**Байкова И.В., Копытов М.А., Кулагин М.В.,
Метелкин А.В., Михайлов Г.М., Плечов П.Ю. Рогов Ю.П.**

Распределенные информационно-вычислительные системы

Выпуск 2

Инфраструктура и базовые средства локальной сети ВЦ РАН

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Вычислительный центр РАН (ВЦ РАН) - старейшая организация нашей страны, работающая в области создания и практического внедрения методов вычислительной математики, обработки информации с помощью ЭВМ. На протяжении многих лет ВЦ РАН является ведущим центром коллективного использования вычислительной техники (ВТ), предоставляя институтам Академии наук, вузам и другим исследовательским организациям свои вычислительные ресурсы и услуги, интеллектуальный потенциал своих сотрудников и более чем тридцатилетний практический опыт разнообразного применения ЭВМ.

В прошлом ВЦ РАН при реализации своих планов оснащения ВТ всегда ориентировался на отечественную вычислительную технику, работал в тесном контакте с нашими разработчиками, предоставляя им своеобразный полигон для создания новой техники.

В начале 90-х годов в связи с резким ухудшением перспектив развития отечественной вычислительной техники мы были вынуждены пересмотреть программу технического переоснащения нашего института. Стало ясно, что в нынешних условиях устранить компьютерный голод можно только путем установки современной зарубежной ВТ. Очевидным был и тот факт, что использование одиночных, не объединенных в сеть вычислительных систем ушло в прошлое. Было решено при проектировании будущей системы серьезнейшим образом развивать ее информационную составляющую. Это означало, что проектируемая система через выход в глобальные вычислительные сети должна обеспечивать нашим ученым доступ к информационным ресурсам всего мирового сообщества и одновременно собственной локальной сети - ресурсы для накопления собственного информационного материала по всем направлениям научных исследований ВЦ РАН, а также предоставлять доступ к этим материалам через глобальную сеть.

Предстояло спроектировать и реализовать на практике информационно-вычислительную систему (ИВС ВЦ РАН) как динамически развивающуюся пилотную модель, основанную на принципах современных открытых вычислительных систем. Проектированию предшествовало глубокое изучение материалов по открытым вычислительным системам и существующим программно-аппаратным платформам. Был определен прикладной профиль нашей ИВС (по терминологии открытых систем, Application Environment Profile), и на его основе осуществлялся выбор программно-технических средств для построения системы.

В настоящее время реализованы два этапа развития ИВС ВЦ РАН. О первом этапе - проектировании и развертывании базовых средств локальной вычислительной сети ВЦ РАН (ЛВС ВЦ РАН) - подробно рассказано в монографии Байковой И.В., Копытова М.А., Кулагина М.В., Михайлова Г.М., Привезенцева Ю.А., Рогова Ю.П. "Распределенные информационно-вычислительные системы" (см.[1]).

Данная работа посвящена второму этапу - развитию инфраструктуры ЛВС ВЦ РАН, организации выхода в INTERNET через Южную московскую опорную сеть (ЮМОС). В 1994 г. ВЦ РАН принял решение о подключении своей локальной сети к ЮМОС и после согласования с дирекцией Программы телекоммуникаций Международного научного фонда (МНФ) и Российским фондом фундаментальных исследований (РФФИ) заключил договор о подключении к узлу ЮМОС. Подключение к узлу было осуществлено при материальной поддержке РФФИ.

1. Развитие базовых средств ИВС ВЦ РАН

Базовым средствам ИВС ВЦ РАН было уделено должное внимание в [1]. Однако полезно дать дополнительные сведения о некоторых вопросах развития базовых средств и характеристику их состояния на июнь 1996 г.

1.1. Некоторые концептуальные вопросы развития базовых средств

Мы уже отмечали, что ЛВС ВЦ РАН построена на принципах открытых вычислительных систем, определяемых стандартом IEEE POSIX 1003.0. Согласно этому стандарту открытая система должна обеспечивать мобильность прикладных систем для различных компьютерных платформ и опера-

ционных сред, обладать свойством интероперабельности, т.е. обеспечивать совместную работу распределенных прикладных систем на неоднородных (гетерогенных) локальных и удаленных программно-аппаратных платформах, обладать свойством масштабируемости, т.е. обеспечивать возможность функционирования прикладных систем при изменении конфигурации, количества, мощности и типа программно-аппаратных платформ. Удовлетворить этим требованиям можно, используя открытые спецификации на форматы данных, службу и интерфейсы.

ИВС ВЦ РАН - открытая вычислительная система - по природе своей гетерогенная. Открытость гетерогенных систем или гетерогенной среды заключается во взаимодействии самых разнообразных платформ, где "прозрачность" между ними обеспечивается международными стандартами.

При интеграции гетерогенных ИВС можно выделить прежде всего следующие проблемы:

- совместимость аппаратных платформ;
- совместимость операционных платформ;
- совместимость коммуникационных протоколов.

О совместимости аппаратных платформ применительно к ИВС ВЦ РАН можно сказать следующее. В ЛВС ВЦ РАН мы имеем четыре значительно различающиеся по архитектуре аппаратные платформы - IBM PC, SPARC, Digital, PARSYTEC. Бинарная совместимость обеспечивается только в рамках каждой из платформ. Например, имеется полная бинарная совместимость всех программных продуктов Sun Microsystems за счет масштабируемой технологии SPARC (Scalable Processor ARChitecture): все программы исполняются на всех SPARCstation нашей ЛВС (SPARCstation - 10, 20, SLC, IPC).

Для каждой машины любой платформы можно создавать соответствующие аппаратные модификации: наращивать память (оперативную и внешнюю), устанавливать дополнительные процессоры, производить upgrade для процессорных модулей. Это не влияет, как правило, на бинарную совместимость программ данной платформы.

Поскольку имеется совместимость на уровне языков высокого уровня (FORTRAN 77, C, C++, PASCAL), то отсутствие бинарной совместимости между платформами делается менее заметным. Поэтому использование различных эмуляторов не очень распространено. Относительное распространение имеют разве что эмуляторы для PC-архитектуры. Например, для платформы SPARC это SunPC 4.1 для Solaris 2.x и SunPC для Solaris 1.x, эмулятор Microsoft Windows 3.x - WABI 2.1 для Solaris 2.x (WABI - Windows Application Binary Interface).

Совместимость операционных платформ обеспечивается использованием ОС UNIX. Эта операционная система является базой для создания единой операционной среды гетерогенных систем. И хотя процесс реализации конкретных версий UNIX для различных аппаратных платформ чаще всего опережает процесс стандартизации UNIX, тем не менее совместная работа различных диалектов UNIX в гетерогенной среде дает неплохие результаты. UNIX в Solaris 1 и 2 для машин фирмы SUN, UNIX в OSF/1 для машин фирмы DEC и "параллельный" UNIX (PARIX) для PARSYTEC GCel 1/64 имеют различия, но все-таки их совместимость по основным функциям и форматам достаточно высокая. Вообще говоря, совместная работа различных реализаций UNIX заслуживает особого анализа.

С помощью ОС UNIX организуется работа сложных систем, при функционировании которых взаимодействуют процессы, исполняемые на различных аппаратных платформах. Средствами UNIX строятся различные виртуальные структуры и обеспечивается унифицированный доступ к ним из программ, работающих на разных аппаратных платформах. Примером такой структуры является распределенная файловая система (NFS), с помощью которой программы, исполняемые на разных платформах, используют общее дисковое пространство.

Совместимость коммуникационных протоколов в нашей ЛВС, являющейся UNIX-сетью, определяется прежде всего тем, что в программных средах на всех аппаратных платформах используются единые стандартные

сетевые протоколы. Несколько подробнее о протоколах INTERNET и UNIX-сети речь пойдет ниже.

Исключительно важным фактором, влияющим на выбор спектра платформ, на которых строится система, является функциональное назначение. В этом смысле не может быть универсальных систем. Любая пилотная система проектируется в рамках выбранного профиля открытых систем. Общепринятый термин "профиль" представляет собой набор международных стандартов в конкретной прикладной области. Требования, с учетом которых строится профиль системы, одновременно определяют и его идентификацию.

Профиль определяется теми задачами, которые должны решаться на данной системе. Нужно также, чтобы была возможность использовать более мощные ресурсы в других центрах, где развернуты подобные же профили на других программно-аппаратных платформах. Мы рассматриваем только принципиальные вопросы взаимодействия различных научных центров по профилю в открытых сетях, в том числе и зарубежных, вне экономических и политических аспектов.

Выбор профиля нашей пилотной модели, построенной на стандартах открытых сетей, был одной из главных задач.

Функционально профиль ИВС ВЦ РАН определялся исходя из тех научно-технических задач, которые уже традиционно составляют предметную деятельность ученых ВЦ РАН.

Иными словами, в части функциональной профиль ИВС как системы, ориентированной на использование учеными для решения своих фундаментальных и прикладных проблем в соответствующих областях, был в значительной степени определен.

Следовательно, при отработке профиля надо было правильно определить, использование каких стандартных элементов, платформ и сред приведет к наиболее эффективному решению этих задач.

Оставалось фактически по каждой функции профиля сделать правильный выбор из множества существующих элементов программного обеспечения. О выбранных вычислительных платформах, о компиляторах, библиотеках, программистском инструментарии и многих других элементах пользовательского интерфейса мы уже говорили в [1]. Отметим здесь, что содержание профиля подвержено изменению с точки зрения расширения функциональной наполняемости, повышения эффективности. А поскольку принцип развития системы - использование стандартов и лицензионных программных продуктов, то работа по развитию профиля требует порой достаточно больших финансовых затрат.

1.2. Базовые аппаратные средства ИВС ВЦ РАН

Базовые средства всегда находятся в состоянии перманентной модификации. Во-первых, в рамках используемых платформ появляются новые, более мощные системы, выпускаются новые версии существующего программного обеспечения, появляются новые элементы программного обеспечения. Во-вторых, всегда надо быть в курсе того, как развиваются другие платформы и среды и насколько их можно использовать в нашей ИВС.

Повышение эффективности вычислительных серверов локальной сети является одной из главных задач развития ИВС.

Правильный выбор направления развития в области повышения эффективности вычислительных серверов - это непростая задача, требующая многофакторного анализа.

Сейчас при достаточно богатом спектре предложений на рынке и отсутствии ограничений на приобретение любых компьютеров важно правильно распорядиться финансовыми средствами при выборе новой аппаратной структуры. В 1993 г., когда проектировалась наша ИВС, ситуация

была в значительной мере иной, поскольку действовали ограничения на продажу в Россию вычислительной техники.

Поэтому важно внимательно следить за развитием вычислительной техники прежде всего по выбранным нами платформам, рассматривать возможность установки других архитектур (благо открытость нашей ЛВС позволяет это делать). При принятии решения, очевидно, необходимо исследовать, как новая архитектура вписывается в наш профиль, и проводить собственные системные измерения и сравнительные оценки.

1.3. Еще раз о структурированных кабельных системах

Авторы работы [1], имеющие непосредственное отношение к первому выпуску данной работы, а также реализовавшие проект структурированной кабельной сети Вычислительного центра АН СССР еще в 1986 г., сочли необходимым еще раз вернуться к данной тематике в связи с ее все возрастающей актуальностью. Анализ публикаций в данной области, которые появились в течение 1994-1995 гг. [2,3], показывает, что оценить значимость выполненных работ возможно только после апробации кабельной сети на реальной программно-аппаратной платформе и проведения комплекса системных измерений ее параметров с последующим сопоставлением их с международными стандартами IEEE.

Есть два важнейших фактора, которые определили, почему не была оценена своевременно в полном масштабе эта наша работа.

Во-первых, в то время еще не были определены до конца стандарты IEEE 802.3(5) на кабельные сети 10BASE2, 10BASE5, а самое главное - на неэкранированные витые пары 10BASET. Именно использование неэкранированных витых пар было положено в основу будущей структурированной кабельной системы, хотя в 1986 г., когда началось развертывание сети на витых парах в ВЦ РАН, термина и понятия "структурированная кабельная сеть" в нашей отечественной телекоммуникационной отрасли еще не существовало. Немного позже ведущие фирмы мира активно занялись исследованиями в области использования таких сетей. Одной из первых фирма AT&T предложила для локальных сетей SYSTIMAX многоуровневую кабельную систему с разбивкой ее на структурные подсистемы.

Во-вторых, аппаратная платформа, которая базировалась в то время на отечественном оборудовании, как правило, работающем на собственных стандартах, не позволяла в сущности, понять, что же в конечном счете лежит в основе коммуникационной среды и каковы ее критические возможности. Кстати, следует заметить, что этот фактор был тогда свойствен практически всем без исключения терминальным сетям, развернутым на базе mainframe, включая и зарубежные.

В данной работе нет необходимости описывать различные типы кабельных сетей Ethernet, так как в литературе отечественных и зарубежных авторов, работающих в области информатики и телекоммуникаций, в настоящее время нет недостатка.

Нам представляется более интересным сопоставление полученных в результате сертификационных измерений параметров сети с теми, которые сформулированы и приняты в виде стандартов во всем мире.

Стандарты EIA/TIA-568 и TSB-36 нормируют следующие параметры витых пар: емкость, волновое сопротивление, коэффициент затухания и переходное затухание на ближнем конце (NEXT). При этом в соответствии со стандартами емкость не должна превышать 6.56 нф/100м для категории 3 и 5.57 нф/100м для категорий 4 и 5, а волновое сопротивление не должно превышать 100 + 15% ом.

Проведенные измерения кабельной системы в целом подтвердили категорию 3 по всем параметрам, за исключением некоторых лучей, длина которых превышала 175 м. Импеданс, а также затухание и NEXT имеют величины, превосходящие по качеству категорию 3. Однако в целом кабель-

ная сеть сертифицирована по 3-й категории и этот факт необходимо учитывать при дальнейшем развитии сети. В то же самое время структурированность кабельной системы позволяет заменять по сегментам части ее на более высокие категории или же перейти на оптоволоконные кабели на некоторых сегментах. Возможности для реализации высокоскоростных сегментов связи были заложены изначально в выборе устройства высокоинтеллектуального центра коммутации Linkbuilder 3GH, суммарная пропускная способность которого составляет 300 Мбит/с.

2. Развитие инфраструктуры ИВС ВЦ РАН

В настоящее время глобальные информационные сети, объединяющие все информационно-телекоммуникационные мировые структуры и сообщества различных стран и континентов, стали определяющими для общечеловеческого развития.

Развитие инфраструктуры ИВС ВЦ РАН связано с реализацией выхода ЛВС ВЦ РАН в глобальные сети. В качестве таковой была выбрана сеть INTERNET, являющаяся в настоящее время наиболее известной мировой сетью, охватывающей в силу своей специфики практически все глобальные, региональные и многие локальные сети, которые пожелали приобщиться к мировому сообществу.

Свойство INTERNET связывать в единое целое сети различных архитектур с помощью достаточно простых программных "шлюзов" позволяет называть ее сетью сетей.

Выбор нами INTERNET в качестве глобальной сети, в которой должна функционировать ЛВС ВЦ РАН, был также предопределен соответствующими решениями и планами РАН, Министерства науки РФ, РФФИ относительно развития средств взаимодействия научных исследовательских организаций России и крупнейших научных центров мира.

2.1. INTERNET. Общие сведения об архитектуре и истории развития

INTERNET - это название глобальной сети передачи данных.

Глобальная сеть - сложная программно-аппаратная система определенной архитектуры, объединяющая с целью обмена информацией множество ЭВМ (узлов сети), расположенных в самых различных местах земного шара. Узлы сети связаны каналами передачи данных. Непосредственными физическими каналами связаны близлежащие узлы. Обмен с удаленными узлами осуществляется по цепочке, маршруту, через промежуточные узлы. Но реализация обмена - это внутреннее дело системы, пользователь при обмене с удаленным узлом должен знать лишь его адрес, и при обмене с любым узлом всегда создается иллюзия непосредственной связи. Можно говорить, что между узлами сети существуют виртуальные каналы связи.

Все сетевые операции регламентируются определенным набором соглашений и правил - сетевыми протоколами. Протокол определяет виды сигналов, типы разъемов и кабелей, форматы данных, способы проверки и коррекции ошибок, алгоритмы для сетевых интерфейсов, методику и принципы подготовки и передачи сообщений и другие сетевые спецификации.

Архитектура сети определяется совокупностью отдельных структурных элементов (их часто не совсем точно тоже называют протоколами). Для получения в конкретном узле сети соответствующих сетевых функций эти элементы должны быть установлены (инсталлированы) и настроены (конфигурированы) для соответствующей программно-аппаратной среды уз-

ла. Во всех узлах сети в том или ином объеме эти элементы устанавливаются и настраиваются.

Архитектуры всех сетей многоуровневые. Все структурные элементы распределены по уровням. Нижний уровень - физический, на нем находятся элементы (в основном реализованные аппаратно), обеспечивающие физический обмен информацией между соседними узлами. Самый верхний уровень - прикладной - определяет набор основных функций пользователя в сети. На интерфейс прикладного уровня "сверху" выходят различные прикладные системы и так называемые программные оболочки, реализующие для пользователя доступ к сетевым функциям в удобном, комфортном виде. Между прикладным и физическим уровнями находятся промежуточные уровни сети.

Соседние уровни каждого узла имеют интерфейсы, с помощью которых и происходит реальная физическая передача информации с уровня на уровень. Преимущество уровневой архитектуры состоит прежде всего в том, что более высокие уровни узла сети могут "не знать" всех деталей операций на нижних уровнях. Наличие уровней облегчает также процесс модификации сетевых элементов. Так, если произошли изменения на физическом уровне, например изменился способ физической передачи информации, то достаточно поменять соответствующие протоколы, управляющие новым оборудованием, не трогая верхние уровни сети. И, наоборот, установка новых пользовательских систем, выходящих на интерфейс прикладного уровня, не требует модификации или замены протоколов, обеспечивающих передачу данных.

В начале 70-х годов Министерство обороны США разработало экспериментальную компьютерную сеть под названием Advanced Research Projects Agency (ARPA). К концу 70-х сформировались базовые протоколы этой сети Transmission Control Protocol (TCP) и Internet Protocol (IP). На основе этих протоколов в конце 80-х годов Национальный научный фонд США National Science Foundation (NSF) развернул новую сеть. Эта сеть первоначально объединяла несколько суперкомпьютерных центров с целью обеспечения комфортного доступа к вычислительным мощностям. Успех использования сети превзошел ожидания. Стало ясно, что сеть кроме удобного доступа к вычислительным ресурсам может предоставлять качественно новые средства по обмену разнообразной информацией. Сеть быстро развивалась вширь вначале на территории США, а затем и по всему миру, получив название INTERNET по имени своего стержневого протокола IP.

INTERNET объединяет в единую сеть отдельные ЭВМ (хосты), локальные сети ЭВМ, региональные сети, а также может иметь выходы через специальные "шлюзы" в глобальные сети другой архитектуры. Поэтому часто INTERNET называют сетью сетей.

Каждый узел сети INTERNET должен иметь по крайней мере один уникальный 32-разрядный адрес (IP-адрес). Регистрация этих адресов - важный организационный момент функционирования INTERNET. Об административных службах INTERNET будет сказано ниже.

Имеется 5 типов адресов (A,B,C,D,E). Принята специальная нотация для записи IP-адресов (dotted decimal notation). Адрес записывается в виде 4 байтов, разделенных точкой, каждый байт - в десятичном виде. Например, 193.232.81.200 .

Для средних по размерам локальных сетей, подключаемых в INTERNET, наибольшее распространение имеют сети класса C, где три старших байта - номер сети, а младший байт - номер хоста. В сети класса C не может быть хостов больше, чем 255.

Кроме цифровой идентификации в виде IP-адресов INTERNET поддерживает идентификацию хостов в виде составных имен. Каждое такое составное имя является либо именем хоста, либо именем множества имен конкретной локальной сети, либо именем множества множеств имен локальных сетей. Эти множества носят названия доменов. INTERNET поддерживает иерархию имен. Например, составное имя SUNNY.CCAS.RU обозначает, что хост под именем SUNNY находится в домене CCAS.RU, а домен

CCAS.RU - в домене RU. Степень вложенности имен может быть достаточно большой. Подобно регистрации IP-адресов существует регистрация имен доменов. Имеются также ответственные (организации и люди) за поддержание системы имен данного домена. Самый правый элемент в имени (RU, EDU, GOV и т.д.) - это идентификатор, соответствующий достаточно большому домену (страны или крупного ведомства). Например, RU - имя корневого домена локальных сетей России, EDU - сетей Министерства науки США, GOV- сетей правительства США, MSK.RU - сетей города Москвы. Сразу же обратим внимание, что такое "географическое" или "ведомственное" понимание структуры имен достаточно условно. Определяющим является не "география", а ответственность за данный домен. Важно то, где данный домен зарегистрирован.

Рассмотрим грубую схему передачи информации с некоторого узла A сети на узел B. В обоих узлах (A и B), как, впрочем, и в других узлах сети, установлено (инсталлировано) программное обеспечение, соответствующее протоколам разных уровней, произведено конфигурирование этих протоколов (настройка и заполнение соответствующих таблиц). Причем с точки зрения работы сети среда может быть разной. В узле A система протоколов может быть погружена, например, в MS DOS (или WINDOWS), поскольку в узле A - ЭВМ IBM PC, а в узле B - в среду OSF для ЭВМ ALPHA DEC 3000.

Допустим, пользователь на узле A с помощью соответствующего сервиса передает некоторый файл на узел B. Это значит, что на вход прикладного уровня на узле A поступает содержимое этого файла и адрес домена получателя на узле B. Программы прикладного уровня определяют IP-адрес получателя и формируют сообщение (message), которое поступает на вход транспортного уровня. Программы транспортного уровня "разрезают" message на пакеты (packets). В общем случае длинное сообщение на транспортном уровне преобразуется в цепочку пакетов определенной структуры и формата. Транспортный уровень по очереди передает пакеты сетевому уровню IP.

На уровне IP пакет преобразуется в дейтаграмму (datagram) - вид пакета на уровне IP. Программы канального уровня "разрезают" datagram и формируют так называемые кадры (frame), которые с помощью специальных программ канального уровня, умеющих управлять физической средой передачи, передаются одному из соседних узлов сети. Пройдя по физической цепочке узлов, информация кадр за кадром в конце концов дойдет до узла B. В узле B в результате последовательного перехода от программ нижнего уровня к верхнему произойдет обратное преобразование информации (frame - datagram - packet - message).

В INTERNET кадры и дейтаграммы передаются бесконтрольно. Только когда на транспортном уровне узла B будет принят и собран пакет, осуществится проверка и отправитель получит информацию о качестве передачи пакета. При передаче коротких сообщений в INTERNET используется специальный протокол транспортного уровня для быстрой бесконтрольной передачи User Datagram Protocol (UDP).

Ключевым уровнем является сетевой уровень IP. Информация (datagram) от отправителя к получателю проходит через цепочку IP-уровней различных узлов, пока не достигнет адреса получателя, где будет передана на уровень выше - на транспортный уровень.

Сеть INTERNET, в отличие от других глобальных сетей, не является сетью коммутации каналов. Это сеть коммутации пакетов. В INTERNET на время передачи сообщения не фиксируется маршрут движения информации (нет понятия сеанс - session). Поэтому очень важным является алгоритм IP-уровня, который определяет, куда дальше надо отправить принятую дейтаграмму, чтобы она в конце концов оптимальным образом дошла до адресата. IP-протокол перед отправкой дейтаграммы постоянно решает задачу выбора маршрута, естественно, если на узле имеется несколько интерфейсов для выхода дейтаграммы (gateway).

Выбор маршрута может быть реализован статически и динамически.

Статическая маршрутизация реализуется с помощью раз и навсегда заполненных при конфигурировании узла таблиц маршрутизации. Статическая маршрутизация применяется на хостах локальной сети и в узлах с небольшим числом gateway, когда алгоритм маршрутизации достаточно прост. В этом случае маршрутизационная таблица содержит несколько строчек с указанием соседей и маршрутизатора по умолчанию (default gateway). Обычно в каждой локальной сети, подключаемой к INTERNET, на один из хостов возлагаются функции главного маршрутизатора. Как правило, это хост со специфической архитектурой и средой, ориентированной на эффективное выполнение функций маршрутизации.

Маршрутизатор всегда должен быть в локальной сети, которая имеет много подсетей или обеспечивает выход в INTERNET для других сетей. Обычно сеть, имеющая подчиненные сети, особым образом регистрируется в административных структурах INTERNET в качестве так называемой автономной системы (АС). На маршрутизаторах на уровне IP задача маршрутизации часто реализуется динамически с помощью использования специальных обменов маршрутизационными таблицами между соседними АС. Это протоколы для определения достижимости узла (reachability) конечного адресата Border Gateway Protocol (BGP) или более старый аналогичный протокол Exterior Gateway Protocol (EGP). При динамической маршрутизации другие специальные протоколы самостоятельно формируют таблицы маршрутизации на основании накопления статистической информации для конкретных маршрутов. Это делается либо путем подсчета числа звеньев в маршруте (hope count), либо на базе детального знания топологии INTERNET Shortest Path First (SPF).

Как мы уже отмечали, сеть INTERNET является самой распространенной глобальной сетью в мире. Протоколы INTERNET стали стандартами де-факто. В 80-х годах была предпринята попытка создать сетевые стандарты. Международная организация по стандартизации International Standard Organization (ISO) представила в качестве стандарта 7-уровневую модель для взаимодействия открытых систем Open System Interconnection (OSI) - модель ISO-OSI. Этот стандарт является хорошим методическим средством при анализе различных сетей, отдельные сети используют некоторые протоколы ISO-OSI, но полной реализации этого стандарта не существует. INTERNET была реализована, когда стандарта ISO-OSI еще не существовало. Но и в настоящее время, несмотря на критику, протоколы INTERNET, являясь стандартами де-факто, имеют очень широкое распространение и продолжают развиваться.

Есть целый ряд причин такой живучести INTERNET. Прежде всего надо отметить, что практически для любой среды все фирмы вместе с системным программным обеспечением поставляют протоколы INTERNET, по крайней мере нижний уровень (TCP, IP и ниже). Популярность протоколов INTERNET сильно возросла с распространением ОС UNIX. Интеграция протоколов INTERNET с ОС Bercley Software Distribution UNIX (BCD UNIX) положила начало этому процессу. Сейчас ОС UNIX и протоколы INTERNET стали основными и обязательными компонентами операционной среды открытых систем. Часто даже говорят о UNIX-сети, как разновидности INTERNET.

Возвращаясь к причинам жизнестойкости INTERNET, отметим достаточную простоту включения отдельных узлов или локальных сетей в INTERNET. Поскольку практически все сетевые программные элементы уже имеются, то для того, чтобы стать пользователем INTERNET, достаточно лишь решить вопросы физического подключения, проведения линий связи, организационные вопросы по регистрации и идентификации подключаемых элементов, выполнить процедуры установки (инсталляции) и конфигурирования сетевых программных продуктов.

Получив через INTERNET следующие возможности: использование электронной почты (e-mail), обмен файлами (ftp), средства по работе с multimedia (например, www), удаленный доступ к вычислительным мощностям (telnet), - пользователь попадает в качественно новую среду использования вычислительной техники. Отдельные недостатки INTERNET на

первых порах не замечаются, они заслоняются новыми функциональными возможностями, которые приобрел пользователь. И только по истечении определенного времени использования INTERNET эти недостатки начинают проявляться (прежде всего в вопросах организации security).

Будущее покажет, в каком направлении пойдет развитие протоколов INTERNET. Скорее всего, не будет механического перехода на протоколы ISO-OSI, а будет происходить постепенное совершенствование и развитие собственных протоколов INTERNET под влиянием идей протоколов ISO-OSI в частности, а также новых идей, которые подсказывает реальная практика использования вычислительных сетей.

2.2. INTERNET как организационная структура

Организационная структура INTERNET достаточно своеобразна. Прежде чем ее описать, уточним, что понимается под термином INTERNET. Это сеть сетей, объединяющая на основе протоколов IP как сети TCP/IP-архитектуры, так и сети других архитектур, которые имеют общий с INTERNET пользовательский уровень.

Первоначально (еще во времена сети NSFNET - предшественницы INTERNET) было продекларировано некоммерческое использование INTERNET. Это совсем не значит, что через INTERNET нельзя выходить в коммерческие сети или что коммерческие сети не могут использовать TCP/IP-архитектуру. Коммерческие сети органично существуют в INTERNET как региональные сети, предоставляющие собственный сервис в виде линий связи, коннективности, информационных услуг. Естественно, у коммерческих региональных сетей должна быть договоренность с INTERNET по вопросам регистрации IP-адресов, политики маршрутизации, которая организуется таким образом, чтобы трафик коммерческих и некоммерческих сетей не смешивался.

В INTERNET нет общих централизованных финансовых расчетов за сетевые услуги. Каждый владелец локальной сети решает эти вопросы непосредственно со своим сетевым оператором. Сетевой оператор (network operator) - это организация, предоставляющая те или иные виды сетевых услуг.

Сетевые операторы подразделяются на поставщиков услуг Service Provider (SP) и клиентов (customers). SP - это такой сетевой оператор, сеть которого служит для предоставления какого-либо сетевого сервиса для других организаций - своих клиентов. Под сервисом понимаются самые различные услуги: от предоставления физической возможности выхода в INTERNET (коннективность) до самых разнообразных функций верхнего прикладного уровня (e-mail, ftp, telnet, www, news и т.д.).

В действительности граница между SP и customers не такая четкая. Многие клиенты для других организаций в свою очередь являются SP по другим функциям. Даже SP, предоставляющий коннективность своим клиентам, может быть клиентом у другого SP, поскольку, например, покупает у него коннективность на зарубежные узлы сети.

Очень распространенным является бесплатное предоставление сервиса INTERNET. На самом деле в этом случае оплата производится централизованно государством, спонсором, ассоциацией или фондом. Часто эти субъекты на свои средства сами создают и содержат специальных сетевых операторов. Возможны случаи смешанной оплаты сетевого сервиса: за линии связи и соответствующее оборудование платит организация-пользователь, а услуги оплачиваются названными выше субъектами. Примерно по такой схеме организуется работа с INTERNET в научных, исследовательских и учебных организациях России.

Итак, в INTERNET нет надобности в центральном финансовом органе и практически отсутствует жесткое центральное администрирование. Функции администрирования исполняются распределенно, на местах. Очень

важной является фигура местного сетевого администратора. Надежная работа INTERNET в значительной степени зависит от квалификации и качества работы сетевых администраторов на местах, которые работают в тесном контакте друг с другом, постоянно в случае необходимости обмениваясь служебной информацией через e-mail. Особенно актуальными в настоящее время являются корпоративные действия сетевых администраторов в борьбе со всякого рода нарушителями и "взломщиками", поскольку "взлом" частной локальной сети может существенно отразиться на надежной работе INTERNET в целом.

Сетевых администраторов можно, таким образом, считать представителями организационных структур INTERNET на местах.

В то же время имеются по крайней мере три задачи организационного плана, которые необходимо решать "сверху":

- изучение и обобщение информации по техническим проблемам в результате использования INTERNET, выработка новых методик и стандартов;
- регистрация узлов, локальных и региональных сетей (раздача IP-адресов, имен доменов);
- рассмотрение жалоб и применение санкций к участникам INTERNET, нарушающим общие правила работы в INTERNET.

Для решения прежде всего этих задач существуют центральные административные органы INTERNET.

Центральный орган INTERNET называется INTERNET Activities Board (IAB) и состоит из 2 подкомитетов: INTERNET Research Task Forse (IRTF) и INTERNET Engineering Task Forse (IETF).

IRTF - это общественная исследовательская организация, собирающая разнообразную информацию на базе опыта эксплуатации INTERNET, проводит исследования и разработки, направленные на повышение эффективности и комфортности работы в INTERNET.

IETF занимается оформлением новых стандартов, которые описываются в специальных документах INTERNET под названием Request For Comments (RFC). Этих документов несколько тысяч. Доступ к ним имеет каждый пользователь через средства самой сети. Базы данных, где хранятся документы RFC, постоянно пополняются и обновляются. Если создаются новые проекты, протоколы или правила регистрации, то IETF через сеть может устроить обсуждение проектов (draft-документов). IETF собирает мнение пользователей по draft-документам, а затем создает новый документ или новую версию старого RFC-документа. База данных с RFC-документами - ценнейшая информация прежде всего для системных программистов, обеспечивающих администрирование INTERNET на местах.

Другую важную организационную работу, связанную с регистрацией IP-адресов и других атрибутов сети, производит специальный орган INTERNET под названием Network Information Center (NIC).

В связи с значительным расширением INTERNET (в среднем за месяц число узлов увеличивается на 6%) уже в 1989 г. некоторые административные функции были частично переданы из центра (США) на материки соответствующим континентальным организациям. В Европе это организации Reseaux IP Europeens (RIPE) и RIPE Network Coordination Centre (RIPE NCC).

RIPE - открытая и добровольная организация, осуществляющая в тесном взаимодействии с IAB административную и техническую координацию в INTERNET. RIPE строит свою работу при тесном взаимодействии с общественной организацией - ассоциацией пользователей INTERNET под названием Trans-European Research and Education Networking Association (TERENA), которая была создана в октябре 1994 г. в результате слияния двух организаций Reseaux Associes pour la Recherche Europeens (RAPE) и European Academic and Research Network (EARN) с целью содействия развитию и распространению новых передовых методов создания высококачественных международных информационных систем и сетевой инфраструктуры в области науки и образования.

Другая европейская организация RIPE NCC имеет чисто организационные функции с точки зрения функционирования INTERNET:

- регистрирует в своей базе данных (Network Management Database) информацию об IP-сетях. Любой пользователь может прочитать любую информацию о любой сети из этой базы данных (функция WHOIS);
- выдает IP-адреса по согласованию с NIC и с помощью местных организаций стран, работающих в INTERNET - Local INTERNET Registry (LIR);
- координирует сбор статистики;
- координирует службу имен - Domain Name Service (DNS);
- составляет графическую карту сетей.

Так выглядит система центральных органов INTERNET. Группа сетей, имеющая четко определенную маршрутизационную политику, которая используется несколькими сетевыми операторами, называется автономной системой. АС - это еще один субъект сети; АС, так же как и IP-адрес и имя домена, должна быть зарегистрирована в RIPE NCC.

Не вдаваясь в данной работе в разъяснение термина "маршрутизационная политика", отметим, что она существенно определяет эффективность работы INTERNET, объем трафика. Показатели производительности сети INTERNET, являющейся сетью коммутации пакетов, во многом зависит от того, как на уровне IP реализуется задача маршрутизации. Объединение отдельных сетей в АС и использование специальных служебных протоколов (IGP, EGP или BGP) позволяют за счет организации так называемой динамической маршрутизации использовать INTERNET более эффективно.

Объединение сетей в АС также преследует цель минимизировать размеры маршрутизационных таблиц на маршрутизаторах сети. Эти таблицы с ростом INTERNET имеют тенденцию переполняться.

Как мы отмечали, важной функцией административных органов является раздача и регистрация IP-адресов. Уникальность адреса любого узла в INTERNET - это необходимое условие функционирования INTERNET. Функции регистрации исполняются по цепочке NIC - RIPE NCC - LIR - заказчик. Выдача IP-адресов происходит на основании заявок от заказчика, оформляемых по специальным формам. В случае удовлетворения заявки соответствующая информация помещается в базу данных RIPE.

32-разрядный адрес INTERNET - это ее слабое место. Сейчас в связи с бурным ростом числа узлов в INTERNET совершенно очевидно, что этого количества адресов может в скором времени не хватить. Действительно, сейчас в INTERNET в Европе зарегистрировано примерно 1 млн. узлов, а в мире - 4 млн. Это значит, что в INTERNET может наступить адресный кризис. Предпринимаются попытки выхода из этого кризиса. Есть два направления. Первое, глобальное, состоит в увеличении размерности адреса. Рассматривается переход на 48-разрядный адрес. Второе направление (оно не противоречит первому, а лишь дополняет его) состоит в совершенствовании методики раздачи адресов локальных сетей и АС.

Кратко суть этой методики заключается в следующем.

Необходимо обеспечить уникальность каждого регистрируемого адреса, поэтому место, где получается адрес локальной сети, должно быть единственным. Как правило, функции LIR возложены на SP. Если неизвестно, куда обращаться по поводу регистрации, то всегда можно выяснить это, послав e-mail в RIPE NCC.

При раздаче IP-адресов должны преследоваться две главные цели:

- routability - маршрутизируемость, которую можно повышать при определенной методике раздачи адресов. Сети должны объединяться в АС. И если адреса сетей, входящих в АС, будут совпадать по старшим адресам, то можно агрегировать маршрутизационную информацию, т.е., повышение степени routability достигается за счет агрегации (aggregation);
- conservation - сокращение, которое достигается тем, что при рассмотрении заявок надо тщательно рассматривать их обосно-

ванность; заявки не должны заказывать адреса впрок, хотя при заявке учитывается планирование развития в сети на два года вперед.

Эта процедура, которая вводится в действие в 1996 г., должна усовершенствовать процесс регистрации адресов. Выдавать адреса будут в агрегированном виде и достаточно экономно, ровно столько, сколько их в действительности нужно.

Таковы вкратце некоторые организационные особенности INTERNET. Они, безусловно, так же, как и протоколы INTERNET, будут меняться и совершенствоваться.

2.3. Основные возможности пользователей INTERNET

Успехи и удачи INTERNET (и неудачи тоже) определяются в значительной мере теми возможностями, которые предоставляет INTERNET непосредственно пользователю.

Пользователи INTERNET работают со специальными программными системами и оболочками, которые существенно используют различные протоколы прикладного уровня сети. Некоторые программы протоколов прикладного уровня доступны пользователям непосредственно:

- r-команды (remote) для выполнения различных функций на удаленных машинах (rlogin, rcp, rsh и др.), фактически это сетевые аналоги некоторых UNIX-команд;
- telnet - протокол прикладного уровня INTERNET для эмуляции терминала, обеспечивающий доступ к удаленным машинам (во многом аналогичен rlogin);
- ftp (file transfer protocol) - протокол прикладного уровня INTERNET, обеспечивающий обмен файлами с удаленной машиной.

С помощью перечисленных и некоторых других протоколов прикладного уровня сети создан определенный сервис в виде ряда информационных систем и оболочек. Назовем некоторые из них.

E-mail (electronic mail) - электронная почта. Самая распространенная в настоящее время прикладная система INTERNET. Фактически в настоящее время e-mail стала новым способом обмена информацией между людьми, новым видом связи наряду с обычными: почтой и телеграфом, радио и телесвязью, факсом.

Существуют различные системы поиска информации о людях и организациях. Имеются, например, службы справочной информации о пользователях на машинах. Для поиска может быть использована UNIX-команда finger. Другой пример такого рода систем - это доступ с помощью команды whois к базе данных, хранящей информацию о всех зарегистрированных в NIC и RIPE организациях, работающих в INTERNET.

WAIS - это интерактивная оконная система для поиска по ключевым словам.

GOPHER - интерактивная оболочка INTERNET. В виде системы вложенных меню в удобной форме предоставляет возможность использовать большинство функций и систем прикладного уровня INTERNET, переключаться в рамках одного сеанса с одной системы на другую.

WWW - World Wide Web - самая распространенная в настоящее время система верхнего уровня INTERNET. Подробнее о WWW - в разд. 3.5.2.

ARCHIE - это система сбора, поиска и выдачи информации об общедоступных файлах. Если ftp - это средство, помогающее непосредственно добраться до файла, местонахождение которого известно, то система ARCHIE помогает организовать поиск информации и найти имена соответствующих файлов, где находится искомая информация. По всему миру разбросаны archie-серверы, которые осуществляют сбор информации, ее систематизацию по областям знаний и поиск информации по запросам archie-клиентов.

Прикладной системный уровень INTERNET развивается достаточно стремительно, и не исключено, что, пока готовится к изданию данная монография, появится новая, более совершенная по своим возможностям прикладная система INTERNET.

3. Особенности подключения ЛВС ВЦ РАН к INTERNET

3.1. Маршрутизатор CISCO 4500

Выше отмечалось, что IP-протокол в системе протоколов INTERNET играет ключевую роль. Главная функция протокола IP - маршрутизация. В самом общем виде задачу маршрутизации можно определить так: на входе программы протокола IP на некотором хосте имеется пакет (от верхних протоколов - TCP или UDP, например) с адресом доставки и задача маршрутизации должна определить, куда, на какой сетевой интерфейс необходимо отправить этот пакет.

Внутри локальной сети задача маршрутизации решается на каждом узле достаточно просто и эффективно, поскольку число узлов локальной сети относительно невелико, а маршруты в пределах одной сети в основном однозвенные и определены статически.

Для эффективной производительной работы при обменах между локальными сетями, включенными в INTERNET, необходимо на входе (выходе) в каждую локальную сеть иметь специальный компьютер, который занимался бы исключительно задачей маршрутизации.

Задача маршрутизации работает с маршрутизационными таблицами. Выше уже говорилось о статической и динамической маршрутизации, о локальных сетях, имеющих подсети и объявленных так называемыми автономными системами, и о специальных протоколах по обмену маршрутизационной информацией (EGP, BGP). Со всем этим работает задача маршрутизации протокола IP.

Совершенно очевидно, что общая эффективность работы в INTERNET во многом зависит от того, насколько эффективно выполняется задача маршрутизации.

Поэтому требования к специализированному компьютеру, занимающемуся задачей маршрутизации, достаточно высоки. Это должен быть компьютер достаточно быстрый, а память его не должна быть сдерживающим фактором для имеющих тенденцию расширяться маршрутизационных таблиц.

Очевидно, что по мере расширения INTERNET вширь будет постоянно стоять проблема замены маршрутизатора на более мощный. Именно с учетом этого опережающего фактора вместо рекомендованного маршрутизатора CISCO 4000-M была приобретена более мощная его модификация - CISCO 4500.

Фирма CiscoSystems, Inc выпускает целый спектр специализированных компьютеров с соответствующим программным обеспечением. Главное назначение этих компьютеров - реализация соответствующих сетевых функций.

Серия CISCO 4000 - это высокопроизводительные маршрутизаторы. Имеется несколько модификаций этой серии: CISCO 4000-M, CISCO 4500, CISCO 4500-M.

В ЛВС ВЦ РАН в качестве главного маршрутизатора используется модель CISCO 4500. По сравнению с CISCO 4000-M она имеет более мощный процессор, более объемную и быструю оперативную память и обладает возможностями для расширения такой памяти.

Маршрутизаторы серии CISCO 4000 работают под управлением операционной системы Cisco IOS. В настоящее время используется версия IOS 10.3

Для обеспечения возможности централизованного обновления версии программного обеспечения в маршрутизаторах используется технология Flash EEPROM. После того как программное обеспечение обновлено, маршрутизатор может быть перезагружен с помощью программ, хранящихся в локальной Flash-памяти. CISCO 4000 под управлением IOS 10.3 помимо функций маршрутизации реализует дополнительно еще шесть функций, что определяет достаточно универсальное использование этого компьютера.

С помощью Cisco IOS обеспечивается надежное сетевое взаимодействие, поддерживаются различные протоколы локальных и глобальных сетей, оптимизируется работа с глобальными и локальными сетями, имеется возможность управлять доступом на различных уровнях сети.

Последнее очень важно, поскольку позволяет более надежно решать проблемы повышения защищенности системы от несанкционированного доступа к ресурсам ЛВС.

Маршрутизаторы CISCO 4000 могут поддерживать различные комбинации до трех модулей сетевых процессоров (имеется три слота для установки соответствующих микросхем). Могут быть установлены следующие сетевые процессоры:

- однопортовый Ethernet;
- двухпортовый Ethernet;
- однопортовый Token Ring;
- двухпортовый Token Ring;
- многорежимный (многомодовый) FDDI с одинарным или двойным подключением;
- однорежимный FDDI с двойным подключением;
- двухпортовый последовательный;
- четырехпортовый последовательный;
- четырехпортовый ISDN BRI;
- восьмипортовый ISDN BRI;
- однопортовый канальный T1/ISDN PRI;
- однопортовый канальный E1/ISDN PRI (сбалансированный и несбалансированный);
- четырехпортовый последовательный G.703 (сбалансированный и несбалансированный);
- однопортовый, одномодовый или многомодовый ATM.

Поддерживается очень большое количество различных протоколов, а также скоростей и сред передачи. Как следствие этих возможностей CISCO 4000 могут быть использованы во всех наиболее распространенных программно-аппаратных средах.

3.2. Сетевой терминальный сервер NTS

(Network Terminal Server)

Доступ к вычислительным и информационным ресурсам ЛВС возможен как с рабочих станций и персональных компьютеров, которые непосредственно являются узлами ЛВС, так и с терминалов.

Различают терминалы, находящиеся в непосредственной близости от узлов локальной сети (до 300 м), и удаленные терминалы. В качестве терминалов могут быть использованы как специальные устройства, так и универсальные компьютеры: персональные или рабочие станции, где функция удаленного терминала реализуется как одна из множества функций среды.

Удаленные терминалы чаще всего связаны с узлами локальной сети по обычным телефонным линиям (выделенным или коммутируемым). Для связи используется два модема (один у терминала и один у узла сети).

Количество терминальных входов у узлов локальной сети обычно ограничено (1 или 2 последовательных порта). Поэтому при желании иметь достаточно развитую терминальную сеть, необходим специальный компьютер, через который осуществляется вход в локальную сеть от большого количества терминалов.

Имеется еще одна важная причина организации специального терминального входа в ЛВС через специальный компьютер - это более надежная организация защиты системы от несанкционированного доступа.

В качестве такого специализированного компьютера для организации работы с терминалами по выделенным и коммутируемым линиям используется продукт фирмы SUN под названием Network Terminal Server (NTS).

NTS - это достаточно универсальное устройство, которое хотя и использовано в ЛВС ВЦ РАН прежде всего для работы с терминалами, но может быть использовано для решения других задач в локальной сети.

NTS - это мощное средство для организации разнообразного доступа к Ethernet, повышения мощности ЛВС. С помощью NTS осуществляется подключение практически любых последовательных и параллельных внешних устройств (например, принтеров).

Поскольку NTS был спроектирован специально для использования в UNIX-среде, то пользовательские интерфейсы соответствуют стандартам UNIX (BSD 4.2 и 4.3), а сетевые интерфейсы реализуют соответствующие протоколы INTERNET (TCP/IP, SLIP, PPP и т.д.).

NTS для собственного включения в локальную сеть имеет два интерфейсных порта:

- 10BASE5 Ethernet-порт с коннектором DB15;
- 10BASET Ethernet-порт для связи с локальной сетью по витым парам через коннектор RJ45.

Имеется специальный порт с 8-контактным коннектором RJ45 для связи с консолью. Этот порт предоставляет возможность работы NTS в автономном режиме через монитор со специальным программным обеспечением. Монитор предоставляет определенный набор команд.

Программируемый порт для подключения принтера с 25-контактным коннектором поддерживает стандартные параллельные интерфейсы принтеров (centronics или dataproducts).

Основное оборудование NTS - это главный процессор и два контроллера по управлению терминалами Serial Line Controllers (SLC). Каждый SLC имеет внешний выход на шесть 50-контактных PBX Champ-коннекторов. Каждый коннектор обеспечивает выход на 4 или 6 последовательных портов. Таким образом, один SLC имеет 32 порта. Всего имеется два SLC, т.е. максимальное число портов 64. Один NTS обеспечивает одновременную работу по 64 выделенным и коммутируемым телефонным линиям. При реальной работе по телефонным линиям на входе каждой линии должен быть модем (при 64 портах - 64 модема).

В ЛВС ВЦ РАН при работе по телефонным линиям все 64 модема собраны в единый блок. Для этих целей используется специальная модемная стойка ZyXEL RS1602, о которой будет рассказано ниже.

Основной процессорный узел NTS - это три 32-разрядных процессора и оперативная память (RAM) необходимого объема для поддержки заданной конфигурации.

NTS имеет еще постоянную память (ROM). Эта память хранит специальный командный монитор. Специальная энергонезависимая память EEPROM хранит конфигурационные параметры NTS. Через терминал, подключенный к консольному порту, можно использовать команды ROM-монитора:

- изменять и просматривать установки EEPROM-параметров;
- исполнять интерактивные диагностические тесты NTS;
- получать информацию и статистику по использованию соответствующего оборудования и локальной сети;
- загружать NTS (вручную).

Собственных дисков NTS не имеет. Поэтому программное обеспечение в виде исполняемого кода загружается через сеть со специальной ЭВМ, объявленной для данного NTS загрузочным сервером, либо с другого NTS, также сконфигурированного в качестве загрузочного сервера для данного NTS, либо из специальной FLASH-памяти.

Предполагается, что NTS вместе со своим специальным программным обеспечением должен функционировать постоянно. Поэтому имеется специальный аппарат (watchdog timer), который перевызывает системное программное обеспечение и делает соответствующие начальные установки (reset) через определенные интервалы времени.

Кроме автономного программного обеспечения (команд монитора) имеется специальная операционная система NTS, которую часто называют Annex. Annex - это фабричная марка фирмы Xilogics, Inc. На NTS в ЛВС ВЦ РАН используется версия 7 этого программного обеспечения - 1.0 Sun Network Terminal Server (R7.0). После процедур установки и конфигурирования Annex постоянно работает, размещаясь в оперативной памяти NTS, и связывается по сети с UNIX-хостом либо через аппарат стандартного протокола TFTP, либо через аппарат RPC (запуск удаленных процедур в UNIX), взаимодействуя со специальным "демоном" ERPCD, запущенным на UNIX-хосте.

Операционная система NTS Annex предоставляет пользователю множество команд. Это множество делится на две группы. Первая группа команд - это команды администратора. Их реализует программа сетевого администратора Network Administrator (NA). С помощью этих команд можно просмотреть и изменить параметры NTS и его портов, выдать соответствующие распечатки (dumps), передать сообщения по соответствующим портам, произвести перезагрузку NTS.

Другая группа команд Command Line Interpreter (CLI) - это командный интерфейс для пользователя. В частности, через команду admin суперпользователь (системный администратор) также может выйти на подмножество команд администратора NA.

Первичная настройка NTS осуществляется с помощью команд монитора (с терминала, подключенного через консольный порт), а затем вся работа производится через команды NA и CLI.

Разбиение команд на пользовательские и команды администратора предполагает, что, вообще говоря, можно по отдельным портам дать возможность пользователю самому управлять настройкой параметров порта. Речь идет о том, что главный администратор может предоставить исполнение некоторых функций администратору отдельной линии (порта). Для среды ЛВС ВЦ РАН фактически все действия с NTS - это прерогатива системных администраторов и поэтому пользователь (в понимании ВЦ РАН) не имеет доступа к командам Annex и, естественно, монитора.

Ограничимся изложенным выше в рассказе об NTS и его возможностях. Конкретная работа администратора при работе с NTS заключается в следующем:

- установка NTS;
- конфигурирование NTS;
- загрузка NTS;
- конфигурирование портов.

Конфигурирование портов состоит в определении через команды CLI соответствующих спецификаций и в возможности использования через эти порты определенных сетевых протоколов. Через соответствующие команды администратор может просматривать и менять установки, собирать статистику.

NTS предоставляет системному администратору сети возможность сделать работу ЛВС более защищенной от несанкционированного доступа к ЛВС. Иными словами, NTS имеет дополнительные средства для security. Кроме средств по защите собственно Annex можно повысить уровень контроля по входу в ЛВС, поскольку вход в ЛВС по всем выделенным и коммутируемым линиям проходит через NTS.

На NTS реализовано так называемое host-based security, т.е. защита, реализованная с помощью "демона" на сервере. С этой целью имеется специальный программный протокол Access Control Protocol (ACP), предоставляющий следующие функции:

- разрешение (запрещение) пользователю работать с CLI;
- разрешение (запрещение) пользователю использовать данный порт;
- разрешение использовать через порт конкретный узел ЛВС;
- протоколирование действий пользователя через порт;
- разрешение пользоваться через данный порт протоколом Point to Point Protocol (PPP);
- разрешение доступа через порт по коммутируемой линии.

В последующих версиях Annex мы намереваемся использовать новые средства защиты, с тем чтобы в значительной степени повысить надежность системы при работе по коммутируемым линиям.

Непосредственная работа по выделенным и коммутируемым линиям возможна только после соответствующей настройки модемов (по 2 на каждую линию). Очевидно, что при 64 линиях она требует создания определенной методики их обслуживания. Такая методика с использованием модемной стойки ZyXEL RS1602, управление которой со стороны администратора организуется с персонального компьютера с помощью специального программного средства ZyVIEW, работающего в среде MS Windows, отработана в ВЦ РАН и описывается ниже.

3.3. Модемная стойка ZyXEL RS1602

Доступ к ИВС ВЦ РАН через коммутируемые линии реализован с помощью модемной стойки ZyXEL RS1602, которая представляет собой модульную систему, имеющую 16 слотов для установки модемов-модулей, платы управления NB-100 и контроллер. Данная структура позволяет легко наращивать и модернизировать систему, причем замена одного из элементов может быть произведена без остановки системы в целом.

В качестве модемов-модулей используются модемы U-1496R Plus, поддерживающие все стандартные протоколы передачи данных для скоростей от 300 до 14400 бит/с, а также высокоскоростные протоколы передачи данных фирмы ZyXEL (ZyX 16800 и ZyX 19200) на скоростях 16800 и 19200 бит/с в режиме полного дуплекса. Для совместимости с различным программным обеспечением в модеме реализованы две системы команд - Hayes AT и V.25bis. Коррекция ошибок и компрессия данных могут производиться по протоколам MNP3-4, V.42 и MNP5, V.42bis.

Контроллер модемной стойки осуществляет опрос состояния и программирование модемов, находящихся в блоке, хранит конфигурацию модемов, контролирует работоспособность источника питания, реализует порт Network Management System (NMS). Контроллер имеет на передней панели небольшой дисплей. Конфигурация модемов и просмотр текущего состояния может осуществляться при помощи клавиш управления, расположенных также на передней панели контроллера.

Модуль NB-100, входящий в состав стойки, используется для подключения компьютера администратора. Плата занимает 1 слот и является интерфейсом для подключения к NMS-порту контроллера RS-1602. Дополнительно плата NB-100 поддерживает режим UDP/IP, позволяющий организовать управление системой модемов через сеть.

3.3.1. Система администрирования модемной сети

ZyVIEW - это программа администратора системы ZyXEL NMS. Пакет ZyVIEW 2.5 работает в среде Microsoft Windows и позволяет осуществлять управление системой ZyXEL RS1602 как с компьютера, непосредственного подключенного к ней, так и через локальную сеть с использованием протокола Serial Line IP (SLIP).

Пользуясь пакетом ZyVIEW, можно тестировать, изменять конфигурацию и переустанавливать любой модем, входящий в систему. Кроме информации о состоянии модемов мы можем также получить данные о качестве используемого канала. Контроль за качеством канала включает в себя контроль за текущим протоколом передачи данных, за используемым способом коррекции ошибок, отношением уровня шума и принимаемого сигнала и за другими параметрами. Программа может работать в фоновом режиме, а вся статистика о работе модемов и сообщения об обнаруженных неполадках автоматически фиксируются в непрерывно ведущемся журнале, что позволяет существенно сократить время на наладку системы, локализацию и устранение неисправностей.

3.3.2. Подключение модемов

Каждый из модемов, входящих в состав стойки ZyXEL RS1602, через разъем RS232 подключается к одному из портов терминального сервера NTS. Модемы на NTS могут быть сконфигурированы так:

- передающий;
- принимающий;
- двунаправленный.

При этом параметры модема и параметры порта должны быть согласованы между собой. Порты NTS обрабатывают три входных и два выходных сигнала модема. Методы обработки этих сигналов определяются следующими параметрами порта: control_lines, input_flow_control, output_flow_control, bidirectional_modem, need_dsr.

При использовании управляющих сигналов модема NTS выдает сигнал Data Terminal Ready (DTR) и ожидает от модема сигналов Data Carrier Detect (DCD) и Data Set Ready (DSR), после чего начинает сессию. Во время сессии каждая потеря сигнала DCD более чем на 400 мс, или потеря DSR вызывает сброс порта. При этом сигнал DTR перестает подаваться и все процессы, связанные с портом, прерываются.

При использовании аппаратного контроля передачи данных NTS выдает сигнал Reguest To Send (RTS), когда он готов принимать данные, и проверяет наличие сигнала Clear To Send (CTS) от модема перед началом процесса передачи.

При использовании программного контроля передачи данных NTS посылает сигнал XOFF, если он не может принимать данные, и XON, когда он опять готов к приему. При получении сигнала XOFF NTS приостанавливает передачу данных до тех пор, пока не будет получен сигнал XON.

Возможно использование смешанного контроля передачи данных. При этом NTS обрабатывает сначала аппаратные (программные) сигналы, а затем сигналы модема.

Параметр bidirectional_modem говорит о возможности управления модемом до посылки сигнала DCD. Если этот параметр установлен в Y для порта с включенным режимом обработки сигналов модема, то пользователь не сможет подключаться к порту и посылать команды модему до тех пор, пока сигнал DCD не будет послан.

Если параметр need_dsr устанавливается в Y, то связь будет обрываться при отсутствии сигнала DSR, иначе NTS будет подтверждать на-

личие связи, но в действительности связь с модемом будет установлена только после получения сигналов DSR и DCD.

3.4. Системные работы по подключению к INTERNET

Не вдаваясь в детали, перечислим основные работы по развитию инфраструктуры ЛВС ВЦ РАН:

- получение в RIPE (через соответствующие местные регистрирующие организации - LIR) IP-адреса для нашей локальной сети; вначале была зарегистрирована сеть класса С для ЛВС ВЦ РАН, затем в соответствии с планом развития ЛВС ВЦ РАН и ее подсетей получены 16 адресов сетей класса С (по 255 адресов для каждой подсети);
- регистрация имени домена (ccas.ru);
- регистрация ВЦ РАН в качестве автономной системы (AS2587);
- выбор и приобретение системного маршрутизатора ЛВС ВЦ РАН - CISCO 4500;
- выбор и приобретение NTS и CISCO 2522, а также модемной стойки ZyXEL для организации эффективной работы по выделенным и коммутируемым линиям;
- проведение согласования с соседними АС по маршрутизации AS2587;
- установка и конфигурирование соответствующего сетевого программного обеспечения во всех узлах сети, включая коммуникационное оборудование.

В результате проведенных системных работ для ЛВС ВЦ РАН обеспечены следующие виды доступа в INTERNET из ЛВС ВЦ РАН:

- непосредственный доступ с узлов ЛВС ВЦ РАН (через CISCO 4500 и CISCO CATALIST в узле ЮМОС);
- доступ по выделенным линиям с отдельных машин, вне ЛВС ВЦ РАН, и от подсетей с использованием асинхронных модемов (скорости до 19200 бод), стойки ZyXEL, NTS с обеспечением работы по протоколам SLIP и PPP;
- то же для коммутируемых линий (режим dial up со звонком).

С целью увеличения скорости работы по выделенным и коммутируемым линиям в настоящее время начаты работы по подключению удаленных локальных подсетей и отдельных машин вне ЛВС по синхронным модемам с использованием CISCO 2522 и модемов Motorolla Codex, Rad.

Со всех узлов ЛВС ВЦ РАН в полном объеме обеспечена работа с основными прикладными системами и оболочками INTERNET. Основными внешними функциями ЛВС ВЦ РАН (официально поддерживаемыми системными администраторами) считаются в настоящее время e-mail, ftp, www.

В течение первого года использования INTERNET доступ извне был возможен на все узлы ЛВС ВЦ РАН и разрешалось по любым видам доступа использование полного набора функций INTERNET. Однако, столкнувшись с неоднократными попытками взломов системы, мы пришли к необходимости ограничения функций внешнего доступа.

В настоящее время начаты работы по развитию средств защиты для ЛВС ВЦ РАН. В связи с этим приняты следующие ограничения по доступу в ЛВС ВЦ РАН извне:

- доступ извне по telnet возможен только к специально выделенным для этих целей машинам (шлюзам);
- доступ в INTERNET извне через ЛВС ВЦ РАН возможен через выделенные и коммутируемые линии, но при этом четко определены конкретные функции для работы по этим линиям с одновременным запретом использования других функций.

Для реализации всех средств защиты активно используются соответствующие средства на CISCO 4500 (например, закрытие конкретных

внешних функций на серверах ЛВС ВЦ РАН) и NTS (например, контроль работы по коммутируемым линиям). Также активно используется наличие нескольких сетей: внутренняя сеть имеет одни IP-адреса, по которым доступ извне невозможен, а все серверные машины, обеспечивающие доступ к ЛВС ВЦ РАН извне (анонимный ftp, www-сервер, e-mail), собраны в отдельной подсети.

Это лишь фрагмент из большой работы по развитию средств защиты ЛВС ВЦ РАН, к которой мы только приступили и которую собираемся активно продолжать на третьем этапе развития ИВС ВЦ РАН. Некоторые общие подходы к проблеме защиты изложены ниже.

3.5. Особенности некоторых системных работ

В этом разделе мы решили подробнее осветить содержание некоторых системных работ, связанных с настройкой отдельных компонент INTERNET.

3.5.1. Организация работы с электронной почтой в ЛВС ВЦ РАН

Работа с электронной почтой (e-mail) осуществляется в ЛВС ВЦ РАН на базе межсетевой почтовой службы sendmail в операционной системе SunOs.

Для функционирования этой службы было проведено конфигурирование локальной сети для e-mail. Для этого в сети должно быть три типа машин (хостов): mailbox-сервер, mail-клиенты и mail-хост. На mailbox-сервере находится так называемый системный "почтовый ящик" - mailbox в каталоге /var/spool/mail. В этом каталоге располагаются файлы с именами ./user_name, являющиеся почтовыми ящиками соответствующих пользователей. В ЛВС ВЦ РАН mailbox-сервер один (sunny), а системный mailbox (каталог /var/spool/mail) общий для всех хостов сети. Это означает, что все хосты локальной сети могут "монтировать" этот каталог сервера по NFS-протоколу. Сервер, в свою очередь, осуществляет "экспортирование" этого каталога всем хостам сети. Таким образом, локальные каталоги mail-клиентов (хостов) становятся одним общим почтовым каталогом. Это дает возможность собирать и хранить почту в одном месте независимо от того, по какому адресу было отправлено письмо: по адресу username@domainname или username@hostname.domainname.

Главная почтовая машина - mailhost осуществляет прием и передачу почтовых сообщений как внутри локальной сети, так и вне ее. В ЛВС ВЦ РАН mailhost-сервер и mailbox-сервер - это одна и та же рабочая станция. Для того чтобы ее отметить как mailhost в файле /etc/hosts (а также в NIS-базе данных) рядом с именем этой рабочей станции необходимо поместить и синоним mailhost. Остальные хосты локальной сети носят название subsidiares, т.е. вспомогательные хосты, они же - mail-клиенты.

На каждой из рабочих станций сети выполняется программа sendmail, которая реально и ведет диалог с пользовательским почтовым интерфейсом по отправлению и получению почтовых сообщений. Sendmail связан со своим конфигурационным файлом /etc/sendmail.cf. Содержимое этого файла должно совпадать с содержимым файла /usr/lib/sendmail.main.cf или файла /usr/lib/sendmail.subsidiary.cf соответственно для mail-хоста и вспомогательных хостов. По умолчанию на рабочих станциях конфигурационный файл соответствует файлу для вспомогательных хостов.

В локальной сети ВЦ РАН функционирует DNS, поэтому на mail-хосте (он же DNS-сервер) вместо sendmail-демона запущена программа /usr/lib/sendmail.mx. Кроме этого, в конфигурационных файлах службы DNS указывается mail-хост как Mail eXchanger (MX), т.е. хост, умеющий передавать почтовые сообщения для всех машин локальной сети.

Кроме /var/spool/mail (главного системного "почтового ящика") на почтовом сервере имеется еще один важный каталог /var/spool/mqueue - каталог очередей почтовых сообщений. Вся входящая и исходящая почта проходит через этот каталог и оседает здесь только в случае невозможности сразу передать почтовое сообщение. Периодически производятся повторные попытки "освободить очередь", а по истечении определенного срока сообщение возвращается пославшему его. Периодичность и предельные сроки определяются как содержимым конфигурационного файла (sendmail.cf), так и наличием соответствующих параметров в командной строке при запуске самого sendmail-демона.

В файле /etc/aliases располагаются почтовые синонимы (алиасы) для отдельных пользователей и для группы определенных пользователей. Эти алиасы создаются системным администратором и служат для того, чтобы по одному имени рассылать почту нескольким адресатам либо получать почту для адресата под несколькими именами. Существуют несколько предопределенных алиасов. В домене должен существовать адресат postmaster. У нас это алиас для суперпользователя (root), который будет реагировать в случае проблем с системной почтой. Далее, необходимо наличие алиаса для почтового демона, который возвращает диагностические сообщения по указанному адресу. Этот алиас выглядит следующим образом: MAILER-DAEMON: postmaster. Таким образом, вся диагностическая информация отсылается системному администратору. Очевидно, что можно распределить ее и по другим адресатам, отредактировав файл /etc/aliases. После редактирования этого файла необходимо выполнить команду /usr/ucb/newaliases. Кроме этого, необходимо модифицировать базу данных сетевой информационной службы NIS, чтобы алиасы были доступны со всех хостов сети.

Еще несколько слов о конфигурационном файле sendmail.cf. Этот файл на mail-клиентах не подвергался изменениям. В конфигурационный файл mail-хоста были внесены изменения, связанные с управлением маршрутизацией почты, форматом выдаваемых и принимаемых почтовых сообщений, описанием домена, определением отдельных параметров для sendmail.

Почтовый адрес абонентов сети ВЦ РАН - username@ccas.ru, где username - входное имя пользователя сети, а ccas.ru - имя домена для сети. Все такие UNIX-пользователи объединены в специальную группу, и каждому выделено по 1 Мб дисковой памяти для хранения почтовых сообщений. Пользователи на своих рабочих местах могут использовать различные инструментальные средства для отправки и получения почты. В первую очередь, это UNIX-команда mail, непосредственно связанная с демоном sendmail. Графический интерфейс Open Windows позволяет использовать программу mailtool. Пользователи персональных компьютеров (ПК), подключенных к локальной сети, используют средства программы PC-NFS (rsh - выполнение удаленных UNIX-команд). Подробно ознакомиться с командой mail можно, набрав команду man mail, а с программой mailtool - в справочнике (help) для Open Windows. Имеется специализированное программное обеспечение для работы с электронной почтой на ПК под управлением PC-NFS: Life Line Email.

3.5.2. О WWW в ИВС ВЦ РАН

World Wide Web (WWW) (всемирная "паутина" - система, подобно Gopher обеспечивающая работу пользователя практически со всем множе-

ством функций и систем прикладного уровня) в настоящее время становится все более распространенной.

WWW - это система, основанная на работе с так называемым гипертекстом. Гипертекст - это информация, отдельные фрагменты которой одновременно являются ссылками на другие фрагменты. Фрагменты информации - это не только текст, но и бинарная информация (коды программ), графическая информация, звук (аудиоинформация), изображение (видеоинформация), т.е., в отличие от так называемого плоского текста, гипертекст - это фактически дерево файлов самой разнообразной природы. Совокупность разнообразных видов представления информации (текст, графика, аудио, видео) сейчас принято называть мультимедиа (multimedia).

Итак, WWW - это распределенная информационная система мультимедиа, использующая гипертекст.

Узлы сети, где хранится информация, - это www-серверы. Узлы, откуда пользователи могут добраться до www-серверов, называются www-клиенты. На www-клиентах установлено специальное программное обеспечение, при помощи которого осуществляется доступ к www-серверам и просмотр информации.

Эти программы на www-клиентах часто называют www-browsers. В настоящее время наибольшее распространение имеют www-browsers двух фирм: NCSA Mosaic (11.2%) и Netscape (84.1%). Кроме Netscape и Mosaic имеются и другие просматривающие программы (Linx, EINet, Air Mosaic, GWHIS и многие другие).

В UNIX-сети взаимодействие www-сервера и www-клиента - это традиционный "разговор" удаленных процессов с помощью RPC. При этом используется специально разработанный для WWW протокол Hyper Text Transport (Transfer) Protocol (HTTP). Клиент может не только осуществлять поиск гипертекстовой информации и обмениваться ею с www-сервером, но и исполнять удаленные программы.

Протокол, обеспечивающий запрос удаленной программы, исполнение ее и передачу результатов клиенту, называется Common Gateway Interface (CGI). При работе с WWW часто используется термин Uniform Resource Locator (URL), или просто Location. URL имеет следующую структуру: <протокол>://<адрес www-сервера>: <номер порта>:/<имя директории>/<имя файла>.

Пример URL: http://www.ccas.ru:80/~kop/www.html

В качестве протокола в URL, в силу своей "всеядности", browsers кроме "родного" http могут использовать ftp, gopher и другие протоколы, на работу с которыми настроена система WWW. Номер порта, если он равен 80, можно не задавать (принимается по умолчанию). Выше приведена конструкция URL в полном объеме. Иногда в конкретной работе используется сокращенный URL без задания директории и файла. В этом случае при поиске нужной информации пользователь сначала связывается с нужным сервером, а затем более глубокое проникновение осуществляется через соответствующую работу с меню.

Фрагменты гипертекстовой информации часто называют www-документами. Каждый www-документ первоначально записывается на специальном языке - Hyper Text Markup Language (HTML), отсюда и файлы, соответствующие www-документам, имеют расширение .html.

Существует определенная методика работы с html-файлами и соответствующий программный инструментарий, поддерживающий эту методику.

Ниже мы рассматриваем конкретные вопросы создания и использования системы WWW в рамках ИВС ВЦ РАН. WWW-серверы, работающие в ЛВС ВЦ РАН, являются носителями основных информационных ресурсов ИВС ВЦ РАН.

3.5.2.1. WWW-серверы ИВС ВЦ РАН

В сети Вычислительного центра РАН расположены два различных по назначению www-сервера: www.ccas.ru и www.web.ru. Назначением первого, www.ccas.ru, является предоставление информации о структуре Вычислительного центра, его сотрудниках, информационных и вычислительных ресурсах, ведущихся научных проектах, разработанных программных продуктах, а также о конференциях, организованных с участием Вычислительного центра. Для обеспечения наиболее мобильного предоставления информации на данном сервере поддерживаются две параллельные файловые структуры. Одна отражает общую информацию о Вычислительном центре, его подразделениях, сетевой и информационной политике и т.д. Наполнение этой структуры производится централизованно. Другая файловая структура распределена по домашним директориям сотрудников Вычислительного центра. Каждый пользователь локальной сети (в том числе и групповые пользователи) может независимо от других создавать или изменять www-страницы в собственной директории.

Наполнение другого www-сервера, www.web.ru, обусловлено его консультационным характером. Данный сервер создавался для информационной помощи администраторам российских www-серверов (www-мастеров) и для развития инфраструктуры WWW. Поэтому на данном сервере представлена обширная документация по проблемам, связанным с WWW, собраны интересные решения в области дизайна www-страниц. Необходимо отметить, что сервер Russian Web-Masters Association (RWMA) создавался как корпоративный, усилиями ряда ведущих web-мастеров России из ряда городов (Москва, Ярославль, Петрозаводск и др.). Поскольку сервер RWMA предназначен в первую очередь для российских www-мастеров, большинство документов представлено на русском языке. Большое внимание уделяется решению характерных для России проблем (поддержанию нескольких кодировок русского языка параллельно, использованию WWW в условиях плохой коннективности и т.д.).

3.5.2.2. Некоторые проблемы развертывания www-серверов

Существует ряд общих проблем, связанных с WWW. Отметим некоторые из них:

- защита информации;
- русскоязычная информация;
- плохое качество линий передачи информации;
- неустоявшиеся стандарты.

В Вычислительном центре применяется целый ряд мер для защиты информации от несанкционированного доступа. Используемые www-серверы (Apache-0.8.14 и Apache-1.0.3) позволяют ограничивать доступ к внутренней файловой системе несколькими средствами. Во-первых, определяется директория DOCUMENT_ROOT, являющаяся корневой для http-сервера. В нашем случае для www-дерева создана отдельная директория, не включающая в себя никаких запрещенных для доступа файлов или поддиректорий. Во-вторых, для каждой директории, в которую есть доступ через WWW, определяется отдельно, какие функции может производить сервер с файлами в данной директории (например, "только читать", "читать и переходить в поддиректории" или "выполнять программы"). Как правило, в директориях, где хранятся документы, запрещено хранить выполняемые программы (CGI-скрипты), и, наоборот, директория, где хранятся CGI-скрипты, закрыта для чтения.

В каждой пользовательской домашней директории была создана отдельная поддиректория для www-документов, к которой обеспечивается доступ через www-сервер с помощью вызова: "http://www.ccas.ru/~username". Такой подход позволяет хранить www-документы отдельно от остальных пользовательских файлов, а кроме того, закрыть для доступа саму пользовательскую директорию и другие поддиректории пользователя. Отдельной проблемой является обеспечение безопасности системы при выполнении CGI-программ, запускаемых с удаленной машины. Эта тема широко обсуждалась в сетевых конференциях. В сети ВЦ РАН приняты следующие меры для обеспечения безопасной работы с CGI-скриптами:

- все CGI-скрипты выполняются под идентификатором nobody, что не позволяет данным программам получить доступ к привилегированным системным ресурсам;
- все CGI-скрипты компилируются и запускаются только www-администратором, что исключает возможность запуска "троянского коня";
- при написании CGI-скриптов не используются интерпретаторы (sch, sh, perl, emacs и т.д.), с помощью которых было произведено большинство взломов.

Поскольку главная задача www-сервера - предоставление информационных ресурсов, необходимо оценивать, насколько посещаем тот или иной раздел www-сервера и какой круг пользователей заинтересован в предложенной информации. Для этого на серверах ВЦ РАН производится сбор и анализ разнообразных статистических данных о посещаемости сервера. Во-первых, был написан CGI-скрипт (счетчик), который поддерживает неограниченное количество счетных объектов. Он удобен тем, что пользователь ВЦ РАН может самостоятельно создать или удалить свой объект с помощью того же самого CGI-скрипта через простую html-форму. При этом данный объект можно использовать в нескольких страницах одновременно (при этом он будет учитывать суммарную посещаемость). Этот счетчик удобен не только для использования, но и для администрирования сервера, поскольку при соответствующем запросе этот скрипт выдает в html-форме сводную таблицу всех объектов.

Подробнее об этом можно прочитать по "http://www.web.ru/CGI/count.html". Кроме этого, каждый час с помощью программы AccessWatch анализируется и выводится в виде html-файла общая статистика по www-серверам ВЦ РАН.

Проблема русскоязычной информации заключается в том, что не существует общепринятой кодировки для кириллицы, т.е., если на www-сервере русскоязычная информация хранится в стандарте CP1251 (MS-Windows), то те, кто не пользуются этой кодировкой, будут испытывать определенные проблемы при чтении этих разделов сервера.

Практически все виды кодировок для кириллицы собраны на страничке нашего сервера http://www.web.ru/Rus/Coding/. Однако наиболее популярны из них кодировки KOI8-r, ISO-8859-5, CP866, CP1251, как показывает статистика обращений, собранная на различных российских www-серверах и опубликованная в почтовой конференции sovam-teleport:

сервер www.online.ru, данные И.Семенюка

	Всего	Windows	X11	Mac	MSIE	Other
alt	1306	701	137	63	52	353
koi	38423	21603/11	5148/26	3412	1676	2053
mac	4872	452	52	4121	95	152
win	93410	83801	369/24	454	6848/6	1920
www	54554	35570/12	3937/20	4703	4747	5600

Примечание: www - это кодировка по умолчанию (KOI8-r).

сервер www.free.net, данные Е.Миронова

cp1251	85%
cp866	< 1%
koi8-r	10%
iso8859-5	4%

Как видно из приведенной статистики, невозможно ограничиться какой-либо одной из кодировок, а необходимо, чтобы была возможность получения информации в любой из кодировок. Пути решения этой проблемы широко обсуждаются на сервере http://www.web.ru/Rus/Diskuss/.

На наших серверах в качестве базовой кодировки выбрана KOI8-r (по причине доступности шрифтов и благодаря хорошей поддержке этого стандарта). При обращении www-клиента к серверу сервер делает попытку определить кодировку клиента по той информации, которую он передает. Если это удается, то www-сервер передает клиенту уже перекодированные в новую кодировку файлы (перекодировка on-fly). Если нет, то передается кодировка по умолчанию. Каждый www-сервер использует 4 TCP порта: 80 - KOI8-r, 8001 - CP1251, 8002 - ISO-8859-5, 8003 - CP866. При этом пользователю предоставляется возможность переключиться с любого порта на тот, который передает файлы в требуемой кодировке.

В России существует специфическая проблема, связанная с плохим качеством линий передачи информации. Большинство пользователей использует коммутируемые или, в лучшем случае, выделенные телефонные линии. При такой работе тратится очень большое время на передачу графической информации с сервера клиенту.

Для оптимизации трафика, связанного с передачей изображений, в Вычислительном центре РАН применены следующие приемы:

- оптимизация цветовой палитры: для всех графических элементов основных разделов серверов используется сжатая цветовая палитра (4, 8, максимум 16 цветов), что позволяет максимально уменьшить размер изображения;
- из протестированных нами форматов наиболее экономным является compressed GIF (использующий алгоритм Давида Кобласа), поэтому все графические файлы, генерируемые CGI-скриптами или программами обработки изображений, создаются в этом формате;
- для просмотра графических архивов написано несколько различных программ и CGI-скриптов, позволяющих в удобной форме получать представление о содержании архива (графический индекс), чтобы клиент имел возможность просматривать только те изображения, которые ему интересны.

HTML в данный момент переживает период стремительного развития. Практически каждый день появляются новые предложения по расширению языка, которые реализуются тем или иным приложением. Наиболее мощными html-клиентами на сегодняшний день являются продукты фирмы Netscape, которая разработала серию нововведений в HTML, получивших название Netscape HTML extention. Это расширение поддерживает форматирование сложных таблиц, позволяет изменять цвет текста. поддерживает систему независимых окон и многое другое. Хотя, как показывает статистика обращений, 65% пользователей используют Netscape-browser (Mozilla), большинство других клиентских программ не поспевают за всеми нововведениями.

Последний утвержденный стандарт HTML (2.0), которого придерживается большинство browsers, не позволяет вставлять в html-файлы дополнения, интерпретируемые одними клиентами и неинтерпретируемые другими. К тому же большинство компаний, предлагающих свои нововведения, не заботятся о том, чтобы html-файл, созданный для одного клиента, мог быть просмотрен другим.

Поэтому при создании html-документов приходится использовать только те конструкции, которые поддерживаются подавляющим большинством клиентов (т.е. HTML2.0), или корректно сформулированные дополне-

ния к HTML (которые могут игнорироваться клиентом, поддерживающим стандарт HTML2.0).

3.5.2.3. О файловой структуре WWW и методике наполнения файлов

Наполнение www-серверов ВЦ РАН осуществляется двумя различными способами: централизованным и распределенным, что и определяет файловую структуру сервера.

Централизованно подбирается общая информация о Вычислительном центре, его структуре, руководстве, общих для ВЦ РАН мероприятиях. Поскольку эта информация является практически официальной в INTERNET, она обычно согласуется с руководством Вычислительного центра. Доступ к каталогам, в которых хранятся эти данные, имеет только webmaster Вычислительного центра.

С другой стороны, www-сервис предназначен для оперативной смены информации, наглядно отображающей текущее состояние. www-клиенты заходят на сервер, желая узнать самые последние новости в жизни ВЦ РАН. И хотя www-технология предоставляет возможность моментальной публикации материалов, централизованное наполнение сервера сильно ограничивает гибкость и оперативность системы.

Для того чтобы каждое подразделение ВЦ имело возможность быстро реагировать на изменение какой-либо своей информации, каждому подразделению предоставлена возможность самим наполнять разделы сервера, относящиеся к работе данного подразделения. Webmaster следит только за тем, чтобы на страницах этих подразделений не появлялись материалы, противоречащие установленным в INTERNET правилам и основной информации сервера.

Технически такое решение реализовано следующим образом. Для центральной части сервера (редко меняемой информации) выделена отдельная директория, которая соответствует DOCUMENT_ROOT директории сервера. Такой подход практически гарантирует, что внешние клиенты не смогут получить несанкционированного доступа к директориям сервера, лежащим вне DOCUMENT_ROOT директории. В данной директории хранятся только те файлы, доступ к которым разрешен внешним пользователям. CGI-скрипты и Java-классы (т.е. исполняемые программы, с помощью которых можно взломать систему) хранятся в отдельных директориях, куда закрыт доступ "на чтение" всем пользователям. WWW-сервер при выполнении по запросу клиента CGI-скрипта автоматически переводит стандартное обращение к CGI_BIN директории в действительный путь к месту хранения скриптов.

Распределенные разделы сервера хранятся в домашних директориях пользователей. Здесь организуется отдельная поддиректория, в которой хранятся только те файлы, которые пользователь хочет сделать доступными для чтения. Таким образом, внешний пользователь не может получить доступа к файлам в домашней директории без разрешения их хозяина. Поскольку отдельным пользователям не разрешается хранить в своих www-директориях исполняемые скрипты (это может привести к взлому системы), все скрипты для сервера пишутся и устанавливаются только администратором WWW.

Чтобы связать воедино эти две разнородные схемы наполнения сервера, существует часть разделов общего пользования, которыми может воспользоваться любой пользователь локальной сети ВЦ РАН. Например, для сбора статистики посещаемости своего раздела пользователь может самостоятельно завести один или несколько объектов счетчика, защитить паролем и вставить его в нужные www-страницы. Счетчик автоматически проверяет принадлежность пользователя к ЛВС ВЦ РАН. Подробнее это описано на http://www.web.ru/CGI/count.html .

Для того чтобы пользователь мог поместить какую-то общую информацию, существует специальная локальная группа на NEWS-сервере, в которую любой пользователь ЛВС ВЦ РАН может послать сообщение, а также доска объявлений (WWW Message Board), доступная на http://www.web.ru/.

В ВЦ РАН через http-протокол также осуществлен доступ к файловому архиву свободно распространяемых программ. По сути такой архив заменяет анонимный ftp-сервер, но предоставляет дополнительные возможности по наглядному структурированию файлов. В этом архиве обычно хранятся самые свежие версии программ FREEWARE , используемых в ВЦ РАН. Кроме того, создан отдельный архив документации в html-формате. В архиве хранятся все основные коммуникационные и компьютерные стандарты, и реализуется система быстрого поиска нужных документов средствами WWW. HTML - основа для файлового архива - позволяет включать в него также файлы, находящиеся на удаленных машинах и даже на тех, где нет www-сервера, а присутствует только старомодный ftp-сервер. Для этого достаточно только сделать соответствующую ссылку в html-файле. Необходимость таких ссылок диктуется экономией дискового пространства и ресурсов сервера за счет распределенного хранения единого архива на нескольких серверах (при этом обычные ftp-серверы должны хранить весь архив на своих дисках). Кроме этого, HTML удобно использовать, если в файловые архивы необходимо (для целостности) включить какие-либо программы или документацию, защищенные авторскими правами и запрещенные к перераспределению. Самый наглядный пример такого архива - это бесплатная копия Netscape Browser, которой пользуются 80% www-клиентов, но для нее запрещено свободное распространение. В таких случаях, чтобы не нарушать целостность и логичность построения архива, можно в директории WWW-Browsers поместить не сам архив, а ссылку, по которой пользователь получит копию Netscape, но не с данного сервера, а с центрального сервера ftp.netscape.com.

4. Проблемы надежности ИВС

INTERNET в целом можно рассматривать как глобальную гетерогенную систему, объединяющую множество региональных и локальных сетей, отличающихся не только по своей архитектуре и составу, но и по надежности. Поскольку INTERNET - децентрализованная система, ее надежность определяется надежностью составляющих, прежде всего надежностью отдельных региональных и локальных сетей и построенных на их базе ИВС.

Надежность работы ИВС определяется многими факторами. Главными, на наш взгляд, являются следующие:

- качество используемых программно-аппаратных средств;
- обеспечение надлежащих внешних условий функционирования аппаратных средств (качество электропитания и энергонезависимость, климатические условия, защищенность от физического воздействия злоумышленников, пожарозащищенность и т.д.);
- обеспечение информационной безопасности;
- квалификация персонала и уровень организации поддержки и использования программно-аппаратных средств.

В данной работе мы не ставим цель дать полный анализ всех факторов надежности ИВС, а ограничиваемся лишь изложением взгляда на отдельные элементы факторов надежности на базе собственного опыта двухлетней эксплуатации ИВС ВЦ РАН.

4.1. Система бесперебойного питания

Система бесперебойного питания для локальных сетей - один из важнейших факторов обеспечения надежности работы элементов сети и защиты информации. К большому сожалению, в результате сложившейся не лучшей традиции, проектирование систем бесперебойного питания в связи с массовым внедрением персональных компьютеров, не столь критичных к электропитанию, как бы потеряло свою актуальность. Однако если это было допустимо еще для разрозненных компьютерных точек, то с появлением локальных сетей, развертыванием в них мощных серверов, внешних накопителей на дисках с большими объемами памяти до 100 Гб и более, с установкой в сетях современных баз данных актуальность защиты по электропитанию сетей и информационной структуры становится первоочередной задачей.

Кроме того, выход ВЦ РАН в INTERNET, реализованный в рамках проекта развития Южной московской опорной сети (ЮМОС), потребовал гарантированной защиты по электропитанию всех элементов сети, обеспечивающих стыковку с ЮМОС.

Прежде чем рассмотреть вопросы концептуального характера по выбору источников бесперебойного питания (ИБП), необходимо дать краткую характеристику наиболее часто встречающихся искажений и аварийных ситуаций в сети питания.

1. Всплески напряжения: кратковременные повышения напряжения в сети на величину более 110% от номинального значения на время более одного периода синусоиды (20 мс).
   Причина - отключение энергоемкого оборудования.
   Последствия - сбой в оперативной памяти, возникновение ошибок и выход из строя аппаратуры.
2. Высоковольтные выбросы: кратковременные импульсы напряжения до 6000 в с длительностью до 10 мс.
   Причина - удары молнии, искрение переключателей, статический разряд.
   Последствия - сбой оперативной памяти, выход из строя аппаратуры.
3. Высокочастотный шум: радиочастотные помехи, помехи электромагнитного происхождения.
   Причина - электродвигатели, силовая коммутационная электроника, реле и др.
   Последствия - возникновение ошибок, как следствие - "зависание" систем, сбой оперативной памяти.
4. Выбег частоты: уход частоты на величину более 3 гц от номинального значения (50 гц).
   Причина - нестабильность источника электроэнергии, вращения генератора.
   Последствия - выход из строя накопителей, "зависание" компьютерных систем, программные сбои, потеря данных.
5. Проседание напряжения: кратковременное снижение напряжения в сети до величины менее 80-85% от номинального значения на время более 20 мс.
   Причина - включение энергоемкого оборудования, запуск мощных потребителей энергии.
   Последствия - сбои оперативной памяти, возникновение ошибок, выход из строя аппаратуры.
6. Подсадка напряжения: падение напряжения на длительное время.
   Причина - включение энергоемкого оборудования, запуск мощных электродвигателей, перегрузка по линии электропитания.
   Последствия - потеря данных, выход из строя аппаратуры.

7. Пропадание напряжения: отсутствие напряжения более 40 мс (двух периодов).

   Причина - неполадки на электростанции, в линии электропередачи, срабатывание защиты короткого замыкания.

   Последствия - аварийная остановка серверов, разрушение информации, отказ или выход из строя внешних накопителей.

Из указанных семи случаев 45% и более составляет подсадка и пропадание напряжения в сети. Мировая практика показала, что наиболее удачной является система двойного преобразования входного напряжения: выпрямление с последующим обратным преобразованием через инвертор в режиме ON-LINE. Такая схема имеет три важнейших преимущества перед другими:

- полная фильтрация высокочастотных помех;
- полная развязка нагрузки от первичной сети;
- полное отсутствие времени переключения при возникновении аварии в сети.

Режим работы ИБП в ON-LINE предусматривает прежде всего наличие порта в устройстве управления ИБП, который позволяет работать с данным оборудованием, как с элементом локальной сети. Для обеспечения и поддержки работы ИБП в автоматическом режиме слежения, а также для выполнения функций нормальной остановки - "сворачивания" серверов в случае пропадания напряжения и ведения протоколов системных измерений разработан программный пакет (ПП) ONLINET для серий Prestige и Plus фирмы EXIDE ELEKTRONICS (США).

Концепция автоматического управления электропитанием ЛВС включает в себя три основных элемента:

- контроль основных параметров сетевого напряжения, питающего ЛВС;
- автоматическое "сворачивание" работы ЛВС при возникновении длительных перебоев в системе электроснабжения;
- дистанционное управление состоянием агрегатов бесперебойного питания.

Все три указанные здесь проблемы должны решаться комплексно при проектировании системы ИБП ЛВС. Важнейшим фактором при этом является гетерогенность ИВС.

Для выработки концепции системы ИБП исключительную важность приобретает вопрос распределения элементов ЛВС по критичности электропитания. Различают четыре категории элементов по степени критичности:

- максимально высокая;
- высокая;
- средняя;
- низкая.

К категории максимально высокой относятся коммуникационные устройства ЛВС: мосты, разветвители, маршрутизаторы, концентраторы и др.

К категории высокой относятся файловые серверы, дисковые накопители большой емкости различного типа, работающие непосредственно с серверами.

К категории средней критичности относятся практически все остальные элементы ЛВС: серверы, рабочие станции, персональные компьютеры всех модификаций.

Перечисленные три категории защиты по электропитанию предусматривают использование ИБП в режиме ON-LINE с сетевыми адаптерами и поддержкой протокола TCP/IP или SNMP. Программное обеспечение может быть реализовано в двух вариантах исполнения:

а) ONLINET, который выполняет следующие основные функции:

- автоматическое сворачивание работы ЛВС;
- управление работой ЛВС;
- мониторинг параметров сетевого напряжения;
- взаимодействие с администратором сети.

б) ONLISAFE, который не производит мониторинга системы электропитания ЛВС и управления, сохраняя при этом функции автоматической свертки и анализа режимов ИБП.

Не менее актуальным является вопрос выбора адаптеров для сопряжения ИБП с ЛВС. Сетевые адаптеры выполняют следующие основные функции:

- трансляцию информации о состоянии ИБП и параметрах электросети;
- передачу сообщений о неполадках в системе электроснабжения;
- дистанционное управление работой ИБП.

С точки зрения обеспечения работы ИБП в сетевом режиме с использованием серверов локальных сетей различают следующие модификации адаптеров:

- Ethernet Adapter, обеспечивающий работу с протоколами TCP/IP и программно совместимый с пакетом ONLINET;
- Ethernet SNMP Adapter, обеспечивающий работу с протоколами TCP/IP, SNMP и программно совместимый с пакетом ONLINET;
- Network Adapter, обеспечивающий работу с протоколами TCP/IP, совместимый с программным пакетом ONLINET NETWORK;
- Network SNMP Adapter, обеспечивающий работу с протоколами TCP/IP и SNMP, совместимый с программным пакетом ONLINET NETWORK.

При выборе программного обеспечения для управления электропитанием ЛВС могут рассматриваться два решения: либо это ONLINET, либо ONLISAFE. Если ONLISAFE выигрывает по стоимости, то ONLINET имеет целый ряд преимуществ по сравнению с первым:

- сохранение и последующий анализ основных параметров сети;
- определение текущего состояния агрегатов бесперебойного питания ЛВС;
- определение и диагностика неисправностей в системе аккумуляторных батарей;
- наличие графического интерфейса и др.

Характер распределения нагрузок по критичности, а также топология локальной сети ВЦ РАН применительно к территориальному распределению элементов ЛВС с учетом представленных выше концептуальных положений определяют конкретную схему реализации системы ИБП ЛВС ВЦ РАН.

Для ВЦ РАН можно выделить четыре группы потребителей энергии:

- центр обеспечения выхода "Узла" на ЮМОС, включающий в себя маршрутизаторы, разветвители;
- центр коммутации ЛВС ВЦ РАН, включающий в себя интеллектуальный концентратор LinkBuilder 3GH, блок HUB, терминальный сервер с модемной стойкой ZyXEL;
- серверный центр ЛВС, включающий в себя группу серверов, в том числе сервер администратора сети, дисковые накопители, транспьютерную систему параллельных вычислений GCel 1/64 с собственной рабочей станцией SUN, графические рабочие станции на базе SPARCstation 10, SPARCstation 20 и др.;
- спектр персональных компьютеров PC AT/386,486,Pentium и др., подключенных к ЛВС ВЦ РАН и распределенных в пределах зданий ВЦ РАН.

Первый из перечисленных центров, обеспечивающий стыковку Узла с ЮМОС, безусловно относится к категории максимально высокой степени критичности по определению. С другой стороны, в Узле нет необходимости иметь серверную станцию. Поэтому достаточно иметь сетевой адаптер, обеспечивающий связь ИБП Узла с локальной сетью.

Два следующих центра - серверный и коммутационный - относятся к категории высокой степени критичности по электропитанию. В серверном центре развернуты также СУБД, сервер администратора сети, файловые серверы, рабочая станция для GCel 1/64 и ряд других элементов сети. Коммутационный центр оборудования сосредоточен территориально в одном коммутационном боксе, где нет постоянного персонала и нет свободного

доступа, за исключением лиц, обеспечивающих инженерно-техническое обеспечение по регламенту. В качестве ИБП для данного узла может быть выбран один из двух вариантов:

- UPS PRESTIGE 6kva (Exide El.);
- UPS PLUS 6kva (Exide El.).

Для управления электропитанием необходим сервер, имеющий ПП ONLINET NETWORK, а также сетевой адаптер, обеспечивающий связь через локальную сеть с ИБП. Возможен вариант связи с сервером по стыку RS-232. В обоих вариантах обеспечивается работа протоколов TCP/IP и SNMP. На деле это означает, что при реализации проекта необходимо установить на сервере администратора или на другом сервере сертифицированный пакет ONLINET NETWORK, требующий дополнительных капиталовложений.

Массовая часть потребителей энергии - персональные компьютеры пользователей, общее количество которых колеблется в пределах 100-120, половина которых имеет непосредственный доступ к локальной сети ВЦ РАН, остальные используются в автономном пользовательском режиме. В отличие от представленных выше узлов, здесь нет необходимости защиты по категории высшей или высокой критичности. Поэтому проект предусматривает использование одного ИБП PLUS 36 kva без пакетов ONLINET. Однако это не исключает возможности установки пакета ONLINET NETWORK на некоторых станциях, если в этом будет необходимость, например для поддержки и защиты локальных кластеров в подразделениях.

Серверный узел локальной сети, где сосредоточены практически все основные серверные и вычислительные средства:

- сервер администратора ЛВС;
- дублирующий сервер для обеспечения надежности;
- вычислительный сервер на базе ALPHA 3000;
- система параллельных вычислений GCel 1/64 с собственным HOST-компьютером;
- RAID-диски и другие серверные станции.

По функциональному назначению этот узел является наиболее ответственным, поскольку он обеспечивает "сворачивание" информации в случае долговременного пропадания напряжения первичного ввода. Следовательно, ИБП для данного узла должен обеспечивать время бесперебойного питания не менее 10 мин, что с учетом нагрузки может быть обеспечено модификацией Prestige 6kva (Exide El., США). Обязательным условием управления питанием данного узла является наличие ПП ONLINET NETWORK, который должен быть загружен на всех серверах, обеспечивающих работу пользователей всех уровней по системе "клиент-сервер", в том числе и администратора сети.

Для обеспечения автоматического управления ИБП наиболее приемлемым является выход в локальную сеть через Network Adapter, поддерживающий протоколы TCP/IP и SNMP.

Предложенная схема бесперебойного питания, с учетом критичности элементов локальной сети к электропитанию и гарантированности интервалов времени обеспечения бесперебойного питания в аварийных ситуациях в случае пропадания напряжения в первичной сети, может быть рекомендована как пилотная система ИБП, требующая дополнительных капиталовложений. Она наиболее полно учитывает топологию локальной сети, распределение нагрузок по участкам и классифицирует эти нагрузки по критичности, требует при этом для реализации как минимум трех-четырех Network Adapter, а также трех-четырех сертифицированных ПП ONLINET NETWORK для включения в состав ПО серверных станций.

Финансовые ограничения при реализации проекта определяют условия для его поэтапного выполнения. Одним из указанных этапов является ввод общего источника бесперебойного питания, который имеет достаточную мощность, высокий к.п.д. международных стандартов (90-92%), высокую технологию производства и современные международные стандарты ISO. При условии обеспечения времени работы в автономном режиме (t > 5 мин) альтернативно могут рассматриваться два варианта решения:

- ИБП Plus 36 kva (Exide El.,США);
- ИБП Plus 80, модель 50.

Если первый вариант предпочтительней по капиталовложениям, то ИБП Plus 80 является с точки зрения технологичности наиболее современным решением и практически перекрывает все технические требования, изложенные здесь применительно к данному классу оборудования. Непременным условием при реализации любых решений остается требование обеспечить Узел оптоволоконной магистрали ЮМОС автономным блоком бесперебойного электропитания по категории максимально высокой.

Следует заметить, что для каждого объекта, где развернута локальная сеть, не существует универсальной системы бесперебойного питания в силу различия топологии сетей, территориального распределения элементов сетей, а также функциональных и электрических нагрузок. В данной работе представили общие концепции проектирования подобных систем и технико-экономическое обоснование реализации принципиальных решений.

4.2. Обеспечение надежной работы с дисками большой емкости

Как уже говорилось выше, качество программно-аппаратных средств является важным фактором надежности системы в целом. Для ИВС особую роль играют средства хранения информации на магнитных дисках. При подключении к локальной сети новых хостов (рабочих станций, персональных компьютеров) и с увеличением количества пользователей обязательно возникает потребность в расширении дискового пространства для новых клиентов. Кроме этого, появляются проблемы надежности хранения информации на данном пространстве. Многие из этих проблем решаются за счет применения в системе накопителей, использующих технологию Redundant Array of Independent Disks (RAID) - так называемых RAID-дисковых массивов.

Кроме большого объема и высокого быстродействия эти диски обладают и повышенной надежностью. Эта надежность обеспечивается за счет того, что диски имеют модульную структуру и некоторую избыточность. При отказе или сбое одного из дисковых модулей в массиве аварийная ситуация не возникает, так как наличие избыточной емкости позволяет хранить информацию, обеспечивающую восстановление потерянных данных. Процесс чтения или записи не прекращается. Когда неисправный модуль заменяется на запасной, автоматически производится программное реконструирование нового дискового модуля.

Реконструирование, а также отслеживание работоспособности осуществляется оперативно и без отключения накопителя и файлового сервера. Управление этими операциями производится через специальный порт, к которому подключается либо персональный компьютер, либо рабочая станция или сам файловый сервер. Подробнее о RAID-дисках см. в [4].

Несколько слов о проблемах, возникающих при подключении дисков большой емкости. В [1] подробно говорилось о возможном разбиении диска на 7 частей (партиций): A, B, D, E, F, G, H. Часть C соответствует всему объему диска. Далее выяснилось, что на длину партиции налагается ограничение 2 Гб. Таким образом, общий объем диска, доступный для использования, составляет 14 Гб. Если реальный объем диска больше, воспользоваться оставшейся частью нельзя и приходится ограничиваться 14 Гб. Но так как к рабочей станции (фирмы SUN) можно подключить одновременно 4 дисковых устройства, максимальный объем дисковой памяти, подключаемой к одной рабочей станции, 56 Гб. Это небольшое ограничение можно преодолеть путем подключения новых дисков к другому сетевому файловому серверу, что значительно увеличит размеры распределенной файловой системы.

Хотя надежность упомянутых выше дисков достаточно высока, потеря информации по вине самого пользователя или из-за несанкционирован-

ного доступа не исключается. Чтобы хотя бы частично избежать этого, регулярно (1-2 раза в две недели) производится копирование "домашних" каталогов пользователей на магнитную ленту (8mm и 4mm). При больших объемах дисковой памяти емкость магнитных лент должна быть соответствующей. Она составляет для 8mm до 4 Гб, для 4mm до 14 Гб. Кроме этого, важным является и скорость записи (чтения) на эти ленты. Никого не устроит, если копирование такого большого объема данных будет занимать несколько суток. К счастью, время доступа к этим лентам соответствует их объему и вполне приемлемо (для 8mm - около 20 Мб/мин, а для 4mm - более 30 Мб/мин).

Большое значение имеет правильная организация копирования дисков на ленту. В настоящее время отрабатывается методика копирования с использованием различных устройств. Методика определяет, какие части дисковой памяти копировать и с какой частотой, а также каковы используемые для этого программные средства.

4.3. Обеспечение информационной безопасности ИВС

Рассматриваемый нами фактор надежности своеобразен и в значительной мере отличается от других тем, что его определяет целенаправленная человеческая деятельность.

С одной стороны, имеются люди, которые путем разработки и использования соответствующих готовых программных и аппаратных средств и методов организуют преграды случайным и неслучайным попыткам несанкционированного доступа к различным информационным компонентам системы, а с другой стороны, опыт показывает, что имеются люди, пытающиеся "взломать" систему и получить доступ к информации, которую им запрещено использовать.

Защита ИВС от несанкционированного доступа, построение системы безопасности (СБ) - это важная и актуальная задача, требующая комплексного подхода.

Грамотное построение СБ для конкретной ИВС требует прежде всего определения того, что надо защищать и от кого. Универсального решения этой задачи быть не может, поскольку в общем случае все ИВС имеют свою специфику. СБ, например, банковской системы будет отличаться от СБ ИВС научного профиля. Понять и изучить, кто взламывает систему, т.е. построить "модель нарушителя", важно для того, чтобы решить экономический вопрос - какие средства понадобятся для борьбы с нарушителями.

Следует различать следующие виды угроз для ИВС, которая является системой хранения данных для научного использования:

- угроза от "случайного" проникновения (угроза от "дурака");
- угроза от "любознательного" сотрудника, имеющего законный вход в ЛВС;
- угроза от внешнего "хакера" - "свободного художника", упражняющегося ради собственного удовольствия в приемах взламывания системы;
- угроза от криминальных и специальных внешних структур, стремящихся обеспечить проникновение в ИВС незаконными методами.

Очевидно, что различные угрозы требуют различных адекватных защитительных мер.

Цели проникновения тоже могут быть различны. Не претендуя на полноту, выделим некоторые:

- скрытое получение вычислительных и информационных ресурсов;
- кража информации;
- порча информации;
- закладывание различного вида программных "мин" с целью нарушить работу системы.

Можно выделить три основные составляющие проблемы защиты информации:

- правовая защита;
- организационная защита;
- инженерная защита.

Правовая защита - это основание для проведения мероприятий по построению СБ и признание действий злоумышленников незаконными, криминальными. Последнее очень важно. И, очевидно, необходимо в масштабе государства, и в особенности в системе обучения и воспитания специалистов, предусмотреть необходимость их просвещения в отношении законности и незаконности тех или иных действий программистов-пользователей.

Законодательство России в отношении компьютерных преступлений еще недостаточно совершенно, но тем не менее начало построению системы законов в этой части уже положено.

Так, соответствующая информация на эту тему содержится в статье 139 "Гражданского кодекса РФ" (Об охране служебных и коммерческих тайн), а также в статьях 27 и 28 "Уголовного кодекса РФ", где говорится о преступлениях в сфере использования компьютерной информации и сформулированы нормы уголовной ответственности за компьютерные преступления.

Под организационной защитой обычно понимают систему мероприятий, которые необходимо проводить, с одной стороны, чтобы внедрять соответствующие инженерные методы защиты, а с другой стороны, чтобы правовой механизм работал в полном объеме, т.е. необходимо производить разработку, покупку и внедрение средств СБ среди персонала, занимающегося эксплуатацией и поддержкой ИВС, иметь подготовленных специалистов по вопросам безопасности, наладить учет и контроль за работой пользователей, учет правонарушений и т.д., а в масштабах государства соответствующие правоохранительные органы должны надлежащим образом следить за соблюдением гражданами и организациями законов в данной области.

Под инженерной защитой понимаются все те программно - аппаратные средства и методы, которые должны разрабатываться и применяться при построении СБ.

Задача построения СБ носит международный характер не только в силу своей важности, но и в силу специфики INTERNET. Поэтому правовые, организационные и инженерные формы защиты будут совершенствоваться в направлении международной унификации, выхода на единые мировые стандарты.

Известно, что в США сейчас проявляют очень большое внимание к обеспечению нормального функционирования компьютерных сетей. Проблемы безопасности компьютерных сетей рассматриваются на уровне обеспечения безопасности страны, что справедливо для общества, функционирование которого на рубеже XXI века все более зависит от автоматической обработки информации через сеть.

В рамках принятой Национальной информационной инфраструктуры (National Information Infrastructure (NII)) США проводят серьезные исследования в законодательной и технологической областях. Эти исследования финансируются NSF и правительством США.

В 1994 г. была создана специальная правительственная комиссия США по компьютерной безопасности. Комиссия в своих выводах говорит об угрозе информационного противоборства. Появляются новые термины: "информационное противоборство", "информационные войны". В мае 1996 г. в Брюсселе Национальная ассоциация компьютерной безопасности США проводила конференцию "INFOWAR", где помимо уже традиционных проблем информационной безопасности шла речь об активных формах специального программно-математического воздействия.

В связи с тем, что проект NII был поддержан рядом европейских стран, в настоящее время реализуется новый проект под названием

Global Information Infrastructure, в котором одно из главных мест занимают вопросы безопасности информационных систем.

В рамках INTERNET проводятся регулярные телеконференции и создаются RFC-документы по вопросам СБ.

За период двухлетней эксплуатации ИВС ВЦ РАН мы смогли в полной мере убедиться на примере немногочисленных, но имевших место фактах взлома системы, что необходимо самым серьезным образом подойти к построению надежной системы безопасности. В 1996 г. мы приступили к реализации новой системы безопасности для ИВС ВЦ РАН.

Отметим сразу, что излагать особенности создаваемой нами СБ - дело неблагодарное, поскольку это может быть использовано во вред ВЦ РАН. Поэтому ограничиваемся описанием того, как нами используются традиционные средства защиты UNIX. Еще раз подчеркиваем, что этих средств, являющихся фактически средствами от случайной угрозы, в целом недостаточно.

Обеспечение безопасности в UNIX начинается с того, что каждый пользователь получает свой уникальный (для данного хоста или сети) идентификатор и свой собственный "домашний" каталог. Этому идентификатору соответствует также уникальное "входное" имя пользователя (login-name), по которому он идентифицируется системой. Для каждого пользователя задается пароль, который служит для авторизации пользователя. Рекомендуется заводить пароль, не являющийся каким-либо осмысленным словом, но содержащий различные символы (цифры, знаки), строчные и прописные буквы. Пароль необходимо менять периодически, к тому же имеются системные средства, подталкивающие пользователя к такой замене и контролирующие ее.

Пароль заводится и меняется с помощью команды "passwd" или "yppasswd", если на локальной сети установлена NIS - сетевая информационная система. Особенностью выполнения этой процедуры на NIS-сервере в ВЦ РАН является отсутствие команды "passwd". При попытке выполнить ее на этом сервере выдается диагностическое сообщение "usage yppasswd [username]", т.е. предлагается воспользоваться командой "yppasswd". Это сделано для того, чтобы локальный пароль для пользователя на сервере и пароль в базе данных системы NIS были идентичны.

Затем осуществляется защита по доступу (чтение, запись) к информации пользователя, к его "домашнему" каталогу. Необходимо следить, чтобы сам каталог и содержащиеся в нем файлы были закрыты на запись для других пользователей (возможно, и на чтение). Владелец файлов и каталога может предоставить права на доступ к ним либо всем пользователям (хотя бы на чтение), что не рекомендуется делать, либо пользователям, принадлежащим к одной группе с владельцем этих ресурсов. Разбиение пользователей на группы, как и регистрация новых пользователей, - прерогатива системного администратора. К тому же администратор обязан следить, чтобы все пользователи имели пароль на вход в систему. Защита своих собственных файлов и каталогов - обязанность самого пользователя. Для этого имеется специальная UNIX-команда "chmod".

Системному администратору следует особо следить за тем, чтобы пароль для суперпользователя был известен ограниченному кругу лиц (лучше ему одному). Главная задача любых "злоумышленников" - определить пароль для суперпользователя или уметь его обходить. Как уже было сказано выше, абсолютной защиты от попыток добиться этого нет.

Следующий этап защиты от несанкционированного доступа относится к предоставлению соответствующих прав хостам и пользователям локальной сети. Разрешение на удаленный доступ к хосту (команды "rlogin", "rcp", "rsh"), осуществляемый без дополнительного подтверждения пароля для пользователей хостов сети, определяется содержимым файла "/etc/hosts.equiv" (системный файл) и файла ".rhosts" в "домашнем" каталоге каждого пользователя. Особо следует обратить внимание на файл ".rhosts" в корневом каталоге ("домашний" каталог суперпользова-

теля). Этот файл должен обязательно существовать и быть пустым на всех хостах локальной сети. Это необходимо для дополнительного подтверждения прав суперпользователя на каждом локальном хосте (что не лишнее).

При создании распределенной файловой системы для локальной сети файловый сервер должен "экспортировать" свои локальные файловые системы другим хостам сети, т.е. предоставлять соответствующие права на доступ к этим файловым системам. Права могут предоставляться либо только на чтение, либо на чтение и запись как конкретным хостам, так и всем хостам локальной сети. Не рекомендуется "экспортировать" файловые системы "для всех" (everyone), т.е. для доступа с любого удаленного узла глобальной сети, а также для локальных хостов без особой необходимости разрешать доступ на запись. Подробнее о распределенной файловой системе локальной сети ВЦ РАН см. [1].

И, наконец, несколько слов о защите от непосредственного несанкционированного доступа со стороны "внутренних злоумышленников". Системная плата рабочей станции содержит так называемый монитор EPROM (или несколько таких мониторов), который осуществляет контроль за системой во время ее старта. Этот монитор тестирует систему перед попыткой загрузить операционную систему и поддерживает три режима защиты:

- "non-secure",
- "command",
- "fully"

и пароль на доступ. Доступ к командам монитора контролируется этими режимами. В режиме non-secure (без защиты) разрешено выполнение всех команд монитора, в режиме command без подтверждения пароля можно выполнить только команду "b" ("boot") без параметров и команду "c" ("continue"), в режиме fully - только команду "c" (continue). Таким образом в режимах с защитой (command, fully) нельзя без подтверждения пароля загрузить операционную систему в однопользовательском режиме и с носителя, который не задан по умолчанию. Для установки соответствующего режима служит команда UNIX - "eeprom". Это можно осуществить и при помощи команд самого монитора.

Следует отметить, что в очередных версиях UNIX для всех платформ уделяется повышенное внимание вопросам безопасности систем. Поэтому с установкой новых версий системного программного обеспечения (Solaris, OSF, Parix) общая надежность системы должна повышаться.

ЗАКЛЮЧЕНИЕ

Завершение второго этапа развития ИВС ВЦ РАН сделало возможным ее полномасштабное использование. Дальнейшее развитие системы будет направлено прежде всего на совершенствование ее информационной составляющей (подключение и освоение систем управления базами данных, их информационное наполнение, развитие www-серверов ЛВС ВЦ РАН).

Двухлетний опыт эксплуатации ИВС ВЦ РАН показал важность работ по защите системы от несанкционированных действий злоумышленников. Частично в настоящей работе мы уже коснулись проблем security. На третьем этапе развития системы также будет уделено достаточное внимание развитию программно-аппаратных средств защиты, отработке методики и созданию концепции защиты.

Проводя переоснащение ВЦ РАН в части ВТ в 1992-1994 гг., мы старались приобрести наиболее эффективную технику и современное системное программное обеспечение. Однако технический прогресс в этой области настолько стремителен, что спустя три года стало ясно, что приобретенная нами техника и ее системное программное обеспечение быстро устаревают. Поэтому процесс обновления программно-аппаратных

средств, составляющих основу ИВС ВЦ РАН, является естественным и непрерывным. Правда, реализация планов обновления сильно зависит от тех финансов, которыми мы будем располагать для реализации этой цели.

ЛИТЕРАТУРА

1. Байкова И.В., Копытов М.А., Кулагин М.В., Михайлов Г.М., Привезенцев Ю.А., Рогов Ю.П. Распределенные информационно - вычислительные системы. Вып.1. Локальная сеть ВЦ РАН. М.: ВЦ РАН, 1995.
2. Гальперович Д.Я. Тенденция развития проводки для ЛВС //Сети. 1994. N5. С.44-51.
3. Гальперович Д.Я. Открытым системам - открытые проводки //Открытые системы. 1995. N3. С.70-79.
4. Байкова И.В., Кулагин М.В. Современные дисковые системы RAID //Открытые системы. 1995. N3. С.50-55.