

### Окончание. Начало — в № 23

**ПРАВТЕЛЬСТВО** Канады продвигает принятие PQC (пост-квантовой криптографии. — Ред.), но канадская национальная квантовая стратегия также обещает разработать коммерчески жизнеспособное распределение квантовых ключей и запустить спутник QKD. Канадские военные включили QKD (квантовое распределение ключей. — Ред.) в список важных оборонных возможностей и в настоящее время финансируют академические исследования сетей QKD, хотя их квантовая дорожная карта признаёт, что QKD в настоящее время не рекомендуется для защиты систем национальной безопасности.

Тем временем правительство Южной Кореи, похоже, с энтузиазмом относится как к PQC, так и к QKD. Её Национальная разведывательная служба выступила соорганизатором конкурса, в ходе которого в январе 2025 года PQC для стандартизации. В то же время правительство Кореи подключило 48 правительственных департаментов к сети QKD протяжённостью 800 километров, а его национальная квантовая стратегия поощряет быстрое принятие министерствами и государственными учреждениями QKD и аналогичных систем квантовой криптографии. В январе 2025 года Национальная разведывательная служба Южной Кореи аккредитовала систему QKD, соответствующую стандартам национальной безопасности.

Японская квазиправительственная организация по развитию новых энергетических и промышленных технологий финансирует развитие технологий PQC и QKD в стране. Японское правительство, по-видимому, не инвестировало напрямую столько ресурсов в развёртывание QKD, сколько южнокорейское, но японская стратегия инноваций в области квантовых технологий ставит цель "повысить неуязвимость различных приложений безопасности за счёт коммерциализации устройств квантовой криптографии", а её стратегия развития будущей квантовой промышленности "продвигает использование государственных органами сетей квантовой безопасности".

### ПОСЛЕДСТВИЯ ПРИ ВЗАИМОДЕЙСТВИИ СИСТЕМ КОММУНИКАЦИИ

Почему важно, какое решение выберет другая страна? Потому что PQC и QKD работают на совершенно разных принципах, а системы связи, использующие разные способы в криптографии, могут столкнуться с огромными проблемами взаимодействия.

Объединение PQC и QKD в одной системе связи возможно, хотя и нелегко. Но системы информационной безопасности создают дополнительные проблемы, выходящие за рамки чисто технических. Для подобных систем недостаточно, чтобы данные надёжно передавались от отправителя к получателю; необходимо также предотвратить перехват информации или её изменение

по пути. Предположим, что организация не доверяет безопасности QKD и запрещает использовать её для передачи конфиденциальной информации — или аналогично с PQC. В сложной сети связи (например, в Интернете), использующей как PQC, так и QKD, чрезвычайно сложно гарантировать, что данное сообщение никогда не пройдёт через запрещённую систему.

Этот факт повышает риск того, что разные страны могут принять разные криптографические контрмеры против угрозы квантовых вычислений, которые могут быть или не быть взаимно совместимыми. В лучшем случае подключение систем связи, использующих разные протоколы, может оказаться очень дорогим. В худшем случае некоторые страны могут запретить использование систем связи, принятых другими странами, тем самым лишив эти страны возможности безопасно общаться в принципе.

Интероперабельные (интероперабельность — способность двух или более систем обмениваться ин-

формацией с союзными военными, которые могут использовать QKD?

Вероятнее всего, пройдёт много лет, прежде чем квантовые компьютеры смогут реализовать алгоритм для атаки на криптографию, тем не менее есть риск, что противники США уже получили и хранят зашифрованную информацию, которую они смогут раскодировать через несколько лет, когда квантовые компьютеры станут достаточно мощными. Поэтому раннее и преднамеренное развёртывание контрмер будет намного дешевле, чем поспешное развёртывание, когда угроза приблизится".

Вывод статьи на сайте "Джаст секьюрити": правительствам стран — союзников США следует как можно скорее приступить к решению проблемы защиты своих систем связи от угрозы квантовых вычислений. При этом им следует чётко изложить свою общую стратегию относительно того, какие контрмеры они планируют принять и когда, а также какие контрмеры они, возможно, уже исключили. Это



# КВАНТОВАЯ ГОТОВНОСТЬ

## Часть вторая, заключительная. Коммерческие кубиты

даст коммерческим поставщикам в этих странах чёткие указания относительно того, какие системы разрабатывать для государственных клиентов и в какие сроки.

Военные союзники также должны достичь общего понимания относительно того, какие протоколы безопасности будут приемлемы для информации, влияющей на национальную безопасность, которой обмениваются страны. Даже между странами, принявшими на себя обязательство взять на вооружение метод PQC, существуют важные различия в деталях реализации, которые могут привести к проблемам взаимодействия. Эти различия также должны быть гармонизированы.

Агентство перспективных исследований обороны США (DARPA) расширяет своё исследование квантовых вычислений, выбрав около 20 компаний для участия в создании промышленно полезного квантового компьютера.

Интернет-журнал "Нэшнл дифенс" пишет, что Инициатива DARPA по квантовому бенчмаркингу (QBI) является расширением её существующей программы "Малозначенные системы квантовых вычислений общего назначения" (US2QC). По словам Джо Алтпетера, менеджера программы в Агентстве микросистемных технологий, оба проекта направлены на определение того, сможем ли кто-то создать квантовый компьютер общего назначения (то есть его вычислительная ценность превысит его стоимость) в течение следующего десятилетия.

В феврале 2025 года агентство выбрало "Майкрософт" и "Пси-Квантум" для участия в финальном

этапе программы US2QC, а в апреле объявило, что ещё 18 компаний примут участие в этапе "А" инициативы по квантовому бенчмаркингу — шестимесечном спринте, в ходе которого участники представят исчерпывающие технические подробности своих концепций квантовых вычислений, чтобы показать, как их можно реализовать менее чем за 10 лет.

Агентство решило расширить свои квантовые исследования, поскольку, пока оно работало над US2QC, появлялось всё больше компаний, заявлявших, что они добились больших успехов на пути создания промышленно полезного квантового компьютера. "QBI не похоже ни на одну из известных мне программ DARPA, поскольку агентство не управляет автобусом, — сказал Алтпетер. — DARPA занимает скептическую позицию на начальном этапе, поскольку мы не уверены, смогут ли эти компании добиться успеха, и мы хотим задействовать ресурсы, время и экспертизу, чтобы выяснить, кто из них стоящий, а кто нет".

Он добавил, что выбор 18 компаний для этапа "А" инициативы стал "большим сюрпризом". DARPA не установило квоту на количество технологий, которые оно выберет. В число участников входят компании разных размеров из США и других стран, реализующие самые разные подходы к квантовым вычислениям.

Одна из компаний, выбранных для этой инициативы, "Элис и Боб", головной офис которой находится в Париже, а отделения — в Бостоне, разрабатывает технологию, известную как "кошачьи кубиты". Жюльетт Пейронне, генеральный директор "Элис и Боб" в США, сказала, что "большие накладные расходы, с которыми сейчас сталкиваются все в

этой отрасли, связаны с необходимостью исправлять ошибки". Компании разработали кубиты — строительные блоки для квантовых компьютеров, — "но мы не можем доверять полученным результатам, потому что существует очень высокий процент ошибок, возникающих в результате измерения наших кубитов".

"Многие компании внедрили коды исправления ошибок, но их реализация очень затратна по ресурсам. Если вы посмотрите на некоторые из последних разработок "Гугл" (компания нарушает законодательство РФ. — Ред.), вы увидите, что им нужно около 1000 физических кубитов для создания одного логического кубита — набора физических кубитов, организованных для предотвращения ошибок, — в то время как технологии "кошачьих кубитов" "Элис и Боб" требуются всего 16 физических кубитов для формирования логического кубита, — сказала Пейронне. — Главное отличие нашего подхода заключается в том, что мы обеспечиваем высокую эффективность оборудования, а это означает, что у нас нет такой же нагрузки на инженеров, как у других систем, что увеличивает скорость, с которой компания может создать и внедрить квантовый компьютер.

Ещё один участник этапа "А" QBI — канадская компания "Фотоник" — занимается разработкой оптически связанных кремниевых спино-кубитов.

Стефани Симмонс, основатель и главный квантовый директор компании "Фотоник", сказала, что квантовые компьютеры должны обеспечивать исправление ошибок и не быть шумными. А чтобы они не были шумными, они должны быть идеальными.

Это означает, что они должны всегда контролировать своё окружение, и многие системы сегодня сталкиваются с физическими ограничениями, поскольку их производительность снижается после достижения определённого размера.

"Для этих разных систем существуют разные ограничения, и если вы взглянете на них, то увидите, что все они ограничивают себя гораздо меньше, чем размеры, необходимые для того, чтобы представлять из себя некую ценность, — сказала Симмонс. — Подход "Фотоник" заключается в объединении атомов кремния — стандартного материала, который используется для всех чипов сегодня, — с небольшой молекулой, испускающей при активации с помощью оптики или электроники фотон телекоммуникационной длины волны, который может пройти по всем волокнам, уже проложенным по всему миру, решая проблему масштабирования, с которой сталкиваются другие квантовые системы".

"Цель компании — создать рас-пределённое квантовое вычислительное решение, — заявила Симмонс. — Вместо того чтобы помещать все кубиты в одну коробку и требовать миллионы, мы могли бы подумать о том, чтобы извлечь выгоду, как в случае с классическими суперкомпьютерами, взяв один компьютер, а затем распараллелив и собрав множество вместе".

В пресс-релизе DARPA сказано, что после этапа "А" оно выберет компании для перехода к годичному этапу "В", в ходе которого агентство изучит их подходы к исследованиям и разработкам, затем последует финальный этап "С", на котором независимая группа проверки и валидации QBI протестирует компьютерное оборудование компаний. Финальный этап US2QC имеет те же технические цели, что и этап "С" инициативы квантового бенчмаркинга. Алтпетер отметил, что квот на количество компаний, прошедших на каждый этап, не существует.

Владимир ОВЧИНСКИЙ

**ПОСЛЕ ТОГО** как Израиль нанёс авиаудары по реактору в Натанзе, по ядерным и другим объектам в Иране, когда были убиты некоторые видные иранские военачальники и учёные-ядерщики, катарское агентство "Аль-Джазира" сразу поставило вопрос: "Почему именно сейчас израильские военные начали военную операцию "Восходящий лев" и объявили атаку "упреждающей и точной"? При этом эксперты агентства указывали на то, что с 12 апреля Вашингтон и Тегеран при посредничестве Омана провели пять раундов переговоров, стремясь найти альтернативу заключённому с Ираном в 2015 году международному соглашению по ограничению его ядерной программы в обмен на ослабление введённых против него санкций. Также была достигнута договорённость о проведении шестого раунда в Маскате.

Правда, в отличие от предыдущих раундов, подготовка шестого сопровождалась невиданной информационной войной, в которой стороны в публичном пространстве выставляли друг другу претензии и условия, а Израиль грозился проведением военной операции против Ирана. Тем не менее президент США Дональд Трамп, с одной стороны, допускал предварительные утки в американские СМИ о готовящейся военной акции Израиля против Ирана, с другой — в телефонном разговоре с премьер-министром Израиля Биньямином Нетаньяху предостерегал от такого шага, считая его "преждевременным". Если допустить версию о согласованных закулисных действиях Трампа с Нетаньяху, то было бы логично выставить Ирану жёсткие условия на переговорах в Маскате

# А ПОГОВОРИТЬ?

## Оценка перспектив России как посредника между Ираном, Израилем и США

и только после этого дать "добро" на удар по его ядерным объектам. Но такого не произошло по неизвестным причинам. Согласно опубликованному NBC News за две недели до удара Израйля сведениям о секретных контактах между советниками по национальной безопасности США и Израйля, американские войска в Персидском заливе были приведены в состояние боевой готовности.

Тель-Авиву удалось сорвать переговоры. Он мотивировал свою акцию тем, что "был вынужден действовать на основании новых разведанных, свидетельствующих о том, что Иран приближается к точке невозврата" в своём стремлении к созданию ядерного оружия". Но этот аргумент не выдерживает критики. На столе у Трампа лежит доклад Национальной разведки США, в котором говорится, что "Иран не создаёт ядерное оружие" и что Тегеран "не возобновил программу создания ядерного оружия, которую он приостановил в 2003 году".

Теперь о следующей загадке в ситуации. Трамп заявил, что он был заранее проинформирован "о крупномасштабных израильских

ударах по Ирану". В широком контексте, как считает агентство "Фокс ньюс", "это верно, но в конкретике есть неясности", так как ранее официальные лица США говорили телеканалу CNN, что "любимой израильской удар по Ирану будет вопиющим отклонением от подхода Трампа к Ближнему Востоку". Это — первое. Второе: госсекретарь США Марко Рубио подчёркивал, что "США не участвовали в ударах" и что "Израиль действовал в одностороннем порядке в целях самообороны". Напрашивается вывод: либо Трамп не информировал Рубио об операции Израйля, либо сам был поставлен перед фактом, а дальше действовал уже по обстоятельствам. Наконец, эксперты задаются вопросом: удалось ли Израйлю действительно нанести удары по иранской ядерной программе или это было прикрытием для каких-то иных целей?

**ПО ВСЕМ ПРИЗНАКАМ**, главную работу в Иране проводила израильская разведка "Моссад", продемонстрировавшая свои оперативные возможности. Оказывается, она располагала информацией о местонахождении высокопоставленных представителей иранской системы безопасности и учёных-ядерщиков и провела их ликвидацию. Самое парадоксальное заключается в том, что "Моссад" удалось создать базу ударных дронов, которые были перемещены на территорию Ирана агентами разведки задолго до атаки. Но до ядерной программы Ирана им добраться всё же не удалось, несмотря на пять волн ударов. Также не пострадали объекты нефтепереработки и нефтехранилища.

Иранский ответ не заставил себя ждать, поскольку Тегеран через несколько часов после израильской атаки запустил сотни дронов и баллистических ракет партиями по различным районам оккупированной Палестины, от Тель-Авива до Хайфы и Галилеи, причинив огромный ущерб, вынудив миллионы оставаться в убежищах и безопасных районах.

Что дальше? Трамп сейчас оказался зажат между прежде заявленными принципами своей внешней политики на Ближнем Востоке и неспособностью сдержать Израиль. Как пишет глава вашингтонского бюро новостного веб-сайта "Политико" Рейчел Бейд, "Америка теперь сталкивается с перспективой быть втянутой в новый конфликт на Ближнем Востоке не по своему собственному решению, а из-за односторонних действий Израйля, что может серьёзно сказаться на результатах предстоящих промежуточных выборов в Конгресс". Стало очевидно, что "Трампу не хватает влияния, чтобы обуздать ближайшего союзника", и ситуация на Ближнем Востоке переведена в новое качество: в течение многих лет Иран и Израиль предпочитали действовать друг против друга косвенно, теперь же вступили в открытую схватку. При этом в специальном отчёте спецслужб Израйля говорится, что "Иран — это не "Хезболла" и уж точно не ХАМАС". Он находится очень далеко от Израйля. Площадь Ирана более чем в 150 раз превышает размеры Ливана, характеризуется высокой степенью институционального дублирования, когда существующая структура военно-политического управления позволяет назначать замену тем, кто был ликвидирован. К тому же лица,

принимающие решения в Израиле, понимают, что эта авантюра сопряжена с большими издержками, особенно если Иран решит перевести битву на уровень региональной конфронтации или открытой ядерной эскалации, что вернёт регион к модели крупной войны, при которой Израиль в одиночку не в состоянии контролировать все её последствия. К тому же ставка Израйля на свержение иранского режима предполагает радикальное изменение баланса сил между режимом и его сторонниками и противниками, из которых пока лишь меньшинство демонстрирует оппозиционные настроения. Для всего региона наступят трудные времена, и главный вопрос заключается в том, как долго продлится израильская операция, не превращаясь ли она в полномасштабную войну.

На сей счёт на Ближнем Востоке циркулирует несколько версий. Утверждается, что удар Израйля по Ирану "является завершающей фазой его действий против ХАМАС в Палестине. "Хезболла" в Ливане и свержение режима Башара Асада в Сирии". Согласно другой версии, так называемая "отложенная конфронтация с Ираном не означает, что события будут развиваться в интересах Тель-Авива или что он может нанести поражение Ирану". Израиль, ограниченный пространством, может не выдержать последовательных ударов по своей территории, и "эта реальность может подталкивать Израиль к сокращению продолжительности войны". Как ни крути, это первый случай с 1948 года, когда израильтяне оказываются осаждёнными ракетами в своих городах и вынуждены иметь дело с мёртвыми людьми под обломками и ранеными, застрявшими в рухнувших зданиях. Символика ударов, нанесённых вглубь территории Израйля, становится психологически жестокой по отношению к израильскому обществу, которая не ожидала ни такого количества разрушений, ни точности иранских ракет (некоторые из них, по оценкам, несли боеголовки весом более 600 килограммов).

**ВАКАОМ КОНТЕКСТ** событий вписываются суждения, что "Израиль инициировал эту войну с Ираном, чтобы помешать ходу переговоров между Тегераном и Вашингтоном". Но если США станут активной стороной боевых действий, чего отчаянно добивается премьер-министр Израйля Нетаньяху, это вызовет значительную эскалацию с длительными и, скорее всего, разрушительными последствиями. Эксперты полагают, что, если Ирану не удастся нанести ущерб хорошо защищённым израильским военным объектам, он может расширить список своих целей. К тому же Иран может перекрыть Ормузский пролив, что спровоцирует рост цен на энергоносители во всём мире, а также увеличение инфляции и стоимости жизни. С другой стороны, если планы Израйля в отношении Ирана увенчаются успехом, это может проложить путь к гражданской войне внутри страны и вызовет хаос, подобный тому, который ранее происходил в других странах региона, подвергаемых непрерывному циклу ударов и контратак.

В данном случае речь ведётся о явлениях и событиях, которые лежат на поверхности. Ситуация нуждается в более тщательном анализе, так как ход и предполагаемые последствия войны между Израилем и Ираном затрагивают проблемы региональных и политических структур безопасности на всём Ближнем Востоке, что напрямую связано с США, поставленными Трампом на новый перекрёсток интересов — "узких" израильских и своих, более "широких", стратегических, вызовов. Но его тактика и стратегия действий в отношении Ирана, "через давление и угрозы к ядерному соглашению", проваливается. Не сбываются и прогнозы о том, что

после удара Израйля Иран возьмёт "тактическую паузу". В Тегеране взяли верх страхи Исламской революции и нанесли ответный удар, что уже воспринимается как признак "большой войны" с "возможностью выхода США на линию фронта". Так, хуситское движение "Ансар Аллах" в Йемене уже объявило о вступлении в войну на стороне Ирана, и, конечно, движение ХАМАС, которое сталкивается с войной на уничтожение в секторе Газа, заявило о своей ироанской позиции. Страны Персидского залива опасаются, что их территории или нефтяные объекты станут целями в ходе этой конфронтации, и призывают стороны "проявлять сдержанность", хотя все понимают, что ситуация в регионе пошла вразнос. Но пока прогнозируемая карта региональной обстановки остаётся открытой для противоречивых сценариев, и наблюдатели полагают, что "Трамп будет использовать усилия для привлечения России в качестве посредника, чтобы заполнить созданный им стратегический вакуум, требующий пересмотра союзов и правил на Ближнем Востоке". Если это так, то следует ждать возобновления диалога США — Россия по иранской ядерной тематике.

**РЕАКЦИЯ МОСКВЫ** на события последовала быстро. МИД России охарактеризовало израильский удар как "нарушение международного права и суверенитета государства — члена Организации Объединённых Наций". Министр иностранных дел Сергей Лавров связался по телефону со своим иранским коллегой Аббасом Араки. Озабоченность Москвы понятна, ведь "любая эскалация в этом регионе негативно скажется на совместных энергетических проектах России с Ираном, особенно в газовой сфере и в отношении новых экспортных линий через Каспийское море". Тем более, что США на данном этапе играют двойственную роль, они видят в эскалации возможность провести новую ядерную сделку с Ираном. Тегеран тоже обладает манёвренностью, и доступные ему варианты включают привлечение региональных союзников для косвенного реагирования или вступления в новую переговорную "игру", демонстрируя свою "ядерную гибкость" в обмен на экономические и политические уступки.

Напомним, что в ходе четвёртого телефонного разговора с российским президентом Владимиром Путиным Трампу было предложено посредничество России на переговорах с Ираном по вопросу ядерной программы. Затем последовало заявление замглавы МИД России Сергея Рябкова, что "мы не ослабляем наших усилий, направленных на содействие энергичному поиску нужных переговорных решений". По его словам, такие решения "вполне достижимы при должной опоре на международное право, принцип равной и неделимой безопасности, а также при тщательно выверенном балансе интересов и поэтапном движении, которое позволит укрепить и нарастить доверие за счёт соблюдения достигаемых договорённостей". На текущий момент нет ясности, как будет и будет ли вообще Москва интервироваться в переговорный процесс между Вашингтоном и Тегераном, хотя стороны имеют на этом направлении определённые наработки. Кстати, четыре успешных раунда переговоров между Ираном и США проходили под заметным влиянием России. Несомненно пока только то, что после удара Израйля по Ирану правила ведения боевых действий на Ближнем Востоке уже не будут прежними, независимо от того, сядут ли все за стол переговоров или ринутся в новый раунд конфронтации.

Станислав ТАРАСОВ



Момент старта иранской новейшей баллистической ракеты средней дальности «Хоррамшахр-4» («Хайбар»)