

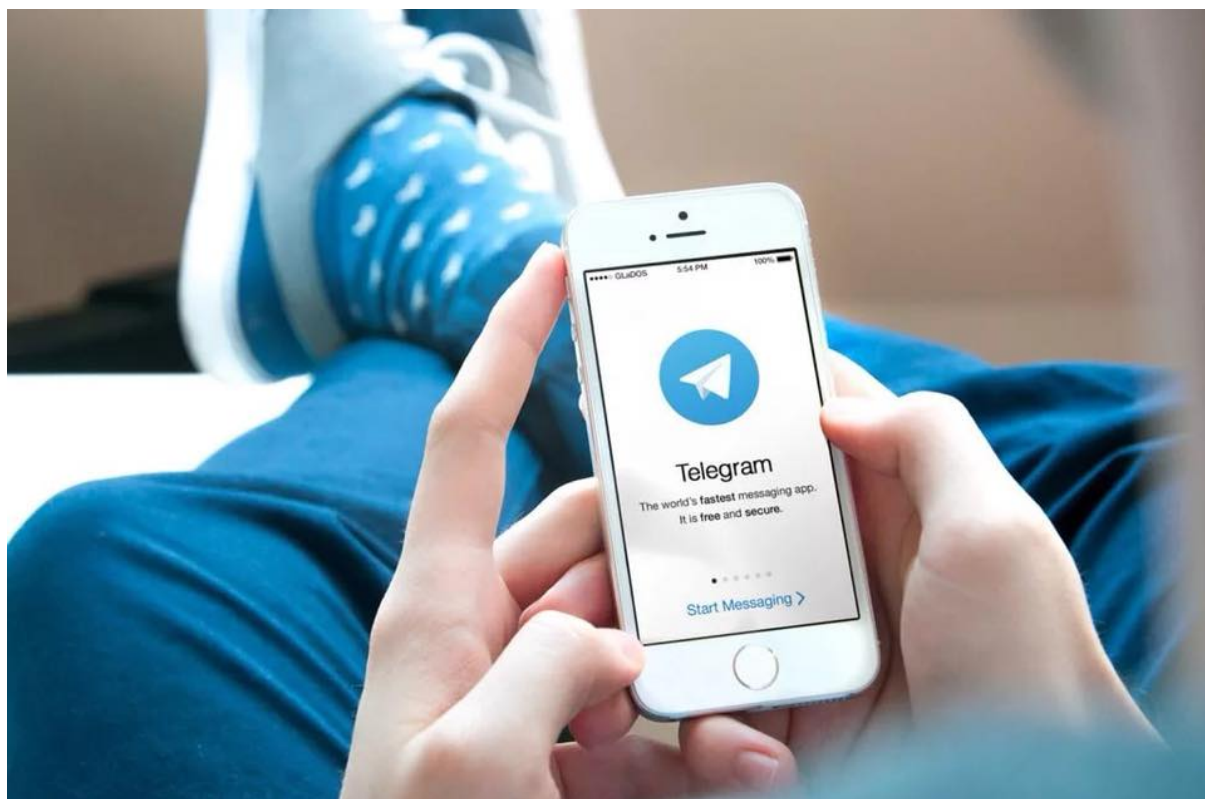
Блогнот. Соображения по поводу блокировки Телеграм

Телеграм работает в двух режимах. В режиме облачного чата и секретного чата. Защищенность облачного чата от спецслужб довольно низкая. Ведь спецслужбы всегда могут обеспечить себе подключение к аккаунту через мобильного оператора связи. Аутентификация полностью завязана на мобильный телефон, а проблем с доступом к данным телефона нет.

В режиме секретного чата все сложнее. Там применяется асимметричное шифрование, и приватный ключ доступен только непосредственно на устройстве, с которого инициирован секретный чат. Коммуникация строится на основе peer-to-peer, на серверах ничего не сохраняется, шифрование идёт end-to-end. Поэтому даже при получении доступа к аккаунту данных о секретных чатах не будет.

Вы это легко можете проверить даже на любых своих двух устройствах, подключённых к аккаунту. Облачные чаты доступны с любого устройства, плюс при подключении к аккаунту с нового устройства вы получите полную переписку, которую вели на других. Секретные чаты вы при этом не увидите нигде, кроме устройств, с которых они были инициированы.

Следовательно, вой насчёт страшной защищенности облачных чатов (а это режим по умолчанию, в котором происходит 99% коммуникаций обычных пользователей - просто смехотворен. Спецслужбы, безусловно, при желании могут получить доступ к облачным чатам любого пользователя без всякой помощи Дурова.



Насчёт секретных чатов. Все отличие Телеграм от других подобных коммуникаций с асимметричным шифрованием находится в области маркетинга и удобства интерфейса.

WhatsApp, например, по умолчанию использует режим асимметричного шифрования и в этом смысле гораздо неприятнее для спецслужб. Подобных мессенджеров большое количество и непонятно, чем секретные чаты Телеграм более опасны, чем иные средства, включая, например, зашифрованные с помощью PGP сообщения в обычной почте, игровом чате, мессенджере соцсети, обмена данными через файлообменник и т.п. Причём

говоря о защищенности, не надо совсем уж переоценивать спецслужбы, даже хорошо составленный пароль на симметричном шифровании для архиватора WinRAR станет таким крепким орешком, на который понадобятся серьёзные вычислительные ресурсы, которые попросту невозможно выделять под массовое изучение коммуникаций...

История противостояния спецслужб и разработчиков защищённых коммуникаций продолжается давным давно. Наиболее громким был процесс АНБ против Фила Циммермана, который в 1991 году выпустил программу асимметричного шифрования PGP. Интересно, что АНБ судилось 3 года с Циммерманом не потому что официально было против приватной переписки граждан США, а из-за распространения PGP за пределы США, что делало крайне затруднительным вскрытие иностранной переписки и нарушало законы США по распространению средств криптозащиты за пределы США. Однако, Циммерман остроумно обошёл запреты, выпустив исходные коды в виде книги, экспорт которых по законам США не может быть запрещен. Это интересная история, которую стоит изучить отдельно.

Выводом для нас будет лишь то, что история с попытками запрета средств шифрования далеко не нова. В России принят например довольно-таки технически безграмотный закон о запрете всех средств шифрования без лицензии ФСБ. Давным-давно, кстати. И де-факто не работающий в полном смысле. Почему он безграмотный? Потому что под его действие попадает сегодня почти все - от обычного архиватора, до защищённых протоколов обмена данными при работе с банковским приложением, например. В реальности, закон использовался скорее для контроля госзакупок и не более.

Что мы имеем сегодня? Блокировка Телеграм, безусловно, не только не усилит возможности контроля переписки злоумышленников в сети, но вероятно, в целом приведёт к падению степени контроля за коммуникациями. Причина заключается в массовом использовании прокси-серверов и VPN.

Параллельно существовали, существуют и будут существовать и развиваться все более совершенные средства защиты, которые уже давно сделали практически неуживимой в практическом плане переписку для тех, кто действительно озабочен безопасностью. Есть и массовые популярные средства, и знакомые широкой публике, но эффективные инструменты шифрования, как симметричного типа (с тем самым единственным паролем), так и асимметричного (с приватным и публичным ключами). Эффективность симметричного шифрования при этом в общем случае ВЫШЕ, чем асимметричного. Но в практическом плане симметричное шифрование всегда наталкивается на проблему безопасной передачи ключа шифрования, именно через его перехват производятся взломы. Асимметричное шифрование эффективно решает эту проблему.

Хочется подчеркнуть, что требование «передать ключи шифрования» бессмысленно в случае открытых чатов, поскольку доступ обеспечивается имеющимися возможностями спецслужб, а в случае секретных чатов невозможен к выполнению без катастрофического падения надёжности сервиса. Ведь в практическом плане это означает техническую возможность удалённого воровства приватного ключа! Проблема тут не в секретах от ФСБ. Помимо них мир наводнён хакерами всех мастей и видов, которые безусловно воспользуются этой лазейкой - это спровоцирует рост взломов и мошенничеств всех родов и видов. Возможность предоставления приватных ключей кому бы ни было, в итоге открывает ящик Пандоры, чреватый ростом преступлений!

В практическом плане эффективны многие средства закрытия информации. Даже относительно примитивные. Знаете ли вы что такое стеганография, например? Да и даже обычный эзопов язык полностью способен скрыть смысл сообщений, если не знать заранее о чем идёт речь. О даже теоретически невскрываемом (при отсутствии ошибок в обмене и применении) методе шифрблокнота тоже не забудем.

Успеха во вскрытии информации, особенно в потоке миллиардов (!) сообщений всегда добиваются с помощью первого этапа - обнаружении такого обмена, вычислении круга участников и т.д. А это методы, которые в общем случае далеки собственно от проблем мессенджеров и шифрования. Не будем забывать, что даже в бытовых взломах успех, как правило, обеспечивается методами социальной инженерии. Самое простое - подсмотр пароля. Но и методы терморектального криптоанализа никто не отменял. Кто знает, тот поймёт (с)

В общем, надеюсь после прочтения, вам станет понятно что борьба с терроризмом в случае блокировки Телеграм - просто предлог. Или же невероятная глупость. Удар нанесён обычным пользователям Телеграм, массовое использование которого, возможно будет несколько затруднено. Следует учитывать, что Телеграм всегда проводил эффективную политику пресечения использования сервиса в экстремистских целях. Поэтому обвинения в якобы потаканию терроризму просто возмутительны.

При этом, конечно, не исключено что и террористы использовали Телеграм. Впрочем, также террористы ели

хлеб, ездили на машине и общественном транспорте, пользовались телефонами и прочим, что окружает нашу жизнь. Это все нужно запретить?! Вы не находите, что логика запрета тут не сильно отличается от сентенции «Огурцы смертельно опасны, поскольку все умершие ели огурцы»?...

Также удивляет следующее. Жертв т.н. террора на порядки меньше, чем например жертв недисциплинированных водителей. В ДТП гибнут десятки тысяч и ранены сотни тысяч людей лишь в течении года. С 2000 года в ДТП погибло более полумиллиона (!) и ранено более 4 миллионов людей. Однако терроризм стал универсальным предлогом для чего угодно... Безусловно, это является манипуляцией.

Есть и другой аспект. Запрет Телеграм - это свидетельство неумения России обеспечить развитие. Да, именно так - развитие! Телеграм - глобальный сервис, созданный Павлом Дуровым и нашими командами программистов. Мы должны были бы гордиться и получать налоги с этого глобального проекта, чувствовать сопричастность к мировым трендам, но... Но бизнес этот не в России. Причина проста - под разговоры и провозглашения всяких инновации, к сожалению, в России сформировалась почти феодальная система отношений. Усугублённая капиталистической жадой наживы. И это очень прискорбно.

Запрет Телеграм наносит удар не по террористам и преступникам, а по огромному комьюнити совершенно добропорядочных пользователей, которым пришёлся по душе этот удобный мессенджер. Многие новостные агентства и системы оповещения завязаны на Телеграм. Крайне важное отличие Телеграм от других мессенджеров - это развитые средства автоматизации, боты и каналы. Они стали уже привычным и удобным средством работы с информацией для большого количества российских компаний! После запрета многим придётся радикально переделывать системы коммуникаций. Да, все проблемы решаемы, но какого черта мы теперь должны решать проблемы, которых не было и которые созданы нашим же правительством? Этот запрет - демонстрация неуважения к гражданам России!

Анализ технической стороны дела, а также текущих социально-политических отношений показывает, что запрет Телеграм является либо циничной попыткой принуждения Дурова к дележу прибылей Телеграм, либо попыткой расчистки места под свой сервис (под подозрение попадает, например, «ТамТам» с участием олигарха Усманова). Либо же это может быть объяснено просто тупостью.

Вот и выбирайте, чем является запрет Телеграм - тупостью или негодяйством. Третьего не дано.

Автор: Александр Евсин © Babr24 ИНТЕРНЕТ И ИТ, РОССИЯ 👁 5795 16.04.2018, 17:27 📌 941

URL: <https://babr24.com/?ADE=175503> Bytes: 9203 / 9156 [Версия для печати](#)

 [Порекомендовать текст](#)

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:

- [Телеграм](#)

- [ВКонтакте](#)

Связаться с редакцией Бабра:

newsbabr@gmail.com

Автор текста: **Александр Евсин.**

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: [@babr24_link_bot](https://t.me/babr24_link_bot)

Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

[Прислать свою новость](#)

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: equatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

[Подробнее о размещении](#)

[Отказ от ответственности](#)

[Правила перепечаток](#)

[Соглашение о франчайзинге](#)

[Что такое Бабр24](#)

[Вакансии](#)

[Статистика сайта](#)

[Архив](#)

[Календарь](#)

[Зеркала сайта](#)