DOI: 10.7242/1998-2097/2018.3.3
УДК 004.7; 004.4

АСПЕКТЫ НАДЕЖНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ*

Г.Ф. Масич, *Институт механики сплошных сред УрО РАН,*
Пермский национальный исследовательский политехнический университет (ПНИПУ)
С.Р. Латыпов, *Институт механики сплошных сред УрО РАН*
Д.П. Чугунов, *Институт механики сплошных сред УрО РАН*

Рассмотрен комплексный подход построения надежной корпоративной информационно - телекоммуникационной инфраструктуры, охватывающий приложения и сервисы, серверы и системы хранения, сети передачи данных и инженерное обеспечение. Показаны особенности использования гиперконвергентной технологии виртуализации для построения отказоустойчивых информационных систем.

Ключевые слова: *IT-инфраструктура, виртуализация, надежность, безотказность, готовность.*

Введение. Информационно-телекоммуникационная инфраструктура (ИТКИ) – это организационно-техническое объединение программных, вычислительных и телекоммуникационных средств и связей между ними, обеспечивающее предоставление информационных, вычислительных и сетевых сервисов. Компоненты корпоративной ИТКИ, как правило, территориально распределены в пространстве, находятся под одним системным администрированием, следуют единой политике управления и развития, в том числе используемых способов реализации надежного функционирования сервисов.

Надёжность компонент ИТКИ удерживается на высоком уровне с помощью надлежащего проектирования, тестирования, монтажа и комплексного обслуживания, включая поддержку всех необходимых обновлений программного обеспечения. Однако традиционные методы достижения требуемой надежности аппаратных средств недостаточны, поскольку технологии и физические законы ограничивают их надёжность. Только внедрение резервных элементов обеспечивает отказоустойчивость системы, которая обладает уникальным свойством: общая надёжность системы выше, чем надёжность её составных частей. Уместно привести справедливое высказывание профессора Hubert Kirrmann [4] из ABB Corporate Research и École Polytechnique Fédérale de Lausanne, Швейцария: «Типичный вопрос отказоустойчивости – это «Может ли надёжный мост быть построен из слабых балок?», и ответом техники на него является «В принципе да, если достаточное количество балок доступны, и они правильно скрепле-

* Работа выполнена в рамках государственного задания; номер государственной регистрации темы АААА-А16-116122310003-4

ны». Секрет отказоустойчивости в том, чтобы интегрировать эти избыточные балки так, чтобы повреждение одной не повлекло за собой крушение всего моста».

Эволюция IT-инфраструктур привела к расслоению систем на уровни управления и нескольких слоев абстрактных (виртуальных) ресурсов посредством технологий виртуализации. Развивающиеся технологии виртуализации позволили нам перейти к гиперконвергентному подходу построения информационных систем, в том числе к новым способам реализации надежной работы сервисов.

В статье приводятся используемые термины и понятия, сформулированные экспертами в стандартах органов стандартизации: Международная организация по стандартизации (ISO – International Organization for Standardization), Международный союз электросвязи (ITU – International Telecommunication Union), Международная электротехническая комиссия (IEC – International Electrotechnical Commission), ГОСТ 27.002-2015 (Надежность в технике (ССНТ) Термины и определения).

1. ОПРЕДЕЛЕНИЯ И ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1. Система и сервис

Трактовка понятия информационные технологии (IT) в документе ISO\IEC JTC1 №430, декабрь 1996: «*Информационные технологии* включают спецификацию, проектирование и разработку систем и средств, имеющих дело со сбором, представлением, обработкой, безопасностью, передачей, организацией, хранением и поиском информации, а также обменом и управлением информацией».

Понятие слова «система» и трактовка сопутствующих терминов «сервис» и «услуга» адекватно представлено Техническим Комитетом 97 ISO в стандарте 7498 в 1979 году. Этот стандарт определил базовую эталонную модель Взаимодействия Открытых Систем (basic reference model of Open Systems Interconnection – RM OSI) и является, по сути, структурированной коллекцией понятий и их взаимосвязей, описанных достаточно общими средствами.

Реальная Система (real system) в RM OSI – автономное целое, способное осуществлять обработку информации. Система состоит из одной либо нескольких ЭВМ с программным обеспечением, внешними устройствами, средствами передачи информации и персоналом операторов. Расположенный в системе прикладной процесс (application process) выполняет для нужд пользователей процесс обработки данных, другими словами, реализует некоторую функцию.

Прикладные объекты (application-entities), являющиеся частью прикладных процессов, обеспечивают взаимодействие прикладных процессов территориально распределенных реальных систем по соединениям (connections). В RM OSI функциональная возможность прикладного процесса называется ***«сервис» (service)***. В русскоязычных документах электросвязи используется понятие «служба», являющееся синонимом слова «сервис».

Услуга (facility) является частью сервиса. Например, сервис голосовой связи, соединяющий абонентов телефонной системы, может иметь услугу отображения номера вызывающего абонента, а сервис электронной почты иметь услугу подтверждения прочтения письма получателем. Словосочетание «реальная система» подчеркивает факт нахождения системы в состоянии предоставления сервисов, а не состояния системы в стадии проектирования или изготовления на предприятии. Далее вместо словосочетания «реальная система» будем использовать слово «система», поскольку речь будет идти о действующих и эксплуатируемых в ИТКИ системах.

Сервисами современных ИТКИ являются: доступ в интернет, электронная почта, доменная система имен, облачное

хранилище данных, передача файлов, Web-сайты, электронные библиотеки, поисковые системы и многие другие вычислительные, информационные и телекоммуникационные сервисы. Эти сервисы предоставляются реальными системами, взаимодействующими между собой по физическим средствам соединений.

Таким образом, согласно терминологии RM OSI, предоставляемые инфраструктурой (ИТКИ) сервисы зависят от надежной работы поддерживающих эти сервисы систем и соединений между ними, прокладываемым по физическим средам (оптика, медь, эфир).

1.2. Надежность

При использовании терминов «надежность», «отказоустойчивость» и «готовность» нужно быть аккуратными, так как их формальное определение несколько отличается от того значения, в котором мы их используем каждый день. Ситуация усугубляется тем, что английские названия этих терминов в статьях, обзорах в public internet и стандартах могут отличаться. А в англоязычном определении понятия надёжности произошёл переход от термина «reliability» к более широкому понятию «dependability» [3], используемому для общего (качественного) описания надежности сервисов, которые определяют, в нашем случае, функциональность ИТКИ. Далее будем следовать терминам и содержанию их понятий, определенных в стандарте «ГОСТ 27.002-2015 Надежность в технике (ССНТ). Термины и определения. Дата введения 2017-03-01» [1]. Стандартизованные термины приведены с указанием их англоязычных эквивалентов и номера статьи. В случае отсутствия в ГОСТе требуемых понятий и терминов будем использовать терминологию международных органов стандартизации IEC, ITU, ISO.

Как ранее было отмечено, ИТКИ предоставляет сервисы (service), работоспособность которых зависит от надежной работы большого числа входящих в инфраструктуру ***реальных систем*** в терминологии RM OSI или ***объектов*** в терминологии ГОСТ 27.002-2015, которую приведем и поясним далее.

Объект (item) {термин 3.1.1}: «Предмет рассмотрения, на который распространяется терминология по надежности в технике. Может включать в себя аппаратные средства, программное обеспечение, персонал или их комбинации». ***Элемент (element)*** {термин 3.1.2}: «Объект, для которого в рамках данного рассмотрения не выделяются составные части». То есть мы будем говорить об «элементе», когда будем рассматривать часть системы, которую мы не хотим далее детализировать, хотя она может состоять из подэлементов. ***Система (system)*** {термин 3.1.3}: «Объект, представляющий собой множество взаимосвязанных элементов, рассматриваемых как единое целое и отделенных от окружающей среды». ***Подсистема (subsystem)*** {термин 3.1.4}: «Часть системы, которая представляет собой систему».

Таким образом, согласно терминологии по надежности в технике, предоставляемые инфраструктурой (ИТКИ) сервисы зависят от надежной работы входящих в эту инфраструктуру объектов. Объектами ИТКИ являются информационные, вычислительные и телекоммуникационные системы, которые в современных ИТКИ размещаются Центрах Обработки Данных (ЦОД), оснащенных системами бесперебойного электропитания и системами кондиционирования воздуха. Примерами элементов перечисленных систем являются сервер, вычислительный кластер, коммутатор, маршрутизатор, кондиционер, источник бесперебойного питания, кабельная система, каналы связи, линии связи и другое программно-техническое оборудование.

Надежность (dependability) {термин 3.1.5}: «Свойство объекта сохранять во времени способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирова-

ния». «Во времени» в этом понятии означает естественный ход времени, в течение которого объект предоставляет сервис, а не какой-либо конкретный интервал времени. Надежность является комплексным свойством, которое в зависимости от назначения объекта и условий его применения может включать в себя «безотказность (reliability), ремонтопригодность (maintainability), восстанавливаемость (recoverability), долговечность (durability), сохраняемость (storability), готовность (availability) или определенные сочетания этих свойств». Комплексным показателем надежности является коэффициент готовности (availability factor) {термин 3.6.6.1}: «Вероятность того, что объект окажется в работоспособном состоянии в данный момент времени». Определение понятия термина надежность (dependability) в документах IEC аналогично. Таким образом, свойство объекта «надежность» может относиться к элементу, конкретному объекту, системе и подсистеме.

Безотказность (reliability) {термин 3.1.6}: «Свойство объекта непрерывно сохранять способность выполнять требуемые функции в течение некоторого времени или наработки в заданных режимах и условиях применения». Безотказность объекта по определению IEC – это «вероятность того, что объект обеспечит требуемый сервис при заданных условиях в течение указанного периода времени». Безотказность, как правило, зависит от времени нахождения объекта в рабочем состоянии, а вероятность обеспечения требуемого сервиса уменьшается со временем. Для практических целей предпочитают выражать её одним числом, например, «вероятность безотказной работы» (reliability <measure>, reliability function) {термин 3.6.2.1} или «средняя наработка до отказа» (mean operating time to failure) {термин 3.6.2.2}.

Готовность (availability) {термин 3.1.11}: «Свойство объекта, заключающееся в его способности находиться в состоянии, в котором он может выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания и ремонта в предположении, что все необходимые внешние ресурсы обеспечены. Примечание: готовность зависит от свойств безотказности, ремонтопригодности и восстанавливаемости объекта». Синонимом слова «готовность» является слово «доступность», часто используемое в русскоязычной литературе. Готовность часто выражается в процентах или как отношение времени работы к времени простоя. Пример: доступность телефонной станции должна быть равна 99,9994%, то есть 3 минуты простоя в год.

Все три свойства объекта: надежность (dependability), безотказность (reliability) и готовность (availability) фиксируют «рабочее состояние» (operating state) {параметр 3.2.5} объекта: «Состояние объекта, в котором он выполняет какую-либо требуемую функцию». И неочевидно их различие и особенности. Однако, как следует из определений ГОСТ 27.002-2015, понятие «надежность» (dependability) является обобщенным, качественным понятием, в состав которого входят свойства объектов безотказность (reliability) и готовность (availability), поддающиеся количественной оценке этих свойств. А принципиальная разница между безотказностью и готовностью объекта убедительно проиллюстрирована в работе Hubert Kirrmann [4], жизненные циклы которых изображены на рис. 1.

Когда в reliability объекте происходит событие отказ (failure) {термин 3.4.1}, объект выбрасывают. Безотказность сама по себе не учитывает никаких ремонтных действий, которые могут иметь место, а фиксирует время «наработки до отказа» ((operating) time to failure) {термин 3.3.2}. В течение этого времени объект, находящийся в «рабочем состоянии» (operating state) {термин 3.2.5}, может перейти в «нерабочее состояние» (non-operating state) {термин 3.3.6} с некоторой «вероятностью безотказной работы» (reliability function) {термин 3.3.2}. Безотказность не отражает интервала времени, требуемого для возвраще-

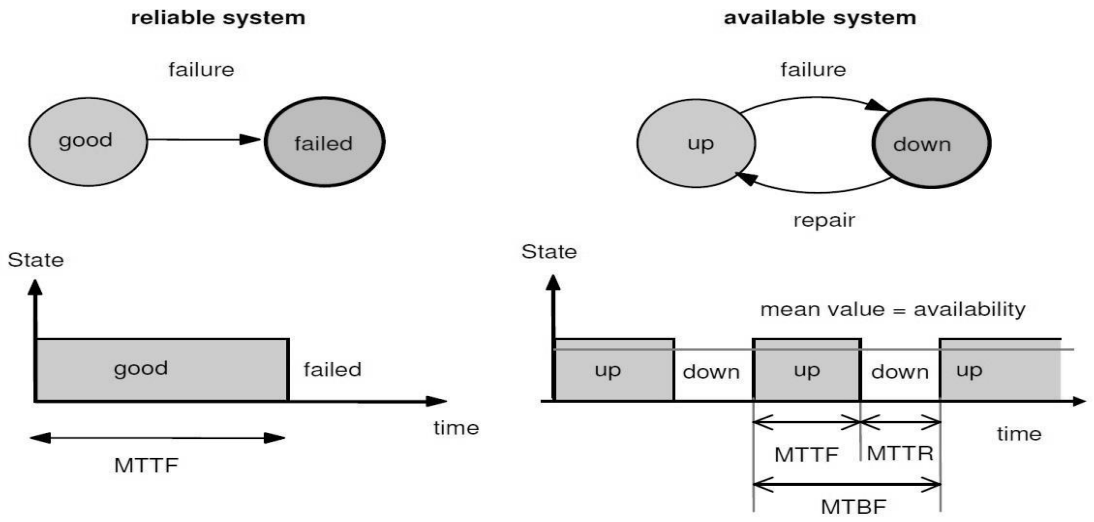

Рис. 1. Безотказность (reliability) и готовность (availability)

ния объекта в рабочее состояние.

Когда в available объекте происходит событие отказ, объект может быть отремонтирован или возвращен в строй после сбоя. У available объекта время службы колеблется между работоспособным состоянием (up state) {термин 3.2.3} и неработоспособным состоянием (down state) {термин 3.2.4}.

На рис. 1 показаны следующие временные параметры: среднее время безотказной работы MTTF (Mean Time To Failure) {термин 3.6.2.2}, средний интервал между двумя последовательными отказами MTBF (Mean Time Between Failures) {термин 3.6.2.4} и среднее время ремонта MTTR (Mean Time To Repair). Эти времена соотносятся, соответственно, с терминами ГОСТа наработка до отказа (time to failure) {термин 3.3.2}, наработка между отказами (time between failures) {термин 3.3.3}, время ремонта (repair time) {термин 3.3.8}.

Available объект описывается «показателями ремонтопригодности и восстанавливаемости» раздел 3.6.3 ГОСТ 27.002-2015, например, «среднее время восстановления» (mean restoration time) {термин 3.6.3.2}.

В принципе, продолжительность неисправного состояния в available системе не ограничена, в то время как превышение длительности сбоя в reliability системе приводит к отказу. Это различие становится важным в отказоустойчивых системах, которые требуют определенного времени на восстановление самих себя и, следовательно, приводят к отказам ограниченной длительности. Если отказ не может быть обработан в пределах допустимой в спецификации максимальной продолжительности сбоя, возникает неисправность.

1.3. Отказоустойчивость

«Отказоустойчивость» (fault-tolerance) есть свойство объекта сохранять свою работоспособность после отказа одного или нескольких элементов в объекте. В ГОСТе, в большей степени, этому понятию соответствует понятие ***«Восстанавливаемость (recoverability)*** {термин 3.1.8}: свойство объекта, заключающееся в его способности восстанавливаться после отказа без ремонта».

Отказоустойчивость сервисов, предоставляемая инфраструктурой (ИТКИ), заключается в способности инфраструктуры обеспечивать бесперебойное предоставление сервисов, несмотря на то, что один или несколько компонентов инфраструктуры (сервер, хранилище, канал или линия связи, система электропитания и охлаждения) не работают. Цель состоит в том, чтобы предотвратить катастрофиче-

ский сбой, который может возникнуть из-за единственной точки отказа.

Для более тонкого учета свойства ИТКИ (системы), а именно потери только части своей функциональности при каждом отказе, без полной потери работоспособности, вводится понятие ***постепенная / изящная деградация (Graceful Degradation)***. Этому понятию соответствует термин ГОСТа ***«Повреждение (degraded state)*** {3.4.3}: событие, заключающееся в нарушении исправного состояния объекта при сохранении работоспособного состояния». Graceful Degradation предполагает на этапе проектирования спецификации классов обслуживания и соответствующих им классов производительности. *Например, агрегация 4 портов коммутатора по 1 Гбит/с обеспечивает проектную суммарную скорость передачи данных 4 Гбит/с. При выходе из строя (или неконтактах в соединительных разъемах) одного или нескольких портов общая пропускная способность будет функцией от числа исправных агрегированных портов коммутатора.*

В некоторых случаях Graceful Degradation используется для перевода системы в безопасное состояние (safety / safe state). Классический пример – использование источников бесперебойного электропитания (ИБП) серверного или суперкомпьютерного оборудования. В случае отключения первичного электропитания временной ресурс аккумуляторных батарей ИБП должен быть достаточен для корректного отключения дорогостоящего суперкомпьютерного или иного оборудования.

Касательно аппаратной части требуемый уровень достигается резервированием (redundancy) {термин 3.2.4} элементов, входящих в состав аппаратуры. Например, помимо ставшего уже стандартом де-факто резервирования блоков питания, вентиляторов и жестких дисков (RAID) на критически важных направлениях уже используются серверы и коммутационное оборудование, позволяющие резервировать системные платы и супервизорные модули, оперативную память и центральные процессоры. В случае аппаратного сбоя система автоматически исключает неисправный элемент, не нарушая при этом работоспособности объекта в целом.

Аналогичный подход используется и для обеспечения отказоустойчивости программной составляющей информационных сервисов, изображенный на рис. 2. В этом случае для защищаемого (primary) инфор-

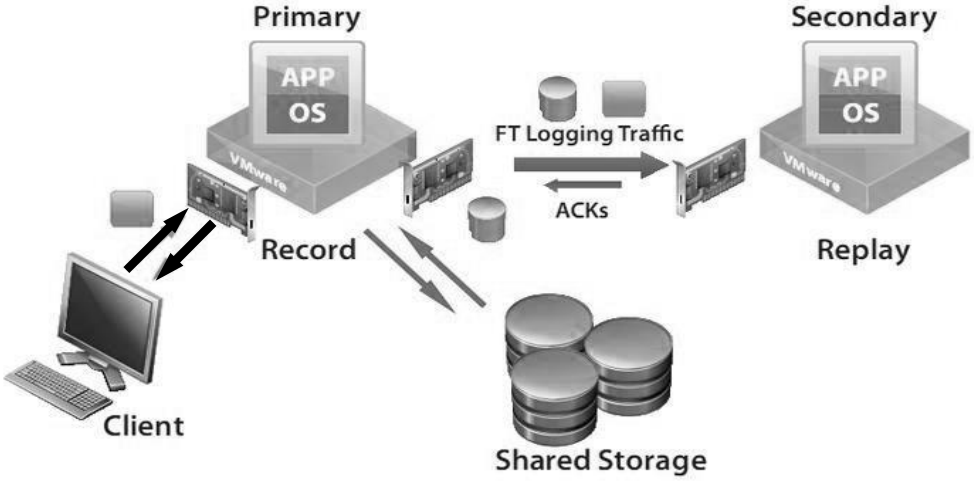

Рис. 2. Механизм обеспечения отказоустойчивости[1]

[1] Сравнение производительности отказоустойчивости и использование накладных расходов VMmark v1.1.1 Режим доступа: https://blogs.vmware.com/performance/2009/08/comparing-fault-tolerance-performance-overhead-utilizing-vmmark-v111.html (дата обращения: 01.06.2018 г.)

мационного сервиса создается его полная резервная копия (secondary). Идея состоит в том, что копия постоянно актуализируется (logging traffic) и в любой произвольный момент времени полностью соответствует защищаемому сервису. Состояние (работоспособность) основного сервиса непрерывно отслеживается, и в случае возникновения сбоя или отказа все клиентские запросы незамедлительно перенаправляются на копию. Основной сервис программно выключается, резервный сервис становится основным, и для него создается новая резервная копия. Основным местом хранения всех необходимых данных (ОС, приложения, пользовательские данные) является хранилище (shared storage), доступное как защищаемому (primary) сервису, так и его копии (secondary).

Такой подход называется ***аварийное восстановление (DR – disaster recovery)***. Для достижения большей эффективности следует помещать основной сервис и его копию в разные ***домены отказа (fault domain)***. Под доменом отказа понимается группа серверов, с некоторой степенью вероятности подверженная одновременному отказу. Чаще всего это серверы и оборудование, расположенные в пределах одного Центра обработки данных (ЦОД). В этом случае, например при продолжительном отключении электроснабжения или обрыве связи, будет зафиксирован отказ сразу всего оборудования. Распределение сервисов по разным доменам отказа (разным ЦОД) выручает практически в любой ситуации, включая стихийные бедствия (наводнение) и антропогенные катастрофы (сбой инфраструктуры, терроризм).

Расстояние между ЦОД является основным соображением для организации DR-подхода. Небольшое расстояние позволяет упростить синхронизацию, а большие расстояния могут создавать проблемы репликации. Однако ЦОДы должны быть подключены к разным энергосистемам и расположены достаточно далеко друг от друга, чтобы серьезная катастрофа не повлияла на оба места их размещения.

1.4. Высокая готовность системы

Высокая готовность (high availability – HA) сервисов в информационных технологиях, которые постоянно работают в течение желаемого длительного периода времени, является свойством системы минимизировать время простоя. Измеряется относительно 100% готовности, при которой отсутствуют перерывы доступа к сервисам. Трудно реализуемый уровень высокой готовности известен экспертам как «пять девяток» (99,999 %).

Поскольку компьютерная система или сеть состоит из многих частей, присутствие которых обеспечивает ее рабочее состояние, планирование высокой готовности сосредотачивается на обработке резервных копий и восстановлении после сбоев, а также на хранении и доступе к данным.

В отличие от отказоустойчивых систем системы высокой готовности допускают некоторый простой (отказ в обслуживании) в случае сбоя. Время простоя есть сумма времени обнаружения сбоя и времени запуска нового экземпляра сервиса из резервной копии. На рис. 3 показан механизм восстановления готовности сервисов после выхода из строя одного из серверов. В качестве примера рассмотрен кластер высокой готовности (High Availability Cluster, HA Cluster), построенный на платформе VMware. В случае аппаратного отказа любого из серверов кластеру требуется некоторое время на его диагностику и, если за отведенное время не удалось установить связь с сервером, принимается решение о принудительной миграции всех виртуальных машин (VM) с неисправного сервера на рабочие. Необходимо отметить, что, как и в случае с отказоустойчивыми системами, все данные, необходимые для корректной работы сервиса, должны находиться в хранилище, доступном всем узлам кластера. Таким образом, в случае выхода из строя одного из серверов время простоя сервисов будет скла-

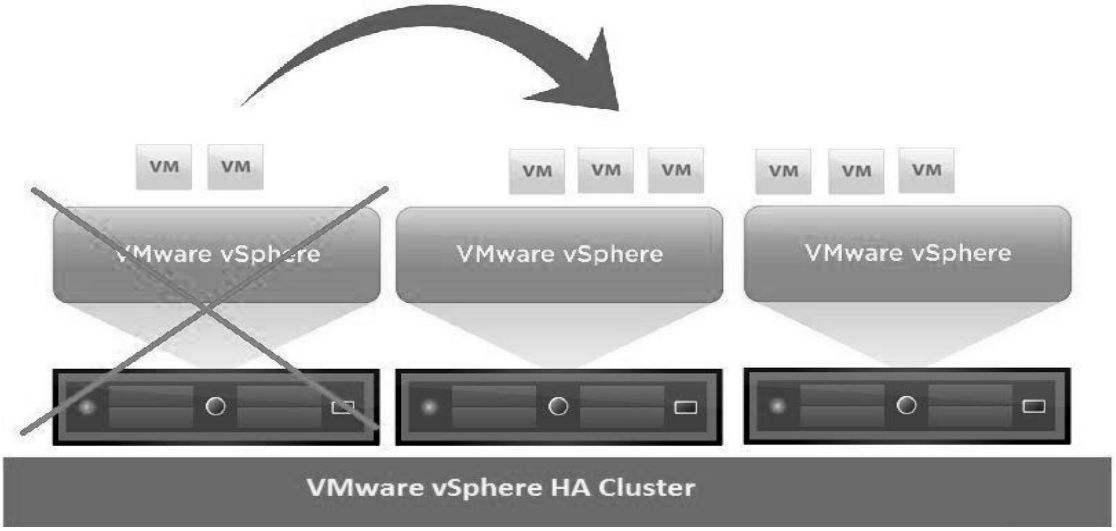

Рис. 3. Механизм обеспечения высокой готовности[2]

дываться из двух составляющих: времени, необходимого для диагностирования сбоя и времени, необходимого для запуска сервиса на другом узле кластера.

В системах высокой готовности одновременно существует только один экземпляр сервиса. При этом все данные, необходимые для перезапуска сервиса, должны храниться отдельно и быть доступными сразу для нескольких серверов. В этом случае при отказе одного из серверов сервис может быть запущен на любом другом, оставшемся доступным.

1.5. Виртуализация и надежность

Важное влияние на методы построения надежных информационных систем оказывают развивающиеся технологии виртуализации. Таковыми являются гипервизорная и контейнерная виртуализация в серверном / вычислительном оборудовании, программно определяемые сети и сетевые функции виртуализации в сетевом оборудовании.

В начале своего пути, *в классических системах*, серверная виртуализация применялась для эффективного использования физических серверов для экономии финансовых средств, а задача отказоустойчивости сервисов решалась разработчиками и администраторами сервисов. *Так, например, требование отказоустойчивого функционирования кровеносной для интернет-доменной системы имен (DNS) в корпоративной сети требует инсталляции первичного и вторичного DNS серверов. Таймерные механизмы DNS протокола регламентируют обработку DNS запросов. А, например, высокая готовность (доступность, малое время ответа) 13 корневых серверов DNS в мире достигается их клонированием до нескольких сотен посредством ANYcast технологии / адресации.* Проприетарно решались задачи надежного функционирования и других критически важных для предприятий сервисов. Все это требовало квалифицированного администрирования ИТКИ многими специалистами, приводя к значительным финансовым затратам.

В связи с нарастающим объемом обрабатываемых данных выросла роль систем хранения данных (СХД), которые подключались к серверному оборудованию посредством разных технологий и стандартизированных протоколов. *Конвергентный подход* к построению платформы виртуализации высокой готовности (High Availability) предполагает использование не менее двух СХД с

[2] Что такое VMware vSphere HA? Режим доступа: http://masteringvmware.com/what-is-vmware-vsphere-ha/ (дата обращения: 01.06.2018 г.)

настроенной репликацией для хранения образов виртуальных машин (VM). Подключение СХД к вычислительным ресурсам платформы (серверам) также должно быть задублировано. Типовая схема конвергентного подхода изображена на рис. 4.

Гиперконвергентный подход позволяет отказаться от использования классических СХД, переложив нагрузку на накопители, установленные непосредственно в серверах. В гиперконвергентной инфраструктуре компоненты виртуализации и программно определяемого хранилища работают совместно на одних и тех же серверах, позволяя эффективно использовать как вычислительные ресурсы, так и распределенные по разным машинам диски. Появились облегчающие администрирование средства централизованного управления виртуальной средой (конфигурирование, мониторинг, отчетность).

Нами выбрано VMware гиперконвергентное программное решение [5], в котором вычислительные и сетевые ресурсы предоставляются с помощью аппаратного гипервизора ESXi, разделяющего физические серверы на несколько логических серверов, которые называются виртуальными машинами (VM – Virtual Machine). Используется VMware Virtual SAN (vSAN) – технология виртуализации ресурсов хранения, которая объединяет прямо подключенные к серверам диски и флэш-накопители в общее распределенное хранилище данных для организации гиперконвергентной инфраструктуры на базе vSphere.

vSAN встроен в гипервизор ESXi и не требует развертывания дополнительных сервисов и служебных VM. vSAN позволяет объединить локальные носители хостов в единый пул хранения, обеспечивающий заданный уровень отказоустойчивости и предоставляющий свое пространство для всех хостов и виртуальных машин кластера. Типовая схема виртуальной инфраструктуры с использованием гиперконвергентного подхода и технологии vSAN, приведена на рис. 5.

vSAN представляет собой объектное хранилище, данные в котором хранятся в виде объектов, или «гибких контейнеров» (flexible containers), распределенных по всему кластеру. Управление хранением осуществляется с помощью политик Storage Policy Based Management. При распределении объектов по кластеру vSAN контролирует корректное распределение компонентов по разным узлам или доменам отказа (fault domain).

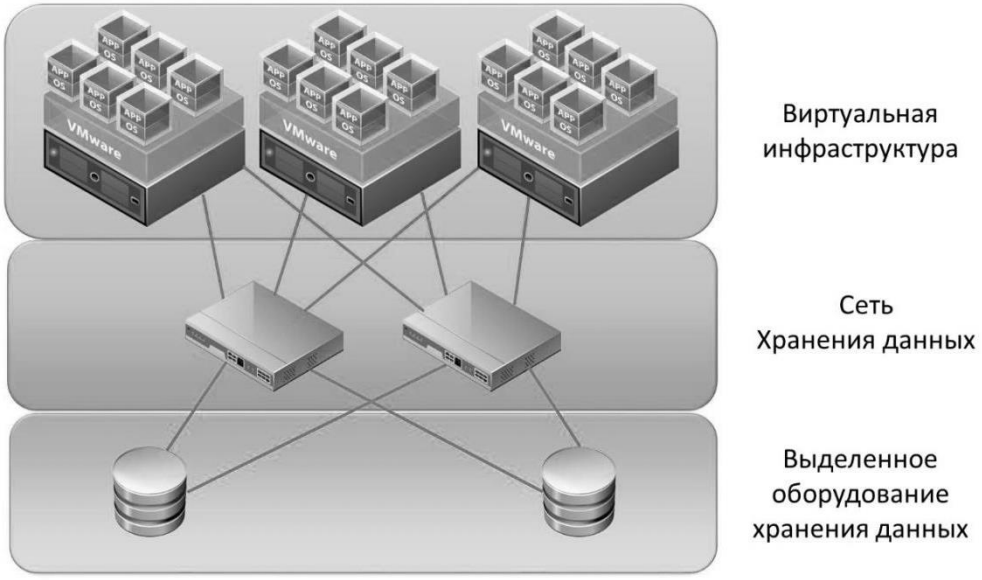

Рис. 4. Виртуальная инфраструктура с традиционной СХД

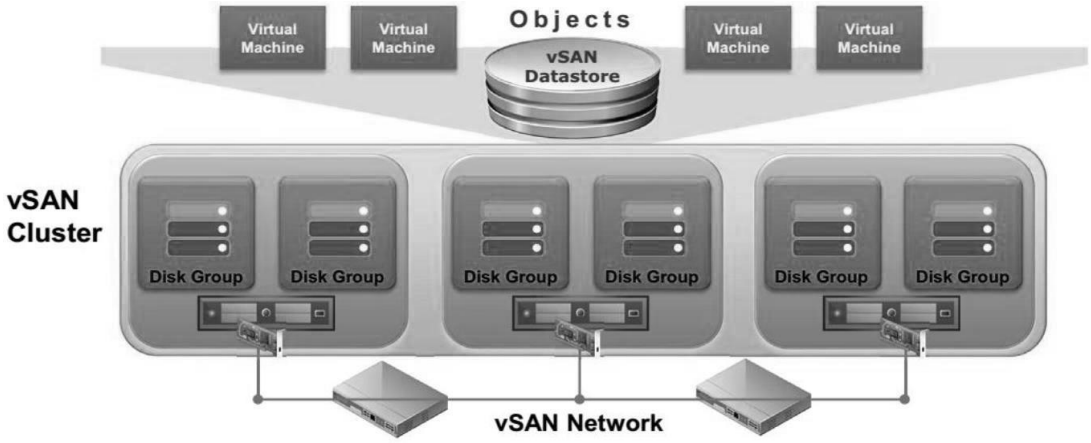

Рис. 5. Виртуальная инфраструктура, использующая технологию vSAN

Существенными атрибутами политик виртуальных машин и виртуальных дисков являются количество дисков на каждый объект и механизмы резервирования пространства объектов. Ключевым является параметр количества отказов для достижения требуемой отказоустойчивости (Failures to Tolerate – FTT). Требуемая отказоустойчивость обеспечивается за счет сохранения нескольких копий данных для уменьшения риска отказа хостов, приводящих к потере связи с данными или потенциальной потере данных. Политика FTT работает в сочетании с VMware vSphere High Availability для обеспечения высокой готовности, т.е. «почти» непрерывной работы сервисов. В базовой конфигурации политика FTT=1 обеспечивает создание одной копии.

Далее описаны разработанные архитектурные решения, используемые для построения надежной информационно-телекоммуникационной инфраструктуры Пермского федерального исследовательского центра (ПФИЦ) УрО РАН.

2. ИТКИ ПФИЦ

2.1. География и физические средства соединения

Размещение оборудования в одном месте приводит к проблеме «одиночной точки отказа». Поэтому, как показано на рис. 6, в корпоративной инфраструктуре ПФИЦ сформированы две площадки, названные ЦОД ИМСС УрО РАН и ЦОД ПНЦ УрО РАН. Между собой площадки связаны по двум разным трассам волоконно-оптической линии связи (ВОЛС). Протяженность оптической линии составляет 23 км. Доступ к ресурсам суперкомпьютерного центра ИММ УрО РАН в Екатеринбурге (ЦОД ИММ УрО РАН) выполнен по двум волокнам магистральных операторов связи. Другие институты ПФИЦ УрО РАН (ГИ, ИЭГМ, ИТХ) подключены по оптическим линиям к ЦОДам согласно рис. 6.

2.2. Инженерное обеспечение

Резервирование инженерных систем является обязательной составляющей обеспечения отказоустойчивости сервисов.

Охлаждение. Система охлаждения (кондиционирования) воздуха на площадке ПНЦ представлена двумя прецизионными кондиционерами Uniflair Leonardo с выносными конденсаторами воздушного охлаждения. Суммарная холодопроизводительность составляет 2×25=50 кВт. При этом общее тепловыделение оборудования не превышает 10 кВт. Таким образом, каждый из используемых кондиционеров имеет примерно 50%-ный резерв по мощности, а вся система охлаждения имеет резервирование по схеме 2N. Система охлаждения (кондиционирования) воздуха на пло-

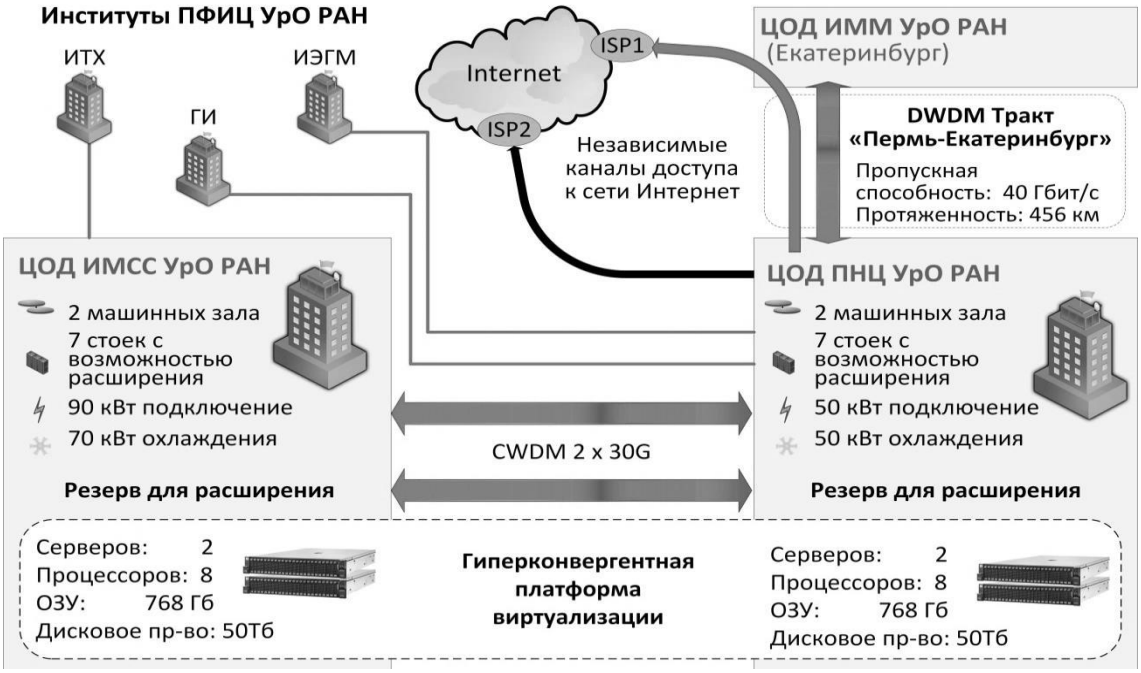

Рис. 6. Структура ИТКИ ПФИЦ УрО РАН

щадке ИМСС представлена пятью кондиционерами Mitsubishi PU-P140YHA с выносными конденсаторами воздушного охлаждения. Суммарная холодопроизводительность составляет 5×14=70 кВт. При этом общее тепловыделение оборудования сильно зависит от загрузки суперкомпьютера, но не превышает 30 кВт. Таким образом, система охлаждения имеет резервирование по схеме N+2.

Электропитание. Для обеспечения бесперебойного электроснабжения серверных помещений ЦОД используются источники бесперебойного питания (ИБП) APC Symmetra LX 16 kVA и APC SmartArray 16 kVA. Оба типа ИБП комплектуются несколькими модулями электропитания, каждый из которых увеличивает нагрузочную способность ИБП на 4kVA. Количество модулей в каждом ИБП подобрано таким образом, чтобы запас по мощности был более 4 kVA (один «запасной» модуль), что позволяет обеспечить резервирование по схеме не ниже N+1.

2.3. Сеть

Оптическая сеть создана [2] и развивается для объединения по оптическому волокну институтов ПФИЦ УрО РАН. Для надежного соединения в Перми площадок расположения ЦОД ИМСС и ЦОД ПНЦ между площадками проложены две трассы ВОЛС, на которых развернуты две системы разряженного спектрального уплотнения каналов (CWDM) по 30Гбит/с для предоставления гарантированных каналов связи для нужд конкретных проектов и инициатив.

Соединения ресурсов суперкомпьютерного центра ИММ УрО РАН в Екатеринбурге (ЦОД ИММ УрО РАН) с ресурсами ПФИЦ УрО РАН в Перми реализовано по каналам связи системы плотного волнового мультиплексирования (DWDM) на скорости 4×10 Гбит/с. Скоростные и протяженные каналы связи DWDM тракта «Пермь-Екатеринбург» используются как для исследования протоколов передачи данных, так и для построения распределенных в пространстве вычислительных систем и систем хранения.

Public Internet. Надежность доступа в Интернет достигается подключением к двум интернет-сервис провайдерам (ISP) по двум независимым линиям связи. Как показано на рис. 6, основное подключение к ISP1 в Екатеринбурге выполнено по

каналу связи DWDM тракта «Пермь-Екатеринбург». Второе подключение реализовано по оптике к ISP2 в Перми.

Высокая готовность (high availability) сервиса доступа в Интернет обеспечена использованием провайдеро-независимого (Provider Independent, PI) блока IPv4-адресов и номера автономной системы (AS). Это позволяет без переадресации конечных систем подключаться к нескольким ISP, реализовывать балансировку нагрузки и управлять политиками маршрутизации IP-трафика.

2.4. Серверное оборудование

До внедрения гиперконвергентной платформы для размещения всех информационных сервисов использовались сервера HP со следующими характеристиками: CPU 2×Intel® Xeon® CPU E5-2660, объём ОЗУ 128 Гб, жёсткие диски: 6×900 Гб.

Для обеспечения бесперебойности работы серверного оборудования было произведено резервирование компонентов, наиболее часто подверженных отказам, – блоков питания, сетевых интерфейсов.

Само количество серверов и их характеристики были подобраны таким образом, чтобы обеспечить не менее чем 2-кратный резерв по всем основным характеристикам – производительности процессоров, объёму оперативной памяти, объёму жестких дисков. Такое решение позволяло обеспечить работу всех информационных сервисов при отказе отдельных компонентов сервера, сервера целиком и даже одного ЦОД путем ручного администрирования процесса восстановления работоспособности.

3. АРХИТЕКТУРА ГИПЕРКОНВЕРГЕНТНОЙ СИСТЕМЫ ПФИЦ

В качестве аппаратной платформы гиперконвергентной системы ПФИЦ используются сервера модели PRIMERGY RX2540 M4 производства компании Fujitsu. Двухпроцессорный стоечный сервер высотой 2U построен на процессорах Intel® Xeon® Silver 4114 (семейство Skylake Scalable Processors), поддерживающих усовершенствованные технологии аппаратной поддержки виртуализации приложений с интенсивным использованием памяти. Объём оперативной памяти на каждом сервере составляет 384 Гб, объём дискового пространства – 24,1 Тб. Модульная конструкция обеспечивает расширяемость – до 28 дисковых накопителей, до 8 разъемов расширения PCIe Gen 3, а также, благодаря двум блокам питания с возможностью горячей замены, лучшую в своем классе энергоэффективность – до 96%. Серверы, участвующие в построении платформы, установлены на двух территориально удалённых площадках и соединены скоростными каналами связи. Архитектура платформы приведена на рис. 7.

В качестве программного обеспечения гиперконвергентной платформы виртуализации используется VMware vSphere 6.5 и vSAN 6.6. Управляется виртуальная среда посредством vCenter Server. Для резервного копирования и восстановления данных виртуальной инфраструктуры установлено Veeam Backup & Replication 9.5.

Существенной компонентой виртуальной инфраструктуры vSphere является распределенный виртуальный коммутатор vNetwork Distributed vSwitch (vDS), поддерживающий конфигурации на уровне L3 и конфигурации с Jumbo Frames. Централизованное управление с консоли vCenter Server делает настройку сети VMware vSphere быстрой и удобной.

3.1. Обеспечение высокой готовности сервисов

vSAN использует понятие доменов отказа (fault domain) для защиты кластера от отказов на уровне серверных стоек или корзин, которые логически группи-

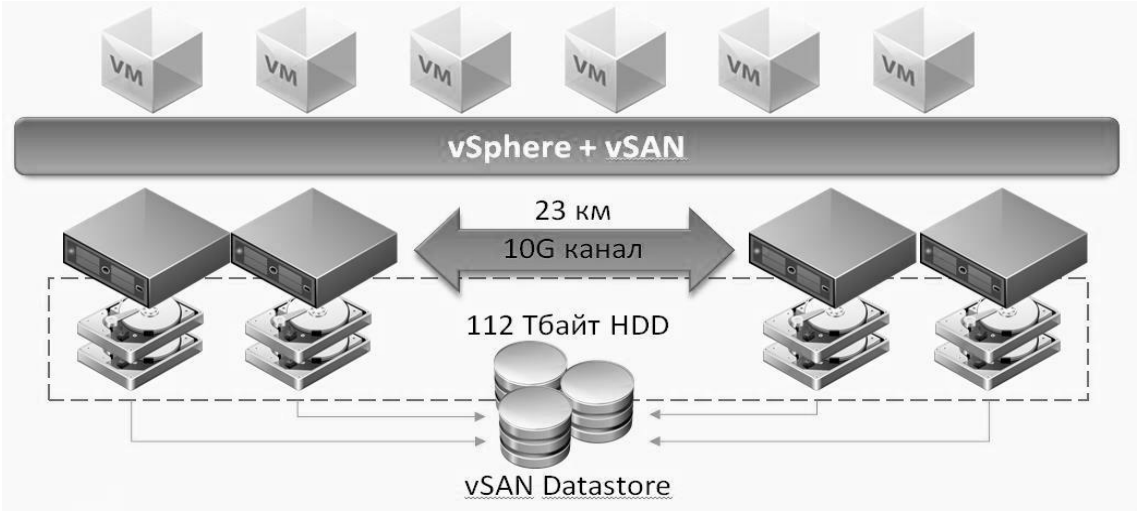

Рис. 7. Архитектура гиперконвергентной системы

руются в эти домены. Включение этого механизма приводит к распределению данных для обеспечения их отказоустойчивости не на уровне отдельных узлов, а на уровне доменов, что позволит пережить отказ целого домена – всех сгруппированных в нем узлов (например серверной стойки или ЦОДа), поскольку реплики объектов будут обязательно размещаться на узлах из разных доменов отказа.

Для обеспечения требований отказоустойчивости решения на уровне ЦОД установлено по 2 хост-сервера хранения в ЦОДах на площадке ИМСС и на площадке ПНЦ (рис. 7, 8). Хост-серверы каждой площадки будут принадлежать своему домену отказа, что позволит принудительно распределять разные копии одного объекта хранения по хост-серверам, принадлежащим разным доменам отказа. При отказе одной площадки целиком вторая площадка должна обладать резервом вычислительных ресурсов, достаточным для обеспечения работоспособности виртуальных машин отказавшей площадки.

3.2. Механизм обеспечения кворума

Свидетель (witness) – это служебный компонент, не содержащий полезных данных (только метаданные), его размер равен 2–4 Мб. Он выполняет роль тай-брейкера (tie-breaker) при определении живых компонентов объекта хранения в случае отказов.

Механизм вычисления кворума в vSAN работает следующим образом. Каждый компонент объекта получает определенное число голосов (1 и более). Кворум достигается, и объект считается «живым» если мы имеем полную реплику данных либо доступно более половины (50%) компонентов объекта или его голосов.

Наш проект имеет два домена отказа с одинаковым количеством серверов в каждом. Для выполнения требования доступности более половины компонентов объекта хранения на основной площадке разворачивается хост-сервер-свидетель, на котором хранятся метаданные объектов хранения. В случае отключения хост-серверов одного домена отказа, за счет метаданных хранящихся на хост-сервере свидетеле, основная площадка получает более половины голосов. Это является основанием для того, чтобы система управления кластером приняла решение для переноса сервисов с отказавшей площадки на уцелевшую.

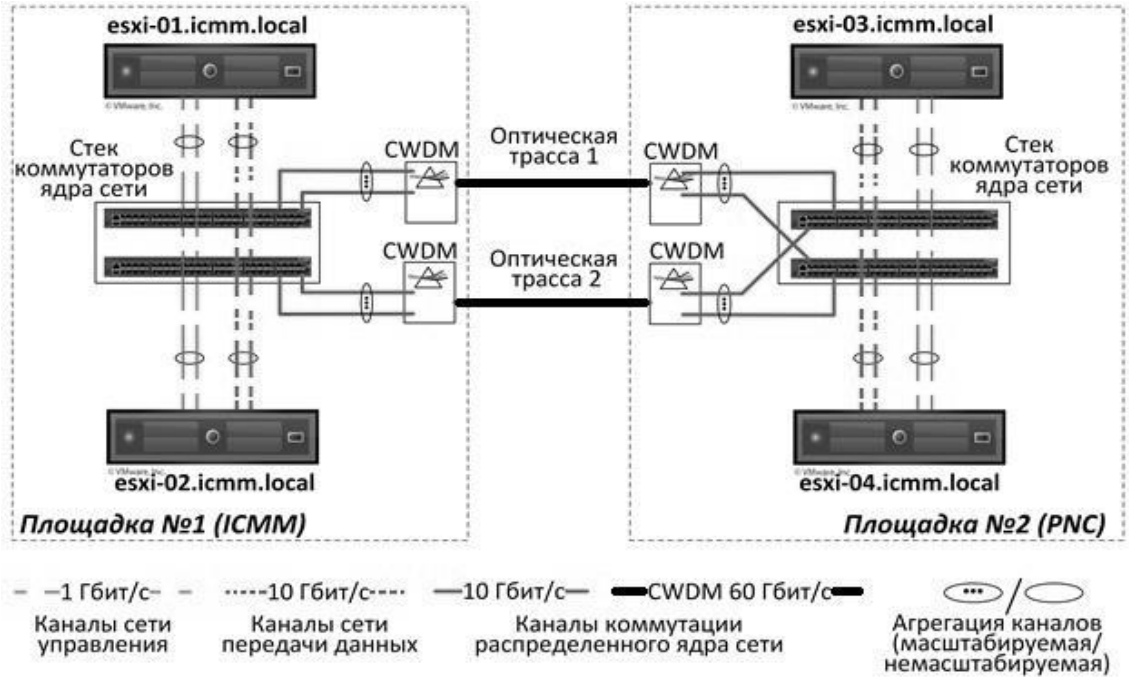

Рис. 8. Сеть гиперконвергентой системы ПФИЦ

3.3. Отказоустойчивость сетевой инфраструктуры

Обеспечение требуемого уровня отказоустойчивости и готовности (доступности) телекоммуникационной части инфраструктуры достигается благодаря обеспечению дублирования всех критически важных устройств коммутации и каналов связи. Как показано на рис. 8, на каждой из площадок собран стек из 2 коммутаторов. К каждому из коммутаторов в стеке с каждого сервера, входящего в состав платформы гиперконвергенции, подключен один физический канал 10 Гбит/с для передачи данных и один физический канал 1 Гбит/с для осуществления управления. Таким образом, благодаря стекированию коммутаторов и агрегированию (либо резервированию с использованием протокола STP) каналов связи при выходе из строя одного из коммутаторов стека на площадке доступность всех узлов платформы гиперконвергенции не изменится. Уменьшится только пропускная способность агрегированных каналов связи путем распределения нагрузки по оставшимся работоспособным каналам. И это есть ранее описанное свойство «изящной деградации» «Graceful Degradation» системы, являющееся, по-нашему мнению, наиболее перспективным способом построения надежных IT-систем.

В случае отсутствия резервирования коммутаторов на площадке система перестает быть отказоустойчивой в связи с тем, что отказ любого из коммутаторов приводит к потере связности кластера, которая выражается в появлении двух взаимно изолированных доменов отказа. При этом если «свидетель» оказался изолирован от обоих доменов отказа, ни одна из площадок не может считаться рабочей и сервисы будут остановлены до восстановления связности кластера.

4. ТЕСТИРОВАНИЕ

При вводе гиперконвергентной платформы в эксплуатацию были проведены следующие тесты: 1. Выход из строя одного любого диска хранения. Выход из строя имитировался «горячим» отключением произвольного диска.

2. Выход из строя любого кэш-диска или дисковой группы. Ситуация имити-

ровалась «горячим» отключением кэш-диска.

3. Выход из строя любого SAS-контроллера. Ситуация имитировалась программным отключением контроллера.

4. Отключение любого хост-сервера или его сетевая изоляция. Ситуация имитировалась отключением хоста от всех каналов передачи данных.

5. Отключение резервной площадки или ее сетевая изоляция. Ситуация имитировалась отключением всех хостов на резервной площадке.

6. Отключение основной площадки или ее сетевая изоляция. Ситуация имитировалась отключением всех хостов на основной площадке.

7. Отключение свидетеля или его сетевая изоляция. Ситуация имитировалась программным выключением виртуальной машины с установленным на ней свидетелем.

Отключения компонент дискового пространства серверов, выполненное в тестах 1–3, не привело к нарушению работоспособности сервисов, развёрнутых на платформе виртуализации. Тесты 4–6 приводят к временной приостановке работы сервисов, размещенных на отказавших ресурсах. В течение 3 минут система управления пытается установить связь с отказавшими объектами. Если попытка не удалась, то принимается решение о запуске сервисов на серверах, оставшихся доступными. Тест 7 не влияет на работоспособность системы, т.к. хост-свидетель необходим лишь во время выхода из строя узлов кластера.

Таким образом, отказ любого из серверных компонентов не приводит к остановке сервисов. Сам механизм отработки отказов реализован следующим образом. Если отказ был предсказуем, например, когда регулярная самопроверка указывает на деградацию диска, то перенос данных и восстановление условий их доступности (дупликация) начинается незамедлительно. Если же отказ (потеря сети, отказ сетевой карты, отключение хоста, отключение диска) произошел внезапно (временное отключение с возможностью восстановления), то vSAN начинает восстановительные процедуры отложенно (по умолчанию, через 60 мин). После обнаружения отказа vSAN останавливает ввод/вывод на 5–7 секунд для оценки готовности (доступности) потерянного объекта. Если объект переходит в состояние готовности, то ввод/вывод возобновляется. Если через 60 минут после отказа хоста или потери сети (началась процедура восстановления), потерянный хост возвращается в строй (восстановлен или поднята сеть), vSAN сама определяет, что лучше (быстрее) сделать: завершить восстановление или синхронизировать вернувшийся хост.

ВЫВОДЫ

Приведена эволюционирующая трактовка понятий и терминов надежности. Показано влияние технологий виртуализации на способы построения отказоустойчивых информационных сервисов. Проиллюстрирован комплексный подход построения корпоративной ИТКИ, обеспечивающий возможность построения отказоустойчивых информационных сервисов и систем высокой готовности.

Библиографический список

1. ГОСТ 27.002-2015. Межгосударственный стандарт. Надежность в технике. Термины и определения. – М.: Стандартинформ, 2015. – 24 с.
2. *Масич Г.Ф., Масич А.Г.* От «Инициативы GIGA UrB RAS» к Киберинфраструктуре УрО РАН // Вестник Пермского научного центра УрО РАН. – 2009. – № 4. – С. 41–56.
3. *Струков А.В.* Анализ международных и российских стандартов в области надежности, риска и безопасности [Электронный ресурс] – URL: http://szma.com/standarts_analysis.pdf (дата обращения 01.06.2018).

4. *Kirrmann, H.* Fault Tolerant Computing in Industrial Automation Switzerland: ABB Research Center. P. 94. Retrieved 2015-03-02.
5. vSphere: The Efficient and Secure Platform for Your Hybrid Cloud [Электронный ресурс]. – URL: https://www.vmware.com/products/vsphere.html (Дата обращения 01.06.2018).

THE ASPECTS OF INFORMATION AND TELECOMMUNICATION INFRASTRUCTURE'S DEPENDABILITY

G.F. Masich[1,2], S.R. Latypov[1], D.P. Chugunov[1]

[1] *Institute of Continuous Media Mechanics UB RAS*
[2] *Perm National Research Polytechnic University*

The article examines a complex approach to building a dependable corporate information and telecommunication infrastructure which covers the applications and services, servers and storage systems, data transmission networks and engineering support. It also shows the peculiarities of using hyper-converged technology of virtualization for building fault-tolerant information systems.

Keywords: IT-infrastructure, virtualization, dependability, reliability, availability.

Сведения об авторах

Масич Григорий Федорович, кандидат технических наук, заведующий лабораторией телекоммуникационных и информационных систем, Институт механики сплошных сред УрО РАН – филиал Пермского федерального исследовательского центра УрО РАН (ИМСС УрО РАН), 614013, г. Пермь, ул. Академика Королёва, 1; доцент, Пермский национальный исследовательский политехнический университет (ПНИПУ), 614990, г. Пермь, Комсомольский пр., 29; e-mail: masich@icmm.ru

Латыпов Станислав Рашидович, ведущий инженер, ИМСС УрО РАН; e-mail: LatypovSR@icmm.ru

Чугунов Денис Петрович, ведущий инженер, ИМСС УрО РАН; e-mail: chugunov@icmm.ru

Материал поступил в редакцию 10.09.2018 г.