**Глава 3**

***Рабочие станции***

При правильном обслуживании рабочих станций (как настольных компьютеров,

так и ноутбуков) у новых сотрудников с первого дня на работе будет все необходимое, включая основную инфраструктуру, в том числе электронную почту.

Обслуживание операционных систем на рабочих станциях сводится к выполнению трех основных задач (**большая тройка**):

1. первоначальная установка системного программного обеспечения и приложений;
2. обновление системного программного обеспечения и приложений;
3. настройка сетевых параметров.

Если вам не удастся должным образом решить эти три задачи, если они не будут

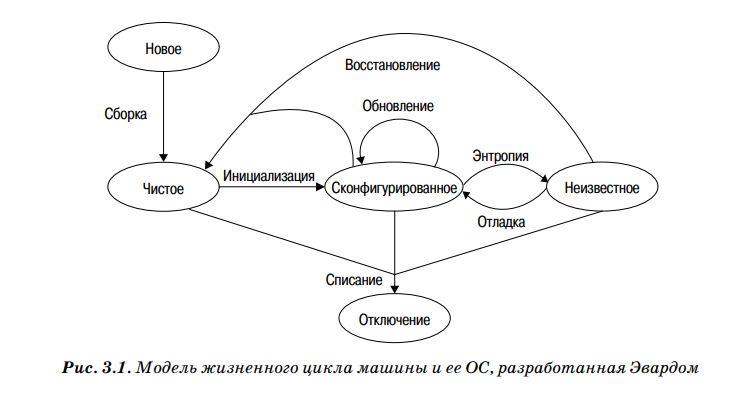
выполняться единообразно на всех системах или если вы будете вообще их игнорировать, остальная ваша работа значительно осложнится. Автоматизация этих задач значительно изменит ситуацию к лучшему.

Рабочая станция – компьютерное оборудование, выделенное для работы одного пользователя. Как правило, имеется в виду настольный компьютер или ноутбук пользователя. Также это могут быть компьютеры с удаленным доступом, виртуальные машины и ноутбуки с док-станциями.

Рабочие станции, как правило, используются в больших количествах и отличаются долгим жизненным циклом (рождение, использование, смерть), и тем самым вносить изменения во все рабочие станции сложно, но критически важно.

***Жизненный цикл компьютера и его операционной системы на примере UNIX-систем. Модель***

***Реми Эварда на рис. 3.1.***



На схеме отображено пять состояний: **новое, чистое, сконфигурированное, неизвестное и отключенное.**

**Новое** состояние относится к совершенно новой машине.

**Чистое** состояние относится к машине с установленной, но еще не настроенной ОС.

**Сконфигурированное** состояние означает, что система настроена и функцио­нирует должным образом.

**Неизвестное** состояние относится к компьютеру, который был неправильно

сконфигурирован или конфигурация которого устарела.

**Отключенное** состояние относится к машине, которая была списана и отключена.

Существует множество способов перевести машину из одного состояния жизненного цикла в другое.

**Сборка и инициализация** переводит машину из чистого в сконфигурированное состояние.

**Энтропия** – процесс нежелательной амортизации, приводящий компьютер

в неизвестное состояние, которое можно исправить с помощью **отладки. Обновления, переустановка системы и восстановление данных** позволяет вернуть систему обратно в сконфигурированное состояние.

Эти различные процессы повторяются в течение месяцев и лет. И наконец машина устаревает и списывается, т.е., переводится в **отключенное** состояние.

***Какую информацию мы можем получить из этой схемы?***

1. Сбои будут неизбежно происходить, и необходимо разработать план по их своевременному устранению.
2. Компьютер можно использовать только в сконфигурированном состоянии. Необходимо до максимума увеличить время, проводимое в этом состоянии. Восстановления должны проводиться быстро, эффективно и, желательно,

автоматически.

Чтобы продлить время пребывания компьютера в сконфигурированном состоянии, необходимо максимально замедлить деградацию ОС. Главным фактором здесь являются архитектурные решения поставщика ОС.

Одни операционные системы позволяют загружать дополнения практически

в любые каталоги. ОС Microsoft Windows известна своими проблемами в этой

области. С другой стороны, UNIX предоставляет разграничение доступа к каталогам, благодаря чему приложения, установленные пользователем, не могут

разрушить целостность ОС.

Системные администраторы должны найти баланс между предоставлением пользователям полного доступа и ограничением их прав. Этот баланс влияет на скорость разрушения операционной системы. Установка вручную всегда предполагает возможность ошибок. Если ошибки возникают в процессе установки, узел сети начнет свой жизненный цикл с тенденцией к разрушению. Если процесс установки полностью автоматизирован, новые рабочие станции будут развернуты должным образом.

Переустановка (процесс восстановления) подобна установке с той разницей, что в первом случае, возможно, понадобится перенести старые данные и приложения. Решения, принимаемые системным администратором на ранних стадиях, определяют, насколько простым или сложным будет этот процесс. Переустановка будет проще, если на машине не хранится никаких данных. В случае рабочих станций это означает, что как можно больше данных должно храниться на файловом сервере. Это позволит предотвратить случайное удаление данных при переустановке. В случае серверов это означает, что данные необходимо переместить на удаленную файловую систему. И наконец, эта модель показывает, что машины в конце концов списываются.

Со списанием машины связаны различные задачи:

1. Сохранить данные со списанной машины (перенести на новую или сохранить на файловом сервере)
2. Проводить списание в течение определенного срока (обычно 3 года) в рамках выделенного бюджета

В этой главе термин платформа используется для обозначения определенной

комбинации поставщика оборудования и ОС. В некоторых компаниях компьютеры от разных поставщиков под управлением одной и той же операционной системы могут считать разными платформами. Например, настольный компьютер и ноутбук под управлением Windows XP считаются разными платформами. Обычно разные версии одной и той же операционной системы считаются разными платформами, если их требования поддержки значительно различаются.

***3.1. Основы***

С обслуживанием операционных систем рабочей станции связаны т**ри критически важных аспекта:**

1. Первоначальная установка системного ПО и приложений.

2. Обновление системного ПО и приложений.

3. Настройка сетевых параметров.

Если вы хотите, чтобы управление вашей сетью производилось с минимальными затратами, эти три задачи необходимо автоматизировать для любой платформы, которая используется в вашей сети.

**3.1.1. Установка ОС**

Автоматизация установки ОС решает огромное количество проблем.

1. Экономия денег;  
   2) Экономия времени;

3) Вероятность ошибок стремится к нулю;  
4) Нет неоднородности - при ручной установке невозможно идеально вопроизводить одни и те же настройки на каждой новой машине, что позже приводит к сбоям.

**3.1.1.1. Удостоверьтесь, что ваша автоматизированная система**

**действительно автоматизирована**

Самый важный аспект автоматизации заключается в том, что установка долж-

на быть полностью автоматизирована.

Лучшие системы установки все взаимодействие с человеком выполняют в самом

начале, а затем завершают работу полностью автоматически. В некоторых сис-

темах вообще ничего не нужно вводить, так как автоматика «знает», что делать,

основываясь на MAC-адресе узла сети Ethernet. У техников должна быть воз-

можность покинуть машину, будучи уверенными, что процедура завершится

самостоятельно. Процедуру, требующую возвращения человека посреди уста-

новки для ответа на тот или иной вопрос, нельзя назвать полностью автомати-

зированной, и она теряет эффективность.

Система JumpStart для ОС Solaris – безупречный образец полностью автомати-

зированной программы установки. Программа на сервере JumpStart запраши-

вает, какой шаблон использовать для нового пользователя. Старший системный

администратор может настроить эти шаблоны заранее. Когда приходит время

устанавливать операционную систему, техник – возможно, даже офисный слу-

жащий, направленный для запуска процесса, – должен просто ввести команду

boot net – install. Служащий ожидает подтверждения, что процесс установки

начался, а затем уходит. Через 30–90 мин, в зависимости от скорости сети,

машина загружена, сконфигурирована и готова к работе.

**3.1.1.2. Частично автоматизированная установка**

Частичная автоматизация лучше, чем ее полное отсутствие. До тех пор пока

система установки не будет работать идеально, необходимо обеспечить какие-то

временные средства для некоторых этапов.

Основная временная мера – документирование всего процесса, которое позволит

впоследствии воспроизводить его в точности. Документирование может произ-

водиться в виде записей при создании первой системы, чтобы на различные

запросы можно было давать одни и те же ответы.

Можно автоматизировать различные этапы установки. Некоторые из них отлично поддаются автоматизации. Например, процесс инициализации конфигурирует ОС, установленную с настройками по умолчанию, в соответствии с конкретным сетевым окружением. Как правило, сюда входят установка определенных файлов, настройка доступа и перезагрузка. Спасительным решением здесь может быть скрипт, копирующий определенный набор файлов в определенное место на диске. Можно даже упаковать в архив tar или zip файлы, измененные во время настройки, а затем распаковать их на машины после стандартной процедуры установки.

**Временные меры**

**Вопрос**: Что необходимо сделать, чтобы временные меры не стали посто-

янным решением?

**Ответ**: Следует создать заявку, в которой будет отмечена необходимость

в постоянном решении.

**3.1.1.3. Клонирование и другие методы**

Клонирование жесткого диска - создание узла с точной конфигурацией ПО, которая необходима для всех развертываемых узлов. Затем жесткий диск этого узла клонируется (копируется) на все новые компьютеры. Первую машину часто называют «золотым узлом».

Вместо того чтобы снова и снова копировать жесткий диск, его содержимое можно скопировать на компакт-диск, ленточный накопитель или файловый сервер, которые

впоследствии будут использоваться при установке.

Минусы такого вида установки:

1) Для более новых машин необходимо создать отдельный

мастер-образ. Это может привести к необходимости иметь большое количество мастер-образов и вносить изменения в них.  
2) Наличие резервных машин для каждого типа оборудования, требующего новых образов, значительно повышает расходы и усилия, необходимые для установки.

3) Поставщики некоторых ОС не поддерживают клонированные диски.

Можно достичь золотой середины, применяя как автоматизацию, так и клони-

рование. В некоторых сетях клонируют диски для минимальной установки ОС,

а затем используют автоматическую систему установки приложений и патчей

поверх ОС. В других сетях используют стандартную систему установки ОС,

а затем «клонируют» приложения или модификации системы на машины.

**3.1.1.4. Стоит ли доверять установкам от поставщиков**

Обычно компьютеры поставляются с предустановленной ОС. Зная это, вы мо-

жете решить, что вам не надо переустанавливать ОС, если кто-то сделал это за

вас. Но нет. На самом деле переустановка ОС скорее будет выгоднее:

1. Вам, вероятно, потребуется установить другие приложения и локализации поверх установленной поставщиком ОС, в таком случае проще попросту переустановить ОС.

2) Поставщики вносят изменения в конфигурацию предустановленной ОС, никого об этом не уведомляя. Установка с нуля дает вам известное состояние каждой машины.

3) Время от времени ОС узлов сети приходится переустанавливать. Если часть ваших машин работает с предустановленной ОС, а остальные – с установленной вами, у вас появляются две платформы, требующие поддержки.

**3.1.1.5. Контрольные списки при установке**

Какой бы способ установки ОС вы ни использовали – ручной или полностью ав-

томатизированный, – вы можете улучшить согласованность процесса с помощью

контрольных списков. Эти списки помогают удостовериться, что техники не

пропустят ни одного этапа. Польза таких списков очевидна, если процесс уста-

новки полностью выполняется вручную. Даже если установку проводит один

системный администратор, полностью уверенный в согласованности установки

всех ОС («я все делаю сам»), он поймет преимущества использования контрольных

списков. И конечно же, эти списки могут послужить основой для системы обуче-

ния новых системных администраторов или подготовки толкового служащего,

который будет выполнять эту работу в соответствии с пунктами списка.

Даже если процесс установки ОС полностью автоматизирован, грамотный кон-

трольный список все же может принести пользу. В ваш контрольный список могут входить такие задачи, как: обновление инвентаризационных описей, составление заказов на сетевые кабели (если их количество меньше определенного числа), проверка, не возникли ли у пользователей проблемы или какие-либо вопросы.

**3.1.2. Обновление системного ПО и приложений**

С течением времени обнаруживаются новые ошибки и новые бреши

в системе безопасности, и все их необходимо исправлять. Кроме того, появля-

ются прекрасные новые приложения, которые необходимо устанавливать. Все

эти задачи относятся к области обновления программного обеспечения. Процесс

обновления можно автоматизировать, сэкономив время и силы.

Системы обновления ПО должны быть достаточно универсальными, чтобы они

позволяли устанавливать новые приложения и обновлять уже имеющиеся,

а также устанавливать патчи ОС. Если система способна только устанавливать

патчи, новые приложения можно упаковать и использовать их в качестве патчей.

Такие системы также можно использовать для внесения незначительных изме-

нений на большом количестве узлов сети.

**3.1.2.1. Процесс обновления отличается от установки**

Автоматизация обновления ПО схожа с автоматизацией первичной установки,

но между ними есть и несколько существенных различий:

**- Узел сети находится в рабочем состоянии**

**- Узел сети находится в офисе**

**- Отсутствует необходимость в физическом доступе**

**- Узел сети уже используется**

**- Узел сети может не находиться в «известном состоянии»**

**- Узел сети может использоваться сотрудниками в процессе обновления**

**- Узел сети может отсутствовать**

**- Узел сети может иметь мультисистемную загрузку**

**3.1.2.2. Одна, несколько, много**

Последствия ошибок при установке патчей отличаются от таковых при установке ОС. Пользователь, скорее всего, даже не узнает, были ли ошибки при установке ОС, так как до этого узел сети фактически не используется. Однако узел сети, на который устанавливается обновление, как правило, уже находится на рабочем столе сотрудника. Ошибки обновления, которые перевели машину в нерабочее состояние, гораздо заметнее и вызывают гораздо большее раздражение у пользователей.

Вы можете снизить риск ошибок обновления, применив метод **«одна, несколь-**

**ко, много».**

**Одна**. Прежде всего установите патч на одну машину. Лучше всего на свою

собственную – тогда у вас будет дополнительный стимул все сделать пра-

вильно. Если при обновлении возникнут ошибки, вносите в процесс изме-

нения до тех пор, пока он не будет работать на одной машине без ошибок.

**Несколько**. Далее попробуйте установить патч на несколько других машин.

Если это возможно, стоит протестировать автоматизированный процесс об-

новления на рабочих станциях остальных системных администраторов,

прежде чем задействовать машины пользователей. Системные администра-

торы проявляют чуть больше понимания. Затем протестируйте систему на

нескольких машинах дружелюбно настроенных к вам пользователей (не

системных администраторов).

**Много**. Протестировав свою систему и убедившись, что она не уничтожит

ничей жесткий диск, начинайте постепенно переходить ко все большим

и большим группам пользователей, нетерпимых к риску.

Автоматизированная система обновления потенциально способна нанести об-

ширные повреждения. Весь процесс должен быть хорошо документирован,

чтобы обеспечить максимальную степень управления риском. Необходимо

обеспечить грамотное описание и повторяемость процесса, и вы должны пытать-

ся улучшить его после каждого использования. Вы сможете избежать больших

проблем, если будете следовать этой системе. При каждой установке чего-либо

вы идете на риск. Ненужный риск недопустим.

**3.1.3. Конфигурирование сети**

Третий компонент, необходимый для сетей, объединяющих большое количество

рабочих станций, – это способ автоматизации обновления сетевых параметров. Эта информация может значительно различаться в отдельных подсетях или даже в отдельных узлах сети. А следовательно, такое обновление должно производиться иначе, чем установка приложений, когда одно и то же приложение устанавливается на всех узлах сети с одинаковой конфигурацией. Поэтому система автоматизации обновления сетевых параметров обычно создается отдельно от остальных систем.

Наиболее распространенная система автоматизации этого процесса – **DHCP**.

Серверы DHCP от некоторых поставщиков настраиваются за несколько секунд,

другие серверы – значительно дольше. Создание глобальной архитектуры DNS/

DHCP с десятками или сотнями сетей требует основательного планирования

и специальных знаний.

Использование DHCP позволит проводить изменения в сети безболезненно, вместо того, чтобы тратить большое количество времени, чтобы

внести изменения на все узлы вашей сети вручную.   
**3.1.3.1. Используйте шаблоны, а не конфигурируйте**

**каждый отдельный узел**

Системы DHCP должны иметь систему шаблонов. Некоторые системы DHCP

хранят отдельные параметры, присвоенные каждому отдельному узлу сети.

Другие системы DHCP хранят шаблоны, описывающие, какие параметры при-

сваиваются узлам различных классов.

**Преимущества шаблонов:**

1. При внесении изменений на множестве узлов нужно лишь изменить шаблон, а не прокручивать длинный список узлов сети.
2. Значительно уменьшается вероятность появления ошибки в синтаксисе,

если конфигурационный файл генерируется программой. Многие системные адми-

нистраторы пишут небольшие программы, чтобы создать свою систему шаблонов.

Список узлов сети хранится в базе данных (или даже в простом текстовом файле),

и программа использует эти данные для конфигурирования сервера DHCP.

Вместо того чтобы вводить информацию по каждому отдельному узлу сети

в новый файл или создавать сложную базу данных, информацию можно внедрить

в вашу существующую базу данных или файл с перечнем оборудования. Напри-

мер, в UNIX-сетях достаточно просто ввести эту информацию в уже ведущийся

файл /etc/ethers. Этот файл затем используется программой, которая генериру-

ет конфигурацию DHCP. Ниже приведен пример строк из подобного файла:

8:0:20:1d:36:3a adagio #DHCP=sun (рабочая станция Sun)

0:a0:c9:e1:af:2f talpc #DHCP=nt (узел Windows NT)

0:60:b0:97:3d:77 sec4 #DHCP=hp4 (принтер HP LaserJet 4)

0:a0:cc:55:5d:a2 bloop #DHCP=any

0:0:a7:14:99:24 ostenato #DHCP=ncd-barney (Х-терминал NCD, загру-

жающий TFTP-сервер barney)

0:10:4b:52:de:c9 tallt #DHCP=nt

0:10:4b:52:de:c9 tallt-home #DHCP=nt

0:10:4b:52:de:c9 tallt-lab4 #DHCP=nt

0:10:4b:52:de:c9 tallt-lab5 #DHCP=nt

Маркер #DHCP= должен обрабатываться как комментарий всеми действующими

программами, обращающимися к файлу. Последние четыре

строки показывают, что ноутбук Тома должен получить разные IP-адреса

в зависимости от подсети, к которой он может быть подключен: в офисе, дома

или в лаборатории на четвертом либо пятом этаже.

Внедрив эту информацию в файл /etc/ethers, мы снизили вероятность появления

ошибок. Если бы информация была в отдельном файле, данные могли бы про-

тиворечить друг другу.

**3.1.3.2. Когда применять динамическую аренду адресов**

Зачастую лучше закрепить конкретный IP-адрес за конкретным узлом сети. Это особенно важно для серверов, чьи IP-адреса прописываются в конфигурационных файлах других узлов, таких как DNS-серверы и межсетевые экраны. Этот метод называется статическим назначением адресов в RFC или постоянной арендой адресов в DHCP-серверах компании Майкрософт.

Динамическое распределение следует использовать в случаях, когда много узлов

конкурируют за малое количество IP-адресов. Например, у вас может быть сер-

вер удаленного доступа (RAS, Remote Access Server) на 200 модемов для тысяч

узлов, которые могут с ним соединиться. В этой ситуации имеет смысл органи-

зовать динамическое пространство на 220 адресов. Можно привести еще один

пример: сеть с часто сменяющимися временными узлами, такая как лаборатор-

ный испытательный стенд, комнаты настройки компьютеров или сеть для ноут-

буков посетителей. В этих случаях может быть достаточно физического про-

странства или портов только для определенного количества компьютеров.

Пространство IP-адресов можно несколько расширить сверх этого максимума.

Типичная офисная локальная сеть лучше подходит для динамически назнача-

емой аренды. Тем не менее есть преимущества в выделении статической аренды

адресов для отдельных машин:

1. Если конкретные машины всегда получают одни и те же адреса, вы предотвратите вероятность того, что эти машины не смогут получить IP-адрес, когда диапазон адресов будет исчерпан.
2. Повышение удобства использования файлов журнала. Если рабочим станциям всегда присваиваются одни и те же IP-адреса, в файлах журнала они будут отображаться, соответственно, с теми же IP-адресами. Кроме того, некоторые программные пакеты могут некорректно работать с узлом с изменяющимся IP-адресом.

Использование только статических IP-адресов не является достаточной мерой

для безопасности. В некоторых сетях отключают любое динамическое назначение адресов, считая, что это предотвратит использование их сети незваными

гостями. В действительности же кто-нибудь все еще может вручную конфигурировать сетевые настройки.

Лучшее решение здесь – IEEE 802.1x. Этот стандарт управления доступом

к сети определяет, будет ли разрешено новому узлу подключиться к сети. Из-

начально применявшееся в сетях WiFi, управление доступом к сети все шире

используется и в проводных сетях. Коммутатор Ethernet, поддерживающий

стандарт 802.1x, не дает новому узлу подключаться к сети, пока тот не пройдет

определенную процедуру аутентификации. В зависимости от того, пройдена

аутентификация или нет, разрешается передача данных либо узел получает

отказ в доступе к сети.

**3.1.3.3. Использование DHCP в сетях общего пользования**

Например, в отелях или других общественных местах, где сеть была

сконфигурирована следующим образом: в сеть выйти очень легко, но можно

получить доступ только к веб-странице авторизации. После авторизации

(с помощью либо какого-то способа идентификации, либо платежа с кредитной

карты) можно получить полный доступ. В таких ситуациях системные адми-

нистраторы предпочитают решение plug-in-and-go (подключись-и-работай) для

выделения пространства адресов, но при этом должна быть возможность про-

верки, есть ли у пользователей разрешение на использование ресурсов корпо-

рации, университета или отеля. Их системы позволяют незарегистрированным узлам зарегистрироваться от имени человека, который берет на себя ответственность за

любой ущерб, нанесенный этими неизвестными узлами.

**3.1.4. Старайтесь не использовать**

**динамический DNS-сервер с DHCP**

В системах с динамическим DNS-сервером клиентский узел сообщает серверу

DHCP, каким должно быть имя узла сети, а сервер DHCP отправляет обновления

на DNS-сервер (клиентский узел также может отправлять обновления напрямую

на DNS-сервер). Неважно, к какой сети подключена машина, информация DNS

для этого узла соответствует имени узла.

Узлы со статической арендой всегда имеют одно и то же имя в DNS, так как они

всегда получают один и тот же IP-адрес. При использовании динамической

аренды IP-адрес узла выбирается из пространства адресов в DNS, каждый из

которых, как правило, обладает шаблонным именем.

Если узел не запускает никакие службы, никто не будет обращаться к нему по имени, а поэтому не имеет значения, какое имя для него прописано в DNS. Если же узел запускает службы, эта машина должна получить постоянную аренду DHCP и всегда иметь одно и то же фиксированное имя. Если позволить узлу определять собственное имя, появится риск нарушения безопасности. Имена узлов должны контролироваться централизованной системой, а не пользователем узла.

Большинство динамических систем DNS/DHCP позволяют заблокировать имена важных серверов, а это означает, что список важных серверов является новым пространством имен, которое необходимо контролировать и обслуживать. Если вы случайно забудете включить имя нового сервера, может произойти трагедия.

Старайтесь не допускать ситуаций, в которых простые ошибки одних пользова-

телей могут помешать работе других. До появления DHCP пользователи часто «вешали» локальную сеть, случайно устанавливая IP-адрес, аналогичный IP-адресу маршрутизатора. Разрешение клиентам устанавливать собственное имя узла – один из

вариантов той же ситуации, который приведет к подобным результатам. На-

пример, может начаться эпидемия новых проблем, если пользователи в качестве

имени узла выберут предоставленное им имя сервера электронной почты, имя

домена или другой базовой службы.

Еще один вопрос относится к тому, каким образом аутентифицируются обнов-

ления DNS. Протоколы защиты для этих обновлений гарантируют, что узел,

который добавил запись в DNS, – это тот же самый узел, который запрашивает

удаление или замену этой записи. Протоколы не могут предотвратить первичный

ввод данных и не могут контролировать формат или лексикон разрешенных

имен. Добавление новых уровней сложных баз данных ради управ-

ления рисками требует массы усилий, и этого можно избежать, если просто-

напросто не использовать упомянутую возможность.

Кое-кто может поспорить, что эта возможность улучшает отслеживаемость, так

как в журналах всегда указывается одно и то же имя узла. Но для улучшения отслеживаемости лучше всего воспользоваться системой регистрации и слежения.

Динамический DNS-сервер с DHCP создает систему, которая является более

запутанной, более сложной для управления, более подверженной сбоям и менее

безопасной. И все это в обмен на небольшую эстетическую приятность. Оно того

не стоит.

***3.2. Тонкости***

**3.2.1. Полная уверенность в завершении**

Существуют автоматизированные процессы, но помимо этого есть и автомати-

зация процесса. Если мы абсолютно уверены в процессе, мы избавлены от необ-

ходимости беспокоиться об ошибках. И поэтому мы начинаем искать новые

способы применения этого же процесса.

**3.2.2. Вовлечение пользователей в процесс стандартизации**

Если пользователи будут иметь дело со стандартной конфигурацией, вам необ-

ходимо вовлечь их в процесс составления спецификаций и разработки. Назначенные представители или заинтересованные руководители могли бы выбирать приложения, которые будут включены в конфигурацию. Для каждого приложения составляется соглашение об уровне обслуживания, в котором описывается уровень обслуживания со стороны системных администраторов. Новые версии ОС и приложений отслеживаются и одобряются. Контролируемое внедрение новых версий аналогично описанному автоматизированному процессу обновления.

Однако в реальности платформы контролируются либо руководством (с мучи-

тельной точностью), либо отделом системного администрирования, отвечающим

за предоставление основной платформы, которую пользователи могут настраи-

вать под себя.

Вторые случаи более распространенны. В одной сети стандартной платформой

для персонального компьютера считается его операционная система; самые

необходимые приложения; приложения, требуемые компанией-учредителем;

утилиты, которые наиболее часто просят установить пользователи и которые

можно лицензировать оптом.

Для некоторых приложений предусмотрены более формальные процессы. На-

пример, определенной группе разработчиков требуется тот или иной инстру-

ментарий. Для разработки любого ПО предусмотрен набор инструментальных

средств, который описывается, тестируется, одобряется и устанавливается.

Системные администраторы должны принимать участие в этом процессе, чтобы

соотносить ресурсы с планом развертывания.

**3.2.3. Разнообразие стандартных конфигураций**

Наличие нескольких стандартных конфигураций может быть как плюсом, так и минусом. Чем больше стандартных конфигураций используется

в корпоративной сети, тем труднее все их обслуживать. Одна из сфер их применения - разработка особых конфигураций для установки серверов. Хотя серверы запускают совершенно особые приложения, для них существует некая базовая установка, которую можно впоследствии настроить. Если для повышения пропускной способности развертываются резервные веб-серверы, наличие полностью автоматизированной системы установки может оказаться очень полезным.

Стандартные конфигурации также могут облегчить процесс обновления ОС.

Если у вас есть возможность полностью очистить диск и заново все переустано-

вить, обновление ОС становится простейшей задачей. Для этого потребуется

приложить значительные усилия в таких областях, как разделение пользова-

тельских данных и обработка системных данных определенных узлов.

***3.3. Заключение***

Настольные компьютеры, в отличие от серверов, как правило, развертываются в больших количествах, и все они обладают практически одной и той же конфигурацией. У каждого компьютера есть свой жизненный цикл, который начинается с установки ОС и заканчивается в тот момент, когда машину выключают в самый последний раз. В этот

период программное обеспечение компьютера постепенно приходит в негодность

в результате энтропии, обновляется и заново переустанавливается в начале нового цикла. В идеале все узлы сети, относящиеся к определенной платформе, в начале своего жизненного цикла должны иметь одну и ту же конфигурацию. Обновляться они должны параллельно. Некоторые стадии жизненного цикла важнее для пользователей, чем другие. Мы стремимся увеличить продолжительность более важных стадий и сократить продолжительность менее значительных.

Основу всего, чему посвящена данная глава, составляют три процесса:

1. Первичная установка ОС должна быть автоматизирована.

2. Обновление программного обеспечения должно быть автоматизировано.

3. Конфигурация сети должна администрироваться централизованно с помо-

щью такой системы, как DHCP.

Эти три задачи имеют критическое значение для экономного управления. Грамотное их выполнение позволит всем последующим процессам проходить более гладко.

***Глава 4***

***Серверы***

В отличие от рабочих станций, предназначенных для одного пользователя, от сервера зависит множество пользователей. Следовательно, главным приоритетом для них становится надежность и бесперебойная работа.

К серверу могут подключаться сотни, тысячи или даже миллионы пользовате-

лей. Все усилия по повышению производительности или надежности наталки-

ваются на барьер огромного количества пользователей. Cерверы рассчитывают-

ся на более продолжительное времени работы, чем рабочие станции, что также

подразумевает дополнительные расходы. Покупка сервера с избыточной мощ-

ностью становится вложением в продление его срока жизни.

***4.1. Основы***

Оборудование, продаваемое как сервер, качественно отличается от оборудова-

ния, приобретаемого для индивидуальной рабочей станции:  
1) При установке и поддержке серверов используются особые процедуры.

2) Серверы поставляются с контрактом на обслуживание,

системами резервного копирования, операционной системой и возможностью

удаленного доступа.

1. Серверы размещают в вычислительных центрах

с контролируемым микроклиматом и с ограниченным доступом к серверному

оборудованию.

**4.1.1. Покупайте для серверов серверное оборудование**

Попытка сэкономить, покупая для сервера настольное оборудование, может сработать только на короткий срок. Серверное оборудование обычно стоит дороже, но дополнительные возможности оправдывают вложения. Вот некоторые из этих возможностей:

1. **Расширяемость**. Как правило, в серверах больше физического пространства для жестких дисков и больше слотов для карт расширения и централь-

ных процессоров либо они оснащены разъемами с высокой пропускной спо-

собностью для подключения специализированных периферийных уст-

ройств.

1. **Большая производительность центральных процессоров**. Серверы часто

оборудованы несколькими ЦП, а также обладают дополнительными воз-

можностями оборудования, такими как упреждающая выборка данных,

многоступенчатая проверка процессоров и динамическое распределение ре-

сурсов между ЦП. Процессоры различаются частотами, на которых работа-

ют, и зачастую имеет смысл приобретать более скоростные ЦП, которые дольше не будут устаревать.

1. **Высокопроизводительные системы обмена информацией (ввода-вывода).**

Серверы, как правило, более производительны в плане обмена информаци-

ей (ввода-вывода), чем клиенты. Возможности ввода-вывода часто пропор-

циональны количеству пользователей, что оправдывает применение скоро-

стных подсистем ввода-вывода.

1. **Возможности модернизации**. Серверы чаще модернизируют, а не просто за-

меняют, они предназначены для растущих потребностей.

1. **Возможность монтирования в стойку**. Серверы должны иметь возмож-

ность установки в стойки. Если настольный

компьютер может размещаться в пластмассовом корпусе обтекаемой фор-

мы, сервер должен иметь прямоугольную форму для эффективного исполь-

зования пространства в стойке. Все крышки, которые требуется снимать

при ремонте, должны сниматься без необходимости извлечения сервера из

стойки. Еще важнее то, что сервер должен быть сконструирован с учетом

охлаждения и вентиляции при монтировании в стойку. Система, у которой

вентиляционные отверстия расположены только с одной стороны, не смо-

жет поддерживать свою температуру в стойке так же хорошо, как система

со сквозной вентиляцией от передней панели к задней.

1. **Не требуется доступ с боковых сторон.** Компьютер должно быть проще

ремонтировать и обслуживать, если он установлен в стойку. Выполнение

этих задач не должно требовать доступа к боковым стенкам машины. Все

кабели должны быть сзади, а все отсеки приводов и дисков – спереди.

Выключатели питания должны быть доступны, но не слишком, чтобы избежать случайного нажатия.

1. **Дополнения для повышенной надежности**. Многие серверы обладают до-

полнительными возможностями, повышающими надежность, такими как

дублированные источники питания, RAID, несколько сетевых карт и ком-

поненты с поддержкой «горячей» замены.

1. **Контракт на обслуживание**. Поставщики предоставляют контракты на об-

служивание оборудования, где, как правило, оговариваются и гарантий-

ные сроки замены запасных частей.

1. **Альтернативные варианты управления**. В идеале серверы должны иметь

поддержку функций удаленного управления, таких как доступ через после-

довательный порт, который может быть использован для диагностики и ре-

шения проблем, чтобы восстановить сбойную машину.

**4.1.2. Выбирайте поставщиков, известных надежностью продукции**

Очень важно выбирать поставщиков, продукция которых известна своей на-

дежностью. Некоторые поставщики экономят за счет использования компонен-

тов потребительского класса, другие используют компоненты, которые соот-

ветствуют требованиям военного стандарта MIL-SPEC1. Некоторые поставщики

имеют многолетний опыт разработки серверов. Более опытные поставщики

обеспечивают функции, перечисленные выше, а также другие дополнительные

возможности, востребованность которых можно выяснить, только имея много-

летний опыт на рынке. Неопытные или малоопытные поставщики не могут

обеспечить какого-либо технического обслуживания, помимо замены вышедших

из строя узлов.

Оборудование может быть **однотипным или разнотипным**. Однотипное оборудование проще обслуживать, но при разнотипном оборудовании вы не зависите от одного

поставщика, а конкуренция между поставщиками обернется для вас лучшим

обслуживанием.

**4.1.3. Реальные расходы на серверное оборудование**

Чтобы иметь представление о дополнительных расходах на серверы, вы должны

знать, из чего складывается цена компьютера.

У большинства поставщиков есть три серии продукции: д**ля дома, для бизнеса**

**и серверное оборудование.**

1. **Домашняя серия** обычно продается по наименьшей

начальной цене. Дополнения и возможность расширения в бу-

дущем доступны по более высокой цене. При описании компонентов использу-

ются общие технические характеристики.

1. Настольные компьютеры **для бизнеса** обычно разрабатываются с учетом общих

затрат в течение всего срока их службы. Начальная закупочная цена выше, чем

для домашних компьютеров, но серия для бизнеса должна дольше не устаревать.

Оборудование бизнес-класса часто арендуется, а не приобретается, и для таких сетей эти гарантии имеют большую ценность.

1. **Серверные серии** ориентированы на наилучшее соотношение себестои-

мости и производительности. Многие возможности серверов увеличивают закупочную цену машины, но при этом повышают предполагаемое время бесперебойной работы, что делает соотношение цены и производительности более привлекательным.

Серверы стоят дороже и по другим причинам. Корпус, который удобнее для

обслуживания, может быть дороже в производстве. Существуют ограничения

на расположение отсеков для дисководов и других панелей, доступ к которым

должен быть только с определенной стороны. Тем не менее более высокая

начальная закупочная цена оправдана экономией средств в долгосрочной пер-

спективе за счет сокращения времени на ремонт и упрощения обслужи-

вания.

Покупка сервера «с запасом» может отсрочить сложную модернизацию для увеличения производительности в будущем.

**4.1.4. Контракты на обслуживание и запасные компоненты**

Поставщики все чаще предлагают самые разные дополнительные контракты на обслуживание. Вот несколько разумных сценариев, которые помогут вам при выборе подходящего контракта на обслуживание:

1. **Не критически важный сервер**. Некоторые серверы не имеют критической

важности, например один процессор из многопроцессорного сервера. В этой

ситуации контракт со сроком обслуживания заявки на следующий день

или в течение двух дней будет приемлемым вариантом. Или контракт на об-

служивание может вообще не потребоваться, если стандартного гарантий-

ного обслуживания будет достаточно.

1. **Большая группа идентичных серверов**. Иногда в сетях используется боль-

шое количество машин одного типа, возможно, предназначенных для раз-

личных служб. Стоимость комплекта запасных частей разделяется на большое

количество узлов. Для этих узлов может потребоваться только недорогой

контракт на обслуживание, предусматривающий лишь замену компонен-

тов из комплекта запасных частей.

1. **Постепенная модернизация**. В этом случае вы можете стандартизировать срок обеспечения запасными компонентами отдельной модели или группы моделей, которые используют одинаковый комплект. По окончании этого периода вы можете утвердить новую модель и приобрести соответствующий комплект запасных компонентов.
2. **Важные узлы**. Иногда слишком дорого содержать полностью укомплекто-

ванный набор запасных частей. Может быть разумным хранить запас толь-

ко тех компонентов, которые чаще всего выходят из строя, а на остальные

приобрести контракт на обслуживание в тот же день.

1. **Большое количество моделей от одного поставщика**. Особо крупные ком-

пании могут заключить контракт на обслуживание, в условия которого

входит выделение техника для работы в сети компании-заказчика. Такая

возможность оправданна, только когда в сети огромное количество серве-

ров или если в доходах этой компании важную роль играют серверы опреде-

ленного поставщика.

1. **Критически важный узел.** Некоторые поставщики предлагают контракты

на обслуживание, предусматривающие выделение техника для работы в се-

ти компании-заказчика и дублирующей машины, готовой к замене сбойно-

го устройства. Это зачастую так же дорого, как и оплата резервного сервера,

но может иметь смысл для некоторых компаний, для которых высокие тех-

нологии – не основная специализация.

Нужно искать компромисс между хранением запасных частей и сервисным

контрактом. Комплектование собственного склада запасных компонентов может

быть слишком дорогостоящим для небольшой сети. Контракт на обслуживание

включает диагностические услуги, хотя бы по телефону. Иногда, с другой сто-

роны, самый простой способ диагностики – менять запасные части до тех пор,

пока проблема не исчезнет.

Хорошей политикой будет оформлять на 10% больше сервисных позиций, чем

предусматривает цена контракта, с тем чтобы поставщик мог поднимать еже-

месячные платежи по мере добавления новых машин в контракт.

Также полезно пересматривать контракт по крайней мере ежегодно или даже

ежеквартально, чтобы добавить новые серверы и исключить списанные.

Контракты на обслуживание, скорее, борются с последствиями, а не предотвра-

щают проблемы. Контракты на обслуживание предусматривают поставку

запасных компонентов и своевременный ремонт. Как правило, существует вы-

бор из нескольких типов контрактов. По условиям дешевых контрактов достав-

ка запасных компонентов ложится на плечи заказчика, а более дорогие предусматривают доставку запчастей и их установку.

Налаженный обмен новых компонентов на старые – важная часть оперативно-

го ремонта, и в идеале она должна быть предусмотрена в контракте на обслужи-

вание.

Еще больше сократить время на ремонт можно, приобретя комплект запасных

компонентов, снимающий зависимость от поставщика при срочном ремонте

сервера. В комплект должно входить по одному экземпляру каждого компонен-

та системы. Как правило, этот комплект обойдется дешевле, чем покупка дуб-

лирующей системы, так как, например, если в системе используется четыре

центральных процессора, в запасном комплекте достаточно одного. Также

комплект менее дорог за счет того, что ему не требуются лицензии на програм-

мное обеспечение. Но даже если у вас есть ремонтный комплект, вам следует

заключить контракт на обслуживание, по которому вы сможете дополучить

любые компоненты, использованные для ремонта неисправной машины. При-

обретайте по одному комплекту запасных компонентов для каждой модели,

требующей срочного ремонта.

Большое количество комплектов запасных частей может обойтись чрезвычайно

дорого, особенно если для них требуются дополнительные расходы на контракт

на обслуживание. Поставщик может предоставить дополнительные возможности, такие как контракт на обслуживание, гарантирующий доставку запасных

компонентов в течение нескольких часов, что может снизить общую сумму

ваших затрат.

**4.1.5. Обеспечение целостности данных**

На серверах хранятся критически важные данные и уникальные конфигурации,

которые должны быть защищены.

Как правило, достаточно простой системы, каждый вечер делающей резервные копии этих нескольких файлов.

**4.1.6. Размещение серверов в вычислительном центре**

Серверы должны устанавливаться в условиях с надежными энергоснабжением,

противопожарной защитой, сетью, охлаждением и физической безопасностью.

Лучше всего зарезервировать физическое место для размещения сервера при его приобретении.

После сборки оборудование лучше устанавливать в стойку непосредственно

перед установкой ОС и другого программного обеспечения.

Как минимум должна быть выделена комната или шкаф, обеспечивающие как минимум физическую безопасность, источник бесперебойного питания (несколько мелких или один большой) и достаточное охлаждение.

**4.1.7. Конфигурация клиент-серверной ОС**

Серверы необязательно должны работать под управлением тех же ОС, что и их

клиенты. Серверы могут быть совершенно другими, в точности такими же, или

с той же базовой ОС, но с другой конфигурацией для иного предназначения. Для

разных случаев подходят различные варианты.

Иногда на серверах требуется устанавливать все те же программы, что и на

клиентах. Рассмотрим случай UNIX-сети с множеством настольных компьюте-

ров под управлением UNIX и несколькими многопроцессорными UNIX-серве-

рами общего назначения. На клиентах должна устанавливаться одинаковая

клонированная ОС. На многопроцессорные серверы следует установить ту же ОС, хотя она может быть иначе настроена для большего количества процессов, псевдотерминалов, буферов и других параметров.

**4.1.8. Обеспечьте удаленный доступ через консоль**

Для серверов необходима возможность удаленного обслуживания.

**Переключатель КВМ** – устройство, позволяющее нескольким машинам исполь-

зовать одну клавиатуру, видеоэкран и мышь (КВМ). Например, можно устано-

вить три сервера и три консоли в одну телекоммуникационную стойку. Однако

благодаря коммутатору КВМ для этой стойки достаточно только одной клави-

атуры, монитора и мыши. Таким образом, в ту же стойку можно установить

большее количество серверов. Можно сэкономить еще больше места, если уста-

новить один коммутатор КВМ на ряд стоек или на весь вычислительный центр.

Однако более крупные коммутаторы КВМ, как правило, чрезмерно дорогие.

Можно освободить еще больше пространства с помощью IP-КВМ, то есть КВМ,

в которых нет ни клавиатуры, ни монитора, ни мыши. Достаточно просто под-

ключиться к консольному серверу КВМ по сети с программного клиента на

другой машине. Это можно сделать даже с ноутбука в кафе, если ноутбук под-

ключен через VPN к вашей сети!

**Последовательные консоли и переключатели КВМ** позволяют вам управлять системной консолью, если сеть не работает или если система в неисправном состоянии. Например, определенные операции можно выполнять только при перезагрузке системы. Среди них нажатие определенных клавиш для выхода в меню BIOS.

Некоторые поставщики предоставляют карты расширения, которые позволяют

удаленно управлять машиной. Эта возможность зачастую является основным

отличием между серверами и простыми машинами этих поставщиков. Продук-

ция сторонних компаний также может предоставлять эту возможность.

Сетевые устройства, такие как маршрутизаторы и коммутаторы, оснащены

только последовательными консолями. Таким образом, может быть полезно

помимо системы КВМ иметь доступ и к последовательной консоли.

При приобретении серверного оборудования следует обратить особое вни-

мание на то, какой тип удаленного доступа к консоли будет доступен и для ре-

шения каких задач может потребоваться такой доступ. В аварийной ситуации

нет смысла и времени ждать, пока системные администраторы доберутся до

физических устройств, чтобы все исправить. В штатных ситуациях у системных

администраторов должна быть возможность исправить небольшие неполадки

из дома, в дороге и, оптимально, возможность выполнить любую задачу через

удаленное подключение.

У удаленного доступа есть ограничения из-за того, что отде-

льные задачи (включение и выключение питания, загрузка сменных носителей,

замена неисправного оборудования) требуют присутствия человека возле ма-

шины. Дежурный оператор или доброволец, готовый помочь, может стать

глазами и руками удаленного специалиста.

При использовании удаленной консоли придется продумать вопросы безопас-

ности. Часто стратегии безопасности узла базируются на размещении консоли

за запертыми дверями. Удаленный доступ разрушает эти стратегии. Следова-

тельно, для консольных систем требуются продуманные системы аутентифика-

ции и конфиденциальности.

**4.1.9. Зеркалирование загрузочных дисков**

**Загрузочный диск**, или диск с операционной системой, как правило, труднее

всего заменить в случае его повреждения. Поэтому необходимо соблюдать особые

меры безопасности, чтобы ускорить процесс восстановления. Для загрузочного

диска каждого сервера необходимо создать зеркальный диск. Это означает, что

установлено два диска и при любом обновлении основного диска тут же обнов-

ляется и второй. Если один из дисков откажет, система автоматически пере-

ключится на работоспособный диск.

Без зеркального копирования сбой жесткого диска означает простой в работе.

Благодаря зеркальному копированию сбой жесткого диска является событием,

которое можно не только спокойно пережить, но и контролировать. Если неис-

правный диск можно заменить во время работы системы, сбой в работе одного

компонента не приведет к простою. Если неисправные диски можно заменять

только при отключенной системе, перерыв в работе можно запланировать

в соответствии с потребностями компании.

***4.2. Тонкости***

**4.2.1. Повышение надежности и удобства обслуживания**

**4.2.1.1. Одноцелевые серверы**

Одноцелевое устройство – устройство, созданное для выполнения одной конкретной задачи (файловые серверы, веб-серверы, серверы электронной почты, DNS-сервера и т. д.) Первым таким устройством стал выделенныйсетевой маршрутизатор**.**

**Одноцелевой сервер** представляет собой устройство, в котором воплотился мно-

голетний опыт. Конструирование сервера – сложный процесс. Системное проектирование и настройка производительности требуют высокой квалификации и большого опыта в соответствующих областях. Программное обеспечение, необходимое для работы той или иной службы, часто подразумевает компоновку различных программных пакетов, их связывание и создание единой общей системы администрирования для них.

Приобретение одноцелевого устройства позволит сэкономить время, которое

системный администратор может потратить на выполнение других задач. Каж-

дое приобретенное одноцелевое устройство уменьшает количество систем, ко-

торые необходимо устанавливать с нуля, а также дает преимущество поддержки

от поставщика в случае неполадок. Кроме того, одноцелевые устройства позво-

ляют организациям получить качественно настроенные системы без необходи-

мости нанимать опытных специалистов.

**4.2.1.2. Резервные блоки питания**

По предрасположенности к сбоям на втором месте после жестких дисков находятся блоки питания. Поэтому в идеале серверы должны быть обеспечены резервными блоками питания.

Наличие резервных блоков питания не означает, что просто подключено два

таких устройства. Это означает, что система сохраняет работоспособность, если

один из блоков питания не функционирует: избыточность n + 1.

У каждого блока питания должен быть отдельный кабель питания. На практи-

ке самая распространенная причина проблем с питанием – случайно выдернутый

из розетки кабель.

Еще одна причина для применения отдельных кабелей питания – возможность

использовать следующий прием. В некоторых случаях устройство необходимо

подключить к другому удлинителю, UPS или другой электрической сети.

В такой ситуации можно по очереди переключить отдельные кабели питания,

избежав простоя в работе системы.

**4.2.1.3. Полная избыточность, или n + 1**

Как уже упоминалось выше, избыточность n + 1 относится к системам, которые

спроектированы таким образом, что система продолжает функционировать

даже после сбоя одного из компонентов.

Напротив, при полной избыточности два полных набора оборудования объеди-

нены в отказоустойчивую конфигурацию. Первая система обеспечивает испол-

нение службы, а вторая бездействует в полной готовности взять на себя работу

при сбое первой системы. Переключение на резервные мощности может осу-

ществляться вручную (кто-то замечает сбой в первой системе и активирует

вторую) или автоматически (вторая система отслеживает работу первой системы

и сама активируется при ее отказе).

Другие системы с полной избыточностью используют распределение нагрузки.

Обе системы полноценно функционируют и распределяют между собой рабочую

нагрузку. Каждый сервер обладает достаточной мощностью, чтобы взять на

себя всю нагрузку. Если в работе одной из систем возникает сбой, вторая систе-

ма берет всю нагрузку на себя. Системы можно настроить таким образом, чтобы

они отслеживали надежность работы друг друга. Либо можно использовать

внешний источник управления потоками и распределением запросов на обслу-

живание.

Если n равно или больше 2, n + 1 выгоднее, чем полная избыточность. Пользо-

ватели обычно предпочитают этот метод из-за его экономичности.

Как правило, избыточность n + 1 используется только для серверных подсистем,

а не для всех видов компонентов.

**4.2.1.4. Компоненты, поддерживающие «горячую» замену**

Резервные компоненты должны поддерживать «горячую» замену. «Горячая»

замена подразумевает возможность отключить и заменить компонент во время

работы системы. Как правило, компоненты следует заменять только при отклю-

ченной системе.

Преимущества «горячей» замены:

– возможность устанавливать компоненты во время работы системы.   
– благодаря «горячей» замене системный администратор может сменить

компонент, не отключая систему. В RAID-системах предусматривают диск

с «горячей» заменой, который находится системе, но не используется, пока не

возникнет необходимость заменить вышедший из строя диск. Если система

сможет изолировать неисправный диск, чтобы он не остановил работу всей

системы, то она будет способна автоматически активировать диск с «горячей

заменой», сделав его частью соответствующего RAID-массива. Таким образом,

мы получаем систему n + 2.

Если для системы предусмотрены запланированные еженедельные перерывы в работе и работа системы при риске двойного сбоя в течение недели считается приемлемой, не стоит тратить дополнительные средства на компоненты с возможностью «горячей» замены. Если же технический перерыв для системы планируется проводить всего

раз в год, такие затраты будут оправданы.

Если поставщик заявляет о возможности «горячей» замены компонентов, всег-

да задавайте два вопроса: «Какие компоненты не имеют возможности «горячей»

замены? Каким образом и на какой период прерывается работа при «горячей»

замене компонентов?» Некоторые сетевые устройства оснащены интерфейсны-

ми картами, которые поддерживают «горячую» замену, но сам процессор такую

возможность не поддерживает. Некоторые сетевые устройства, для которых

заявлена возможность «горячей» замены, полностью перезапускают всю систе-

му после установки нового устройства.

Возможность «горячей» замены компонентов навсегда устранит простои в работе. Она просто уменьшает их продолжительность.

**4.2.1.5. Раздельные сети для административных функций**

Дополнительные сетевые интерфейсы на серверах позволяют создать раздельные

административные сети. Например, часто создают отдельную сеть для резерв-

ного копирования и мониторинга. Резервное копирование требует высокой

пропускной способности, и отделение этого трафика от основной сети означает,

что резервное копирование не будет мешать пользователям работать с сетью.

Подобную отдельную сеть можно спроектировать с помощью довольно простого

оборудования, таким образом сделав ее более надежной. Но что самое важное,

на эту сеть не будут влиять простои в работе основной сети. Кроме того, она

дает системным администраторам возможность получить доступ к машине во

время такого простоя. Эта форма избыточности решает очень специфическую

проблему.

**4.2.2. Альтернатива: множество недорогих серверов**

Запуск крупной веб-фермы потребует использования нескольких резервных

серверов. Все эти серверы должны быть сконфигурированы абсолютно одина-

ково – путем автоматической установки. Если каждый веб-сервер способен

обрабатывать 500 запросов в секунду, вам понадобится десять серверов, чтобы

обрабатывать 5000 запросов в секунду, будут поступать от пользователей Интернета. Механизм распределения нагрузки может распределять нагрузку среди серверов. Но что самое лучшее, системы распределения нагрузки могут автоматически определять машины, в работе которых произошел сбой. Если один сервер «падает», механизм распределения нагрузки распределяет запросы между оставшимися рабочими серверами и пользователи продолжают получать доступ к сервису. При этом загрузка

каждого сервера повышается на одну десятую, но это лучше простоя в работе.

Традиционное мышление подсказывает, что никогда не стоит запускать ком-

мерческую службу на сервере, созданном из серийных компонентов, который

может обрабатывать всего 20 запросов в секунду. Однако, если вы можете управлять большим количеством таких серверов, ситуация меняется. Пришлось бы приобрести 250 слабых серверов, чтобы добиться производительности 10 традиционных серверов.

В результате на оборудование уйдет та же сумма.

Но по мере повышения количества запросов в секунду такое решение стало менее

дорогостоящим по сравнению с покупкой крупных серверов. Если они обеспе-

чивали производительность 100 запросов в секунду, можно было для получения

той же мощности приобрести 50 серверов по одной пятой от стоимости или потратить те же деньги и получить мощность в пять раз выше.

Отказавшись от компонентов, которые не используются в такой среде, например

видеокарт, USB-разьемов и т. д., можно еще больше снизить затраты. Вскоре

появилась возможность приобрести от пяти до десяти серверов из серийных

компонентов взамен одного традиционного сервера и при этом получить большую

процессорную мощность. Оптимизация требований к физическому оборудованию привела к созданию более эффективных конфигураций, и в результате мощные серверы можно вместить в корпус высотой не более одного юнита.

Еще один способ разместить большое количество машин на ограниченном про-

странстве – использовать технологию **блейд-серверов**. Один корпус содержит

множество ячеек, в каждую из которых можно подключить плату (блейд)

с процессором и памятью. Корпус обеспечивает питание, доступ к сети и системе управления. Так как все устройства схожи друг с другом, можно создать автоматизированную систему, которая позволяет заменить неисправное устройство свободным.

***4.3. Заключение***

Приобретая серверы, мы принимаем различные решения, так как от серверов

зависит деятельность множества пользователей, в то время как клиентская

рабочая станция предназначена только для одного пользователя. В отличие от

рынка настольных компьютеров, на рынке серверного оборудования важнейшее

значение имеют иные экономические факторы. Знание этих факторов помогает

принимать более грамотные решения при покупке. Серверы, как и любое другое

оборудование, иногда дают сбои, поэтому необходимо заключить контракт на

обслуживание или составить план восстановления, а также предусмотреть воз-

можность резервного копирования и восстановления данных. Серверы должны

располагаться в специальных машинных залах, обеспечивающих условия для

надежной работы. Пространство в машинном зале необходимо распределить

до момента покупки, а не когда прибудет сервер. Кроме того, заранее необходи-

мо спланировать электросеть, пропускную способность сети и систему охлаж-

дения.

Одноцелевые серверы – аппаратные или программные системы, которые содер-

жат все необходимое для выполнения определенной задачи: заранее сконфигу-

рированное программное обеспечение, которое установлено на оборудовании,

специально настроенном для конкретного приложения. Одноцелевые серверы

представляют собой высококачественные решения, разработанные с учетом

многолетнего опыта. Они, как правило, являются более надежными и простыми

в управлении, чем менее профессиональные решения. Однако такие системы

достаточно сложно настраивать для нетипичных требований корпоративной

сети.

Серверам необходима возможность удаленного администрирования. Аппарат-

ные или программные системы позволяют удаленно выполнять консольный

доступ. Это позволяет освободить дополнительное пространство в машинном

зале, а также дает возможность системным администраторам осуществлять

работу из своего кабинета или дома. Системные администраторы могут прово-

дить требуемое обслуживание без необходимости находиться непосредственно

рядом с сервером.

Для повышения надежности серверы часто оснащаются дополнительными

системами, предпочтительно в конфигурации n + 1. Наличие зеркалированно-

го системного диска, резервных источников питания и других дополнительных

компонентов повышает период работоспособного состояния системы. Возмож-

ность заменять неисправные компоненты во время работы системы уменьшает

среднее время восстановления и перерывы в обслуживании. Хотя в прошлом

подобная избыточность была роскошью, в современных условиях она зачастую

является необходимостью.

***Глава 5***

***Сервисы***

**Сервер** – это оборудование. **Сервис** – это функция, предоставляемая сервером.

Сервис может быть скомпонован на нескольких серверах, которые работают

совместно друг с другом.

Предоставление сервиса подразумевает не только совмещение оборудования

и программного обеспечения, но и обеспечение надежности сервиса, его масштабирование, а также мониторинг, обслуживание и поддержку. Сервис действительно становится сервисом только тогда, когда он отвечает этим основным

требованиям.

Одной из основных обязанностей системного администратора является предо-

ставление пользователям необходимых им сервисов. И это должно осущест-

вляться постоянно.

Любая типичная сеть обладает большим набором сервисов. Основные сервисы

включают в себя DNS, электронную почту, сервисы аутентификации, подклю-

чения к сети и печати. Эти сервисы являются самыми важными и в случае

сбоев самыми заметными. Другими типичными сервисами являются различные

методы удаленного доступа, сервис сетевого лицензирования, хранилища про-

грамм, сервис резервного копирования, доступ к Интернету, DHCP и файл-сер-

висы.

***5.1. Основы***

Создание исправного и надежного сервиса – ключевая задача системного адми-

нистратора, которому при ее выполнении необходимо учитывать множество

основных факторов. Самым важным таким фактором на всех этапах создания

и развертывания являются потребности пользователей. Поговорите с пользова-

телями и выясните, в чем они нуждаются и чего ожидают от данного конкрет-

ного сервиса. Затем составьте список других требований, таких как админис-

тративные требования, о которых знают только системные администраторы.

Сервисы необходимо создавать на машинах серверного класса, которые содер-

жатся в соответствующих условиях и отличаются разумным уровнем надеж-

ности и быстродействия. За сервисом и машинами, от которых он зависит, не-

обходимо установить мониторинг. При сбоях в работе должны генерироваться

предупреждения или уведомления о неисправностях.

Большинство сервисов зависят от других сервисов. Понимание того, каким

образом работает сервис, позволит вам точно определить, от каких сервисов он

зависит. Например, почти все сервисы зависят от DNS. Некоторые сервисы

зависят от электронной почты, которая, в свою очередь, зависит от DNS и сети.

Другие сервисы зависят от доступа к общим файлам на других компьютерах.

Отказ в работе некоторых сервисов, таких как DNS, вызывает каскадные сбои всех других зависящих от них сервисов. При создании сервиса очень важно понимать, от

каких сервисов он будет зависеть.

Машины и программы, которые являются частью сервиса, должны зависеть от

узлов и программ, созданных в соответствии с теми же или более высокими

стандартами. Надежность сервиса соответствует надежности самого слабого

звена в цепи сервисов, от которых он зависит. Сервис не должен неоправданно

зависеть от узлов сети, которые не являются частью этого сервиса.

Точно так же безопасность системы определяется уровнем безопасности ее са-

мого слабого звена.

Сервер должен быть максимально простым. Простота повышает надежность

машин и упрощает исправление в случае возникновения проблем. Серверы

должны отвечать минимальным требованиям к работе сервиса, и только сис-

темные администраторы должны иметь к ним доступ. Кроме того, системные

администраторы должны получать к ним доступ только с целью обслуживания.

Системный администратор должен принять несколько решений при создании

сервиса: оборудование какого поставщика необходимо приобрести, использовать

ли один или несколько серверов для сложного сервиса, а также какой уровень

избыточности необходимо предусмотреть в сервисе. Сервис должен быть мак-

симально простым с минимальным количеством зависимостей – это позволит

повысить его надежность и упростить поддержку и обслуживание. Еще один

способ упростить поддержку и обслуживание сервиса – использовать стандартные оборудование, программное обеспечение и конфигурации, а также хранить

документацию в стандартных местах.

**5.1.1. Требования пользователей**

Процесс создания нового сервиса всегда необходимо начинать с учета требований

пользователей. Если сервис не будет

соответствовать их нуждам, на его создание будут лишь зря потрачены силы.

Для некоторых сервисов требований пользователей нет. DNS – один из таких

сервисов. Другие сервисы, такие как электронная почта и сеть, более весомы

для пользователей. Пользователям могут понадобиться определенные возмож-

ности их почтовых клиентов, и разные пользователи в различной степени за-

гружают сеть в зависимости от выполняемой ими работы и настройки исполь-

зуемых систем. Другие сервисы в первую очередь ориентированы на пользова-

телей.

Обеспечьте участие сотрудников в тестировании удобства использования демонстрационной версии сервиса. Если вы выберете

систему, которая покажется людям слишком сложной в использовании, ваш

проект окажется неудачным. Постарайтесь оценить, как много сотрудников

будут пользоваться этим сервисом и какого уровня быстродействия они от него

ожидают. Это поможет вам создать надежный и работоспособный сервис.

Кроме того, необходимо разработать соглашение об уровне обслуживания

для нового сервиса. В этом соглашении перечислены предоставляемые сервисы

и уровень их поддержки. Как правило, в нем описаны проблемы, разбитые по

категориям приоритетов. Для каждой категории указывается время ответных

действий, возможно, по времени суток или дням недели, если в сети не предо-

ставляется круглосуточная поддержка без выходных. Это соглашение всегда обсуждается и утверждается обеими сторонами.

Процесс составления соглашения об уровне обслуживания – возможность для

системных администраторов понять ожидания пользователей и соответственно

их направлять, чтобы пользователи понимали, что выполнить возможно, а что

нет и почему. Это же соглашение должно содержать описание будущих потреб-

ностей и возможностей, чтобы все стороны понимали план развития.

**5.1.2. Эксплутационные требования**

Системным администраторам необходимо продумать административный интерфейс нового сервиса: будет ли он взаимодействовать с существующими сервисами и можно ли его интегрировать в центральные сервисы, такие как сервис аутентификации или каталогов. Кроме того, системным администраторам необходимо учитывать масштабирование сервиса. Потребность в сервисе со временем может превысить изначально планируемый уровень и практически наверняка вырастет по мере роста самой компании. Сюда же относится и вопрос обновления сервиса.

Начиная с уровня надежности, ожидаемого пользователями и прогнозируемого

системными администраторами как требования к будущей надежности системы,

системные администраторы должны быть готовы составить перечень желательных функций, таких как кластеризация, вторичные или избыточные серверы

либо запуск на оборудовании или ОС с высокой отказоустойчивостью. Системным администраторам также потребуется продумать вопросы производи-

тельности сети в отношении сетевой инфраструктуры в месте работы сервиса

и в месте расположения пользователей.

**Пропускная способность или время ожидания**

Термин «**пропускная способность**» означает количество данных, которое

может быть передано в секунду. Время ожидания – это количество вре-

мени до момента, когда другая сторона примет данные. Подключение

с большим временем ожидания, независимо от пропускной способности,

отличается долгим временем передачи и подтверждения. Некоторые приложения, например неинтерактивное (потоковое) видео, нечувствительны ко времени ожида-

ния. Другие же сильно от него зависят.

Каждый системный администратор и разработчик должен понимать, как время

ожидания влияет на создаваемые сервисы. Системным администраторам также

стоит выяснить, как они смогут вести мониторинг сервиса по показателям ра-

ботоспособности и быстродействия. Возможность интеграции нового сервиса

с существующими системами мониторинга – ключевое требование для выпол-

нения соглашения об уровне обслуживания. Кроме того, системным админис-

траторам и разработчикам следует выяснить, может ли система генерировать

уведомления о неисправностях при обнаружении проблем в существующей

системе регистрации неисправностей, если это потребуется.

**5.1.3. Открытая архитектура**

Всегда, когда это возможно, новые сервисы следует строить, опираясь на архи-

тектуру, которая использует открытые протоколы и форматы файлов. В част-

ности, мы говорим о протоколах и форматах файлов, описание которых публич-

но обсуждается, так что многие поставщики могут участвовать в написании

этих стандартов и создавать интероперабельные продукты. Любой сервис с от-

крытой архитектурой проще интегрировать с другими сервисами, которые

следуют тем же стандартам.

Напротив, закрытые сервисы используют проприетарные протоколы и форма-

ты файлов, которые способны взаимодействовать только с ограниченным

кругом решений, так как протоколы и форматы файлов могут изменяться без

уведомления и требовать лицензирования у создателей протокола. Поставщи-

ки используют проприетарные протоколы, когда осваивают новую территорию

или пытаются удержать свою долю рынка, препятствуя росту уровня конку-

ренции.

Также остерегайтесь поставщиков, которые дополняют и расширяют стандарт,

пытаясь препятствовать интероперабельности с конкурентами. Такие постав-

щики делают это, чтобы они могли заявить о поддержке стандарта, при этом не

предоставляя своим пользователям преимуществ интероперабельности. Они не

ориентированы на нужды пользователей.

С точки зрения бизнеса смысл использования открытых протоколов прост: это

позволяет вам создать более качественные сервисы, потому что вы можете вы-

брать лучший сервер и лучший клиент, а не быть вынужденным, например,

выбрать лучший клиент, а потом оказаться привязанным к менее оптимально-

му серверу.

Лучшим способом будет выбор протоколов, основанных на открытых стандартах

и позволяющих каждой стороне выбрать свое собственное программное обеспе-

чение. Такой подход позволяет отделить процесс выбора клиентского приложе-

ния от процесса выбора серверной платформы. Пользователи могут свободно

выбрать программное обеспечение, наилучшим образом соответствующее их

нуждам, склонностям и даже платформе. Системные администраторы могут

независимо выбрать серверное решение, основываясь на своих потребностях по

параметрам надежности, масштабируемости и управляемости.

Это называется разъединением выбора клиента и сервера.

Открытые протоколы и форматы файлов обычно статичны либо изменяются

только с сохранением обратной совместимости и обладают широкой поддержкой,

дающей максимальный выбор конечных продуктов и максимальные шансы

получить надежный, интероперабельный продукт. Еще одно преимущество

открытых систем в том, что вам не потребуются шлюзы для связи с остальным

миром. Шлюзы – это «клей», соединяющий различные системы. Хотя шлюз

может стать выходом из положения, системы, основанные на общепри-

нятых открытых протоколах, вообще не нуждаются в каких-либо шлюзах.

Шлюзы – это дополнительные сервисы, которые требуют планирования мощ-

ностей, проектирования, мониторинга и всего остального, описанного в данной

главе. Лучше уменьшить количество сервисов.

**5.1.4. Простота**

При разработке нового сервиса прежде всего следует обращать внимание на

простоту. Самое простое решение, удовлетворяющее всем требованиям, будет

самым надежным, удобным в обслуживании, легко расширяемым и легко ин-

тегрируемым с другими системами. Чрезмерная сложность приводит к путани-

це, ошибкам и потенциальной трудности в использовании, а также может все

замедлить. Сложные системы требуют больших расходов на их создание и об-

служивание.

По мере своего роста система становится более сложной. Следовательно, если создавать ее как можно более простой, это позволит отсрочить день,

когда система станет слишком сложной.

Иногда одно-два требования пользователей или системных администраторов

могут значительно увеличить сложность системы. Если на стадии разработки

архитектуры вы столкнетесь с такими требованиями, лучше вернуться назад

и провести повторную оценку важности требования. Объясните пользователям

или системным администраторам, что эти требования можно удовлетворить, но

только за счет снижения надежности, уровня поддержки и своевременности

обслуживания. Затем попросите их заново оценить свои требования с этой точ-

ки зрения и решить, какие из них следует удовлетворить, а какими можно

пренебречь.

**5.1.5. Отношения с поставщиком**

При выборе аппаратного и программного обеспечения для сервиса у вас должна

быть возможность побеседовать с техническими консультантами поставщиков,

чтобы посоветоваться насчет выбора наилучшей конфигурации для вашего

приложения. У поставщиков оборудования иногда бывают готовые конфигура-

ции, оптимизированные для определенных приложений, таких как базы данных

или веб-серверы. Если вы создаете типичный сервис, у вашего поставщика

может найтись подходящая готовая конфигурация.

При выборе поставщика, особенно программных продуктов, важно понимать,

в каком направлении поставщик будет развивать продукт. В случае

ключевых, центральных сервисов, таких как сервис аутентификации или ка-

талогов, необходимо оставаться в русле направления развития продукта, иначе

вы можете внезапно обнаружить, что поставщик перестал поддерживать вашу

платформу. Ущерб от необходимости изменения центральной части инфраструк-

туры может быть очень велик. По возможности старайтесь налаживать посто-

янные отношения с поставщиками, которые в первую очередь разрабатывают

продукты для платформы, используемой вами, а не с теми, кто портирует свою

продукцию на эту платформу. Обычно в этом случае встречается меньше ошибок,

в первую очередь добавляются новые функции и обеспечивается лучшая поддержка в продуктах, разрабатываемых для основной платформы. Меньше вероятность, что поставщик прекратит поддержку этой платформы.

**5.1.6. Независимость от конкретной машины**

У пользователей всегда должен быть доступ к сервису с использованием стан-

дартного имени, основанного на назначении сервиса. Например, клиентские

приложения должны находить свои общие календари на сервере calendar, поч-

товые клиенты – на POP-сервере с именем pop, IMAP-сервере с именем imap и SMTP-сервере mail.

Основное имя машины не должно совпадать с названием функции. Например,

у календарного сервера может быть основное имя dopey, а обращаться к нему

будут как к calendar, но нельзя давать ему основное имя calendar, так как рано

или поздно может потребоваться перенести функцию на другую машину.

Для сервисов, в которых привязка осуществляется к IP-адресам, а не к именам,

обычно есть возможность выделить для машины, на которой запущен сервис,

несколько виртуальных IP-адресов в дополнение к основному, настоящему

IP‑адресу и использовать для каждого сервиса свой виртуальный адрес. Тогда

будет относительно просто перенести на другую машину виртуальный адрес

вместе с сервисом.

При создании сервиса на машине продумайте, как вы будете впоследствии пе-

реносить его на другую машину. В какой-то момент кому-то придется ее пере-

носить. По возможности максимально упростите работу этому человеку, спро-

ектировав все как следует с самого начала.

**5.1.7. Среда окружения**

Надежному сервису требуется надежная среда окружения. Сервис влияет на

эффективность работы ваших пользователей, напрямую либо косвенно, через

другие машины и сервисы, зависящие от этого. Пользователи ожидают, что

сервис будет доступен всегда, когда он им потребуется. Основная часть постро-

ения сервиса заключается в предоставлении обоснованно высокого уровня до-

ступности, что подразумевает размещение всего оборудования, относящегося

к сервису, в вычислительном центре, способном обеспечивать надежность.

Вычислительный центр обеспечивает надежное энергоснабжение, хорошее

охлаждение, контролируемую влажность (что особенно важно в сухом или

влажном климате), системы пожаротушения и безопасное место, где машины

не могут быть случайно повреждены или отключены.

Серверам часто требуется большая скорость подключения к сети, чем клиентам, так как им необходимо связываться на приемлемой скорости с большим числом клиентов одновременно. Сервер часто бывает подключен к нескольким сетям, в том

числе и административным, с целью снижения трафика в основной сети. Все серверы, составляющие основу вашей сервиса, должны находиться в вычислительном центре, чтобы использовать преимущества высокоскоростной сети.

Ни один из компонентов сервиса не должен зависеть от каких-либо программ,

выполняющихся на машинах, расположенных за пределами вычислительного

центра. Если вы обнаружите зависимость от компонентов,

работающих на машине за пределами вычислительного центра, найдите способ

изменить ситуацию: переместите машину в вычислительный центр, продубли-

руйте сервис на одной из машин в вычислительном центре или избавьтесь от

зависимости от менее надежного сервера.

В случае фундаментальных сервисов, таких как DNS-серверы, нужно особенно

стараться избегать зависимостей от других систем.

**5.1.8. Ограничение доступа**

Ограничение прямого доступа к серверам – одна из составляющих сервиса.

Доступ к машине, как консольный, так и с помощью других способов удален-

ного доступа, должен быть разрешен только для системных администраторов,

ответственных за работу сервиса. Это ограничение важно, так как взаимодействующие с машиной пользователи могут ей дать нагрузку выше допустимой.

Чем больше людей подключаются напрямую к машине, тем выше вероятность

сбоя. Даже операционные системы, известные своей ненадежностью, могут

месяцами стабильно работать, предоставляя сетевые сервисы, если с ними не

взаимодействуют пользователи.

Человек, привыкший пользоваться конкретным сервером для нересурсоемких

задач, таких как проверка почты, может случайно запустить другие программы,

которые сильно нагрузят центральный процессор, память и систему ввода-вы-

вода. Сам не понимая этого, человек может навредить сервису.

**5.1.9. Надежность**

Наряду с вопросами среды окружения и доступа есть еще несколько моментов

в отношении надежности, которые следует учитывать при планировании сер-

виса. Надежность серверов как компонентов сервиса – еще один аспект повышения

надежности сервиса в целом.

Если у вас есть избыточное оборудование, используйте его по возможности эф-

фективно. Например, если в системе два блока питания, подключите их к раз-

ным электрическим сетям и разным розеткам. Если у вас есть избыточные ма-

шины, по возможности используйте раздельное подключение к питанию

и к сети, например к разным коммутаторам.

Все компоненты каждого сервиса, кроме избыточных элементов, должны быть

плотно взаимосвязаны, использовать одни и те же источники питания и сетевую

инфраструктуру, чтобы сервис в целом, насколько это возможно, зависел от

наименьшего числа компонентов. Рассеивание неизбыточных компонентов по

многочисленным частям инфраструктуры просто приведет к тому, что у серви-

са будет больше вероятных точек неисправностей, каждая из которых может

вызвать отказ всего сервиса.

Наиболее эффективный способ добиться максимальной надежности сервиса –

сделать его настолько простым, насколько это возможно. Найдите самое простое

решение, которое соответствует всем требованиям. При оценке надежности

создаваемого вами сервиса разбейте его на составные части и изучите зависи-

мости и степень надежности каждой из них, пока не добьетесь набора серверов

и сервисов, которые ни от чего больше не зависят.

Одним из компонентов системы является сеть. При создании централизованного сервиа с удаленным доступом к нему, особенно важно

учитывать в расчетах топологию сети. Например, сервис имен должен

оставаться доступным для обеих сторон при затрудненной связи, так как многое

из того, от чего зависят люди в удаленной сети, находится только на машинах

этой сети. Но люди не смогут ничего сделать, если им не обеспечить разрешение

имен. Даже если база данных их сервера имен не получает обновлений, уста-

ревшая база данных по-прежнему будет полезна. Если у вас организован цент-

рализованный сервис аутентификации удаленного доступа с системами удален-

ного доступа в других офисах, возможно, у этих систем удаленного доступа

должна оставаться возможность аутентификации людей, подключающихся

к ним, даже при отказе связи с центральным сервером. И в том и в другом слу-

чае в программном обеспечении должна быть заложена возможность предостав-

ления вторичных серверов в удаленных офисах и возобновления синхронизации

баз данных после восстановления подключения. Однако, если вы создаете боль-

шую базу данных или файл-сервер, обеспечить доступ удаленных офисов

к сервису в случае отказа связи практически нереально.

При частичном отказе по-прежнему предоставляется частичная функциональ-

ность. Например, при отказе DNS-сервера пользователи продолжат работу,

хотя иногда несколько медленнее или с потерей отдельных функций.

При полном отказе, с другой стороны, нарушается работа всех сервисов, из-за

чего останавливается вся работа. Лучше группировать пользователей, сервисы

и серверы таким образом, чтобы полный отказ сервиса нарушал работу только

отдельных групп пользователей, а не всех сразу.

**5.1.10. Один сервер или несколько**

**Независимые сервисы, или демоны**, всегда должны находиться на отдельных

машинах, если позволяет уровень финансирования и количество персонала.

Тем не менее, если создаваемый вами сервис объединен более чем с одним новым

приложением или демоном, связь с которыми осуществляется через сеть, вам

придется подумать, размещать ли все компоненты на одной машине или разде-

лить их между несколькими машинами.

Этот выбор может быть обусловлен соображениями безопасности, производи-

тельности или масштабируемости. Например, если вы создаете веб-сайт с базой

данных, вам придется разместить базу данных на отдельной машине, чтобы вы

могли настроить доступ к базе данных, защитить ее от несанкционированного

доступа из Интернета и расширить внешний интерфейс вашего сервиса за счет

подключения дополнительных веб-серверов, не затрагивая машину с базой

данных.

Иногда два приложения или демона могут быть полностью взаимосвязаны

и никогда не использоваться отдельно. В этой ситуации при прочих равных

условиях имеет смысл размещать их на одной машине, чтобы сервис зависел

только от одной машины, а не от двух.

**5.1.11. Централизация и стандарты**

Еще один элемент построения сервиса – **централизация инструментария**, при-

ложений и сервисов, необходимых вашим пользователям. Централизация

подразумевает, что инструментарий, приложения и сервис управляются в пер-

вую очередь центральной группой системных администраторов на едином

центральном наборе серверов, а не многочисленными корпоративными группа-

ми, дублирующими работу друг друга и закупающими собственные серверы.

Поддержку этих сервисов предоставляет центральная служба поддержки. Цен-

трализация сервисов и создание их стандартными способами упрощает поддержку и снижает затраты на обучение персонала.

Общая централизация не отменяет централизации на уровне региональных или

организационных подразделений, в особенности если в каждом регионе или

организации есть своя служба поддержки. Некоторые сервисы, такие как элек-

тронная почта, аутентификация и сети, являются частями инфраструктуры

и должны быть централизованными. В крупных компаниях эти сервисы могут

быть созданы вокруг центрального ядра, обменивающегося информацией

с распределенными региональными или организационными системами. Для

других, таких как файловые серверы и процессорные фермы, более естественной

будет централизация на уровне подразделений.

**5.1.12. Производительность**

При разработке сервиса придется уделить внимание характеристикам его производи-

тельности, даже если потребуется преодолеть массу других сложных техничес-

ких задач.

По мере роста скоростей процессоров, сетевого и видеооборудования возрастают

ожидания в отношении производительности. Приемлемая производительность

сегодня не может быть такой же, как полгода или год назад. Следует стремиться к тому, чтобы в течение нескольких лет вам не потребовалась модернизация.

Нужна машина, которая не обесценится слишком быстро. Для создания сервиса с достойной производительностью вы должны понимать,

как он устроен, и, возможно, найти способы эффективно разделить его между

несколькими машинами. С самого начала вы также должны учитывать, как

будет масштабироваться производительность начальной системы по мере роста

нагрузки и ожиданий от нее.

При выборе машин для запуска сервиса учитывайте особенности работы сер-

виса. Есть ли в нем процессы, часто обращающиеся к диску? Если есть, выби-

райте для этих процессов серверы с быстрой дисковой системой ввода-вывода

и быстрыми дисками. Для дальнейшей оптимизации определите, какая опе-

рация чаще требуется при обращении к диску: чтение или запись? Если сервис

держит в памяти большие таблицы с данными, ищите серверы с большим

количеством быстрой памяти и большим кэшем. Если сетевой сервис обмени-

вается большим количеством данных с клиентами или между серверами сер-

виса, приобретите побольше высокоскоростных сетевых интерфейсов и изыс-

кивайте способы распределения трафика между интерфейсами.

**5.1.13. Мониторинг**

Сервис не готов, пока не налажен мониторинг производительности, проблем, работоспособности и не внедрены механизмы планирования мощностей. Служба поддержки или оперативная группа поддержки должна автоматически

получать оповещения о проблемах сервиса, чтобы начать их исправлять до того,

как они затронут слишком большое количество людей.

Группа системных администраторов должна вести упреждающий мониторинг сервиса с точки зрения планирования мощностей. В зависимости от типа сервиса, в планирование мощностей может включаться пропускная способность сети, производительность сервера, скорость транзакций, лицензии и доступность физических устройств. Кроме того, системные администраторы должны обоснованно прогнозировать и планировать возможности роста сервиса. Чтобы делать это эффективно, мониторинг использования должен быть неотъемлемой частью сервиса.

**5.1.14. Разворачивание сервиса**

То, как среди пользователей будет внедряться новый сервис, так же важно, как

и то, как система разрабатывалась. От внедрения и от первых впечатлений

пользователей зависит, как в дальнейшем будет восприниматься сервис. Так

что постарайтесь, чтобы первые впечатления были положительными.

В числе ключевых моментов создания хорошего впечатления – готовность до-

кументации, ознакомленная с новым сервисом и хорошо подготовленная служ-

ба поддержки и проработанные процедуры поддержки.

Процесс внедрения также включает в себя создание и тестирование механизма

установки нового программного обеспечения или необходимых настроек кон-

фигурации на каждый настольный компьютер. В идеале сервису не должно требоваться новое программное обеспечение или конфигурирование настольных компьютеров, потому что это более удобно для пользователей и снижает необходимость обслуживания, но зачастую установка новых клиентских программ на настольные компьютеры необходима.

***5.2. Тонкости***

**5.2.1. Выделенные машины**

В идеале сервис необходимо создавать на выделенных машинах. Наличие выделенных машин для каждого сервиса повышает надежность сервисов, упрощает отладку при возникновении каких-либо проблем с надежностью, снижает масштаб простоев, а также намного упрощает модернизацию и планирование мощностей.

В растущих корпоративных сетях, как правило, выделяется одна центральная

административная машина, являющаяся ядром всех критически важных сер-

висов. Она предоставляет сервисы имен, аутентификации, печати, электронной

почты и т. д. В результате из-за увеличения нагрузки эту машину приходится

разделять, а сервисы – распределять по нескольким серверам. Зачастую к тому

времени, как системным администраторам удается добиться финансирования

для дополнительных административных машин, эта машина уже настолько

загружена сервисами и зависимостями, что разделить ее очень сложно.

Сложнее всего при распределении сервисов с одной машины на несколько разо-

браться с зависимостями IP-адресов. Некоторые сервисы подразумевают жест-

ко запрограммированные на всех пользователей IP-адреса. В конфигурации

многих сетевых продуктов, таких как брандмауэры и маршрутизаторы, IP-ад-

реса жестко запрограммированы в их конфигурации.

Разделение узла на несколько разных узлов – очень сложная задача. И чем дольше такой узел существует, чем больше сервисов на нем создается, тем сложнее становится такая задача. В этом случае может помочь использование имен, основанных на названиях сервисов, однако их необходимо стандартизировать и внедрить эти стандарты во все отделения компании.

**5.2.2. Полная избыточность**

Наличие дублирующего сервера или набора серверов, которые готовы принять

на себя роль основных серверов в случае сбоя, называется **полной избыточностью.**

Программное обеспечение, которое вы используете для предоставления сервиса, может потребовать избыточности в виде постоянно подключенного пассивного подчиненного сервера, который реагирует на запросы только в случае отказа основного сервера. В любом случае механизм избыточности должен обеспечивать синхронизацию данных и поддерживать их целостность.

В крупных фермах клонированных серверов и в других случаях, когда избы-

точные серверы постоянно работают параллельно с основными, избыточные

машины можно использовать для распределения нагрузки и увеличения быст-

родействия при безотказной работе. Если вы используете этот подход, будьте

осторожны и не позволяйте нагрузке достигнуть точки, при которой произво-

дительность стала бы неприемлемой в случае отказа одного из серверов.

Некоторые сервисы являются неотъемлемой частью ежеминутного функцио-

нирования сети, поэтому их полная избыточность обеспечивается на самых

ранних стадиях создания этой сети. Другие сервисы в этом отношении игнори-

руются до тех пор, пока сеть не достигнет очень крупных размеров или не про-

изойдет серьезный, заметный сбой такого сервиса.

**5.2.3. Потоковый анализ для масштабирования**

**Потоковая модель** – список транзакций и их зависимостей со всей информацией, которую можно получить об использовании ресурсов по каждой транзакции. Эта информация может включать в себя объем памяти, используемой на сервере этой транзакции; размер и количество пакетов, используемых в транзакции; количество открытых сокетов, используемых для обслуживания транзакции, и т. д.

При моделировании отдельной служебной транзакции с помощью потоковой

модели включаются все детали, необходимые для проведения транзакции, даже

такие, как поиск интернет-имен через DNS, чтобы получить истинную картину

транзакции.

Когда потоковая модель точно изображает сервис, вы можете локализовать

проблемы производительности и масштабируемости, увидев, какая часть моде-

ли потоков данных является слабым звеном, провести мониторинг этого участка

в реальных или искусственно созданных условиях и посмотреть, как он функционирует или дает сбой.

Ресурсы сервера тоже могут стать проблемой. Чтобы проанализировать ресурсы, вам также придется выяснить, загружает ли процесс IMAP в память сервера файловые индексы, или что-то другое, или даже все содержимое почтового ящика. Если так, вам нужно узнать средний размер загружаемых данных, который может быть вычислен как среднее арифметическое размера пользовательских файловых индексов, как средняя линия или медиана участка кривой размера файлов, на котором находится большинство файловых индексов, или даже путем учета только тех файловых индексов,

которые используются в период максимальной нагрузки и проведения тех же

вычислений с ними. Выберите тот способ, который кажется более подходящим

для вашего приложения. Можно использовать систему мониторинга для про-

верки вашего прогноза.

Наконец вернитесь назад и проделайте такой же анализ на всех этапах движения

потока данных. Если настольный компьютер пользователя делает внутренние

запросы для поиска имен, чтобы найти почтовый сервер, вместо того чтобы

кэшировать информацию о том, где его можно найти, следует это включить

в анализ потока данных как нагрузку на сервер имен.

Потоковая модель работает на всех уровнях масштабирования. Вы можете успешно спроектировать модернизацию сервера для отдела с тридцатью сотрудниками или кластеры мультимедийного сервиса для трех миллионов пользователей одновременно. Чтобы получить точные цифры, которые вам нужны для крупномасштабного планирования, можно использовать анализ трафика тестовой установки, а также информацию от поставщика, отслеживание системы и т. д.

***5.3. Заключение***

Разработка и создание сервисов – важная часть работы каждого системного

администратора. От того, насколько хорошо системный администратор выпол-

нит эту часть работы, зависит то, насколько легко будет обслуживать и поддерживать каждый сервис, насколько он будет надежным, производительным,

соответствующим требованиям пользователей и в конечном счете насколько

довольны будут пользователи работой команды системных администраторов.

Вы создаете сервис для улучшения обслуживания ваших пользователей, непосредственно, за счет предоставления необходимого им сервиса, или опосредованно, за счет улучшения эффективности работы команды системных администраторов.

В число условий создания лучшего сервиса входит ваша способность видеть дальше начальных требований будущих проектов по модернизации и обслуживанию. Создание сервиса, максимально независимого от машин, на которых он выполняется, – основной способ упростить обслуживание и модернизацию.

Сервисы должны быть настолько надежны, насколько это требуется пользова-

телям. Спустя некоторое время в более крупных компаниях вы должны быть

готовы сделать большее количество сервисов полностью избыточными, чтобы

при сбое любого из компонентов и его замене сервис не прекращал работу. Рас-

пределите приоритеты в том порядке, который обеспечит для сервисов полную

избыточность, основываясь на потребностях ваших пользователей.

Последняя часть создания нового сервиса – постепенное развертывание сервиса с минимальными помехами в работе пользователей. Мнение пользователей о сервисе формируется в основном во время процесса внедрения, так что очень важно провести его правильно.

***Глава 6***

**Вычислительные центры**

Эта глава посвящена созданию **вычислительного центра** – места, в котором

находятся машины, предоставляющие общие ресурсы. Как правило, вычислительный центр

оснащен системами охлаждения, регулировки влажности, электропитания

и противопожарными системами. Все эти системы – часть вашего вычислитель-

ного центра. Зачастую вычислительные центры – это отдельные здания, построенные

специально для вычислительных и сетевых операций.

***6.1. Основы***

Для начала вам понадобится выбрать качественные стойки и сетевые кабели, подготовить питание, которое будет подаваться к оборудованию; потребуется серьезное охлаждение и нужно будет продумать систему пожаротушения. Кроме того, надо основательно спланировать устойчивость помещения к стихийным бедствиям. Правильная организация зала подразумевает продуманную разводку кабелей, службу консолей, пометку ярлыками, наличие инструментов, запасных частей, рабочих мест и мест парковки для передвижных устройств. Также понадобится проработать механизмы безопасности вычислительного центра и продумать способы транспортировки оборудования в зал и из зала.

**6.1.1. Размещение**

Нужно решить, где будет размещаться вычислительный центр.

Сначала придется выбрать город и здание в этом

городе. Когда здание выбрано, необходимо выбрать подходящее место внутри

здания. На всех этих этапах при принятии решения следует принимать во вни-

мание стихийные бедствия, типичные для этого региона.

Если вычислительный центр обслуживает весь мир или значительный регион и при этом расположен в местности, где часты стихийные бедствия, способные

повредить информационному центру или вызвать перебои с энергоснабжением

и связью, вы должны быть подготовлены к подобным случайностям. Кроме

того, вы должны быть готовы к тому, что чей-то экскаватор случайно повредит

ваши линии энергоснабжения и связи, независимо от того, насколько хорошо

вы защититесь от стихийных бедствий. Против перебоев со связью

вы можете внедрить технологии резервных подключений на случай, если ос-

новные каналы выйдут из строя. Также вы можете поставить вопрос о создании второй сети, полностью дублирующей все службы

вычислительного центра, когда основная сеть выходит из строя. Такой подход

обходится дорого и может быть оправдан только в случае, если временный

отказ вычислительного центра угрожает компании сопоставимыми убытками.

Когда приходит время выбирать помещение для вычислительного центра внут-

ри здания, команда системных администраторов должна в этом участвовать.

Надо обсудить размеры необходимого вам помещения. Также вы должны быть гото-

вы предоставить отделу недвижимости требования, которые помогут им выбрать

подходящее место. Как минимум, вы должны быть уверены, что пол достаточ-

но прочный, чтобы выдержать вес оборудования. Однако есть и другие факторы,

которые необходимо учитывать.

Если в регионе часто случаются наводнения, по возможности надо избегать

размещения вычислительного центра в подвале или даже на первом этаже.

Также вам надо учитывать, как это отразится на размещении вспомогательной

инфраструктуры вычислительного центра: таких систем, как источники беспе-

ребойного питания, автоматы включения резерва (АTS), генераторы и системы

охлаждения. Если эти вспомогательные системы откажут, то и вычислительный

центр тоже.

При размещении вычислительных центров в сейсмически опасных регионах

надо учитывать несколько факторов. Вы должны выбирать стойки, которые

в достаточной степени устойчивы к вибрации, и удостовериться, что оборудова-

ние хорошо закреплено в стойке и не выпадет при землетрясении. Вам следует

установить соответствующие сейсмостойкие конструкции, усиливающие, но не

слишком жесткие.

Существует несколько уровней сейсмической готовности вычислительных

центров. Хороший консультант по информационным центрам должен быть

готов согласовать с вами возможности и затраты, чтобы вы могли решить, что

соответствует требованиям вашей компании.

**6.1.2. Доступ**

Надо продумать, как перемещать стойки и оборудование в зал. Некоторые элементы оборудования могут быть шире стандартных

дверных проемов, так что могут понадобиться более широкие двери. Если

у вас двойные двери, убедитесь, что между ними нет стояка. Стоит пре-

дусмотреть проходы между стойками, достаточные для транспортировки обо-

рудования на места. Может понадобиться усилить некоторые зоны пола

и проходы к ним, чтобы пол выдержал особо тяжелое оборудование. Также вам

надо предусмотреть свободный доступ от погрузочной платформы на всем пути

до вычислительного центра. Обычно оборудование доставляется в таре, габариты которой превышают размер самого оборудования.

**6.1.3. Безопасность**

Вычислительный центр должен быть физически защищен настолько, насколько

это возможно сделать, не препятствуя работе системных администраторов. До-

ступ должен предоставляться только тем, чьи обязанности того требуют. Ответственный за пожарную безопасность и, в некоторых случаях, аварийные бригады, приписанные к этой зоне, должны назначаться из тех, у кого уже есть доступ.

Ограничение доступа в вычислительный центр повышает надежность и безот-

казность размещенного там оборудования и увеличивает вероятность, что

стандарты прокладки кабелей и монтажа в стойки будут соблюдаться. К серве-

рам, по определению, предъявляются высокие требования по безотказной ра-

боте, и следовательно, все изменения должны вноситься группой системных

администраторов в соответствии с установленными правилами и процедурами,

направленными на выполнение либо превышение обязательств по уровню об-

служивания. Сотрудники, не входящие в число системных администраторов,

не имеют таких обязательств и не обучены ключевым процессам группы систем-

ных администраторов. Поскольку эти сотрудники посвящают меньше времени

обслуживанию инфраструктурного оборудования, они скорее могут допустить

ошибки, которые способны вызвать дорогостоящий простой. Если кому-то из

ваших пользователей нужен физический доступ к машинам в вычислительном

центре, они не могут считаться высоконадежными или инфраструктурными

машинами и поэтому должны быть перемещены в лабораторные условия, где

пользователи смогут получить к ним доступ. Либо можно использовать техно-

логии удаленного доступа, такие как КВМ-коммутаторы.

Подумайте о внедрении систем бесконтактных пропусков, они

более удобны и автоматически регистрируют входящих. В вычислительных

центрах с особо высокими требованиями к безопасности используют

датчики движения, чтобы убедиться, что зал действительно пуст, когда это

отмечено в записях регистрации пропусков.

Эффективность биометрических систем была поставлена под сомнение.

Цутому Мацумото (Tsutomu Matsumoto), японский специалист в области крип-

тографии, доказал, что лучшие системы сканирования отпечатков пальцев можно надежно обмануть, приложив немного изобретательности и потратив подручных материалов на 10 долларов: из обычного желатина он сделал поддельный палец (SPIE 2002).

**6.1.4. Электричество и охлаждение**

Энергоснабжение и охлаждение вычислительного центра непосредственно вза-

имосвязаны. Оборудование работает от электричества, охлаждение борется

с теплом, выделяемым аппаратурой при ее работе. При слишком высокой тем-

пературе оборудование может работать с ошибками или даже сгореть.

Как правило, на каждый ватт, потребляемый вашим оборудованием, вам при-

дется потратить по меньшей мере 1 ватт на охлаждение. Значит, половина вашего счета за электричество идет на охлаждение, а половина – на питание оборудования. Кроме того, это означает, что аппаратура, которая потребляет меньше электроэнергии,

экономит ее вдвое больше за счет меньшей потребности в охлаждении.

Вы можете направить воздушные потоки в вычислительном центре двумя ос-

новными способами.

**Первый способ** – это использование фальшпола в качестве

воздухопровода для холодного воздуха. Вентиляционная система нагнетает

холодный воздух и создает достаточное давление, чтобы воздух поступал через

отверстия в фальшполе. Вентиляционные отверстия размещаются так, чтобы

воздух из них шел снизу в оборудование, выводя тепло наверх и наружу.

**Другой способ** – подавать холодный воздух со стороны потолка и обдувать ма-

шины сверху вниз. Так как горячий воздух поднимается вверх, потребуется

дополнительная работа для нагнетания холодного воздуха вниз. Используя

такую систему, вы можете также прокладывать кабели над стойками либо ис-

пользовать фальшпол исключительно для кабелей.

Еще один компонент кондиционирования – контроль влажности. В вычисли-

тельном центре нужно регулировать влажность воздуха, так как высокая влаж-

ность приводит к образованию конденсата и выходу оборудования из строя,

а при низкой влажности возникают статические разряды, которые также могут

повредить оборудование. В идеале влажность воздуха должна быть от 45 до 55%.

Системы энергоснабжения, отопления1, вентиляции и кондиционирования гро-

моздки, их сложно заменять, и почти наверняка для этого потребуется перерыв.

Поэтому старайтесь планировать эти системы хотя бы на 8–10 лет вперед.

Системы бесперебойного питания должны иметь возможность оповещать пер-

сонал о сбоях или иных проблемах. Небольшие источники бесперебойного пи-

тания при истощении батарей должны уметь посылать серверам оповещения

о необходимости выключения.

При приобретении источников бесперебойного питания наиболее важно учиты-

вать следующее: как показывают исследования, перебои в электросети обычно

либо очень короткие (исчисляемые секундами), либо очень длинные (полдня

и дольше). Большинство перебоев с напряжением длятся не более 10 с. С точки

зрения статистики, если электричества нет более 10 мин, наиболее вероятно,

что его не будет весь день и вы можете отпустить сотрудников домой.

Следовательно, приобретение ИБП, который обеспечивает резервное питание

значительно дольше часа, с точки зрения статистики будет пустой тратой денег.

Если электричества нет в течение часа, скорее всего, его не будет до конца дня

или около того, а ИБП с таким запасом емкости стоит слишком дорого. Если

в вашем соглашении об уровне обслуживания требуется устойчивость к перебо-

ям в электросети длительностью более часа, вашему информационному центру

потребуется генератор.

Питание системы охлаждения от ИБП потребует удвоить его емкость, что примерно вдвое увеличит его стоимость.

**Автомат включения резерва** – это устройство, управляющее переключением

питания ИБП от сети или генератора. АВР отслеживает напряжение в сети

и, если оно находится в пределах нормы, подключает к сети ИБП. Если АВР

фиксирует перебои в сети, то питание ИБП отключается, включается генератор

и, когда генератор начинает вырабатывать стабильное напряжение, ИБП пере-

ключается на него. Когда напряжение в сети возвращается в норму, АВР снова

переключает ИБП на питание от сети и выключает генератор.

Всегда устанавливайте переключатель, позволяющий включить питание в обход

ИБП в случае его отказа. Все питание вычислительного центра идет через ИБП.

Следовательно, если он откажет, то на время ремонта вам понадобится пере-

ключиться на другой источник питания. Переключатель должен быть отдельным от ИБП и находиться на разумном расстоянии от него.

Генераторы должны проходить тщательную профилактику, ежемесячные ис-

пытания и периодически дозаправляться. В противном случае в тех немногих

ситуациях, когда они понадобятся, генераторы не будут работать и вы зря потратите деньги.

Если в вычислительном центре есть генератор, то системы отопления, вентиля-

ции и кондиционирования тоже должны иметь резервное питание. Иначе сис-

темы будут перегреваться.

Для выявления горячих точек полезно распределить по информационному

центру и подключить к системам мониторинга датчики температуры. Другой

вариант, быстрый и дешевый, – перемещать по залу цифровые термометры,

записывающие показания о высокой и низкой температуре. После выявления горячих точек проблема сводится к перемещению оборудования или замене системы отопления, вентиляции и кондиционирования.

Системы отопления, вентиляции и кондиционирования часто выходят из строя

незаметно и иногда возобновляют работу так же незаметно. Так как сбои систем

отопления, вентиляции и кондиционирования повышают вероятность сбоев

другого оборудования, важно вовремя заметить их сбой. Если в самих системах

не предусмотрен механизм автоматического оповещения службы поддержки,

следует включить температурные датчики в конфигурацию систем мониторин-

га сети.

В дополнение к подключению систем отопления, вентиляции и кондициониро-

вания к генератору может быть полезно подключить и другие цепи здания

к резервному питанию от генератора. Эти цепи должны быть устойчивы к ко-

ротким перебоям и скачкам напряжения. Подходящий кандидат – освещение,

особенно в помещениях службы поддержки и эксплуатационного отдела.

**Максимальная нагрузка** – это не просто суммарное потребление оборудования

вычислительного центра. Все компоненты электрической системы, а также

выключатели и автоматические предохранители между ними должны иметь

запас мощности, достаточный, чтобы выдержать максимальную нагрузку вы-

числительного центра, системы отопления, вентиляции и кондиционирования,

работающих с максимальной производительностью, и нагрузку ИБП, заряжа-

ющих батареи.

Даже если вы устанавливаете систему, которая наверняка будет временной, вы

все равно должны проверять каждый компонент с тем же вниманием к деталям,

как если бы это была постоянная система. Ни один из компонентов не должен

быть недостаточно мощным. Ни один из компонентов не должен быть установ-

лен нестандартным образом. Иначе, независимо от того, насколько хорошо вы

будете готовиться к каждой случайности, система преподнесет вам неожиданные

сюрпризы, когда вы меньше всего этого ожидаете.

Промышленные устройства работают круглосуточно без выходных в течение

всего года. Так как они должны работать безостановочно, они проектируются

по-другому и оснащаются более надежными двигателями и компонентами, что

повышает их цену.

Обеспечив свой вычислительный центр стабилизированным питанием, вы

должны подвести питание к стойкам. Хороший способ сделать это – проложить

подвесную шину питания, что даст вам возможность подвести к каждой стойке

разные напряжения, если у вас есть оборудование, требующее нестандартного

питания, что встречается среди оборудования высшего класса. Кроме того,

подвесной монтаж снижает риск контакта с водой на полу или под фальшполом,

например, от утечки из кондиционера или из водопроводных труб. Электрические розетки можно разместить подальше от источников протечек и закрыть

чем-нибудь от брызг. При наличии фальшпола нужно установить под ним дат-

чики воды. Строительный подрядчик, скорее всего, поможет вам найти впади-

ны, где вода будет скапливаться в первую очередь. Кроме того, следует разместить датчики под кондиционером.

Некоторые блоки распределения питания обладают функцией удаленного

управления питанием, то есть дают возможность удаленно управлять каждым

отдельным разъемом питания. Возможность включить или выключить конкрет-

ный разъем позволит не ходить в вычислительный центр, когда машине не

хватает обычной перезагрузки. Такие распределительные блоки очень дороги,

и сложно оправдать их использование для всего оборудования. Часто использо-

вание такого типа блоков распределения ограничено сетевым оборудованием,

используемым для внешних подключений к информационному центру, и обо-

рудованием, необходимым для удаленного управления другим оборудованием.

Питание должно правильно распределяться внутри стойки с помощью распре-

делительного блока питания. Если в вычислительном центре есть разные ис-

точники питания, обеспечивающие защищенное или незащищенное питание

или питание от двух раздельных систем бесперебойного питания и генераторов,

они должны быть однозначно идентифицируемыми по цвету розеток распреде-

лительного блока.

**6.1.5. Системы пожаротушения**

Настоятельно рекомендуется установить в вычислительном центре систему

пожаротушения.

Блоки питания, батареи ИБП и диски могут случайно перегореть или загореть-

ся. При проблемах с электропроводкой может возникнуть искра, которая по-

дожжет находящиеся поблизости материалы.

Как правило, местные законодательные акты не только требуют наличия сис-

темы пожаротушения, но и четко оговаривают, какие системы можно исполь-

зовать, а какие нельзя. Подумайте, какой опасности могут подвергаться люди, работающие в помещении; насколько вредное воздействие система оказывает на окружающую среду; какой ущерб она может нанести оборудованию, не подверженному пожару; а также насколько хорошо система справляется с возгоранием электроаппаратуры.

Еще один фактор, который необходимо учесть, – стоит ли связать активацию

системы пожаротушения с переключателем, отключающим питание в компью-

терном зале. В некоторых системах предусмотрен блок предварительной активации, который сообщает сотрудникам о небольшом локальном облаке дыма перед активацией системы пожаротушения. Это дает сотрудникам время на отключение задымившегося устройства, прежде чем начнется пожар и система пожаротушения активируется в полном масштабе.

Помимо технологии вашей системы пожаротушения, вам необходимо устано-

вить несколько важных процедурных компонентов. Если ваша система пожа-

ротушения связана с оперативным центром, необходимо проинструктировать

сотрудников этого центра, что они должны делать в случае тревоги. Если в по-

мещении круглосуточно дежурят люди, которые не разбираются в компьютерах,

для них необходимо провести инструктаж, как следует реагировать на пожарную

тревогу. После активации системы пожаротушения вам, скорее всего, придется

какое-то время обойтись без нее, так как системе нужно время на дозаправку.

Если пожар вновь разгорится после активации системы пожаротушения, вы

рискуете потерять все здание. Вам необходима четкая процедура, которая поз-

волит максимально снизить риск повторного возгорания, а также отследить

и эффективно ликвидировать его в случае возникновения.

**6.1.6. Cтойки**

Каждый вид стоек предназначен для определенной цели. Некоторые больше подходят для серверов, а другие – для сетевого оборудования.

Стойки позволяют организовать оборудование. Грамотная организация позво-

ляет разместить в помещении большее количество компьютеров. Повышенная

плотность достигается благодаря вертикальному размещению оборудования

в стойках.

Стойки – часть системы охлаждения. Воздушные потоки в помещении в основ-

ном определяются расположением стоек. Внутри самой стойки хороший воз-

душный поток позволяет должным образом охлаждать компьютеры. Стойки

с плохой проходимостью воздуха осложняют охлаждение оборудования.

Стойки – часть кабельной инфраструктуры. Возможность создать грамотную,

управляемую кабельную систему в основном зависит от того, позволяют ли

стойки как следует проложить кабели. Без стоек не будет возможности

управления кабелями: кабели разных машин будут путаться и постоянно ока-

зываться на полу, где на них могут наступить. Это может привести к поврежде-

нию кабелей и их случайному отключению. Найти поврежденный кабель может

быть очень сложно, а иногда и невозможно, не потянув при этом другие кабели

с риском повредить или отключить их.

Стойки – часть инфраструктуры питания. Блоки распределения питания, как

правило, расположены внутри стоек. Без стоек снабжение питанием станет

бессистемным и повысится риск возникновения пожара из-за множества удли-

нителей. Стойки позволяют разделить кабели питания и сетевые кабели, что снижает количество сетевых проблем.

ковые панели стоек, а также продумайте возможности управления кабелями.

**6.1.6.1. Обзор стоек**

Вертикальные перекладины, к которым крепится оборудование, называ-

ются **рельсами**. Как правило, две или четыре рельсы располагаются на рассто-

янии 17,75 дюймов (45 см) друг от друга. Вместе с их собственной толщиной это

обычно составляет ровно **19 дюймов**. У современных стоек есть по бокам допол-

нительные крепежи для кабелей, которые увеличивают ширину стоек.

Отверстия в стойках располагаются группами по три: над первым отверстием

на расстоянии 0,5 дюйма (12,7 мм) расположено второе; выше, через 0,625 дюй-

ма (15,875 мм), идет следующее отверстие; и через 0,625 дюйма (15,875 мм) –

еще одно. Далее образец расположения повторяется.

Вертикальное расстояние между двумя крайними отверстиями из трех называ-

ется рэк-юнитом, или U (от англ. unit). 1U равен 1,75 дюйма (4,5 см). Высота

оборудования измеряется в рэк-юнитах, или U. Дисковый массив может иметь

высоту 4U, крупный сервер – 8U, 16U или даже больше. Высота небольших

серверов, как правило, составляет 2U, если у них много дисков, и 1U, если нет.

Устройство высотой 1U из-за его формы часто называют «коробкой от пиццы».

Высота стандартной полноразмерной стойки составляет 42U.

На хороших стойках имеются отметки, обозначающие первые отверстия в каж-

дой группе из трех отверстий. Кроме того, на хороших стойках все отверстия

пронумерованы. Если вам нужно найти пару одному из отверстий на другой

стороне, достаточно просто отыскать отверстие с тем же номером.

У более старых стоек оборудование крепится болтами к круглым отверстиям

с резьбой. Иногда эти отверстия загрязняются, резьба срывается и данную часть

стойки дальше использовать невозможно. У стоек разных производителей от-

верстия могут быть разного диаметра, и иногда на поиск подходящих болтов

уходит немало усилий. У стоек с отверстиями без резьбы эти проблемы реша-

ются простым наличием болта и гайки. Если резьба вдруг сорвется, достаточно

заменить болт и гайку.

В современных стойках болты не используются, а отверстия квадратные. На

устройствах предусмотрены зацепы, которые проходят в квадратное отверстие

по диагонали. Устройство устанавливается в стойку, и его удерживает сила

тяжести. Крупногабаритное оборудование закрепляется дополнительными

винтами. Более старое оборудование можно установить в такие стойки с помо-

щью монтажных гаек – металлических квадратов с резьбовым отверстием.

**6.1.6.2. Вертикальные штанги**

Рельсы по углам стойки называют **вертикальными штангами**. Стойки могут

быть двухштанговыми (или однорамными) и четырехштанговыми (или двух-

рамными).

**Однорамные** стойки, как правило, используются для сетевого и телекоммуни-

кационного оборудования, для которого обычно предусмотрена возможность

центрального крепления, а также крепления на лицевой и/или задней панели.

Однако часто проще и безопаснее установить крупногабаритное сетевое и теле-

коммуникационное оборудование в двухрамную стойку, которая лучше защи-

щает аппаратуру от случайных толчков, способных ослабить или повредить

кабели. Кроме того, двухрамные стойки, как правило, лучше приспособлены

для горизонтальной укладки кабелей.

Если в вашей компании решили приобрести однорамные стойки, при их уста-

новке удостоверьтесь, что между рядами достаточно свободного места. Проходы

должны быть достаточно широкими, чтобы вместить полторы глубины обору-

дования плюс пространство для прохода людей. Минимальная ширина проходов,

как правило, указана в правилах пожарной безопасности.

**6.1.6.3. Высота**

Высота стойки может влиять на надежность, если стойка высокая и системному

администратору приходится тянуться к машине через другое оборудование.

Кроме того, высокие стойки могут просто не уместиться в помещении, если

к потолку что-нибудь прикреплено (например, шины питания, системы охлаж-

дения или противопожарные системы) или над ними будет недостаточно места

для циркуляции воздуха либо нормальной работы противопожарной системы.

Может быть опасно выдвигать полки в верхней части стойки. С другой стороны,

высокие стойки позволяют более эффективно использовать пространство в вы-

числительном центре.

**6.1.6.4. Ширина**

Большинство оборудования подходит для 19-дюймовых стоек, но телекомму-

никационное оборудование, как правило, устанавливается в стойки, совмести-

мые с системой построения сетевого оборудования (NEBS, Network Equipment

Building System). У таких стоек расстояние между штангами составляет 21 дюйм

(53,3 см).

**6.1.6.5. Глубина**

Двухрамные стойки могут быть различной глубины из-за различных габаритов

оборудования. Стоит выбирать стойки, глубина которых позволяет целиком

разместить в них аппаратуру, чтобы все кабели были защищены от случайных

задеваний и при необходимости можно было бы использовать в стойке горизон-

тальную укладку кабелей. Если машины будут выступать в проходах, появится

угроза безопасности.

**6.1.6.6. Циркуляция воздуха**

Тепло отводится от оборудования благодаря циркуляции воздуха. В некоторых

стойках предусмотрены встроенные вентиляторы, позволяющие усилить поток

воздуха. Если хотите приобрести такие стойки, обдумайте способ, с помощью

которого воздух будет в них попадать. Может потребоваться фальшпол с пер-

форацией, чтобы воздух подавался в стойку снизу. Если вы выбрали более

простую стойку, не оснащенную собственной системой циркуляции воздуха,

вам, возможно, не стоит устанавливать дверцы для передней, задней или боко-

вых панелей, чтобы они не препятствовали потоку воздуха, охлаждающему

оборудование в стойке.

**6.1.6.7. Укладка кабеля**

При приобретении стойки всегда продумывайте укладку кабелей. Чтобы опре-

делить, что именно вам необходимо, продумайте, каким образом вы собираетесь

прокладывать проводку в своем вычислительном центре. Обдумайте возможность горизонтальной и вертикальной укладки ка-

белей. Кабели, должным образом уложенные между стойками и внутри них,

позволят работать эффективно, не затрагивая при этом другое оборудование.

Распутывание кабелей – достаточно непростое дело. Кроме того, оно всегда со-

провождается отключением аппаратуры. Если вы не обеспечите должное управ-

ление кабелями, люди начнут подключать оборудование, как им заблагорассу-

дится. В результате выяснится, что не получится вытащить неисправное устройс-

тво из стойки, чтобы заменить его, не отключив при этом три других критически

важных устройства, которые не имеют ничего общего с нужной вам машиной.

**6.1.6.8. Прочность**

Стойки должны быть достаточно прочными, чтобы выдержать вес устанавли-

ваемого в них оборудования. Как уже говорилось ранее, в сейсмоопасных реги-

онах могут быть повышенные требования к прочности стоек.

**6.1.6.9. Окружающая среда**

Если ваши стойки будут установлены в удаленных районах, учитывайте фак-

торы окружающей среды в этих районах. Например, в Китае повсеместное ис-

пользование угля приводит к загрязнению воздуха серой. Сера приводит

к высокой влажности воздуха, что, в свою очередь, способствует появлению

ржавчины на стойках. Чтобы предотвратить ржавчину, можно использовать

специальное покрытие.

**6.1.6.10. Полки**

Малогабаритное оборудование, не предназначенное для установки в стойку,

можно разместить на полке. Есть специальные полки, устанавливаемые

в стойки.

Тщательно продумайте, как полки и различное оборудование будут установле-

ны в стойке, а также каким образом, если это вообще возможно, следует объ-

единить разную аппаратуру в одной стойке. Продумайте, можно ли установить

полки в стойки, в которых вертикальные рельсы передвигаются вперед или

назад. Зачастую крупное оборудование для стоек требует определенного рассто-

яния между вертикальными рельсами, чтобы можно было прикрепить аппара-

туру со всех четырех углов.

**6.1.6.11. Дополнительная площадь**

Подсчитайте количество крупного, свободно стоящего оборудования, которое

занимает площадь, сопоставимую со стойкой или больше, и при этом не может

быть установлено в стойку. Если вы оставите место для такого оборудования,

это повлияет на количество заказываемых вами стоек и на план проводки

в вычислительном центре.

**6.1.7. Проводка**

В вычислительном центре держать проводку в порядке достаточно сложно.

Однако при планировании центра у вас есть несколько способов, с помощью

которых вы облегчите системным администраторам задачу по поддержке про-

водки в приличном состоянии.

Фальшпол поможет скрыть неряшливые кабели, которые будут путаться как попало. Вытаскивая тот или иной кабель из-под пола, вы обнаружите, что он запутался

среди прочих кабелей. Возможно, и вытащить его будет не так просто. Это при-

ведет к тому, что кабели будут просто оставлять на месте, чтобы разобраться

с ними «позже, когда будет время».

Лучшее, что вы можете сделать, – это заранее максимально подготовить проводку

на стойках. Выберите в вычислительном центре отделение, в котором будет уста-

новлено только сетевое оборудование. Например, задний ряд. Затем на верх каж-

дой стойки установите патч-панель с хорошо читающимся ярлыком. К панели

с запасом подключите кабели. Сделайте хорошо читающийся ярлык для стоек.

На ярлыках стоек должен быть указан ряд и позиция стойки в ряду. Ярлыки

разместите на стенах достаточно высоко, чтобы их было видно с любой точки

и стойки можно было легко найти.

В некоторых корпоративных сетях используют сетевые кабели разных цветов. По

крайней мере, кабели разного назначения (категория 5, категория 6) и кабели

с разной разводкой (прямой, кроссоверный) должны быть разных цветов. В неко-

торых сетях по цветам разделяют разные подсети. Мы рекомендуем использовать

красный цвет для сетей, которые подключены к Интернету без брандмауэра.

Все сетевые и консольные кабели для серверов, размещенных в стойке, должны

располагаться в этой же стойке, не считая тех, что были проведены заранее.

Удостоверьтесь, что внутри стойки достаточно места для кабелей. Приобретите

кабели различной длины, чтобы всегда было можно подобрать нужный вариант.

Всегда должна быть возможность использовать кабель, длина которого после

прохода кабеля через все крепления позволяет чуть выдвинуть машину вперед

на случай сейсмических событий. При этом кабель не должен быть слишком

длинным, чтобы не образовывались большие свисающие петли.

Основными аргументами против предварительной укладки кабелей являются

уменьшение свободного пространства в стойке и стоимость. Однако повышение

надежности, производительности и управляемости благодаря отсутствию запу-

танных проводов как на полу, так и за стойками является огромным.

Еще один прием по оптимизации системы кабелей – наличие на боковых панелях

стоек вертикальных блоков распределения питания с множеством розеток.

Приобретите два коротких кабеля питания разной длины (например, 30 и 60 см)

и подключите каждое устройство к ближайшей розетке. Это позволит предотвратить использование длинных кабелей питания, которые могут путаться с кабелями передачи данных и вдобавок к беспорядку создавать помехи.

**6.1.8. Маркировка**

Грамотная маркировка и ярлыки необходимы для безотказной работы вычисли-

тельного центра. Все устройства должны иметь ярлыки как на лицевой, так и на

задней панели. На этих ярлыках должно присутствовать полное имя устройства,

которое указано в корпоративном пространстве имен и в системе кон-

сольного сервера.

Если к машине имеется несколько подключений одного вида и с первого взгляда

неясно, какое из них для какой цели используется (например, несколько сетевых

интерфейсов, принадлежащих разным сетям), необходимо наклеить ярлыки как

на интерфейсы, так и на кабели. Здесь же полезно использовать сетевые кабели

разных цветов, например, распределив цвета по разным доменам.

Если на сетевом устройстве много портов, приклеивать ярлык у каждого из них

непрактично. Однако стоит прикрепить ярлыки к оборудованию, на котором

разные порты связаны с сетями или виртуальными локальными сетями.

Для сетевого оборудования, подключаемого к глобальной вычислительной сети

(ГВС), на ярлыке должно быть указано имя другой стороны подключения

и идентификационный номер поставщика подключения. Этот ярлык должен

быть на устройстве, на котором находятся индикаторы ошибок данного подклю-

чения.

Сетевое оборудование, как правило, предоставляет средства для маркировки пор-

тов в программном обеспечении. Средства программной маркировки должны

использоваться в полной мере, предоставляя как минимум ту же информацию,

что и обычные ярлыки. Сетевое оборудование становится малогабаритным и более

интегрированным, поэтому подробную информацию на обычных ярлыках стано-

вится уместить все сложнее. Из-за этого программная маркировка является самым

удобным способом хранения информации, которая необходима при отладке.

Использование вместе стандартных ярлыков и программной маркировки обес-

печивает наличие нескольких источников «знания». Важно удостовериться,

что оба эти средства синхронизированы и предоставляют одну и ту же инфор-

мацию.

Если вы наклеиваете ярлыки на кабели вручную, делайте это до укладки кабе-

лей. Это стоит повторить: сначала ярлык, потом укладка. В противном случае

вы полдня проведете, играя в угадайку, пока будете наклеивать ярлыки на уже

проложенные кабели. Это мы знаем по собственному опыту.

**6.1.9. Связь**

Системным администраторам, работающим в вычислительном центре, часто

приходится общаться с пользователями, другими системными администратора-

ми (работающими за пределами центра) и поставщиками. Системным админис-

траторам может потребоваться кто-то, кто станет проверять, была ли решена

проблема, кто будет следить за работоспособностью служб или заниматься поис-

ком информации, оборудования и кадров. Иногда поставщики предпочитают

поддерживать связь с сотрудником, проводящим процедуру диагностики.

Рекомендуем обеспечить какой-либо способ связи. Некоторые системные адми-

нистраторы пользуются рациями или мобильными телефонами, так как многие

из них редко находятся за своим рабочим столом. Все большую популярность

приобретают мобильные телефоны с режимом нажми-и-говори (push-to-talk).

Однако рации и мобильные телефоны могут плохо работать в вычислительных

центрах из-за высокого уровня электромагнитных помех или (в некоторых

компаниях) из-за экранирования от радиопомех. В некоторых случаях простые

телефонные аппараты работают намного лучше. В таком случае рекомендуем

установить телефон у края каждого ряда стоек. А шнур должен быть достаточ-

но длинным, чтобы системный администратор мог в случае необходимости

пройти весь ряд с трубкой в руке

Определенные задачи можно выполнить исключительно с консоли компьютера.

Консольные серверы и переключатели КВМ позволяют получить удаленный доступ

к компьютерной консоли.

Консольные серверы бывают двух основных видов. В одних есть переключатели,

позволяющие подключить одну клавиатуру, видеомонитор и мышь (КВМ)

к портам клавиатуры, монитора и мыши нескольких машин. Старайтесь созда-

вать подобных точек как можно меньше и располагать их в наиболее эргоно-

мичных местах вычислительного центра.

Другой тип – консольные серверы для машин, которые поддерживают последо-

вательные консоли. К последовательному порту каждой такой машины подклю-

чается последовательное устройство, например терминальный сервер. Эти тер-

минальные серверы подключены к сети. Как правило, определенная программа

на центральном сервере все их контролирует и распределяет консоли машин по именам при аутентификации и определении уровня

контроля доступа. Преимущество этой системы состоит в том, что системный

администратор, пройдя аутентификацию, может получить доступ к консоли

системы откуда угодно: с рабочего места, из дома или даже с дороги.

**6.1.11. Рабочее место**

Еще один важный аспект любого вычислительного центра – легкий доступ

к рабочему месту, оборудованному достаточным количеством розеток и анти-

статической поверхностью, где системный администратор может выполнять

работу с машинами: устанавливать память, диски и процессоры на новое обо-

рудование перед его установкой или решать ту или иную аппаратную проблему.

В идеале рабочее место должно находиться рядом с вычислительным центром,

но не внутри него. Таким образом, оно не будет использоваться в качестве вре-

менной стойки и не станет создавать беспорядок в вычислительном центре.

Людям вредно проводить в вычислительном центре весь рабочий день.

В таком центре поддерживается идеальная температура и влажность

воздуха для компьютеров, но не для людей. В холодном помещении ра-

ботать вредно для здоровья, а проводить много времени с источниками

такого шума может быть даже опасно.

Кроме того, это вредно и для систем. Люди выделяют тепло. Каждому

человеку, находящемуся в вычислительном центре, требуется дополни-

тельно 600 БТЕ охлаждения. А это дополнительная нагрузка в 600 БТЕ

на систему охлаждения и систему энергоснабжения.

Системным администраторам необходим постоянный доступ к справоч-

ным материалам, эргономичным рабочим столам и т. д. Необходима

среда, максимально повышающая производительность. Системы удален-

ного доступа некогда были достаточно редкими, но сейчас они стали не-

дорогими и приобрести их очень просто.

Люди должны заходить в вычислительный центр исключительно для

выполнения задач, которые невозможно осуществить каким-либо другим

способом.

**6.1.12. Инструменты и запасы**

В крупном отделе системного администрирования приходится постоянно отсле-

живать наличие запасных частей и материалов. Сами системные администра-

торы должны следить за тем, чтобы нужные запасы не заканчивались, а если

заканчивались, то редко и ненадолго. Системный администратор, заметивший,

что в вычислительном центре заканчиваются определенные запасы или пред-

стоит использование большого количества тех или иных запасов, должен сооб-

щить об этом сотруднику, который несет ответственность за отслеживание за-

пасных деталей и материалов.

Небольшие предметы, такие как винты и терминаторы кабелей, необходимо хранить в контейнерах или небольших ящиках. Во многих компаниях предпочитают выделять отдельное помещение для хранения запасных частей, обеспечивая легкий доступ из этого помещения к информационному центру. Идеально для этих целей подходит рабочая комната рядом с информационным центром. Хранение запасных деталей в отдельной комнате может защитить их от события, из-за которого «погибают» используемые детали в вычислительном центре. Крупные предметы, такие как запасные машины, всегда должны храниться в отдельном помещении, чтобы не занимать ценное пространство в вычислительном центре. Ценные запасные части, такие как память и процессоры, как правило, хранятся в запирающемся шкафу.

**6.1.13. Места для хранения**

Простой, дешевый и эффективный способ упростить жизнь людям, работающим

в вычислительном центре, – распределить место для хранения переносимых

объектов. Для инструментов, хранящихся в тележке, должны быть точно рас-

пределенные и маркированные места. А для самих тележек должны быть мар-

кированные парковочные места, где тележки будут стоять, когда ими никто не

пользуется.

***6.2. Тонкости***

**6.2.1. Повышенная избыточность**

Если от вас требуется особо высокая готовность, вам, среди прочего, необходи-

мо распланировать избыточность систем электропитания и отопления, венти-

ляции и кондиционирования воздуха. Для этого вам необходимо разбираться

в коммутационных схемах и строительных чертежах. Вы должны проконсуль-

тироваться с конструкторами системы, чтобы удостовериться, что вы усвоили

малейшие детали, ведь именно малейшие детали могут все испортить, если их

упустить.

Что касается систем отопления, вентиляции и кондиционирования воздуха,

возможно, стоит предусмотреть наличие двух независимых систем, работаю-

щих параллельно. При отказе одной из них вторая тут же примет на себя всю

нагрузку. Каждая из этих систем должна быть способна охладить все помеще-

ние в одиночку.

В вычислительном центре, возможно, стоит предусмотреть несколько источни-

ков электропитания. Может быть, вам понадобится переменный и постоянный

ток, но, возможно, вам также понадобится два разных источника переменного

тока для оборудования, которое будет подключаться к двум источникам или

для разделения питания пар избыточных машин. Если оборудование подклю-

чается к нескольким блокам питания, стоит использовать для них разные ис-

точники питания.

**6.2.2. Больше пространства**

Если площадь позволяет, проходы в компьютерном зале рекомендуется сделать

шире, чем того требуют правила техники безопасности, чтобы можно было

спокойно перемещать оборудование.

***6.3. Заключение***

Чтобы вычислительный центр работал правильно, необходимо при его плани-

ровании учитывать множество факторов. Но, что бы вы ни планировали, буду-

щий вычислительный центр будет работать долгое время, поэтому лучше с са-

мого начала все сделать правильно. Вычислительный центр, который был

плохо спроектирован, которому не хватает энергоснабжения или охлаждения,

может стать источником множества проблем.

Системы энергоснабжения, кондиционирования и пожаротушения являются

практически обязательными ключевыми компонентами вычислительного цен-

тра. Их отказ может значительно повлиять на его работу.

Еще один ключевой аспект, который необходимо продумать заранее, – доступ

в центр для доставки и перемещения оборудования. А где доступ – там и систе-

ма безопасности. Вычислительный центр – критически важное помещение,

в котором находится множество ценного оборудования. Это должно быть отра-

жено в политике получения доступа к центру, но при этом выбранная система

должна быть удобной для людей, которым постоянно приходится работать

с оборудованием.

Создание хорошего, надежного вычислительного центра требует немало вложе-

ний, но все они быстро окупаются. При этом можно внедрить простые, недорогие

решения, которые позволят создать более приятную атмосферу в вычислительном

центре, а также повысить эффективность его работы. Ярлыки на всем обору-

довании и строго отведенные места для передвижных устройств не требуют боль-

ших материальных затрат, но дают массу преимуществ, позволяя сэкономить

время. Прислушайтесь к советам системных администраторов. У каждого из них

есть свое мнение по поводу того или иного вопроса. Внедрите решения, которые

они считают положительными, и усвойте уроки из их негативного опыта.

Если площадь позволяет, лучше сделать вычислительный центр просторнее,

чем это необходимо. А если позволяют финансы и существуют очень жесткие

требования к надежности, можно многого добиться с помощью избыточных

систем энергоснабжения и кондиционирования, которые повысят надежность

работы центра.