Post Quantum Cryptography Coalition

План перехода на постквантовую криптографию (PQC)

Май 2025

Коалиция постквантовой криптографии (PQCC) — это сообщество технологов, исследователей и экспертов-практиков, миссией которого является содействие прогрессу в направлении более широкого понимания и общественного принятия постквантовой криптографии (PQC) и связанных с ней стандартов Национального института стандартов и технологий (NIST). PQCC уделяет особое внимание классическим криптосистемам с квантово-безопасной безопасностью для обеспечения информационной безопасности в эпоху криптографически значимых квантовых компьютеров.

Содержание

Фон **4**
Обзор миграции 4
Рекомендуемая реализация дорожной карты 5
Категория 1: Подготовка **6**
Упражнение 1.1: Определение релевантности PQC 6
Действие 1.2: Назначение руководителя для управления миграцией PQC 7
Упражнение 1.3: Выявление существующих запасов и повышение осведомленности 7
Упражнение 1.4: Выявление заинтересованных сторон и разработка стратегических сообщений 8
Упражнение 1.4 a: Начало взаимодействия с поставщиками и операторами систем 9
Категория 2: Базовое понимание **10**
Упражнение 2.1: Составьте план и бюджет на обнаружение 10
Упражнение 2.2: Создание инвентаризации для миграции PQC 10
Упражнение 2.2 a: Рассмотрение инструментов и методов, используемых для инвентаризации 11
Мероприятие 2.2 b: Сбор и категоризация информации о криптографических активах 11
Упражнение 2.3: Определение приоритетности критически важных активов для миграции 12
Категория 3: Планирование и исполнение **13**
Упражнение 3.1: Составление плана и бюджета миграции 13
Упражнение 3.2: Поиск решений 13
Мероприятие 3.2 a: Согласование потребностей в миграции с поставщиками 14
Упражнение 3.2 b: Создание решений 15
Деятельность 3.3: Разработка краткосрочных мер 15
Упражнение 3.5: Внедрение решений PQC 16
Категория 4: Мониторинг и оценка **17**
Деятельность 4.1: Проверка правильности реализации 17
Упражнение 4.1 a: Обеспечение соответствия отраслевым стандартам 17
Упражнение 4.2: Создание мер для отслеживания успешности миграции PQC 18
Упражнение 4.3: Оценка потребностей в рабочей силе 18
Упражнение 4.4: Непрерывный мониторинг и обновление 19
Заключение **19**
Ссылки **20**

Фон

Прорывы в гонке за развитием передовых квантовых вычислений угрожают нашим нынешним системам, которые обеспечивают безопасность коммуникаций, подлинность и защиту конфиденциальных данных при хранении и передаче, что обуславливает необходимость перехода к постквантовой криптографии (PQC). Несмотря на то, что разработка криптографически релевантного квантового компьютера (CRQC), способного проникнуть в текущую криптографическую безопасность, может потребоваться еще от 10 до 20 лет, необходимо начать процесс миграции уже сейчас, чтобы обеспечить успешное планирование и сроки реализации. Начало миграции на PQC также снижает угрозу сбора данных сейчас, чтобы злоумышленник мог расшифровать их позже.

Эта дорожная карта миграции написана в качестве руководства для вашей организации по планированию и реализации постквантового перехода, в котором представлен обзор четырех ключевых категорий для продвижения миграции к PQC: (1) Подготовка, (2) Понимание базовых показателей, (3) Планирование и выполнение и (4) Мониторинг и оценка. Кроме того, для каждой категории и связанных с ними видов деятельности перечислены желаемые результаты, что дает организациям представление о том, где они должны находиться на протяжении всего процесса, описанного в этой дорожной карте.

Обзор миграции

Миграцию на PQC в вашей организации можно разбить на четыре основные категории. К этим категориям прилагаются действия, которые ваша организация может предпринять для продвижения и поддержания миграции PQC. Реализация категорий и действий будет выглядеть по-разному от организации к организации, и, как видно на рисунке 1, компоненты этой дорожной карты могут выполняться одновременно или в шахматном порядке.

Категория 1: Подготовка
Ваша организация настраивает миграцию на PQC, получая обзор целей миграции PQC, назначая руководителя миграции, определяя необходимых заинтересованных лиц и согласовывая заинтересованные стороны с помощью стратегических сообщений.

Категория 2: Базовое понимание
Ваша организация получает базовое представление о своем запасе данных, приоритетных активах, которые необходимо обновить, а также о необходимых ресурсах и доступном бюджете.

Категория 3: Планирование и исполнение
Ваша организация сотрудничает с поставщиками систем и владельцами внутренних систем, чтобы гарантировать, что постквантовые решения приобретаются внешними поставщиками или разрабатываются внутри компании и эффективно внедряются.

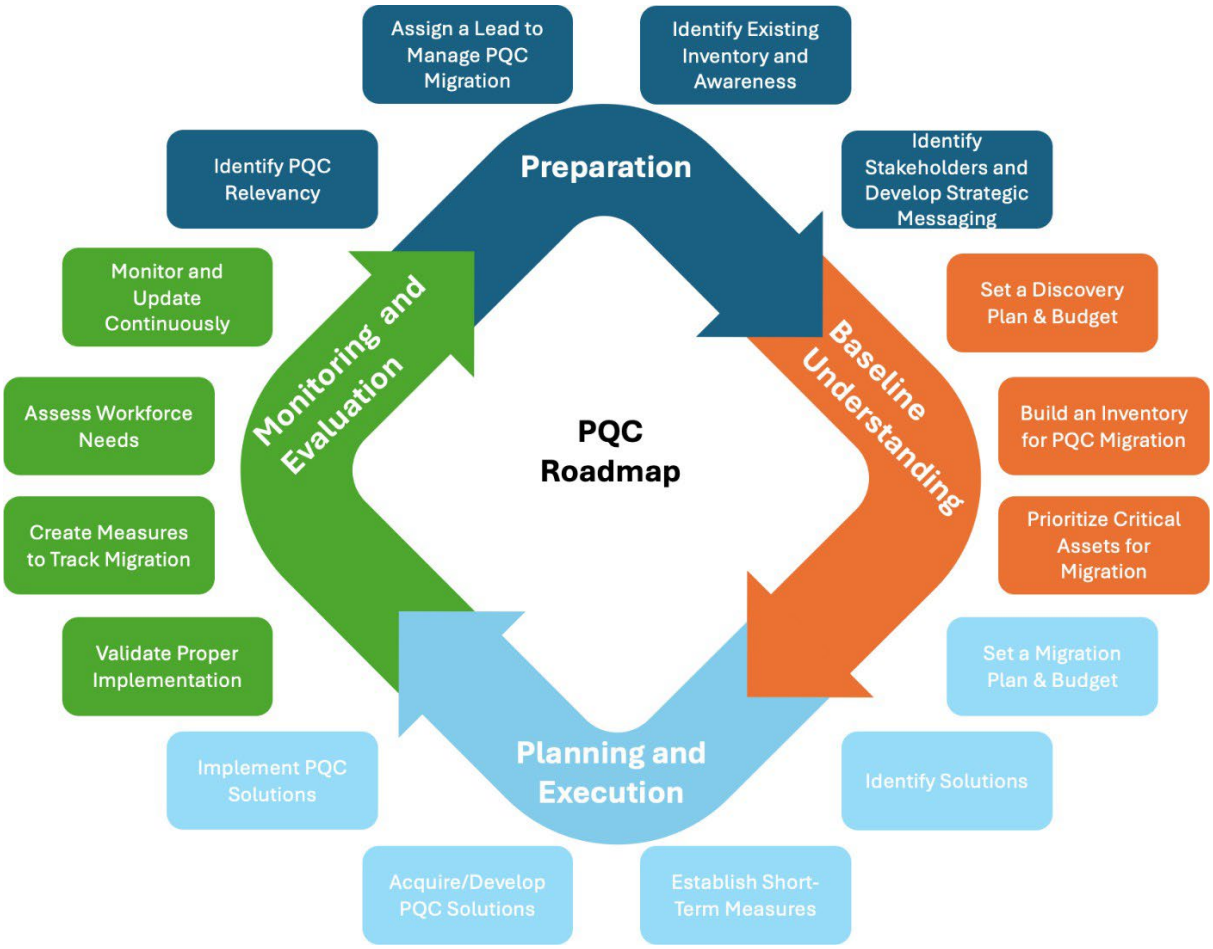
Категория 4: Мониторинг и оценка
Ваша организация разрабатывает меры для отслеживания процесса миграции и формулирует процесс переоценки криптографической безопасности по мере развития

квантовых возможностей.

Рекомендуемая реализация дорожной карты

То, как организация применяет эту дорожную карту, зависит от срока годности и объема критически важных данных, объема доступной информации о своих активах, бюджета на потенциально значительные обновления программного и аппаратного обеспечения, а также от множества других влияющих факторов. Реализация категорий и видов деятельности зависит от организации и может происходить одновременно, последовательно или по отдельности.

Рисунок 1. Категории дорожной карты PQC.



Категория 1: Подготовка

В категории подготовки к миграции PQC организация проводит подготовку, получая обзор своих целей миграции PQC, назначая руководителя миграции, определяя необходимых заинтересованных лиц и согласовывая заинтересованные стороны с помощью стратегических сообщений.

Исходы категории 1:

- Организация знакомится со своими уязвимостями и уровнем их срочности, определяя подходящие сроки для начала миграции PQC.
- Организация назначает руководителя по миграции, ответственного за выполнение миграции PQC.
- Организация определяет существующие запасы и осведомленность о PQC.
- Организация определяет и согласовывает свои ключевые заинтересованные стороны с потребностями в миграции PQC, используя стратегические сообщения.

Упражнение 1.1: Определение релевантности PQC

Прежде чем начать переход на PQC, вашей организации необходимо оценить, следует ли начать этот процесс сейчас или следовать более позднему графику. Определение подходящей временной шкалы для миграции PQC в вашей организации включает в себя оценку миграции, срока хранения информации и временных шкал угроз. Как видно на рисунке 2 ниже, срок хранения конфиденциальной информации может повлиять на срочность внедрения PQC, поскольку злоумышленники могут собирать современную информацию для последующей расшифровки с помощью CRQC. Независимо от того, сталкивается ли ваша организация с угрозой «собрать урожай сейчас, расшифровать позже», она должна быть готова защитить критически важную информацию от угроз целостности и подлинности, которые будут существовать с появлением CRQC.

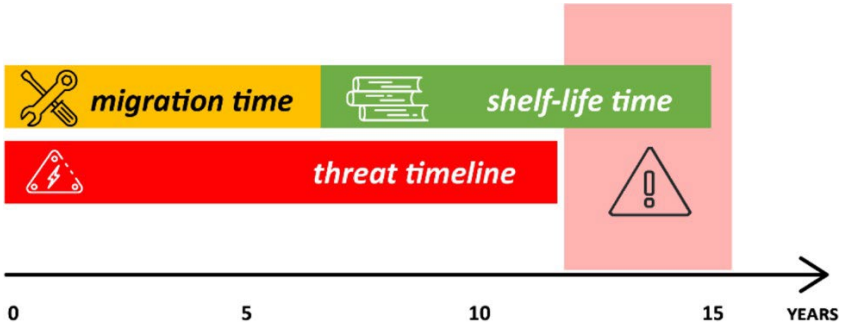


Рисунок 2. Временная шкала модели для определения срочности миграции PQC (рабочая группа по квантовой готовности).

Чтобы понять, какой общий уровень вовлеченности требуется вашей организации при переходе на PQC, необходимо определить цели миграции PQC. Это первоначально прояснит, на какой риск готова пойти ваша организация, когда дело доходит до защиты

своих данных и активов. Чтобы определить цели миграции вашей организации, вы можете рассмотреть такие характеристики, как:

- Поверхность атаки вашей организации
- Виды систем и их возможные неисправности
- Критичность и конфиденциальность обрабатываемых данных
- Необходимость срочной миграции
- Ожидаемый срок службы замененных или перенесенных активов
- Взаимозависимость с другими организациями

Ваша организация будет либо срочным внедрением, либо постоянным внедрением. Те, кто срочно внедряет эти технологии, работают с конфиденциальными данными или активами, где нарушение безопасности может поставить под угрозу критически важную инфраструктуру или раскрыть конфиденциальные личные или организационные данные. Постоянные последователи — это организации, которые не попадают в категорию срочных усыновителей. В то время как обычные пользователи могут хранить данные или эксплуатировать системы, они подвергаются меньшему риску использования схем «хранить сейчас-расшифровать-потом».

Упражнение 1.1 Результаты:

- Организация уточняет свои цели миграции PQC и определяет подходящий график для начала миграции PQC.
- Организация знакомится со своими уязвимостями и уровнем их актуальности.

Действие 1.2: Назначение руководителя для управления миграцией PQC

Когда ваша организация принимает решение начать график миграции PQC, она должна назначить отдельного сотрудника или команду («руководитель миграции») для мониторинга и продвижения миграции PQC. Обязанности этой роли будут специфичны для вашей организации, но могут включать в себя установление сроков, обращение к поставщикам и другие обязанности по реализации миграции. В конечном счете, миграция PQC включает в себя активное взаимодействие с различными руководящими и техническими ролями, поэтому руководитель миграции должен иметь хорошие возможности для работы в различных областях внутри и за пределами вашей организации.

Упражнение 1.2 Результаты:

- Организация определяет роль и результаты, ожидаемые от своего руководителя по миграции.
- Организация назначает руководителя по миграции, ответственного за выполнение

Упражнение 1.3: Выявление существующих запасов и повышение осведомленности

В этом упражнении руководитель миграции составляет план для получения базового представления о криптографических потребностях своей организации. Это может включать в себя определение уже доступных инвентаризаций, определение текущих усилий по миграции и получение целостного представления о состоянии миграции в вашей организации. Ваша организация захочет проверить, какие запасы, оценки рисков и

криптографические спецификации материалов (CBOM) у нее уже есть. Организации могут иметь несколько инвентаризаций и оценок рисков, которые были разработаны для удовлетворения конкретных требований в разные моменты времени. При изучении существующих запасов и оценок рисков задокументируйте местонахождение данных и активов, кто ими владеет и управляет, почему они были созданы и как они используются. Документирование информации, которой в настоящее время располагает ваша организация —

и не имеет — поможет руководителю миграционной службы прояснить свои потребности на раннем этапе и избежать ненужных затрат и усилий.

Упражнение 1.3 Результаты:

- Руководитель отдела миграции оценил и задокументировал все существующие инвентаризации, оценки рисков и осведомленность, связанные с миграцией PQC.

Связанные задания: 2.2, 2.3

Упражнение 1.4: Выявление заинтересованных сторон и разработка стратегических сообщений

Критически важным для выполнения действий, описанных в этой дорожной карте, является согласование между руководителями вашей организации и ключевыми заинтересованными сторонами ценности и цели миграции PQC. В связи с этим руководитель миграционной службы должен разработать план коммуникации с учетом особенностей вашей организации, в котором (1) определяются и согласовываются заинтересованные стороны и (2) сообщается о процессе и необходимости миграции PQC. Это действие может включать в себя первоначальное взаимодействие с системными операторами и поставщиками для определения текущего контекста миграции вашей организации. Некоторые вопросы, которые следует учитывать при разработке стратегических сообщений, включают:

- Какова стоимость/рентабельность инвестиций (ROI) от миграции нашей организации на PQC?
- Насколько срочно нам нужно начать миграцию PQC?
- Как мы можем измерить влияние внедрения PQC?
- Что требует от нас миграция PQC в финансовом и операционном плане?

Заинтересованные стороны — это те, кто зависит от миграции PQC вашей организации, поддерживает ее или может извлечь из нее выгоду. Понимание ожиданий заинтересованных сторон включает в себя понимание того, как они могут влиять и влияют на других заинтересованных сторон. Прислушиваясь к заинтересованным сторонам и используя их вклад для постоянного совершенствования и удовлетворенности, ваша организация будет продолжать повышать заинтересованность заинтересованных сторон в прогрессирующем переходе на PQC.

В своих стратегических сообщениях ваша организация может захотеть рассмотреть заявление о позиционировании, которое дает обзор цели и объема миграции PQC. Ваша организация также может захотеть предвидеть проблемы, с которыми заинтересованные стороны могут столкнуться при переходе на PQC, и составить проект ответных сообщений, которые могут помочь заинтересованным сторонам лучше понять цели PQC и согласовать их с ними. Кроме того, ваша организация может подготовить презентации, чтобы кратко донести ценность миграции PQC до заинтересованных сторон, как внутренних, так и внешних по отношению к вашей организации. Поскольку взаимодействие с заинтересованными сторонами и стратегические сообщения будут

охватывать весь процесс миграции PQC в вашей организации, вам также потребуется разработать меры для отслеживания влияния ваших стратегических сообщений на деятельность заинтересованных сторон.

Упражнение 1.4 Результаты:

- Организация определяет и согласовывает свои ключевые заинтересованные стороны с категориями и действиями по миграции PQC.
- Организация может решительно донести ценность и цель миграции PQC до экосистемы заинтересованных сторон.

Упражнение 1.4 а: Начало взаимодействия с поставщиками и операторами систем

Взаимодействие с ключевыми заинтересованными сторонами в вашей организации будет включать в себя первоначальные переговоры с поставщиками и внутренними операторами систем для определения потребностей в миграции. Предварительные вопросы, которые ваша организация захочет задать, включают:

- Когда будут доступны PQC-решения от вендора?
- Когда будут доступны решения PQC для систем собственной разработки?
- Потребуются ли для обновления PQC аппаратные или программные реализации?
- Какова стоимость новых решений?
- Каково ожидаемое влияние усилий по внедрению на бизнес?
- Будет ли CBOM включен в состав решений?
- Каково состояние криптографически гибких решений?

Мероприятие 1.4 (а) Результаты:

- Организация устанавливает каденцию со своими поставщиками, если она еще этого не сделала.
- Поставщики и внутренние операторы помогают предоставить ориентировочные сроки доступности решения PQC, а также затраты на

Категория 2: Базовое понимание

Во второй категории руководитель миграции получает базовое представление о своем запасе данных, приоритетных активах, которые необходимо обновить, а также о необходимых ресурсах и доступном бюджете для инициатив по обнаружению.

Исходы категории 2:

- Организация определяет необходимость дополнительных усилий по инвентаризации и расстановке приоритетов.
- Организация определила и задокументировала все криптографические активы, необходимые для достижения желаемого уровня отказоустойчивости PQC.

Упражнение 2.1: Составьте план и бюджет на обнаружение

В этом упражнении руководитель миграции использует собранную исходную информацию (действие 1.3), чтобы определить, следует ли организации принять дополнительные меры для разработки инвентаризации и приоритизации активов. Используя уже доступную информацию, руководитель миграции определяет, необходимы ли дополнительные инициативы по инвентаризации (упражнение 2.2) или организация может сразу перейти к приоритизации активов (упражнение 2.3). Руководитель миграции также может определить доступный бюджет для инвентаризации, приоритизации активов и других инициатив по обнаружению.

Результаты мероприятия 2.1:

- Руководитель миграции определяет, какие действия по инвентаризации и приоритизации необходимо провести для миграции PQC.
- Руководитель миграции определяет бюджет для инициатив по обнаружению.

Связанные задания: 1.3, 2.2, 2.3

Упражнение 2.2: Создание инвентаризации для миграции PQC

Централизованные инвентаризации необходимы для отслеживания сроков миграции на уровне предприятия и обеспечения комплексного планирования для устранения всех пробелов в безопасности. Создав четкую инвентаризацию активов и их использования, ваша организация может заблаговременно выявлять проблемы и обеспечивать гибкость при планировании требований PQC. Чтобы эффективно спланировать миграцию PQC, руководитель миграции сотрудничает с системными операторами для того, чтобы:

- Определите, какие инструменты и методы использовать при инвентаризации
- Документируйте информацию о своих наиболее важных активах
- Классифицируйте свой инвентарь (запасы)

Следующие подмероприятия (Мероприятия 2.2 (a) и (b)) не являются хронологическими, а служат соображениями, которые следует учитывать на протяжении всего процесса инвентаризации.

Результаты мероприятия 2.2:

- Организация документирует свою инвентаризацию активов и криптографическое использование.

Смежные виды деятельности: 2.2 (a), 2.2 (b)

Упражнение 2.2 a: Рассмотрение инструментов и методов, используемых для инвентаризации

Ваша организация может рассмотреть возможность использования автоматизированных средств для идентификации криптографических алгоритмов в различных компонентах инфраструктуры предприятия, включая оборудование, программные модули, библиотеки и встроенный код. Эти инструменты также должны точно определять алгоритмы, используемые для создания криптографических ключей и управления ими, которые имеют решающее значение для защиты криптографически защищенной информации и управления доступом. Кроме того, автоматизированные инструменты должны определять алгоритмы, обеспечивающие целостность данных при хранении, передаче и использовании, защищая как источник, так и содержимое данных. При выборе инструментов и методов учитывайте уровень допустимого риска в вашей организации, так как некоторые из них обеспечивают большую детализацию, чем другие.

Деятельность 2.2 (a) Результаты:

- Руководитель миграции и технические команды определяют, какие методы и инструменты лучше всего подходят для сбора данных инвентаризации вашей организации.

Мероприятие 2.2 b: Сбор и категоризация информации о криптографических активах

В этом действии руководитель миграции организации и системные операторы документируют подробную техническую информацию о наиболее важных активах, в том числе о том, кто ими управляет, какие данные они защищают, а также какие архитектурные проекты, протоколы проектирования и интерфейсы они используют. Также важно задокументировать то, чего ваша организация не знает, и знать о потенциальных слепых зонах в вашем инвентаре, таких как автономные ключи, ключи в файловой структуре, недоступные автоматизированным инструментам, или ключи с неизвестным форматом. По мере формирования перечня запасов в организации организуйте продукты по поставщикам, чтобы вы знали, с кем следует связаться в упражнении 3.2 (a).

Деятельность 2.2 (b) Результаты:

- Организация имеет категоризированный список всех криптографических активов, которые соприкасаются с ценной информацией.
- Организация выявила слепые зоны и информацию, которую она не знает о своих активах.
- Организация знает, к кому обращаться по поводу каждого актива, и знает, какие обновления ей потребуется внедрить самостоятельно, а какие обновления должны будут выполнить ее поставщики.

Связанная с этим деятельность: 3.2 a)

Упражнение 2.3: Определение приоритетности критически важных активов для миграции

В этом действии руководитель миграции определяет приоритеты критически важных активов и сроки их миграции. Это упражнение включает в себя анализ инвентаризации активов и криптографических средств, собранных в упражнении 2.2, и оценку его конфиденциальности и срока действия. Это фундаментальное понимание помогает расставить приоритеты в отношении систем, требующих немедленного внимания, и спланировать будущие потребности в области безопасности. Руководитель миграционного проекта продолжит консультироваться с соответствующими поставщиками и операторами систем, чтобы определить результаты этой деятельности.

Ваша организация может принять решение о проведении подробной оценки рисков для критически важных систем для дальнейшего выявления потенциальных рисков безопасности, эксплуатации и соответствия требованиям. Ключевым аспектом оценки является оценка рисков в сценариях, в которых противники обладают крупномасштабными квантовыми компьютерами, а некоторые криптографические алгоритмы оказываются неэффективными. Это требует переоценки угроз и приоритизации систем миграции для поддержания безопасности. Проведение количественной оценки рисков может привести к получению полного перечня всех рисков, имеющихся средств контроля для их снижения и любых дальнейших действий, которые необходимо предпринять для их снижения.

Независимо от того, решит ли ваша организация провести оценку рисков, она захочет использовать и использовать свои временные шкалы миграции, срока хранения и угрозы (см. рис. 2), определенные в упражнении 1.1. В окончательном списке приоритетных активов будут учтены предполагаемое время миграции, срочность миграции активов и эффективные стратегии снижения рисков.

Результаты мероприятия 2.3:

- Организация оценивает свои запасы и создает список приоритетных активов на основе конфиденциальности и срока службы.
- Если организация выбирает оценку рисков, она разрабатывает полный список всех рисков, действующих средств контроля для снижения этих рисков и любых дальнейших действий, которые необходимо предпринять для их снижения.

Связанные задания: 1.1, 2.2

Категория 3: Планирование и исполнение

Категория 3 этой дорожной карты сосредоточена на действиях высокого уровня, которые ваша организация должна рассмотреть в начале процессов миграции. Ваша организация будет определять, какие постквантовые решения могут быть приобретены у поставщиков или разработаны собственными силами. Краткосрочные и долгосрочные риски снижаются за счет внеполосных механизмов и внедрения решений PQC. Этот раздел намеренно менее директивный из-за отсутствия доступной информации о процессах миграции в организации.

Исходы категории 3:

- Организация разрабатывает план управления миграцией на PQC, определяя, какие системы необходимо приобрести или разработать.
- Организации внедрили, приобрели или разработали решения PQC в своей инфраструктуре.
- Организация внедряет краткосрочные меры по снижению риска раскрытия конфиденциальных данных.

Упражнение 3.1: Составление плана и бюджета миграции

Используя список приоритетных активов из действия 2.3, определите подходящий план действий для каждого приоритетного актива, будь то снижение риска, начало миграции на PQC или управление исключениями, приняв квантовый риск. Вы также можете захотеть связаться с поставщиками вашей организации, чтобы полностью понять уровень риска актива (Упражнение 3.2 (a)). Кроме того, вы захотите получить представление о том, какие кадровые изменения потребуется осуществить вашей организации, чтобы выполнить миграцию PQC (упражнение 4.3).

Затем руководитель миграции в координации с финансовой командой вашей организации и системными операторами оценит затраты на перенос этих активов в PQC. Для выполнения этого действия необходимо понять структуру декомпозиции работ по переносу приоритетных активов, которая может включать запланированные задачи и предполагаемые затраты на каждую задачу.

Упражнение 3.1 Результаты:

- Организация оценивает затраты на перенос своих приоритетных активов в PQC и составляет план бюджетирования.

Связанная деятельность: 2.3, 3.2 (a), 4.3

Упражнение 3.2: Поиск решений

В этом действии руководитель миграции определяет решения, соответствующие потребностям вашей организации в миграции. Руководитель миграции использует список приоритетных активов, созданный в действии 2.3, для координации с внутренними операторами и/или специалистами по обслуживанию системы. Во время первоначальных усилий по координации руководитель миграционной службы должен попытаться

определить и задокументировать, какие системные обновления необходимо получить, а какие обновить внутри компании. Кроме того, руководитель миграции должен определить, какие системы можно перенести на PQC с помощью обновлений программного обеспечения, а какие системы потребуют обновления оборудования.

Кроме того, прежде чем выбирать продукты для миграции, которые лучше всего подходят вашей организации, важно убедиться, что они соответствуют текущим стандартам PQC. Проверьте, соответствуют ли ваши поставщики или системы стандартам и рекомендациям NIST по криптографическим алгоритмам, которые в настоящее время изложены в FIPS 203, 204 и 205. Организации также должны быть осведомлены о программе валидации криптографических модулей NIST, которая проверяет криптографические алгоритмы с использованием набора тестируемых криптографических требований и требований безопасности, чтобы предоставить агентствам метрику для оценки безопасности. Наконец, на протяжении всего этого действия ваша организация должна документально подтвердить свое соответствие.
Документация обеспечит легкий доступ для использования в будущем и предотвратит дублирование усилий.

Необязательно: В течение этого периода руководитель миграции должен оценить жизнеспособность гибридных и/или гибких криптографических реализаций. Гибридные криптографические реализации могут помочь снизить некоторые затраты на процессы миграции и помочь в обеспечении обратной и прямой совместимости. Инвестиции в гибкие криптографические системы и методы и их внедрение помогут повысить способность вашей организации быстро адаптироваться к новым угрозам безопасности эффективным с точки зрения затрат и времени способом. Внедрение гибких решений сейчас снизит затраты на будущие криптографические обновления, обеспечит долгосрочное обслуживание систем и снизит риски, связанные с привязкой к поставщику или устаревшей криптографией.

Упражнение 3.2 Результаты:

- Организация создает план внедрения системы/решения.
- Организация определяет, какие уязвимые системы необходимо модернизировать, чтобы снизить риски и обеспечить соответствие нормативным требованиям.
- Организация определяет, соответствуют ли доступные решения текущим стандартам PQC.
- Организация определяет необходимость и желание гибких криптографических внедрений/решений.
- Организация оценивает методы внедрения решений PQC и прогнозируемые организационные эффекты.

Связанные задания: 2.3

Мероприятие 3.2 a: Согласование потребностей в миграции с поставщиками

Используя список приоритетных активов, руководитель миграции, в координации с соответствующими организационными органами, ответственными за закупки, должен продолжить взаимодействие с поставщиками систем, чтобы определить доступность постквантовых решений. Руководитель миграционной службы должен подтвердить и повторно проанализировать следующие вопросы из Мероприятия 1.4 (a):

- Когда будут доступны PQC-решения от вендора?
- Потребуются ли для обновления PQC аппаратные или программные реализации?

- Какова стоимость новых решений?
- Каково ожидаемое влияние усилий по внедрению на бизнес?
- Будет ли СВОМ включен в состав решений?

Деятельность 3.2 (a) Результаты:

- Организация определяет, какие решения PQC доступны у коммерческих поставщиков.
- Организация обновляет формулировки закупок и контракты, чтобы обеспечить соответствие вновь приобретенных систем стандартам PQC.
- Организация определяет сроки доступности решений PQC и их стоимость.
- Организация координирует свои действия с поставщиками, чтобы определить степень сбоев в работе организации в процессе внедрения.

Связанные с этим мероприятия: 1.4 (a), 2.3

Упражнение 3.2 b: Создание решений

Используя список приоритетных активов, руководитель миграции должен координировать свои действия с системными операторами пользовательских систем или систем, у которых еще нет коммерческого обновления, чтобы начать процесс разработки. Руководитель миграции должен учитывать следующие аспекты:

- Каковы сроки разработки постквантовых решений?
- Потребуются ли для обновления PQC аппаратные или программные реализации?
- Какова стоимость разработки решений?
- Существуют ли коммерческие решения?

Деятельность 3.2 (b) Результаты:

- Организации определяют сроки, затраты и ресурсы, необходимые для разработки решений для нишевых или пользовательских приложений.
- Организации определяют, существуют ли коммерческие решения, обеспечивающие сопоставимую производительность.

Связанные задания: 2.3

Деятельность 3.3: Разработка краткосрочных мер

Используя временную шкалу доступности решения и оценку приоритетов, руководитель миграции должен определить, какие меры необходимо принять для обеспечения защиты конфиденциальных систем и информации. Кроме того, для систем и данных, подверженных риску атак по принципу «собери сейчас, расшифруй позже», руководитель миграции должен координировать свои действия с операторами и специалистами по обслуживанию систем, чтобы оценить, какие краткосрочные решения могут быть реализованы для снижения риска. Эти меры могут включать:

- Сокращение срока действия новых сертификатов
- Увеличение длины новых сертифицированных ключей
- Планирование отзыва сертификатов с избыточным сроком действия
- Модернизация для поддержки TLS 1.3
- Пересмотр процедур физической безопасности и защиты данных в состоянии покоя для данных с длительным сроком хранения

- Рассмотрите возможность добавления дополнительных уровней безопасности в системы, защищающие данные (VPN)

Хотя эти меры безопасности могут быть полезны для снижения некоторых рисков, связанных с угрозой квантовых вычислений, они **не являются** заменой миграции на PQC.

Результаты мероприятия 3.3:

- Организация определяет необходимость принятия краткосрочных мер по снижению риска квантовой угрозы.
- Организация разрабатывает и внедряет стратегии снижения рисков для снижения риска утечки данных.

Смежные виды деятельности: 3.2 a), 3.2 b)

Деятельность 3.4: Приобретение/разработка решений PQC

В координации с организационными органами по закупкам руководитель миграции начинает приобретать постквантовые решения и распределять ресурсы для внутренней разработки решений.
Эти процессы приобретения и разработки происходят в порядке приоритетных активов, определенных в Мероприятии 2.3.

Результаты мероприятия 3.4:

- Организация распределяет ресурсы для приобретения и развития.
- Организация закупает решения PQC у поставщиков.
- Организация начинает внутреннюю разработку PQC решений.

Связанные задания: 2.3

Упражнение 3.5: Внедрение решений PQC

Ваша организация устанавливает краткосрочные и долгосрочные меры по смягчению последствий и решения. Руководитель миграции определяет масштабы сбоев в организации и создает планы действий в чрезвычайных ситуациях на случай продолжительных сбоев. Если в организации выполняется поэтапное развертывание систем, руководитель миграции упрощает координацию для обеспечения прямой и обратной совместимости.

Упражнение 3.5 Результаты:

- Организация внедряет приобретенные или разработанные решения PQC.
- Организация обновляет инвентаризацию в соответствии с новым состоянием системы.

Категория 4: Мониторинг и оценка

Ваша организация отслеживает процесс миграции и формулирует процесс повторной оценки криптографической безопасности по мере развития квантовых возможностей. В этой категории ведущий специалист по миграции также должен следить за тем, чтобы вся документация по миграции сохранялась, и создавать процессы для непрерывной оценки, чтобы помочь в потенциальной будущей миграции технологий.

Исходы категории 4:

- Организация проверяет внедрение решений и соответствие стандартам.
- Организация подготовила своих сотрудников к использованию/внедрению решений PQC.
- Организация отслеживает ход миграции и проверяет желаемые результаты.
- Организация создает процессы для постоянного мониторинга своей защищенности от технологических разработок.

Деятельность 4.1: Проверка правильности реализации

Руководитель миграции в сотрудничестве с разработчиками системы оценивает эффективность внедренных PQC-систем. В ходе этой деятельности операторы системы убеждаются в том, что внедренное решение соответствует криптографическим и операционным требованиям системы (т.е. обратной и прямой совместимости). После успешной проверки реализации руководитель миграции должен убедиться, что инвентаризация была обновлена в соответствии с новым состоянием системы.

Необязательно: В зависимости от размера и структуры организации руководитель миграции и руководство организации могут выбрать реализацию механизма принудительного применения для поощрения и ускорения процессов миграции в организации.

Упражнение 4.1 Результаты:

- Руководитель отдела миграции оценил эффективность PQC в обеспечении приоритетных активов.
- Требования к функциональной совместимости и эксплуатации проверяются и документируются.
- Запасы обновляются в соответствии с новым состоянием системы.

Упражнение 4.1 a: Обеспечение соответствия отраслевым стандартам

В зависимости от типа данных, с которыми работает ваша организация, она должна убедиться, что миграция PQC учитывает существующие отраслевые нормы. Например, организация сектора здравоохранения может оценить свою миграцию PQC на соответствие стандартам HIPAA, или организация, работающая в ЕС, сертифицирует соответствие NIS2. Кроме того, эти стандарты уже могут требовать действий, связанных с PQC, таких как подготовка к будущему и регулярная оценка рисков, что является более веской причиной для начала планирования миграции PQC. В целом, оценивая текущие стандарты, а также

Предвидение будущих изменений в них позволит вашей организации лучше опережать изменения в нормативных требованиях, а также ландшафт угроз.

Деятельность 4.1 (a) Результаты:

- Организация интегрирует существующие отраслевые стандарты в планирование миграции PQC.
- Организация документирует, как ее миграция PQC соответствует отраслевым стандартам.

Упражнение 4.2: Создание мер для отслеживания успешности миграции PQC

Критически важным для понимания влияния миграции PQC в вашей организации является определение объема конфиденциальной информации, которая была криптографически обновлена. Для выполнения этого действия руководитель миграции может использовать список приоритетных активов, определенный в действии 2.3, для отслеживания криптографического состояния инвентаризации.

При разработке плана измерения производительности помните, что «вы получаете то, что измеряете». Выбирайте показатели, которые эффективно указывают на производительность и могут быть практически собраны. Меры должны быть основаны на данных, ориентированы на прогресс, ориентированы на принятие решений и ограничены несколькими критическими вопросами. Наконец, меры будут направлены на различные категории миграции PQC в вашей организации. Например, для категории подготовки вы можете определить меры по отслеживанию влияния вашего стратегического сообщения на согласование действий заинтересованных сторон. Для планирования и выполнения необходимо отслеживать количество систем, которые перешли на PQC.

Еще предстоит провести обширные исследования о том, как наилучшим образом измерить безопасность миграции PQC. В то же время, организации должны ссылаться на стандарты NIST и NSA, чтобы обеспечить использование самых современных методов измерения.

Упражнение 4.2 Результаты:

- Организация определяет меры, которые позволяют отслеживать успешность миграции PQC.
- Организация может определить объем конфиденциальной информации, которая будет защищена новыми решениями PQC.

Связанные задания: 2.3

Упражнение 4.3: Оценка потребностей в рабочей силе

Руководитель миграции оценит, как оптимизировать текущую рабочую силу вашей организации для внедрения и обслуживания недавно приобретенных/разработанных решений PQC. Это может включать в себя координацию действий с

владельцами/операторами систем для выявления пробелов в текущих рабочих процессах, распределение необходимого обучения и/или определение необходимости привлечения дополнительных специалистов для выполнения процессов миграции. Необходимые изменения, внесенные в персонал организации, могут повлиять на то, как организация планирует бюджет (Действие 3.1) и продолжает осуществлять (Действие 3.5) миграцию PQC.

Результаты мероприятия 4.3:

- Организация определяет, необходимы ли дополнительные тренинги по безопасности для новых реализаций безопасности PQC.
- Организация определяет, требуется ли дополнительная рабочая сила для помощи в эксплуатации/миграции систем на PQC.

Связанные задания: 3.1, 3.5

Упражнение 4.4: Непрерывный мониторинг и обновление

Руководитель миграции будет продолжать отслеживать и измерять изменения в области безопасности вашей организации, обновлять списки инвентаризации, отслеживать соответствие новым стандартам и оценивать среду рисков вашей организации. Как упоминалось в предыдущих действиях, документирование этих изменений и обновлений будет неотъемлемой частью поддержания устойчивости безопасности вашей организации.

Упражнение 4.4 Результаты:

- Организация продолжает актуализировать инвентаризацию криптографических алгоритмов.
- Организация постоянно измеряет прогресс миграции в соответствии с ее целями.
- Организация поддерживает готовность, создавая процесс мониторинга технологического развития и состояния рисков.

Связанная деятельность: Все

Заключение

Для многих организаций переход на PQC имеет решающее значение для защиты своих данных от будущих квантовых угроз. Эта дорожная карта представляет собой адаптируемое руководство по четырем важнейшим категориям этого перехода: (1) Подготовка, (2) Базовое понимание, (3) Планирование и реализация и (4) Мониторинг и оценка. Каждая категория предназначена для того, чтобы предоставить организациям необходимые инструменты и стратегии для эффективного управления сложностями миграции PQC. Процесс, описанный в этой дорожной карте, подчеркивает важность стратегического планирования, согласования действий с заинтересованными сторонами, а также непрерывного мониторинга и документирования для адаптации к технологическим достижениям и поддержания надежной системы безопасности. Поскольку ландшафт квантовых вычислений продолжает развиваться, организации должны оставаться адаптивными, отслеживая обновления в руководствах для поддержания безопасного перехода на PQC.

Ссылки

Аттема Т., Дуарте Дж., Даннинг В., Лекес М., ван дер Шут В., Стивенс М. (2023) Справочник по миграции PQC. (Прикладная криптография и квантовые алгоритмы, Группа криптологии и Национальное агентство по безопасности коммуникаций Нидерландов). https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf

Агентство кибербезопасности и безопасности инфраструктуры (2023) Квантовая готовность: переход к постквантовой криптографии. https:// www.nccoe.nist.gov/sites/default/files/2023-08/quantum-readiness-fact-sheet.pdf

FS-ISAC (2023) Техническая документация по инвентаризации инфраструктуры рабочей группы PQC. https:// www.fsisac.com/hubfs/Knowledge/PQC/InfrastructureInventory.pdf

FS-ISAC (2023) Технический документ по модели рисков рабочей группы PQC. https:// www.fsisac.com/hubfs/Knowledge/PQC/RiskModel.pdf

Д., Перлнер Р., Регеншайд А., Робинсон А., Купер Д. (2024) Переход к стандартам постквантовой криптографии. (Национальный институт стандартов и технологий, Гейтерсбург, штат Мэриленд), внутренний отчет NIST (IR) NIST IR 8547 ipd. https://doi.org/10.6028/NIST.IR.8547.ipd

Национальный институт стандартов и технологий (2024) Стандарт механизма инкапсуляции ключей на основе модульной решетки. (Министерство торговли, Вашингтон, округ Колумбия), Публикация федеральных стандартов обработки информации (FIPS) NIST FIPS 203. https://doi.org/10.6028/NIST.FIPS.203

Национальный институт стандартов и технологий (2024) Стандарт цифровой подписи на основе модульной решетки. (Министерство торговли, Вашингтон, округ Колумбия), Публикация федеральных стандартов обработки информации (FIPS) NIST FIPS 204. https://doi.org/10.6028/NIST.FIPS.204

Национальный институт стандартов и технологий (2024) Стандарт цифровой подписи на основе хэша без сохранения состояния. (Министерство торговли, Вашингтон, округ Колумбия), Публикация федеральных стандартов обработки информации (FIPS) NIST FIPS 205. https://doi.org/10.6028/NIST.FIPS.205

Рабочая группа по квантовой готовности Канадского форума по устойчивости цифровой инфраструктуры (2024 г.) Канадские национальные передовые практики и рекомендации по квантовой готовности. https://ised-isde.canada.ca/site/spectrum-management- телекоммуникации/сайты/default/файлы/документы/Quantum-Readiness%20Best%20Practices%20-%20v04%20-%2010%20July%202024.pdf