3. Безопасность

Резервное копирование ключей шифрования

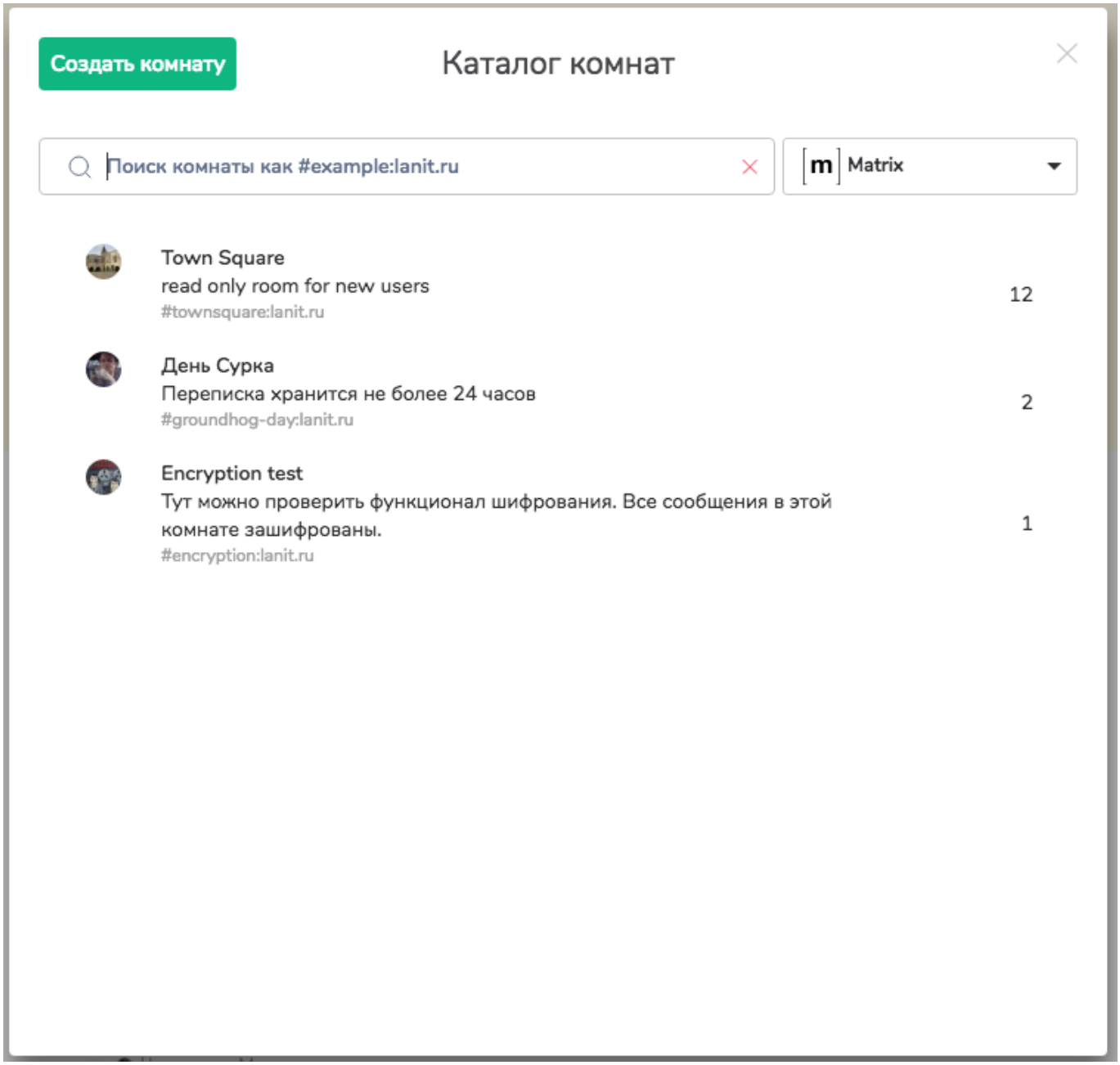
При включенном шифровании вся переписка надежно защищена шифрованием точка-точка (между клиентами) от прочитывания и прослушивания . Таким образом сервер не получает оригиналов сообщений а передает все в зашифрованном незименном виде.

> Если вы потеряете ключи шифрования то никто, включая администратора сервера не сможет восстановить историю ваших сообщений. Храните пароль шифрования и резервные копии ключей в надежном и безопасном месте!

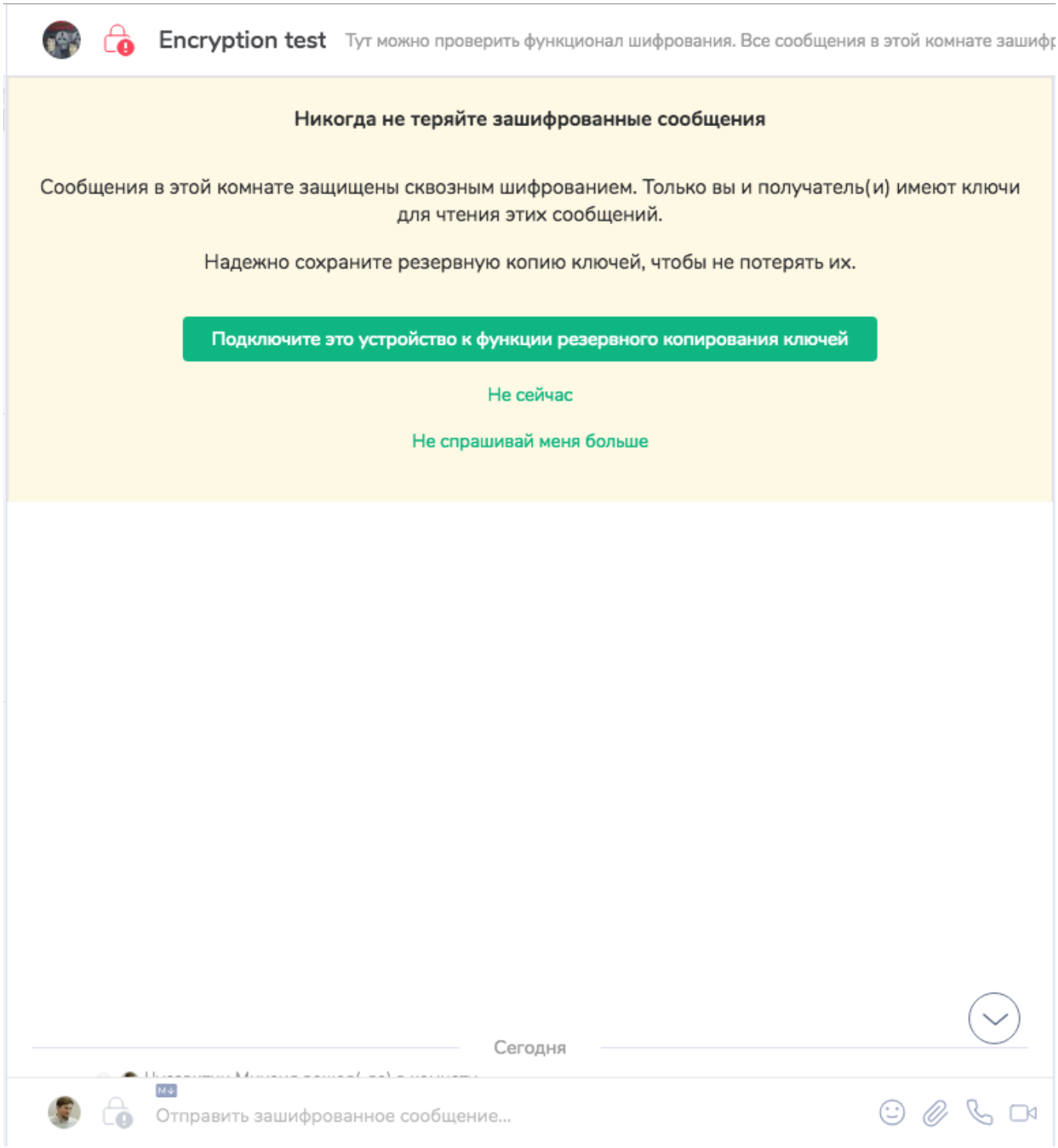
Настройка резервного копирования ключей

Чтобы проверить шифрование можно подключиться к специальной зашифрованой комнате.

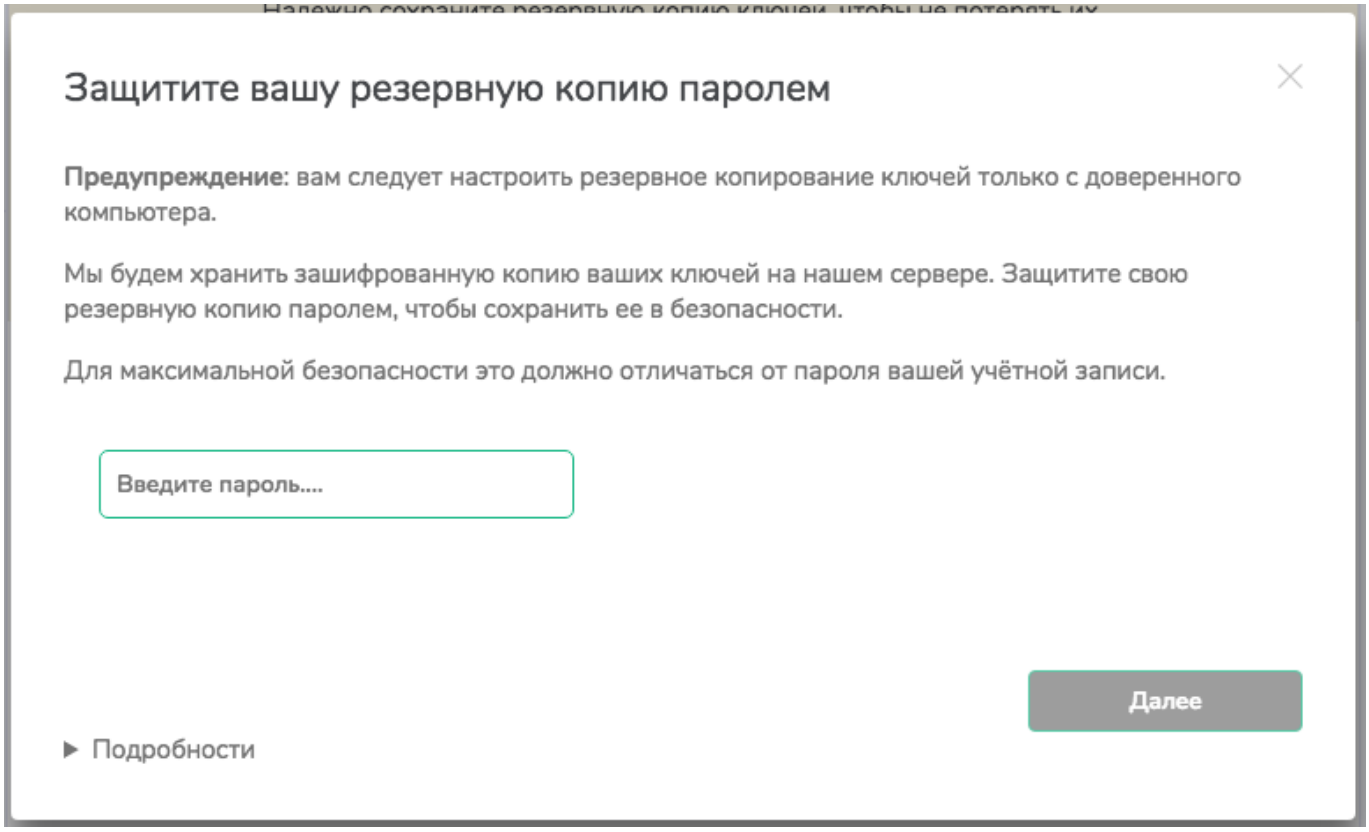
#encryption:lanit.ru



Для этого нажмите кнопку подключения к комнате и выберите “Encryption test” или введите в поиске #encryption:lanit.ru, предварительно выбрав сервер lanit.ru



Теперь ваш клиент сгенерировал ключи шифрования, которые будет использовать для защиты информации при передаче. Данное сообщение будет отображаться каждый раз при входе с нового устройства.



Нажмите “Подключить это устройство к функции резервного копирования ключей” для сохранения **зашифрованной** копии ключей шифрования на сервере. Выбирайте пароль, отличный от пароля своей учетной записи иначе в случае компроментации вашего доменного пароля шифрованные сообщения станут известны злоумшленнику (или администратору домена).

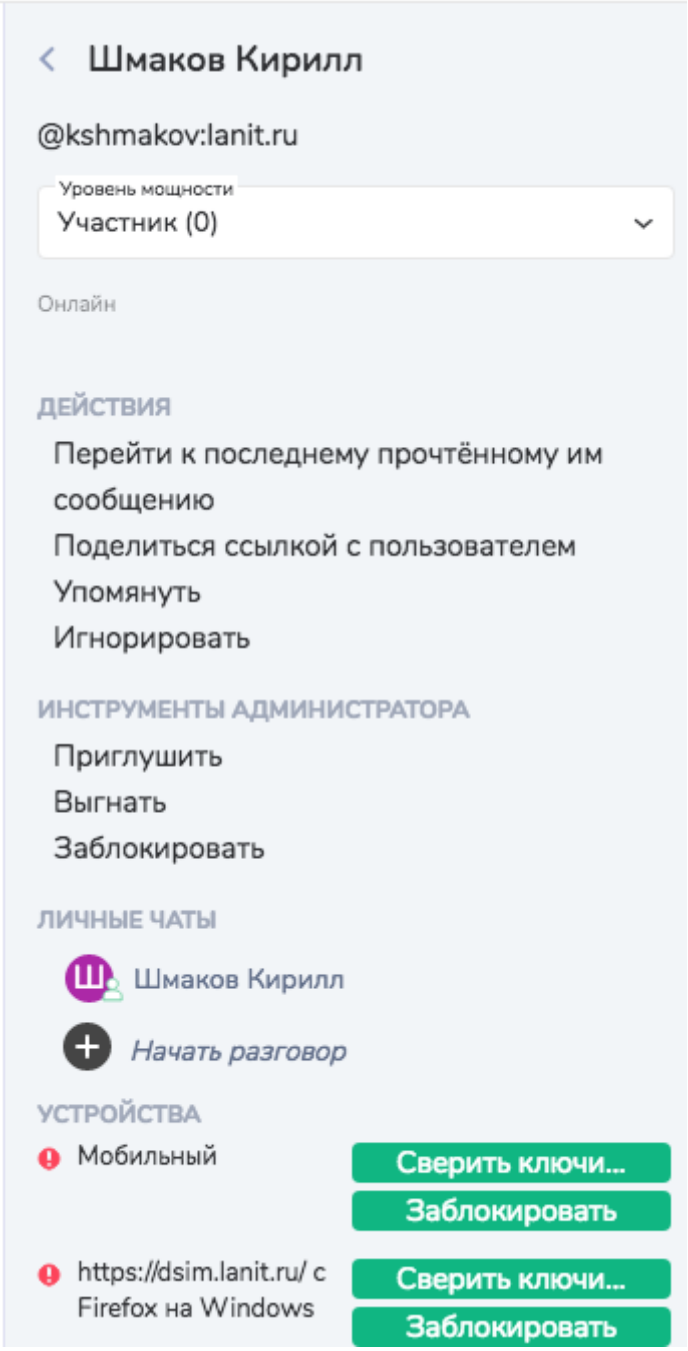
В случае если вы не подключите сессию к функции резервного копирования - при закрытии браузера или при выходе из приложения ключи шифрования будут стерты и вы не сможете прочитать зашифрованные сообщения которые ранее отправляли другим пользователям.

Теперь когда вы настроили функцию резервного копирования ключей шифрования можно приступать к созданию собственных зашифрованных комнат.

Проверка собеседника

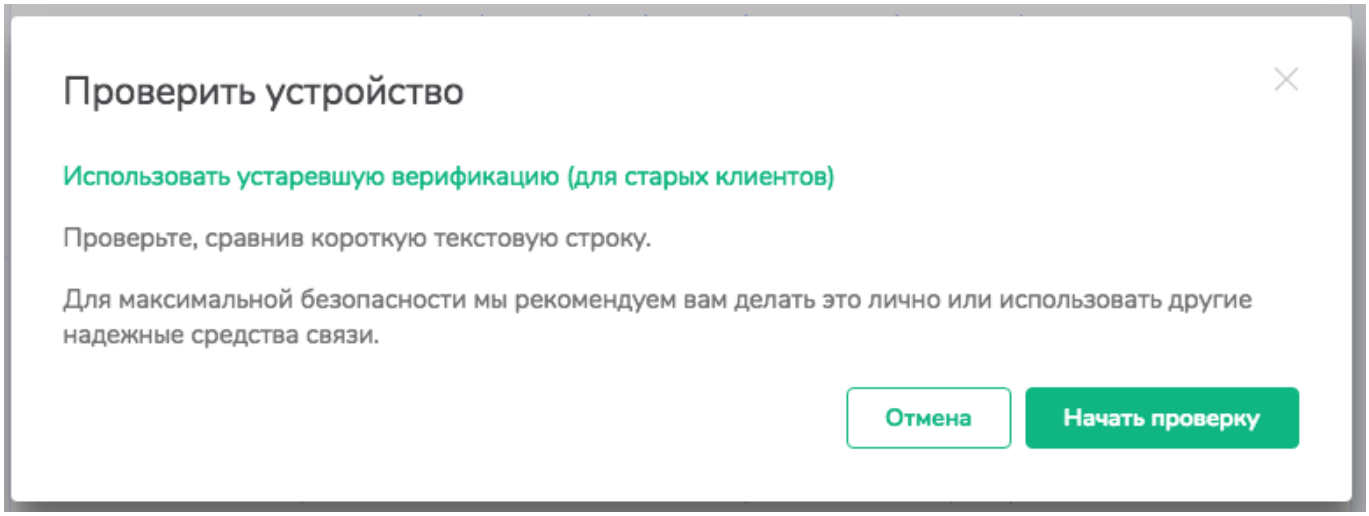
Важная мера безопасности, которую не стоит недооценивать - проверка того, что ваш собеседник именно тот, кто за кого себя выдает.

Данная мера позволяет защититься от кражи учетной записи и позволяет ограничить обмен сообщениями с непроверенными устройствами. Для этого необходимо нажать на имя собеседника в групповой или личной переписке:

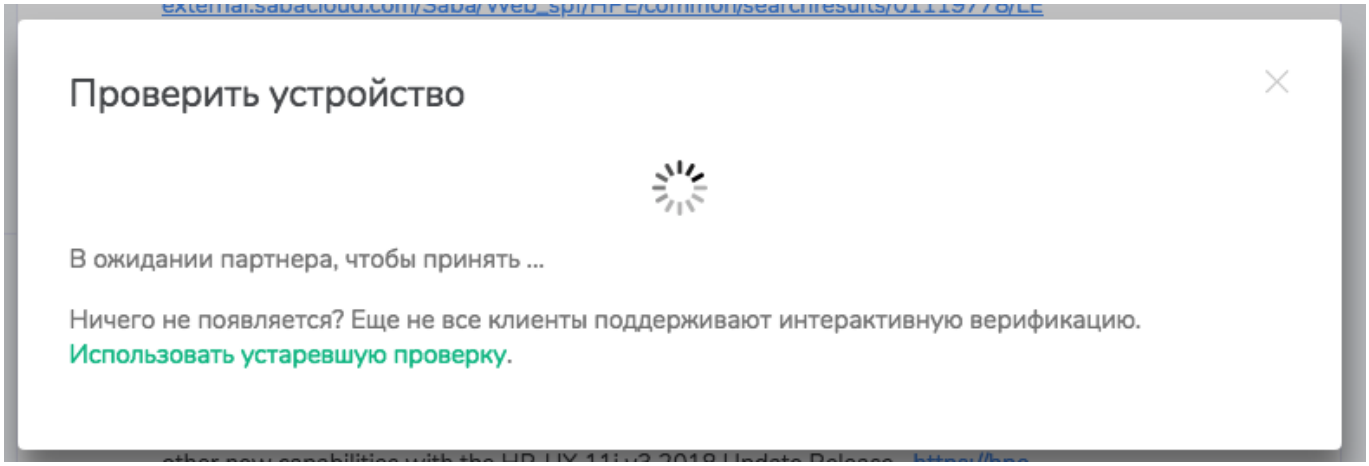


Для каждой сессии пользователя создается отдельная аутентификационная запись в системе. В данном примере Кирилл входил в сеть с мобильного устройства и с помощью брауреза Firefox на Windows. Чтобы обезопасить себя от прослушивания обменяемся с Кириллом ключами шифрования, чтобы подтвердить аутентичность сессии.

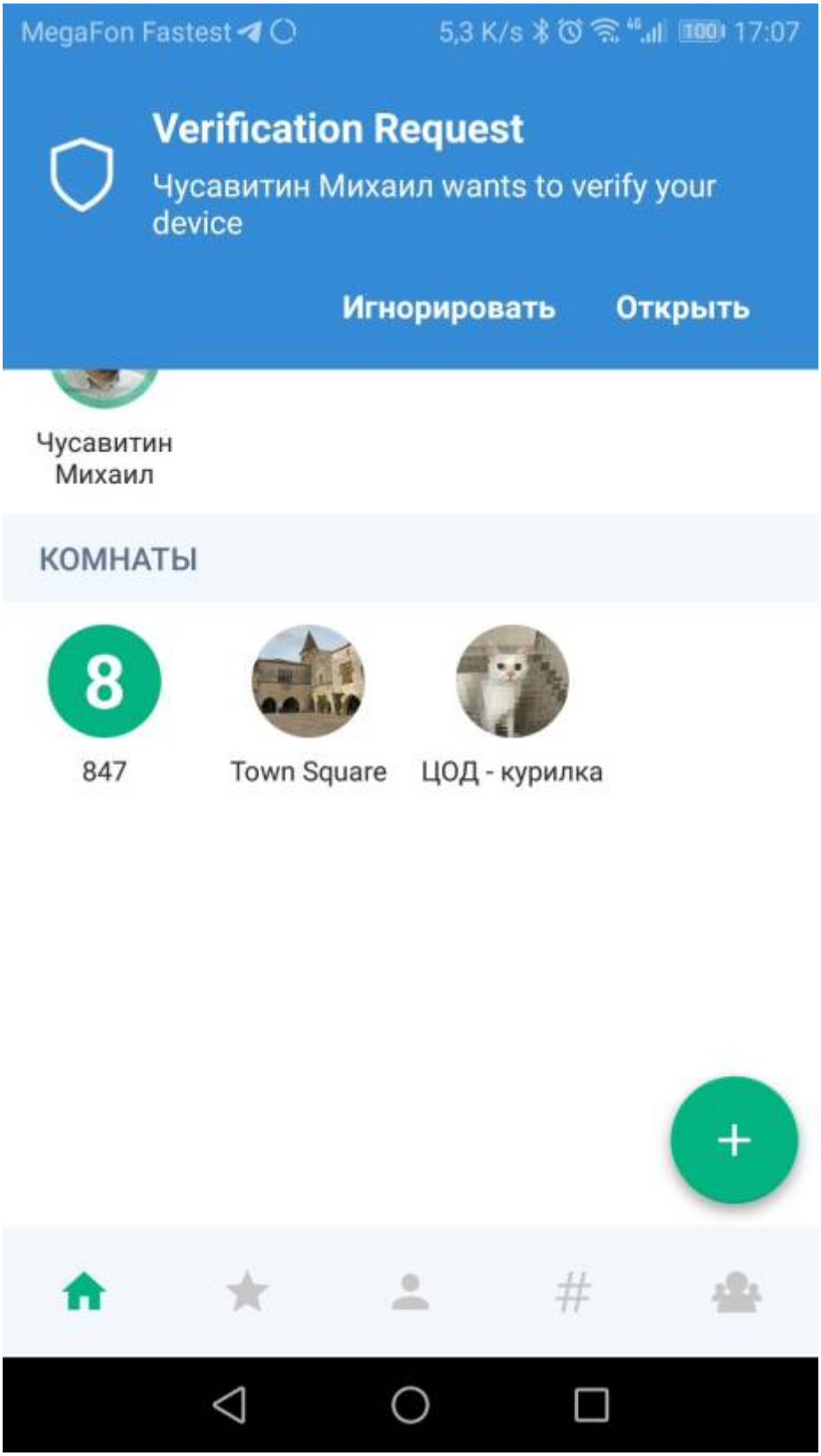
Нажимаем на кнопку “Сверить ключи”



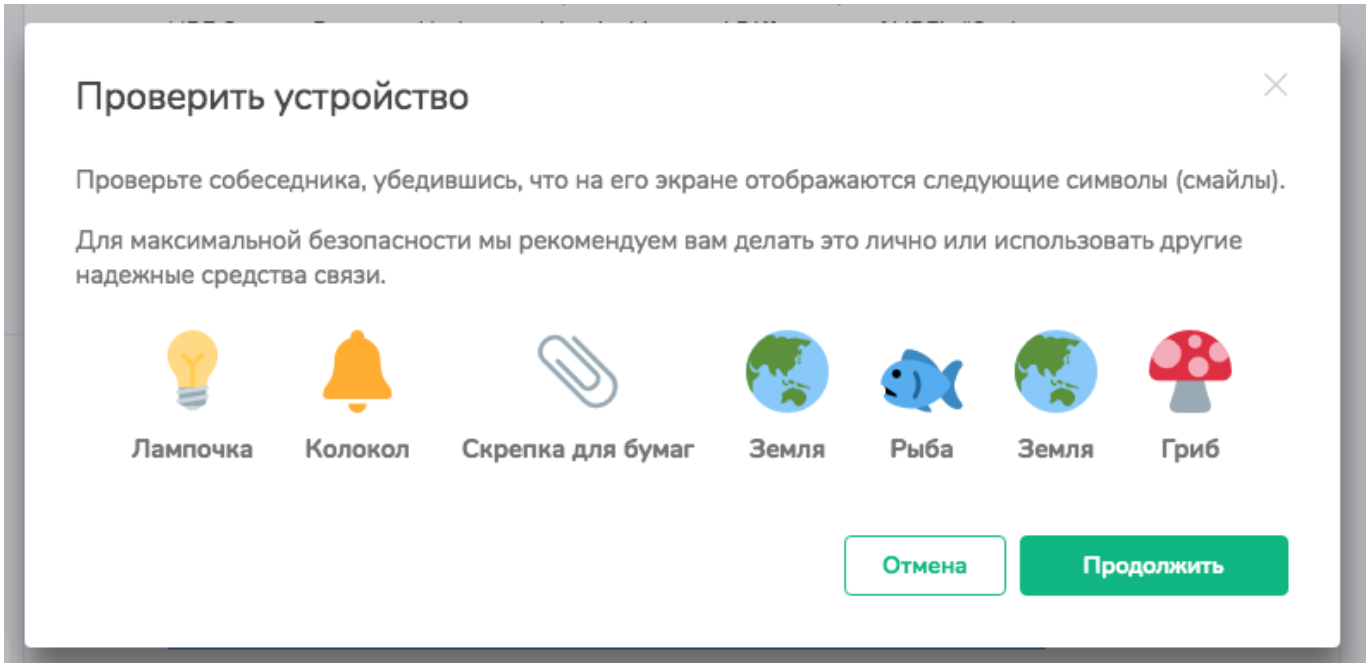
Нажимаем кнопку современной проверки - начать проверку. Это более безопасный и простой способ.

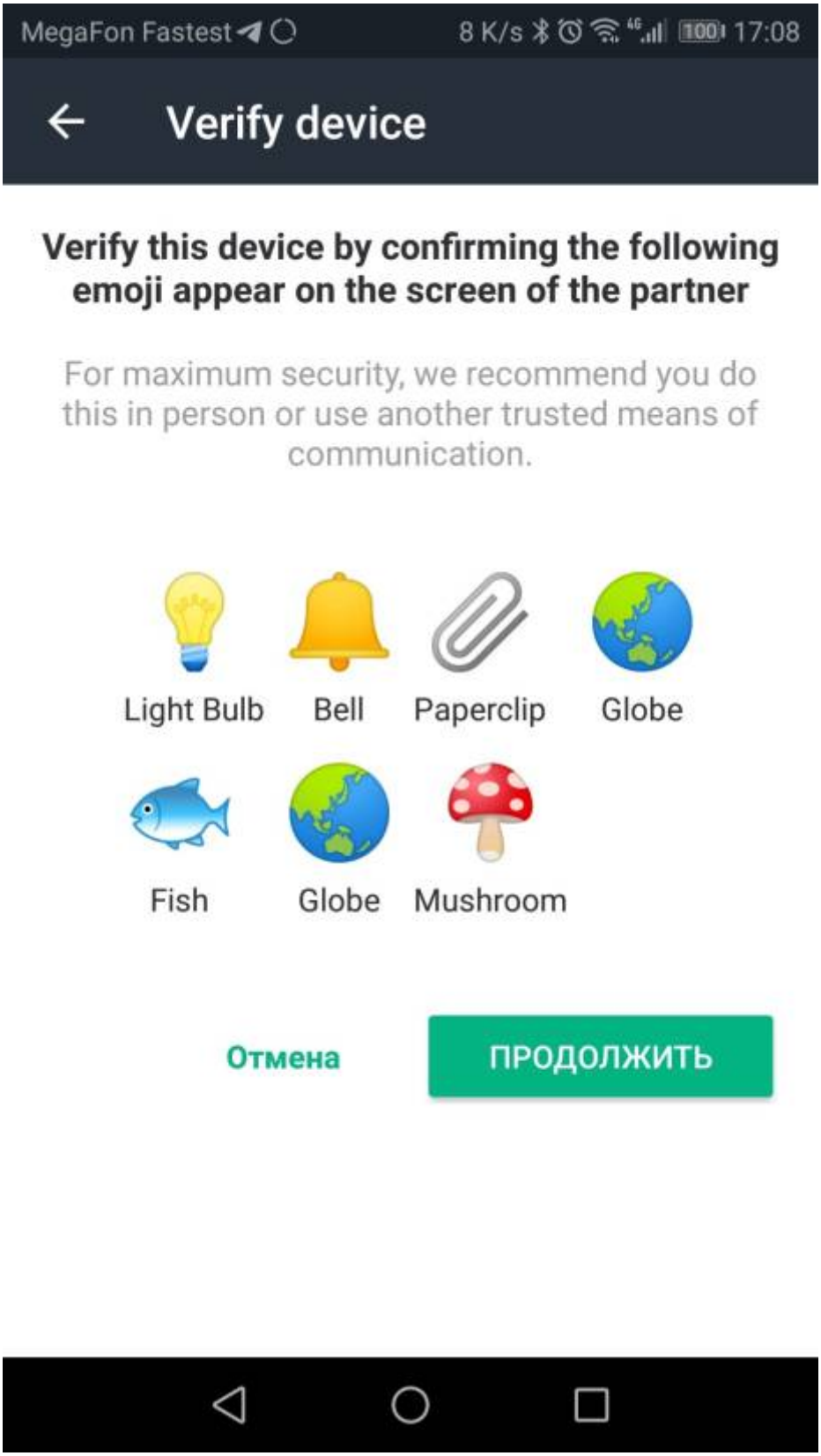


Для безопасности второй человек не получит никакого всплывающего уведомления, ему необходимо будет специально открыть приложение и пройти верификацию. Это сделано для безопасности.



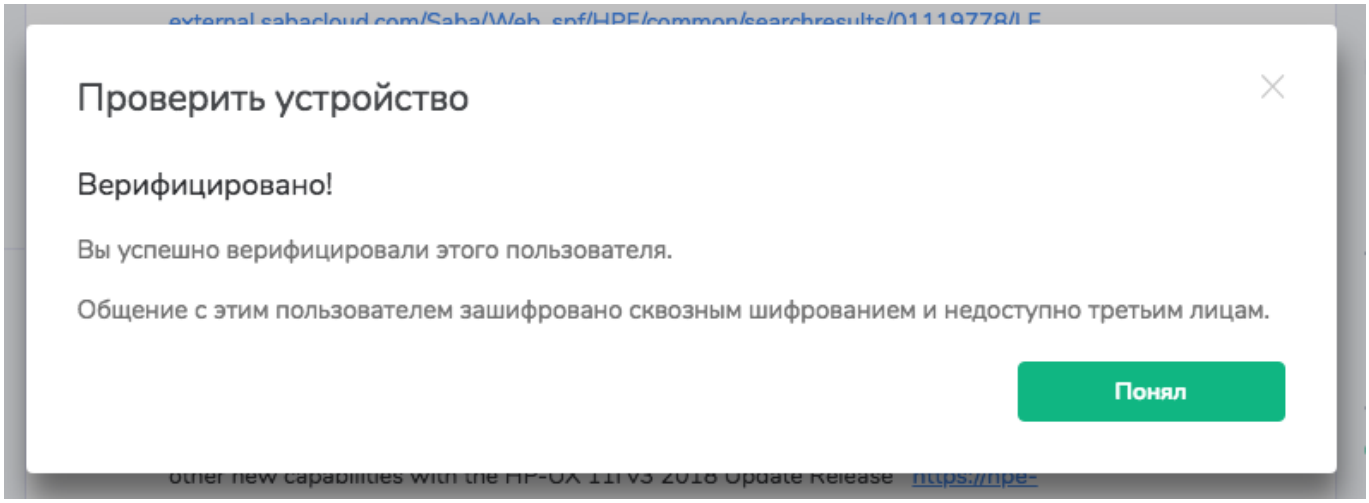
После принятия приглашения о верификации и обоих пользователей появляется ряд эмодзи, которые в простом и удобном для человека виде позволяют сравнить подписи протокола шифрования. Если эмодзи совпадают - значит человек тот, за кого себя выдает.


Проверить устройство
Проверьте собеседника, убедившись, что на его экране отображаются следующие символы (смайлы).
Для максимальной безопасности мы рекомендуем вам делать это лично или использовать другие надежные средства связи.
Лампочка
Колокол
Скрепка для бумаг
Земля
Рыба
Земля
Гриб
Отмена
Продолжить

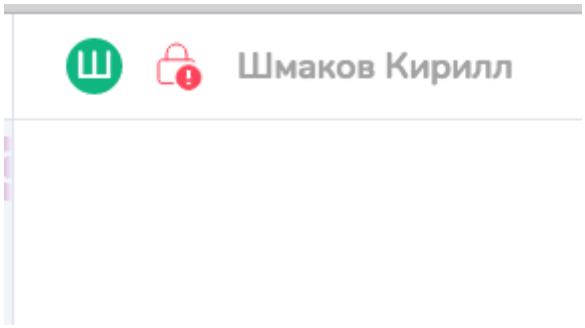


Если эмодзи совпадают - нажимаем “Продолжить”

На разных платформах начертания изображения могут немного отличаться друг от друга, это не играет особого значения и не влияет на безопасность переписки.

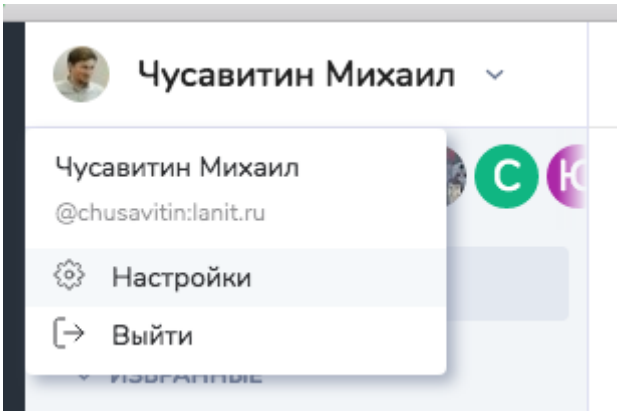


Теперь в случае если один из участников переписки войдет в сеть с незнакомого нового устройства или это сделает злоумышленник - иконка безопасных чатов изменится у обоих участников разговора на **красную**:

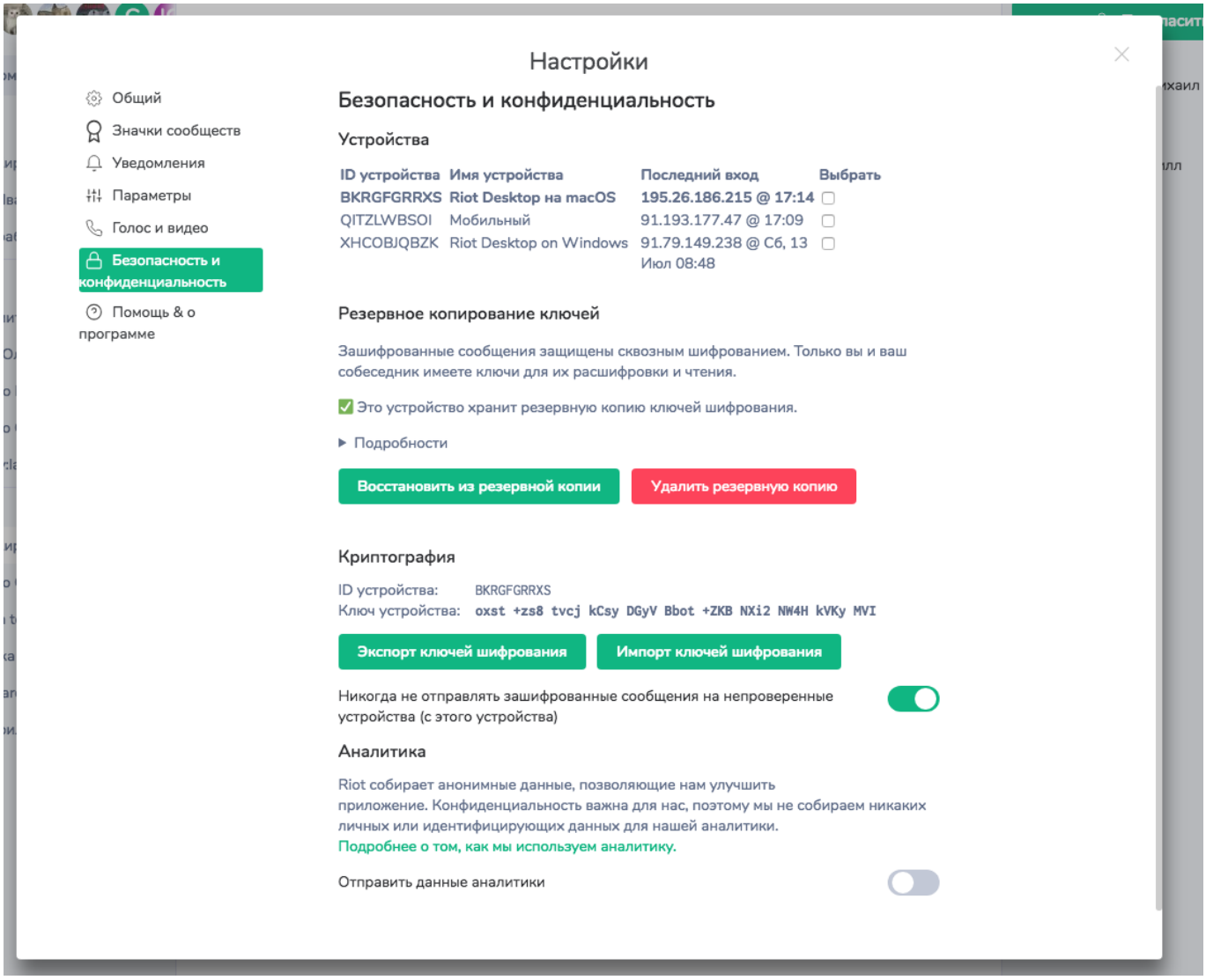


Вы можете обезопасить себя от невнимательности и запретить отправку сообщений на непроветренные устройства в настройках своего акаунта.

Нажмите на свою учетную запись сверху слева, выберите настройки.



Перейдите в раздел “Безопасность и конфиденциальность” и включите переключатель “**Никогда не отправлять зашифрованные сообщения на непроверенные устройства (с этого устройства)**”

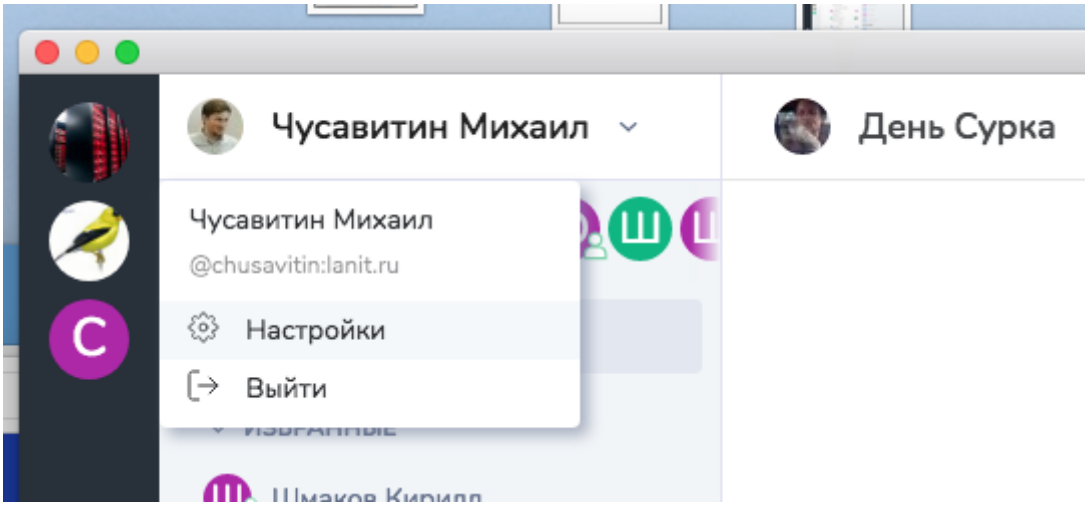


Управление сессиями

Иногда бывает необходимо удалить старые сессии, чтобы пройти верификацию шифрования у собеседников или просто узнать что злоумышленник не пользуется вашей учетной записью чтобы читать переписку.

Проверить сколько сессий открыто к серверу и удалить неиспользуемые очень просто.

Нажмите на свое имя в левой верхней части окна и выберите настройки:



Перейдите на вкладку “Безопасность и конфиденциальность”

Перед вами отображены все серии, адрес и последняя дата входа. Чтобы закрыть не используемые сессии - поставьте галочку и выберите удалить.

Так-же вы можете нажать на имя устройства и заменить его на что-то более понятное для ваших собеседников и вас самих, например следующим образом:

Данное действие часто придется повторять - если вы пользуетесь веб-клиентом и не сохраняете пароль, так-же при переустановке мобильного или приложения для ПК. Советую держать данный список минимальным чтобы упросить верификацию вас как абонента у собеседников.