УДК 20.53.19, 28.23.13

Е. Г. Воробьев
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Концепция обеспечения непрерывности функционирования распределенных информационно-телекоммуникационных систем на основе квантовых методов представления информации

Анализируется возможность использования квантовой теории информации для обеспечения непрерывности функционирования глобальных информационных систем, предложена новая концепция отображения мобильных и стационарных объектов и их паспортов в едином информационном пространстве.

Квантовая теория информации, единое информационное пространство, обеспечение непрерывности функционирования информационных систем, пространственная модель

В настоящее время разработка планов обеспечения непрерывности функционирования единых автоматизированных информационных систем масштаба министерств и крупных корпораций опирается на разработки западных институтов, в частности BCI и существующие технологии от производителей вычислительной техники (кластеры и облачные технологии).

Как показывает практика, данные разработки предъявляют либо слишком упрощенные требования к менеджерам по обеспечению непрерывности функционирования организации: рассчитать время возможной потери информации (recovery point objective – RPO) и время возможного восстановления (recovery time objective – RTO) и сообщить его поставщикам оборудования, которые на основе готового списка оборудования гарантируют необходимое время восстановления информационных технологий за указанное время и выход на штатный режим функционирования (западный подход), либо слишком сложные: создание модели угроз и нарушителя, расчет частных показателей качества функционирования и затем индивидуальный подбор организационно-технических мер (отечественный подход).

Проблема обеспечения непрерывности функционирования современных отечественных распределенных вычислительных систем и сетей в наибольшей степени связана с необходимостью учитывать огромное количество факторов, угроз, уязвимостей, путей их реализации и условий внешней среды, в которой функционирует типовой объект информатизации. Чаще всего ошибки возникают из-за экономии денежных средств, при этом актуализированная модель угроз не отражает действительного положения дел в области информационной безопасности. К тому же, процессы восстановления, описанные в планах, как правило, предполагают отсутствие мешающих воздействий их реализации.

На самом деле современное видение проблем, связанных с глобальными природными катаклизмами и злонамеренным воздействием человека на существующие процессы, таким, как информационные и обычные войны, предполагает разработку новой концепции обеспечения непрерывности функционирования информационных систем на основе альтернативных технологий, в частности квантовых.

Оптимизация средств резервного восстановления информации. Задача восстановления информации в случае ее злонамеренной или слу-

чайной модификации или уничтожения в настоящее время решается на основе концепции резервного хранилища и резервных площадок. Резервное хранилище предполагает периодическое перемещение сохраняемой информации для ее долговременного хранения в защищенное от типовых воздействий помещение. При этом объем выделенной для хранения информации существенно меньше реального объема информации, циркулирующей в организации. Резервная площадка (в трактовке Microsoft) может быть «холодной», «теплой» или «горячей», стационарной или мобильной и предполагает наличие полного набора вычислительных средств и необходимой информации. В этом случае также решается вопрос о размещении ее в защищенном месте. Как показывает практика ведущих министерств России [1], анализ местоположения такой резервной площадки предполагает работу с данными регионального МЧС и картой местности с расчетом времени развития опасных техногенных и стихийных чрезвычайных ситуаций.

Если для стационарных объектов организаций задача их защищенного расположения может быть решена вручную, несложными геометрическими построениями и расчетами, то оптимизация сети с учетом размещения информации в базах данных на основании концепции «распределенная обработка» или «budge up», предполагающей перенос рабочей нагрузки на уцелевшие серверные и рабочие станции, уже требует расчетов на основе метода «ветвей и границ» [2], что является частным решением «задачи о коммивояжере» и даже для современных компьютерных систем представляет сложную вычислительную задачу.

В то же время, такой метод основан только на простых оценках длин маршрутов, а не на их защищенности, или оценке безопасного расположения узлов на местности с учетом антропогенных, техногенных и стихийных факторов. Любой из этих дополнительно учитываемых параметров увеличивает сложность задачи приблизительно на порядок.

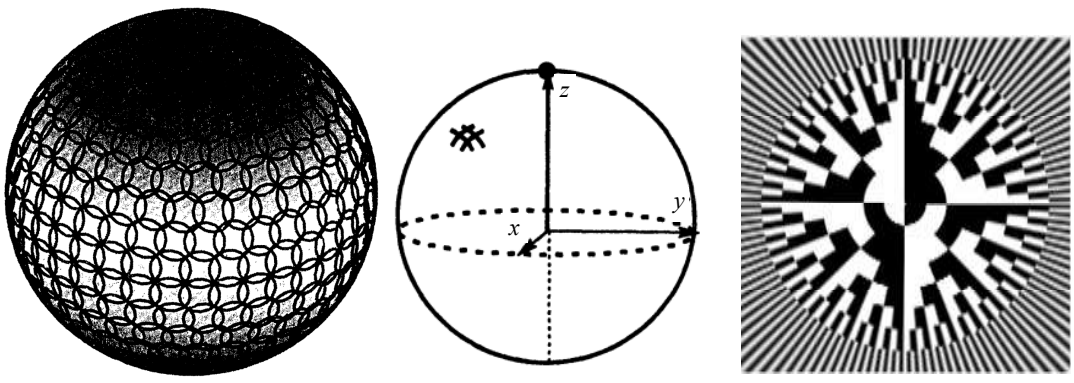
Свой вклад вносит и современная архитектура сетей, предполагающая формирование рабочих коллективов и сегментов сетей «на лету», в реальном масштабе времени с применением большого количества мобильных устройств, требующих для проверки безопасности их размещения решения задач топопривязки, а затем – указанных ранее задач.

Построение современных сетей ориентировано на массовый обмен информацией без ограничений, из-за чего рост необходимой пропускной способности каналов также связан с постоянным прогнозированием развития инфраструктуры и оптимизацией размещения резервных центров хранения информации.

Как правило, объем данных центров верхнего уровня иерархии (с размещением в рамках г. Москвы и ее области) таков, что требует именно стационарного размещения и практически не способен к переносу.

Исходя из вышеизложенного первой задачей оптимизации является разработка модели пространства, позволяющей на основе базы знаний иметь заранее составленную характеристику безопасности каждой его точки. Типовой моделью подземного, наземного и околоземного (воздушного и космического) пространства является комплекс вложенных друг в друга сфер различного радиуса, поверхность которых может служить для размещения карт интересующих объектов (рис. 1, где *а* – пространство состояний (кодовых слов), *б* – сфера Блоха, *в* – двоичное поле байта (младшие разряды снаружи)).

Элементарная единичная анализируемая площадь описывается отдельной записью в специальной базе знаний, которая может обновляться существующими техническими средствами наблюдения.



а *б* *в*

Рис. 1

Таблица 1

Количество разрядов в двоичном представлении	Количество элементов дуги	Угол, образующий элемент дуги, … °	Длина элемента дуги, км	Точность отображения координаты объекта
8	256	1.40625	156.2885938	–
15	32 768	0.010986328	1.221004639	1.2 км
19	524 288	0.000686646	0.07631279	70 м
22	4 194 304	8.58307E-05	0.009539099	9 м
25	33 554 432	1.07288E-05	0.001192387	1.1 м
28	268 435 456	1.3411E-06	0.000149048	15 см
32	4 294 967 296	8.3819E-08	9.31553E-06	0.93 см
35	34 359 738 368	1.04774E-08	1.16444E-06	1.16 мм

В работе [3] были описаны подходы к отображению координат объекта в виде его двоичного кода, соотнесенного с его расположением в упорядоченном двоичном поле. Для длины окружности поверхности Земли 40 009.88 км в табл. 1 иллюстрируется размерность элементарного отрезка (сегмента) на воображаемой окружности радиуса Земли, т. е. точность отображения координат объекта на поверхности Земли, а табл. 2 описывает количество разрядов двоичного кода, которое нужно для указания номера некоторого отрезка (сегмента). Из табл. 1 видно, что для отображения местоположения объекта на расстоянии, равном радиусу Земли, с точностью 1 см достаточно 32 бит кода, а с точностью 1 мм – 35 бит. Количество разрядов в двоичном представлении позволяет рассчитать количество элементов на окружности, проведенной на поверхности сферы. В то же время, для удобства считывания такой информации в условиях уменьшения углов между соседними сегментами внешнего лимба требуется увеличивать радиус сферы, чтобы получить приемлемую длину элемента дуги, отображающего сегмент. Из табл. 2 видно, что при увеличении радиуса сферы от поверхности Земли до расстояния в 4 006 370 км рост разрядности двоичного кода составляет всего лишь 2 разряда.

Таблица 2

Количество разрядов в двоичном представлении	Радиус сферы (R), км
10.85579164	6370
11.87287287	1 006 370
12.15250714	2 006 370
12.32122566	3 006 370
12.44243056	4 006 370

Таким образом, наращивание длины кода при неизменном радиусе расчетной сферы увеличивает точность отображения местоположения объекта. С другой стороны, для геоинформационных систем может быть принят один общий радиус для расчетной сферы, в пределах которой обеспечивается достаточная различимость сегмента при приемлемой точности целеуказания.

Таблица 3

Код местоположения объекта		Паспорт объекта (информационный кластер)				
Код положения вектора направления на объект	Дальность до объекта	Текстовая информация (описания + анализ ИБ)	Звуковая информация (сообщения)	Фото /ИК-фото и т. д.	Видео	3D-карта (с оценкой опасности расположения)
Подземное/подводное пространство и объекты						
Наземное/надводное пространство и объекты						
Воздушное пространство и объекты						
Околоземное космическое пространство и объекты						
Дальний космос						

Поскольку для получения информации о характеристиках объекта (его паспорта) необходима специальная запись в базе знаний, предлагается представлять информацию в следующем виде (табл. 3).

В этом случае моделью любой пространственной системы объектов (в частности, вычислительных комплексов и сетей) является суперпозиция кодовых записей в базе знаний. Причем эта суперпозиция для любой частной системы является конкатенацией кодов записей отдельных объектов, т. е. одним длинным кодом в более общем поле упорядоченных двоичных кодов, которые были описаны автором в работе [4].

На основании такой модели пространственной системы объектов можно строить различные аналитические модели и проводить проверку решений при синтезе автоматизированных систем в защищенном исполнении.

Для статических во времени и пространстве систем параметры безопасности могут быть рассчитаны на основе долгосрочного прогноза. Для динамически формируемых систем быстро проводятся оценки и принимаются решения по мониторингу.

При постоянной поддержке средствами наблюдения космического, воздушного и наземного базирования информационные кластеры могут обновляться в реальном масштабе времени, что при замкнутости общей надсистемы по управлению и информации позволит непосредственно влиять на данные прогноза, мониторинга, непосредственного оповещения в условиях чрезвычайных ситуаций, стихийных бедствий и целенаправленных антропогенных воздействий.

Второй задачей оптимизации является снижение нагрузки на системы связи ввиду необходимости передавать большие объемы информации «от каждого – каждому». В данном случае возможно построение системы, в которой не вся информация, содержащаяся в вычислительных системах всего мира, может быть представлена как кодовая суперпозиция одним сверхдлинным информационным словом (файлом).

На основе метода сжатия, базирующегося на квантовых подходах [4], может быть получена резервная информация, имеющая малый объем, пригодная для централизованной рассылки с помощью систем спутниковой радиосвязи, учитывая, что в этом случае реализуется разовая рассылка по принципу «от одного – ко многим», в пределах зоны радиопокрытия определенного пространства или части территории планеты.

Легко видеть, что в данном случае исключается потребность в обмене информацией всех вычислительных средств зоны, за исключением работы по передаче обновленной информации. В этом случае требуется специальный координирующий центр резервирования, который будет регулярно производить сжатие и обновление резервной копии, а также управлять ее рассылкой, т. е. давать команды спутникам радиотрансляции.

Такой защищенный центр может располагаться в земных условиях, но, исходя из количества угроз антропогенного, техногенного и стихийного характера, предпочтительнее выглядит модель угроз центра, расположенного на борту орбитальных космических средств. При этом реализуется только защита от космической радиации, метеоритных потоков и противоспутникового оружия. К тому же, при необходимости автономной работы такой центр сможет сам управлять сбором и обновлением информации в базе знаний о заданном пространстве, так как обладает возможностью перемещения в космическом пространстве.

Реализация бортовых систем такого центра с учетом массогабаритных требований может быть реализована лучше всего на основе нано- и квантовых технологий.

И, наконец, третьей задачей является исключение воздействий на каналы передачи информации, связывающие резервный центр с целевыми заказчиками. Современные методы реализации непрерывности функционирования информационных систем практически не учитывают целенаправленное воздействие именно на процессы восстановления информации. Наиболее характерно это для существующих международных классов восстановления информационных систем, где расчет показателя RTO и фаз восстановления ведется для «идеальных» условий.

Появление квантовой криптографии ознаменовало собой переход к защищенным технологиям передачи информации за счет использования управляемой поляризации, когда каждый бит формируется за счет разных состояний поляризационных параметров световой волны.

Внедряемые сейчас за рубежом протоколы BB84, B92 построены на принципе формирования на передающей стороне случайного набора поляризационно-модулированных бит и фиксированных настроек поляризационных фильтров на приемной стороне, что требует дальнейшего обсуждения по открытому каналу с целью выделения правильной информации. Протокол Экерта использует взаимодействие двух бинарных процессов на передающей и приемной сторонах за счет создания «связанных» частиц на физическом уровне, что технологически трудно реализуемо.

Тем не менее, возможно создание отечественных квантовых протоколов, свободных от недостатков западных подходов. Целью синтеза должен быть сигнал в канале передачи, для которого выполняется критерий Шеннона для теоретически не вскрываемого шифра – вероятность 0.5 для правильного распознавания состояния информационного бита.

Для этого достаточно формировать на приемной стороне ожидаемое состояние поляризации на каждый передаваемый бит. Тогда для передачи единицы это состояние должно быть сформировано на передающей стороне, а для передачи нуля – любое другое состояние. Оно не выделяется фильтром, подключенным в этот момент на приемной стороне, но носит характер единицы для любого злоумышленника, прослушивающего канал.

В простейшем случае – для бинарной передачи информации – достаточно иметь 2 фильтра, переключаемых под управлением любой сгенерированной по ГОСТ 28147–89 двоичной последовательности, известной также на передающей стороне.

Подведем итоги:

1. Создание современных информационных систем, реализующих единое информационное пространство, должно опираться на современные технологии реализации непрерывности их функционирования, а также быстрого и надежного восстановления информации.

2. Исследования автора показывают, что имеется возможность реализации всех необходимых элементов систем резервирования на основе квантовых технологий.

3. Важным направлением исследований является развитие предложенной автором концепции, позволяющей реализовать защищенное от воздействий единое информационное пространство.

4. Возможно создание глобальных информационных систем, в которых информация о положении объекта может являться и информационным кластером, описывающим его важные характеристики.

5. В статье впервые предлагается структура единой информации о точках земного и околоземного пространства и объектах, расположенных в них, в виде отображения в едином математическом поле двоичных кодов.

СПИСОК ЛИТЕРАТУРЫ

1. Воробьев Е. Г. Процесс и процедуры обеспечения непрерывной работы и восстановления ресурсов информационных систем ФТС России. М.: Академия Ай-Ти, 2008.

2. Янбых Г. Ф. Применение метода «ветвей и границ» для топологической оптимизации сети телеобработки данных при ограничении на время реакции// Автоматика и вычислительная техника. 1980. № 5. С. 3–7.

3. Воробьев Е. Г. Использование фрактальной структуры полей, образованных кодами с различными основаниями, для решения задачи создания единого информационного пространства // Изв. СПбГЭТУ «ЛЭТИ». 2015. № 3. С. 11–16.

4. Воробьев Е. Г. Комплексные числа и оптимизация средств хранения информации в глобальных информационных системах // Изв. СПбГЭТУ «ЛЭТИ». 2015. № 2. С. 22–26.

E. G. Vorobiev
Saint-Petersburg state electrotechnical university «LETI»

THE CONCEPT OF PROVIDING A CONTINUITY OF FUNCTIONING OF THE DISTRIBUTED INFORMATION AND TELECOMMUNICATION SYSTEMS ON THE BASIS OF QUANTUM METHODS OF SUBMISSION OF INFORMATION

The possibility of use of the quantum theory of information for providing a continuity of functioning of global information systems is analyzed, the new concept of display of mobile and stationary objects and their passports in a common information space is offered.

Quantum theory of information, common information space, providing of information systems functioning continuity, spatial model

УДК 004.3’144

А. Х. Мурсаев, В. О. Ameленко
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Высокопроизводительные устройства шифрации информации

Рассматриваются вопросы аппаратной реализации устройств шифрации информации. Представляется ряд структурных решений, отличающихся по затратам и производительности.

Устройства шифрации информации, аппаратная реализация

Шифрация информации является одним из важнейших средств обеспечения информационной безопасности. До последнего времени зашифровывали в основном текстовые и звуковые сообщения, а со скоростями передачи подобной информации вполне справляются процессорные средства общего назначения. Но в последнее время возникла потребность и возможность обработки более интенсивных потоков данных, в том числе передача в реальном времени результатов секретных испытаний, закрытые видеоконференции или хотя бы кодирование телевизионных сигналов в закрытых платных кабельных сетях и т. п. Здесь необходима скорость обработки до нескольких десятков миллионов символов в секунду, поэтому требования по производительности шифраторов/дешифраторов непрерывно растут и вызывают к жизни аппаратную реализацию этих задач.

Большинство современных алгоритмов шифрации, таких, как Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES) Рейндаля, а также ГОСТ 28147–89 [1]–[4] используют разбиение потока исходных данных на блоки по нескольку десятков бит (поэтому их называют блочными). Блоки кодируются независимо, последовательно друг за другом. Алгоритмы объединяет то, что для каждого блока выполняется многократное повторение двух базовых операций – перестановки бит в шифруемом блоке и поэлементная замена фрагментов шифруемых блоков (байт, тетрад и т. п.) на соответствующие им значения, содержащиеся в памяти ключей шифрации. В ряде алгоритмов операция замены интерпретируется как арифметическое преобразование исходного данного и соответствующего подключа или сочетания замены и арифметического преобразования. Подключом называют отрезок кода секретного ключа, используемого для шифрования.

В качестве примера на рис. 1 приведена схема алгоритма IDEA. Выполняется последовательность из нескольких шагов, на каждом из которых осуществляются двухместные операции с отрезками блока данных и подключами, а также соот-