

УТВЕРЖДЕН  
РОФ.42584334.58.29.12.01 ЛУ

Программное обеспечение «Мультифактор»

Руководство пользователя

РОФ.42584334.58.29.12.01 РП 01

Листов 60

## **Аннотация**

В документе содержатся сведения о назначении Программное обеспечение «Мультифактор» РОФ.42584334.58.29.12.01 (далее – ПО «КОМРАД»), изделие, объект оценки (ОО), комплекс), условиях применения, последовательности действий оператора, обеспечивающих загрузку, запуск, выполнение и завершение работы программного изделия. Также приведены описания функций, формата и возможных вариантов команд, с помощью которых оператор осуществляет загрузку и управляет выполнением программного изделия, ответы программного изделия на эти команды, тексты сообщений, выдаваемых в ходе выполнения программного изделия.

## Оглавление

Аннотация.....	2
Общая информация.....	6
Двухфакторная аутентификация .....	6
В чем проблема паролей .....	6
Что дает двухфакторная аутентификация .....	7
Начало работы.....	8
Возможности Мультифактора .....	9
Обзор решения .....	9
Компоненты платформы .....	10
1. Мультифакторная аутентификация и контроль доступа (MFA).....	10
1.1. Доступные методы аутентификации.....	11
2. Единый Вход (SSO) .....	12
3. Портал Самообслуживания (SSP) .....	12
4. Аудит-трейл и уведомления .....	12
5. Личный кабинет администратора.....	12
6. Инструменты разработчика - REST API.....	12
Ценностное предложение.....	13
Сотрудники.....	13
Менеджмент .....	13
СЕО.....	14
СФО.....	14
СОО .....	14
ССО.....	14
Режимов работы средства .....	14
Штатный режим .....	14
Аварийный режим.....	15
Принципов безопасной работы средства Защита учётных данных .....	16
Описание личного кабинета .....	16
Общее описание .....	16
Вход.....	16
Главная.....	17
Ресурсы .....	18
Функций и интерфейсов функций средства, доступных каждой роли пользователей .....	21
Пользователи.....	21
Группы .....	24

Безусловный и условный запрос второго фактора .....	25
Запросы доступа.....	28
Проект .....	29
Настройки .....	29
Учетные записи .....	30
СМС.....	30
Звонки .....	32
Расширенное API .....	32
Поставщики учетных записей .....	33
Диапазоны IP .....	33
Журнал .....	34
Тариф и оплата .....	34
Способы аутентификации .....	36
Сводная таблица.....	36
Мобильное приложение Multifactor .....	36
Регистрация .....	36
Аутентификация.....	36
Универсальная web аутентификация с поддержкой биометрии .....	36
Регистрация .....	37
Аутентификация.....	37
Маскирование логинов в мобильном приложении .....	37
Система маскирования .....	37
Как работает .....	37
Включение функции .....	38
ОТР Токен.....	40
Регистрация .....	40
Аутентификация.....	40
НОТР Токен.....	40
Регистрация .....	40
Аутентификация.....	41
Google authenticator .....	41
Регистрация .....	41
Аутентификация.....	41
СМС сообщение или звонок .....	41
Регистрация .....	41
Аутентификация.....	41
Регистрация пользователей в системе .....	42

Способы регистрации второго фактора.....	42
Автоматизация .....	42
Экспорт пользователей из Active Directory .....	42
Импорт пользователей через API и отправка конфигурационных email .....	43
Способы аутентификации .....	45
Мобильное приложение Multifactor .....	45
Биометрия и U2F.....	47
Google Authenticator/Я.Ключ .....	48
ОТР-токен .....	50
Мобильное приложение Multifactor .....	52
Функциональные возможности .....	52
Мои аккаунты.....	52
Добавление аккаунта .....	53
Удаление аккаунта .....	53
Настройки мобильного приложения Multifactor.....	54
Запрос доступа от Multifactor .....	55
Push-системы .....	56
Внешние приложения.....	57
Визуализация антиспама .....	58
Кто попадает в антиспам.....	58
Действий после сбоев и ошибок эксплуатации средства.....	58

## 1 Общая информация

### 1.1 Двухфакторная аутентификация

MULTIFACTOR — система двухфакторной аутентификации, которая позволяеткратно усилить защиту от несанкционированного доступа к вашим сайтам и приложениям.

Выражение "Двухфакторная аутентификация" или более современное название — "Многофакторная аутентификация" означает, что для проверки личности пользователя используется более одного фактора.

Всего факторов существует три вида:

1. То, что известно пользователю, обычно это логин и пароль.
2. То, что есть у пользователя, например телефон или usb-токен.
3. То, чем является пользователь — биометрические данные: отпечаток пальца, сетчатка глаза, лицо.

Наиболее уязвимым фактором является первый, наиболее защищенным — третий.

### 1.2 В чем проблема паролей

Дело в том, что люди выбирают пароли, которые легко запомнить, а значит и легко подобрать. Очень распространены варианты — свое имя, номер автомобиля или телефона, год рождения, музыкальная группа и т.п. Существуют базы данных паролей, которые когда-либо были взломаны и анализ этих баз показывает, что пароли у всех одинаковые или сформированы по единому шаблону.

Следующая проблема паролей заключается в том, что обычно пользователи устанавливают один пароль на все сайты, поэтому взлом наименее защищенного дает злоумышленнику доступ ко всем остальным.

Тенденция последних лет на "усиленные пароли", которые должны быть достаточной длины, содержать буквы разного регистра, цифры, спецсимволы, а также меняться каждые три месяца не дает эффекта. Пользователи устанавливают пароли "Password@123", следующий "Password@124", потом "Password@125" и так далее. По одной простой причине — они не могут при каждой смене запоминать новый пароль.

Отчасти проблему паролей решают программы хранения паролей, такие как keeprass, но лишь отчасти, потому что пользуются ими единицы, а помимо подбора есть еще множество способов взлома систем с аутентификацией только по паролю.

Стоит также отметить, что взлом может осуществить сотрудник компании, имеющий доступ к базе с паролями, даже, если они хранятся в рекомендованном, безопасном формате.

### **1.3 Что дает двухфакторная аутентификация**

Двухфакторная (многофакторная) аутентификация по статистике уменьшает вероятность взлома на 99% за счет использования второго и/или третьего факторов.

В отличие от паролей, второй и третий фактор невозможно подобрать, поскольку в них используются современные алгоритмы и стойкие ключи шифрования данных.

Намного меньше риск перехвата данных аутентификации при передаче по небезопасным каналам связи, так как эти данные каждый раз уникальны и ограничены по времени использования.

В многофакторной аутентификации практически отсутствует "человеческий фактор".

Все вышесказанное относится только к качественно спроектированным системам, потому что единый стандарт многофакторной аутентификации отсутствует, а необдуманные внедрения могут даже негативно сказаться на безопасности.

## 2 Начало работы

Вы решили подключить многофакторную аутентификацию — верное решение, о котором вы никогда не пожалеете. Половина дела уже сделана, осталось немного:

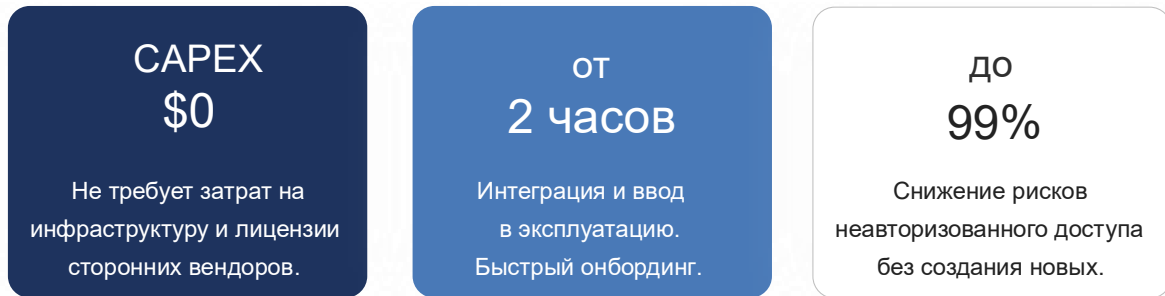
1. Зарегистрируйтесь в системе управления Мультифактором, создайте информационную систему и ресурсы.
2. Для подключения сайтов:
  - О Проанализируйте все процессы вашего приложения, которые требуется защитить от несанкционированного доступа. Как минимум это вход (логин) и восстановление пароля.
  - О Хорошей мыслью будет добавить второй фактор аутентификации для действий, требующих особого контроля и аудита, например, выгрузки отчета по продажам со всеми контрагентами.
  - О Интегрируйте Мультифактор и обязательно протестируйте интеграцию перед запуском. Интеграция простая и не займет у вас много времени.

## 3 Возможности Мультифактора

### 3.1 Обзор решения

Инструмент для надёжной 2FA-аутентификации ваших пользователей вторым фактором при доступе к любым корпоративным ресурсам (VPN, VDI, Windows и Linux-инфраструктура, облачные приложения) с поддержкой технологии единого входа (SSO).

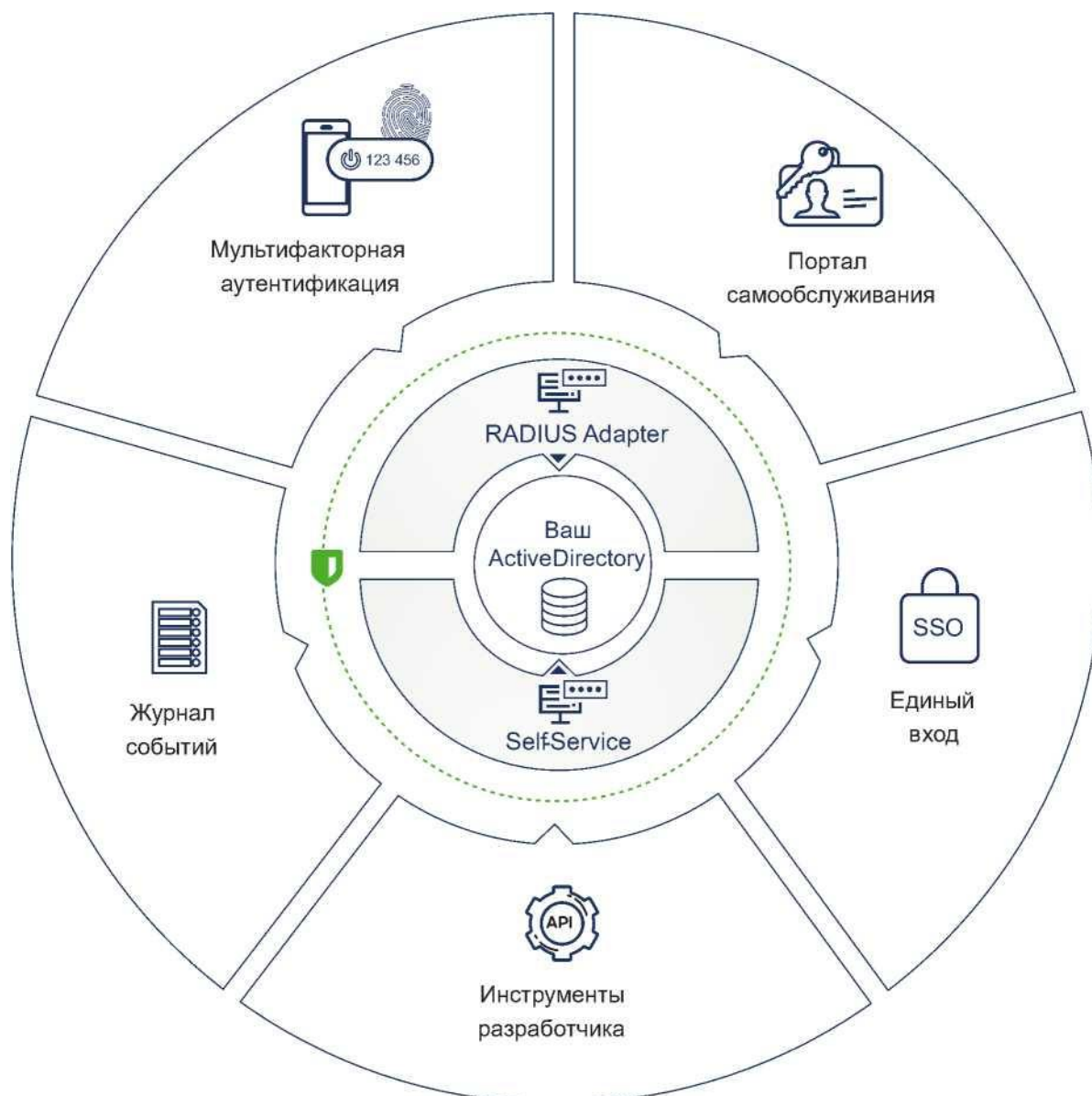
Простое, легковесное, не требующее дополнительных капитальных затрат на инфраструктуру и лицензии сторонних вендоров гибридное решение.



Быстро завершите проект по внедрению Multifactor в организации (от 2 часов), проведите автоматический онбординг сотрудников и реализуйте преимущества в тот же день:

- Дополнительный уровень безопасности поверх основного метода аутентификации;
- Комфортный доступ внешних пользователей к корпоративным ресурсам без ущерба безопасности, непрерывности и целостности бизнес- процессов;
- Оптимизация затрат на IT-поддержку и процессы управления доступом.

## 3.2 Компоненты платформы



## 3.3 Мультифакторная аутентификация и контроль доступа (MFA)

Инструмент для надёжной аутентификации пользователей обеспечивает безопасность доступа к информационным ресурсам и сетевой инфраструктуре компании. Снижает риск неавторизованного доступа на 99%, не создавая новых рисков. Предотвращает угоны учетных записей, утечку данных и сетевые атаки. Защищает любые ресурсы независимо от их типа и варианта развёртывания.

Защите ресурсы:

- Средства коммутации, аппаратные и программные межсетевые экраны (Check Point, Cisco, UserGate, Citrix Gateway и др.);
- Средства облачной виртуализации (VMware vCloud, Huawei Cloud и др.);

- Удалённые рабочие станции и VDI (Citrix, RDP, VMware Horizon и др.);
- Облачные приложения (GSuite, Trello, Salesforce, Slack и др.);
- Windows инфраструктура (Outlook Web Access, Windows VPN, NPS, Remote Desktop Gateway и др.);
- Linux инфраструктура (OpenVPN, SSH, Sudo и др.).

Настраивайте групповые политики доступа:

- Способы аутентификации;
- Информационные ресурсы и объекты доступа;
- Ограничение доступа по IP-адресу или диапазону адресов;
- Ограничение доступа по дням недели и времени.

### 3.4 Доступные методы аутентификации

MULTIFACTOR предоставляет несколько различных способов аутентификации, которые доступны в зависимости от типа защищаемого ресурса

	VPN и VDI	Linux инфраструктура	Windows инфраструктура	Облачные приложения (SAML)	API (Web)
 Telegram	✓	✓	✓	✓	✓
 Приложение	✓	✓	✓	✓	✓
 SMS или звонок	✓	✓	✓	✓	✓
 OTP-токены	✓	✓		✓	✓
 U2F / FIDO токены				✓	✓
 Биометрия				✓	✓

Возможные способы настраиваете вы, как администратор сайта, а ваши пользователи выбирают для себя наиболее удобные из доступных.

### **3.5 Единый Вход (SSO)**

Позволяет объединить учётные записи пользователей из всех корпоративных систем и популярных облачных приложений (Trello, Slack, Salesforce и др.) под единым провайдером учётных записей (например, Active Directory).

- Исключает мультипликацию учётных данных;
- Снижает затраты на IT-поддержку;
- Повышает уровень комплайнс внутренним политикам безопасности и требованиям регуляторов.

### **3.6 Портал Самообслуживания (SSP)**

Позволяет пользователю самостоятельно настраивать и подтверждать владение вторым фактором доступа, менять текущий или истёкший пароль после полной аутентификации.

- Самостоятельный онбординг пользователей;
- Самостоятельная конфигурация 2FA;
- Решение проблем с доступом без участия IT-поддержки.

### **3.7 Аудит-трейл и уведомления**

Все транзакции аутентификации записываются в журнал, доступный через личный кабинет администратора. Журнал незаменим при расследовании инцидентов и форензике.

Система информирует администратора системы об аномалиях:

- Вход с нового устройства;
- Одновременный вход с разных IP адресов;
- Неуспешные попытки входа.

### **3.8 Личный кабинет администратора**

В личном кабинете администратора MULTIFACTOR можно управлять пользователями, группами пользователей, ресурсами и объектами доступа, способами аутентификации.

### **3.9 Инструменты разработчика - REST API**

Интегрируйте двухфакторную аутентификацию Multifactor с вашими проприетарными приложениями и северной инфраструктурой:

- Аутентификация в системе Multifactor;
- Создание запросов доступа на двухфакторную аутентификацию;
- Управление пользователями (регистрация, изменение данных пользователя, удаление);
- Генерация ссылки на интерфейс для самостоятельной регистрации второго фактора пользователем;
- Отправка ссылки для самостоятельной регистрации на email пользователя.

Подробное описание API представлено в руководстве администратора.

### 3.10 Ценностное предложение



Создаём ценность как для компании в целом, так и для всех её стейкхолдеров, начиная от сотрудников до менеджмента и партнёров.

### 3.11 Сотрудники

Сотрудники получают удобный инструмент, позволяющий им оставаться продуктивными. В отличие от аппаратного токена, в котором пользователь не видит для себя большой ценности и который может легко забыть или потерять, мобильный телефон с приложением для аутентификации всегда под рукой.

### 3.12 Менеджмент

Менеджмент получает инструмент для обеспечения непрерывности и целостности бизнес-процессов; снижения издержек на IT-поддержку; оптимизации резервов под кибер-риск; обеспечения безопасности критических точек входа в инфраструктуру.

Выстраивается доверие с партнёрами и регуляторами для обеспечения долгосрочной устойчивости бизнеса.

### **3.12.1 CEO**

- Построение доверия с различными сторонами: клиентами, партнёрами, инвесторами, потребителями, регулирующими органами;
- Повышение устойчивости бизнеса.

### **3.12.2 CFO**

- Доступное решение для управления кибер-риском;
- Оптимизация резервов под кибер-риск;
- Защита критической информации.

### **3.12.3 COO**

- Непрерывность рабочих процессов;
- Координация предоставления доступов;
- Управление процессом найма и увольнения сотрудников.

### **3.12.4 CSO**

- Безопасность точек входа в инфраструктуру;
- Повышение барьеров для злоумышленников;
- Организация безопасности удалённой работы;
- Оптимизация аудитов безопасности.

## **3.13 Режимов работы средства**

ПО «Мультифактор» может работать в двух режимах.

### **3.13.1 Штатный режим**

После успешной проверки первого фактора ресурс направляет в систему запрос второго фактора система запрашивает второй фактор.

- Код отправляется пользователю через заранее выбранный канал:
- SMS на зарегистрированный номер телефона.
- Push-уведомление в мобильное приложение.
- Код, сгенерированный в приложении-аутентификаторе (например, Google Authenticator).
- - Пользователь вводит полученный код в соответствующее поле.
- Система уведомляется об успешном прохождении проверки второго фактора

### **3.13.2 Аварийный режим**

После успешной проверки первого фактора ресурс направляет в систему запрос второго фактора система запрашивает второй фактор

В случае если система не отвечает, предусмотрено 2 сценария работы аварийного режима

- Не пускать пользователей без подтверждения второго фактора.
- Пропускать пользователей с подтверждённым первым фактором, без проверки второго фактора.

## **4 Принцип безопасной работы средства.**

### **4.1 Защита учётных данных**

- Используйте сложный, уникальный пароль, не повторяющийся на других сервисах.
- Не передавайте логин и пароль третьим лицам, избегайте записи их в незащищённых местах.
- Проверяйте URL страницы авторизации, чтобы избежать фишинговых сайтов.
- Следите за уведомлениями о попытках входа в систему; при подозрительной активности немедленно сообщайте администратору

#### **Защита от компрометации второго фактора**

- Используйте надёжные методы подтверждения второго фактора, например , мобильное приложение , будет исключать возможность подмены номера.
- В случае подтверждения второго фактора через почту опасайтесь фишинговых писем, проверяйте домен отправки.
- Используйте наложенные методы ограничений на подтверждение второго фактора, такие как проверку по ip.

## **5 Описание личного кабинета**

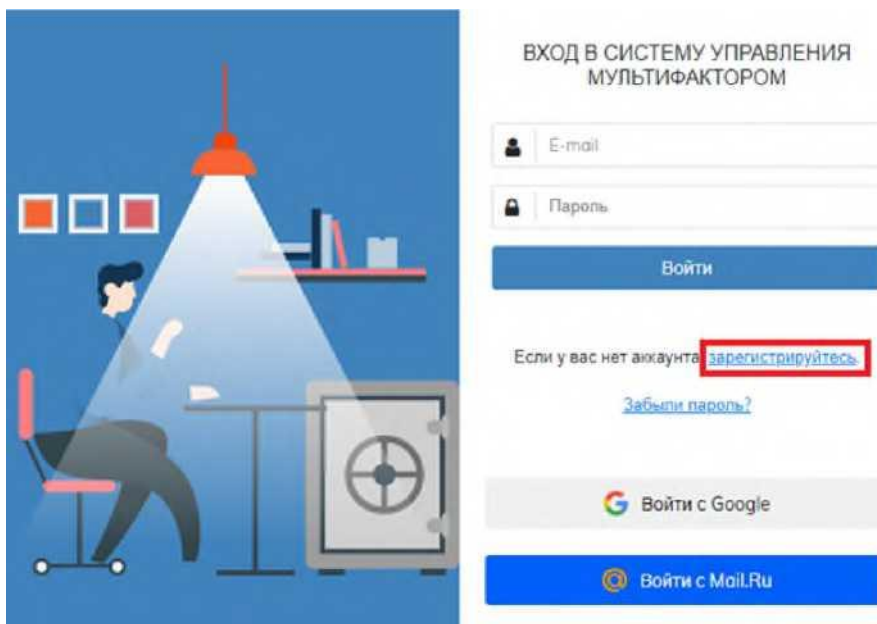
### **5.1 Общее описание**

Личный кабинет администратора MULTIFACTOR необходим для того, чтобы управлять вашими ресурсами, пользователями и их группами.

Это краткое руководство поможет вам разобраться в функционале и раскроет все возможности управления сервисом многофакторной аутентификации.

#### **5.1.1 Вход**

Вы можете зарегистрироваться, нажав на соответствующую гиперссылку



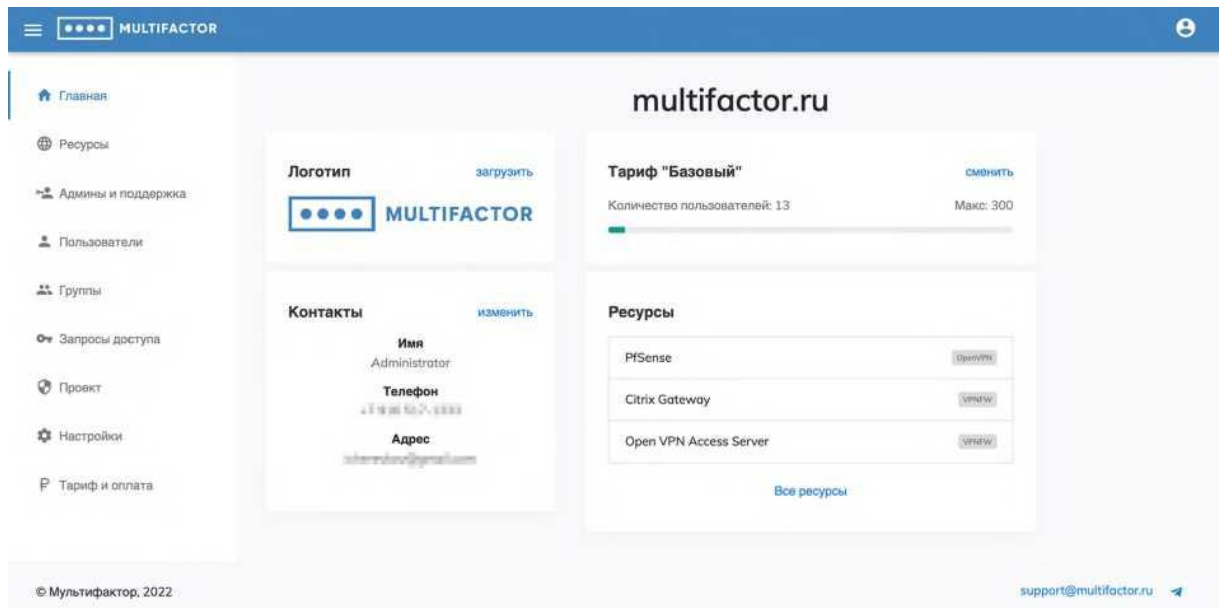
Вход доступен по логину\паролю, а также через mail.ru почту или ваш аккаунт Google. В случае утери пароля вы можете восстановить его самостоятельно в окне входа. В случае невозможности подтверждения 2фа, например замена телефона, обратитесь к другому администратору. Ему нужно будет удалить администратора с потерянным методом подтверждения и отправить ссылку на регистрацию по новой. Если вы являетесь единственным администратором, напишите на почту [support@multifactor.ru](mailto:support@multifactor.ru) с уточнением, что вы единственный администратор и просьбой сбросить метод подтверждения 2фа

### 5.1.2 Главная

На главной странице представлена краткая сводка о проекте.

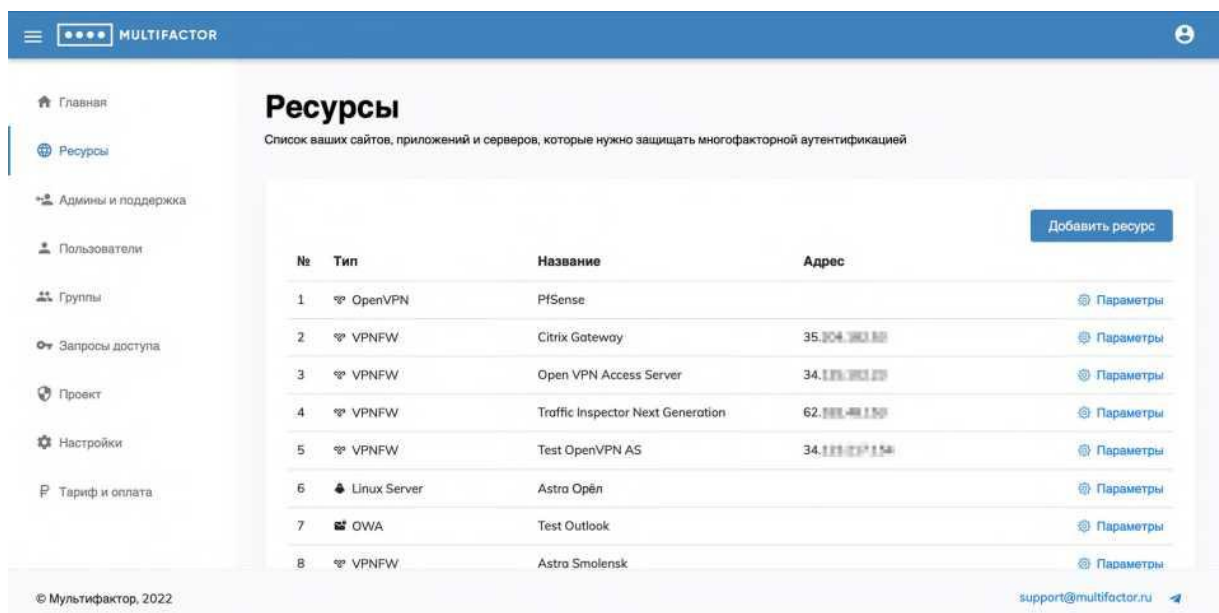
Изменение логотипа на главной странице ЛК позволит персонализировать страницу входа в веб-приложения для ваших пользователей.

Контакты на главной странице Личного кабинета будут отображаться вашим пользователям в случае возникновения проблем с использованием сервиса. Вы можете указать как номер телефона, так и электронную почту.

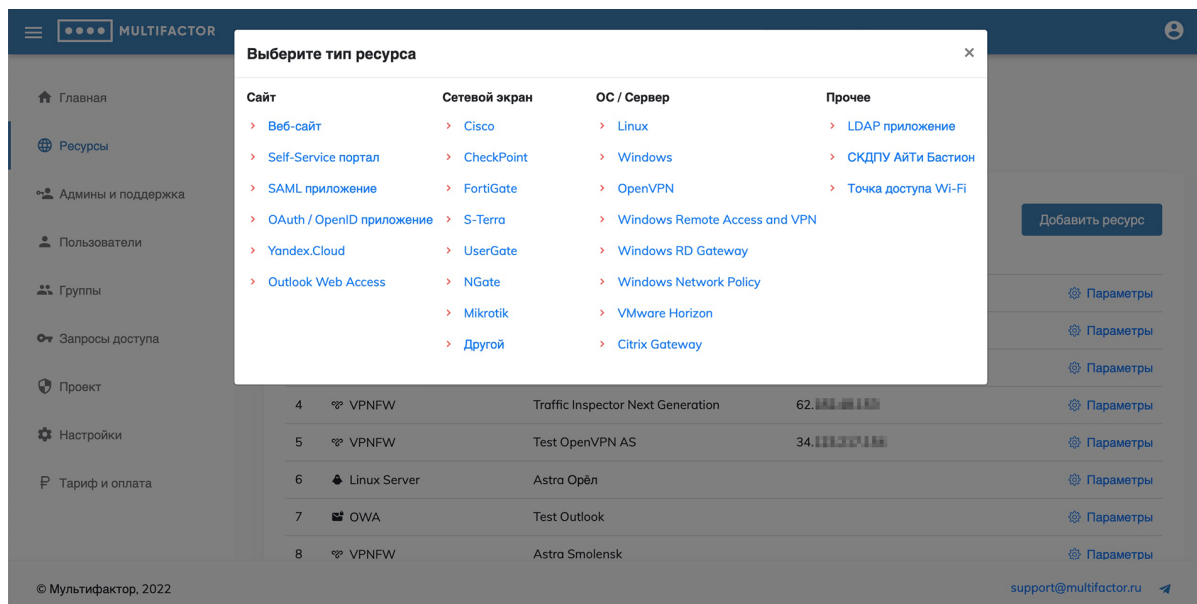


### 5.1.3 Ресурсы

В этом разделе осуществляется управление вашими информационными ресурсами и системами с многофакторной аутентификацией.



Для добавления доступны ресурсы 4-х типов: "Сайт", "Сетевой экран", "ОС/Сервер" и "Прочее".



1. Для работы с типом ресурса "Сайт" представлены следующие варианты решений:

- Веб-сайт;
- Self-Service портал;
- SAML-приложение;
- OAuth / OpenID-приложение;
- Yandex.Cloud;
- Outlook Web Access.

Подробнее с ними можно ознакомиться в руководстве администратора.

Работа с ресурсами "Веб-сайт" ведется через API, а для аутентификации используются API Key и API Secret.

Работа с ресурсами "SAML" осуществляется по SAML протоколу, между ресурсом и Мультифактором устанавливается взаимное доверие путем обмена публичными сертификатами.

Работа с ресурсами "OAuth / OpenID" осуществляется по протоколу OAuth, для аутентификации используются Client ID и Client Secret.

2. Для работы с типом ресурса «Сетевой экран»:

- Cisco;
- CheckPoint;
- FortiGate;
- S-Terra;

- UserGate;
- NGate;
- Mikrotik;
- Другой.

Если вашего сетевого оборудования нет в списке, используйте тип ресурса "Другой", который является универсальным.

3. Для работы с типом ресурсов «ОС/Сервер»:

- Linux;
- Windows;
- OpenVPN;
- Windows Remote Access and VPN;
- Windows RD Gateway;
- Windows Network Policy;
- VMware Horizon;
- Citrix Gateway.

Для ресурсов этого типа работа построена с использованием Radius сервера, для аутентификации в нем нужны параметры NAS-Identifier и Shared Secret.

4. Тип ресурса «Прочее» включает в себя:

- LDAP приложение;
- СКДПУ АйТи Бастион;
- Точка доступа Wi-Fi.

Ресурсы типа "LDAP приложение" использует LDAP Proxy компонент, для аутентификации в нем нужны параметры NAS-Identifier и Shared Secret.

Вы можете добавить необходимый вам тип ресурса, а в разделе настроек просмотреть данные для аутентификации и отредактировать название или адрес ресурса.

## 5.2 Функций и интерфейсов функций средства, доступных каждой роли пользователей

В этом разделе ведется управление администраторами вашей системы. Предусмотрена ролевая система доступов. Роли:

- Admin: все полномочия;
- Support 1: доступ только для чтения к разделам "Пользователи" и "Запросы доступа";
- Support 2: доступ к разделам "Пользователи" и "Запросы доступа" с возможностью отправки ссылки на настройку второго фактора и отключения способов аутентификации пользователя;
- Support 3: доступ к разделам "Пользователи" и "Запросы доступа", полное управление пользователями за исключением импорта и экспорта.
- Support 4: включает в себя все полномочия Support 3 с возможностью пропускать пользователей без аутентификации.

При добавлении администратору придёт ссылка для первого входа, при переходе по которой он сможет установить пароль и настроить многофакторную аутентификацию.

Любого администратора, кроме себя, можно заблокировать.

The screenshot shows the 'Админы и поддержка' (Admins and Support) section of the Multifactor system. The interface includes a sidebar with navigation options: Главная, Ресурсы, Админы и поддержка (selected), Пользователи, Группы, Запросы доступа, Проект, Настройки, and Тариф и оплата. The main content area displays a table of administrators and support staff. A 'Добавить сотрудника' button is visible in the top right of the table area. The footer contains the copyright information '© Мультифактор, 2022' and the email address 'support@multifactor.ru'.

№	Аккаунт	Имя	Роль	Статус	Дата регистрации	Последний вход	
1	[Redacted]	Илья Че	Admin	Активный	2/19/2020	11/20/2022	<a href="#">Параметры</a>
2	[Redacted]	Support	Support 3	Активный	6/9/2022	6/9/2022	<a href="#">Параметры</a>

## 5.3 Пользователи

В этом разделе отображаются ваши пользователи.

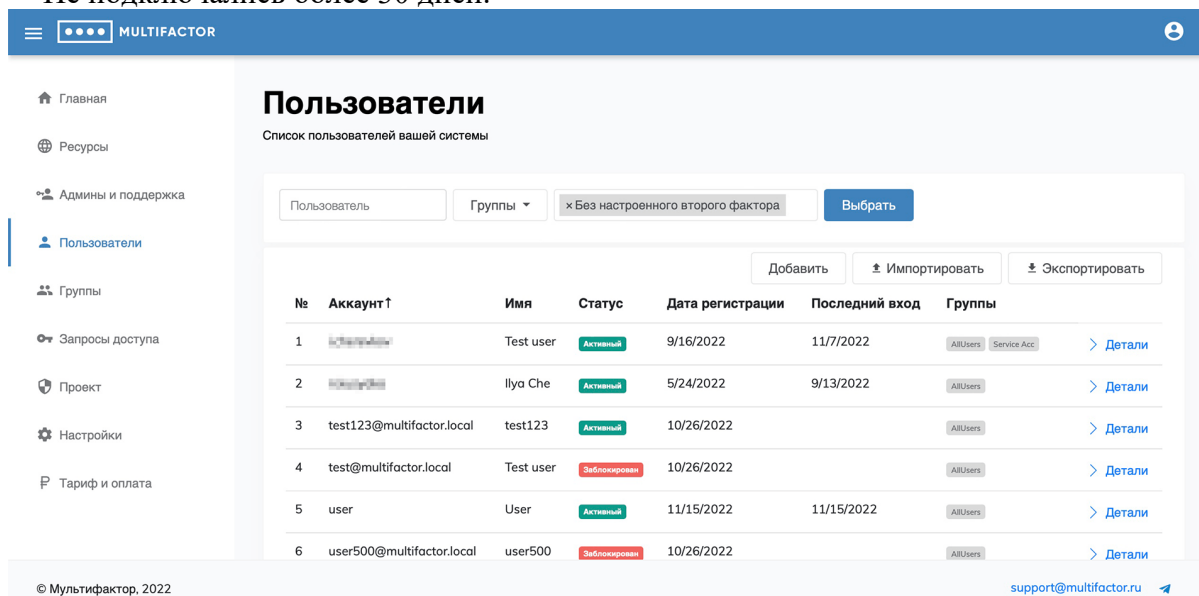
По умолчанию, сюда добавляются все ваши пользователи, которых вы направили на двухфакторную аутентификацию, но вы можете добавить пользователя вручную или массово импортировать пользователей из CSV или TXT файла.

При добавлении пользователя вы можете указать его имя и логин в системе, настроить принадлежность его к той или иной группе пользователей. При этом автоматически созданные пользователи попадают в системную группу All Users.

Для пользователей без указанного в явном виде имени мы подтягиваем имя из Telegram в случае, если они подключили этот метод аутентификации.

Есть возможность фильтрации пользователей по имени, группам и дополнительным фильтрам:

- Заблокированные;
- Без настроенного второго фактора;
- Без e-mail;
- Ни разу не подключались;
- Не подключались более 30 дней.





№	Аккаунт ↑	Имя	Статус	Дата регистрации	Последний вход	Группы	
1	[Redacted]	Test user	Активный	9/16/2022	11/7/2022	AllUsers, Service Acc.	> Детали
2	[Redacted]	Ilya Che	Активный	5/24/2022	9/13/2022	AllUsers	> Детали
3	test123@multifactor.local	test123	Активный	10/26/2022		AllUsers	> Детали
4	test@multifactor.local	Test user	Заблокирован	10/26/2022		AllUsers	> Детали
5	user	User	Активный	11/15/2022	11/15/2022	AllUsers	> Детали
6	user500@multifactor.local	user500	Заблокирован	10/26/2022		AllUsers	> Детали

При просмотре пользователя вы можете узнать данные его регистрации, последнего входа, статус и настройки доступа, настроенные методы аутентификации.

Пользователя можно заблокировать или удалить, если вы не хотите, чтобы он аутентифицировался с помощью Multifactor. Также можно изменить данные в профиле пользователя и отвязать настроенные методы аутентификации.

Вы можете отправить пользователю ссылку для настройки аутентификации, если он по какой-то причине не включил многофакторную аутентификацию ранее. При отправке настраивается время жизни ссылки, максимальное значение 48 часов (2880 минут).

Сама настройка доступов пользователя производится с помощью редактирования доступов для групп.

Логин	user
Имя	User
E-mail	blabla@yandex.ru
Телефон	+7 916 XXX-1333
Зарегистрирован	Tuesday, November 15, 2022 10:59 AM
Последний вход	Tuesday, November 15, 2022 11:12 AM
Группы	<ul style="list-style-type: none"><li>AllUsers (системная группа)</li></ul>
Подключенные способы аутентификации	<b>СМС</b> <ul style="list-style-type: none"><li>+7 916 XXX-1333 </li></ul> <b>Биометрия и U2F</b> <ul style="list-style-type: none"><li>Биометрия и U2F </li></ul> <a href="#">Отправить ссылку для настройки аутентификации</a>

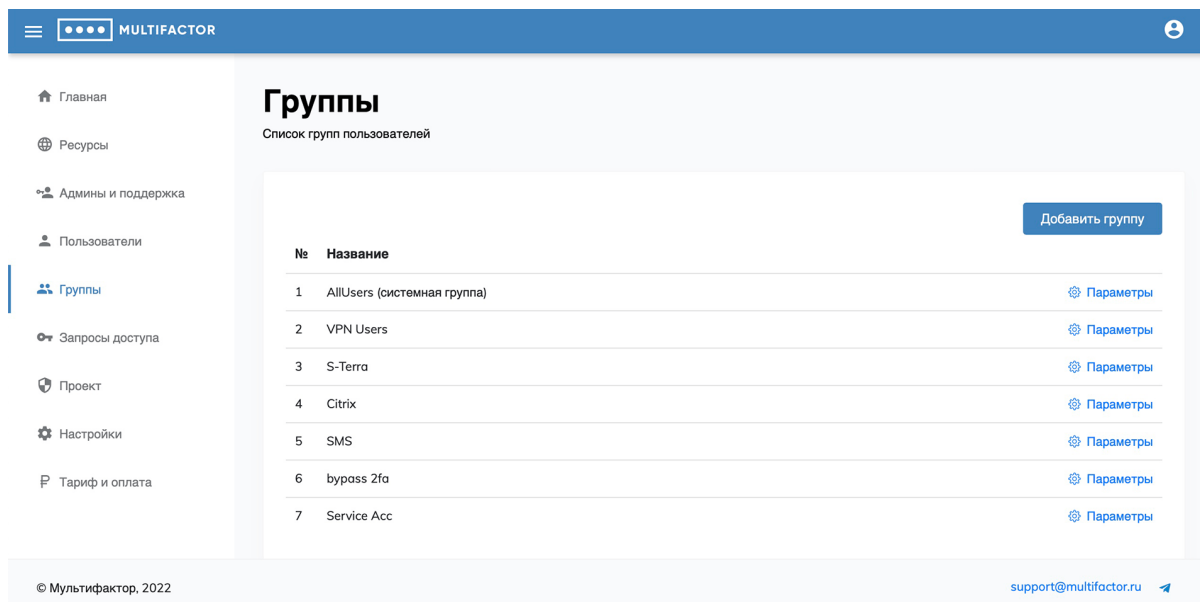
Статусы пользователей:

- Активный** - пользователь прошел регистрацию и подключил 2FA
- Приглашение отправлено** - пользователь ожидает подключения 2FA
- Заблокирован** - пользователь заблокирован администратором проекта
- Временно заблокирован** - пользователь временно заблокирован после нескольких неудачных попыток входа
- Приостановлено** - пользователь приостановлен ввиду недостаточного количества лицензий в проекте

## 5.4 Группы

Параметры безопасности средства, доступных каждой группе пользователей, и их безопасных значений.

По умолчанию вам доступна одна системная группа доступа All Users. В нее попадают новые пользователи, созданные автоматически.



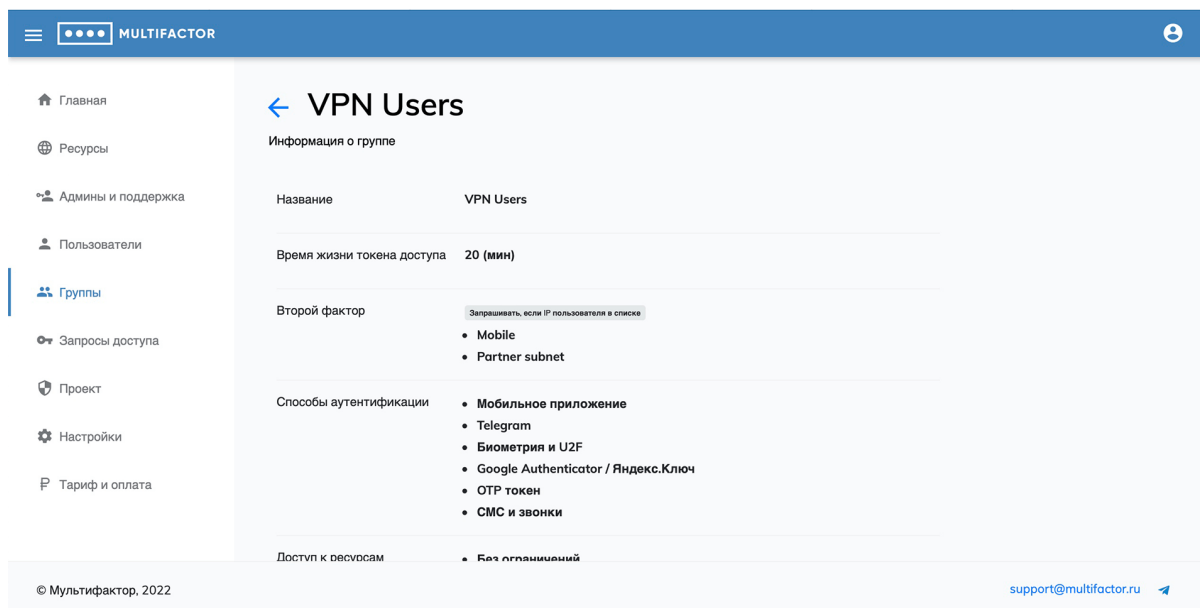
The screenshot shows the 'Группы' (Groups) page in the MULTIFACTOR interface. The page title is 'Группы' and the subtitle is 'Список групп пользователей'. A 'Добавить группу' button is located in the top right corner. The main content is a table with the following data:

№	Название	
1	AllUsers (системная группа)	<a href="#">Параметры</a>
2	VPN Users	<a href="#">Параметры</a>
3	S-Terra	<a href="#">Параметры</a>
4	Citrix	<a href="#">Параметры</a>
5	SMS	<a href="#">Параметры</a>
6	bypass 2fa	<a href="#">Параметры</a>
7	Service Acc	<a href="#">Параметры</a>

At the bottom of the page, there is a copyright notice '© Мультифактор, 2022' and a support email address 'support@multifactor.ru'.

При создании и редактировании группы вы можете указать:

- название группы;
- время жизни токена доступа;
- в каком случае запрашивать второй фактор;
- методы аутентификации, доступные пользователям этой группы (не забудьте оставить доступным хотя бы один);
- ресурсы, к которым группа имеет доступ;
- IP-адреса или подсети, с которых разрешено подключение к ресурсам;
- дни недели, в которые доступ для этой группы пользователей разрешен.



## 5.5 Безусловный и условный запрос второго фактора

Доступны 2 варианта логики запроса второго фактора:

- Безусловная

- Всегда запрашивать;
- Никогда не запрашивать;

### Второй фактор

В каком случае запрашивать второй фактор

- Всегда запрашивать
- Никогда не запрашивать
- Запрашивать, если IP пользователя в списке
- Не запрашивать, если IP пользователя в списке

- Условная

○ Запрашивать, если IP пользователя в списке (черный список);

## Второй фактор

В каком случае запрашивать второй фактор

- Всегда запрашивать
- Никогда не запрашивать
- Запрашивать, если IP пользователя в списке
  - Mobile
  - Office
  - Partner subnet
- Не запрашивать, если IP пользователя в списке

o Не запрашивать, если IP пользователя в списке (белый список).

## Второй фактор

В каком случае запрашивать второй фактор

- Всегда запрашивать
- Никогда не запрашивать
- Запрашивать, если IP пользователя в списке
- Не запрашивать, если IP пользователя в списке
  - Mobile
  - Office
  - Partner subnet

Последние два режима "Запрашивать, если IP пользователя в списке" и "Не

запрашивать, если IP пользователя в списке" представляют соответственно черный и белый списки. Диапазоны IP предварительно настраиваются в разделе "Настройки" -> "Диапазоны IP".

При вычислении итоговой политики учитываются настройки всех групп, в которых находится пользователь – системной "AllUsers" и пользовательских групп.

- при использовании в группах пользователей безусловной логики, настройки в пользовательских группах имеют более высокий приоритет, чем в системной группе AllUsers. При этом "Никогда не запрашивать" выше в приоритете, чем "Всегда запрашивать";
- при использовании в группах пользователей разных логик (условная/ безусловная), условная логика всегда выше в приоритете, чем безусловная;
- логика с черным списком ("Запрашивать, если IP пользователя в списке") приоритетнее логики с белым списком ("Не запрашивать, если IP пользователя в списке").

Итоговую политику запроса второго фактора и доступа к ресурсам для каждого пользователя можно проверить в деталях пользователя.

## Настройка доступа

На основании групповой политики

Время жизни токена доступа 10 (мин)

Второй фактор **Всегда запрашивать**

Доступные способы аутентификации

- Мобильное приложение
- Telegram
- Биометрия и U2F
- Google Authenticator / Яндекс.Ключ
- OTP токен
- СМС и звонки

Доступ к ресурсам

- Без ограничений

IP адреса

- Без ограничений

Дни недели

- Понедельник
- Вторник
- Среда

## 5.6 Запросы доступа

В этом разделе администратор системы видит все запросы доступов своих пользователей.

Вы можете использовать фильтр для удобства отслеживания доступов конкретного пользователя к интересующим вас ресурсам. В том числе, за определенный период времени.

Запросы доступа

Раздел отображает запросы доступа к вашим ресурсам

Пользователь Ресурсы 29 сен 2022 — 30 сен 2022 Выбрать

Дата	Пользователь	Ресурс	Локация	Доступ
9/30/2022 1:10:48 PM	zabbix_admin	Zabbix	RU  Волгоград	<span>Разрешено</span> <a href="#">Детали</a>
9/30/2022 1:04:32 PM	administrator	Cisco ASA	KZ  Атырау	<span>Запрещено</span> <a href="#">Детали</a>
9/30/2022 1:03:13 PM	accounting_user	Cisco ASA	RU  Уфа	<span>Ожидается</span> <a href="#">Детали</a>
9/30/2022 1:02:24 PM	service_account	Cisco ASA	RU  Самара	<span>Разрешено</span> <a href="#">Детали</a>
9/30/2022 1:00:13	it_staff	Citrix Gateway	CY  Limassol	<span>Разрешено</span> <a href="#">Детали</a>

© Мультифактор, 2022 support@multifactor.ru

В детализированной информации о запросе доступа вы сможете найти следующие данные:

- ресурс, к которому пользователь получал доступ;
- какой способ аутентификации был выбран;
- в какое время пришёл запрос на авторизацию;
- отпечаток устройства, с которого производился запрос;
- IP адрес и геолокация.

Администратор может пропустить пользователя без авторизации. Для этого нужно зайти в детали запроса со статусом "Ожидается аутентификация" и нажать на кнопку "Пропустить без аутентификации". Данный метод сработает только в том случае, если время жизни токена еще не истекло, а пользователь не ушёл с экрана аутентификации.

The screenshot shows the 'service\_account' page in the MULTIFACTOR interface. The left sidebar contains navigation items: Главная, Ресурсы, Админы и поддержка, Пользователи, Группы, Запросы доступа (highlighted), Проект, Настройки, and Тариф и оплата. The main content area displays the following information:

- Пользователь:** service\_account
- Ресурс:** Cisco ASA ()
- Статус:** Доступ предоставлен
- Создан:** Friday, September 30, 2022 в 1:02:24 PM
- Доступ предоставлен:** Friday, September 30, 2022 в 1:02:29 PM
- Способ аутентификации:** Telegram
- Устройство:** Radius-Adapter-Client

At the bottom of the page, there is a footer with '© Мультифактор, 2022' on the left and 'support@multifactor.ru' on the right.

## 5.7 Проект

В этом разделе вы можете задать описание профиля: название информационной системы и контакты администратора, к которому ваши пользователи могут обращаться за помощью.

The screenshot shows the 'Проект' (Project) configuration page in the MULTIFACTOR interface. The left sidebar is identical to the previous screenshot. The main content area displays the following form fields:

- Название проекта:** multifactor.ru
- Администратор:** Administrator
- Адрес:** Email
- Телефон:** в любом формате
- Язык:** English

At the bottom of the form, there are two buttons: 'Сохранить' (Save) and 'Отмена' (Cancel). The footer at the bottom of the page contains '© Мультифактор, 2022' on the left and 'support@multifactor.ru' on the right.

## 5.8 Настройки

Раздел содержит 6 вкладок, которые вы можете настраивать под свои потребности: Учетные записи, СМС, Звонки, Расширенное API, Поставщики учетных записей, Диапазоны IP.

## 5.9 Учетные записи

Формат имени пользователя определяет, как MULTIFACTOR будет преобразовывать учетные записи для обработки и хранения.

Варианты могут быть:

- Без преобразования: имя пользователя обрабатывается как есть.
- Active Directory: из имени пользователя убирается название домена таким образом, что "domain\user", "user@domain.local" и "user" будут обрабатываться как "user".

В разделе есть переключатель "а также переименовать пользователей и удалить дубликаты (безопасно)", чтобы переименовать существующих. Логика переименования:

i V Если в системе существует больше 1 формата УЗ одного пользователя (domain\user, user, user@domain), то выбирается одна запись по критериям:

- с привязанным 2fa
- с последней датой входа

ii. Далее эта запись приводится в формат Active Directory (только логин - user), остальные форматы удаляются.

The screenshot shows the 'Настройки' (Settings) page in the Multifactor application. The left sidebar contains navigation items: Главная, Ресурсы, Админы и поддержка, Пользователи, Группы, Запросы доступа, Проект, **Настройки**, and Тариф и оплата. The main content area is titled 'Настройки' and has several tabs: 'Учетные записи' (selected), СМС, Звонки, Расширенное API, Поставщики учетных записей, and Диапазоны IP. The 'Учетные записи' section contains the following text: 'Формат имени пользователя определлет, как Мультифактор будет преобразовывать учетные записи для обработки и хранения. Варианты могут быть:' followed by a bulleted list: '• Без преобразования: имя пользователя обрабатывается как есть.' and '• Active Directory: из имени пользователя убирается название домена таким образом, что "domain\user", "user@domain.local" и "user" будут обрабатываться как "user".'. Below this, it states 'Текущий формат: без преобразований'. There are two radio button options: 'Без преобразований' (unselected) and 'Active Directory' (selected). A third option is a checkbox labeled 'а также переименовать пользователей и удалить дубликаты (безопасно)'. At the bottom of the settings area are 'Сохранить' and 'Отмена' buttons. The footer of the page shows '© Мультифактор, 2022' on the left and 'support@multifactor.ru' on the right.

## 5.10 СМС

По умолчанию используется АТС Мультифактора. Есть возможность интеграции по SIP-протоколу. Работа протестирована с АТС Asterisk (FreeBPX).

Учетные записи **СМС** Звонки Расширенное API Синхронизация УЗ Поставщики учетных записей Диапазоны IP

Используется СМС-провайдер Мультифактора.

СМС-провайдер Мультифактора  
 Ваш СМС-провайдер

Если же сервис внешний, то вот список токенов, вместо которых наш сервис подставляет значения. Эти токены можно использовать, например, при указании аргументов запроса во внешний сервис. Запрос GET имеет формат QUERY.

Настраивает администратор заказчика в ЛК.

Используется СМС-провайдер Мультифактора.

СМС-провайдер Мультифактора  
 Ваш СМС-провайдер

HTTP метод

Адрес

Укажите адрес с параметрами для использования внешнего СМС-провайдера. Например:  
`https://smc.ru/sys/send.php?login=ЛОГИН&psw=ПАРОЛЬ&phones={phone}&mes=Код доступа: {code}`

Шаблоны для подстановки:  
{phone} – номер телефона  
{code} – одноразовый код  
{identity} – логин пользователя  
{userid} – идентификатор пользователя

Авторизация (если требуется)

Из HTTP методов доступны GET и POST

HTTP метод

GET

GET  
POST

http://orky.name/mf/post.php

В режиме POST появляются два поля:

- Значение заголовка Content-Type
- Тело запроса в формате JSON

Авторизация (если требуется)

Bearer ...

Content-Type

application/json

Body

## Звонки

По умолчанию используется АТС Мультифактора. Есть возможность интеграции по SIP-протоколу. Работа протестирована с АТС Asterisk (FreeBPX).

Меню: Главная, Ресурсы, Админы и поддержка, Пользователи, Группы, Запросы доступа, Проект, **Настройки**, Тариф и оплата

Учетные записи СМС Звонки Расширенное API Поставщики учетных записей Диапазоны IP

Используется ваша АТС.

АТС Мультифактора

**Ваша АТС**

Имя пользователя: 1234

Пароль: 123456

Сервер: 164.92.213.38

© Мультифактор, 2022 support@multifactor.ru

## 5.11 Расширенное API

Расширенное API позволяет управлять пользователями, ресурсами и настройками доступа к вашей системе через программный интерфейс. Если вы не планируете интегрировать расширенное API, не включайте доступ.

The screenshot shows the 'Настройки' (Settings) page in the Multifactor application. The left sidebar contains navigation items: Главная, Ресурсы, Админы и поддержка, Пользователи, Группы, Запросы доступа, Проект, Настройки (selected), and Тариф и оплата. The main content area is titled 'Настройки' and has a sub-tab 'Расширенное API'. Below the sub-tab, there is a description: 'Расширенное API позволяет управлять пользователями, ресурсами и настройками доступа к вашей системе через программный интерфейс. Если вы не планируете интегрировать расширенное API, не включайте доступ.' The current status is 'доступ включен'. There are two input fields: 'API Key' and 'API Secret', both containing masked text. At the bottom, there are two buttons: 'Выключить API' and 'Сменить ключ'.

Также в нашей базе знаний есть инструкции по API для управления пользователями (субъектами доступа) и API для управления ресурсами (объектами доступа).

## 5.12 Поставщики учетных записей

В данной вкладке вы можете добавить и настроить SAML-поставщиков учетных записей для последующего их использования в SAML и OpenID-Connect ресурсах.

The screenshot shows the 'Настройки' (Settings) page in the Multifactor application. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Настройки' and has a sub-tab 'Поставщики учетных записей'. Below the sub-tab, there is a table with columns: №, Тип, Название, Дата регистрации. There are two rows of data. To the right of the table is a 'Добавить поставщика' button. Below each row, there is a 'Параметры' link.

№	Тип	Название	Дата регистрации
1	SAML	WSO2	3/25/2022
2	SAML	Keycloak	4/20/2022

## 5.13 Диапазоны IP

В данной вкладке задаются диапазоны IP для использования в групповых политиках для управления запросом второго фактора на базе IP-пользователя.

**Настройки**

Учетные записи СМС Звонки Расширенный API Поставщики учетных записей Диапазоны IP

Списки диапазонов IP-адресов пользователей.

[Добавить диапазон IP](#)

№	Название	Описание
1	Office	<a href="#">Параметры</a>
2	Mobile	<a href="#">Параметры</a>
3	Partner subnet	<a href="#">Параметры</a>

© Мультифактор, 2022 [support@multifactor.ru](mailto:support@multifactor.ru)

## 5.14 Журнал

Типы событий безопасности, связанных с доступными пользователю функциями средства. В данной вкладке отображаются действия админов. В ней отображаются следующие действия:

- Вход в админ-панель
- Удаление\Создание\Изменение ресурса
- Удаление\Создание\Изменение группы
- Удаление\Добавление\Изменение сотрудника
- Удаление\Создание\Изменение списка IP-адресов
- Изменение формата имен учетных записей
- Запуск переименования учетных записей / удаления дубликатов
- Отображение секрета ресурса
- Включение\Выключение API
- Изменение секрета API
- Отображение секрета API
- Отправка ссылки на настройку 2FA

## 5.15 Тариф и оплата

В этом разделе отображается информация о текущем тарифе, количестве доступных и использованных лицензий.

Система двухфакторной аутентификации MULTIFACTOR доступна бесплатно до 3-х пользователей (включительно).

☰ MULTIFACTOR 👤

- 🏠 Главная
- 🌐 Ресурсы
- 👤 Админы и поддержка
- 👤 Пользователи
- 👤 Группы
- 🔑 Запросы доступа
- 🛡️ Проект
- ⚙️ Настройки
- 📄 Тариф и оплата**

## Тариф и оплата

**Текущий тариф "Базовый"** Бесплатный

Количество пользователей: 12 Макс: 300

Для смены тарифа, пожалуйста, свяжитесь с отделом продаж по адресу [sales@multifactor.ru](mailto:sales@multifactor.ru) или телефону +7 499 444 08 82.

© Мультифактор, 2022 [support@multifactor.ru](mailto:support@multifactor.ru) ↗

## 6 Способы аутентификации

Сводная таблица

	Способ	Требования	Использовать	Безопасность
1	Мобильное приложение Multifactor	Приложение на телефоне, доступ в интернет	Удобно	Максимальная
2	Универсальная web аутентификация с поддержкой биометрии	Устройство с биометрическим датчиком или внешний токен, современный браузер	Удобно	Очень высокая
3	ОТР Токен	Внешний токен	Зависит от токена	Высокая
4	НОТР Токен	Внешний Токен	Зависит от токена	Высокая
5	Google authenticator	Приложение на телефоне	Менее удобно	Высокая
6	СМС сообщение или звонок	Телефон	Менее удобно	Средняя

### 6.1 Мобильное приложение Multifactor

Безопасный и удобный доступ к VPN, VDI, облачным приложениям, сайтам, персональным и корпоративным ресурсам в одном приложении: Multifactor. Доступно для платформ Аврора.

### 6.2 Регистрация

Пользователю необходимо отсканировать регистрационный QR-код с помощью приложения Multifactor, либо открыть специальную ссылку на телефоне с установленным приложением Multifactor.

### 6.3 Аутентификация

Пользователю приходит PUSH-уведомление с просьбой подтвердить действие и двумя кнопками в приложении: подтвердить или отклонить соответственно.

### 6.4 Универсальная web аутентификация с поддержкой биометрии

Набор протоколов: U2F (Universal Second Factor), UAF (Universal Authentication Framework) FIDO (Fast IDentity Online), CTAP (Client to Authenticator Protocol), объединенные в единый стандарт WebAuthn.

Стандарт работает прямо из браузера без установки стороннего программного обеспечения и драйверов. Поддерживает биометрические датчики и сканеры, а также внешние устройства аутентификации, подключаемые через USB, Lightning, NFC или Bluetooth, например, RuToken U2F.

Универсальная аутентификация поддерживается браузерами Chrome, Safari, Firefox, Edge, Opera на платформах Windows, Linux, MacOS и Android.

#### **6.4.1 Регистрация**

Пользователю будет предложено использовать биометрический датчик, если он есть на его телефоне или ноутбуке, либо подключить и активировать внешний токен после чего MULTIFACTOR получит публичные ключи устройств и сможет использовать их для аутентификации.

#### **6.4.2 Аутентификация**

Пользователь использует биометрию (отпечаток пальца, сканер лица), либо прикасается к внешнему токenu — совершает осознанное действие.

### **6.5 Маскирование логинов в мобильном приложении**

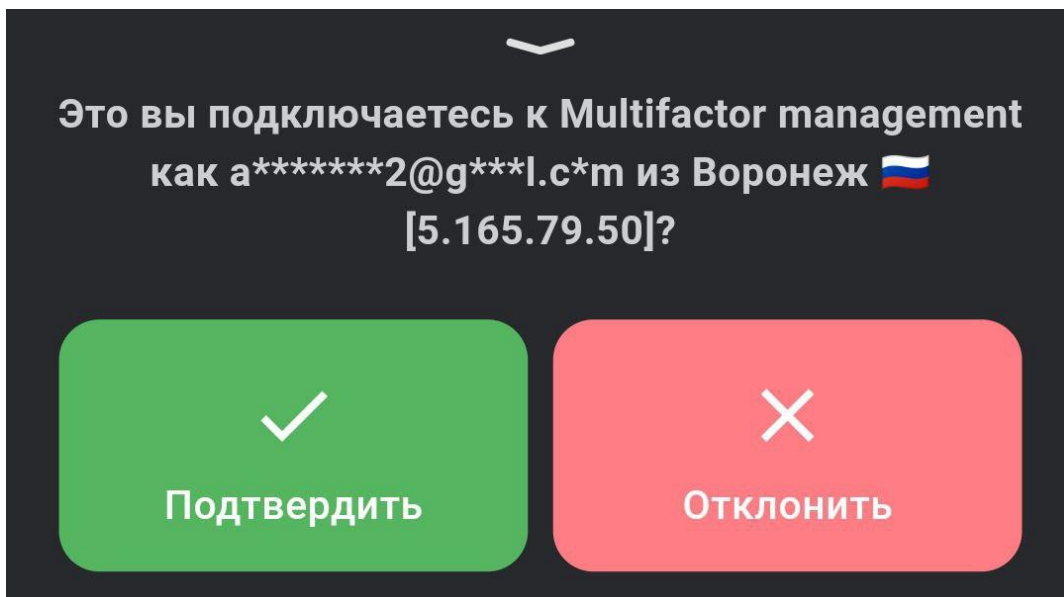
#### **6.5.1 Система маскирования**

В сообщениях запросов в мобильном приложении вставляется логин пользователя, который по закону является личной информацией пользователя, а так как пользователь может пользоваться нашими продуктами из-за рубежа, то возникла необходимость иметь возможность скрывать эти данные.

#### **6.5.2 Как работает**

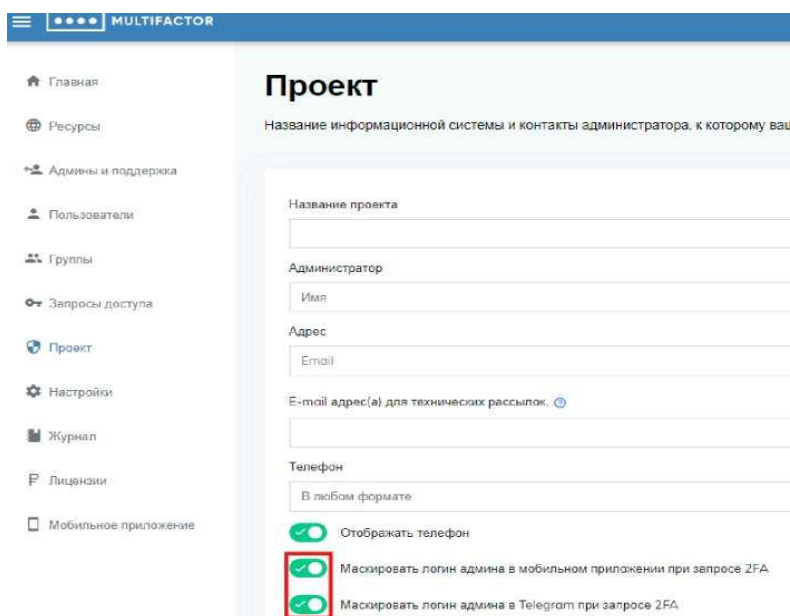
При включении данного функционала все нотификации, сообщения и другие формы вывода логина будут маскироваться.

Пример маскирования в мобильном приложении:



### 6.5.3 Включение функции

Для администраторов:



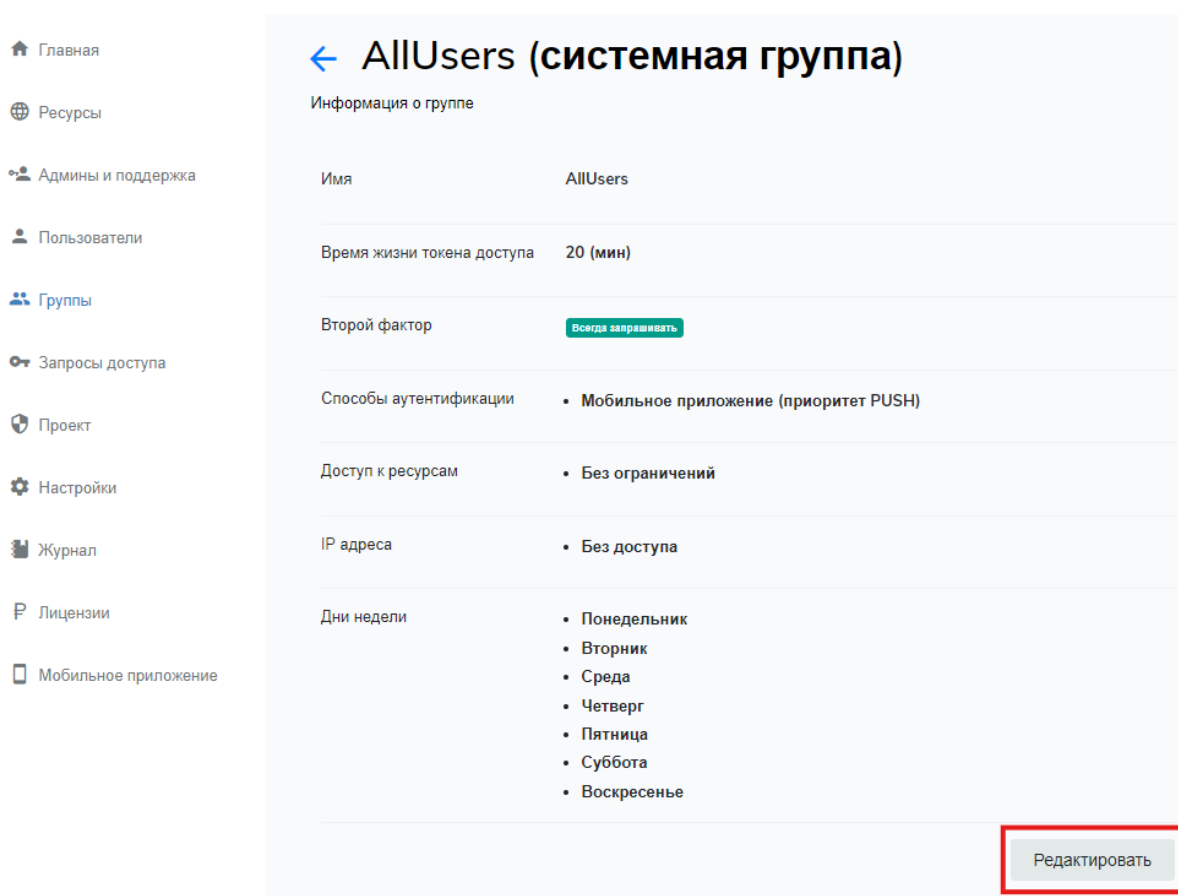
Для пользователей:

Для обычных пользователей данную функцию можно отдельно настраивать для каждой группы. Помните, если пользователь состоит в нескольких группах, то даже если данная функция будет включена в политиках только одной группы, то логин этого пользователя будет маскироваться.

Для того чтобы включить функцию зайдите во вкладку “Группы“:

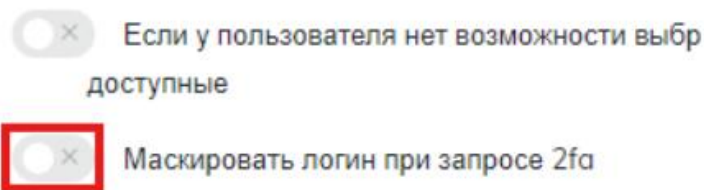


Далее найдите в списке интересующую вас группу и нажмите для ней “Параметры“ и вы увидите окно параметров для данной группы:



Нажмите “Редактировать“ и в появившемся окне вы увидите список всех настраиваемых политик, найдите разделы “Мобильное приложение“ и “Телеграм“:

## Мобильное приложение



### 6.6 OTP Токен

OTP токен — устройство для формирования одноразовых кодов доступа, обычно в виде брелка, который показывает цифры на экране, пример — Feitian с100 или в виде флешки, пример — RuToken OTP.

Второй формат более удобный, так как цифры не нужно перепечатывать: устройство определяется операционной системой, как клавиатура и автоматически вводит код в фокусное поле. С другой стороны, брелки с экраном не требуют подключения к компьютеру и работают полностью автономно.

#### 6.6.1 Регистрация

Для регистрации OTP-токена необходимо загрузить в MULTIFACTOR ключ устройства и ввести очередной одноразовый код. По требованию, MULTIFACTOR может самостоятельно сформировать ключ устройства для последующей загрузки в токен.

#### 6.6.2 Аутентификация

Пользователю необходимо ввести одноразовый код доступа, сформированный токеном.

### 6.7 HOTP Токен

HOTP (HMAC-based One-Time Password) токен - это метод генерации одноразового пароля (OTP), который зависит от счетчика. Каждый раз, когда пользователь входит, счетчик увеличивается, и OTP генерируется на основе этого счетчика.

#### 6.7.1 Регистрация

Для регистрации HOTP токена необходимо сгенерировать секретный ключ, связать его с учетной записью пользователя и предоставить QR-код или секретный ключ для

настройки аутентификации. После этого пользователь может использовать ОТР для двухфакторной аутентификации при входе в систему.

### **6.7.2 Аутентификация**

После всех проведенных настроек скопировать ключ в форму привязки от- устройства Multifactor.

## **6.8 Google authenticator**

Google Authenticator — самое популярное приложение для формирования одноразовых кодов доступа на телефонах Android и iPhone. Можно даже сказать, что это обобщенное название серии подобных способов аутентификации. Помимо Google Authenticator, такую же функцию выполняют Яндекс.Ключ, Microsoft Authenticator, а также некоторые менее известные приложения.

### **6.8.1 Регистрация**

Пользователю будет предложено запустить приложение Google Authenticator или Яндекс.Ключ, сканировать QR код, содержащий ключ системы MULTIFACTOR и ввести одноразовый код доступа, сформированный приложением.

### **6.8.2 Аутентификация**

Для аутентификации необходимо запустить приложение и ввести код доступа.

## **6.9 СМС сообщение или звонок**

Наиболее консервативный способ, который используется в системах многофакторной аутентификации много лет, считается устаревшим и не самым безопасным, но оставлен в системе MULTIFACTOR для случаев, когда прочие способы по разным причинам не используются. Разумеется, в настройках личного кабинета его можно выключить для всех пользователей или определенных групп.

### **6.9.1 Регистрация**

Для регистрации пользователю будет предложено ввести номер телефона и одноразовый код из СМС сообщения, отправленного системой MULTIFACTOR.

### **6.9.2 Аутентификация**

Пользователю необходимо ввести одноразовый код доступа, полученный в СМС сообщении, либо ответить на входящий звонок и нажать решетку.

## 7 Регистрация пользователей в системе

### 7.1 Способы регистрации второго фактора

Мультифактор предлагает несколько простых в настройке и использовании методов регистрации второго фактора.

При выборе ориентируйтесь на тип защищаемой системы, а также требования по поддержке определённых методов аутентификации и источников учётных записей.

#	Способ регистрации 2FA	Подходит для систем	Методы аутентификации	Источники учётных записей
1	В режиме диалога с пользователем	VPN и VDI клиенты	- Multifactor Push - Telegram Push - OTP - SMS	- ActiveDirectory - RADIUS (NPS) - Локальные учётные записи
2	В веб-приложениях	- Web и SAML приложения - Outlook Web Access (OWA)	Все доступные	- ActiveDirectory - Внешние IdP - RADIUS (NPS) - Локальные учётные записи
3	На портале самообслуживания	Любые	- Все доступные - Может работать как единая точка входа SSO	ActiveDirectory
4	По конфигурационной ссылке, высылаемой на email	Любые	Все доступные	- ActiveDirectory - Внешние IdP - RADIUS (NPS) - Локальные учётные записи
5	Автоматическая регистрация SMS	Любые	SMS	ActiveDirectory

### 7.2 Автоматизация

В данном разделе приведены примеры PowerShell-автоматизации для регистрации пользователей и рассылки конфигурационных ссылок на email.

#### 7.2.1 Экспорт пользователей из Active Directory

Экспорт всех пользователей, имеющих e-mail адрес в домене multifactor.local в CSV-файл C:\temp\ADusers.csv .

```
### start export
```

```
Get-ADUser -Filter {mail -like '*'} -SearchBase "CN=Users,DC=multifactor,DC=local" -Properties * |
Select -Property samaccountname,EmailAddress,DisplayName | Export-CSV "C:\\temp\\ADusers.csv" -
NoTypeInfo -Encoding UTF8
```

```
## end export
```

## 7.2.2 Импорт пользователей через API и отправка конфигурационных email

Импорт всех пользователей, имеющих e-mail адрес в домене multifactor.local в API

Мультифактора с одновременной отправкой ссылки для настройки второго фактора сроком 3 часа.

```
### start import
```

```
[Net.ServicePointManager]::SecurityProtocol =
```

```
[Net.SecurityProtocolType]::Tls12
```

```
$apiKey = "<API Key>"
```

```
$apiSecret = "<API Secret>"
```

```
$encodedCredentials =
```

```
[Convert]::ToBase64String([Text.Encoding]::ASCII.GetBytes("{0}:{1}" -f $apiKey, $apiSecret))
```

```
$parameters = @{
```

```
Uri = 'https://api.multifactor.ru/users'
```

```
Headers = @{ 'Authorization' = "Basic $encodedCredentials" }
```

```
Method = 'POST'
```

```
ContentType = 'application/json; charset=utf-8'
```

```
}
```

```
$users = Get-ADUser -Filter {mail -like '*'} -SearchBase
```

```
"CN=Users,DC=multifactor,DC=local" -Properties SamAccountName, Mail, DisplayName
```

```
$users | ForEach-Object {
```

```
$body = @{
```

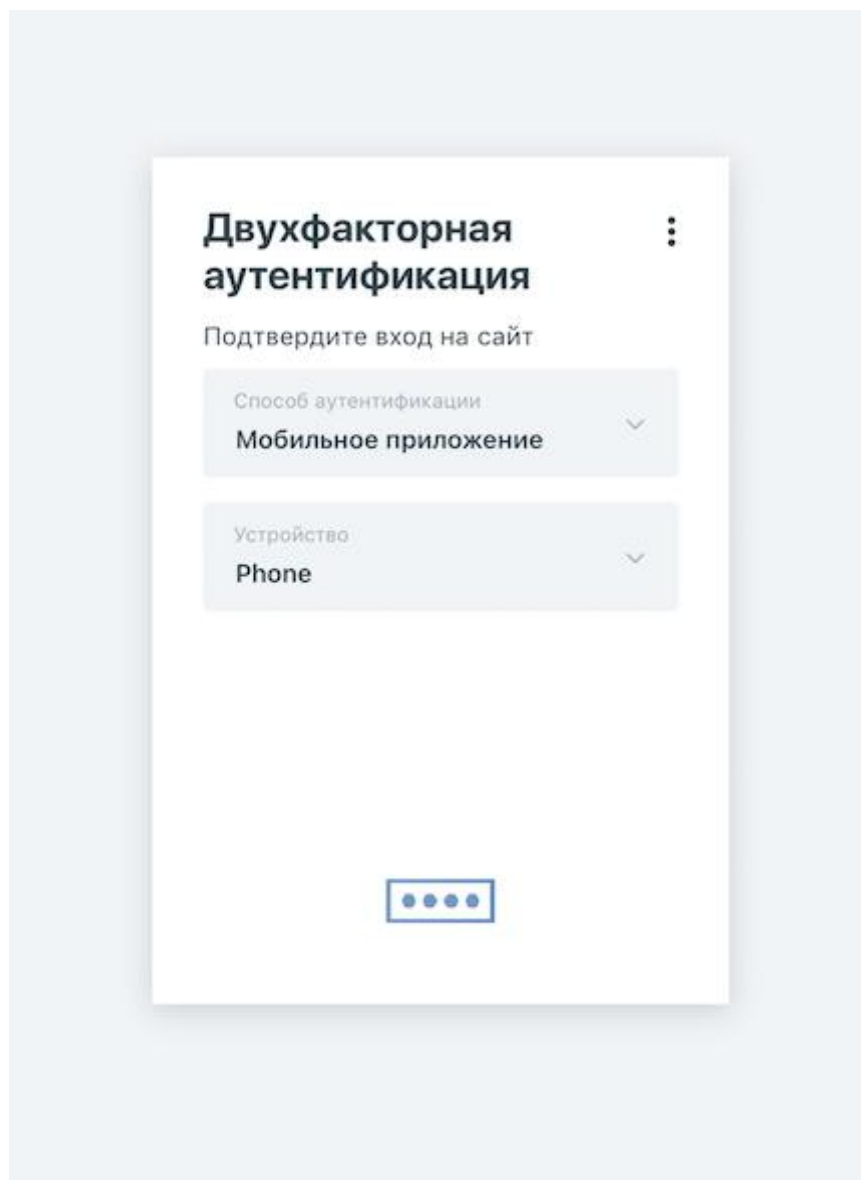
```
Identity = $_.SamAccountName
```

```
Email = $_.Mail  
  
Name = $_.DisplayName  
  
EnrollmentLink = @{ To = "email"  
  
Ttl = 180  
  
}  
  
} | ConvertTo-Json  
  
Invoke-RestMethod @parameters -Body $body }  
  
## end import
```

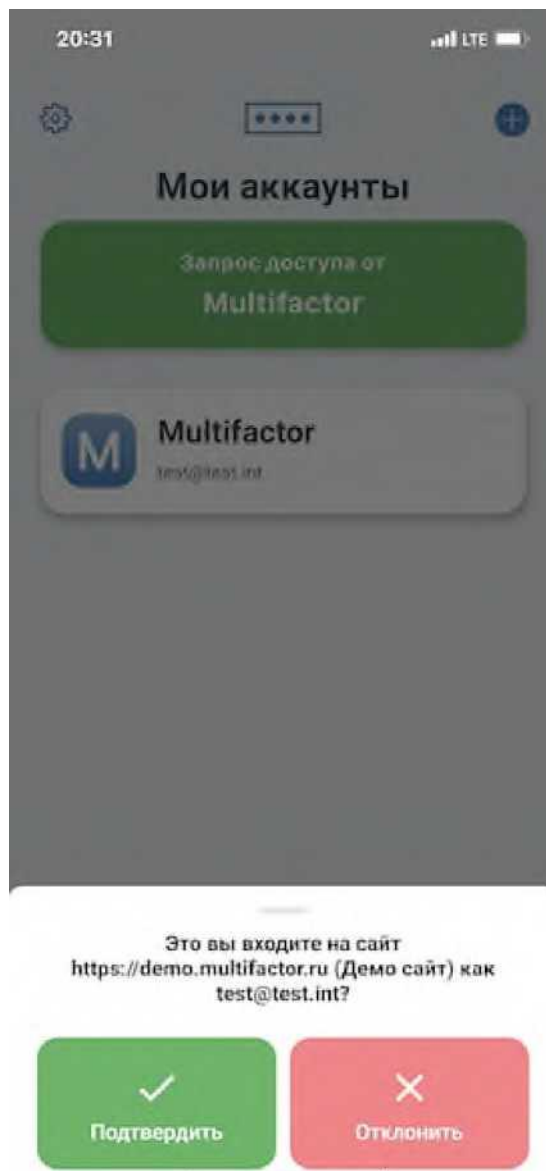
## 8 Способы аутентификации

### 8.1 Мобильное приложение Multifactor

Выберите аутентификацию через мобильное приложение Multifactor и устройство, на котором установлено приложение с привязанным аккаунтом.



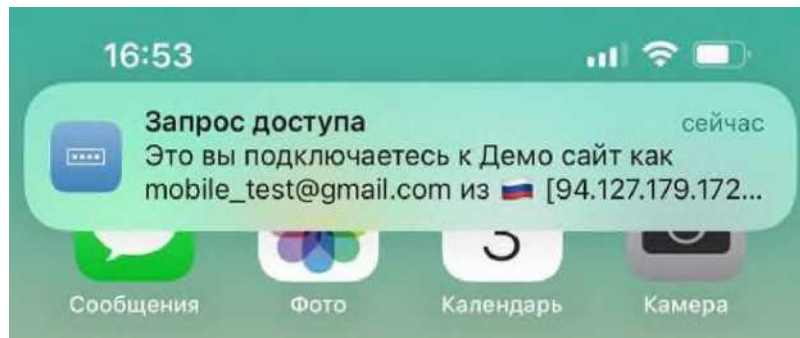
Мобильное приложение пришлёт Push-уведомление, в котором запросит, действительно ли вы подключаетесь к ресурсу.



Нажмите "Подтвердить", если сейчас действительно вы совершаете аутентификацию.

Нажмите "Отклонить", если не вы инициализировали процесс аутентификации. При этом тому, кто совершает вход, будет отказано в аутентификации.

Для удобства Push-уведомление доступно из "шторки".

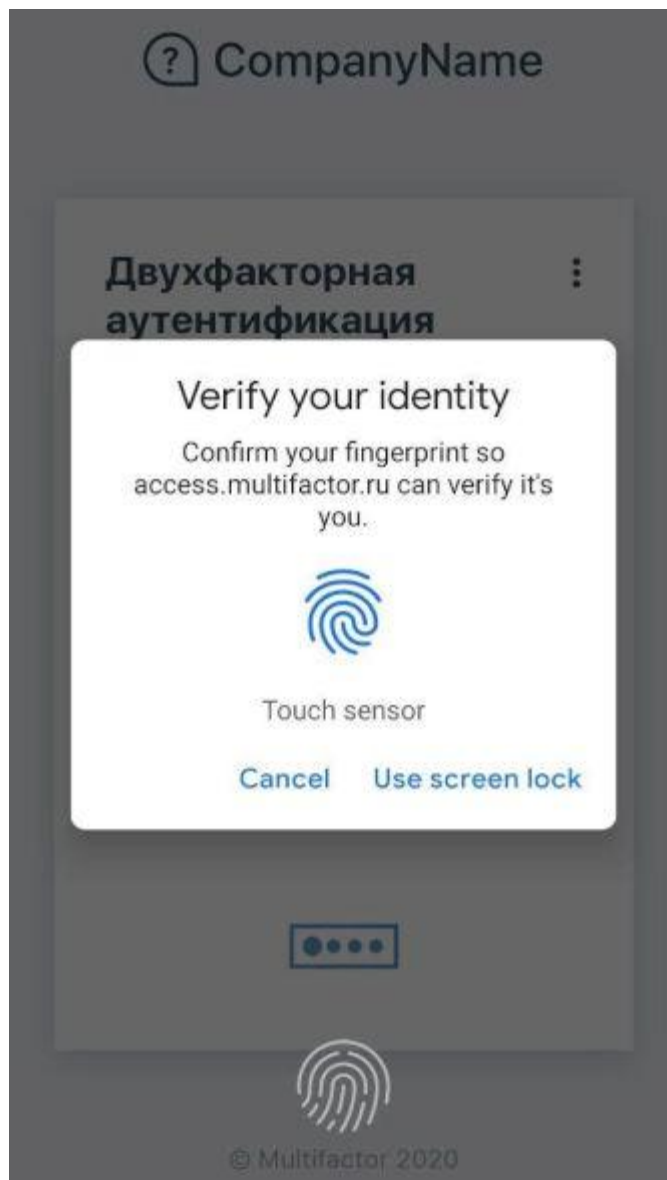


Если Push-уведомление не пришло в фоновом режиме, просто откройте приложение Multifactor.

## 8.2 Биометрия и U2F

Выберите пункт "Биометрия и U2F".

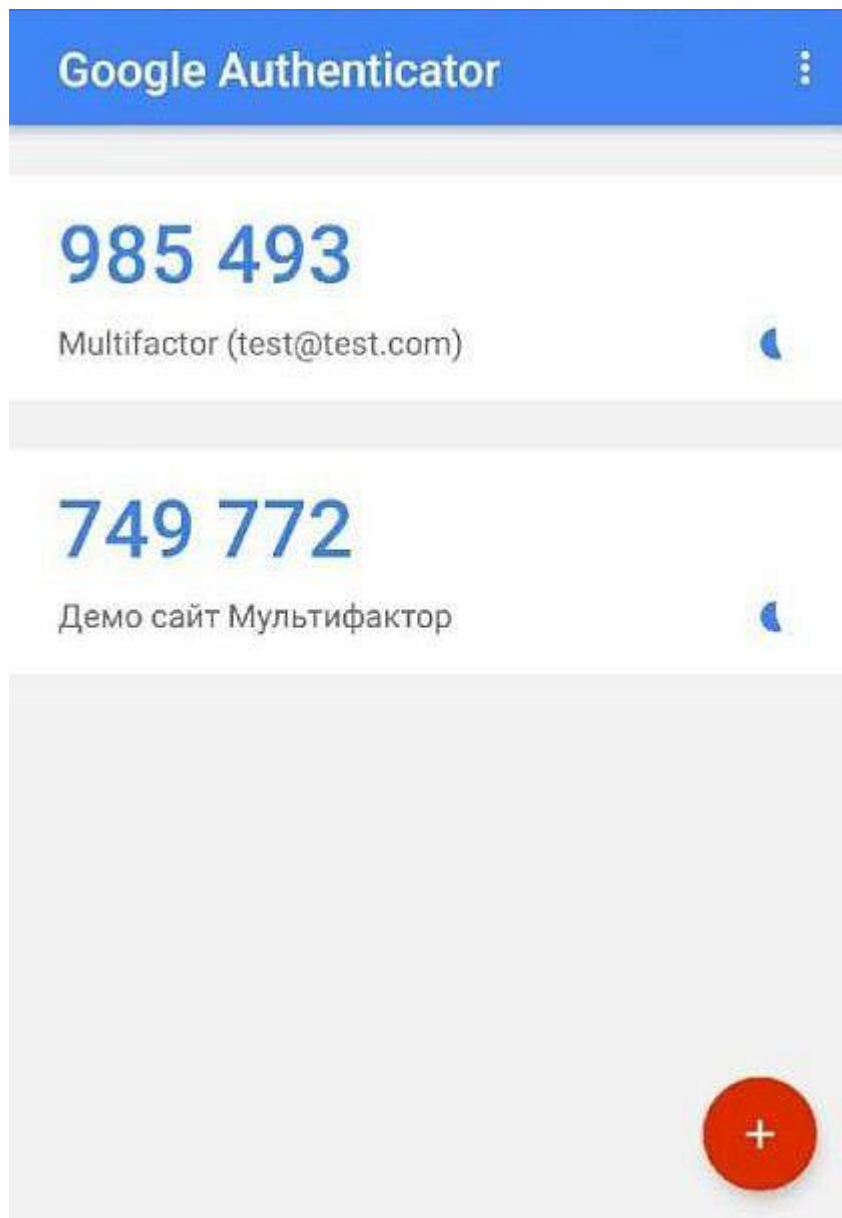
Ваше устройство может предложить вам авторизоваться с помощью биометрического датчика



Так же вы можете воспользоваться аппаратным U2F-токеном: вставьте его в устройство, на котором проходите авторизацию и активируйте.

### 8.3 Google Authenticator/Я.Ключ

Откройте соответствующее мобильное приложение с одноразовыми кодами.



Введите код аутентификации из мобильного приложения в форму аутентификации.

**Двухфакторная аутентификация**

Подтвердите вход на сайт

Способ аутентификации  
**Google Authenticator/Я.Ключ**

Приложение  
**Authenticator 1**

Введите код  
**74977**

⋮

## 8.4 ОТР-токен

Для авторизации с помощью ОТР-токена вставьте его в ваше устройство, установите курсор поле с подсказкой "Введите код" и активируйте сам токен.

## Двухфакторная аутентификация



Подтвердите вход на сайт

Способ аутентификации

**ОТР-токен**



Токен

**ОТР 1**



Введите код



## 9 Мобильное приложение Multifactor

Мобильное приложение Multifactor является собственной разработкой компании МУЛЬТИФАКТОР и рекомендуется как один из самых безопасных методов аутентификации.

Установите приложение Multifactor на свой смартфон

- RuStore
- [Huawei AppGallery](#)  
[Аврора Маркет](#)  
Скачайте apk файл
- [Скачайте rpm файл для Аврора](#)

### I

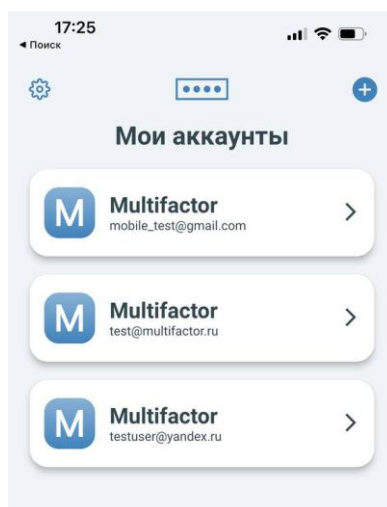
#### © ОБНОВЛЕНИЕ ПРИЛОЖЕНИЯ

В случае возникновения проблем с приходом push-уведомлений после обновления пользователям необходимо открыть мобильное приложение Multifactor и подтвердить запрос доступа внутри приложения.

## 9.1 Функциональные возможности

### 9.1.1 Мои аккаунты

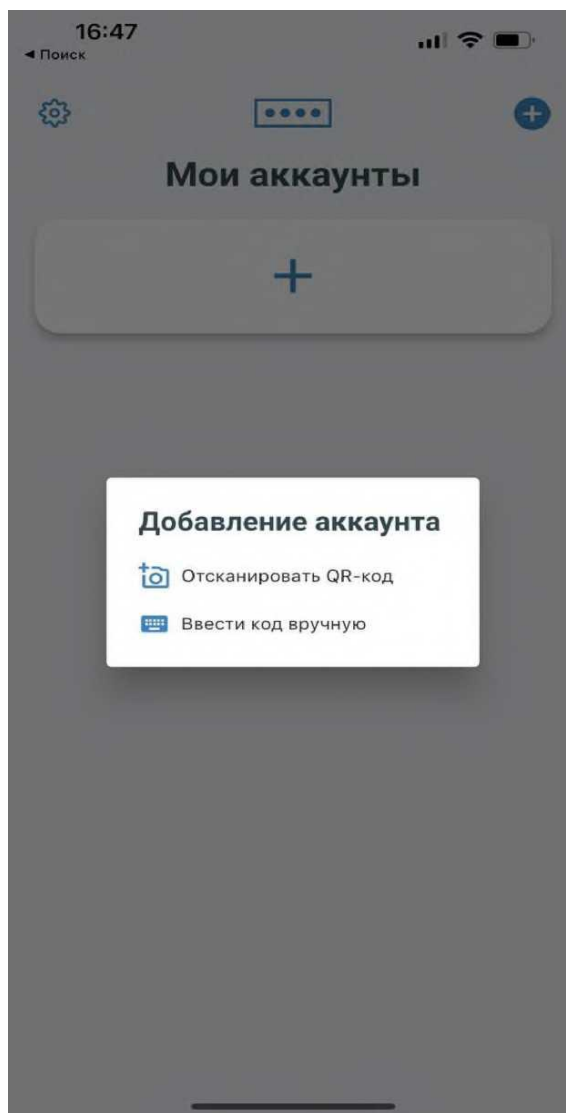
Данный раздел мобильного приложения отображает все аккаунты, которые были созданы вами.



### 9.1.2 Добавление аккаунта

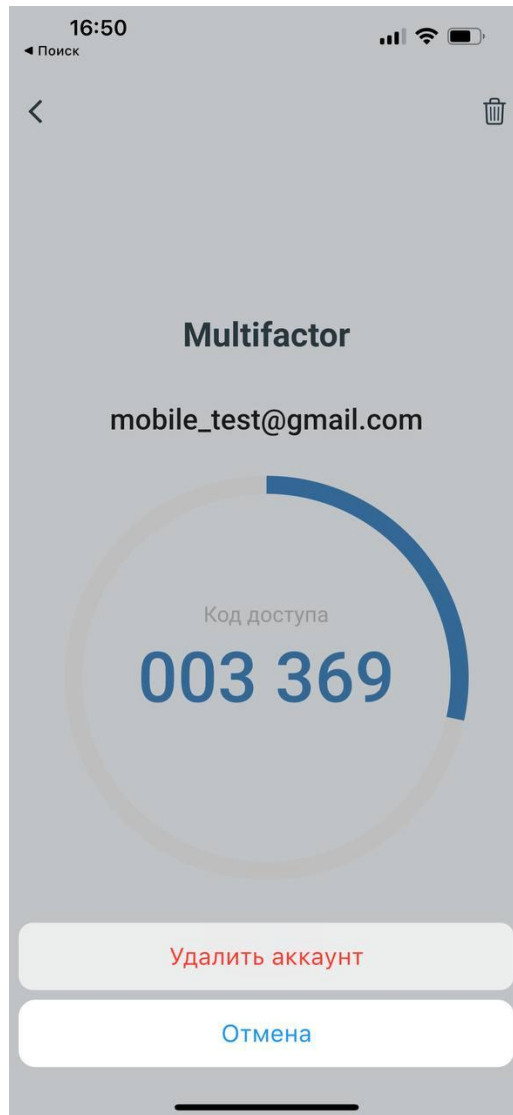
Чтобы добавить новый аккаунт в мобильном приложении нажмите на “+” в верхнем правом углу:

- Отсканировать QR-код
- Ввести код вручную



### 9.1.3 Удаление аккаунта

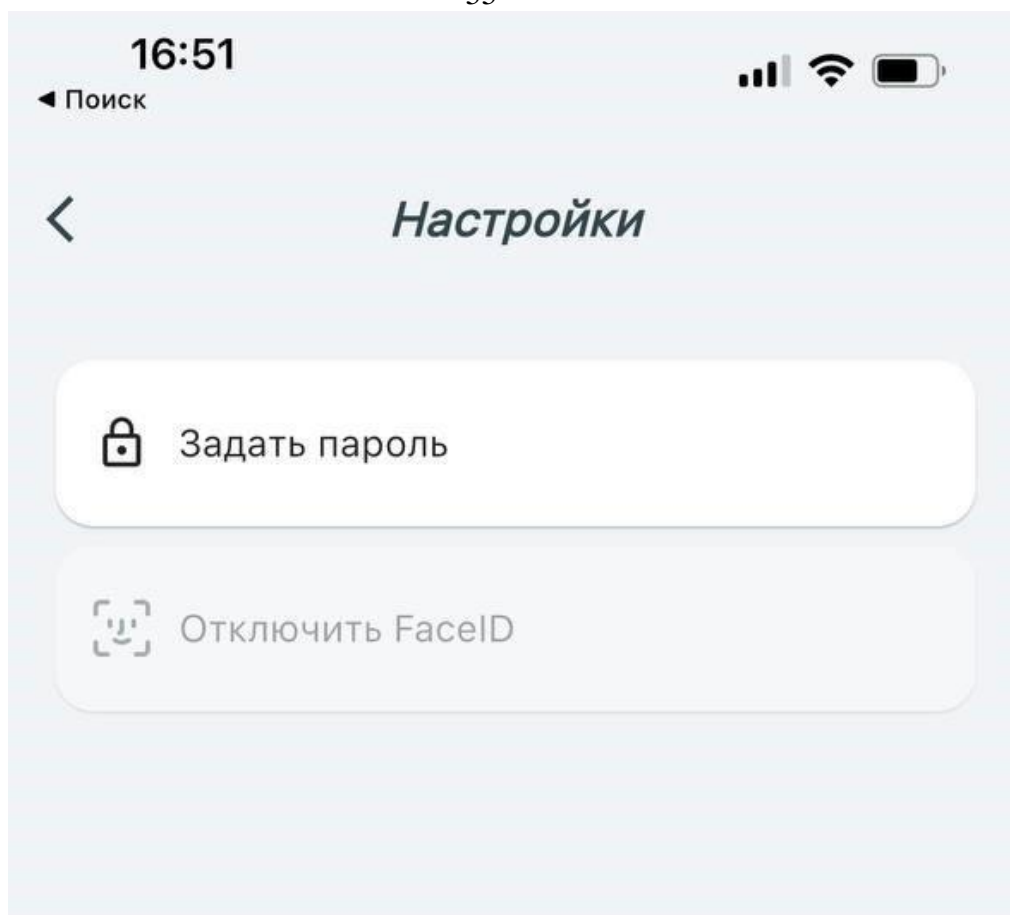
Для удаления аккаунта из приложения Multifactor необходимо зайти в аккаунт и нажать на “корзину” в правом верхнем углу и далее подтвердить удаление нажав кнопку Удалить аккаунт или отменить.



#### 9.1.4 Настройки мобильного приложения Multifactor

Для входа в режим настройки нажмите на "шестеренку" в левом верхнем углу.

- Вы можете задать пароль для входа в приложение Multifactor
- Вы можете отключить или подключить вход в приложение Multifactor, используя биометрию доступную в смартфоне. Например, FaceID, Fingerprint и др.

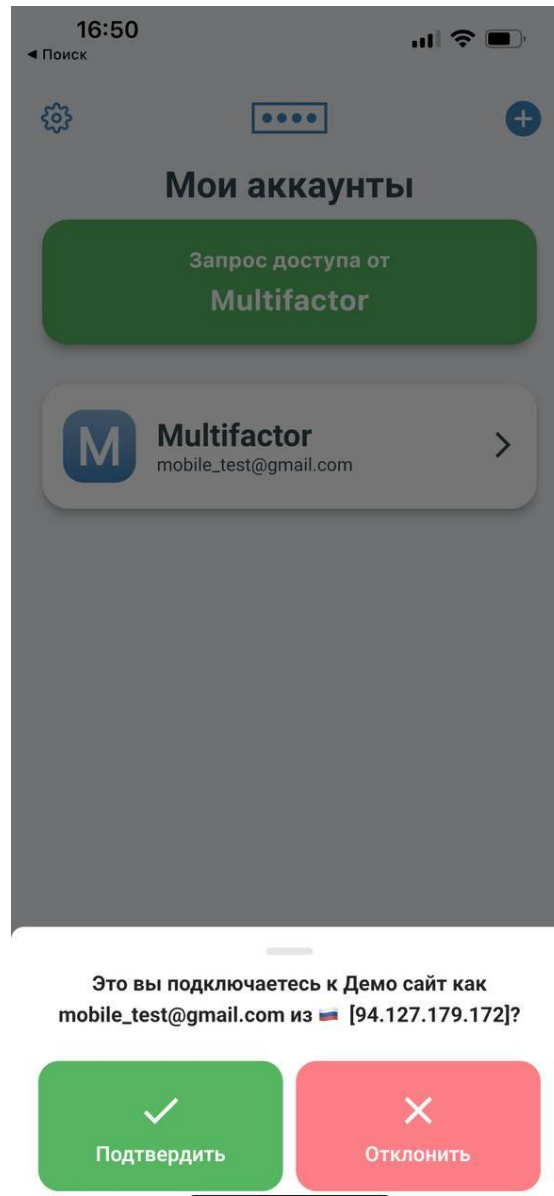


#### © ЯЗЫК ПРИЛОЖЕНИЯ

Язык приложения Multifactor зависит от языка вашей операционной системы.  
Доступные языки Русский и Английский.

#### 9.1.5 Запрос доступа от Multifactor

Мобильное приложение пришлёт Push-уведомление, в котором запросит, действительно ли вы подключаетесь к ресурсу. Подробнее запросы доступа описаны в разделе Аутентификация.



#### © СПАМ-ФИЛЬТР

Если вы не подтвердили несколько запросов доступа через Push- уведомления подряд, то автоматически включается спам-фильтр. Для его отключения необходимо открыть приложение и подтвердить запрос доступа внутри приложения Multifactor.

#### 9.1.6 Push-системы

Мобильное приложение Multifactor работает с несколькими Push-системами которые подключаются в приоритетном порядке:

- Google firebase
- Huawei Mobile Services
- Собственная Push-система Pushed . Доступна для android

### © УСТАРЕВШИЕ ТОКЕНЫ

Особенность работы с push-системой firebase - по истечении времени клиентские токены устаревают. Для обновления токена пользователям необходимо просто зайти в мобильное приложение Multifactor.

### 9.1.7 Внешние приложения

Мобильное приложение Multifactor поддерживает подтверждение доступа одноразовым кодом на основе времени (Time-based one-time password). Аккаунты пользователей в приложении Multifactor содержат динамический (меняющийся раз в 30 секунд) 6-значный код, который можно использовать для получения доступа в аккаунты внешних поставщиков аутентификации (аналогично Google Authenticator). Для регистрации таких аккаунтов пользователю достаточно отсканировать QR-код, используя приложение Multifactor. Аккаунты будут добавляться с пометкой “Внешний”.



## Антиспам

Спам в нашем понимании - это слишком частые неподтвержденные запросы доступа. Попасть в антиспам - это значит перестать получать пуш-уведомления. В антиспам могут попасть **только пользователи ресурсов типа radius.**

Антиспам имеет две ступени:

1. Сокращенное время ожидания подтверждения запроса доступа.
2. Отключение пуш-уведомлений в нашем мобильном приложении.

### 9.1.8 Визуализация антиспама

В админке появились бэйджики "Антиспам". Они могут отображаться на запросах и юзерах. Если **на момент создания** запроса доступа юзер находился в антиспаме, бэйджик отобразится на запросе доступа в общем списке и на странице с деталями запроса доступа. То же самое касается и юзера - если он **в данный момент** в антиспаме, в общем списке и на странице с деталями будет этот бэйджик. Нет, фильтровать список юзеров по антиспаму нельзя.

### 9.1.9 Кто попадает в антиспам

Если пользователь не подтвердил подряд два запроса доступа за 10 минут, он попадает на первую ступень. Если пользователь продолжил не подтверждать запросы доступа, и появились еще два неподтвержденных запроса доступа за 90 секунд, юзер попадает на вторую ступень.

Подтверждение фактора в приложении снимает с юзера все санкции.

## 10 Действий после сбоев и ошибок эксплуатации средства

Список возможных ошибок представлен в РОФ.42584334.58.29.12.01 РА 01 с.342  
Действия после сбоев указаны в разделах «Вопросы и ответы» в РОФ.42584334.58.29.12.01 РА 01.

## Перечень принятых сокращений

АРМ	–	автоматизированное рабочее место
БД	–	база данных
ИАФ	–	идентификация и аутентификация субъектов доступа и объектов доступа
ИБ	–	информационная безопасность
ОС	–	операционная система
ОЦЛ	–	обеспечение целостности информационной системы и персональных данных
ПО	–	программное обеспечение
РСБ	–	регистрация событий безопасности
СЗИ	–	средства защиты информации
СОВ	–	система обнаружения вторжений
СУБД	–	система управления базами данных
УПД	–	управление доступом субъектов доступа к объектам доступа
ЭВМ	–	электронная вычислительная машина

