**Балтийский Государственный Технический Университет "ВОЕНМЕХ"**

Информационная безопасность и защита информации

**Реферат по теме (задаче)**

Информационная безопасность мессенджеров

Отметка о зачете «_____»
_____ Ю.В.Лычагин
«___» _____ 2019 г.

Выполнил магистрант гр. И8М32

_____ / Дровосеков К.С./
«___» _____ 2019 г.

Санкт-Петербург 2019г

# Оглавление

## 1. Введение

Парадоксально, но факт: при всем разнообразии мессенджеров выбирать их обычно не приходится — люди просто пользуются тем же, чем их друзья и знакомые. Но что, если секретность действительно важна? В этой работе мы пройдемся по списку современных мессенджеров и посмотрим, какие гарантии защиты есть у каждого из них.

Большинство людей ответят на Какой мессенджер вы считаете самым надежным?» ответят «Telegram»

Составим список мессенджеров и рассмотрим с точки зрения безопасности. В список пошли как популярные, так и перспективные в плане безопасности программы. Углубляться в техническую сторону мы будем настолько, насколько это необходимо для среднего пользователя, не дальше.

## 2. Критерии выбора защищенного мессенджера

Распространяется ли исходный код мессенджера на условиях одной из свободных лицензий? Если да, то ведется ли разработка открытым методом? Насколько тесно разработчики взаимодействуют с сообществом? Все это важно учитывать при выборе.

### 2.1 Степень централизации

Здесь возможен один из трех вариантов:

- централизованный — требует сервера, возможно заблокировать. Пример: VK, Telegram, Facebook;
- федеративный — сеть из серверов, которые общаются друг с другом. Каноничные примеры: Email, Jabber (XMPP), Riot Matrix;
- децентрализованный (имеется в виду P2P) — каждый клиент является одновременно и сервером.

### 2.2 Возможность анонимной регистрации и использования

Для некоторых сервисов телефон может понадобиться только для защиты от спама при регистрации, соответственно, очень просто использовать сервисы аренды номеров для SMS.

В остальных случаях мессенджер плотно привязан к телефону. Это плохо тем, что если не включена двухфакторная аутентификация, то при получении доступа к этому номеру можно зайти в аккаунт и слить все данные. Но даже если двухфакторка включена, все равно остается возможность удалить все данные с аккаунта. Ну и конечно, регистрация по паспорту

Но не все так плохо. Есть мессенджеры, которые позволяют

регистрироваться с использованием почтового ящика или учетной записи в социальной сети. Есть и такие, где учетную запись можно создать в самом мессенджере без привязки к чему-то.

### 2.3 Наличие End-to-End Encryption (E2EE)

Некоторые мессенджеры имеют такую функцию по умолчанию, в других ее можно включить, но есть и те, где сквозного шифрования просто нет.

### 2.4 Синхронизация E2EE-чатов

Опять же эта функция пока что встречается не так часто, как хотелось бы. Ее наличие сильно упрощает жизнь.

### 2.5 Уведомление о необходимости проверки отпечатков E2EE

При старте E2EE-чатов некоторые мессенджеры предлагают проверить отпечатки собеседников, другие не предлагают это открыто. Но не все мессенджеры имеют функцию проверки отпечатков.

**Запрет делать скриншот секретного чата**

Не самая полезная функция, потому что для обхода запрета достаточно, например, иметь под рукой второй телефон.

**Групповые E2EE-чаты**

Групповые E2EE-чаты обычно не такая уж необходимая функция, но весьма удобная. Правило «больше двух — говори вслух» стоит оставить для детей.

**Уведомление о необходимости проверки отпечатков E2EE в групповых чатах**

При добавлении нового собеседника, с которым не сверены отпечатки, в секретный групповой чат не все мессенджеры предлагают проверить его

отпечатки. Из-за такого упущения теряется смысл секретных чатов.

### 2.6 Защита социального графа

Некоторые мессенджеры собирают информацию о контактах пользователя и другую метаинформацию, например кому звонил пользователь, как долго разговаривал.

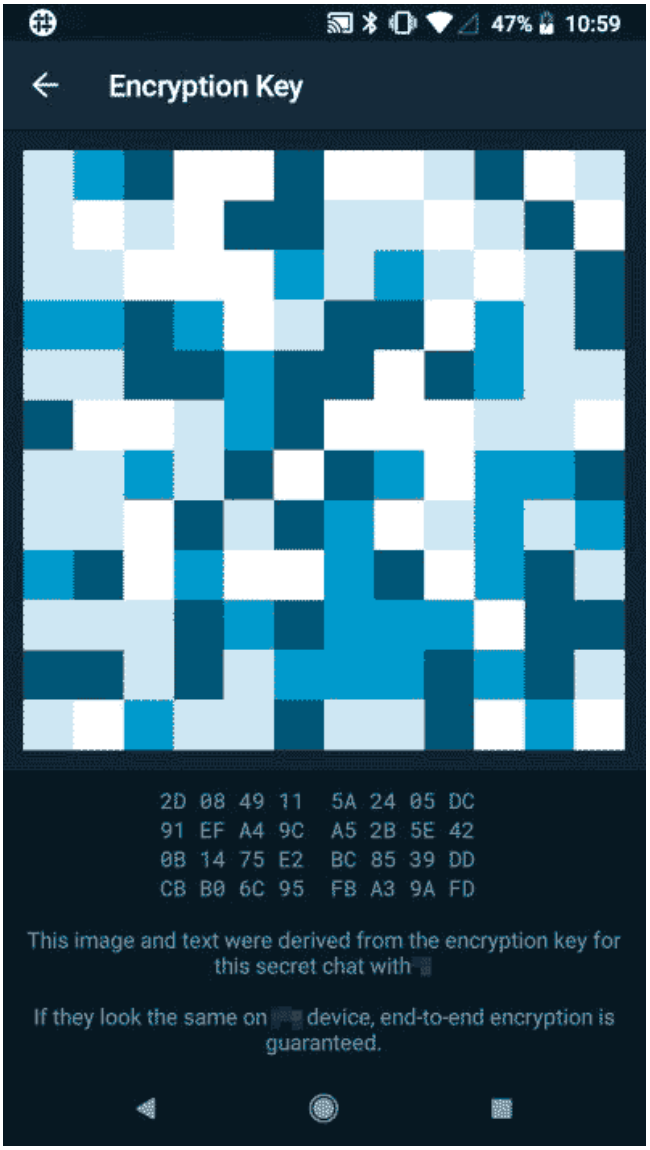
Мы выбрали лишь часть критериев, которые могут сыграть роль при выборе мессенджера. Существуют и другие, но не всегда они связаны с безопасностью. Группа ученых из европейских университетов неплохо разложила все по полочкам в работе Obstacles to the Adoption of Secure Communication Tools. Также всегда полезно знакомиться с результатами независимого аудита, если они есть. Например, в случае с Signal такой аудит проводился.

## 3. Обзор защищённых мессенджеров

### 3.1 Telegram

Мессенджер, созданный командой Павла Дурова, построен на технологии шифрования переписки MTProto. На данный момент частично заблокирован на территории России, но эта блокировка — отдельная тема для разговора.

Мессенджер неоднозначный. Вокруг него много шума, но оправдан ли он? Доступа к исходникам нет, чаты по умолчанию не шифруются, нет защиты социального графа (все твои контакты хранятся на серверах Telegram), нет групповых E2EE-чатов, E2EE-чаты не поддерживаются в настольной версии программы, только в мобильной, мессенджер централизованный, сообщения хранятся на сервере (и они, как уже было отмечено, не зашифрованы), и при всем этом отсутствует возможность анонимной регистрации.




Если нужно использовать Telegram, то для защиты переписки нужно не забывать создавать секретные чаты. В мобильной версии для этого нужно выбрать команду New Secret Chat. Из настольных версий секретные чаты поддерживают только некоторые (например, один из двух клиентов для macOS).

В секретном чате сообщения шифруются и не хранятся на серверах мессенджера. Также нельзя сделать скриншот секретного чата, но ничто не

мешает сфотографировать такой чат с экрана.

- **Лицензия:** формально — GPLv3. Однако важная часть разработки закрыта. Если взглянуть на репозитории, то видно, что в последнее время какое-то движение наблюдалось только в вебовой версии. Увы, в таком виде это скорее иллюзия открытости
- **Степень централизации:** централизованный
- **Возможность анонимной регистрации и работы:** нет
- **Наличие E2EE:** реализованы, но как дополнение. По умолчанию чаты не шифруются
- **Синхронизация E2EE-чатов:** нет. Секретный чат можно использовать только с одного устройства, с другого доступа к нему уже не будет
- **Уведомление о проверке отпечатков E2EE:** нет. Пользователи могут сами зайти в настройки, чтобы сравнить отпечатки
- **Запрет на скриншоты секретных чатов:** есть, но работает не на всех устройствах
- **Групповые чаты E2EE:** нет
- **Защита социального графа:** нет

### 3.2 Signal

Мессенджер Signal разработан американским стартапом Open Whisper Systems, где, кроме двоих основателей, работает всего несколько человек. Для шифрования сообщений используется созданный специально для него криптографический протокол — Signal Protocol. Он применяется для сквозного (end-to-end) шифрования звонков (голосовых и видео), а также обычных сообщений. Протокол Signal с тех пор стали использовать и другие мессенджеры: WhatsApp, Facebook Messenger, Google Allo.

Казалось бы, в этом случае любой мессенджер может стать таким же безопасным, как и Signal. Но, как показывает практика, — нет. В отличие от Signal, где шифрование включено по умолчанию, в этих мессенджерах оно выключено. Для его включения в Facebook Messenger нужно активировать Secret Conversations, а в Google Allo — режим инкогнито (Incognito Mode).


Помимо этого, Signal децентрализованный, а его исходные коды открыты. Есть поддержка групповых E2EE-чатов, есть защита социального графа, поддерживаются исчезающие по таймеру сообщения.

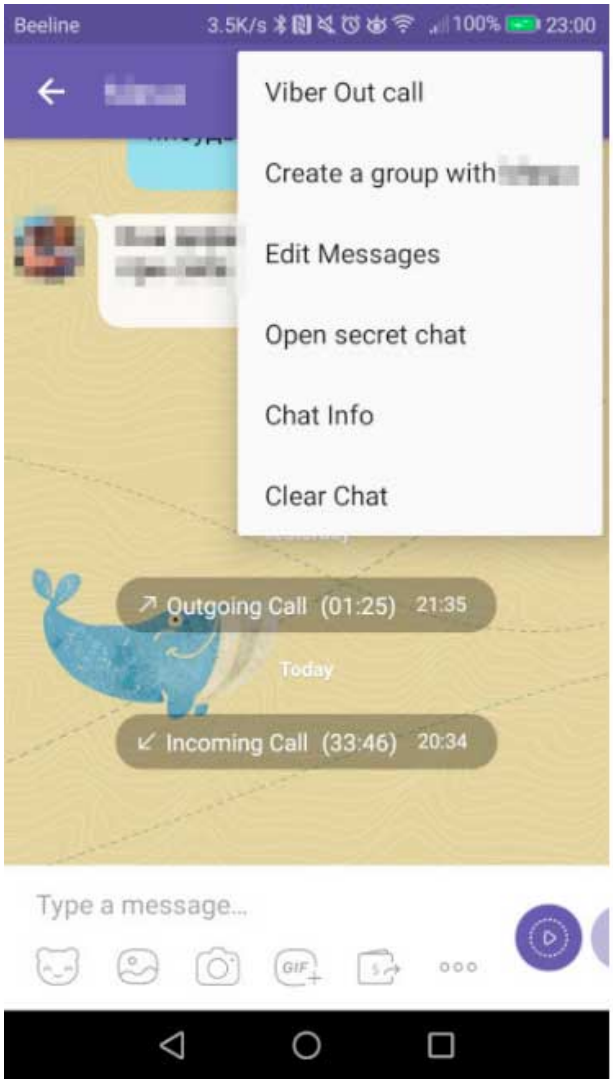
Однако не стоит путать защиту с анонимностью. Signal не анонимен: при регистрации нужно указывать номер телефона, к которому мессенджер и привязывается. Что касается исчезающих сообщений, то эта фишка встречается и в других мессенджерах, например в Viber и Telegram (в меню секретного чата нужно выбрать команду Set self-destruct timer).

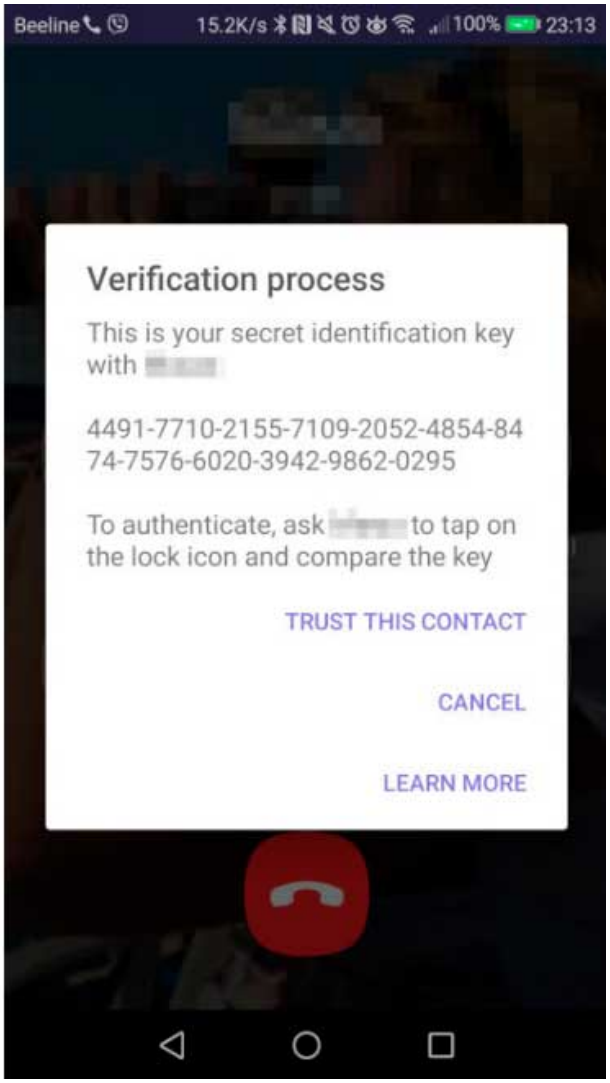
- **Лицензия:** AGPLv3
- **Степень централизации:** децентрализованный
- **Возможность анонимной регистрации и работы:** нет. Кроме номера телефона, других вариантов нет. Использование временного приведет к тому же результату, что и в случае с Telegram
- **Наличие E2EE:** есть. Используется Signal Protocol — специально разработанный для этого мессенджера протокол шифрования сообщений
- **Синхронизация E2EE-чатов:** есть
- **Уведомление о проверке отпечатков E2EE:** нет. Пользователям предлагается сосканировать QR-коды друг у друга или сравнить отпечатки
- **Запрет на скриншоты секретных чатов:** можно включить или выключить
- **Групповые чаты E2EE:** есть
- **Уведомление о необходимости проверки отпечатков E2EE в групповых чатах:**нет
- **Защита социального графа:** есть

### 3.3 Viber

Viber — интересный мессенджер. С одной стороны, он проприетарный, централизованный, привязывается только к номеру телефона, не обеспечивает защиту социального графа. С другой стороны, сквозное шифрование основано на протоколе Signal и включено по умолчанию, даже в настольной версии. Для дополнительной безопасности существуют секретные чаты с возможностью общаться группой.

Секретные чаты позволяют настроить таймер самоуничтожения для каждого сообщения: оно будет удалено через установленное время после просмотра — как с твоего устройства, так и со всех устройств получателей. Сообщения секретного чата защищены от пересылки, а скриншоты или запрещены, или оставляют уведомление на экране чата.




Для перехода в секретный чат нужно открыть чат с пользователем и выбрать из его меню команду «Перейти в секретный чат». Такой чат будет отмечен замком.

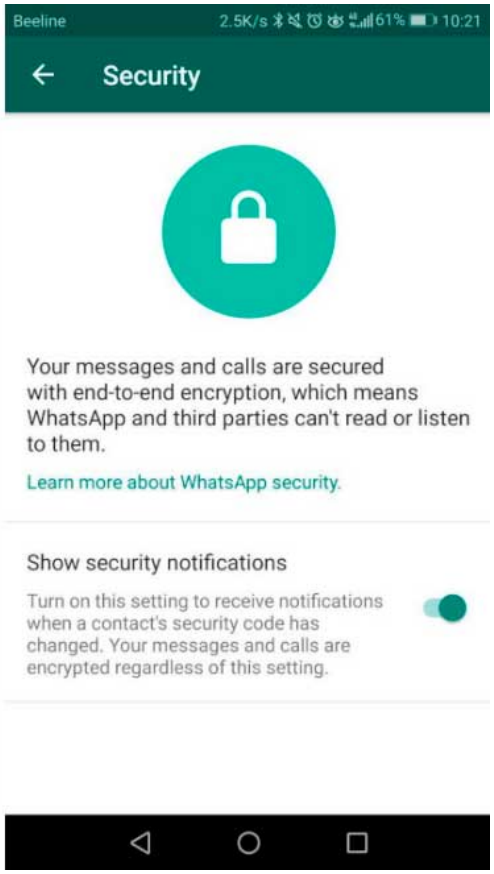
Дополнительно Viber позволяет создавать скрытые секретные чаты — они не будут отображаться в общем списке. Чтобы получить доступ к скрытому чату, нужно ввести установленный ранее PIN-код. Это дополнительная защита на тот случай, если телефон попадет в чужие руки.

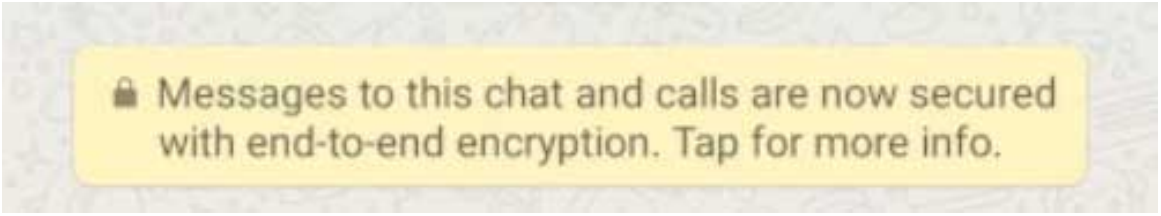
- **Лицензия:** проприетарная
- **Степень централизации:** централизованный
- **Возможность анонимной регистрации и работы:** только по номеру телефона
- **Наличие E2EE:** есть, по умолчанию. Также есть секретные и скрытые чаты, которые обеспечивают дополнительную безопасность
- **Синхронизация E2EE-чатов:** нет. Созданный в мобильной версии секретный чат не отобразился в десктопной версии
- **Уведомление о проверке отпечатков E2EE:** для проверки отпечатков предлагается совершить звонок собеседнику, сообщить свой идентификатор, после чего подтвердить его корректность, но уведомления, что это необходимо для обеспечения собственной безопасности, нет
- **Запрет на скриншоты секретных чатов:** есть
- **Групповые чаты E2EE:** есть
- **Уведомление о необходимости проверки отпечатков E2EE в групповых чатах:** нет
- **Защита социального графа:** нет

### 3.4 WhatsApp

WhatsApp использует Signal Protocol, но это само по себе не дает никаких гарантий. Конечно, этот мессенджер интересен тем, что не хранит твои сообщения на своих серверах. Вместо этого сообщения хранятся на телефоне (а также в облачных сервисах, с которыми он синхронизирован, например iCloud). Также E2EE используется по умолчанию с поддержкой групповых чатов.

Однако хоть WhatsApp и не получает самой переписки, его владельцы имеют доступ к метаданным, в том числе собирают телефонные номера из адресной книги, время отправки сообщений и звонков и так далее. Представь, что в 2:30 ты звонил в «секс по телефону» и твой разговор длился 24 минуты. Ну да, никто не узнает, как конкретно шла беседа, но это в данном случае не очень-то и нужно.


Кроме этого, WhatsApp собирает тонны информации о пользователе: модель его телефона, ОС, информацию, полученную от браузера, IP-адрес, мобильный номер и так далее.

Добавь к этому проприетарный код, и ты получишь далеко не самый лучший с точки зрения анонимности вариант. Может, никто и не перехватит твои сообщения, но сам мессенджер будет знать о тебе многое.

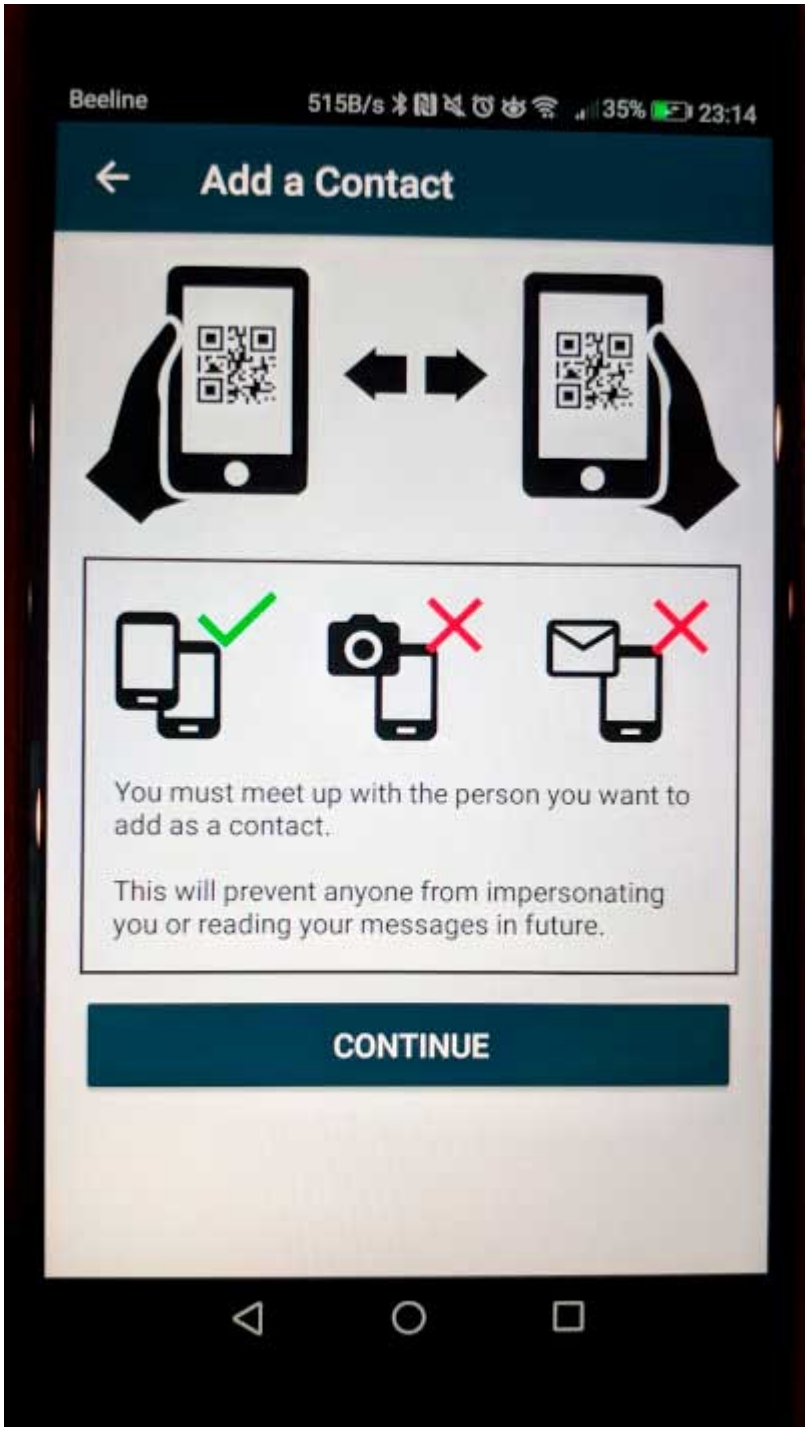
- **Лицензия:** проприетарная
- **Степень централизации:** централизованный
- **Возможность анонимной регистрации и работы:** только по номеру телефона
- **Наличие E2EE:** по умолчанию
- **Синхронизация E2EE-чатов:** есть
- **Уведомление о проверке отпечатков E2EE:** есть только в случае смены ключа собеседником. Чтобы уведомление пришло, необходимо зайти в настройки и включить эту функцию. При старте чата никаких уведомлений нет
- **Запрет на скриншоты секретных чатов:** нет
- **Групповые чаты E2EE:** есть
- **Уведомление о необходимости проверки отпечатков E2EE в групповых чатах:**нет
- **Защита социального графа:** нет

Наличие сквозного шифрования — еще не гарантия того, что переписка не будет перехвачена. Его можно обойти либо проэксплуатировать какую-то уязвимость, как это уже было в случае с WhatsApp

### 3.5 Briar

Briar — не очень популярный мессенджер, и готов поспорить, что далеко не все наши читатели знают о его существовании. Однако он хорош: основан на технологии децентрализованных сетей (mesh), может работать по Bluetooth или Wi-Fi либо через интернет, но в таком случае он подключится через Tor.

Исходники Briar открыты, есть возможность анонимной регистрации и использования, а чаты шифруются по умолчанию, причем не хранятся на серверах Briar (то есть твои сообщения в зашифрованном виде хранятся только на твоем телефоне). Есть защита социального графа (никто никому не сливает твою адресную книгу), есть групповые E2EE-чаты, но нет синхронизации E2EE-чатов между устройствами, поскольку нет возможности использовать одну и ту же учетную запись на разных устройствах.




На фоне всех остальных мессенджеров Briar выглядит очень неплохо, если нужна анонимность общения. Но у него есть и недостатки: нет версии для iPhone, нет возможности голосовых звонков. Если с отсутствием звонков еще можно мириться, то без версии для одной из крупных платформ круг

общения окажется еще более узким.

- **Лицензия:** GPLv3
- **Степень централизации:** децентрализованный
- **Возможность анонимной регистрации и работы:** есть
- **Наличие E2EE:** есть, по умолчанию
- **Синхронизация E2EE-чатов:** нет
- **Уведомление о проверке отпечатков E2EE:** при добавлении контакта необходимо сосканировать QR-код собеседника с экрана его телефона, другого варианта добавить его нет. Считаем, что уведомление есть
- **Запрет на скриншоты секретных чатов:** есть
- **Групповые чаты E2EE:** есть
- **Уведомление о необходимости проверки отпечатков E2EE в групповых чатах:**в групповой чат можно добавить только собеседника из тех, чьи QR-коды уже проверены. Также считаем, что уведомление есть
- **Защита социального графа:** есть

### 3.6 ТамТам

При создании «ТамТама» никто не делал упор на безопасность, и об этом нужно помнить. Внимание к нему может привлечь разве что возможность регистрации через почту Google или «Одноклассники». Однако шифрование сообщений не поддерживается (или разработчики об этом не сообщают), и нет защиты социального графа. То есть, «как бы ты ни регистрировался, без дополнительных мер все равно будет понятно, кто ты». В общем, даже как замена для «Телеграма» этот мессенджер не годится, несмотря на все чаяния его разработчиков.

- **Лицензия:** проприетарная
- **Степень централизации:** централизованный
- **Возможность анонимной регистрации и работы:** возможна регистрация с использованием почты Google или через «Одноклассники»
- **Наличие E2EE:** нет
- **Защита социального графа:** нет

### 3.7 Вконтакте

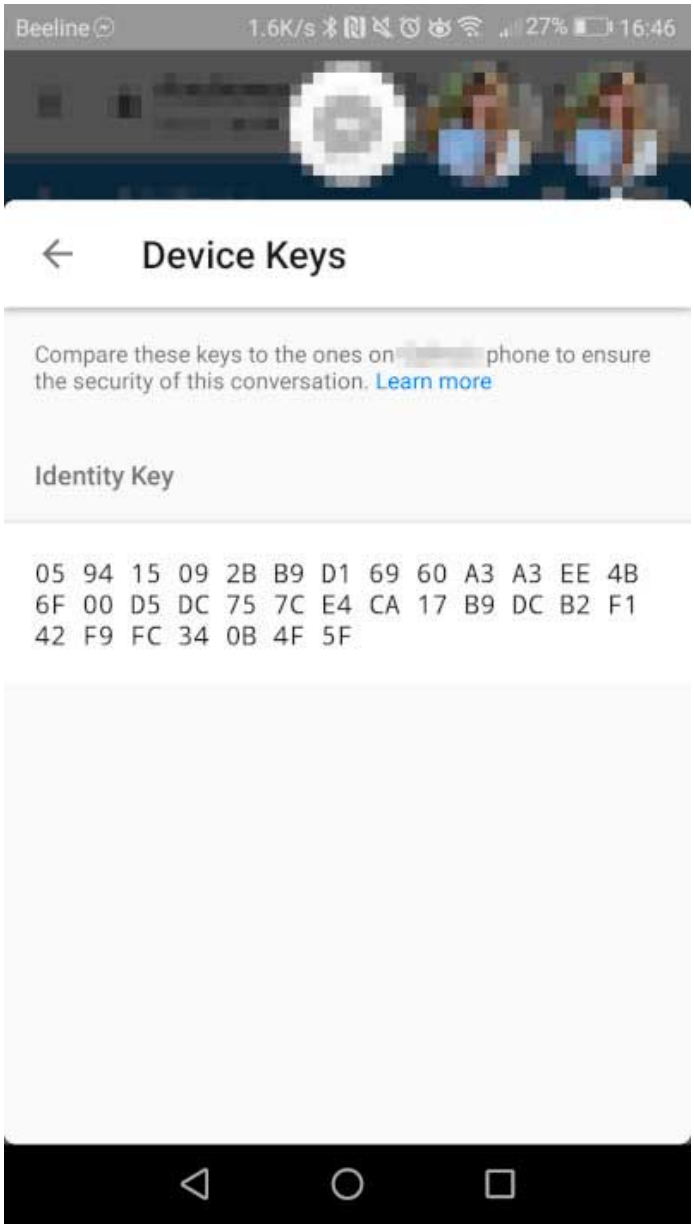
Снова проходим мимо: вряд ли кому-то в здравом уме придет в голову мысль использовать «Вконтакте» как средство для анонимного общения. Сообщения хранятся на серверах соцсети, не шифруются, регистрация только по номеру телефона — в общем, полный набор того, чего мы тут пытаемся избежать.

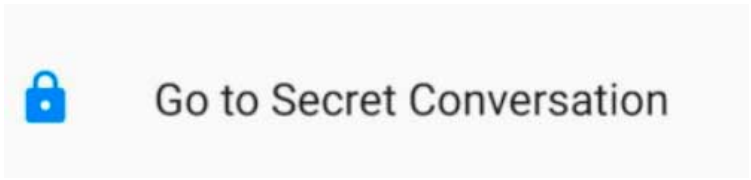
- **Лицензия:** проприетарная
- **Степень централизации:** централизованный
- **Возможность анонимной регистрации и работы:** только по номеру телефона

- **Наличие E2EE:** нет
- **Защита социального графа:** нет

### 3.8 Facebook Messenger

Мессенджер, прилагающийся к Facebook, построен на основе открытого протокола MQTT. На всякий случай напомню, что это именно протокол обмена сообщениями — не путать с протоколом шифрования. После того как на мобильных телефонах Messenger выселили в отдельное приложение, у пользователей Facebook оставалось мало выбора, кроме как установить еще и его. Однако регистрироваться в «Мессенджере» можно и без аккаунта в FB.




Если сравнивать чаты «Вконтакте» и Facebook Messenger, то второй оказывается на голову выше. Во-первых, можно регистрироваться с анонимной почтой. Во-вторых, поддерживаются E2EE-чаты, но не по

умолчанию. Для включения шифрования сообщений нужно активировать Secret Conversations.

Однако Facebook собирает очень много всевозможной информации о пользователе, поэтому вряд ли подойдет для анонимного общения. Также не поддерживается синхронизация E2EE-чатов и многого другого (см. выше).

- **Лицензия:** проприетарная
- **Степень централизации:** централизованный
- **Возможность анонимной регистрации и работы:** есть. Регистрация в «Фейсбуке» возможна с использованием электронной почты, а вход в Messenger — через учетную запись Facebook
- **Наличие E2EE:** есть, но не по умолчанию
- **Синхронизация E2EE-чатов:** нет
- **Уведомление о проверке отпечатков E2EE:** нет. Но собеседники могут сравнить отпечатки друг друга
- **Запрет на скриншоты секретных чатов:** нет
- **Групповые чаты E2EE:** нет
- **Защита социального графа:** нет

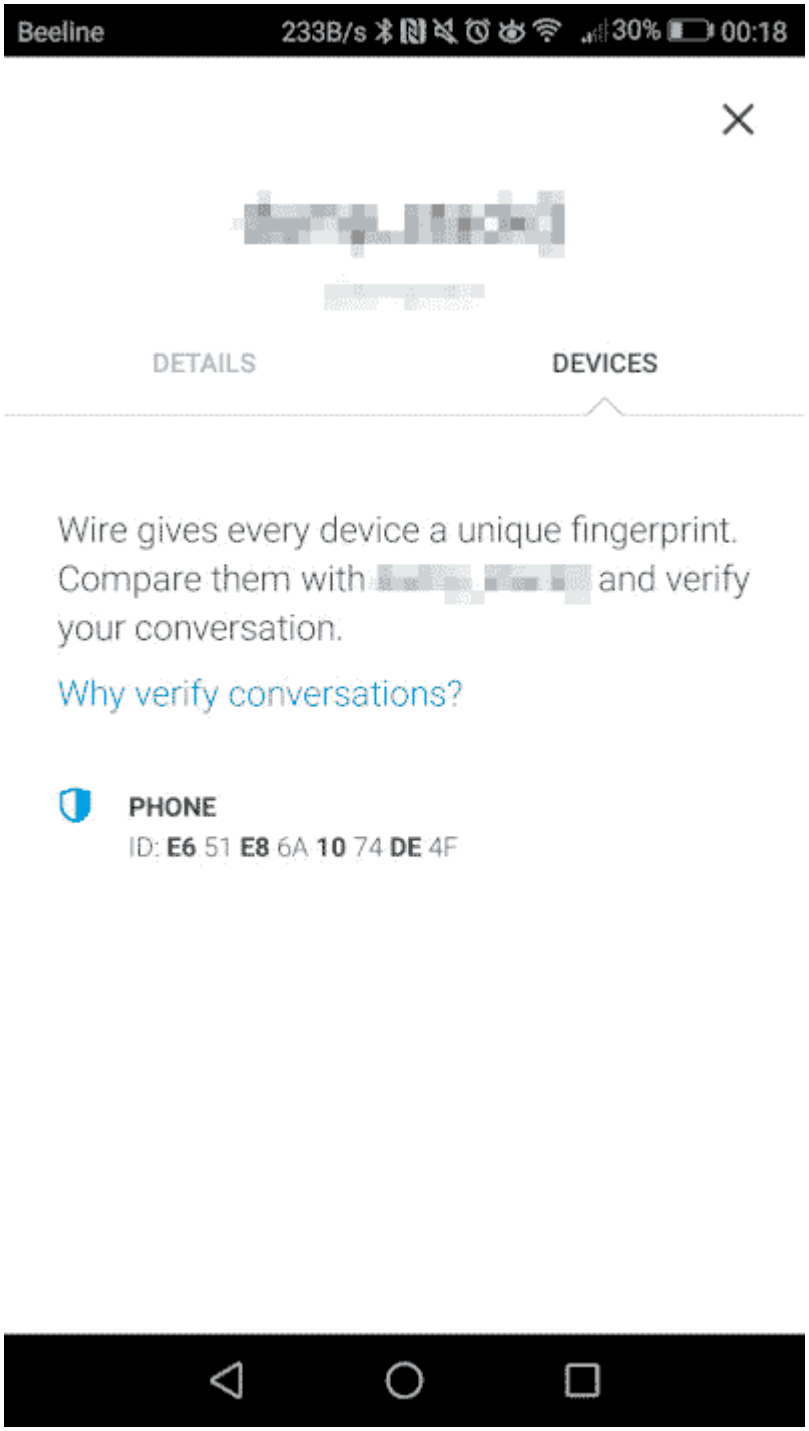
### 3.9 Wire

Wire — один из наиболее анонимных мессенджеров. В его основе — протокол Wire Swiss, основанный на Signal. Чем он хорош?

Во-первых, есть возможность анонимной регистрации.

Во-вторых, по умолчанию поддерживается сквозное шифрование с возможностью синхронизации зашифрованных чатов.

В-третьих, есть защита социального графа, поддерживаются групповые зашифрованные чаты (до 128 человек) и безопасные конференц-звонки (до 10 человек). Что-то подобное мы видели в Briar, но у Wire еще и огромный выбор поддерживаемых платформ: Android, iOS, Windows, macOS, Linux.



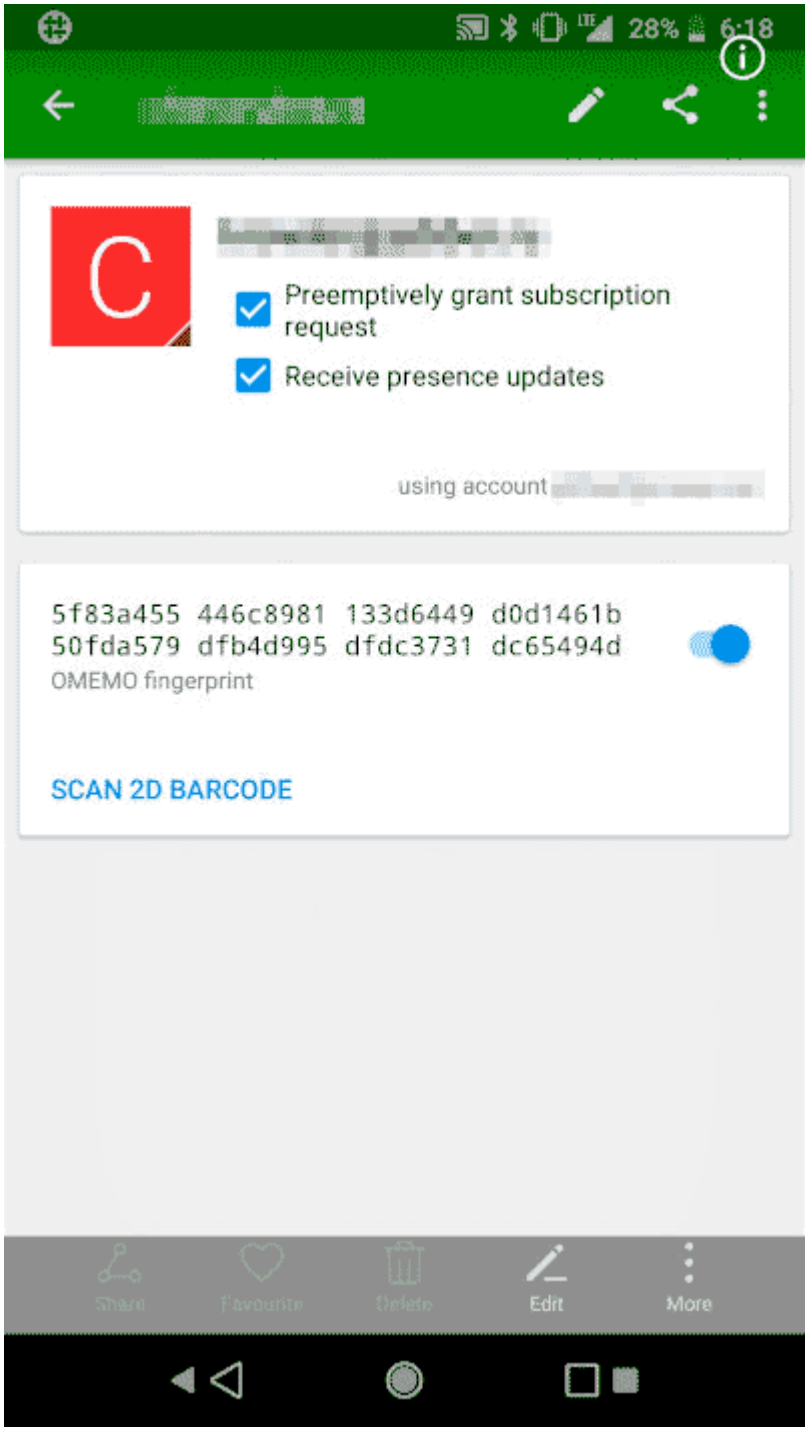

Должна быть ложка дегтя? Она есть: мессенджер платный и стоит шесть евро в месяц (четыре при оплате за год). Разработчики утверждают, что это плюс: подобная бизнес-модель — это хоть какая-то гарантия того, что на твоих данных не попытаются заработать. С другой стороны, денежные транзакции

плохо ладят с анонимностью. Зато есть пробный период на месяц!

- **Лицензия:** GPLv3
- **Степень централизации:** централизованный
- **Возможность анонимной регистрации и работы:** есть. С помощью почты
- **Наличие E2EE:** есть, по умолчанию
- **Синхронизация E2EE-чатов:** есть
- **Уведомление о проверке отпечатков E2EE:** нет, но возможность есть
- **Запрет на скриншоты секретных чатов:** нет
- **Групповые чаты E2EE:** есть
- **Уведомление о необходимости проверки отпечатков E2EE в групповых чатах:**есть. Если один из пользователей отправляет в секретный групповой чат сообщение с устройства, которое не верифицировано у другого пользователя, то, когда второй попытается отправить сообщение, перед ним появится предупреждение о том, что у первого новое устройство
- **Защита социального графа:** есть

### 3.10 Jabber (OMEMO)

Если Jabber и выбивается из компании современных мессенджеров с веселыми стикерами и голосовыми звонками, то в плане приватности он по-прежнему во многом незаменим. Он федеративный, поддерживает анонимную регистрацию, E2EE-шифрование (правда, нужно расширение OMEMO), в том числе групповое.



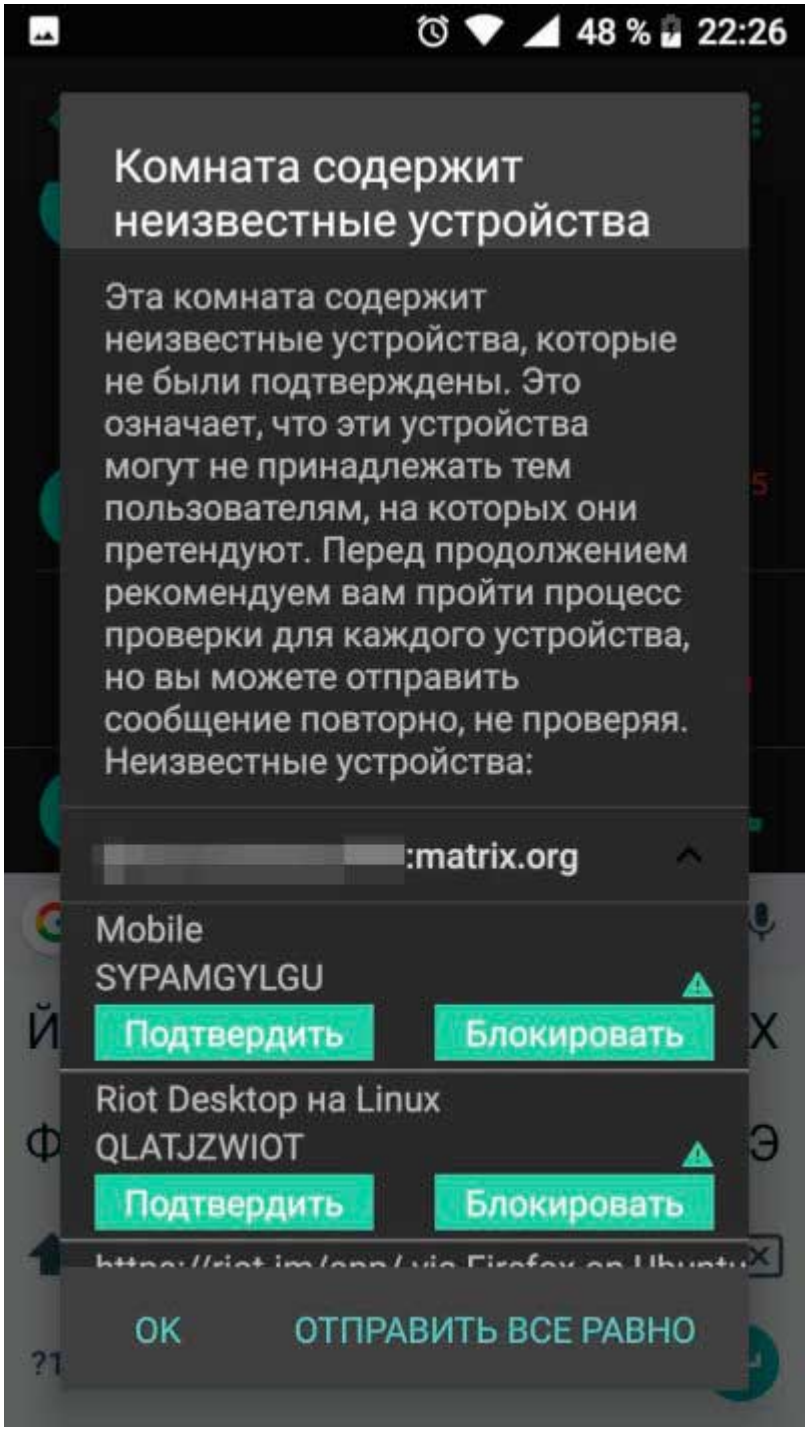

Да, возможности не поражают воображение, но Jabber проверен временем и к тому же имеет реализации на всех возможных платформах. ChatSecure для iOS, Conversations — для Android, Pidgin — для Linux и так далее, список огромен.

- **Лицензия:** разные свободные лицензии
- **Степень централизации:** федеративный
- **Возможность анонимной регистрации и работы:** есть. Регистрация с использованием почтового ящика, учетной записи в Facebook или Twitter
- **Наличие E2EE:** есть. Необходимо дополнение OMEMO
- **Синхронизация E2EE-чатов:** есть
- **Уведомление о проверке отпечатков E2EE:** уведомления нет, но возможность есть
- **Запрет на скриншоты секретных чатов:** нет
- **Групповые чаты E2EE:** есть
- **Уведомление о необходимости проверки отпечатков E2EE в групповых чатах:**нет
- **Защита социального графа:** нет

### 3.11 Riot (Matrix)

Чего создателям этого мессенджера не занимать, так это умения придумывать крутые названия. Собственно, Matrix — это протокол коммуникации, а Riot — это клиентское приложение (бывают и другие — в том числе для консоли). Использовать можно как вебовый вариант, так и программы для iOS и Android.

В целом это еще один малоизвестный федеративный мессенджер с поддержкой и синхронизацией чатов E2EE, в том числе групповых. Регистрация анонимная, без привязки к номеру мобильного телефона или почте. Поддерживается голосовая связь и видеозвонки.




Шифрование переписки в Riot можно включить или выключить — индикатором этого служит значок замочка рядом с полем отправки сообщения. Также если в секретном групповом чате появится пользователь, чьи устройства не верифицированы другими пользователями, собеседники

увидят уведомление об этом при попытке отправить сообщение.

В целом Matrix выглядит как интересный вариант, смутить может только его новизна в сочетании с тем, что протокол свой.

- **Лицензия:** Apache
- **Степень централизации:** федеративный
- **Возможность анонимной регистрации и работы:** есть
- **Наличие E2EE:** есть, по выбору пользователя
- **Синхронизация E2EE-чатов:** есть
- **Уведомление о проверке отпечатков E2EE:** есть
- **Запрет на скриншоты секретных чатов:** нет
- **Групповые чаты E2EE:** есть
- **Уведомление о необходимости проверки отпечатков E2EE в групповых чатах:**есть
- **Защита социального графа:** есть

### 3.12 Status

Status — это нечто большее, чем просто мессенджер. Конечно, его можно использовать только для общения, но это все равно что ставить Windows ради «Блокнота». Да и общаться здесь не очень-то удобно, даже картинку не отправишь, не говоря уж про такую роскошь, как стикер. Зато прямо в чате есть возможность отправить ETH и создать запрос на его получение.

Приложение пока находится на стадии бета-теста.

Поскольку есть возможность анонимной регистрации и все чаты шифруются по умолчанию, можно считать, что каждый чат в Status — секретный. Есть и синхронизация секретных чатов, но синхронизироваться будут только входящие сообщения, а вот отправленные с одной учетной записи, но с разных устройств — нет.

Еще один возможный недостаток: сообщения хранятся и на телефоне, и на сервере мессенджера, но разработчики уверяют, что в зашифрованном виде. Зато твоя книга контактов не сливается на серверы мессенджера, что нынче дорогого стоит. В общем, безопасность здесь есть, а возможность перевода криптовалюты, вероятно, кого-то порадует. Но Status пока что скорее интересная диковинка, чем рабочий инструмент.

- **Лицензия:** MPLv2
- **Степень централизации:** децентрализованный
- **Возможность анонимной регистрации и работы:** есть
- **Наличие E2EE:** по умолчанию
- **Синхронизация E2EE-чатов:** частичная (см. описание)
- **Уведомление о проверке отпечатков E2EE:** есть (чтобы начать диалог с пользователем, необходимо ввести его идентификатор или сосканировать с экрана смартфона)
- **Запрет на скриншоты секретных чатов:** нет
- **Групповые чаты E2EE:** нет
- **Защита социального графа:** есть

### 3.13 Threema

Threema — проприетарный централизованный мессенджер, серверы которого находятся в Швейцарии. Кроме текстового общения, пользователям доступны голосовые звонки, возможность отправлять свое местоположение, голосовые сообщения и файлы. Поддерживаются групповые чаты до 50 человек.

Сообщения здесь шифруются полностью и децентрализованным способом на устройствах пользователя, а не на сервере Threema. Сервер скорее играет роль коммутатора: сообщения пересылаются через него, но не хранятся постоянно.

Для регистрации не нужно указывать данные, которые могут способствовать установлению личности, — ни номер телефона, ни email. При первом запуске программы случайным образом генерируется идентификатор пользователя, на его основе будет сгенерирован QR-код. Все это обеспечивает анонимность общения.

Чтобы начать диалог с собеседником, необходимо ввести его идентификатор. В Threema есть три уровня доверия личности пользователя. Наивысший будет при сканировании идентификатора с экрана смартфона, а самый низкий — при вводе его вручную. Где-то посередине находится синхронизация контактов. Уровень проверки каждого контакта отображается в виде точек рядом с именем.

В отличие от WhatsApp или, например, Facebook Messenger Threema не регистрирует, кто и с кем общается, и не хранит адресную книгу

пользователя на своих серверах. Все сообщения на устройствах пользователя хранятся в зашифрованном виде. Способ шифрования зависит от устройства. В iOS используется функция iOS Data Protection, в Android и Windows Phone — AES-256. Шифруются сообщения, изображения и другие данные, передаваемые между пользователями.

Хоть каждый чат шифруется и может считаться секретным, помимо этого, есть и приватные чаты. Они защищены PIN-кодом и помечены значком со шляпой и очками. Нечто подобное мы уже встретили в Viber.

В общем, Threema оставляет неплохое впечатление. Сообщения не могут быть расшифрованы — даже по решению суда, так как хранятся только на телефоне и Threema не имеет доступа к секретным ключам пользователей. Серверы Threema знают только, кто отправляет сообщение и кому, но они не логируют эту информацию и не могут расшифровать содержимое сообщения.

Переходим к минусам. Во-первых, это необходимость разово заплатить. 2,6 евро разово — не бог весть что, но сам факт оплаты может быть нежелательным. Также отсутствие синхронизации и хранения сообщений означает, что сохранить историю ты можешь только сам, сделав бэкап.

- **Лицензия:** проприетарная для приложений, AGPLv3 для веб-клиента
- **Степень централизации:** централизованный
- **Возможность анонимной регистрации и работы:** есть. Можно создать учетную запись без привязки к номеру телефона или почте. Пользователю присваивается уникальный ID, который можно сменить
- **Наличие E2EE:** есть, по умолчанию
- **Синхронизация E2EE-чатов:** нет: для каждого устройства генерируется отдельный ID
- **Уведомление о проверке отпечатков E2EE:** есть. Сообщения в групповых чатах отправляются каждому собеседнику индивидуально, а диалог можно начать только с тем, чей идентификатор подтвержден
- **Запрет на скриншоты секретных чатов:** нет
- **Групповые чаты E2EE:** есть
- **Уведомление о необходимости проверки отпечатков E2EE в групповых чатах:**есть
- **Защита социального графа:** есть. Адресная книга по умолчанию не загружается на сервер, но при желании пользователь может разрешить доступ к ней

## 4. Итоги

Рекомендовать какой-либо мессенджер не будем. Представим рассмотренные мессенджеры в виде таблицы

| MESSENGER | FOSS | ЦЕНТРАЛИЗАЦИЯ | АНОНИМНОСТЬ | E2EE | СИНХРОНИЗАЦИЯ E2EE | ПРОВЕРКА ОТПЕЧАТКОВ | ЗАПРЕТ НА СКРИНШОТЫ | ГРУППОВЫЕ E2EE-ЧАТЫ | УВЕДОМЛЕНИЕ О ПРОВЕРКЕ E2EE | ЗАЩИТА СОЦ. ГРАФА | SCORE |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Telegram | Нет | Централизованный | Нет | По выбору | Нет | Нет | Есть | Нет | Нет | Нет | 1.5 |
| Signal | Да | Децентрализованный | Нет | По умолчанию | Есть | Нет | Есть | Есть | Нет | Есть | 7 |
| Viber | Нет | Централизованный | Нет | По выбору | Нет | Нет | Есть | Есть | Нет | Нет | 2.5 |
| WhatsApp | Нет | Централизованный | Нет | По умолчанию | Есть | Нет | Нет | Есть | Нет | Нет | 3 |
| Briar | Да | Децентрализованный | Есть | По умолчанию | Нет | Есть | Есть | Есть | Есть | Есть | 9 |
| ТамТам | Нет | Централизованный | Есть | Нет | Нет | Нет | Нет | Нет | Нет | Нет | 1 |
| Вконтакте | Нет | Централизованный | Нет | Нет | Нет | Нет | Нет | Нет | Нет | Нет | 0 |
| Facebook Messenger | Нет | Централизованный | Есть | По выбору | Нет | Нет | Нет | Нет | Нет | Нет | 1.5 |
| Wire | Да | Централизованный | Есть | По умолчанию | Есть | Нет | Нет | Есть | Есть | Есть | 7 |
| Jabber | Да | Федеративный | Есть | Плагин | Есть | Нет | Нет | Есть | Нет | Нет | 5 |
| Riot Matrix | Да | Федеративный | Есть | По выбору | Есть | Есть | Нет | Есть | Есть | Есть | 8 |
| Status | Да | Децентрализованный | Есть | По умолчанию | Частично | Есть | Нет | Нет | Нет | Есть | 6.5 |
| Threema | Нет | Централизованный | Есть | По умолчанию | Нет | Есть | Нет | Есть | Есть | Есть | 6 |