Последнее обновление: 12.09.2021 03:03

Настройки безопасности

Перейдите на вкладку «Настройки» в раздел «Настройки безопасности».

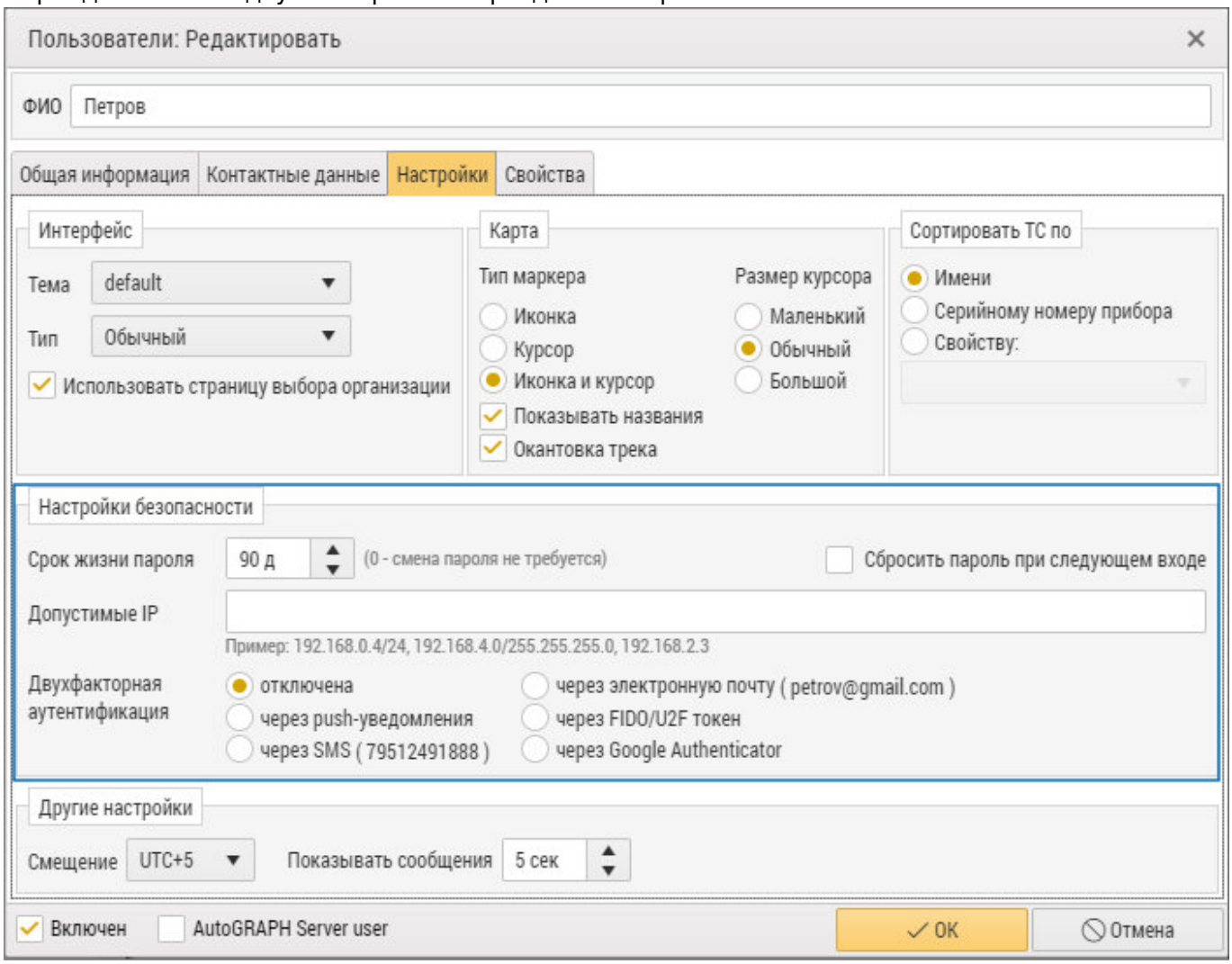

Рис. 1: Настройки безопасности

Настройте следующие параметры безопасности для учетной записи:

- **Срок жизни пароля**, в днях. По истечении указанного срока вход в организации пользователя, используя текущий пароль, будет невозможен – пользователю будет предложено сменить пароль. Значение 0 разрешает использование бессрочного пароля. Включите чек-бокс **«Сбросить пароль при следующем входе»** для отправки пользователя запроса смены пароля при следующем входе на web-сервер.
- **Допустимые IP** — список IP-адресов (через запятую), с которых разрешено подключение к web-серверу, используя учетную запись пользователя.
- **Двухфакторная аутентификация** — дополнительный метод идентификации пользователя при авторизации. Для отключения двухфакторной аутентификации выберите настройку **«отключена»**. В этом случае для входа на web-сервер достаточно ввести логин и пароль на стартовой странице программы.

Ниже рассмотрены методы двухфакторной аутентификации, поддерживаемые в

текущей версии ПО «АвтоГРАФ.WEB».

Через push-уведомления

Данный метод используется в мобильных приложениях АвтоГРАФ-MOBILE. После ввода пароля пользователя на мобильное устройство будет выслан код подтверждения в виде push-уведомления.

Через SMS

При использовании данного метода, после ввода пароля пользователя на номер телефона, указанный в настройках пользователя, будет выслано SMS-сообщение с кодом подтверждения. Номер телефона дублируется в скобках после настройки «через сервер».

Пример сообщения:

```
226029
IP Address: 192.168.6.180
Server: ag2new.tk-chel.ru
```

Через электронную почту

При использовании данного метода, после ввода пароля пользователя на адрес электронной почты, указанный в настройках пользователя, будет выслано письмо с кодом подтверждения. Адрес пользователя дублируется в скобках после настройки «через электронную почту». 6-значный код подтверждения указывается в теме письма.
Отправитель письма — webmap@ag-navi.com.

Через FIDO/U2F токен

При выборе данного метода для авторизации пользователя в системе требуется подключение к компьютеру, с которого выполняется вход, USB-устройства (токена), поддерживающего протокол web-аутентфикации U2F.

Регистрация токена

Используемый токен должен быть зарегистрирован. Для этого подключите токен к компьютеру по интерфейсу USB и нажмите кнопку «Регистрировать».

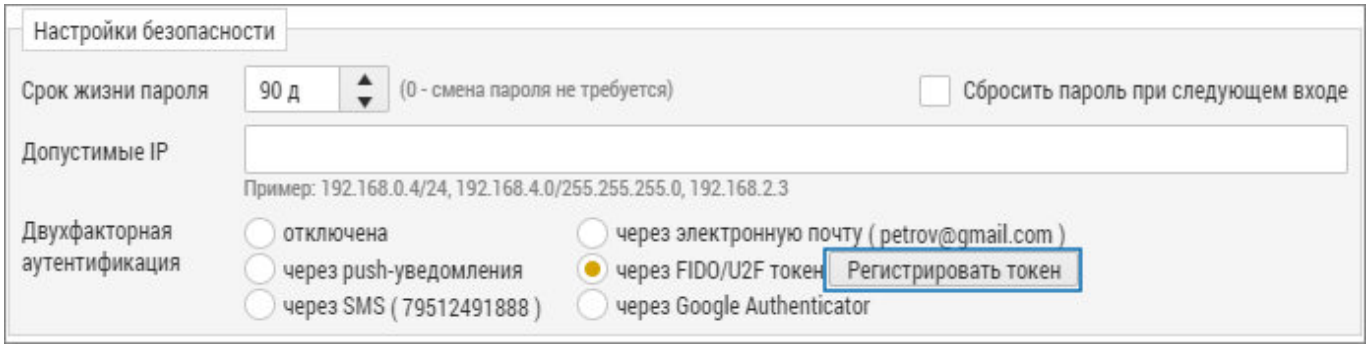

Рис. 2: Регистрация токена

Через Google Authenticator

При использовании данного метода для авторизации пользователя в системе требуется ввод кода из мобильного приложения Google Authenticator.

Google Authenticator — это мобильное приложение, доступное для OS iOS и Android и предназначенное для создания кодов двухэтапной аутентификации с привязкой к учетной записи. Приложение доступно для скачивания в App Store и Google Play.

Для использования данного метода необходимо зарегистрировать приложение Google Authenticator.
Для этого нажмите кнопку «Регистрировать приложение».

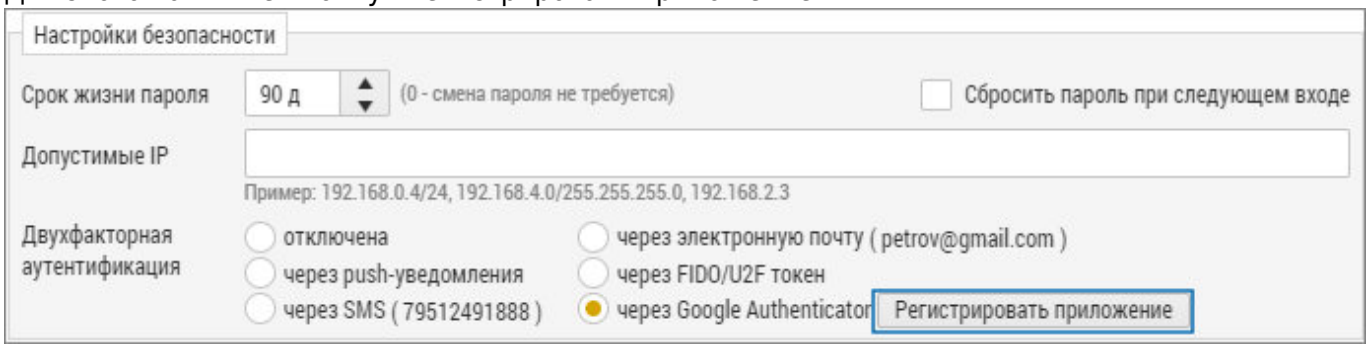

Рис. 3: Регистрация приложения
На экране появится QR-код, который необходимо считать с помощью функции «Сканировать QR-код» в приложении Google Authenticator на вашем телефоне. После этого аккаунт пользователя будет сохранен в приложении.
При входе пользователя на web-сервер нужно будет ввести код подтверждения, сгенерированный в приложении Google Authenticator для сохраненной учетной записи.

Для отключения привязки учетной записи с экземпляром приложения Google Authenticator нажмите кнопку «Отозвать приложение».

Двухфакторная аутентификация,, токен,, Google Authenticator,, безопасность