УДК 004.7 : 003.26

К ВОПРОСУ О БЕЗОПАСНОМ ШИФРОВАНИИ В ИНТЕРНЕТ-МЕССЕНДЖЕРАХ

ON THE ISSUE OF SECURE ENCRYPTION IN INTERNET INSTANT MESSENGERS

Молоков Вячеслав Витальевич,
начальник кафедры информационно-правовых дисциплин и специальной техники Сибирского юридического института МВД России (г. Красноярск),
кандидат технических наук, доцент

vvmolokov@mail.ru

Ключевые слова:
криптография, сквозное шифрование, интернет-мессенджеры, безопасность информации, Интернет.

В статье рассматриваются современные методы обеспечения безопасности интернет-коммуникаций. Раскрывается принцип end-to-end шифрования, использующийся в большинстве интернет-мессенджеров. Обозначаются проблемы сохранения конфиденциальности передаваемой и обрабатываемой с их помощью информации и формулируются выводы о возможной уязвимости интернет-мессенджеров.

Keywords:
cryptography, end-to-end encryption, Instant messengers, information security, Internet.

This paper discusses modern methods of ensuring the safety of Internet communications. The principle of end-to-end encryption, which is used in most Internet messengers, is revealed. The problems of maintaining the confidentiality of information transmitted and processed by them are identified and conclusions are drawn about the possible vulnerability of Internet instant messengers.

Эпоха существования интернет-коммуникаций на каждом этапе своего развития демонстрировала нарастающий тренд в обеспечении безопасности передаваемой и обрабатываемой информации. А ведь во времена зарождения Всемирной паутины было лишь одно стремление – обеспечить максимальную доступность информации всем пользователям Интернета. Глобальное виртуальное пространство виделось открытым, неконтролируемым, без цензуры и иных вмешательств в информационное взаимодействие со стороны третьих лиц. Однако реалии последнего десятилетия изменили отношение пользователей к безопасности персональных данных, да и иного рода личной информации, передаваемой и постоянно размещенной на просторах мирового облачного хранилища, каким можно считать Всемирную паутину. Такому поведению способствовали провокации со стороны хакерских групп, развивающаяся индустрия интернет-мошенничества, большой объем обрабатываемой персональной информации, нагнетание общественного мнения о возможной слежке спецслужб за гражданами и т.п. Все это подтолкнуло к развитию технологий безопасной передачи данных в сетях. Основным способом такой защиты является криптография – шифрование данных на стадии как передачи, так и хранения. Криптографическое закрытие информации на рубеже веков было и остается мощным инструментом обеспечения тайны, что неминуемо гарантировало его применение в различных сферах информационной безопасности. Современные алгоритмы и криптографические средства способны обеспечивать защиту государственной тайны, не говоря уже об иной конфиденциальной информации. В этих условиях рассмотрим, какие методы шифрования наиболее популярны в телекоммуникационных сетях, как они способны обеспечить тайну личных данных пользователей сети Интернет.

Обозначим основные методы шифрования данных, использующиеся в современной криптографии. Это симметричное и ассиметричное шифрование. В симметричном шифровании, по аналогии с дверным замком, для закрытия и открытия информации используется один и тот же ключ. В ассиметричном шифровании применяется пара взаимно связанных ключей, генерируемых совместно, при этом один ключ является публичным, а второй – секретным. Такой механизм позволяет осуществлять взаимно исключающие действия: шифровать открытым ключом, расшифровывать закрытым и наоборот, это зависит от объекта применения, например, использование цифровой подписи. В телекоммуникационных системах в основном ставится задача шифрования в реальном времени, что предъявляет определенные требования как к алгоритму, так и к способу обмена ключами. Поэтому чаще всего используются гибридные криптосистемы, в которых канальное шифрование осуществляется симметричной криптографией, а уже для секретной передачи сеансового симметричного ключа применяется ассиметричный алгоритм. Частным случаем

такого шифрованного взаимодействия можно считать end-to-end шифрование, когда только пользователи, участвующие в обмене информацией, имеют к ней доступ. Самый известный метод реализации оконечного шифрования – алгоритм Диффи-Хеллмана[1]. Задача алгоритма состоит в безопасной передаче симметричного ключа шифрования в открытом канале данных.

Рассмотрим, где, как и зачем применяется шифрование, каким образом оно может обезопасить передачу информации в сети Интернет.

Основной способ информационного взаимодействия пользователей сети Интернет заключается в просмотре содержимого ресурса либо работе с ним, а также переписке с остальными участниками информационного процесса посредством интернет-мессенджеров. Оба варианта информационного контакта преследуют цели безопасной передачи данных по телекоммуникационным каналам, исключающей перехват и использование в корыстных целях конфиденциальных данных, а также защиты от слежки.

На текущий момент безопасность большинства сайтов обеспечивает расширенный протокол передачи гипертекстовых данных HTTPS, который использует систему сертификатов и удостоверяющих центров для подтверждения подлинности открытых ключей серверов и организации канального шифрования между клиентом и сетевым ресурсом. Данный протокол гарантирует безопасную передачу любых пользовательских данных, будь то пароли, персональная информация или иные данные. Действительно, это надежный протокол электронного взаимодействия, но защищающий от перехвата только данные, направляемые в канал связи. Если существуют уязвимости на конечных устройствах электронного обмена, то информация может быть скомпрометирована. Например, если компьютерное абонентское устройство заражено троянской программой, то данные могут быть перехвачены до начала действия алгоритма потокового шифрования. Та же ситуация возможна на стороне сервера, утечка информации допустима в случае наличия уязвимостей в защите ресурса. И последнее, данный протокол никак не защищает пользовательскую информацию от возможности ее документирования правоохранительными органами, но такое мероприятие применяется только на законных основаниях. Как известно, Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» предусматривает хранение оператором связи полной информации абонентов до 6 месяцев, а факты ее передачи – до 3 лет.

Объективно наибольший поток личной конфиденциальной информации передается посредством интернет-мессенджеров. На рынке интернет-услуг их предлагается большое количество. Одни мессенджеры очень популярны (например, WhatsApp, Viber, Telegram) другие – менее (например, Signal, Pinngle, Threema, VIPole), но каждый из перечисленных сервисов непременно предла-

1 Основы шифрования (часть 1) – Алгоритм Диффи-Хеллмана. URL: https://www.securitylab.ru/analytics/478912.php (дата обращения: 10.05.2020).

гает своим абонентам конфиденциальное общение, без возможности перехвата и передачи содержимого сообщений специальным службам. Все эти утверждения поддерживаются заявлениями об использовании алгоритма сквозного шифрования, ранее упомянутого нами как end-to-end. Причем используются современные модификации алгоритмов с открытым ключом, например криптография на эллиптических кривых[2]. Каждый из продуктов декларирует неуязвимость и приватность переписки, утверждается, что даже не доставленные абонентам сообщения хранятся на серверах в зашифрованном виде, а доступа к ключам расшифровки у компаний нет. На этой волне обеспечения полной конспирации стал так популярен мессенджер Telegram. Еще большей популярности ему добавила шумиха с попытками блокировки сервиса якобы за нежелание передать органам безопасности ключи доступа к шифрованным сообщениям.

Постараемся разобраться в надежности и возможности обеспечения полной конфиденциальности информации, передаваемой с помощью интернет-мессенджеров. Для этого сформулируем несколько тезисов:

– оригинальный алгоритм Диффи-Хеллмана, как и другие современные технологии сквозного шифрования, в настоящий момент обладает высокой криптостойкостью, что не позволяет их взломать при утечке на канале связи;

– большинство интернет-мессенджеров являются программными продуктами с закрытым кодом, следовательно, отсутствует возможность проверить используемые алгоритмы шифрования на наличие уязвимостей и бэкдоров[3].

Разработчики интернет-мессенджеров заявляют о полной анонимности переписки пользователей, однако по существующему законодательству Российской Федерации операторы связи, осуществляющие свою деятельность на территории страны, обязаны предоставлять сведения о передаваемых сообщениях по запросу правоохранительных органов [1].

Каждое мобильное устройство связи, работающее, к примеру, под управлением операционных систем Android или iOS, в большинстве случаев автоматически создает резервные копии системы и приложений со всеми пользовательскими данными. Вопрос доступа самих интернет-компаний к данным этих копий является открытым. Стоит заметить, что и сами мессенджеры хранят историю переписки.

Таким образом, передаваемые по интернет-каналам сообщения могут быть абсолютно защищены от перехвата, но безопасность и конфиденциальность

2 Доступно о криптографии на эллиптических кривых. URL: https://habr.com/ru/post/335906 (дата обращения: 10.05.2020).

3 Шифруйся грамотно! Почему мессенджеры не защитят тайну твоей переписки. URL: https://rnbee.ru/post-wall/shifrujsja-gramotno-pochemu-messendzhery-ne-zashhitjat-tajnu-tvoej-perepiski (дата обращения: 10.05.2020).

информации на конечном оборудовании, включая серверы интернет-компаний, не так надежно гарантированы. Также невозможно сохранить «лицо» компании организатора услуг связи, если оно соблюдает законодательство страны, в которой осуществляет свою деятельность, при этом алгоритмы шифрования, которые ими позиционируются, невозможно проверить, а субъективные оценки надежности не выдерживают критики. Уточним, что в рамках действия закона о безопасном Интернете все операторы связи и интернет – компании, не соблюдающие требования законодательства, будут блокированы и уже не теми устаревшими методами, что использовались не так давно в отношении мессенджера Telegram, так как Федеральным законом от 1 мая 2019 г. № 90-ФЗ были внесены изменения в федеральные законы «О связи» и «Об информации, информационных технологиях и о защите информации».

Анализируя представленные доводы, можно сделать вывод, что конфиденциальность личной переписки пользователей интернет-мессенджеров, обеспечивающаяся встроенными средствами криптографии, условна. Однако лицам, которые пользуются мессенджерами в повседневной жизни, а не используют их в противоправной деятельности, не следует опасаться разглашения информации, такая параноидальная конфиденциальность излишняя.

Библиографический список

1. Молоков, В.В. Вопросы технического противодействия экстремизму и терроризму в сети Интернет / В.В. Молоков // Современные системы безопасности – Антитеррор : материалы конгрессной части XIV специализированного форума (30-31 мая 2018 г.) / отв. ред. С.В. Гапонов. – Красноярск : СибЮИ МВД России, 2018. – Ч. 2. – С. 56-59.