Dropbox, Google, Facebook и Twitter

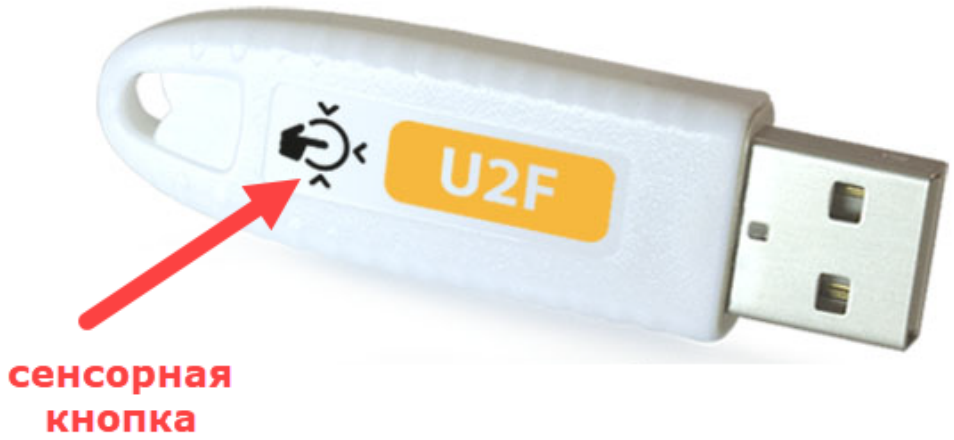
В этом документе

- Общая информация
- Первое подключение Рутокен U2F к компьютеру
- Настройка двухфакторной аутентификации с использованием устройства Рутокен U2F в облачном хранилище Dropbox
  - Проверка включения двухэтапной проверки в Dropbox
  - Включение двухэтапной проверки в Dropbox
  - Добавление устройства Рутокен U2F к аккаунту в Dropbox
  - Вход в аккаунт с помощью устройства Рутокен U2F в Dropbox
  - Удаление сведений о Рутокен U2F в Dropbox
- Настройка двухфакторной аутентификации с использованием устройства Рутокен U2F в Google
  - Проверка включения двухэтапной аутентификации в Google
  - Включение двухэтапной аутентификации в Google
  - Добавление устройства Рутокен U2F к аккаунту в Google
  - Вход в аккаунт с помощью устройства Рутокен U2F в Google
  - Удаление сведений о Рутокен U2F в Google
- Настройка двухфакторной аутентификации в социальной сети Facebook
  - Проверка включения двухфакторной аутентификации в Facebook
  - Включение двухфакторной аутентификации в Facebook
  - Добавление устройства Рутокен U2F к аккаунту в Facebook
  - Вход в аккаунт с помощью устройства Рутокен U2F в Facebook
  - Удаление сведений о Рутокен U2F в Facebook
- Настройка двухфакторной аутентификации с использованием устройства Рутокен U2F в социальной сети Twitter
  - Проверка включения двухфакторной аутентификации в Twitter
  - Включение двухфакторной аутентификации в Twitter
  - Добавление устройства Рутокен U2F к аккаунту в Twitter
  - Вход в аккаунт с помощью устройства Рутокен U2F в Twitter
  - Удаление сведений о Рутокен U2F в Twitter
- Приложение 1. Очистка кэша и временных данных в браузере
  - Браузер Google Chrome
  - Браузер Mozilla Firefox
  - Браузер Opera

Общая информация

Рутокен U2F — устройство, предназначенное для усиления парольной защиты учетных записей пользователя на различных интернет-ресурсах.

На корпусе устройства Рутокен U2F есть встроенная сенсорная кнопка. Она предназначена для подтверждения физического присутствия пользователя. Кнопка приводится в действие при нажатии на нее пальцем.



Одно устройство может использоваться для доступа к различным ресурсам.

Процедура аутентификации с Рутокен U2F состоит из двух этапов:

1. Ввод логина и пароля от аккаунта.
2. Подключение устройства Рутокен U2F и нажатие на сенсорную кнопку.

Процессы, описанные в данной инструкции, актуальны для работы со следующими ресурсами:

- облачным хранилищем Dropbox (в браузерах Mozilla Firefox, Google Chrome и Opera);
- сайтом Google (в браузерах Google Chrome и Opera);
- социальной сетью Facebook (в браузерах Google Chrome и Opera);
- социальной сетью Twitter (в браузерах Google Chrome и Opera).

Полный список публичных сервисов, поддерживающих стандарт FIDO U2F: http://www.dongleauth.info

Первое подключение Рутокен U2F к компьютеру

Для подключения Рутокен U2F вставьте его в USB-порт компьютера. Если устройство подключено корректно, то на нем начнет светиться индикатор.

При первом подключении устройства к компьютеру выполнится поиск и автоматическая установка необходимых драйверов.

Настройка двухфакторной аутентификации с использованием устройства Рутокен U2F в облачном хранилище Dropbox

В Dropbox двухфакторная аутентификация называется **двухэтапной проверкой**. Поэтому далее в описаниях раздела используется именно этот термин.

В этом разделе:

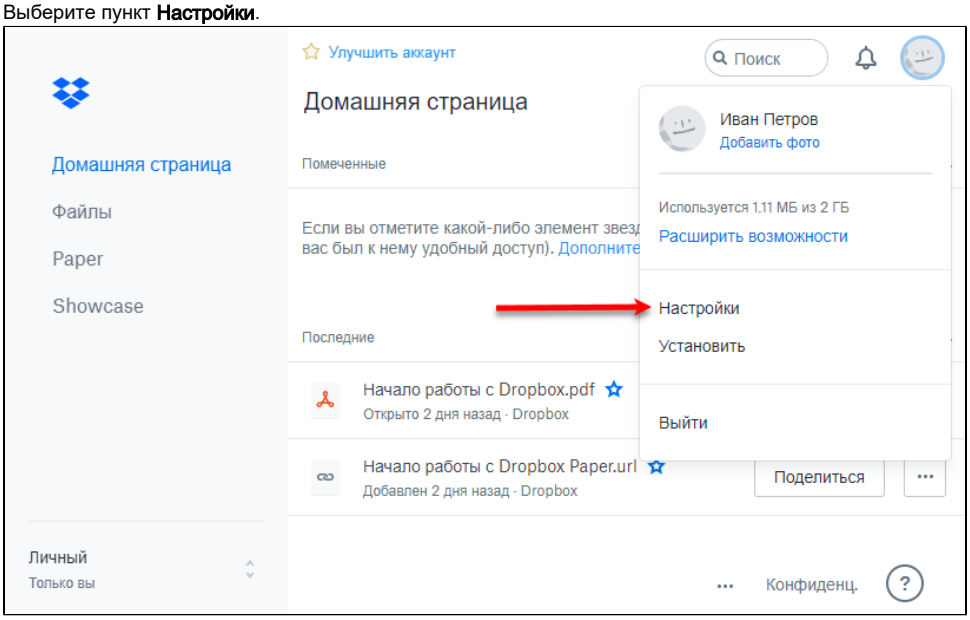
- Как проверить статус включения двухэтапной проверки?
- Как включить двухэтапную проверку?
- Как добавить Рутокен U2F к аккаунту?
- Как войти в аккаунт с помощью Рутокен U2F?
- Что делать, если потерял устройство Рутокен U2F?

Перед тем, как настроить двухэтапную проверку необходимо проверить включена она или нет в аккаунте.

Проверка включения двухэтапной проверки в Dropbox

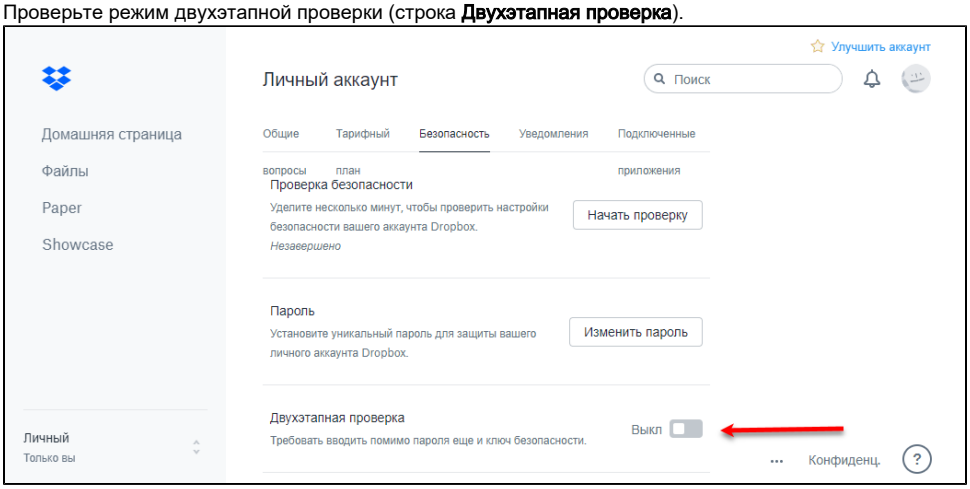
Для проверки включения двухэтапной проверки:

1. Зайдите в свой аккаунт.
2. Нажмите на фото своего профиля.
3. Выберите пункт **Настройки**.



4. Перейдите на вкладку **Безопасность**.

5. Проверьте режим двухэтапной проверки (строка **Двухэтапная проверка**).



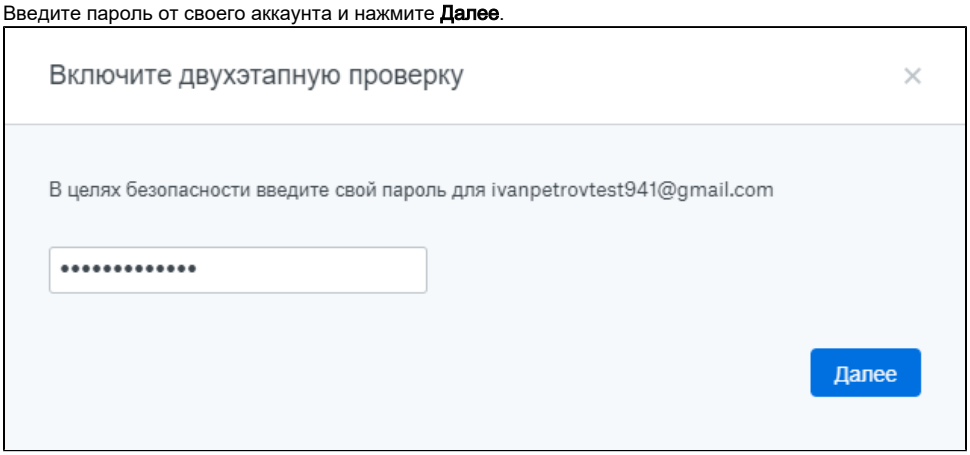
6. Если двухэтапная проверка выключена (выбран режим **Выкл**), то ее необходимо включить. Для этого перейдите в раздел Включение двухэтапной проверки.
7. Если двухэтапная проверка включена (выбран режим **Вкл**), то необходимо сразу перейти к настройке устройства Рутокен U2F. Для этого перейдите в раздел Добавление устройства Рутокен U2F к аккаунту.

Включение двухэтапной проверки в Dropbox

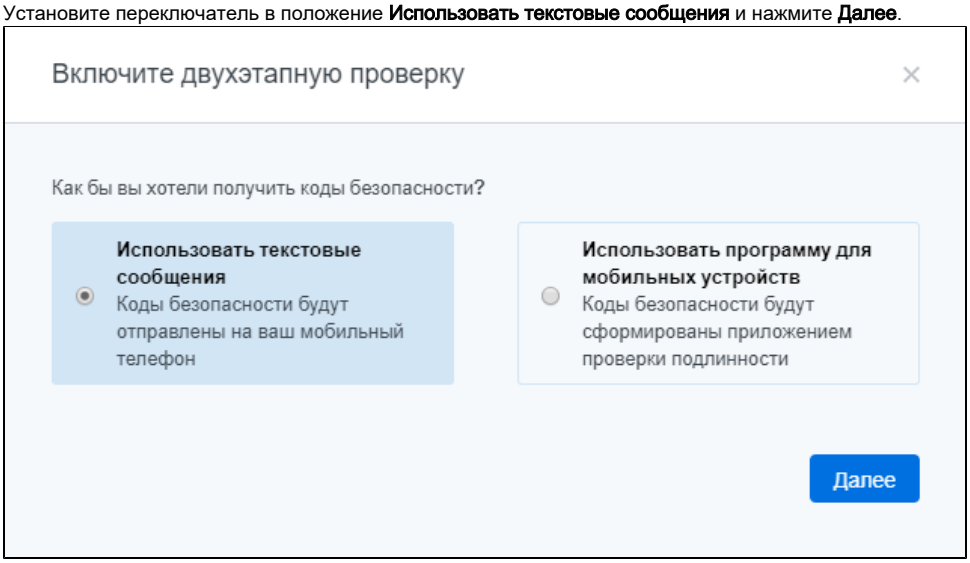
Для включения двухэтапной проверки вам понадобится мобильный телефон.

Чтобы включить двухэтапную проверку:

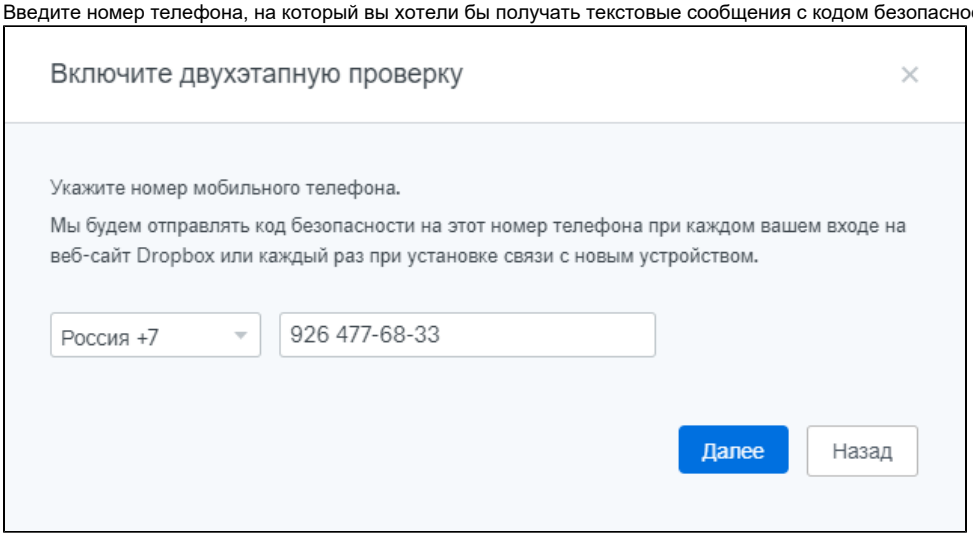
1. На вкладке **Безопасность** измените режим в строке **Двухэтапная проверка** на **Вкл**.
2. Нажмите **С чего начать**.
3. Введите пароль от своего аккаунта и нажмите **Далее**.



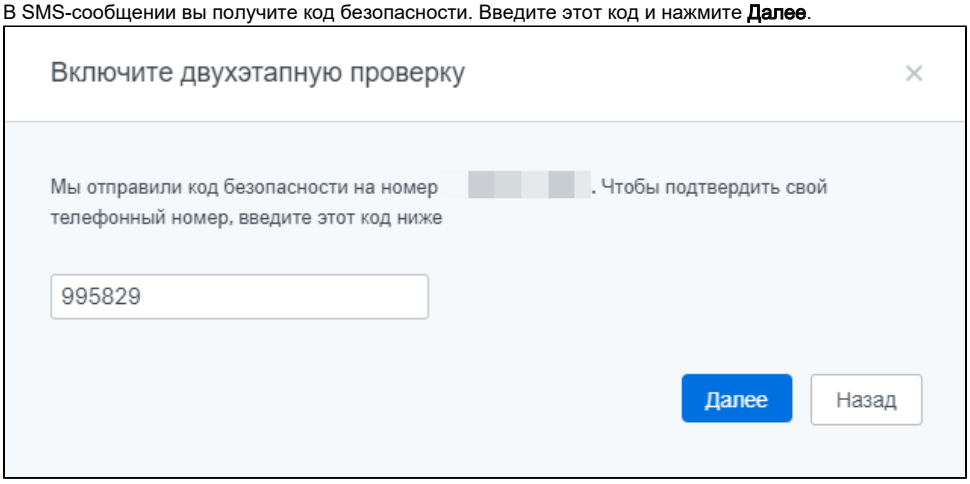
4. Установите переключатель в положение **Использовать текстовые сообщения** и нажмите **Далее**.



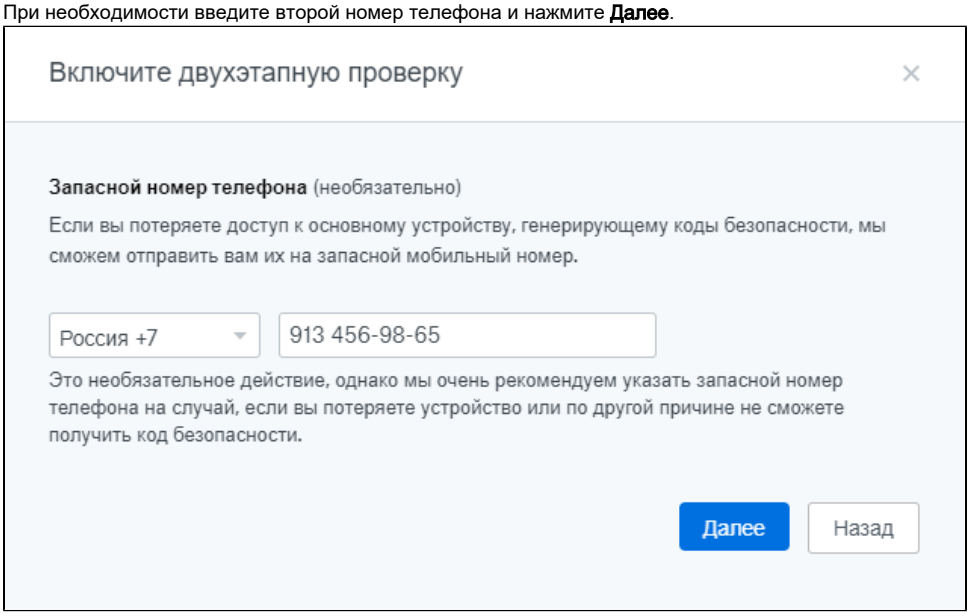
5. Введите номер телефона, на который вы хотели бы получать текстовые сообщения с кодом безопасности, и нажмите **Далее**.



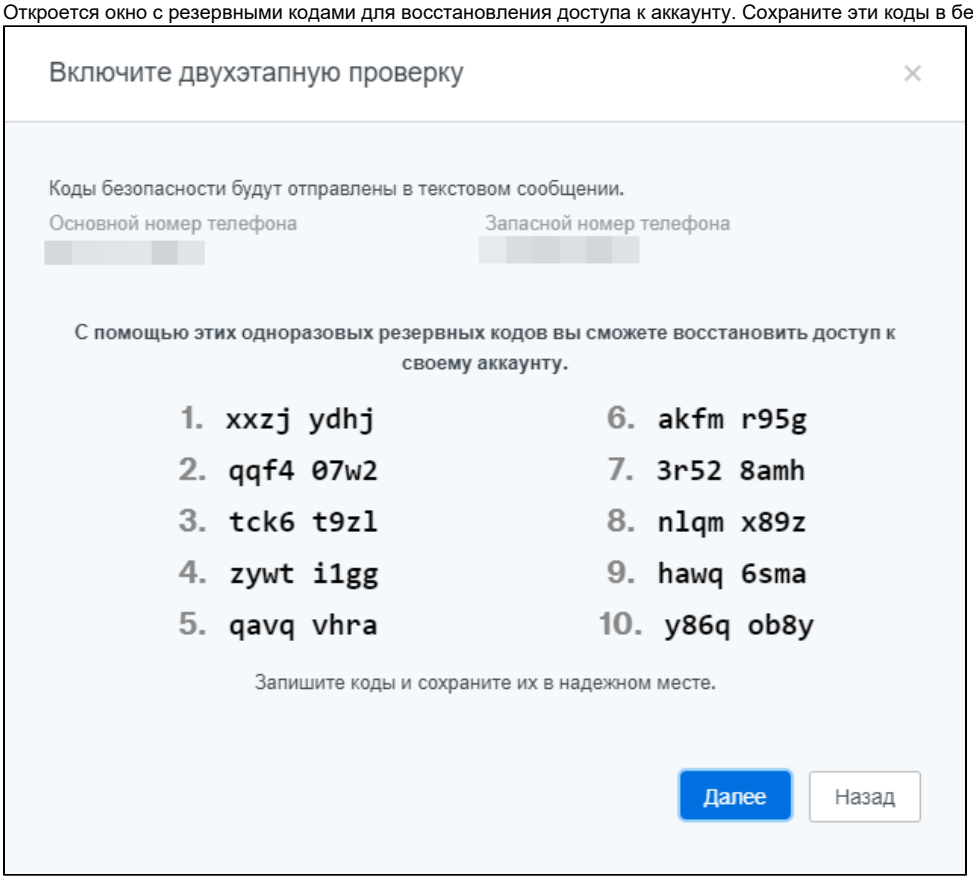
6. В SMS-сообщении вы получите код безопасности. Введите этот код и нажмите **Далее**.



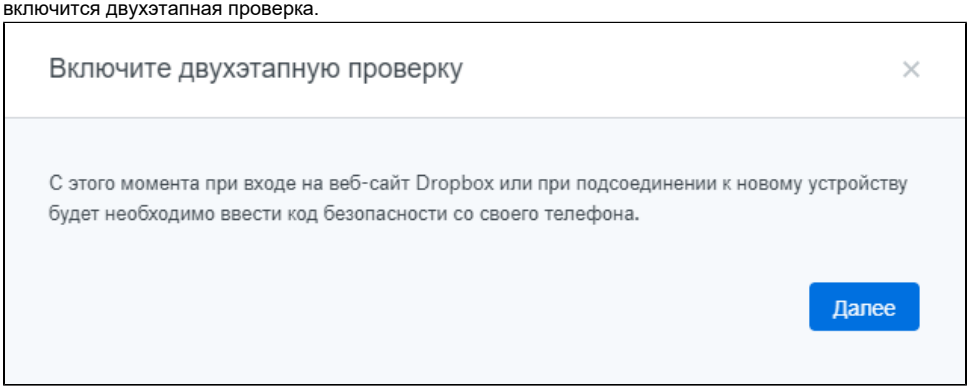
7. При необходимости введите второй номер телефона и нажмите **Далее**.



8. Откроется окно с резервными кодами для восстановления доступа к аккаунту. Сохраните эти коды в безопасном месте и нажмите **Далее**.



9. В окне с уведомлением о том, что теперь для входа в аккаунт нужно будет ввести код безопасности нажмите **Далее**. В результате включится двухэтапная проверка.



После этого необходимо добавить устройство Рутокен U2F к аккаунту (этот процесс описан в следующем разделе).

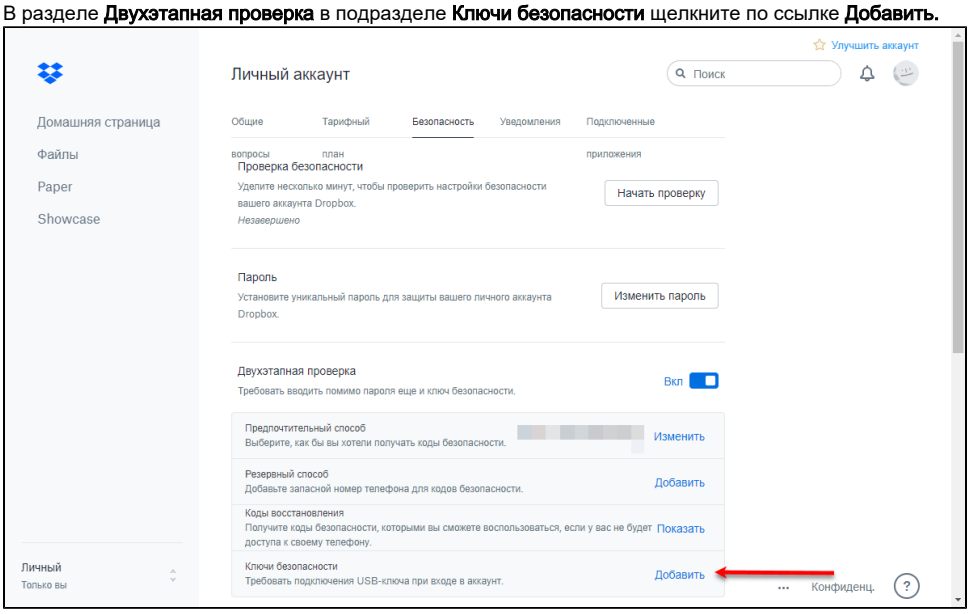
Добавление устройства Рутокен U2F к аккаунту в Dropbox

Перед тем, как добавить устройство к аккаунту необходимо проверить корректность его работы. Для этого подключите Рутокен к USB-порту компьютера. Если он подключен корректно, то на нем начнет светиться индикатор. Если этого не произошло, то попробуйте подключить Рутокен к другому USB-порту компьютера.

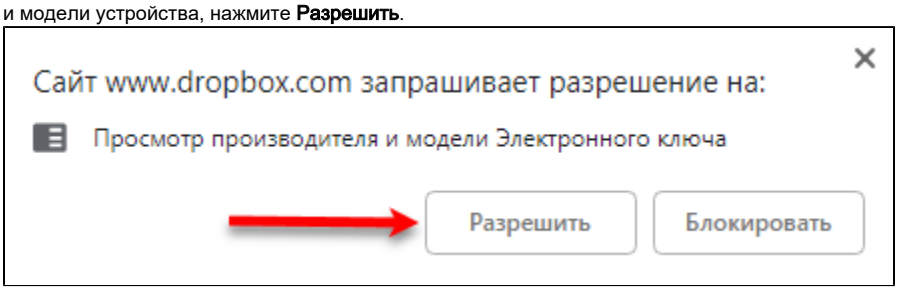
Чтобы добавить Рутокен U2F к аккаунту:

1. Подключите Рутокен U2F к компьютеру.
2. Зайдите в свой аккаунт.
3. Перейдите на вкладку **Безопасность**.

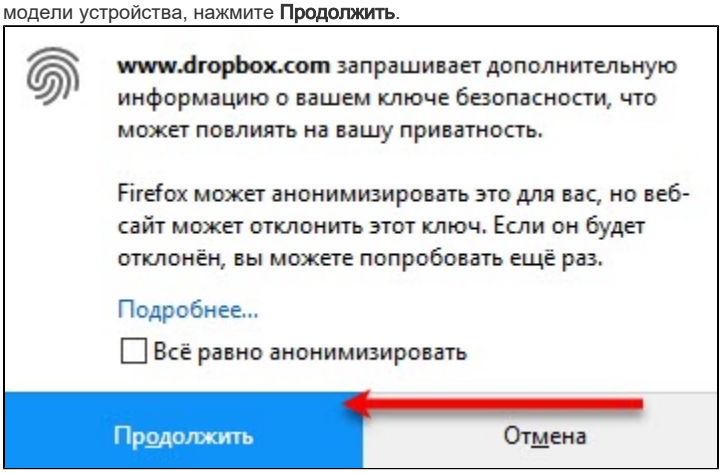
4. В разделе **Двухэтапная проверка** в подразделе **Ключи безопасности** щелкните по ссылке **Добавить.**



5. Нажмите **Начать установку**.
6. Введите пароль от своего аккаунта и нажмите **Далее**.
7. Нажмите **Ключ вставлен**. На токене начнет мигать индикатор.
8. Нажмите на сенсорную кнопку на устройстве Рутокен U2F.
9. Браузер Google Chrome: в окне с уведомлением о том, что сайт www.dropbox.com запрашивает разрешение на просмотр производителя и модели устройства, нажмите **Разрешить**.



Браузер Mozilla Firefox: в окне с уведомлением о том, что сайт www.dropbox.com запрашивает разрешение на просмотр производителя и модели устройства, нажмите **Продолжить**.

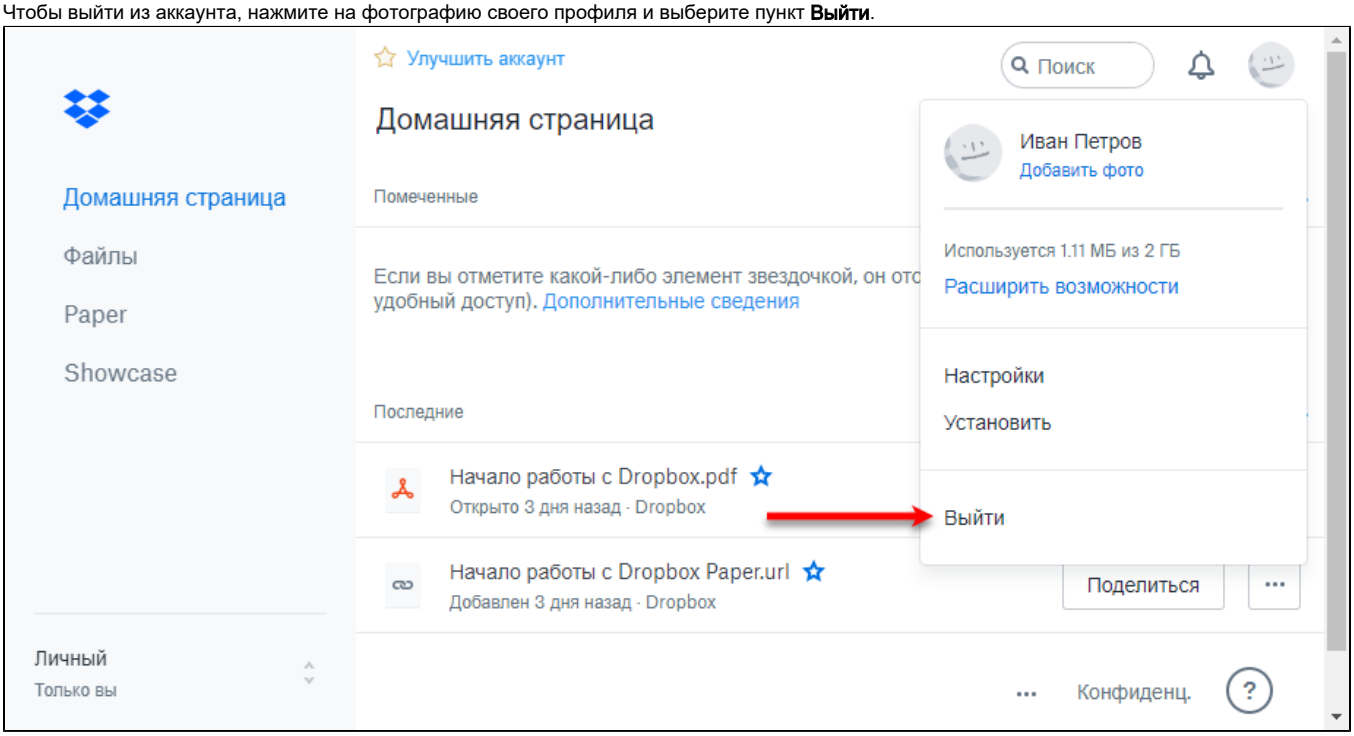


10. На экране отобразится окно с подтверждением того, что устройство добавлено и с полем для ввода имени устройства. Введите имя устройства и нажмите **Готово**.



В результате для аутентификации на сайте www.dropbox.com будет использоваться Рутокен U2F. Давайте это проверим. Для этого выйдите из своего аккаунта и снова зайдите в него.

Чтобы выйти из аккаунта, нажмите на фотографию своего профиля и выберите пункт **Выйти**.



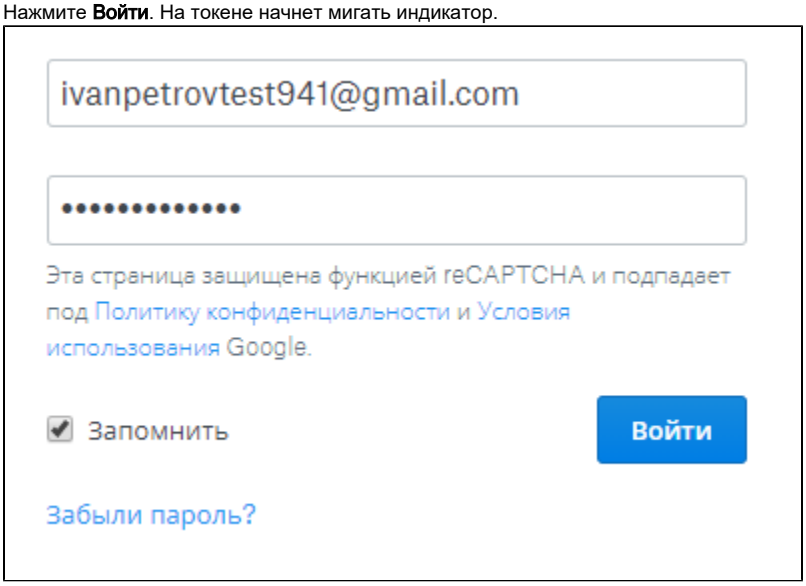
Теперь зайдите в свой аккаунт с помощью Рутокен U2F (этот процесс описан в следующем разделе).

Вход в аккаунт с помощью устройства Рутокен U2F в Dropbox

Чтобы войти в аккаунт:

1. Подключите Рутокен U2F к компьютеру.
2. Введите логин и пароль от своего аккаунта.

3. Нажмите **Войти**. На токене начнет мигать индикатор.



   Если после нажатия на кнопку **Войти** вы сразу зашли в свой аккаунт, то двухфакторная аутентификация с использование Рутокен U2F не сработала, а значит вам надо очистить кэш и временные данные, а затем перезагрузить компьютер. Этот процесс описан в приложении.
4. Нажмите на сенсорную кнопку на устройстве Рутокен U2F. В результате вы зайдете в свой аккаунт.

Удаление сведений о Рутокен U2F в Dropbox

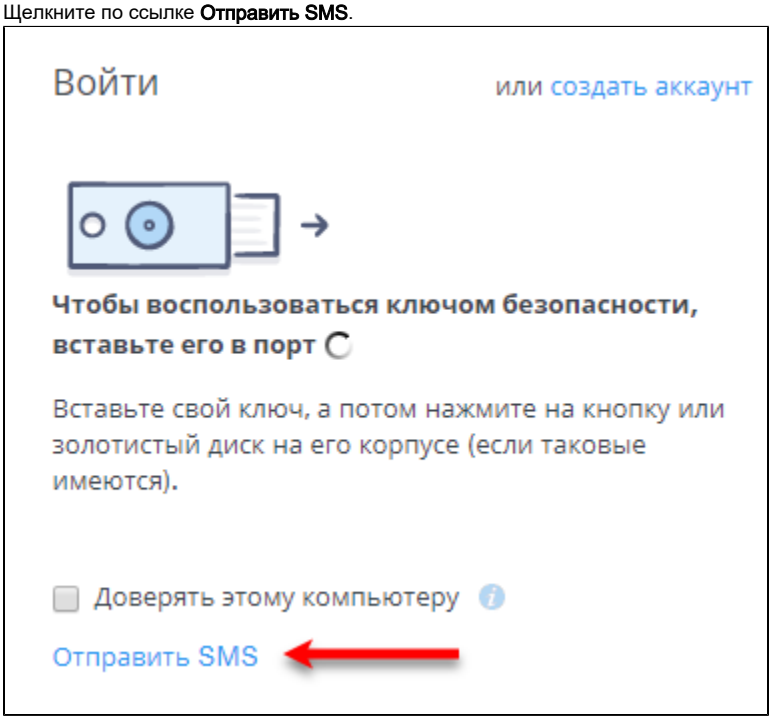
Если вы потеряли Рутокен U2F, который был привязан к аккаунту, или он перестал работать, то необходимо в Dropbox удалить сведения о нем.

Для удаления сведений об устройстве вам понадобится мобильный телефон, номер которого был указан при включении двухэтапной проверки, или один из одноразовых кодов безопасности.

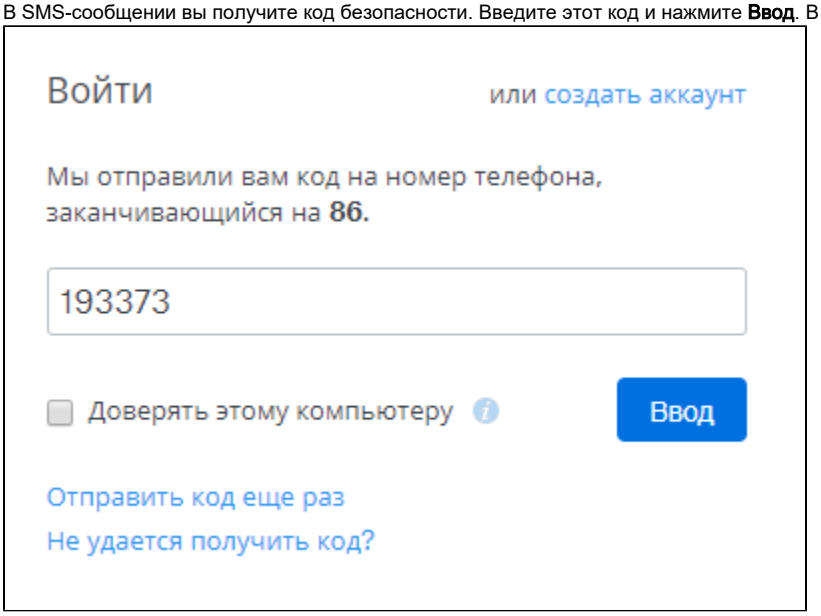
Для начала войдите в свой аккаунт при помощи мобильного телефона или кода безопасности (10 таких кодов вы сохранили на этапе включения двухэтапной проверки).

Чтобы войти в свой аккаунт при помощи мобильного телефона:

1. Введите пароль от своего аккаунта и нажмите **Войти**.
2. Щелкните по ссылке **Отправить SMS**.

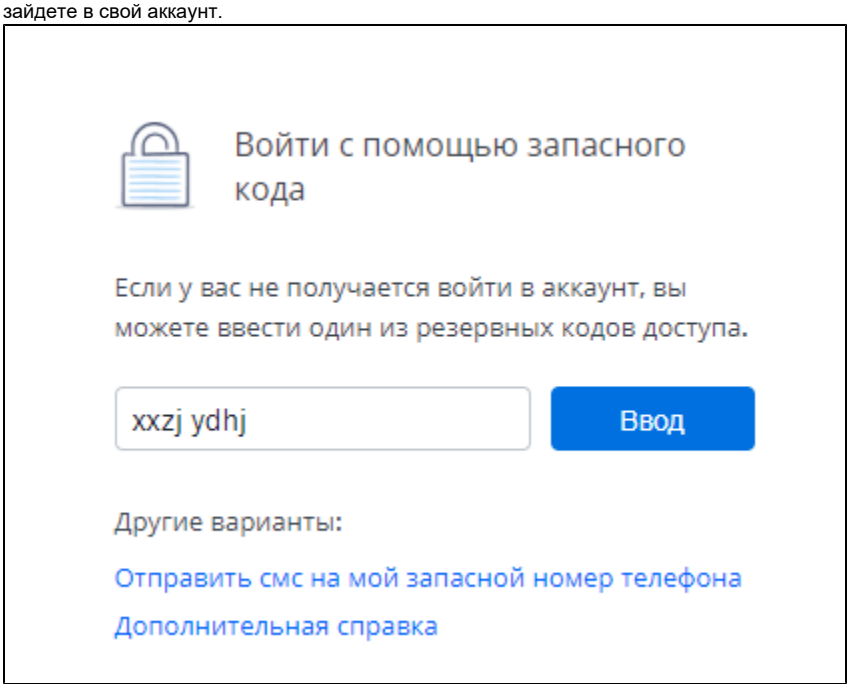


3. В SMS-сообщении вы получите код безопасности. Введите этот код и нажмите **Ввод**. В результате вы зайдете в свой аккаунт.



Чтобы войти в свой аккаунт при помощи кода безопасности:

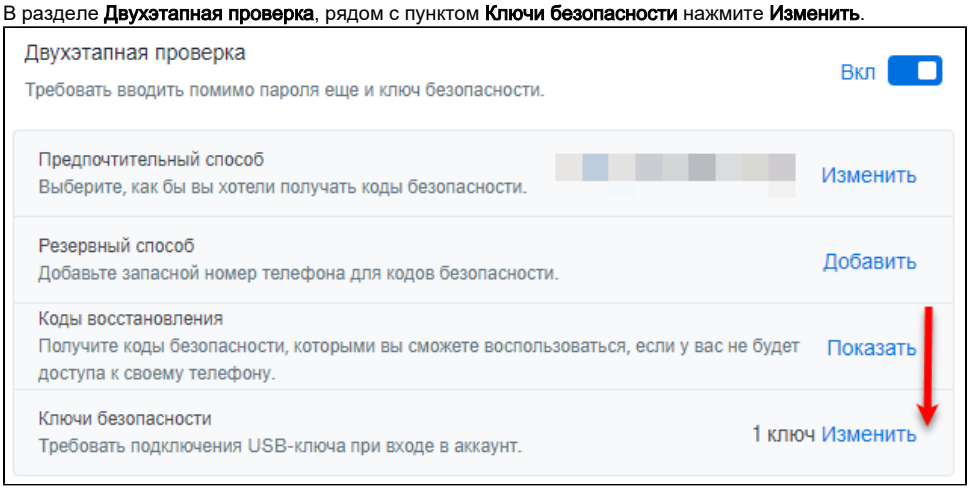
1. Введите пароль от своего аккаунта и нажмите **Войти**.
2. В всплывающем окне для входа по токену нажмите **Отмена**.
3. Щелкните по ссылке **Отправить SMS**.
4. Щелкните по ссылке **Не удается получить код?**.
5. Щелкните по ссылке **Введите запасной код доступа**.
6. Введите код безопасности (10 таких кодов вы сохранили на этапе включения двухэтапной проверки) и нажмите **Ввод**. В результате вы зайдете в свой аккаунт.



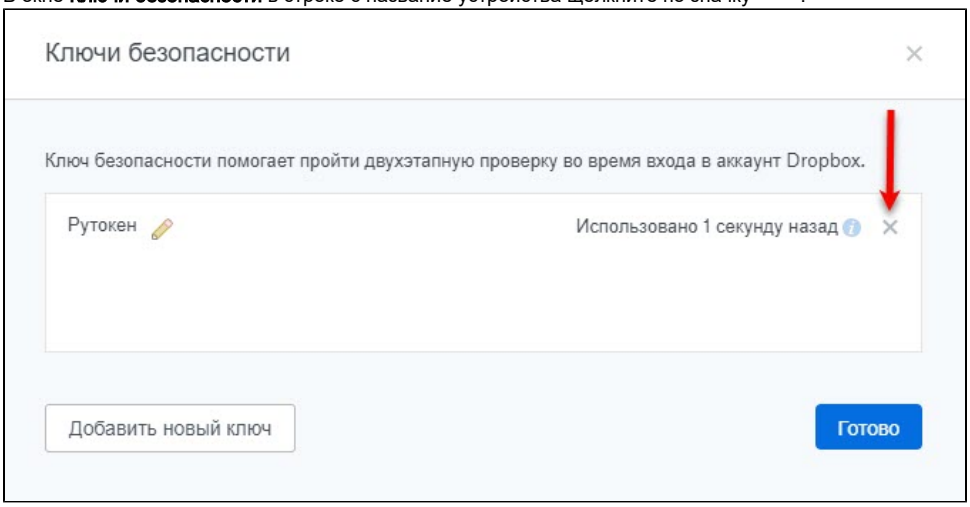
Для удаления сведений об устройстве:

1. Нажмите на фото своего профиля.
2. Выберите пункт **Настройки**.
3. Перейдите на вкладку **Безопасность**.

4. В разделе **Двухэтапная проверка**, рядом с пунктом **Ключи безопасности** нажмите **Изменить**.



5. В окне **Ключи безопасности** в строке с название устройства щелкните по значку ✕.



6. Введите пароль от своего аккаунта и нажмите **Далее**.
7. Для подтверждения удаления сведений об устройстве нажмите **Отключить**. В результате сведения об устройстве Рутокен U2F будут удалены и при следующем входе в аккаунт нужно будет ввести логин, пароль и код безопасности.

Настройка двухфакторной аутентификации с использованием устройства Рутокен U2F в Google

В Google двухфакторная аутентификация называется **двухэтапной аутентификацией**. Поэтому далее в описаниях раздела используется именно этот термин.

В этом разделе:

- Как проверить статус включения двухэтапной аутентификации?
- Как включить двухэтапную аутентификацию?
- Как добавить Рутокен U2F к аккаунту?
- Как войти в аккаунт с помощью Рутокен U2F?
- Что делать, если потерял Рутокен U2F?

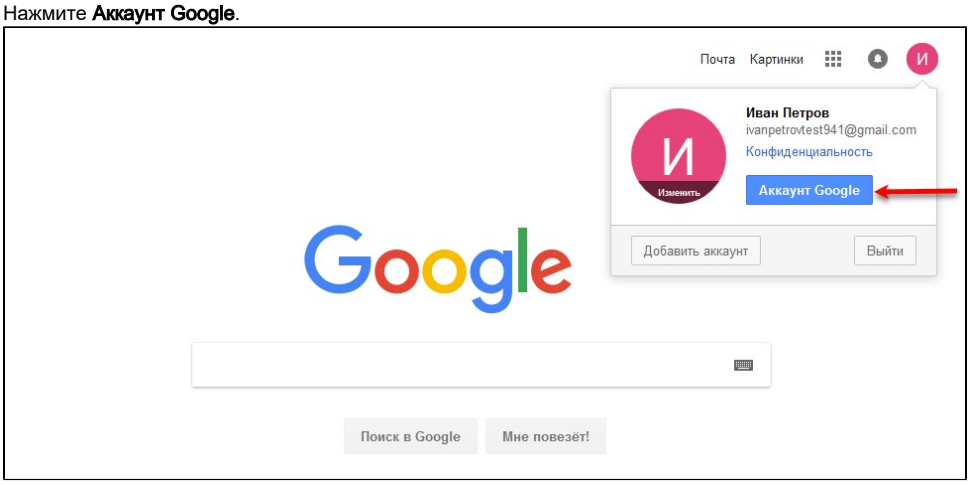
Перед тем, как настроить двухэтапную проверку необходимо проверить включена она или нет в аккаунте.

Проверка включения двухэтапной аутентификации в Google

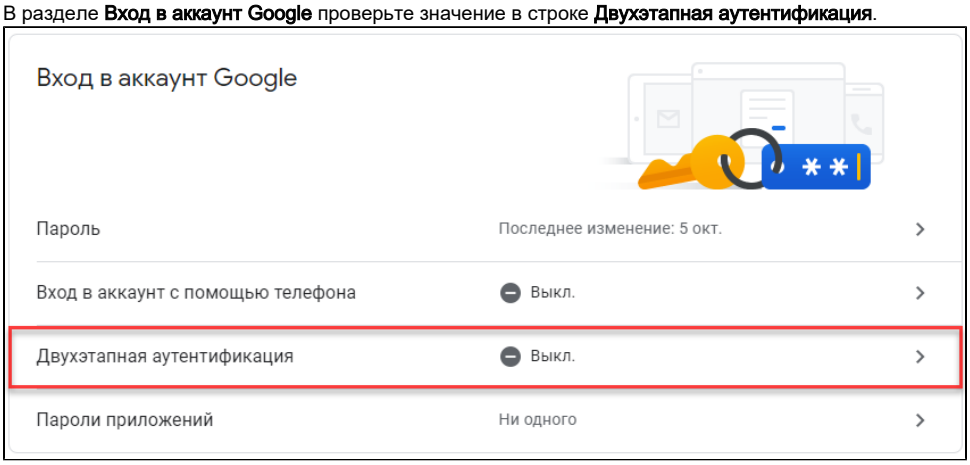
Для проверки включения двухэтапной аутентификации:

1. Зайдите в свой аккаунт.
2. Нажмите на фото своего профиля.

3. Нажмите **Аккаунт Google**.



4. Перейдите в меню **Безопасность**.
5. В разделе **Вход в аккаунт Google** проверьте значение в строке **Двухэтапная аутентификация**.



6. Если в строке **Двухэтапная аутентификация** отображается значение — **Выкл**, то ее необходимо включить. Для этого перейдите в раздел Включение двухэтапной аутентификации.
7. Если в строке **Двухэтапная аутентификация** отображается значение — **Вкл**, то необходимо сразу перейти к настройке устройства Рутокен U2F. Для этого перейдите в раздел Добавление устройства Рутокен U2F к аккаунту.

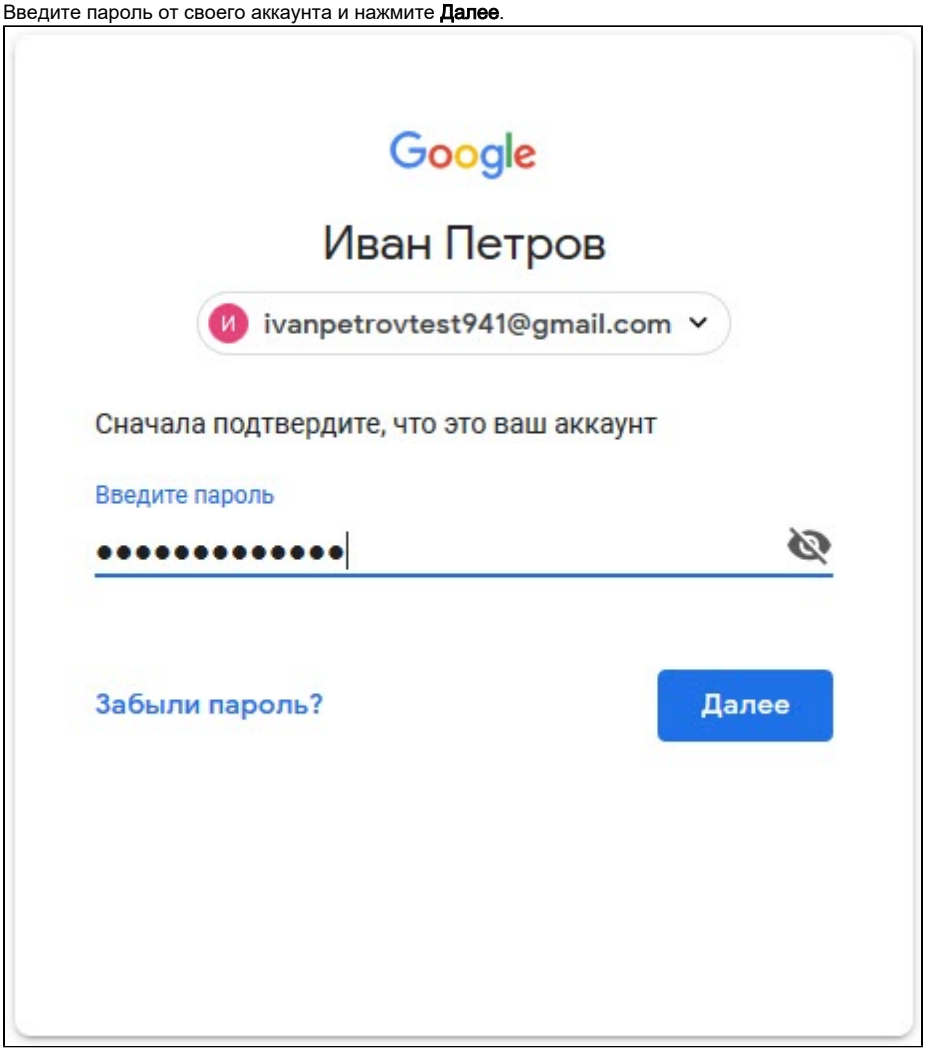
Включение двухэтапной аутентификации в Google

Для включения двухэтапной аутентификации вам понадобится мобильный телефон.

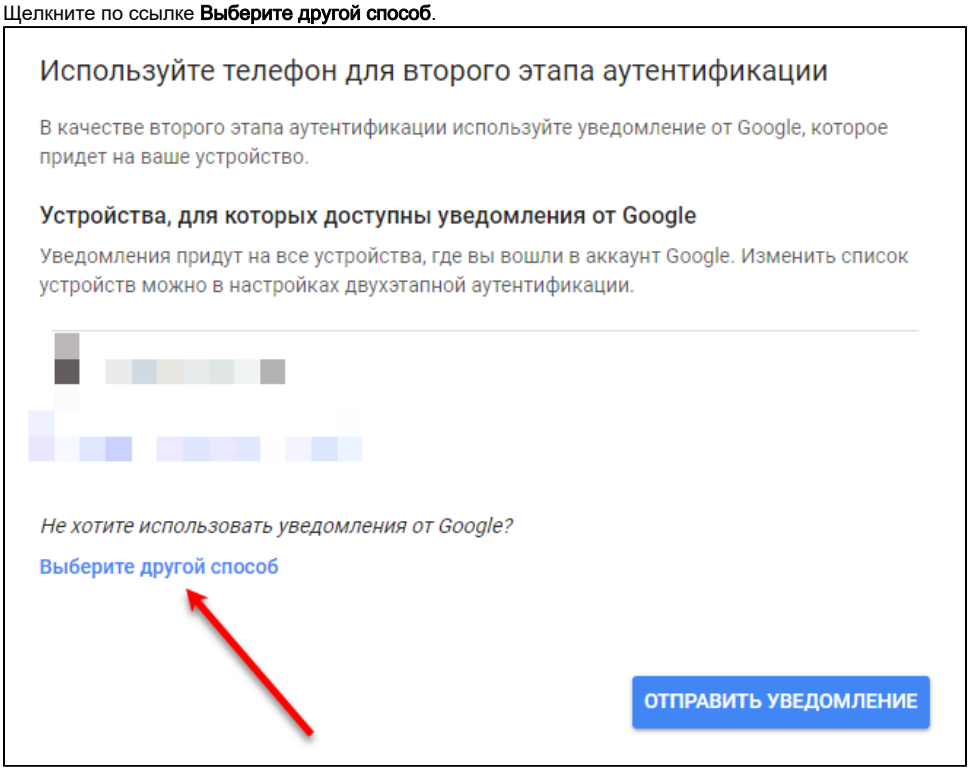
Чтобы включить двухэтапную аутентификацию:

1. Перейдите в меню **Безопасность**.
2. В разделе **Вход в аккаунт Google** щелкните по строке **Двухэтапная аутентификация**.
3. Нажмите **Начать**.

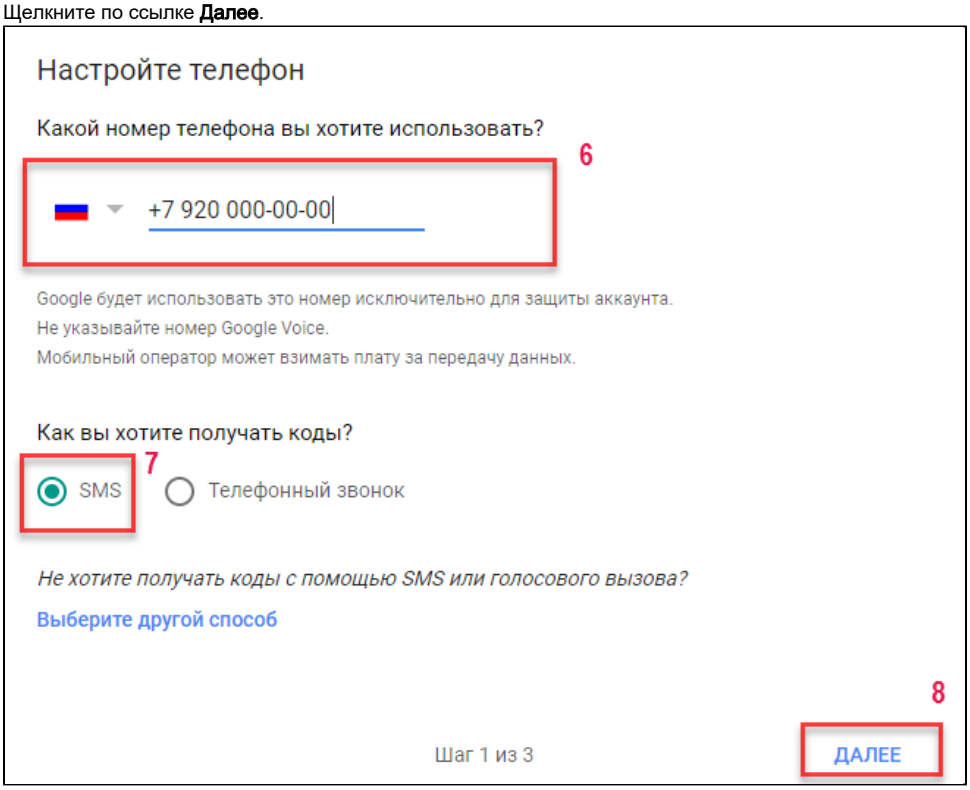
4. Введите пароль от своего аккаунта и нажмите **Далее**.



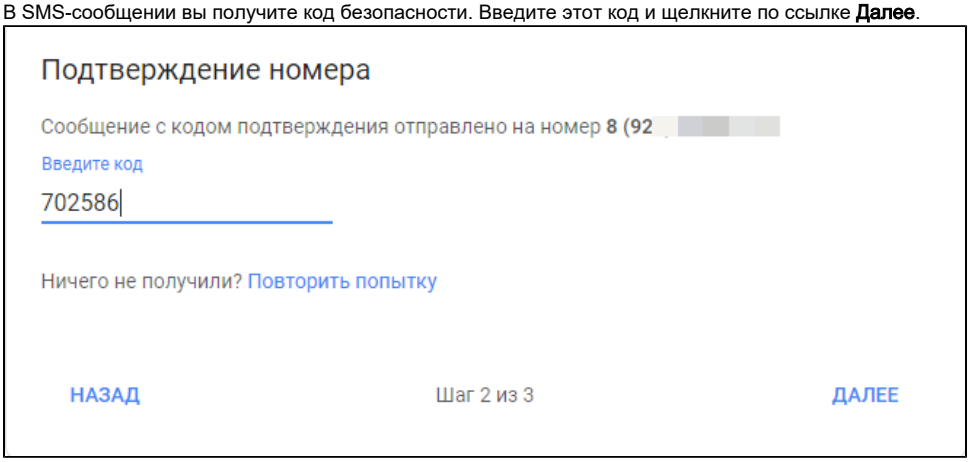
5. Щелкните по ссылке **Выберите другой способ**.



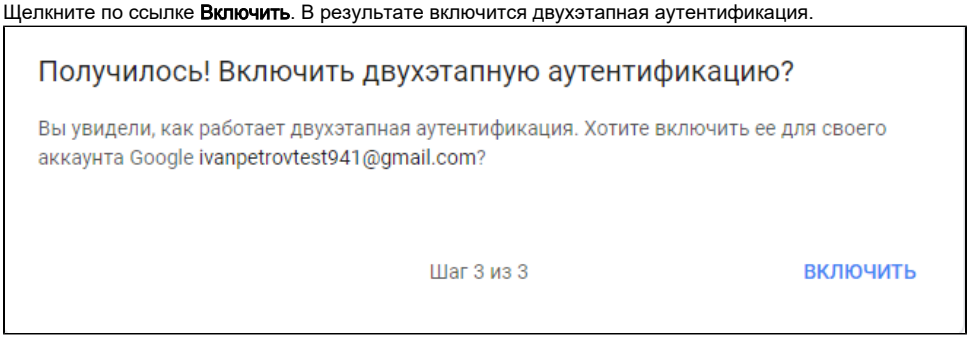
6. Выберите пункт **SMS или телефонный звонок**.
7. На странице **Настройте телефон** введите номер телефона, на который вы хотели бы получать текстовые сообщения с кодами безопасности.
8. Установите переключатель в положение **SMS**.
9. Щелкните по ссылке **Далее**.



10. В SMS-сообщении вы получите код безопасности. Введите этот код и щелкните по ссылке **Далее**.



11. Щелкните по ссылке **Включить**. В результате включится двухэтапная аутентификация.



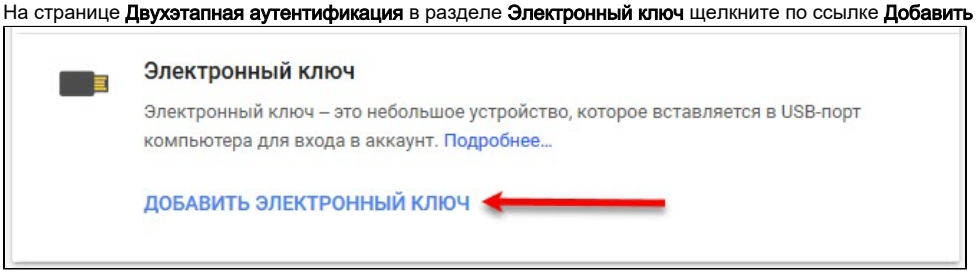
После этого необходимо добавить устройство Рутокен U2F к аккаунту (этот процесс описан в следующем разделе).

Добавление устройства Рутокен U2F к аккаунту в Google

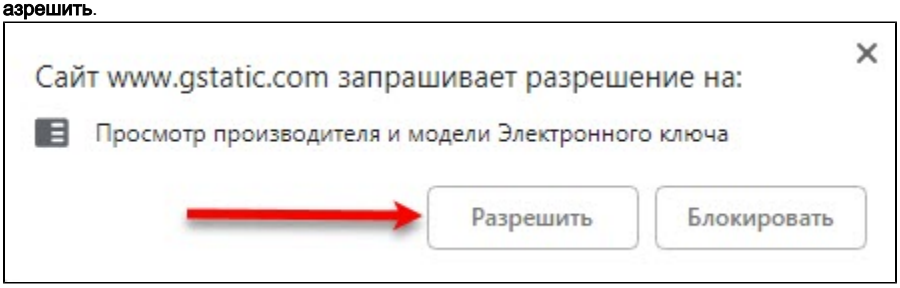
Перед тем, как добавить устройство к аккаунту необходимо проверить корректность его работы. Для этого подключите Рутокен к USB-порту компьютера. Если он подключен корректно, то на нем начнет светиться индикатор. Если этого не произошло, то попробуйте подключить Рутокен к другому USB-порту компьютера.

Чтобы добавить Рутокен U2F к аккаунту:

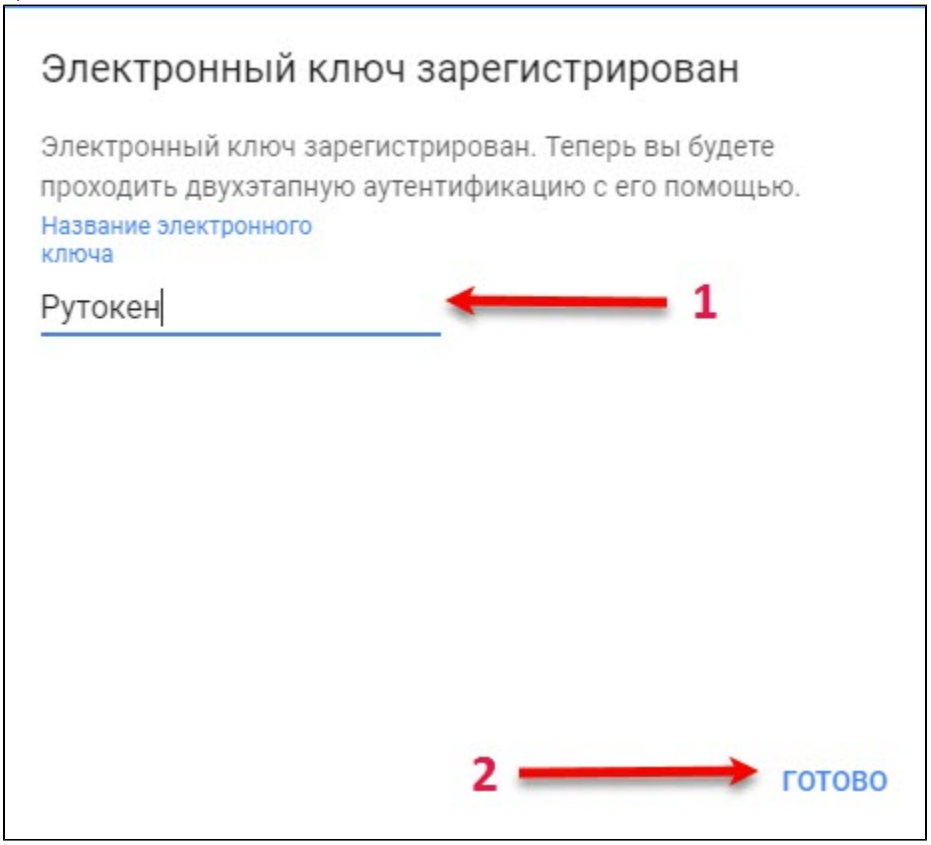
1. Подключите Рутокен U2F к компьютеру.
2. Зайдите в свой аккаунт.
3. На странице **Двухэтапная аутентификация** в разделе **Электронный ключ** щелкните по ссылке **Добавить электронный ключ**.



4. Щелкните по ссылке **Далее**.
5. На токене начнет мигать индикатор.
6. Нажмите на сенсорную кнопку на устройстве Рутокен U2F.
7. В окне с уведомлением о том, что сайт gstatic.com запрашивает разрешение на просмотр производителя и модели устройства нажмите **Разрешить**.

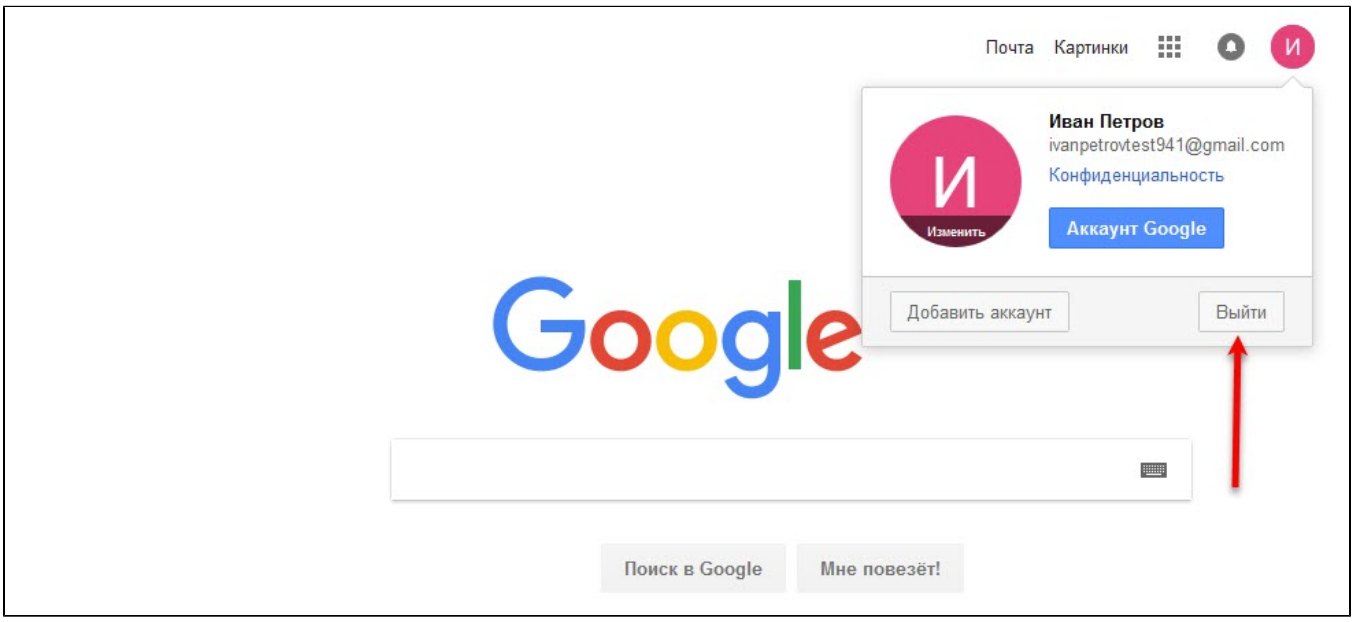


8. Отобразится окно с подтверждением того, что устройство добавлено и с полем для ввода имени устройства. Введите имя устройства и щелкните по ссылке **Готово**.



В результате для аутентификации на сайте www.google.com будет использоваться Рутокен U2F. Давайте это проверим. Для этого выйдите из своего аккаунта и снова зайдите в него.

Чтобы выйти из аккаунта, нажмите на фотографию своего профиля и выберите пункт **Выйти**.



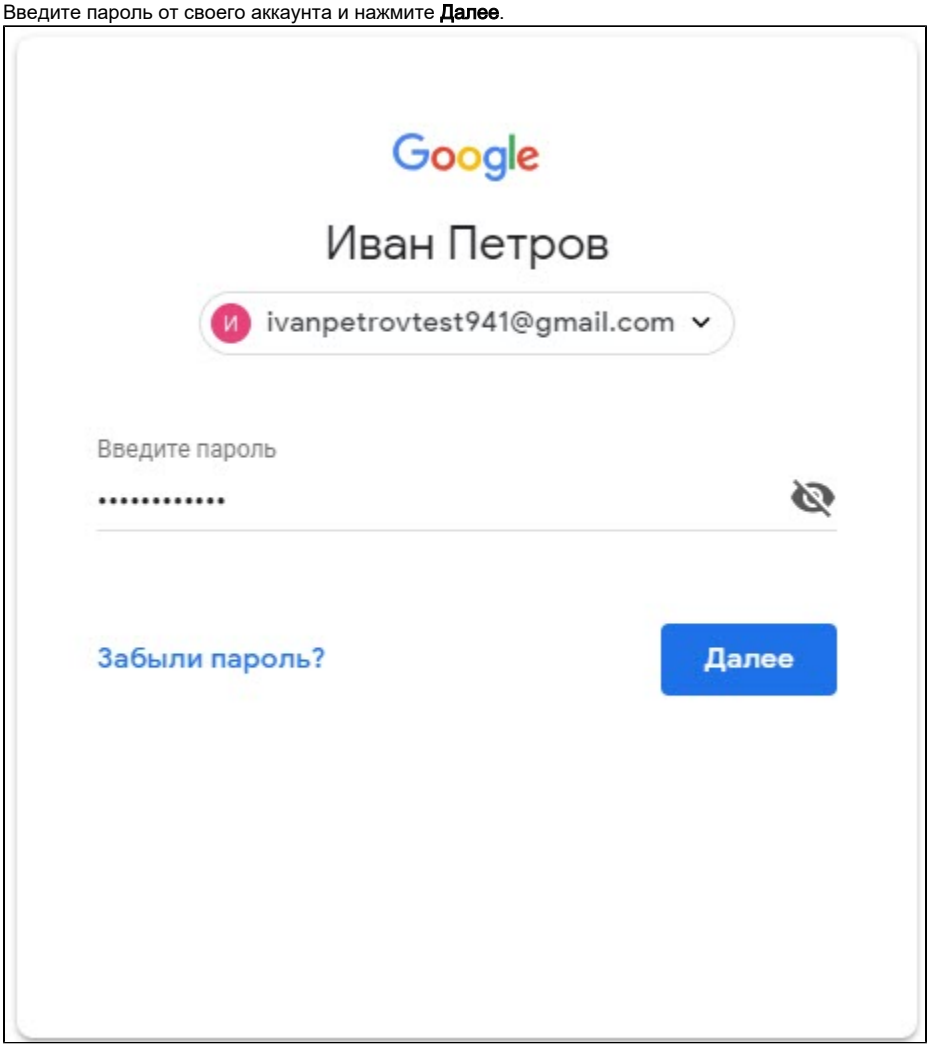
Теперь зайдите в свой аккаунт с помощью устройства Рутокен U2F (этот процесс описан в следующем разделе).

Вход в аккаунт с помощью устройства Рутокен U2F в Google

Чтобы войти в аккаунт:

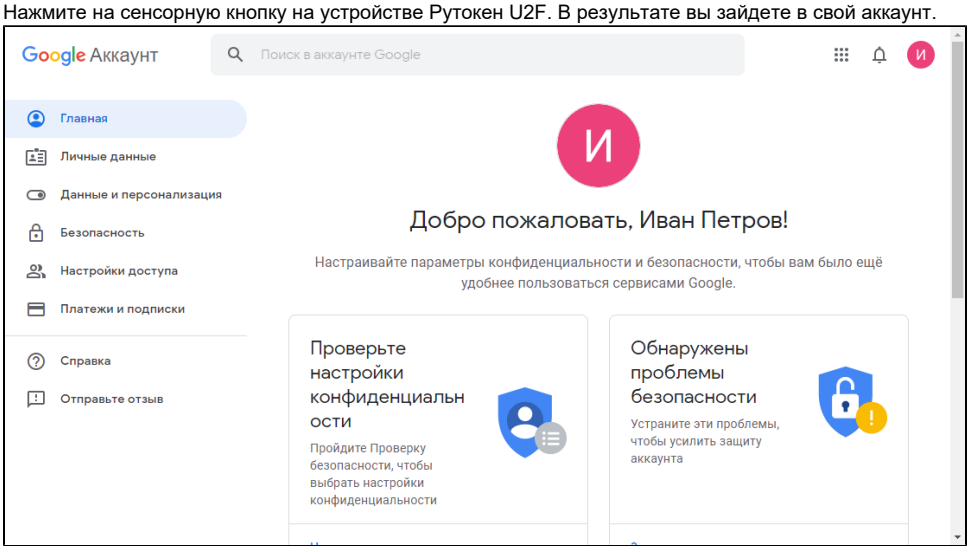
1. Подключите Рутокен U2F к компьютеру.
2. На странице для входа в аккаунт введите логин и нажмите **Далее**.

3. Введите пароль от своего аккаунта и нажмите **Далее**.



Если после нажатия на кнопку **Далее,** вы сразу зашли в свой аккаунт, то двухфакторная аутентификация с использование Рутокен U2F не сработала, а значит вам надо очистить кэш, временные данные и перезагрузить компьютер. Этот процесс описан в приложении.

4. На токене начнет мигать индикатор.
5. Нажмите на сенсорную кнопку на устройстве Рутокен U2F. В результате вы зайдете в свой аккаунт.



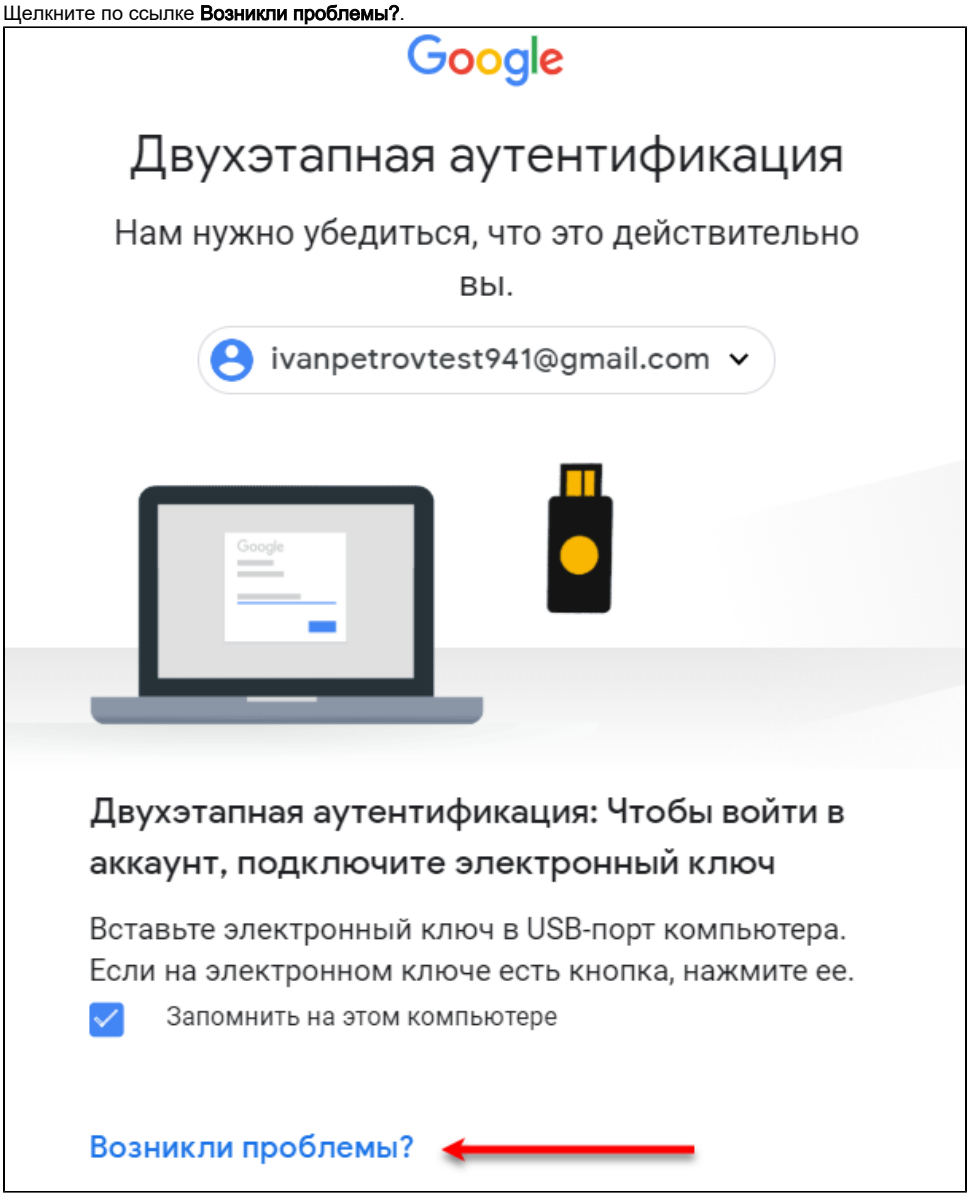
Удаление сведений о Рутокен U2F в Google

Если вы потеряли Рутокен U2F, который был привязан к аккаунту, или он перестал работать, то необходимо в Google удалить сведения о нем.

Для удаления сведений об устройстве вам понадобится мобильный телефон, номер которого был указан при включении двухфактовной аутентификации.

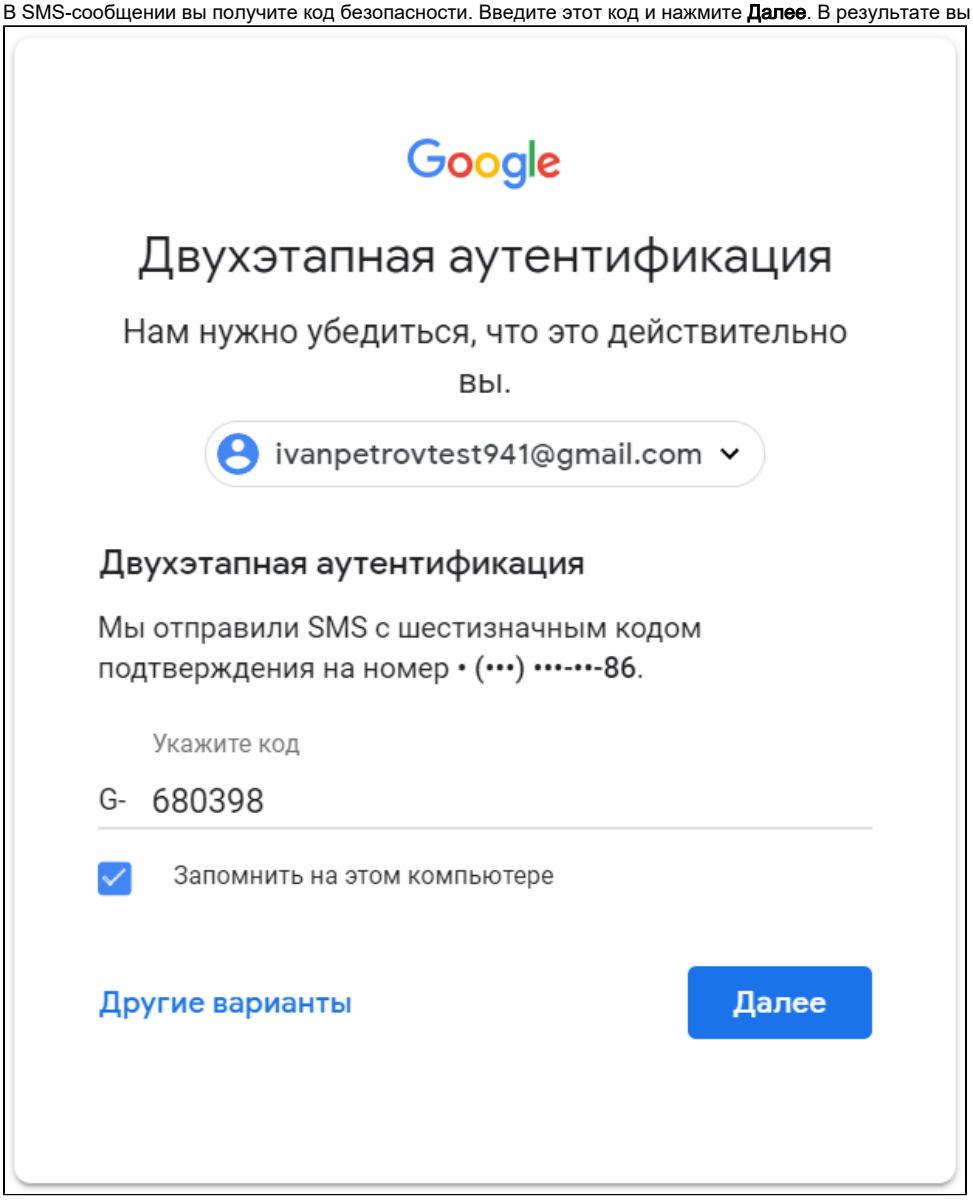
Для удаления сведений об устройстве:

1. Введите пароль от своего аккаунта и нажмите **Далее**.
2. Щелкните по ссылке **Возникли проблемы?**.

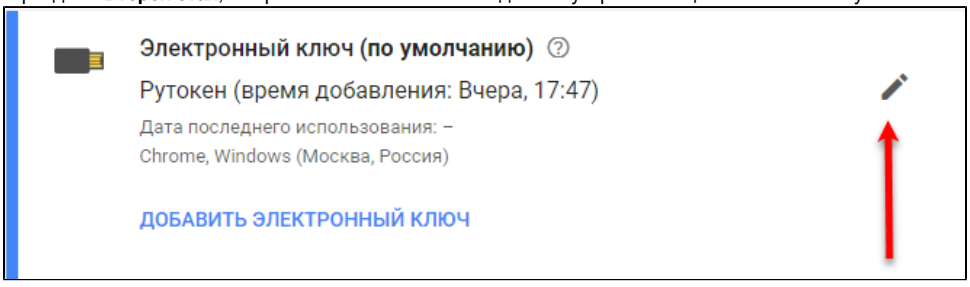


3. В окне для выбора другого способа входа в аккаунт щелкните по строке **Получите код подтверждения на номер**.

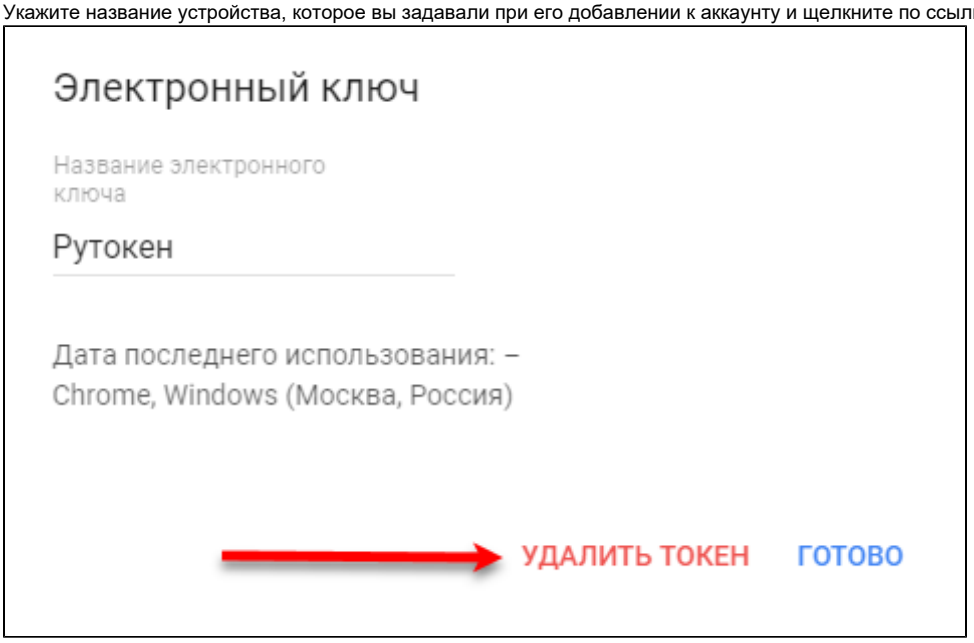
4. В SMS-сообщении вы получите код безопасности. Введите этот код и нажмите **Далее**. В результате вы зайдете в свой аккаунт.



5. Перейдите в меню **Безопасность**.
6. В разделе **Вход в аккаунт Google** щелкните по строке **Двухэтапная аутентификация**.
7. Введите пароль от своего аккаунта и нажмите **Далее**.
8. В разделе **Второй этап**, в строке с названием необходимого устройства щелкните по значку .



9. Укажите название устройства, которое вы задавали при его добавлении к аккаунту и щелкните по ссылке **Удалить токен**.



10. Для подтверждения удаления сведений об устройстве из аккаунта щелкните по ссылке **ОК**. В результате сведения об устройстве Рутокен U2F будут удалены и при следующем входе в аккаунт нужно будет ввести логин, пароль и код безопасности.

Настройка двухфакторной аутентификации в социальной сети Facebook

В этом разделе:

- Как проверить статус включения двухэтапной проверки?
- Как включить двухэтапную проверку?
- Как добавить Рутокен U2F к аккаунту?
- Как войти в аккаунт с помощью Рутокен U2F?
- Что делать, если потерял устройство Рутокен U2F?

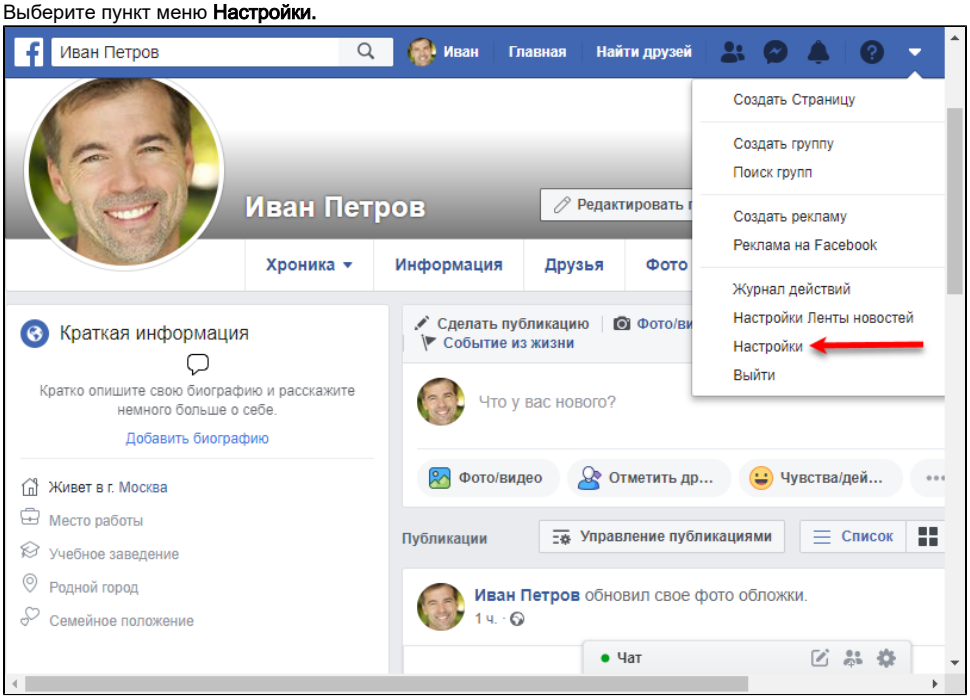
Перед тем, как настроить двухфакторную аутентификацию необходимо проверить включена она или нет в аккаунте.

Проверка включения двухфакторной аутентификации в Facebook

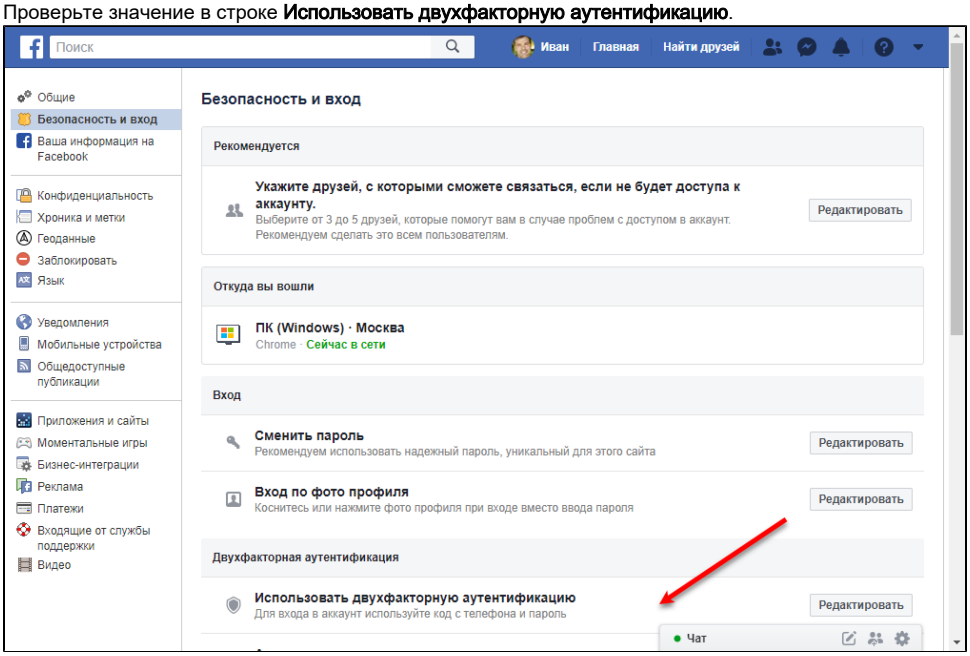
Для проверки включения двухфакторной аутентификации:

1. Зайдите в свой аккаунт.
2. Щелкните по значку .

3. Выберите пункт меню **Настройки.**



4. Перейдите в раздел **Безопасность и вход**.
5. Проверьте значение в строке **Использовать двухфакторную аутентификацию**.



6. Если в этой строке **нет значения Вкл**, то двухфакторную аутентификацию необходимо включить (для этого перейдите в раздел Включение двухфакторной аутентификации).
7. Если в этой строке отображается значение **Вкл**, то необходимо сразу перейти к настройке устройства Рутокен U2F (для этого перейдите в раздел Добавление устройства Рутокен U2F к аккаунту).

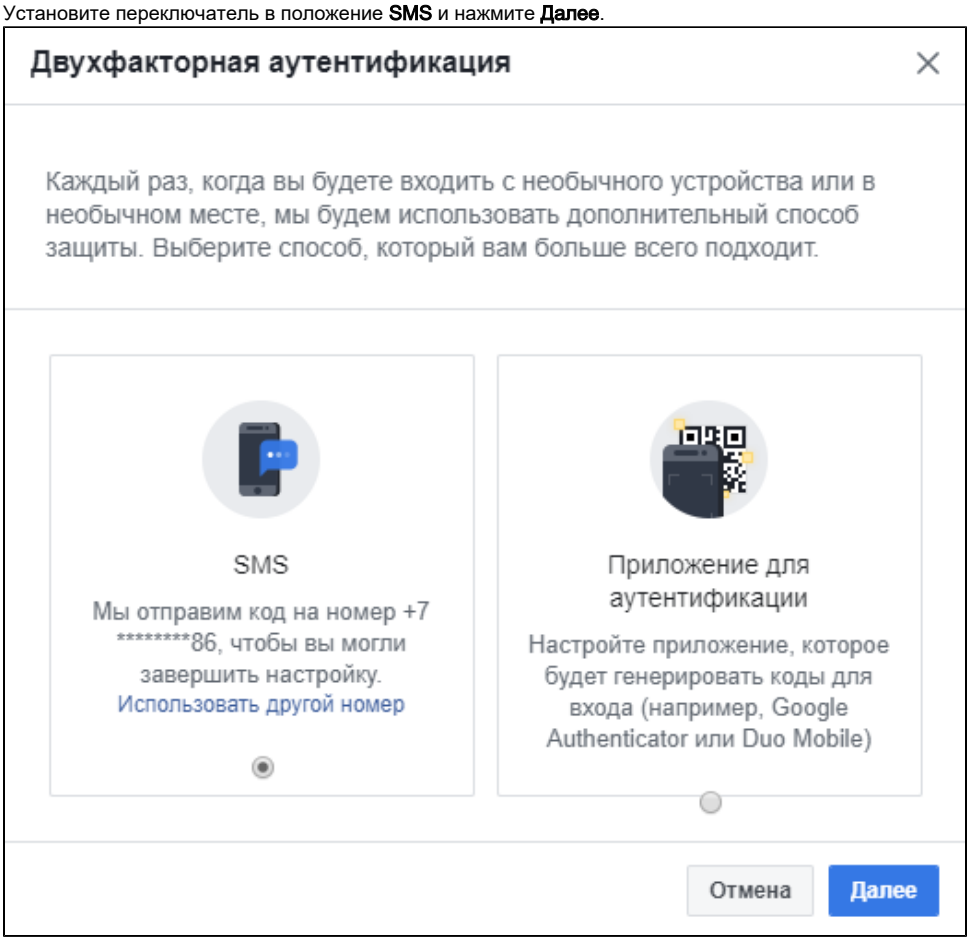
Включение двухфакторной аутентификации в Facebook

Для включения двухфакторной аутентификации вам понадобится мобильный телефон.

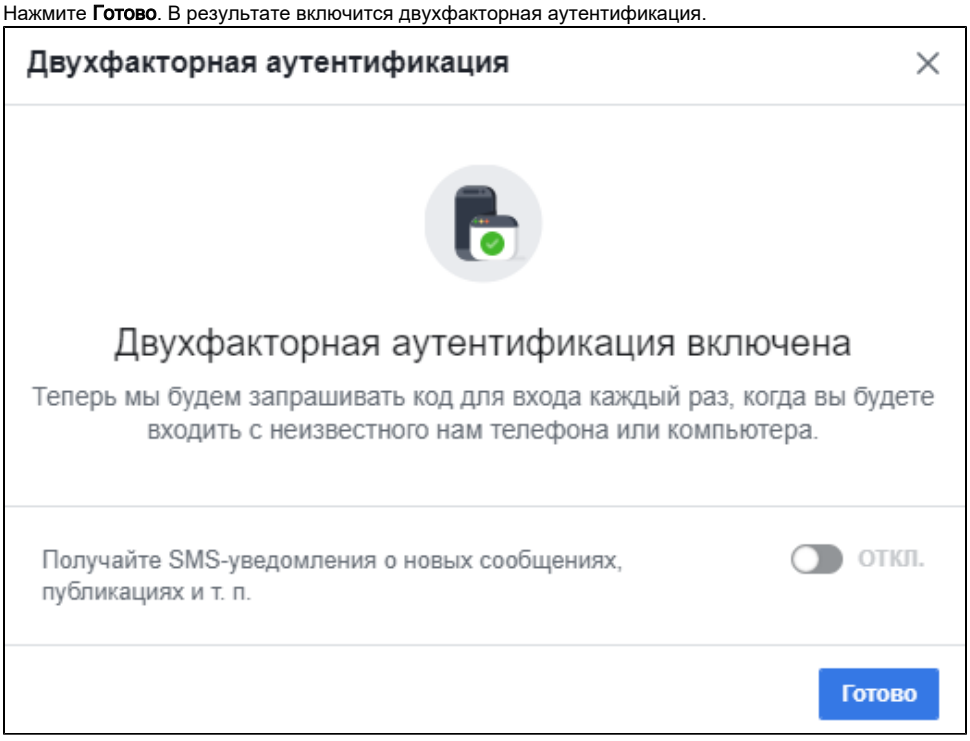
Чтобы включить двухфакторную аутентификацию:

1. На странице **Безопасность и вход**, в разделе **Двухфакторная аутентификация**, в строке **Использовать двухфакторную аутентификацию** нажмите **Редактировать**.
2. Нажмите **Начать**.

3. Установите переключатель в положение **SMS** и нажмите **Далее**.



4. В SMS-сообщении вы получите код безопасности. Введите этот код.
5. Нажмите **Готово**. В результате включится двухфакторная аутентификация.



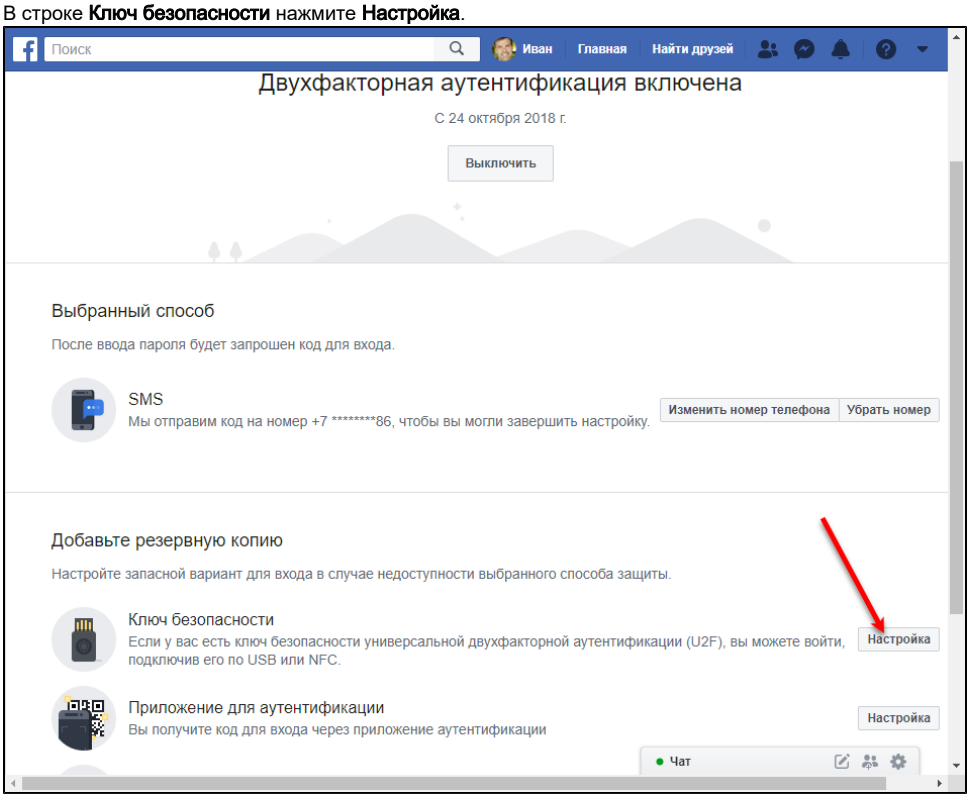
После этого необходимо добавить устройство Рутокен U2F к аккаунту (этот процесс описан в следующем разделе).

Добавление устройства Рутокен U2F к аккаунту в Facebook

Перед тем, как добавить устройство к аккаунту необходимо проверить корректность его работы. Для этого подключите Рутокен к USB-порту компьютера. Если он подключен корректно, то на нем начнет светиться индикатор. Если этого не произошло, то попробуйте подключить Рутокен к другому USB-порту компьютера.

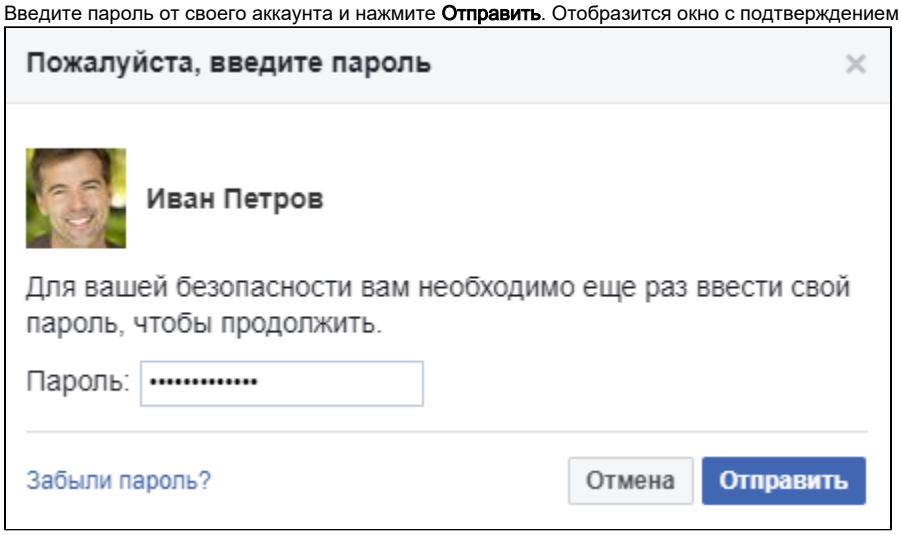
Чтобы добавить устройство к аккаунту:

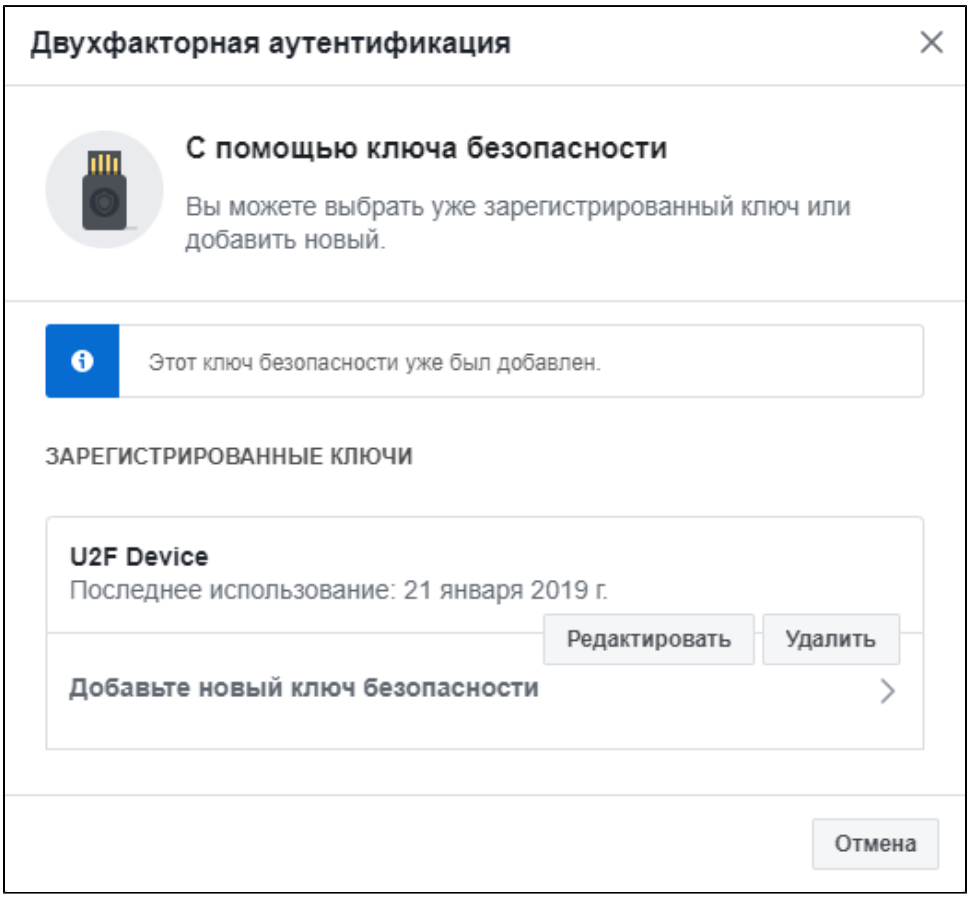
1. Подключите Рутокен U2F к компьютеру.
2. Зайдите в свой аккаунт.
3. Перейдите в раздел **Безопасность и вход**.
4. В строке **Использовать двухфакторную аутентификацию** нажмите **Редактировать**.
5. В строке **Ключ безопасности** нажмите **Настройка**.



6. На токене начнет мигать индикатор.
7. Нажмите на сенсорную кнопку на устройстве Рутокен U2F.

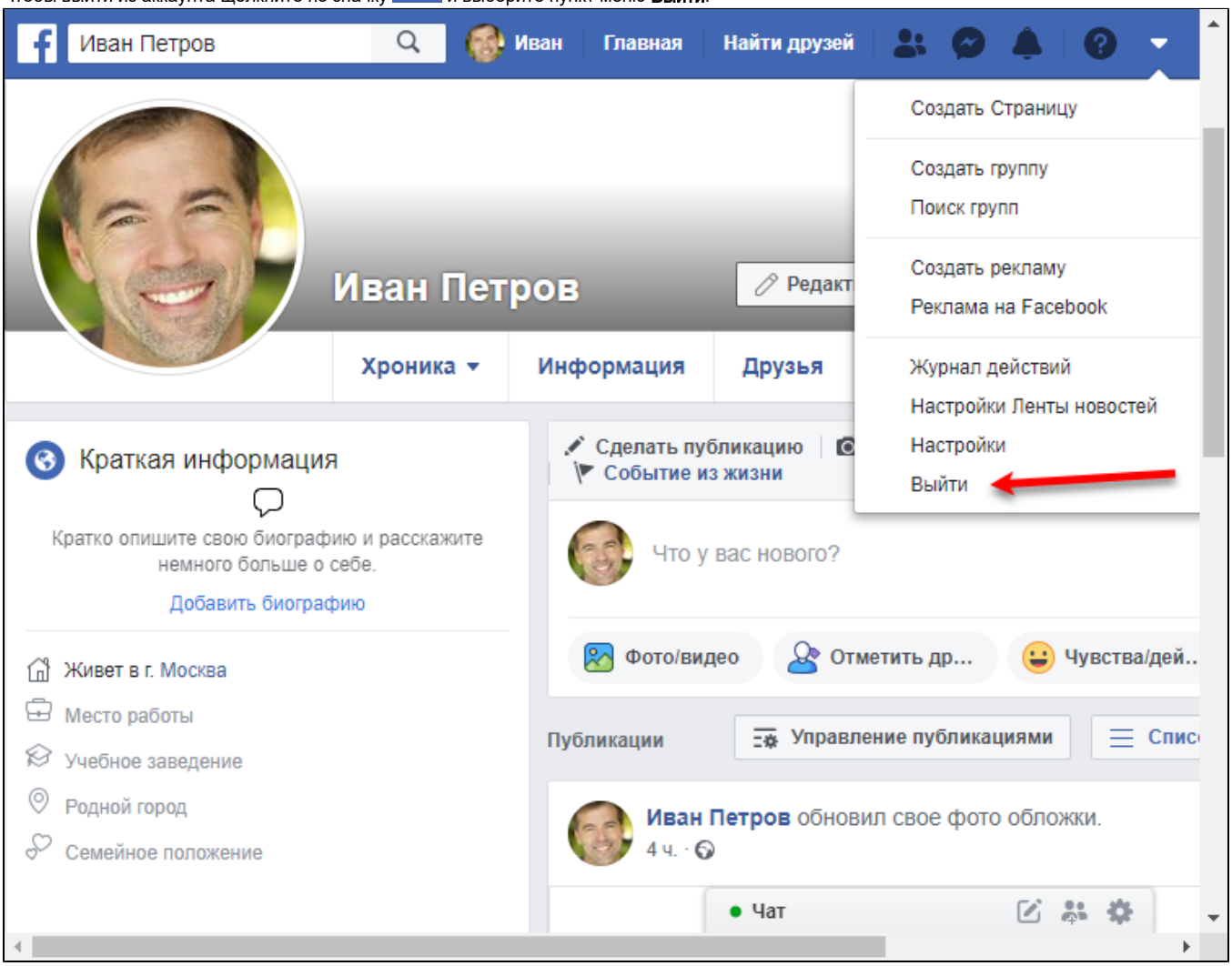
8. Введите пароль от своего аккаунта и нажмите **Отправить**. Отобразится окно с подтверждением того, что устройство добавлено.





9. Закройте окно **Двухфакторная аутентификация**. В результате для аутентификации в социальной сети Facebook будет использоваться Рутокен U2F. Давайте это проверим. Для этого выйдите из своего аккаунта и снова зайдите в него.

Чтобы выйти из аккаунта щелкните по значку  и выберите пункт меню **Выйти**.



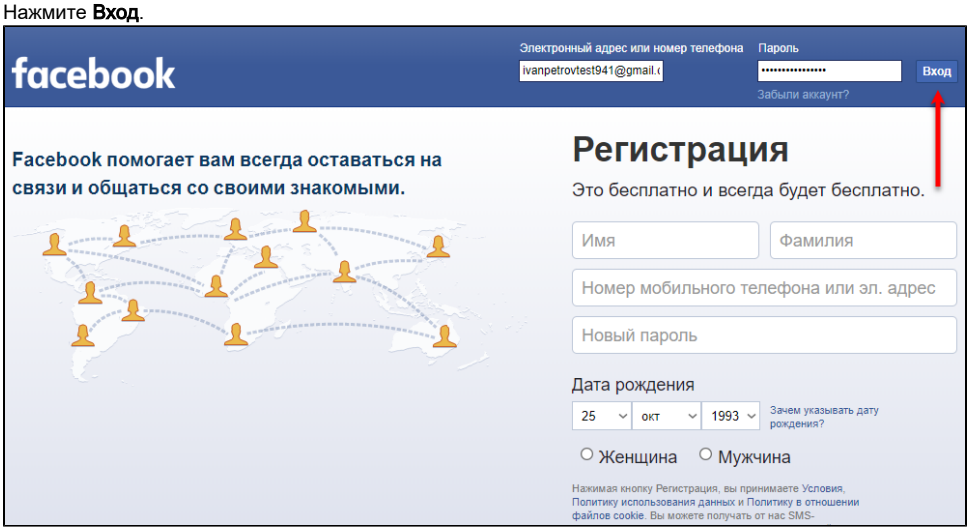
Теперь зайдите в свой аккаунт с помощью Рутокен U2F (этот процесс описан в следующем разделе).

Вход в аккаунт с помощью устройства Рутокен U2F в Facebook

Чтобы войти в аккаунт:

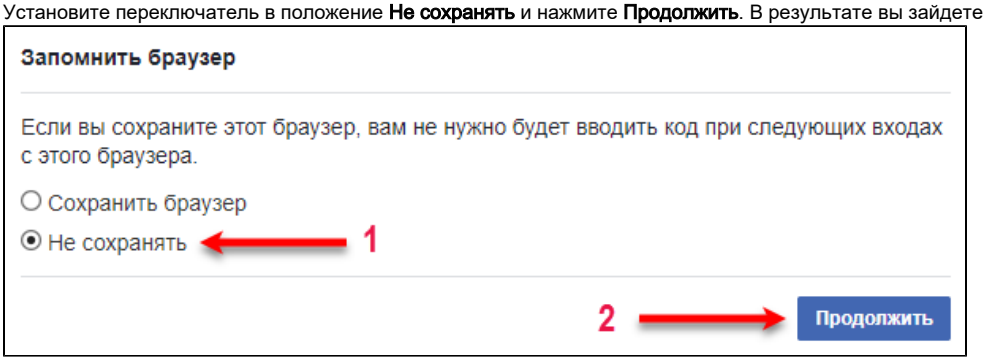
1. Подключите Рутокен U2F к компьютеру.
2. Введите логин и пароль от своего аккаунта.

3. Нажмите **Вход**.



Если после нажатия на кнопку **Далее** вы сразу зашли в свой аккаунт, то двухфакторная аутентификация с использование Рутокен U2F не сработала, а значит вам надо будет очистить кэш и временные данные, а после этого перезагрузить компьютер. Этот процесс описан в приложении.

4. На токене начнет мигать индикатор.
5. Нажмите на сенсорную кнопку на устройстве Рутокен U2F.
6. Установите переключатель в положение **Не сохранять** и нажмите **Продолжить**. В результате вы зайдете в свой аккаунт.



Удаление сведений о Рутокен U2F в Facebook

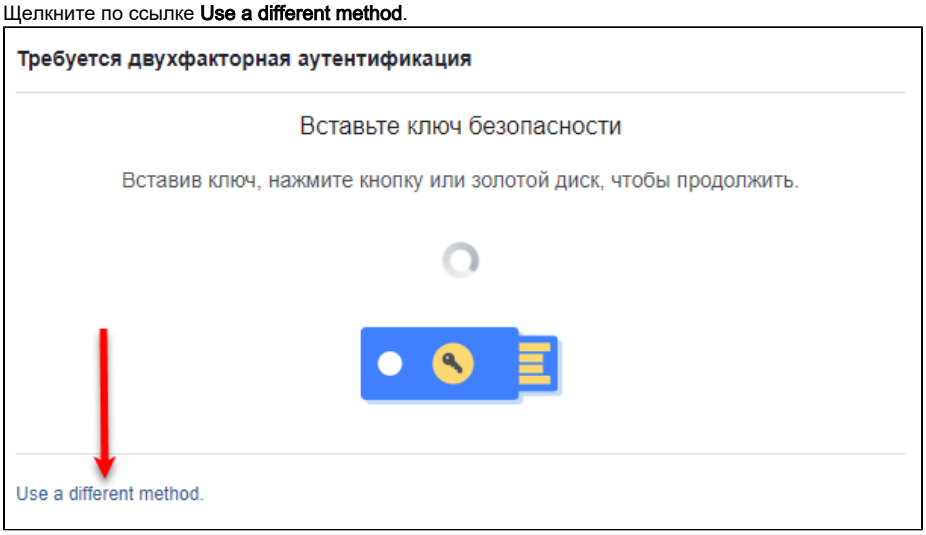
Если вы потеряли Рутокен U2F, который был привязан к аккаунту или он перестал работать, то необходимо в социальной сети Facebook удалить сведения о нем.

Для удаления сведений об устройстве вам понадобится мобильный телефон, номер которого был указан при включении двухфакторной аутентификации.

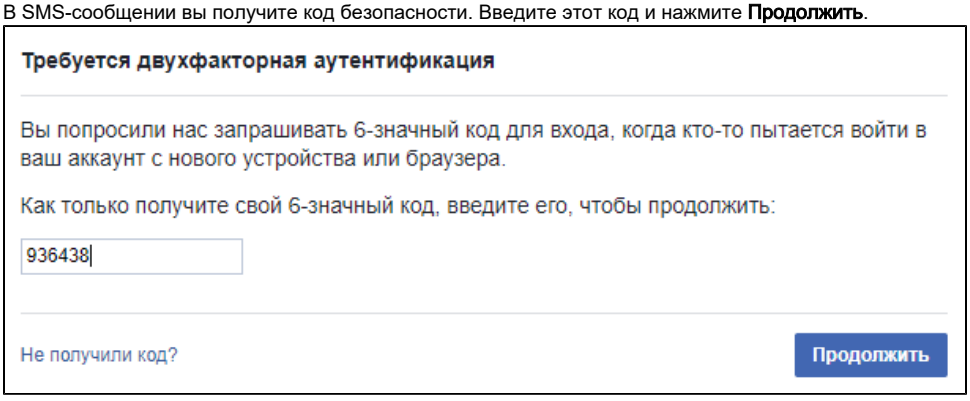
Для удаления сведений об устройстве:

1. Введите логин и пароль от своего аккаунта.
2. Нажмите **Вход.**

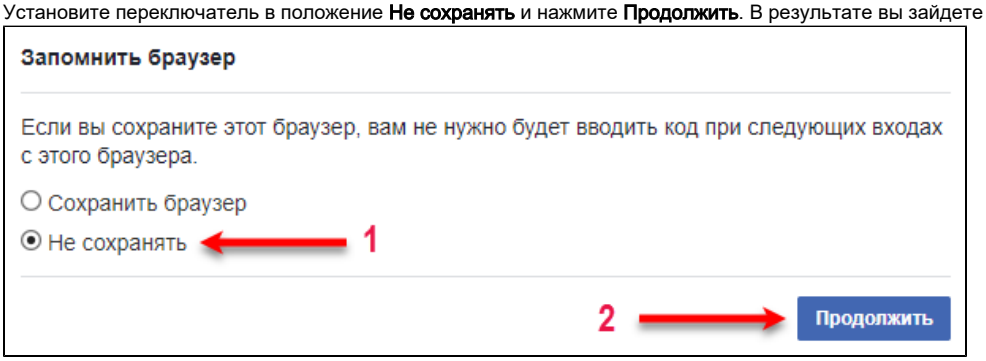
3. Щелкните по ссылке **Use a different method**.



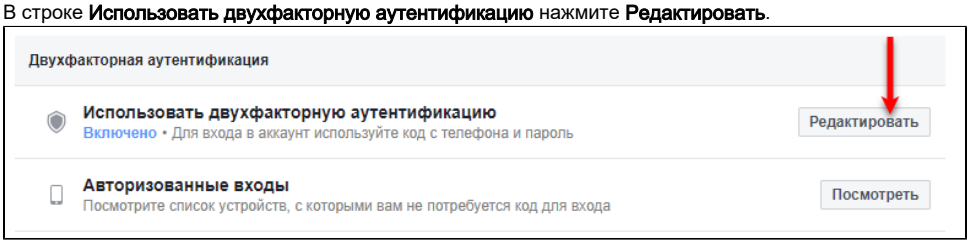
4. В SMS-сообщении вы получите код безопасности. Введите этот код и нажмите **Продолжить**.



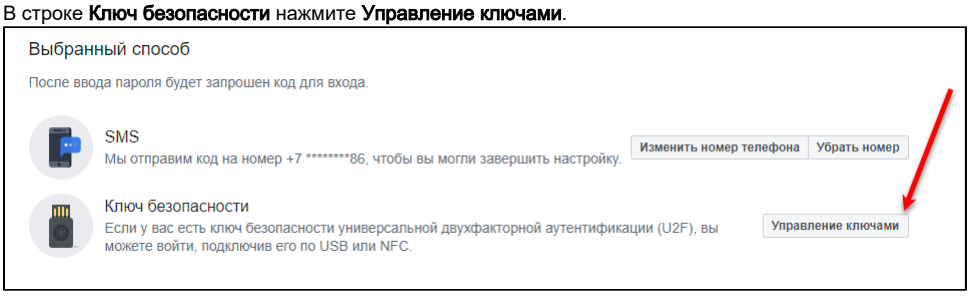
5. Установите переключатель в положение **Не сохранять** и нажмите **Продолжить**. В результате вы зайдете в свой аккаунт.



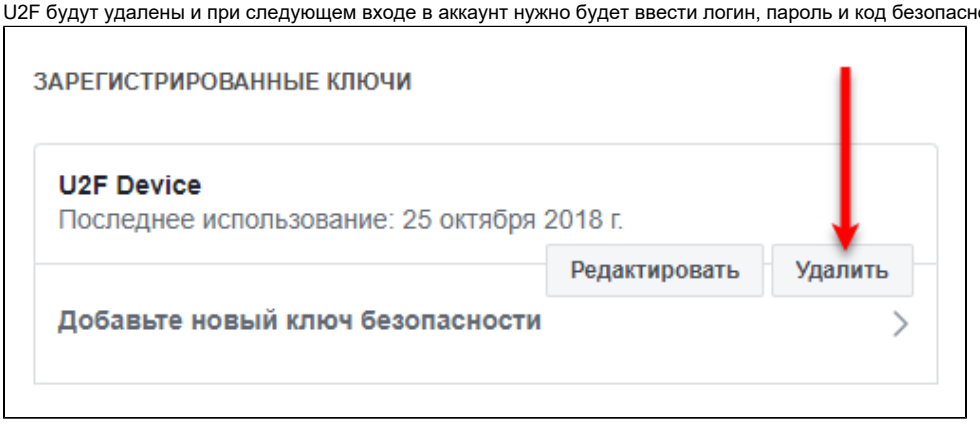
6. Щелкните по значку .
7. Выберите пункт меню **Настройки**.
8. Перейдите в раздел **Безопасность и вход**.
9. В строке **Использовать двухфакторную аутентификацию** нажмите **Редактировать**.



10. В строке **Ключ безопасности** нажмите **Управление ключами**.



11. В окне **Двухфакторная аутентификация** рядом с названием устройства нажмите **Удалить**. В результате сведения об устройстве Рутокен U2F будут удалены и при следующем входе в аккаунт нужно будет ввести логин, пароль и код безопасности.



Настройка двухфакторной аутентификации с использованием устройства Рутокен U2F в социальной сети Twitter

В этом разделе:

- Как проверить статус включения двухфакторной аутентификации?
- Как включить двухфакторную аутентификацию?
- Как добавить Рутокен U2F к аккаунту?
- Как войти в аккаунт с помощью Рутокен U2F?
- Что делать, если потерял устройство Рутокен U2F?

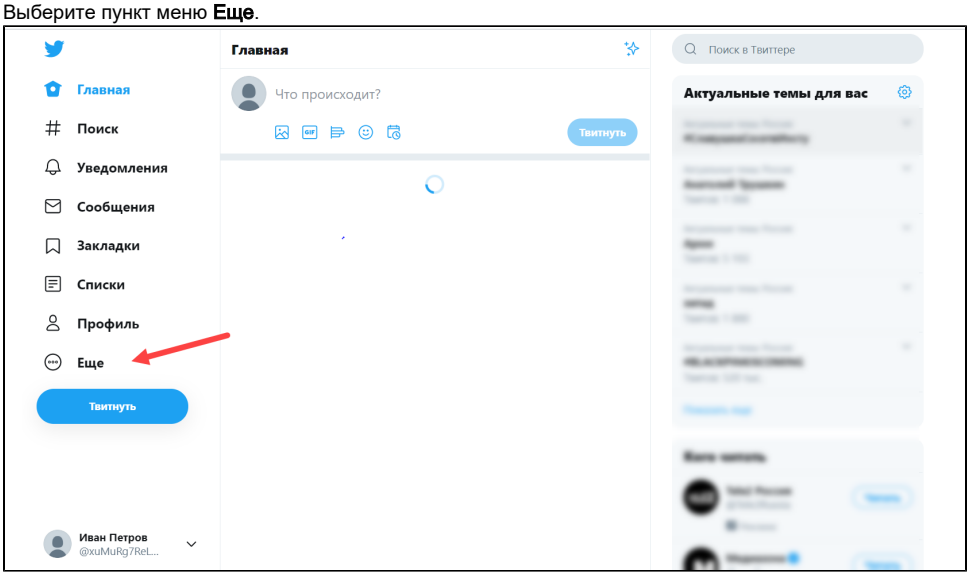
Перед тем, как настроить двухфакторную аутентификацию необходимо проверить включена она или нет в аккаунте.

Проверка включения двухфакторной аутентификации в Twitter

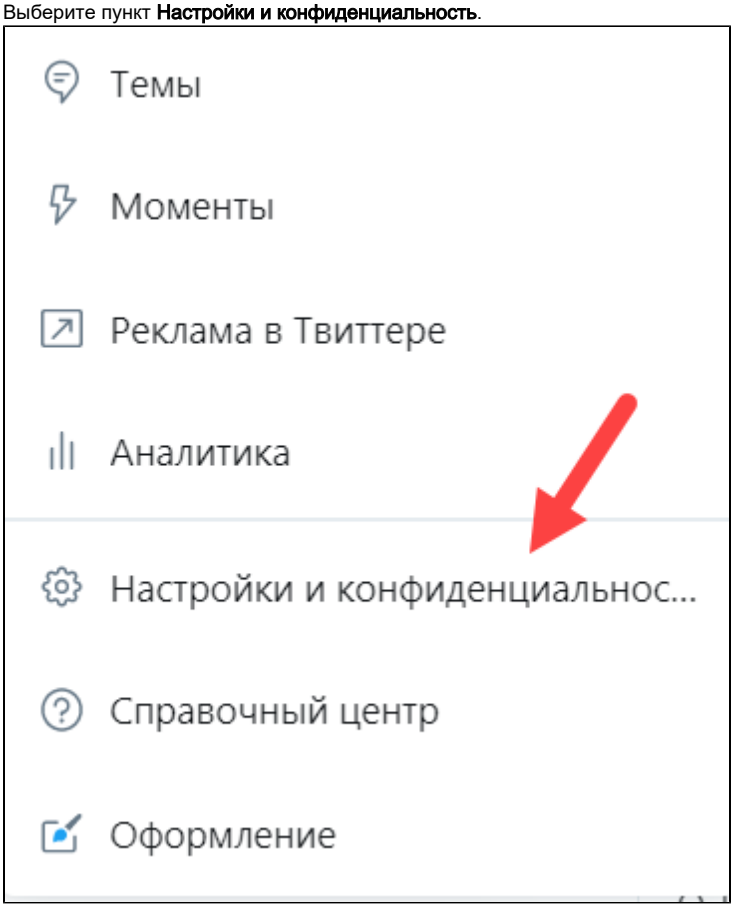
Для проверки включения двухфакторной аутентификации:

1. Зайдите в свой аккаунт.

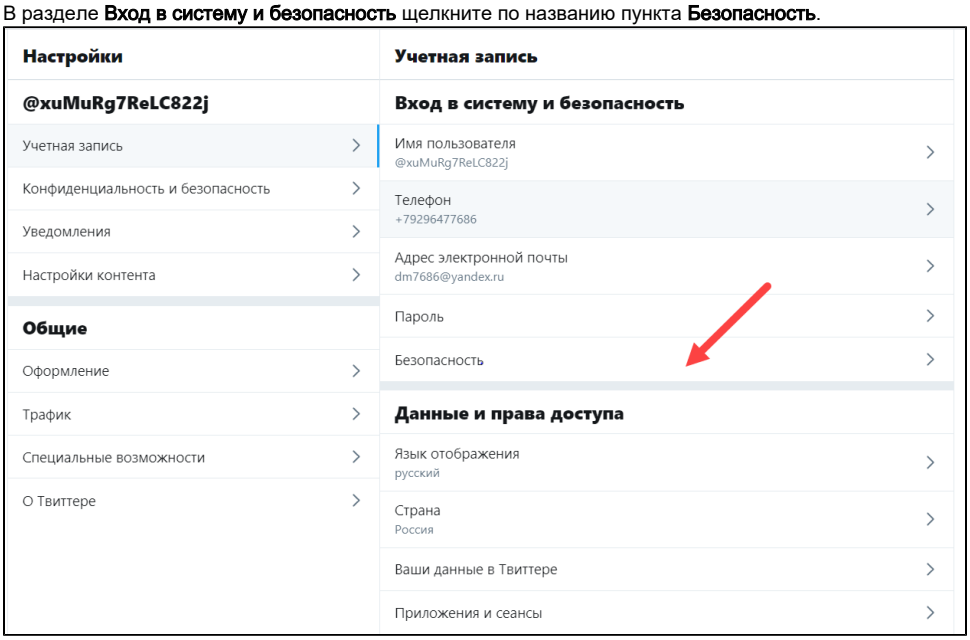
2. Выберите пункт меню **Еще**.



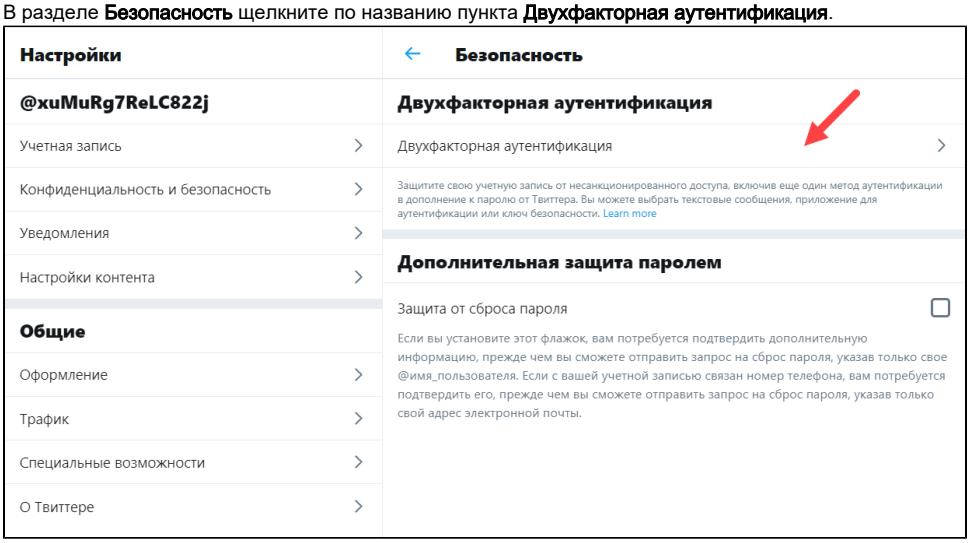
3. Выберите пункт **Настройки и конфиденциальность**.



4. В разделе **Вход в систему и безопасность** щелкните по названию пункта **Безопасность**.



5. В разделе **Безопасность** щелкните по названию пункта **Двухфакторная аутентификация**.

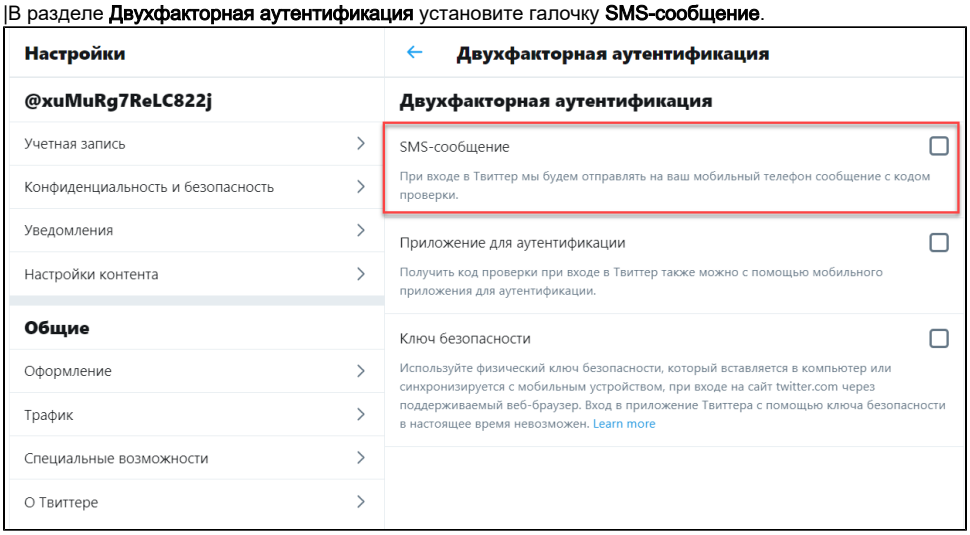


6. Если в разделе **Двухфакторная аутентификация** не установлено ни одной галочки, то двухфакторную аутентификацию необходимо включить (для этого перейдите в раздел Включение двухфакторной аутентификации).
7. Если в разделе **Двухфакторная аутентификация** рядом с одним из пунктов **SMS-сообщение** или **Приложение для аутентификации** установлена галочка, то двухфакторная аутентификация включена и необходимо сразу перейти к настройке устройства Рутокен U2F (для этого перейдите в раздел Добавление устройства Рутокен U2F к аккаунту).

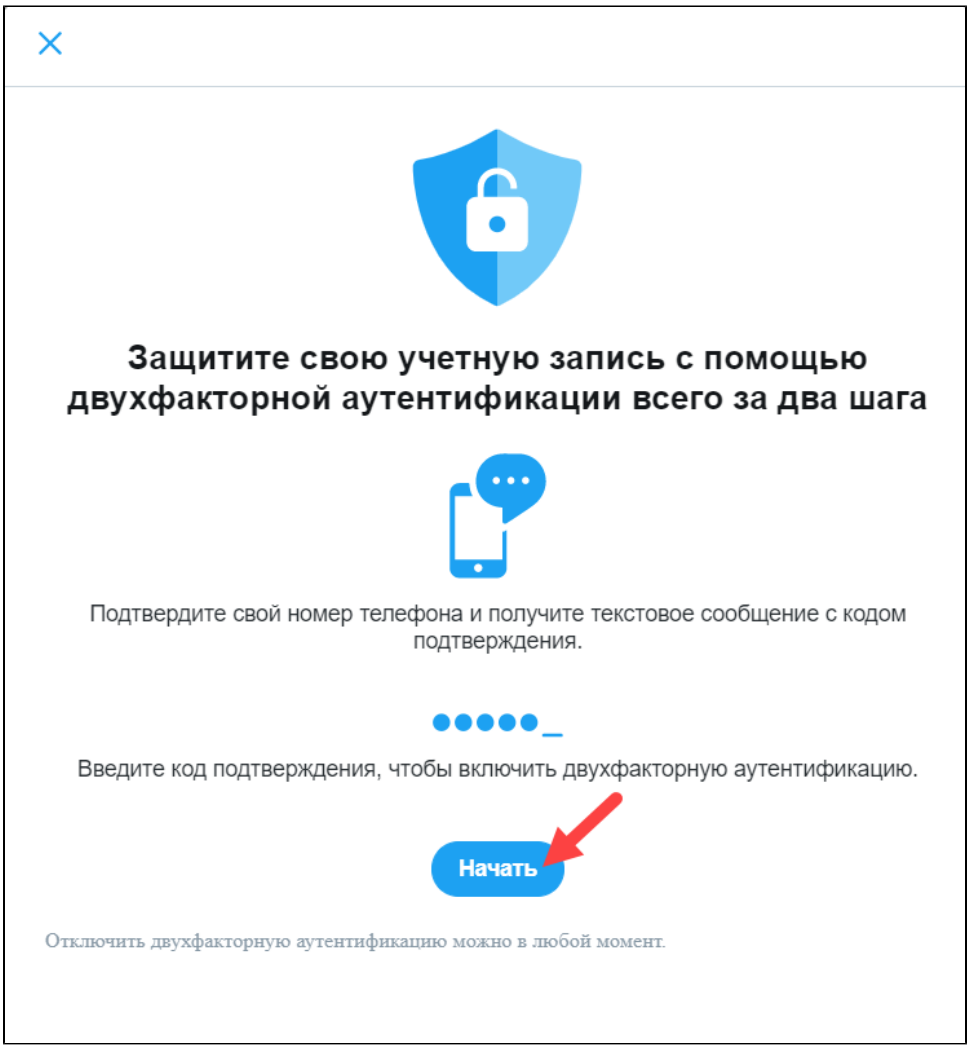
Включение двухфакторной аутентификации в Twitter

Чтобы включить двухфакторную аутентификацию:

1. В разделе **Двухфакторная аутентификация** установите галочку **SMS-сообщение**.

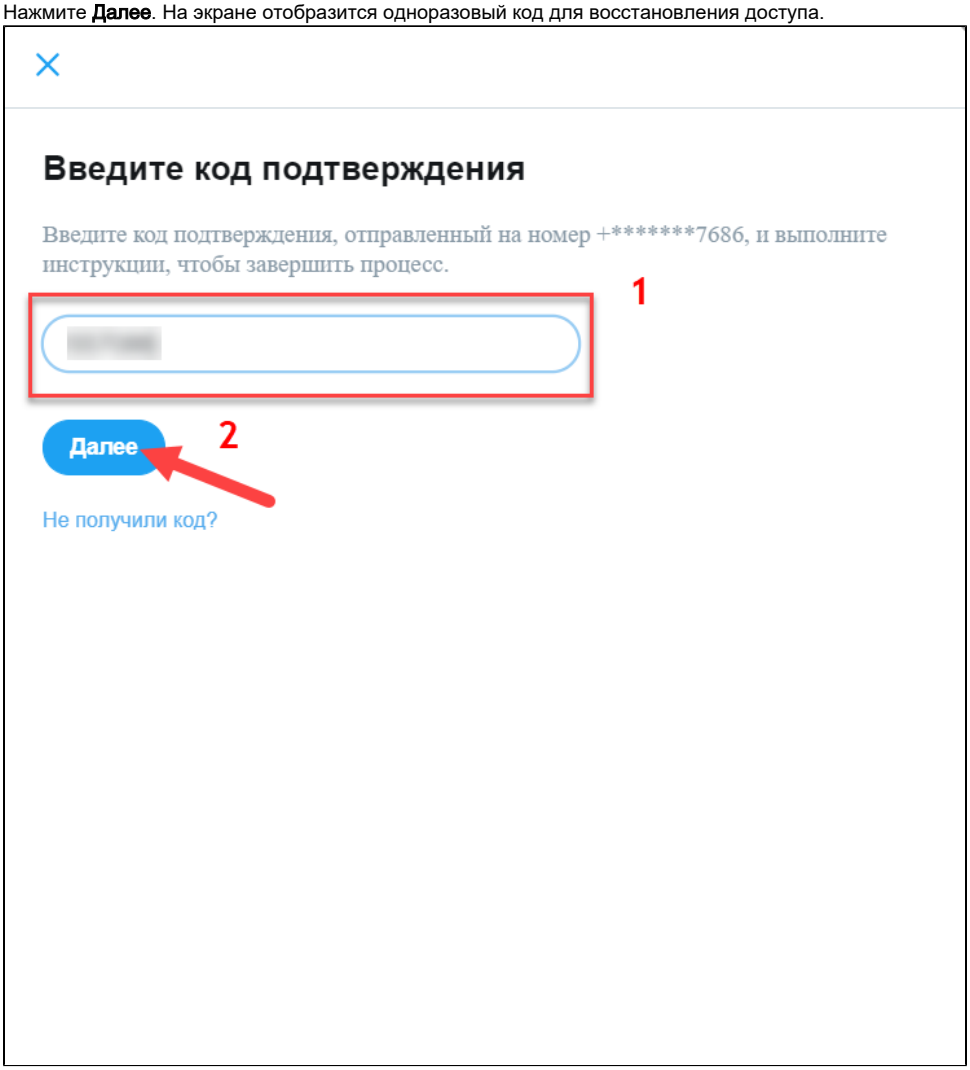


2. Нажмите **Начать**.



3. Введите пароль от своего аккаунта и нажмите **Подтвердить**.
4. Нажмите **Отправить код**.
5. В SMS-сообщении вы получите код безопасности. Введите этот код.

6. Нажмите **Далее**. На экране отобразится одноразовый код для восстановления доступа.



7. Сохраните его на компьютере и нажмите **Понятно**. В результате включится двухфакторная аутентификация.

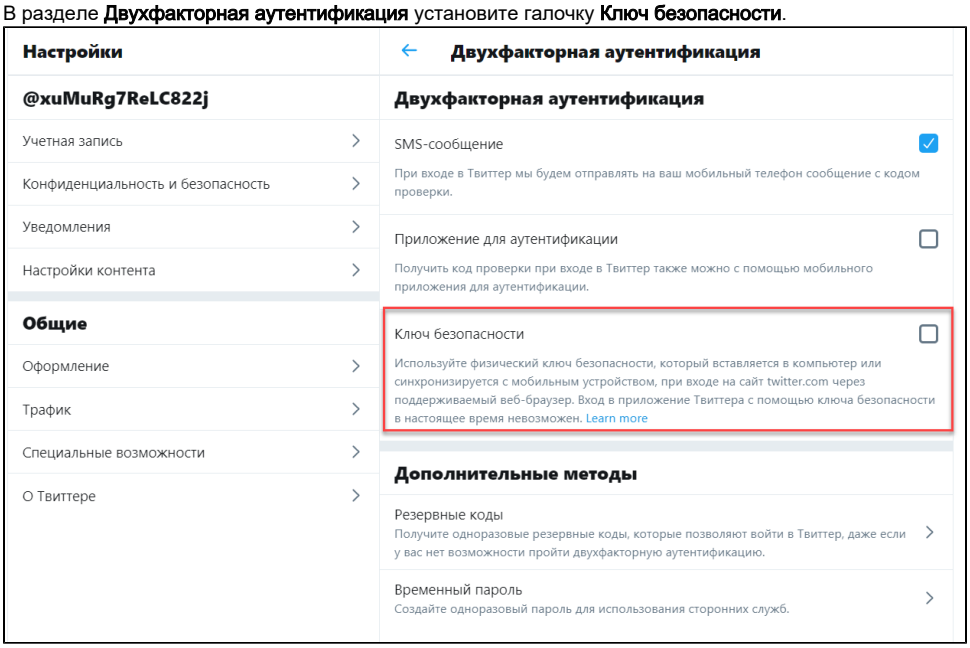
После этого необходимо добавить Рутокен U2F к аккаунту (этот процесс описан в следующем разделе).

Добавление устройства Рутокен U2F к аккаунту в Twitter

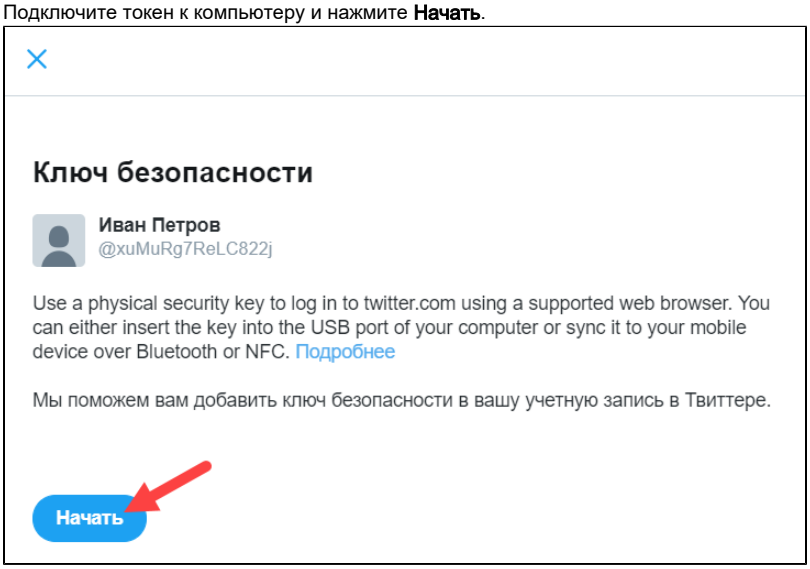
Перед тем, как добавить устройство к аккаунту необходимо проверить корректность его работы. Для этого подключите Рутокен к USB-порту компьютера. Если он подключен корректно, то на нем начнет светиться индикатор. Если этого не произошло, то попробуйте подключить Рутокен к другому USB-порту компьютера.

Чтобы добавить Рутокен U2F к аккаунту:

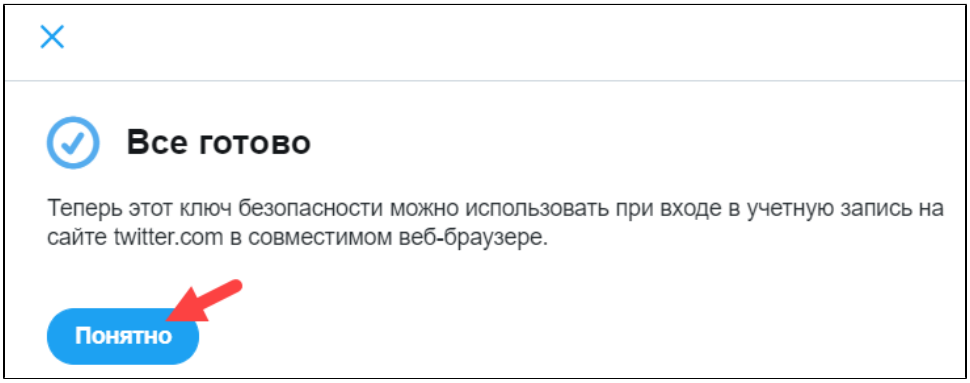
1. В разделе **Двухфакторная аутентификация** установите галочку **Ключ безопасности**.



2. Введите пароль от своего аккаунта и нажмите **Подтвердить**.
3. Подключите токен к компьютеру и нажмите **Начать**.



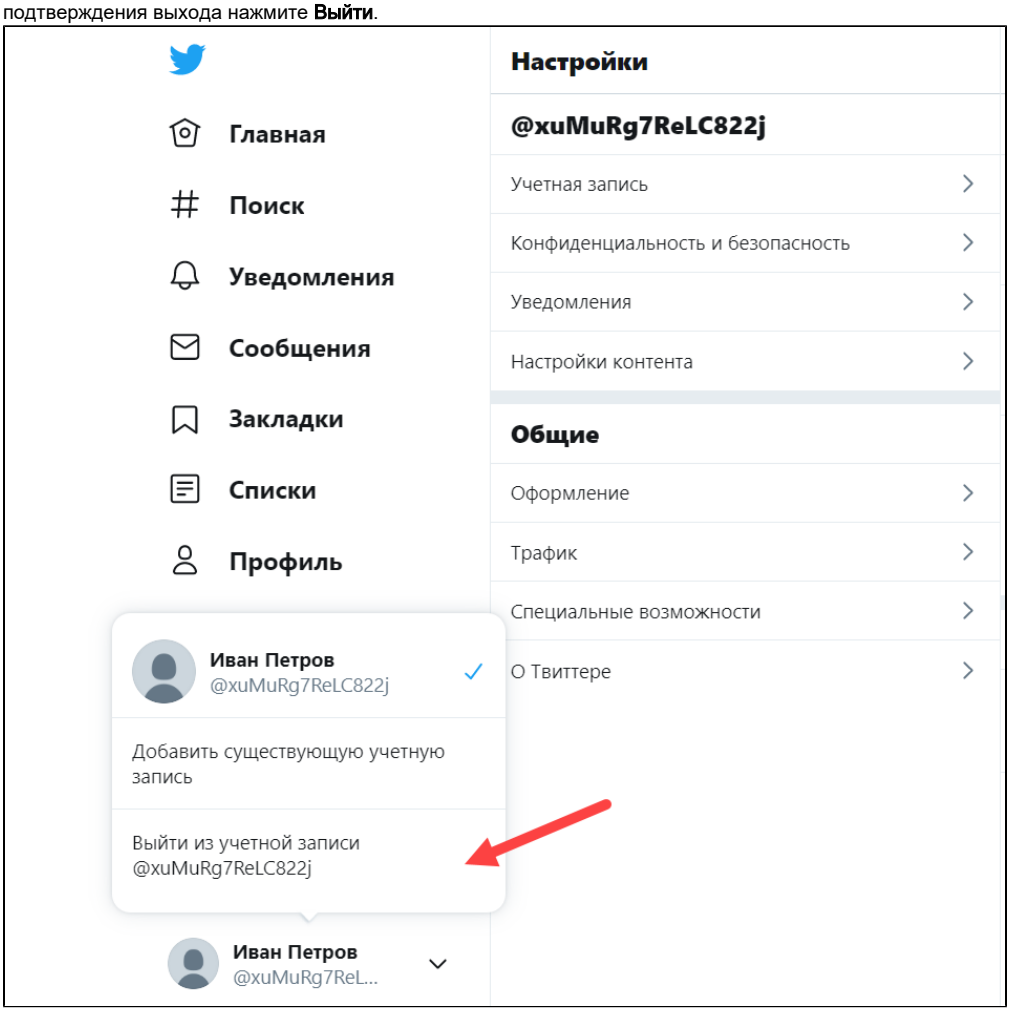
4. Нажмите **ОК**.
5. На токене начнет мигать индикатор.
6. Нажмите на сенсорную кнопку на устройстве Рутокен U2F. На токене начнет мигать индикатор.
7. Нажмите еще раз на сенсорную кнопку.
8. Нажмите **Понятно**.



В результате для аутентификации в социальной сети Twitter будет использоваться Рутокен U2F.

Давайте это проверим. Для этого выйдите из своего аккаунта и снова зайдите в него.

Чтобы выйти из аккаунта в левом нижнем углу щелкните по значку и выберите пункт **Выйти из учетной записи**. После этого для подтверждения выхода нажмите **Выйти**.



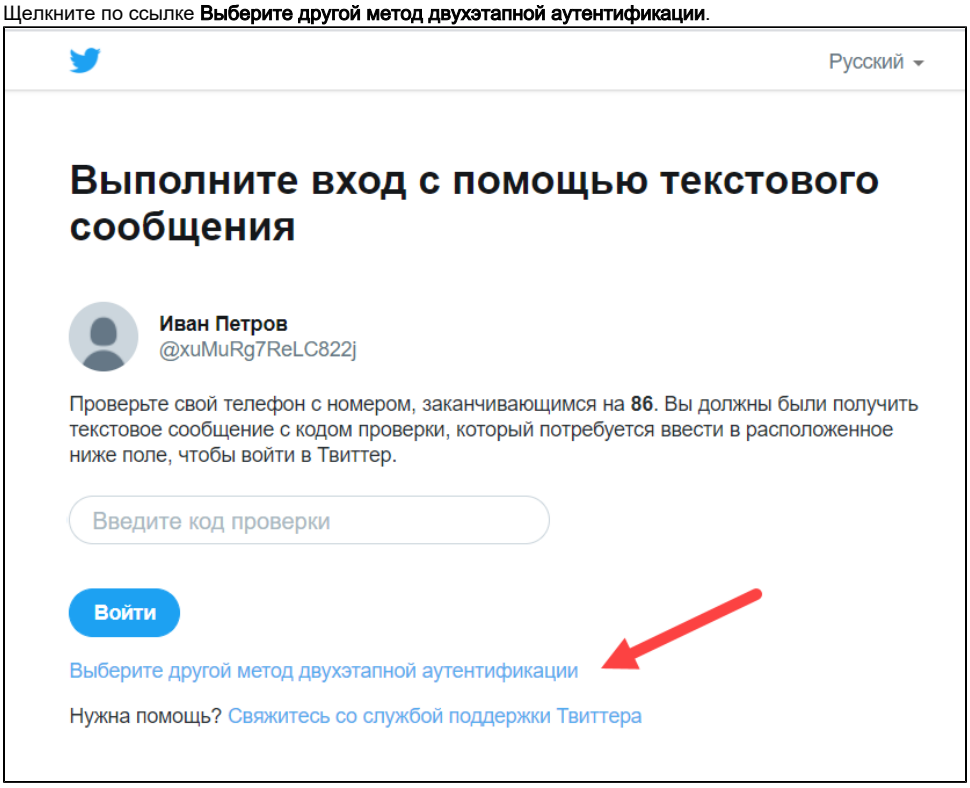
Теперь зайдите в свой аккаунт с помощью Рутокен U2F (этот процесс описан в следующем разделе).

Вход в аккаунт с помощью устройства Рутокен U2F в Twitter

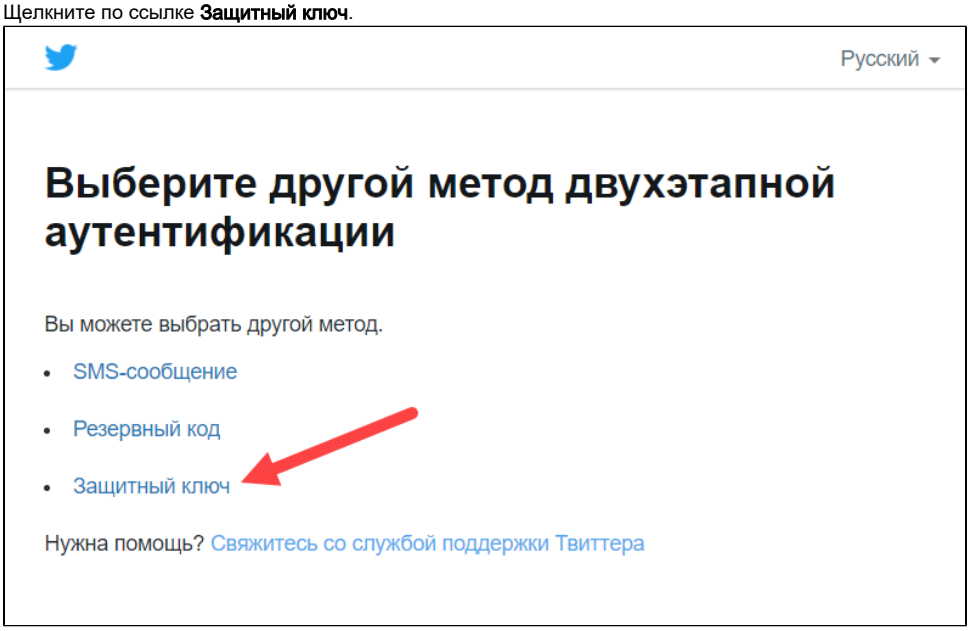
Чтобы войти в аккаунт:

1. Зайдите на страницу социальной сети Twitter.
2. Введите логин и пароль от своего аккаунта.

3. Щелкните по ссылке **Выберите другой метод двухэтапной аутентификации**.



4. Щелкните по ссылке **Защитный ключ**.



5. На токене начнет мигать индикатор.
6. Нажмите на сенсорную кнопку на устройстве Рутокен U2F. В результате вы зайдете в свой аккаунт.

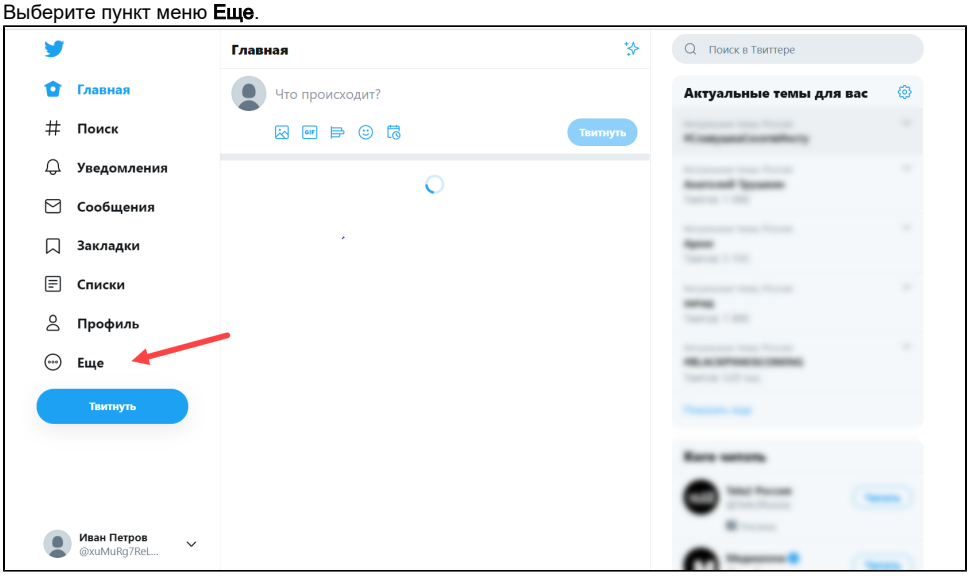
Удаление сведений о Рутокен U2F в Twitter

Если вы потеряли Рутокен U2F, который был привязан к аккаунту, или он перестал работать, то необходимо в Twitter удалить сведения о нем.

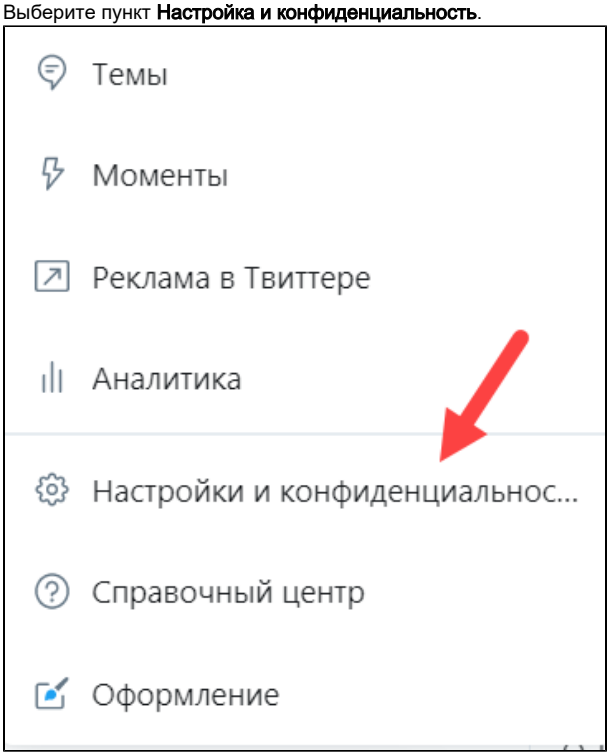
Для удаления сведений об устройстве:

1. Зайдите на страницу социальной сети Twitter.
2. Введите логин и пароль от своего аккаунта.
3. В окне **Подтверждение личности** нажмите **Отмена**.
4. Щелкните по ссылке **Выберите другой метод двухфакторной аутентификации**.
5. Щелкните по ссылке **Резервный код**.
6. Введите резервный код, который вы получили при включении двухфакторной аутентификации и нажмите **Войти**.

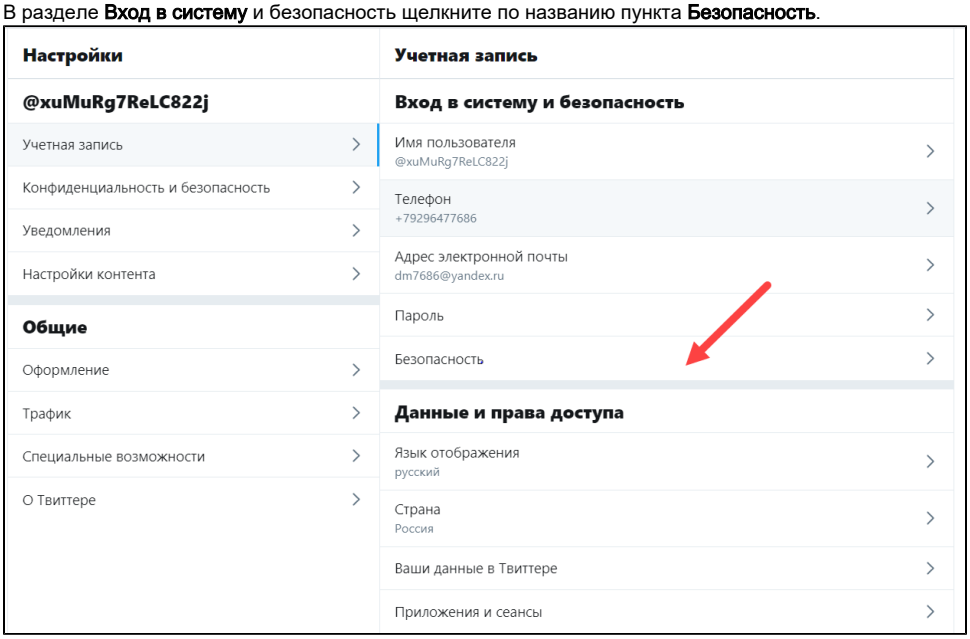
7. Выберите пункт меню **Еще**.



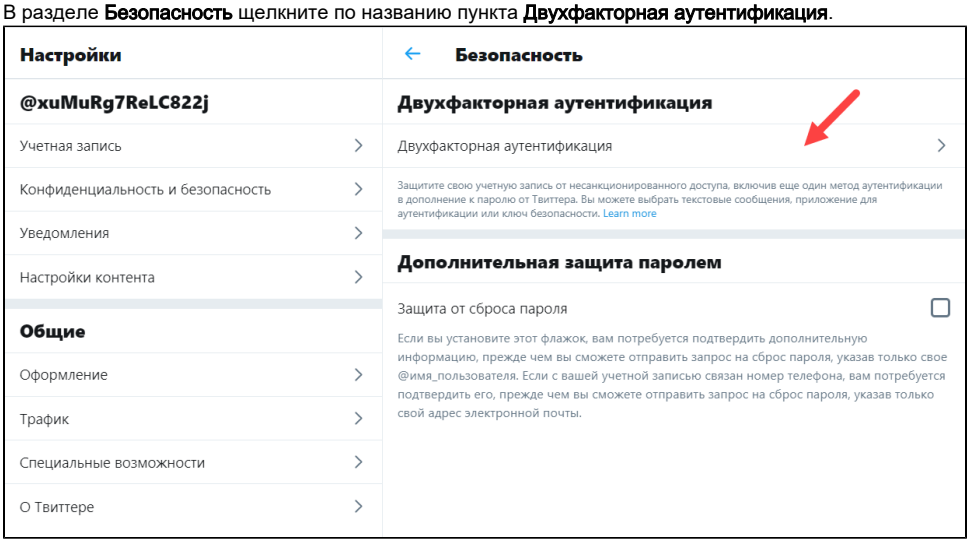
8. Выберите пункт **Настройка и конфиденциальность**.



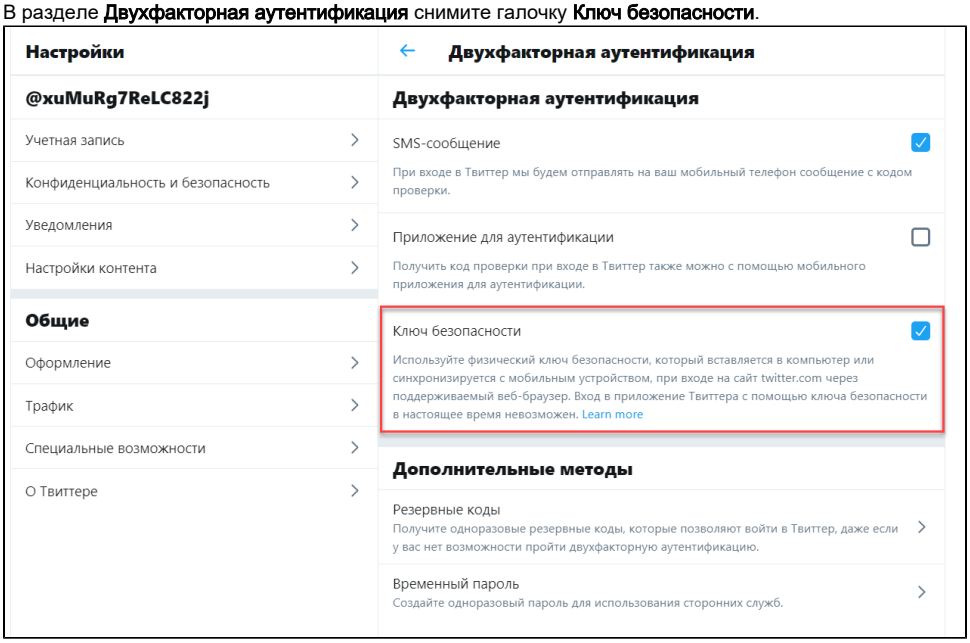
9. В разделе **Вход в систему** и безопасность щелкните по названию пункта **Безопасность**.



10. В разделе **Безопасность** щелкните по названию пункта **Двухфакторная аутентификация**.



11. В разделе **Двухфакторная аутентификация** снимите галочку **Ключ безопасности**.



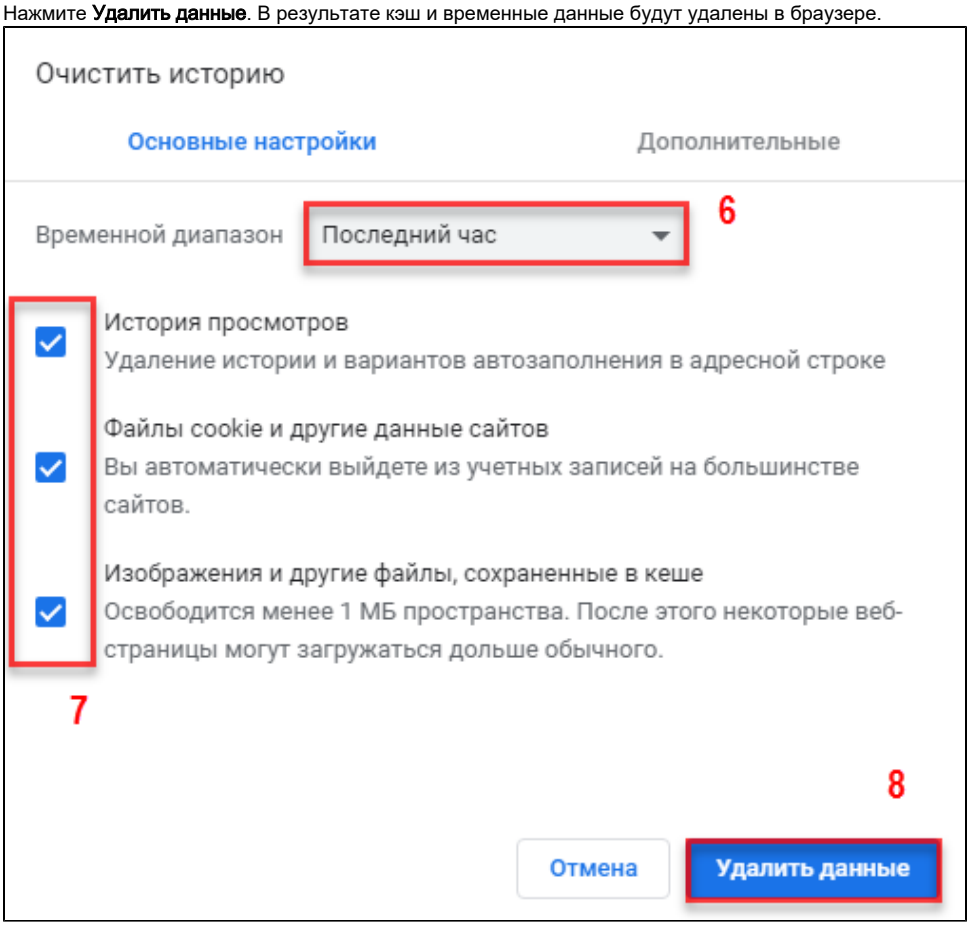
12. Нажмите **Отключить**. В результате сведения об устройстве Рутокен U2F будут удалены и при следующем входе в аккаунт нужно будет ввести логин, пароль и код безопасности.

Приложение 1. Очистка кэша и временных данных в браузере

Браузер Google Chrome

Для очистки кэша и временных данных:

1. Запустите браузер на компьютере.
2. В правом верхнем углу щелкните по значку blocked URL.
3. Выберите пункт **Настройки**.
4. В нижней части окна **Настройки** щелкните по ссылке **Дополнительные**.
5. В секции **Конфиденциальность и безопасность** щелкните по строке **Очистить историю**.
6. В окне **Очистить историю** в раскрывающемся списке **Временной диапазон** выберите необходимое значение.
7. Установите галочки: **История просмотров**; **Файлы cookie и другие данные сайтов**; **Изображения и другие файлы, сохраненные в кеше**.
8. Нажмите **Удалить данные**. В результате кэш и временные данные будут удалены в браузере.



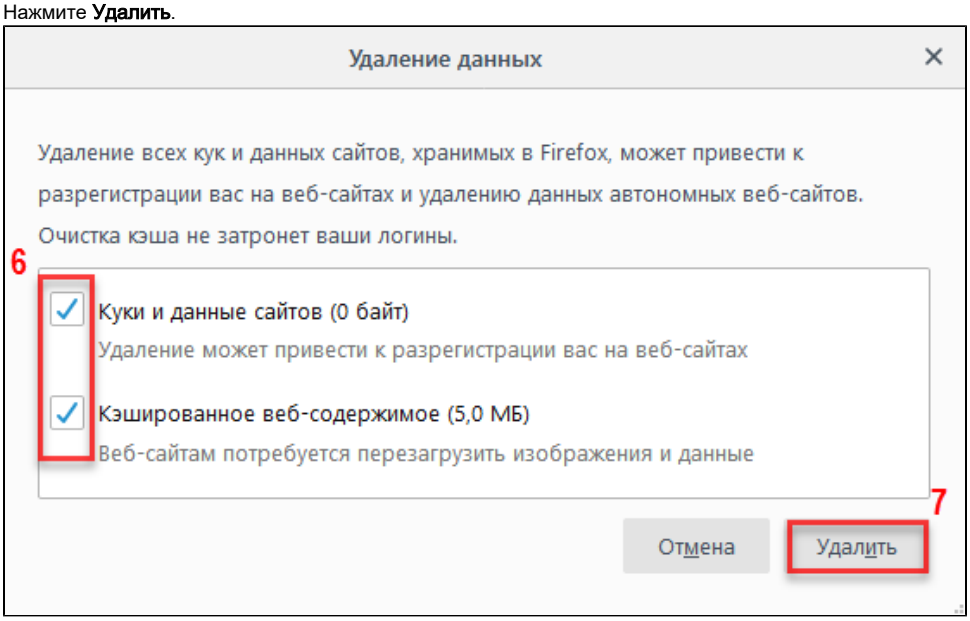
9. Перезагрузите компьютер.

Браузер Mozilla Firefox

Для очистки кэша и временных данных:

1. Запустите браузер на компьютере.
2. В правом верхнем углу щелкните по значку ☰.
3. Выберите пункт меню **Настройки**.
4. Щелкните по названию раздела **Приватность и Защита**.
5. В секции **Куки и данные сайтов** нажмите **Удалить данные**.
6. Установите галочки: **Куки и данные сайтов**, **Кэшированное веб-содержимое**.

7. Нажмите **Удалить**.



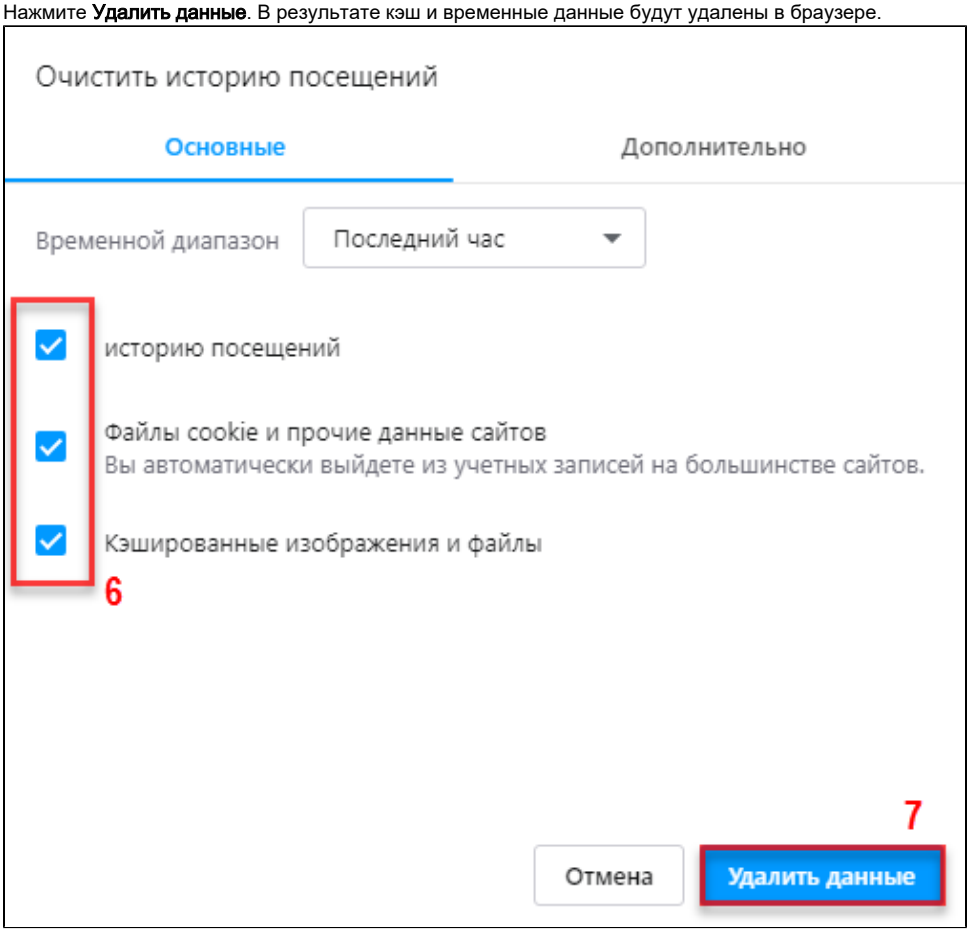
8. Нажмите **Удалить сейчас**. В результате кэш и временные данные будут удалены в браузере.
9. Перезагрузите компьютер.

Браузер Opera

Для очистки кэша и временных данных:

1. Запустите браузер на компьютере.
2. В левом верхнем углу щелкните по значку .
3. Выберите пункт меню **Настройки**.
4. Щелкните по названию раздела **Дополнительно** и подраздела **Безопасность**.
5. Щелкните по строке **Очистить историю посещений**.
6. Установите галочки: **история посещений**, **Файлы cookie и прочите данные сайтов**, **Кэшированные изображения и файлы**.

7. Нажмите **Удалить данные**. В результате кэш и временные данные будут удалены в браузере.



8. Перезагрузите компьютер.

Для включения двухфакторной аутентификации вам понадобится мобильный телефон.