Секретные чаты в Telegram Android

# Введение

Сегодня информация в мессенджерах чаще всего передается в зашифрованном виде, однако в некоторых случаях возникает необходимость усиленной защиты. Эта возможность реализуется путем сквозного шифрования между устройствами. В мессенджере Telegram чаты с поддержкой сквозного шифрования называются секретными чатами. Эта инструкция предназначена для тех, кто уже знаком с мессенджером Telegram, но хочет научиться использовать секретные чаты.

# Особенности секретных чатов

По сравнению с обычными секретные чаты имеют ряд следующих характерных отличий:

* **Количество участников.** В обычных чатах максимальное количество участников зависит от технических ограничений мессенджера. Например, в чате Telegram может быть до 200 000 участников. В секретных чатах со сквозным шифрованием может быть не более двух участников, что обусловлено особенностями протокола шифрования.
* **Шифрование.** В обычных чатах используется стандартное шифрование по схеме «[клиент-сервер](https://core.telegram.org/techfaq#q-how-does-server-client-encryption-work-in-mtproto)», ключ которого известен как устройствам участников чата, так и серверу, который отвечает за хранение и защиту переписки. В секретных чатах применяется сквозное шифрование «[клиент-клиент](https://core.telegram.org/techfaq#q-how-does-end-to-end-encryption-work-in-mtproto)», ключ которого известен только двум устройствам участников чата.
* **Хранение данных.** Информация из обычных чатов хранится на серверах, которые синхронизируют переписку между устройствами пользователей. В секретных чатах данные не сохраняются на серверах и не синхронизируются с другими устройствами пользователей. Поэтому секретный чат будет доступен пользователю только на том устройстве, на котором этот чат был создан. Кроме того, когда участник выходит из учетной записи на устройстве с секретным чатом, содержимое этого чата удаляется без возможности восстановления.
* **Защита данных.** Обычные чаты позволяют делать скриншоты (снимки экрана) и пересылать сообщения из чата другим пользователям. В секретных чатах этих возможностей нет.

Telegram Desktop и Telegram Web не поддерживают секретные чаты. Разработчики объясняют это тем, что люди намного чаще оставляют без присмотра персональные компьютеры, нежели свои мобильные устройства, поэтому персональные компьютеры менее защищены от несанкционированного доступа. Вторая причина заключается в том, что, в отличие от версий для Android и iOS, Telegram Desktop и Web не хранят сообщения локально, а загружают их из облака при каждом запуске. На компьютере сохраняются только файлы, изображения и видео из чатов. Следовательно, при выключении или перезагрузке компьютера все созданные секретные чаты будут удаляться.

# Преимущества секретных чатов

Исходя из вышесказанного, секретные чаты предлагают следующие преимущества с точки зрения безопасности и конфиденциальности:

* Сообщения в секретных чатах шифруются между устройствами участников диалога, что делает их недоступными для посторонних лиц.
* Данные не сохраняются на серверах мессенджера, что исключает возможность их перехвата третьими лицами.
* Сообщения из секретного чата невозможно переслать другому пользователю или сделать скриншот, что предотвращает утечку информации.
* Если участник выходит из учетной записи, то чат автоматически удаляется, что гарантирует безвозвратное удаление данных.

Несмотря на защиту от скриншотов и пересылки, Android-версия Telegram всё же позволяет копировать текст сообщений и сохранять медиафайлы из секретного чата. Кроме того, текущий кадр видеосообщения отобразится на скриншоте в режиме «картинка в картинке», если во время его воспроизведения вернуться к списку чатов и сделать скриншот.

Из других факторов риска можно также отметить, что ваш собеседник может сфотографировать экран устройства с секретным чатом.

# Инструкции по использованию секретных чатов

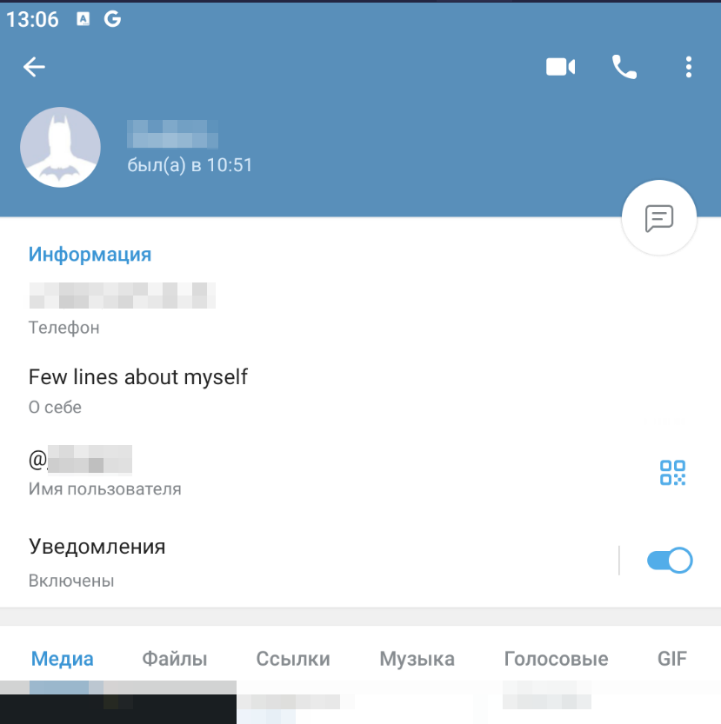
**Примечание**: инструкции актуальны для Telegram Android версии 11.3.3 (5396). Интерфейс и функции в других версиях могут отличаться.

## Создание секретного чата

Секретный чат можно создать для любого пользователя Telegram. Если вы уже переписывались с этим пользователем, то его можно найти в списке чатов или поиском. Если его нет в списке чатов, то его можно найти в списке контактов. Если собеседник отсутствует в списке контактов, но вам известно имя пользователя, то его можно найти поиском. Если вам известен только номер пользователя, то его можно добавить в список контактов.

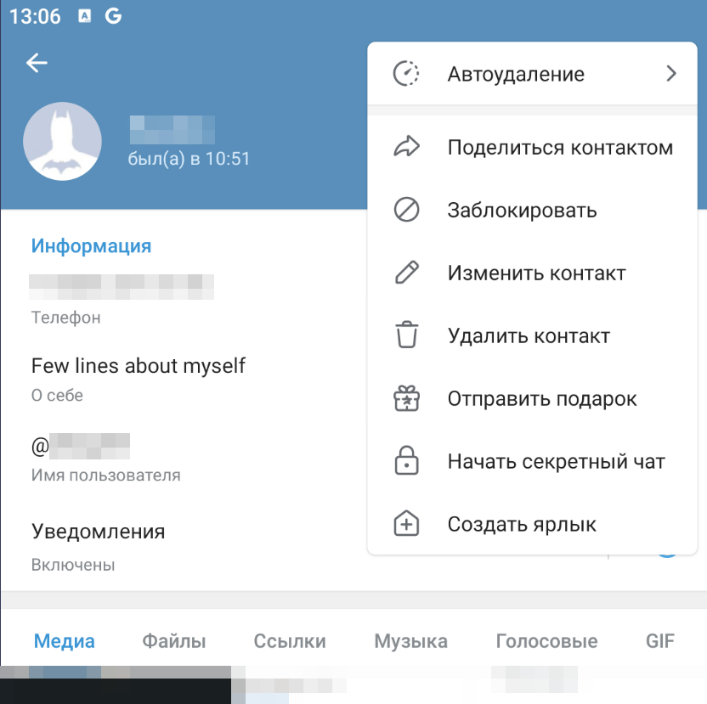
Секретный чат не заменяет собой обычный, а создается в дополнение к нему. Вы можете создать несколько секретных чатов с одним и тем же собеседником.

1. Откройте Telegram.
2. Найдите и выберите пользователя, с которым вы хотите создать секретный чат. Откроется обычный чат с этим пользователем.
3. Нажмите на имя или значок пользователя, чтобы открыть его профиль.
4. Нажмите кнопку  в правом верхнем углу экрана, чтобы открыть меню дополнительных действий (Рисунок 1).



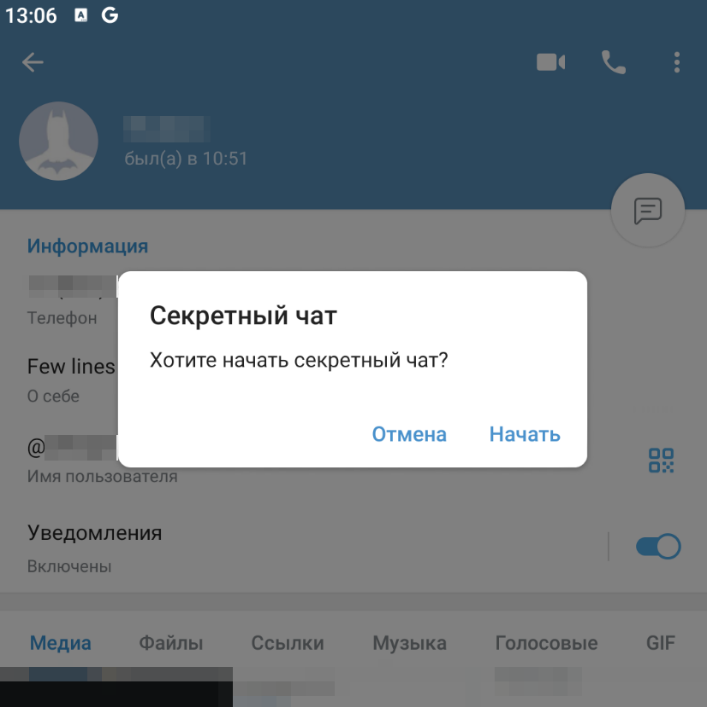
*Рисунок 1 Профиль пользователя*

1. Выберите пункт **Начать секретный чат** (Рисунок 2).



*Рисунок 2 Меню дополнительных действий*

1. Нажмите кнопку **Начать**, когда появится запрос подтверждения (Рисунок 3).



*Рисунок 3 Запрос подтверждения*

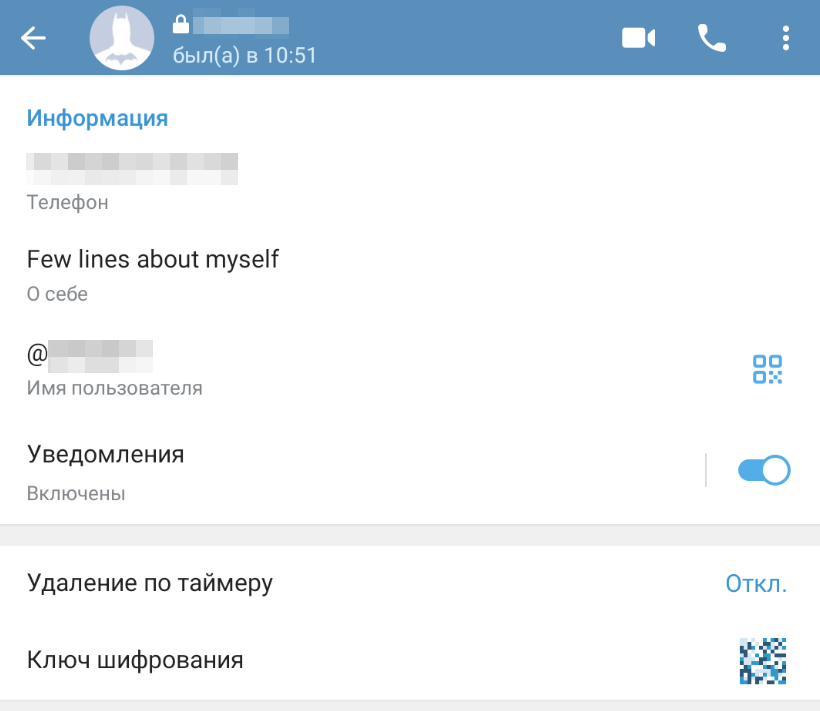
Секретный чат создан, и вы можете начать общение.

**Примечание**: если пользователь добавил вас в черный список, то при попытке создать с ним секретный чат вы получите сообщение об ошибке.

## Настройка удаления по таймеру

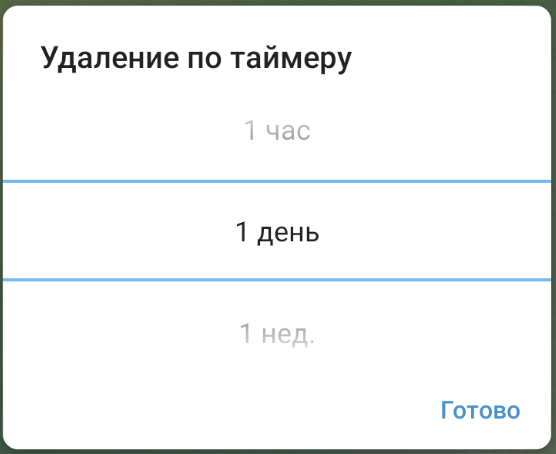
Эта функция удаляет сообщения по истечении заданного времени и служит дополнительной мерой безопасности. Время может составлять от одной секунды до одной недели, отсчет начинается после того, как собеседник просмотрит сообщение. По умолчанию удаление по таймеру в секретных чатах отключено. Чтобы включить его, нужно выполнить следующие действия:

1. Откройте секретный чат.
2. Нажмите на имя вашего собеседника, чтобы открыть его профиль.
3. Выберите пункт **Удаление по таймеру** (Рисунок 4).



*Рисунок 4 Профиль пользователя в секретном чате*

1. Прокруткой выберите нужное время из списка (Рисунок 5).



*Рисунок 5 Настройка удаления по таймеру*

1. Нажмите кнопку **Готово** (Рисунок 5).

Удаление по таймеру настроено.

**Примечание:** есть два других способа включить, отключить или изменить время удаления по таймеру:

* Нажмите на значок собеседника в чате и выберите время из списка.
* Нажмите кнопку  в правом верхнем углу чата и выберите пункт **Включить удаление по таймеру**, затем выберите время из списка и нажмите кнопку **Готово**.

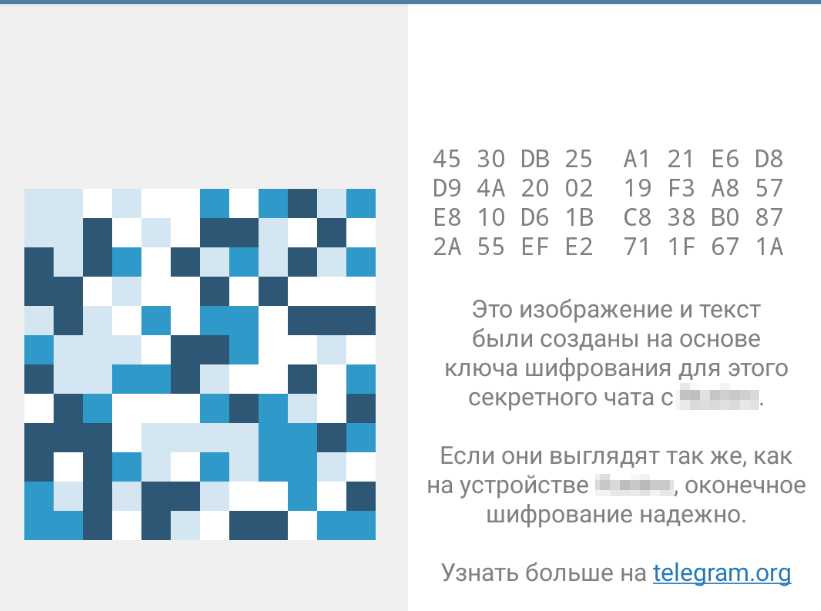
**Важно:** настройки удаления по таймеру применяются только к новым сообщениям и не влияют на предыдущие.

## Сверка ключа шифрования

Сверка ключа шифрования позволяет убедиться в надежности защиты и отсутствии внешнего вмешательства (так называемой «атаки посредника», или [MITM-атаки](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%D0%BF%D0%BE%D1%81%D1%80%D0%B5%D0%B4%D0%BD%D0%B8%D0%BA%D0%B0)) в канал связи. Для этого клиент Telegram формирует изображение и текст на основе ключа шифрования.

Сверку ключа следует проводить по защищенному каналу связи, чтобы исключить подмену пересылаемых данных, и лучше всего это делать при личной встрече с собеседником. Для сверки ключа шифрования выполните следующие действия:

1. Откройте секретный чат.
2. Нажмите на имя вашего собеседника, чтобы открыть его профиль.
3. Выберите пункт **Ключ шифрования** (Рисунок 4).
4. Попросите собеседника выполнить те же действия на своем устройстве.
5. Сверьте изображения и текст (Рисунок 6).



*Рисунок 6 Изображение и текст, созданные на основе ключа шифрования*

Если текст и изображения на двух устройствах совпадают, то чат надежно защищен.