Руководство пользователя мессенджера «РЕД V»

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Мессенджер «РЕД V» разработан компанией РЕД СОФТ для корпоративных нужд, в том числе для ведения проектов с различными государственными структурами. Он поддерживает следующие операционные системы:

- Android,
- РЕД ОС М,
- РЕД ОС 7 и 8 (потенциально любой дистрибутив Linux),
- Microsoft Windows,
- macOS (на декабрь 2024 года находится в бетаверсии).

Данный продукт обеспечивает высокий уровень защищённости передаваемой конфиденциальной информации ввиду локализации серверной части мессенджера в инфраструктуре Компании и изоляции её от глобальной сети для предотвращения утечек информации, наличия всех исходных кодов у разработчиков Компании, поддержки ряда функций обеспечения информационной безопасности (секретные чаты по умолчанию для двух и более участников, необходимость верификации через QR-код новых устройств и др.).

В этом руководстве представлено описание наиболее важных функций, сопровождаемое наглядными иллюстрациями. Стоит отметить, что на некоторых снимках экрана можно увидеть первоначальное название продукта «РЕД ЭФИР», что не должно смущать конечного пользователя, равно как и некоторые скрытые конфиденциальные данные. Наиболее подробно описана функциональность мобильной версии приложения. Описания версий под операционные системы РЕД ОС и Microsoft Windows в большей степени носят сравнительный характер, показаны отличия от мобильной версии приложения. Версия под ОС Microsoft Windows рассматривается в меньшем объёме ввиду расставленных приоритетов по поддержке различных платформ.

1 УСТАНОВКА КОРПОРАТИВНОГО МЕССЕНДЖЕРА

1.1 Операционная система Android

Установка и обновление приложения корпоративного мессенджера выполняются ручным образом из APK-файла, распространяемого через внутренние информационные ресурсы Компании.

Внимание! Конечным пользователям запрещается размещать данный файл в неограниченном доступе до его официальной публикации в магазинах приложений (как отечественных, так и иностранных)!

1.2 Операционная система РЕД ОС

Приложение под данную операционную систему распространяется в виде gz-архива, содержащего в себе все его файлы. Процесс его установки, например, на рабочий стол текущего пользователя будет состоять из следующих шагов:

1. Открыть системное приложение «Терминал» из меню «Пуск».
2. Ввести команду: sudo yum install wireguard-tools.
3. Ввести пароль текущего пользователя. Если он не подойдёт, вызвать системного администратора для установки пакета wireguard-tools.
4. Подтвердить готовность к установке вводом символа «Д». Если возникла ошибка с кодом 404, ввести и исполнить команду sudo yum update.
5. Разместить на рабочем столе текущего пользователя предназначенные для установки файлы приложения.
6. Переключиться на окно терминала и ввести команду cd ~/Рабочий\ стол.
7. Выполнить команду: tar -xf red-v-desktop-1.0.12.tar.gz (скорректировать для конкретного имени файла архива).
8. Выполнить команду: cd red-v-desktop-1.0.12 (см. предыдущий пункт).
9. Выполнить команду sudo ./resolv_names.sh с полным путём к выданному администратором мессенджера conf-файлу VPN-подключения в качестве входного аргумента.

   Например: sudo ./resolv_names.sh ~/Документы/conf/ml_surgeon.conf.
10. Выполнить команду ./red-v-desktop для запуска приложения мессенджера.

После выполнения всех выше перечисленных шагов будет открыто VPN-соединение и запущен мессенджер, а на рабочем столе текущего пользователя появится ярлык. Необходимо отметить, что перемещение каталога, в который был распакован gz-архив, не разрешается, т.к. в таком случае ссылка на исполняемый файл приложения станет недействительной. После перезапуска операционной системы VPN-соединение будет открываться автоматически.

1.3 Операционная система Microsoft Windows

Установщик приложения под данную операционную систему состоит из одного исполняемого файла. Установка самого мессенджера не требует прав системного администратора. Данный процесс занимает не более пяти минут, во время него отображается заставка в виде логотипа приложения. После установки на рабочем столе текущего пользователя появится ярлык.

2 АВТОРИЗАЦИЯ

Процесс авторизации, осуществляемый после настройки подключения к отдельной VPN-сети Компании, требует знания учётных данных – имени пользователя и пароля. В текущей (на декабрь 2024 года) версии мессенджера отсутствует поддержка самостоятельной регистрации учётной записи. Также нет возможности авторизации по электронной почте или номеру телефона, не поддерживается двухфакторная аутентификация. Учётная запись создаётся системным администратором после соответствующего запроса на электронный адрес redvsup@red-soft.ru.

2.1 Операционная система Android

На рисунке 1 изображено окно, отображаемое при первом запуске установленного приложения мессенджера и после выхода из текущей учётной записи. Для перехода к следующему шагу необходимо нажать на кнопку «SIGN IN». После этого откроется окно с полем ввода адреса сервера. Данный адрес доступен только из отдельной VPN-сети Компании.

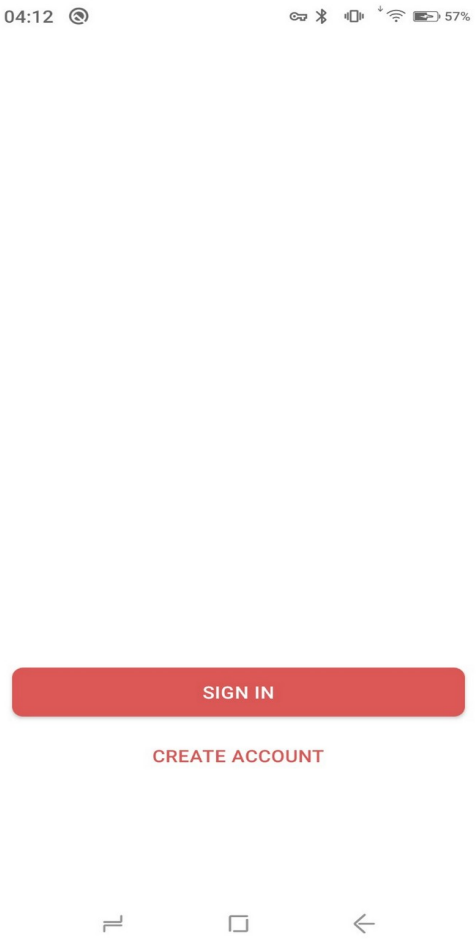

Рисунок 1 - Окно авторизации мессенджера (ОС Android)

На рисунке 2 показано окно с полем ввода адреса сервера. Выделенная зелёным цветом часть свидетельствует об использовании первой версии сервера. *После миграции на вторую версию она изменится с «http» на «https»*, таким образом повысится защищённость конечных пользователей. Также частично изменится синяя часть - вместо поддомена «ether» будет поддомен «rv» (таким образом, полное значение поля будет равно «https://rv.redsoft.localdomain»). Для перехода к следующему шагу необходимо нажать на кнопку «NEXT».

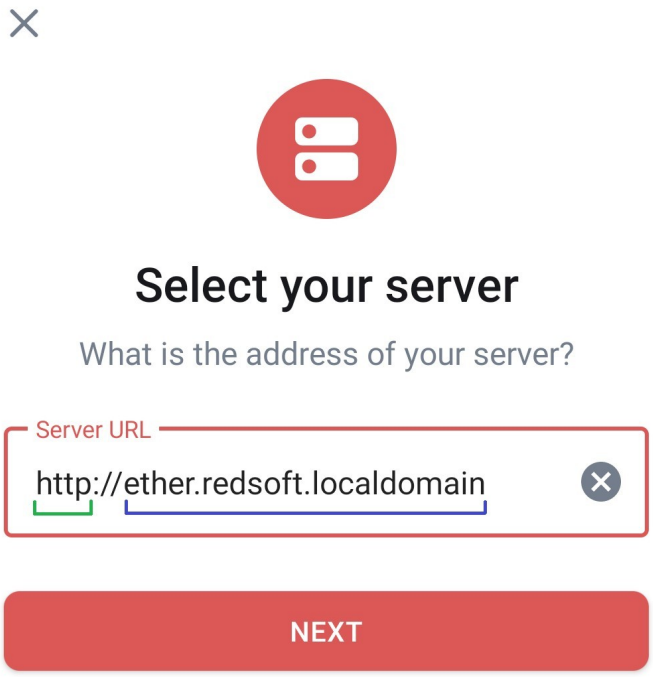

Рисунок 2 - Окно ввода адреса сервера (актуальное значение – https://rv.redsoft.localdomain)

После нажатия на кнопку «NEXT» пользователю будет предложено ввести его учётные данные (Рисунок 3). В случае их корректности с сервера загрузятся чаты и группы, в которых состоит обладатель учётной записи, если вход в систему им выполняется не в первый раз. Для дешифрования сообщений в них необходимо пройти верификацию новой сессии (см. пункты Обеспечение доступа к сообщениям и Подтверждение сеанса на новом устройстве).

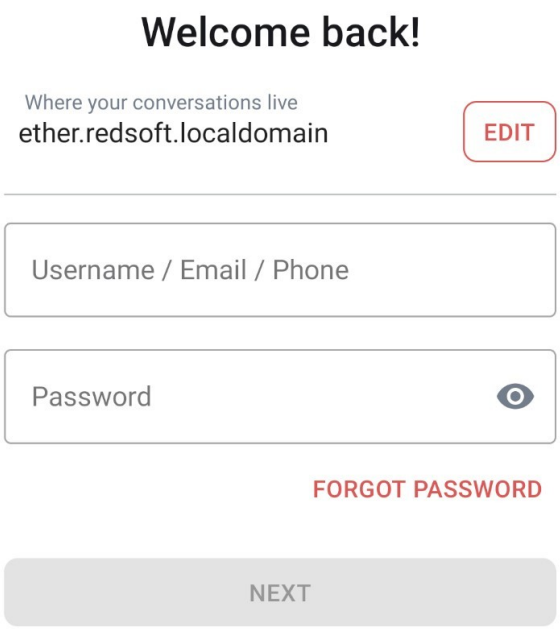

Рисунок 3 - Окно ввода учётных данных пользователя (Android)

2.2 Операционная система РЕД ОС

На рисунке 4 изображено окно, аналогичное представленному на рисунке 1. Для перехода к следующему шагу необходимо нажать на кнопку «Войти», после чего откроется окно выбора адреса сервера, которое может выглядеть так, как показано на рисунке 5. На нем видно, что подключение к серверу невозможно ввиду недоступности адреса. Пользователь может устранить эту проблему, выбрав другой адрес (Рисунок 6).

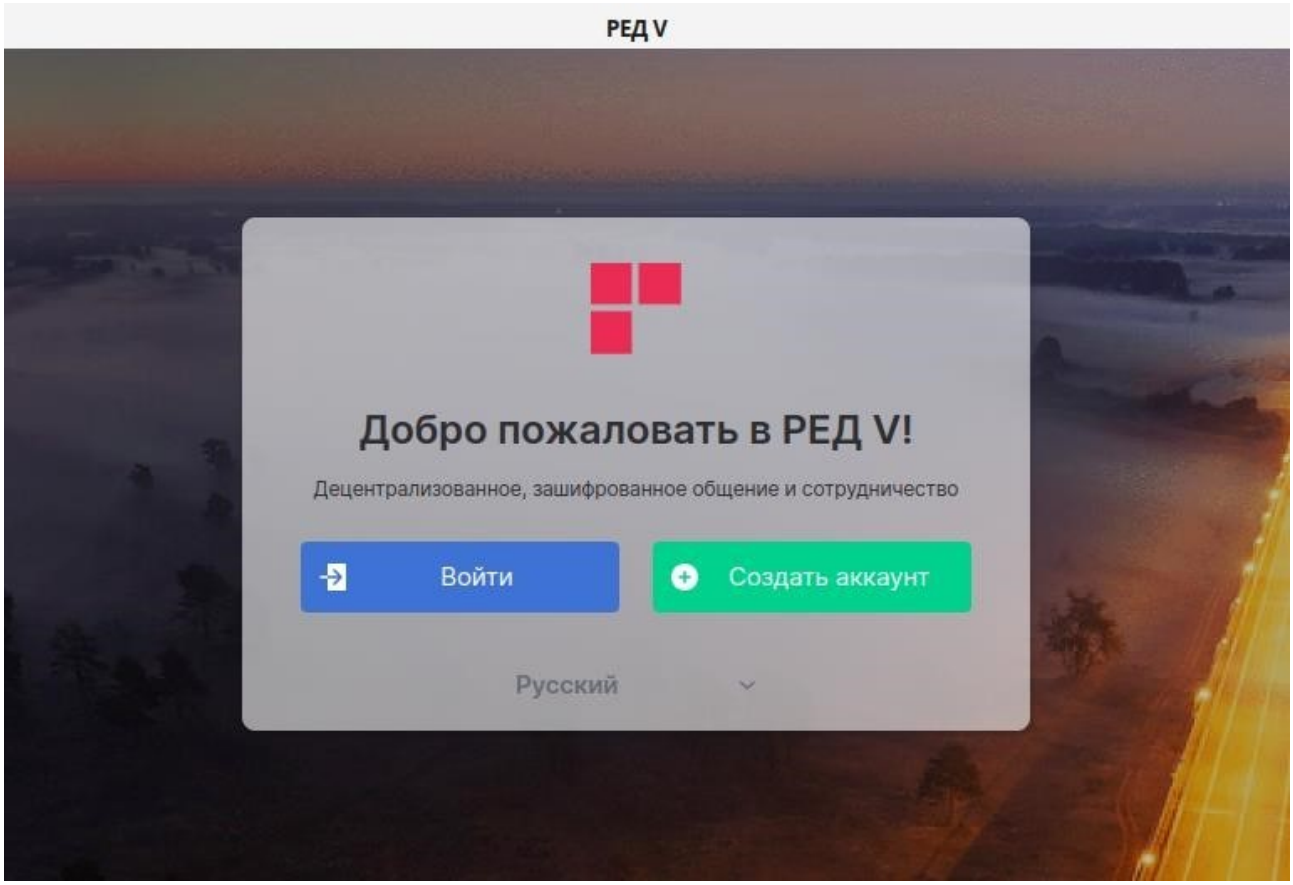

Рисунок 4 - Окно авторизации мессенджера (РЕД ОС)

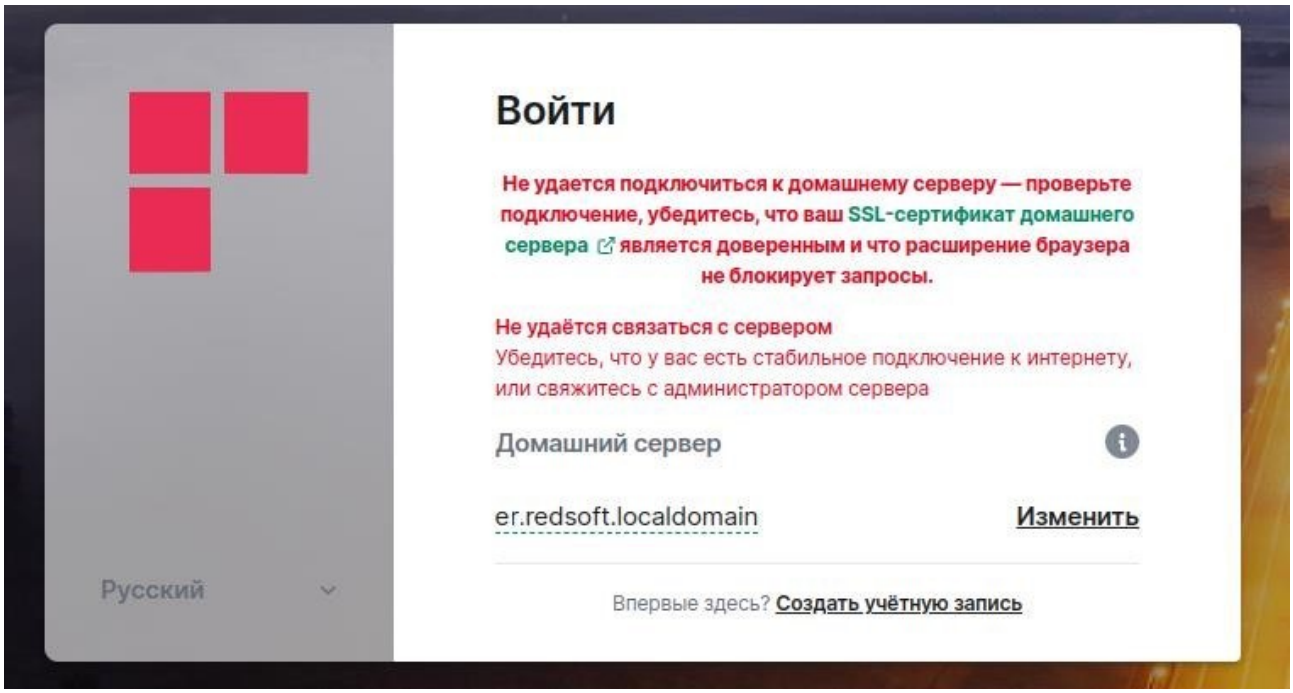

Рисунок 5 - Сообщение об ошибке при подключении к серверу по предопределенному адресу

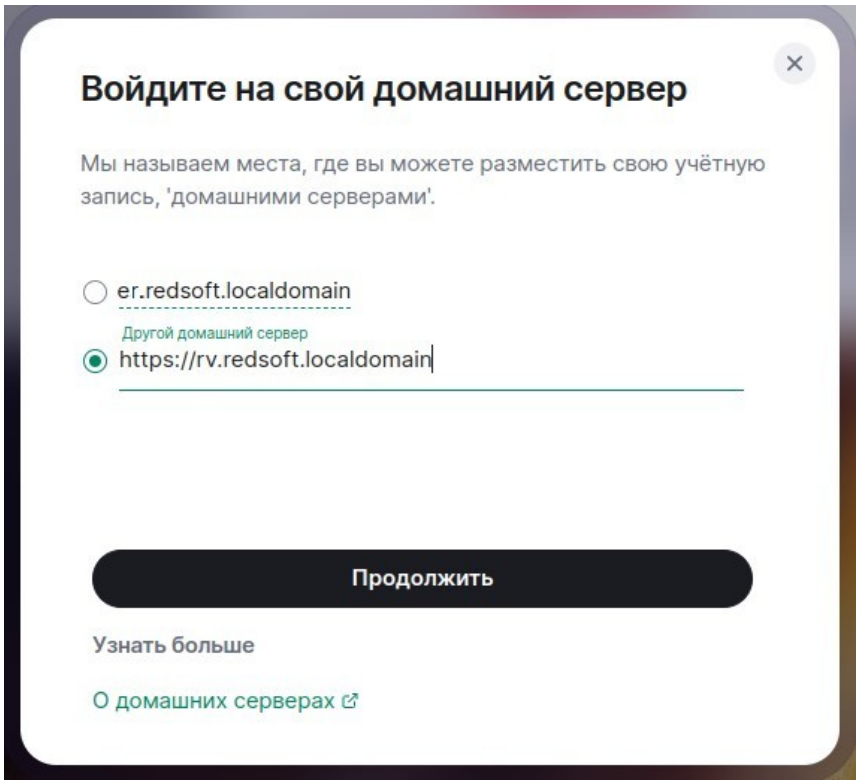

Рисунок 6 - Изменение адреса сервера

После выбора корректного адреса откроется окно ввода учётных данных, показанное на рисунке 7.

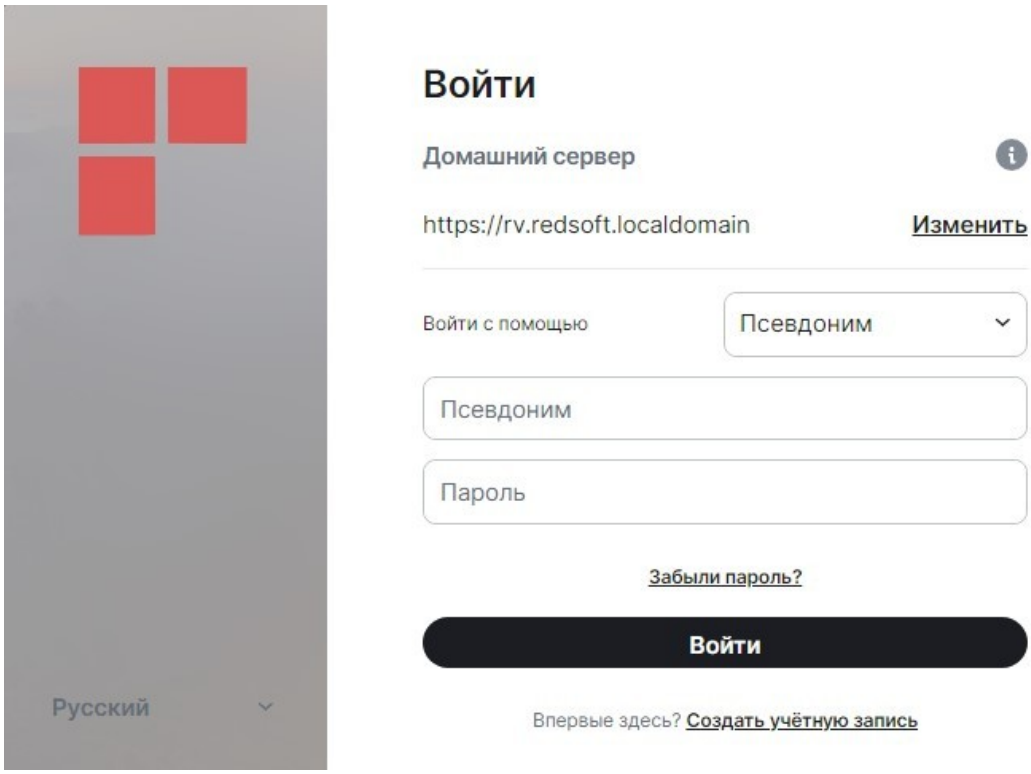

Рисунок 7 - Окно ввода учетных данных пользователя (РЕД ОС)

2.3 Операционная система Microsoft Windows

Процесс авторизации для данной операционной системы аналогичен процессу авторизации на РЕД ОС (см. п. 2.2 Операционная система РЕД ОС).

3 ОБЩАЯ ФУНКЦИОНАЛЬНОСТЬ

Корпоративный мессенджер Компании поддерживает множество функций, доступных в популярных продуктах этого класса. В их число входят следующие:

- секретные чаты;
- создание опросов;
- поддержка ботов;
- реакции на сообщения;
- отправка аудиосообщений;
- аудиозвонки и видеозвонки;
- аудиоконференции и видеоконференции (в текущей версии их поддержка находится в режиме тестирования);
- демонстрация экрана в ходе видеозвонка;
- поддержка каналов (через группы с выключенными правами размещения сообщений для всех участников, кроме администраторов);
- сохранённые сообщения (через группы);
- гибкое управление правами участников групп;
- экспорт чатов в файловую систему;
- противодействие бесследному удалению сообщений;
- редактирование написанного сообщения в течение определённого интервала времени;
- отображение времени прочтения последнего сообщения;
- цитирование отдельных частей (но не слов) сообщения;
- поиск по конкретному чату или группе;
- управление активными сессиями аккаунта;
- интеграция с другими мессенджерами (в текущей версии функция импорта сообщений из Telegram находится в режиме тестирования).

Для отдельных функций необходимо указать, каким образом ими следует пользоваться, ввиду недостаточной интуитивности процесса. В частности, создание чатов с новыми собеседниками и групп с множеством участников требует указания точных полных имён пользователей, которые выглядят так: @КороткоеИмяПользователя:rv.redsoft.org (правая часть была в том числе показана на рисунке 2 в пункте 2.1). Например: @surgeon:ether.redsoft.localdomain, @a.koptev:rv.redsoft.org, @m.musaev:rv.redsoft.org.

В текущей (на декабрь 2024 года) версии мессенджера на сервере отсутствует поддержка поиска пользователей по коротким именам. Также стоит отметить, что после создания чата с новым собеседником необходимо написать первое сообщение, чтобы адресат увидел запрос на вступление в новую беседу (который он при желании может отклонить).

4 ОБЕСПЕЧЕНИЕ ДОСТУПА К СООБЩЕНИЯМ

По умолчанию все чаты пользователя мессенджера являются секретными, и для прочтения сообщений на новом устройстве или после повторного входа в учётную запись, из которой был произведён выход, нужны ключи шифрования. Их можно сохранять ручным образом или автоматически, настроив резервное копирование на сервер. Во втором случае необходим т.н. «бумажный ключ» («security key», «recovery key», ключ безопасности), которым эти ключи шифруются в резервной копии. Также можно использовать парольную (мнемоническую) фразу, на основании которой автоматически генерируется данный ключ.

Ключ безопасности или парольную фразу необходимо вводить после авторизации с нового устройства или повторного входа в учётную запись, из которой был произведён выход. При наличии резервной копии на сервере все сообщения во всех чатах будут автоматически (для этого нужно выполнить определённое действие, описанное далее) дешифрованы, в противном случае (при её отсутствии) пользователю необходимо самостоятельно загрузить ранее выгруженные ключи шифрования.

Доступ к сообщениям с нового устройства может быть осуществлён при отсутствии резервной копии на сервере, а также ручным образом с помощью сохранённых ключей шифрования, если есть другая активная сессия, в которой имеются эти ключи. После подтверждения сеанса через QR-код (см. п. Подтверждение сеанса на новом устройстве) требуемые ключи будут автоматически переданы на новое устройство, где и произойдёт дешифрование сообщений.

4.1 Операционная система Android

Экспорт ключей шифрования в мобильном приложении доступен из раздела «Безопасность» (Рисунок 8-9). Там же они могут быть импортированы. Необходимо отметить, что ключи шифрования периодически обновляются, и для обеспечения возможности прочтения последних сообщений необходимо иметь актуальный набор данных ключей. Поэтому представляется целесообразным всегда включать резервное копирование, настройка которого описана далее в этом пункте.

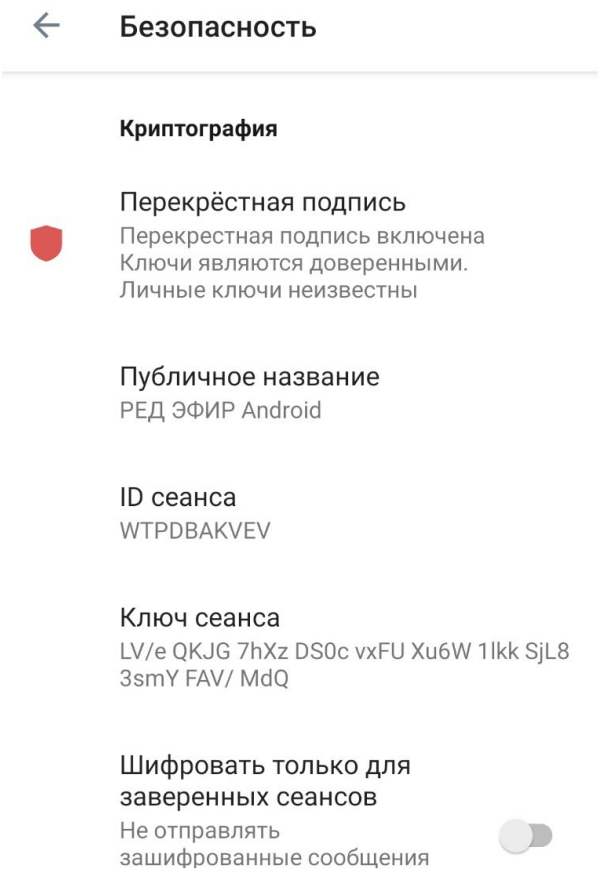

Рисунок 8 - Настройки ключей шифрования

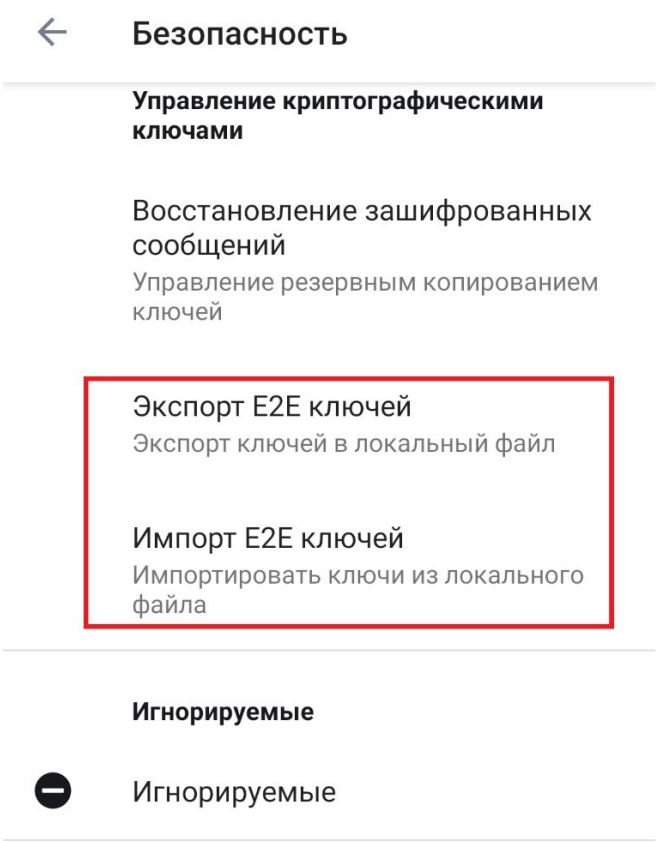

Рисунок 9 - Экспорт и импорт ключей шифрования (Android)

Ключи шифрования хранятся в файлах на устройстве, которые могут быть скопированы с него на любой носитель информации или переданы через другой мессенджер, чего следует избегать, несмотря на наличие парольной защиты, устанавливаемой на эти файлы. После выбора элемента меню «Экспорт E2E ключей» открывается окно определения имени файла и его расположения, показанное на рисунке 10.

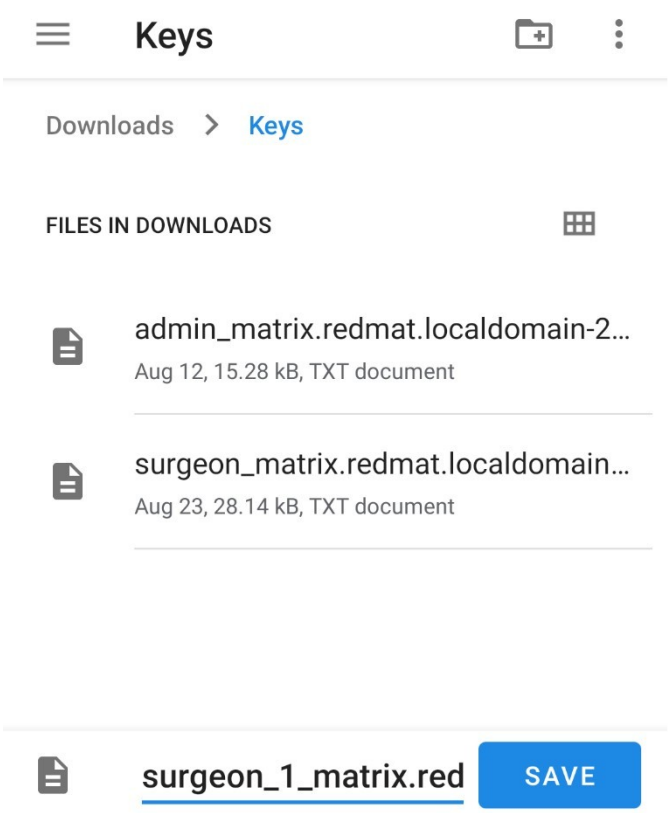

Рисунок 10 - Выбор имени файла с ключами шифрования (Android)

После нажатия кнопки «SAVE» открывается окно ввода пароля, защищающего содержимое файла (Рисунок 11). Строго рекомендуется задавать пароль, соблюдая парольную политику Компании, и не хранить его рядом с файлом ключей шифрования. Этот пароль не должен совпадать с паролем учётной записи.

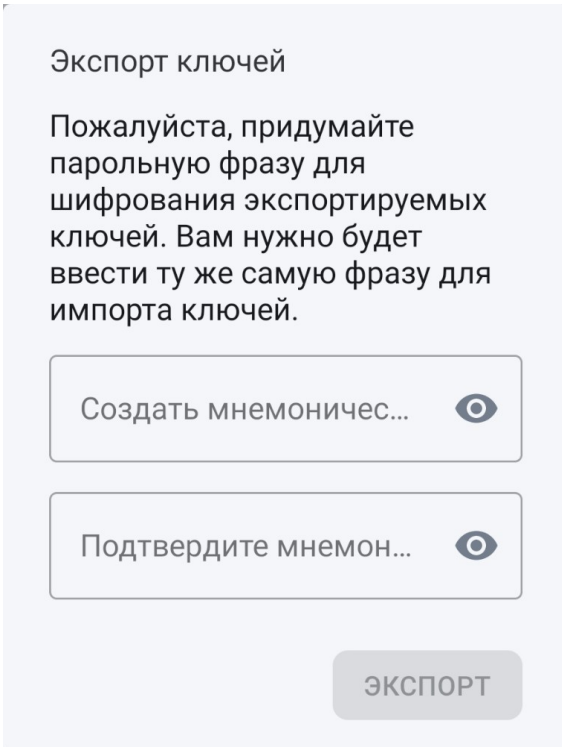

Рисунок 11 - Указание пароля файла с ключами шифрования (Android)

Необходимо отметить, что в текущей (на декабрь 2024 года) версии мессенджера нет поддержки одновременной работы в нескольких аккаунтах. Поэтому для переключения между ними требуется выходить из используемой в данный момент учётной записи (Рисунок 12). В случае, если ранее на этом устройстве не выполнялась настройка резервного копирования ключей шифрования, это будет предложено сделать (Рисунок 13-14).

Внимание! Если нет активных сеансов на других устройствах, и данный шаг будет пропущен, то доступ к переписке будет утерян!

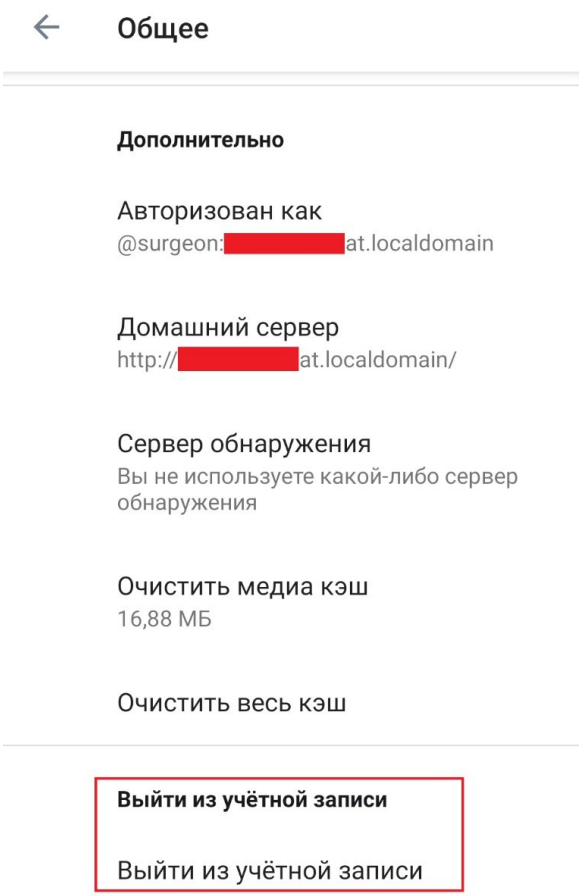

Рисунок 12 - Выход из текущей учетной записи

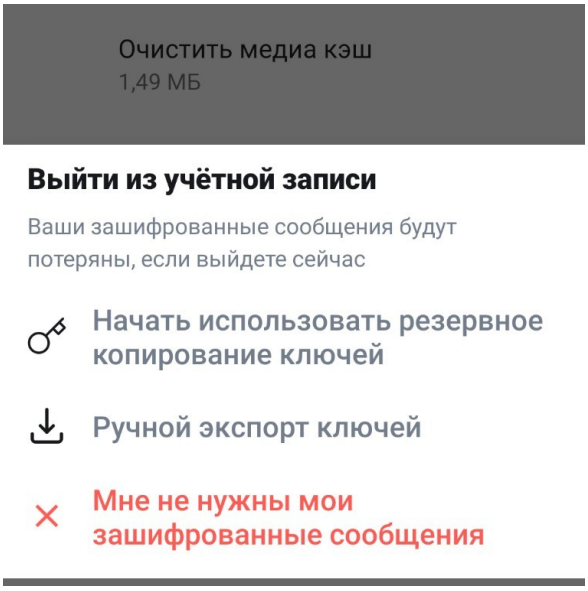

Рисунок 13 - Первое предупреждение о необходимости сделать копию ключей шифрования

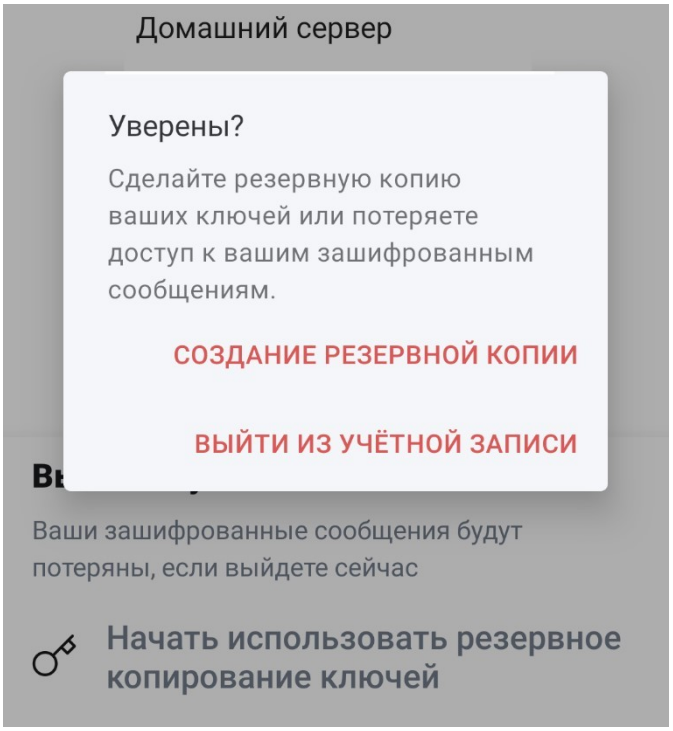

Рисунок 14 - Второе предупреждение о необходимости сделать копию ключей шифрования

После выбора опции использования резервного копирования будет предложено сразу создать ключ безопасности или указать парольную фразу (Рисунок 15-16), на основе которой он будет сгенерирован. После непродолжительного ожидания будет сформирован ключ безопасности (Рисунок 17), который можно сохранить на устройство.

Внимание: утечка ключа безопасности или парольной фразы может позволить злоумышленнику прочесть сообщения пользователя при получении доступа к его учётной записи!

После завершения описанной процедуры отобразится окно, предлагающее выйти из учётной записи (Рисунок 18).

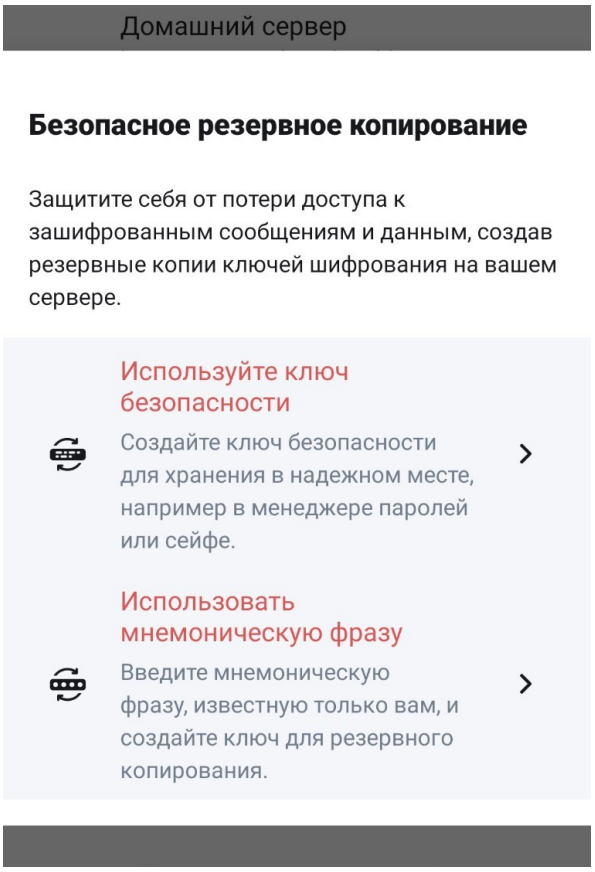

Рисунок 15 - Окно выбора секрета для защиты резервной копии (Android)

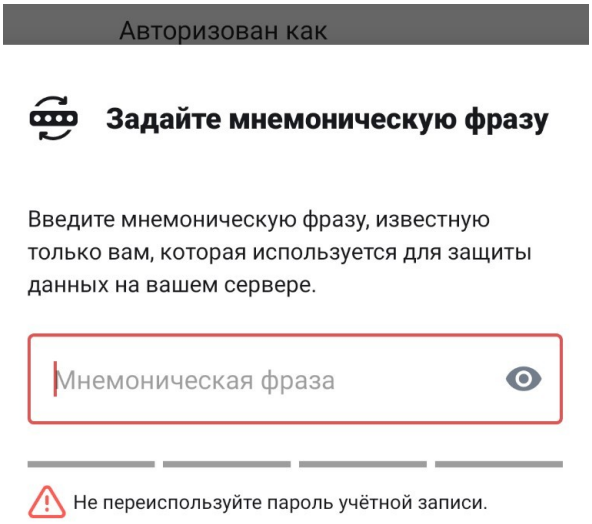

Рисунок 16 - Окно ввода парольной фразы

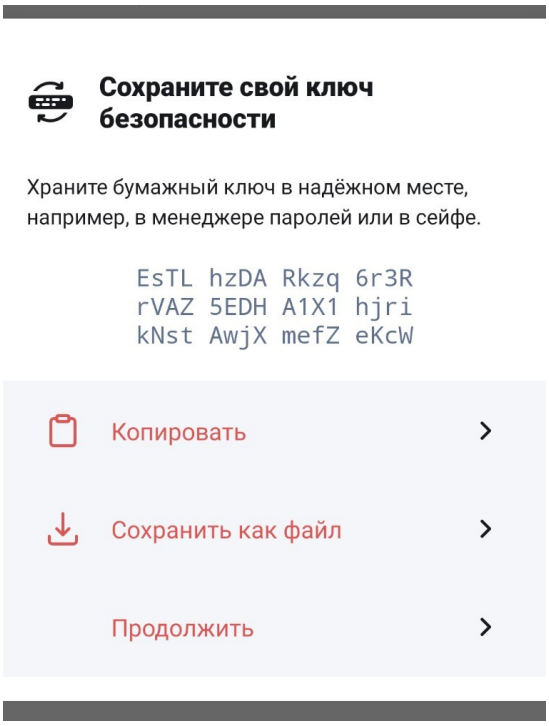

Рисунок 17 - Созданный ключ безопасности (Android)

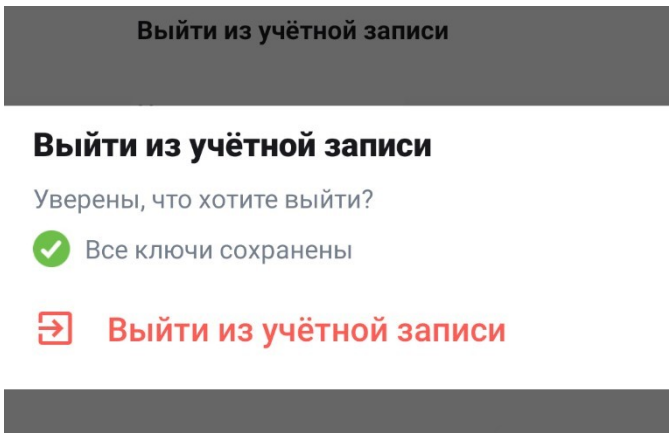

Рисунок 18 - Финальное окно выхода из учётной записи после создания резервной копии ключей шифрования

После повторной авторизации или после входа в учётную запись на другом устройстве при отсутствии возможности провести верификацию с другой активной сессии необходимо пройти верификацию ранее экспортированным ключом безопасности или парольной фразой. После этого для дешифрования сообщений в чатах необходимо войти в подраздел «Восстановление зашифрованных сообщений» раздела «Безопасность» настроек приложения мессенджера и нажать кнопку «Восстановить из резервной копии» (Рисунок 19). **При этом строго не рекомендуется удалять эту копию нажатием соответствующей кнопки!**

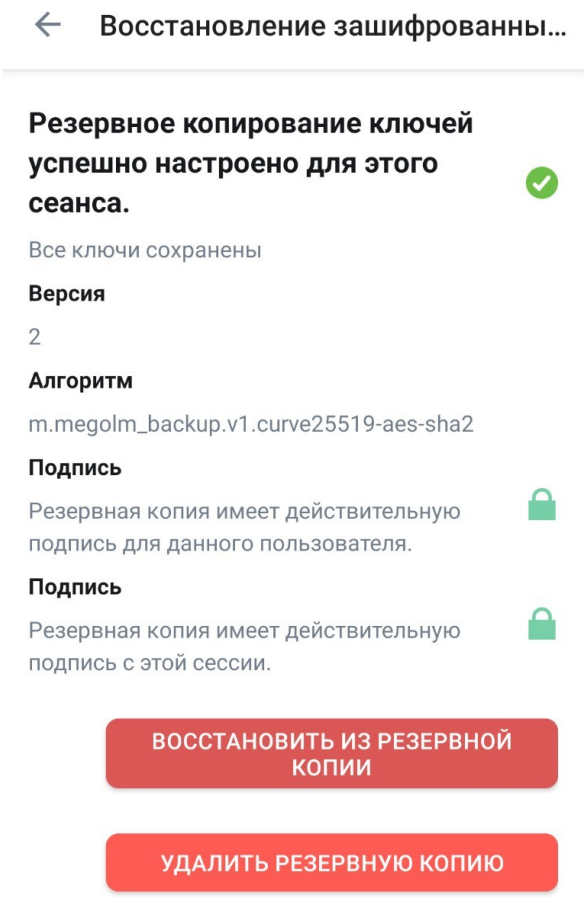

Рисунок 19 - Восстановление ключей шифрования из резервной копии на сервере

4.2 Настольные операционные системы

Экспорт и импорт ключей шифрования в настольных версиях приложения, так же как и в мобильной, доступен из раздела «Безопасность» (Рисунок 20). После выбора функции экспорта открывается окно, показанное на рисунке 21 (аналогичное изображённому на рисунке 10 для мобильной версии).

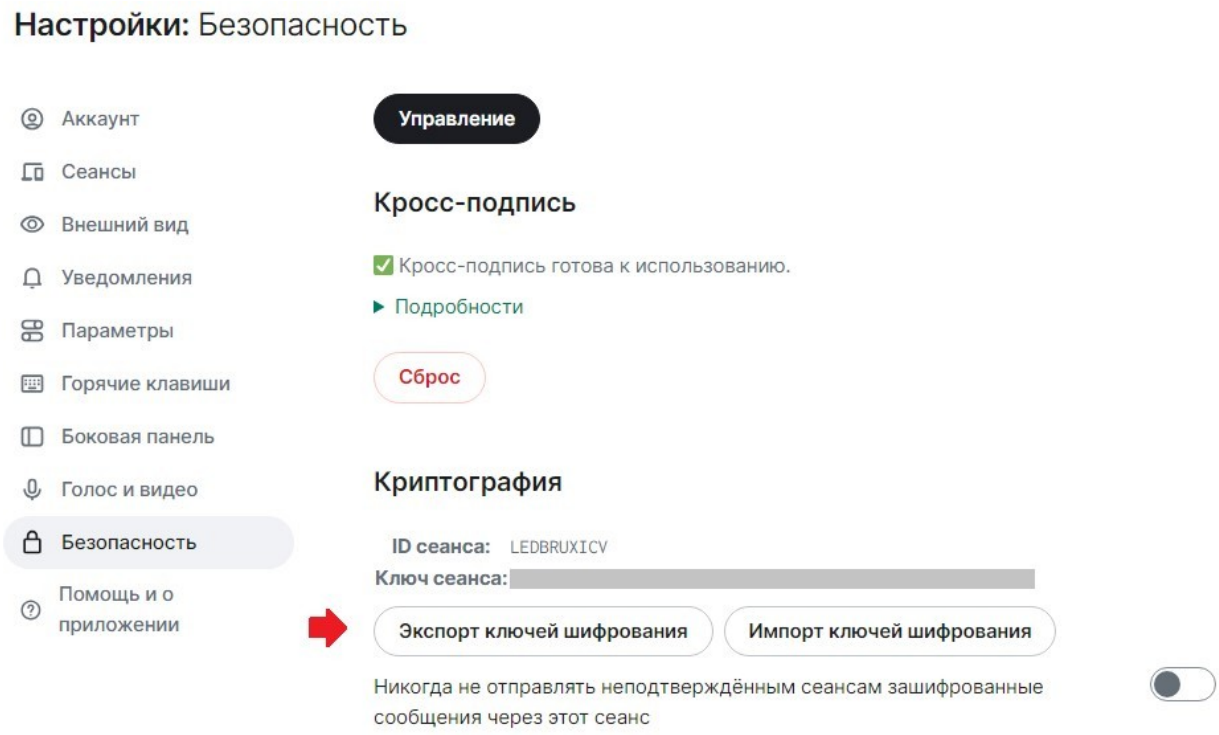

Рисунок 20 - Экспорт и импорт ключей шифрования (РЕД ОС)

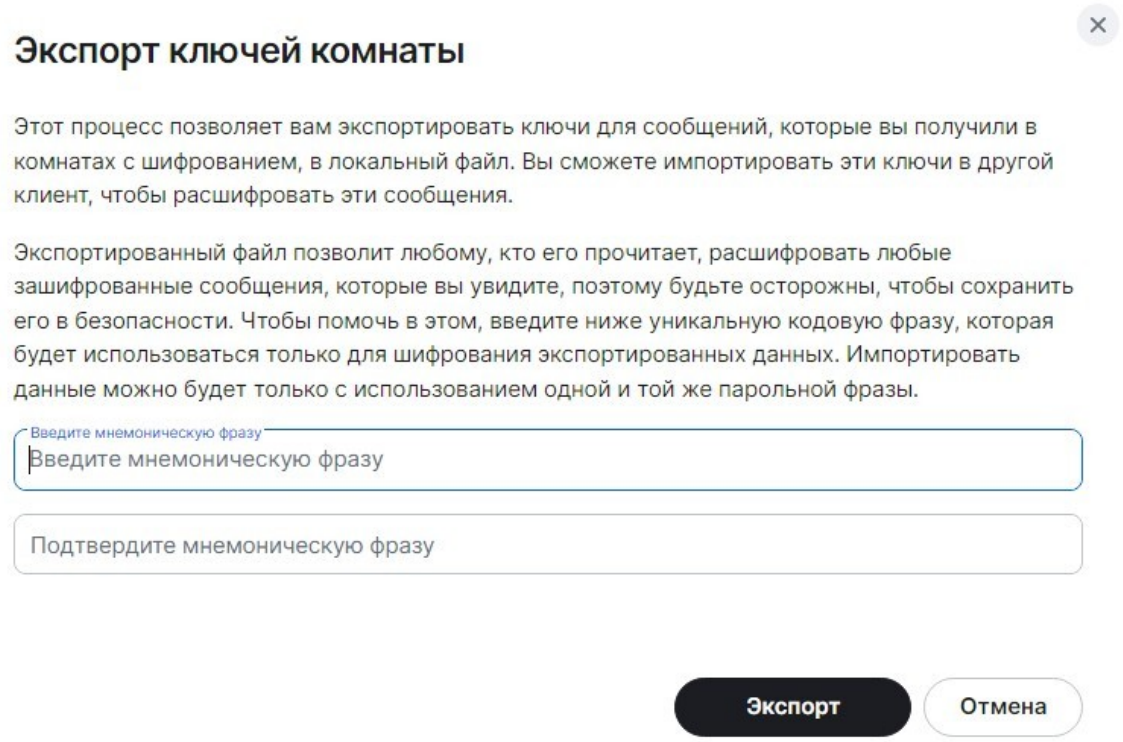

Рисунок 21 - Указание пароля файла с ключами шифрования (РЕД ОС)

После задания пароля файла откроется диалоговое окно выбора его имени (Рисунок 22). Данный файл будет хранить ключи на момент его создания.

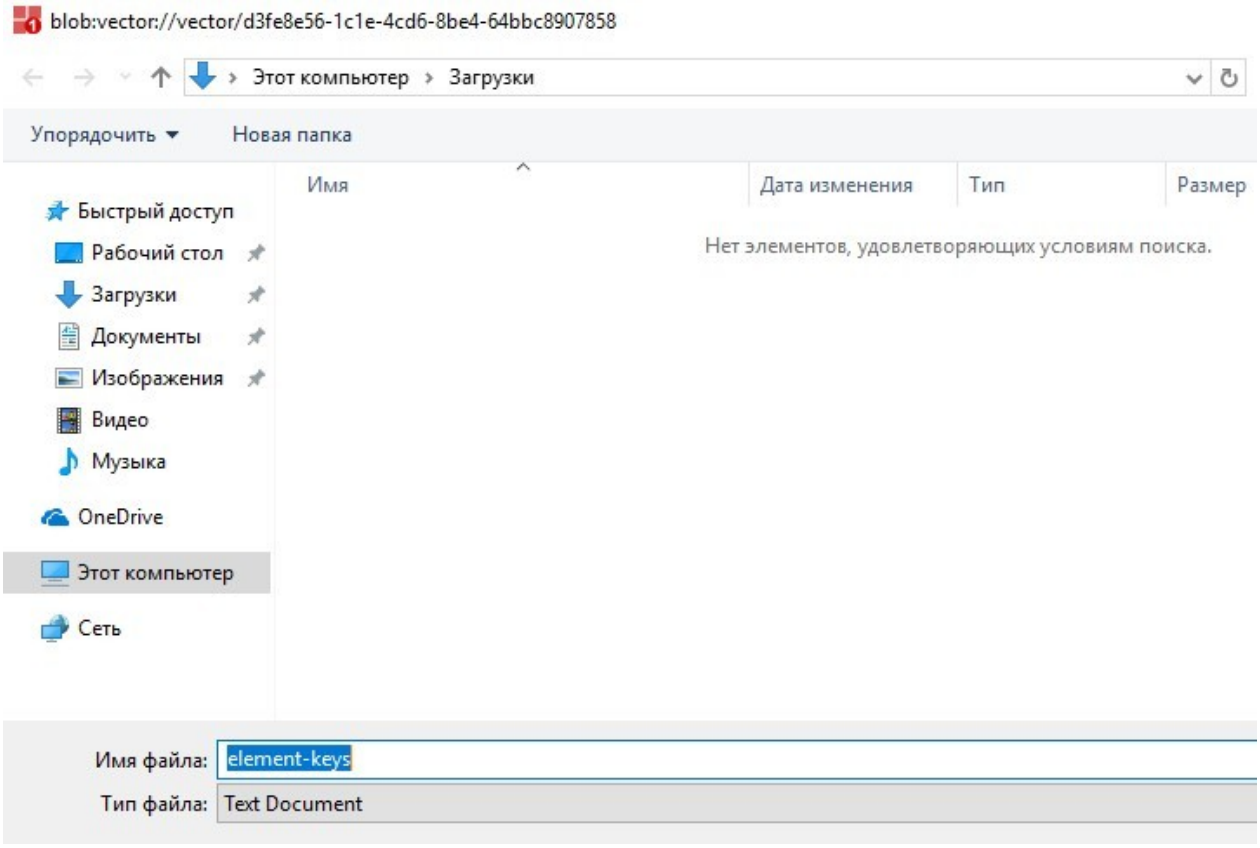

Рисунок 22 - Выбор имени файла с ключами шифрования (Microsoft Windows)

Резервное копирование ключей шифрования, информация о котором подробно изложена в п. 4.1 (**подлежит обязательному изучению!**), доступно из раздела «Безопасность» настроек приложения (Рисунок 23). При первом входе в учётную запись пользователю будет сразу же предложено настроить данную функцию (Рисунок 24).

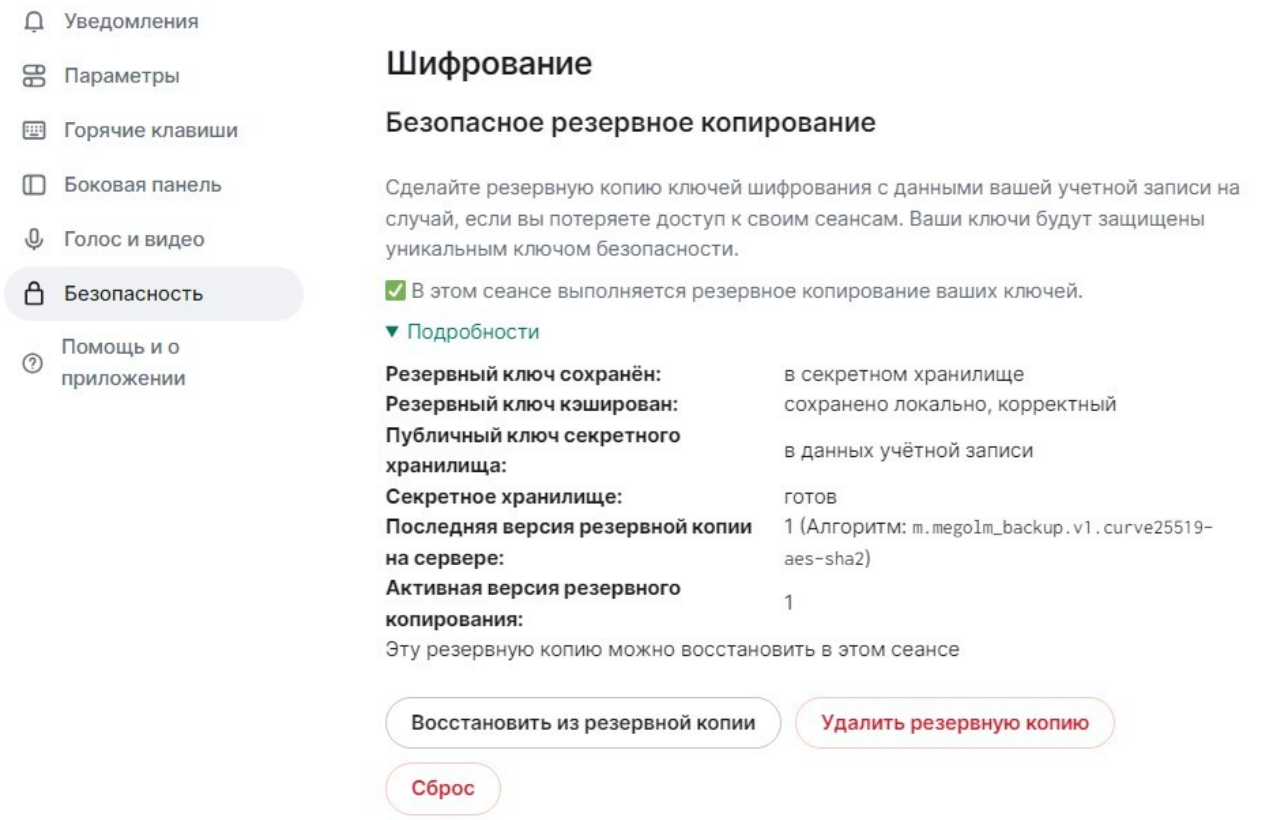

Рисунок 23 - Управление резервной копией на сервере

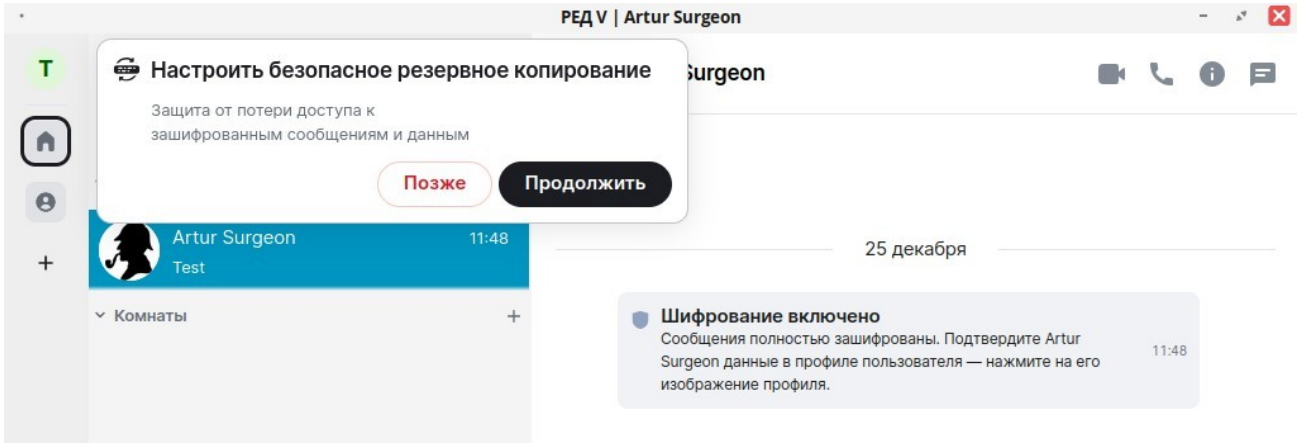

Рисунок 24 - Предложение сделать копию ключей шифрования

Процесс настройки резервного копирования ключей шифрования для настольных версий приложения мессенджера существенным образом не отличается от такового для мобильной версии. На рисунке 25 показаны доступные варианты защиты копии (аналогично представленным на рисунке 15). Получившийся в итоге ключ предлагается скопировать или сохранить в файловую систему (Рисунок 26). Так же как и для мобильной версии приложения, **строго не рекомендуется удалять резервную копию**. Стоит отметить, что версия для РЕД ОС поддерживает параметр profile комадной строки, новое значение которого создаёт новую пользовательскую сессию. Таким образом реализуется возможность переключения между различными аккаунтами или даже одновременного их использования.

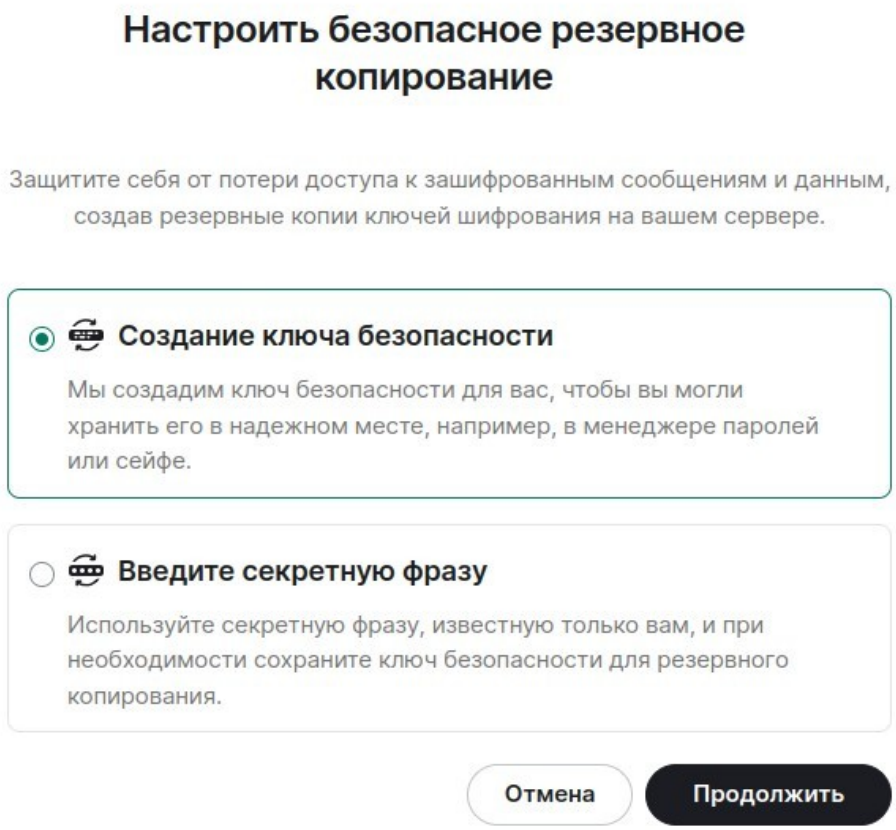

Рисунок 25 - Окно выбора секрета для защиты резервной копии (РЕД ОС)

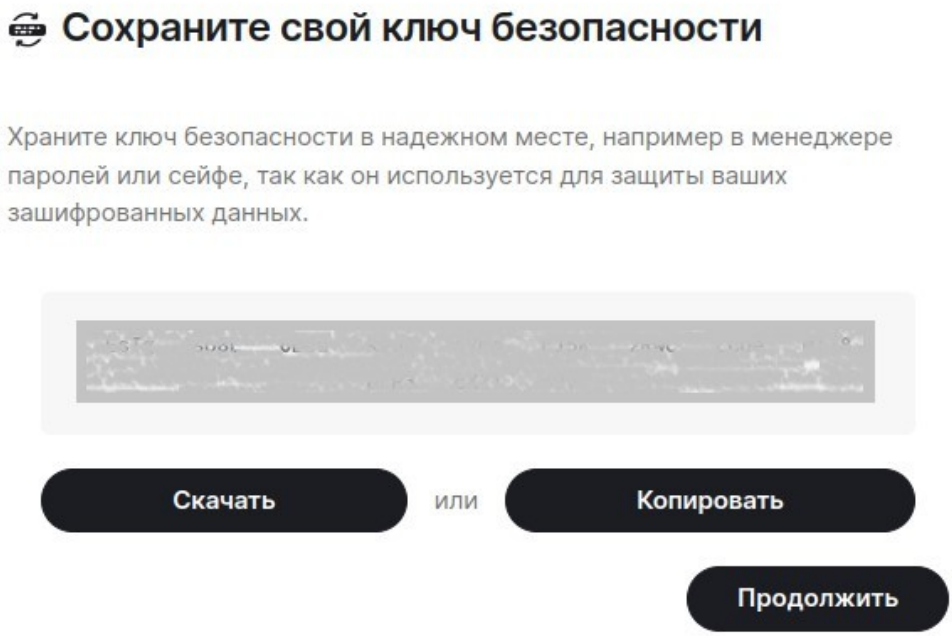

Рисунок 26 - Созданный ключ безопасности (РЕД ОС)

5 ПОДТВЕРЖДЕНИЕ СЕАНСА НА НОВОМ УСТРОЙСТВЕ

При входе в учётную запись мессенджера на новом устройстве необходимо верифицировать его в одной из активных сессий на других устройствах. Необходимо отметить, что после выхода из учётной записи и повторного входа в неё на этом же устройстве также требуется выполнить данную операцию. Если это было единственное устройство, то верификация возможна только с помощью ранее сохранённого ключа безопасности (см. п. Обеспечение доступа к сообщениям).

5.1 Операционная система Android

После открытия нового сеанса в верхней части основного окна появляется навязчивое предложение, показанное на рисунке 27. Нажатие на него открывает диалоговое окно, изображённое на рисунке 28. В нём красным цветом выделена опция верификации в одной из других активных сессий (при их наличии), синим – опция верификации ключом безопасности или парольной фразой (см. п. Обеспечение доступа к сообщениям). Третья опция позволяет задать новый ключ безопасности, потеряв доступ к сообщениям.

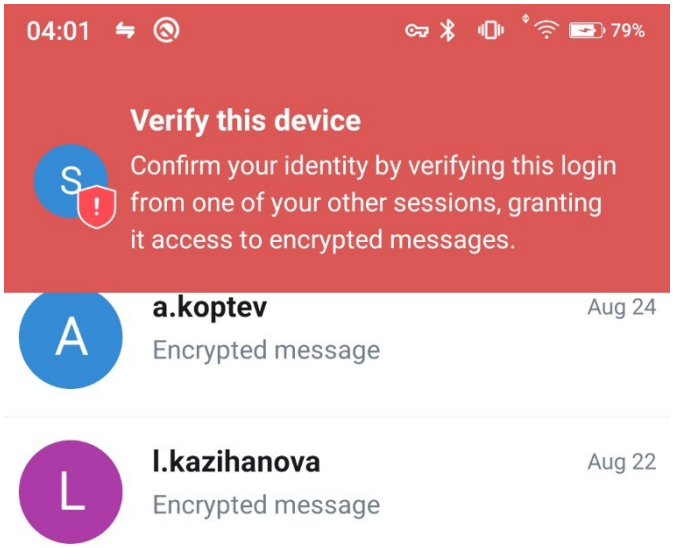

Рисунок 27 - Предложение пройти верификацию устройства

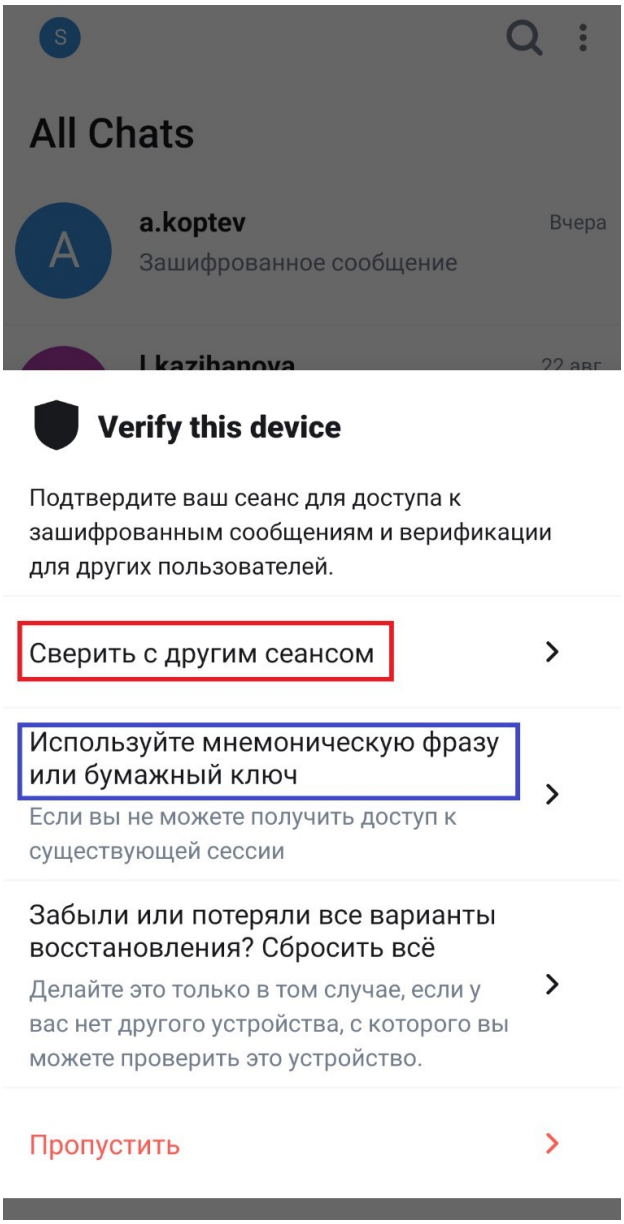

Рисунок 28 - Окно выбора опций верификации (Android)

Верификация в одной из других активных сессий требует наличия доступа к таковой. При выборе этой опции откроется окно, показанное на рисунке 29. После этого в другой сессии отобразится соответствующий запрос (Рисунок 30). Пользователю необходимо его подтвердить, после чего на новом устройстве откроется окно с предложением отсканировать QR-код или сверить случайную последовательность картинок (Рисунок 31).

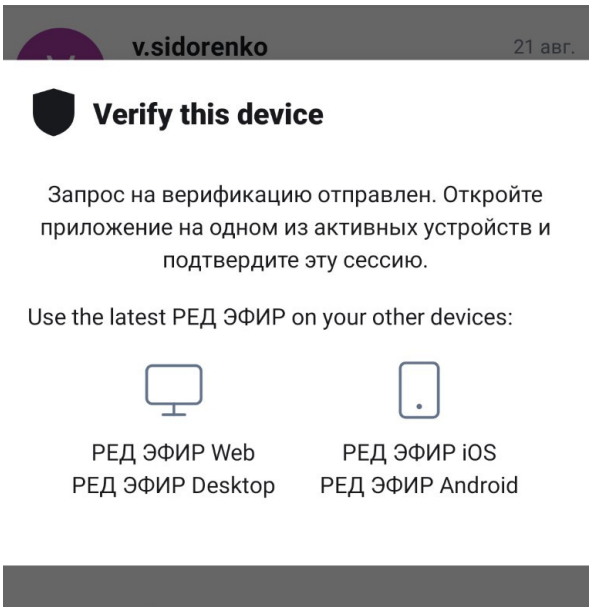

Рисунок 29 - Окно ожидания подтверждения начала процесса верификации

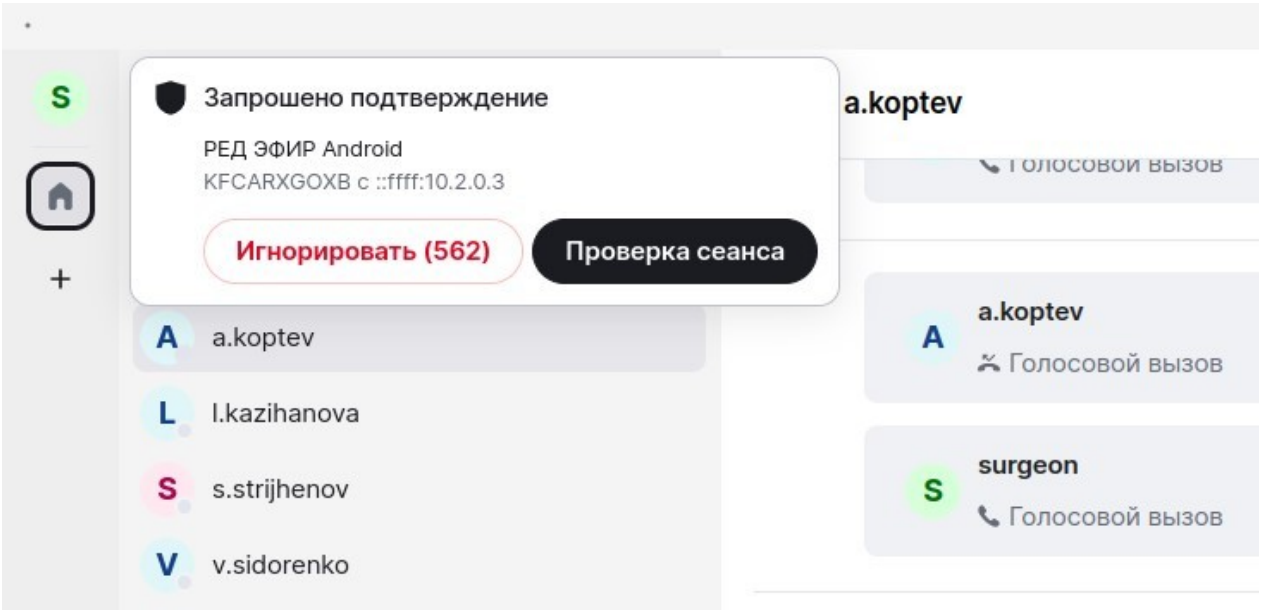

Рисунок 30 - Запрос на верификацию в другой активной сессии (на примере версии приложения мессенджера под РЕД ОС)

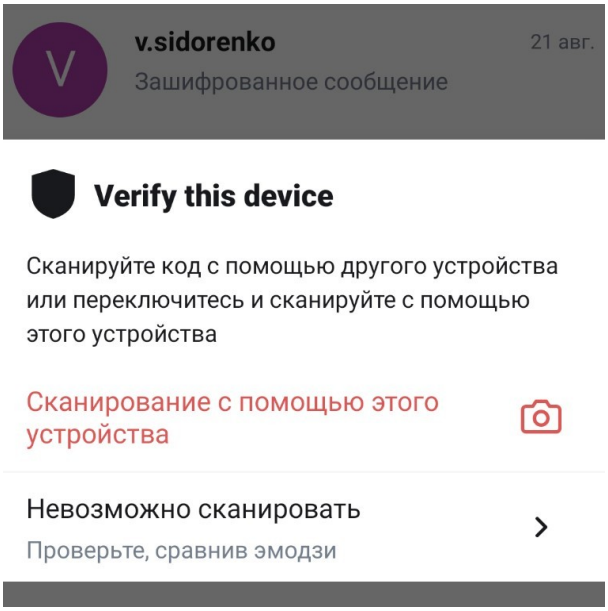

Рисунок 31 - Окно выбора способа верификации

После выбора способа верификации на новом устройстве в другой сессии отобразится окно с информацией, которую необходимо сверить, при этом данный выбор можно изменить (Рисунок 32).

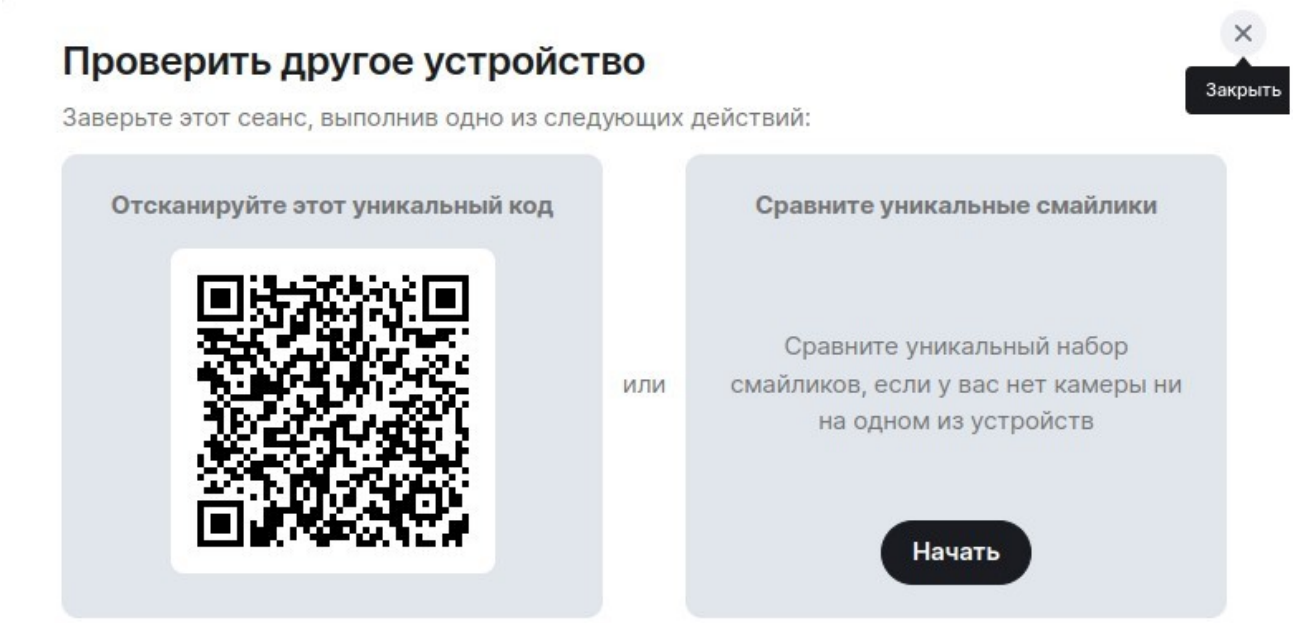

Рисунок 32 - Информация для верификации в другой активной сессии

Процесс верификации с помощью QR-кода и последовательности картинок несколько отличается: в первом случае после успешного сканирования в другой сессии отображается диалоговое окно с щитом (Рисунок 33). Если такой же щит (его цвет не важен) показывается на новом устройстве (Рисунок 34), то верификация прошла успешно, и можно нажать кнопку «Да». После этого появится возможность закрыть окно щита на новом устройстве, нажав кнопку «Готово» (Рисунок 35).

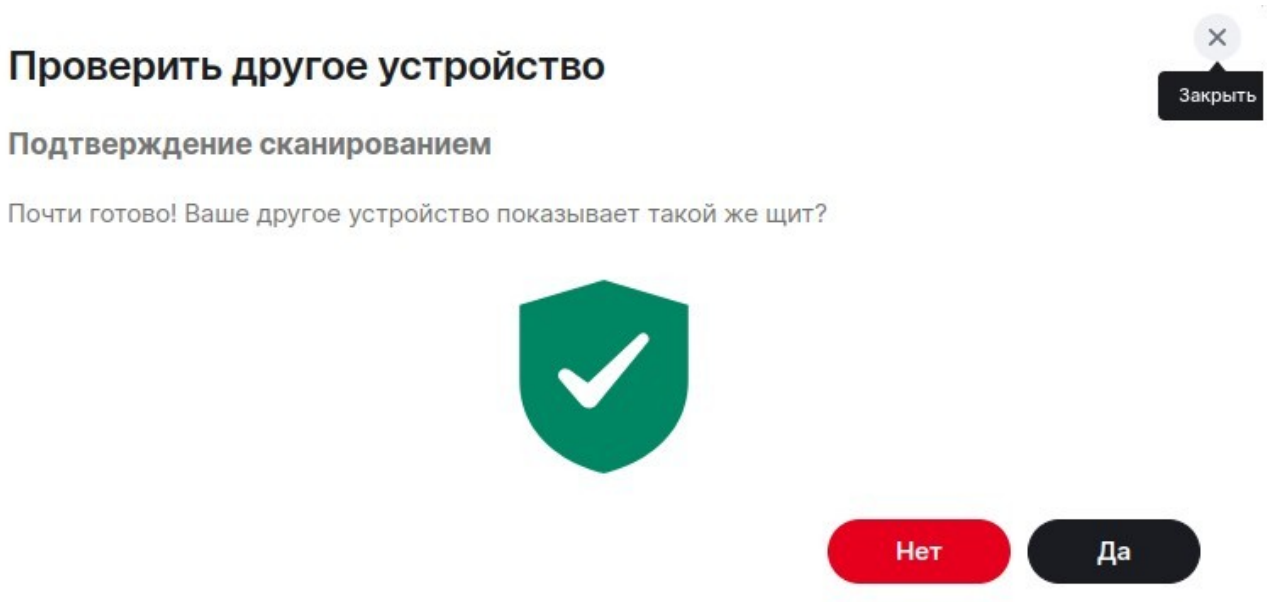

Рисунок 33 - Подтверждение в другой сессии после сканирования QR-кода

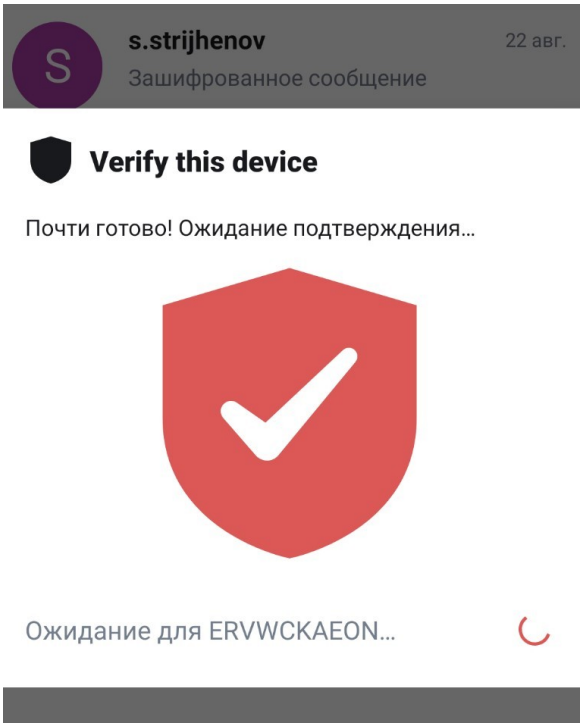

Рисунок 34 - Ожидание подтверждения верификации

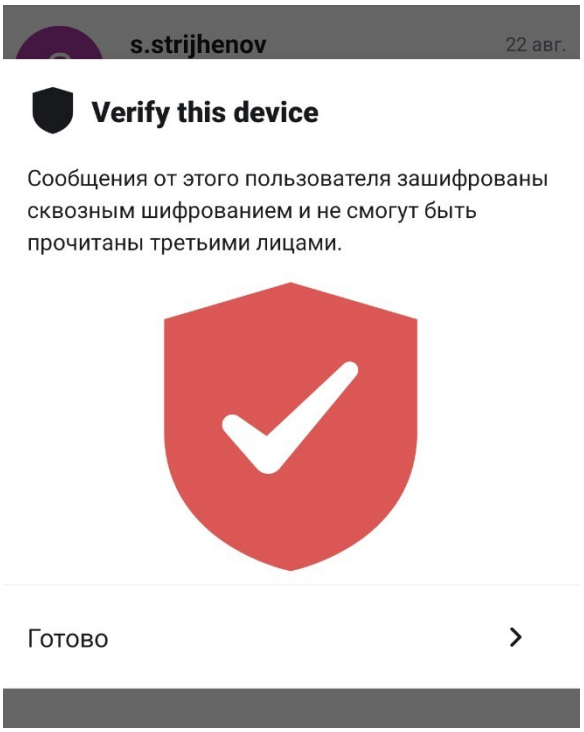

Рисунок 35 - Успешное завершение верификации

Процесс верификации по последовательности картинок устроен несколько проще: в ходе него нужно подтвердить на каждом устройстве совпадение их порядка (Рисунок 36), после чего окно, изображённое на рисунке 35, появится на обоих экранах.

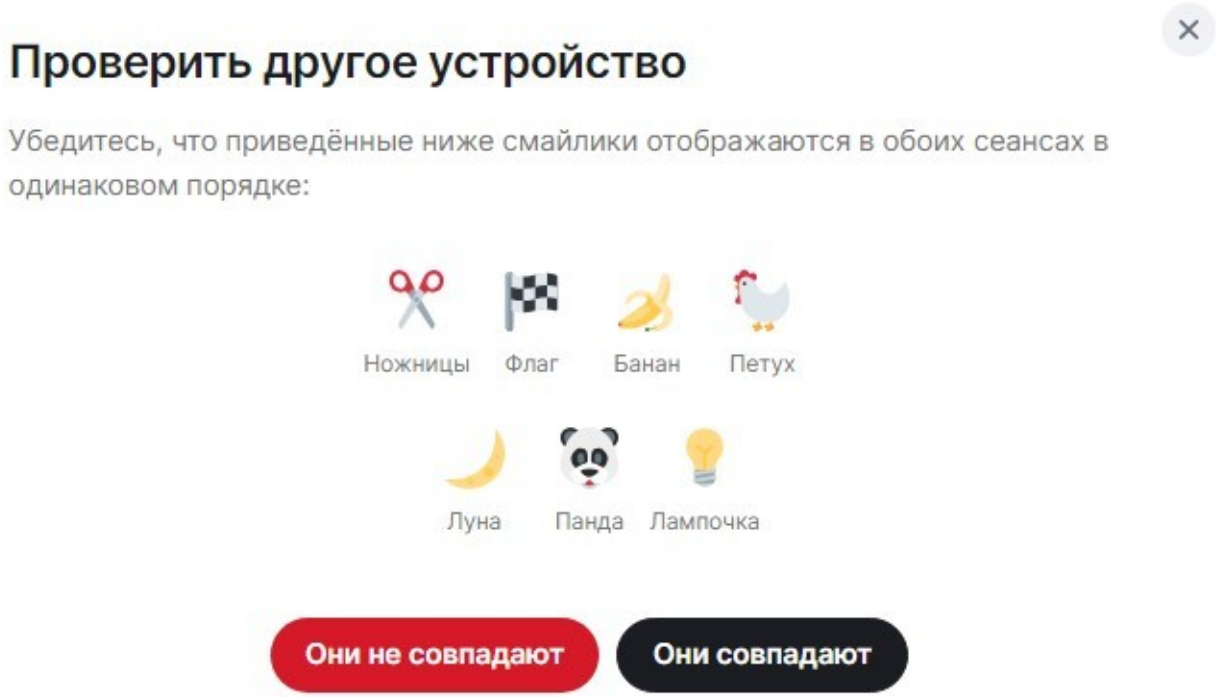

Рисунок 36 - Отображаемая последовательность картинок для верификации (версия приложения мессенджера под ОС Microsoft Windows)

5.2 Настольные операционные системы

Графический интерфейс в настольных версиях приложения отличается от такового для мобильной версии. Сразу после ввода учётных данных появляется окно, изображённое на рисунке 37. Кнопка «Сверить с другим сеансом» в нём будет присутствовать, только если такой сеанс существует, в противном случае потребуется ключ безопасности или парольная фраза.

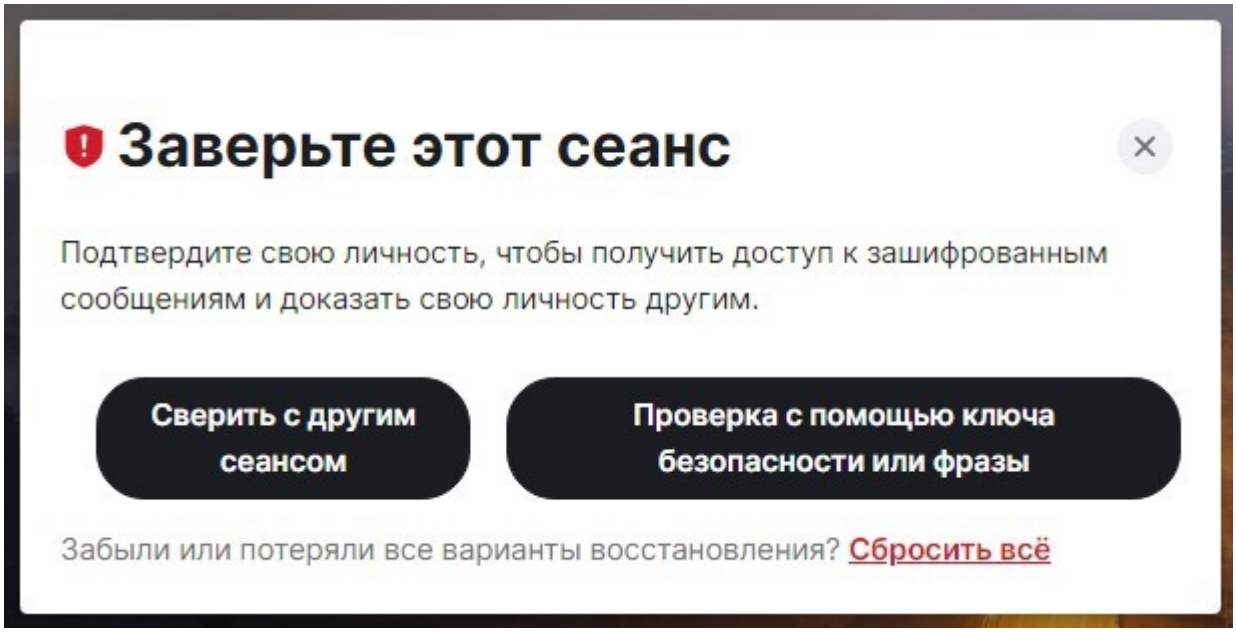

Рисунок 37 - Окно выбора опций верификации (Microsoft Windows)

6 НАСТРОЙКА УВЕДОМЛЕНИЙ О ПРИШЕДШИХ СООБЩЕНИЯХ

Настройка уведомлений о пришедших сообщениях требуется только на мобильных устройствах под управлением операционных систем Android и РЕД ОС М. Связано это с особенностями функционирования мобильных приложений.

Распространяемая сборка мобильной версии приложения мессенджера поддерживает два способа получения уведомлений – через отдельное приложение ntfy и посредством фоновой синхронизации (Рисунок 38). Поддержка push-уведомлений компании Google отсутствует, что обеспечивает высокий уровень безопасности коммуникаций. Первый способ ввиду сложности настройки в данном руководстве пользователя не предлагается и не описан.

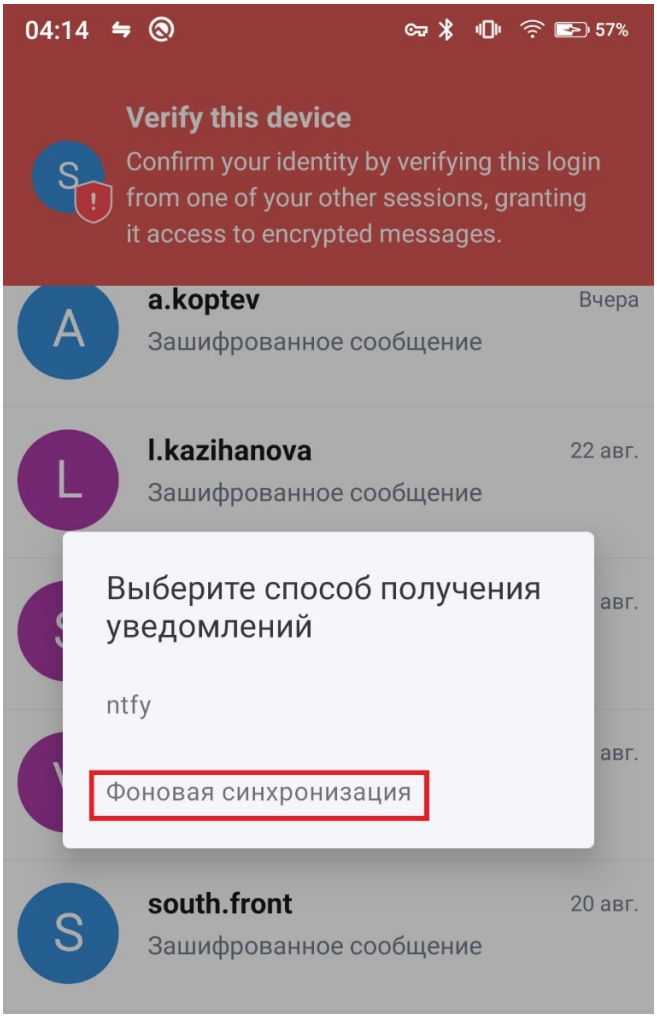

Рисунок 38 - Выбор способа получения уведомлений после авторизации

Второй способ получения уведомлений требует внесения изменений в настройки ОС Android. Предварительно необходимо открыть раздел «Уведомления» в приложении мессенджера. На рисунке 39 показаны его ключевые настройки. При первоначальной конфигурации необходимо сменить режим фоновой синхронизации.

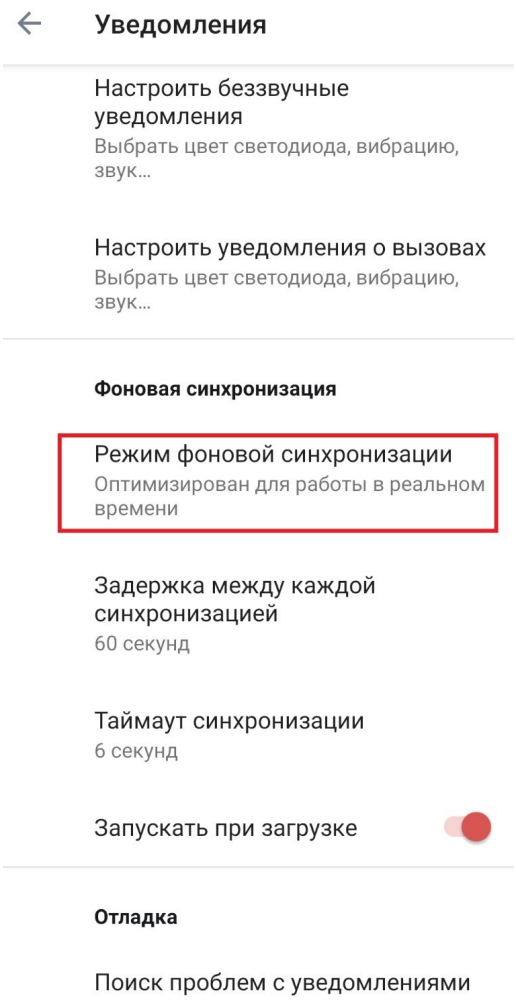

Рисунок 39 - Основные настройки уведомлений

На рисунке 40 показаны два основных режима фоновой синхронизации. Для своевременной доставки уведомлений о сообщениях и звонках рекомендуется использовать второй режим, оптимизированный для работы в реальном времени. При первом его выборе будет отображено модальное окно, изображённое на рисунке 41. В нём нужно нажать на кнопку «ALLOW».

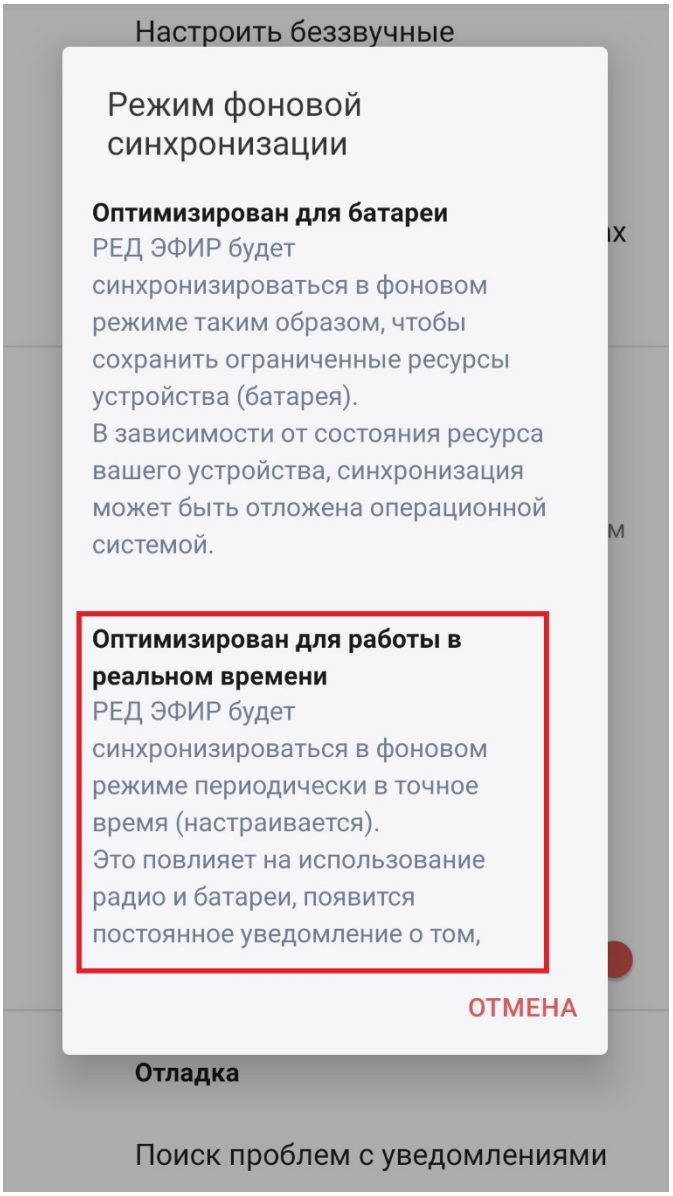

Рисунок 40 - Доступные режимы фоновой синхронизации

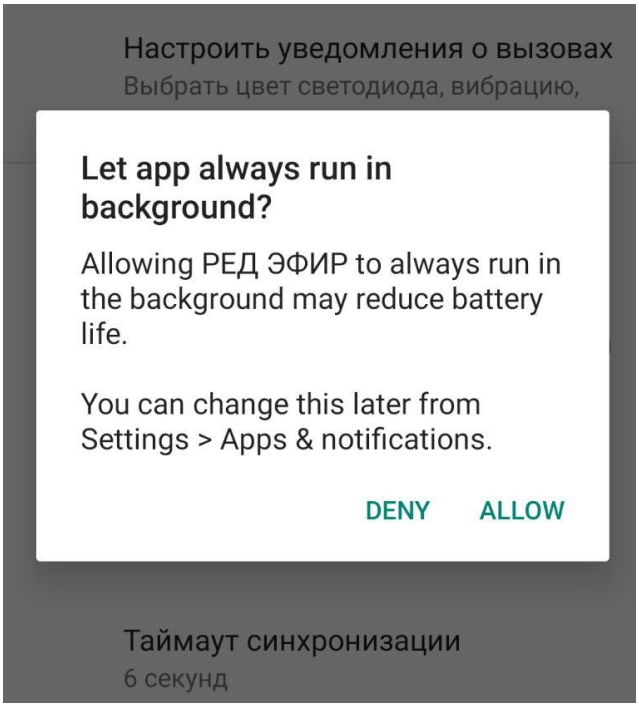

Рисунок 41 - Окно разрешения работы приложения в фоновом режиме

После внесения изменений в конфигурацию приложения необходимо убедиться, что системные настройки его энергопотребления соответствуют рекомендуемым. Для этого необходимо открыть подраздел «Apps & notifications» раздела «Settings» операционной системы Android. В нём нужно найти приложение мессенджера и перейти в его настройки батареи. Их необходимо изменить так, как показано на рисунке 42. Для этого нужно нажать на характеристику «Battery optimization», выбрать в открывшемся списке «All apps» («Все приложения»), после чего найти приложение мессенджера (оно, вероятно, будет в конце списка) и изменить её значение на «Don’t optimize» («Не оптимизировать»).

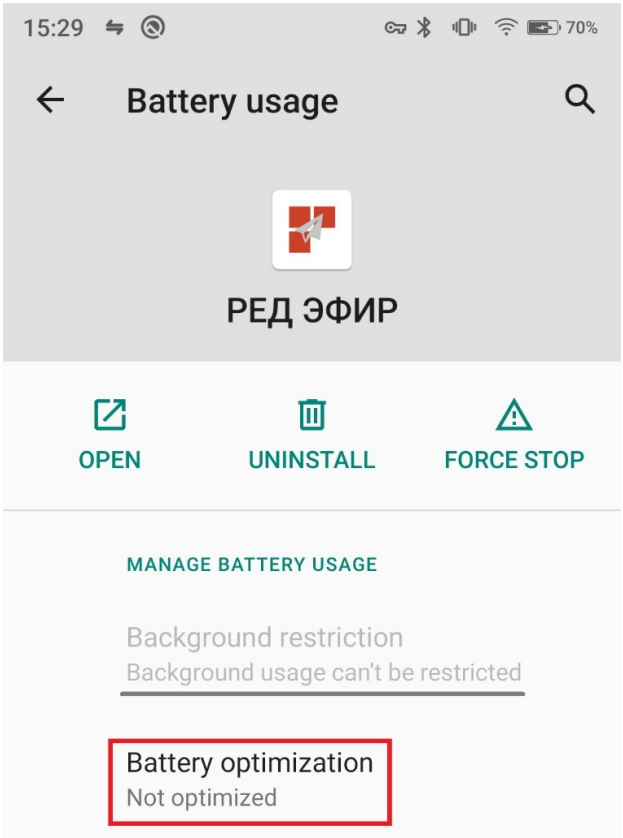

Рисунок 42 - Рекомендуемые настройки энергопотребления мессенджера

После внесения этих изменений на экране блокировки на постоянной основе будет отображаться уведомление «Listening for notifications» (Рисунок 43). В случае появления новых сообщений или поступления звонков соответствующие уведомления будут отображаться на этом же экране.

В текущей (на август 2024 года) версии приложения это наиболее быстрый в настройке и удобный в эксплуатации вариант доставки уведомлений. Впоследствии в РЕД ОС М будет добавлена поддержка собственных push-уведомлений.

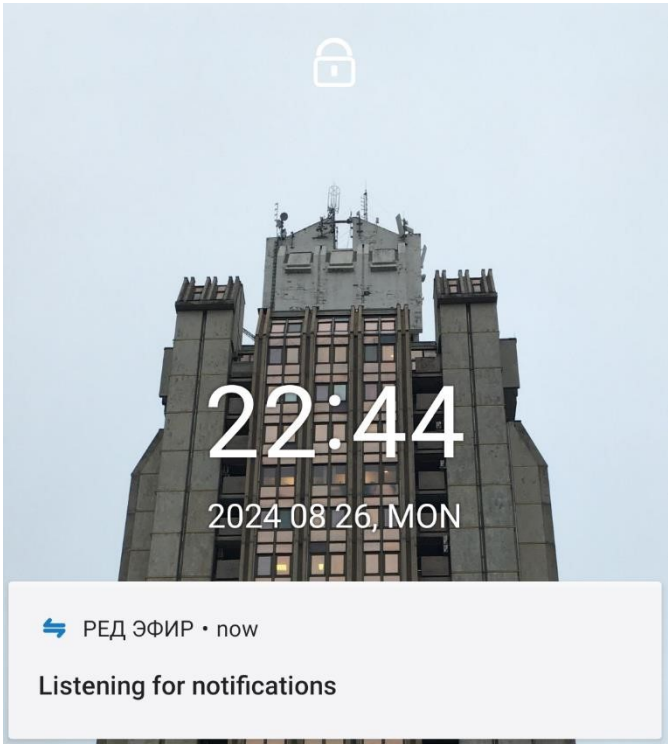

Рисунок 43 - Уведомление об ожидании поступления уведомлений

7 ПРОЧИЕ ФУНКЦИИ БЕЗОПАСНОСТИ

Помимо перечисленных в предыдущих разделах, приложение мессенджера поддерживает дополнительные функции безопасности, состав которых несколько отличается для разных платформ.

7.1 Операционная система Android

В мобильной версии приложения можно определить PIN-код и время бездействия, после которого его необходимо вводить. На рисунке 44 показано окно ввода заданного ранее кода. Настроить его можно в разделе «Безопасность» вместе с некоторыми другими полезными функциями (Рисунок 45).

Рисунок 44 - Окно ввода PIN-кода

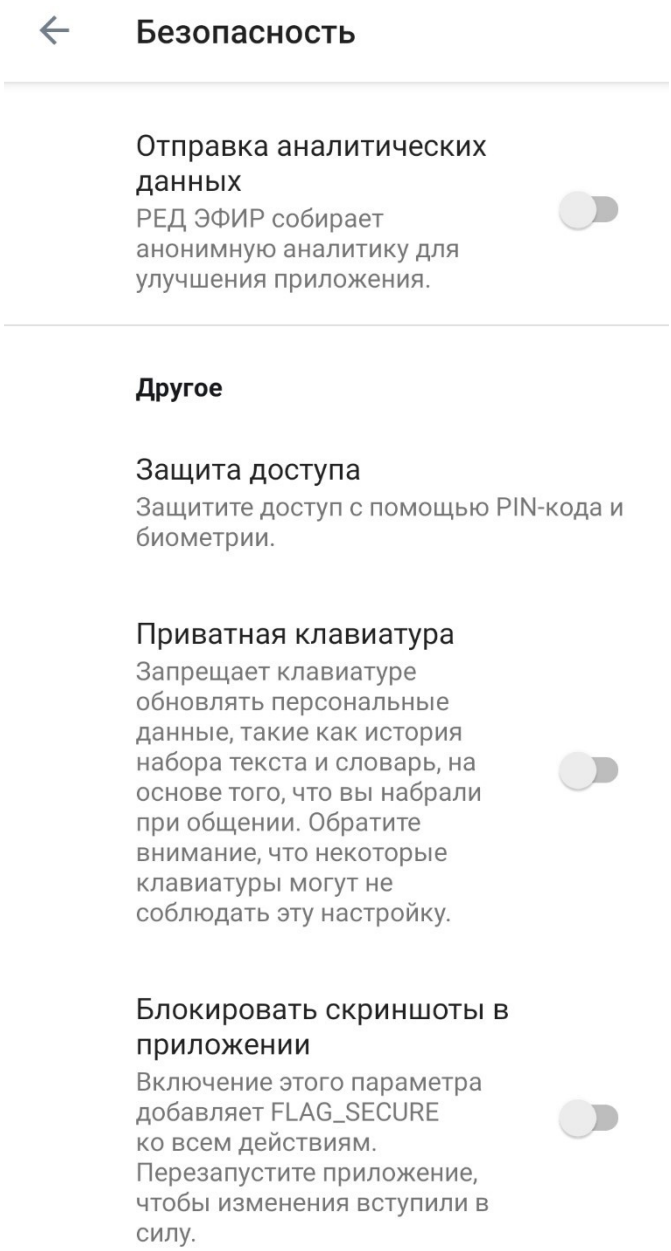

Рисунок 45 - Настройки раздела «Безопасность»

Так же как и в других мессенджерах, в РЕД V есть возможность управления активными сессиями, в частности, завершать их при возникновении подозрений о компрометации учётной записи. На рисунке 46 показано несколько таких сессий в разделе «Управление сеансами».

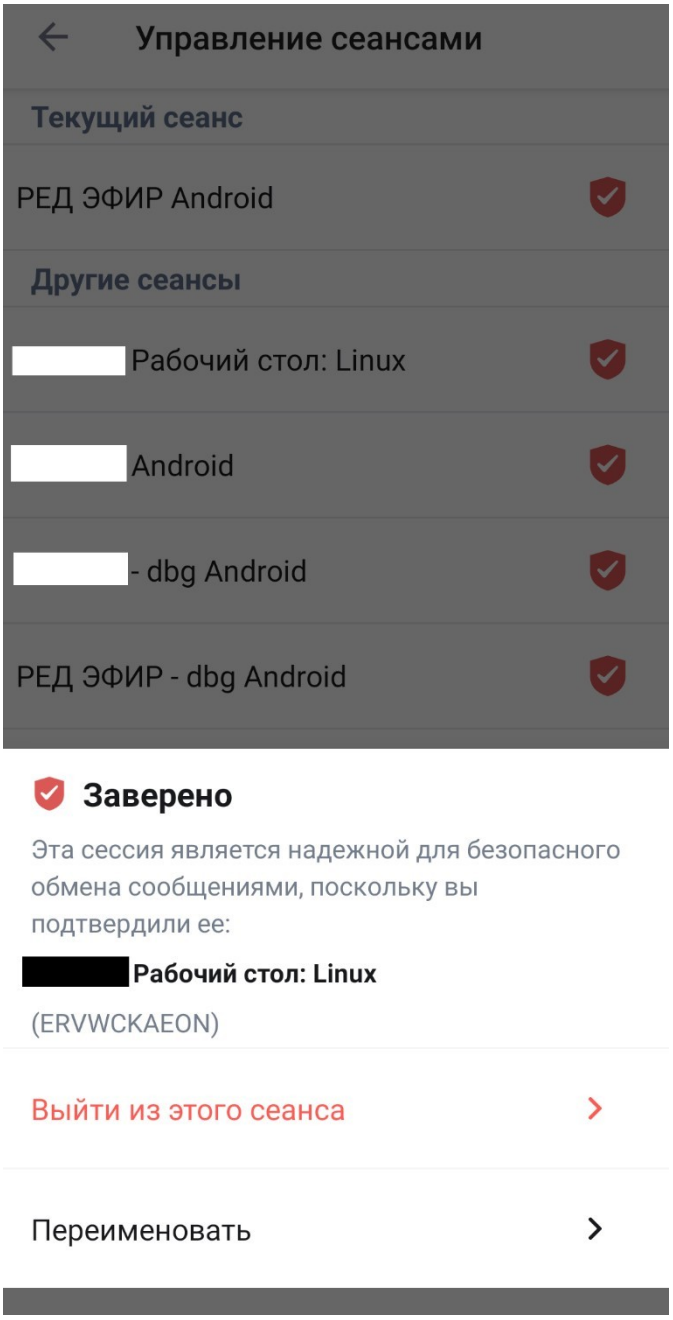

Рисунок 46 - Окно управления активными сессиями (Android)

7.2 Настольные операционные системы

Интерфейс управления открытыми сеансами в настольных версиях мессенджера РЕД V отличается от такового для мобильной версии. Он представлен на рисунке 47.

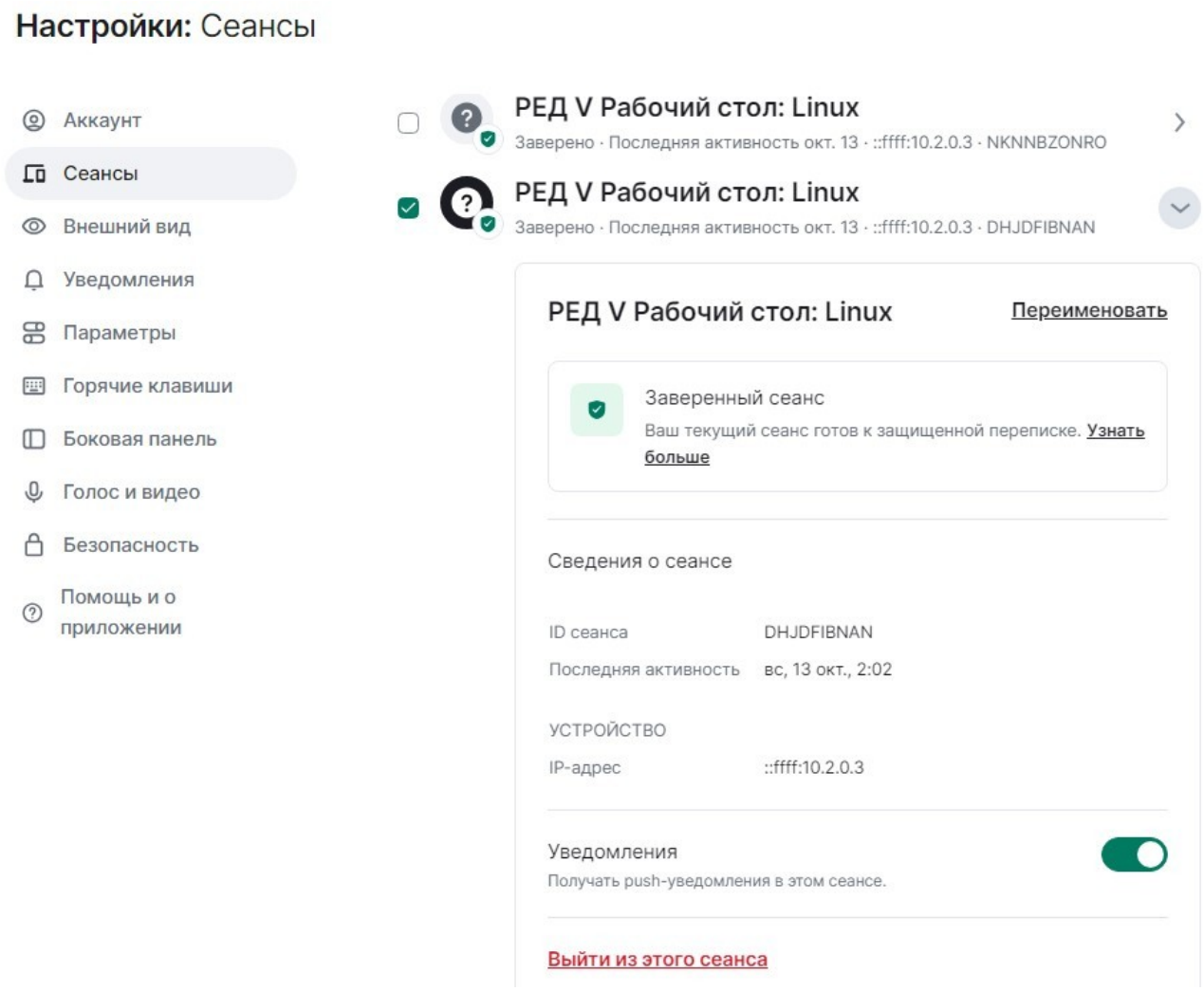

Рисунок 47 - Окно управления активными сессиями (Microsoft Windows)

Выделяющейся функцией безопасности в настольных версиях приложения является возможность управления авторством пересылаемых сообщений. На рисунке 48 показана соответствующая опция в диалоговом окне, открываемом при пересылке выбранных пользователем сообщений. Пересланное сообщение с сокрытым авторством выглядит так, как изображено на рисунке 49.

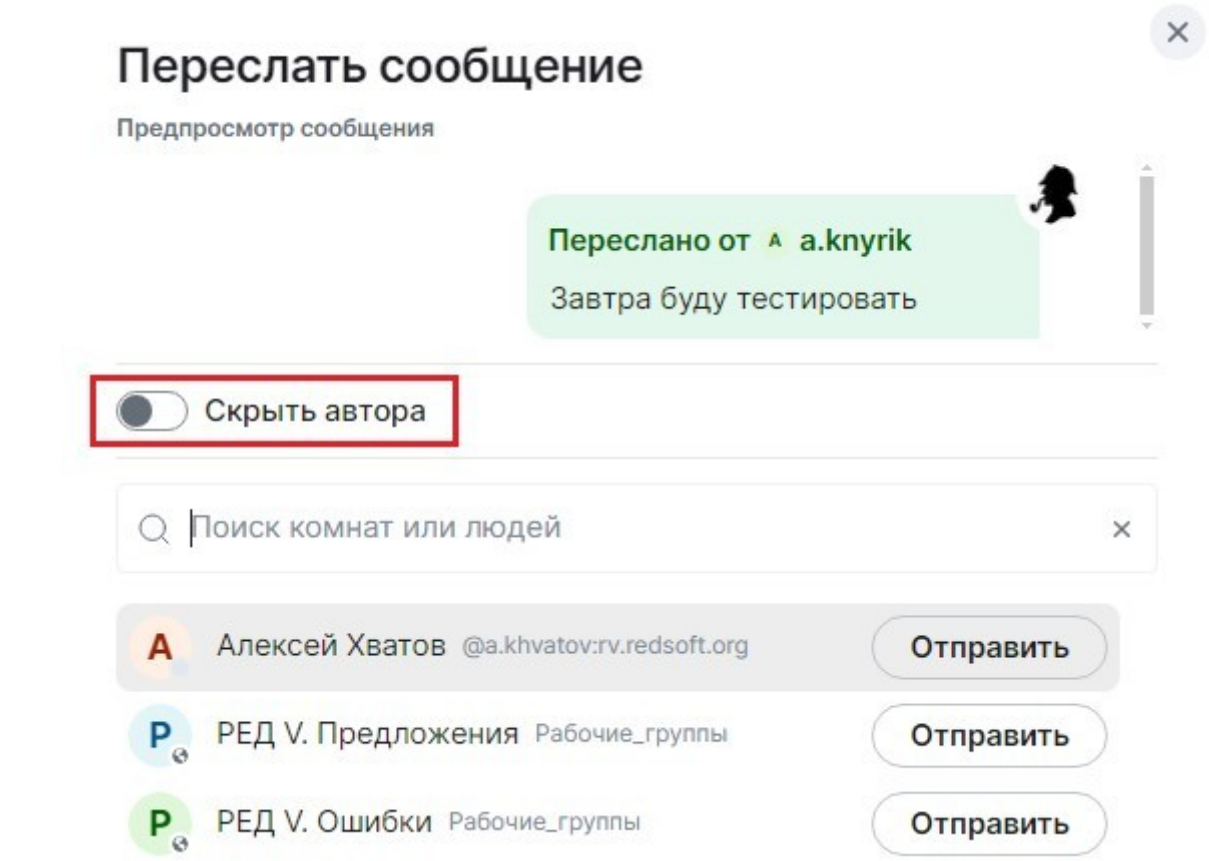

Рисунок 48 - Окно управления пересылкой сообщений

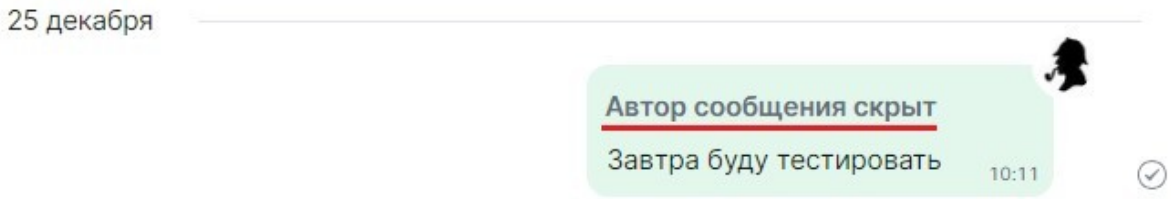

Рисунок 49 - Скрытое авторство пересланного сообщения

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ версии	*Дата изменения*	*Автор*	*Состав изменений*
1.0	28.02.2025	Антонова Ю.В.	Первоначальная версия документа.