УДК 681.3

А. А. АЛИЕВ[1], Р. Б. САМЕДОВ[2]

ОТКАЗОУСТОЙЧИВАЯ ВОЛОКОННО-ОПТИЧЕСКАЯ ИНФОРМАЦИОННАЯ РАСПРЕДЕЛЕННАЯ СИСТЕМА В ЧАСТНОМ ОБЛАКЕ

[1]***Бакинский Государственный Университет***
улица академика Захида Халилова, 23, г. Баку, Азербайджан.
Тел.: +994503528150, E-mail: aaliyev@mail.ru

[2]***Бакинский Государственный Университет***
улица академика Захида Халилова, 23, г. Баку, Азербайджан.
Тел.: +994502785192, E-mail: ramin.samedov@gmail.com

Аннотация. В статье представлены современные технологии по обеспечению отказоустойчивой работы волоконно-оптической информационной распределенной системы в частном облаке. Разработан алгоритм отказоустойчивой работы, на примере работы базы данных Oracle 11G, который обеспечивают автоматическую восстановление работы базы данных в случаи выхода из строя основного сервера базы данных. Проведены эксперименты, результаты которых приведены в таблице и на графике.

Ключевые слова: облачные вычисления, отказоустойчивость, распределенная система, волоконно-оптические кабели, частное облако

Анотація. У статті представлені сучасні технології щодо забезпечення відмовостійкої роботи волоконно-оптичної інформаційної розподіленої системи в приватному хмарі. Розроблено алгоритм відмовостійкої роботи, на прикладі роботи бази даних Oracle 11G, який забезпечують автоматичну відновлення роботи бази даних у випадку виходу з ладу основного сервера бази даних. Проведено експерименти, результати яких наведені в таблиці і на графіку.

Ключові слова: хмарні обчислення, відмовостійкість, розподілена система, волоконно-оптичні кабелі, приватна хмара

Abstract. The article presents the latest technologies of high availability to ensure fail-safe operation of fiber-optic distributed information systems in a private cloud. The algorithm for fault-tolerant operation, by the example of Oracle 11G database, which provide automatic restoration of the database in case of failure of the main database server was shown in the article. Experiments and the results are shown in the table and in the graph.

Keywords: cloud computing, fault tolerance, distributed systems, fiber optic cables, a private cloud

ВВЕДЕНИЕ

Благодаря технологиям виртуализации появилась возможность объединения многочисленных интернет-серверов в единые кластеры с практически неограниченной производительностью. Помимо высокой надежности, такие кластеры позволяют оптимизировать нагрузку на каждый сервер, а следовательно, значительно снизить стоимость компьютерных ресурсов.

Низкая стоимость, высокая надежность и передача на аутсорсинг задач поддержки информационных технологий инфраструктуры - вот те факторы, которые стали залогом стремительного успеха облачных технологий.

Основные сферы применения Cloud Computing [1]:

— IaaS (Infrastructure as a Service) — облачные платформы, на которых можно арендовать операционную систему Windows/Linux сервера с масштабируемой мощностью. Примеры: Amazon Web Services, Rackspace Cloud.

— PaaS (Platform as a Service) — облачные платформы со всем необходимым промежуточным и вспомогательным программным обеспечением (СУБД, фреймворк, сервисы). Примеры: Windows Azure, Force.com.

— SaaS (Software as a Service) — бизнес-приложения, поставляемые в качестве интернет-сервисов. Примеры: Google Apps, Salesforce CRM.

ЧАСТНЫЕ ОБЛАКА

С развитием облачных вычислений, в больших компаниях создаются частные облака. Частное облако — это концепция построения информационных технологий (ИТ), направленная на реализацию принципа «ИТ, как услуга». Серверы объединяются в пул, из которого на решение определенных задач выделяются вычислительные ресурсы, не привязанные к конкретным физическим серверам. Предоставление мощностей из такого динамического пула осуществляется по запросам клиентов. При этом могут быть выделены виртуальные серверы под задачи бизнес-приложений или тестирования, предоставлены отдельные приложения или целые виртуальные рабочие места пользователей, а персональные компьютеры на столах сотрудников могут быть заменены «тонкими клиентами» — небольшими устройствами, тихими и экономичными.

В отличие от публичных облачных сервисов, частное облако способствует повышению уровня информационной безопасности за счет локализации всех данных в защищенном дата центре, а не на рабочих станциях пользователей. Централизованное хранение и обработка данных открывает новые возможности для мобильной работы — с любого подходящего устройства из разных точек мира можно получить доступ к корпоративным информационным ресурсам и к своему персональному рабочему окружению [2].

Предпосылки для перехода к частному облаку

— Изменение структуры предприятия (выделение дочерних обществ, поглощение компаний).

— Замена парка персональных компьютеров

— Выделение ИТ-службы в аффилированную структуру.

— Планируется масштабная замена или внедрение корпоративных информационных систем.

— Планируется значительное повышение нагрузки на ИТ-инфраструктуру или повышение ценности ИТ для бизнеса.

Преимущества частного облако:

— Повышение способности ИТ быстро подстраиваться под потребности бизнеса.

— Сокращение простоев пользователей.

— Повышение безопасности хранения и обработки данных.

— Рост мобильности пользователей.

— Повышение качества предоставляемых ИТ услуг.

— Гарантия доступности ИТ-ресурсов в периоды пиковых нагрузок.

— Повышение уровня полезного использования дата центров.

— Снижение временных затрат на внедрение новых приложений.

— Сокращение затрат на ИТ, предотвращение расширения штата сотрудников.

КАНАЛЫ СВЯЗИ ДАТА ЦЕНТРОВ

Дата центр представляет собой специализированное строение, в котором размещается серверное и сетевое оборудование, выполняющая функции, связанные с обработкой, хранением и распространением информационных распределённых данных.

Стабильность и бесперебойность работы напрямую зависят от серверного оборудования и условий, в которых оно функционирует. При этом в частных облаках одним дата центром работы не останавливаются, ввиду необходимости дублирование дата центра в другом здании. Естественно одним из основных вопросов является вопрос канала связи для передачи данных. В подавляющем большинстве компьютерных сетей (особенно локальных) используется кабельные каналы связи, удовлетворяющие определенным стандартам. Стандарты определены для четерых типов кабеля: на основе неэкранированной витой пары, на основе экранированной витой пары, коаксиального и волоконно-оптического кабелей. Каждый тип кабеля имеет свои преимущества и недостатки, так что при выборе типа кабеля надо учитывать как особенности решаемой задачи, так и особенности конкретной сети, в том числе и используемую технологию.

В настоящее время волоконно-оптические линии связи прочно занимают свои позиции и интенсивно развиваются. Стремительными темпами идет замена кабелей с медными жилами

на волоконно-оптические кабели на всех участках сетей. На смену традиционным кабелям связи с медными жилами, приходят волоконно-оптические волноводы, в которых носителем информации являются электромагнитные волны инфракрасного диапазона. Передача информации по волоконно-оптическим кабелям осуществляется по принципу полного внутреннего отражения. Отражение достигается за счет защитного покрытия, накладываемого на оптическое волокно (сердцевину), на этой границе луч полностью отражается и распространяется по волноводу. В связи с ростом требований, предъявляемых к телекоммуникационным сетям, применение оптоволоконной технологии становится незаменимой.

Для того, чтобы спроектировать трассу прохождения волоконно-оптической линии связи и выбрать нужный тип кабеля, необходимо знать условия эксплуатации, конструкцию кабеля и его технические параметры. Спрос на компоненты волоконно-оптических линий связи постоянно увеличивается. Динамика роста наблюдается не только в сегменте магистральных сетей, которые строят операторы связи. Стабильное увеличение количества оптических инсталляций заметно и в сфере структурированных кабельных систем, что объясняется, в первую очередь, развитием информационных технологий. Уже сегодня закладывается основа для построения высокоскоростных оптических линий передачи с возможностью работы на скорости 10 Гбит/с. Востребованными становятся приложения, в которых осуществляется интеграция голоса, данных и видео, где также наилучшим решением является волоконная оптика.

В настоящее время имеется большое количество конструкций волокно-оптических кабелей, ориентированных на различные условия применения (прокладка внутри зданий, в телефонной канализации или в грунте, оптический кабель может быть проложен по опорам железных дорог, на линиях электропередачи, в канализационных и водопроводных трубах, по руслу рек и дну озер, вдоль автомобильных дорог, вместе с силовыми кабелями) [3].

Основной задачей в построении и обслуживании каналов связей является решения задачи отказоустойчивости работы распределенной системы.

ОСНОВНЫЕ ПОНЯТИЯ И МЕХАНИЗМЫ ОТКАЗОУСТОЙЧИВОСТИ В ЧАСТНОМ ОБЛАКЕ

Обеспечения отказоустойчивости в вычислительных системах (ВС) является залогом высокой надежности работы. Надежная ВС в состоянии готовности должна при любом обращении к ней обеспечивать пользователей адекватной информацией. Само же состояние готовности должно охватывать, возможно, больший процент времени. Процесс функционирования каждой системы можно рассматривать как последовательность переходов из одного состояния в другое. Возможны переходы, приводящие к ошибочным состояниям, при которых проявляется неисправность.

В последнее время в рамках общей проблемы надежности возникло новое направление — отказоустойчивость ВС. В связи с расширением потребности в отказоустойчивых ВС и значительным снижением стоимости электронных компонентов в ближайшем будущем ожидается, что подобные системы найдут широкое применение. Для обеспечения эффективного функционирования ВС необходима их полная устойчивость к небольшим отказам. При этом допускается некоторое уменьшение производительности ВС [4].

Введение свойства отказоустойчивости позволяет несколько иначе подойти к решению проблемы неисправностей, возложив на саму систему функции устранения их влияния и восстановления нормального функционирования. Можно сказать, что отказоустойчивость обеспечивает жизнеспособность ВС, так как ее задачей является возвращение из ошибочного состояния к регулярному состоянию системы, что обеспечивает возможность практически стопроцентного правильного функционирования.

Отказоустойчивость — одна из надежностных характеристик компьютерных систем, отражающая способность выполнять возложенные на систему функции (быть может, не в полной мере) при отказах аппаратных средств. При рассмотрении отказоустойчивости принимается, что основные характеристики надежности аппаратных средств заданы и рассматривают только негативные последствия сбоев и отказов аппаратных средств на функционирование системы и методы минимизации влияния этих последствий на выполнение основных функциональных задач. С этой точки зрения целесообразно было бы вместо термина «отказоустойчивость» применять термин «функциональная устойчивость системы к отказам». Это подчеркивало бы тот факт, что для полной характеристики системы недостаточно знать коэффициенты готовности отдельных компонент аппаратных средств, но необходимо учитывать, как деградируют функции компьютерной системы за время отказа этих компонент и как деградация отдельных функций влияет на основную функциональную задачу системы [5].

Свойством отказоустойчивости обладают многие технические системы, но компьютерные являются в данном случае наиболее характерными, так как они способны адаптироваться к изменяющимся условиям, т. е. перестраивать алгоритмы своего функционирования в широком

диапазоне. Среди компьютерных систем свойство отказоустойчивости в наибольшей степени присуще, во всяком случае, потенциально, распределенным системам, функционирующим на основе компьютерной сети. Мало того, можно утверждать, что полезное функционирование распределенных систем, не обладающей свойством отказоустойчивости (или обладающей этим свойством в малой степени), попросту невозможно.

Отказоустойчивое функционирование системы обеспечивается за счет введения разнообразных форм избыточности аппаратной, программной и временной, обеспечиваемой как на аппаратном, так и на программном уровнях. А всякая избыточность, как известно, повышает стоимость системы. При правильном проектировании систем необходимо стремиться минимизировать их стоимость и максимизировать эффективность.

Механизмы повышения отказоустойчивости разнообразны. Особенно сложной является задача разработки таких механизмов отказоустойчивости, которые позволяют сохранить целостность распределенной базы данных. В общем случае отказоустойчивость обеспечивается с помощью следующих механизмов:

— обнаружение отказа в системе;

— диагностирование отказавшего устройства;

— устранение влияния отказавшего устройства (реорганизация системы);

— восстановление нормального функционирования системы.

Все эти механизмы являются неотъемлемыми частями отказоустойчивой системы и могут реализоваться аппаратным, программным или смешанным программно-аппаратным способом [6].

Среди механизмов обеспечения отказоустойчивости системы обязательными являются механизмы восстановления, которые запускаются сигналами от алгоритмов обнаружения неисправностей и задачей которых является возврат системы к нормальному функционированию. Выбор методов восстановления ориентирован на отказы определенного типа, а поскольку они весьма разнообразны, то существует и много разных методов восстановления. Восстановление состоит из всех тех действий, которые осуществляются по получении сигнала неисправности. Сюда могут входить:

— исправление ошибки;

— обнаружение места неисправности;

— исключение или замена поврежденных деталей;

— регистрация предпринятых действий;

— запуск нормальной работы или выполнение безопасности остановки.

Невыполнение механизмом восстановления своих функций приводит к отказу системы.

ОПИСАНИЯ ПРОБЛЕМЫ

ИТ инфраструктура частного облака должна постоянно стабильно функционировать. Основным требованиям к работе ИТ инфраструктуры — это бесперебойная работа системы. К сожалению на практике добиться подобного эффекта очень сложно. Обычно вся ИТ инфраструктура, со всеми серверами и сетевым оборудованием располагается в одном дата центре и в одном физическом помещение одного здания. В случае пожара в здании и потери серверной вся ИТ инфраструктура теряется.

В частном облаке иметь инфраструктуру зависящую от одного здания нельзя. Необходимо серверную инфраструктуру продублировать в другом здании на достаточно удаленном расстоянии от первого здания.

В таких случаях дублирования серверной кроме финансовых затрат создает проблему, в виде определения события для переключения на запасной дата центр. При этом все сервисы должны автоматически подняться и работать на запасном дата центре. После активации запасного дата центра подключения других систем уже должны будут идти не к основному дата центру, а запасному. Простая проверка связи не достаточно для начала процесса активации запасного дата центра, ввиду того что кабель связи или провайдер канала связи может быть поврежден. Необходимо найти оптимальный способ определения события для автоматического переключения на запасной дата центр.

РЕШЕНИЯ ПРОБЛЕМЫ

Для решения выше описанной проблемы, в частном облаке предлагается определить кворум сервер. Слово кворум с перевода латинского означает — число участников собрания, необходимое для признания данного собрания правомочным принимать решения по вопросам его повестки дня. В нашем случаи необходимо как минимум добавить дополнительный один элемент для определения работоспособности основного сервера, с целью не допущения автоматического ошибочного запуска и перенастройки работы всей системы на запасной дата центр. Таким образом, в случаи потери связи с основным дата центром, запасной должен запросить статус также у кворум сервера, расположенного в

другом здании. В случаи если и кворум сервер также потерял связь с основным дата центром, но при этом имеет связь с запасным дата центром, происходит переключения на запасной дата центр.

АЛГОРИТМ РАБОТЫ ОТКАЗОУСТОЙЧИВОЙ ВОЛОКОННО-ОПТИЧЕСКОЙ ИНФОРМАЦИОННОЙ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ

Шаг 1. Все приложения подключаются к двум сетевым свитчам предоставляющий услуги связи от двух разных провайдеров связи.

Шаг 2. Основной дата центр при помощи двух волоконно-оптических кабелей соединяется с запасным дата центром. При этом волоконно-оптических кабели проложены по двум разным путям, с целью избежание механического воздействия и случайного события на одном из волоконно-оптических кабелей.

Шаг 3. Создается третий дополнительный кворум сервер в отдельном здании.

Шаг 4. Между основным дата центром и третьим кворум сервером двумя разными маршрутами прокладывается волоконно-оптических кабелей.

Шаг 5. Между запасным дата центром и третьим кворум сервером двумя разными маршрутами также прокладывается волоконно-оптический кабель.

Шаг 6. Между двумя дата центрами и третьим кворум сервером происходит постоянный обмен сетевыми пакетами.

Шаг 7. В случаи потери сетевых пакетов между запасным дата центром и основным дата центром, идет отправка запроса о статусе основного дата центра на третий кворум сервер.

Шаг 8. Кворум сервер отправляет сетевые пакеты на основной дата центр. Если кворум сервер не получает ответ от основного дата центра, то он дает команду запасному дата центру на автоматический запуск всех сервисов.

Шаг 9. Запасной дата центр получив команду на переключения запускает все сервисы и становится основным дата центром

Шаг 10. После восстановления работы основного дата центра, он превращается в запасной дата центр. И вся вышеописанная схема опять становится работоспособной вновь.

На рисунке 1 отображена схема соединения волоконно-оптическими кабелями два дата центра и один кворум сервер, где в качестве стрелок отображены волоконно-оптические кабеля

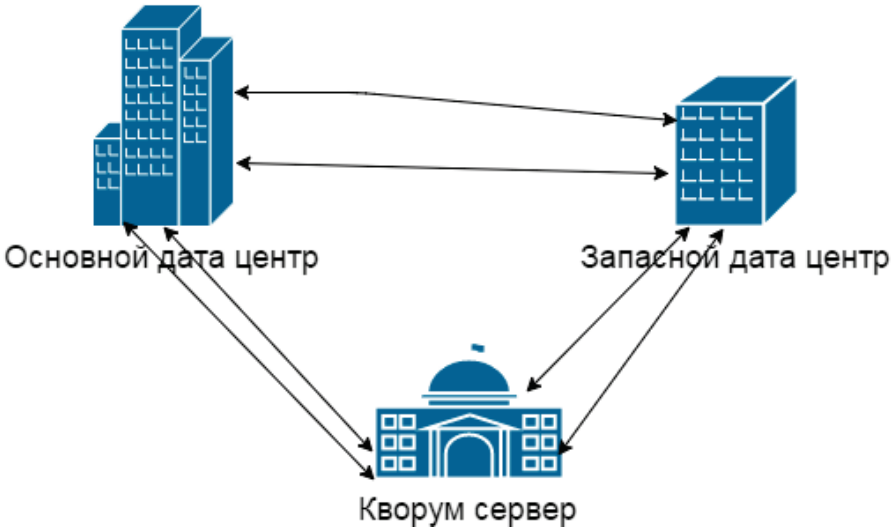

Рис. 1. Схема соединения волоконно-оптических кабелей

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА

Для практической реализации данного алгоритма создаем три виртуалыных сервера с операционной системой Linux.

```
# cat /proc/version
Linux version 2.6.32-20.el6.x86_64 (brewbuilder@ls20-bc2-13.build.redhat.com) (gcc version 4.4.5 20071124
(Red Hat 4.4.5-6)) #1 SMP Wed Nov 9 13:16:15 EDT 2011
```

Каждому из виртуальных серверов присваиваем разные IP адрресса из разных подсеток. Каждой отдельной подсетки соотвествует отдельное здание.
На сервере из основного дата центра установлен следующий IP адрес

```
# /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:17:9A:0A:F6:44
          inet addr:192.168.2.123  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::217:9aff:fe0a:f644/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:227614 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60421 errors:0 dropped:0 overruns:0 carrier:0
          collisions:272 txqueuelen:1000
          RX bytes:71110981505 (62.4 GiB)  TX bytes:42182095716 (27.5 GiB)
          Interrupt:17
```

На сервере из запасного дата центра установлен следующий IP адрес

```
# /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:17:9A:0A:F6:44
          inet addr:192.168.10.11  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::217:9aff:fe0a:f644/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:227614 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60421 errors:0 dropped:0 overruns:0 carrier:0
          collisions:272 txqueuelen:1000
          RX bytes:81110981505 (66.4 GiB)  TX bytes:42182095716 (29.5 GiB)
          Interrupt:19
```

На кворум сервере установлен следующий IP адрес

```
# /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:17:9A:0A:F6:44
          inet addr:192.168.100.61  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::217:9aff:fe0a:f644/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:227614 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60421 errors:0 dropped:0 overruns:0 carrier:0
          collisions:272 txqueuelen:1000
          RX bytes:69110981505 (63.7 GiB)  TX bytes:42182095716 (33.5 GiB)
          Interrupt:14
```

Проверка связи между серверами показывает, что связь стабильно работает

```
# ping 192.168.2.123
PING 192.168.2.123 56(84) bytes of data.
64 bytes from 192.168.2.123: icmp_seq=1 ttl=64 time=0.236 ms
64 bytes from 192.168.2.123: icmp_seq=2 ttl=64 time=0.235 ms
^C
--- 192.168.2.123 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.251/0.235/0.236/0.015 ms
```

На сервере основного дата центра установлена база данных Oracle версии 11.2.0.4. На сервере запасного дата центра также установлена база данных Oracle версии 11.2.0.4 только с настроенной технологией Oracle Data Guard, работающая в режиме active-passive, где в качестве Primary Database является база данных основного дата центра. Проверим работу Data Guard запускам SQL скрипта, для проверки зачитались ли присланные лог файлы с основного дата центра.

```
SQL> SELECT SEQUENCE#, FIRST_TIME, NEXT_TIME
  2>  FROM V$ARCHIVED_LOG ORDER BY SEQUENCE#;

 SEQUENCE# FIRST_TIME        NEXT_TIME
---------- ----------------- -----------------
         3 19-NOV-16 17:50:45 19-NOV-16 17:50:53
         4 19-NOV-16 17:50:53 19-NOV-16 17:50:58
         5 19-NOV-16 17:52:58 19-NOV-16 17:52:03
         6 19-NOV-16 17:53:03 19-NOV-16 18:01:11
```

Для проверки связи между запасным серверам и основным используется утилита базы данных Oracle tnsping. Где в качестве параметра указывается имя базы данных сервера из основного дата центра.

```
$ tnsping MAIN_SERVER
Ok (10 msec)
```

В случаи если основной сервер не ответит на tnsping, будет запущена сетевая утилита ping для проверки работы сети. В случаи отказа и от сетевой утилиты ping, то отправляется запрос на кворум сервер с помощью bash скрипта. Кворум сервер получив запрос начинает проверять сетевая утилитой ping работу способность основного сервера. В случаи не получения ответа, кворум отправляет запрос на переключения запасного сервера в основной сервер при помощи bash скрипта. Получив ответ о переключении, запасной сервер переводит standbay базу в режим активной базы данных, при помощи следующих Oracle команд

```
ALTER DATABASE COMMIT TO SWITCHOVER TO PRIMARY;
SHUTDOWN IMMEDIATE;
STARTUP;
```

РЕЗУЛЬТАТЫ ЭСКПЕРИМЕНТА

Для эксперимента, на сервере основного дата центра специально выключим сервер с базой данных Oracle. В результате всех проверок база данных должна из режима Standby перейти в режиме active на сервере запасного дата центра. Процесс работы отказоустойчивого алгоритма:

Процесс 1 (П1) Отключаем сервер основного дата центра. С этого момента пошел отсчет времени, сервер полностью отключится в течении 20 секунд

Процесс 2 (П2) Каждую минуту запускается проверка работы базы данных запасного дата центра и основного дата центра — 60 секунд

Процесс 3 (П3) Обнаружив потерю связи с базой данных, запускается проверка связи — 15 секунд

Процесс 4 (П4) Отправляется скрипт на кворум сервер для проверки связи между кворум сервером и основным сервером — 5 секунд

Процесс 5 (П5) Кворум сервер запускает проверку работоспособности сервера в течение одной минуты — 60 секунд

Процесс 6 (П6) Не получив ни одного успешного ответа в течении минуты отправляется команда на активацию сервера из запасного дата центра — 5 секунд

Процесс 7 (П7) Сервер из запасного дата центра получив команду, автоматически изменяет параметры базы данных и перезагружает базу данных — 120 секунд

В итоге проведенного выше эксперимента получаем, что за 285 секунд сервер из запасного дата центра активизируется, после падения сервера базы данных из основного дата центра. Результаты эксперимента приведены в таблице 1.

Таблица 1.

Результат работы отказоустойчивого алгоритма

Имя процесса	**Время (в секундах)**
Отключения основного сервера	20
Проверка работы Базы данных	60
Проверка связи	15
Отправка комманды на Кворум сервер	5

Продолжение табл.

Имя процесса	**Время (в секундах)**
Кворум запускает проверку	60
Кворум отправляет комманду на запасной	5
Активация StandBy базы данных	120

Ниже на рисунке 2 по оси X отображены процессы, а по оси Y отображено время в секундах выполнения процессов.

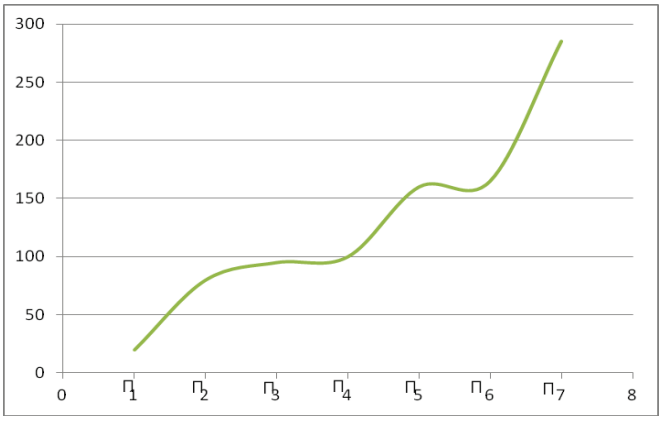

Рис. 2. График работы алгоритма отказоустойчивости

ВЫВОД

Таким образом, в результате проведенных исследований был разработан алгоритм отказоустойчивой работы оптоволоконной информационной распределенной системы в частном облаке. Как показали эксперименты в течении нескольких минут работа база данных Oracle активизируется автоматически без участия человека. При этом фактор ошибочной активации был убран за счет кворум сервера.

СПИСОК ЛИТЕРАТУРЫ

1. «Что такое Облачные вычисления (Cloud Computing)? », [Electronic resource]. — Available at: \www/URL:http://livebusiness.ru/tags/CLOUD_COMPUTINGhttp://tproger.ru/translations/adventures-in-android-user-notifications/
2. Mr. Ray J Rafaels «Cloud Computing: From Beginning to End», April 2015, 152 p.
3. Особенности и отличия волоконно-оптических кабелей LAPP [Electronic resource]. август 2007. — Available at: \www/URL: http://market.elec.ru/nomer/12/lapp/
4. M Evan Marcus, Hal Stern «Blueprints for High Availability», September 2003, 624 p.
5. Peter S. Weygant «Clusters for High Availability: A Primer of HP Solutions», May 2001, 336 p.
6. Floyd Piedad, Michael W. Hawkins «High Availability: Design, Techniques and Processes», December 2000, 288 p.

Надійшла до редакції 22.10.2016 р.

АЛИЕВ АЛЕКПЕР АЛИ АГА — д.т.н., профессор, заведующий кафедрой информационных технологий и программирования Бакинского Государственного Университета г. Баку, Азербайджан.

САМЕДОВ РАМИН БАХТИЯР — аспирант кафедры информационных технологий и программирования Бакинского Государственного Университета г. Баку, Азербайджан