WhatsApp враг рода человеческого

Арс Либрев

Будучи самым популярным еще с 2015 года приложением для обмена сообщениями,[1] WhatsApp стал основным средством для общения во многих странах мира.[2] В 2020 году общее количество его пользователей перевалило за 2 миллиарда.[3] Очень грустно осознавать, что такому количеству людей совершенно наплевать на себя, что такой процент человечества готов принести свою безопасность и свободу в жертву удобству. Как это почти всегда бывает с несвободной программой,[4] WhatsApp построен на принципах весьма далеких от приватности.

WhatsApp распространяется под проприетарной лицензией.[5] Это значит, что пользователь не может ни проверить, что делает программа, ни изменить ее как ему нужно (для этого необходим доступ к исходному коду, который не предоставляется пользователю, выяснять его с помощью обратной разработки также запрещено лицензией). Пользователь не контролирует программу. Ее контролирует корпорация, которая ей владеет. Соответственно, эта корпорация имеет над пользователями WhatsApp власть. Как и почти всегда бывает в таких случаях, эта власть подталкивает корпорацию к внедрению в программу вредоносных особенностей.

Одним из «удобств» WhatsApp является отсутствие необходимости формировать базу общения, поскольку приложение автоматически получает доступ к адресной книге устройства и создает на ее основе список контактов. Однако, при такой реализации, на сервера контролирующей WhatsApp корпорации сливаются номера всех людей занесенных в адресную книгу, даже тех, кто не пользуется WhatsApp. Таким образом, пользователь данного мессенджера, возможно сам того не осознавая, может совершить подлость по отношению к тому, кто не желает светить какие бы то ни было свои данные перед контролирующей WhatsApp корпорацией. Перед отправкой номера хешируются, однако происходит это без использования «соли», ввиду чего обратное преобразование данного хеша в номер телефона можно спокойно осуществить даже на бытовом компьютере, причем в течении нескольких минут.[6]

При регистрации пользователю приходит СМС с кодом подтверждения. При этом WhatsApp требует разрешения на доступ к чтению СМС, и получая его, прочитывает содержание сообщения. Таким образом, приложение имеет доступ к СМС пользователя и может сливать их содержание корпорации.

WhatsApp собирает и сливает контролирующей его компании личные данные пользователя, сведения о его устройствах и его контактах, о чем прямо сказано в их Политике конфиденциальности.[7] У контролирующей WhatsApp корпорации имеется возможность создавать уникальные профили пользователей, на основании сопоставления различных данных, сливаемых WhatsApp и другими инструментами. Это дает возможность прогнозировать поведение пользователя и манипулировать им.[8] Также корпорация может передавать данные пользователей тем, с кем она сотрудничает.[9]

В WhatsApp применяется оконечное шифрование, т.е. сообщения шифруются на устройстве пользователя и отправляются через сервер компании собеседнику в зашифрованном виде. По идее, такая схема должна препятствовать возможности даже самой корпорации иметь доступ к содержимому сообщений. Facebook,* после приобретения мессенджера, согласился оставить эту функцию очень неохотно, поскольку это препятствовало сбору данных о пользователях, которые можно было бы монетизировать, к примеру, показом таргетированной рекламы или продажей бизнес-инструментов. Несмотря на то, что оконечное шифрование, как было сказано, продолжает присутствовать в WhatsApp, корпорация Facebook* искала пути ее обхода, как отмечал в 2018 году один из основателей WhatsApp Брайан Эктон.[10]

При этом еще в 2016 году была обнаружена уязвимость, которая позволяла Facebook* скрытно сменить ключи шифрования и требовать от приложения отправителя перешифровки новыми ключами с последующей повторной отправкой. То есть, фактически, это позволяет Facebook* расшифровывать сообщения и получать доступ к их содержанию.[11] Когда это вскрылось, Facebook* заявил, что такой функционал необходим для доставки сообщений в случае смены пользователем телефона или сим-карты.[12]

В том же году выяснилось, что удаленные сообщения в WhatsApp удаляются не полностью и подлежат восстановлению.[13]

Существует также возможность получить доступ к переписке пользователя через iCloud, если настроено резервное копирование сообщений в этот сервис.[14] Возможно это осуществить и при наличии резервных копий в других сервисах удаленного хранения.[15]

В 2019 году в приложение был внедрен функционал для изучения интересов пользователей. Разработчики заявляют, что информация об активности людей храниться не на серверах корпорации, а непосредственно на устройствах, на которых установлено приложение.[16] Однако все это лишь слова, которые сложно воспринимать всерьез, пока приложение не станет

распространяться под свободной лицензией, о чем корпорация, конечно, даже не помышляет.

Подводя итог, можно заключить, что WhatsApp, это несвободное небезопасное средство, собирающее данные пользователей и отдающее их на произвол контролирующей корпорации. Причем под угрозой оказывается не только информация непосредственных пользователей WhatsApp, но и их близких, друзей, знакомых, которые, возможно, даже не пользуются этим приложением.

Но если WhatsApp не допустим для использования, чем его заменить? Как общаться? Альтернативы в виде таких же несвободных инструментов, вроде Viber,[17] не подходят. В них пользователи получают похожий букет проблем. Такие средства как Telegram, приложения которых свободны, но программное обеспечение на централизованных серверах проприетарное, и к безопасности которых также много вопросов, тоже сомнительный вариант.[18] Существуют, однако, действительно безопасные средства для общения, уважающие конфиденциальность пользователей.

Одним из таких инструментов является MEGA.[19] Данный сервис, это в первую очередь, облачное хранилище, однако в нем также присутствуют средства для общения, в которых реализуется оконечное шифрование. То есть, сообщения шифруются непосредственно на устройстве, и даже сам сервер MEGA не сможет прочитать содержимое. Лазеек подобных той, что присутствует в WhatsApp, не имеется. Передаваемые файлы, аудио и видеосвязь, также шифруются. Использовать ее можно как на компьютере, через браузер, так и на мобильном устройстве, через приложение.[20] MEGA, к сожалению, является не полностью свободным ПО, поскольку налагается ограничение на коммерческое распространение копий исходного кода. Однако сам исходный код открыт. Минусом также можно считать то, что вся сеть серверов контролируется одной компанией. Кроме этого, аккаунты в MEGA привязываются к электронной почте. Это не так критично, как привязка к номеру телефона, подобная той, что есть в WhatsApp или Telegram, но все же снижает приватность.

Для действительно высокой приватности можно обратить внимание на инструмент Session. В отличии от MEGA, он является полностью свободным. Этот инструмент формирует свою собственную сеть серверов, и подключение в нем организуется по принципу Tor, — трафик пропускается последовательно через три узла, что позволяет скрывать сведения о том, кто с кем общается.[21] При этом он подключается к серверу, который координирует пересылку сообщений, а также некоторое время хранит их, что позволяет осуществлять оффлайн-отправку. Сервер при этом может поднять любой желающий.

Существуют версии клиентов как для компьютера,[22] так и для мобильного устройства.[23]

Для тех же, кому нужен очень высокий уровень приватности, стоит порекомендовать инструмент Briar.[24] Данный мессенджер позволяет обмениваться только сообщениями, однако он является полностью децентрализаванным, т.е. в процессе общения не участвуют вообще никакие сервера, связь осуществляется непосредственно между устройствами пользователей. Также Briar может быть использован для Mesh-связи. То есть общение возможно производить вообще без Интернета, подключаясь к устройствам собеседников через Wi-Fi или Bluetooth. При общении же по Интернету возможно пропускать трафик через сеть Tor, для сокрытия от следящих систем не только содержимого сообщений, но и информации о том, кто с кем общается.

Этим список свободных инструментов для общения не исчерпывается. Существуют и другие свободные средства связи, такие как XMPP[25], Matrix[26] и Kontalk.[27] Это федеративные средства, т.е. их сервера распределены по всему миру, пользователь может выбрать любой, и любой человек может поднять свой сервер. Таким образом, нет единственной корпорации, которая бы все контролировала и могла бы навязывать пользователям свою политику. Существуют еще гибридные инструменты, такие как Jitsi Meet[28] и Status.[29] В них общение может осуществляться как непосредственно между собеседниками, так и через координирующий сервер, который также можно поднять самостоятельно. Из полностью децентрализованных средств для общения можно упомянуть Tox[30] и Jami[31]. К сожалению, приходится констатировать, что в них связь не всегда осуществляется без проблем. Даже они, однако, не только этичные и безопасные популярных проприетарных мессенджеров. Проблемы в них, фактически, может исправить любой, обладающий компетентностью. Это одно из главных отличий свободных программ от несвободных.

Основным препятствием массовому переходу на свободные мессенджеры является социальная инерция («Все пользуются WhatsApp, а значит и мне нужно пользоваться именно им»). Также у проектов свободных средств общения нет возможности обеспечить своим разработкам мощную рекламу.

Когда встает вопрос о том, пользоваться ли популярной вредоносной программой, такой как WhatApp, или же свободной, этичной, хотя возможно, не такой удобной, как например Session, или иногда не до конца корректно работающей, такой как Jami, необходимо помнить, что несовершенство и угнетение не одно и тоже.[32] Выбирая свободную программу, вы снижайте социальную инерцию и вносите вклад в доброе и справедливое будущее. Выбирая же несвободную, вы вносите вклад лишь в процветание олигархии.

1 *Leo Sun* «Facebook* Inc.'s WhatsApp Hits 900 Million Users: What Now?» https://www.fool.com/investing/general/2015/09/11/facebook-incs-whatsapp-hits-900-million-users-what.aspx
2 *Metz Cade* «Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People» https://web.archive.org/web/20160405164942/http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/. *Leo Sun* «Facebook* Inc.'s WhatsApp Hits 900 Million Users: What Now?» http://www.fool.com/investing/general/2015/09/11/facebook-incs-whatsapp-hits-900-million-users-what.aspx
3 Блог WhatsApp «Два миллиарда пользователей: конфиденциальная связь по всему миру» https://blog.whatsapp.com/10000666/Two-Billion-Users--Connecting-the-World-Privately
4 Множественные свидетельства наличия вредоносных особенностей в проприетарном программном обеспечении можно посмотреть по ссылкам на данной странице https://www.gnu.org/proprietary/proprietary.html
5 Официальная информация о WhatsApp
6 Findings under the Personal Information Protection and Electronic Documents Act «Report of Findings Investigation into the personal information handling practices of WhatsApp Inc.» https://web.archive.org/web/20130202011011/http://www.priv.gc.ca/cf-dc/2013/2013_001_0115_e.asp
7 См. ссылку в сноске 5. Также представление о спектре собираемых данных дает статья: *Никита Горяинов* «Посмотрел на WhatsApp и ужаснулся. Apple раскрыла, как за вами следит каждое приложение» https://www.iphones.ru/iNotes/teper-apple-naglyadno-pokazyvaet-kak-za-vami-sledit-kazhdoe-prilozhenie-sravnite-telegram-i-whatsapp-01-06-2021
8 Главный радиочастотный центр «WhatsApp обновил Условия использования и Политику приватности» https://web.archive.org/web/20210320094003/http://www.rfs-rf.ru/grfc/news/detail/index.php?ID=49495
9 *Thomas Brewster* «WhatsApp Ordered To Help U.S. Agents Spy On Chinese Phones — No Explanation Required» https://www.forbes.com/sites/thomasbrewster/2022/01/17/whatsapp-ordered-to-spy-on-chinese-phones-by-america-no-explanation-given/?sh=46354e516f01
10 *Маргарита Герасюкова* «Сооснователь WhatsApp рассказал о причинах ухода из Facebook*» https://www.gazeta.ru/tech/2018/09/27/12000001/bryan_acton_sad.shtml?updated

11 *Tobias Boelter* «WhatsApp Retransmission Vulnerability» https://tobi.rocks/2016/04/whats-app-retransmission-vulnerability/
12 *Tobias Boelter* «WhatsApp vulnerability: Bug or Backdoor?» https://tobi.rocks/2017/01/whatsapp-vulnerability-bug-or-backdoor/
13 *Kate Conger* «Research shows deleted WhatsApp messages aren't actually deleted» https://techcrunch.com/2016/07/29/research-shows-deleted-whatsapp-messages-arent-actually-deleted/
14 Об этом сказано в статье «В США рассекретили документ о том, какой доступ и к каким мессенджерам имеет ФБР» https://habr.com/ru/news/t/592515/
15 *Гектор Гернандес, Мария Жушков* «Как шпионить за разговорами в WhatsApp: мифы и факты» https://ru.malavida.com/faq/whatsapp/android/how-to-spy-on-whatsapp-conversations-myths-and-realities.html
16 *Антон Благовещенский* «WhatsApp начинает следить за пользователями. Вот что об этом известно» https://rg.ru/2019/02/14/whatsapp-nachinaet-sledit-za-polzovateliami-vot-chto-ob-etom-izvestno.html
17 Политика конфиденциальности Viber https://www.viber.com/ru/terms/viber-privacy-policy/. Приложение Viber собирает и отсылает информацию пользователя различным компаниям, таким как Google, Facebook* и иные, что можно увидеть на этой странице https://reports.exodus-privacy.eu.org/en/reports/com.viber.voip/latest/#trackers
18 О проблемах Telegram сказано на странице его клиента на сайте F-Droid https://f-droid.org/ru/packages/org.telegram.messenger/. Также о них сказано на сайте проекта Whonix https://www.whonix.org/wiki/Telegram. *Татьяна Сидорова* «В сеть утекли данные миллионов пользователей Telegram» https://profile.ru/news/scitech/v-set-utekli-dannye-millionov-polzovatelej-telegram-348298/
19 Сайт MEGA https://mega.nz
20 К сожалению, в свободном магазине приложений F-Droid этого приложения нет, оно доступно для скачивания только через сервисы Google. Скачивать его лучше не через Play-маркет, а через Aurora Store, который есть в F-Droid https://f-droid.org/ru/packages/com.aurora.store/. Страница мобильного приложения MEGA https://play.google.com/store/apps/details?
21 Сайт Session https://getsession.org/
22 Страница с версиями Session для скачивания https://getsession.org/download
23 Страница неофициального клиента Session, полностью лишенного несвободных компонентов, на сайте F-Droid https://f-droid.org/ru/packages/network.loki.messenger.fdroid/. Для скачивания через F-Droid официального клиента необходимо подключить репозитории,

которые указаны на этой странице https://fdroid.getsession.org/

24 Сайт Briar https://briarproject.org/. Страница Briar на сайте F-Droid https://f-droid.org/ru/packages/org.briarproject.briar.android/

25 Страница XMPP-клиента Conversation на сайте F-Droid https://f-droid.org/ru/packages/eu.siacs.conversations/

26 Сайт Matrix https://matrix.org/. Страница с версиями для скачивания Matrix-клиента Element https://element.io/download. Страница Matrix-клиента Element на сайте F-Droid https://f-droid.org/ru/packages/im.vector.app/

27 Сайт Kontalk https://www.kontalk.org/. Страница Kontalk на сайте F-Droid https://f-droid.org/ru/packages/org.kontalk/

28 Сайт Jitsi Meet https://jitsi.org/jitsi-meet/

29 Сайт Status https://status.im/ru. Страница с образами скачивания клиента Status https://status.im/ru/get/. Страница Status на сайте F-Droid https://f-droid.org/ru/packages/im.status.ethereum/

30 Сайт Tox https://tox.chat/. Страница клиента qTox https://wiki.tox.chat/clients/qtox. Страница клиента TRIfa на сайте F-Droid https://f-droid.org/ru/packages/com.zoffcc.applications.trifa/

31 Сайт Jami https://jami.net/. Страница клиента на сайте F-Droid https://f-droid.org/ru/packages/cx.ring

32 *Ричард Столмен* «Несовершенство и угнетение — не одно и то же» https://www.gnu.org/philosophy/imperfection-isnt-oppression.ru.html

*— Запрещен на территории РФ