

# ИНСТРУКЦИЯ ПО УСТАНОВКЕ

## СИСТЕМА УПРАВЛЕНИЯ ИТ-АКТИВАМИ A-TRACKER

Подготовлено: ITAM2ru  
Версия: 4.0  
Дата версии: 09.02.2022  
Листов: 25

## ОГЛАВЛЕНИЕ

1. Требования к аппаратному и программному обеспечению .....	3
2. Описание дистрибутива системы A-Tracker .....	4
3. Общий порядок выполнения установки системы A-Tracker .....	5
4. Настройка сервера СУБД.....	6
4.1 Подготовка .....	6
4.2 Установка PostgreSQL .....	6
4.3 Настройка доступа к СУБД .....	7
4.4 Пароль суперпользователя postgres.....	8
4.5 Создание базы данных ATRACKER .....	8
4.6 Восстановление базы данных из резервной копии .....	9
5. Настройка сервера приложений .....	10
5.1 Установка NGINX.....	10
5.2 Настройка HTTPS.....	10
5.3 Установка DOTNET и зависимостей .....	17
5.4 Установка приложения A-TRACKER .....	18
6. Настройка параметров приложения A-Tracker .....	21
6.1 Файл лицензии .....	21
6.2 Файл конфигураций .....	21
6.3 Настройка точки подключения .....	22
6.4 Настройка подключения к базе данных.....	22
7. Настройка отправки уведомлений.....	23
8. Настройка аутентификации с использованием MS Active Directory.....	23
9. Настройка двухфакторной аутентификации для всех пользователей .....	25
10. Пароль Администратора A-Tracker .....	27

## 1. ТРЕБОВАНИЯ К АППАРАТНОМУ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

Перед установкой системы A-Tracker необходимо удостовериться, что выполняются требования к аппаратному обеспечению и системному ПО, описанные в документе «Требования к серверам».

## 2. ОПИСАНИЕ ДИСТРИБУТИВА СИСТЕМЫ A-TRACKER

В состав дистрибутива системы A-Tracker входят следующие компоненты:

Компонент	Описание
<b>database.sql</b>	Бэкап базы данных, который необходимо восстановить на сервере СУБД PostgreSQL.
<b>A-Tracker.zip</b>	Архив с приложением A-Tracker, который (в распакованном виде) используется на Web-сервере.
<b>ITAM2RU_Documentation.rar</b>	Документация к системе A-Tracker
<b>lic-&lt;Date&gt;.txt</b>	Файл с лицензией системы A-Tracker. Лицензия выдается на определенный срок и привязана к имени сервера, на котором развернуто приложение A-Tracker

### 3. ОБЩИЙ ПОРЯДОК ВЫПОЛНЕНИЯ УСТАНОВКИ СИСТЕМЫ A-TRACKER

Выполнение установки и настройки системы A-Tracker предпочтительно выполнять в следующем порядке:

1. На сервере базы данных выполнить установку PostgreSQL
2. Создать новую базу данных под A-Tracker
3. Восстановить новую базу данных из backup
4. На сервере приложений выполнить установку NGINX
5. На сервере приложений выполнить установку .Net и зависимостей
6. Создать и настроить приложение A-Tracker на Web-сервере
7. Настроить параметры подключения к SMTP-серверу для возможности отправки уведомлений
8. Если требуется, настроить параметры подключения к серверу MS Active Directory

## 4. НАСТРОЙКА СЕРВЕРА СУБД<sup>1</sup>

### 4.1 ПРЕДПОДГОТОВКА

#### 4.1.1 Перед началом установки проверьте, установлена ли в системе кодировка ru-RU UTF-8.

```
# Проверка, установлена ли в системе locale ru_RU.UTF-8
# В противном случае, возможны проблемы с кодировкой в базе PostgreSQL
locale -a
```

#### 4.1.2 Если кодировка отсутствует, добавьте ее.

```
# Если в списке кодировок нет ru_RU.UTF-8
sudo locale-gen ru_RU.UTF-8

# В открывшемся окне необходимо нажать дважды на enter
sudo dpkg-reconfigure locales
```

### 4.2 УСТАНОВКА POSTGRESQL

#### 4.2.1 Для начала установки обновите существующие в системе пакеты и установите необходимые компоненты PostgreSQL.

```
# Устанавливаем PostgreSQL
- Для менеджера пакетов APT
sudo sh -c 'echo "deb http://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg
main" > /etc/apt/sources.list.d/pgdg.list'
wget --quiet -O - https://www.postgresql.org/media/keys/ACCC4CF8.asc | sudo apt-key add
-
sudo apt-get update
sudo apt-get install postgresql13 postgresql13-contrib postgresql13-server
- Для менеджера пакетов DNF
sudo dnf install -y https://download.postgresql.org/pub/repos/yum/reporepms/F-34-
x86_64/pgdg-fedora-repo-latest.noarch.rpm
sudo dnf update
sudo dnf install postgresql13 postgresql13-contrib postgresql13-server
- Для менеджера пакетов YUM
sudo yum install -y https://download.postgresql.org/pub/repos/yum/reporepms/EL-7-
x86_64/pgdg-redhat-repo-latest.noarch.rpm
sudo yum update
sudo yum install postgresql13 postgresql13-contrib postgresql13-server
```

#### 4.2.2 Для продолжения настройки требуется инициализация базы данных, прежде чем можно будет запустить службу.

```
# Инициализация базы данных
sudo /usr/pgsql-13/bin/postgresql-13-setup initdb
```

Основная конфигурация базы данных записывается в файл:  
`/var/lib/pgsql/13/data/postgresql.conf`

<sup>1</sup> Инструкция написана для PostgreSQL версии 13. Для других версий PostgreSQL необходимо, как минимум перепроверять пути.

#### 4.2.3 Для запуска и включения службы сервера базы данных выполните команду:

```
# Запуск и включение службы
```

```
sudo systemctl enable --now postgresql-13
```

```
[admin@home-redos-db01 ~]$ sudo systemctl enable --now postgresql-13
[sudo] пароль для admin:
Created symlink /etc/systemd/system/multi-user.target.wants/postgresql-13.service → /usr/lib/systemd/system/postgresql-13.service.
```

#### 4.2.4 Необходимо убедиться в отсутствии ошибок в работе службы PostgreSQL.

```
# Проверка состояния службы
```

```
systemctl status postgresql-13
```

```
[admin@home-redos-db01 ~]$ systemctl status postgresql-13
● postgresql-13.service - PostgreSQL 13 database server
   Loaded: loaded (/usr/lib/systemd/system/postgresql-13.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2022-02-02 09:53:27 MSK; 8min ago
     Docs: https://www.postgresql.org/docs/13/static/
    Process: 1150 ExecStartPre=/usr/pgsql-13/bin/postgresql-13-check-db-dir %!(PGDATA) (code=exited, status=0/SUCCESS)
   Main PID: 1150 (postmaster)
      Tasks: 0 (limit: 2252)
     Memory: 33.9M
          CPU: 244ms
   CGroup: /system.slice/postgresql-13.service
           └─1150 /usr/pgsql-13/bin/postmaster -D /var/lib/pgsql/13/data/
             └─1151 postgres: logger
               └─1153 postgres: checkpointer
                 └─1154 postgres: background writer
                   └─1155 postgres: walwriter
                     └─1156 postgres: autovacuum launcher
                       └─1157 postgres: stats collector
                         └─1158 postgres: logical replication launcher

feb 02 09:53:25 home-redos-db01.localdomain systemd[1]: Starting PostgreSQL 13 database server...
feb 02 09:53:26 home-redos-db01.localdomain postmaster[1150]: 2022-02-02 09:53:26.125 MSK [1150] СООБЩЕНИЕ: передача вывода в протокол процессу сбора протоколов
feb 02 09:53:26 home-redos-db01.localdomain postmaster[1150]: 2022-02-02 09:53:26.125 MSK [1150] ПОДСКАЗКА: В дальнейшем протоколы будут выводиться в каталог "log".
feb 02 09:53:27 home-redos-db01.localdomain systemd[1]: Started PostgreSQL 13 database server.
```

### НАСТРОЙКА ДОСТУПА К СУБД

#### 4.2.5 Для настройки интерфейсов, с которых сервер будет принимать подключения, отредактируйте файл `/var/lib/pgsql/13/data/postgresql.conf` и укажите конкретный IP-адрес вашего сервера или « \* » для прослушивания всех интерфейсов.

```
# Открываем текстовый редактор
```

```
sudo nano /var/lib/pgsql/13/data/postgresql.conf
```

```
# Устанавливаем значение '*'
```

```
listen_addresses = '*'
```

```
# или конкретное значение IP-адреса:
```

```
listen_addresses = '192.168.1.7'
```

```
-----
# CONNECTIONS AND AUTHENTICATION
-----

# - Connection Settings -

listen_addresses = '192.168.1.7'           # what IP address(es) to listen on;
                                           # comma-separated list of addresses;
                                           # defaults to 'localhost'; use '*' for all
                                           # (change requires restart)
```

#### 4.2.6 Для настройки адресов, от которых сервер будет принимать запросы на удаленное подключение, необходимо отредактировать файл `/var/lib/pgsql/13/data/pg_hba.conf`, разрешив доступ из всех источников или только из конкретной подсети.

```
# Открываем текстовый редактор
sudo nano /var/lib/pgsql/13/data/pg_hba.conf

# Разрешаем доступ из всех источников
host all all 0.0.0.0/0 md5

# или из конкретной подсети:
host all all 192.168.1.0/24 md5
```

```
# IPv4 local connections:
host      all             all             127.0.0.1/32     scram-sha-256
host      all             all             192.168.1.0/24   md5
```

#### 4.2.7 После внесения изменений необходимо перезапустить службу базы данных.

```
# Перезагружаем службу
sudo systemctl restart postgresql-13
```

### 4.3 ПАРОЛЬ СУПЕРПОЛЬЗОВАТЕЛЯ POSTGRES

Для работы с базой данных требует создать пароль администратора СУБД PostgreSQL.

```
# Переключаемся в контекст пользователя postgres
sudo su - postgres

# Задаем пароль для пользователя postgres
psql -c "alter user postgres with password 'P@ssw0rd'"
```

```
[admin@home-redos-db01 ~]$ sudo su - postgres
[postgres@home-redos-db01 ~]$ psql -c "alter user postgres with password 'P@ssw0rd'"
ALTER ROLE
[postgres@home-redos-db01 ~]$ exit
ВЫХОД
[admin@home-redos-db01 ~]$
```

### 4.4 СОЗДАНИЕ БАЗЫ ДАННЫХ ATRACKER

Для создания базы данных необходимо подключиться к СУБД к с помощью утилиты `psql`, или альтернативного инструмента (например, `pgAdmin`), под пользователем `postgres` и выполнить следующие запросы:

#### 4.4.1 Создание базы данных:

```
-- Создать базу данных
CREATE DATABASE "atracker"
ENCODING 'UTF-8'
LC_COLLATE 'ru_RU.UTF-8'
LC_CTYPE 'ru_RU.UTF-8'
TEMPLATE template0;
```

```
[postgres@home-redos-db01 ~]$ psql
psql (13.5)
Введите "help", чтобы получить справку.

postgres=# CREATE DATABASE "atracker" ENCODING 'UTF-8' LC_COLLATE 'ru_RU.UTF-8' LC_CTYPE 'ru_RU.UTF-8' TEMPLATE template0;
CREATE DATABASE
```

#### 4.4.2 Создание пользователя и назначение прав

-- Создание пользователя

```
CREATE USER "atracker" WITH encrypted password '1234567890';  
GRANT ALL privileges ON DATABASE "atracker" TO "atracker";
```

```
postgres=# CREATE USER "atracker" WITH encrypted password '1234567890';  
CREATE ROLE  
postgres=# GRANT ALL privileges ON DATABASE "atracker" TO "atracker";  
GRANT
```

-- Предоставление пользователю прав на базу данных

```
ALTER USER "atracker" CREATEDB;  
ALTER DATABASE "atracker" OWNER TO "atracker";
```

```
postgres=# ALTER USER "atracker" CREATEDB;  
ALTER ROLE  
postgres=# ALTER DATABASE "atracker" OWNER TO "atracker";  
ALTER DATABASE  
postgres=# █
```

ВНИМАНИЕ: рекомендуется использовать одинаковые имя пользователя БД и имя БД.

#### 4.4.3 Если необходимо удалить базу данных или пользователя используйте следующие команды:

-- Удаление базы данных

```
DROP DATABASE "atracker";
```

-- Удаление пользователя

```
DROP USER "atracker";
```

### 4.5 ВОССТАНОВЛЕНИЕ БАЗЫ ДАННЫХ ИЗ РЕЗЕРВНОЙ КОПИИ

В составе поставки A-Tracker идёт файл **database.sql** с резервной копией базы данных A-Tracker с предварительно настроенной структурой данных и демонстрационными данными.

#### 4.5.1 Скопируйте файл **database.sql** в папку **/tmp/** с помощью утилиты **WinSCP** или альтернативного решения.

#### 4.5.2 Для восстановления содержимого резервной копии в базу **atracker** воспользуйтесь следующей командой с правами суперпользователя **postgres**:

```
# Вход в контекст пользователя postgres  
sudo su - postgres  
  
# Запись содержимого в базу данных atracker  
psql "atracker" < "/tmp/database.sql"
```

## 5. НАСТРОЙКА СЕРВЕРА ПРИЛОЖЕНИЙ

### 5.1 УСТАНОВКА NGINX

Для начала установки обновите существующие в системе пакеты и установите пакет **nginx**.

```
# Устанавливаем веб-сервера NGINX
- Для менеджера пакетов APT
sudo apt-get update
sudo apt-get install nginx
- Для менеджера пакетов DNF
sudo DNF update
sudo DNF install nginx
- Для менеджера пакетов YUM
sudo YUM update
sudo YUM install nginx
```

### 5.2 НАСТРОЙКА HTTPS

#### 5.2.1 В начале настройки необходимо создать ключ для настройки протокола шифрования Диффи — Хеллмана (если ранее не был настроен).

```
# Создание ключа Diffie-Hellman
sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048
```

```
[admin@home-redos-app01 ~]$ sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem
2048
[sudo] пароль для admin:
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....+++++*++++*++++*
[admin@home-redos-app01 ~]$
```

#### 5.2.2 Далее, необходимо создать файл с настройками протокола шифрования SSL.

```
# Создание директории snippets.
mkdir /etc/nginx/snippets

# Создание файла с параметрами SSL.
sudo nano /etc/nginx/snippets/ssl-params.conf
```

```
[admin@home-redos-app01 /]$ sudo mkdir /etc/nginx/snippets
[sudo] пароль для admin:
[admin@home-redos-app01 /]$ sudo nano /etc/nginx/snippets/ssl-params.conf
```

Содержание файла:

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_prefer_server_ciphers on;
ssl_ciphers "EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH";
ssl_ecdh_curve secp384r1;
ssl_session_cache shared:SSL:10m;
ssl_session_tickets off;
ssl_stapling on;
ssl_stapling_verify on;
resolver 8.8.8.8 8.8.4.4 valid=300s;
resolver_timeout 5s;

ssl_dhparam /etc/ssl/certs/dhparam.pem;
```

**5.2.3** Для первичной настройки сервиса допустимо создание локальных серверных сертификатов с помощью утилиты OpenSSL (шаги 5.2.4 – 5.2.11), но в дальнейшем их **НЕОБХОДИМО** заменить на действующий сертификат от доверенных центров сертификации.

Если действующий сертификат на сервер есть в наличии, вы можете переходить к шагу 5.2.12.

#### 5.2.4 Создание каталога `mycompany.ru`.

*# Создание каталога `mycompany.ru` и переход к нему. (где `mycompany.ru` – имя корпоративного домена)*

```
mkdir mycompany.ru && cd mycompany.ru
```

```
[admin@home-redos-app01 ~]$ mkdir home.local && cd home.local  
[admin@home-redos-app01 home.local]$ █
```

#### 5.2.5 Генерация файла секретного ключа центра сертификации.

*# Генерация закрытого ключа CA*

```
openssl genrsa -out ca.key 2048
```

```
[admin@home-redos-app01 home.local]$ openssl genrsa -out ca.key 2048  
Generating RSA private key, 2048 bit long modulus (2 primes)  
.....+++++  
.....  
.....+++++  
e is 65537 (0x010001)  
[admin@home-redos-app01 home.local]$ █
```

#### 5.2.6 Генерация файла сертификата центра сертификации x509 с помощью секретного ключа центра сертификации.

Вы можете определить срок действия сертификата в днях. В рамках инструкции указывается срок в 1825 дней. Следующая команда запросит детали сертификата, такие как название компании, местоположение, страна и т. д.

```
# Генерация сертификата x509 для CA
```

```
openssl req -x509 -new -nodes -key ca.key -sha256 -days 1825 -out ca.crt
```

```
[admin@home-redos-app01 home.local]$ openssl req -x509 -new -nodes -key ca.key -
sha256 -days 1825 -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:Moscow
Locality Name (eg, city) [Default City]:Balashikha
Organization Name (eg, company) [Default Company Ltd]:HOME
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:home.local
Email Address []:gava04@mail.ru
[admin@home-redos-app01 home.local]$ ls
ca.crt  ca.key
```

## 5.2.7 Генерация закрытого ключа сервера

```
# Генерация закрытого ключа для сервера
```

```
openssl genrsa -out server.key 2048
```

```
[admin@home-redos-app01 home.local]$ openssl genrsa -out server.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
[admin@home-redos-app01 home.local]$ ls
ca.crt  ca.key  server.key
[admin@home-redos-app01 home.local]$
```

## 5.2.8 Создание файла конфигурации для генерации запроса на подпись сертификата (CSR)

Запустите команду для создания файла конфигурации. Замените значения в соответствии с вашими потребностями.

```
# Создание файла конфигурации
```

```
cat > csr.conf <<EOF
```

```
# Пример содержимого файла конфигурации
```

```
[ req ]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn
[ dn ]
CN = server.mycompany.ru
[ req_ext ]
subjectAltName = @alt_names
[ alt_names ]
DNS.1 = atracker.mycompany.ru
IP.1 = 192.168.1.2
[ v3_ext ]
authorityKeyIdentifier=keyid,issuer:always
basicConstraints=CA:FALSE
keyUsage=keyEncipherment,dataEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName=@alt_names
EOF
```

```
[admin@home-redos-app01 ~]$ cat > csr.conf <<EOF
> [ req ]
> default_bits = 2048
> prompt = no
> default_md = sha256
> req_extensions = req_ext
> distinguished_name = dn
> [ req_ext ]
> subjectAltName = @alt_names
> [ alt_names ]
> DNS.1 = home-redos-app01.home.local
> DNS.2 = atracker.home.local
> IP.1 = 192.168.1.5
> [ v3_ext ]
> authorityKeyIdentifier=keyid,issuer:always
> basicConstraints=CA:FALSE
> keyUsage=keyEncipherment,dataEncipherment
> extendedKeyUsage=serverAuth,clientAuth
> subjectAltName=@alt_names
> EOF
```

## 5.2.9 Генерация файла запроса на подпись сертификата (CSR)

# Создание файла запроса

```
openssl req -new -key server.key -out server.csr -config csr.conf
```

```
[admin@home-redos-app01 home.local]$ openssl req -new -key server.key -out server.csr -config csr.conf
[admin@home-redos-app01 home.local]$ ls
ca.crt ca.key csr.conf server.csr server.key
[admin@home-redos-app01 home.local]$
```

## 5.2.10 Создание SSL-сертификата сервера

# Создание сертификата

```
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 10000 -extensions v3_ext -extfile csr.conf
```

```
[admin@home-redos-app01 home.local]$ openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 10000 -extensions v3_ext -extfile csr.conf
Signature ok
subject=CN = atracker.home.local
Getting CA Private Key
[admin@home-redos-app01 home.local]$ ls
ca.crt ca.key ca.srl csr.conf server.crt server.csr server.key
```

## 5.2.11 Объединение сертификатов центра сертификации и сервера в один файл.

# Объединение сертификатов

```
cat server.crt ca.crt >> server_ca.crt
```

```
[admin@home-redos-app01 home.local]$ cat server.crt ca.crt >> server_ca.crt
[admin@home-redos-app01 home.local]$ ls
ca.crt ca.srl server_ca.crt server.crt server.key
ca.key csr.conf '~server.crt' server.csr
```

## 5.2.12 Необходимо создать дополнительный файл конфигураций с указанием путей к сертификату и закрытому ключу для сервера.

# Параметры для конкретного домена (ссылки на сертификат)

```
sudo nano /etc/nginx/snippets/ssl-mycompany.ru.conf
```

где **mycompany.ru** – название корпоративного домена.

В файле необходимо указать пути либо к только что созданным сертификату и закрытому ключу сервера (п. 5.2.4 – 5.2.11), либо к существующим сертификату и закрытому ключу, выпущенным для вашего сервера ранее доверенным центром сертификации.

Содержание файла:

```
ssl_certificate [path]/mycompany.ru/server_ca.crt;  
ssl_certificate_key [path]/mycompany.ru/server.key;
```

```
GNU nano 4.3 /etc/nginx/snippets/ssl-home.local.conf  
ssl_certificate /home/admin/home.local/server_ca.crt;  
ssl_certificate_key /home/admin/home.local/server.key;
```

### 5.2.13 Создание файла конфигурации для приложения A-Tracker в nginx

Структура каталога `/etc/nginx/` может существенно различаться в зависимости от используемой операционной системы. В данной инструкции предполагается, что в каталоге `/etc/nginx/` создан каталог **sites-enabled**, в котором размещаются конфигурации отдельных сайтов и веб-приложений.

Если данный каталог отсутствует в системе, размещение файла конфигурации в системе может быть выбрано в соответствии с установленной структурой. Главное, чтобы в блоке **http** главного файла конфигурации **nginx.conf** была корректная ссылка **include** на файл конфигурации приложения.

*# Настраиваем файл конфигурации приложения (сайта) в nginx*

```
sudo nano /etc/nginx/sites-enabled/atracker-application
```

Содержание файла:

```
server {  
    listen          80;  
    listen          [::]:80;  
    server_name     atracker.mycompany.ru;  
    access_log      off;  
    return          301 https://$server_name$request_uri;  
}  
  
server {  
    listen 443 ssl http2;  
    listen [::]:443 ssl http2;  
    include snippets/ssl-mycompany.ru.conf;  
    include snippets/ssl-params.conf;  
    server_tokens off;  
    keepalive_timeout 70;  
    server_name     atracker.mycompany.ru;  
    access_log      /var/log/nginx/ru.mycompany.atracker.sub-access.log;  
    error_log       /var/log/nginx/ru.mycompany.atracker.sub-error.log;  
  
    location / {  
        proxy_pass          http://localhost:5021;  
        proxy_http_version 1.1;  
        proxy_set_header    Upgrade $http_upgrade;  
        proxy_set_header    Connection keep-alive;  
        proxy_set_header    Host $host;  
        proxy_cache_bypass  $http_upgrade;  
        proxy_set_header    X-Forwarded-For $proxy_add_x_forwarded_for;  
        proxy_set_header    X-Forwarded-Proto $scheme;  
    }  
}
```

### 5.2.14 Проверка конфигурации nginx

```
# Проверяем, что конфигурация написана верно
sudo nginx -t
```

### 5.2.15 Перезагрузка службы nginx

```
# Если ошибок нет, перезагружаем nginx
sudo nginx -s reload
```

### 5.2.16 Настройка параметров SELinux

Если на сервере используется механизм Security-Enhanced Linux (SELinux) - метод контроля доступа в Linux на основе модуля ядра Linux Security (LSM), то для корректной работы настройки `proxy_pass` в `nginx` необходимо проверить настройку правила `httpd_can_network_connect`:

```
# Проверка настройки правил SELinux
getsebool -a | grep httpd_can_network_connect
[admin@home-redos-app01 ~]$ getsebool -a | grep httpd_can_network_connect
httpd_can_network_connect --> on
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
```

Если правило `httpd_can_network_connect` установлено в значение `off`, необходимо изменить его командой:

```
# Изменение значения правила SELinux
sudo setsebool -P httpd_can_network_connect 1
```

### 5.2.17 Добавление службы nginx в автоматическую загрузку.

```
# Добавление службы nginx в автоматическую загрузку
sudo systemctl enable nginx.service
[admin@home-redos-app01 ~]$ sudo systemctl enable nginx.service
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service - /usr/lib/systemd/system/nginx.service.
```

## 5.3 УСТАНОВКА DOTNET И ЗАВИСИМОСТЕЙ

### 5.3.1 Загрузка скрипта установки

Загрузите скрипт установки с сайта компании Microsoft:

# Загрузка скрипта установки

wget <https://dot.net/v1/dotnet-install.sh>

```
[admin@home-redos-app01 ~]$ wget https://dot.net/v1/dotnet-install.sh
--2022-02-07 18:52:00-- https://dot.net/v1/dotnet-install.sh
Распознаётся dot.net (dot.net)... 40.76.4.15, 40.112.72.205, 104.215.148.63, ...
Подключение к dot.net (dot.net)[40.76.4.15]:443... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа... 301 Moved Permanently
Адрес: https://dotnet.microsoft.com/download/dotnet/scripts/v1/dotnet-install.sh [переход]
--2022-02-07 18:52:02-- https://dotnet.microsoft.com/download/dotnet/scripts/v1/dotnet-install.sh
Распознаётся dotnet.microsoft.com (dotnet.microsoft.com)... 13.107.246.45, 13.107.213.45, 2620:1ec:bdf::45
/ ...
Подключение к dotnet.microsoft.com (dotnet.microsoft.com)[13.107.246.45]:443... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа... 200 OK
Длина: 55535 (54K) [application/x-sh]
Сохранение в: «dotnet-install.sh»

dotnet-install.sh      100%[=====>]  54,23K  ---.KB/s   за 0,001s
2022-02-07 18:52:02 (46,0 MB/s) - «dotnet-install.sh» сохранён [55535/55535]
```

### 5.3.2 Проверка и настройка прав

Проверьте наличие у скачанного файла сценария прав на исполнение:

# Получение списка прав

ls -l

```
[admin@home-redos-app01 ~]$ ls -l
итого 60
-rw-rw-r--. 1 admin admin 55535 фев  5 01:05 dotnet-install.sh
drwxrwxr-x. 2 admin admin  4096 фев  7 15:38 home.local
```

Если права на исполнение отсутствуют, то предоставьте их с помощью команды **chmod**:

# Предоставление прав на исполнение:

chmod +x dotnet-install.sh

```
[admin@home-redos-app01 ~]$ chmod +x dotnet-install.sh
[admin@home-redos-app01 ~]$ ls -l
итого 60
-rwxrwxr-x. 1 admin admin 55535 фев  5 01:05 dotnet-install.sh
drwxrwxr-x. 2 admin admin  4096 фев  7 15:38 home.local
```

### 5.3.3 Установка пакета dotnet sdk 6.0

Запустите сценарий для установки пакета dotnet sdk 6.0:

# Установка dotnet sdk 6.0:

./dotnet-install.sh -c 6.0 --install-dir /usr/bin/dotnet

```
[admin@home-redos-app01 ~]$ sudo ./dotnet-install.sh -c 6.0 --install-dir /usr/bin/dotnet
dotnet-install: Note that the intended use of this script is for Continuous Integration (CI) scenarios, where:
dotnet-install: - The SDK needs to be installed without user interaction and without admin rights.
dotnet-install: - The SDK installation doesn't need to persist across multiple CI runs.
dotnet-install: To set up a development environment or to run apps, use installers rather than this script. Visit https://dotnet.microsoft.com/download to get the installer.
dotnet-install: Attempting to download using aka.ms link https://dotnetcli.azureedge.net/dotnet/Sdk/6.0.101/dotnet-sdk-6.0.101-linux-x64.tar.gz
dotnet-install: Extracting zip from https://dotnetcli.azureedge.net/dotnet/Sdk/6.0.101/dotnet-sdk-6.0.101-linux-x64.tar.gz
dotnet-install: Adding to current process PATH: '/usr/bin/dotnet'. Note: This change will be visible only when sourcing script.
dotnet-install: Note that the script does not resolve dependencies during installation.
dotnet-install: To check the list of dependencies, go to https://docs.microsoft.com/dotnet/core/install, select your operating system and check the "Dependencies" section.
dotnet-install: Installation finished successfully.
```

## 5.4 УСТАНОВКА ПРИЛОЖЕНИЯ A-TRACKER

### 5.4.1 Создание пользователя, под которым будет запускаться приложение A-Tracker

```
# Создание пользователя  
sudo adduser atracker
```

### 5.4.2 Создание папки для хранения приложения

```
# Создание папки  
sudo mkdir /var/www/atracker-application
```

### 5.4.3 Скопируйте в созданную папку файлы приложения A-Tracker с помощью утилиты WinSCP или аналогичных решений.

### 5.4.4 Предоставление прав на папку группе atracker

```
# Делаем группу atracker владельцем папки с приложением  
sudo chgrp -R atracker /var/www/atracker-application
```

### 5.4.5 Установка флага setgid на папку (для того, чтобы все новые файлы в каталоге относились к группе atracker)

```
# Установка флага SGID, чтобы все новые файлы внутри папки попадали в группу atracker  
sudo chmod 2750 /var/www/atracker-application
```

### 5.4.6 Создание сервиса приложения

Для создания сервиса необходимо создать в папке `/etc/systemd/system` соответствующий файл:

```
# Создаем сервис  
sudo nano /etc/systemd/system/atracker-application.service
```

Содержание файла:

```
[Unit]  
Description=.NET Core A-Tracker Application  
  
[Service]  
WorkingDirectory=/var/www/atracker-application  
ExecStart=/usr/bin/dotnet /var/www/atracker-application/ATracker.dll  
Restart=always  
RestartSec=10  
KillSignal=SIGINT  
SyslogIdentifier=dotnet-atracker-application  
User=atracker  
Environment=ASPNETCORE_ENVIRONMENT=Production  
Environment=DOTNET_PRINT_TELEMETRY_MESSAGE=false  
  
[Install]  
WantedBy=multi-user.target
```

### 5.4.7 Запуск сервиса приложения

```
# Запуск сервиса приложения  
sudo systemctl start atracker-application.service
```

## 5.4.8 Проверка состояния сервиса приложения

```
# Проверяем статус сервиса приложений
systemctl status atracker-application.service
```

```
[admin@home-redos-app01 ~]$ systemctl status atracker-application.service
● atracker-application.service - .NET Core A-Tracker Application
   Loaded: loaded (/etc/systemd/system/atracker-application.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2022-02-08 12:48:10 MSK; 13min ago
     Main PID: 4042 (dotnet)
        Tasks: 13 (limit: 2252)
       Memory: 24.2M
          CPU: 2.252s
     CGroup: /system.slice/atracker-application.service
            └─4042 /usr/bin/dotnet/dotnet /var/www/atracker-application/Plug.dll

feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]: info: Microsoft.Hosting.Lifetime[14]
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]:   Now listening on: http://localhost:5021
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]: info: Microsoft.Hosting.Lifetime[0]
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]:   Application started. Press Ctrl+C to shut down.
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]: info: Microsoft.Hosting.Lifetime[0]
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]:   Hosting environment: Production
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]: info: Microsoft.Hosting.Lifetime[0]
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]:   Content root path: /var/www/atracker-application/
feb 08 12:48:27 home-redos-app01.home.local dotnet-atracker-application[4042]: warn: Microsoft.AspNetCore.HttpsPolicy.HttpsRedirectionMiddleware[3]
feb 08 12:48:27 home-redos-app01.home.local dotnet-atracker-application[4042]:   Failed to determine the https port for redirect.
```

Полный журнал событий в работе сервиса приложений можно посмотреть с помощью команд:

```
# Просмотр журналов событий сервиса
sudo journalctl -fu atracker-application.service
sudo journalctl -fu atracker-application.service --since today
sudo journalctl -fu atracker-application.service --until 1 hour ago
sudo journalctl -fu atracker-application.service --since "2016-10-18" --until "2016-10-18 04:00"
```

```
[admin@home-redos-app01 ~]$ sudo journalctl -fu atracker-application.service
-- Logs begin at Fri 2022-01-28 10:22:46 MSK. --
feb 08 12:48:10 home-redos-app01.home.local systemd[1]: Stopped .NET Core A-Tracker Application.
feb 08 12:48:10 home-redos-app01.home.local systemd[1]: Started .NET Core A-Tracker Application.
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]: info: Microsoft.Hosting.Lifetime[14]
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]:   Now listening on: http://localhost:5021
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]: info: Microsoft.Hosting.Lifetime[0]
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]:   Application started. Press Ctrl+C to shut down.
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]: info: Microsoft.Hosting.Lifetime[0]
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]:   Hosting environment: Production
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]: info: Microsoft.Hosting.Lifetime[0]
feb 08 12:48:11 home-redos-app01.home.local dotnet-atracker-application[4042]:   Content root path: /var/www/atracker-application/
feb 08 12:48:27 home-redos-app01.home.local dotnet-atracker-application[4042]: warn: Microsoft.AspNetCore.HttpsPolicy.HttpsRedirectionMiddleware[3]
feb 08 12:48:27 home-redos-app01.home.local dotnet-atracker-application[4042]:   Failed to determine the https port for redirect.
```

## 5.4.9 Добавление сервиса приложения в автозагрузку

```
# Добавляем сервис в автозагрузку после перезагрузки системы
sudo systemctl enable atracker-application.service
```

```
[admin@home-redos-app01 ~]$ sudo systemctl enable atracker-application.service
Created symlink /etc/systemd/system/multi-user.target.wants/atracker-application.service → /etc/systemd/system/atracker-application.service.
```

## 5.4.10 Добавление инициатора планировщика задач.

Добавьте в расписание службы **cron** задачу по выполнению инициации планировщика задач A-Tracker.

```
curl
http://localhost/Account/Ping?S=v1LEt6COMKvpxA3mhbLR2uqQ8n0L9RWKNNTR1JH9hTn2Rg0oh6
```

с частотой выполнения раз в минуту.

```
# Открытие файла конфигурации службы cron
sudo nano /etc/crontab
```

```
# Добавление строки
*/1 * * * * curl http://localhost/Account/Ping?S=v1LEt6COMKvpxA3mhbLR2uqQ8n0L9RWKNNTR1JH9hTn2Rg0oh6
```

Проверьте, что задача инициации планировщика успешно выполняется.

```
# Редактирование файла конфигурации службы cron  
sudo cat /var/log/cron
```

```
Mar 2 07:34:01 atracker-itam CROND[24427]: (atracker) CMD (curl http://localhost/Account/Ping?S=v1LEt6C0MKvpxA3mhBLR2uq08n0L9RWKNTRLJH9hTn2Rg0oh6)
Mar 2 07:35:01 atracker-itam CROND[24505]: (atracker) CMD (curl http://localhost/Account/Ping?S=v1LEt6C0MKvpxA3mhBLR2uq08n0L9RWKNTRLJH9hTn2Rg0oh6)
Mar 2 07:36:01 atracker-itam CROND[24574]: (atracker) CMD (curl http://localhost/Account/Ping?S=v1LEt6C0MKvpxA3mhBLR2uq08n0L9RWKNTRLJH9hTn2Rg0oh6)
Mar 2 07:37:01 atracker-itam CROND[24637]: (atracker) CMD (curl http://localhost/Account/Ping?S=v1LEt6C0MKvpxA3mhBLR2uq08n0L9RWKNTRLJH9hTn2Rg0oh6)
Mar 2 07:38:01 atracker-itam CROND[24705]: (atracker) CMD (curl http://localhost/Account/Ping?S=v1LEt6C0MKvpxA3mhBLR2uq08n0L9RWKNTRLJH9hTn2Rg0oh6)
Mar 2 07:39:01 atracker-itam CROND[24772]: (atracker) CMD (curl http://localhost/Account/Ping?S=v1LEt6C0MKvpxA3mhBLR2uq08n0L9RWKNTRLJH9hTn2Rg0oh6)
Mar 2 07:40:01 atracker-itam CROND[24841]: (atracker) CMD (curl http://localhost/Account/Ping?S=v1LEt6C0MKvpxA3mhBLR2uq08n0L9RWKNTRLJH9hTn2Rg0oh6)
```

## 6. НАСТРОЙКА ПАРАМЕТРОВ ПРИЛОЖЕНИЯ A-TRACKER

### 6.1 ФАЙЛ ЛИЦЕНЗИИ

Перед началом работы с системой создайте каталог Licenses в папке приложения и скопируйте в него файл лицензии, полученный в составе дистрибутива.

```
# Создание каталога Licenses
mkdir /var/www/atracker-application/Licenses
```

```
# Копирование файла лицензии
cp <имя файла лицензии>.txt /var/www/atracker-application/Licenses
```

### 6.2 ФАЙЛ КОНФИГУРАЦИЙ

Настройка параметров сервиса A-Tracker осуществляется посредством редактирования файла конфигураций **appsettings.json**.

```
# Настройка параметров осуществляется через файл конфигурации
sudo nano /var/www/atracker-application/appsettings.json
```

Основные параметры файла конфигурации приведены в таблице ниже:

Параметр	Описание	Пример
Global Settings	Общие настройки системы	<pre>"Global Settings": {   "Object List Row Count": 25,   "Wizard List Row Count": 15,   bDeleted=true   "Real Delete From DB": true,   "Two Factor Authentication": false,   "Guest Entry": false,   "Script Using Strings": [     "System",     "System.Collections.Generic",     "System.Linq",     "System.Threading.Tasks",     "Microsoft.Extensions.Logging",     "Microsoft.Extensions. DependencyInjection",     "TemplateEngine.Docx",     "ATracker",     "ATracker.Models",     "ATracker.Services"   ],   "Show Script Error To User": false }</pre>
Kestrel	Настройка точки подключения к сервису	<pre>"Kestrel": {   "Endpoints": {     "Http": {       "Url": "http://localhost:5021"</pre>

		<pre> } } } </pre>
<b>ConnectionStrings</b>	Настройки строки подключения к базе данных ATracker.	<pre> "ConnectionStrings": {   "Database Type": "PostgreSQL",   "DefaultConnection": "Host=127.0.0.1;Port=5432;User Id=atracker;Password=1234567890; Database=atracker" } </pre>
<b>LDAP Authentication</b>	Строка подключения к серверу MS Active Directory. Заполняется в случае настройки аутентификации при входе в систему A-Tracker с помощью MS Active Directory. Не обязательно для заполнения.	<pre> "LDAP Authentication": {   "Enable": false,   "Server": "172.0.0.1",   "Domain": "",   "Port": 389 } </pre>
<b>SMTP Settings</b>	Настройки подключения к серверам SMTP для отправки почтовых уведомлений	<pre> "SMTP Settings": {   "MailFrom": "noreply@company.com",   "Password": "password",   "Host": "smtp.gmail.com",   "Port": 587,   "EnableSsl": true,   "Application URL": "https://atracker.company.com/" }, </pre>

После внесения изменений в параметры необходимо выполнить перезапуск сервиса.

### 6.3 НАСТРОЙКА ТОЧКИ ПОДКЛЮЧЕНИЯ

В секции **Kestrel** укажите адрес и порт, по которым сервис будет ожидать подключения от службы **nginx**:

```

"Kestrel": {
  "Endpoints": {
    "Http": {
      "Url": "http://localhost:5021"
    }
  }
}

```

Значение параметра **Url** должно совпадать со значение параметра **proxy\_pass** файла конфигураций **atracker-application** (см. Раздел 5.2.13).

### 6.4 НАСТРОЙКА ПОДКЛЮЧЕНИЯ К БАЗЕ ДАННЫХ

Для выполнения настройки параметров подключения к базе данных необходимо указать значения в секции **ConnectionStrings**:

```
"ConnectionStrings": {  
  // Тип базы данных  
  "Database Type": "PostgreSQL",  
  
  // Строка подключения  
  "DefaultConnection": "Host=127.0.0.1;Port=5432;User Id=atracker;Pass-  
word=1234567890;Database=atracker"  
}
```

В поле **Host** необходимо указать IP-адрес или имя сервера, на котором развернута база данных Atracker. Значения полей **User ID**, **Password** и **Database** должны совпадать со значениями, настроенными в Разделе 4.

## 7. НАСТРОЙКА ОТПРАВКИ УВЕДОМЛЕНИЙ

Для настройки исходящих уведомлений необходимо заполнить параметры секции **SMTP Settings** файла конфигураций (см. Раздел 6):

- **MailFrom** – почтовый адрес, от которого будут рассылаться уведомления;
- **Password** – пароль для подключения к серверу отправки. Если почтовый сервер разрешает отправку без авторизации укажите значение "Password": "[WithoutAuthentication]";
- **Host** – имя почтового сервера;
- **Port** – порт подключения к почтовому серверу;
- **EnabledSsl** – разрешено или нет безопасное подключение к серверу;
- **Application URL** – путь к приложению A-Tracker для формирования ссылки в письме.

Для отправки исходящих уведомлений используется поле **email (sEmail)** справочника сотрудников (таблица **itamEmplDept**).

## 8. НАСТРОЙКА АУТЕНТИФИКАЦИИ С ИСПОЛЬЗОВАНИЕМ MS ACTIVE DIRECTORY

При входе в систему A-Tracker для авторизации может быть использована пара логина и пароля доменного пользователя. (При входе в систему под пользователем **Admin** всегда используется проверка пароля по базе данных системы A-Tracker).

Для настройки аутентификации с использованием MS Active Directory необходимо установить следующие параметры:

1. Заполнить секцию **LDAP Authentication** в файле конфигураций **appsetting.json** (см. Раздел 6);
2. Добавить в справочник сотрудников A-Tracker всех пользователей, которые будут подключаться к системе;
3. Создать в справочнике учетных записей A-Tracker всех пользователей, которые будут подключаться к системе. При этом поле **Имя** должно соответствовать имени

- учетной записи пользователя в MS Active Directory (без имени домена). Поле пароль можно заполнить произвольным значением;
4. Установить признак **enable=true** в разделе «**LDAP Authentication**» файла `appsetting.json`;
  5. Выполнить перезагрузку сервиса системы A-Tracker.

## 9. НАСТРОЙКА ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ ДЛЯ ВСЕХ ПОЛЬЗОВАТЕЛЕЙ

При входе в систему A-Tracker может быть использована двухфакторная аутентификация.

Для того, чтобы принудительно включить двухфакторную аутентификацию для всех пользователей, необходимо в файле конфигураций **appsetting.json** (см. Раздел 6) параметру **Two Factor Authentication** в секции **Global Settings** задать значение **true**. В этом случае новый пользователь после авторизации по логину и паролю будет перенаправлен на страницу с конфигурацией двухфакторной аутентификации.

Пользователю необходимо будет установить на свой смартфон одно из следующих приложений:

- Google Authenticator;
- Яндекс Ключ;
- Microsoft Authenticator.

← Двухфакторная аутентификация  
Администрирование

---

Для работы с системой необходимо настроить двухфакторную аутентификацию.

Установите любое из приложений на смартфон:

- **Google Authenticator** для [Android](#) и [iOS](#)
- **Яндекс Ключ** для [Android](#) и [iOS](#)
- **Microsoft Authenticator** для [Windows Phone](#), [Android](#) и [iOS](#)

Откройте приложение и отсканируйте QR-код



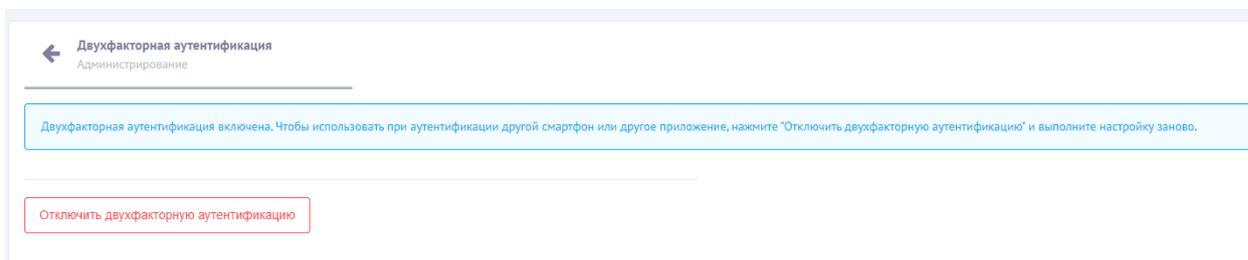
Введите код из приложения в поле подтверждения

---

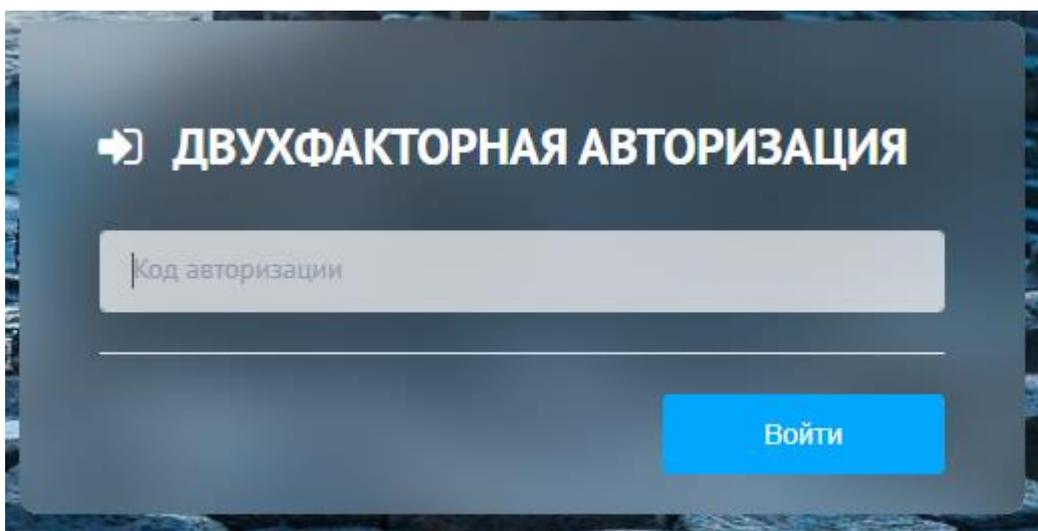
Подтвердить код

В приложении необходимо создать новую учетную запись и отсканировать QR на экране браузера. После создания учетной записи в ней будут генерировать одноразовые пароли. Введите текущий одноразовый пароль в поле **Код подтверждения** и нажмите кнопку **Подтвердить код**.

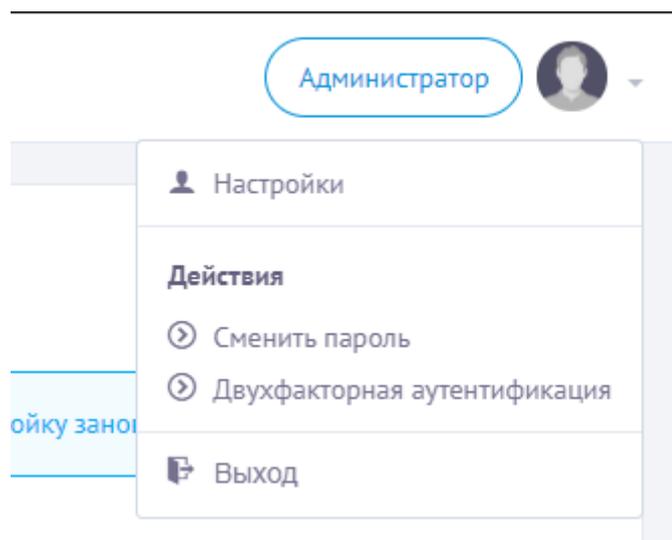
После ввода кода подтверждения пользователь увидит уведомление, что двухфакторная аутентификация включена. С этого момента учетная запись A-Tracker будет связана с конкретной учетной записью в конкретном приложении на конкретном устройстве.



При следующей входе в систему приложение A-Tracker снова попросит после ввода логина/пароля ввести одноразовый пароль из приложения.



Чтобы использовать при аутентификации другой смартфон или другое приложение, используйте опцию "Двухфакторная аутентификация" в меню пользователя и выполните настройку заново.



## 10. ПАРОЛЬ АДМИНИСТРАТОРА A-TRACKER

В системе есть преднастроенный пользователь с ролью Администратора:

- Логин **Admin**
- Пароль **supp0rT**

**Настоятельно рекомендуется сменить пароль сразу после установки системы A-Tracker.**

**Также, рекомендуется создать учетные записи сотрудников и выдать им роль Администратора, а не использовать встроенную учетную запись Admin.**