digital

Безопасность до блокировки доведет

— технологии —

Одна из главных особенностей мессенджеров, декларируемая их создателями,— это безопасность общения. Digital изучил, какие методы шифрования используются в популярных мессенджерах и как на их работе в России отразится государственное регулирование.

ЕВГЕНИЙ ПАВЛЕНКО

Даже самый надежный метод шифрования end-to-end не может полностью застраховать пользователя от взлома переписки, уверены эксперты

Вернуть право на приватность

В 2013 году Павел Дуров запустил мессенджер Telegram под лозунгом «Taking back our right to privacy» («Вернем себе право на приватность»). Ставка на защиту данных сработала удачно: спустя три месяца после запуска Telegram приложение скачали более миллиона раз, а сейчас его аудитория в мире превышает 100 млн человек. При этом безопасность в мессенджерах стала идеей фикс для всех разработчиков.

За тайну переписки в мессенджерах отвечает функция шифрования. По словам замдиректора центра информационной безопасности «Инфосистемы Джет» Андрея Янкина, все шифрование упрощенно можно разделить на два типа: «клиент-сервер-клиент» и «клиент-клиент». «В первом случае данные расшифровываются на серверах мессенджера и могут быть переданы, например, правоохранительным органам. Во втором — прочесть данные в канале нельзя, владельцы мессенджера в принципе не могут передать данные посторонним лицам. Этим гордятся многие мессенджеры, и именно это вызывает недовольство у правоохранительных органов многих стран»,— говорит господин Янкин.

End-to-end-шифрование (то есть между конечными пользователями) впервые было внедрено в секретных чатах Telegram, которые отдельно может создавать пользователь, а в 2016 году появилось по умолчанию и в других популярных мессенджерах — WhatsApp и Viber.

«Шифрование end-to-end означает, что сообщение передается в виде миллионозначных чисел, которые закодированы шифровальным ключом. Этот ключ генерирует и хранит только устройство пользователя, поэтому сообщение не могут прочитать даже владельцы мессенджера. Сквозное шифрование надежно, ведь без ключа сообщение можно расшифровать только подбором всех чисел до миллиона знаков, а на это уйдут годы даже с кластерами из множества современных ЭВМ»,— объясняет директор IT-департамента QBF Иван Августон.

Но даже надежный метод шифрования не может полностью застраховать пользователей от взлома переписки. Ведущий специалист департамента сетевой безопасности компании Rcntec Герман Наместников отмечает, что проблема заключается в непосредственной защищенности мобильных устройств, завладеть которыми на необходимое для получения конфиденциальной информации время не составляет большого труда. Другая же проблема, по мнению эксперта, состоит в том, что в качестве второго фактора аутентификации (или для аутентификации вообще без использования пароля — что возможно в Telegram) используются коды, передаваемые посредством СМС.

«Несмотря на то, что Telegram, казалось бы, надежно защищает пользовательские данные, в апреле-мае 2016 года оппозиционные политики Георгий Албуров и Олег Козловский сообщили о взломе их учетных записей в этом мессенджере. В ходе их расследования было установлено, что к взлому привела утечка авторизационного СМС-кода, которая была организована, по словам Албурова и Козловского, МТС в интересах российских спецслужб. Говорить о том, что безопасность переписки в мессенджере зачастую зависит от безопасности пользовательского устройства, на котором он установлен и используется, думаю, не стоит»,— напоминает господин Наместников.

Глава компании «Интернет-розыск | CABIS» Игорь Бедеров согласен, что все методы шифрования выглядят, по меньшей мере, наивными в то время, когда на рынке имеется возможность «пробить» любой телефонный номер по базе сотового оператора, подделать паспорт и заказать дубль сим-карты в салоне сотовой связи. «На всю операцию будет затрачено не более 30 тыс. рублей. Получив копию симкарты жертвы, злоумышленник запросто переключит на себя все мессенджеры, социальные сети и электронную почту жертвы»,— отмечает господин Бедеров.

Кроме того, взлом переписки может произойти из-за уязвимостей в самом мессенджере. Так, в марте 2017 года исследователи израильской компании Check Point обнаружили уязвимость в веб-версиях мессенджеров WhatsApp и Telegram, которая подвергла риску полного захвата аккаунты миллионов пользователей .

«Используя эти уязвимости, злоумышленники могли полностью завладеть аккаунтом жертвы и получить доступ к ее персональным и групповым перепискам, фото, видео и другим переданным файлам, контактам. Уязвимость позволяет хакерам отправить жертве вредоносный код, зашитый в безобидную с виду картинку. Как только пользователь кликает на изображение, злоумышленник получает полный доступ к хранящимся данным пользователя WhatsApp или Telegram, что дает ему контроль над аккаунтом жертвы. Затем хакер может разослать вредоносный файл всем контактам жертвы — это позволяет организовать масштабную атаку»,— объясняет Никита Дуров, технический директор Check Point Software Technologies в России и СНГ.

Эксперты отмечают, что в таких вопросах, как безопасность, надо ставить под сомнение добросовестность разработчиков программного обеспечения. «Алгоритмы реализуют конкретные люди в конкретных компаниях. Что они заложили в свои конкретные решения, обычно тайна, но Эдвард Сноуден показал, что закладки — это обычное дело. Поскольку и алгоритмы шифрования, и ключи шифрования, и уже расшифрованные сообщения находятся внутри софта мессенджера на конечном устройстве, доступ к любой информации у владельца мессенджера может быть»,— комментирует гендиректор компании «Облакотека» Максим Захаренко.

Господин Августон говорит, что единственный способ удостовериться, что в приложении нет спрятанных закладок,— просмотреть исходный код приложения. «У WhatsApp, Viber и Skype протокол полностью закрыт для стороннего аудита, так что защищенность чатов в этих мессенджерах держится на честном слове: мы не будем читать вашу переписку и другим не позволим. В Telegram открыта большая часть исходного кода, это одна из причин считать этот мессенджер достаточно надежным»,— подчеркивает эксперт.

Кроме того, по его словам, WhatsApp и Viber компрометируют себя функцией создания копий истории переписки, а WhatsApp еще передает на сервер Facebook незашифрованные метаданные о характере общения пользователей.

Дуров против Роскомнадзора

В июне этого года глава Роскомнадзора Александр Жаров публично пригрозил заблокировать Telegram в России, если его создатель Павел Дуров не подчинится требованиям ведомства и не предоставит данные, необходимые для включения сервиса в реестр организаторов распространения информации. Предприниматель согласился предоставить эти данные не сразу, а после бурной дискуссии с главой Роскомнадзора, которая обозначила конфликт интересов между компаниями, для которых важна задача любой ценой сохранить тайну переписки пользователей, и государством, которое эти мессенджеры стремится зарегулировать.

Господин Дуров поставил главе Роскомнадзора в упрек заявление о том, что Telegram должен выдать спецслужбам «ключи для дешифрации», чтобы те могли читать переписку пользователей и ловить террористов. «Это требование не только противоречит 23-й статье Конституции РФ о праве на тайну переписки, но и демонстрирует незнание того, как шифруется коммуникация в 2017 году»,— писал господин Дуров. Обмен секретной информацией построен на оконечном шифровании, к которому у владельцев мессенджеров нет и не может быть «ключей для дешифрации», подчеркивал он.

В ответ господин Жаров назвал Telegram «если не основным, то одним из основных каналов коммуникаций для террористов». Впрочем, он отметил, что никакой речи о том, что будет доступ к переписке пользователей, не идет. В конце концов господин Дуров, согласившись предоставить Роскомнадзору данные для регистрации Telegram в реестре организаторов распространения информации, обозначил, что не будет выполнять российские законы, несовместимые с защитой частной жизни и политикой конфиденциальности мессенджера.

Максим Али, старший юрист юрфирмы «Максима Лигал», говорит, что уже сейчас мессенджер должен хранить логи переписок между пользователями, а с 1 июля 2018 года будет обязан сохранять и содержание переписки, а также предоставлять ФСБ России информацию для декодирования зашифрованных сообщений. Подобные требования — одно из положений «пакета Яровой» — законов антитеррористической направленности, которые внесла в Госдуму депутат Ирина Яровая.

«Очевидно, что такие обязанности идут вразрез с той политикой компании, которую декларирует господин Дуров. Более того, и он сам, и другие эксперты уже не раз говорили, что возлагаемые на сервисы обмена сообщениями обязанности зачастую являются технически нереализуемыми»,— считает юрист.

Запрет на анонимность

Кроме того, в конце июля президент России Владимир Путин подписал закон о регулировании мессенджеров (вступает в силу с 1 января 2018 года). Иван Августон из QBF отмечает, что два главных пункта в законе — это обязательная идентификация пользователей по номеру телефона и ограничение рассылки сообщений «содержащих информацию, распространяемую с нарушением требований законодательства РФ».

«По первому пункту все ясно: владельца аккаунта должны легко найти спецслужбы. В принципе, уже сейчас авторизация большинства аккаунтов проходит через номер мобильного и пользователям это не мешает. Но теперь мессенджеры должны сотрудничать с сотовыми сетями напрямую, и это выгодно операторам. Идея законопроекта появилась в Медиакоммуникационном союзе, куда входят операторы сотовой связи. Возможно, мессенджеры будут заключать договор с операторами на платной основе, но и сами мессенджеры в таком случае могут стать платными»,— комментирует эксперт.

Касательно обязанности мессенджера в течение суток блокировать запрещенную информацию, содержащуюся в переписке пользователей, у юриста Максима Али возникает вопрос: возможно ли технически отследить такой незаконный контент, причем так, чтобы не нарушить право граждан на тайну переписки?

«Владельцам мессенджеров имеет смысл уже сейчас заняться решением этой задачи, чтобы избежать в будущем санкций за нарушение законодательства. Для рядовых же пользователей важно будет то, что вместе с законом о мессенджерах одобрен закон о блокировке тех VPN, которые не согласятся фильтровать запрещенный контент. Поэтому пока что не стоит возлагать чрезмерных надежд на разного рода средства обхода блокировок»,— рассуждает юрист.

Также мессенджеры будут обязаны рассылать сообщения от имени органов государственной власти. «Для мессенджеров это означает дополнительные расходы, а для пользователей — потенциально — поток спама, если госорганы начнут злоупотреблять своими полномочиями. Хотя при должной реализации ничего плохого в этой идее, конечно, нет»,— комментирует Максим Али.

Следуя глобальной тенденции

Принятие в России «антианонимного» закона соответствует глобальной тенденции попытки усмирить мессенджеры, считает господин Августон. «В июне 2017 года в Германии приняли закон, согласно которому полицейские будут просматривать всю переписку подозреваемых в преступлениях в WhatsApp с помощью программы-шпиона. В Великобритании рассматривают законопроект об обязательном предоставлении данных о переписке по запросу спецслужб и о запрете шифрования переписки»,— говорит эксперт.

Опыт массового перехвата мессенджеров на уровне госслужб пока еще не столь значителен, а вот тенденция иметь возможность контролировать переписку как минимум в целях противостояния угрозе терроризма и организованной преступности характерна для всех развитых стран, говорит технический директор и основатель DeviceLock Ашот Оганесян. «Вплоть до прямого запрета использовать шифрование в мессенджерах в отдельных государствах. К примеру, власти Китая способны не просто перехватывать, но и в реальном времени цензурировать общение для исключения политически нежелательного контента в мессенджере WeChat, аудитория которого превышает 700 млн человек. Если в переписке будет детектировано одно из специфичных 200 слов и выражений, сообщение не будет отправлено»,— отмечает эксперт. Недавно выяснилось, что спецслужбы обладают возможностью еще и анализа изображений: некоторые пользователи не смогли получить отправленные им фотографии, добавляет он.

Следовать примеру Китая, который ограничил или существенно затруднил работу всех «чужих» приложений в стране, уже поздно, считает Дмитрий Хомутов, замдиректора по развитию компании «Айдеко». По его словам, аудитория иностранных мессенджеров успела набрать критическую массу, например, WhatsApp использует почти 70% пользователей «Вымпелкома» «Топорные методы регулирования отрасли (требованием ключей шифрования) не будут успешны прежде всего из-за того, что все компании — владельцы платформ находятся вне юрисдикции России, а основная часть их пользователей и коммерческого интереса также лежит за пределами России»,— говорит господин Хомутов.

Любой официальный запрет и блокирование мессенджеров, не сотрудничающих с государством, приводит к оттоку массовых пользователей, пользоваться ими продолжит только узкий слой технически продвинутых абонентов, говорит гендиректор компании «Айтоника» Алексей Болдырев. «С другой стороны, популярные мессенджеры не монетизируют сейчас миллионы своих пользователей напрямую, так что можно допустить, что они готовы будут рискнуть потерей массового российского пользователя, чтобы показать всему миру свою защищенность и сделать себе этим дополнительную рекламу»,— отмечает эксперт.

Иван Августон на примере Ирана вспоминает, как власти сначала боролись с Telegram, а потом начали сотрудничать. «В Иране Telegram — самый популярный мессенджер, потому что главные мировые соцсети заблокированы. Несколько раз власти Ирана блокировали Telegram, но потом перестали давить на владельцев мессенджера и усилили контроль над пользователями. Сейчас в Иране владелец Telegram-канала от пяти тысяч подписчиков проходит государственную регистрацию и подключает бота, который следит за контентом»,— говорит он.

Алексей Кириченко

ПРЯМАЯ РЕЧЬ

Максим Али, *старший юрист юрфирмы «Максима Лигал»:*

— По всей видимости, конфликт между Telegram и Роскомнадзором еще не исчерпан. И нам предстоит увидеть их дальнейшее противостояние.

Покупки запутались в сетях

— инструменты продвижения —

с14

Мессенджеры сейчас в тренде у маркетологов, так как это сравнительно новый рекламный канал, отметил основатель сервиса обратного звонка Perezvoni.com Виталий Ягодкин. По его словам, сегодня показатель CTR (коэффициент кликабельности) в правильных пабликах Telegram — один из самых высоких. Так как пока мало рекламодателей в мессенджерах, то и стоимость рекламы ниже, чем в соцсетях. «Как можно эффективно использовать Telegram для рекламы? Сейчас есть много тематических чат-ботов и каналов. Например, когда мы рекламируем сервис Perezvoni (продукт в сегменте b2b), то мы находим авторские каналы по продажам, маркетингу и закупаем рекламный пост. Именно авторские, где люди подписаны на авторитетного для них человека и рекламный пост выглядит как совет, а не как реклама. В сравнении с соцсетями „В контакте“ и Facebook, в Telegram на 20–25% больше переходов и продаж по рекламе. Это связано с тем, что пока этот источник не заспамлен и посты еще адекватно „заходят“. Конечно, это будет не всегда, скоро тренд и эффективность спадут. Есть маркетинговые агентства, которые, в том числе, размещают рекламу в Telegram, но это посредники, гораздо лучше открыть одну из бирж и связаться с автором напрямую»,— рассказал господин Ягодкин.

Максим Сундалов, напротив, считает, что использование мессенджеров для продвижения товаров и услуг дает противоположный эффект. По его мнению, 99,9% людей считают этот «маркетинговый ход» навязчивым, вторжением в личное пространство. «Подобные рассылки, как и холодные звонки, застающие врасплох, не вызывают никаких положительных эмоций, но действуют раздражающе. Даже если вы предварительно заручились согласием клиента получать от вашей компании уведомления о чем-либо, в большинстве случаев ваша рассылка попадает в спам-фильтр. Исключением являются паблик-чаты компании в Viber, на которые подписывается сам клиент. Это, кстати, самый популярный мессенджер в России»,— прокомментировал господин Сундалов.

Основатель Qometa Сергей Филимонов отметил, что постепенно появляется интерес продвигаться в мессенджерах, но это пока мало у кого получается из-за того, что часто аудитория пользуется разными мессенджерами. Кроме этого, такие приложения для человека пока еще остаются личной территорией, где неприемлема реклама, а также просто мало успешных кейсов на которых можно учиться.

Президент группы компаний Pro-Vision Владимир Виноградов говорит, что даже маститые рекламщики не могут до конца сказать, насколько глубок потенциал мессенджеров как канала продвижений. Сейчас речь идет скорее о некоем периоде «обкатки», поскольку нет четкого понимания, как их использовать для брендов с выгодой. «Главное преимущество мессенджеров в том, у них огромная аудитория и они всегда под рукой, точнее в руке,— рассуждает господин Виноградов.— Согласно результатам исследований, проведенных аналитическим агентством TNS, среднестатистический пользователь смартфона смотрит на экран своего гаджета до 150 раз в день. Ежедневно владелец коммуникатора обращается к его функциям на протяжении 3,2 часа (49 дней в год). При этом, несмотря на многообещающую статистику, работать с мессенджерами нужно аккуратно. Если форумы и соцсети — это публичное пространство, где пользователь может быть относительно лояльным к рекламе и посланиям брендов, то мессенджер — это личная переписка, где подобный контент зачастую вызывает негатив».

Юлия Рыжих отмечает, что мессенджеры пока используются как дополнительный канал для коммуникации с пользователями (общение клиентов с брендами в удобном для них канале), хотя Viber в прошлом году дал возможность создания официальных бизнес-аккаунтов (и при согласии пользователя проводит рассылки рекламного содержания — замена привычным СМС). Telegram пока использует группы для размещения новостей и полезного контента, но скорее всего, также работает над возможностью монетизации, это вопрос времени.

Лидия Горборукова