdout контейнера	`docker logs neurokey-frontend -f`
External Gateway	`/app/logs/gateway.log` + stdout	`docker logs external-gateway -f`
Internal Gateway	`/app/logs/gateway.log` + stdout	`docker logs internal-gateway -f`
NER Service	stdout контейнера	`docker logs ner-service-1 -f`
PostgreSQL	`/var/lib/postgresql/data/log/`	`docker logs neurokey-postgres -f`
Redis	stdout контейнера	`docker logs redis-protected -f`
Apache Kafka	`/var/log/kafka/`	`docker logs kafka -f`
NGINX	`/var/log/nginx/`	`docker logs nginx -f`

5.6 Контакты технической поддержки

При возникновении проблем, не описанных в данном разделе:

- **Внутренний трекер** — создайте тикет в системе управления задачами проекта
- **Логи** — приложите к обращению логи всех затронутых компонентов (последние 500 строк)
- **Воспроизведение** — опишите шаги для воспроизведения проблемы
- **Окружение** — укажите версии компонентов (`docker compose version`, `java --version`, etc.)