УДК: 004.775.056

А.А. Рязанова, А.Ю. Щербаков

К формулированию положений платформено-сервисной модели для информационно-телекоммуникационных систем

Рассматривается расширение модели платформ до сервисной модели с целью интеграции и селектирования сервисов и достижения высокого уровня информационной безопасности для информационно-телекоммуникационных систем, понимаемых как цифровые платформы. В качестве примера показана магистральная квантовая сеть.

Ключевые слова: *платформа, сервисная модель (СМ), инфраструктура, киберфизическая система, магистральная квантовая сеть (МКС), квантовые ключи*

DOI: 10.36535/0548-0027-2021-05-2

ПОСТАНОВКА ЗАДАЧИ

В публикациях последнего времени понятие «платформа» часто используется как основа для построения различных информационных систем.

Наиболее исчерпывающе свойства цифровых платформ описаны в работе [1]. Рассмотрение базовых понятий платформ составляет основу для предлагаемого в настоящей статье расширения модели информационно-телекоммуникационных систем. Итак, сформулируем семь базовых свойств платформ:

1) масштабируемость – способность информационной системы обрабатывать растущий объем задач, добавляя дополнительные ресурсы (вычислительные возможности или функциональные элементы, в том числе нового поколения, выполняющие сходные задачи);

2) тиражируемость – возможность адаптировать и внедрять систему в других условиях, например, на каком-либо предприятии без изменения его структуры и состава субъектов;

3) расширяемость – вероятность дополнять систему субъектами, реализующими новые функции;

4) развитие – сохранять и при возможности приобретать новые качества (наращивать потенциал) на всех этапах жизненного цикла платформы. Это свойство проявляется, например, при переходе от количественных характеристик к качественным в системе обработки Больших Данных. Одно их необходимых условий развития – это включенность в состав информационной системы средств разработки информационного и программного обеспечения;

5) замкнутость в текущий момент времени – наличие фиксированного количества субъектов в конкретный момент времени;

6) целостность – система должна решать задачи, которые не могут быть решены отдельными ее компонентами, сохраняя внутреннюю логику и структуру;

7) безопасность – это целостность и замкнутость, что дополняет свойства конфиденциальности и доступности;

8) возможность связи цифровых платформ между собой, в первую очередь за счет единых или стандартизированных интерфейсов.

Кроме того, в работе [1] было показано, что многие информационно-телекоммуникационные системы, анонсированные как «платформы», на самом деле не являются таковыми. Поскольку не обеспечивают, например, свойств развития или целостности.

На самом деле свойства платформ необходимы, но недостаточны для того, чтобы обеспечивать реализацию услуг и сервисов. Это можно проиллюстрировать на примере равенства нулю производной функции: если функция имеет экстремум, максимум или минимум, то производная в этой точке обязательно равна нулю, но не наоборот – равенство производной нулю еще не обеспечивает экстремума.

Так, наличие всех свойств цифровой платформы еще недостаточно для реализации необходимых для её заказчика или пользователя услуг или сервисов.

СЕРВИСНАЯ МОДЕЛЬ ЦИФРОВОЙ ПЛАТОРМЫ

Инфраструктурное понятие, необходимое для целостного описания и моделирования процессов оказания услуг клиентам, в первую очередь связанных с защитой передачи данных и информации, означает сервисную модель (СМ) платформы.

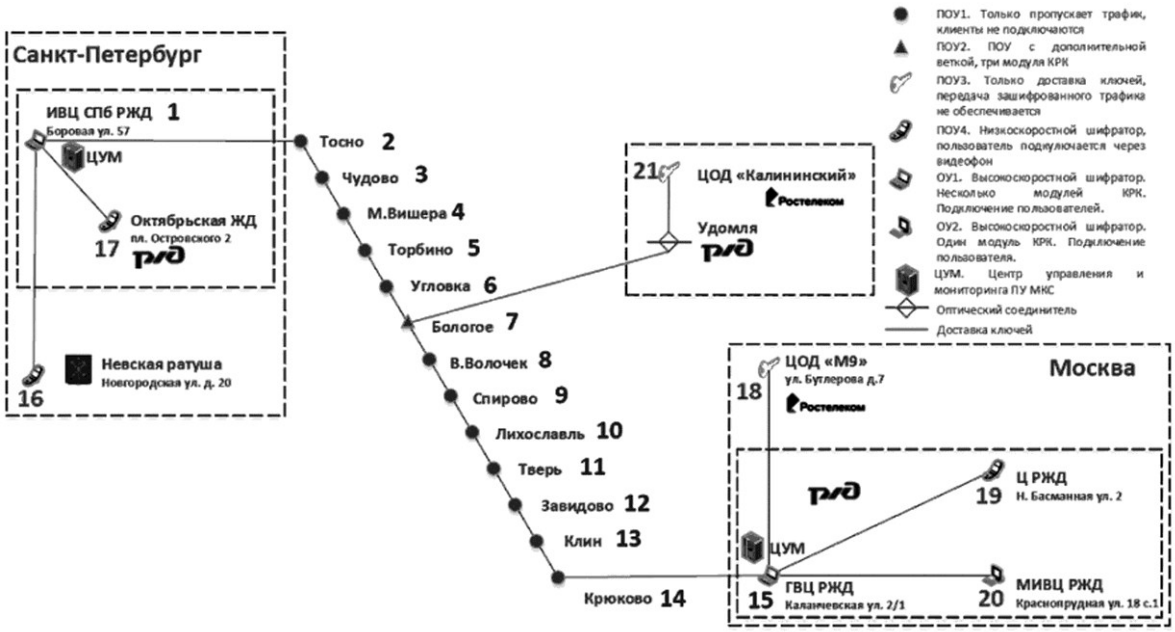

Схема магистральной квантовой сети (МКС), участок Москва – Санкт-Петербург.

Сформулируем и проиллюстрируем положения сервисной модели на примере киберфизической платформы квантово-защищенной сети [2], представленной на рисунке.

Принципиальное отличие квантово-защищенной сети от произвольной сети передачи данных заключается в наличии в ней механизма выработки и распределения квантовых и связанных с ними ключей. Основу сервисной модели составляют процедуры распределения и хранения ключевой информации пользователей и построенные на их базе разнообразные сервисы. В данном случае сервисы цифровой платформы связаны в первую очередь с защищенными услугами передачи данных, включая голосовой трафик, а также приватную электронную почту и мессенджеры.

АРХИТЕКТУРА МАГИСТРАЛЬНОЙ КВАНТОВОЙ СЕТИ И КЛЮЧЕВЫЕ КОНТЕЙНЕРЫ

Обмен квантовыми ключами физически возможен только для смежных узлов сети, поэтому для обмена информации транзитного характера (для произвольной топологии магистральной квантовой сети – МКС) необходимо применять другие виды ключей, последовательно используя защищенные каналы, образованные между смежными узлами.

Передача ключей абонентам или в оконечные узлы сети, не содержащие квантового оборудования, должна происходить в зашифрованном виде, для чего используется конструкция ключевого контейнера.

Ключевой контейнер (КК) – это информационный объект сервисной модели, который применяется для защищенной (обеспечивающей целостность и конфиденциальность) передачи ключей между элементами МКС, и состоит из совокупности открытых и закрытых полей, целостность которых зафиксирована, и в обязательном порядке содержит ключи, которые зашифрованы таким образом, чтобы обеспечить их безопасную передачу и хранение внутри или вовне МКС (для этого используется шифрование на квантовых ключах, на паролях, на ключах аппаратных хранилищ, входящих в состав МКС и т.д.). Кроме того, КК содержит дополнительную информацию, обеспечивающую его функционирование в рамках сервисной модели: назначение ключа, данные о владельце ключа, количество использований ключа и другую информацию.

В магистральной квантовой сети формируются, распределяются, хранятся, архивируются, выводятся из действия следующие типы криптографических ключей:

1) квантово-связанные ключи (КСК), которые получены абонентами, соединенными системой квантового распределения ключей (системой КРК) – на рисунке соседние по нумерации узлы;

2) квантово-защищенные ключи (КЗК), передаваемые одному или нескольким узлам, защищенные при помощи КСК;

3) ключи парной связи защиты трафика (КЗТ) – элементы матрицы ключей, предназначенные для передачи (в том числе и транзитной) трафика от одного узла к другому без перешифрования на узле;

4) ключи оконечных узлов (ОКУ), доставляемые и используемые на ОКУ для связи с узлом МКС, либо другим ОКУ;

5) сервисные ключи – поставляемые абонентам в рамках сервисной модели и используемые различными службами МКС;

6) служебные ключи, используемые для реализации сервисных функций, например, подсистемы управления и мониторинга.

По криптографическому алгоритму из реального имени абонента или узла формируется сетевое имя абонента, по которому невозможно восстановить реальное имя абонента.

В МКС используются также датчики случайных чисел (ДСЧ) – квантовые, аппаратные и программные. Их использование определяется требованиями регулятора. При генерации ключей при помощи ДСЧ происходит статистический контроль качества ключа.

Формат ключа в рамках платформенно-сервисной модели

№	Поле	Длина, байт	Примечание
1	Идентификатор «Ключ системы»	4	
2	Идентификатор ключа	16	Сквозной идентификатор, по которому ключ используется во всей системе; для ОКУ может совпадать с сетевым именем
3	Идентификатор узла-отправителя	4	Может быть сформирован из сетевого имени
4	Идентификатор узла-получателя	4	
5	Тип ключа	4	Определяет тип (КЗК, КЗТ и др.)
6	Ограничения ключа	4	Определяет срок действия ключа сервисной модели, количество использований или максимальный трафик, зашифрованный (имитозащищенный) на нем, другие ограничения; действует по правилу «или»
7	Длина ключа	4	
8	Тело ключа под маской	Длиной из поля 7	
9	Тело маски	Длиной из поля 7	
10	Дата создания ключа	8	
11	Дата прекращения действия ключа	8	
12	Текущее количество использований ключа	8	
13	Предельное количество использований ключа	8	
14	Текущий трафик на ключе	16	
15	Предельный трафик на ключе	16	
16	Имитовставка на поля 2-15	8	
17	Резервное поле	N	

Ключи хранятся в системе и передаются в виде контейнеров – ключей, зашифрованных на транспортном ключе, в качестве которого может использоваться КСК, либо ключ, доставленный по альтернативному (отличающемуся от квантового) каналу связи.

Периодичность обновления и, соответственно, архивирования КЗТ, а также скорость и объемы формирования КСК и КЗК определяются с учетом технических возможностей МКС и требований и рекомендаций регулятора.

В таблице в рамках платформенно-сервисной модели рассматриваются форматы ключей.

Исходя из данных таблицы полагаем, что при поле *N*=16 и его размере 7 в 32 байта длина ключа составит 192 байта. Ключевой контейнер может иметь бо́льшую длину, но может быть сформирован путем зашифрования части полей ключа с последующей проверкой правильности расшифрования при помощи имитовставки.

ПРОТОКОЛ ИСПОЛЬЗОВАНИЯ И РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ. ПОНЯТИЕ КОНСИСТЕНТНОСТИ ПЛАТФОРМЫ

Предположим, что система магистральной квантовой сети состоит из *N* узлов произвольной топологии (на рисунке приведена практически линейная топология, когда узлы от второго до пятнадцатого соединены линейно-последовательно), описанной матрицей KV размера MxM (в случае примера МКС Москва – Санкт-Петербург M=21), где KVij элемент матрицы, равный 1, если существует квантовый обмен между узлами i и j, и равный нулю в ином случае.

Для избежания перешифрования информации на каждом узле необходимо доставить полную матрицу ключей (КЗТ) на каждый узел, причем для передачи необходимо использовать КСК. Желательно в этом случае минимально использовать шифрование и операции типа XOR – исключающее «или» (одноразовый блокнот) при передаче ключей.

Допустим, что в рамках любого узла (от 1 до 21) в МКС выделена одна ключевая мастер-нода – независимый узел, который управляет выработкой и распределением матрицы ключей узлов размера MxM.

С учетом приложенного формата ключа (ключ длиной 192 байта при длине резервного поля в 16 байт) матрица будет иметь размер 192xNx(N-1). Например, при 10 узлах 192x10x9=17280 байт.

Для передачи такого блока между узлами предполагается концепция развёрнутого квантово-связанного ключа. Пусть имеется КСК KKLij, используемый между узлами i и j МКС, тогда вырабатывается ключ RKLij – развернутый квантовый ключ, получаемый по следующей схеме:

$$RKLij = GAMMAt(iv, KKLij),$$

где iv – начальный вектор, например i^j; KKLij – квантовый ключ; GAMMAt – алгоритм выработки гаммы длиной t байт (например, при помощи алгоритма «Кузнечик»).

Далее, развернутый квантовый ключ RKLij накладывается на передаваемую матрицу ключей узлов размера NxN, предназначенную для транзитной передачи между узлами без перешифрования. При при-

еме на узле формируется подтверждение о получении матрицы ключей узлов размера NxN для ключевой мастер-ноды.

Для передачи информации от узла i к узлу j используется KMij при его наличии. Таким образом, возникает понятие ключевого консенсуса, когда матрица доставлена на все узлы МКС. При отсутствии матрицы ключей узлов размера NxN на узле для передачи информации на связанный узел(ы) используется ключ KKLij.

Для оконечных узлов ключевая мастер-нода формирует контейнеры – ключи ОКУ, предназначенные для его связи с другими узлами сети, в том числе с другими ключами оконечных устройств, зашифрованными на TKm. В простом случае ОКУ имеет один ключ KOm, где m – идентификатор ОКУ (4 байта), предназначенный для связи с узлом, к которому он подключен.

В этом случае узел подключения расшифровывает информацию от ОКУ. В каналах МКС она шифруется на ключе из матрицы ключей узлов размера NxN в зависимости от маршрута.

Требование приватности «точка–точка» предполагает выработку KOmr и помещение его в контейнер, где m – идентификатор ОКУ отправителя, r – идентификатор ОКУ получателя. В этом случае на узле происходит транзитная передача информации от m к r. При этом KOm используется для аутентификации, либо происходит шифрование на KOmr, а затем на KOm.

Для обеспечения целостности информации можно использовать KKLij, модифицированные константой, чтобы избежать шифрования и вычисления имитовставки на одном ключе. Такой подход позволит достигнуть еще одного важного свойства цифровой платформы в рамках сервисной модели – консистентности, т. е. связанности всех узлов в единую систему доступных друг для друга сервисов.

ВОЗМОЖНЫЕ СЕРВИСЫ ДЛЯ ПЛАТФОРМЕННО-СЕРВИСНОЙ МОДЕЛИ

Магистральная квантовая сеть имеет следующие виды защищенных сервисов, называемые ключами:

1) транзитной передачи данных между узлами;

2) клиентов для связи с опорными узлами – подключение новых пользователей к МКС;

3) клиентов для связи между собой (для поддержания режима конфиденциальности абонентской связи) – для работы мессенджеров и телефонной связи;

4) инициализации датчиков случайных чисел (ДСЧ) для программных ДСЧ, расположенных у клиента или в опорных узлах – для формирования новых ключей и получения новых типов сервисов;

5) оконечных внешних сервисов (IP-телефония, видеосвязь), предоставляемых внешними операторами связи;

6) корпоративных хранилищ и облаков – для хранения данных пользователей, в том числе и персональных;

7) внутрисетевых и корпоративных распределенных реестров;

8) для работы с аппаратными хранилищами данных;

9) для взаимодействия со сторонними сервисами и другими системами защищенной передачи данных, включая системы государственных услуг, Федеральную налоговую службу и других.

ВЫВОДЫ

Для реализации сервисной модели киберфизической системы необходимо расширение модели платформы в сторону платформенно-сервисной модели.

Это должно облегчить коммерциализацию и увеличение сервисов цифровой платформы, поскольку добавление, селектирование, управление и билинг (учет использования сервисов пользователями) сервисов могут быть достаточно просто реализованы.

Кроме того, механизм контейнеров позволяет легко добавлять в систему различные сервисы, реализовывать механизмы конвертации ключевых форматов для других платформ и сервисов, в первую очередь защищенных.

Дополнительные свойства платформенно-сервисной модели – это повышение устойчивости и надежности сети за счет хранения контейнеров как минимум у двух подсистем платформы, а также возможность как мониторинга информации о сервисах (используя информацию в контейнерах, например, объем трафика, закрытый на некотором ключе), так и восстановления платформы при сбоях или поломках оборудования.

Для платформенно-сервисной модели в нашей работе дополнительно введено понятие консистентности как связанности всех узлов и подсистем в единую систему доступных друг для друга сервисов.

СПИСОК ЛИТЕРАТУРЫ

1. Рязанова А.А. Цифровые платформы: интегративный потенциал, основные понятия и свойства // Вестник современных цифровых технологий. – 2020. – №4. – С. 26-36
2. Техническое задание на разработку «Пилотного участка магистральной квантовой сети», шифр «7.422». Минобрнауки РФ, 2020. – 84 с.

Материал поступил в редакцию 28.02.21.

Сведения об авторах

РЯЗАНОВА Алина Александровна – научный сотрудник Центра развития криптовалют и цифровых финансовых активов ВИНИТИ РАН, аспирант ВИНИТИ РАН, Москва.
e-mail: a.ryazanova@c3da.org

ЩЕРБАКОВ Андрей Юрьевич – доктор технических наук, профессор, начальник Центра развития криптовалют и цифровых финансовых активов ВИНИТИ РАН, профессор кафедр «Интеллектуальные системы информационной безопасности» Российского технологического университета МИРЭА и «Безопасность цифровой экономики и управления рисками» Российского государственного университета нефти и газа имени И.М. Губкина, Москва
e-mail: x509@ras.ru