

## Отчет

1. Добавляем дополнительный контейнер для расшифровки файла секретов. Создаем папку /env, которую будем загружать во все контейнеры, чтобы у них был доступ к ключам.

### Листинг 1 - Код docker-compose.yml.

```
services:
  decrypt:
    image: python:3.9-slim
    container_name: decrypt_env
    volumes:
      - ./env:/app/env
    working_dir: /app/env
    command: bash -c "
      ls -la
      && source vault-pass.env
      && pip install ansible-vault
      && echo $$VAULT_PASSWORD > vault-pass.txt
      &&          ansible-vault          decrypt          secrets.env
--vault-password-file vault-pass.txt --output .env
      && rm -rf vault-pass.txt"
  web:
    build: .
    container_name: web
    depends_on:
      redis:
        condition: service_healthy
      decrypt:
        condition: service_completed_successfully
    volumes:
      - ./env:/app/env
    command: bash -c "
      ls -la
      && python src/preprocess.py
      && python src/train.py
      && python src/predict.py -m LOG_REG -t func
```

```

    && coverage run src/unit_tests/test_preprocess.py
    && coverage run -a src/unit_tests/test_training.py
    && coverage run -a src/unit_tests/test_database.py
    && coverage run -a src/unit_tests/test_app.py
    && coverage report -m
    && (python src/app.py --model LOG_REG &)
    && sleep 30
    && curl -X GET http://localhost:8000/
    && curl -X POST http://localhost:8000/predict \
        -H 'Content-Type':" application/json' \
        --data-binary @tests/test_0.json"
ports:
  - 8000:8000
image: zarus03/ml-big-data-lab-3:latest
redis:
image: redis:latest
container_name: redis_db
depends_on:
  decrypt:
    condition: service_completed_successfully
volumes:
  - ./env:/app/env
working_dir: /app/env
command: bash -c "
    ls -la
    && source .env
    && redis-server --requirepass $$REDIS_PASSWORD"
ports:
  - 6379:6379
healthcheck:
  test: ["CMD", "bash", "-c", "
    cd /app/env
    && source .env
    && redis-cli -a $$REDIS_PASSWORD ping"]
  interval: 1s
  timeout: 2s
  retries: 10

```

2. Пишем пароль для расшифровки в файл и копируем его на этапе CI Pipeline.

#### Листинг 5 -Копирование файла секретов в сборку.

```
stage('Use .env File') {  
    steps {  
        withCredentials([file(  
            credentialsId: 'vault-pass',  
            variable: 'VAULT_PASS')]) {  
            bat 'xcopy /F %VAULT_PASS% %REPO_DIR%\\env'  
        }  
    }  
}
```