7 мифов

Миф № 1. «MAX – это шпионская программа, которая получает полный доступ к данным смартфона без ведома пользователя».

Как на самом деле. Это не правда. Как и любой современный мессенджер, MAX запрашивает разрешения, нужные для его базовых функций. К примеру, доступ к контактам нужен для общения, к камере и микрофону – для звонков, к хранилищу – для обмена файлами. Можно эти разрешения, конечно, не давать. Но тогда как общаться? Все мессенджеры просят такие разрешения. Для сравнения, у WhatsApp их 85, у Telegram – 71, а у MAX – всего 63. При этом каждое приложение проходит обязательную проверку в официальных магазинах (таких как App Store, Google Play и RuStore). Там оценивается обоснованность этих запросов.

Миф № 2. «MAX будет доносить властям на пользователей за использование VPN или чтение запрещенных материалов».

Как на самом деле. Такое утверждение (ложное, естественно) можно отнести к любому приложению, установленному на телефон. Не важно – российскому или иностранному. Никаких прецедентов с оформлением «доносов» с помощью приложений в России не было. Если гражданин этого боится, то должен в принципе удалить с телефона приложение «Госуслуги», а также крупных госбанков и прочих сервисов, связанных с государством. И вообще завести себе вместо смартфона обычный кнопочный телефон. Так точно будет спокойнее. Хотя жить так в современном мире будет не очень удобно.

Миф № 3. «MAX – это шаг к созданию «цифрового рубильника» и изолированного сегмента интернета».

Как на самом деле. Создание MAX – это обеспечение цифрового суверенитета и безопасности данных, которые хранятся в российских дата-центрах и не передаются за рубеж. Это мировой тренд – развивать национальные цифровые платформы. Проблема с иностранными мессенджерами в том, что они хранят все данные на зарубежных серверах, нередко нарушают российское законодательство и плохо сотрудничают в борьбе с мошенниками и прочими преступниками (например, наркодилерами). Зарубежные мессенджеры (даже вроде бы наш «родной» дуровский Telegram) действуют очень выборочно. К примеру, в последние три года они удалили только 10 % противоправной информации по запросам российских властей. Это несет большие риски для пользователей. В том числе, для несовершеннолетних.

Миф № 4. «Мошенники уже и так массово звонят пользователям, представляясь сотрудниками мессенджера MAX».

Как на самом деле. Да, мошенники используют все имеющиеся возможности. Но Центр безопасности MAX оперативно реагирует на запросы пользователей и властей. К примеру, только в июле заблокировал более 10

тысяч телефонных номеров, принадлежащих мошенникам, и удалил около 32 тысяч вредоносных и спам-документов.

Миф № 5. «MAX использует открытый код, позаимствованный у других мессенджеров, что делает его уязвимым для хакеров через разные «бэкдоры» и «закладки».

Как на самом деле. Это не так. Использование открытого кода – общепринятая мировая практика. Такие технологические гиганты, как Google, Apple, Microsoft, WeChat, Яндекс и Сбер, активно используют и адаптируют открытые библиотеки. По-другому никак. В противном случае они проиграют в конкурентной борьбе. При этом сами библиотеки не взаимодействуют с сетью и не передают данные вовне. Весь код MAX проходит строгий аудит безопасности.

Миф № 6. «MAX самостоятельно активирует камеру каждые 5 – 10 минут и следит за человеком».

Как на самом деле. Об этом сообщил один из пользователей. Чем вызвал взрыв «паранойи» в социальных сетях. Якобы при работе в MAX у пользователя постоянно вылетало сообщение антивируса Касперского, что мессенджер «лезет» в камеру. Как выяснилось, это было связано с некорректной работой самого антивируса. Любой мессенджер так устроен, что время от времени проверяет доступность видеоустройств. Это стандартная процедура. При этом никакого исходящего видео- или фото-потока не происходит. А значит, нет и «слежки». К слову, 12 августа этого года Лаборатория Касперского обновила программное обеспечение. Теперь этот «баг» устранен.

Миф № 7. «Оператор MAX – фирма-однодневка, которая не несет ответственности за утечки данных».

Как на самом деле. Оператором мессенджера является ООО «Коммуникационная платформа». Это дочерняя компания холдинга VK. Она действует в соответствии с российским законодательством о защите персональных данных. Ответственность за безопасность пользователей полностью лежит на компании.