ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования
Московский технический университет связи и информатики

В.А. Докучаев, А.А. Кальфа, Д.В. Гадасин, А.В. Ермалович,
В.В. Маклачкова, А.В. Шведов

АРХИТЕКТУРА ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Учебное пособие

Москва 2018

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования

Московский технический университет связи и информатики

В.А. Докучаев, А.А. Кальфа, Д.В. Гадасин, А.В. Ермалович,
В.В. Маклачкова, А.В. Шведов

АРХИТЕКТУРА ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Учебное пособие

для направлений: 05.13.01, 09.03.02, 09.04.02, 11.03.02, 11.04.02

Москва 2018

УДК 004.6

Гадасин Д.В., Докучаев В.А., Ермалович А.В., Кальфа А.А., Маклачкова В.В., Шведов А.В. Архитектура центров обработки данных: учебное пособие / Под ред. проф. А.А. Кальфа и проф. В.А. Докучаева / МТУСИ. – М., 2018. - 157 с.

Учебное пособие по дисциплинам «Архитектура центров обработки данных», «Корпоративные инфокоммуникационные системы и услуги» и «Теория построения инфокоммуникационных сетей и систем». Для направлений подготовки бакалавров:

11.03.02 – «Инфокоммуникационные технологии и системы связи», профиль подготовки: «Инфокоммуникационные технологии в сервисах и услугах связи»;

09.03.02 – «Информационные системы и технологии», профиль подготовки: «Информационные системы и технологии».

Для направлений подготовки магистров:

09.04.01 – «Информатика и вычислительная техника», профиль подготовки: «Разработка мобильных и интернет приложений»;

11.04.02 – «Инфокоммуникационные технологии и системы связи», профиль подготовки: «Облачные инфокоммуникационные технологии и пакетизация услуг».

Для направлений подготовки аспирантов:

05.13.01 – «Системный анализ, управление и обработка информации (по отраслям)».

Ил. 48, табл. 2, список лит. 8 назв.

Издание утверждено Методическим советом университета в качестве учебного пособия. Протокол №1 от 17.10.2017.

Рецензенты: А.А. Новиков, к.т.н., ген. директор (АО «РНТ»)
В.Ю. Статьев, к.т.н., с.н.с., начальник информационно - аналитического отдела Управления по защите персональных данных (ОАО «РЖД»)

Введение

Данное учебное пособие предназначено для студентов, изучающих курс «Архитектура центров обработки данных».

Центр обработки данных (ЦОД или дата-центр) понимается в данном учебном пособии не в узком смысле слова, т.е. исключительно, как помещение с инженерной инфраструктурой, предназначенное для размещения оборудования. Особое внимание в данном пособии уделено именно «начинке» этого помещения, т.е. серверам, системам хранения данных, коммуникационному оборудованию. Будут рассмотрены также «коробочные» и мобильные ЦОД.

Главная трудность при работе над данным пособием состояла в том, что ЦОД и, в особенности, их содержимое, быстро совершенствуются. Это характерно для всей области инфокоммуникационных технологий. Причем обновления носят иногда качественный характер и требуют пересмотра идеологии построения как отдельных подсистем, так и ЦОД в целом. Поэтому учебный курс по данной тематике должен ежегодно обновляться, а с тем, что пособие фиксирует состояние дел на вполне конкретный период времени, авторам и читателю придется смириться.

Вторая проблема заключалась в том, что в условиях быстрого изменения ситуации отсутствует строгая терминология, нормативная база, стандарты на ряд работ и оборудование. Мы старались решить эту проблему, давая определение каждому употребляемому нами понятию и термину. Все аббревиатуры расшифрованы в тексте, а иностранные переведены на русский язык. Кроме того, в конце пособия приведен перечень используемых аббревиатур с их расшифровкой.

Несмотря на эти трудности, мы надеемся, что учебное пособие будет полезным не только студентам, но и разработчикам ЦОД и их отдельных подсистем, хотя бы потому, что послужит систематизации уже накопленных знаний и опыта в области создания современных ЦОД.

1. История, стандарты, нормативная база, архитектура ЦОД

1.1. Определение ЦОД

Предметом данного пособия являются *центры обработки данных* (ЦОД). Иногда ЦОД называют также дата-центрами (от английского Data Center), причем в русскоязычных публикациях под дата-центром чаще понимают *коммерческие ЦОД* (см. ниже). Но в общем случае оба термина эквивалентны. Ранее отмечалось, что, как и вообще в области инфокоммуникационных технологий, терминология и классификация понятий, относящихся к ЦОД, не всегда однозначны. Тем не менее, существует американский стандарт TIA/EIA-942, который определяет ЦОД как *«здание (или его часть), основная функция которого состоит в том, что в нём находятся машинный зал и вспомогательные (подсобные) помещения для него»*. В свою очередь под *машинным залом (computing room)* понимается *«архитектурное пространство, предназначенное главным образом для того, чтобы размещать в нём оборудование для обработки данных»*. Под это определение подпадает даже одна стойка с серверным оборудованием, размещенная в отдельном помещении. Существует также, на наш взгляд, более точное определение того, что в настоящее время понимают под ЦОД – это «*инженерно-технический комплекс, предназначенный для размещения вычислительных ресурсов обработки и хранения информации, а также предоставления клиентам разнообразных бизнес-услуг*». Но сюда следует добавить достаточно сложную и специфическую коммуникационную среду, с одной стороны, интегрирующую вычислительные ресурсы, а с другой – обеспечивающую связь с внешними сетями, включая глобальную сеть Интернет. Современный ЦОД – это, безусловно, сложный комплекс инженерного оборудования, обеспечивающего работу вычислительной подсистемы и подсистемы хранения информации. В правильно сконструированном ЦОД эти подсистемы составляют единый *высокоэффективный комплекс.* Под эффективностью будем понимать относительно низкое энергопотребление вспомогательных систем, высокую надежность, доступность к вычислительным ресурсам, безопасность, управляемость, ремонтопригодность и масштабируемость.

Энергетическая эффективность ЦОД определяется коэффициентом энергоэффективности - PUE (Power Utilization Efficiency), определяемым как отношение полной мощности, потребляемой ЦОД, к мощности, потребляемой информационно-

технологическим оборудованием (ИТО). Энергопотребление типичного российского ЦОД по данным на 2012 год распределялось следующим образом: примерно 60% шло на основные процессы (ИТО), около 35% — на охлаждение, около 5% — на потери в источниках бесперебойного питания (ИБП), до 3% — на освещение и нужды прочих потребителей электроэнергии (см. Рисунок 1), что соответствует PUE=1,65–1,80.

Рисунок 1- Распределение энергопотребления типичного ЦОД

ЦОД фирмы Google, которые считаются одними из наиболее крупных и совершенных в мире, в 2011 году имели PUE=1,14, что выше результатов 2010 года, в котором этот показатель равнялся 1,16. Казалось бы, изменение коэффициента энергоэффективности незначительно. Но надо помнить, что уже первый контейнерный ЦОД Google, открытый в 2005 году, который состоял из 45 стандартных контейнерных модулей, размещенных на двух этажах и вмещавший более 45000 серверов, потреблял мощность 10 МВт. Фирма не публикует современные данные о потребляемых мощностях своих ЦОД, разбросанных по всему миру. Но очевидно, что снижение PUE даже на сотую долю дает громадную экономию средств, затрачиваемых на энергообеспечение фирменных ЦОД.

По данным 2015 года, одними из наиболее совершенных по энергоэффективности считаются ЦОД правительства Нидерландов (Гронинген) с PUE=1,12. Ожидается, что ЦОД Lefdal Mine Datacenter (Норвегия), размещенный в шахте и охлаждаемый водой из фьорда, строительство которого завершилось в мае 2017 г., будет иметь PUE=1,1.

Энергоэффективность типичного российского ЦОД составляет примерно 1,3-1,5. У одного из самых совершенных российских ЦОД,

принадлежащего Федеральной налоговой службе и введенного в строй в середине 2015 года в Дубне PUE=1,13 (см. рисунок 2).

Рисунок 2 - Общий вид ЦОД Федеральной налоговой службы

На базе крупных высокоэффективных ЦОД реализуются такие современные технологии, как grid-вычисления, облачные вычисления, обработка «больших данных».

1.2. История создания ЦОД

На заре компьютерной эры вычислительные центры, которые мы будем отличать от современных ЦОД, представляли собой одну или несколько электронно-вычислительных машин (ЭВМ), каждая из которых занимала помещение величиной с крупный спортзал. Первые ЭВМ, как в США, так и в СССР были созданы для использования в атомной и ракетной промышленности. Одним из самых первых коммерческих компьютеров был «Универсальный Автоматический Компьютер 1» (Universal Automatic Computer 1), или Univac 1, использовавшийся американским Бюро переписи в марте 1951 (Рисунок 3). Но в 60-е годы прошлого века такие компании, как IBM, начали предоставлять клиентам доступ к своим системам на почасовой основе, для выполнения задач по обработке данных.

Рисунок 3 - Американский «Univac 1 - Универсальный Автоматический Компьютер 1»

Большие электронно-вычислительные машины (в СССР наиболее распространенным их представителем стала БЭСМ-6 (см. рисунок 4), выпускавшаяся с 1968 по 1987 годы и имевшая характеристики на уровне своих зарубежных аналогов) получили также название мэйнфреймов. Изначально этот термин употреблялся для обозначения

типовых процессорных стоек, но позже под ним стали понимать высокопроизводительные компьютеры с огромным (по тем временам) запасом оперативной памяти, предназначенные для обработки и хранения большого объема данных. Ввод данных в такие машины осуществлялся с помощью перфокарт, которые подготавливались на специальных устройствах, а позже – с электронных терминальных устройств. Выводилась информация путем печати на бумажных лентах. В тех случаях, когда выходная информация служила входной для иных устройств (например, станков с числовым программным управлением), она выводилась на специальные перфорированные ленты.

Рисунок 4 - Советский мейнфрейм – ЭВМ БЭСМ-6

Уже на уровне мэйнфреймов размещение в одном или нескольких близко расположенных помещениях вычислительных средств большой мощности стимулировало развитие некоторых концепций, используемых в современных ЦОД. К ним можно отнести расположение оборудования в стойках, использование фальшполов, прокладку кабелей в специальных коробах и т.д. Кроме того, первые системы охлаждения, вентиляции, источников бесперебойного и гарантированного питания, контроля доступа, пожарной и охранной сигнализации, пожаротушения первоначально создавались для помещений, в которых располагались мэйнфреймы, а уже затем получили развитие в ЦОД.

Появление клиент-серверной архитектуры и усложнение ее структуры привело к переходу от одного компьютера в виде мэйнфрейма к тому, что мы можем назвать первыми ЦОД. Это были помещения, в которых размещалось некоторое количество серверов, используемых для вычислений и хранения данных (позже появились специализированные

системы хранения данных - СХД), а также набор инженерных систем, обеспечивающих работоспособность этого оборудования.

К 1980 году подобные центры начинают появляться на многих предприятиях и компаниях крупного, среднего и даже малого бизнеса, и они используются и в настоящее время. Разумеется, в небольших ЦОД их оптимизация по энергопотреблению не имеет принципиального значения. Иное дело крупные современные ЦОД, в которых на одной площади сосредоточены мощные серверы, осуществляющие обработку информации, СХД и активное сетевое оборудование отвечающее, как за обмен данными с внешним миром, так и за передачу данных внутри ЦОД. Такие ЦОД обязательно включают сложные инженерные системы, обеспечивающие его жизнедеятельность. Сюда входят, прежде всего, так называемые подсистемы HVAC (от английских слов Heating, Ventilation and Air Conditioning — Теплоснабжение, Вентиляция и Кондиционирование). Поскольку к крупным ЦОД предъявляются повышенные требования по надежности их функционирования, они обязательно включают подсистемы бесперебойного и гарантированного электроснабжения, а подсистемы HVAC обычно дублируются. К перечисленным следует добавить подсистемы технологического видеонаблюдения, пожарной сигнализации и пожаротушения. Надежность хранения данных обеспечивается также подсистемами безопасности, как информационной (разграничение доступа к информации, протоколирование действий пользователей, использование системы паролей, антивирусной защиты, межсетевых экранов и т.д.), так и физической (охранного видеонаблюдения, контроля доступа). Кроме того, крупный современный ЦОД обязательно включает службу мониторинга, управления и сервисной поддержки. Мониторинг состояния всех подсистем ЦОД и оптимизация их функционирования с помощью средств управления – одно из важных отличий современного ЦОД от вычислительных центров второй половины прошлого века.

1.3. Стандарты

1.3.1. Североамериканский стандарт TIA/EIA–942

Стандартизация рассматривается как один из принципов системного подхода к построению инфраструктуры, обеспечивающий масштабируемость решений и сокращение капитальных расходов. Она помогает унифицировать реализацию взаимосвязанных инфраструктурных систем ЦОД. Сейчас проектировщики чаще всего руководствуются американским (точнее, североамериканским, потому

что он распространяется и на Канаду) стандартом TIA-492 (или TIA/EIA-492) «Telecommunications Infrastructure Standard for Data Centers», которому мы уделим наибольшее внимание. Свое название стандарт получил по названию организации, его выпустившей, а именно, Ассоциации телекоммуникационной промышленности США (Telecommunications Industry Association - TIA). Поскольку последняя является филиалом Альянса электронной промышленности (Electronic Industries Alliance – EIA), то в названии стандарта часто отражают наименование и этой организации: TIA/EIA-942. Этот стандарт, принятый в 2005 году, дал серьезный толчок для развития отрасли ЦОД.

Стандарт TIA/EIA–942 рассматривает следующие вопросы, связанные с проектированием и организацией ЦОД:

- общий подход к проектированию ЦОД;
- структура и архитектура структурированной кабельной системы (СКС) в ЦОД;
- требования к помещениям и территории, на которой планируется размещать ЦОД;
- архитектурные решения ЦОД;
- подходы к проектированию систем охлаждения, электроснабжения в ЦОД;
- построение системы кабельных каналов для ЦОД;
- резервирование и уровни надежности ЦОД.

Стандарт ничего не говорит об информационной «начинке» ЦОД - серверах, СХД, активном коммуникационном оборудовании. Это объясняется, с одной стороны, тем, что его предметом является именно инфраструктура. С другой стороны, само оборудование ЦОД может быть самым разнообразным, в том числе, установленным непосредственно заказчиками. Тем не менее, как отмечалось во введении, в данном пособии мы рассмотрим и оборудование, функционирующее в типичных современных ЦОД.

Стандарт TIA/EIA-942 фиксирует четыре уровня постоянной готовности инфраструктуры ЦОД к выполнению им своих функций. Для каждого из выделенных четырех инфраструктурных уровней готовности приводятся детальные рекомендации, относящиеся к архитектуре ЦОД, к проблемам их безопасности, электрике, механике и телекоммуникациям. Более высокий уровень соответствует более высокой постоянной готовности ЦОД к выполнению им своих функций. Описание каждого уровня содержит такие сведения, как, например, высота фальшпола,

удельные параметры мощности и критические точки. Латинская буква "N" (от "Need" – минимально необходимое число) с последующим числовым параметром означает избыточность инфраструктурных компонентов по сравнению с минимальными потребностями системы.

Уровень 1 — базовый:

- ЦОД подвержен нарушениям нормального хода работы, как от плановых, так и от внеплановых действий;
- он имеет лишь один путь (канал) распределения электропитания и охлаждения без резервированных компонентов (N);
- может иметь или не иметь фальшпол, источник бесперебойного питания (ИБП), генератор электроэнергии;
- развертывается за три месяца;
- годовое время простоя — 28,8 часов, что соответствует коэффициенту постоянной готовности Кп.г.= (365*24 – 28,8)/365*24=99,671%, где 365*24=8760 – число часов в году;
- ЦОД должен полностью останавливаться для планового обслуживания и профилактического ремонта.

Уровень 2 — ЦОД с резервированием:

- менее подвержен нарушениям нормального хода работы, как от плановых, так и от внеплановых действий;
- имеет один путь (канал) распределения электропитания и охлаждения, но с резервированными компонентами (N+1);
- имеет фальшпол, ИБП и генератор;
- время развертывания - от трех до шести месяцев;
- годовое время простоя — 22,0 часа, соответствует коэффициенту постоянной готовности Кп.г.= (365*24 – 22,0)/365*24=99,749%;
- техническое обслуживание и ремонт канала электропитания и других частей инфраструктуры объекта требует остановки процесса обработки данных.

Уровень 3 — ЦОД с возможностью параллельного проведения ремонтно-профилактических работ:

- допускает плановую деятельность без нарушения нормального хода работы оборудования машинного зала, однако внеплановые события все же могут привести к нарушению его работы;

- имеет несколько путей (каналов) для распределения электропитания и охлаждения, но лишь один из них активен; имеет резервированные компоненты (N+1);
- время развертывания - от 15 до 20 месяцев;
- годовое время простоя — 1,6 часа, соответствует коэффициенту постоянной готовности Кп.г.= (365*24 – 1,6)/365*24=99,982%;
- имеет достаточно мощности и распределительных возможностей для того, чтобы при загруженности одного пути (канала) можно было одновременно осуществлять обслуживание или тестирование другого пути.

Уровень 4 — отказоустойчивый ЦОД:

- плановые действия не нарушают критически важной нагрузки, причем ЦОД способен справиться, по крайней мере, с одним неплановым инцидентом наихудшего свойства без последствий для критически важной нагрузки;
- имеет несколько активных путей распределения нагрузки и охлаждения с резервными компонентами 2 (N+1), т.е. два ИБП с избыточностью N+1 каждый);
- время развертывания - от 15 до 20 месяцев;
- годовое время простоя — 0,4 часа, соответствует коэффициенту постоянной готовности Кп.г.= (365*24 – 0,4)/365*24=99,995%.

Именно на требования стандарта TIA/EIA-942 мы будем ориентироваться в дальнейшем при рассмотрении требований к месту расположения ЦОД, его инженерной структуре, климатическим условиям и т.д., изложенных в соответствующих разделах.

Сертификацию на соответствие тому или иному уровню стандарта TIA/EIA-942 производит компания Uptime Institute, имеющая отделение в России - Uptime Institute Russia. Причем сертификаты выдаются на проект, площадку (готовое здание), а с 2012 года и на стабильность в работе (операционную устойчивость) -Tier Sertification of Operational Stability. Этот сертификат очень важен для коммерческих ЦОД, поскольку их владельцы склонны скрывать информацию о сбоях.

На середину 2017 года в России были сертифицированы по уровню Tier III 26 **проектов** ЦОД, из которых только 13 находятся в Москве. А проект ЦОД Саранского технопарка в Мордовии имеет сертификат Tier IV. Сертификат Tier III непосредственно **на площадку**

имели на тот же период только 7 ЦОД – компаний Dataine, DataPro, DataSpace, GAU “CIC SO” КРОК, Сбербанка и ВТБ.

Поскольку сертификат **на стабильность** в работе стал выдаваться относительно недавно, на середину 2017 года во всем мире его имели всего 41 ЦОД (9 - уровня Tier IV и 32 - уровня Tier III). В России этим сертификатом к середине 2017 года обладали ЦОДы компаний Dataine, DataPro, DataSpace, КРОК и Сбербанка.

1.3.2. Европейский стандарт EN 50173-5 и международный стандарт ISO/IEC 24764

Стандарт TIA/EIA–942 явился отправной точкой для разработки европейского стандарта EN 50173-5 (Information technology – Generic cabling systems. Part 5: Data centres). Он был опубликован в 2007 году. В этом стандарте рассматриваются следующие вопросы:

— структура, иерархия и функциональные элементы структурированной кабельной системы (СКС) в ЦОД;

— интерфейсы в СКС;

— требования к каналу, к медным и оптическим кабельным линиям в СКС;

— требования к соединительному и распределительному оборудованию;

— требования к шнурам и перемычкам, используемым в ЦОД.

Как следует из приведенного перечисления, этот стандарт затрагивает более узкие вопросы построения ЦОД, чем TIA/EIA-942. Так, в нем не рассматриваются требования к помещениям и территории, на которой планируется размещать ЦОД, архитектурные решения, требования к системам охлаждения, электроснабжения и т.д. Зато в этом стандарте более подробно регламентируется построение СКС в ЦОД. И требования к СКС мы рассмотрим в разделе 4.3 именно на основе этого стандарта.

Международный стандарт ISO/IEC 24764 (Information technology – Generic cabling systems for Data Centres) был разработан совместно Международной организацией по стандартизации (International Organization for Standardization) и Международной электротехнической комиссией (International Electrotechnical Commission) на основе европейского стандарта и введен в действие в 2010 году. Он включает помимо вопросов, рассматриваемых стандартом EN 50173-5, еще и следующие положения:

— резервирование компонент систем;

— требования к заземлению;

— требования к маркировке и идентификации пассивных компонентов;

— использование решений высокой плотности для оптической кабельной системы.

В этом стандарте приводятся также конкретные требования по минимально и максимально допустимым длинам кабелей в СКС.

1.3.3. Европейский стандарт BICSI 002 2010

В 2010 году появился еще один стандарт, имеющий непосредственное отношение к ЦОД - BICSI 002 2010 «Data Center Design and Implementation Best Practices». Этот стандарт разработан профессиональной некоммерческой ассоциацией Building Industry Consulting Service International, основанной более 30 лет назад для консультационной поддержки телефонных строительно-монтажных компаний. Аббревиатура названия ассоциации и дала название стандарту, а последующие цифры указывают на номер редакции и дату создания документа.

Стандарт BICSI 002 2010, в создании которого участвовали более 150 экспертов, не повторяет, а дополняет существующие стандарты TIA/EIA, EN 50173-5 и ISO/IEC, ликвидировав пробелы в таких областях создания ЦОД, как выбор места для их строительства, формирование требований к планировке и составу помещений, а также к организации систем жизнеобеспечения, включая широкий спектр вопросов безопасности. В частности, в разделе, посвященном безопасности, содержатся данные, регламентирующие комплекс мероприятий, осуществляемых на основе анализа возможных рисков (эти меры необходимы для организации физической защиты ЦОД, формирования планов противодействия потенциальным злоумышленникам и выхода из аварийных ситуаций), а также требования к обеспечению безопасности на всех этапах проектирования и строительства.

Стандарт включает следующие разделы:

— планирование пространства ЦОД;

— выбор строительной площадки;

— архитектурные аспекты планирования;

— структурные аспекты планирования;

— системы электроснабжения;

— механические системы;

— системы пожаротушения;

— системы безопасности;

— системы диспетчеризации инженерного оборудования здания;

— телекоммуникационные системы;

— информационные технологии;

— сдача объекта в эксплуатацию;

— эксплуатация и обслуживание ЦОД, процесс проектирования, надежность и техническая готовность.

Особое внимание уделено этапу приемки объекта и ввода его в эксплуатацию. В частности, дается методология анализа последствий для проекта, которые возможны в случае внесения изменений в дизайн (все это входит в обязанности инженеров, отвечающих за ввод ЦОД в эксплуатацию). На этапе приемки ведется тестирование продукта на функциональность и выполняется полный аудит площадки. Фаза приемки также включает подготовку персонала. Сотрудников рекомендуется готовить к поиску проблем, неисправностей, учить корректно включать и выключать оборудование, предпринимать правильные действия в случае неполадок, форс-мажорных обстоятельств.

В отличие от стандарта TIA/EIA-942, модель, предложенная BICSI, определяет не четыре, а пять классов готовности ЦОД на основе четырех критериев: резервирования компонентов, резервирования систем, использования продуктов с определенным уровнем качества и мер противодействия любым внешним воздействиям, включая природные явления.

Раздел, посвященный информационным технологиям, содержит сведения о планировке помещений и размещении оборудования, кабельных системах, мерах по обеспечению заданного уровня готовности ЦОД. В состав последних входят, в частности, рекомендации по резервированию, включая создание и размещение резервных ЦОД.

Несмотря на то, что BICSI 002 2010 является самой поздней разработкой и более подробен, чем TIA/EIA-942, мы в дальнейшем будем ориентироваться именно на последний. Это связано с тем, что он получил более широкое распространение (возможно, именно потому, что был первым), на него чаще ориентируются разработчики ЦОД, и предложенная в нем классификация чаще используется в литературе для оценки уровня готовности ЦОД.

1.3.4. Российские стандарты

В настоящее время к действующим российским стандартам в области построения ЦОД можно отнести строительные нормы СН512-78 «Инструкция по проектированию зданий и помещений для электронно-

вычислительных машин», разработанные еще в 1978 году, и ГОСТ Р 52919-2008 «Методы и средства физической защиты. Классификация и методы испытаний на огнестойкость». СН512-78 регламентирует следующие вопросы организации ЦОД:

— места размещения;

— объемно-планировочные и конструктивные решения зданий и помещений;

— организацию отопления, вентиляции, кондиционирования, горячего водоснабжения, водопровода и канализации;

— организацию электроснабжения и требования к электротехническим устройствам.

Но, несмотря на то, что последняя редакция СН512-78 относится к 2000 году, они морально устарели, что следует хотя бы из того, что в них содержатся рекомендации к помещениям для хранения перфолент и перфокарт, давно не используемых в информационных технологиях.

Разработка ГОСТ Р 52919-2008, безусловно, положительное явление. Но он носит достаточно частный характер, что следует уже из его названия, и не решает проблему организации ЦОД в целом. Поэтому чаще всего российские разработчики ЦОД ориентируются на американский или европейские стандарты.

1.4. Нормативно-правовая база функционирования ЦОД

1.4.1. Федеральный закон №242-ФЗ

21 июля 2014 года был подписан Федеральный закон № 242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях" - так называемый закон о хранении персональных данных россиян на территории РФ. Пункт 1 статьи 2 Федерального закона № 242-ФЗ дополняет статью 18 часть Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" следующим положением:

«При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, **находящихся на территории Российской Федерации**».

Этот закон побудил ряд зарубежных компаний к переносу на территорию России ЦОД, в которых хранились персональные данные

российских граждан. Еще в 2014 году переносить серверы в Россию начала компания Google. О готовности хранить персональные данные российских пользователей на серверах России в апреле 2015 года сообщали eBay и китайская торговая площадка AliExpress. По состоянию на апрель 2015 года в СМИ фигурировала информация о готовности в общей сложности более ста зарубежных компаний разместить данные россиян на российских ЦОД.

1.4.2. Распоряжение Правительства Российской Федерации от 7 октября 2015 г. № 1995-р

7 октября 2015 года своим Распоряжением № 1995-р Правительство Российской Федерации утвердило «Концепцию перевода обработки и хранения государственных информационных ресурсов, не содержащих сведения, составляющие государственную тайну, в систему федеральных и региональных центров обработки данных». В Концепции констатируется крайне низкий уровень эффективности использования энергоресурсов информационно – телекоммуникационной инфраструктуры органов государственной власти. В частности, отмечается, что информационно-телекоммуникационная инфраструктура органов государственной власти в основном размещается в серверных комнатах, в которых:

— среднее количество серверных стоек на один собственный машинный зал или серверную составляет 1,3 единицы;

— 67 процентов общего количества собственных серверных стоек имеют мощность потребления не более 3 кВт на стойку.

В Концепции также отмечается, что в 2014 году расходы на облачные услуги госучреждений составили только 10 процентов от общих расходов на развитие объектов информационно-телекоммуникационной инфраструктуры госструктур, а 70 процентов государственных служащих используют для служебной переписки почтовые сервисы коммерческих организаций.

Поскольку информационно – телекоммуникационная инфраструктура органов государственной власти базируется, как правило, на импортных технических и программных средствах, она становится уязвимой для внешних компьютерных атак. Возможные мероприятия по импортозамещению и организации комплексной защиты информации от внешних воздействий существенно ограничиваются

разнородностью используемых технологий и программно-аппаратных средств.

В Концепции описывается подход к переводу государственных информационных ресурсов в систему ЦОД, используемую для нужд органов государственной власти, государственных органов, государственных корпораций и открытых акционерных обществ с государственным участием (далее соответственно - пользователи). Согласно Концепции, система ЦОД должна создаваться в виде сети федеральных и региональных ЦОД, связанных резервированными магистральными каналами связи высокой пропускной способности в единый катастрофоустойчивый кластер. Защита от компьютерных атак должна быть реализована с использованием надежных программно-аппаратных средств и соблюдением принципа невыхода трафика указанного кластера за пределы Российской Федерации. Концепция содержит также План реализации системы ЦОД органов государственной власти, реализация которого должна быть завершена в 2021 году.

1.5. Архитектура коммерческих и корпоративных ЦОД

1.5.1. Особенности коммерческих и корпоративных ЦОД

ЦОД можно разделить на две категории:

— *коммерческие*, предоставляющие свои ресурсы потребителям за определенную плату;

— *корпоративные*, обслуживающие одну организацию, фирму или корпорацию.

Это деление весьма условно, поскольку коммерческие ЦОД зачастую предоставляют услуги и внутренним потребителям, а корпоративные — внешним. Более того, корпоративные ЦОД часто выделяются в отдельное юридическое лицо, которое предоставляет услуги своему единственному клиенту на коммерческой основе.

Коммерческие ЦОД обычно оказывают следующие виды основных услуг:

— размещение клиентом своего оборудования в ЦОД с использованием технических ресурсов последнего (colocation);

— предоставление клиенту серверов в аренду (dedicated server);

— размещение клиентом телекоммуникационной инфраструктуры в ЦОД (telehousing),

— аренда дискового пространства на оборудовании владельца ЦОД с заранее согласованной платформой и конфигурацией операционной системы (shared).

Кроме того, на коммерческой основе могут предоставляться следующие дополнительные услуги:

— аутсорсинг информационных систем, когда поставщик услуг получает в полное управление всю ИТ-инфраструктуру клиента;

— хостинг обслуживания и администрирования программного обеспечения (ПО), когда поставщик услуг осуществляет централизованное управление программным обеспечением, находящимся на его территории, а заказчик имеет к нему удаленный доступ;

— хостинг инфраструктурных услуг, когда поставщик предоставляет стандартные элементы ИТ-инфраструктуры в удаленное пользование на определенный период.

Корпоративные ЦОД обычно принадлежат компаниям, для которых критичны максимальная степень готовности, отказоустойчивость, надёжность и защищенность информационных систем. Это крупные компании, например, ритейлеры, эксплуатирующие сложные бизнес-приложения, такие, как системы ERP (enterprise resourse planning - управление ресурсами предприятия), CRM (customer relationship management – управление заказами), BI (Business Intelligence - бизнес аналитики), операторы услуг связи, банки, обслуживающие клиентские счета и проводящие расчёты по пластиковым карточкам, страховые компании и другие.

Корпоративный ЦОД должен обеспечивать:

— заданный уровень производительности приложений;

— надежность хранения данных, отказоустойчивость оборудования и ПО;

— адаптируемость под быстро меняющиеся задачи бизнеса;

— масштабируемость, т.е. возможность наращивания ресурсов без кардинального перестроения архитектуры вычислительного комплекса;

— повышение уровня услуг, предоставляемых компанией своим клиентам;

— повышение производительности труда сотрудников за счет увеличения скорости выполнения операций, улучшения контроля исполнения обязанностей, а следовательно, уменьшения обслуживающего персонала.

1.5.2. Архитектура ЦОД

Архитектурную модель ЦОД можно представить в виде следующих пяти уровней.

Уровень инженерной инфраструктуры включает в себя СКС, системы бесперебойного и гарантированного электропитания, микроклимата, безопасности, пожарной сигнализации и пожаротушения, мониторинга и управления, а также монтажные конструктивы для размещения оборудования. Этот уровень играет роль фундамента ЦОД, обеспечивая оптимальные условия для функционирования всех систем и работы персонала.

В коммерческих ЦОД к этому уровню предъявляются жесткие требования, обусловленные сверхвысокой плотностью размещения серверов, критической важностью сохранения информационных ресурсов пользователей и, как правило, достаточно большими рабочими площадями. Инженерная инфраструктура коммерческого ЦОД обычно строится «с нуля», ориентируясь на лучшие мировые достижения в этой области, на рассмотренные в разделе 1.3 специализированные стандарты и на рекомендации ведущих поставщиков инженерного оборудования. Современные коммерческие ЦОД имеют уровень не ниже третьего в соответствии с классификацией стандарта TIA/EIA-942.

Для корпоративных ЦОД столь жесткие требования отсутствуют. На этом уровне они варьируются от минимальных до таких, которые соответствуют коммерческим ЦОД или даже превышают их. Они определяются как финансовыми возможностями корпорации или компании, так и критичностью простоя сервисов, который может повлечь за собой значительные финансовые потери.

Уровень технической архитектуры обеспечивает платформу для функционирования служебных и бизнес-сервисов, в составе которой можно выделить следующие подсистемы:

— серверная, состоящая из вычислительных ресурсов, поддерживающих надежное функционирование служебных сервисов и бизнес-приложений;

— СХД, обеспечивающая надежное хранение данных, их архивных копий и приложений, быстрый доступ к ним;

— сетевого взаимодействия, которая отвечает как за надежную внутреннюю передачу информации между компонентами технической архитектуры ЦОД, так и за доступ внешних потребителей к ресурсам ЦОД;

— информационной безопасности, обеспечивающая защиту данных от уничтожения и модификации.

В коммерческих ЦОД серверная подсистема характеризуется высокой плотностью вычислительных мощностей, эффективным использованием инфраструктуры, взаимозаменяемостью компонентов, использованием виртуализации (см. раздел 2.6). В СХД используется как локальное хранение, так и более дорогое сетевое хранение (Storage Area Networks – SAN), а также частичная консолидация (одна система хранения на группу серверов). Для защиты данных в СХД обычно применяется резервное копирование и базовая репликация. Подсистема межсетевого взаимодействия коммерческих ЦОД характеризуется многократным резервированием внешних каналов связи, резервированием сетевых соединений серверов, массовой консолидацией сетевых портов, разделением клиентских и служебных сетей, развитым функционалом управления адресацией, маршрутизацией, а также масштабируемостью и модульностью архитектуры. Подсистема информационной безопасности на техническом уровне обычно базируется на межсетевых экранах.

В серверном комплексе корпоративных ЦОД одновременно применяются как горизонтально масштабируемые вычислительные системы (для инфраструктурных задач, Web-сервисов и приложений), так и вертикально масштабируемые системы для приложений типа уже упоминавшихся ERP, BI и CRM.

Для подсистемы сетевого взаимодействия корпоративного ЦОД основными задачами являются обеспечение доступа пользователей к приложениям из корпоративной сети и поддержка эффективного взаимодействия серверов и приложений. Требования к сетевой архитектуре не превышают требований у коммерческих ЦОД.

Уровень служебных сервисов представлен набором специализированных технологий, которые оптимизируют работу технической архитектуры ЦОД, обеспечивают эффективное функционирование и взаимодействие приложений. На этом уровне можно выделить сервисы информационной безопасности, унифицированных коммуникаций, хранения и управления данными, управления и мониторинга, идентификации и авторизации, виртуализации и ряд других.

В коммерческих ЦОД на этом уровне формируются несколько стандартных сервисов:

— управление хостингом, представляющее собой специфичный сервис коммерческих ЦОД, которое состоит в поддержке автоматизированного централизованного управления серверами, ресурсами и пользователями;

— обеспечивающие сервисы, которые в силу их критичности требуют обязательного резервирования и организации комплексов защиты;

— сервисы информационной безопасности, представляющие собой набор систем межсетевого экранирования, обнаружения атак и антивирусной защиты;

— сервисы управления, которые могут реализовываться, в частности, с помощью отдельной системы сетевого управления (NMS – Network Management Service).

В корпоративных ЦОД используются сервисы, специфичные для приложений, а также стандартные сервисы информационной безопасности и системы управления. Сервисы информационной защиты могут быть очень развитыми, с полнофункциональными системами обнаружения и предотвращения вторжений, антивирусной защиты, контентной фильтрации, управления и мониторинга событий, средствами организации VPN (virtual private network – виртуальных частных сетей) и т.д. Система управления, обычно реализуемая в централизованном варианте, обеспечивает как функционал сетевого управления, так и возможность управления серверами и системами хранения. Также следует упомянуть распространенные сервисы для организации "тонких" клиентов унифицированных коммуникаций, мобильного доступа персонала.

Уровень бизнес-приложений состоит, естественно, из бизнес-приложений, коммуникационных приложений и средств коллективной работы, которые в совокупности обеспечивают эффективность работы организации.

На этом уровне в коммерческих ЦОД действуют преимущественно пользовательские телематические сервисы (факсимильные службы, службы электронных и голосовых сообщений, аудио/видеоконференции, а также доступа к информации, хранящейся в электронном виде). В зависимости от типа хостинга (размещение собственных серверов или аренда выделенного сервера) можно разворачивать бизнес-приложения разной степени критичности. На этом же уровне функционируют собственные приложения провайдера, такие как биллинг и CRM.

В корпоративных ЦОД на этом уровне действуют немногочисленные корпоративные телематические сервисы, средства обеспечения совместной работы и документооборота, бизнес-приложения с индивидуальными, но достаточно типовыми требованиями.

Уровень организационной структуры включает в себя персонал, политики и процедуры, поддерживающие функционирование всех перечисленных уровней.

Организация обслуживания коммерческого ЦОД — очень важный процесс, и применение практик ITIL/ITSM (IT Service Management on the base of IT Infrastructure Library - Управление ИТ-сервисами на основе библиотеки методик и правил постановки процессов работы ИТ-служб) становится необходимым элементом поддержки его эффективности. Для коммерческих ЦОД обязательны документированные, доведенные до персонала, протестированные планы и процедуры аварийного восстановления, политики и регламенты. Типовые требования к коммерческому ЦОД — круглосуточный режим работы службы поддержки (в несколько смен), доступность call-центра, организация служб поддержки и обслуживания - HelpDesk/ServiceDesk. Жестко регламентируются зоны ответственности каждого сотрудника и каждой службы.

В корпоративных ЦОД внедрение практик ITIL/ITSM также считается действенным инструментом управления, но это не всегда признает высшее бизнес-руководство. Иногда сложившиеся структуры и процедуры становятся незыблемыми основами деятельности. Все большее распространение в обслуживания корпоративных ЦОД приобретает аутсорсинг. В этом случае к уровню организационной структуры предъявляются такие же требования, как и к коммерческим ЦОД. При этом особое внимание следует уделить вопросам восстановления бизнес-приложений и политике информационной безопасности.

1.6. ЦОД в России

По количеству ЦОД, их площади и потребляемой мощности Россия пока уступает не только развитым, но и многим развивающимся странам. Однако ситуация быстро меняется. Если в 2011 году в стране насчитывалось около 130 крупных и средних коммерческих ЦОД, то в 2013 году было уже более 165, в 2014 году –175, а в 2015 – более 180.

Основной показатель для рынка ЦОД — количество установленных в центрах стоек, или стандартных шкафов для размещения оборудования. По оценкам экспертов рынка, в начале 2016 года численность стоек, используемых для коммерческой деятельности, составляла 30,5 тыс. единиц. Из них 14% располагалось на площадках, сертифицированных на соответствие Tier III, 44% — на площадках, которые не имели сертификата, но готовы были гарантировать доступность сервисов не ниже 99,98% (Tier III заявленные). Согласно прогнозам, к концу 2017 года общее количество стоек в российских дата-центрах вырастет на 24,5%, до 38 тыс. штук. Объем этого рынка увеличится до 20 млрд руб., то есть на 19% по сравнению с 2016 годом.

10 компаний, обладающих крупнейшими в России ЦОД по данным на 2017 год, представлены в Таблице 1.

Таблица 1 - 10 компаний, обладающих крупнейшими в России ЦОД по данным на 2017 г.

№ 2017	Название компании	Количество введенных в эксплуатацию стойко-мест, все ЦОД	Совокупная площадь серверных залов, кв м	Совокупная подведенная мощность ко всем ЦОД, мВт	Количество ЦОД на территории РФ
1	DataLine	4 207	7 669	30,6	7
2	Ростелеком	4 100	12 500	35	22
3	Linxtelecom	2 040	2 186	17	2
4	Selectel	1 610	6 700	11,4	6
5	Stack Group	1 400	2 800	8,7	2
6	DataPro	1 350	1 360	20	1
7	Сервионика (ГК «АйТеко»)	1 200	6 000	8	1
8	DataSpace	1 152	3 000	9,5	1
9	Xelent (SDN)	1 074	6 500	9,3	1
10	Крок	1 000	3 000	11	3

Приведенные рейтинги весьма условны, поскольку, как правило, они строятся на уровне экспертных оценок. По итогам 11 месяцев 2017 года крупнейшие ЦОД принадлежали компаниям DataLine, Ростелеком, Linxtelecom, Selectel, Stack Group, DataPro, Сервионика (ГК «Ай-Теко»), DataSpace, Xelent, Крок. В банковском секторе крупнейший корпоративный ЦОД имеет «Сбербанк» – 12 МВт. Более 70% коммерческих ЦОД расположены в Москве, 17% - в Санкт-Петербурге. Но по результатам 2014 г. Россия занимала всего 0,2% мирового рынка коммерческих ЦОД по общей площади технических залов.

Примерное распределение ЦОД по секторам экономики представлено на Рисунке 5. Как видно из рисунка, наибольшее число ЦОД принадлежит ИТ-компаниям. Среди российских компаний следует отметить компанию DataLine, владеющую самым крупным коммерческим ЦОД в РФ NORD-4, общей площадью 11,7 тыс м^2, и рассчитанным на мощность 20 000 кВА, запущенным в 2015 году. Также

компания владеет еще несколькими площадками ЦОД в г. Москва: OST, включающую в себя три ЦОД (OST-1, OST-2, OST-3), общей площадью 5 769 м^2, и рассчитанные на мощность 15 000 кВА, запущенные в 2009 году; NORD, включающую в себя четыре ЦОД (NORD-1, NORD-2, NORD-3, NORD-4), общей площадью 13 688 м^2, и рассчитанные на мощность 20 200 кВА, запущенные в 2010 году

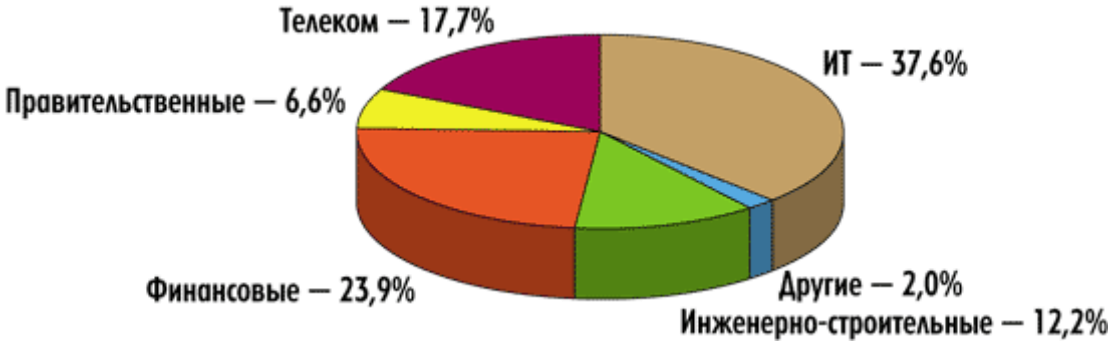

Рисунок 5 - Распределение ЦОД по секторам экономики

Компания DataSpace имеет ЦОД общей площадью 6 тыс. м^2 (площадь фальшпола для размещения оборудования — 3 тыс. м^2) и рассчитанный на мощность 9 МВт.

Компания Linxdatacenter представила ЦОД, введенный в эксплуатацию в октябре 2011 года в Санкт-Петербурге. Его общая площадь составляет 7,5 тыс. м^2 (в 2012 году она будет увеличена до 9 тыс. м^2), а мощность энергоснабжения — 3 МВт (с возможностью расширения до 12 МВт).

Крупным игроком на российском рынке ЦОД является и компания «Крок». Самым крупным из трех ЦОД компании является центр обработки данных «Компрессор» общей мощностью 8 МВт и вместимостью 800 стоек.

Можно отметить и компанию «Ай-Теко» с коммерческим ЦОД «ТрастИнфо» (уровень надежности Tier III). В декабре 2011 года в Финляндии открыт резервный ЦОД «ТрастИнфо» - TrustNet Oy, который предоставляет клиентам как классические для ЦОД услуги, так и облачные сервисы. TrustNet Oy — это первый и на сегодня единственный российский ЦОД на территории Финляндии.

Как видно из рисунка 5, второе место по использованию ЦОД принадлежит банковскому сектору. В России безусловный лидер этого сектора – Сбербанк, которому принадлежит один из крупнейших в России ЦОД, располагающийся в районе Южного порта на месте бумажной фабрики «Восход». В нем консолидированы ресурсы, которые ранее размещались в 36 региональных ЦОД. Общая площадь здания

центра — около 16 500 м^2, мощность ИТ-нагрузки — 10–12 МВт. МегаЦОД Сбербанка имеет сертификат на проект Tier III, и в 2012 году была произведена сертификация уже построенного объекта.

Хотя отечественные ЦОД сейчас, безусловно, уступают зарубежным не только в количественном отношении, но и по уровню проектирования, оснащенности системами диспетчеризации и управления, однако, и здесь заметен явный прогресс. ЦОД усложняются и увеличиваются в размерах. Давно обзаведшиеся ими крупные компании все чаще прибегают к созданию резервных мощностей. В целом же рынок системной интеграции эволюционирует теперь в сторону предоставления облачных сервисов.

Контрольные вопросы

1. Определение ЦОД.
2. История создания ЦОД.
3. Уровни выделяемые в стандарте TIA/EIA–94.
4. Основные положения стандартов EN 50173-5 и ISO/IEC 24764.
5. Основные разделы стандарта BICSI 002 2010.
6. Действующие российские стандарты в области построения ЦОД.
7. Основные положения Федерального закона №242-ФЗ.
8. Основные положения Распоряжения Правительства Российской Федерации от 7 октября 2015 г. N 1995-р.
9. Особенности коммерческих и корпоративных ЦОД.
10. Основные различия и сходства коммерческих и корпоративных ЦОД.
11. Уровни архитектуры ЦОД.

2. Серверная подсистема ЦОД

2.1. Что такое серверы?

Как уже отмечалось, стандарты не определяют, какой должна быть «начинка» ЦОД. Это естественно, поскольку в ЦОД может размещаться оборудование заказчика по его желанию (colocation). Но в любом ЦОД присутствуют четыре основные подсистемы – серверная, хранения данных, коммуникационная и безопасности. Без понимания особенностей и тенденций развития этих систем спроектировать и построить высокоэффективный ЦОД невозможно. В данной главе мы рассмотрим особенности серверной подсистемы ЦОД.

Прежде всего, ответим на вопрос, что понимается под сервером? Сервер (от английского serve – служить, обслуживать) – это компьютер, выделенный из группы рабочих станций для выполнения какой-либо сервисной (обслуживающей сеть) задачи без непосредственного участия человека. Таким образом, роль сервера в принципе может выполнять любой компьютер сети, оптимизированный для оказания услуг другим «клиентам» - компьютерам, принтерам, факсам и т.д. Сервер и клиенты образуют клиент-серверную сеть, обеспечивающую централизованный доступ к:

— информации;
— ресурсам;
— данным;
— Интернету;
— корпоративной почте и т.д.

Но, поскольку нагрузка на сервер, как правило, значительно больше, чем нагрузка клиентского компьютера, он комплектуется дополнительными компонентами:

— супервайзером – управляющей платой;
— памятью с повышенной устойчивостью к сбоям;
— резервированием:
  — блоков питания,
  — жестких дисков (HDD),
  — оперативной памяти (RAM),
— системой охлаждения.

Разумеется, сервера, используемые в ЦОД, - это специализированные и высокоэффективные устройства, о некоторых особенностях которых будет сказано ниже. Поскольку основной задачей сервера является выполнение вычислительных функций, важнейшая его

характеристика – это быстродействие, определяемое в значительной степени быстродействием процессора. Пути повышения быстродействия процессоров мы обсудим ниже.

2.2. Закон Мура и пределы уменьшения размеров транзисторов

Центральный процессор (также центральное процессорное устройство — ЦПУ, по английски - central processing unit, CPU) — это электронный блок либо интегральная схема (микропроцессор), исполняющая машинные инструкции (код программ) - главная часть аппаратного обеспечения компьютера или сервера. Долгое время единственным ресурсом повышения производительности процессоров считалось увеличение их тактовой частоты f_t. Достигалось это уменьшением длины затвора транзисторов, составляющих элементную базу любого процессора. Чем меньше длина затвора $l_з$, тем меньше время пролета электрона под затвором $t_{пр}= l_з/v$ (где v – скорость электрона) и тем, следовательно выше тактовая частота, обратно пропорциональная времени пролета $f_t=1/t_{пр}$. Именно длина затвора определяла размер самого транзистора. Следовательно, чем меньше длина затвора, тем больше число транзисторов на кристалле микросхемы.

В 1965 году Гордон Мур, будущий основатель корпорации Intel, сформулировал эмпирический закон, получивший его имя: «Число транзисторов на кристаллах микросхем будет удваиваться каждые полтора-два года». И, надо сказать, что на протяжении более, чем 40 лет этот закон работал с высокой степенью точности, что демонстрирует рисунок 6.

Но в 2007 году тот же Гордон Мур заявил: «Закон вскоре перестанет действовать из-за атомарной природы вещества и ограничения скорости света». И, по-видимому, мы как раз на пороге этого события. Дело в том, что у выпускаемых в настоящее время планарных (т.е. плоских) транзисторов фирмы Intel или Samsung длина затвора составляет всего 14 нм, а размер атома кремния – 0,56 нм. Т.е на длине затвора укладывается всего 25 атомов. Заявлено о разработке транзисторов с длиной затвора 10 и даже 7 нм. Очевидно, что повышение тактовой частоты за счет уменьшения длины затвора близко к своему пределу.

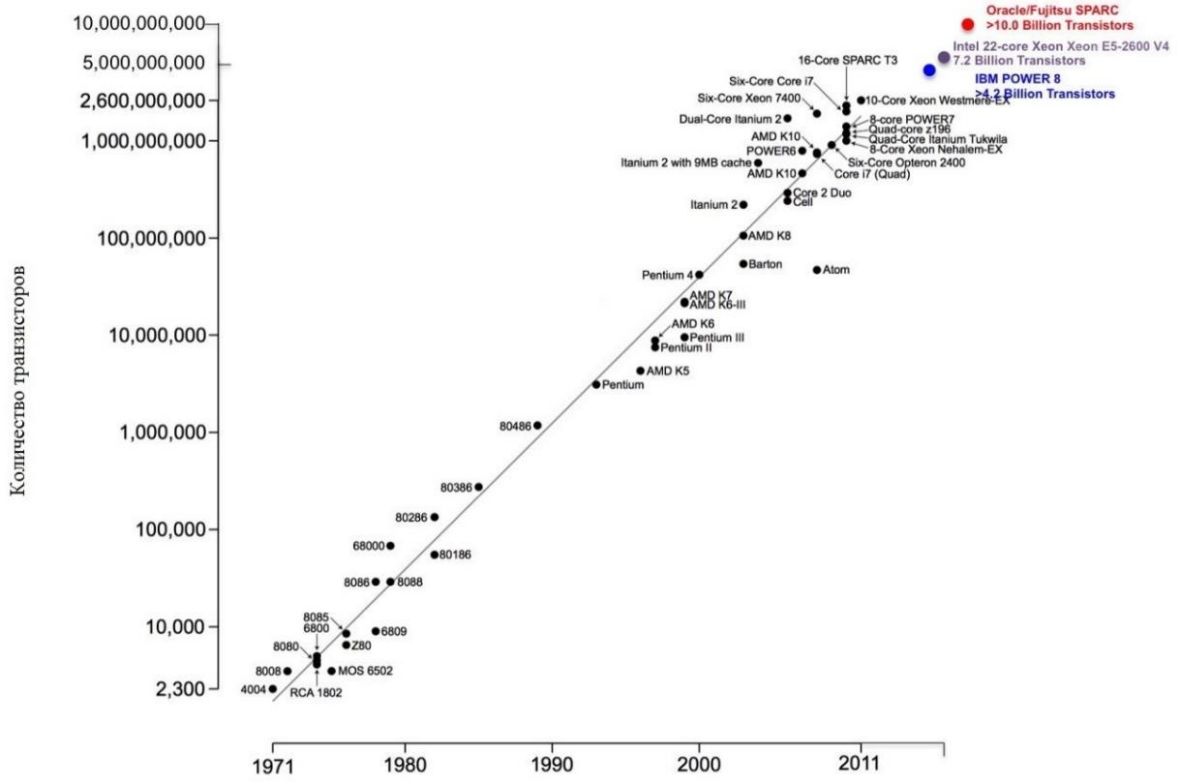

Рисунок 6 - Закон Мура (сплошная линия) и его экспериментальное подтверждение (точки)

Есть ли иные пути повышения тактовой частоты транзисторов? Безусловно, есть. Коль скоро исчерпаны возможности уменьшения длины затвора, представляется естественным сыграть на повышении скорости электронов. Но реализация идей, лежащих на этом пути, сопряжена с рядом трудностей. Не вникая в детали, перечислим некоторые из них.

1.Охлаждение процессора. Известно, что с понижением температуры скорость электронов возрастает, поэтому довольно давно были созданы образцы компьютеров и серверов, процессор которых охлаждается тем или иным образом. И сейчас применяются устройства, действующие на основе эффекта Пельтье, охлаждающие процессор на несколько десятков градусов (при протекании тока через пластину, состоящую из двух разнородных полупроводников, пластина нагревается с одной стороны и охлаждается с другой). Широкого применения такие процессоры не получили, поскольку выигрыш в производительности сопровождался непропорциональным усложнением конструкции, хотя существуют специальные области применения, где подобные конструкции работают. Были попытки построить сервера с процессорами, охлаждаемыми до температуры жидкого азота, но и они себя не оправдали.

2.Использование полупроводниковых материалов с более высокой подвижностью и скоростью электронов. Такие материалы есть, и они даже используются в электронике, но не вычислительной, а в СВЧ-электронике. Это, прежде всего, GaAs, применяемый в монолитных интегральных схемах СВЧ. Но это двухкомпонентный полупроводник, он гораздо дороже кремния и допускает сравнительно малую степень интеграции (порядка десятка активных и пассивных элементов). Это явно недостаточно для интегральных схем вычислительной техники, где интеграция на порядки больше. Есть материалы с еще большей подвижностью электронов, например, InGaAs, но с ними работать еще труднее. Соответственно, у них выше цена и ниже степень интеграции.

3.Использование сложных полупроводниковых структур. Не вдаваясь в детали использования полупроводниковых структур для создания полевых транзисторов, можно указать на гетероструктуру с селективным легированием на основе GaAs/AlGaAs, которая уже используется для создания СВЧ-транзисторов. Успех применения этой структуры основан именно на принципе селективного (т.е выборочного) легирования. Широкозонный AlGaAs легируется сильно, а узкозонный GaAs оставляют по возможности максимально чистым. Стремясь занять положение с минимальной потенциальной энергией, электроны «сваливаются» в узкозонный GaAs, где рассеяние на ионизованных примесях гораздо слабее из-за малой их концентрации. Соответственно, и скорость электронов оказывается выше. Кроме того, электронный газ в GaAs является двумерным (толщина слоя меньше длины волны Де Бройля), что еще больше способствует увеличению подвижности электронов. Проблемы здесь те же, что и у транзисторов на GaAs – высокая цена и малая степень интеграции, но проявляются они еще в большей степени.

4.Применение принципиально новых материалов и новых принципов работы транзисторов. Транзисторы, использующие новые принципы модуляции потока электронов или принципиально новые материалы, предлагаются достаточно регулярно. Большинство из них по ряду причин оказываются недееспособными, и нет смысла их рассматривать. В качестве примера можно указать на транзистор, в котором используется и новый материал, и новый принцип. Как известно, Нобелевская премия 2011 года в области физики была присуждена двум ученым – Андрею Гейму и Константину Новоселову, имеющим российские корни, за открытие и исследование свойств графена – двумерного материала на основе графита. В начале 2012 года в

журнале Science появилось сообщение о разработке опытных образцов вертикальных полевых транзисторов на основе графена. В авторском коллективе – 15 человек, которые представляют семь научных организаций США, Англии, Нидерландов, Португалии и России. Структура транзистора представлена на рисунке 7. Она состоит из двух пленок графена, разделенных слоями диэлектрика, например нитрида бора. Ток возникает в результате туннельного эффекта, когда под действием электрического поля электроны проскакивают из одного слоя графена в другой через изолирующий барьер диэлектрика. Такая конструкция позволяет избавиться от больших токов утечки, характерных для графеновых транзисторов в состоянии покоя. Она требует меньшего напряжения для переключения состояний, а значит, у нее значительно меньшее энергопотребление. Появилось также сообщение исследователей фирмы IBM о создании транзистора с частотой 155 ГГц при длине затвора 40 нм. Работы в этом направлении продолжаются, но пока трудно сказать, возможно ли создание монолитных интегральных схем, а значит и процессоров на этом материале.

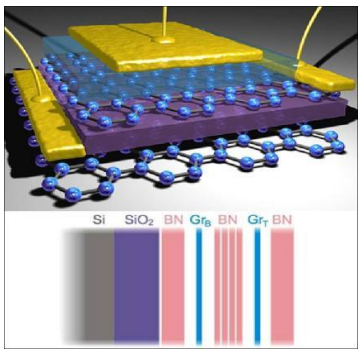

Рисунок 7 - Структура вертикального транзистора на основе графена

2.3. Ситуация в России

В настоящее время в России одной из ведущих компаний по производству микросхем является компания «Ситроникс», объединяющая предприятия «Микрон» и НИИ Молекулярной электроники (НИИМЭ) города Зеленограда. Но по минимальным размерам элементов микросхем (90 нм) «Ситроникс» значительно отстает от лидеров производства интегральных схем, таких, как Intel, AMD или Samsung. Переход к 65-нанометровой технологии планировался давно, но о его реализации сообщения отсутствуют. Поэтому микросхемы, производимые компанией «Ситроникс», не используются в вычислительной технике вообще и в серверном оборудовании в частности. Они находят применение в бесконтактных билетах для метрополитена, банковских картах и т.д.

Однако на рынке производства микропроцессоров появились и новые игроки. Это, прежде всего, ЗАО МЦСТ, работающая в тесном сотрудничестве с Институтом электронных управляющих машин (ИНЭУМ) имени И. С. Брука, известного своими разработками ЭВМ

«Эльбрус-1» (70-е годы прошлого века), «Эльбрус-2» (80-е годы) и «Эльбрус-3» (начало 90-х годов). С 2011 года компания МЦСТ проводит разработку микропроцессоров, линейка которых (получившая также название «Эльбрус) приведена на рисунке 8.

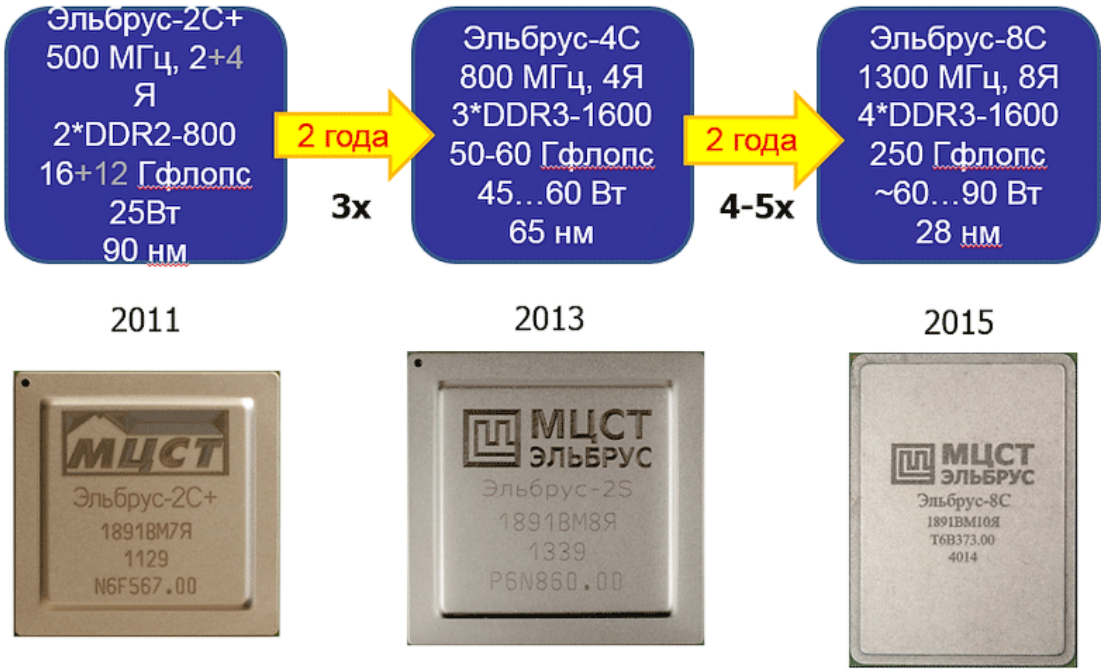

Рисунок 8 - Линейка процессоров «Эльбрус» разработки МЦСТ

Это полностью российская разработка. Архитектура, схемотехника и топология микропроцессора спроектированы специалистами ИНЭУМ и компании ЗАО МЦСТ. Процессор разработан, прежде всего, для использования в компьютерах и серверах Министерства обороны и других государственных учреждений, предъявляющих повышенные требования к защите информации. По оценкам ежегодная потребность в них составляет до 700 000 компьютеров и 300 000 серверов. Хотя производится он на Тайване компанией TSMC (услугами этой компании пользуется, в частности фирма Apple), оригинальная архитектура, схемотехника, а также собственная операционная система (ОС) «Эльбрус» на базе ядра Linux служат надежной защитой от несанкционированных проникновений. Процессор изготовлен по технологии 28 нм. Он имеет следующие параметры:

— рабочая частота – 1,3 ГГЦ;

— число ядер – 8 (см. раздел 2.4);

— число транзисторов – 2,7 млрд;

— производительность – 250 Гфлопс (250 млрд. операций в секунду);

— архитектура - суперскалярная (возможность выполнения на каждом ядре до 30 операций за один машинный такт);

— поддержка режима защищённых вычислений с особым аппаратным контролем целостности структуры памяти.

Здесь ядро – это часть процессора, осуществляющая выполнение одного потока команд. Соответственно, многоядерные процессоры имеют несколько ядер и поэтому способны осуществлять независимое параллельное выполнение нескольких потоков команд одновременно.

Для сравнения отметим, что процессор Intel Core i7-4930K, работающий на частоте 4,2 ГГц, обладает производительностью 140 Гфлопс.

Компания анонсировала выпуск в 2018 году 16-ядерного процессора «Эльбрус-16» с расчетной производительностью 1 Тфлопс.

Следует также отметить еще одну российскую разработку компании «Байкал Электроникс», дочерней компании разработчика суперкомпьютеров ОАО «Т-Платформы» по заказу Минпромторга РФ. Процессоры этой компании производятся в модификациях «M» и «Baikal M/S» для использования в коммуникационном оборудовании, средствах автоматизации (ЧПУ), персональных компьютерах и микросерверах (см. рисунок 9). Процессоры строятся на 64-битном ядре Cortex A-57 британской компании ARM. Как и «Эльбрус», «Байкал» производится на Тайване компанией TSMC по технологии 28 нм. Он также восьмиядерный и имеет суперскалярную архитектуру. Рабочая частота – 2 ГГЦ. ОС разработана на базе свободного ПО Linux. Компания также анонсировала выпуск в 2016 году 16-ядерного процессора по технологии 16 нм. Есть сообщения о том, что компания Lenovo заявила о своих планах выпустить компьютеры на процессоре Baikal.

Рисунок 9 - Процессор «Байкал»

2.4. Процессоры современных серверов

Кроме увеличения тактовой частоты, существуют и иные пути повышения их производительности. Чтобы их проанализировать, отметим, что в настоящее время используются две архитектуры (два принципа построения) процессоров – x86 и ARM. Основное их различие состоит в том, что x86 – это микропроцессоры, чипы которых построены на основе архитектуры CISC (Complex Instruction Set Computing, то есть

"с полным набором инструкций"). Производятся они корпорациями Intel и AMD. С 1993 года процессоры x86 стали первыми суперскалярными (то есть выполняющими несколько операций за такт) и суперконвейерными, где под конвейером понимается способ организации вычислений, используемый в современных процессорах и контроллерах с целью повышения их производительности. В суперконвейерных процессорах в единицу времени выполняется несколько инструкций одновременно.

Современные ARM-процессоры – это также суперскалярные и суперконвейерные микросхемы, но построенные на основе архитектуры RISC - Reduced Instruction Set Computer, то есть с сокращённым набором инструкций. До последнего времени они применялись в телефонах, смартфонах, а ныне – в iPad и iPod.

Казалось бы, что применительно к серверам конкуренции здесь быть не может и "телефонный" процессор никогда не найдет применение в "персоналках", серверах и, тем более, в суперкомпьютерах. Между тем, развитие технологий и причуды рынка привели к ситуации, когда специалисты всерьёз обсуждают возможность конкуренции между процессорами ARM и x86.

Может показаться, что чуть ли не единственное формальное отличие семейств ARM и x86 – это их архитектуры RISC и CISC, соответственно. Однако и это уже нельзя считать принципиальным отличием: сейчас чипы x86 демонстрируют максимальную производительность только с ограниченным набором простых инструкций, который похож на набор RISC-команд. Поэтому сегодняшние x86 можно смело считать CISC-процессорами с RISC-ядрами. Встроенный в микросхему аппаратный транслятор декодирует сложные CISC-инструкции в набор простых внутренних RISC-команд.

2.5. Основные тенденции развития процессоров с архитектурой x86

Основная тенденция в развитии процессоров с архитектурой x86 - увеличение их производительности на единицу потребляемой мощности. Для реализации этой общей тенденции используются следующие технологические и конструктивные приемы.

1. Увеличение мощности и плотности оборудования достигается за счет перехода к многоядерным серверам. Применительно к ЦОД компактность оборудования означает более эффективное использование площади пола, более простое управление, снижение потребляемой мощности и тепловыделения.

2. Уменьшение энергопотребления связано с использованием многоядерных процессоров. Например, двухъядерный процессор Opteron модели 885, предназначенный для многопроцессорных серверов корпоративного класса (до восьми процессоров и, соответственно, 16 ядер), позволяет экономить до 75% электроэнергии, тем самым снижая нагрузку на системы кондиционирования и вентиляции и сокращая общий расход энергии.

3. Объединение двухъядерных процессоров с управлением электропитанием позволяет снизить мощность электропитания слабо загруженных элементов. В процессорах Intel Xeon такого типа производительность на ватт потребляемой мощности оказывается в два-четыре раза выше, чем у предыдущих моделей семейства.

4. Использование более производительных конвейеров, т.е. выполнение большего числа команд за такт работы процессора. В Intel Xeon 5100 каждое ядро выполняет четыре команды одновременно благодаря эффективному 14-этапному конвейеру, ускоряющему передачу данных.

5. Эффективное использование кэш-памяти позволяет одному из исполняющих ядер при простое другого ядра использовать всю кэш-память процессора (Intel Xeon 5100).

6. Динамическое управление питанием в ЦОД реализуется с помощью ПО планирования заданий разработки Intel, распределяющего нагрузку с учетом температуры серверов. В результате создается среда контроля температуры, ведущая мониторинг и управляющая производительностью в масштабе ЦОД.

7. Перенос на процессорный уровень задач, решавшихся на уровне ПО – это дополнение процессоров x86 новой функциональностью, в результате чего часть задач, реализовавшихся ранее на уровне ПО, переносится на процессорный уровень. Например, на процессорном уровне осуществляются такие инструменты управления, как хранение паролей, ключей, цифровых сертификатов и аутентификации. Для серверов это означает более эффективную работу ПО, что позволяет снизить расходы на обслуживание серверов, повысить безопасность и энергоэффективность.

2.6. Виртуализация серверов в ЦОД

Прежде чем перейти от процессоров к серверам, перспективным для использования в ЦОД, рассмотрим технологию виртуализации

серверов, в настоящее время широко применяемую как в коммерческих, так и в корпоративных ЦОД.

Виртуализация заключается в том, что на одном компьютере или сервере создается несколько так называемых виртуальных машин, в каждой из которых может быть своя среда – операционная система (ОС), приложения, настройки и т.п. Эти машины абсолютно изолированы друг от друга и ведут себя как обычные физические компьютеры. Виртуальные машины по заданным правилам сами и без прерывания сессии пользователей способны «переезжать» с одного физического сервера на другой, всегда обеспечивая при этом максимальную производительность и функциональность ЦОД в целом.

Известны, по крайней мере, две причины, по которым виртуализация оказывается чрезвычайно эффективной и полезной. Во-первых, статистика показывает, что при отсутствии виртуализации средняя загрузка серверов в мире не превышает 15-20%, т.е. 80-85% денег, потраченных на формирование серверной инфраструктуры, оказывается израсходованными впустую. К этому следует добавить весьма значительные расходы на электроэнергию и охлаждение серверов.

Во-вторых, для решения каждой новой задачи многие компании используют отдельные серверы, в результате чего количество последних разрастается и становится плохо управляемым. Значительное количество времени и человеческих ресурсов тратится на обслуживание рабочих станций, ликвидацию неисправностей и простоев, возникают сложности с резервным копированием, восстановлением данных и т.д. Очевидно, что оба достоинства данной технологии критически важны для ЦОД, где она применяется достаточно широко.

На первом этапе виртуализация осуществлялась двумя путями: “hosted” и “bare-metal”, различие между которыми иллюстрирует Рисунок 10.

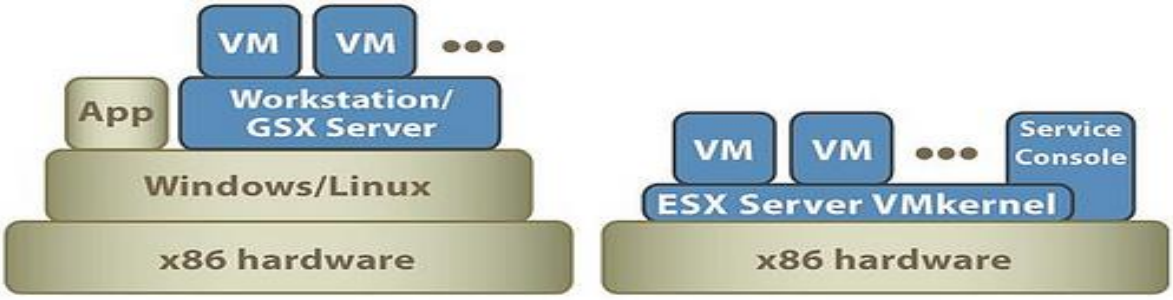

Рисунок 10 - Способы и осуществления виртуализации

В первом случае для запуска виртуальных машин использовалась базовая операционная система (Windows, Linux), а во втором - на “голом железе” запускался так называемый гипервизор, поверх которого создавалось необходимое число виртуальных машин.

Именно второй путь, наиболее полно воплощенный фирмой VMWare, сейчас наиболее распространен. Особенно популярен он стал после того, как компания объявила о доступности для бесплатного скачивания и использования своего гипервизора ESXi. Хотя, справедливости ради, надо отметить, что использование дополнительных функционалов, таких как резервное копирование виртуальных машин или решения по отказоустойчивости все же требуют приобретения дополнительных лицензий и продуктов VMWare.

Безусловные достоинства технологии виртуализации, особенно при ее применении в ЦОД, заключаются в:

— **увеличении коэффициента использования аппаратного обеспечения**, повышении загруженности серверов с 15-20 до 80%, что позволяет получать значительную экономию на оборудовании;

— **уменьшении затрат на замену аппаратного обеспечения,** поскольку виртуальные сервера не привязаны к конкретному оборудованию и при обновлении парка физических серверов не требуется повторная установка и настройка программного обеспечения; виртуальная машина просто копируется на другой сервер;

— **повышении гибкости использования виртуальных серверов,** которые могут быть безболезненно перенесены на другие платформы, когда физический сервер испытывает повышенные нагрузки;

— **обеспечении быстрого восстановления после сбоев и аварий**, т.к. восстановление из резервных копий виртуальных серверов занимает меньшее время и является более простой процедурой, чем физических; при выходе из строя оборудования резервная копия виртуального сервера может быть сразу запущена на другом физическом сервере;

— **повышении управляемости серверной инфраструктуры** за счет использования специальных продуктов управления виртуальной инфраструктурой, позволяющих централизованно обеспечивать балансировку нагрузки и «живую» миграцию;

— **экономии на обслуживающем персонале** вследствие упрощения управления виртуальными серверами и, соответственно, экономии на квалифицированных специалистах, обслуживающих инфраструктуру компании;

— **экономии на электроэнергии,** что особенно актуально для крупных ЦОД, где затраты на поддержание большого парка серверов включают в себя как расходы на электропитание, так и на системы охлаждения.

2.7. Блейд-серверы в ЦОД

2.7.1. Что такое блейд-система и причины ее популярности

Модульные или блейд-серверы впервые появились в 2001 году, однако проблемы надежности, энергопотребления и теплоотвода несколько затормозили их внедрение. В последние годы данный вид серверов приобрел "второе дыхание". Для развития ЦОД чрезвычайно важным оказалось то обстоятельство, что эти тонкие микрокомпьютеры в виде лезвий (отсюда и их название, см. рисунок 11), устанавливаются в специальную блейд-корзину и поддерживают горячую замену (т.е. замену без остановки работы оборудования), не вызывая нарушения в работе остальных компонентов сервера.

Рисунок 11 - Стойка с блейд-серверами компании Dell.

Следующие технические особенности блейд-систем обусловили их широкое применение в информационных технологиях вообще и в ЦОД в частности:

— возможность горячей замены;

— отсутствие кабельных соединений;

— наличие специализированных модулей;

— наилучшее решение с точки зрения масштабируемости (защита инвестиций), но только для продукции одного вендора и в пределах жизненного цикла оборудования;

— каждый блейд-сервер может работать над своей вычислительной задачей, разные модули могут работать под разными ОС;

— хорошее системное ПО для управления ресурсами, разделения нагрузок, горячей замены;

— низкая стоимость обслуживания

— относительно невысокая стоимость;

— низкое энергопотребление и, как следствие, пониженные расходы на кондиционирование.

2.7.2. Специализированные модули блейд-систем

В настоящее время для блейд-систем разработаны следующие специализированные модули:

— **вычислительный модуль**, содержащий один или несколько процессоров (обычно многоядерных), а также, как правило, кэш-память и набор микросхем для проведения вычислений; в функции такого модуля, кроме принятия на себя вычислительной нагрузки, может входить и загрузка ОС после включения блейд-системы;

— **модуль дисковой памяти**, предназначенный для оперативного хранения данных и зачастую дополняемый внешними дисковыми и ленточными системами хранения; благодаря быстрой шине, связывающей все модули в корзине (включая вычислительный модуль), данный модуль обеспечивает производительность, значительно превышающую производительность систем, использующих только внешние СХД;

— **модуль оперативной памяти**, ресурсы которого, благодаря высокоскоростной шине данных в корзине блейд-системы, можно разделять между несколькими вычислительными модулями в соответствии с приложениями, которые выполняются на этих модулях; благодаря виртуализации ресурсов в блейд-системе, выход из строя одной или нескольких микросхем памяти внутри модуля не приводит к его полному отказу и позволяет использовать модуль и дальше, перераспределив оставшуюся память между вычислительными модулями;

— **модуль маршрутизатора/коммутатора**, отвечающий за сетевое взаимодействие блейд-системы с другими серверами и внешними каналами связи; включение модуля маршрутизатора/коммутатора в состав блейд-системы ускоряет обмен данными между отдельными модулями за счет высокоскоростной шины;

— **модуль сетевого интерфейса**, включающий дополнительные аппаратные средства для ускоренного сетевого обмена; этот модуль применяется в тех конфигурациях блейд-системы, где требуется обеспечить особо быстрый обмен данными с локальной сетью предприятия, и он обслуживает все сетевые запросы других блейд-модулей;

— **модуль рабочей станции (PC Blade),** реализующий функционал мощного настольного ПК в виде модуля рабочей станции - аналог «тонкого клиента», позволяющего оставить на рабочем столе пользователя только монитор, мышь и клавиатуру; преимущество такой

системы перед тонкими клиентами в том, что можно использовать ресурсы других блейд-модулей (модулей памяти и т. д.) для поддержки вычислительной мощности PC Blade; модуль обычно используется для поддержки специализированных приложений, например, функционала графической станции.

2.7.3. Технические особенности блейд-систем

1. **Корзина** (или, как ее еще иногда называют, шасси) — основа блейд-системы. Корзина обеспечивает все соединения между модулями, их централизованное питание и охлаждение. Шины данных в корзинах разных вендоров несовместимы, а потому требуют использования модулей того же производителя, что и корзина. Разные вендоры реализовали в корзинах те или иные технические решения (ноу-хау), которые они считают важными конкурентными преимуществами, и не следует ожидать появления недорогих «совместимых» корзин и модулей от различных производителей. В целом такое положение дел не вызывает особых возражений покупателей, так как при использовании в одной корзине модулей от разных производителей было бы сложно гарантировать требуемый уровень надежности и обеспечить фирменный сервис/поддержку.

2. **Коммуникационные порты блейд-систем** выполнены на базе открытых стандартов — InfiniBand, Fibre Channel, Fast Ethernet, iSCSI и Serial Attached SCSI (SAS), поскольку корзины должны обмениваться данными друг с другом на высокой скорости. Конкретный набор коммуникационных портов указан в технической спецификации на корзину.

3. **Модули со специализированными процессорами** обслуживают особые вычислительные потребности, например, используются для ускорения параллельной обработки данных, потоковых приложений, поддержки виртуальной среды. С теоретической точки зрения никаких препятствий для производства блэйд-модулей на базе специальных процессоров нет.

4. **Функция виртуализации** обычно встраивается в ПО блейд-системы, как и ПО управления физическими модулями, хотя для полной поддержки функции виртуализации может потребоваться и дополнительное ПО.

5. **Резервирование N+N** рекомендуется для критически важных модулей, поскольку при наличии резервного модуля ПО управления автоматически переводит на него задачу в случае выхода из строя

основного модуля. Вообще говоря, блейд-модули изначально сконструированы для перераспределения нагрузки на случай, если какой-то модуль в корзине выходит из строя. Но, если модуль данного типа в корзине всего один, то в случае его выхода из строя система не сможет продолжить работу. Поэтому целесообразно резервирование критически важных модулей, таких как модули сетевых соединений, питания и т. д.

6.Мультипроцессорные модули выгодны при большой вычислительной нагрузке, включая параллельную обработку данных. В современных системах они применяются все шире.

7.Модули с многоядерными процессорами обеспечивают, как уже говорилось выше, улучшенное использование ресурсов кэш-памяти. В настоящее время трудно встретить блейд-серверы, построенные на одноядерных процессорах. Как правило, используемые процессоры имеют двухъядерную и более сложную архитектуру.

8.Автоматическое развертывание и удаление приложений обеспечивается включением в комплект поставки блейд-системы ПО для управления системой. Вновь устанавливаемые модули должны быть распознаны системой, и для них должны быть автоматически развернуты те приложения, которые им требуются для работы. Аналогично при удалении из блейд-системы того или иного модуля соответствующее ПО тоже должно быть удалено.

9.Виртуализация нажатием одной кнопки реализована в системах Dell vStart, которая берет на себя решение всех задач ИТ-персонала по проектированию виртуальной инфраструктуры, сборке, интеграции и настройке различных элементов, а также тестирование созданной системы на соответствие требуемым параметрам скорости работы, надежности и возможности масштабирования.

2.7.4. Когда выгодно использование блейд-систем?

«Под проекты»

Развертывание блейд-систем в организациях с унаследованной гетерогенной ИТ-инфраструктурой можно рекомендовать вести «попроектно», т. е. под нужды новых ИТ-проектов и, в первую очередь, — для поддержки тех бизнес-процессов, которые находятся на стадии интенсивного развития и могут потребовать значительного увеличения вычислительной мощности в ближайшем будущем. Как пример подобных приложений можно назвать системы биллинга, обеспечения терминального доступа, Web-сервисы и т. п.

При плановой консолидации вычислительных ресурсов

Консолидация вычислительных ресурсов — одна из ступеней развития ИТ-инфраструктуры организации, движущая сила которой — стремление к повышению безопасности данных и снижению затрат на владение (администрирование серверов, техническое обслуживание, стоимость развертывания и обновления приложений и т. д). Блейд-системы — это очень удачный пример оборудования, которое может успешно решить задачи консолидации вычислительных ресурсов в организациях любого уровня.

Под вновь создаваемые организации и бизнес-проекты

Как крупным организациям, так и малому бизнесу следует обратить внимание на блейд-системы для построения адаптивной ИТ-инфраструктуры, которая позволит гибко реагировать на вызовы рынка. Сегодня в списке моделей блейд-систем ведущих вендоров есть такие, которые ориентированы специально на малый бизнес. Малым компаниям необязательно самим покупать и обслуживать блейд-систему — на рынке имеются достаточно привлекательные предложения хостинга корпоративных приложений малого бизнеса на блейд-системах в ЦОД, принадлежащих системным интеграторам или компаниям, специализирующимся на аутсорсинге ИТ-услуг.

2.8. Микросерверы

Как и многие термины в области ИТ, термин «микросерверы» строго не определен. Иногда под термином «микросервер» в литературе понимают класс серверов, предназначенных для использования в ситуациях, где многоядерная архитектура и виртуализация были бы избыточными, т.е целесообразнее предоставлять пользователям выделенные физические, а не виртуальные ресурсы.

В последние годы микросерверами стали называть специализированные устройства, предназначенные для решения конкретных задач. Терминология не устоялась, и стандарты на понятие «микросерверы» пока не приняты, хотя еще некоторое время назад такая идея активно обсуждалась.

Тем не менее, изделия под названием микросерверы активно продаются. При этом под микросервером обычно понимается горизонтально масштабируемый сервер начального уровня с:

— большим числом процессоров,

— низким энергопотреблением,

— высокой плотностью установки,

— эффективным разделением ресурсов,

который можно быстро конфигурировать и переконфигурировать для любого количества нагрузок в ЦОД, в частности, для облачных приложений.

В некоторой степени микросерверы действительно представляют собой аппаратную альтернативу виртуализации: сервер делится не на виртуальные машины, а на небольшие физические микросерверы, которые можно назначать конкретному приложению. По замыслу разработчиков, в результате будут обеспечиваться более дешевое масштабирование и лучшее соотношение производительности на ватт потребляемой мощности.

В качестве примера можно привести микросерверы компании Dell, которая в 2016 году представляла линейку PowerEdge серии C, рекомендуя ее для провайдеров, желающих максимально увеличить энергоэффективность ЦОД. Это серверы на базе Intel, с 22-нанометровыми процессорами Xeon. Преимуществом данного направления является масштабируемость и гибкость в конфигурации. Микросерверы имеют возможность горячей замены, так как они смонтированы в 3U корпус PowerEdge C5000. Корпус содержит до 12 компактных микросерверов, расположенных на вертикальных салазках. Каждый сервер, в свою очередь, может выполнять поставленную задачу, не завися от другого процессора. Такое выполнение серверов позволяет сократить расходы на обслуживание, уменьшить занимаемую площадь, уменьшить электропотребление сервера и повысить его производительность.

В частности, микросервер PowerEdge C6320 (см. рисунок 12) представляет собой систему из четырех двухпроцессорных серверов с поддержкой до 18 ядер в процессоре семейства Intel Xeon E5 2600 v3 и поддерживает до 16 модулей памяти DIMM суммарной емкостью до 512 Гбайт. Рабочее дисковое пространство обеспечивается поддержкой до 24 2,5-дюймовых или 12 3,5-дюймовых накопителей типа SAS или SATA, либо твердотельных накопителей. Устройства хранения данных или флеш-накопители поддерживают возможность горячей замены в каждом модульном корпусе.

Рисунок 12 - Микросервер PowerEdge C6320

Данная модель оптимизирована для задач создания высокопроизводительных кластеров и решений с горизонтальным

масштабированием для высокопроизводительных вычислений, аналитики и обработки больших объемов данных в режиме реального времени, а также облачных решений. Она также поддерживает большой спектр дополнительного оборудования. Опционально возможна установка встроенного гипервизора и контроллера RAID (см. раздел 3.5), что позволяет расширить функционал модели.

Многие узлы сервера и источники питания имеют возможность горячей замены. Каждый в отдельности взятый микропроцессор установлен на вертикальных салазках, что позволяет сэкономить до 25 процентов места в ЦОД и повысить производительность на 10 процентов. За счёт взаимозаменяемости и простоты в использовании данная модель серверов является очень надёжной и долговечной. Несмотря на относительно малые размеры, сервер может выполнять широкий круг задач и функций.

Следует, однако, отметить, что принцип аппаратного дробления вычислительных ресурсов на большее число серверов оказался менее популярным, чем программное разделение вычислительных ресурсов, т.е. виртуализация. Последняя позволяет обеспечить лучшую балансировку нагрузки, при этом избегая потерь на промежуточные коммуникации.

Более оправданным представляется применение микросерверов для решения узкоспециализированных задач. Подобного рода решения, скорее всего, останутся нишевыми, тогда как программная виртуализация обеспечивает существенно большую гибкость, и за ней, по-видимому, будущее.

Контрольные вопросы

1. Закон Мура и пределы уменьшения размеров транзисторов.
2. Процессоры современных серверов.
3. Основные тенденции развития процессоров с архитектурой x86.
4. Виртуализация серверов в ЦОД.
5. Характеристики блейд-систем.
6. Специализированные модули блейд-систем.
7. Технические особенности блейд-систем.
8. Место микросерверов в архитектуре ЦОД.

3.Системы хранения данных для ЦОД

3.1. Общие положения

Использование современных специализированных систем хранения данных (СХД) вместо сохранения данных непосредственно на дисковых массивах серверов стало одним из важных направлений повышения эффективности ЦОД. Их широкое применение обусловлено следующими обстоятельствами.

1.Удобнее и экономичнее хранить информацию в централизованном виде. В противном случае каждая функциональная система потребует отдельного хранилища. Кроме того, при централизованном хранении легче осуществить поиск необходимой информации.

2. Лавинообразный рост информации, который имеет место в настоящее время, увеличивает число жёстких дисков настолько, что их уже нельзя установить в один сервер. При этом, с одной стороны, невозможно полноценно защитить хранимые данные из-за сложности резервного копирования данных, находящихся на разных серверах и (или) разнесенных территориально. С другой стороны, не обеспечивается высокая скорость обработки информации: даже при достаточно «толстом» канале скорость передачи больших объемов информации ограничена.

3. Сложно или невозможно предугадать требуемый объём дискового пространства при развертывании компьютерной системы. На одном сервере трудно создать память объемом несколько терабайт. Кроме того, в этом случае ресурсы используются неэффективно. Память одного из серверов может быть перегружена, а другого – практически не использована.

4. Распределённые данные имеют низкую степень конфиденциальности. При распределенном характере хранения информации очень трудно проконтролировать и ограничить доступ носителям информации и каналам ее передачи в соответствии с политикой безопасности предприятия.

5. Сложность управления распределёнными потоками информации. Любые действия, направленные на изменение данных в каждом хранилище (например, в филиале), содержащем часть распределённых данных, создает определённые проблемы.

6. Низкий экономический эффект внедрения «классических» решений. По мере роста информационной сети, объёмов данных и всё

более расширяющейся структуре предприятия финансовые вложения оказываются все менее эффективными и, в конце концов, не обеспечивают решение возникающих проблем.

7. Высокие затраты используемых ресурсов. Для поддержания работоспособности информационной системы ЦОД с распределенным хранением информации требуется большой штат квалифицированного персонала, недешёвые аппаратные решения.

Под СХД в дальнейшем мы будем понимать специализированное оборудование и программное обеспечение для надежного хранения и передачи больших массивов информации. Отметим, что хранение данных занимает второе место среди расходов на ИТ.

Современные СХД включают в себя:

— устройства хранения (дисковые массивы, ленточные библиотеки, оптические накопители, SSD);

— инфраструктуру доступа к устройствам хранения;

— подсистему резервного копирования и архивирования данных;

— программное обеспечение управления хранением;

— систему управления и мониторинга всей системы в целом.

3.2. Устройства хранения данных и многоуровневое хранение

В современных СХД используется несколько типов устройств хранения данных. Причем, как это обычно бывает, наиболее эффективные устройства оказываются и наиболее дорогими. Можно выделить несколько наиболее значимых из ныне доступных устройств хранения:

— SSD — твердотельные накопители (Solid State Drive). Это наиболее передовая технология, за которой, по-видимому, будущее, и мы на ней ниже остановимся подробнее. SSD очень производительны, но и пока достаточно дороги. Они, как правило, применяются для активно используемых данных.

— HDD - накопители на жёстких магнитных дисках (Hard Disk Drive). Это устройства хранения информации произвольного доступа, основанные на принципе магнитной записи. Они представляют собой жёсткие (алюминиевые или стеклянные) пластины, покрытые слоем ферромагнитного материала. В HDD используется одна или несколько пластин на одной оси. Считывающие головки в рабочем режиме не касаются поверхности пластин благодаря прослойке набегающего потока воздуха, образующейся у поверхности при быстром вращении, причем именно отсутствие механического контакта обеспечивает сравнительно

долгий срок службы устройства. Массивы из жестких дисков (см. рисунок 13) менее производительны по сравнению с SSD, но эта технология довольно широко используется для первичных систем хранения.

Рисунок 13 - Одна из конструкций массива жестких дисков

— Магнитные ленты имеют наиболее низкую удельную стоимость одного терабайта информации, однако эта технология не позволяет осуществлять выборочный доступ к данным и поэтому в настоящее время не используется в качестве первичного источника хранения. Но они применяются для репликации и архивирования данных.

— Оптические диски CD-ROM (Compact Disc Read Only Memory, компакт-диск с возможностью только чтения) отвечают всем требованиям к долгосрочному архивированию. В отличие от ленточных накопителей, эта технология позволяет осуществлять выборочный доступ к данным и обладает хорошей производительностью, однако, перезапись на эти носители невозможна. Существует также технология CD-RW (Compact Disc-ReWritable, перезаписываемый компакт-диск), допускающая перезапись. Но число циклов записи-перезаписи ограничено.

Как видно из приведенного списка, различные технологии хранения заметно отличаются, как по скорости записи и воспроизведения данных, так и по стоимости. Поэтому в ЦОД обычно используется многоуровневая архитектура хранения (Multi Tier Storage). Она основывается на принципе различной доступности к информации различной важности. Важность информации, в свою очередь, определяется частотой обращения к ней. Существует специальное ПО для управления хранением и иерархическим размещением данных. При внедрении подобного решения вначале анализируется жизненный цикл различных данных. При этом, как правило, выясняется, что доступ к ним и их обновление вначале осуществляется достаточно часто, затем все реже, а спустя какое-то время они вообще почти никому не требуются. Достоинство концепции многоуровневого размещения данных заключается в том, что в ЦОД могут использовать все преимущества различных технологий хранения, оптимизируя их по эффективности и стоимости.

Обычно используют три уровня хранения, каждому из которых предписываются определенные функции. Например, уровень 1 —

«уровень производительности» (Performance Tier) представляет собой первичную инстанцию хранения, состоящую, как правило, из высокопроизводительных и высокодоступных систем жестких дисков, таких как массивы с последовательным интерфейсом, поэтому он оказывается наиболее дорогостоящим. На этом же уровне хранения находятся и SSD. В соответствии с правилами, заданными администратором, ПО для управления хранением автоматически переносит данные на более низкие уровни, однако по-прежнему обеспечивает к ним прозрачный доступ.

Уровень 2, именуемый «уровнем емкости» (Capacity Tier), реализуется с использованием более дешевых систем хранения и обеспечивает большую емкость при меньшей производительности систем (например, массивы с параллельным интерфейсом). Хотя параллельный обмен данными в принципе должен давать б**о**льшие скорости обмена информацией, производительность жестких дисков с параллельным ниже, чем с последовательным за счет меньшей тактовой частоты устройств. На этом уровне все файлы и папки сохраняют свои изначальные имена и структуры, поэтому для чтения данных возможен прямой доступ.

Уровень 3 – «уровень архивирования» (Archive Tier), предназначается для долгосрочного архивирования, реализуется с помощью оптических дисков или ленточных накопителей и поддерживает автономные среды.

Автоматическая миграция между уровнями или в пределах одного из них реализуется на основе правил управления данными в соответствующем программном решении. Независимо от физического места хранения данных такая программа позволяет приложениям осуществлять к ним прозрачный доступ. Потребность в дорогостоящих устройствах первичного хранения сокращается за счет того, что неактивная или редко используемая информация переносится на более дешевые уровни емкости и архивирования.

Благодаря такой разгрузке первичных систем хранения, процессы резервного копирования (Backup) и восстановления (Recovery) завершаются быстрее. В результате не только снижаются затраты на приобретение нового аппаратного оборудования для хранения, но и оптимизируется процесс резервного копирования. Перемещенные данные не приходится сохранять повторно, поэтому сокращается не только требуемый объем ресурсов хранения (к примеру, за счет снижения количества необходимых ленточных накопителей), но и время,

затрачиваемое на создание резервных копий. Кроме того, меньший объем резервных копий и отсутствие необходимости в приобретении дополнительных программных продуктов для интеграции систем с ленточными и оптическими накопителями приводят к заметному сокращению расходов. Немалый выигрыш владельцы ЦОД получают также от сокращения трудозатрат на администрирование систем.

3.3. Твердотельный накопитель SSD – перспективное устройство хранения информации

SSD (Solid State Drive) или твердотельный накопитель - устройство для постоянного хранения данных с использованием твердотельной (обычно - флэш) памяти (см. рисунок 14). Эти накопители все шире применяются в СХД, в том числе, в ЦОД. Поэтому остановимся подробнее на этих устройствах.

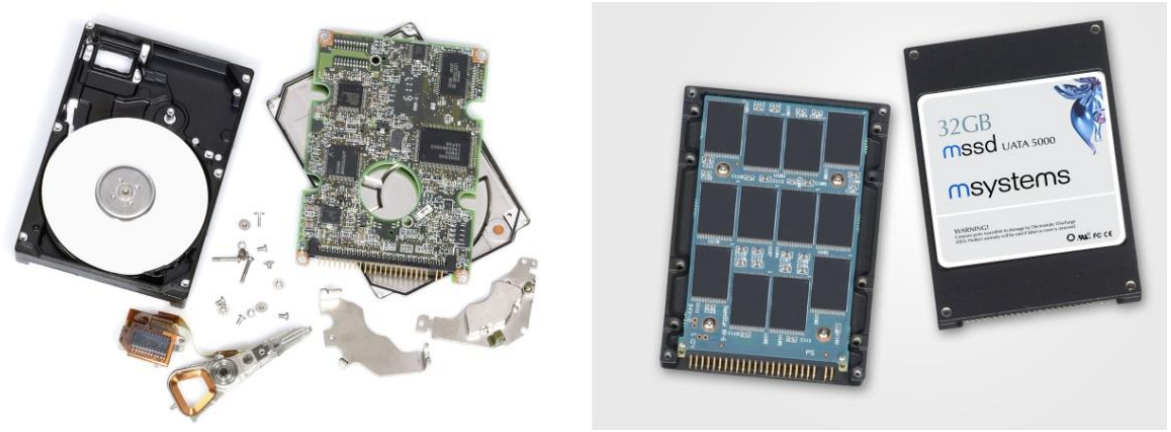

Рисунок 14 - Дисковый и твердотельный накопители в разобранном состоянии

Первые твердотельные накопители, использующие флэш-память, появились в 1995 году и изначально были ориентированы на применение в военной и аэрокосмической технике, где исключительно высокая стоимость подобных устройств в расчёте единицу объема хранимых данных компенсировалась высокой надёжностью и уникальной способностью функционировать в условиях экстремальных температур, вибраций и перегрузок.

Преимущества SSD перед HDD состоят в следующем:

— более быстрый переход в рабочее состояние, поскольку не требуется раскрутка шпинделя;

— очень быстрый случайный доступ к данным из-за отсутствия необходимости перемещать блок головок и, вследствие этого, более быстрые загрузка системы и запуск приложений;

— отсутствие шума при отсутствии внутренних вентиляторов для охлаждения;

— более низкое энегопотребление и, следовательно, тепловыделение (только для SSD небольших объёмов);

— высокая механическая надёжность вследствие отсутствия движущихся частей;

— лучшая способность переносить экстремальные внешние условия - перегрузки, вибрации, перепады давления и температуры, что важно в специальных областях применения, в ноутбуках и другой мобильной электронике;

— постоянная производительность по всему объёму хранения, связанная с постоянным временем поиска данных;

— относительно низкий вес и размеры для SSD относительно низкой ёмкости.

Недостатки SSD:

— высокая, хотя и постоянно снижающаяся, цена;

— меньшая, хотя и быстро растущая ёмкость;

— большая уязвимость к внезапному отключению питания, магнитным полям, статическому электричеству;

— ограниченное число циклов записи для SSD на базе флэш-памяти - до 300 – 500 тысяч операций стирания/записи в одну и ту же ячейку, что отчасти компенсируется специальными алгоритмами динамического распределения часто перезаписываемых кластеров равномерно по диску ("выравнивание износа").

— меньшая скорость записи в силу конструктивных особенностей флэш-памяти, допускающей стирание только достаточно большими блоками, что сильно снижает скорость случайной записи.

В последнее время кроме одноуровневых SSD (SLC - Single Level Cells) стали использоваться SSD с многоуровневой структурой ячеек MLC (Multi-Level Cells),под которыми подразумевается двухуровневая структура с возможностью записи двух бит информации в одну ячейку и даже Triple Level Cells(TSL), соответственно, трехуровневая структура ячеек. Многоуровневые структуры ячеек памяти имеют очевидное преимущество: на той же микросхеме памяти можно разместить больше информации. Это приводит к значительному снижению цены за 1 Гб пространства на таких накопителях, а также наращивать суммарный объем SSD.

Но SSD типа MLC и TLC гораздо больше подвержен ошибкам, которые отследить труднее, из-за чего снижается скорость работы

устройства и его надежность. Число циклов перезаписи для MLC SSD составляет примерно 3-5 тысяч.

3.4. Типы соединения СХД с вычислительными системами

3.4.1. Прямое подсоединение памяти к серверу

DAS (direct-attached storage) — устройство внешней памяти, напрямую подсоединенное к основному серверу или компьютеру и используемое только им. Простейший пример DAS — встроенный жесткий диск.

Конфигурация DAS приемлема для применений, нетребовательных к объемам, производительности и надежности систем хранения. DAS не обеспечивает возможности совместного использования емкости хранения разными серверами или рабочими станциями и, тем более, возможности разделения данных. Это относительно дешевый способ подсоединения устройств хранения, однако, для больших организаций, его нельзя считать оптимальным. Много DAS-подключений означает разрозненные и разбросанные по всей компании островки внешней памяти, избытки которой не могут использоваться другими серверами или компьютерами, что приводит к неэффективной трате емкости хранения в целом (см. рисунок 15).

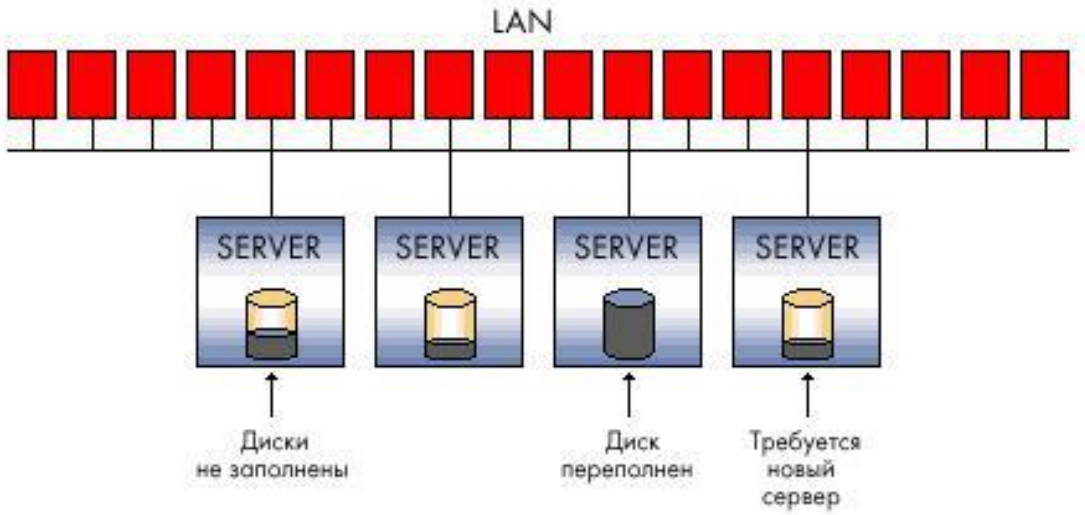

Рисунок 15 - DAS схема подключения СХД

Кроме того, при такой организации хранения нет никакой возможности создать единую точку управления внешней памятью, что неизбежно усложняет процессы резервирования/восстановления данных и создает серьезную проблему защиты информации. В итоге общая стоимость владения подобной системой хранения может оказаться значительно выше, чем более сложная, на первый взгляд, и изначально более дорогая сетевая конфигурация.

В последние годы интерес к DAS схемам вновь возродился в связи с созданием систем программно-определяемого хранения (раздел 0) и необходимостью хранения «больших данных» (см. раздел 11.3).

3.4.2. Сетевое хранение данных

В настоящее время более широко используются сети хранения данных — SAN (storage area network). SAN представляет собой выделенную сеть устройств хранения, которая позволяет множеству серверов использовать совокупный ресурс внешней памяти без нагрузки на локальную сеть.

В сеть хранения могут подключаться дисковые массивы RAID (см. раздел 3.5), ленточные или оптические библиотеки для резервирования и архивирования данных. Основными компонентами для организации сети SAN, помимо самих устройств хранения, являются адаптеры для подключения серверов к сети, устройства поддержки топологии сети и специализированное ПО для управления сетью хранения. ПО может размещаться как на сервере общего назначения, так и на самих устройствах хранения, хотя иногда часть функций выносится на специализированный тонкий сервер для управления сетью хранения.

Задача программного обеспечения для SAN — это, прежде всего, централизованное управление сетью хранения, включая конфигурирование, мониторинг, контроль и анализ компонентов сети. Одной из наиболее важных является функция управления доступом к дисковым массивам, если в SAN хранятся данные разнородных серверов. Сети хранения обеспечивают одновременный доступ множества серверов к множеству дисковых подсистем, Привлекательность сетей хранения объясняется преимуществами, возникающими при работе с большими объемами данных. Выделенная сеть хранения разгружает основную (локальную или глобальную) сеть вычислительных серверов и клиентских рабочих станций, освобождая ее от потоков ввода/вывода данных (см. рисунок 16).

Этот фактор, а также высокоскоростная среда передачи, используемая для SAN, обеспечивают повышение производительности процессов обмена данными с внешними системами хранения. SAN означает консолидацию систем хранения, создание на разных носителях единого пула ресурсов, который разделяется всеми вычислительными мощностями, и в результате необходимую емкость внешней памяти можно обеспечить меньшим числом подсистем. В SAN резервирование данных с дисковых подсистем на ленты происходит вне локальной сети и потому становится более производительным — одна ленточная

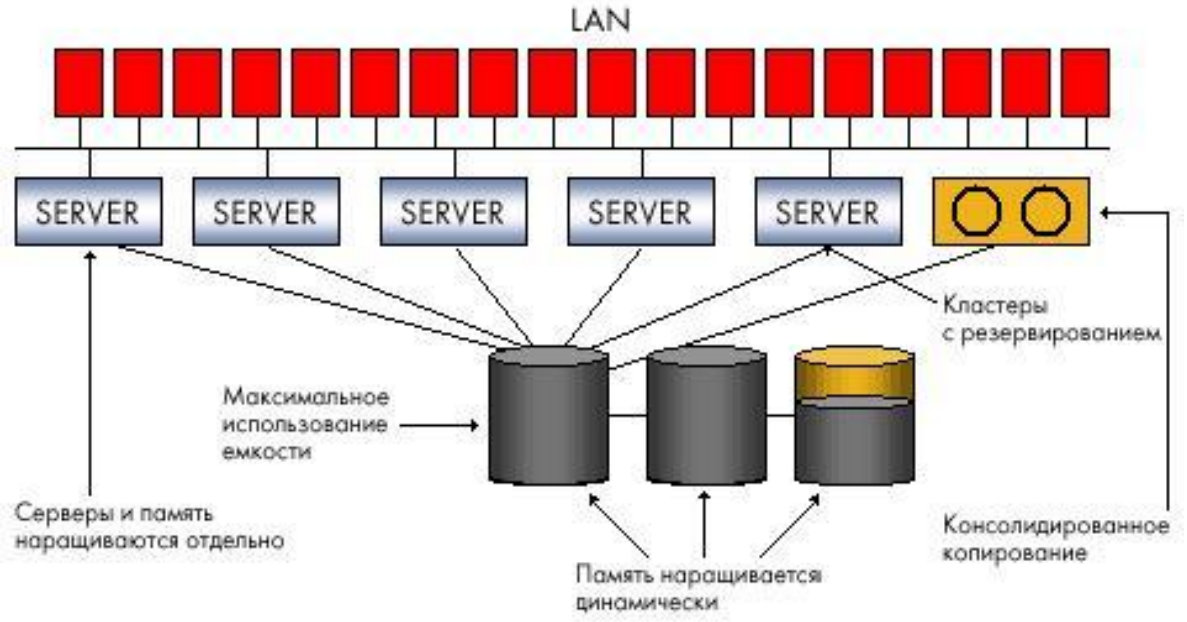

Рисунок 16 - Схема организации сети хранения SAN

библиотека может служить для резервирования данных с нескольких дисковых подсистем. Кроме того, при поддержке соответствующего ПО можно реализовать прямое резервирование в SAN без участия сервера, тем самым разгружая процессор. Возможность разнесения серверов и памяти на большие расстояния отвечает потребностям повышения надежности корпоративных хранилищ данных. Консолидированное хранение данных в SAN лучше масштабируется, поскольку позволяет наращивать емкость хранения независимо от серверов и без прерывания их работы. Наконец, SAN дает возможность централизованного управления единым пулом внешней памяти, что упрощает администрирование.

Безусловно, сети хранения, недешевое и непростое решение, причем, совместимость устройств организации SAN от разных производителей не гарантируется. Поэтому могут возникнуть дополнительные расходы на организацию выделенной сети и покупку управляющего ПО, в результате чего начальная стоимость SAN в крупной компании окажется выше организации хранения с помощью DAS, однако совокупная стоимость владения должна все-таки оказаться ниже.

3.4.3. Файловый сервер хранения NAS

В отличие от SAN, NAS (network attached storage) — не сеть, а сетевое устройство хранения, точнее, выделенный файловый сервер с подсоединенной к нему дисковой подсистемой. Иногда в конфигурацию NAS может входить оптическая или ленточная библиотека. NAS-

устройство (NAS appliance) напрямую подключается в сеть и предоставляет клиентским станциям доступ к файлам на своей интегрированной подсистеме внешней памяти.

NAS-устройство напоминает конфигурацию DAS (см. рисунок 17), но принципиально отличается от нее тем, что обеспечивает доступ на уровне файлов, а не блоков данных, и позволяет всем приложениям в сети совместно использовать файлы на своих дисках. Запрос к NAS-устройству не определяет том или сектор на диске, где находится файл. Задача операционной системы NAS-устройства транслировать обращение к конкретному файлу в запрос на уровне блоков данных. Файловый доступ и возможность разделения информации удобны для приложений, которые должны обслуживать множество пользователей одновременно, но не требуют загрузки очень больших объемов данных по каждому запросу. Поэтому обычной практикой становится использование NAS для Internet-приложений, Web-служб или САПР, в которых над одним проектом работают сотни специалистов.

Рисунок 17 - Сетевое устройство хранения - NAS

Вариант NAS прост в установке и управлении. В отличие от сети хранения, установка NAS-устройства не требует специального планирования и затрат на дополнительное управляющее ПО — достаточно просто подключить файловый сервер в локальную сеть. NAS освобождает серверы в сети от задач управления хранением, но не разгружает сетевой трафик, поскольку обмен данными между серверами общего назначения и NAS идет по той же локальной сети. На NAS-устройстве может быть сконфигурирована одна или несколько файловых систем, каждой из которых отводится определенный набор томов на диске. Всем пользователям одной и той же файловой системы по требованию выделяется некоторое дисковое пространство. Таким образом, NAS обеспечивает более эффективные по сравнению с DAS организацию и использование ресурсов памяти.

3.4.4. Что выбрать, SAN или NAS?

Ответ на вопрос, сформулированный в подзаголовке, зависит от возможностей и потребностей организации, однако сравнивать или тем более противопоставлять их в принципе неверно, поскольку эти две конфигурации решают разные задачи. Файловый доступ и совместное использование информации для приложений на разнородных серверных

платформах в локальной сети — это NAS. Высокопроизводительный блоковый доступ к базам данных, консолидация хранения, гарантирующая его надежность и эффективность, разрешение проблем, связанных с интенсивными процедурами резервного копирования и обмена данными путем перенесения всей системы в выделенную подсеть — это SAN.

Сеть хранения позволяет создать единый пул ресурсов памяти и выделять на физическом уровне необходимую квоту дискового пространства каждому из хостов, подключенных к SAN. NAS-сервер обеспечивает разделение данных в файловой системе приложениями на разных операционных платформах, решая проблемы интерпретации структуры файловой системы, синхронизации и контроля доступа к одним и тем же данным.

3.5. Повышение надежности хранения информации путем создания RAID-массивов

Как указывалось в разделе 3.2, основная информация в современных СХД хранится на дисковых массивах. Эти массивы организуются в так называемые RAID-системы, где аббревиатура RAID расшифровывается как Redundant Array of Independent Disks — избыточный массив независимых дисков. Изначально RAID расшифровывался как Redundant Array of Inexpensive Disks — избыточный массив недорогих дисков. Под недорогими подразумевались диски, предназначенные для использования в персональных компьютерах (ПК), в противовес дорогим дискам для мэйнфреймов. Но так как вскоре в RAID-массивах стали использовать диски, стоимостью существенно выше, чем в большинстве компьютеров, слово «недорогой» было заменено на «независимый», но аббревиатура была сохранена.

Принцип функционирования RAID-системы заключается в следующем: из набора дисковых накопителей создается массив, который управляется специальным контроллером и определяется компьютером как единый логический диск большой емкости. За счет параллельного выполнения операций ввода-вывода обеспечивается высокое быстродействие системы, а повышенная надежность хранения информации достигается дублированием данных или вычислением контрольных сумм.

Различают несколько основных уровней RAID-массивов: RAID 0, 1, 2, 3, 4, 5, 6, 7. Также существуют комбинированные уровни, такие как RAID 10, 0+1, 30, 50, 53 и т.п. Мы коротко рассмотрим только пять

основных уровней, чтобы пояснить принцип формирования и функционирования подобных систем.

3.5.1. RAID 0 - дисковый массив без отказоустойчивости (Striped *Disk Array without Fault Tolerance)*

RAID 0 – это дисковый массив без избыточного хранения данных. Информация разбивается на блоки, которые одновременно записываются на отдельные диски, что обеспечивает повышение производительности (см. рисунок 18). Такой способ хранения информации ненадежен, поскольку поломка одного диска приводит к потере всей информации, поэтому уровнем RAID как таковым не является.

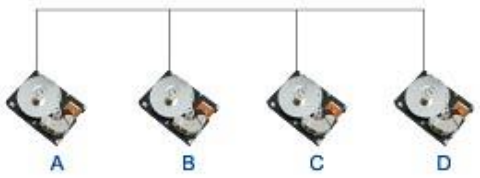

Рисунок 18 – Организация дискового массива RAID 0

За счет возможности одновременного ввода/вывода с нескольких дисков массива RAID 0 обеспечивает максимальную скорость передачи данных и максимальную эффективность использования дискового пространства, так как не требуется места для хранения контрольных сумм. Реализация этого уровня очень проста. RAID 0, как правило, применяется в тех областях, где требуется быстрая передача большого объема данных. Разумеется, для реализации массива требуется не меньше двух дисков.

Преимущества:

— наивысшая производительность в приложениях, требующих интенсивной обработки запросов ввода/вывода и данных большого объема;

— простота реализации;

— низкая стоимость;

— максимальная (стопроцентная) эффективность использования дискового пространства.

Недостатки:

— не является «настоящим» RAID-массивом, поскольку не поддерживает отказоустойчивость;

— отказ одного диска влечет за собой потерю всех данных массива.

3.5.2. RAID 1 - дисковый массив с зеркалированием (Mirroring & *Duplexing)*

RAID 1 – это дисковый массив с полным дублированием (зеркалированием) информации. В простейшем случае два накопителя содержат одинаковую информацию и являются одним логическим

диском (см. рисунок 19). При выходе из строя одного диска его функции выполняет другой. Естественно, что для реализации массива требуется не меньше двух дисков.

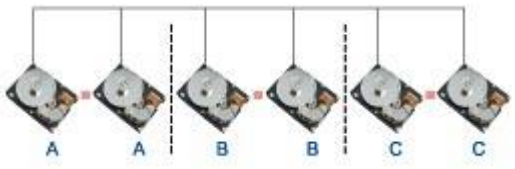

Рисунок 19 – Организация RAID 1 – простейшего отказоустойчивого массива

Преимущества:

— простота реализации;

— простота восстановления массива в случае отказа (копирование).

Недостатки:

— высокая стоимость, благодаря 100-процентной избыточности;

— невысокая скорость передачи данных.

3.5.3. RAID 2 - отказоустойчивый дисковый массив с использованием кода Хемминга (Hamming Code ECC)

Схема резервирования данных с использованием кода Хэмминга (Hamming code) для коррекции ошибок. Поток данных разбивается на слова — причем размер слова соответствует количеству дисков для записи данных. Для каждого слова вычисляется код коррекции ошибок, который записывается на отдельную группу дисков, выделенных для хранения контрольной информации (см. рисунок 20). Их число равно количеству бит в слове контрольной суммы.

RAID 2 — один из немногих уровней, позволяющих обнаруживать двойные ошибки и исправлять "на лету" одиночные. При этом он является самым избыточным среди всех уровней с контролем четности. Эта схема хранения данных не получила коммерческого применения, поскольку плохо справляется с большим количеством запросов, но используется для ряда специфических применений, когда важно обнаружение двойных ошибок и исправление "на лету" одиночных.

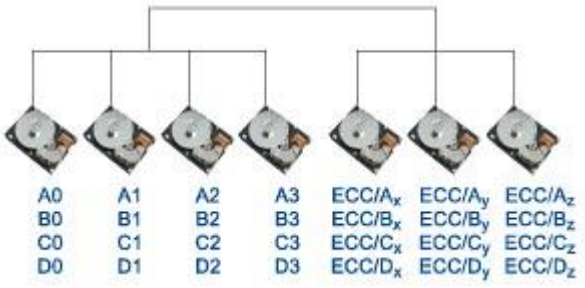

Рисунок 20 - Организация RAID 2 с использованием кода Хемминга

Преимущества:

— достаточно простая реализация;

— коррекция ошибок "на лету";

— очень высокая скорость передачи данных;

— уменьшение накладных расходов при увеличении количества дисков.

Недостатки:

— низкая скорость обработки запросов;

— высокая стоимость;

— большая избыточность.

3.5.4. RAID 3 - отказоустойчивый дисковый массив с параллельной передачей данных и четностью (Parallel Transfer Disks with Parity)

Отказоустойчивый массив с параллельным вводом/выводом данных и диском контроля четности. Поток данных разбивается на порции на уровне байт (хотя возможно и на уровне бит) и записывается одновременно на все диски массива, кроме одного (см. рисунок 21). Один диск предназначен для хранения контрольных сумм, вычисляемых при записи данных. Поломка любого из дисков массива не приводит к потере информации.

Рисунок 21 - Организация отказоустойчивого дискового массива RAID 3; поток данных разбивается на байты и записывается на все диски, кроме одного

Этот уровень имеет намного меньшую избыточность, чем RAID 2. За счет разбиения данных на порции RAID 3 имеет высокую производительность. Поскольку при каждой операции ввода/вывода производится обращение практически ко всем дискам массива, то одновременная обработка нескольких запросов невозможна.

Этот уровень подходит для приложений с файлами большого объема и малой частотой обращений (в основном это сфера мультимедиа). Использование только одного диска для хранения контрольной информации объясняет тот факт, что коэффициент использования дискового пространства достаточно высок (как следствие этого — относительно низкая стоимость). Для реализации массива требуется не меньше трех дисков.

Преимущества:

— отказ диска мало влияет на скорость работы массива;

— высокая скорость передачи данных;

— высокий коэффициент использования дискового пространства.

Недостатки:

— сложность реализации;

— низкая производительность при большой интенсивности запросов данных небольшого объема.

3.5.5. RAID 4 - отказоустойчивый массив независимых дисков с общим диском четности (Independent Data Disks with Shared Parity Disk)

Этот массив очень похож на уровень RAID 3. Отличие состоит в том, что поток данных разделяется не на уровне байтов, а на уровне блоков информации, каждый из которых записывается на отдельный диск. После записи группы блоков вычисляется контрольная сумма, которая записывается на выделенный для этого диск (Рисунок 22).

Рисунок 22 - Организация отказоустойчивого дискового массива RAID 4; поток данных разбивается на блоки и записывается на все диски, кроме одного

У RAID 4 возможно одновременное выполнение нескольких операций чтения. Этот массив повышает производительность передачи файлов малого объема (за счет распараллеливания операции считывания). Но, поскольку при записи должна изменяться контрольная сумма на выделенном диске, одновременное выполнение операций невозможно (налицо асимметричность операций ввода и вывода). Этот уровень имеет почти все недостатки RAID 3 и не обеспечивает преимущества в скорости при передаче данных большого объема. Схема хранения разрабатывалась для приложений, в которых данные изначально разбиты на небольшие блоки, поэтому нет необходимости разбивать их дополнительно. Эта схема хранения данных имеет невысокую стоимость, но ее реализация достаточно сложна, как и восстановление данных при сбое.

Преимущества:

— высокая скорость передачи данных;

— отказ диска мало влияет на скорость работы массива;

— высокий коэффициент использования дискового пространства.

Недостатки:

— достаточно сложная реализация;

— очень низкая производительность при записи данных;

— сложное восстановление данных.

3.5.6. RAID 5 - отказоустойчивый массив независимых дисков с распределенной четностью (Independent Data Disks with Distributed Parity Blocks)

Самый распространенный уровень. Блоки данных и контрольные суммы циклически записываются на все диски массива, отсутствует выделенный диск для хранения информации о четности, нет асимметричности конфигурации дисков (Рисунок 23).

В случае RAID 5 все диски массива имеют одинаковый размер — но один из них невидим для операционной системы. В общем случае полезная емкость массива из N дисков равна суммарной емкости N–1 диска.

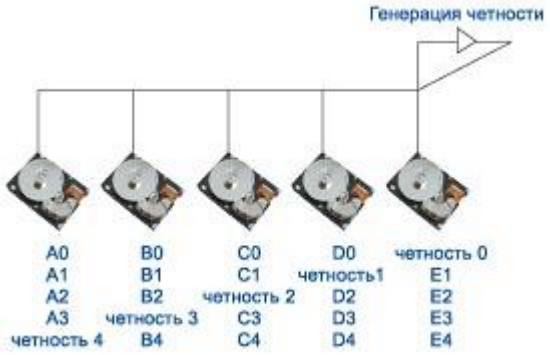

Рисунок 23 - Организация RAID 5 – массив независимых дисков с распределенной четностью

Самый большой недостаток уровней RAID от второго до четвертого — это наличие отдельного диска (или дисков), хранящего информацию о четности. Скорость выполнения операций считывания достаточно высока, так как не требует обращения к этому диску. Но при каждой операции записи на нем изменяется информация, поэтому схемы RAID 2-4 не позволяют проводить параллельные операции записи. RAID 5 не имеет этого недостатка, так как контрольные суммы записываются на все диски массива, что делает возможным выполнение нескольких операций чтения или записи одновременно. RAID 5 имеет достаточно высокую скорость записи/чтения и малую избыточность.

Преимущества:

— высокая скорость записи данных;

— достаточно высокая скорость чтения данных;

— высокая производительность при большой интенсивности запросов чтения/записи данных;

— высокий коэффициент использования дискового пространства.

Недостатки:

— низкая скорость чтения/записи данных малого объема при единичных запросах;

— достаточно сложная реализация;

— сложное восстановление данных.

3.6. Инновационные технологии, применяемые в современных классических СХД

Отметим некоторые инновационные технологии, применяемые в современных классических СХД, представляющие интерес с точки зрения их применения в ЦОД. В качестве примера взяты СХД двух мировых лидеров их разработки и производства – компаний Dell EMC и Hewlett Packard.

1. Широкое применение SSD (см. раздел 3.3). Это обеспечивает малое время отклика, снижение энергопотребления на одну операцию ввода-вывода, уменьшение веса в расчете на 1Тб хранения, повышение надежности из-за отсутствия подвижных деталей и ускорения восстановлений RAID.

2. Технология «spin-down», снижающая скорость вращения дисков при неактивной (например, в ночное время) системе. Это позволяет дополнительно снижать энергопотребление СХД в целом, даже с учетом того, что в системе применяются диски с пониженным энергопотреблением.

3. Постоянный обмен данными между кэш-памятью и первыми пятью дисками, содержащими управляющее ПО и структуру данных. Это обеспечивает их сохранность при отказе по питанию в течение любого промежутка времени.

4. Включение ПО виртуализации в управляющее программное обеспечение.

5. Использование специального ПО, позволяющего применять различные механизмы репликации данных как на локальные, так и на удаленные площадки в однородных и гетерогенных средах, осуществлять исторический анализ производительности массива, гибкое управление путями от массива к серверам.

6. Построение СХД по модульному принципу, который позволяет поддерживать «горячую замену». При появлении новых стандартов обеспечивается полная защита инвестиций, поскольку достаточно добавить/заменить модуль для того, чтобы обеспечить поддержку новых стандартов.

7. Механизм проактивной замены диска (pro-active hot sparing) позволяет точно определить диск, который выйдет из строя в ближайшее время, и начать перенос данных на резервный диск без остановки сервисов и деградации производительности.

8. Технологии переноса данных между физическими дисками и добавления физических дисков без остановки сервисов.

9. Подтверждение готовности системы 99,999%, что означает не более трех минут незапланированного и запланированного простоя за год эксплуатации.

10. Разработка, оптимизация и встраивание в контроллерную пару специализированного ПО управления под конкретную СХД.

11. Возможность самостоятельной установки, настройки и подключения СХД заказчиками без привлечения сертифицированных специалистов.

12. Реализация страйпинга (технологии виртуализации, распараллеливания операций ввода/вывода) по большому количеству дисков, ограниченному только максимальным количеством дисков которые можно установить в массив.

13. Использование виртуальных выделенных резервных дисков вместо физических. Емкость виртуальных дисков равномерно распределена по всем дискам дисковой группы. Данная технология позволяет использовать все физические диски для увеличения производительности и существенно сократить время восстановления данных после сбоя.

14. Автоматическое и динамическое увеличение и уменьшение емкости томов, упрощающее администрирование и позволяющее более эффективно расходовать дисковые ресурсы массива.

15. Возможность в пределах одной дисковой группы создавать логические тома с разным уровнем RAID, что позволяет более эффективно расходовать дисковые ресурсы, поскольку, не требуется создавать отдельную дисковую группу для нового уровня RAID.

16. Выполнение многих операций на уровне микрокода, в результате чего для конфигурирования массива данных требуется меньше времени по сравнению с любым другим дисковым массивом.

3.7. Новые принципы построения современных СХД

3.7.1. Горизонтально масштабируемые СХД

В последние годы активно развивается рынок горизонтально масштабируемых СХД, называемых также gridstorage или кластерными системами, которые отличаются высокой масштабируемостью и управляемостью. Ведущие компании, в числе которых EMC, HP и IBM, заявили о своих продуктах в области этого технического решения.

При разработке данных СХД ставилась цель создания систем с наименьшей стоимостью хранения, управления и обслуживания как на единицу емкости, так и на единицу производительности. Одновременно

эти системы должны были просто и максимально масштабироваться как по емкости (до сотен и более терабайт), так и по производительности. Для достижения этих целей использовались стандартные массово производимые серверы (блейд-серверы) в комплекте с дисками с последовательным и параллельным считыванием информации. При этом интегрируются десятки или даже сотни серверов, что позволяет достичь массового параллелизма при организации доступа к данным и практически линейной масштабируемости по производительность. Интегрирующая компонента в таких системах – это, в основном, ethernet/infiniband свитчи. Соответственно, вся основная функциональность в таких системах привносится программным обеспечением, а не специализированными аппаратными компонентами (блоками, контроллерами) в модульных и монолитных системах хранения.

Представленные на рынке системы хранения с горизонтальным масштабированием значительно отличаются как по позиционированию (high-end, средний или мелкий бизнес различного профиля), способа доступа к данным (блоковый, файловый), надежности исходных компонентов и т.д. Особенно актуальны СХГМ при использовании в программно-определяемых системах хранения (раздел 0).

3.7.2. Блочная дедупликация в системах резервного копирования

При традиционном копировании данных на высокопроизводительные дисковые системы эти достаточно дорогие устройства используются неэффективно за счет постоянного накопления избыточной информации. Эта избыточность возникает из-за того, что данные в информационных системах часто дублируются, причем одни и те же блоки данных могут присутствовать в самых разных системах, например на почтовых серверах (особенно, если одни и те же файлы рассылаются сразу многим получателям), в файловых системах различных компьютеров, в базах данных. В традиционном варианте резервного копирования эта избыточность только увеличивается. В результате объем хранимых резервных копий может превышать объем продуктивных данных в 10-20 раз, притом, что различия между двумя копиями могут составлять единицы процентов.

Для решения этой проблемы уже достаточно давно используется технология дедупликации данных, в основе которой лежит выделение уникальных блоков данных, сохраняемых только один раз. Хотя такие

решения присутствуют на рынке достаточно давно, в последнее время интерес к ним растет лавинообразно.

Существуют две основные технологии дедупликации данных на блочном уровне – в источнике, т.е. на клиентах системы резервного копирования и на целевом устройстве (в самой системе резервного копирования). Компания EMC предлагает реализацию обоих подходов в своих решениях EMC Avamar и EMC Data Domain соответственно.

В EMC Avamar используется дедупликация в источнике, что позволяет резко уменьшить объем данных до передачи в сеть и достичь 500-кратного снижения загрузки сети и 20-кратного снижения емкости устройств хранения данных резервного копирования. Специальный патентованный алгоритм разбивает исходные данные на блоки переменной длины, пытаясь выделить как можно больше одинаковых блоков. Клиенты системы передают только уникальные блоки, еще не содержащиеся в хранилище. Если же блок уже содержится в хранилище, то передается только метаинформация о том, что данный блок существует и на данном клиенте.

В EMC Data Domain дедупликация закладывалась изначально. В них используется наиболее эффективный алгоритм дедупликации на уровне блоков данных переменной длины, позволяющий сократить объем хранилища резервных копий в десятки раз по сравнению с традиционными решениями. Система поддерживает дедупликацию «на лету» (inline), за счет чего достигается более эффективное (в разы) использование дискового пространства по сравнению с системами, использующими отложенную репликацию. Она обеспечивает наилучшие показатели по производительности при резервном копировании и восстановлении. Продуктовая линейка Data Domain включает ряд моделей от ориентированных на удаленные офисы до предназначенных для использования в крупных ЦОД.

3.7.3. Программно-определяемое хранение

Одним из актуальных направлений в индустрии хранения стало программно-определяемое (или программируемое) хранение - Software Defined Storage (SDS). Этот термин отражает общую тенденцию постепенного внедрения концепции «программно-определяемого ЦОД» (Software Defined Data Center, SDDC), которая будет рассмотрена в разделе 6.

Строгого определения SDS пока не существует, но обычно под программно-определяемым хранением понимают группу программ для хранения данных, работающую на серверах с процессорами x86,

гипервизорах и в облаках, которая должна независимо от оборудования с помощью виртуализации дисковых ресурсов обеспечивать полный набор используемых для хранения сервисов хранения (включая дедупликацию, репликацию и динамическое выделение ресурсов).

В системах, реализующих концепцию SDS, отсутствуют какие-либо специально спроектированные аппаратные компоненты. Аппаратной платформой подавляющего большинства представленных сегодня решений SDS является сервер x86, к которому для расширения емкости напрямую (а не через сеть) подключены внешние дисковые полки (схема DAS, рассмотренная в разделе 0). Как правило, для ускорения доступа к данным в сервере вместе с жесткими дисками устанавливаются твердотельные накопители, выполняющие функции кэш-памяти системы.

Традиционно считалось, что использование СХД DAS приводит к неэффективному расходу дисковых ресурсов, плохому масштабированию и более сложному управлению хранением. Однако применение современных скоростных интерконнектов (например, 10-гигабитного Ethernet и InfiniBand) в сочетании с твердотельной кэш-памятью чтения/записи позволяет построить на базе систем DAS хорошо масштабируемую сетевую архитектуру с полностью независимыми узлами хранения, построенными на базе серверов стандартной архитектуры с полками расширения. По мнению экспертов, SDS постепенно может стать компонентом любого ЦОД, поскольку обеспечивает более эффективное и экономичное хранение данных. Особенно активно SDS будет внедряться для хранения неструктурированных данных в виде файлов и объектов.

Виртуализация ресурсов давно применяется в СХД корпоративного класса. Однако раньше она чаще всего реализовывалась с помощью специализированных микросхем контроллера дискового массива. SDS, в дополнение к традиционной виртуализации ресурсов СХД, реализует механизмы самообслуживания и использования политики управления, значительно упрощающие администрирование хранения и позволяющие легко и быстро предоставлять нужные данные и дисковую емкость приложениям и пользователям.

Внедрение технологии SDS обеспечивает следующие результаты, которые невозможно получить при использовании традиционной виртуализации СХД:

— координацию предоставления сервисов хранения (независимо от того, где хранятся данные) для выполнения требований соглашения об обслуживании SLA с помощью программного обеспечения;

— улучшение эффективности использования ресурсов и продуктивности персонала за счет обработки запросов на сервисы и управления текущими операциями с помощью программного обеспечения;

— использование стандартного оборудования для уменьшения зависимости от специализированного железа и реализация всех интеллектуальных функций на уровне программного обеспечения;

— использование общего набора интерфейсов прикладного программирования (application programming interface – API) для интеграции между собой различных сервисов хранения и вычислений, сетевых и прикладных сервисов.

Применение SDS решений существенно снижает расходы на приобретение СХД по сравнению с традиционными дисковыми массивами, поскольку использует стандартное серверное оборудование. Они также легко масштабируются добавлением в конфигурацию нового сервера.

Решения SDS горизонтально масштабируются до нескольких десятков узлов и по максимальной емкости могут превосходить традиционные дисковые массивы корпоративного класса, а также обеспечивают высокий уровень отказоустойчивости благодаря резервированию узлов. Например, решение VMware Virtual SAN масштабируется до 32-узлового серверного кластера с 32 тыс. виртуальных машин и 4,4 Пбайт емкости и обеспечивает производительность чтения/записи до 2 млн IOPS (Input/Output Operations Per Second – количество операций ввода/вывода в секунду), а виртуальная приставка HP StoreVirtual VSA масштабируется до 16-узловой конфигурации, поддерживая от 4 до 50 Тбайт емкости на один узел. По мнению экспертов, SDS решения могут существенно изменить рынок СХД, дополнив его сектором относительно дешевых горизонтально хорошо масштабируемых решений на базе стандартного оборудования x86.

3.7.4. СХД на ДНК

В 2016 году корпорация Microsoft объявила о покупке 10 миллионов волокон синтетической ДНК для исследования возможностей построения устройств хранения данных на основе молекул из генетического кода. Исследователи из Microsoft намерены выяснить,

каким образом молекулы, из которых состоит генетический код человека и всех живых существ, могут быть использованы для кодирования цифровой информации.

До разработки коммерческой продукции пока еще очень далеко, однако первичные тесты показали, что синтетическая ДНК позволяет расшифровать 100% данных, закодированных с ее помощью.

Новая технология призвана решить проблему Больших данных (см. раздел 11), количество которых удваивается каждые два года. Системы хранения, построенные на основе синтетических ДНК, смогут обойти две ключевых проблемы нынешних СХД – ограниченный срок жизни носителей и низкую плотность хранения. Специалисты ожидают, что носители на основе ДНК смогут сохранять информацию до двух тысяч лет, а в устройстве весом один грамм может поместиться 1 Зетабайт (один Зетабайт равен 10^{21} байт или триллиону Гигабайт) цифровых данных.

В рамках проведенного эксперимента команда ученых сконвертировала бесчисленные ряды единиц и нулей с четырех образов диска в четыре основания ДНК — аденин, гуанин, тимин и цитозин. Она смогла также произвести и обратный процесс — найти нужные последовательности уже в полной цепочке ДНК и реконструировать образы диска без каких-либо потерь, причем в ходе этого процесса не «потерялось» ни одного байта.

Возможность хранения информации в течение сотен или даже тысяч лет выгодно отличает «ДНК-память» от привычных сегодня способов хранения цифровой информации — жестких дисков, твердотельных накопителей, магнитных и оптических дисков. Последние, как известно, сохраняют работоспособность только в течение нескольких лет или, максимум, нескольких десятилетий.

Сегодня главный барьер на пути внедрения «ДНК-памяти» — высокая стоимость производства, а также эффективность, с которой ДНК можно синтезировать и считывать в больших масштабах. Но ученые считают, что технически все эти проблемы можно решить.

Контрольные вопросы

1. Основные положения систем хранения данных для ЦОД.
2. Устройства хранения данных ЦОД.
3. Многоуровневое хранение данных ЦОД.
4. Перспективные устройства хранения информации.
5. Преимущества прямого подсоединения памяти к серверу.

6. Схема организации сети хранения SAN.
7. Схема организации сетевого устройства хранения NAS.
8. Сравнительный анализ SAN и NAS.
9. Пути повышения надежности хранения информации.
10. Организация дискового массива RAID 0.
11. Организация дискового массива RAID 1.
12. Организация дискового массива RAID 2.
13. Организация дискового массива RAID 3.
14. Организация дискового массива RAID 4.
15. Организация дискового массива RAID 5.
16. Организация дискового массива RAID 6.
17. Современные технологии, применяемые в современных классических СХД.
18. Горизонтально масштабируемые СХД.
19. Применение блочной дедупликации для систем резервного копирования.
20. Концепция программно-определяемого хранения.
21. Возможность использования СХД на ДНК.

4. Инженерные подсистемы ЦОД

4.1. Общие положения

Для надлежащего функционирования современного вычислительного и телекоммуникационного оборудования требуется поддержка довольно жесткого режима температуры и влажности, поэтому в современных ЦОД система кондиционирования и вентиляции является обязательной. Кроме того, аппаратура требовательна к качеству электропитания, поэтому приходится устанавливать источники бесперебойного питания (ИБП) - аккумуляторные батареи необходимой мощности и источники гарантированного питания (электрогенераторные установки). Серверы, системы хранения и сетевые устройства размещаются в специальных монтажных стойках и шкафах, которые должны быть достаточно надежными и удобными для обслуживания находящихся в них устройств. Не менее важными для нормальной жизнедеятельности ЦОД являются система обеспечения физической безопасности (контроль доступа, охранное видеонаблюдение, пожарная сигнализация, средства пожаротушения и т. д.), а также система контроля и управления инженерными средствами. Исключительно важна и структурированная кабельная система (СКС), своего рода кровеносная

система ЦОД. Она связывает воедино все компоненты — начиная от основного оборудования и заканчивая датчиками и контроллерами инженерных средств. Именно благодаря ей ЦОД превращается в единый организм. Поэтому к вопросам проектирования, инсталляции и обслуживания кабельной системы следует подходить максимально внимательно. К тому же к такого рода инфраструктуре предъявляется ряд специфических требований, вследствие чего кабельные системы для ЦОД несколько отличаются от офисных СКС.

Как уже отмечалось в разделе 0, наиболее подробно требования к СКС для ЦОД изложены в европейском стандарте EN 50173-5 и базирующемся на нем международном стандарте ISO/IEC 24764. Поэтому при изложении структуры кабельной системы ЦОД мы будем основываться на требованиях европейского стандарта.

Инженерная инфраструктура составляет большую часть себестоимости ЦОД, нередко доходя до 70%. При этом распределение затрат на подсистемы дата-центров неравномерно. Наибольшая доля (около трети всех потраченных финансовых ресурсов), приходится на стоимость системы гарантированного электропитания (34%). Также значительные траты предусматривают организация кондиционирования (21%) и архитектура самого здания (23%). На коммуникационные сети приходится 7% плюс еще около 9% на оборудование газового пожаротушения, систем управления доступом и видеонаблюдения и шкафную инфраструктуру. Наименьшую долю в крупных затратах составляет организация системы мониторинга (1%). Очевидно, что на три первых системы ложится подавляющая часть расходов (78%). Следовательно, можно добиться значительной экономии за счет их оптимизации. Рассмотрим более подробно указанные выше подсистемы ЦОД.

4.2. Выбор помещения для ЦОД

Требования к выбору помещения для ЦОД условно можно разделить на три группы. К первой относятся все количественные требования, на основании которых рассчитывается мощность ЦОД. Ко второй — требования, соблюдение которых обязательно, а к третьей — все дополнительные, выполнение которых желательно, но не обязательно (или они реализуются без существенных капитальных вложений).

Что касается первой группы требований, то начинать следует с расчета максимальной мощности ЦОД, поскольку в дальнейшем этот параметр будет ограничителем его роста.

Далее рассчитывается емкость размещаемого оборудования, измеряемая в стандартных единицах высоты или, в просторечии, юнитах (U). Зная стандартные размеры стоек, можно определить их необходимое количество, а затем и минимальную площадь помещения, которая зависит, в том числе, и от его планировки. Обычно на одну стойку отводится 2-2,5 квадратных метра площади ЦОД, поскольку в последнем размещаются не только стойки и/или шкафы для оборудования, но и вспомогательное оборудование - организаторы кабелей, системы электропитания, вентиляции, кондиционирования и пожаротушения. Поэтому требования к площади ЦОД определяются также такими факторами, как расчетный отвод тепла и необходимый уровень резервирования для обеспечения отказоустойчивости.

Следующий важный параметр — энергопотребление основного оборудования. В паспортах устройств обычно указывают среднюю мощность потребления, поэтому следует учесть, что реальная потребляемая мощность оборудования может быть значительно выше. Для грубой оценки мощность, потребляемую стойкой с современным оборудованием, следует считать порядка 10-15 кВт. Соответственно мощность источников бесперебойного питания выбирается в зависимости от энергопотребления основного оборудования и времени включения источников гарантированного питания – автономных генераторов электрической энергии.

Зная полезную мощность, можно определить подводимую мощность к ЦОД. В разделе 1.1 был определен коэффициент PUE – отношение полной мощности, потребляемой ЦОД, к мощности, потребляемой ИТ-оборудованием. Таким образом, полная подводимая мощность к хорошо сконструированному российскому ЦОД должна быть, по крайней мере, в 1,4-1,6 раз выше полезной потребляемой мощности. На практике потребляемая мощность оценивается с запасом, т.е. примерно в 2, а иногда и в 2,5 раза больше полезной. Как уже говорилось, избыточная мощность тратится, в первую очередь, на отвод выделяемого оборудованием тепла, т. е. на кондиционирование помещений. Другие инженерные системы являются менее ресурсоемкими — освещение, в том числе аварийное, вентиляция, газовое пожаротушение, контроль доступа, видеонаблюдение потребляют энергию в значительно меньшем количестве.

Размеры и общий вес стоек определяют требования к минимальной нагрузочной способности перекрытий и фальшпола, при этом допустимая нагрузка на пол должна быть не менее 500 кг на квадратный метр. Исходя из состава и производительности информационных систем формулируются требования к кабельным системам и внешним кабельным вводам для каналов связи.

Рассмотрим теперь вторую группу требований. Сюда относится, прежде всего, легитимность сооружения, его соответствие требованиям федеральных, республиканских и местных законов применительно к конкретному расположению ЦОД. Один из существенных моментов — расположение центра. Он должен отвечать следующим обязательным четырем условиям:

— допускать возможность подключения к двум независимым линиям электропитания, причем, в свою очередь, подключенным к разным подстанциям;

— иметь возможность организации не менее двух независимых вводов магистральных линий связи от разных колодцев кабельной канализации до помещения ЦОД с достаточной свободной емкостью; при этом трассы прокладки не должны пересекаться или проходить в непосредственной близости друг от друга;

— иметь удобные основные и резервные подъездные пути для автомобильного транспорта с хорошим покрытием и достаточной пропускной способности;

— располагать дополнительными площадями вокруг ЦОД с целью размещения источников гарантированного питания (электрогенераторов), конденсаторных блоков кондиционеров, площадок для разгрузки тяжелых и негабаритных грузов, проезда машин-заправщиков к генераторным установкам, парковки машин персонала.

Подобным условиям отвечают многие современные технопарки, а также территория пустующих предприятий в старых промышленных зонах.

Кроме того, в помещении под ЦОД для организации фальшпотолков и фальшпола обязательно должно быть предусмотрено дополнительное пространство, особенно в тех случаях, когда охлажденный воздух предполагается подводить к стойкам снизу и для обеспечения требуемой плотности и скорости потока фальшпол придется поднять достаточно высоко. Категорически исключено наличие транзитных магистралей с водой (водопровод, отопление), располагаемых этажом выше. Если это условие принципиально

невыполнимо, то необходимо обеспечить дополнительную гидроизоляцию помещения. ЦОД должен быть расположен выше уровня грунтовых вод. Ни в нем самом, ни поблизости от него не должно быть источников электромагнитного и радиочастотного излучения — радиопередатчиков, рентгеновского оборудования и трансформаторов.

Третья группа требований к помещению ЦОД объединяет необязательные, но желательные требования. К ним относится возможность организации двух и более периметров охраны, поскольку доступ в помещения ЦОД должен быть ограничен и строго регламентирован. В целях безопасности в помещении ЦОД также желательно не иметь окон. При отсутствии возможности полностью заделать оконные проемы следует оставить фальшокна с дополнительной отражательной пленкой. Крайне нежелательны для размещения ЦОД подвалы как из-за потенциальной угрозы подтопления или затопления, так и из-за большого количества инженерных сооружений, как правило, размещаемых в них и представляющих потенциальную опасность для оборудования

Для энергоснабжения предпочтительнее использовать подземные магистрали, нежели подвесные, чтобы свести к минимуму возможность механического повреждения последних.

Для систем вентиляции следует предусмотреть определенный резерв, чтобы при необходимости подключить к ним помещения ЦОД. При размещении ЦОД на этажах выше первого надо предусмотреть вентиляционные шахты и возможность дополнительной нагрузки на них, а также раздельные вертикальные подводы для электричества и слаботочных/оптических кабелей, причем желательно иметь два независимых пути подвода.

Поскольку значительная часть оборудования ЦОД не допускает кантования при транспортировке, желателен грузовой лифт достаточной грузоподъемности.

4.3. Кабельная система ЦОД

4.3.1. Структура кабельной системы

Стандарт EN 50173-5 предусматривает иерархическую структуру кабельной системы ЦОД (см. Рисунок 24). Подключение внешних сетей и служб осуществляется через сетевые интерфейсы оборудования (Equipment Network Interface, ENI). Физически эти элементы располагаются, как правило, в отдельной комнате, где установлено активное оборудование для доступа к службам сервис-провайдера или

территориально распределенной корпоративной сети. Поступивший извне трафик обрабатывается и далее направляется уже по кабельной системе ЦОД. Первый ее участок называется подсистемой сетевого доступа и ведет к основному кроссу (Main Distributor, MD). Далее — до зонных кроссов (Zone Distributor, ZD) — располагается основная (магистральная) подсистема распределения. Подключение розеток оборудования (Equipment Outlet, EO) осуществляется по зонной подсистеме распределения. Отметим, что в стандарте TIA/ EIA-942 аналогичный участок называется горизонтальной подсистемой.

Между зонным кроссом ZD и розетками оборудования EO может находиться еще один элемент — локальный пункт распределения (Local Distribution Point, LDP). Будучи факультативным (необязательным), он

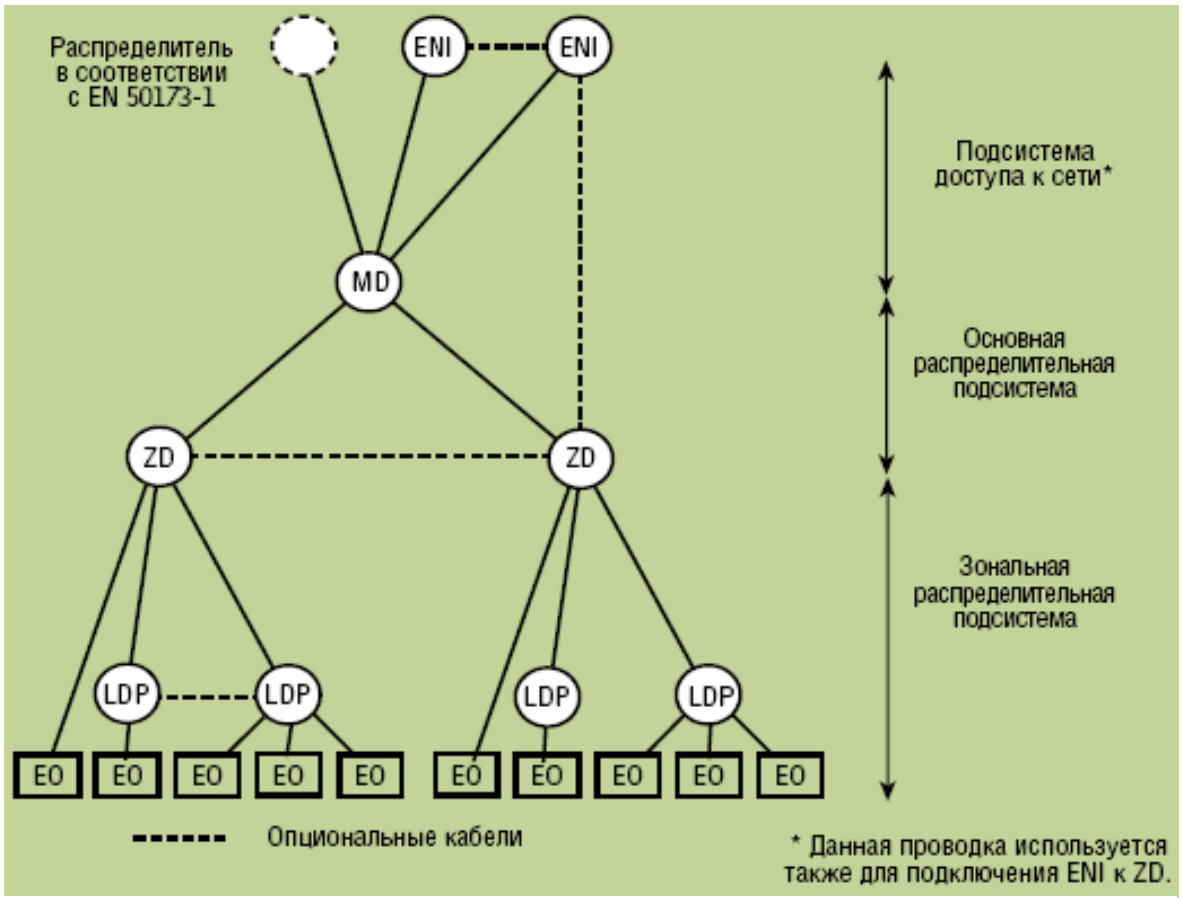

Рисунок 24 - Структура кабельной системы ЦОД

обычно содержит только пассивные соединения. Использование LDP имеет смысл, когда происходят частые перемещения и добавления оборудования, что и характерно для ЦОД. Стандарт допускает его размещение под фальшполом или у потолка. Пункт LDP должен располагаться не ближе 15 м от зонного кросса ZD во избежание ухудшения характеристик, связанных с перекрестными помехами и возвратными потерями.

С целью резервирования стандарт EN 50173-5 допускает организацию дополнительных кабельных линий между зонными кроссами ZD и локальными пунктами распределения LDP.

4.3.2. Требования к гибкости и масштабируемости

ЦОД представляет собой объект, на котором происходят постоянные изменения. Причем, если основная доля изменений в инфраструктуре ИТ обычного офиса связана с перемещениями отдельных сотрудников и подразделений, то в ЦОД основные изменения связаны с добавлением или перемещением новых устройств. Кабельную систему ЦОД следует строить таким образом, чтобы обеспечивалось быстрое переконфигурирование имеющегося оборудования и ввод в эксплуатацию нового. Стоимость эксплуатации ЦОД очень высока, поэтому его простои надо минимизировать, а следовательно, все работы на кабельной инфраструктуре должны выполняться в кратчайшие сроки. Возможности масштабирования должны обеспечивать не только подключение новой техники, но и изменение технологии передачи информации, например, переход с технологии Gigabit Ethernet на 10 Gigabit Ethernet.

Важное условие масштабируемости и гибкости кабельной системы является ее модульное построение. Система должна допускать быструю активацию новых кабельных трактов, добавление дополнительных разъемов для подключения оборудования, замену одного типа разъема на другой (например, медный на оптический). Следует выбирать такие коммутационные панели и розетки, в которые можно устанавливать модули разъемов как для медных, так и для волоконно-оптических трактов. Этим обеспечивается модульность на уровне подключения отдельных разъемов. Желательно использовать коммуникационные панели, обеспечивающие модульность на уровне групп разъемов (см. Рисунок 25). Подобные решения позволяют, исходя из специфики решаемой задачи, получить необходимое число различных разъемов и выбрать подходящий способ терминирования.

Рисунок 25 - Коммуникационная панель

Современные ЦОД с уровнем надежности 2 и выше по классификации стандарта TIA/EIA-942 имеют фальшпол, под которым располагаются элементы многих инженерных подсистем. Обычно именно под фальшполом организуется распределение охлаждающего воздуха и подвод его к оборудованию. Во многих проектах там же

прокладываются каналы для подведения кабелей к стойкам с оборудованием. Такое решение обеспечивает удобное обслуживание, изменение и модернизацию кабельной системы.

Возможность максимально оперативно вносить изменения в кабельную инфраструктуру ЦОД не должно сказываться на ее рабочих характеристиках. Однако, как известно, качественная установка разъемов на волоконно-оптические кабели занимает продолжительное время, а необходимое для этого оборудование не всегда удобно применять непосредственно на местах монтажа. Поэтому иногда целесообразно использовать претерминированные кабельные сборки, в состав которых входят соединительные кабели различной длины, оконцованные разъемами в заводских условиях (см. рисунок 26). Это гарантирует высокое качество и проверенные характеристики.

Рисунок 26 - Претерминированная кабельная сборка

4.3.3. Надежность кабельных систем

Стандарт EN 50173-5 на кабельную систему ЦОД предусматривает ряд мер для повышения надежности на уровне ее структуры. В частности, уже упоминавшуюся в разделе 0 возможность организации дополнительных линий связи между локальными пунктами распределения LDP, а также между зонными кроссами ZD. Но резервирование структуры не исключает высоких требований к надежности отдельных элементов кабельной системы.

Как уже отмечалось, ЦОД характеризуется высокой плотностью кабельных подключений, а также частыми добавлениями и переключениями. Поэтому особое внимание надо уделить качеству изготовления разъемов, которое должно быть подтверждено соответствующими тестами. Желательно проведение тестирования, гарантирующего сохранение механических характеристик контактов разъемов после, например, нескольких сотен циклов подключений/отключений.

В настоящее время все шире применяется технология подачи электропитания по кабельной системе сети Ethernet (Power over Ethernet, PoE). Такой способ значительно повышает удобство подключения конечных активных устройств и позволяет задействовать эффективные схемы централизованного резервирования источников электропитания. В ЦОД эта технология может использоваться для дистанционного электропитания установленных в нем камер видеонаблюдения и работающих в составе IP-УАТС IP-телефонов. Однако не следует

забывать, что электропитание подается по «чужой» кабельной проводке, а значит важно исключить его негативное влияние на характеристики элементов кабельной системы. Во избежание вредного влияния на контакты разъемов «силовой составляющей» (например, их обугливания при возникновении электрической дуги) желательно предварительное тестирование разъемов на наличие необходимой электрической устойчивости при большом числе циклов подключений/отключений под нагрузкой.

Высокая плотность подключений может приводить к дополнительной нагрузке на хвостовики вилок. Например, в случае большого числа коммутационных шнуров в ограниченном пространстве при отключении одного из них могут возникнуть нежелательные изгибы вилок других шнуров. В такой ситуации гарантировать надежность опять-таки способны лишь тщательно протестированные продукты.

4.3.4. Безопасность и управляемость

Как показывают многочисленные исследования, человеческий фактор остается одной из основных причин, приводящих к отказам в сети. Неправильные действия персонала способны нанести непоправимый ущерб оборудованию, привести к потере ценных данных, вывести ЦОД из строя на значительное время. Поскольку в ЦОД могут работать не только инженеры-кабельщики, но и специалисты по обслуживанию других инженерных систем или основного оборудования, защита точек физического подключения от несанкционированных действий становится важнейшим элементом обеспечения безопасности ЦОД. Условно можно выделить 3 уровня такой защиты:

— уровень 1 — визуальное кодирование, т.е. цветовое кодирование разъемов, розеток и коммутационных панелей с помощью специальных клипс, крышек и рамок, которые подсказывают обслуживающему персоналу, как правильно подключать медные и оптические шнуры (синюю вилку в синюю розетку, красную — в красную и т.д);

— уровень 2 — механическое кодирование, дополняющее цветовое, которое механически не позволяет вставить вилку в «неправильный» разъем;

— уровень 3 — блокировка разъемных соединений, т.е. использование специальных защитных рамок, вставок, клипс, которые позволяют заблокировать соединения так, что их разблокирование оказывается возможным только с помощью специального ключа.

При выборе среды передачи информации в ЦОД предпочтение оптическим кабелям отдается не только по причине более высокой скорости и дальности, но и по соображениям безопасности. Несанкционированный «съем» информации с оптического тракта осуществить значительно труднее, чем с медного. Поэтому в ЦОД широко применяются кабели для различных условий прокладки с одномодовыми и многомодовыми волокнами. Внутри зданий применяются кабели с многомодовыми волокнами и оболочкой, не выделяющей дыма и галогенов при горении.

4.4. Система бесперебойного и гарантированного электроснабжения

4.4.1. Общие положения

Источником бесперебойного питания (ИБП) (по английски - Uninterruptible Power Supply, UPS) называется автоматическое устройство, предназначенное для обеспечения электрооборудования с бесперебойным снабжением электрической энергией в пределах нормы. ИБП также служат для нейтрализации негативных факторов, влияющих на чистоту электропитания (броски по напряжению, изменение частоты, наличие гармоник и т. п.);

ГОСТ 13109-97 определяет следующие нормы в сети электропитания: напряжение 220 В ± 10 %; частота 50 Гц ± 1 Гц; коэффициент нелинейных искажений формы напряжения менее 8 % (длительно) и менее 12 % (кратковременно).

Неполадками в питающей сети считаются:

— авария сетевого напряжения (напряжение в питающей сети полностью пропало);

— высоковольтные импульсные помехи (резкое увеличение напряжения до 6 кВ продолжительностью от 10 до 100 мс);

— долговременные и кратковременные подсадки и всплески напряжения;

— высокочастотный шум (высокочастотные помехи, передаваемые по электросети);

— побег частоты (отклонение частоты более чем на 3 Гц).

Использование ИБП обеспечивает бесперебойную работу оборудования при полном пропадании электрического тока или при выходе его параметров за допустимые нормы в течение некоторого непродолжительного времени. Это время должно быть достаточным для включения электрических генераторов, представляющих собой

источники гарантированного питания (ИГП) или, хотя бы, корректного завершения работы оборудования.

Основными показателями, обуславливающими выбор схемы построения ИБП, являются время переключения нагрузки на питание от аккумуляторных батарей и время работы от аккумуляторной батареи.

4.4.2. Составные части ИБП

Реализация основной функции ИБП достигается работой устройства от аккумуляторов, установленных в корпусе ИБП, под управлением электрической схемы, поэтому в состав любого ИБП, кроме схемы управления, входит зарядное устройство, которое обеспечивает зарядку аккумуляторных батарей при наличии напряжения в сети, обеспечивая тем самым постоянную готовность к работе ИБП в автономном режиме. Для увеличения автономного режима работы можно оснастить ИБП дополнительной (внешней) батареей.

В ряде случаев, например при проведении профилактического обслуживания ИБП или замены его узлов без отключения нагрузки, целесообразно использовать так называемый режим байпас (bypass по-английски означает «обход»). В этом случае питание нагрузки отфильтрованным напряжением электросети осуществляется в обход основной схемы ИБП. Переключение в режим байпас выполняются автоматически или вручную. Блок, осуществляющий перевод в этот режим, также называется байпас.

Для сглаживания бросков по питающему напряжению используется устройство, называемое «бустер» (от английского «booster» - усилитель, стимулятор) — ступенчатый автоматический регулятор напряжения, представляющий в своей основе автотрансформатор. Часто ИБП оснащается только повышающим «бустером», который имеет всего лишь одну либо несколько ступенек повышения, но есть модели, которые оснащены универсальным регулятором, работающим и на повышение, и на понижение напряжения. Использование бустеров позволяет создать схему ИБП, способную выдержать долгие глубокие «подсадки» и «проседания» входного сетевого напряжения (одной из наиболее распространенных проблем отечественных электросетей) без перехода на аккумуляторные батареи, что позволяет значительно увеличить срок «жизни» аккумуляторной батареи.

Подключение нагрузки к резервным источникам электроэнергии осуществляется с помощью автоматов ввода (включения) резерва (АВР). Основная характеристика АВР - время переключения на резервный источник в случае выхода из строя основного.

Для преобразования постоянного напряжения аккумуляторных батарей ИБП в переменное напряжение, потребляемое оборудованием, используется инвертор. Инверторами называются также устройства, осуществляющие обратный процесс - перевод переменного напряжения в постоянное.

Для подачи «чистого» напряжения на установленное в ЦОД оборудование используется гальваническая развязка между входом и выходом. Для этого во входной цепи ИБП (между электросетью и выпрямителем) устанавливается входной изолирующий трансформатор. Соответственно, в выходной цепи ИБП между преобразователем и нагрузкой размещается выходной изолирующий трансформатор, который обеспечивает гальваническую развязку между входом со схемы ИБП и выходом на подключенную нагрузку.

Для того чтобы повысить надежность всей системы в целом, применяется резервирование — схема, которая состоит из двух или более ИБП.

4.4.3. Схемы построения ИБП

Существуют три схемы построения ИБП.

1) Резервная (standby), при которой питание подключенной нагрузки осуществляется из первичной электрической сети, а ИБП только производит фильтрацию высоковольтных импульсов и электромагнитных помех. При выходе электропитания за нормированные значения напряжения (или полном исчезновении напряжения) ИБП автоматически переключает нагрузку на питание от собственных аккумуляторов. А при появлении напряжения в пределах нормы ИБП снова переключается нагрузку на питание от первичной сети. Этот режим, как правило, реализуется в недорогих маломощных ИБП, предназначенных для локальных вычислительных сетей (ЛВС) начального уровня, и не применяется в крупных ЦОД.

2) Интерактивная (interactive) — схема, аналогичная предыдущей, но дополнительно на входе ставится ступенчатый стабилизатор напряжения, позволяющий получить регулируемое выходное напряжение. В этом случае удается достичь меньшего времени переключения, чем в предыдущем варианте, так как осуществляется синхронизация инвертора с входным напряжением. Но КПД интерактивной схемы ниже, чем у резервной.

3) Неавтономная (online), используемая для питания оборудования, предъявляющего повышенные требования к качеству сетевого электропитания. Принцип работы состоит в двойном

преобразовании (double conversion) тока. Сначала входное переменное напряжение с помощью инвертора преобразуется в постоянное, затем снова в переменное напряжение с помощью обратного инвертора. Время переключения равно нулю. ИБП двойного преобразования имеют относительно невысокий КПД (от 80 % до 94 %), из-за чего отличаются повышенным тепловыделением и уровнем шума. Но в отличие от двух предыдущих схем, они способны корректировать не только напряжение, но и частоту, и их применение наиболее целесообразно в ЦОД.

4.4.4. Системы гарантированного питания (СГП)

Существуют два определения СГП. В первом случае в состав СГП включают электросеть, ИБП, резервную генераторную установку, а также автоматические переключатели нагрузки и вспомогательное оборудование. Ниже под СГП мы будем понимать исключительно генераторные установки, являющиеся неотъемлемой частью ЦОД, к которым предъявляются повышенные требования по обеспечению функционирования при любых сроках отключения внешнего питающего напряжения.

Генераторы – первичные источники электроэнергии различаются, как правило, по типу применяемого топлива (газ, бензин, дизельное топливо). Наиболее широко используются дизельные генераторные установки (Рисунок 27).

Рисунок 27 - Дизельные генераторные установки

Генераторы предназначены для потребителей, нуждающихся в однофазном электропитании мощностью до 100 кВт или трехфазном электропитании мощностью до 2000 кВт. Электрические генераторы автоматически запускаются при полном пропадании электропитания либо несоответствия его требуемым параметрам (напряжение, частота, "чистота"). Запас топлива составляет, как правило, не менее 8 часов непрерывной работы и восполняется без остановки генератора.

4.5. Система кондиционирования (искусственного климата)

4.5.1. Традиционные системы кондиционирования

В задачи системы кондиционирования входит поддержание внутри ЦОД рабочей температуры в пределах от 19 до 24 °С и влажности от 40 до 80%. Обычно в ЦОД среднего размера (площадь 100 — 200 кв. м) используются шкафные прецезионные фреоновые кондиционеры, забирающие теплый воздух в верхней части помещения и нагнетающие охлажденный воздух под фальшпол. Резервирование системы кондиционирования для ЦОД второго и третьего уровня по классификации стандарта TIA/EIA-942 осуществляется по схеме N+1, т.е. при потребности в N фреоновых кондиционеров их должно быть установлено не менее N+1. При этом целесообразно, чтобы все шкафы были связаны в единую систему управления. В этом случае программное обеспечение осуществляет ротацию роли запасного шкафа, что позволяет более эффективно расходовать ресурс системы в целом.

Для мощных ЦОД целесообразно установить систему кондиционирования с применением жидкого теплоносителя. Для этого на улице устанавливается мощный чиллер - система кондиционирования воздуха, в которой теплоносителем между центральной холодильной машиной (чиллером) и локальными теплообменниками служит охлаждённая жидкость. Охлажденный до 16°С хладагент (как правило, вода) по трубопроводу подается в помещение ЦОД, где через шкафные кондиционеры происходит теплоотвод воздуха. Нагретый агент возвращается в чиллер для охлаждения, круг замыкается. Хладопроизводительность чиллеров может ограничиваться лишь финансовыми возможностями — существуют машины до 5 — 10 МВт холода.

19-дюймовый шкаф, полностью заполненный современным серверным оборудованием, способен выделить до 20 кВт тепла. Следует помнить, что в силу конструктивных и физических его особенностей обычным путем, т. е. продувая холодным воздухом из-под фальшпола, практически невозможно снять более 5 кВт тепла. Для решения проблемы существует несколько подходов, в частности, организация "горячих" и "холодных" коридоров (Рисунок 28). Под коридором подразумевается проход между рядами шкафов. В "горячий" коридор направляются вентиляторы, выдувающие горячий воздух из серверов, а из "холодного" забирается холодный воздух, выдуваемый из-под фальшпола через решетки. Такая схема позволяет существенно поднять КПД системы холодоснабжения. Реализация данной схемы в одном из

самых современных российских ЦОД, принадлежащих Федеральной налоговой службе в г.Дубна, приведена на Рисунке 29. Здесь горячие коридоры закрыты дверями, и воздух из них удаляется через воздухозаборники.

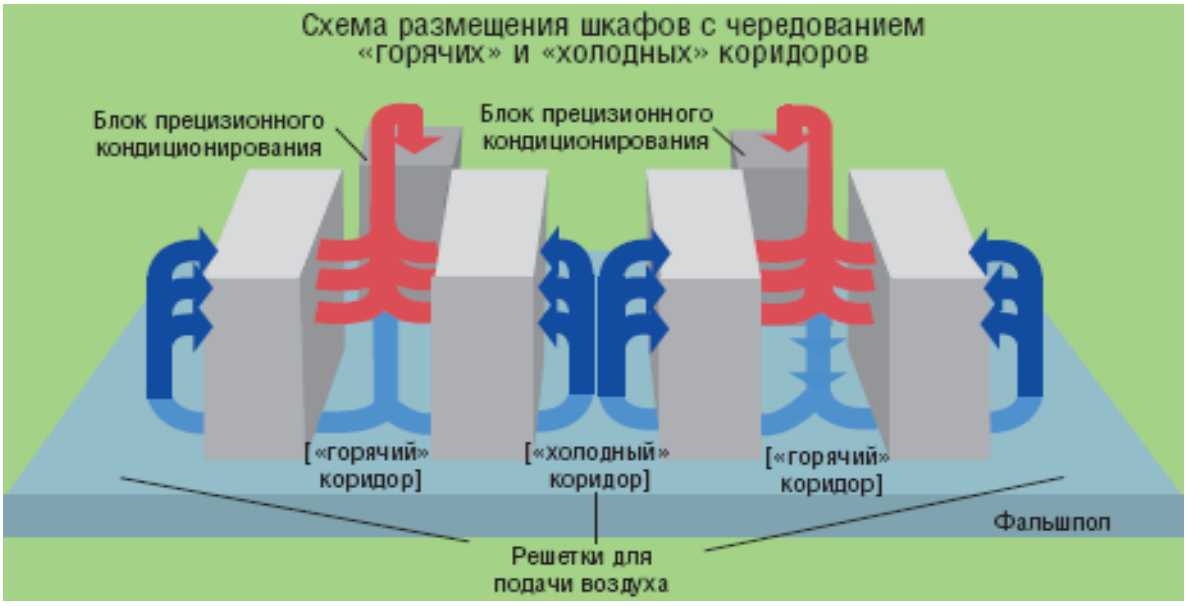

Рисунок 28 - Схема организации «горячих» и «холодных» коридоров

Рисунок 29 - Реализация системы горячих (за дверями) и холодных коридоров в ЦОД Федеральной налоговой службы (г.Дубна)

Также требуется организовать приток свежего воздуха с улицы. Дело в том, что воздух, постоянно циркулирующий через компьютерные шкафы и кондиционеры, "выгорает" и требует обновления. Приток осуществляется через специальную установку, нагревающую и

осушающую уличный воздух. Кроме того, она создает внутри ЦОД дополнительное давление, что препятствует проникновению внутрь пыли.

Для увлажнения воздуха используются парогенераторы. Сухой воздух малоэффективен для охлаждения системой хладоснабжения в силу физических принципов кондиционирования. При понижении влажности электростатический потенциал увеличивается, что может быть причиной выхода оборудования из строя.

Система кондиционирования — сложный и тонкий механизм. Как показывает практика, это самая критичная и ненадежная составляющая комплекса ЦОД. Ее остановка на 30 мин. может повлечь за собой нагрев помещения до 60 — 70^{o}C, что влечет за собой выход из строя оборудования, в первую очередь, магнитных носителей.

Фальшпол является необходимым компонентом ЦОД. Под него нагнетается охлажденный воздух, под ним располагаются кабели электроснабжения и слаботочная инфраструктура. Как правило, фальшпол изготавливается из МДФ-плиток на металлической основе с ламинированным покрытием, размером 600 х 600 мм. Высота над уровнем пола — от 100 до 800 мм, для ЦОД наиболее оптимальна высота 350 — 500 мм.

4.5.2. Фрикулинг и гринкулинг

Как упоминалось выше, системы охлаждения ЦОД весьма энергозатратны. Существенно уменьшить общее энергопотребление ЦОД можно за счет использования холода внешней среды. Нормальная температура охлаждающего воздушного потока, подаваемого на серверы, составляет 22-25^{0}C. Это теоретически позволяет в средней полосе России почти три четверти года охлаждать ЦОД воздухом с улицы. Этот метод получил название фрикулинг (от английского «free cooling» - свободное охлаждение). Иногда говорят также о гринкулинге (от английского «green cooling» - «зеленое» охлаждение), понимая под этим тот же фрикулинг, но при доминирующем естественным охлаждении.

Однако получить готовый холод из внешней среды хоть и относительно несложно, но все же процесс сопряжен с некоторыми нюансами, которые следует учитывать.

Наиболее простой способ заключается в подаче внешнего холода в помещение серверной при помощи естественного теплоносителя, в роли которого выступает воздух (так называемый, свободный фрикулинг). Поскольку, как уже упоминалось, большую часть года

температура наружного воздуха в средней полосе России значительно ниже $+25^0$C (согласно TIA/EIA-942, это максимальное рекомендуемое значение температуры для подачи на воздухозаборники ИТ-оборудования). Поэтому логично для охлаждения оборудования использовать внешний воздух или его подмес. Существует ряд технических решений по фрикулингу, из которых можно выделить два основных направления, а именно, прямой и непрямой.

Схема прямого фрикулинга (Рисунок 30) реализуется по принципу приточно-вытяжной установки, которая может быть как отдельной подсистемой, так и встроенной в существующую схему кондиционирования (например, подпотолочные кондиционеры), и применяется для небольших серверных и мобильных ЦОД. По сути, воздух забирается из внешней среды, фильтруется и подается в серверное помещение.

Рисунок 30 - Схема реализации метода прямого фрикулинга

К несомненным достоинствам подобного метода можно отнести низкую стоимость реализации и простоту конструкции, поскольку обычно схема представляет собой сборку из вентиляторов, фильтров, клапанов, заслонок с электроприводом и воздуховодов. Энергопотребление вентиляторов в таком случае будет на порядок ниже по сравнению с традиционными компрессорными фреоновыми кондиционерами. Вместе с тем прямой фрикулинг имеет и ряд существенных недостатков. Так, например, отсутствует возможность поддержания определенного уровня влажности в помещении. Для предотвращения выпадения конденсата зимой из-за большой разницы температур и достижения точки росы, воздух подогревают калорифером, установленным в приточном воздуховоде. Однако калорифер — это весьма энергозатратный элемент, резко снижающий выгоды от использования фрикулинга. С увлажнением задача еще сложнее, поскольку данный процесс требует постоянной подачи очищенной воды.

Кроме того, при прямом фрикулинге возникает проблема накопления мелкодисперсной пыли, проникающей в чистое серверное помещение извне. Существует также мнение, что прямая подача воздуха с улицы в серверное помещение способствует проникновению продуктов горения (в случае пожара), смога, активных окислителей, содержащихся в выбросах промышленных предприятий, автотранспорта и др. Эти элементы, которые потенциально могут содержаться в уличном воздухе, отрицательно влияют на срок службы ИТ-оборудования.

В случае непрямого фрикулинга внешний холодный воздух охлаждает либо воздух, циркулирующий по незамкнутому контуру внутри ЦОД, либо хладагент, например, тот же хладон. В основе первого метода лежит использование роторного рекуператора в качестве теплообменника для двух незамкнутых контуров воздуховодов. Роторный рекуператор представляет собой промежуточный вентилятор весьма крупных размеров, который разделяет два контура воздуховодов — внешний и внутренний (Рисунок 31).

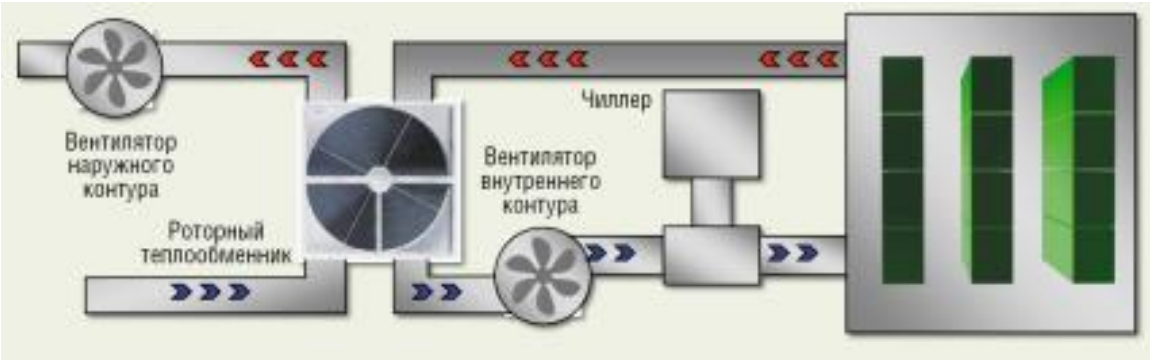

Рисунок 31 - Использование роторного рекуператора в системе непрямого фрикулинга

Рекуператор выполняет функцию теплообменника «воздух/воздух» и выступает в роли передатчика тепла между внешним и внутренним контурами. В данном случае отсутствует прямая подача воздуха с улицы, и при этом сохраняются все достоинства прямого фрикулинга.

Принцип охлаждения помещения ЦОД основывается на эффекте «затопления» холодным воздухом всего помещения благодаря избыточному давлению, искусственно создаваемому приточной вентиляцией. При скорости воздушного потока в два-три метра в секунду теплопритоки ИТ-оборудования сдуваются мощной струей. Этот фактор вместе с положительным дисбалансом давления в серверном помещении позволяет равномерно обеспечить холодным воздухом все оборудование. К несомненным преимуществам данного метода можно отнести

энергоэффективность (благодаря отсутствию компрессоров) и высокую экологичность — в серверной отсутствуют трубопроводы с токсичными теплоносителями (хладоном). Простота реализации и высокая ремонтопригодность позволяют использовать относительно дешевые и широко распространенные компоненты и детали, основу которых составляют воздуховоды и вентиляторы. Еще одно достоинство заключается в отсутствии необходимости формирования в ЦОД «холодных» и «горячих» коридоров, т.е. в конечном счете, в экономии площади.

Однако серьезным недостатком подобной схемы является то, что установка на базе роторного рекуператора не сможет эффективно охлаждать серверное помещение при наружных температурах выше $+22^0$C. В этом случае все равно потребуется чиллер, что значительно увеличит стоимость оборудования и усложнит обслуживание.

В случае использования наружного холодного воздуха для охлаждения хладагента в холодное время года холодильная машина выполняет лишь функцию теплообменника между теплоносителем и внешней средой, переключаясь на режим охлаждения лишь при наружных температурах выше $+22^0$C.

4.5.3. Альтернативные варианты

Существуют и альтернативные варианты, обеспечивающие нормальную работу оборудования в современных ЦОД, пока не получившие широкого распространения, но уже применяющиеся в отдельных ЦОД. К ним следует отнести:

— охлаждение испарением (адиабатное), использующее форсуночное распыление воды, при котором образующаяся влага удаляется в атмосферу, присутствуя только во внешнем контуре, который связан с внутренним через теплообменник;

— непосредственный подвод хладагента к источнику тепла (например, процессорам) без промежуточной среды — воздуха;

— использование естественных источников охлаждения (помимо воздуха) подземных источников воды, рек, морей океанов.

Очень перспективным представляется путь повышения допустимой рабочей температуры для ИТ-оборудования. В 2011 году появились два новых класса оборудования для ЦОД — A3 и A4, которые отсутствовали ранее. Допустимый температурный диапазон для такого оборудования увеличен до +40°C и +45°C соответственно. Создание «высокотемпературного» оборудования значительно уменьшит роль систем охлаждения и повысит энергоэффективность ЦОД. При этом

иногда оказывается, что разработка специального оборудования не требуется. Данные тестирования, проведенного Dell, показали, что серверы этой компании более 12 тыс. часов работали при температуре +40°C и влажности 85%, что соответствует примерно семи годам эксплуатации в условиях фрикулинга. При этом число отказов лишь незначительно превысило число отказов серверов при температуре +22°C и влажности 50%.

В ЦОД суперкомпьютера МГУ (см. Рисунок 32) реализованы сразу две из перечисленных инноваций - повышенная рабочая температура ИТ-оборудования и непосредственный подвод хладагента к источнику тепла (см. Рисунок 33).

Рисунок 32 - Внешний вид здания ЦОД суперкомпьютера МГУ

Рисунок 33 - Стойка для охлаждаемого оборудования суперкомпьютера (слева) и реализация непосредственного подвода хладагента к источнику тепла (справа)

Существуют пока не реализованные проекты «зеленых» ЦОД, размещаемых на плавающих платформах в области сильных приливных течений. Электроснабжение таких ЦОД могли бы обеспечить приливные

электростанции в совокупности с солнечными батареями, размещаемыми на крыше здания, и, возможно, ветряные электростанции. А для охлаждения оборудования могла бы быть использована забортная вода. Однако, упомянутый в разделе 1.1 строящийся в Норвегии высокоэффективный ЦОД Lefdal Mine Datacenter вполне можно отнести к «зеленым». Этот ЦОД расположен на 5 ярусах реконструированной шахты (см. Рисунок 34). Оборудование размещено в 75 камерах высотой до трех этажей и площадью 120 000 кв.м. Планируемая мощность, потребляемая ЦОД, составит 200 МВт, причем она на 100% будет генерироваться ветряными и приливными электростанциями. Охлаждение должно осуществляться водой фьорда температурой 7,5 градуса, связанного с четырьмя ледниками. ЦОД будет соответствовать третьему уровню стандарта TIA/EIA-942. Как уже упоминалось, планируемая энергоэффективность должна составить PUE=1,1.

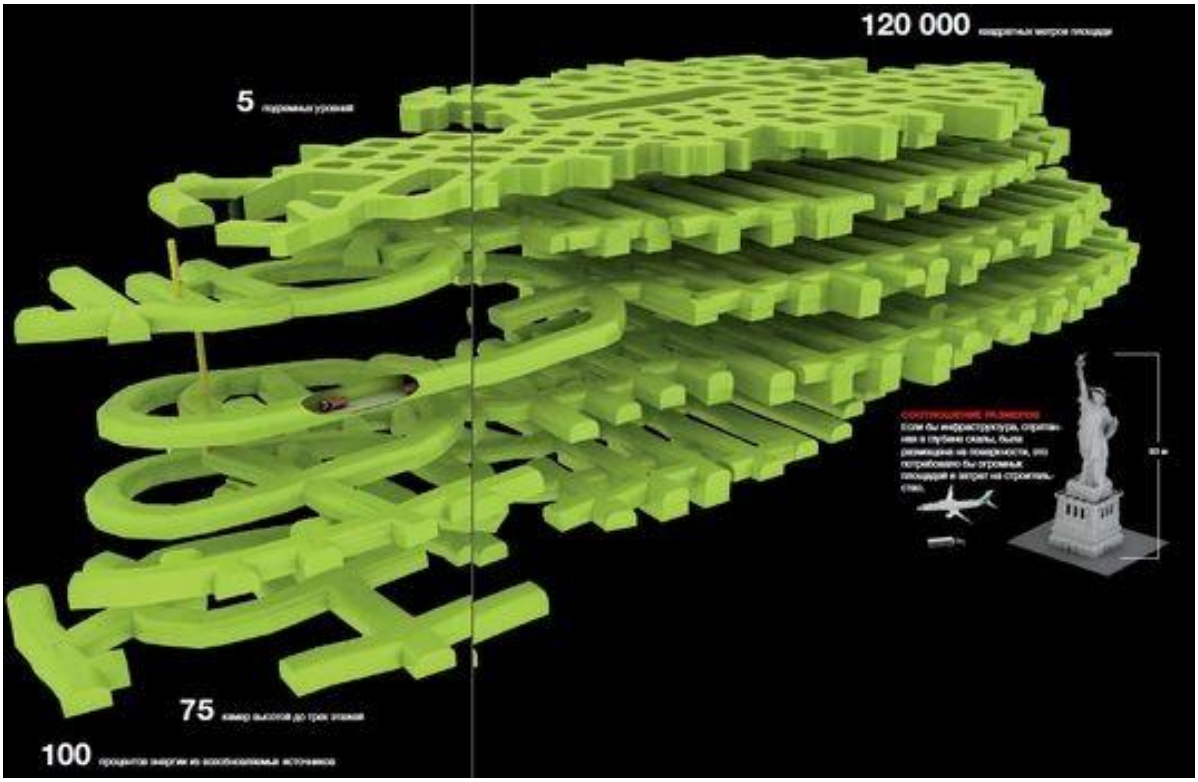

Рисунок 34 - Схема ЦОД Lefdal Mine Datacenter (Норвегия)

4.6. Системы раннего обнаружения пожара и газового пожаротушения

Максимально эффективная система газового пожаротушения в ЦОД должна сработать в зачаточной фазе развития пожара, т. е. когда происходит тление нагревающихся элементов или начальное воспламенение, и за время менее одной минуты потушить очаг возгорания. Комплекс же предупреждения о пожаре должен сообщить о

потенциальной возможности возгорания намного раньше, чем придется задействовать систему тушения. При этом следует отметить, что отключение электропитания у серверных шкафов или применение ручных средств пожаротушения неэффективно, поскольку снижает надежность работы ЦОД и повреждает оборудование.

Поэтому раннее обнаружение пожара достигается установкой большого количества высокочувствительных пожарных извещателей, максимально приближенных к возможному месту возгорания, увязанных в единую интеллектуальную систему оповещения о пожаре и совмещенных со средствами пожаротушения. Раннее обнаружение пожара достигается также комплексом организационных мероприятий. В него входит постоянный визуальный осмотр оборудования, соблюдение пожарных норм и правил, а также правил эксплуатации электроустановок.

Существующие системы сигнализации позволяют регистрировать концентрации дыма, начиная с уровня потери видимости на метр – 0,0015%, то есть на уровне, не ощутимом для человеческого глаза.

По своему типу пожарные извещатели делятся на:

— дымовые (распознаются твердые частицы дыма);

— пламени (распознается наличие пламени);

— тепловые (датчик распознает повышение температуры);

— газовые (реагирующие на газ);

— комбинированные (сочетающие в себе все четыре типа перечисленных выше датчиков).

В свою очередь, дымовые датчики (см. Рисунок 35) делятся на ионизационные (источник ионизирующего излучения + счетчик, заключенные в камеру), оптические (светодиод + фотодиод, заключенные в камеру) и линейные (то же, что и оптические, но без камеры). При задымлении сигнал на счетчике ионизирующего излучения или фотодиоде падает, и, соответственно, меняется ток в цепи, в которую они включены.

Рисунок 35 - Дымовые датчики

Датчики пламени (Рисунок 36) реагируют на ультрафиолетовое или инфракрасное излучение пламени. Они делятся на категории в зависимости от дальности обнаружения пламени.

Рисунок 36 - Датчики пламени

Тепловые датчики (Рисунок 37) реагируют на изменение тока в цепи, в которую включен элемент с отрицательным температурным коэффициентом.

Рисунок 37 - Тепловые датчики

И, наконец, в газовых датчиках (Рисунок 38) газ воздействует на вещество, находящееся на поверхности металлоксидной полупроводниковой пластины. При этом меняется емкость пластины и подается сигнал тревоги.

В соответствии со Сводом правил СП 5.13130.2009 при пожаротушении должны использоваться следующие газы: хладон 23, хладон 227еа, хладон 125, хладон 218, хладон 318Ц, азот, аргон, инерген, двуокись углерода, шестифтористая сера. Хладоны - это органические соединения, которые в зоне горения распадаются с образованием свободных радикалов, которые вступают в реакцию с первичными продуктами горения. Однако, некоторые виды хладона ядовиты и опасны для людей. Только хладон 23 и хладон 227еа применяются для защиты помещений, в которых могут находиться люди.

Рисунок 38 - Газовый датчик

Автоматические установки газового пожаротушения (Рисунок 39) должны обеспечивать:

— своевременное обнаружение пожара;

— задержку подачи газа на время, необходимое для эвакуации людей (если это необходимо);

— создание концентрации газа в защищаемом объёме или над поверхностью горящего материала на время, необходимое для тушения пожара;

— включать световые табло «Газ — уходи!» и «Газ — не входить!» и сигналы звукового оповещения.

Рисунок 39 - Установка газового пожаротушения

Разбавляющие атмосферу газы понижают процент кислорода в помещении до величины ниже 12%, после чего горение прекращается. К ним относятся такие сжатые газы, как аргон, азот, инерген. Однако, следует учесть, что их применение опасно для человека. Используется также тонкодисперсная вода и порошки. В данном случае существует принцип — чем дороже решение, тем больше останется исправного работоспособного оборудования после срабатывания системы пожаротушения. Наиболее дорогими, но и наиболее лояльными к оборудованию, являются огнетушащие смеси на основе хладонов либо инертных газов.

4.7. Комплексные системы безопасности

Системы охранного видеонаблюдения, а также контроля и управления доступом (СКУД) — важнейшие атрибуты современного ЦОД.

Наиболее простой и достаточно эффективной является СКУД на основе пластиковых карт. Она состоит из сервера управления, системы контроллеров и считывателей, а также карт (ключей). В комплексе с системой охранного видеонаблюдения она в состоянии обеспечить разумный уровень безопасности ЦОД.

На каждую обслуживаемую дверь устанавливаются считыватели карты, замок и видеокамера. Сотрудникам и клиентам по официальному запросу выдаются персональные ключи, которые являются пропуском на территорию физического периметра ЦОД. Типовые атрибуты ключа — фотография владельца, его персональные данные и название компании, в которой он работает. Ключ постоянно находится у сотрудника и обеспечивает беспрепятственный доступ в необходимые помещения. Их список и разрешенное время доступа прописываются на сервере

управления при заведении учетной записи и привязке к ней конкретного ключа.

Более сложные системы включают микрочип, вмонтированный в персональную карту, который позволяет охраннику увидеть фотографию владельца карты на специальном мониторе, подключенном к считывателю карт. Подобная система исключает передачу карты посторонним лицам и позволяет охране контролировать проход персонала на объект, не беря карты в руки.

Наиболее продвинутые и, соответственно, дорогие системы контроля доступа позволяют идентифицировать сотрудника по дактилоскопическим отпечаткам пальца, структуре радужной оболочки глаза или на основе интеллектуального анализа изображения его лица.

Наряду со СКУД, обязательной частью современных ЦОД является система охранного видеонаблюдения (ее следует отличать от системы технологического наблюдения, позволяющей удаленно контролировать работу оборудования). Она состоит из видеокамер, установленных так, чтобы осуществлять наблюдение практически за всеми техническими помещениями, входами-выходами, проходами и скрытыми площадями ЦОД. Видеоизображение поступает на мониторы службы безопасности и архивируется на цифровом носителе.

В процессе эксплуатации ЦОД большое значение уделяется регламентирующим и организационным процедурам, соблюдение которых формирует еще один "виртуальный" уровень безопасности.

4.8. Коммуникационная подсистема

4.8.1. Общие положения

Коммуникационная подсистема ЦОД представляет собой телекоммуникационную сеть, включающую в себя СКС (см. раздел 4.3), активное и пассивное телекоммуникационное оборудование, обеспечивающие единое информационное пространство ЦОД. С повышением требований к сетевой инфраструктуре и увеличением количества «тяжелых» приложений повышаются требования к пропускной способности, надежности и защите сети, ее управляемости и снижению стоимости эксплуатации. Данная подсистема обеспечивает как передачу данных внутри ЦОД (LAN), так и связь с сетью общего пользования (WAN). Отметим, что для качественного функционирования ЦОД коммуникационная подсистема должна подключаться к высокоскоростным каналам передачи данных. Кабельные (или радио)

линии связи могут находиться как на балансе организации-собственнике ЦОД, так и арендоваться у телеком-операторов.

Помимо передачи данных, коммуникационная подсистема обеспечивает корпоративную связь (IP-телефония) как между внутренними службами ЦОД, так и для связи с телефонной сетью общего пользования. Подробно корпоративные сети передачи данных и IP-телефонии рассмотрены в [1-5]. Поэтому ниже рассмотрим современные технологии, на базе которых могут организовываться коммуникационные подсистемы.

4.8.2. Программно-конфигурируемые сети и виртуализация сетевых функций

Современные тенденции, такие как рост числа подключенных к Интернету устройств, экспоненциальный рост объемов информации, развитие облачных технологий, Большие Данные приводят к увеличению объемов сетевого трафика и требуют конфигурации крупномасштабных сетей.

Упростить эту задачу могут технологии программно-конфигурируемых сетей SDN (Software-Defined Networking) и функциональной виртуализации сетей NFV (Network Function Virtualization), которые позволяют перевести сетевые элементы под контроль настраиваемого ПО, сделать их более интеллектуальными и облегчить управление ими.

Традиционное управление сетями обычно требует настройки каждого подключаемого к сети устройства отдельно. Например, конфигурирование списка контроля доступа виртуальной части локальной сети на нескольких коммутаторах требует входа на каждый из них и выполнение необходимых настроек. Подобный подход может потребовать значительных временных затрат при увеличении числа устройств и облачных сервисов.

В SDN уровни управления сетью и передачи данных разделяются за счет переноса функций управления (маршрутизаторами, коммутаторами и т. п.) в приложения, работающие на отдельном сервере (контроллере). Идея таких сетей была сформулирована специалистами университетов Стэнфорда и Беркли еще в 2006 году, одной из первых практическую реализацию SDN предложила компания Nicira, вошедшая в состав VMware.

Для ЦОД заинтересованность в использовании SDN вызвана тем, что данная технология позволяет повысить эффективность сетевого оборудования на 25–30%, снизить на 30% затраты на эксплуатацию

сетей, превратить управление сетями из искусства в инженерию, повысить безопасность и предоставить пользователям возможность программно создавать новые сервисы и оперативно загружать их в сетевое оборудование.

Основные принципы построения SDN:

— разделение процессов передачи и управления данными;

— единый унифицированный не зависящий от поставщика интерфейс между уровнем управления и уровнем передачи данных;

— логически централизованное управление сетью, осуществляемое с помощью контроллера с установленной сетевой операционной системой и реализованными поверх сетевыми приложениями;

— виртуализация физических ресурсов сети.

В архитектуре SDN можно выделить три уровня:

— *инфраструктурный уровень*, предоставляющий набор сетевых устройств (коммутаторов и каналов передачи данных);

— *уровень управления*, включающий в себя сетевую операционную систему, которая обеспечивает приложениям сетевые сервисы и программный интерфейс для управления сетевыми устройствами и сетью;

— *уровень сетевых приложений* для гибкого и эффективного управления сетью.

Наиболее перспективным и активно развивающимся стандартом для SDN является OpenFlow (OpenFlow версия 1.3) — открытый стандарт, в котором описываются требования, предъявляемые к коммутатору, поддерживающему протокол OpenFlow для удаленного управления.

Согласно спецификации 1.3 стандарта OpenFlow, взаимодействие контроллера с коммутатором осуществляется посредством протокола OpenFlow — каждый коммутатор должен содержать одну или более таблиц потоков (flow tables), групповую таблицу (group table) и поддерживать канал (OpenFlow channel) для связи с удаленным контроллером — сервером. Спецификация не регламентирует архитектуру контроллера и API для его приложений. Каждая таблица потоков в коммутаторе содержит набор записей (flow entries) о потоках или правила. Каждая такая запись состоит из полей-признаков (match fields), счетчиков (counters) и набора инструкций (instructions).

Механизм работы коммутатора OpenFlow достаточно прост. У каждого пришедшего пакета «вырезается» заголовок (битовая строка

определенной длины). Для этой битовой строки в таблицах потоков, начиная с первой, ищется правило, у которого поле признаков ближе всего соответствует (совпадает) заголовку пакета. При наличии совпадения над пакетом и его заголовком выполняются преобразования, определяемые набором инструкций, указанных в найденном правиле. Инструкции, ассоциированные с каждой записью таблицы, описывают действия, связанные с пересылкой пакета, модификацией его заголовка, обработкой в таблице групп, обработкой в конвейере и пересылкой пакета на определенный порт коммутатора. Инструкции конвейера обработки позволяют пересылать пакеты в последующие таблицы для дальнейшей обработки и в виде метаданных передавать информацию между таблицами. Инструкции также определяют правила модификации счетчиков, которые могут быть использованы для сбора разнообразной статистики.

Если нужного правила в первой таблице не обнаружено, то пакет инкапсулируется и отправляется контроллеру, который формирует соответствующее правило для пакетов данного типа и устанавливает его на коммутаторе (или на наборе управляемых им коммутаторов), либо пакет может быть сброшен (в зависимости от конфигурации коммутатора).

Запись о потоке может предписывать переслать пакет в определенный порт (обычный физический порт либо виртуальный, назначенный коммутатором, или зарезервированный виртуальный порт, установленный спецификацией протокола). Зарезервированные виртуальные порты могут определять общие действия пересылки: отправка контроллеру, широковещательная (лавинная) рассылка, пересылка без OpenFlow. Виртуальные порты, определенные коммутатором, могут точно определять группы агрегирования каналов, туннели или интерфейсы с обратной связью.

Записи о потоках могут также указывать на группы, в которых определяется дополнительная обработка. Группы представляют собой наборы действий для широковещательной рассылки, а также наборы действий пересылки с более сложной семантикой, например, быстрое изменение маршрута или агрегирование каналов. Механизм групп позволяет эффективно изменять общие выходные действия для потоков. Таблица групп содержит записи о группах, содержащие список контейнеров действий со специальной семантикой, зависящей от типа группы. Действия в одном или нескольких контейнерах действий применяются к пакетам, отправляемым в группу.

Разработчики коммутаторов могут быть свободны в реализации их внутренней начинки, однако процедура просмотра пакетов и семантика инструкций должны быть для всех одинаковы. Например, в то время как поток может использовать все группы для пересылки в некоторое множество портов, разработчик коммутатора может выбрать для реализации этого единую битовую маску внутри аппаратной таблицы маршрутизации. Другой пример — это процедура просмотра таблиц: конвейер физически может быть реализован с помощью различного количества аппаратных таблиц. Установка, обновление и удаление правил в таблицах потоков коммутатора осуществляются контроллером. Правила могут устанавливаться реактивно (в ответ на пришедшие пакеты) или проактивно (заранее, до прихода пакетов).

Управление данными в OpenFlow осуществляется не на уровне отдельных пакетов, а на уровне их потоков. Правило в коммутаторе OpenFlow устанавливается с участием контроллера только для первого пакета, а затем все остальные пакеты потока его используют.

Логически централизованное управление данными в сети предполагает вынесение всех функций управления сетью на отдельный физический сервер, называемый контроллером, который находится в ведении администратора сети. Контроллер может управлять как одним, так и несколькими OpenFlow-коммутаторами и содержит сетевую операционную систему, предоставляющую сетевые сервисы по низкоуровневому управлению сетью, сегментами сети и состоянием сетевых элементов, а также приложения, осуществляющие высокоуровневое управление сетью и потоками данных.

Сетевая ОС (СОС) обеспечивает приложениям доступ к управлению сетью и постоянно отслеживает конфигурацию средств сети. В отличие от традиционного толкования термина ОС, под СОС понимается программная система, обеспечивающая мониторинг, доступ и управление ресурсами всей сети, а не ее конкретного узла.

Подобно традиционной операционной системе, СОС обеспечивает программный интерфейс для приложений управления сетью и реализует механизмы управления таблицами коммутаторов: добавление, удаление, модификацию правил и сбор разнообразной статистики. Таким образом, фактически решение задач управления сетью выполняется с помощью приложений, реализованных на основе API сетевой операционной системы, позволяющих создавать приложения в терминах высокоуровневых абстракций (например, имя пользователя и имя хоста), а не низкоуровневых параметров конфигурации (например,

IP- и MAC-адресов). Это позволяет выполнять управляющие команды независимо от базовой топологии сети, однако требует, чтобы СОС поддерживала отображения между высокоуровневыми абстракциями и низкоуровневыми конфигурациями.

В каждом контроллере имеется хотя бы одно приложение, которое управляет коммутаторами, соединенными с этим контроллером, и формирует представление о топологии физической сети, находящейся под управлением контроллера, тем самым централизуя управление. Представление топологии сети включает в себя топологию коммутаторов, расположение пользователей, хостов, других элементов и сервисов сети. Представление также включает в себя привязку между именами и адресами, поэтому одной из важнейших задач, решаемых СОС, является постоянный мониторинг сети. Таким образом, СОС позволяет создавать приложения в виде централизованных программ, использующих высокоуровневые имена, на основе таких алгоритмов, как, например, алгоритм Дейкстры поиска кратчайшего пути в графе, вместо сложных распределенных алгоритмов вроде алгоритма Беллмана – Форда, в терминах низкоуровневых адресов, которые используются в современных маршрутизаторах.

Одна из идей, активно развиваемая в рамках SDN, — это виртуализация сетей с целью более эффективного использования сетевых ресурсов. Под виртуализацией сети понимается изоляция сетевого трафика — группирование (мультиплексирование) нескольких потоков данных с различными характеристиками в рамках одной логической сети, которая может разделять единую физическую сеть с другими логическими сетями или сетевыми срезами (network slices). Каждый такой срез может использовать свою адресацию, свои алгоритмы маршрутизации, управления качеством сервисов и т. д.

Виртуализация сети позволяет: повысить эффективность распределения сетевых ресурсов и сбалансировать нагрузку на них, изолировать потоки разных пользователей и приложений в рамках одной физической сети. Администраторы разных уровней получают возможность использовать свои политики маршрутизации и правила управления потоками данных, проводить эксперименты в сети, используя реальную физическую сетевую инфраструктуру, использовать на каждом уровне только те сервисы, которые необходимы конкретным приложениям.

Благодаря снятию с коммутаторов нагрузки по обработке тракта управления, SDN позволяет этим устройствам направить все свои

ресурсы на ускорение перемещения трафика, что существенно повышает производительность. При этом за счет виртуализации управления сетью снижаются расходы на их построение и сопровождение. По результатам тестов, проведенных на базе крупнейших провайдеров США, использование SDN позволяет на 20–30% увеличить утилизацию ресурсов ЦОД и в несколько раз снизить эксплуатационные расходы.

Программные средства SDN позволяют администраторам добавлять новую функциональность к уже имеющейся сетевой архитектуре. При этом новые функции будут работать на многих платформах — их не придется реализовывать заново во встроенном программном обеспечении коммутаторов каждого поставщика.

На централизованном контроллере SDN системный администратор может наблюдать всю сеть в едином представлении, за счет чего повышаются удобство управления, безопасность и упрощается выполнение ряда других задач. Действительно, поскольку администратор видит все потоки трафика, то ему легче замечать вторжения, назначать приоритеты различным типам трафика и разрабатывать правила реагирования сети при заторах и проблемах с оборудованием.

Теоретически неограниченные возможности сетей SDN к расширению позволяют строить реальные облака (см. раздел 9), масштабируемые в зависимости от решаемых задач. При этом сеть обладает требуемой «интеллектуальностью», необходимой, в частности, для оркестровки работы обширных групп коммутаторов.

Программно-конфигурируемые сети открывают большие возможности для промышленности и бизнеса, позволяя решать задачи повышения пропускной способности каналов, упрощения управления сетью, перераспределения нагрузки, повышения масштабируемости сети. Каждая компания, в зависимости от своих потребностей, может внедрить решение, соответствующее конкретно ее задачам. Данной технологией могут заинтересоваться хостеры и провайдеры, владельцы ЦОД и операторы связи, финансовые и банковские структуры, телекоммуникационные компании, которым внедрение SDN позволит повысить эффективность их работы.

Ряд мировых производителей еще в 2012 году имели готовые к продаже собственные решения в области SDN. Например, Cisco Systems, помимо запуска линейки коммутаторов Nexus и Catalyst 35XX, способных работать как в традиционных сетях, так и в SDN, разработала платформу Open Network Environment, специально предназначенную для

поддержки решений SDN. В том же году компания Google объявила о переводе всей внутренней сети для обмена трафиком между своими ЦОД по всему миру на SDN, самостоятельно изготовив коммутаторы OpenFlow, поскольку существующие аналоги на рынке были в тот момент для компании недоступны. Использование SDN позволило компании выбирать оборудование, строго соответствующее необходимому ПО, осуществлять централизованное управление сетью и потоками данных, оптимизировать процессы тестирования и мониторинга.

В России в начале 2016 года «КоммИТ Кэпитал» корпоративный венчурный фонд «Ростелекома» инвестировал около 100 миллионов рублей в ООО «Программируемые сети» (бренд Brain4Net), решения которого ориентированы на построение сетей операторов и корпоративных сетей на базе архитектуры SDN и смежной технологии NFV. До конца 2016 года планируется запустить первые пилотные зоны.

По технологиям SDN и NFV «Ростелеком» уже сотрудничает с отечественным Центром прикладных исследований компьютерных сетей (ЦПИКС). Целью сотрудничества является исследование возможностей и условий внедрения технологий SDN и NFV в сети «Ростелекома». В частности, компании сосредоточатся на разработке архитектуры, средств управления SDN-сетями, приложений для SDN-контроллера, протоколов управления и программного обеспечения для SDN-коммутаторов в региональных сетях и ЦОД, а также на разработке платформы и виртуальных сетевых сервисов. Сотрудничество направлено на реализацию программы импортозамещения в области программного обеспечения Министерства цифрового развития, связи и массовых коммуникаций РФ.

Другие российские операторы в 2016 году также изучали внедрение технологий SDN и NFV. Так в ПАО "МегаФон" вопросы, связанные с SDN/NFV, в этот период находились на стадии анализа и возможного внедрения в инфраструктуре в части сервисных платформ. А ПАО "ВымпелКом" (бренд "Билайн") активно изучал и тестировал технологии и решения, ориентированные на NFV. В частности, были успешно проведены тестирования и внедрения ряда виртуализированных сетевых функций.

4.9. Системы мониторинга и управления

В реальной интегрированной системе управления инфраструктурой ЦОД приходится анализировать очень большое число

источников данных и управляющих воздействий, включая контроль ИТ-систем (серверов, СХД), активного сетевого оборудования, распределенных сетей передачи данных, инженерных и охранных систем.

Реализация этих функций достигается путем создания систем управления класса Data Center Infrastructure Management (DCIM). Как и во многих других областях ИТ, единой терминологии в этой области нет. Некоторые авторы понимают под DSIM исключительно системы, обеспечивающие согласованное функционирование инженерной инфраструктуры и безопасности. Мониторинг ИТ-систем ЦОД осуществляется с помощью других средств, например, управления виртуализацией серверов (раздел 2.6), ПО управления хранением – SDS (раздел 0) или программно-конфигурируемой сетью – SDN (раздел 4.8). Причем средства контроля ИТ-структуры и инженерных систем могут быть даже пространственно разнесены, как это сделано в упоминавшемся ранее ЦОД Федеральной налоговой службы (Рисунок 40).

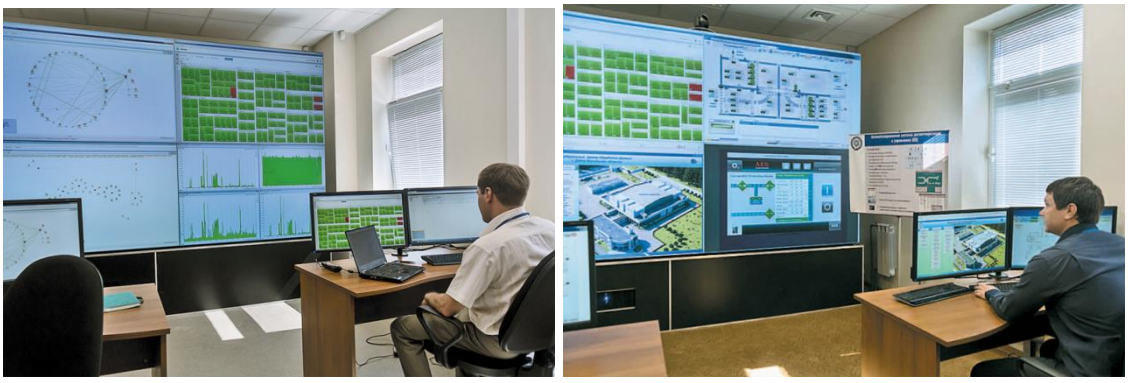

Рисунок 40 - Диспетчерские мониторинга ИТ-инфраструктуры (слева) и инженерной инфраструктуры (справа) ЦОД ФНС в г.Дубна

Поскольку для всеобъемлющей системы мониторинга и управления ЦОД в целом в 2012 году появился иной термин, в дальнейшем под DSIM будем понимать только систему управления и мониторинга инженерных подсистем и подсистемы безопасности. Данная система обеспечивает:

— слаженную работу большого количества подсистем;

— быстроту и высокое качество диагностики отказов в пассивном и активном оборудовании, а также в программном обеспечении;

— исключение влияния человеческого фактора;

— автоматическое включение системы пожаротушения при обнаружении возгорания или задымления;

— контроль и интерактивное отражение:

— состояния всего оборудования,
— электрической нагрузки,
— температуры и влажности среды,
— затопления и задымление помещения,
— открывания дверей,
— попыток несанкционированного доступа в помещения,
— сообщения об авариях,
— предупреждения об ошибках.

Контрольные вопросы

1. Общие положения инженерных подсистем ЦОД.
2. Основные параметры, влияющие на выбор помещения для ЦОД.
3. Структура кабельной системы ЦОД.
4. Требования, предъявляемые к гибкости и масштабируемости ЦОД.
5. Повышение надежности кабельных систем ЦОД на уровне ее структуры.
6. Уровни защиты от несанкционированных действий.
7. Составные части и схемы построения ИБП.
8. Организация систем гарантированного питания.
9. Организация традиционных систем кондиционирования.
10. Способы уменьшения общего энергопотребления ЦОД в системах охлаждения.
11. Альтернативные варианты, обеспечивающие нормальную работу оборудования в современных ЦОД.
12. Системы раннего обнаружения пожара и газового пожаротушения.
13. Комплексные системы безопасности.
14. Системы мониторинга и управления инфраструктурой ЦОД.

5. Информационная безопасность ЦОД

5.1. Особенности ЦОД, как объекта защиты информации

На организацию защиты информации в ЦОД влияют такие ключевые особенности этих объектов, как:

— концентрация больших вычислительных мощностей в ограниченном пространстве;

— обслуживание большого количества пользователей, приложений, бизнес-процессов;

— совместная обработка в одной программно-аппаратной среде информации разного характера — открытой информации, персональных данных, информации, содержащей коммерческую тайну, и т. п.

Поэтому в работе ЦОД основными рисками информационной безопасности, приводящими к наиболее тяжелым последствиям, оказываются:

— приостановка деятельности ЦОД;

— масштабное хищение или модификация информации за счет внешнего или внутреннего взлома.

Нарушителей информационной безопасности ЦОД следует разделять на внутренних, имеющих права доступа различной категории на территорию контролируемой зоны ЦОД и к его ресурсам, и внешних, не имеющих таких прав.

Типичной угрозой для ЦОД являются целевые атаки, в которых эффективно используется инсайд.

Основные цели атак на ЦОД:

— получение, уничтожение или модификация ценной информации;

— остановка работы ЦОД и тем самым нанесение ущерба репутации владельца или пользователям;

— завладение удаленным управлением для изменения внутренних процессов системы и т. п.

Риски масштабного хищения информации, обусловленные большими объемами данных, которыми оперирует ЦОД, связаны с действиями внешних злоумышленников, которым могут помогать инсайдеры из ЦОД. Для этого злоумышленники выявляют и используют уязвимости в системе разграничения доступа в инфраструктуре ЦОД. Злоумышленники могут легально арендовать виртуальную площадку, размещенную в ЦОД, и использовать ее далее для проникновения в другие информационные системы, расположенные по соседству.

Угрозу для ЦОД представляет также использование открытого ПО, которое требует особенно внимательного отношения к разработке алгоритмов системного и прикладного ПО для ЦОД, а также к своевременной установке обновлений.

Современный ЦОД — это, как правило, физически изолированная от пользователя инфраструктура, что повышает значимость шифрования информации, резервирования каналов связи и защищенности от DDoS-атак (Distributed Denial of Service - распределенная атака типа «отказ в обслуживании»). Среди технологий информационной безопасности можно выделить контроль трафика, межсетевое экранирование, защиту от проникновений за счет уязвимостей с помощью системы

предотвращения вторжений (Intrusion Prevention System – IPS) и системы обнаружения вторжений (Intrusion Detection System – IDS).

5.2. Технологические особенности ЦОД и информационная безопасность

Специфика организации информационной безопасности в ЦОД связана, прежде всего, с использованием виртуализации и включением ЦОД в облачные структуры (см. раздел 9).

Предметом атаки в виртуальной среде становится гипервизор, поскольку он представляет собой единую точку отказа в виртуальной инфраструктуре и открывает новое направление в информационной безопасности. И хотя его изолированность от внешней по отношению к нему среды обеспечивает изначально высокую защищенность, в системы информационной безопасности виртуальных сред уже стали вводить средства контроля целостности гипервизора. Если последний оказывается захваченным злоумышленниками, то установленные внутри виртуальных машин средства информационной безопасности, такие как антивирусы, межсетевые экраны и т. п. будут неспособны защитить данные виртуальной среды.

Поскольку физически разделить виртуальные машины невозможно, так же как и использовать аппаратные средства обнаружения и предотвращения атак между ними, то следует размещать средства защиты непосредственно на серверах виртуализации. Прежде всего, это такие программные средства защиты, как межсетевой экран, система обнаружения и предотвращения вторжений, система контроля целостности, система анализа журналов, система защиты от вредоносного кода.

В современных ЦОД повышаются риски нарушения конфиденциальности, целостности и подлинности информации, связанные с тем, что при удаленном доступе к размещенным в ЦОД информационным системам, каналы передачи данных, как правило, неподконтрольны компании-пользователю и обеспечиваются провайдером. Злонамеренный инсайд на стороне провайдера, взлом интерфейсов управления или недостаточный контроль за деятельностью пользователей, DDoS-атаки на ЦОД провайдера могут привести к краже, подделке или уничтожению информации, к прекращению доступа к сервисам, остановке бизнес-процессов.

В связи с этим провайдеры, обеспечивающие доступ к ЦОД, должны перейти от принципа: «делаю, что могу» к принципу «делаю, как требуют».

Высокие требования предъявляются и к производительности средств защиты (в первую очередь, речь идет об их сетевой пропускной способности), а также к необходимости экономного расходования вычислительных ресурсов виртуальной среды. Целесообразно нагрузку, связанную с обеспечением безопасности, переносить на выделенные серверы. Серьезную угрозу представляют также зараженные выключенные виртуальные машины. При очередном включении они могут скомпрометировать безопасность всего ЦОД. Поэтому целесообразно проводить детектирование и устранение заражений в режиме офлайн.

Существуют также риски, связанные с обязанностью провайдера услуги содействовать правоохранительным органам при проведении оперативно-следственных мероприятий, поскольку из-за претензий к одному клиенту ЦОД доступа к сервисам могут быть лишены и другие. Это обстоятельство может оказаться серьезным препятствием для использования услуг ЦОД, связанных с использованием критически важных ресурсов.

Специфические угрозы для ЦОД связаны также с появлением новой ИТ-роли — администратора виртуальной инфраструктуры, действия которого трудно контролировать на уровне операционной среды виртуальных машин без дополнительных наложенных средств. Администраторы, имеющие в силу своих должностных обязанностей непосредственный доступ к информационным системам клиентов ЦОД, представляют самую серьезную угрозу информационной безопасности. При этом риски связаны как с их преднамеренными действиями, преследующими злой умысел, так и с их ошибками.

5.3. Информационная безопасность в ЦОД и человеческий фактор

Появление в ЦОД администратора виртуальной инфраструктуры повышает значимость противодействия как злонамеренному инсайду, так и непреднамеренным ошибкам со стороны этих специалистов.

Противодействие инсайду следует начинать с правильного разграничения доступа к ресурсам. Необходимо исключать единоличный доступ специалистов к критически важным системам. Этому должна препятствовать жесткая политика информационной безопасности, обязывающая привлекать к контролю использования таких систем

нескольких сотрудников с различным уровнем прав, а также тщательный контроль исполнения самих этих политик. Разделение ролей и сфер ответственности между разными специалистами позволяет исключить возможность появления “суперпользователя”. Например, за назначение прав доступа к защищаемым ресурсам клиентов ЦОД должен отвечать администратор безопасности, который, в свою очередь, не получает прав доступа к самим ресурсам.

Основой стратегии, направленной на снижение рисков, связанных с инсайдом, должно стать максимальное исключение из функционирования системы информационной безопасности ЦОД человеческого фактора. Важным шагом в этом направлении является централизация управления средствами защиты информации. Устанавливать и настраивать, например, межсетевой экран администратору гораздо удобнее и быстрее со своего рабочего места, чем на каждом объекте в отдельности.

5.4. Нормативная база информационной безопасности ЦОД

Следует отметить, что даже в последних редакциях документов, регламентирующих защиту информации в информационных системах, включая Федеральный закон “О персональных данных”, отсутствуют регламенты использования виртуализации и облачных вычислений с позиций информационной безопасности. Существует насущная потребность в разработке соответствующей нормативной базы, методов сертификации процессов оказания услуг и инфраструктуры провайдера, в том числе, по работе с информацией разных классов требований к защите.

Отсутствие нормативной базы, регулирующей соответствие ЦОД требованиям к размещению и обработке информации разной категории, создает проблемы потребителям услуг ЦОД, которым необходимы закрепленные договором обязательства по соблюдению в отношении размещаемой клиентами информации требований федеральных законов, включая закон “О персональных данных”. В настоящее время типовой договор провайдеров предполагает предоставление услуг “как есть”, что переносит все риски, связанные с защитой информации на потребителей услуг. Именно это обстоятельство заметно сдерживает развитие рынка коммерческих ЦОД, так как неопределенность в части обеспечения информационной безопасности останавливает значительное число потенциальных потребителей.

Для ЦОД, эксплуатируемых несколькими юридическими лицами, разрешение некоторых вопросов информационной безопасности по упомянутым выше причинам могут вызвать юридические проблемы и создать конфликтные ситуации.

5.5. Фактор доверия и информационная безопасность в ЦОД

Отсутствие нормативного регулирования защиты информации в ЦОД увеличивает роль фактора доверия в отношениях между провайдерами и клиентами. Эти отношения во многом зависят от того, насколько тщательно поставщик услуг предусмотрел различные аспекты обеспечения информационной безопасности и заложил их в свою систему. Трудности, связанные с обеспечением информационной безопасности, провайдеры зачастую стараются переадресовывать самим клиентам, если предоставляемые им ресурсы допускают доработку систем провайдеров под их требования. Поэтому следует максимально внимательно оценивать поставщика услуг и договор с ним.

В настоящее время доля использования коммерческих ЦОД в ИТ-проектах начинает вытеснять собственные площадки. Для этого есть ряд причин: более высокий уровень маштабируемости, быстрый для клиента запуск ИТ-решений, круглосуточно доступный компетентный персонал и другие преимущества, реализовать которые самостоятельно сложнее и дороже. При использовании сервисной модели в информационных технологиях все зависит от степени готовности клиента делегировать оператору ЦОД определенные задачи, в том числе, в области обеспечения информационной безопасности. А далее уже оператор разрабатывает сценарии поддержки политики информационной безопасности клиента и контроля за ее исполнением. При этом окончательное заключение об отношениях между провайдером и клиентом можно дать, только проанализировав стратегические планы конкретного клиента.

Способствовать установлению доверительных отношений между клиентами и поставщиками услуг ЦОД может реализация на стороне провайдера возможности контроля исполнения политики безопасности клиента. В настоящее время на российском рынке уже появляются даже сертифицированные продукты, с помощью которых это можно реализовать. Безусловно, свою положительную роль сыграет и сертификация ЦОД по уровню стабильности работы, включающая вопросы информационной безопасности (см. раздел 0).

Контрольные вопросы

1. Особенности ЦОД как объекта защиты информации.
2. Специфика организации информационной безопасности в ЦОД.
3. Влияние «человеческого фактора» на информационную безопасность в ЦОД.
4. Нормативная база информационной безопасности ЦОД.
5. Роль фактора доверия в информационной безопасности ЦОД.

6. Концепция программно-определяемого ЦОД и его ее реализация

6.1. Основные положения концепции программно-определяемого ЦОД

Одной из новых и интересных идей, возникших в 2012 году, стала идея программно-определяемых (также в литературе применяется термин «программно-конфигурируемых») ЦОД (Software Defined Data Center, SDDC). Эта концепция является естественным развитием решений виртуализации, развиваемым компанией VMware. В качестве основной единицы виртуализации при этом предполагается не виртуальный сервер или виртуальная СХД, а полностью виртуальный ЦОД. При этом необходимым условием создания такого ЦОД является виртуализация абсолютно всех вычислительных ресурсов.

Виртуализация — одна из ключевых технологий, вошедших за несколько десятилетий в корпоративную инфраструктуру. Наибольших успехов удалось добиться в сегменте серверной виртуализации (см. раздел 2.6), причем ее применение резко расширяется. Виртуальные решения нашли свое воплощение и в СХД, где были реализованы программно-определяемые системы хранения – SDS (см. раздел 0).

Серьезным тормозом в реализации всех возможных выгод от использования виртуализированных сред была негибкая и плохо управляемая сетевая инфраструктура. И именно виртуализация сетей – SDN (см. раздел 0) должна коренным образом изменить ситуацию.

Реализация концепции SDDC идет в нескольких направлениях. Сетевая индустрия активно работает над протоколом OpenFlow. Производители систем хранения тоже все больше ориентируют свою продукцию на технологии виртуализации. Наконец, производители гипервизоров развивают функциональность автоматического создания и конфигурации виртуальных ресурсов.

Суть концепции SDDC заключается в окончательном абстрагировании от конкретного оборудования и системного ПО,

необходимых для функционирования приложений. То есть виртуализируются не только серверы, но и остальные инфраструктурные компоненты: дисковые массивы, сети, контроллеры. При этом для каждого пользователя программных средств может быть создан его собственный ЦОД с уникальными характеристиками, изолированный от других клиентов.

Создание концепции SDDC стало абсолютно логичным шагом, продолжающим разработки компаний, и в первую очередь VMware, в области виртуализации, придающим законченность идее комплексной виртуализации. Именно SDDC способна придать новый импульс развитию облачных сервисов (см. главу 9). Предполагается, что SDDC позволит делать облачные сервисы намного более гибкими, чем раньше, а также серьезно экономить на необходимой для их функционирования инфраструктуре. Концепция SDDC требует существенного пересмотра подходов во многих областях ЦОД. Платой за гибкость и эффективное использование ресурсов является потребность во взаимодействии между абсолютно всеми виртуальными устройствами. Иначе говоря, каждый компонент ЦОД должен «знать» все о состоянии остальных компонентов. При этом гипервизор должен быть способен динамически перераспределять использование каждого вида ресурсов для обеспечения необходимой производительности.

Усилия VMware в продвижении концепции программно-определяемых ЦОД не случайны. Ее позиции стали особенно сильны после приобретения компании Nicira — разработчика решений в области виртуализации сетей - SDN.

На сегодняшний день продуктом, способным реализовать подходы SDDC, является VMware Cloud Management, охватившим три области — предоставление сервисов, управление операциями и контроль бизнес-процессов. Безусловно, значительная часть функциональности VMware Cloud Management существовала и раньше, в том числе в решениях других производителей, однако лишь сейчас стала возможной полная виртуализация инфраструктуры, а также автоматизация сервисов.

Концепция SDDC еще слишком нова, многие компании используют ее отдельные компоненты, но о применении в полном объеме говорить пока не приходится. Необходимо не только продвижение и популяризация самой идеи среди заказчиков — крайне важна активная работа других разработчиков по созданию конкурентных продуктов. При этом не стоит забывать, что их понимание SDDC может несколько отличаться. На данный момент далеко не все производители

оборудования обеспечивают в своих решениях необходимый уровень интеллекта и способности к интеграции. Им необходимо провести большую работу, чтобы SDDC из еще одной аббревиатуры стала реальностью.

6.2. Базовые уровни программно-определяемого ЦОД

В SDDC выделяют три базовых уровня:

— уровень абстрагирования аппаратных средств (вычислительных, сетевых ресурсов и ресурсов хранения), для чего используются виртуализация и облачная модель;

— программно-определяемые сервисы, функционирующие в виртуальных машинах (включая межсетевые экраны, балансирование нагрузки, дедупликацию данных, подсистемы обнаружения и предотвращения вторжений - IDS/IPS и др.);

— автоматизацию на основе определяемых правил (политик).

Ожидается, что SDDC сделает развертывание сервисов, предоставление ресурсов, управление конфигурациями и другие операции в ЦОД более интеллектуальными благодаря наличию трех названных выше уровней.

Контрольные вопросы

1. Суть концепции SDDC.
2. Направления реализации концепции SDDC.
3. Преимущества и недостатки внедрения и использования концепции SDDC.
4. Архитектура SDDC.

7.«Коробочные» ЦОД различных вендоров

Вычислительная инфраструктура современных ЦОД представляет собой сложную комбинацию серверов, систем хранения данных, сетевого оборудования, объединенных физически и логически в рамках очень небольшого пространства. Создать подобную инфраструктуру из оборудования различных производителей достаточно сложно, в результате чего результат не всегда соответствует ожиданиям. Поэтому производители оборудования попытались создать комплексные системы, содержащие все основные компоненты ЦОД, которые можно назвать «коробочными» решениями. Такие решения включают в себя серверы (обычно, x86), СХД, коммутаторы ЛВС, а также набор специального ПО для виртуализации и управления. Все это, как правило, установлено в

шкаф, обеспеченный системой кондиционирования, связано между собой, протестировано и готово к работе.

Характерной особенностью всех комплексных систем, представленных ниже, является их ориентация на облачные вычисления, которые будут рассмотрены в главе 9, использование технологий высокой плотности для размещения оборудования (например, блейд-серверов), а также применение набора специализированного ПО для виртуализации и удаленного управления. Отметим, что большинство упомянутых систем предварительно сконфигурированы изготовителем (как физически, так и программно), и для их запуска в коммерческую эксплуатацию надо произвести минимум действий.

7.1. Решение корпорации Dell

На рынке «коробочных» ЦОД компания Dell представлена системой «Dell vStart», которая представляет собой установленные в стойку серверы, СХД, сетевые устройства, источники бесперебойного питания, уже объединенные кабельными соединениями, с полностью готовым к запуску программным обеспечением оптимизации загрузки серверов, мониторинга, удаленного обновления BIOS и микропрограмм, а также готовыми к работе гипервизорами (см. рисунок 41). В зависимости от цифры, следующей за наименованием системы, система разворачивает 50, 100 или 200 виртуальных серверов, что делает данное решение пригодным для использования на предприятиях как среднего так и крупного бизнеса.

Рисунок 41 - Dell vStart компании Dell

Технические решения, реализованные в «Dell vStart», позволяют создать мощную, высокодоступную и хорошо масштабируемую виртуальную среду «в один клик». Они дополняются важным функционалом повышения производительности и управляемости линейки серверов 12-го поколения (12G) Dell PowerEdge, у которых значительно улучшены параметры энергетической эффективности. Кроме того, за счет специального инструмента OpenManage Power Center администраторы смогут дополнительно оптимизировать энергопотребление на уровне сервера, стойки, ряда стоек и ЦОД с одной консоли.

Dell vStart берет на себя решение всех задач ИТ-персонала по проектированию виртуальной инфраструктуры, сборке, интеграции и настройке различных элементов, а также тестированию созданной системы на соответствие требуемым параметрам скорости работы, надежности и возможности масштабирования. Фактически вместе с Dell vStart заказчик получает готовую виртуальную инфраструктуру своего ЦОД.

7.2. Решение корпорации IBM

Основными серийными системами для IBM были и остаются мейнфреймы, которые с определенной натяжкой можно считать «коробочными» ЦОД из-за их относительно небольших размеров. Уже в 2016 году корпорация представила новый мейнфрейм, доступный для небольших компаний и обеспечивающий дополнительный уровень безопасности с помощью шифрования данных без потери скорости и производительности. Новая система IBM z13s разработана и оптимизирована для гибридных облачных сред и способна обеспечить защиту особо важной информации и операций (см. рисунок 42). Корпорация также анонсировала новые партнерства в области безопасности и внедрение инноваций с высокой степенью интеграции с мейнфреймом.

Рисунок 42 - Мэйнфрейм zEnterprise фирмы IBM

Скорость обработки защищенных операций в сочетании с новой аналитической технологией для обнаружения вредоносной активности и встроенными сервисами IBM Security позволяют владельцам даже небольших компаний успешно развивать свой бизнес.

В качестве «ядра» системы используется мейнфрейм IBM z196, оснащенный новыми CISC-процессорами, но к нему может быть подсоединен модуль расширения, технологически представляющий собой обычный серверный шкаф, в котором установлены до четырех блейд-шасси, коммутаторы и блоки распределения питания.

Обе системы объединяются в общую виртуализированную среду и управляются с помощью новой программной системы разработки IBM. В системе z196 может быть установлено до 24 специальных четырехъядерных процессоров, работающих на частоте 5,2 ГГц, которые устанавливаются в специальные картриджи — по шесть штук в каждом. В один мейнфрейм помещается до четырех таких картриджей, что в сумме дает 96 вычислительных ядер. Также в системе может быть

установлено до трех ТБ оперативной памяти, организованной в отказоустойчивый массив. Одной из важных функций z10 является возможность оперативного перераспределения дискового пространства и процессорных ресурсов без остановки работы приложений. Если производительности одной системы будет недостаточно, возможно объединение 32 мейнфреймов в общую вычислительную систему.

Мейнфрейм z13s включает обновленные и аппаратно-ускоренные шифровальные карты сопроцессора с защитой от несанкционированного доступа с более быстрыми процессорами и большим объемом памяти. Они позволяют увеличить скорость шифрования в два раза по сравнению с серверами средней производительности. Таким образом, благодаря использованию функции защиты от несанкционированного доступа, появляется возможность обработки в два раза большего числа крупномасштабных защищенных протоколов. Например, новый мейнфрейм способен обрабатывать в два раза больше запросов, поступающих с компьютера или мобильных устройств, при более низкой стоимости транзакций.

«z Systems» может также использовать приложение «z Systems» Cyber Security Analytics, которое обеспечивает оптимизированный мониторинг угроз на основе поведенческого анализа. Приложение запоминает поведение пользователей и затем помогает обнаружить аномальные комбинации на платформе, предупреждая администраторов о потенциально опасной активности. Серверы «z Systems» используют программное обеспечение системы безопасности IBM Security QRadar, которое сопоставляет данные, полученные из более чем 500 источников, и помогает определить, являются ли связанные с защитой происшествия просто аномалиями или они несут потенциальную угрозу. Таким образом, «z Systems» предоставляет интеллектуальные решения в сфере безопасности, которые обеспечивают бесперебойную, основанную на передовых аналитических методах защиту.

Корпорация объединила мейнфрейм и решения IBM Security, направленные на управление привилегированной идентификацией и защиту данных с сенсорных устройств. В сочетании с серверами «z Systems» эти решения позволяют обеспечить постоянную защиту гибридной облачной среды пользователя.

Сервис IBM Security Identity Governance and Intelligence помогает предотвратить случайные или злоумышленные утечки корпоративных данных при помощи системы управления и контроля доступа на основе известного порядка действий. Используя аналитические сведения,

приложение IBM Security Guardium обеспечивает сохранность информации путем интеллектуального микропроцессорного мониторинга данных. Такой мониторинг отслеживает, кому и какие специальные данные были предоставлены, и помогает быстро обнаружить источники угроз в случае атаки. Приложения IBM Security zSecure и QRadar используют уведомления об опасности в режиме реального времени, что позволяет сосредоточиться на обнаруженных критических угрозах безопасности — наиболее важном аспекте деятельности предприятия.

7.3. Решение компании Cisco

Рынок комплексных решений для ЦОД оказался настолько заманчивым, что за его освоение взялись даже те компании, которые никогда на этот рынок не претендовали. В частности, еще в 2010 году компания Cisco не только разработала собственный блейд-сервер, но и вместе с EMC и VMware образовала технологическую коалицию, результатом которой стал выпуск комплексной системы Vblock (см. рисунок 43).

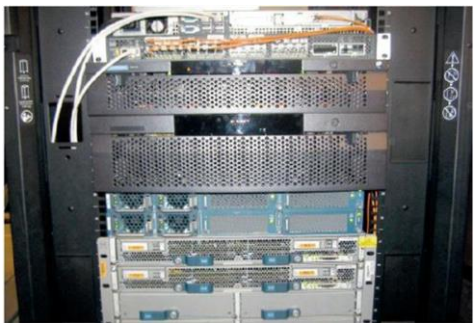

Рисунок 43 - «Коробочный» ЦОД Vblock фирмы Cisco

Решение представляет собой серверный шкаф, в котором установлены модульные серверы и коммутаторы разработки Cisco, СХД компании EMC, набор ПО для виртуализации фирмы VMware и специализированные фирменные приложения всех трех компаний. Кроме того, выполнены все необходимые кабельные подключения оборудования. Для дифференциации рыночных сегментов Vblock разделен на три уровня — 0, 1 и 2.

Конфигурация начального уровня Vblock 0 помещается в одном шкафу высотой 42U и рассчитана для поддержки до 800 виртуальных машин. Решение среднего уровня Vblock 1, размещаемое в двух стандартных шкафах, поддерживает до 3 тыс. виртуальных машин и, в отличие от серии «0», может использовать еще и коммутаторы для сетей хранения данных Cisco MDS и СХД EMC CLARiiON. Наиболее развитой системой серии является Vblock 2, предназначенный для работы с 6 тыс. виртуальных машин. Если даже этой системы будет недостаточно, мощность комплекса можно нарастить путем добавления необходимого количества дополнительных модулей Vblock. Для централизованного

управления системами серии Vblock используется специальное решение компании EMC.

В конце 2015 года Cisco уже совместно с компанией VCE представили очередную версию Vblock System с ориентированной на приложения инфраструктурой Cisco Application Centric Infrastructure (ACI). С ее помощью упрощается создание гибких и безопасных ЦОД, способных быстро адаптироваться к изменению требований приложений и бизнеса. Сочетание конвергентной инфраструктуры VCE Vblock Systems и Cisco ACI обеспечивает операционную простоту в области программного конфигурирования, необходимого в эпоху облачных технологий.

Сочетание ACI и Vblock System позволяет реализовать высокие требования, предъявляемые к информационной безопасности и управлению данными. Благодаря широкому спектру сервисов для обеспечения информационной безопасности и работы с сетью комбинация Cisco ACI и Vblock Systems упрощает управление приложениями на ведущих платформах облачного управления и обеспечивает единообразный контроль виртуальных и физических задач, а также наглядное представление состояния приложений и сегментов с использованием комплексной, продвинутой телеметрии.

Cisco ACI предоставляет модель политик, позволяющую заказчикам определять свои сети, отталкиваясь от требований приложений, в то время как архитектура Vscale позволяет множеству систем VCE функционировать как единый автоматизированный на базе политик пул системных ресурсов.

7.4. Решение корпорации Oracle

Неожиданным игроком на рынке «коробочных» ЦОД стала компания Oracle, известная разработкой операционных систем. Это явилось результатом приобретения ею Sun Microsystems, вследствие чего в распоряжении компании оказался большой арсенал аппаратных решений, огромный опыт разработчиков и множество передовых технологий в сфере серверов и СХД.

Результатом симбиоза программных разработок Oracle и аппаратно-программных решений Sun стало появление в сентябре 2010 года комплексной системы Oracle Exalogic Elastic Cloud (OEEC). Решение включает в себя x86-серверы, сетевое оборудование, подсистему хранения данных, операционную систему, ПО виртуализации и связующее программное обеспечение.

В декабре 2013 года корпорация Oracle анонсировала поступление в продажу оптимизированного программно-аппаратного комплекса Oracle Exalogic Elastic Cloud X4-2 – четвертой модернизации модели 2010 года (см. рисунок 44). Oracle Exalogic X4-2 обладает более высокой пропускной способностью по сравнению с предыдущей версией и, по мнению разработчиков, в сочетании с технологией Oracle Exabus, обеспечивает почти неизменное время отклика для виртуализованных приложений, повышая преимущества консолидации. Аппаратные средства Oracle Exalogic Elastic Cloud X4-2 предлагают увеличенный объем оперативной памяти, а также повышенную емкость дисковой и флэш-памяти.

Рисунок 44 - Система Oracle Exalogic Elastic Cloud X4-2 разработки компании Oracle

В новой версии ПО Exalogic Elastic Cloud Software реализована возможность объединения различных архитектур развертывания приложений в одной аппаратной стойке, возможность использования шаблонов и пакетов виртуализации с помощью Oracle VM Templates и Oracle Virtual Assembly Builder.

По информации Oracle, из-за повышенной вычислительной плотности и расширенного спектра вариантов развертывания, затраты на развертывание и консолидацию корпоративных приложений Exalogic Elastic Cloud X4-2 ниже по сравнению с предыдущей версией.

По данным разработчика, Exalogic Elastic Cloud X4-2 предоставляет:

— на 50% больше вычислительной мощности в расчете на серверный узел при использовании серверов Oracle Sun Server X4 с 12-ядерными процессорами Xeon Processor E5-2697 v2;

— развертывание 720 процессорных ядер, 7,7 ТБ оперативной памяти и 24 ТБ флэш-памяти хранения в одной аппаратной стойке для высокой вычислительной плотности;

— на 33% больше емкости ресурсов хранения благодаря использованию СХД Oracle ZS3 Series Storage, спроектированной совместно с оптимизированными программно-аппаратными

комплексами Oracle для достижения высокой пропускной способности ввода-вывода.

Согласно заявлению корпорации, заказчики могут развернуть виртуализованные критически важные бизнес-приложения и выполнять их без потери производительности на комплексах Oracle Exalogic с Oracle VM Server и Oracle Virtual Assembly Builder.

Оптимизированный программно-аппаратный комплекс Oracle Exalogic X4-2 поставляется с возможностью выбора операционной системы — Oracle Linux или Oracle Solaris.

7.5. Решение корпорации Fujitsu

Комбинированный подход к вопросу построения вычислительной инфраструктуры ЦОД предлагает компания Fujitsu, представляя на рынке два основных решения в этом направлении — комплексную систему для облачных вычислений PRIMERGY CX1000 (рисунок 45) и программный набор ServerView Resource Orchestrator (ROR).

Комплекс представляет собой стандартный серверный шкаф высотой 42U, в котором может быть установлено до 38 однотипных двухпроцессорных серверов. Благодаря специальному ПО сервисы, работающие на PRIMERGY CX1000, не привязываются к аппаратной платформе, что позволяет безболезненно для системы в целом удалить или установить любой из ее серверов (например, в случае выхода из строя или для модернизации). Переконфигурирование происходит автоматически без остановки в работе.

Рисунок 45 - Комплекс PRIMERGY CX1000 фирмы Fujitsu

Сервер превращается в подобие легко заменимого «кирпичика». PRIMERGY CX1000 в полной конфигурации представляет собой один шкаф, который занимает в ЦОД чуть более 2 кв. м (с учетом технологического пространства), вычислительную систему, содержащую 456 вычислительных ядер, почти 2,5 ТБ оперативной памяти, СХД общей емкостью 38 ТБ, коммутаторы и комплексную систему охлаждения. Причем, благодаря специальной архитектуре охлаждения нагретый воздух забирается сверху, и, следовательно, система не требует формирования «горячих» коридоров. Шкаф можно поставить тыльной стороной к другому шкафу или к стене, что существенно экономит место в ЦОД.

7.6. Решение компании Hewlett-Packard

В разработке «коробочных» ЦОД не могла не принять участия компания Hewlett-Packard, самостоятельно производящая практически все компоненты системы. В комплексной системе BladeSystem Matrix, разработанной этой фирмой (рисунок 46), используются блейд-серверы ProLiant DL360 CMS, СХД 3PAR StoreServ моделей 7200, 7400 и 10800, фирменные коммутаторы, специализированное ПО и набор сервисных услуг.

Рисунок 46 - Система BladeSystem Matrix фирмы Hewlett-Packard

HP CloudSystem Matrix создавалось с применением таких технологий как, Matrix Operating Environment и HP BladeSystem, которые оптимизированы для использования на моделях серверов HP ProLiant и HP Integrity. Кроме этого, предлагаемое решение от HP можно использовать в системах сетевых коммуникаций хранения данных от HP, а также адаптировать для работы с серверными решениями x86. Положительным фактом является и возможность использования с сетевыми решениями, предлагаемыми сторонними производителями серверной и сетевой продукции.

Решения HP работают с операционными системами Linux, HP-UX и Windows, поддерживают совместимость с такими гипервизорами, как Microsoft Hyper-V, Integrity VM и VMware, Red Hat KVM.

CloudSystem Matrix предоставляется пользователям в трех конфигурациях – малая, средняя, широкая. Более низкая конфигурация может усовершенствоваться благодаря применению дополнительных плагинов, программ и аппаратной части как от HP, так и от сторонних производителей.

HP CloudSystem Matrix – это «инфраструктура как услуга» (IaaS, см. раздел 9.3) для частных и гибридных облачных сред, которая предоставляет физическую и виртуальную инфраструктуру за считанные минуты.

Это решение включает в себя самообслуживающийся портал инфраструктуры для осуществления ее быстрой автоматической инициализации, а также встроенную возможность обслуживания в течение срока эксплуатации, которая позволяет оптимизировать эту инфраструктуру, управлять пулами ресурсов и обеспечить безотказную работу.

Благодаря включенным в комплект облачным интерфейсам прикладного программирования, можно настроить рабочую среду под конкретные потребности. По своей конструкции CloudSystem Matrix – интегрированное решение, которое поддерживает широкий ряд разнородных сред и позволяет осуществлять распределение облаков для различных провайдеров публичных облачных сред, включая облачные сервисы HP.

В одном шкафу может быть установлено до четырех блейд-шасси, что в общей сложности дает почти 1,5 тыс. вычислительных ядер и до 16 ТБ оперативной памяти, а суммарная емкость внутренней системы хранения данных потенциально может достигать сотен ТБ. Правда, одновременно столько серверов и дисков в один шкаф не поместятся — надо выбирать оптимальную конфигурацию, либо увеличивать количество шкафов. Система позволяет управлять в рамках единого адресного поля виртуализированных ресурсов тысячей физических серверов. Программный комплекс собственной разработки предназначен для планирования, построения и оптимизации информационной системы предприятия на основе шаблонов приложений и сервисов.

Контрольные вопросы

1. Основные характеристики «коробочных» ЦОД.
2. Возможности системы «Dell vStart» для организации ЦОД.
3. Возможности мейнфреймов для организации ЦОД.
4. Возможности системы «Vblock» для организации ЦОД.
5. Возможности системы «Oracle Exalogic Elastic Cloud» для организации ЦОД.
6. Возможности комплекса PRIMERGY CX1000 для организации ЦОД.
7. Возможности системы «HP CloudSystem Matrix» для организации ЦОД.

8. Мобильные ЦОД

8.1. Достоинства и области применения

В настоящее время производством мобильных ЦОД занимается целый ряд мировых компаний. Пионерами в этой области, как и во многих других направлениях развития техники, были вооруженные силы, которые в США уже давно используют контейнеры с предустановленными и готовыми к работе серверами. Это быстрое и модульное решение более удобно для развертывания ЦОД, чем установка серверов и настройка систем при перемещении центра.

Перспективной областью применения мобильных центров обработки данных является их использование в чрезвычайных ситуациях. Очевидное преимущество состоит в скорости развертывания компьютерной и коммуникационной инфраструктуры для помощи местным властям и облегчения координации работы служб, занятых в мероприятиях по устранению катастрофы. Внешний вид типичного мобильного ЦОД представлен на Рисунке 47.

Рисунок 47 - Внешний вид мобильного ЦОД в одноконтейнерном исполнении

Во многих ситуациях мобильное решение является либо единственно возможным, либо более эффективным по сравнению со стационарным ЦОД. Во-первых, мобильный, или контейнерный ЦОД эффективен в тех случаях, когда инфраструктуру ИТ требуется развернуть на удаленной площадке. С такими задачами обычно сталкиваются нефтяные, газодобывающие и телекоммуникационные компании. Во-вторых, мобильный ЦОД может быть основным для офисов, местоположение которых часто меняется. Здесь потенциальные области применения весьма разнообразны, начиная от упомянутых выше задач министерства обороны и служб МЧС и заканчивая строительными площадками, где создается временная инфраструктура. В-третьих, мобильный ЦОД — эффективное решение для резервирования основного центра обработки данных.

В принципе, и основной, и резервный ЦОД могут быть контейнерными. Если, например, компании предстоит масштабный переезд в новый офис, то на время переезда резервному мобильному ЦОД передаются функции основного. Кроме уже упомянутых задач, мобильный ЦОД может применяться для расширения инфраструктуры ИТ. При активной экспансии в регионы или поглощении других компаний он дает существенный выигрыш: новые торговые площадки и филиалы открываются без задержек, а приобретенные активы оперативно интегрируются в единую информационную инфраструктуру.

Преимущества эксплуатации мобильного ЦОД тоже весомы. Мобильность подразумевает не только перемещение с места на место, но дает возможность выбора места размещения и, в случае необходимости, быстрой миграции на другую площадку. Его развертывание занимает в

7-10 раз меньше времени, чем ввод в эксплуатацию стационарного ЦОД, поскольку все системы заранее установлены, налажены и протестированы. Экономические плюсы состоят в возможности размещения поблизости от дешевых источников энергии, в отсутствии арендной платы за помещение и сохранении инвестиций при переезде или перемещении офиса. Мобильный ЦОД отличают гибкость конфигурирования, практически неограниченные возможности масштабирования, а также настройка решения в соответствии с индивидуальными требованиями заказчика. Вот далеко не полный, но весьма внушительный список преимуществ контейнерных ЦОД, на которые стоит обратить внимание при принятии решения о создании центра обработки данных.

8.2. Инженерная инфраструктура

Минимальный комплект инженерных систем мобильного ЦОД включает:

— гарантированное энергоснабжение (ИБП и дизель-генераторные установки);

— прецизионное кондиционирование с необходимым уровнем резервирования системы;

— комплексную систему безопасности (газовое пожаротушение, охранно-пожарную сигнализацию, контроль доступа и видеонаблюдение);

— автоматизированную систему диспетчерского управления;

— кабельное и сетевое оборудование.

Прецизионная система кондиционирования может быть организована при помощи воздушного и водяного охлаждения. Она призвана обеспечить требуемые климатические условия для оборудования ИТ при установке контейнера в жестких климатических условиях, например, при повышенной влажности, резких перепадах температур, нестандартном составе атмосферы.

Контроль за работой систем и оборудования осуществляется в удаленном режиме посредством автоматизированной системы диспетчерского управления (АСДУ). Минимальный функционал АСДУ предполагает контроль:

— состояния инженерного оборудования;

— температуры и влажности;

— системы энергоснабжения;

— аварийных ситуаций всех систем обеспечения;

— противопожарной ситуации в ЦОД;

— систем безопасности.

Сообщения от АСДУ могут передаваться как по локальной сети, так и через Интернет на удаленное рабочее место оператора и различные информационные устройства других ответственных лиц.

Контейнер, в котором находится оборудование, должен быть соответствующим образом подготовлен. Стены и пол мобильного ЦОД утепляют специальными материалами, а все пространство контейнера (при размещении оборудования в одном контейнере) делится на две зоны посредством тамбур-шлюза. Первая из зон отделяется тамбур-шлюзом и от входа, чтобы изолировать оборудование от резких перепадов температур и влажности. Здесь устанавливается вычислительная техника и резервный ИБП. Во втором отсеке размещаются все остальные технологические системы.

При размещении мобильного ЦОД в двух контейнерах выделяются:

— энергетический модуль (ЭМ),

— модуль функционального оборудования (МФО).

Двухконтейнерное размещение позволяет исключить влияние энергетического оборудования модуля ЭМ на ИТ оборудование МФО. При этом также учитываются принципиально различные требования к микроклимату внутри модулей.

Контейнеры ЭМ и МФО связываются электросиловыми цепями, коммуникациями мониторинга, видеонаблюдения, пожарной сигнализации и контроля доступа. Внешние ИТ сети и сети АСДУ подключаются к МФО, внешняя электросиловая сеть - к вводному устройству ЭМ.

ЭМ содержит:

— АВР;

— дополнительную электрическую генераторную установку с запасом топлива не менее, чем на 24 часа автономной работы;

— систему видеонаблюдения;

— систему мониторинга с передачей информации через МФО.

Вводное устройство ЭМ может предусматривать узел коммерческого учета электроэнергии.

В контейнере МФО (Рисунок 48) предусмотрены три отсека:

— тамбур;

— отсек ИТ-оборудования;

— отсек внешних блоков системы кондиционирования.

Тамбур предназначен для обеспечения необходимого температурно-влажностного режима в отсеке ИТ оборудования и размещения:

Рисунок 48 - Размещение оборудования в МФО

— шкафа аккумуляторов ИБП и аварийного освещения МФО;

— внутренних блоков системы кондиционирования и вентиляции тамбура;

— распределительного устройства МФО с байпасом ИБП;

— баллонов системы газового пожаротушения МФО;

— вводного щита электропитания (от ЭМ) и коммуникационных устройств системы мониторинга и видеонаблюдения с внешними устройствами;

— внутренних коммуникаций;

— системы основного и аварийного освещения.

Отсек ИТ-оборудования предназначен для размещения:

— серверного оборудования;

— СХД;

— систем кондиционирования и вентиляции;

— систем газового пожаротушения;

— основного и аварийного освещения;

— систем видеонаблюдения и мониторинга (в том числе и ЭМ).

Компоновка оборудования в ИТ-отсеке обеспечивает удобный эксплуатационный доступ к стойкам, предусматривающий поочередное выдвижение стоек в холодный коридор без отключения от сетей для обслуживания и замены блоков.

Система кондиционирования ИТ-отсека организована с помощью воздушных кондиционеров. Внешние блоки системы кондиционирования размещены в «холодном» отсеке.

8.3. Особенности информационной инфраструктуры мобильного ЦОД

Особенность информационной инфраструктуры мобильного ЦОД определяется необходимостью учета ряда следующих его особенностей:

— небольшой площадью;

— высоким тепловыделением;

— пригодностью для эксплуатации в удаленных точках и, возможно, в суровых климатических условиях;

— минимумом обслуживающего персонала.

В контейнерном ЦОД обычно используются самые передовые технологические решения, предлагаемые производителями ИТ-оборудования. Среди таких технологий выделим широкое применение блейд-серверов, преимущества которых при их использовании именно в мобильных ЦОД заключаются в:

— высокой плотности размещения серверов, сетевой инфраструктуры, дисковых модулей, ленточных накопителей;

— отсутствии кабелей для подключения серверов к коммутаторам;

— возможности резервирования модулей охлаждения и энергопитания по схеме 2N;

— экономии электроэнергии (до 30%);

— сокращении времени подготовки сервера к работе (до 6 раз);

— экономии пространства для размещения (до 4 раз).

Повышение эффективности использования оборудования достигается также использованием предустановленного ПО виртуализации ИТ-инфраструктуры. За счет виртуализации улучшается управляемость мобильным ЦОД, снижается количество аппаратных сбоев, уменьшается общее время простоев, повышается доступность приложений.

В целях повышения надежности всей системы в мобильных ЦОД часто используется серверное и коммуникационное оборудование, сертифицированное в соответствии с международными стандартами для телекоммуникационных мобильных контейнеров, эксплуатация которых осуществляется при похожих условиях (хотя и при существенно меньшем потреблении энергии).

8.4. Подготовка и ввод в эксплуатацию

Как уже упоминалось, одно из ключевых преимуществ мобильного решения состоит в быстроте его развертывания. Процесс подготовки мобильного ЦОД к вводу в эксплуатацию состоит из нескольких этапов (работа по некоторым из них ведется параллельно). Первый — это подготовка ровной площадки, подведение к ней энергоснабжения и кабельных коммуникаций (или организации беспроводной связи, например, спутниковой или по радиоканалу), возведение солнцезащитного шатра, обеспечение заземления и молниезащиты, выполнение других необходимых мероприятий.

Контейнер может быть установлен как «в чистом поле», так и в любом другом подходящем месте: в ангаре, на складе, на территории завода и т.д. В случае использования воздушного охлаждения специальный подвод воды и/или установка чиллера не требуются.

Зачастую одновременно выполняется второй этап — сборка самого контейнера, заказ оборудования, установка и наладка всех необходимых систем. Третий этап — монтаж и тестирование работы контейнера на площадке заказчика. Во многих подобных решениях используются стандартные 20-футовые транспортные контейнеры. Соответственно, и транспортировка осуществляется любыми стандартными способами: на трейлере, по железной дороге, морским путем и т.д.

Контрольные вопросы

1. Области применения мобильных ЦОД.
2. Достоинства мобильных ЦОД.
3. Инженерная инфраструктура мобильных ЦОД.
4. Особенности информационной инфраструктуры мобильного ЦОД.
5. Подготовка и ввод в эксплуатацию мобильных ЦОД.

9. Облачные вычисления и ЦОД

9.1. Определение и общее описание

Последнее десятилетие ознаменовалось резким возрастанием интереса к так называемым, облачным вычислениям (cloud computing), развитие которых оказалось связанным с появлением и распространением крупных коммерческих ЦОД. Термин «cloud computing» был впервые использован еще в 1993 году Эриком Шмидтом, членом правления компании Sun Microsystems, для обозначения сервисов, дистанционно поддерживающих различные данные и приложения, размещенные на удаленных серверах. Своим названием технология обязана обозначениям на схемах сети Интернет в виде облака. Организация облачного сервиса осуществляется, как правило, на базе крупных ЦОД.

В 2002 году Национальный Институт Стандартов и Технологи США (The National Institute of Standards and Technology - NIST) разработал неформальный документ, в котором дал определение понятия облачных вычислений. В документе, кроме определения, приведены характеристики облачных вычислений, сервисные модели и модели развертывания. Неформальный характер определения означает, что оно

носит рекомендательный характер и вводится лишь в целях информирования заинтересованных лиц, а также для расширения публичных обсуждений тематики облачных вычислений. При этом в преамбуле документа отмечалось, что облачные вычисления являются эволюционирующей концепцией. Поэтому данное определение, его атрибуты, характеристики, применяемые технологии, проблемы и преимущества будут со временем уточняться и конкретизироваться.

В соответствии с определением NIST облачные вычисления - это модель предоставления повсеместного и удобного сетевого доступа «по мере необходимости» к общему пулу конфигурируемых вычислительных ресурсов (сетей, серверов, систем хранения, приложений и сервисов), которые могут быть быстро предоставлены и освобождены с минимальными усилиями по управлению и необходимостью взаимодействия с провайдером услуг.

Облачная модель поддерживает высокую доступность сервисов и описывается пятью основными характеристиками, тремя сервисными моделями (моделями предоставления услуг) и четырьмя моделями развертывания, которые буду рассмотрены ниже.

Принципиальная разница между обычным и облачным сервисами состоит в следующем. При традиционном (обычном) подходе провайдер на месячной основе получает фиксированное вознаграждение за использование его вычислительных ресурсов (серверов, СХД, коммуникационного оборудования и пр.). При этом не имеет значения, использовал ли клиент выделенные ему ресурсы в полном объеме на протяжении всего месяца или только несколько дней, а остальное время вычислительные ресурсы простаивали.

При предоставлении облачного сервиса используется тип оплаты "плата за использование". Обычно за единицу измерения времени работы принимается минута или час пользования ресурсами. При оценке объемов данных за единицу измерения принимается мегабайт хранимой информации. В этом случае пользователь оплачивает ровно тот объем ресурсов, который им в реальности использовался в течение определенного времени. Кроме того, облачная инфраструктура предоставляет пользователю возможность при необходимости "поднимать" или "опускать" максимальные лимиты выделяемых ресурсов, пользуясь тем самым эластичностью предоставляемого сервиса. Пользователю облачных сервисов нет необходимости заботиться об инфраструктуре, которая обеспечивает работоспособность предоставляемых ему сервисов. Все задачи по настройке, устранению

неисправностей, расширению инфраструктуры и пр. берет на себя сервис-провайдер.

Популярность облачных вычислений неизбежно привела к определенным спекуляциям на этом понятии и использовании его в маркетинговых целях. Последнее даже не особенно скрывается. Так, Ларри Эллисон, глава корпорации Oracle, прямо заявил: «Мы переопределяем вычислительные облака для того, чтобы включить в это понятие все, что мы создаем». Тем не менее представляется, что переход к облачным вычислениям стал закономерной стадией развития предоставления коммунальных услуг, таких, как водо-, тепло-, электро-, газоснабжение или мобильная связь. Сходство с коммунальными услугами определяется тем, что при использовании технологии облачных вычислений:

— потребители платят только за реально потребленные услуги;

— для потребления ресурсов нет необходимости обращаться непосредственно к их производителю, в данном случае владельцу ЦОД (подобно тому, как при потреблении воды или электричества нет необходимости обращаться в насосную или электрогенерирующую станции);

— поставщики сервисов (сервис-провайдеры) обеспечивают их доступность в виде арендуемых «ресурсов» на основе заключенного договора, оставляя за собой вопросы создания и поддержания инфраструктуры доставки.

Важным стимулом развития ИТ-сервисов, предоставляемых по запросу, стали мобильные устройства подключения к сети Интернет (ноутбуки, нетбуки, планшетники, смартфоны, iPad, iPod). Уменьшение их веса во многом связано с уменьшением вычислительных возможностей и емкостей хранения. Поэтому насущным и закономерным этапом развития таких устройств стала возможность перенесения части функций в «облако» (фактически – в удаленный ЦОД) при обеспечении надежной и устойчивой с ним связи, обеспечиваемой провайдером.

9.2. Характеристики облачных вычислений

NIST определяет пять следующих характеристик облачных вычислений.

1. Самообслуживание по мере возникновения необходимости (On-demand self-service). Потребитель самостоятельно обеспечивает себя вычислительными возможностями, средствами или ресурсами, такими как серверное время или емкость сетевого хранилища, по мере

необходимости запрашивая их у сервис-провайдера в одностороннем автоматическом режиме, без необходимости взаимодействия с персоналом сервис-провайдера.

2. Свободный сетевой доступ (Broad network access). Запрашиваемые сервисы доступны по сети через стандартные механизмы, поддерживающие использование гетерогенных платформ тонких и толстых клиентов (например, мобильных телефонов, ноутбуков, планшетников и т.д.).

3. Пул ресурсов (Resource pooling). Вычислительные ресурсы провайдера организованы в виде пула для обслуживания различных потребителей с возможностью динамического назначения и переназначения различных физических и виртуальных ресурсов в соответствии с потребностями потребителей. Особое значение имеет независимость размещения ресурсов, при котором заказчик, в общем случае, не знает и не контролирует точное физическое местоположение предоставляемых ресурсов, но может специфицировать их расположение на более высоком уровне абстракции (например, страна, штат или ЦОД). Примерами таких ресурсов являются системы хранения, вычислительные возможности, память, пропускная способность сети, виртуальные машины.

4. Быстрое изменение объема (эластичность) услуг. Вычислительные возможности могут быть предоставлены быстро и с изменяемым объемом, в ряде случаев - автоматически, для оперативного повышения или быстрого уменьшения масштабов потребления. Для потребителя эти ресурсы часто выглядят, как доступные в неограниченном объеме, и могут быть приобретены в любой момент времени в любом количестве.

5. Измеримый сервис. Облачные системы автоматически контролируют и оптимизируют использование ресурса, измеряя по факту его потребления на определенном уровне абстракции, соответствующем типу сервиса (например, объема хранения, вычислительной мощности, полосы пропускания) и активных учетных записей пользователей. Использование ресурсов может подвергаться мониторингу, быть контролируемым и сопровождаться отчетностью, обеспечивая прозрачность потребления и для провайдера, и для потребителя использованного сервиса.

9.3. Основные сервисные модели (модели предоставления услуг)

1. Инфраструктура как услуга - Infrastructure as a Service (IaaS). Потребителю предоставляются средства обработки данных, хранения, сетей и других базовых (фундаментальных) вычислительных ресурсов с уникальным IP-адресом, на которых потребитель может развертывать и выполнять произвольное программное обеспечение, включая ОС и приложения. Потребитель не управляет облачной инфраструктурой и не контролирует ее, но может контролировать операционные системы, средства хранения, развертываемые приложения и, возможно, обладать ограниченным контролем над выбранными сетевыми компонентными (например, межсетевой экран, управляемый потребителем).

Основные потребители данной услуги – владельцы приложений и ИТ-специалисты, подготавливающие образы ОС для их запуска в сервисной инфраструктуре. IaaS предоставляет сервисы для запуска виртуальных машин и сервисы хранения данных. Соглашение об уровне предоставляемых сервисов (SLA – Service Level Agreement) обычно определяет доступность виртуального сервера и время развертывания образа ОС.

IaaS характеризуется различным уровнем предоставления услуг провайдерами, платформами гипервизора, возможностями управления и т.д. При этом следует обращать внимание не только на стоимость услуг, но и на:

— способ виртуализации (тип гипервизора),

— способ управления виртуальной услугой,

— типы СХД, способы их организации,

— доступ к вышедшим из строя системам;

— способ измерения уровня обслуживания;

— возможность доступа к приложениям при прекращении обслуживания;

— последствия для конфиденциальных данных при их шифровании, случайной утрате, судебных действиях.

2. Платформа как услуга - Platform as a Service (PaaS). Потребителю предоставляется возможность аренды платформы, которая включает ОС и прикладные сервисы.

Сервис PaaS включает в себя IaaS и облегчает разработку, тестирование, развертывание и сопровождение приложений без необходимости инвестиций в инфраструктуру и программную среду. Основные потребители сервиса - компании, разрабатывающие

приложения. Платформа обеспечивает среду для выполнения приложений, сервисы по хранению данных и ряд дополнительных сервисов, например интеграционные или коммуникационные сервисы.

SLA обычно определяет:

— доступность среды выполнения приложений;

— ее производительность.

Возможности настройки приложений под нужды потребителей практически не ограничены. Оплата облачной платформы рассчитывается исходя из объема использованных вычислительных ресурсов, таких как:

— время работы приложения;

— объем данных и количество операций с данными (транзакций);

— сетевой трафик.

3. Программное обеспечение как услуга - Software as a Service (SaaS). Потребителю предоставляются программные средства - приложения провайдера, выполняемые на облачной инфраструктуре. Приложения доступны с различных клиентских устройств через интерфейс тонкого клиента (например, электронная почта с web-интерфейсом). Потребитель не управляет и не контролирует саму облачную инфраструктуру, на которой выполняется приложение, будь то сети, серверы, операционные системы, системы хранения или даже некоторые специфичные для приложений возможности. В ряде случаев потребителю может быть предоставлена возможность доступа к некоторым пользовательским конфигурационным настройкам.

Услуга SaaS предоставляет возможность аренды приложений и включает в себя IaaS и PaaS. Доступ к приложениям осуществляется через Интернет с оплатой по факту их использования. Эта модель наиболее распространена среди облачных сервисов. Она может быть реализована на основе частных облаков с использованием внутренних сетевых каналов, дополнительно защищенных и не связанных с Интернетом.

Потребители - конечные пользователи, работающие с приложениями, предоставляемыми в «облаках».

SLA определяет:

— доступность сервисов;

— их производительность.

Возможности настройки приложений под нужды потребителей минимальны или вообще отсутствуют. Их уровень определяется требованиями рынка или возможностями поставщиков приложений.

Оплата сервиса производится ежемесячно и рассчитывается на основе количества пользователей приложения.

Услуга SaaS особенно привлекательна для среднего и малого бизнеса (СМБ) вследствие:

— низких финансовых рисков, поскольку отсутствуют предварительные и скрытые (при обновлении ПО) затраты, а текущие расходы предсказуемы;

— простоты развертывания, поскольку приложения развертываются и конфигурируются практически мгновенно;

— обеспечения технической поддержки требуемого уровня, поскольку цена услуги обычно устанавливается в зависимости от уровня поддержки и качества обслуживания; нет необходимости переплачивать за избыточную функциональность;

— снижения нагрузки на ИТ-персонал, поскольку при увеличении объема ИТ-ресурсов численность специалистов, нагрузка на них и их квалификация не растет;

— высокой защищенности бизнеса, поскольку провайдеры SaaS используют ЦОД с уровнем надежности энергоснабжения, кондиционирования и систем безопасности, который предприятия СМБ не могут обеспечить;

— доступности для пользователей, поскольку сервис предоставляет возможность работы всюду, где есть Интернет; мобильные и дистанционные пользователи могут использовать приложения совместно с коллегами в офисе.

9.4. Дополнительные сервисные модели

В литературе иногда выделяют еще ряд сервисных моделей облачных технологий, которые не рассматриваются в неформальном документе NIST.

1. Унифицированные коммуникации как услуга – Unified Communication as a Service (UCaaS). Потребителю предоставляются средства коммуникации (IP-телефония, почта, обмен сообщениями) на облачной инфраструктуре, техническую поддержку которой осуществляет провайдер.

2. Видеоконференцсвязь как услуга – Videoconferece as a service (VaaS). Потребителю предоставляются услуги видеоконференцсвязи (ВКС) на оборудовании провайдера – частный случай UCaaS. У потребителя находятся только терминалы ВКС.

3. Сетевая инфраструктура как услуга – Network infrastructure as a service (NIaaS). Потребителю предоставляются средства реализации среды, позволяющей несколькими щелчками мыши организовать прямые каналы связи с необходимой пропускной способностью и другими параметрами, оговоренными соглашением о предоставлении услуг (SLA - Service Level Agreement).

4. Безопасность как услуга - Security as a service (SECaas). Потребителю предоставляются услуги по очистке Интернет-трафика пользователя вблизи его местонахождения от вредоносного, нежелательного и избыточного контента. Заказчик определяет корпоративную политику использования Интернета и организует переадресацию Интернет-трафика сотрудников облачному провайдеру, который обеспечивает пропуск полезного контента и блокировку остального.

5. Рабочее место как услуга – Desktop as a Service (DaaS). Потребителю предоставляется полностью готовое к работе виртуальное рабочее место, которое может быть настроено под его задачи; пользователь получает доступ не к отдельной программе, а к необходимому для полноценной работы программному комплексу. Устройство доступа используется в качестве тонкого клиента с минимальными требованиями.

9.5. Модели развертывания

1. Частное облако (Private cloud). Облачная инфраструктура функционирует целиком в целях обслуживания одной организации. Инфраструктура может управляться самой организацией или третьей стороной и может существовать как на стороне потребителя, так и у внешнего провайдера (off premise).

2. Облако сообщества или общее облако (Community cloud). Облачная инфраструктура используется совместно несколькими организациями и поддерживает ограниченное сообщество, разделяющее общие принципы (например, политику безопасности, соответствие регламентам и руководящим документам). Такая облачная инфраструктура может управляться самими организациями или третьей стороной и может существовать как на стороне потребителя, так и у внешнего провайдера.

3. Публичное облако (Public cloud). Облачная инфраструктура создана в качестве общедоступной или доступной для большой группы потребителей, не связанных общими интересами, но, например,

принадлежащих к одной области деятельности. Такая инфраструктура находится во владении организации, продающей соответствующие облачные услуги, предоставляющей облачные сервисы.

4. Гибридное облако (Hybrid cloud). Облачная инфраструктура является сочетанием двух и более облаков (частных, общих или публичных), остающихся уникальными сущностями, но объединенными вместе стандартизированными или частными технологиями, обеспечивающими перенос данных и приложений между такими облаками (например, такими технологиями, как пакетная передача данных для баланса загрузки между облаками).

Иногда также пользуются понятием "виртуального частного облака", когда провайдер использует публичную облачную инфраструктуру для организации частного облака. При такой организационной структуре часть данных клиента хранится и обрабатывается за счет ресурсов собственной инфраструктуры, а часть - за счет ресурсов внешнего провайдера. В качестве примера виртуального частного облака можно привести сервис компании Amazon под названием Amazon Virtual Private Cloud (Amazon VPC).

9.6. Безопасность облачных технологий

Безопасность (как физическая, так и информационная) - главное препятствие для широкого распространения облачных вычислений. И опасения по поводу безопасности имеют основания. Одна из самых масштабных катастроф, получивших широкую огласку – это сбой в системе аутентификации пользователей облачных сервисов Microsoft, в результате чего полмиллиарда пользователей могли заходить в чужие учетные записи. В 2011 году была взломана сеть Sony Playstation Network, в результате чего была осуществлена кража персональных данных и финансовой информации пользователей. Результаты взлома затронули интересы более 77 миллионов человек. В нашей стране одним из самых известных взломов, непосредственно, правда, не имеющего отношения к облачным сервисам, стал взлом сервиса приема онлайн-платежей «Ассист» компании «Аэрофлот». В результате компания целые сутки не могла продавать свои билеты через Интернет, потерпев убытки почти в 100 миллионов рублей.

Существующие стандарты информационной безопасности, такие как SAS 70 и ISO 27001 и 27002, недостаточны для облачных вычислений, а специфические для облачных вычислений стандарты отсутствуют. Технических решений по надежному обеспечению

информационной безопасности в виртуальных и облачных средах тоже нет. Есть лишь отдельные "заплатки", которые решают конкретные задачи в конкретных ситуациях.

Особенности обеспечения безопасности в облачных технологиях во многом сходны с проблемами ЦОД, предоставляющими облачные услуги. Они определяются:

— отсутствием четкого периметра безопасности;

— смещением фокуса с обеспечения безопасности на обеспечение доверия (субъективной субстанции);

— совместным использованием одних и тех же ресурсов различными организациями или компаниями;

— зависимостью пользователя от поставщика услуг.

Потребность в разработке хоть каких-то нормативов побудила к созданию общественной организации Союз облачной безопасности - Cloud Security Alliance (CSA), которая разделила проблему на два направления:

— управление (управление ресурсами предприятия, соответствие законодательным требованиям, управление жизненным циклом информации, совместимость),

— реализация (традиционная безопасность, обеспечение непрерывной работы бизнеса и восстановление после сбоев, ЦОД, реагирование на инциденты, предупреждение и восстановление, безопасность приложений, шифрование).

В результате в 2004 году появился Application Packaging Standard (APS) и предложены спецификации, при использовании которых на разработчиков облачного ПО не налагалось бы никаких ограничений, кроме ряда несложных операций при упаковке приложений для их последующего распространения через облака и телеком-провайдеров, у которых программное обеспечение поддерживает APS.

CSA также определила, что хотя требования к безопасности в трех сервисных моделях облачных вычислений одинаков, уровень контроля над безопасностью сильно различается:

— **SaaS** - основная обязанность по обеспечению безопасности ложится на поставщиков, поскольку клиент не управляет сетью, серверами, операционными системами, хранением данных и даже некоторыми возможностями приложений;

— **PaaS** - часть обязанностей ложится на пользователей, которые отвечают за безопасность приложений, управление API (Application Programming Interface – интерфейс программирования приложений -

набор готовых процедур, функций, структур, предоставляемых приложением, для использования во внешних программных продуктах), подтверждение прав доступа и авторизацию, поскольку именно они контролируют развертывание приложений;

— **IaaS** - пользователи должны управлять и обеспечивать безопасность операционных систем, приложений и контента, как правило, через API, поскольку они имеют контроль над операционными системами, хранением данных и развертыванием приложений и, возможно, ограниченный контроль над выбором сетевых компонентов.

Следует отметить, что строго регламентированной ответственности за безопасность облачных вычислений не существует. Можно лишь условно обозначить следующие ответственности провайдера:

— строгая аутентификация и авторизация пользователей (в том числе администраторов);

— защита информации, передаваемой по каналам связи;

— безопасность виртуальной среды.

и следующие ответственности клиента:

— межсетевой экран (аппаратный или программный);

— обнаружение и предотвращение вторжений;

— контроль целостности;

— анализ журналов;

— защита от вредоносного кода.

Можно, однако, рекомендовать следующие практические меры, способствующие обеспечению информационной безопасности облачных технологий:

— ранжирование корпоративных данных и переноса в облако (по крайней мере, публичное) только наименее критичных; тестирование обновлений, например, можно переносить в облако уже сейчас;

— использование технологий дедупликации, что затруднит доступ к передаваемым и хранимым данным и одновременно радикально снизит затраты на услуги облачных сервисов;

— хранение имен клиентов на одном сервисе, а фамилий - на другом, что сделает их кражу по отдельности бессмысленной; одновременно устраняются проблемы, связанные с соответствием закону о защите персональных данных;

— выполнение всех требований, относящихся к безопасности виртуальных сред, поскольку облачные вычисления базируются практически всегда на виртуальных средах;

— использование либо частных облаков, либо гибридных (с основными компонентами ИТ-инфраструктуры внутри закрытого периметра) при хранении данных, подпадающих под «Закон о персональных данных».

9.7. Облачные технологии и бизнес. Перспективы развития

Рынок услуг облачных сервисов постоянно растет. В роли провайдеров обычно выступают:

— сети, обслуживающие частных лиц (Google, Amazon), обладающие избыточными вычислительными мощностями и стремящиеся получить дополнительную прибыль;

— традиционные производители ИТ-продуктов (IBM, HP, Microsoft, AT&T);

— интеграторы, стремящиеся сформировать новую среду;

— нишевые игроки, работающие в отдельных сегментах ИТ-бизнеса и считающие, что для них или при их посредничестве открываются новые возможности в использовании сервисов.

Для бизнеса основное преимущество в использовании облачных технологий примерно то же, что и в использовании обычного аутсорсинга – он отдает сторонним специалистам заботу о своей инфраструктуре, что позволяет в большей мере сосредоточиться на основных задачах. Применяя использованную выше аналогию с коммунальными услугами, бизнесу не надо колоть дрова и носить воду для обеспечения своей деятельности. Конкретно, факторы, способствующие развитию облачных технологий, можно условно разделить на глобальные и технологические. К глобальным факторам относятся:

— бурный рост объема цифровой информации (примерно на 52% в год);

— незначительный рост ресурсов, необходимых для обработки информации (в среднем рост ИТ-бюджетов составляет 2%, а рост числа ИТ-специалистов – на 1%);

— структура ИТ-бюджета (при традиционном использовании ИТ-ресурсов 77% расходов тратится на их поддержку и обслуживание и лишь 23% - на развитие);

— две важные характеристики уровня развития бизнеса - TCO (Total Coast Ownership) – полная стоимость владения и ROI (Return of Investment) - уровень доходности или убыточности бизнеса (отношение

дохода или убытка к сумме инвестиций) при использовании облаков значительно ниже.

К технологическим факторам, определяющим перспективы облачных вычислений, относятся:

— виртуализация серверов и СХД;

— рост пропускной способности телекоммуникационных каналов;

— дедубликация и сжатие трафика;

— развитие технологий информационной безопасности (шифрования, мониторинга виртуальной структуры, системы управления ею и т.д.).

Контрольные вопросы

1. Определения облачных вычислений.
2. Характеристики облачных вычислений.
3. Модели предоставления облачных услуг.
4. Дополнительные сервисные модели облачных услуг.
5. Модели развертывания облака.
6. Основные критерии безопасности облачных технологий.
7. Перспективы развития облачных технологий.

10. Грид-вычисления

10.1. Определение и концепция

Грид-вычисления (от английского grid — решётка, сеть; по аналогии с «power grid» - электрической сетью) — это форма распределённых вычислений, в которой «виртуальный суперкомпьютер» представлен в виде кластеров, соединённых с помощью сети, слабосвязанных, гетерогенных ЦОД, компьютеров, серверов, СХД, работающих вместе для выполнения большого объема вычислений (заданий, операций, работ). Грид является географически распределённой инфраструктурой, объединяющей множество ресурсов разных типов (процессоры, долговременная и оперативная память, хранилища и базы данных, сети), доступ к которым пользователь может получить из любой точки, независимо от места их расположения.

Идеи грид-системы были собраны и объединены Иэном Фостером, Карлом Кессельманом и Стивом Тики, которых часто называют отцами грид-технологии в начале 90-х годов. Их определение: «грид-компьютинг - это скоординированное разделение ресурсов и решение задач в динамически меняющихся виртуальных организациях со многими участниками». Эти же авторы положили начало созданию

набора инструментов для грид-компьютинга, который включает не только инструменты менеджмента вычислений, но и инструменты управления ресурсами хранения данных, обеспечения безопасности доступа к данным и к самому гриду, мониторинга использования и передвижения данных, а также инструментарий для разработки дополнительных грид-сервисов. В настоящее время этот набор инструментария является де факто стандартом для построения инфраструктуры на базе технологии грид, хотя на рынке существует множество других инструментариев для грид-систем как в масштабе предприятия, так и в глобальном.

Технологической основой грид-компьютинга стало распространение персональных компьютеров, развитие интернета и технологий пакетной передачи данных на основе оптического волокна, а также технологий локальных сетей (Gigabit Ethernet). Для объединения компьютеров в сеть полоса пропускания коммуникационных средств должна была стать достаточной, чтобы при необходимости привлечь ресурсы другого компьютера. Учитывая, что множество подключенных к глобальной сети компьютеров большую часть рабочего времени простаивает и располагает ресурсами, большими, чем необходимо для решения их повседневных задач, возникла возможность применить их неиспользуемые ресурсы в другом месте.

10.2. Области применения

Хотя грид-вычисления используются и в коммерческих инфраструктурах для решения таких трудоёмких задач, как экономическое прогнозирование, разработка и изучение свойств новых лекарств и др., основное ее применение – научные исследования, решение сложных математических задач, требующих огромных вычислительных ресурсов.

Типичный пример применения грид-технологий - моделирование и обработка данных в экспериментах на Большом андронном коллайдере CERN (от французского Conseil Européen pour la Recherche Nucléaire — Европейского совета по ядерным исследованиям), включающие вычисления более, чем по 60 проектам. Второй типичный проект использования грид-технологий - генерация электроэнергии с помощью термоядерного синтеза на экспериментальном реакторе, расположенном во Франции. Запущен также проект коммерциализации грид-технологий, в рамках которого небольшие компании, научные учреждения, вузы, которые нуждаются в вычислительных ресурсах, но не имеют своего

ЦОД достаточной мощности, смогут покупать вычислительное время грида.

Принцип работы грид-систем можно пояснить именно на примере грида Большого андронного коллайдера (БАК), имеющего иерархическую структуру. Самую верхнюю точку иерархии, ее нулевой уровень составляет ЦОД в CERN (получение информации с детекторов, сбор «сырых» научных данных). Первый уровень — хранение второй копии этих данных объединяет 11 ЦОД в Италии, Франции, Великобритании, США, на Тайване, которые обладают значительными ресурсами для хранения данных. Второй уровень включает многочисленные ЦОД, обладающие хорошими вычислительными ресурсами, в том числе российские ЦОД в Дубне (Объединенный институт ядерных исследований), три центра в Москве (НИИ ядерной физики МГУ, Физический институт АН, Институт теоретической и экспериментальной физики), Троицке (Институт ядерных исследований), Протвино (Институт физики высоких энергий) и Гатчине (Петербургский институт ядерной физики). Кроме того, в единую сеть с этими центрами связаны и центры других стран-участниц ОИЯИ — в Харькове, Минске, Ереване, Софии, Баку и Тбилиси. В настоящее время более 85 % всех вычислительных задач БАК выполняется вне CERN, из них более 50 % на центрах второго уровня.

10.3. Критерии грид-системы, сравнение с суперкомпьютерами и облачными вычислениями

Основатели грид-систем – И.Фостер, К.Кессельман и С.Тики выделяют три следующих ее критерия. Система называется грид, если она:

— координирует использование ресурсов при отсутствии централизованного управления этими ресурсами (если это не так, мы имеем дело с локальной системой управления);

— использует стандартные, открытые, универсальные протоколы и интерфейсы (если это не так, мы имеем дело со специализированной прикладной системой);

— нетривиальным (точнее, неаддитивным) образом обеспечивает высококачественное обслуживание (выгода от использования комбинированной системы значительно выше, чем от суммы ее отдельных частей).

В определенном смысле грид-системы представляют собой распределенный суперкопьютер, поскольку и в том, и в другом случае

используется принцип распараллеливания вычислений под управлением некоторого управляющего ПО. Но в суперкомпьютерах большое число процессоров объединяется локальной высокоскоростной шиной. А в грид-системах вычислительные ресурсы, сконцентрированные в различных ЦОД (серверы со стандартными процессорами, СХД, ИБП и т.д.), объединяются через сети (локальные и/или глобальные) при помощи стандартных протоколов.

10.4. Грид-система и облако (grid & cloud)

Нетрудно видеть общие черты в технологиях грид и облачных технологиях. Упоминавшийся выше И.Фостер писал: «Облака выросли из грид-вычислений и основываются на концепции инфраструктуры грид. Эволюция подхода заключается в том, что вместо предоставления "сырых" вычислительных ресурсов и ресурсов хранения данных, в облаках обеспечивается предоставление более абстрактных ресурсов в виде сервисов».

Но, несмотря на схожесть, обе технологии имеют и следующие существенные различия, которые удобно представить в виде таблицы (таблица 2).

Таблица 2 - Различия грид-систем и облачных вычислений

Грид-системы	**Облачные вычисления**
одна сложная задача распределяется на несколько вычислительных узлов, обеспечивая высокую загрузку вычислительных ресурсов	нескольких задач выполняются на одном физическом сервере, разделенном на виртуальные машины
используются для выполнения конкретных научных задач за ограниченный промежуток времени	ориентированы на непрерывное предоставление "долгоживущих" сервисов конечным пользователям
строятся на базе нескольких научных центров или компаний с четкими правилами взаимодействия и предоставления программно-аппаратных ресурсов	позволяют любой компании использовать сервисы, оплачивая только те ресурсы, которые необходимы для решения ее собственных задач
предоставляют программно-аппаратную базу для развертывания вычислительной инфраструктуры	предоставляют интегрированных подход для всех моделей информационных услуг: IaaS, PaaS, SaaS

интерфейсы ориентированы на взаимодействие посредством API, которым может воспользоваться только профессиональный программист	для каждой модели (IaaS, PaaS, SaaS) предоставляется свой интерфейс, что позволяет удовлетворить потребности как отдельных пользователей, так и корпоративных клиентов

В заключение отметим, что грид-технологии стали предтечей облачных вычислений, но они сохранили свое значение для решения крупных вычислительных задач, выполнение которых производится в различных территориально распределенных ЦОД.

Контрольные вопросы

1. Общее представление о грид-вычислениях.
2. Области применения грид-вычислений.
3. Критерии грид-системы.
4. Сравнение грид-вычислений и концепции облачных вычислений.

11. ЦОД и Большие Данные

11.1. Определение, критерии история

Еще одна новая технология, реализация которой невозможна без создания и развития крупных современных ЦОД, получила название «Большие Данные» (Big Data). Под этим понимается серия подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объёмов и значительного многообразия для получения результатов, доступных для восприятия человека. Этот подход актуален в условиях непрерывного прироста информации, увеличения ее неоднородности и распределенности по узлам вычислительной сети. Данный подход сформировался в конце 2000 годов как альтернативный традиционным СУБД, и относится к решениям класса бизнес-аналитики (BI - Business Intelligence).

При введении понятия Больших Данных возникает закономерный вопрос: где же точка перелома, когда данные среднего размера становятся Большими Данными? Отчасти ответ на это вопрос содержится в определении: точка перелома наступает тогда, когда человек перестает воспринимать поток поступающей к нему информации. Существует и более точное определение. Большие Данные это данные, удовлетворяющие критерию «трех больших V»:

— **volume** - объём, достигающий терабайтов - 2^{40}, петабайтов - 2^{50} и даже экзабайтов - 2^{60};

— **velocity** - скорость в смыслах как скорости прироста данных, так и скорости их обработки, выдачи по запросу, желательно, в реальном масштабе времени;

— **variety** – многообразие, т.е. данные должны включать в себя и допускать возможность одновременной обработки различных типов структурированных и неструктурированных данных - информации с сенсоров, поисковых систем, социальных сетей, медицинской и финансовой информация, SMS, мультимедиа: фотографии, презентации с графикой, музыкой, аудио и видео и т.д.

Актуальность анализа Больших Данных определяется тем, что в 2013 году объем мировых данных превысил 1,2 зеттабайт (2^{70}), в 2015 ожидалось уже 8 зеттабайт, т.е. почти удвоение по закону Мура. Если записать 8 зеттабайт на компакт-диски, то получится примерно 20 стопок высотой от Земли до Луны. Для примера напомним, что Google обрабатывает 31 млрд запросов в месяц, а в день - более 1 петабайта. Facebook насчитывает 750 миллионов пользователей, и через него осуществляется до 10 млн загрузок фотографий ежечасно. «Лайки», т.е. «Нравится» ставятся примерно 3 млрд. раз в день. В 2012 году в Twitter было 400 млн обращений в день, причем число обращений увеличивалось в год на 200%.

В добавление к объему, скорости и разнообразию есть еще одна характеристика «Больших Данных» — их ценность. Они помогают принять верное решение в нужный момент времени.

Термин «Большие Данные» был введен относительно недавно Клиффордом Линчем, редактором журнала Nature, подготовившим к 3 сентября 2008 года специальный выпуск журнала с темой «Как могут повлиять на будущее науки технологии, открывающие возможности работы с большими объёмами данных?». В этом номере были собраны материалы о феномене взрывного роста объёмов и многообразия обрабатываемых данных и технологических перспективах вероятного скачка «от количества к качеству». Термин был предложен по аналогии с расхожими в деловой англоязычной среде метафорами типа «большая нефть», «большая руда» и т.д.

Несмотря на то, что термин вводился в академической среде, и прежде всего, в связи с проблемой роста и многообразия научных данных, начиная с 2009 года, он широко распространился в деловой прессе. В 2010 году появляются первые продукты и решения, относящиеся исключительно к проблеме обработки Больших Данных. А в 2011 году большинство крупнейших поставщиков информационных

технологий для организаций в своих деловых стратегиях используют понятие о Больших Данных, в том числе IBM, Oracle, Microsoft, Hewlett-Packard, EMC. С этого времени основные аналитики рынка информационных технологий посвящают концепции выделенные исследования.

По итогам 2011 года Большие Данные фигурировали в качестве явления номер два в информационно-технологической инфраструктуре после виртуализации и перед энергосбережением и мониторингом. Прогнозируется, что внедрение технологий Больших Данных наибольшее влияние окажет на информационные технологии.

11.2. Источники Больших Данных и методы их анализа

Примерами источников создания Больших Данных являются непрерывно поступающие данные с измерительных устройств, радиочастотных идентификаторов, потоки сообщений из социальных сетей, метеорологические данные, данные дистанционного зондирования земли, потоки данных о местонахождении абонентов сетей сотовой связи, устройств аудио- и видеорегистрации. Развитие и начало широкого использования этих источников стало стимулом для проникновения технологий Больших Данных в научно-исследовательскую деятельность, коммерческий сектор и сферу государственного управления.

В настоящее время отсутствует строгая классификация методов, используемых при анализе Больших Данных. К ним, в частности, относят:

— методы обучения ассоциативным правилам, кластерный анализ, регрессионный анализ;

— смешение и интеграция данных — набор техник, позволяющих интегрировать разнородные данные из разнообразных источников для возможности глубинного анализа (например, цифровая обработка сигналов, обработка естественного языка, включая тональный анализ);

— машинное обучение с использованием моделей, построенных на базе статистического анализа или машинного обучения для получения комплексных прогнозов на основе базовых моделей;

— искусственные нейронные сети, сетевой анализ, оптимизация, в том числе генетические алгоритмы;

— распознавание образов;

— прогнозная аналитика;

— имитационное моделирование;

— пространственный анализ — класс методов, использующих топологическую, геометрическую и географическую информацию в данных;

— статистический анализ;

— визуализация аналитических данных — представление информации в виде рисунков, диаграмм, с использованием интерактивных возможностей, анимации как для получения результатов, так и для использования в качестве исходных данных для дальнейшего анализа.

11.3. Средства обработки Больших Данных

В настоящее время программно-аппаратные средства, предназначенные специально для обработки Больших Данных, только, создаются. Можно предположить, что это связано со сравнительно недавним появлением самого термина «Большие Данные». Тем не менее, к средствам их обработки относят следующие уже существующие технические решения:

— аппаратно-программные комплексы, поставляемые, как готовые к установке в ЦОД телекоммуникационные шкафы, содержащие кластер серверов и управляющее ПО для массовой параллельной обработки данных;

— аппаратные решения для аналитической обработки в оперативной памяти, хотя такая обработка изначально не является массово-параллельной, а объёмы оперативной памяти одного узла ограничиваются несколькими терабайтами;

— аппаратно-программные комплексы на основе традиционных реляционных СУБД, как способные эффективно обрабатывать терабайты и экзабайты структурированной информации, решая задачи быстрой поисковой и аналитической обработки огромных объёмов структурированных данных;

— аппаратные решения DAS-систем хранения данных, напрямую присоединённых к узлам, в условиях независимости узлов обработки, иногда относят к технологиям Больших Данных. Именно с появлением концепции Больших Данных связан всплеск интереса к DAS-решениям в начале 2010 годов, а также к сетевым решениям классов NAS и SAN.

11.4. Особенности работы с Большими Данными и области применения

Характерной особенностью работы с Большими Данными являются следующие особенности.

1. Анализируются все данные, а не статистические выборки. Например, для определения зоны распространения гриппа N1H1 специалисты Google выявили 45 из 50 миллионов условий поиска в интернете определенных лекарств и сравнили их с зонами распределения гриппа за 2003-2008 годы. Точность определения территорий распространения заболевания составила 97%. Стив Джобс, основатель компании Apple, продлил себе жизнь на несколько лет, проанализировав свою ДНК полностью, что позволило врачам менять лекарства при мутациях его раковой опухоли. Компания Xoom, специализирующаяся на денежных переводах, проанализировав все данные по операциям с кредитными картами, обнаружила действия преступной группировки. Интересен также анализ результатов всех боев в борьбе сумо, который позволил выявить наиболее вероятные договорные бои.

2. Отсутствие точности. В мире Больших Данных высокая точность невозможна – данные постоянно меняются, они неупорядочены, разного качества, разбросаны по разным серверам иногда по всему миру. Известно, что компьютерные переводчики не обеспечивали переводы нужного качества, поскольку переводился не смысл текста, а каждое слово по отдельности. Google применил иной метод, когда миллионы страниц оригинальных документов различного качества, взятых из интернет-контента сопоставлялись с их переводом. Система содержала триллион слов в 95 миллиардах англоязычных предложений, что позволило в разы улучшить качество перевода. К середине 2012 года эта система охватила более 60 языков и была способна принимать голосовой ввод с 14 языков для моментального перевода.

Ранее индекс потребительских цен в США определялся путем опроса цен на 23000 товаров в 90 городах США. Сканирование Web-страниц позволило учесть стоимость 5 млн товаров, хотя точность сведений была гораздо ниже, чем при опросах.

3. Корреляция, а не причинность. Еще одна особенность работы с Большими Данными – это отход от поиска причинностей. Вместо поиска причин того или иного явления ищутся корреляции. Например, если мы знаем, что сочетание двух веществ излечивает определенную болезнь, то нам не так важно, почему это происходит. Компания Amazon применила этот принцип к предложению книг, покупаемых у нее на сайте. Покупателю предлагается не то, что он покупал ранее, а то, что схоже с заказываемой книгой, т.е. по корреляции содержания. Классический пример результата анализа Больших Данных

дает пример компании сети магазинов Wallmart, которая хотела выяснить, какие товары являются наиболее продаваемыми среди тех, что люди покупают перед ураганом. Ответ № 1 — батарейки — не был сюрпризом. Ответ № 2 был неожиданным — полуфабрикаты для тостов Pop-Tarts. Оказывается, эта сахарная выпечка хороша в чрезвычайных ситуациях. Она легка, не требует приготовления и долго хранится без холодильника. В результате получения этой информации Wallmart теперь запасается перед сезоном штормов тостами Pop-Tarts в магазинах на побережье.

В качестве областей применения Больших Данных можно назвать:

— научные исследования (мониторинг среды, зондирование атмосферы, расшифровка генома человека);

— медицина (обследование организма в целом, анализ аномалий генов конкретного человека);

— коммерция (анализ влияния большого числа факторов на объемы продаж большого числа товаров).

11.5. Российские особенности

Выделим особенности работы с Большими Данными, характерными для России. В настоящее время основными потребителями данной технологии являются банковский (работа с клиентскими базами) и телекоммуникационный (анализ абонентской базы) сектора экономики. К перспективным направлениям относятся государственный сектор (электронное правительство) и медицина (быстрый анализ общего состояния пациента). На российском рынке пока отсутствуют держатели больших объемов данных типа компаний Google и Amazon, но, возможно, таковыми станут «Яндекс», «Mail.ru» и им подобные. Технологией Больших Данных могли бы воспользоваться научно-исследовательские организации, но их бюджеты пока слишком малы, как и бюджеты предприятий малого и среднего бизнеса. Определенные надежды вселяет создание исследовательских центров компании EMC в Санкт-Петербурге и Сколково, которые должны заняться применением технологии Больших Данных в биомедицине и повышении энергоэффективности производства.

Контрольные вопросы

1. Определение и характеристика Больших Данных.
2. Источники Больших Данных и методы их анализа.
3. Средства обработки Больших Данных.

4. Особенности работы с Большими Данными.
5. Области применения Больших Данных.
6. Особенности работы с Большими Данными в РФ.

Заключение

Технологии создания ЦОД и отдельных их подсистем непрерывно совершенствуются. Этому способствуют как быстрое развитие информационных технологий вообще, так и таких направлений, как совершенствование и рост числа мобильных устройств, увеличивающаяся популярность облачных вычислений, расширяющаяся потребность работы с Большими Данными. Все более широко применяется виртуализация как серверов, так и СХД, а также функциональная виртуализации сетей. Управление такими виртуализированными структурами с помощью программного обеспечения позволит в перспективе создать программно-определяемый ЦОД, в разы и более эффективный, чем современные. Уже сейчас понятно, что использование ДНК для создания емких и долговечных СХД может совершить революцию в этих системах. По-видимому, качественный рывок ожидает в перспективе и технологию производства процессоров, поскольку длина транзисторного затвора приблизилась к атомарным размерам и дальнейшее возрастание тактовой частоты транзисторов требует прорывных нетривиальных решений. Пока трудно предсказать, какой прорыв ожидает коммуникационное оборудование вслед за внедрением технологий SDN и NFV. Но, несомненно, будет и он.

Все шире при организации ЦОД будет применяться фрикулинг и гринкулинг, а электропитание будет осуществляться от возобновляемых источников энергии – солнечной, ветровой и приливной. Примеры тому имеются уже сегодня. Трудно предсказать, какими будут ЦОД даже через 50 лет. Но они, несомненно, будут отличаться от нынешних сильнее, чем нынешние отличаются от вычислительных центров и серверных комнат середины и второй половины прошлого века.

Аббревиатуры

№ п/п	Аббревиатура	Расшифровка	Перевод
1	API	Application programming interface	Прикладной программируемый интерфейс
	APS	Application Packaging Standard	Стандарт упаковки приложений в облачных вычислениях
2	BI	Business Intelligence	Бизнес аналитика
3	BPM	Business Performance Management	Управление эффективностью бизнеса
4	CD-ROM	Compact Disc Read Only Memory,	Компакт-диск с возможностью только чтения
5	CD-RW	Compact Disc-ReWritable	Перезаписываемый компакт-диск
6	CISC	Complex Instruction Set Computing	Вычисления с полным набором инструкций
7	CPU	Central Processing Unit	Центральное процессорное устройство
8	CRM	Customer Relationship Management System	Система управления заказами предприятия
9	CSA	Cloud Security Alliance	Союз облачной безопасности
10	DAS	Direct-attached Storage	Устройство внешней памяти, напрямую подсоединенное к основному серверу или компьютеру
11	DCIM	Data Center Infrastructure Management	Система управления инфраструктурой ЦОД
	DDoS-атака	Distributed Denial of Service	Распределённая атака типа «отказ в обслуживании»
12	ENI	Equipment Network Interface,	Сетевые интерфейсы оборудования
13	EO	Equipment Outlet	Розетки оборудования СКС
14	ERP	Enterprise Resource Planning system	Система планирования ресурсов предприятия
15	HDD	Hard Disk Drive	Накопитель на жестком диске
16	HPC	High Performance	Высокопроизводительные

		Computing	вычисления
17	HVAC	Heating, Ventilation, Air Condition	Теплоснабжение, вентиляция, кондиционирование
18	IDS	Intrusion Detection System	Система обнаружения вторжений
19	IOPS	Input/Output Operations Per Second	Количество операций ввода/вывода в секунду
20	IPS	Intrusion Prevention System	Система предотвращения вторжений
21	iSCSI	Internet Small Computer System Interface	Протокол, который базируется на TCP/IP и разработан для установления взаимодействия и управления системами хранения данных, серверами и клиентами
22	ITSM/ITIL	IT Service Management on the base of IT Infrastructure Library	Управление ИТ-сервисами на основе библиотеки методик и правил постановки процессов работы ИТ-служб
23	LDP	Local Distribution Point	Локальный пункт распределения СКС
24	LUN	Logical Unit Number	Адрес дискового устройства.
25	MD	Main Distributor	Основной кросс СКС
26	SLC	Single Level Cells	Твердотельный накопитель с многоуровневыми ячейками
27	NAS	Network attached storage	Сетевое устройство хранения
28	NFV	Network Function Virtualization	Функциональная виртуализация сетей
29	NIST	The National Institute of Standards and Technology	Национальный Институт Стандартов и Технологи США
30	NMS	Network Management Service	Система сетевого управления
31	OEM	Original Equipment Manufactures	Производитель изначальной комплектации
32	PoE	Power over Ethernet	Электропитание по сети Ethernet

33	PUE	Power Utilization Efficiency	Энергоэффективность – отношение полной мощности, потребляемой ЦОД к мощности, потребляемой вычислительным оборудованием
34	QoS	Quality of Service	Качество обслуживания. Для компьютерных сетей - вероятность того, что сеть связи соответствует заданному соглашению о трафике, или же неформальное обозначение вероятности прохождения пакета между двумя точками сети.
35	RAID	Redundant Array of Independent (Inexpensive) Disks	Избыточный массив независимых (недорогих) дисков
36	RISC	Reduced Instruction Set Computing	Вычисления с сокращенным набором инструкций
37	ROI	Return of Investment	Уровень доходности или убыточности бизнеса (отношение дохода или убытка к сумме инвестиций)
38	SAN	Storage Area Network	Сеть хранения данных
39	SDDC	Software Defined Data Center	Программно определяемый ЦОД
40	SDN	Software-Defined Networking	Программно конфигурируемые сети
41	SDS	Software Defined Storage	Программно определяемое хранение
42	SLA	Service Level Agreement	Соглашение об уровне сервиса
43	SLC	Single Level Cells	Твердотельный накопитель с одноуровневыми ячейками
44	SMP	Symmetrical Multiprocessing	Технология симметричного распределения нагрузки между несколькими процессорами одного

			компьютера
45	SSD	Solid State Drive	Твердотельный накопитель
46	TCO	Total Coast Ownership	Совокупная стоимость владения
47	TIA/EIA	Telecommunications Industry Association /Electronic Industries Alliance	Стандарт Ассоциации телекоммуникационной промышленности, филиала Альянса электронной промышленности
48	TSL	Triple Level Cells	Твердотельный накопитель с трехуровневыми ячейками
49	UPS	Uninterruptible Power Supply,	Источник бесперебойного питания (ИБП)
50	VPN	Virtual Private Network	Виртуальная частная сеть
51	ZD	Zone Distributor	Зонные кроссы СКС
52	АВР	Автомат ввода резерва	
53	АСДУ	Автоматизированная система диспетчерского управления	
54	ИБП	Источник бесперебойного питания	
55	ИГП	Источник гарантированного питания	
56	ИТ	Информационные технологии	
57	ИТ-оборудование	Оборудование, используемое в информационных технологиях	
58	ЛВС	Локальная вычислительная сеть	
59	МФО	Модуль функционального оборудования контейнерного ЦОД	
60	ОС	Операционная система	
61	ПО	Программное обеспечение	
62	СГП	Система гарантированного питания	
63	СКС	Структурированная кабельная система	
64	СМБ	Средний и малый бизнес	
65	СОС	Сетевая операционная система	
66	СХД	Система хранения данных	
67	ЦОД	Центр обработки данных	
68	ЭМ	Энергетический модуль контейнерного ЦОД	

Список литературы

1. Беленькая М.Н., Докучаев В.А., Яковенко Н.В. Основы сетевых технологий и высокоскоростной передачи данных: учебное пособие. Ч. 1 /МТУСИ. - М., 2009.
2. Докучаев В.А., Лопатина Е.В., Павлов С.В., Яковенко Н.В. Архитектура, основы построения и проектирования корпоративных сетей на базе IP-технологий: учебное пособие /МТУСИ. - М., 2009.
3. Беленькая М.Н., Докучаев В.А., Малиновский С.Т., Яковенко Н.В. Основы сетевых технологий и высокоскоростной передачи данных: учебное пособие. Ч. 2 /МТУСИ. - М, 2011.
4. Докучаев В.А., Шведов А.В. Защита информации на корпоративных сетях VoIP. // Электросвязь. - 2012.-№ 4.- С. 32-35.
5. Докучаев В.А., Воробьёв М.М., Ермалович А.В., Кондратьев М.Г., Маклачкова В.В., Шведов А.В. Сетевая безопасность и её планирование: учебное пособие/МТУСИ. – М. 2018.
6. Смелянский Р.Л. Программно-конфигурируемые сети. // Открытые системы. СУБД – 2012, № 09.
7. Смелянский Р.Л.. Технологии SDN и NFV: новые возможности для телекоммуникаций // Вестник связи, 2014, №1.
8. Орлов С.В. SDN и другие // Журнал сетевых решений/LAN, 2014 № 6.

СОДЕРЖАНИЕ

План УМД на 2017/2018 уч.г.
С. 8, п. 52

Денис Вадимович Гадасин

Владимир Анатольевич Докучаев

Александр Викторович Ермалович

Александр Алексеевич Кальфа

Виктория Валентиновна Маклачкова

Андрей Вячеславович Шведов

Архитектура центров обработки данных

Учебное пособие

Подписано в печать 16.05.18. Формат 60x90 1/16.
Объем 9,8 усл.п.л. Тираж 50 экз. Изд. № 51. Заказ

ООО «ТР-принт». Москва, ул. Правды, д. 24, стр. 5.
www.tirazhy.ru +7(499)519-01-24