Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ №2(33)/1997

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Интервью Председателя Гостехкомиссии России Юрия Алексеевича Яшина

Материал предоставлен пресс-службой Гостехкомиссии России

— Юрий Алексеевич, что представляет собой Гостехкомиссия России: особого рода спецслужбу, орган государственного управления или временную комиссию для решения отдельного вопроса?

— Сразу надо сказать, что Государственная техническая комиссия при Президенте Российской Федерации не является спецслужбой в том смысле, как это принято понимать. Она создана Указом Президента Российской Федерации от 5 января 1992 г. № 9 как постоянно действующий орган государственного управления и несет ответственность за обеспечение защиты информации, составляющей служебную и государственную тайну, от ее утечки по техническим каналам и за противодействие техническим разведкам на территории Российской Федерации.

Но главное, что характеризует Гостехкомиссию России, это то, что она является коллегиальным органом, в состав которого входят министры, председатели государственных комитетов, первые заместители (заместители) этих руководителей. Всего 23 человека. Принятые Гостехкомиссией решения не являются прерогативой какого-либо ведомства, в них учитываются, прежде всего, интересы государства, общества и личности. Этим полностью исключается монополия в решении важнейших вопросов обеспечения национальной безопасности.

Непосредственное подчинение Президенту Российской Федерации обеспечивает независимость Гостехкомиссии России от региональных, ведомственных и корпоративных влияний, гарантирует соответствие ее деятельности высшим государственным интересам. Решения Гостехкомиссии России являются обязательными для исполнения всеми органами государственного управления, предприятиями, организациями и учреждениями независимо от их организационно-правовой формы и формы собственности, которые по роду своей деятельности обладают информацией, составляющей государственную или служебную тайну.

— В чем заключаются главные задачи, решаемые Гостехкомиссией России?

— Гостехкомиссия России возглавляет Государственную систему защиты информации от технических разведок, решает целый комплекс важных государственных задач, среди которых большое значение имеет, например, проведение единой технической политики и координация работ в области защиты информации, осуществление контроля эффективности принимаемых мер защиты. Одной из главных задач Гостехкомиссии России является разработка нормативной правовой и нормативно-методической базы в области защиты информации и противодействия техническим разведкам. Большое внимание уделяется созданию и методическому обеспечению системы подготовки кадров по вопросам комплексной защиты информации, международному сотрудничеству в этой сфере.

— Каковы основные итоги работы Гостехкомиссии России?

— Основным итогом деятельности Гостехкомиссии является, несомненно, создание в нашей стране Государственной системы защиты информации от технических разведок и от ее утечки по техническим каналам. В составе этой системы действуют соответствующие

структурные подразделения федеральных и многих региональных органов государственной власти, предприятий, учреждений и организаций. Важным итогом нашей пятилетней работы стало создание системы подготовки специалистов в области защиты государственной тайны и информации.

Созданы и успешно развиваются системы лицензирования деятельности предприятий и организаций на право оказания услуг в области защиты информации и сертификации технических средств защиты информации.

Идея международного сотрудничества России со странами СНГ в области защиты информации нашла свое воплощение в заключенных межправительственных соглашениях с республиками Казахстан и Украина. Завершается подготовка аналогичного соглашения с Белоруссией.

Понимая важность интеграции усилий по совершенствованию методов и способов обеспечения защиты информации, Гостехкомиссия России вышла с предложением об организации и проведении в апреле 1997 г. международной конференции и выставки "Безопасность информации". Правительство Российской Федерации поддержало нашу инициативу и определило председателем организационного комитета. конференции заместителя Председателя Правительства Лобова О.И.

И самое главное. Проведение систематического контроля состояния защиты информации в министерствах, ведомствах, на предприятиях, в учреждениях и организациях позволяет проводить анализ эффективности принимаемых мер защиты, готовить предложения и их реализовывать, определять пути совершенствования системы защиты информации.

В качестве примера можно привести один из самых "свежих" — проблема массового применения и в госсекторе, и коммерсантами дешевых миниАТС импортного производства. В ходе проверок, проведенных специалистами Гостехкомиссии России в органах федерального и регионального управления Российской Федерации, а также на предприятиях и организациях, выполняющих оборонные заказы и осуществляющих государственные поставки, было выявлено, что указанными организациями производится закупка и ввод в эксплуатацию цифровых АТС импортного производства.

Такие АТС продаются, в основном, по низким ценам, что обуславливает их привлекательность для потребителя.

Проведенный специалистами Гостехкомиссии России анализ показал, что в случае их применения существует возможность дистанционного управления ими ("полицейские режимы"), в том числе для прослушивания помещений, блокирования работы линий связи, что приводит к разрушению системы управления.

По итогам этой работы мы направили соответствующие письма с предостережением руководителям министерств и ведомств. И результаты этого предостережения не замедлили сказаться. При покупке и определении места применения этих АТС руководители начали оценивать не только сиюминутную выгоду, но и работу системы управления с учетом критерия "стоимость — эффективность".

— Как Вы оцениваете перспективы защиты информации в России в XXI веке?

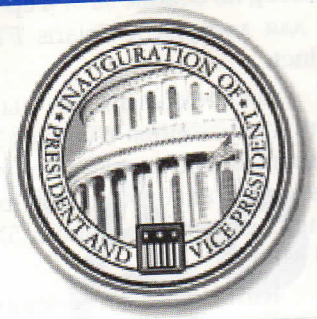
— Конец XX века показал, что информационный ресурс становится главным богатством как страны в целом, так и отдельного предприятия, организации любой формы собственности. Уверен, в новом столетии проблемы защиты информации станут во многом еще более актуальными для безопасности общества, государства и личности. Но, полагаю, сегодня общественность в большей степени интересуют не концептуальные проблемы будущего, а практические перспективы на ближайшее будущее, что делается и надо сделать чтобы заложить крепкий фундамент работы по защите информации в XXI веке.

В практической работе по обеспечению защиты информации в XXI веке именно сейчас нам еще очень многое предстоит сделать. Так, настоятельно требует скорейшей практической реализации Государственная программа обеспечения защиты государственной тайны в Российской Федерации. Требует дальнейшего наращивания законодательная база защиты информации. Острая потребность ощущается в законодательных актах по банковской и коммерческой тайнам, персональным данным, военно-техническому сотрудничеству с иностранными государствами. Эти, как и другие подобные законы, нацеленные на дальнейшее урегулирование информационных отношений в обществе и государстве, напрямую влияют на процесс демократизации нашей страны, обеспечение безопасности государства, законных прав его граждан

На законодательном уровне требуют уточнения и конкретизации с учетом новых условий цели, задачи и организационные основы защиты информации от утечки по техническим каналам и противодействия техническим разведкам. Проект Закона Российской Федерации "О защите информации от утечки по техническим каналам и противодействии техническим разведкам" подготовлен по запросу Комитета по безопасности Государственной Думы Федерального Собрания и представлен в Комитет.

Важным перспективным направлением деятельности Гостехкомиссии России является дальнейшее развитие сотрудничества со странами СНГ. Здесь на повестке дня — координация национальных законодательств в сфере защиты информации на базе уже принятого "Рекомендательного законодательного акта о принципах правового регулирования информационных отношений в государствах — участниках Межпарламентской ассамблеи".

НОВОСТИ ИНТЕРНЕТ



Sun освещает инаугурацию

20 января 1997 года по сети Интернет транслировалась процедура инаугурации президента Соединенных Штатов Вильяма Джеферсона Клинтона (адрес Web-сервера http://www.inaugural97.org). В создании этого Web-сервера заметное место принадлежит компании Sun Microsystems, которая, располагая богатым опытом сетевых решений, предоставила серверы и программное обеспечение на языке Java.

Собственно Web-сервер был сформирован компанией KPE, для которой создание Интернет-приложений является основным видом деятельности. При трансляции "живых" аудио- и видеоизображений использовались рабочие станции Sun Ultra, а для подготовки звукового сопровождения — язык Java.

О значении Web-трансляции вице-президент компании Sun Microsystems по маркетингу Анил Гадре сказал следующее: "Участвуя в трансляции инаугурационной церемонии, Sun, несомненно, делает свой вклад в историю. Интернет уже зарекомендовал себя как эффективное средство сближения правительства с народом. Трансляция инаугурации по сети стала еще одним замечательным актом, в котором раскрываются возможности Интернет для каждого гражданина. Интернет сокращает расстояние до событий, влияющих на жизнь общества. Мы считаем также, что трансляция инаугурации предоставила превосходный шанс наглядно продемонстрировать потенциал языка Java."

Очередной рекордный квартал Sun Microsystems

15 января 1997 года компания Sun Microsystems опубликовала результаты своей деятельности во втором квартале 1997 финансового года, закончившемся 29 декабря. За этот период доход компании оказался рекордным, он составил 2 миллиарда 82 миллиона долларов, что на 19% выше, чем во втором квартале 1996 финансового года. Чистая прибыль возросла в еще большей пропорции — на 41% и составила 178.3 миллионов долларов. Отмечается также рост во втором квартале курса акций Sun Microsystems на 41%.

Экономические достижения своей компании президент Sun Microsystems Скотт МакНили объясняет тем, что продукция с торговыми марками UltraSPARC, Solaris и Java получила признание во всем мире. "Наши серверы и высокопроизводительные станции пользуются устойчивым спросом, поскольку они соответствуют реальным пользовательским нуждам. Они обладают необходимыми масштабируемостью, надежностью и производительностью. Успеху Sun на рынке способствует сотрудничество с такими ведущими производителями программных продуктов, как Oracle, SAP, Informix, PeopleSoft и Sybase. За двадцать лет своей деятельности Sun закрепил за собой образ компании, предлагающей более эффективные и прогрессивные решения по сравнению с теми, что реализуются на персональных компьютерах и мэйнфреймах."

Вице-президент Sun по финансам Михаэл Лехман дал следующий комментарий: "Прогресс в текущем финансовом году — логическое продолжение наших финансовых достижений в прошлом. Sun выигрывает в таких областях, как крупные корпоративные системы Интранет, Интернет и Экстранет. Именно в этих областях особое преимущество компании дает давнишняя приверженность девизу "Сеть — это компьютер". Сегодня мы получаем отдачу от инвестиций, сделанных в исследования и разработки, в инфраструктуры продажи и поддержки".

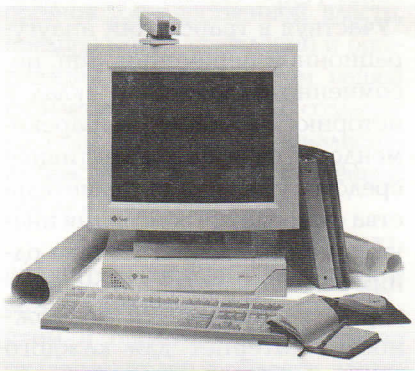
Sun усиливает свои позиции на рынке Unix рабочих станций

По предварительным данным, опубликованным аналитиком рынка компанией IDC, в 1996 году Sun Microsystems, продав 292 000 рабочих станций на базе ОС Unix, упрочила свое лидирующее положение в этом сегменте рынка. Число рабочих станций, проданных Sun, составляет 41% от общего объема продаж (в 1995 году — 38.1%). Это в два раза больше, чем у ближайшего конкурента Hewlett-Packard и больше суммарного объем продаж таких компаний, как Hewlett-Packard, Silicon Graphics, IBM и DEC. В стоимостном выражении Sun принадлежит 32% рынка, а полученная прибыль от поставки на рынок рабочих станций составляет 3.7 миллиарда долларов, то есть почти половину всей прибыли компании.

Доля Sun на рынке увеличилась главным образом за счет падения спроса на продукцию компании Hewlett-Packard, объем которой по данным IDC сократился с 154220 единиц в 1995 году до 134995 единиц в 1996 году (21.7% против 19%). Digital Equipment также сократила объемы поставок, в то время как Silicon Graphics и IBM сохраняют свои позиции.

Игорь Дорошин, Владимир Галатенко

SPARCstation 5 Model 170 – в два раза быстрее и на 30% дешевле



Новая модель самой популярной UNIX рабочей станции по цене и возможностям наиболее привлекательна в качестве рабочего места для разработки программного обеспечения, для самых разнообразных систем автоматизированного проектирования. Она полностью подготовлена для работы в сети. Производительность по сравнению с моделью SPARCstation 5 Model 110 увеличена в два раза.

В рабочей станции модели 170 использован процессор TurboSPARC, выпускаемый Fujitsu Microelectronics. Станция комплектуется пакетом Internet Access PlusPack, куда входят Netscape Navigator Gold 3.0 и собственные приложения от Sun: Java Virtual Machine для выполнения аплетов на Java, навигатор на основе Java и средства для доступа к Solaris FTP и Telnet.

Для тех, кто хочет выполнять приложения Windows 3.1 в родных кодах, может быть установлена дополнительная плата SunPC с сопроцессором 5X86, 133 МГц.

Комплект, включающий 17-дюймовый монитор, 256 Кб кэш, графическую плату TurboGX, 32 Мб ОЗУ, 2.1 Гб НЖМД и ОС Solaris, стоит $4,695. Плата SunPC увеличивает стоимость на 300 долларов.

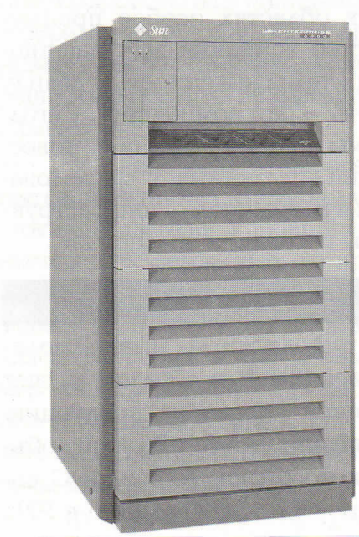
Новые процессорные модули для Ultra Enterprise

14 января компания Sun Microsystems объявила о начале поставки модулей с процессором UltraSPARC с тактовой частотой 250 МГц. Модули предназначены для серверов Ultra Enterprise, они обеспечивают повышение производительности на 50% по сравнению с предшественниками на процессорах с тактовой частотой 167 МГц.

Эти модули сохраняют полную бинарную совместимость, приложения под ОС Solaris могут работать на них без каких-либо изменений. Выпуск новых процессорных модулей подтверждает продекларированную компанией политику, в соответствии с которой гарантируется повышение вычислительной мощности при сохранении инвестиций пользователей. В ближайшие недели ожидаются объявления о новых процессорных модулях повышенной производительности для других моделей компьютеров.

Объявленные процессорные модули поддерживают следующие модели серверов Ultra Enterprise: 3000, 4000, 5000 и 6000. Цена нового модуля составляет 16 тысяч долларов, цена модернизации старого модуля – 12 тысяч долларов.

Ultra Enterprise 6000 – лидер по тестам TPC-C



20-процессорный сервер Ultra Enterprise 6000, оснащенный процессорными модулями с тактовой частотой 250 МГц и кэш-памятью 1 Мб, работая под управлением ОС Solaris 2.5.1, продемонстрировал рекордные результаты на тесте TPC-C.

Результаты превосходят известные данные для систем с симметричной мультипроцессорной архитектурой (SMP), к тому же показано и великолепное соотношение цена/производительность. Испытание проводилось с использованием СУБД Sybase SQL Server 11.0.3. Опубликованы следующие показатели:

- число транзакций TPC-C в минуту (tpmC) – 18,438.70
- соотношение цена/производительность – 139 долларов на tpmC.

Эти значения выше, чем у аналогов (SMP-систем с одним узлом). Так, показатели серверов DEC превзойдены на 30%, HP – 50% и IBM – более чем на 200%.

Показательно, что сервер Sun показал результаты лучше, чем у кластера HP EPS30 (4 узла и 48 процессоров) и у кластера IBM RS/6000 J40 (2 узла и 32 процессора). Ultra Enterprise 6000 превосходит эти системы по обоим показателям: по производительности, соответственно, на 3% и 29%, а по соотношению цена/производительность – на 181% и 60%. Уровень производительности, который раньше был возможен только на кластерных конфигурациях, для пользователя оборачивается возможностью поддерживать единый унифицированный образ базы данных, что снижает стоимость и сложность решений.

Владимир Галатенко,
Игорь Дорошин

Доступность

как элемент информационной безопасности

Содержание

1. Введение

В соответствии с общепринятым современным подходом (см., например, [1]), выделяют следующие аспекты информационной безопасности:

- доступность (возможность за приемлемое время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного ознакомления).

Информационные системы создаются (приобретаются) для получения определенных информационных услуг (сервисов). Если по тем или иным причинам получение этих услуг пользователями становится невозможным, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как существенный элемент информационной безопасности.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления — производством, транспортом и т.п. Так, по утверждениям специалистов, на химическом заводе человек-оператор способен воспринимать менее 1% информации о ходе производственного процесса. В таких условиях выход из строя системы автоматического управления чреват серьезной аварией. Внешне менее драматичные, но также весьма неприятные последствия — и материальные, и моральные — может иметь длительная недоступность информационных услуг,

которыми пользуется большое количество людей. Имеются в виду продажа железнодорожных и авиабилетов, банковские услуги и т.п. Выход из строя информационной системы Центрального банка способен поставить под угрозу национальные интересы. Несомненно, читатели сами без труда умножат число подобных примеров.

Важность доступности как аспекта информационной безопасности находится в разительном противоречии с тем вниманием, которое уделяют данному аспекту потенциально заинтересованные стороны. Если вопросы защиты от несанкционированного доступа (то есть обеспечение конфиденциальности и целостности информации) курирует Гостехкомиссия России, а криптографические средства (что опять—таки связано с обеспечением конфиденциальности и целостности) — ФАПСИ, то доступность пока — сирота. Явно не хватает и современных исследований по данной теме, посвященных конфигурациям клиент/сервер и применимых на практике, в то время как простор для исследований выглядит практически безграничным, а их важность невозможно переоценить (см. [2, 3]). Наконец, забота владельцев информационных систем о доступности в лучшем случае сводится к покупке компьютеров "белой", а не "желтой" или "красной" сборки, что, мягко говоря, недостаточно.

В эпоху господства мэйнфреймов удалось создать инфраструктуру, способную поддержать по существу любой наперед заданный уровень доступности на всем протяжении жизненного цикла информационной системы. Эта инфраструктура включала в себя как технические, так и операционные регуляторы (обучение персонала и пользователей, проведение работ в соответствии с апробированными регламентами и т.п.). При переходе к технологии клиент/сервер инфраструктура обеспечения доступности во многом оказалась утраченной, однако важность данной проблемы не только не уменьшилась, но, напротив, существенно возросла в силу повсеместного распространения вычислительной техники. Перед государственными и коммерческими организациями встала задача соединения упорядоченности и регламентированности, присущих миру мэйнфреймов, с открытостью и гибкостью систем, построенных в архитектуре клиент/сервер.

Такова ситуация на Западе. У российских компаний заботы несколько иные. Подавляющее большинство молодых организаций "избежали" мэйнфреймов, а вместе с ними и присущей им компьютерной культуры. Нашим организациям в плане обеспечения доступности приходится начинать даже не с нуля, а из отрицательной зоны, созданной "персоналочными" привычками (компьютер, стоящий на моем рабочем месте — мой, информация на нем — моя, я его как хочу, так и конфигурирую, и т.д.). Мысль об элементарном наведении порядка, конечно, не нова и обычно воспринимается без энтузиазма, но без подобной отправной точки, увы, не обойтись.

Цель настоящей работы — привлечь внимание к задаче обеспечения доступности информационных услуг и предложить (а в некоторых случаях — просто напомнить) возможные подходы к ее решению.

2. Постановка задачи

Информационная система предоставляет своим пользователям определенный набор услуг (сервисов). Говорят, что обеспечен нужный уровень доступности этих сервисов, если следующие показатели находятся в заданных пределах:

- Эффективность услуг. Эффективность услуги определяется в терминах максимального времени обслуживания запроса, количества поддерживаемых пользователей и т.п. Требуется, чтобы эффективность не опускалась ниже заранее установленного порога.
- Время недоступности. Если эффективность информационной услуги не удовлетворяет наложенным ограничениям, она (услига) считается недоступной. Требуется, чтобы максимальная продолжительность периода недоступности и суммарное время недоступности за некоторой период (месяц, год) не превышали заранее заданных пределов.

Коротко говоря, требуется, чтобы информационная система почти всегда работала с нужной эффективностью. Для некоторых критически важных систем (например, систем управления) время недоступности должно быть нулевым, без всяких "почти". В таком случае говорят о вероятности возникновения ситуации недоступности и требуют, чтобы эта вероятность не превышала заданной величины. Для решения данной задачи создавались и создаются специальные отказоустойчивые системы, стоимость которых, как правило, весьма высока.

К подавляющему большинству коммерческих систем предъявляются менее жесткие требования, и именно этот класс систем — системы высокой доступности — мы будем рассматривать в настоящей работе. Впрочем, современная деловая жизнь и здесь накладывает достаточно суровые ограничения, когда число обслуживаемых пользователей может измеряться тысячами, время ответа не должно превышать не-

скольких секунд, а время недоступности — нескольких часов в год.

Некомпьютерные информационные сервисы за время своего развития достигли чрезвычайно высокого уровня доступности. В таком городе, как Москва, телефонная связь работает без сбоев, так что даже с учетом диверсий среднее время неработоспособности среднестатистического телефонного аппарата не превышает нескольких минут в год. Доступность компьютерных систем и глобальных сетей на 2—3 порядка ниже. Если учесть, что сейчас коммерческие компьютерные решения проникают буквально во все области деятельности, целесообразно поставить задачу "дотягивания" доступности компьютерных сервисов до "телефонного" уровня, привычного для большинства людей.

Как всегда, когда речь идет об информационной безопасности, необходимо уточнить спектр рассматриваемых рисков. Мы будем придерживаться наиболее общей точки зрения, имея в виду следующие классы угроз:

- отказ пользователей — невозможность или нежелание пользователей взаимодействовать с информационной системой в силу неудобства последней, недостаточной квалификации пользователей, невозможности получения ими технической помощи и т.п.;
- внутренний отказ информационной системы — выход из строя аппаратного или программного компонента (компонентов) информационной системы в силу сбоя, технической неисправности или ошибки обслуживающего персонала; выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- отказ поддерживающей инфраструктуры — выход из строя энергоснабжения, связи, кондиционирования и т.п., повреждение или разрушение помещений (зданий), невозможность или нежелание обслуживающего персонала выполнять свои функции.

Подчеркнем, что обслуживающий персонал и пользователей следует считать частью информационной системы, так как их действия впрямую влияют на доступность. Отметим также, что спектр рассматриваемых рисков предельно широк — от появления одного лишнего пользователя до разрушения здания или группы зданий, в которых установлена информационная система.

Задачу обеспечения доступности необходима решать для современных конфигураций, построенных в технологии клиент/сервер. Это означает, что в защите нуждается вся цепочка от пользователей (возможно, удаленных) до критически важных серверов.

В заключение раздела — несколько слов о терминологии. Обычно в литературе по теории надежности вместо доступности говорят о готовности (в том числе о высокой готовности). Мы предпочли термин "доступность", чтобы подчеркнуть, что информационный сервис должен быть не просто "готов" сам по себе, но доступен для своих пользователей в условиях, когда ситуации недоступности могут вызываться причинами, на первый взгляд не имеющими прямого отношения к сервису (пример — отсутствие консультационного обслуживания).

Далее, вместо времени недоступности обычно говорят о коэффициенте готовности. Нам хотелось обратить внимание читателей на два показателя — длительность однократного простоя и суммарную продолжительность простоев, поэтому мы предпочли термин "время недоступности" как более емкий.

Наконец, вместо живучести употребляют термин "восстанавливаемость". На наш взгляд, при этом затушевываются различия между способностью сервиса продолжать работу, несмотря на отказ, и средствами восстановления функциональности отказавших компонентов. Нам это различие представляется важным, поэтому мы решились на использование "ненаучного", но точно отражающего суть дела слова "живучесть".

Мы надеемся, что отмеченные терминологические особенности не помешают восприятию данной работы.

3. Основные понятия

3.1. Безотказность, живучесть, обслуживаемость

В соответствии с ГОСТ 27.002, под отказом понимается событие, заключающееся в нарушении работоспособного состояния изделия. В контексте данной работы изделие — это информационная система или ее компонент.

В простейшем случае можно считать, что отказы любого компонента составного изделия ведут к общему отказу, а распределение отказов во времени представляет собой простой пуассоновский поток событий (см., например, [4]). В таком случае вводят понятие интенсивности отказов и среднего времени наработки на отказ, которые связаны между собой соотношением

$$T_i = \frac{1}{\lambda_i}$$

где i — номер компонента,
λ_i — интенсивность отказов,
T_i — среднее время наработки на отказ.

Интенсивности отказов независимых компонентов складываются:

$$\lambda = \lambda_1 + \lambda_2 + \ldots + \lambda_n$$

а среднее время наработки на отказ для составного изделия задается соотношением

$$T=\frac{1}{\lambda}$$

Уже эти простейшие выкладки показывают, что если существует компонент, интенсивность отказов которого много больше, чем у остальных, то именно он определяет среднее время наработки на отказ всей информационной системы. Это является теоретическим обоснованием изречения "где тонко, там и рвется" и принципа первоочередного укрепления самого слабого звена.

Пуассоновская модель позволяет обосновать еще одно очень важное положение, состоящее в том, что эмпирический подход к построению систем высокой доступности не может быть реализован за приемлемое время. В работе [5] показано, что при традиционном цикле тестирования/отладки программной системы по оптимистическим оценкам каждое исправление ошибки приводит к экспоненциальному убыванию (примерно на половину десятичного порядка) интенсивности отказов. Отсюда следует, что для того, чтобы на опыте убедиться в достижении необходимого уровня доступности, независимо от применяемой технологии тестирования и отладки, приходится потратить время практически того же порядка, что и требуемое среднее время наработки на отказ. Например, для достижения среднего времени наработки на отказ 10^5 часов потребуется более $10^{4.5}$ часов, что составляет более трех лет. Значит, нужны иные методы построения систем высокой доступности, методы, действенность которых доказана аналитически или практически за пятьдесят лет развития вычислительной техники и программирования.

Пуассоновская модель применима в тех случаях, когда информационная система содержит одиночные точки отказа, то есть компоненты, выход которых из строя ведет к отказу всей системы. Для исследования систем с резервированием применяется иной формализм.

Будем считать (см. выше раздел "Постановка задачи"), что существует количественная мера эффективности предоставляемых изделием информационных услуг. В таком случае вводят понятия показателей эффективности отдельных элементов и эффективности функционирования всей сложной системы.

В качестве меры доступности можно принять вероятность приемлемости эффективности услуг, предоставляемых информационной системой, на всем протяжении рассматриваемого отрезка времени. Чем большим запасом эффективности располагает система, тем выше ее доступность. Очевидно, при наличии избыточности отказ компонента не обязательно приводит к отказу системы.

При наличии избыточности в конфигурации системы вероятность того, что в рассматриваемый промежуток времени эффективность информационных сервисов не опустится ниже допустимого предела, зависит не только от вероятности отказа компонентов, но и от времени, в течение которого они остаются неработоспособными, поскольку при этом суммарная эффективность падает и каждый следующий отказ может стать фатальным. Чтобы максимизировать доступность системы, необходимо минимизировать время неработоспособности каждого компонента. Кроме того, следует учитывать, что, вообще говоря, ремонтные работы могут потребовать понижения эффективности или даже временного отключения работоспособных компонентов; такого рода влияние также необходимо минимизировать.

Таким образом, мы видим, что доступность системы в общем случае достигается за счет применения трех групп мер, направленных на повышение:

- безотказности (под эти понимается минимизация вероятности возникновения какого-либо отказа);
- живучести (под этим понимается сохранение доступности системы несмотря на отказ каких-либо компонентов);
- обслуживаемости (под этим понимается минимизация времени неработоспособности отказавших компонентов, а также минимизация отрицательного влияния ремонтных работ на эффективность информационных сервисов).

Наряду с отказами можно рассматривать сбои — события, заключающиеся в кратковременном нарушении работоспособного состояния каких-либо компонентов информационной системы (типичные примеры — случайная ошибка четности при чтении из оперативной или долговременной памяти или опечатка пользователя при вводе команды). Очевидно, для распознавания и нейтрализации последствий сбоя нужна определенная избыточность, а соответствующие меры естественно отнести к мерам обеспечения живучести, что мы и будем делать в дальнейшем.

3.2. Живучесть и зоны риска

В соответствии с подходом клиент/сервер, информационную систему можно представить в виде графа сервисов, ребра в котором соответствуют отношению "сервис А непосредственно использует сервис В". На рис. 1 приведен один из возможных примеров подобного графа.

Пусть в результате осуществления некоторой угрозы из строя выводится подмножество сервисов S_1 (то есть эти сервисы в силу нанесенных повреждений становятся неработоспособными). Назовем S_1 зоной поражения.

В зону риска S мы будем включать все сервисы, эффективность которых при осуществлении уг-

Рис. 1. Граф сервисов, используемых одной из предоставляемых услуг.

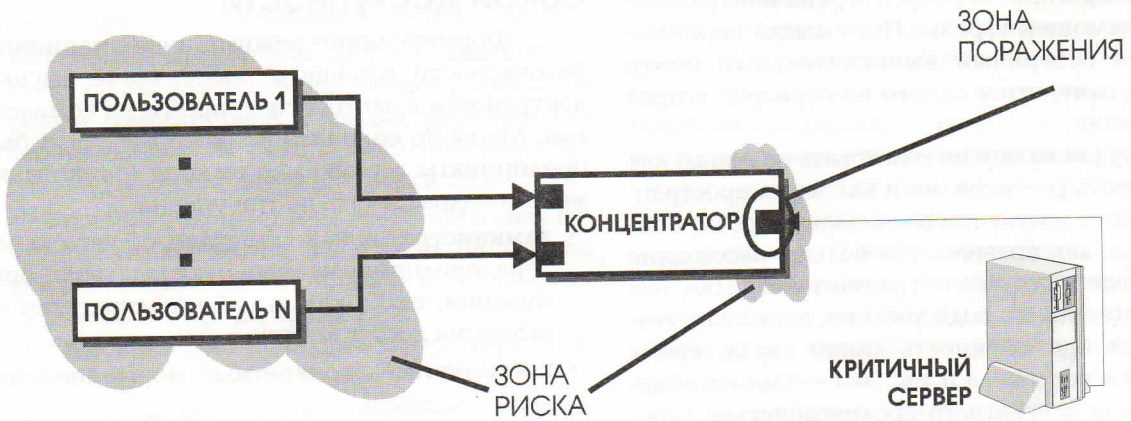


Рис. 2. Зона риска при поломке порта концентратора, обслуживающего критичный сервер, захватывает все рабочие места пользователей.

розы падает ниже допустимого предела. Очевидно, S_1 – подмножество S. S строго включает S_1, когда имеются сервисы, непосредственно не затрагиваемые угрозой, но критически зависящие от пораженных, то есть неспособные переключиться на использование эквивалентных услуг либо в силу отсутствия таковых, либо в силу невозможности доступа к ним. На рис. 2 приведен случай, когда зона поражения сводится к одному порту концентратора, обслуживающего критичный сервер, а зона риска захватывает все рабочие места пользователей.

Очевидно, чтобы система не содержала одиночных точек отказа, то есть оставалась живучей при осуществлении любой из рассматриваемых угроз, ни одна зона риска не должна включать в себя предоставляемые услуги. Нейтрализацию отказов нужно выполнять внутри системы, невидимым для пользователей образом, за счет размещения достаточного количества избыточных ресурсов. На рис. 3 приведена конфигурация, аналогичная рис. 2, с той лишь разницей, что сетевое соединение между сервером и концентратором продублировано. В

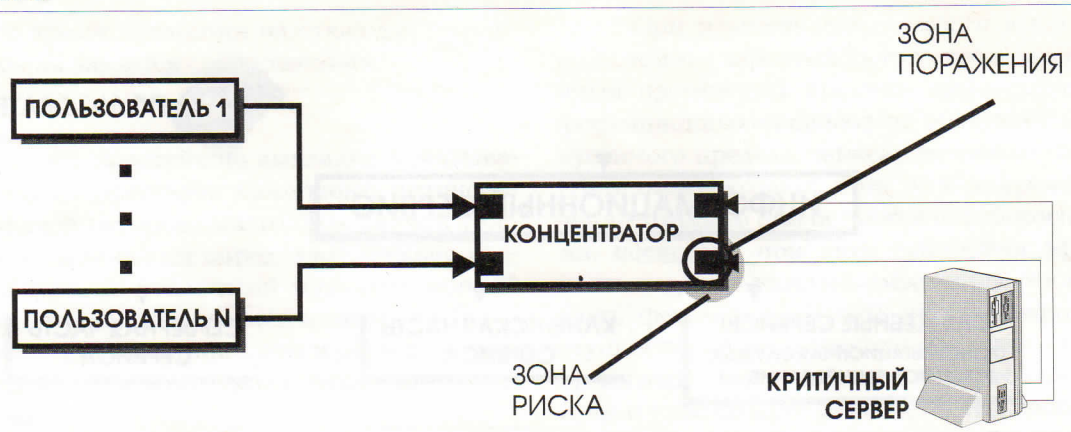


Рис. 3. Если соединение между сервером и концентратором продублировано, зоны поражения и риска при поломке порта концентратора совпадают.

результате зоны поражения и риска при поломке порта концентратора стали совпадать.

С другой стороны, естественно соразмерять меры по обеспечению живучести с рассматриваемыми угрозами. Когда рассматривается набор угроз, соответствующие им зоны поражения могут оказаться вложенными, так что живучесть по отношению к более серьезной угрозе автоматически влечет за собой и живучесть в более легких случаях. Следует учитывать, однако, что обычно стоимость переключения на резервные ресурсы растет вместе с ростом объема этих ресурсов. Значит, для наиболее вероятных угроз целесообразно минимизировать зону риска, даже если в принципе предусмотрена нейтрализация объемлющей угрозы. Нет смысла переключаться на резервный вычислительный центр только потому, что у одного из серверов сгорел блок питания.

Зону риска можно трактовать не только как совокупность ресурсов, но и как часть пространства, затрагиваемую при реализации угрозы. В таком случае, как правило, чем больше расстояние дублирующего ресурса от границ зоны риска, тем выше стоимость его поддержания, поскольку увеличивается протяженность линий связи, время переброски персонала и т.п. Это — еще один довод в пользу адекватного противодействия угрозам, который следует принимать во внимание при размещении избыточных ресурсов и, в частности, при организации резервных центров.

Введем еще одно понятие. Назовем зоной нейтрализации угрозы совокупность ресурсов, вовлеченных в нейтрализацию отказа, возникшего вследствие реализации угрозы. Имеются в виду ресурсы, режим работы которых в случае отказа меняется. Очевидно, зона риска является подмножеством зоны нейтрализации. Чем меньше разность между ними, тем экономнее данный механизм нейтрализации.

Все, что вне зоны нейтрализации, отказа "не чувствует" и может трактовать внутреннюю этой зоны как безотказную. Таким образом, в иерархически организованной системе грань между живучестью и обслуживаемостью с одной стороны и безотказностью с другой стороны, относительна. Целесообразно конструировать целостную информационную систему из компонентов, которые на верхнем уровне можно считать безотказными, а вопросы живучести и обслуживаемости решать в пределах каждого компонента. К этому замечанию мы вернемся в пункте "Обеспечение живучести" раздела "Программно — технические меры".

3.3. Уровни мер обеспечения высокой доступности

Формирование режима информационной безопасности вообще и обеспечение высокой доступности в частности — проблема комплексная. Меры по ее решению, которые могут быть предприняты в рамках отдельной организации, можно подразделить на три уровня:

- административный (действия общего характера, предпринимаемые руководством организации, такие как выработка стратегии повышения доступности);
- процедурный (конкретные меры, имеющие дело с людьми);
- программно — технический (конкретные технические меры).

Соответственно, выделяются три группы людей, от согласованных действий которых зависит обеспечение доступности. Последующее изложение строится с учетом этого разделения, так что каждый читатель при желании может ограничиться знакомством лишь с частью данной работы, соответствующей его служебным обязанностям. Внутри каждой части, там, где это возможно, мы будет подразделять рекомендуемые меры в соответствии с тем, направлены ли они на обеспечение безотказности, живучести или обслуживаемости.

4. Административные меры повышения доступности

Главная цель мер, предпринимаемых на административном уровне, состоит в том, чтобы сформировать программу работ в области повышения доступности информационных сервисов и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя фактическое состояние дел.

Первым этапом выработки подобной программы является анализ рисков.

4.1. Анализ рисков, связанных с покушением на доступность

В разделе "Постановка задачи" мы ввели следующие классы рисков:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие риски:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной культуры, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, невозможность получения справочной информации и т.п.).

Основными источниками внутренних отказов являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание выполнения обслуживающим персоналом и/или пользователями своих обязанностей (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Перечисленные угрозы носят весьма общий характер. Каждая организация может пополнить представленный список и/или конкретизировать в нем отдельные элементы. Так, для общедоступных сервисов (WWW – сервис и т.п.) существенную опасность представляют злонамеренные действия пользователей, выражающиеся в попытках монополизации ресурсов, эксплуатации ошибок в программном обеспечении и т.д.

4.2. Основные положения типовой программы повышения доступности

При разработке программы повышения доступности информационных сервисов рекомендуется реководствоваться следующими стратегическими принципами:

- апробированность всех процессов и составных частей информационной системы;
- унификация процессов и составных частей;
- управляемость процессов, контроль состояния частей;
- автоматизация процессов;
- модульность архитектуры;
- ориентация на простоту решений.

Программа повышения доступности должна предусматривать определение общего порядка работ, выделение ответственных за разработку документов, конкретизирующих программу, и за периодический пересмотр и уточнение документов, разработанных ранее. Главное, что должна обеспечить подобная программа, – это полнота и систематичность при проведении работ в области доступности. Сфера действия программы должна распространяться на все информационные цепочки – от от поддерживающей инфраструктуры до пользователей. Каждый процесс, каждая составная часть информационной системы (ИС) должны иметь ответственного на административном уровне, обладающего достаточными полномочиями для выделения соответствующих ресурсов и для воздействия на исполнителей. В этой связи представляется целесообразным предусмотреть составление карты информационной системы организации (в печатном и компьютерном представлениях), в которой фигурировали бы все объекты ИС, их состояние, связи между ними, процессы, ассоциируемые с объектами и связями. С помощью подобной карты удобно формулировать намечаемые меры, контролировать их исполнение, анализировать состояние ИС. Необходимо разработать регламент, гарантирующий поддержание карты в актуальном состоянии.

В программе должны найти отражение все три основные направления обеспечения доступности:

- безотказность;

- живучесть;
- обслуживаемость.

Очень важно придерживаться не статического, а динамического подхода к рассмотрению конфигурации ИС. Мы еще не раз будем возвращаться к понятию жизненного цикла системы, здесь же отметим следующее. Прежде чем вносить изменения в производственную конфигурацию ИС, их необходимо опробовать. Лучше всего это делать на имитационном стенде. В состав стенда должны входить все виды аппаратного и программного обеспечения, используемого в ИС, на нем должны быть воспроизводимы все ситуации, которые могут возникнуть в процессе эксплуатации ИС. Стенд используют как для отладки и опытной эксплуатации новых систем, так и для тренировки персонала. Целесообразно разработать и утвердить положение об имитационном стенде информационной системы организации.

4.2.1. Административные меры, направленные на обеспечение безотказности

Для обеспечения безотказной работы пользователей как компонентов информационной системы, необходимо прежде всего разработать и утвердить с согласия всех заинтересованных сторон порядок передачи приложений в эксплуатацию. Должна быть предусмотрена подготовка пользователей, разработка регламента их действий и практические занятия по отработке выполнения регламента. Второй момент состоит в автоматизации деятельности пользователей, в особенности в сложных ситуациях, таких как переключение на резервные ресурсы в случае выхода из строя основных. Третий момент — проактивное управление пользователями, анализ профиля их работы, выявление и устранение проблем, возможно, еще до того, как сами пользователи распознали их.

Для аппаратного и программного обеспечения ИС можно рекомендовать следующие меры обеспечения безотказности:

- Ориентация на апробированные продукты известных компаний, поддерживающие современные и перспективные стандарты, допускающие централизованное управление и контроль, простые в использовании и обслуживании (администрировании) с учетом уровня квалификации пользователей и обслуживающего персонала. Продукты должны предоставлять средства настройки на текущее и перспективное окружение и обладать свойством программируемости, то есть допускать определение регламентных и аварийных программных процедур, запускаемых без ручного вмешательства, в автоматическом режиме.
- Ориентация на надежных поставщиков, способных квалифицированно произвести установку, наладку и ввод в эксплуатацию новых продуктов, обучение и консультирование пользователей и обслуживающего персонала, качественное и своевременное проведение регламентных работ.
- Принятие решения о разработке и внедрении регламентов эксплуатации всех компонентов ИС, унификация регламентов.
- Унификация программных и аппаратных конфигураций, в том числе клиентских. Ориентация на модульность архитектуры ИС. Разнородную систему с многочисленными, нестандартными интерфейсами между составными частями очень сложно эксплуатировать, модифицировать, не допуская при этом ошибок. На рубеже 1960—70 годов кризис программирования, вызванный нарастанием сложности разрабатываемых систем, вызвал к жизни структурированный подход. Сейчас нечто подобное происходит с информационными системами в целом. Целесообразно в этой связи вспомнить об уроках истории, перечитать труды Дейкстры и Хоара.
- Проактивный подход к управлению информационной системой, ориентированный на раннее выявление и устранение проблем. Подобное управление включает в себя не только сбор, но и регулярный анализ данных о работе ИС. Следует разработать и утвердить порядок такого анализа, назначить ответственных за выбор и периодический пересмотр параметров, превышение которых требует вмешательства в работу ИС, ее переконфигурирование или наращивание. Проактивное управление — основной инструмент борьбы с замедлением работы компонентов ИС, какими бы причинами это замедление ни вызывалось. Проактивное управление должно охватывать не только чисто компьютерные компоненты, но и пользователей, а также параметры окружающей среды, такие как температура и влажность в серверной комнате.

4.2.2. Административные меры, направленные на обеспечение живучести

Основным средством повышения живучести является внесение избыточности в конфигурацию аппаратных и программных средств, поддерживающей инфраструктуры и персонала, резервирование технических средств и тиражирование информационных ресурсов (программ и данных).

Меры по обеспечению живучести можно подразделить на локальные и распределенные. Локальные меры направлены на достижение живучести отдельных компьютерных систем или их аппаратных и программных компонентов в первую очередь с целью нейтрализации внутренних отказов ИС. Типичные примеры подобных мер — использование кластерных конфигураций в качестве платформы серверов СУБД или горячее резервирование активного сетевого оборудования с автоматическим переключением на резерв.

Если в число рассматриваемых рисков входят серьезные аварии поддерживающей инфраструктуры, приводящие к полному выхода из строя производственной площадки организации, следует предусмотреть распределенные меры обеспечения

живучести, такие как создание или аренда резервного вычислительного центра. При этом, помимо дублирования и/или тиражирования ресурсов, необходимо предусмотреть средства автоматического или быстрого ручного реконфигурирования компонентов ИС, чтобы переключиться с основной площадки на резервную. В этой связи важное значение имеет разработка регламента работы резервного вычислительного центра (РВЦ) в штатном режиме и порядка переключения с основной площадки на РВЦ.

Ресурсы, размещаемые в РВЦ, могут использоваться двояко:

- исключительно как резерв;
- как дополнительный ресурс, вовлеченный в работу в штатном режиме.

Второй вариант предпочтительнее, хотя его осуществление и связано с определенными техническими трудностями.

Политика обеспечения доступности должна предусматривать практическую отработку процедуры переключения на РВЦ. В первую очередь следует отработать действия персонала, проверить действенность технических решений. Кроме того, целесообразно проводить практические занятия и с пользователями.

4.2.3. Административные меры, направленные на обеспечение обслуживаемости

Меры по обеспечению обслуживаемости направлены на снижение сроков диагностирования и устранения отказов. Для достижения обслуживаемости рекомендуются следующие меры:

- Ориентация на построение информационной системы из унифицированных компонентов с целью упрощения замены отказавших частей.
- Ориентация на решения, допускающие выведение из эксплуатации и замену отказавших компонентов в "горячем" режиме.
- Ориентация на организации, предоставляющих качественное и оперативное сервисное обслуживание.
- Заблаговременная подготовка комплекса мер, связанных с реагированием на нарушения доступности. Разработка регламента выполнения ремонтных работ.
- Заблаговременное планирование восстановительных работ, подготовка детального описания действий по принятию решения о полном или частичном переключении на резервные мощности, по осуществлению переключения, работы на резервных мощностях и возврата к нормальному режиму работы.
- Принятие решения о теоретической и практической подготовке персонала к действиям в процессе реагирования на нарушения доступности и во время восстановительных работ. Выделение для этой цели соответствующих ресурсов.
- Организация консультационной службы для пользователей (обслуживаемость пользователей). Разработка и утверждение регламента работы консультационной службы, внедрение программных систем для работы этой службы, обеспечение достаточной пропускной способности каналов связи с пользователями, в том числе в режиме пиковых нагрузок.

4.2.4. Прочие положения программы повышения доступности

Отдельное направление политики доступности должно регламентировать вопросы разработки приложений для ИС, выработку и утверждение типовой технологии создания прикладных систем. В связи с необходимостью обеспечения высокой доступности, перед разработчиками встают новые задачи, которые обычно выпадают из поля зрения административных и технических специалистов. Во — первых, требуется соответствующее расширение имитационного комплекса. Во — вторых (и это главное), выбор архитектуры прикладных систем и их технической реализации должен производиться с учетом необходимости дублирования информационных сервисов и прозрачной для клиентов адресации к работоспособному экземпляру сервиса. Для уменьшения времени отклика системы (как аспекта повышения доступности) целесообразно применять такие меры, как балансировка загрузки между серверами. Все перечисленные проблемы помогает решить программное обеспечение промежуточного слоя (см. [6]).

Реализация мер обеспечения доступности, вообще говоря, связана с определенными неудобствами для персонала. Некоторым разработчикам, вероятно, предстоит овладеть новой технологией программирования с использованием ПО промежуточного слоя. При наличии резервного центра системным администраторам и техническим работникам, возможно, придется совершать более или менее длительные поездки. В этой связи в программе доступности должны быть предусмотрены административные меры (в частности, меры поощрения), укрепляющие сознательную дисциплину персонала.

5. Операционные регуляторы, относящиеся к обеспечению доступности

Данный раздел посвящен мерам, которые ориентированы на людей, а не на технические средства. Именно люди формируют режим информационной безопасности и, в частности, доступности, и они же оказываются главной угрозой.

5.1. Процедурные меры, направленные на обеспечение безотказности

В этом разделе будут рассмотрены рутинные действия, направленные в первую очередь на обеспечение безотказной работы информационных сервисов.

Можно выделить следующие направления повседневной деятельности:

- поддержка пользователей;
- поддержка программного обеспечения;
- синхронизация мер обеспечения доступности с жизненным циклом системы;
- конфигурационное управление.

5.1.1. Поддержка пользователей

Поддержка пользователей состоит прежде всего в обучении, консультировании и в оказании помощи при решении разного рода проблем.

Организация обучения должна обладать тремя свойствами:

- полнота охвата;
- регулярность;
- наличие практических занятий.

Занятия, особенно практические, должны быть увязаны с существующими регламентами и инструкциями. Практические занятия должны проводиться на имитационном стенде, с отработкой действий как в штатных, так и нештатных ситуациях.

Рекомендуемая периодичность учебных курсов — не реже одного раза в год. Как считает известный психолог профессор Ильясов, целесообразно раз в полгода проводить "учения" на имитационном стенде, проверяя и закрепляя практические навыки персонала.

В соответствии с рекомендуемой политикой повышения доступности, работа консультационных служб должна быть строго регламентирована и в максимальной степени стандартизована и автоматизирована. Регламент должен касаться общения с пользователем (нужно собрать максимум информации и одновременно успокоить человека), порядка фиксации обращений пользователей и реакции на них. Целесообразно разработать для перечисленных целей стандартные формы. Для автоматизации консультационной службы могут применяться многочисленные системы управления проблемами (Problem Management Tools) и столы справок (Help Desk).

5.1.2. Поддержка программного обеспечения

Поддержка программного обеспечения — одно из важнейших средств повышения доступности информации. Прежде всего, необходимо контролировать, какое программное обеспечение выполняется на компьютерах. Использование неавторизованных программ или программ с неавторизованными изменениями должно быть запрещено. Особенно это касается клиентских систем. Целесообразно унифицировать операционную среду этих систем и затем централизованно контролировать пользовательские конфигурации, анализируя управляющую информационную базу (Management Information Base — MIB). Подобный контроль следует сделать регулярным и автоматическим.

Необходимо хранить эталонные копии авторизованного программного обеспечения вместе с документацией. Должны присутствовать и регулярно использоваться утилиты, контролирующие не только общую конфигурацию, но и целостность всех компонентов программного обеспечения на всех компьютерах ИС.

Необходимо наладить централизованное хранение конфигурационных файлов всех компонентов ИС, включая не только компьютеры, но и активное сетевое оборудование. Первое действие, которое следует предпринимать при сбое маршрутизаторов или концентраторов — попытка перезагрузить их с использованием эталонных конфигурационных файлов.

Распространение нового программного обеспечения также необходимо производить централизованно, и порядок такого распространения должен быть регламентирован.

5.1.3. Синхронизация мер обеспечения доступности с жизненным циклом системы

Если синхронизировать меры обеспечения доступности с жизненным циклом сервисов, можно добиться большего эффекта с меньшими затратами.

В жизненном цикле информационного сервиса целесообразно выделить следующие этапы:

- Инициация. На этом этапе выявляется необходимость в приобретении или разработке нового сервиса, документируется его предполагаемое назначение.
- Закупка или разработка. На этом этапе составляются спецификации, прорабатываются варианты закупки, выполняется собственно закупка. В случае разработки, после составления спецификации и проработки вариантов выполняется реализация.
- Тестирование и установка. Сервис тестируется, после чего передается в опытную эксплуатацию.
- Пилотная (опытная) эксплуатация. Сервис эксплуатируется в условиях повышенного внимания со стороны служб технической поддержки и/или разработчиков.
- Штатная эксплуатация. На этом этапе сервис не только работает и администрируется, но и подвергается модификациям.
- Выведение из эксплуатации. Происходит переход на новый сервис.

На этапе инициации оформляется понимание того, что необходимо приобрести (разработать) новый или значительно модернизировать существующий сервис; выполняются прикидки, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

Следует указать, что свойства безотказности, живучести и обслуживаемости в значительной мере определяются именно на этапе инициализации, при выборе основных принципов и архитектурных решений, закладываемых в основу нового сервиса. Есть лишь еще один этап, способный столь же радикально повлиять на доступность — это этап установки, на котором вырабатываются нормы и порядок эксплуатации сервиса.

На этапе закупки (разработки) целесообразно обратить особое внимание на надежность компании — поставщика (разработчика), ее способность обеспечить сопровождение продукта, послепродажное обслуживание, обучение персонала, наконец, на время реакции ее сервисной службы. Все эти моменты должны быть оговорены в контракте на закупку (разработку).

Когда продукт закуплен или разработан, его необходимо установить и сконфигурировать и протестировать. Первоначальная установка должна выполняться на имитационном стенде. Следует разработать и утвердить регламент тестирования продукта на стенде, в том числе набор тестовых примеров. Если это возможно, целесообразно привлечь к тестированию пользователей.

На имитационном стенде должны моделироваться различные, в том числе нештатные, режимы работы. Помимо собственно работоспособности, должны проверяться полнота регистрационной информации, возможность удаленного контроля за продуктом с использованием имеющихся средств. На стенде необходимо протестировать ситуации отказов и использования средств обеспечения живучести, если таковые имеются, равно как и порядок ручного переключения на резервный экземпляр продукта. Должны быть отработаны процедуры устранения неисправностей и деинсталляции продукта, а также другие регламентные документы, необходимые на этапе эксплуатации.

Важным результатом тестирования продукта на имитационном стенде должно стать пополнение базы данных консультационной службы, поддерживающей работу пользователей.

Тестирование должно завершаться подготовкой отчета, содержащего описание проведенных действий и их результаты. На основании отчета, с учетом полноты и комплексности тестирования, принимается решение об установке штатного варианта, его конфигурировании и вводе в пилотную эксплуатацию. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоемким и ответственным делом, которое необходимо детально регламентировать.

Фаза пилотной эксплуатации также должна быть тщательно регламентирована. Не следует совмещать фазы пилотной эксплуатации сразу нескольких продуктов. Заранее должны быть оговорены ситуации, требующие немедленного выключения и деинсталляции продукта.

После успешного завершения пилотной фазы, начинается период штатной эксплуатации — самый длительный и сложный. На этом этапе необходимо контролировать следование регламентам, а также периодическую коррекцию регламентов при изменении условий эксплуатации. Целесообразно не реже одного — двух раз в год проверять действенность используемых средств обеспечения доступности сервисов.

При выведении сервиса из эксплуатации следует позаботиться о сохранности обрабатываемых им данных, чтобы гарантировать возможность их импорта в новый сервис.

5.1.4. Конфигурационное управление

Конфигурационное управление позволяет контролировать и фиксировать изменения, вносимые в программную и (что не менее важно) аппаратную и инфраструктурную конфигурации. Необходимо застраховаться от случайных или непродуманных модификаций, уметь как минимум возвращаться к прошлой, работающей версии. Фиксация изменений позволит при необходимости воспроизвести эти изменения для дублирующих ресурсов и восстановить текущую версию после аварии.

Следует регламентировать порядок внесения изменений. Жизненный цикл изменения напоминает цикл нового продукта. На первой фазе (инициация) уполномоченное лицо вносит предложение по изменению текущей конфигурации, после чего определяется круг лиц, которых это изменение затрагивает, и в течение 1 — 3 недель происходит обсуждение. Затем, когда характер и серьезность изменения точно определены и согласованы, разрабатывается регламент его внесения, назначается ответственный за данное мероприятие. Необходимо предусмотреть не только чисто технические аспекты, но и модификацию консультационной базы данных, информирование пользователей и т.п. Заранее, до внесения изменений, должна быть утверждена процедура их отката, если они по каким — либо причинам окажутся некорректными.

Если это предусмотрено регламентом, изменения должны подвергаться тестированию на имитационном стенде. Рекомендуется также явно выделить фазу пилотной эксплуатации, во время которой все, что связано с внесенным изменением, контролируется особенно тщательно и сохраняется возможность быстрого возврата к прежней версии. Само фактически выполненное изменение должно быть тщательно документировано.

Необходимо разработать регламент внесения срочных изменений, когда под угрозой находится работоспособность ИС и на согласования нет времени. Следует определить круг лиц, имеющих право санкционировать подобные действия, а также порядок фиксации изменений, информирования о них заинтересованных лиц и обсуждения произведенного действия.

Технологию конфигурационного управления необходимо применять и к изменениям в аппаратуре и поддерживающей инфраструктуре. Следует фиксировать все изменения в конфигурации клиентских и серверных компьютеров, в локальной сети, в подключении внешних коммуникаций, в размещении кондиционеров и т.п. Удобно использовать для этой цели карту информационной системы.

5.2. Процедурные меры, направленные на обеспечение живучести и обслуживаемости

Процедурные меры, преследующие цель обеспечения живучести и обслуживаемости, образуют в совокупности набор оперативных мероприятий и регламентов, направленных на обнаружение и нейтрализацию отказов и нарушений доступности. Важно, чтобы в подобных случаях последовательность действий была спланирована и отработана до автоматизма заранее, поскольку меры нужно принимать срочные и скоординированные, а действовать людям придется, возможно, в состоянии стресса.

Для обеспечения живучести на процедурном уровне следует предусмотреть избыточность персонала в каждой из критически важных областей (функциональной и территориальной). Подобная избыточность может достигаться за счет наличия резервных специалистов. Целесообразно заключение договоров с родственными организациями о взаимном привлечении персонала в случае возникновения критических ситуаций.

Другой способ создания избыточности персонала — овладение смежными профессиями, способность заменить коллегу. Для поддержания этой формы избыточности нужны как образовательные меры, так и меры материального и/или морального поощрения.

5.2.1. Резервное копирование

Резервное копирование необходимо для восстановления программ и данных, поврежденных в результате отказа. Целесообразно делать как минимум два экземпляра копий. Один из них следует оставлять поблизости, второй хранить в безопасном, по возможности удаленном месте.

Регулярно (не реже одного раза в месяц) на имитационном стенде в тестовых целях следует проверять возможность восстановления информации с резервных копий.

5.2.2. Реакция на нарушения доступности

Реакция на нарушения доступности информационных сервисов преследует две главные цели:

- локализация нарушения и уменьшение наносимого вреда;
- недопущение повторных нарушений.

Для недопущения повторных нарушений необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику, вносить изменения в существующую практику. Заранее все предусмотреть невозможно, поэтому следует запланировать создание рабочей группы (или нескольких групп), анализирующей инциденты и, одновременно, отслеживающей новую информацию в области доступности, рассматривающей новые угрозы, принимающей краткосрочные меры и вырабатывающей рекомендации по корректировке программы повышения доступности с целью принятия долгосрочных мер.

При планировании реакции на инциденты важно руководствоваться соображениями унификации и автоматизации. Например, если в число рассматриваемых рисков входит угроза террористического акта, необходимо или снабдить секретарей, принимающих телефонные звонки, формами для фиксации информации о звонящем (содержание разговора, голос, звуковой фон, психологическое состояние и т.п.), или, что предпочтительнее, обеспечить возможность записи телефонного разговора на магнитофон с целью последующего анализа разговора специалистами (что, впрочем, не отменяет необходимости в аннотации стандартной формы к сделанной записи).

Необходимо стандартизовать процедуру доклада об инциденте и структуру сообщаемой информации. Координаты лиц, которых следует известить об инциденте, должны быть всегда доступны. На случай отсутствия реакции со стороны должностных лиц определенного уровня, должна существовать процедура эскалации докладов, то есть передачи информации на более высокий уровень.

5.2.3. Планирование восстановительных работ

Ни одна организация не застрахована от серьезных аварий, вызванных естественными причинами, злым умыслом, халатностью или некомпетентностью. Планирование восстановительных работ, являясь частным случаем проработки реакции на нарушения доступности, позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию критически важных сервисов.

Процесс планирования восстановительных работ можно подразделить на следующие этапы:

- выявление критически важных сервисов, их ранжирование по степени критичности;
- идентификация ресурсов, необходимых для функционирования критически важных сервисов;

- определение перечня вероятных аварий;
- разработка плана восстановительных работ;
- подготовка к реализации разработанного плана;
- проверка плана.

И при подготовке мер реагирования на нарушения доступности, и при планировании восстановительных работ, необходимо проводить измерения, показывающие, за какое время то или иное действие может быть выполнено на практике. Располагая временной метрикой элементарных действий, можно оценивать продолжительность более сложных мероприятий. Если не удается уложиться в отведенное время, нужно или повысить подготовку персонала, или пересмотреть накладываемые ограничения, или разработать альтернативные, возможно, более дорогостоящие процедуры.

Неотъемлемой частью восстановительных работ является оценка нанесенного ущерба. Процессы оценки ущерба и принятия решения о последующих действиях следует в максимально возможной степени унифицировать. С помощью карты ИС (компьютерной или печатной) ответственный оценивает состояние критических ресурсов по трехбалльной шкале — не пострадал, поврежден, разрушен. Как составная часть оценки, относящейся к компьютерным ресурсам, может использоваться отчет центра управления ИС.

6. Программно-технические меры

Программно—технические меры являются материальной основой работ в области повышения доступности информационных сервисов. Без качественного аппаратного и программного обеспечения, без резервирования аппаратуры, тиражирования программ и данных невозможно добиться приемлемого уровня доступности. Кроме того, необходимо подчеркнуть, что проведение в жизнь большинства административных и процедурных мер осуществляется с использованием соответствующих служебных информационных сервисов (являющихся в данном случае средством автоматизации), которые, в свою очередь, должны обладать свойством высокой доступности. Таким образом, программно—технические меры играют как самостоятельную, так и вспомогательную роли, и обе эти роли представляются отнюдь не второстепенными.

Важнейшей мерой повышения доступности, затрагивающей все уровни — административный, процедурный и программно—технический, является применение структурированного подхода, нашедшего наиболее систематическое и законченное воплощение в объектно—ориентированной методологии. Структуризация необходима по отношению ко всем аспектам и составным частям информационной системы — от архитектуры до административных баз данных, на всех этапах ее жизненного цикла — от инициации до выведения из эксплуатации. Структуризация, важная сама по себе, является одновременно необходимым условием практической реализуемости прочих мер повышения доступности. Только маленькие системы можно строить и эксплуатировать как угодно. У больших систем свои законы, которые, как мы уже указывали, впервые осознали программисты около 30 лет назад.

Вообще говоря, программно—технические меры повышения доступности усложняют информационную систему, поэтому необходим взвешенный подход к их внедрению; в противном случае события будут развиваться в соответствии с известным законом Мерфи — первой выйдет из строя система повышения доступности. Каждая организация должна взвесить свои возможности, уровень квалификации своих специалистов и выбрать реалистичный набор мер.

Далее будут рассмотрены меры повышения доступности, относящиеся в первую очередь к фазе эксплуатации информационных систем, поскольку это представляется наиболее актуальным для большинства читателей.

6.1. Обеспечение безотказности

После того, как на административном уровне приняты решения о принципах построения и архитектуре информационной системы, выполнены закупки и произведена установка аппаратного и программного обеспечения, а на процедурном уровне определен и усвоен персоналом регламент эксплуатации ИС, главным средством обеспечения безотказности на программно—техническом уровне становится проактивное управление всеми компонентами ИС и поддерживающей инфраструктуры.

Проактивное управление базируется на постоянном сборе и анализе информации о функционировании ИС. Для реализации этого процесса целесообразно применять программное обеспечение, построенное в архитектуре менеджер—агент и ориентированное на поддержку распределенных разнородных конфигураций. В качестве претендентов на эту роль можно указать семейства продуктов Solstice (Solstice Enterprise Manager и ассоциированные продукты) компании SunSoft и OpenView компании Hewlett—Packard. Одним из важных достоинств этих решений является возможность дублирования центра управления.

Информация, которая собирается в центре управления, не должна ограничиваться чисто компьютерными параметрами. Не менее важны параметры окружающей среды, такие как качество электропитания, температура и влажность в серверной комнате. Например, выход из строя кондиционера, если не предпринять немедленных мер, может повести к серьезным авариям вычислительной техники.

Системы управления допускают задание программируемых реакций на определенные события, такие как выход отслеживаемого параметра за допустимые пределы. Данная возможность автоматизации анализа регистрационной информации должна использоваться максимально широко.

По результатам анализа может быть принято решение об оптимизации ИС, об установке дополнительного оборудования или о ремонте компонентов, работающих неустойчиво.

Для проведения в жизнь политики безопасности вообще и политики повышения доступности в частности в рамках развитых ИС целесообразно использовать интегрирующие окружения, такие как CA—Unicenter компании Computer Associates или Tivoli Management Environment (TME) компании Tivoli Systems. Эти окружения позволяют управлять пользователями, программным обеспечением, потоком работ посредством интуитивно понятного графического интерфейса.

Централизованное резервное копирование, в том числе для клиентским рабочих мест, проводимое в соответствии с утвержденным расписанием, повышает доступность данных. Перечисленные интегрирующие окружения позволяют единообразно осуществлять копирование с автоматическим учетом специфики обслуживаемых сервисов (например, СУБД) без необходимости приостанавливать последние, но с сохранением целостности информации.

Балансировка загрузки, ее равномерное распределение по наличным ресурсам, является еще одним важным инструментом повышения безотказности. Избегать пиковых нагрузок — значит продлить срок службы оборудования и уменьшить вероятность проявления программных ошибок. Балансировка может осуществляться организационными мерами на основании анализа регистрационной информации, однако предпочтительнее использовать для этой цели программное обеспечение промежуточного слоя.

Консультационная служба является средством повышения безотказности работы пользователей, а также обслуживающего персонала. Для автоматизации консультационной деятельности можно рекомендовать продукты Apriori компании Platinum Technology и Top of Mind компании The Molloy Group.

6.2. Обеспечение живучести

Основным приемом обеспечения живучести является резервирование аппаратуры, программ и данных. Это верно и "в малом", для отдельных устройств, когда в них вводят избыточные модули, и для целых ИС, когда для обеспечения живучести создают резервный центр.

Аппаратура — относительно статичная составляющая, однако было бы ошибкой полностью отказывать ей в динамичности. В большинстве организаций информационные системы находятся в постоянном развитии, поэтому на протяжении всего жизненного цикла ИС следует соотносить все производимые изменения с необходимостью обеспечения живучести.

Программы и данные более динамичны, чем аппаратура, и резервироваться они могут постоянно, при каждом изменении, после завершения некоторой логически замкнутой группы изменений или по истечении определенного интервала времени.

Резервирование программ и данных может выполняться многими способами — за счет зеркалирования дисков, резервного копирования и восстановления, репликации баз данных и т.п. Будем использовать для всех перечисленных способов термин "тиражирование". В следующем пункте сделана попытка проанализировать общие свойства тиражирования как средства обеспечения живучести программ и данных.

6.2.1. Классы тиражирования

Выделяются следующие классы тиражирования:

- Симметричное/асимметричное. Тиражирование называется симметричным, если все серверы, предоставляющие данный сервис, могут изменять принадлежащую им информацию и передавать изменения другим серверам. В противном случае тиражирование называется асимметричным.
- Синхронное/асинхронное. Тиражирование называется синхронным, если изменение передается всем экземплярам сервиса в рамках одной распределенной транзакции. В противном случае тиражирование называется асинхронным.
- Осуществляемое средствами сервиса, хранящего информацию/внешними средствами.

Современные сервисы, такие как СУБД (см., например, [7, 8]) предоставляют все перечисленные возможности. Рассмотрим, какие из них предпочтительнее.

В соответствии с рекомендуемой политикой повышения доступности, следует предпочесть стандартные средства тиражирования, встроенные в сервис.

Асимметричное тиражирование идейно проще симметричного (исключены конфликты по изменениям), поэтому целесообразно выбрать асимметрию.

Самым трудным является выбор между синхронным и асинхронным тиражированием. Синхронное идейно проще (нет периода рассогласования сервисов, когда транзакция успешно завершилась, но ее результаты еще не протиражированы; если в этот период случится отказ основного сервера, клиент будет считать, что заказанная им операция прошла нормально, однако на резервном сервере ее результаты будут отсутствовать),

но его реализация может быть тяжеловесной и сложной, хотя это внутренняя сложность сервиса, невидимая для приложений. Асинхронное тиражирование устойчивее к отказам в сети, оно меньше влияет на работу основного сервиса.

Чем надежнее связь между серверами, вовлеченными в процесс тиражирования, чем меньше время, отводимое на переключение с основного на резервный сервер, и чем жестче требования к актуальности информации, тем более предпочтительным оказывается синхронное тиражирование. Правда (оговоримся еще раз) необходимо также принимать во внимание особенности конкретных сервисов, апробированность реализации синхронного тиражирования, степень влияния тиражирования на работу пользователей.

С другой стороны, недостатки асинхронного тиражирования могут компенсироваться процедурными и программными мерами, направленными на контроль целостности информации в распределенной ИС. Сервисы, входящие в состав ИС, в состоянии обеспечить ведение и хранение журналов транзакций, с помощью которых можно выявлять операции, утерянные при переключении на резервный сервер. Даже в условиях неустойчивой связи с удаленными филиалами организации, подобная проверка в фоновом режиме займет не более нескольких часов, поэтому асинхронное тиражирование может рассматриваться как кандидат на использование практически в любой ИС.

Асинхронное тиражирование может производиться на сервер, работающий в режиме горячего резерва, возможно, даже обслуживающего часть пользовательских запросов, или на сервер, работающий в режиме теплого резерва, когда изменения периодически накатываются, но сам резервный сервер запросов не обслуживает.

Достоинство теплого резервирования в том, что его можно реализовать, оказывая меньшее влияние на основной сервер. Это влияние вообще может быть сведено к нулю, если асинхронное тиражирование осуществляется путем передачи инкрементальных копий с основного сервера (резервное копирование необходимо осуществлять в любом случае). Второе достоинство теплого резерва состоит в том, что его можно использовать как часть имитационного стенда и отрабатывать на нем технические и процедурные решения в условиях, максимально приближенных к реальным.

Основной недостаток теплого резерва состоит в относительном большом времени включения, что может быть неприемлемо для "тяжелых" серверов, таких как кластерная конфигурация сервера СУБД. Здесь необходимо проведение измерений в условиях, близких к реальным.

Второй недостаток теплого резерва вытекает из опасности малых изменений, связанных, например, с использованием резерва в составе имитационного стенда. Может оказаться, что в самый нужный момент срочный перевод резерва в штатный режим невозможен.

Учитывая приведенные соображения, следует в первую очередь рассматривать возможность горячего резервирования, либо тщательно контролировать использование теплого резерва и регулярно (не реже 1 раза в неделю) проводить пробные переключения резерва в горячий режим.

6.2.2. Программное обеспечение промежуточного слоя

Обоснование целесообразности использования программного обеспечения промежуточного слоя (ПО ПС) является одним из существенных моментов настоящей работы. Причина состоит в том, что с помощью ПО ПС можно для произвольных прикладных сервисов добиться высокой живучести с полностью прозрачным для пользователей переключением на резервные мощности.

Основные черты ПО ПС подробно описаны в работе [6] на примере монитора транзакций Tuxedo System, принадлежащего ныне компании BEA Systems. В качестве других решений ПО ПС могут использоваться продукты компании Teknekron, Orbix компании Iona Technologies, семейство продуктов компании Isis Distributed Systems. Допустима и комбинация перечисленных средств, когда Orbix обеспечивает работу в распределенной объектно — ориентированной среде, а Isis — высокую готовность.

Перечислим основные достоинства ПО ПС, существенные для обеспечения доступности.

- ПО ПС уменьшает сложность создания распределенных систем. Подобное ПО берет на себя часть функций, которые в локальном случае выполняют операционные системы.
- ПО ПС берет на себя маршрутизацию запросов, позволяя тем самым обеспечить живучесть прозрачным для пользователей образом.
- ПО ПС осуществляет балансировку загрузки вычислительных мощностей, что также способствует повышению доступности данных.
- ПО ПС в состоянии осуществлять тиражирование любой информации, а не только содержимого баз данных. Следовательно, любое приложение можно сделать устойчивым к отказам серверов.
- ПО ПС в состоянии отслеживать состояние приложений и при необходимости тиражировать и перезапускать программы, что гарантирует живучесть программных систем.
- ПО ПС дает возможность прозрачным для пользователей образом выполнять переконфигурирование (и, в частности, наращивание) серверных компонентов, что позволяет масштабировать систему, сохраняя инвестиции в прикладные системы. Стабильность прикладных систем — важный фактор повышения доступности данных.

6.3. Обеспечение обслуживаемости

Для обеспечения обслуживаемости рекомендуется ориентироваться на решения модульной структуры с возможностью автоматического обнаружения отказов, динамического переконфигурирования аппаратных и программных средств и замены отказавших компонентов в горячем режиме.

Динамическое переконфигурирование преследует две основные цели:

- изоляция отказавших компонентов;
- сохранение работоспособности сервисов.

Изолированные компоненты образуют зону риска реализованной угрозы. Чем меньше эта зона, тем выше обслуживаемость соответствующих сервисов. Так, при отказах блоков питания, вентиляторов и/или дисков в современных серверах зона риска ограничена ровно отказавшим компонентом; при отказах процессорных модулей весь сервер может потребовать перезагрузки (что может означать дальнейшее расширение зоны риска). Очевидно, в идеальном случае зоны поражения и риска совпадают, и современные серверы и активное сетевое оборудование, а также программное обеспечение ведущих производителей весьма близки к этому идеалу.

Возможность программирования реакции на отказ также повышает обслуживаемость систем. Каждая организация может выбрать свою стратегию реагирования на отказы тех или иных аппаратных и программных компонентов и автоматизировать эту реакцию. Так, в простейшем случае возможна отправка сообщения системному администраторы по электронной почте и/или на пейджер, чтобы ускорить начало ремонтных работ; в более сложном случае может быть реализована процедура "мягкого" выключения (переключения) сервиса, чтобы упростить обслуживание.

Возможность удаленного выполнения административных действий — важное направление повышения обслуживаемости, поскольку при этом ускоряется начало восстановительных мероприятий, а в идеале все работы (обычно связанные с обслуживанием программных компонентов) выполняются в удаленном режиме, без перемещения квалифицированного персонала, то есть с высоким качеством и в кратчайшие сроки. Для современных систем возможность удаленного администрирования — стандартное свойство, но важно позаботиться о его практической реализуемости в условиях разнородности конфигураций (в первую очередь клиентских). Централизованное распространение и конфигурирование программного обеспечения, управление и диагностирование компонентов информационной системы — надежный фундамент технических мер повышения обслуживаемости.

Целесообразно заключить договоры с компаниями, способными осуществлять сервисное обслуживание с высоким качеством и в кратчайшие сроки (порядка нескольких часов). Каждый компонент ИС должен входить в сферу действия подобного договора. Здесь имеются в виду не только компьютерные ресурсы, но и поддерживающая инфраструктура — электропитание, водоснабжение, кондиционирование, связь и т.п. В этой связи разумно использовать карту ИС, в которой с каждым компонентом связана история его "жизни" — установка, переконфигурирование, ремонт и прочие действия. Зная предысторию, проще планировать ремонтные мероприятия.

Необходимо создать целостный набор диагностического и тестового программного обеспечения, позволяющего контролировать состояние ИС после ремонта (ведущие компании — поставщики такими наборами располагают). Тестирование после обслуживающих мероприятий позволит убедиться в том, что доступность сервисов действительно восстановлена.

7. Резервный вычислительный центр

Важным и весьма радикальным средством повышения живучести и обслуживаемости информационных систем по отношению к угрозам поддерживающей инфраструктуре является создание резервного вычислительного центра (РВЦ).

Лет пятнадцать — двадцать назад террористические акты или угрозы их осуществления казались чем — то абсолютно нереальным. Вероятность крупномасштабного отключения электроэнергии или водоснабжения можно было считать пренебрежимо малой (по крайней мере, в Москве). Увы, сейчас, на рубеже третьего тысячелетия, никто не застрахован от катаклизмов, способных надолго вывести из строя всю производственную площадку организации или сделать невозможным доступ персонала. В то же время (к сожалению для поставщиков услуг), несмотря на общую нестабильность, потребители успели привыкнуть к относительно высоким стандартам обслуживания (повторимся — по крайней мере в Москве). Все это, с одной стороны, предъявляет жесткие требования к доступности всех сервисов, в том числе информационных, а, с другой стороны, существенно усложняет задачу обеспечения высокой доступности. В случае сколько-нибудь глобальных катаклизмов локальные меры обеспечения живучести и обслуживаемости бессильны. Единственный выход состоит в организации территориально удаленного РВЦ, способного при необходимос-

ти предоставить критически важные информационные сервисы.

В соответствии с общим подходом, развитым в разделе "Живучесть и зоны риска", РВЦ должен располагаться за пределами зон поражения, затрагивающих основную производственную площадку. В типичных российских условиях для этого достаточно организовать РВЦ в удаленном районе того же города, где находится основная площадка. Если в число рассматриваемых угроз входят землетрясения, наводнения, ураганы и т.д., удаленность РВЦ должна быть большей.

В РВЦ необходимо поместить ресурсы (аппаратура, программы, данные, поддерживающая инфраструктура, персонал), достаточные для работы в случае выхода из строя основной площадки. Кроме того, потребители информационных сервисов организации должны располагать линиями связи с РВЦ и технической возможностью переключения на него.

Можно представить себе три реальные схемы создания и поддержания РВЦ. В первом случае организация монопольно владеет резервным центром. Возможно, в роли такого центра выступает один из крупных филиалов, близкий по своему оснащению к основной площадке.

Во втором случае группа компаний, обладающих близкими информационными платформами и расположенных в разных районах, создает совместный РВЦ.

В принципе возможен и третий вариант, когда компания специализируется на создании и сдаче в аренду резервных центров, но пока в российских условиях он представляется проблематичным.

Создание РВЦ и отработка процедуры переключения на него (равно как и процедуры возвращения к штатному режиму работы) требуют решения многочисленных административных и технических проблем. Тем не менее, когда организация достигает определенных масштабов, а ее услуги становятся по-настоящему популярными, она уже не может позволить себе длительных перерывов в обслуживании клиентов, даже если эти перерывы вызваны внешними причинами.

Многие западные компании имеют или создают резервные вычислительные центры. К их числу принадлежит Sun Microsystems, детальнейшим образом регламентировавшая действия до, во время и после событий, способных вывести из строя штаб-квартиру компании. В свою очередь, крупнейшие консультационные компании в качестве одной из услуг предлагают помощь в организации РВЦ. Можно предположить, что со временем число отечественных организаций, нуждающихся в РВЦ и активно прорабатывающих вопросы их создания, будет довольно быстро расти.

8. Заключение

Несмотря на то, что в настоящее время важность вопросов обеспечения доступности информационных сервисов очевидным образом недооценивается, нет сомнений в том, что положение весьма скоро начнет меняться. Ряд организаций уже понесли крупные финансовые потери вследствие нарушения работоспособности своих систем; еще несколько подобных случаев, и все поймут, что "гром грянул".

Чтобы меры по обеспечению доступности были эффективными, они должны распространяться на все уровни — административный, процедурный, программно-технический, охватывать весь жизненный цикл информационной системы, все ее компоненты — поддерживающую инфраструктуру, аппаратуру, программы, данные, персонал, пользователей. Необходимо позаботиться обо всех аспектах доступности — безотказности, живучести, обслуживаемости.

Положения, сформулированные в данной работе, могут служить концептуальной основой при решении проблемы обеспечения доступности информационных сервисов, предоставляемых или используемых организациями. Разумеется, эти общие положения при практическом использовании должны быть дополнены разработкой конкретных административных, процедурных и программно-технических мер.

9. Литература

1. Галатенко В. Информационная безопасность — обзор основных положений. — Jet Info, 1996, 1—3.
2. Липаев В. Программно-технологическая безопасность информационных систем. — Jet Info, 1997 (готовится к печати).
3. Kern H., Johnson R., Hawkins M., Law A., Kennedy W. Managing the New Enterprise. — SunSoft Press, 1996.
4. Шишонок Н., Репкин В., Барвинский Л. Основы теории надежности и эксплуатации радиоэлектронной техники. — М.: Советское радио, 1964.
5. Butler R. The Infeasibility of Experimental Quantification of Life-Critical Software Reliability. — Software Engineering Notes, v. 16, n. 5, pp. 66—76.
6. Ладыженский Г. Tuxedo System — ключевой компонент корпоративных информационных систем. — Jet Info, 1996, 14/15.
7. Вьюкова Н., Галатенко В. Информационная безопасность систем управления базами данных. — СУБД, 1996, 1.
8. Oracle7 Server Distributed Systems, Release 7.3. — Oracle Corporation, 1996.

Десять заповедей современных информационных технологий (по Рэнди и Харрису)

Мы облекли свое учение в легко запоминаемую форму. Следуйте этим заповедям, и вы достигнете совершенства в работе с информационными технологиями

Введение

Мы совершаем тур с курсом лекций по информационным технологиям и используем в выступлениях свои основные убеждения и методы, объясняя с их помощью, как реализовать на новом предприятии подобающую инфраструктуру и управлять ею. Мы называем их "десять заповедей по Рэнди и Харрису".

Во всех крупных организациях сотрудникам предлагаются основные нормы соответствующего поведения. Возможно, Десять заповедей — это древнейший свод правил поведения. Начиная почти с того самого дня, когда Моисей спустился с горы Синай, люди пытаются заключить правила поведения своей группы в десять легко запоминаемых фраз. Мы способны оценить хорошую вещь и сконцентрировали наше учение о новой информационной технологии сегодняшнего дня в Десяти заповедях информационных технологий по Рэнди и Харрису. Многие из этих тем мы обсуждали и раньше, а остальные станут сырьем для будущих статей.

Харрис Керн является консультантом Sun по вопросам миграции на открытые технологии. Рэнди Джонсон владеет консультационной компанией R&H Associates. Харрис и Рэнди руководили процессом миграции информационной системы компании Sun Microsystems с мэйнфремов на Unix. Об этом рассказывают две их книги: "Rightsizing The New Enterprise: The Proof Not the Hype" (SunSoft Press/PTR Prentice Hall, ISBN 0-13-132184-6) и "Managing The New Enterprise: The Proof Not the Hype" (SunSoft Press/PTR Prentice Hall, ISBN 0-13-231184-4).

1 Смотри на сеть свою, как на вычислительный центр свой

Другими словами, "сеть — это вычислительный центр". Не стала ли Sun Microsystems известна благодаря лозунгу "сеть — это компьютер"? Да, стала, и это доказывает, что отдел маркетинга Sun был прав. А теперь пара ребят приходят со старыми добрыми вычислительными центрами и говорят: "сеть — это вычислительный центр". Что это дает?

Спросите себя: какая среда в обработке данных является самой защищенной и надежной? Любой профессионал в области информационных технологий может ответить на этот вопрос — это вычислительный центр! Это спасательный пояс вашей компании для работы с бизнес-системами непрерывного действия и жизненно необходимыми системами работы с финансами, производством и кадрами. Мы уже слышим, как всполошились крутые ребята — любители настольных систем. Да, существуют настольные приложения, которые можно рассматривать как приложения непрерывного действия. До определенной степени мы с ними согласны, но твердо придерживаемся мнения, что настольные машины не формируют центральную нервную систему крупных организаций.

SunWorld Online, ноябрь 1996

2 Чти законы мэйнфрейма твоего, и да будут они святы

Когда вы разворачиваете нужную инфраструктуру, вы должны поставить себе целью, чтобы сеть была так же надежна, доступна и удобна в обслуживании, как вычислительный центр. Это требует процессов, стандартов и процедур, о которых мы скажем во второй заповеди.

Законы мэйнфрейма: с ними жить невозможно, но и без них жить нельзя. В эпоху, когда все и повсюду распределяется, законы становятся важнее, чем когда-либо. Но вы не сможете просто пересадить законы мэйнфрейма со всей их бюрократией в клиент-серверную технологию. Вам нужно настроить и объединить эти законы так, чтобы они позволяли управлять современной, хаотичной и разнородной инфраструктурой. Мы выросли вместе с этими процессами в старых средах, и среди них были управление изменениями, планирование возможностей, восстановление после сбоев и т.д. Сегодня эти законы нужны более, чем когда-либо.

3 Да будет у тебя минимум архитектур, но да будет их достаточно

Разрабатывай стандарты для всей организации по каждой области инфраструктуры, включая сеть, вычислительный центр, настольные системы, инструментарий разработки, мобильные компьютеры, серверы и так далее. Вам нужны стандарты на сегодняшний день и четкое понимание направления развития стандартов, сред и архитектур (выберите самое громкое словцо) на пять лет вперед. Например, ваши настольные системы сегодня могут представлять собой машины под Windows 3.1, подключенные к линии 10BASE-T, ваш пятилетний план может предусматривать сетевые компьютеры, подключенные к магистрали 100BASE-T.

4 Да обеспечишь ты централизованный контроль при децентрализованных операциях

Реализуйте новое предприятие, используя сочетание централизованного управления и децентрализованных операций. Централизованное управление означает управление необходимыми для разработки архитектур расходами и разворачивание стандартов и инструкций из центрального пункта. Децентрализованные операции означают, что местоположение сотрудников по поддержке информационных технологий не играет роли. Их можно разместить так, чтобы они наилучшим образом поддерживали сетевые вычисления в общем и вашего клиента в частности.

5 Почитай пользователей своих и общайся с ними часто

Недостаток связей — большая проблема. Говоря в общем, профессионалы по информационным технологиям предпочли бы тянуть кабель и писать код, а не общаться с пользователями и прислушиваться к их проблемам. Этот недостаток по традиции уже в крови у сотрудников отделов информатизации, и усугубляется культурной средой организации информационных технологий. Что еще хуже, специалисты по информационным технологиям, похоже, не общаются и между собой, в пределах своей среды. В дни мэйнфреймов существовала четкая граница в отношении того, что, кому и как нужно было делать. Обязанности каждого были ясно определены. Администраторы баз данных четко знали, где начинается и кончается их работа. То же самое относилось к системным программистам, и к остальным.

Теперь наступает сумасшедшее время "клиент-сервер" без четких границ, где все распространяется по всей сети. Нам нужен процесс, который инициирует и постепенно развивает взаимоотношения между отделом информационных технологий и его клиентами, а также между разными группами внутри отдела. Этот процесс должен четко определить роли и обязанности каждого.

6 Да будут все производственные системы равны в глазах специалистов по информационным технологиям

С аппаратной точки зрения сегодняшнее предприятие состоит из мэйнфреймов, PC, машин Macintosh, рабочих станций и серверов. У вас может появиться соблазн создать для каждой отдельную группу поддержки. Неверно! Не создавайте особых условий для отдельных технологий. Команда поддержки должна называться отделом технической поддержки (ни больше, ни меньше), его сотрудники должны получить разностороннюю подготовку по обслуживанию такого количества платформ, с которым каждый в состоянии справиться. Если разделять поддержку по технологиям, это приведет к понижению эффективности, проблемам во взаимоотношениях, плохой связи и моральным проблемам. Никогда не производите реорганизацию по технологическим соображениям. В наше время, в нашу эпоху, когда почти все становится распределенным, уделяйте всему равное внимание!

7 Определяй меру всему; воистину, ты не способен управлять тем, меры чему не знаешь

Вспомните свою старую среду и то, как вы могли измерить любой показатель инфраструктуры. Вот некоторые из параметров, которые мы определяли:

- Оперативная доступность систем
- Доступность сети
- Количество жалоб
- Количество аварийных завершений работы приложений
- Время отклика приложений
- Процент звонков с жалобами, решенных в течение 2 часов, 4 часов и так далее.

Если бы вы спросили любого руководителя 70-х и 80-х годов о доступности системы, они были бы горды ответить: 99,5%, 99,8% и так далее. На сегодняшнем оснащенном сетью предприятии об этом придется забыть. У кого найдется время собирать чью-то банальную информацию? Мы первыми согласимся, что для установления системы измерений потребуется потратить немало сил. Чтобы собрать статистические данные по работе системы в эру мэйнфреймов, требовалось время, очень много времени, но ведь это одна из причин, почему старый мир так надежен. Мы знали цифры. Мы могли управлять. Играйте цифровыми показателями работы системы. Пусть люди их знают, и ваши менеджеры как-нибудь найдут способ сделать работу организации более эффективной.

8 Да будет созданная тобой служба информационных технологий привлекательной, и пользователи придут к тебе

Как только вы наведете порядок в доме, клиенты вернутся. Однако большинство поставщиков информационных технологий отнюдь не содержит свой дом в порядке. В 80-х большинство клиентов отделов информационных технологий отказались от услуг централизованной группы поддержки при разработке и разворачивании клиент-серверных приложений. Услуги централизованного отдела информационных технологий были слишком бюрократичны и дороги.

Сегодня те же самые клиенты мучаются, пытаясь поддержать работу своих собственных мини-отделов информационных технологий. Им нужна помощь, а централизованный отдел информационных технологий все никак не может собраться. Процессы, стандарты и инструкции станут фундаментом вашего дома. Поскольку эти процессы станут едиными и экономичными, ваш дом (инфраструктура) начнет поддерживать Новое Предприятие. После этого вам нужно поактивней предлагать свои услуги.

9 Раздели добрую весть с сотрудниками своими

В старое время специалисты по обслуживанию мэйнфреймов сидели в вычислительных центрах, как в огромных башнях из слоновой кости. Единственный случай, когда они взаимодействовали с обычными пользователями — это когда отдел помощи обращался к ним с нестандартной проблемой. Они работали в режиме реагирования.

Сегодня профессионалам по информационным технологиям нужно выйти к людям и работать с клиентами. Мы должны предлагать, продавать и другими способами пропагандировать свои услуги. В 90-е и последующие годы роль информационных технологий должна принципиально измениться!

10 Знай: настолько велик твой успех, насколько ты справляешься с изменениями

Изменения будут всегда. В [illegible] мы сейчас живем по времени Интернет, даже если продукты, которые продает наша организация, не работают ни в одной сети. Технология развивается и меняется быстрее, чем когда-либо. Следуйте первым девяти заветам, чтобы управлять Новым Предприятием, и вы добьетесь успеха.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается компанией Инфосистемы Джет с 1995 года
Подписной индекс по каталогу Роспечати **32555**

Главный редактор: Галатенко В.А. *(galat@jet.msk.su)*
Технический редактор: Демочкин С.И. *(serged@jet.msk.su)*

Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
e-mail: JetInfo@jet.msk.su

Jet infosystems