Отечественные разработки и международная стандартизация

в сфере защиты информации

Валерий СМЫСЛОВ,
архитектор системы, АО «ЭЛВИС-ПЛЮС»

В массовом сознании ситуация в области средств вычислительной и телекоммуникационной техники, а также ПО выглядит примерно так: «Все идет с Запада, мы лишь используем готовые решения». Однако в ряде областей мы если и не «впереди планеты всей», то по крайней мере на острие технического прогресса. Разработки, которые зарождаются в нашей стране, становятся международными стандартами и применяются во всем мире. В качестве примера можно привести участие специалистов ЭЛВИС-ПЛЮС в развитии протокола IPsec (IP security) и, в частности, его адаптации для алгоритмов постквантовой криптографии.

Протокол, а точнее семейство протоколов IPsec, был разработан в IETF (Internet Engineering Task Force) как средство защиты трафика в сетях TCP/IP на сетевом уровне, т. е. на уровне IP-пакетов. Архитектурно IPsec состоит из двух частей – протокола непосредственной защиты IP-трафика ESP (Encapsulating Security Payload) и протокола управления ключами IKEv2 (Internet Key Exchange version 2). Протокол IKEv2 является ядром IPsec: он обеспечивает согласование параметров защиты трафика, взаимную аутентификацию сторон и выработку ключевого материала для протокола ESP. За последние годы для протокола IKEv2 было разработано множество расширений, в том числе при активном участии специалистов «ЭЛВИС-ПЛЮС». Эта работа продолжается и сейчас, в частности, в области адаптации IKEv2 для противодействия атакам с использованием квантовых компьютеров.

IPsec начинал создаваться в 1990-е гг., его ядро окончательно оформилось к 2005 г. Теоретические основы для построения квантовых компьютеров были известны давно и даже описаны алгоритмы для них (например, алгоритм Шора был разработан в 1994 г.), однако сами квантовые компьютеры в то время фигурировали разве что в научно-фантастической литературе. С начала XXI века в лабораториях стали появляться работающие образцы квантовых компьютеров, сначала «игрушечной» размерности, но постепенно увеличиваясь и демонстрируя прогресс.

Насколько реально в обозримом будущем создание криптографически значимого квантового компьютера (Cryptographically Relevant Quantum Computer)? Такой компьютер должен иметь несколько тысяч логических кубитов, т. е. порядка 100 тыс. – 1 млн кубитов физических. Пока в действующих образцах квантовых компьютеров речь идет о сотнях физических кубитов, но прогресс в этой сфере непредсказуем.

В чем опасность криптографически значимого квантового компьютера для протоколов защиты информации? Почти все современные протоколы в той или иной степени используют криптографию с открытым ключом – алгоритмы цифровой подписи для аутентификации и алгоритм Диффи – Хеллмана для выработки общего ключа. Стойкость алгоритмов с открытым ключом базируется на том, что науке неизвестны методы быстрого разложения на множители произведения двух больших простых чисел или быстрого вычисления дискретного логарифма в конечном поле. Но это справедливо только для классических компьютеров. Для квантовых компьютеров существует алгоритм Шора, позволяющий выполнять эти операции за полиномиальное время, т. е. фактически «мгновенно» с точки зрения криптографии. Единственная причина, по которой современные протоколы защиты информации еще не взломаны, – нет квантового

компьютера достаточной размерности, или криптографически значимого.

Удастся ли его создать (если вообще удастся) – вопрос открытый, но криптографы уже готовятся к его появлению. Существуют два направления развития, которые могут защитить криптосистемы от атак с использованием квантовых компьютеров.

Первое – отказ от криптографии с открытым ключом в пользу симметричной или применение смешанных схем. Алгоритм Гровера для квантовых компьютеров теоретически может вдвое снизить эффективную длину ключа, но при тех длинах ключей для симметричных криптоалгоритмов, которые повсеместно используются (например, в российских алгоритмах шифрования «Кузнечик» и «Магма» ключ длиной 256 бит), снижение эффективной длины в два раза не позволяет их взломать за реальное время. Однако повсеместный переход на использование только симметричной криптографии представляется малореальным ввиду проблем с масштабированием и деградации базовой функциональности (например, средствами симметричной криптографии нельзя создать электронную подпись документа).

Второе направление – создание новых криптографических алгоритмов, функционально дублирующих возможности существующих с открытым ключом, но базирующихся на иных математических принципах, о которых известно, что они стойки к атакам с применением квантовых компьютеров. Направление, получившее название постквантовой криптографии (Post-Quantum Cryptography – PQC), бурно развивается в последние годы. В 2016 г. американский национальный институт стандартов и технологий (National Institute of Standards and Technology – NIST) объявил конкурс на постквантовые алгоритмы подписи и выработки общего ключа. К настоящему времени завершились три этапа конкурса, объявлен четвертый. Промежуточный результат: объявление в июле 2022 г. победителей третьего этапа, которыми стали алгоритм выработки общего ключа CRYSTALS-KYBER и три алгоритма подписи: CRYSTALS-DILITHIUM, FALCON и SPHINCS+. В России также ведется разработка постквантовых криптографических алгоритмов в рамках деятельности технического комитета по стандартизации «Криптографическая защита информации» (ТК26).

Казалось бы, осталось лишь заменить в протоколах существующие алгоритмы постквантовыми, но это непросто. Основная проблема – практически все постквантовые алгоритмы имеют значительно больший размер открытого ключа, чем классические. Для некоторых алгоритмов размер столь велик, что открытый ключ не помещается в структуры данных, а если и помещается, то вызывает множество не известных ранее проблем, связанных с передачей большого объема данных при установлении защищенного соединения (например, растет риск атаки отказа в обслуживании). Вторая проблема – многие постквантовые алгоритмы недостаточно исследованы, поэтому среди криптографов бытует мнение, что целесообразно комбинировать несколько алгоритмов. Такой подход называется гибридным, но существующие протоколы, как правило, не предусматривают возможности его использования. То есть для использования постквантовых алгоритмов в существующих протоколах требуется доработка последних.

Возвратимся к IPsec, точнее к IKEv2. Его доработка в IETF в свете угроз квантовых компьютеров началась в 2015 г. по двум направлениям. В качестве краткосрочного решения договорились использовать в IKEv2 смешанную схему выработки общего ключа, когда наряду с алгоритмом Диффи – Хеллмана в процессе участвует симметричный предварительно распределенный ключ. В результате работы, выполненной специалистами Cisco Systems и ЭЛВИС-ПЛЮС, в 2020 г. появился RFC 8784 «Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2».

Второе (долгосрочное) решение – использование постквантового гибридного обмена ключами в IKEv2 – стартовало в IETF в 2017 г. Этот гораздо более сложный путь требовал существенных изменений в протоколе. В первую очередь в IKEv2 был добавлен новый «промежуточный» обмен сообщениями, который позволил последовательно использовать несколько алгоритмов выработки общего ключа. Спецификация «промежуточного» обмена разработана в «ЭЛВИС-ПЛЮС» и в 2022 г. опубликована как RFC 9242 «Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)». Необходимость нового обмена обусловлена тем, что из-за значительного размера открытых ключей при попытке передачи их в начальном обмене возникают проблемы с IP-фрагментацией (IKEv2 использует UDP как транспорт). Поэтому фрагментация должна выполняться на прикладном уровне, т. е. в самом IKEv2. Возможность фрагментации сообщений в IKEv2 присутствует (кстати, этот механизм также был разработан в «ЭЛВИС-ПЛЮС» и принят в качестве международного стандарта в 2014 г., RFC 7383 «Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation)», но ее невозможно использовать в начальном обмене сообщениями, отсюда необходимость нового обмена. Затем была разработана спецификация, описывающая, как именно общий ключ вырабатывается путем последовательного применения нескольких алгоритмов выработки общего ключа (как классических, так и постквантовых) с использованием «промежуточного» обмена. В разработке спецификации участвовали представители компаний Post-Quantum, Quantum Secret, Cisco Systems, ISARA Corporation, Philips и ЭЛВИС-ПЛЮС. В настоящее время спецификация находится на рецензировании в IETF и должна быть опубликована до конца текущего года.

Большая часть этих стандартов впоследствии возвращается в Россию в виде адаптированных для использования алгоритмов ГОСТ рекомендаций по стандартизации, которые разрабатывает ТК26 при непосредственном участии специалистов ЭЛВИС-ПЛЮС, а также реализуются в семействе продуктов VPN/FW ЗАСТАВА (zastava.ru), включая указанные выше стандарты использования постквантовой криптографии в IPsec. ■