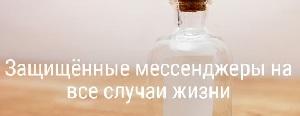
**Самые популярные анонимные мессенджеры в 2020**

С виду даже самая незамысловатая и безобидная переписка может принести немало проблем. К примеру, из частного общения двух или более человек хакеры способны узнать много пикантной информации, чтобы впоследствии шантажировать своих жертв, требуя выкуп. Если у Вас в квартире находятся какие-либо ценности и Вы, совершенно не думая ни о чем плохом, написали друзьям, что собираетесь в отпуск, а квартира будет пустовать, - то есть большая вероятность, что об этом прознают домушники и у них будет шикарная возможность обворовать Вас. А чего стоят шутки, которыми Вы так часто перекидываетесь с коллегами, сидя в офисе за своим компьютером, не имея никакого злого умысла. Отдельно взятая такая шутка способна стать оскорблением в руках «доброжелателей» и стоить Вам карьеры, а то и всей репутации, накопленной годами.

В наши дни стремительного развития цифровых технологий важно бережно относится к собственной безопасности, частью которой является сфера общения – соблюдать секретность переписки.

В 2020-ом году можно выделить несколько мессенджеров мирового масштаба, соответствующих требованиям безопасного общения. Принцип их действия заключается в передаче зашифрованного сообщения от одного участника переписки к другому, причем раскодировать эти сведения способен лишь получивший информацию. Такое шифрование информации носит название «end-to-end».

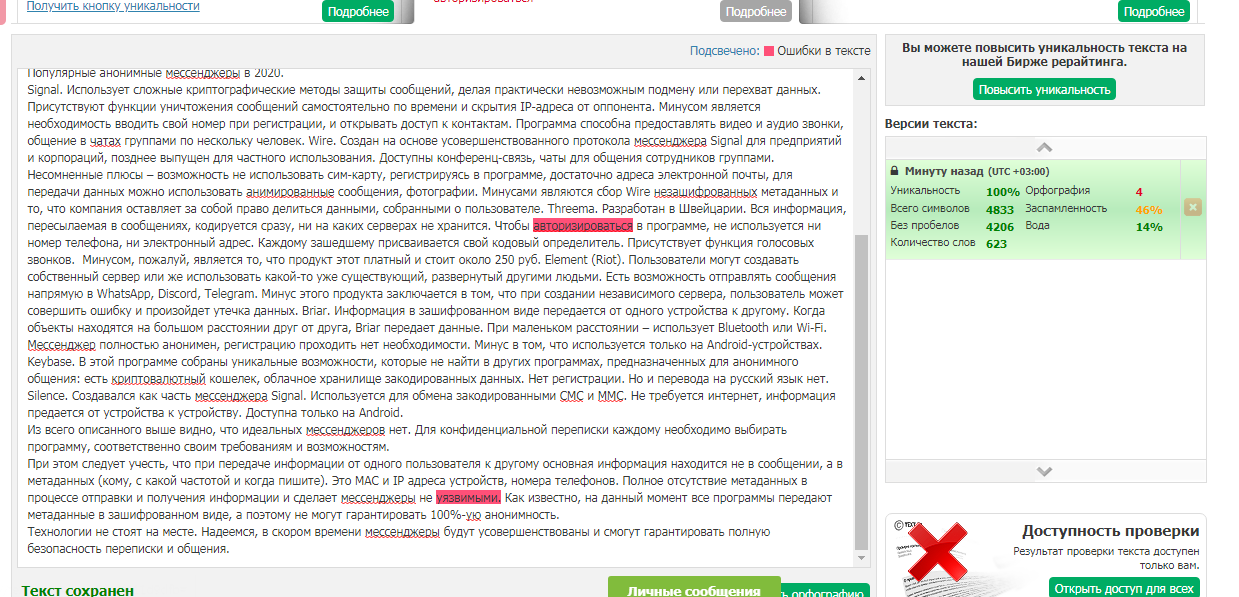
**Популярные анонимные мессенджеры в 2020.**

1. **Signal.** Использует сложные криптографические методы защиты сообщений, делая практически невозможным подмену или перехват данных. Присутствуют функции уничтожения сообщений самостоятельно по времени и скрытия IP-адреса от оппонента. Минусом является необходимость вводить свой номер при регистрации, и открывать доступ к контактам. Программа способна предоставлять видео и аудио звонки, общение в чатах группами по нескольку человек.
2. **Wire.** Создан на основе усовершенствованного протокола мессенджера Signal для предприятий и корпораций, позднее выпущен для частного использования. Доступны конференц-связь, чаты для общения сотрудников группами. Несомненные плюсы – возможность не использовать сим-карту, регистрируясь в программе, достаточно адреса электронной почты, для передачи данных можно использовать анимированные сообщения, фотографии. Минусами являются сбор Wire незашифрованных метаданных и то, что компания оставляет за собой право делиться данными, собранными о пользователе.
3. **Threema.** Разработан в Швейцарии. Вся информация, пересылаемая в сообщениях, кодируется сразу, ни на каких серверах не хранится. Чтобы авторизоваться в программе, не используется ни номер телефона, ни электронный адрес. Каждому зашедшему присваивается свой кодовый определитель. Присутствует функция голосовых звонков. Минусом, пожалуй, является то, что продукт этот платный и стоит около 250 руб.
4. **Element (Riot).** Пользователи могут создавать собственный сервер или же использовать какой-то уже существующий, развернутый другими людьми. Есть возможность отправлять сообщения напрямую в WhatsApp, Discord, Telegram. Минус этого продукта заключается в том, что при создании независимого сервера, пользователь может совершить ошибку и произойдет утечка данных.
5. **Briar.** Информация в зашифрованном виде передается от одного устройства к другому. Когда объекты находятся на большом расстоянии друг от друга, Briar передает данные. При маленьком расстоянии – использует Bluetooth или Wi-Fi. Мессенджер полностью анонимен, регистрацию проходить нет необходимости. Минус в том, что используется только на Android-устройствах.
6. **Keybase.** В этой программе собраны уникальные возможности, которые не найти в других программах, предназначенных для анонимного общения: есть криптовалютный кошелек, облачное хранилище закодированных данных. Нет регистрации. Но и перевода на русский язык нет.
7. **Silence.** Создавался как часть мессенджера Signal. Используется для обмена закодированными СМС и ММС. Не требуется интернет, информация передается от устройства к устройству. Доступна только на Android.

Из всего описанного выше видно, что идеальных мессенджеров нет. Для конфиденциальной переписки каждому необходимо выбирать программу, соответственно своим требованиям и возможностям.

При этом следует учесть, что при передаче информации от одного пользователя к другому основная информация находится не в сообщении, а в метаданных (кому, с какой частотой и когда пишите). Это MAC и IP адреса устройств, номера телефонов. Полное отсутствие метаданных в процессе отправки и получения информации и сделает мессенджеры неуязвимыми. Как известно, на данный момент все программы передают метаданные в зашифрованном виде, а поэтому не могут гарантировать 100%-ую анонимность.

Технологии не стоят на месте. Надеемся, в скором времени мессенджеры будут усовершенствованы и смогут гарантировать полную безопасность переписки и общения.

****