|  |  |  |
| --- | --- | --- |
|  | Всемирная ассамблея по стандартизации электросвязи (ВАСЭ-24)Нью-Дели, 15−24 октября 2024 года |  |
|  |
|  |  |
| ПЛЕНАРНОЕ ЗАСЕДАНИЕ | Дополнительный документ 42к Документу 37-R |
|  | 22 сентября 2024 года |
|  | Оригинал: английский |
|  |
| Администрации стран – членов Азиатско-Тихоокеанского сообщества электросвязи |
| ПРОЕКТ РЕЗОЛЮЦИИ [APT-PQC] – содействие внедрению постквантовой криптографии и переходу на нее |
|  |
|  |

|  |  |
| --- | --- |
| **Резюме**: | В настоящем документе содержится предложение новой Резолюции ВАСЭ о содействии внедрению постквантовой криптографии и переходу на нее. |
| **Для контактов**: | г-н Масанори Кондо (Mr Masanori Kondo)Генеральный секретарь Азиатско-Тихоокеанское сообщество электросвязи | Эл. почта: aptwtsa@apt.int |

Введение

Криптографические алгоритмы представляют собой ключевую основу сетей для укрепления доверия и безопасности при использовании ИКТ.

При появлении доступа к криптографически значимым квантовым компьютерам большинство существующих алгоритмов с открытыми ключами и связанных с ними протоколов окажутся уязвимыми для атак на основе использования квантовых компьютеров. Благодаря исключительной вычислительной мощности квантовые компьютеры представляют собой квантовую угрозу и потенциально могут взломать широко используемые криптографические алгоритмы, включая RSA и ECC (криптография на основе эллиптических кривых). В настоящее время разрабатывается набор криптографических алгоритмов, называемых постквантовой криптографией (PQC), которые считаются обеспечивающими квантовую безопасность или квантовоустойчивыми, что означает, что они, как ожидается, останутся безопасными даже при наличии криптографически значимых квантовых компьютеров.

В этой Резолюции признается, что определение PQC ИК17 относится к классическим квантовоустойчивым алгоритмам.

В настоящее время доверительная инфраструктура сетей связи основана на традиционных криптографических алгоритмах, таких как алгоритм Диффи-Хеллмана и RSA, которые уязвимы для квантовых угроз. Таким образом, в преддверии появления квантовых компьютеров крайне важным становится переход сетей ИКТ на квантовоустойчивую доверительную инфраструктуру.

Несмотря на то что PQC использует существующую инфраструктуру и предлагает экономически эффективное и хорошо зарекомендовавшее себя решение, обеспечивающее квантовую безопасность, для полного перехода на PQC организациям потребуются значительное время и ресурсы.

В связи с этим перед исследовательскими комиссиями МСЭ-Т неизбежно возникает необходимость активного ведения работы по стандартизации в целях содействия внедрению постквантовой криптографии в сетях электросвязи/ИКТ и переходу на нее.

Кроме того, ИК17 МСЭ-Т в процессе подготовки к ВАСЭ-24 согласовала "использование постквантовой криптографии" в качестве новой темы на следующий исследовательский период (2025–2028 гг.).

Предложение

На основании вышеизложенной информации администрации стран – членов АТСЭ предлагают рассмотреть на ВАСЭ-24 возможность принятия новой Резолюции ВАСЭ о содействии внедрению постквантовой криптографии и переходу на нее.

ADD APT/37A42/1

ПРОЕКТ НОВОЙ РЕЗОЛЮЦИИ [APT-PQC] (Нью-Дели, 2024 г.)

Содействие внедрению постквантовой криптографии и переходу на нее

(Нью-Дели, 2024 г.)

Всемирная ассамблея по стандартизации электросвязи (Нью-Дели, 2024 г.),

напоминая

*a)* о Резолюции 130 (Пересм. Бухарест, 2022 г.) Полномочной конференции об усилении роли МСЭ в укреплении доверия и безопасности при использовании информационно-коммуникационных технологий;

*b)* о Резолюции 50 (Пересм. Женева, 2022 г.) настоящей Ассамблеи о кибербезопасности;

*c)* о резолюции 57/239 Генеральной Ассамблеи Организации Объединенных Наций (ГА ООН) о создании глобальной культуры кибербезопасности;

*d)* о резолюции 78/287 ГА ООН о Международном годе квантовой науки и техники, 2025 год,

учитывая,

*a)* что криптографические алгоритмы имеют существенное значение для укрепления доверия и обеспечения безопасности при использовании информационно-коммуникационных технологий (ИКТ);

*b)* что появление криптографически значимых технологий квантовых вычислений поставит под угрозу многие из существующих криптографических алгоритмов, особенно криптографию с открытым ключом, которая широко используется для защиты цифровой информации;

*c)* что криптографические алгоритмы, от которых зависит инфраструктура электросвязи/ИКТ, используются во всем мире в компонентах самых разных систем связи, обработки и хранения данных;

*d)* что при появлении доступа к криптографически значимым квантовым компьютерам большинство существующих алгоритмов с открытыми ключами и связанных с ними протоколов окажутся уязвимыми для атак на основе использования квантовых компьютеров;

*e)* что алгоритмы PQC возможно применять в существующей инфраструктуре и в них могут использоваться системные знания и опыт для реализации решений, обеспечивающих квантовую безопасность;

*f*) что типовые приложения PQC могут охватывать все секторы, например IMT‑2020/IMT‑2030 и DLT;

*g)* что необходимо международное сотрудничество и обмен информацией для устранения угроз безопасности, создаваемых криптографически значимыми квантовыми компьютерами;

*h)* что роль МСЭ направлена на внедрение PQC и переход на нее, чтобы укрепить безопасность и доверие при использовании инфраструктуры электросвязи/ИКТ, а не на стандартизацию алгоритмов или протоколов PQC;

*i)* что PQC может содействовать разработке инфраструктуры доверия, которая способна противостоять воздействию как квантовых, так и классических компьютеров и может взаимодействовать с существующими протоколами и сетями связи;

*j)* что переход от существующих классических криптографических систем к системам на основе PQC, способным противостоять атакам на основе квантовых вычислений, является долгосрочным и дорогостоящим проектом. В настоящее время в мире уже существует большое количество вертикальных отраслей, изучающих возможность применения PQC и перехода на нее, и отрасли электросвязи/ИКТ уже сейчас необходимо готовиться к развитию этой тенденции;

*k)* что процесс перехода на PQC чрезвычайно сложен и займет много лет, поскольку требует замены криптографических алгоритмов, обновления криптографических протоколов, схем, компонентов, инфраструктуры и т. д. на криптографические технологии, обеспечивающие квантовую безопасность;

*l)* что переход на PQC может включать проектирование и разработку механизмов для гибкого обновления криптографических систем и итеративное обновление информационных систем криптографических приложений в целях упрощения процесса внедрения будущих алгоритмов PQC;

*m)* что NIST (Национальный институт стандартов и технологий) ведет непрерывную работу над оценкой безопасности алгоритмов PQC,

учитывая далее,

*a)* что в Рекомендации МСЭ-T X.1811 приведены руководящие указания по безопасности для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность; в документе TR.qs-dlt приведены руководящие указания для системы DLT, обеспечивающей квантовую безопасность, для защиты DLT; а в ИК17 МСЭ-Т разрабатываются два Технических отчета, в том числе "Руководящие указания по использованию усовершенствованной криптографии на основе PQC";

*b)* что РГ2/ПК27/ОТК1 ИСО/МЭК и Европейский институт стандартизации электросвязи (ЕТСИ) работают над стандартизацией постквантовой криптографии (PQC) и обмениваются информацией по PQC;

*c)* что Национальный центр передового опыта в области кибербезопасности (NCCoE) NIST инициирует разработку методов, облегчающих переход от существующего набора криптографических алгоритмов с открытым ключом к алгоритмам замещения, которые устойчивы к атакам, основанным на использовании квантовых компьютеров,

отмечая,

*a)* что МСЭ-T следует играть ведущую роль в разработке стандартов, направленных на укрепление доверия и обеспечение безопасности при использовании ИКТ;

*b)* что в настоящее время по инициативе NIST начат процесс разработки, оценки и стандартизации одного или более устойчивых к квантовым угрозам криптографических алгоритмов с открытым ключом;

*c)* что NIST выпустил стандарты для трех алгоритмов PQC;

*d)* что IETF создала Рабочую группу по использованию постквантовых технологий в протоколах (PQUIP) для учета инженерных проблем PQC и вопросов, связанных с переходом на нее, а также опыта, касающегося деятельности IETF, и активного внедрения PQC в протоколы IETF, включая IPSec, TLS и OpenPGP;

*e)* что ОТК1/РГ2/ПК27 ИСО/МЭК по криптографии и механизмам безопасности ведет работу над стандартизацией алгоритмов PQC, отобранных NIST;

*f)* что рабочая группа ETSI по криптографии, обеспечивающей квантовую безопасность (QSC), выпустила Технический отчет, в котором определены стратегии перехода и рекомендации для схем обеспечения квантовой безопасности;

*g)* что 17-я Исследовательская комиссия МСЭ-Т является ведущей исследовательской комиссией по вопросам безопасности в МСЭ-Т, на которую возложена задача по координации деятельности в области безопасности в рамках МСЭ-Т и с другими организациями по разработке стандартов и форумами, и разрабатывает основы для совершенствования сотрудничества,

признавая,

*a)* что в определении ИК17 PQC относится к классическим квантовоустойчивым алгоритмам;

*b)* что разработка структуры для оценки и понимания развертывания существующих криптографических систем имеет важное значение для организаций, планирующих переход от существующего набора криптографических алгоритмов с открытым ключом к алгоритмам PQC, устойчивым к атакам на основе использования квантовых компьютеров;

*c)* что при переходе на PQC важны три параллельных рабочих потока, связанных с алгоритмами (стандартизация алгоритмов PQC), протоколами (обеспечение протоколов безопасности с поддержкой PQC) и системами (интеграция PQC в системы и процессы),

решает

1 продолжить разработку необходимых Рекомендаций для содействия внедрению PQC и переходу на нее в рамках сети электросвязи/ИКТ;

2 разработать новые Рекомендации, направленные на популяризацию необходимости создания надежной инфраструктуры на основе PQC, и планы действий по переходу на PQC для использования в инфраструктуре электросвязи/ИКТ после того, как организации, в наибольшей степени подходящие для выполнения этой работы, разработают необходимые алгоритмы, протоколы и стандарты;

3 разработать структуру для оказания помощи организациям в оценке развертывания существующих криптографических систем и планировании перехода на PQC,

поручает 17-й Исследовательской комиссии как ведущей исследовательской комиссии по вопросам безопасности, а также другим соответствующим исследовательским комиссиям Сектора стандартизации электросвязи МСЭ

1 провести оценку существующих, дорабатываемых и новых Рекомендаций в отношении внедрения PQC и перехода на нее;

2 продолжать разрабатывать Рекомендации и другие публикации МСЭ-Т, содержащие руководящие указания и передовой опыт, которые помогут организациям подготовиться к внедрению PQC и переходу на нее;

3 взаимодействовать с заинтересованными сторонами отрасли для сбора аналитических материалов и передового опыта в целях содействия внедрению PQC и переходу на нее в рамках сети электросвязи/ИКТ;

4 сотрудничать с другими исследовательскими комиссиями МСЭ-Т и другими организациями в целях выполнения настоящей Резолюции;

5 поощрять обмен информацией о достижениях в соответствующих разработках, которые относятся к внедрению PQC и переходу на нее, а также переходу на PQC в рамках сети электросвязи/ИКТ;

6 представить рекомендации Консультативной группе по стандартизации электросвязи о порядке рассмотрения вопросов, выходящих за рамки мандата указанных исследовательских комиссий,

поручает Консультативной группе по стандартизации электросвязи

обеспечить согласованные меры в рамках соответствующих исследовательских комиссий по ускорению работы по стандартизации для содействия внедрению PQC и переходу на нее, а также переходу на PQC в рамках сети электросвязи/ИКТ,

поручает Директору Бюро стандартизации электросвязи

1 оказывать необходимую помощь в разработке планов действий по содействию внедрению PQC и переходу инфраструктуры электросвязи/ИКТ на PQC и поощрять участие и вклады Государств-Членов, Членов Секторов, Ассоциированных членов и Академических организаций – Членов;

2 организовать семинар(ы)-практикум(ы) по сбору рекомендаций и мнений по этой тематике у широкого круга заинтересованных сторон;

3 оказывать поддержку Директору Бюро развития электросвязи (БРЭ) при оказании помощи Государствам-Членам в содействии внедрению PQC и переходу инфраструктуры электросвязи/ИКТ на PQC,

предлагает Государствам-Членам, Членам Секторов, Ассоциированным членам и Академическим организациям – Членам

1 представлять вклады для разработки Рекомендаций, других публикаций МСЭ-Т, содержащие руководящие указания и передовой опыт по содействию внедрению PQC и переходу инфраструктуры электросвязи/ИКТ на PQC;

2 содействовать проведению образовательных семинаров-практикумов и учебных занятий для содействия внедрению PQC и переходу на PQC, а также переходу на PQC в рамках сети электросвязи/ИКТ.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_