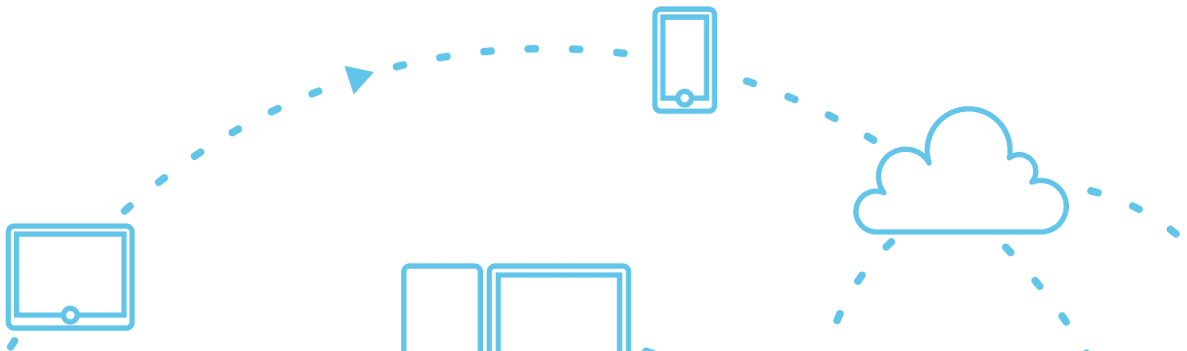
Руководство по работе

с Сервисом / Платформой двухфакторной аутентификации Protectimus

Вер. 1.0.0 RU
от 23 марта 2020



Содержание

1. Настройка сервера аутентификации Protectimus

Сервер аутентификации Protectimus доступен в двух вариантах:

- **Сервис** - облачное SAAS-решение для быстрого старта и эффективного внедрения двухфакторной аутентификации. К вашим услугам: облачная платформа, доступная 24/7, удобные средства мониторинга и управления, а также широкий спектр токенов.
- **Платформа** - комплексное решение двухфакторной аутентификации, располагаемое в вашем окружении, для полного контроля над всеми аспектами функционирования системы аутентификации, в том числе и базой данных пользователей и другой чувствительной информацией. Платформа аутентификации и инструкция по ее установке предоставляется по запросу в службу поддержки Protectimus по адресу support@protectimus.com.

ВНИМАНИЕ! Мы предлагаем начать тестирование с облачным сервисом, чтобы ускорить процесс интеграции. Для переключения между облачными и локальными серверами достаточно лишь изменить несколько строк в файле конфигурации.

Начало работы с SaaS-сервисом Protectimus

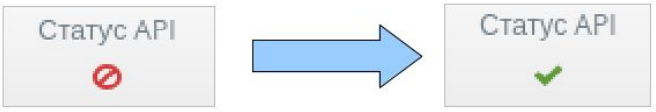
Для начала использования SaaS-сервиса перейдите на страницу регистрации https://service.protectimus.com, заполните регистрационную форму и нажмите кнопку «Регистрация». Письмо для подтверждения регистрации будет отправлено на указанный вами электронный адрес. После перехода по ссылке в письме ваш адрес будет подтвержден, и вы сможете использовать Protectimus Cloud Authentication Service - облачное (SaaS) решение.

2. Активация API

Активация API в Сервисе

В случае использования SaaS-решения необходимо активировать тарифный план для работы API. Для этого перейдите в раздел **“Тарифные планы”** http://service.protectimus.com/pricing и активируйте подходящий вам тарифный план. Пока вы не активируете тарифный план с вашего счета не будут списываться средства, но вы также не сможете использовать API. вы сможете деактивировать тарифный план в любой момент, если по каким-то причинам вам не нужно будет пользоваться сервисом больше одного дня. При первой деактивации тарифа за текущие сутки со счета единоразово списывается плата за использование сервиса согласно расценкам активного тарифа. При активном тарифном плане плата взимается раз в сутки автоматически.

После активации тарифного плана значок статуса API перейдет в состояние “Включено”, что означает готовность сервиса к работе через API.



Активация API и лицензии в Платформе

После запуска платформы вы должны зарегистрироваться в системе. Для этого вам будет необходимо получить лицензию. Перейдите на страницу http://platform_path/licensing, выберите необходимое количество опций и получите ключ лицензирования.

С помощью полученного ключа вы сможете оплатить и загрузить лицензию на сайте по адресу https://service.protectimus.com/platform/licensing. Если необходима другая схема оплаты - обратитесь в службу поддержки Protectimus.

После получения файла лицензии загрузите его на сервер и укажите путь к файлу в параметре **licence.file.path** файла **protectimus.platform.properties**. Перезагрузите сервер для активации изменений.

3. Начало работы с Сервисом / Платформой Protectimus

Базовые настройки, необходимые для работы Сервиса или Платформы двухфакторной аутентификации Protectimus, включают:

1. Создание ресурса.
2. Создание пользователей.
3. Создание токенов.
4. Назначение токенов пользователям.
5. Назначение пользователей с токенами на ресурс.

Дополнительные возможности Сервиса и Платформы Protectimus позволяют:

- Добавить администратора.
- Создать и назначить географические или временные фильтры.
- Настроить интеллектуальную идентификацию (анализ окружения пользователей).
- Настроить уведомления о важных событиях.
- Задать настройки безопасности для собственной учетной записи в сервисе Protectimus.

ОБРАТИТЕ ВНИМАНИЕ!

1. В зависимости от выбранной вами модели пользователь может быть аутентифицирован по статическому паролю, по одноразовому паролю или же по статическому и одноразовому паролю одновременно. Чтобы пользователь или токен мог пройти аутентификацию, он должен быть назначен на запрашиваемый ресурс (а если выполняется аутентификация пользователя и токена на ресурсе одновременно, то пользователь должен быть назначен на ресурс вместе с токеном). Подробнее о возможных способах аутентификации пользователей читайте в разделе Назначение пользователей и токенов на ресурс.

2. Для облегчения работы администратора, предусмотрена возможность настройки портала самообслуживания, который позволяет пользователям самостоятельно выполнять ряд действий по выпуску и обслуживанию токенов, а также их собственных данных. Подробно о настройке и возможностях портала самообслуживания пользователей читайте в разделе Портал самообслуживания.

4. Ресурсы

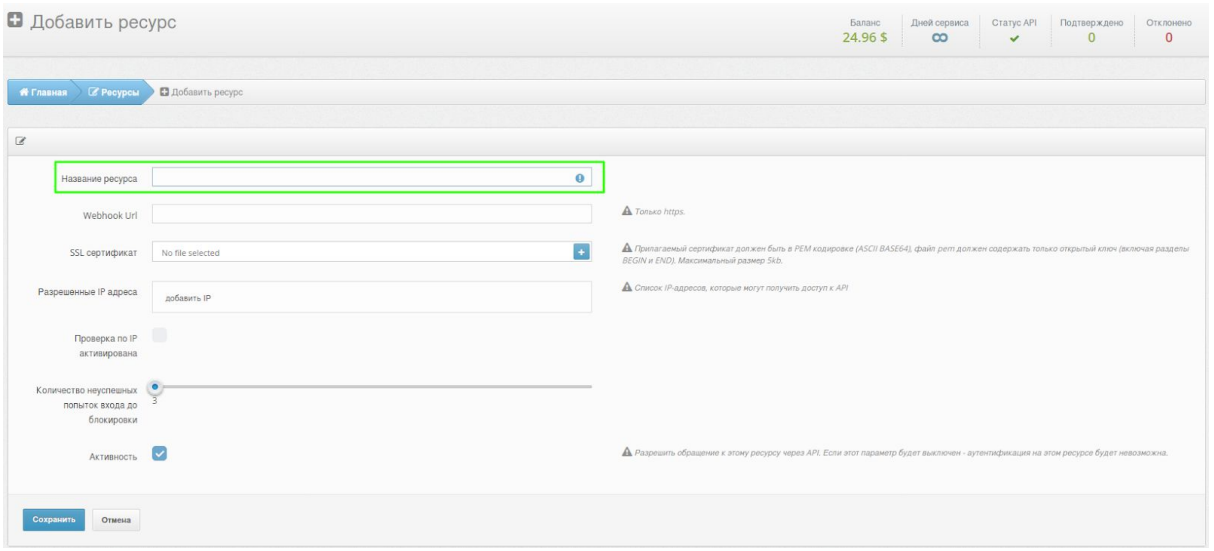
Ресурс является средством группировки пользователей и предоставляет гибкие возможности делегирования полномочий. Под ресурсом следует понимать веб-проект, портал, приложение или отдел ваших сотрудников. Главный администратор может добавить других администраторов в систему и назначить их на определенные ресурсы. Обычным администраторам доступны только действия в пределах ресурса, на которые они назначены, но они могут видеть всех пользователей и все токены, которые существуют в системе, независимо от того, назначены они на ресурсы, которыми управляет администратор, или нет.

Количество доступных для создания ресурсов (проектов) ограничивается выбранным вами тарифным планом. Если вам необходимо создать больше ресурсов, выберите желаемое количество ресурсов настроив собственный тарифный план. Действия по выбору тарифного плана доступны только главному администратору.

Создание ресурса

Чтобы создать ресурс, нажмите на кнопку **“Ресурсы”** в меню слева, а затем нажмите на кнопку **“Добавить ресурс”** в заголовке таблицы.

После этих действий вы попадете на страницу добавления ресурса, где обязательно необходимо указать только **название ресурса**, остальные параметры - по желанию.



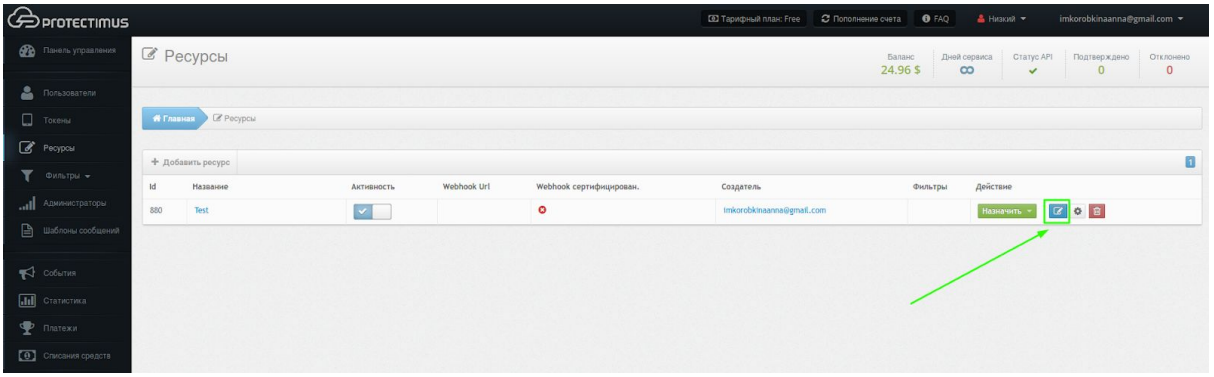
- **Webhook URL**. При определенных событиях связанных с ресурсами вам будет отправлено уведомление, содержащее детальную информации в JSON формате. Для отправки уведомлений используется POST запрос на указанный

webhook. В случае неудачного запроса попытка повторится несколько раз. В настоящее время webhook используется для получения результата интерактивной (INTERACTIVE) аутентификации. Интерактивная аутентификация поддерживается токеном Protectimus Bot.

- **SSL сертификат**. Сертификат открытого ключа удостоверяет принадлежность открытого ключа указанному webhook. Предоставленный сертификат должен быть в кодировке PEM (ASCII BASE64), файл pem должен содержать только открытый ключ начинаться с "-----BEGIN CERTIFICATE----- " и заканчиваться "-----END CERTIFICATE----- "
- **Разрешенные IP адреса**. Позволяет ограничить доступ к системе только с доверенных IP-адресов.
- **Проверка по IP активирована**. Активирует ограничение доступа к системе из указанных IP-адресов.
- **Количество неуспешных попыток входа до блокировки**. Значение этого параметра должно быть в диапазоне от 3 до 10. Если пользователь или токен не пройдет аутентификацию, то для него будет увеличен счетчик неуспешных попыток аутентификации. При превышении порогового значения количества неверных попыток для указанного ресурса пользователь будет заблокирован. Разблокировать пользователя можно через веб-интерфейс. При успешной аутентификации счетчик неуспешных попыток обнулится, если он не превысил допустимый предел для ресурса и пользователь еще не был заблокирован.
- **Активность.** Позволяет активировать и деактивировать ресурс.

Редактирование ресурса

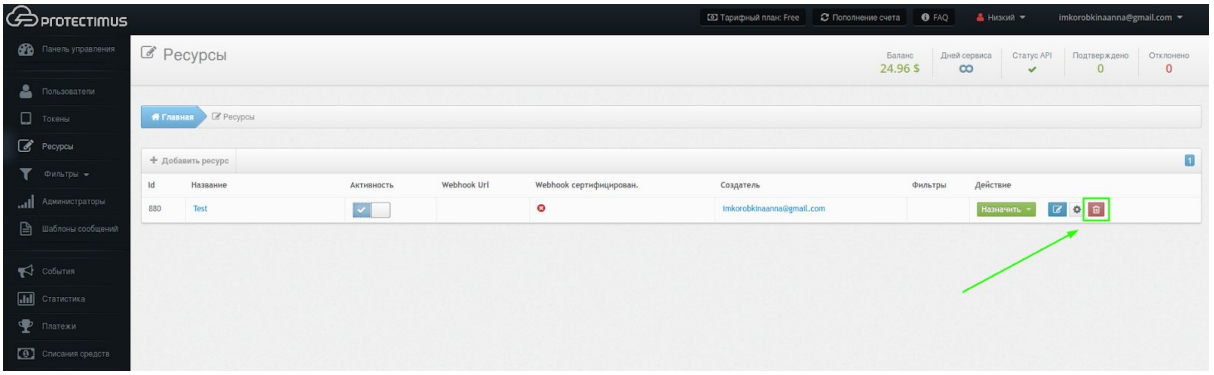
Для редактирования ресурса нажмите на кнопку **“Ресурсы”** в меню слева, выберите нужный ресурс и нажмите на **синюю кнопку справа**. Вы попадете на страницу настроек ресурса и сможете внести изменения.



Удаление ресурса

Удалить ресурс может только администратор, который его создал, либо главный администратор.

Чтобы удалить ресурс, нажмите на кнопку **“Ресурсы”** в меню слева, а затем нажмите на **кнопку красного цвета с изображение корзины** и подтвердите действие.



5. Пользователи

Вы можете хранить некоторый набор информации о ваших пользователях (имя, фамилия, email, номер телефона) в системе Protectimus, но основным параметром является Логин пользователя.

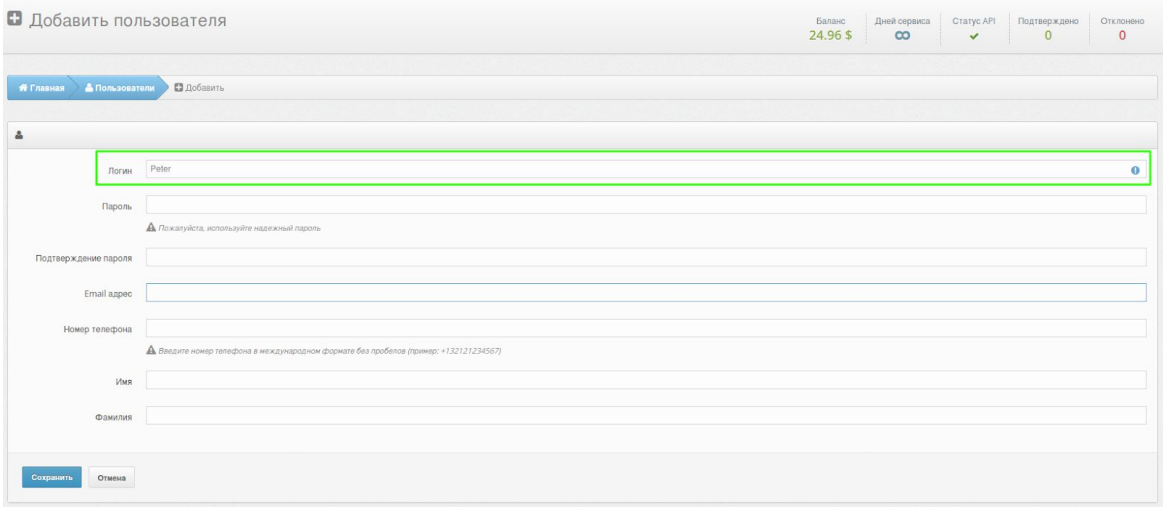
Администратор может создавать пользователей вручную. Также в системе имеется механизм самообслуживания пользователей. Он настраивается для каждого ресурса отдельно, это можно сделать на вкладке “Самообслуживание” на странице просмотра детальной информации о ресурсе. Подробно о настройке и возможностях портала самообслуживания пользователей читайте в разделе Портал самообслуживания.

Количество доступных для создания пользователей ограничивается выбранным вами тарифным планом. Если вам необходимо создать больше пользователей, выберите желаемое количество пользователей настроив собственный тарифный план. Действия по выбору тарифного плана доступны только главному администратору.

Создание пользователей

Чтобы создать пользователя, нажмите на кнопку **“Пользователи”** в меню слева, а затем нажмите на кнопку **“Добавить пользователя”** в заголовке таблицы.

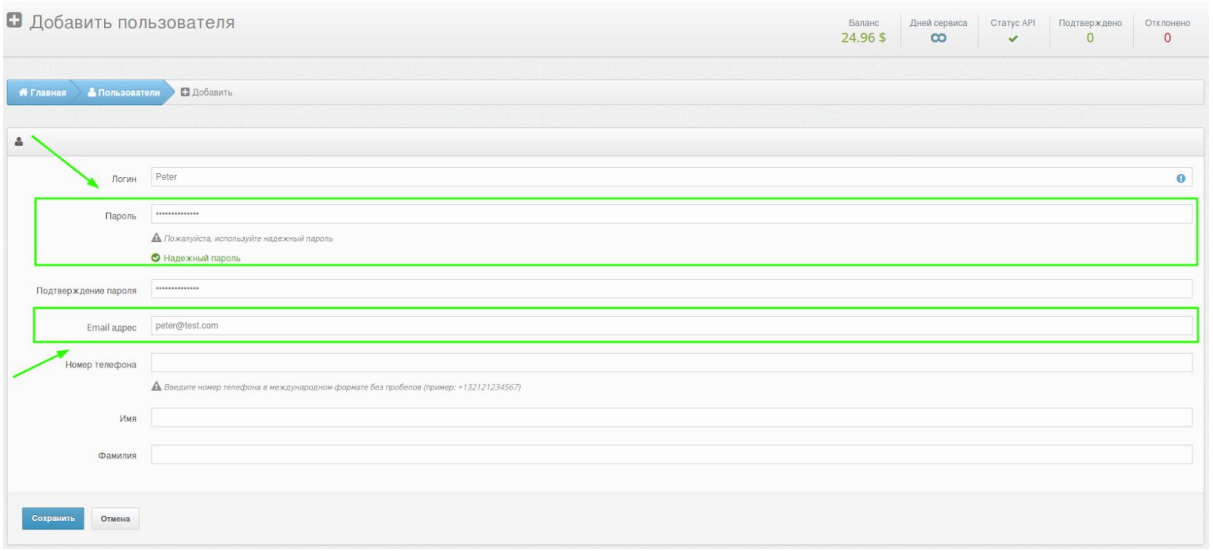
После этих действий вы попадете на страницу добавления пользователя, где обязательно необходимо указать только **Логин**, остальные параметры - по желанию. **Логин** пользователя должен содержать **только латиницу, цифры и следующие символы: _-@∾!#%+.$**. Пробелы и любые другие символы не допускаются.



ОБРАТИТЕ ВНИМАНИЕ!

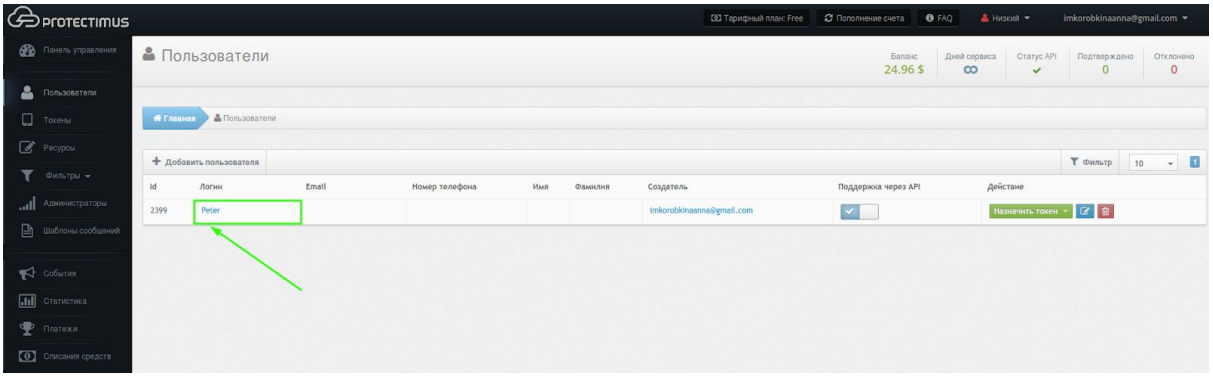
Если вы планируете активировать регистрацию токенов через портал самообслуживания, у пользователей должен быть **установлен пароль** в Protectimus или **указан адрес электронной почты**, на который будет приходить код подтверждения для входа в портал. Если указаны и пароль, и адрес электронной почты, то вход будет осуществляться по паролю. После выпуска и назначения на ресурс токена, для пользователя при входе также будет запрошен одноразовый пароль с этого токена.

Некоторые вспомогательные компоненты, например **Protectimus RPrproxy**, могут автоматически создавать пользователей, уже готовых к использованию портала самообслуживания. Например, при работе RPrproxy с Citrix NetScaler Gateway.



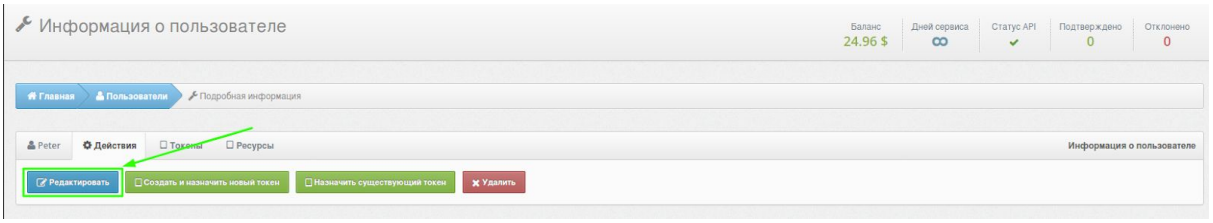
Редактирование пользователей

Для редактирования информации о пользователе нажмите на кнопку **“Пользователи”** в меню слева, найдите его в списке всех пользователей и нажмите на его **Логине**. После чего, вы попадете на страницу просмотра детальной информации пользователя.



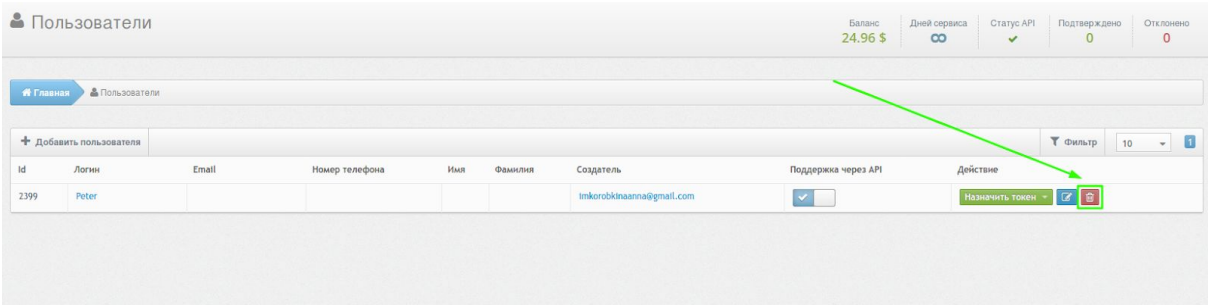
Перейдите на вкладку **“Действия”**.

Нажмите кнопку **“Редактировать”**, внесите необходимые правки и сохраните изменения. Также на этой вкладке можно создать и назначить пользователю новый токен, назначить уже созданный ранее токен или удалить этого пользователя.



Удаление пользователей

Для удаления пользователя нажмите на кнопку **“Пользователи”** в меню слева, чтобы перейти к списку пользователей, найдите его в списке всех пользователей и нажмите на **красную кнопку с изображение корзины** (первая кнопка справа).



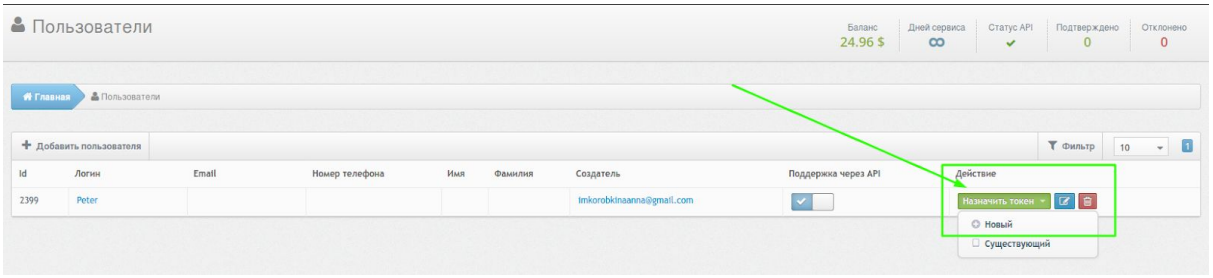
Как назначить токен пользователю

Необходимо указать каким токеном владеет каждый пользователь. Вы можете сделать это тремя способами:

- назначить пользователю уже существующий токен;
- создать токен, если это не было сделано раньше, а потом назначить его пользователю;
- активировать портал самообслуживания, через который пользователи сами смогут создавать программные и активировать аппаратные токены.

Как создать новый токен

Нажмите на кнопку **“Пользователи”** в меню слева, найдите нужного пользователя в списке всех пользователей, нажмите кнопку **“Назначить токен” - “Новый”**



Выберите токен, который хотите добавить. Это могут быть:

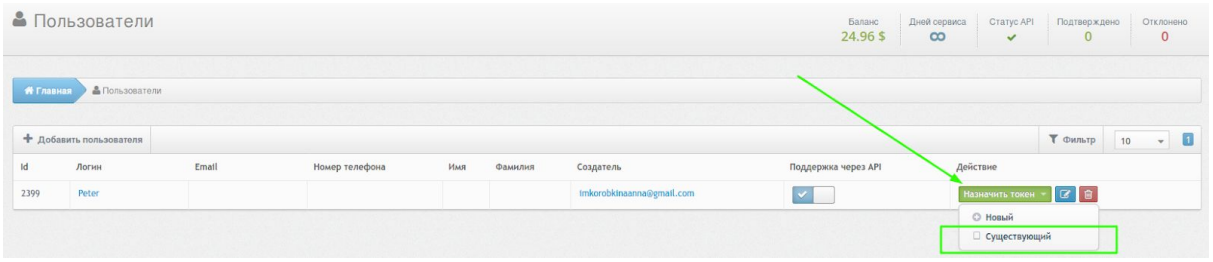
- Аппаратные токены (Protectimus One, Two, Slim, Ultra, Crystal или токены других производителей).
- Программные токены (приложение Protectimus Smart, e-mail, SMS, чат-боты в Messenger, Telegram, Viber).
- Универсальный токен (через этот механизм можно добавить любые аппаратные токены сторонних производителей).

После выбора нужного типа токена необходимо будет заполнить все необходимые поля, ввести одноразовый пароли с токена и нажать кнопку **“Сохранить”**.

Более подробно о создании токенов читайте в разделе Токены.

Как назначить уже существующий токен

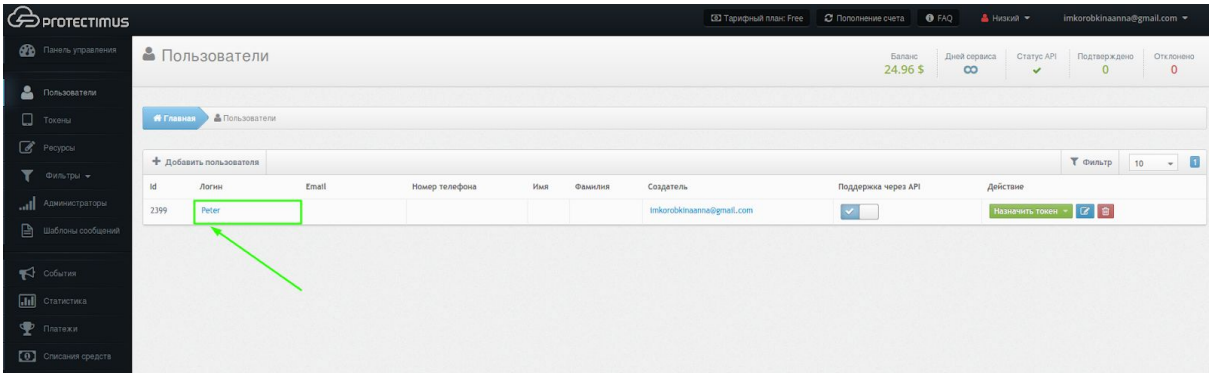
Если вы уже создали токен (подробно о создании токенов читайте в разделе Токены), нажмите на кнопку **“Пользователи”** в меню слева, найдите нужного пользователя в списке всех пользователей, нажмите кнопку **“Назначить токен”** - **“Существующий”**, выберите нужный токен из списка и нажмите **“Назначить”**.



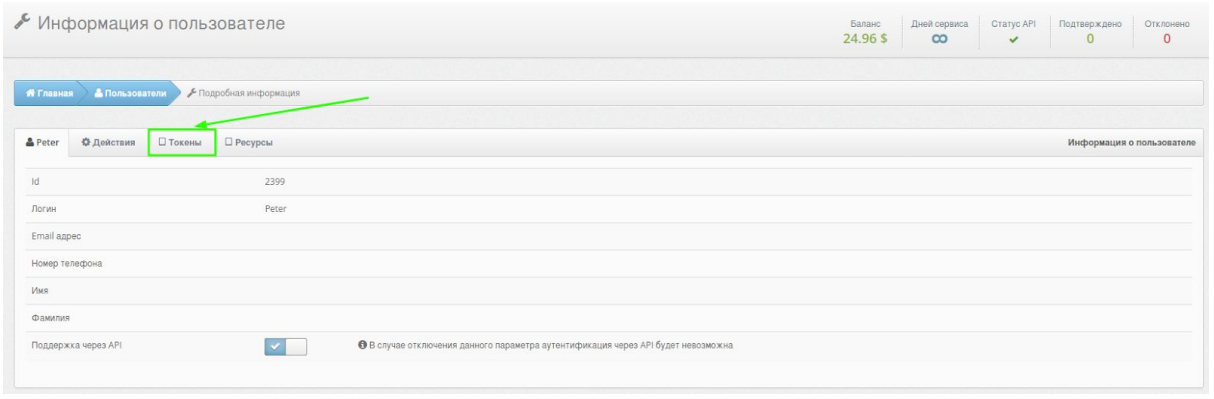
Как деактивировать токен пользователя

Если пользователь потерял токен, но вы хотите предоставить ему срочный доступ, достаточно лишь выключить токен, тогда токен не будет участвовать в процессе аутентификации пользователя.

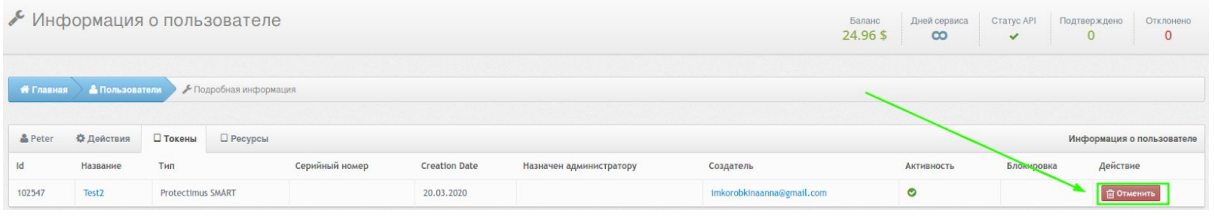
Для отключения токена перейдите в раздел **Пользователи** в системе Protectimus (нажмите на кнопку **“Пользователи”** в меню слева), найдите нужного пользователя в списке и нажмите на его **Логине**.



Перейдите во вкладку **“Токены”**.



Нажмите кнопку **“Отменить”**.



Об удалении и перевыпуске токенов читайте в разделе Токены.

6. Токены

Мы условно разделяем токены на физические и программные. Это разделение связано с особенностями введения и использования секретного ключа в конкретном виде токенов. К программным токенам относятся: Protectimus SMART, Google Authenticator, Protectimus SMS, Protectimus BOT и Protectimus MAIL токены, к физическим - Protectimus One, Protectimus Two, Protectimus Slim, Protectimus Ultra, а также токены других производителей.

В нашей системе могут использоваться любые токены, которые работают по стандартным алгоритмам OATH. Это может быть сделано в режиме добавления универсального токена. В таком случае от вас потребуется больше знаний о вашем токене. Поэтому мы реализовали поддержку нескольких популярных токенов других производителей, что значительно облегчает задачу.

Количество доступных для создания токенов ограничивается выбранным вами тарифным планом. Если вам необходимо создать больше токенов - выберите желаемое количество токенов настроив собственный тарифный план. Действия по выбору тарифного плана доступны только главному администратору.

Администратор может создавать токены и назначать их пользователям вручную или активировать Портал самообслуживания, через который пользователи смогут самостоятельно выполнять ряд действий по выпуску и обслуживанию токенов, а также их собственных данных. Набор доступных пользователю действий определяет администратор системы. Портал самообслуживания подключается и настраивается индивидуально для каждого ресурса.

Токены, которые есть в системе могут быть использованы не только вашими пользователями, но и вами или вашими администраторами для защиты доступа к Protectimus. Поэтому, токеном, который назначен администратору, может управлять только администратор, которому он назначен. Для остальных токенов подход такой же, как и для других объектов в системе: редактировать могут все, удалить может только создатель либо главный администратор.

Если пользователь потерял токен, но вы хотите предоставить ему срочный доступ - вам достаточно лишь деактивировать токен, тогда токен не будет участвовать в процессе аутентификации пользователя.

Если же токен утерян администратором - ему необходимо воспользоваться механизмом резервного доступа для подтверждения оставшихся аутентификаторов. После этого будет создана заявка на отключение токена. Удовлетворить ее может главный администратор либо служба технической поддержки.

ОБРАТИТЕ ВНИМАНИЕ!

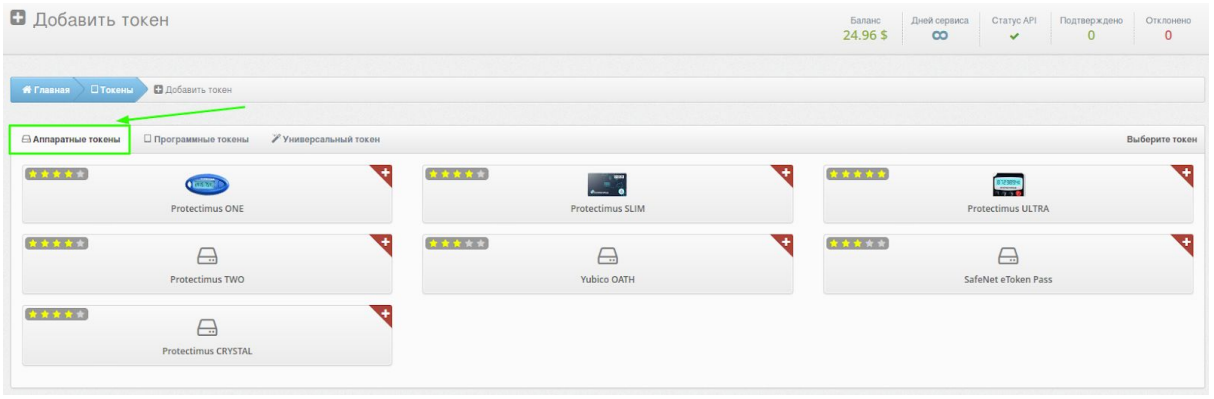
Один пользователь может использовать только один токен для аутентификации в рамках одного ресурса.

Создание токенов вручную

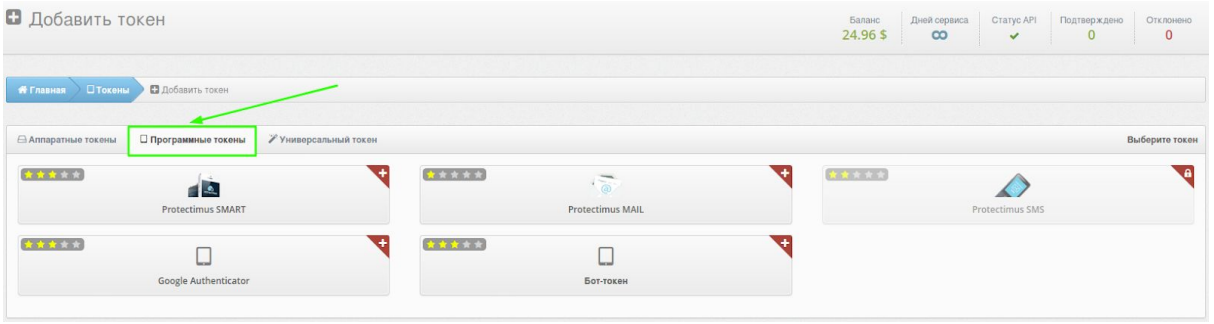
Чтобы создать токен нажмите на кнопку **“Токены”** в меню слева, а затем нажмите на кнопку **“Добавить токен”** в заголовке таблицы.

После этого выберите токен, который хотите добавить. Это могут быть:

1. **Аппаратные токены**. Protectimus One, Protectimus Two, Protectimus Slim, Protectimus Ultra, Protectimus Crystal, Yubiko OATH, SafeNet eToken Pass.



2. **Программные токены**. Приложение для генерации одноразовых паролей Protectimus Smart, доступное для iOS и Android, любые другие мобильные аутентификаторы, доставка OTP пароля по e-mail, SMS или через чат-боты в мессенджерах Facebook Messenger, Telegram, Viber.

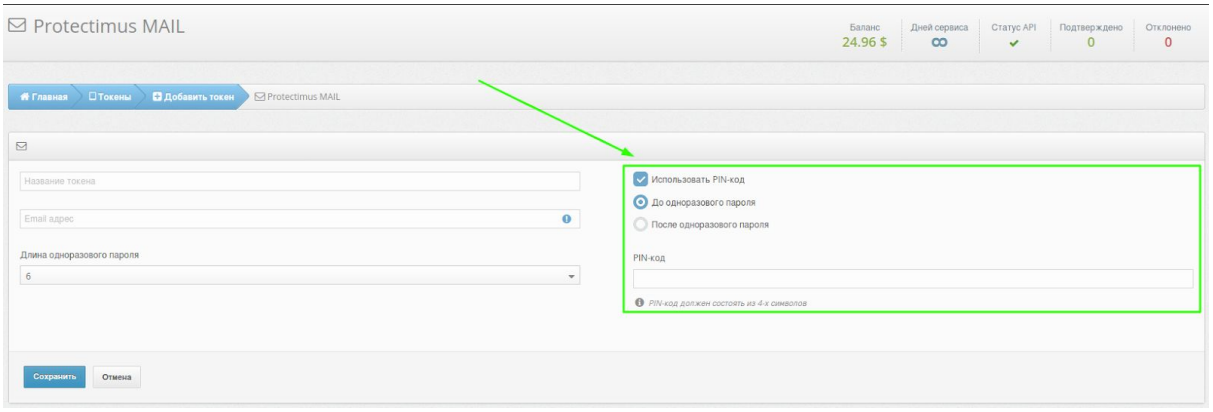


3. **Универсальный токен.** Через этот механизм можно добавить любые аппаратные токены других производителей

После выбора нужного типа токена необходимо будет заполнить все необходимые поля, ввести одноразовый пароли с токена и нажать кнопку **“Сохранить”**.

ОБРАТИТЕ ВНИМАНИЕ!

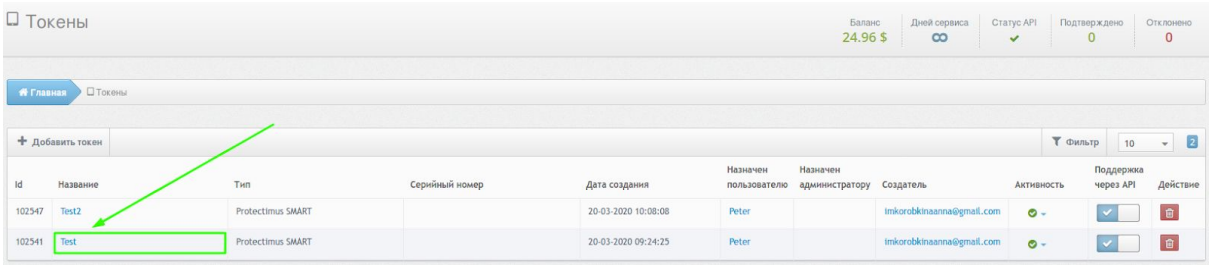
При создании токена любого типа вам доступна функция использования **PIN-кода**. Если вы активируете эту функцию, пользователь должен будет вводить заданный PIN-код каждый раз вместе с одноразовым паролем (до или после одноразового пароля, в зависимости от выбора администратора). Это дополнительный уровень защиты учетной записи пользователя. Даже если злоумышленник подберет пароль и завладеет токеном пользователя, он не сможет скомпрометировать учетную запись без PIN-кода.



После создания токена, необходимо присвоить токен конкретному пользователю (назначить токен пользователю) и связать пользователя с токеном с ресурсом (назначить токен с пользователем на ресурс).

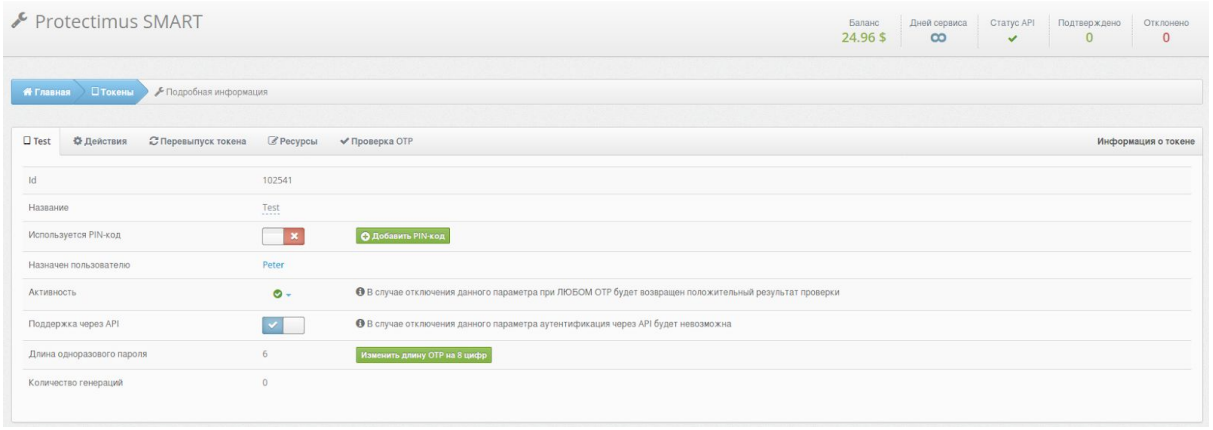
Редактирование токена

Нажмите на кнопку **“Токены”** в меню слева, найдите нужный токен в списке всех токенов, нажмите на его **название**.



Вы попадете на страницу просмотра детальной информации о токене где сможете:

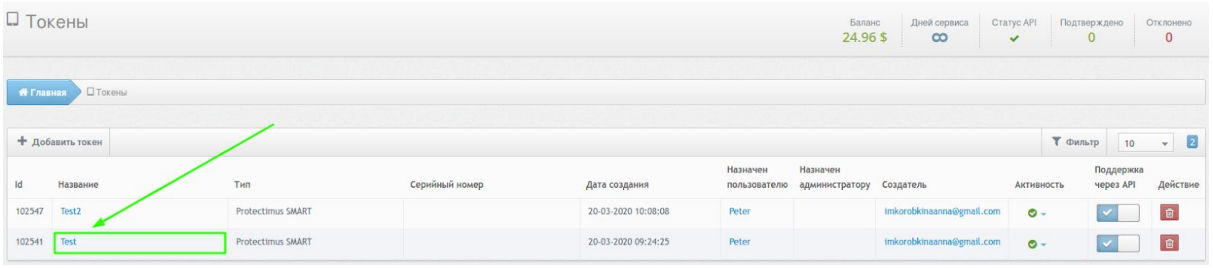
- изменить название токена,
- добавить/изменить/удалить PIN код,
- изменить длину одноразового пароля.



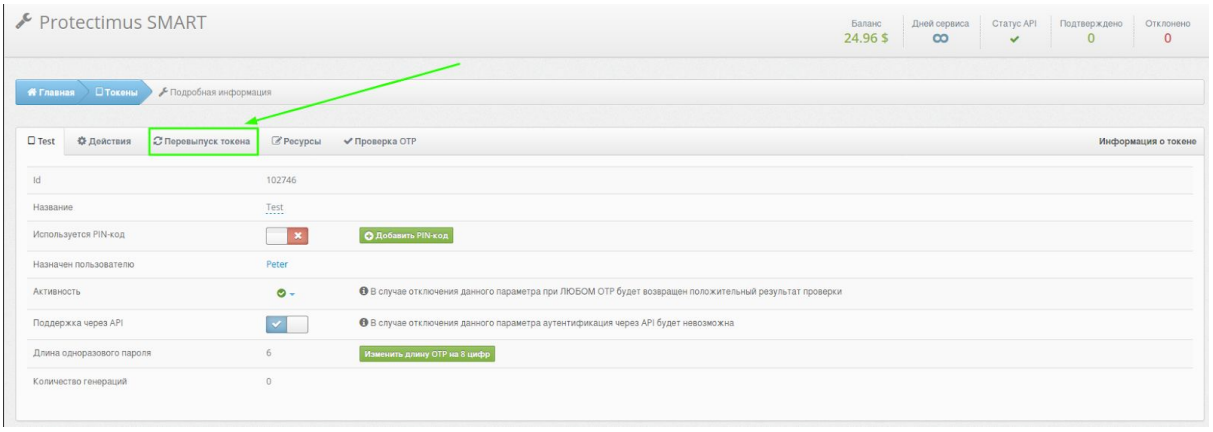
Перевыпуск токена

Если пользователь потерял токен, но вы хотите предоставить ему срочный доступ, достаточно деактивировать токен, тогда токен не будет участвовать в процессе аутентификации пользователя.

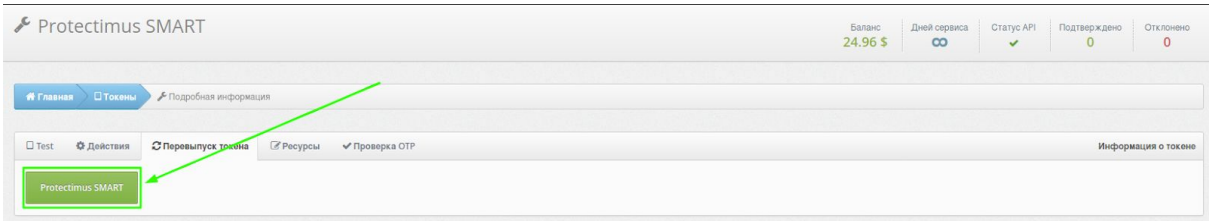
Для **перевыпуска токена** нажмите на кнопку **“Токены”** в меню слева, найдите нужный токен в списке всех токенов, нажмите на его **название**.



Перейдите во вкладку **“Перевыпуск токена”**.



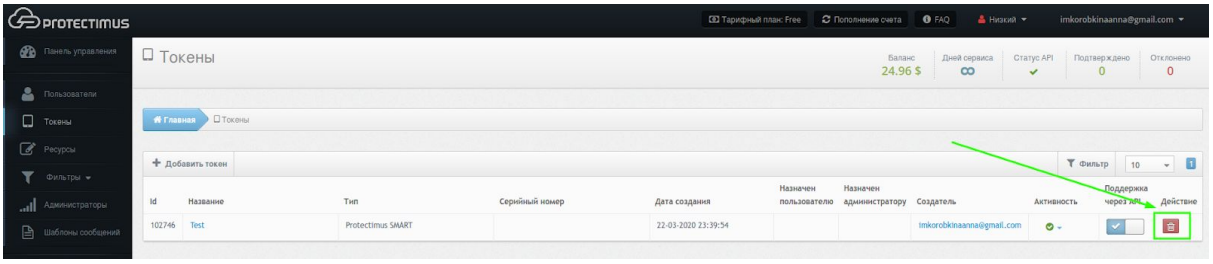
Нажмите на название токена, заполните все необходимые поля и нажмите кнопку **“Перевыпустить”**.



Удаление токена

Удалить токен может только создатель или главный администратор.

Чтобы удалить токен, нажмите на кнопку **“Токены”** в меню слева, найдите нужный токен в списке всех токенов и нажмите на **красную кнопку с изображение корзины** (первая кнопка справа).



Портал самообслуживания

Механизм самообслуживания позволяет пользователям самостоятельно выполнять ряд действий по выпуску и обслуживанию токенов, а также их собственных данных. Набор доступных пользователю действий определяет администратор системы.

Список возможных действий:

- Регистрация и назначение нового токена
- Назначение существующего токена
- Перевыпуск токена
- Отменить назначение токена
- Синхронизация токена
- Настройка PIN-кода
- Удаление PIN-кода
- Создание пароля
- Изменение пароля
- Изменение почты
- Изменение контактного телефона
- Изменение логина
- Изменение имени и фамилии
- Работа с окружением пользователя

ОБРАТИТЕ ВНИМАНИЕ!

Компонент Rproxy в состоянии самостоятельно подготавливать пользователей к работе с механизмом самообслуживания.

Детальная инструкция по настройке портала самообслуживания с заметками для интеграций через компонент RProxy доступна здесь.

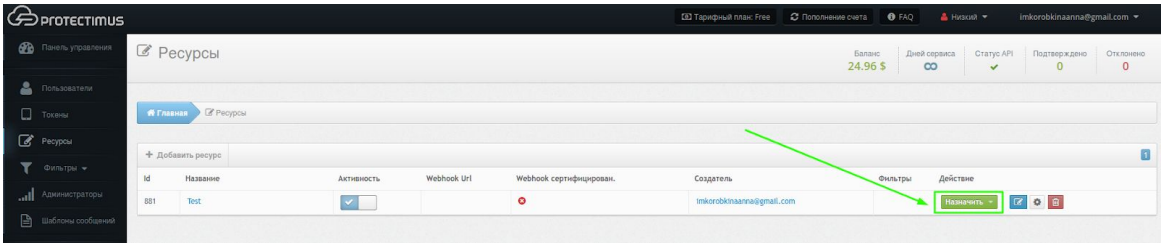
7. Назначение пользователей и токенов на ресурс

Аутентификация пользователя всегда проводится для определенного ресурса, следовательно пользователь должен быть назначен на ресурс, к которому он должен иметь доступ. Если пользователь не назначен на ресурс - пользователь не имеет к нему доступа. Способ назначения пользователя на ресурс зависит от выбранного способа аутентификации. Protectimus поддерживает несколько способов аутентифицировать пользователя:

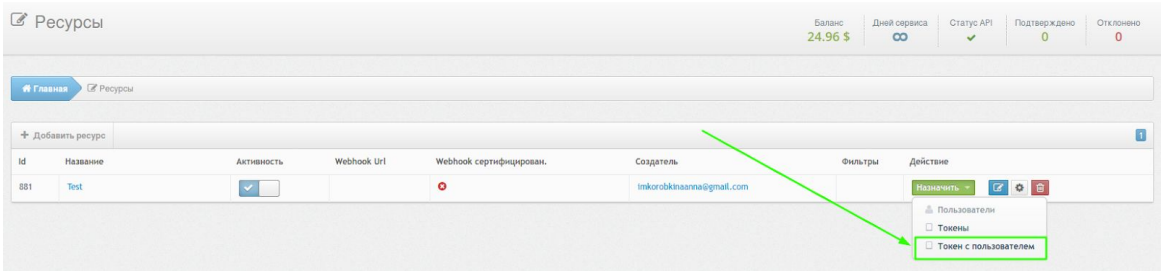
1. **Аутентификация пользователя по статическому паролю.** Для работы этого метода у пользователя должен быть задан пароль и пользователь должен быть назначен на ресурс для которого выполняется проверка.
2. **Аутентификация пользователя по одноразовому паролю.** Для этого у пользователя должен быть токен, и пользователь должен быть назначен на ресурс ВМЕСТЕ с токеном. Назначение на ресурс отдельно пользователя и отдельно токена будет неправильным для работы этого метода.
3. **Аутентификация пользователя по статическому и одноразовому паролю.** Является комбинацией двух вышеописанных методов. Пользователь должен быть назначен на ресурс ВМЕСТЕ с токеном. У пользователя должен быть задан пароль. Если токен пользователя будет отключен, то проверка OTP выполняться не будет, в таком случае будет проверен только статический пароль и проходит ли пользователь фильтры, если они существуют.
4. **Аутентификация токена на ресурсе.** Этот способ позволяет не привязывать токен к какому-то конкретному пользователю и просто проверять валидность сгенерированного одноразового пароля. При использовании этого способа токен должен быть назначен на ресурс.

Как назначить токен с пользователем на ресурс

Перейдите на страницу **“Ресурсы”**, нажмите кнопку **«Назначить»**.



Выберите **“Токен с пользователем”**, выберите токены, которые должны быть назначены на ресурс и нажмите **“Назначить”**.



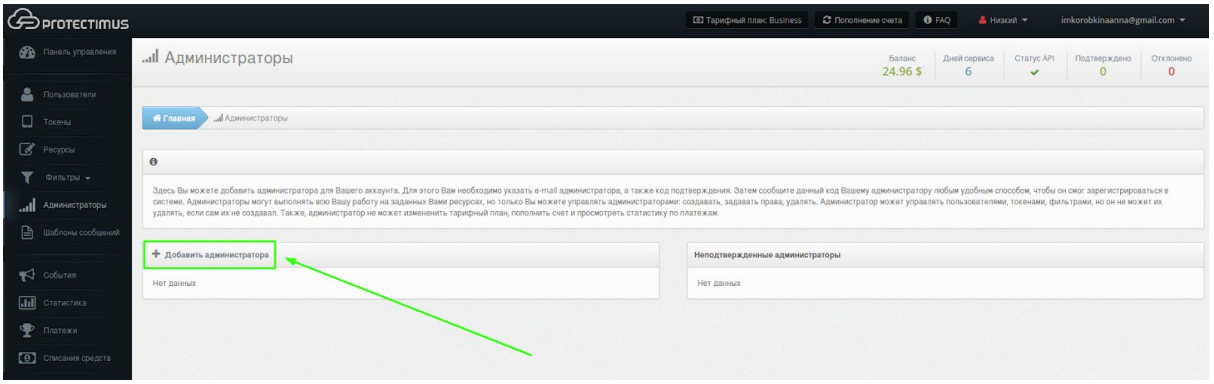
8. Администраторы

Для эффективного управления большим количеством пользователей и ресурсов вам может потребоваться помощь. Создайте администратора и вы сможете делегировать ему желаемый объем работ. Администратору доступно управление только теми ресурсами, которые вы ему разрешите, таким образом, он будет ответственен только за свой участок работ.

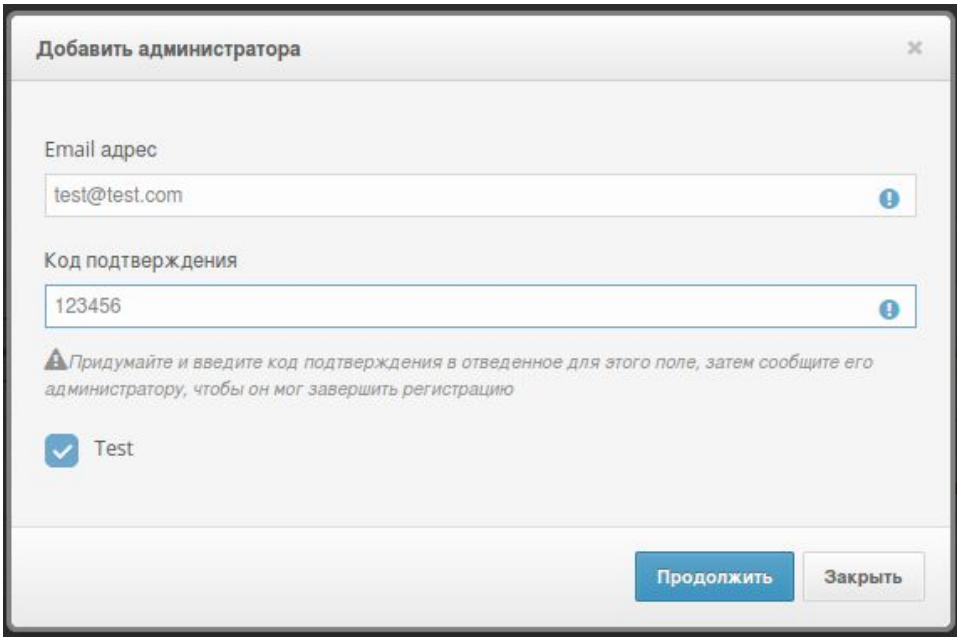
Администраторы могут выполнять всю вашу работу на заданных вами ресурсах, но только вы можете управлять администраторами: создавать, задавать права, удалять. Администратор может управлять пользователями, токенами, фильтрами, но он не может их удалять, если сам их не создавал. Также, администратор не может изменить тарифный план, пополнить счет и просмотреть статистику по платежам.

Количество доступных для создания Администраторов ограничивается выбранным вами тарифным планом. Если вам необходимо создать больше Администраторов - выберите желаемое количество настроив собственный тарифный план. Действия по выбору тарифного плана доступны только главному администратору.

Чтобы создать Администратора, перейдите в раздел **Администраторы** (нажмите на кнопку **“Администраторы”** в меню слева) и нажмите на кнопку **“Добавить администратора”**.



Укажите **e-mail администратора**, **код подтверждения** и **выберите ресурсы**, доступ к которым будет у администратора и нажмите **“Продолжить”**.



Затем сообщите данный код вашему администратору любым удобным способом, чтобы он смог зарегистрироваться в системе.

9. Фильтры

Если вам необходимо ограничить доступ к своему ресурсу в зависимости от страны, в которой находятся пользователи, вы можете создать географический фильтр. А для случая, когда есть необходимость ограничить доступ пользователей к ресурсу в зависимости от времени входа, то вы имеете возможность создать временной фильтр.

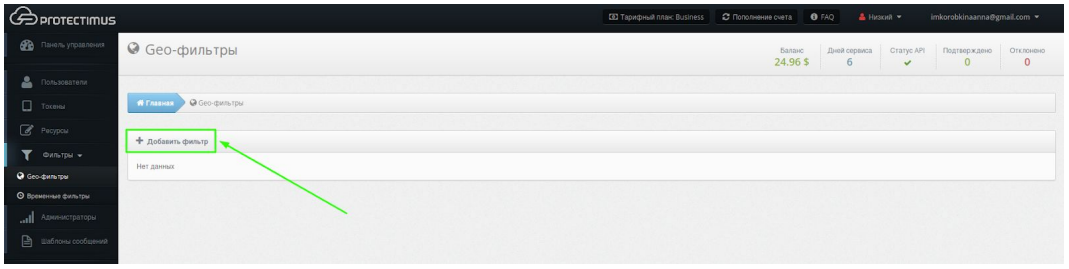
Созданный фильтр необходимо назначить на ресурс, к которому вы хотите его применить.

Количество доступных для создания фильтров ограничивается выбранным вами тарифным планом. Если вам необходимо создать больше фильтров - выберите желаемое количество фильтров, настроив собственный тарифный план. Действия по выбору тарифного плана доступны только главному администратору.

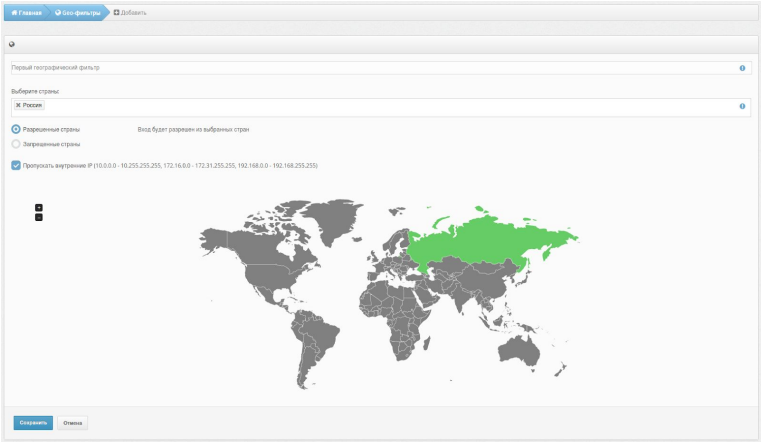
Как создать географический фильтр

Эта функция позволяет открывать доступ к ресурсу только из определенных стран. Если пользователь приходит из запрещенной страны, то у него не будет доступа к сайту, если из разрешенной, то система запросит одноразовый пароль. Также можно запретить доступ из избранных стран.

Перейдите в раздел **Geo-фильтры** (нажмите на кнопку **“Фильтры” - “Geo-фильтры”** в меню слева) и нажмите кнопку **“Добавить фильтр”**.



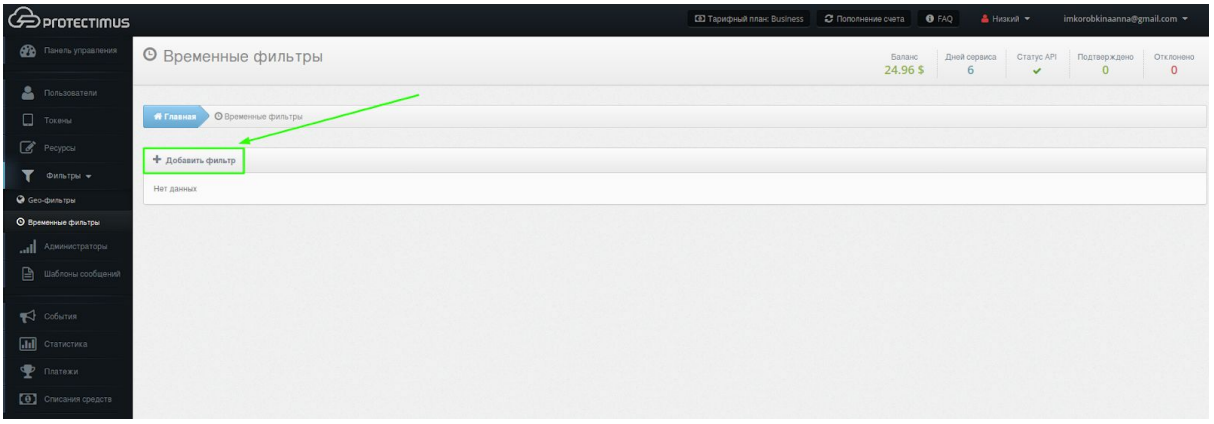
Введите название фильтра и выберите страны в которых будет разрешен или запрещен доступ к вашему ресурсу. После этого нажмите **“Сохранить”**.



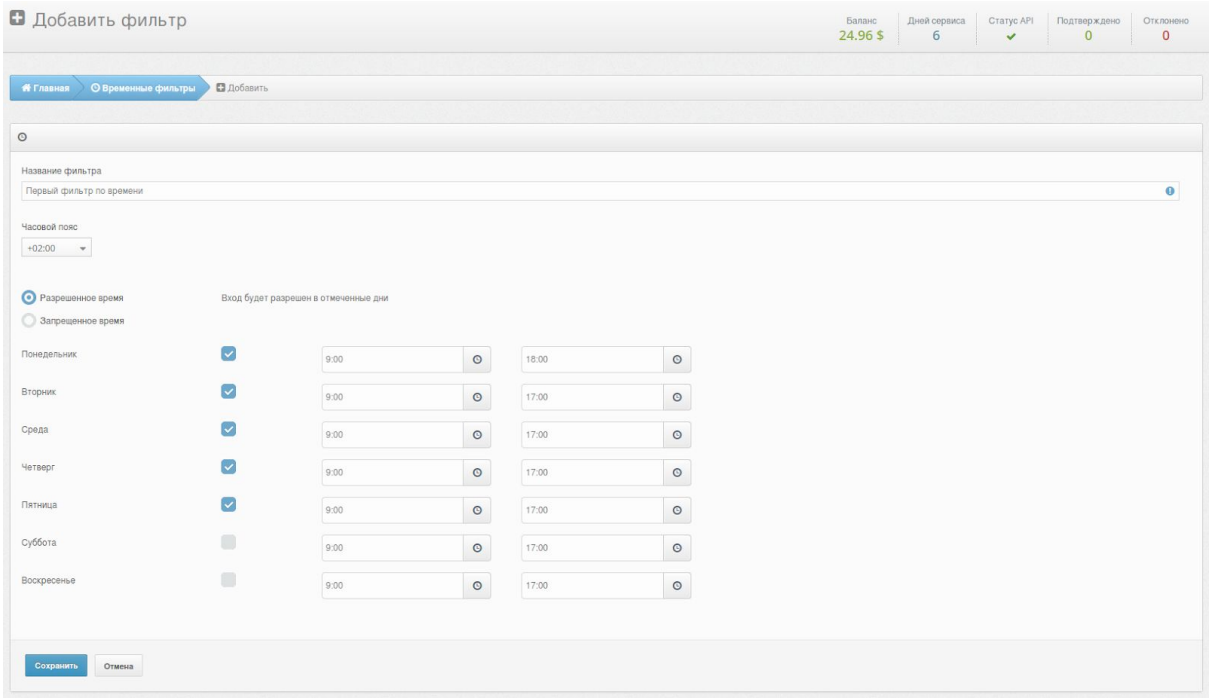
Как создать временной фильтр

Эта функция позволяет открывать доступ к ресурсу только в определенные часы, например, только в рабочее время. Такой подход значительно повышает уровень защиты аккаунтов от несанкционированного доступа. Отлично подходит для корпоративного сектора, даже если сотрудник забыл токен на рабочем месте, никто не сможет войти в его аккаунт в нерабочие часы.

Перейдите в раздел **Временные фильтры** (нажмите на кнопку **“Фильтры” - “Временные фильтры”** в меню слева) и нажмите кнопку **“Добавить фильтр”**.

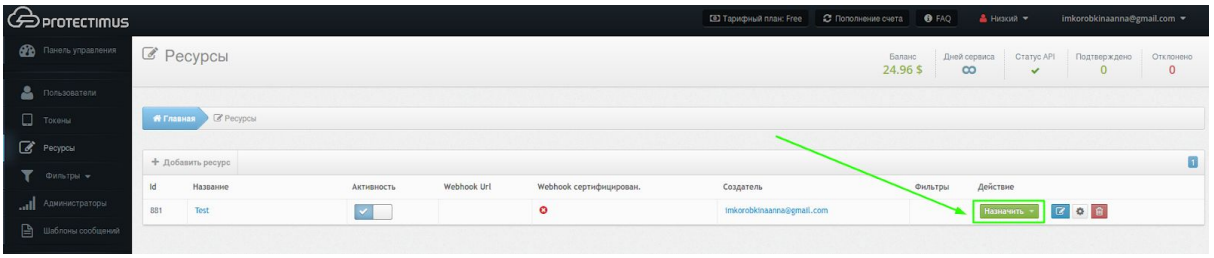


Введите название фильтра, укажите часовой пояс, отметьте дни недели и укажите время, в которое будет разрешен или запрещен доступ к вашему ресурсу. После этого нажмите **“Сохранить”**.

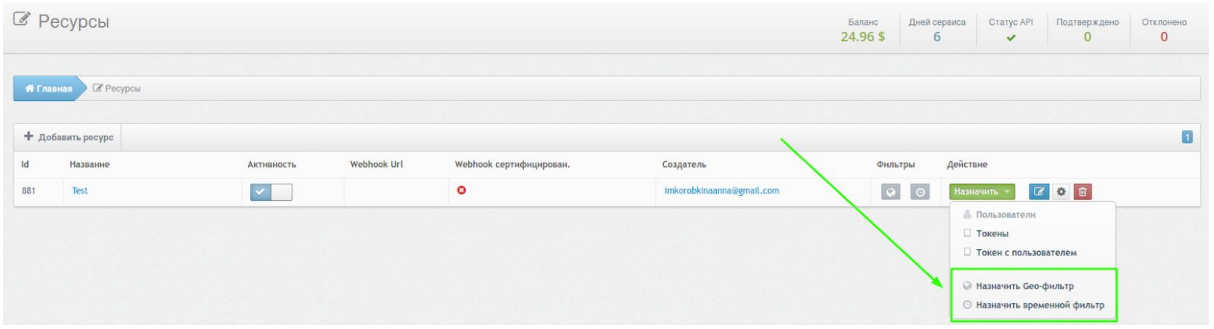


Как назначить фильтры на ресурс

Перейдите на страницу **“Ресурсы”**, выберите нужный ресурс и нажмите кнопку **«Назначить»**.



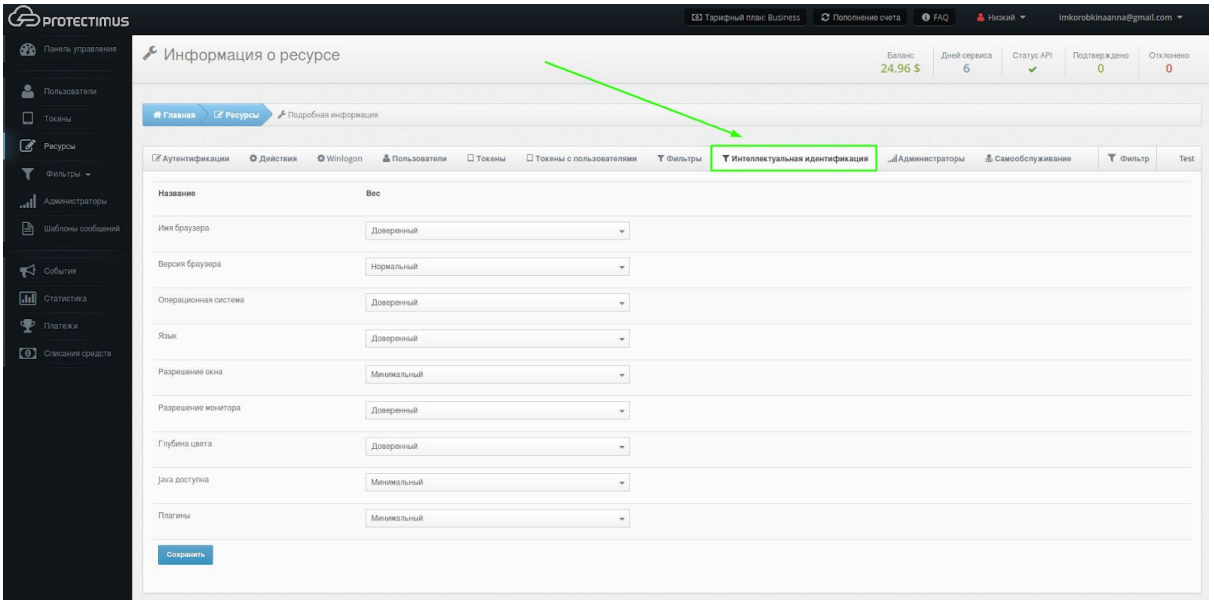
Выберите **Geo-фильтр** или **Временной фильтр** в зависимости от того какой фильтр вы хотите назначить. После этого выберите нужный фильтр из списка, который появится, и нажмите **“Назначить”**.



10. Интеллектуальная идентификация

Эту функцию также можно назвать анализом окружения пользователя. Она создана для удобства конечных пользователей в системах, где подобная лояльность допустима. Функция интеллектуальной идентификации позволяет анализировать окружение пользователя (какое имя браузера, версия браузера, операционная система, язык, разрешение окна, разрешение монитора, глубина цвета, доступна Java или нет, плагины) и запрашивать одноразовый пароль только когда допустимы порог несовпадений превышен.

Чтобы активировать функцию интеллектуальной идентификации, перейдите в раздел **Ресурсы** (нажмите на кнопку **“Ресурсы”** в меню слева), выберите нужный ресурс из списка, нажмите на его **название** и перейдите на вкладку **“Интеллектуальная идентификация”**.



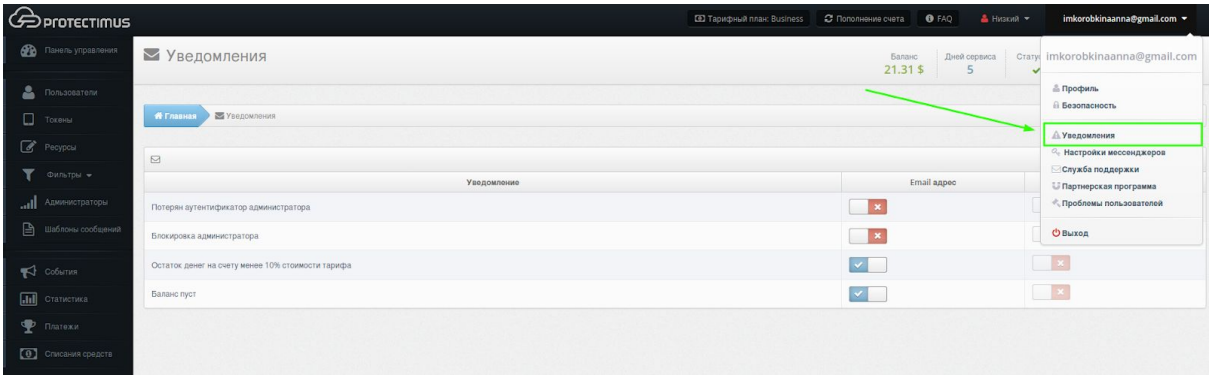
Установите вес каждого параметра (минимальный, нормальный или доверенный) и сохраните настройки.

11. Уведомления о событиях

Вы можете получать уведомления о следующих событиях по электронной почте или по СМС.

- Потерян аутентификатор администратора
- Блокировка администратора
- Остаток денег на счету менее 10% стоимости тарифа
- Баланс пуст

Чтобы перейти на страницу настройки уведомлений, нажмите на **свой email в верхнем правом углу** и выберите **Уведомления**.



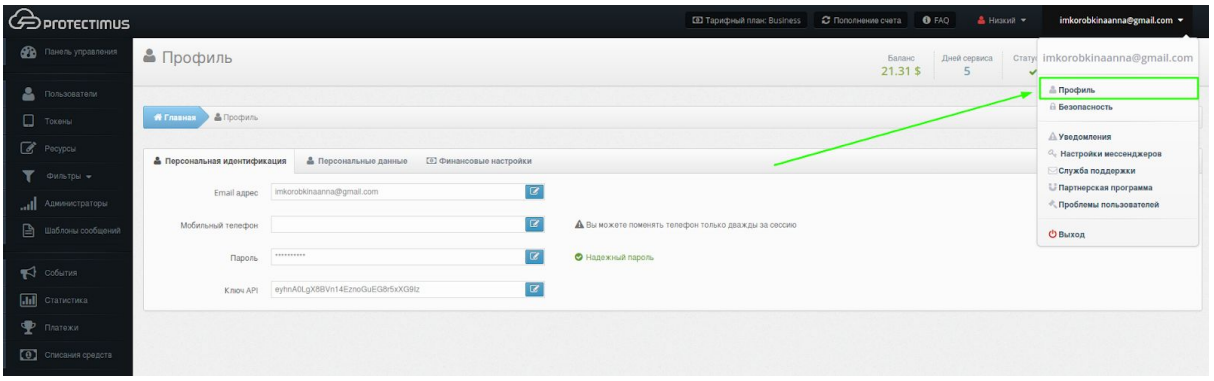
Чтобы получать уведомления по SMS, [укажите свой номер телефона в настройках профиля](#).

12. Защита учетной записи Protectimus

Надежность всей системы определяется надежностью самого слабого звена. Проверьте настройки безопасности и убедитесь, что ваша собственная учетная запись в системе Protectimus защищена надежно.

Используйте безопасный пароль

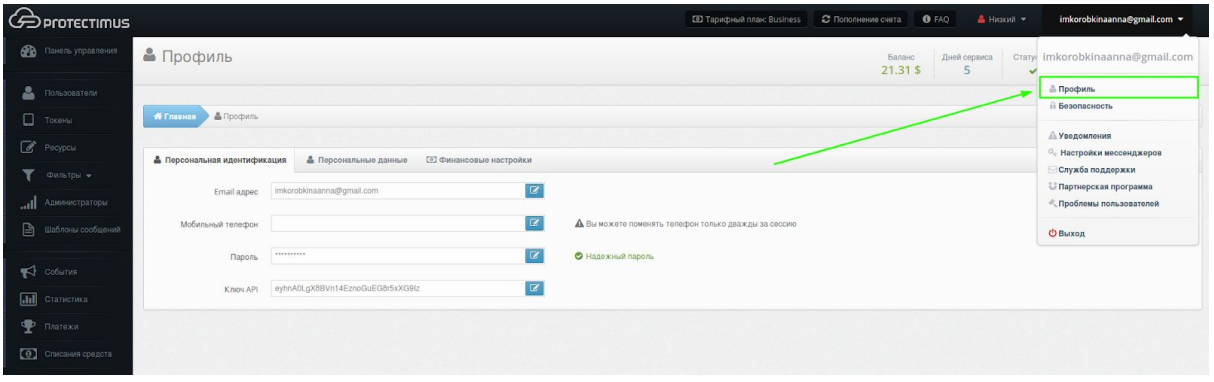
Чтобы изменить пароль, войдите в настройки профиля. Нажмите на **свой email в верхнем правом углу** и выберите **Профиль**.



Безопасный пароль должен состоять как минимум из 10 символов, содержать буквы в разных регистрах, цифры и знаки. Чем длиннее пароль и чем больше разнообразных символов в нем использовано, тем сложнее его подобрать. Помните, что вы должны использовать разные пароли для разных ресурсов и, желательно, периодически менять эти пароли.

Укажите свой номер телефона

Чтобы указать номер телефона, войдите в **настройки профиля**. Нажмите на **свой email в верхнем правом углу** и выберите **Профиль**.



Номер телефона не используется при аутентификации, но в некоторых случаях, при изменении важных параметров Protectimus может запросить подтверждение владения телефоном, отправив проверочный код на указанный вами номер. Это усложняет

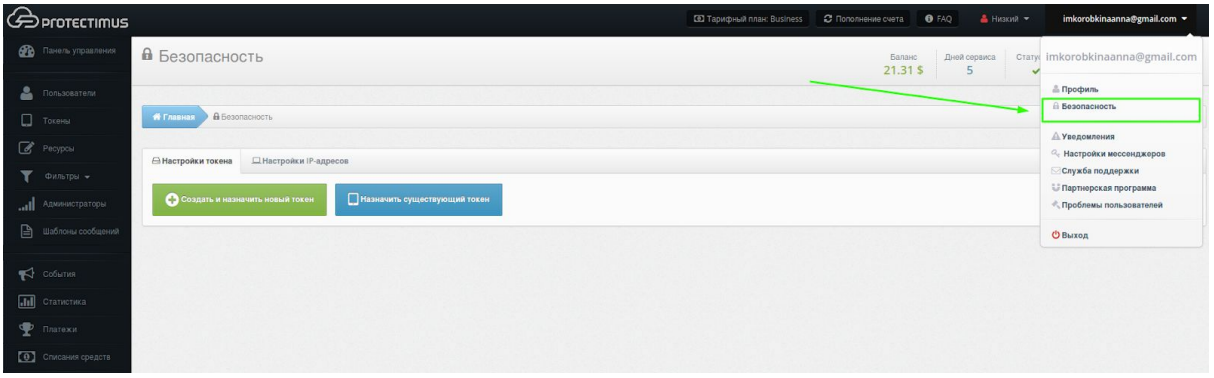
работу злоумышленнику и подает вам сигнал, о том, что кто-то получил доступ к вашему аккаунту и пытается сделать в нем важные изменения.

Также, указав телефон и настроив получение уведомлений через SMS, вы получаете оперативное информирование о важных событиях в системе.

Ваш номер не будет передан третьей стороне и не будет использоваться в целях, отличных от обеспечения вашей безопасности и информированности.

Используйте токен для надежной защиты аккаунта

Чтобы настроить двухфакторную аутентификацию для своей учетной записи в Protectimus, войдите в **настройки безопасности**. Нажмите на **свой email в верхнем правом углу** и выберите **Безопасность**.

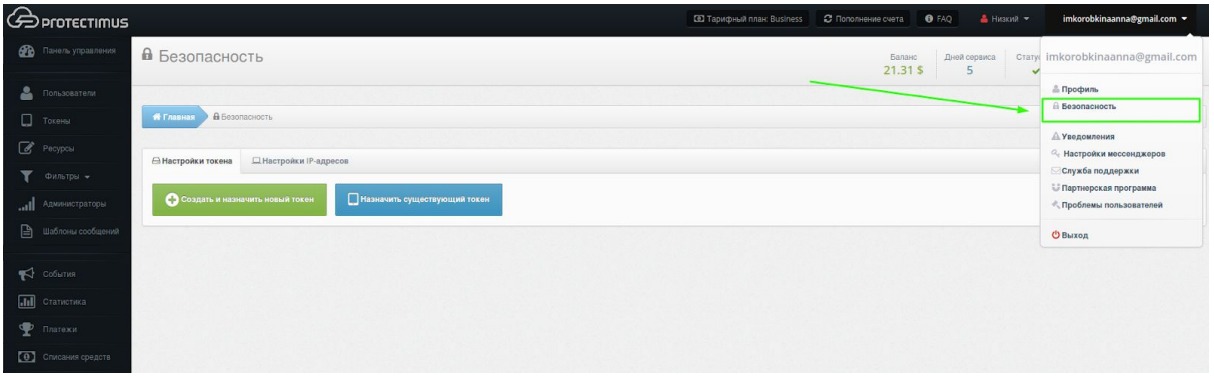


Вы можете создать новый токен или назначить уже существующий токен. Более подробно о типах токенов читайте в разделе Токены.

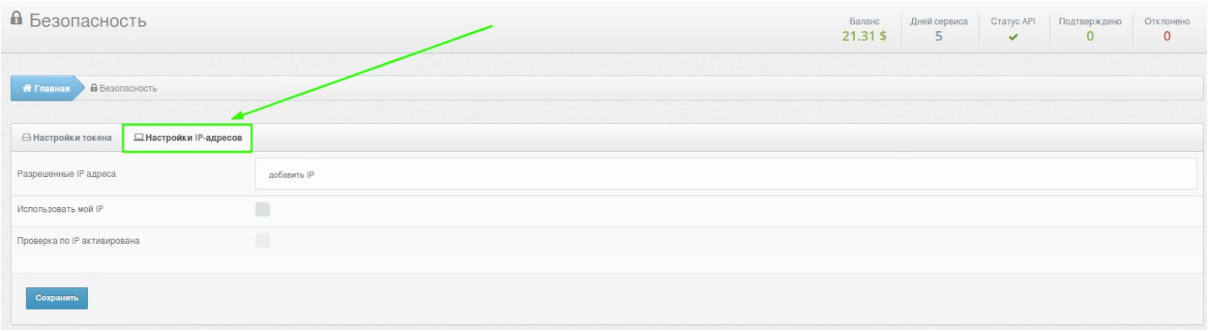
Ограничьте IP-адреса, с которых разрешен доступ

Если вы заходите в систему из нескольких постоянных мест, имеет смысл ограничить доступ к системе только из нескольких IP-адресов. Задать разрешенные адреса вы можете на странице настройки безопасности на вкладке "Настройки IP-адресов".

Чтобы войти в **настройки безопасности**, нажмите на **свой email в верхнем правом углу** и выберите **Безопасность**.



Выберите вкладку **“Настройки IP-адресов”**, добавьте нужные IP адреса, активируйте проверку по IP и нажмите **“Сохранить”**.



Контакты

Технические вопросы, распространение программного обеспечения:

support@protectimus.com

Потенциальное партнерство, продажи:

sales@protectimus.com

Телефон:

Ирландия +3 537 688 899 22

США: +1 786 796 66 64

Великобритания: +44 20 3808 7124

Украина: +38 057 706 21 24

Россия: +7 499 677 16 34

Корпоративная информация

Protectimus Ltd

Carrick house,

49 Fitzwilliam Square,

Dublin D02 N578,

Ireland