

Шпаргалка для работы в мессенджере МАХ:

Миф/страх	Короткий факт	Действие
«Читает всё 24/7»	Облачная модель ≠ E2EE	Шифровать вложения, чистить историю
«Есть E2EE как в Signal»	Публичной спецификации нет	Не слать секреты в «голом» чате
«Анонимная регистрация»	Номер телефона обязателен	Отдельный номер для сервисов
«Адресная книга уходит»	Только по разрешению ОС	Отклонить доступ или включить выборочно
«Полиция в реальном времени»	Доступ по закону/запросам	Минимизировать чувствительное в чатах
«Микрофон пишет тайно»	Ограничения iOS/Android	Разрешение «по запросу»
«GPS льётся без доступа»	Без разрешения — только IP-регион	Выключить геолокацию или «при использовании»
«Кейлоггер вшит»	Нужны привилегии/рут	Не выдавать «Спецвозможности»
«Обновления — шпионаж»	Подписанные апдейты из стора	Проверять разрешения после апдейта
«Накажут за критику»	Модерация против нарушений, не против мнений	Писать корректно, техвопросы — в поддержку

МАХ — не «абсолютный приват», но и не «вездесущая прослушка». Это обычный массовый мессенджер с облачной моделью и нормальным для таких сервисов комплектом настроек. Главное — не путать мифы с фактами и не забывать про цифровую гигиену. Если сомневаетесь — загляните в помощь, перечитайте политику и посмотрите свежие разборы на SecurityLab.

Дисклеймер: материал опирается на открытые страницы МАХ и профильные публикации на момент подготовки текста. Функции и документы могут обновляться — проверяйте первоисточники.

Чеклист приватности за 3 минуты

1. Откройте «Настройки → Приватность» и включите «только контакты» для входящих (см. разделы в помощи).
2. Ограничьте поиск по номеру до «Контактов» и скройте статус «в сети».
3. Проверьте активные сессии и завершите лишние устройства.
4. Отключите доступ к контактам/геолокации, если они не критичны вашему сценарию.
5. Шифруйте чувствительные файлы до отправки; обсуждайте секреты только в узком кругу.
6. Обновляйте клиент через официальные каналы.