16. КОРПОРАТИВНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ (КВС)

16.1. Характеристика КВС

Корпоративная вычислительная сеть (Intranet) — это сеть на уровне компании, в которой используются программные средства, основанные на протоколе TCP/IP Internet. Другими словами, Intranet — это версия Internet на уровне компании, адаптация некоторых технологий, созданных для Internet, применительно к частным локальным (LAN) и глобальным (WAN) сетям организаций.

Корпоративную сеть можно рассматривать как модель группового сотрудничества, вариант решения прикладного программного обеспечения для рабочих групп, основанного на открытых стандартах Internet. В этом смысле КВС представляет собой альтернативу пакету Lotus Notes (LN) фирмы Lotus Corporation, который с 1989г. является стандартом для совместного использования информации и внутрикорпоративного сотрудничества.

Корпоративные сети, как и Internet, основаны на технологии «клиент — сервер», т.е. сетевое приложение делится на стороны: клиента, запрашивающего данные или услуги, и сервера, обслуживающего запросы клиента.

Наблюдаемый в настоящее время громадный рост корпоративных сетей объясняется их преимуществами, основанными на совместном использовании информации, сотрудничестве, быстром доступе к данным и наличии большого числа пользователей, уже знакомых с необходимым программным обеспечением по работе в Internet.

Корпоративная сеть, объединяющая локальные сети отделений и предприятий корпорации (организации, компании), является материально-технической базой для решения задач планирования, организации и осуществления ее производственно-хозяйственной деятельности. Она обеспечивает функционирование автоматизированной системы управления и системы информационного обслуживания корпорации.

Решая задачи прежде всего в интересах всей корпорации, ее отделений и предприятий, корпоративная сеть предоставляет услуги своим пользователям (штатным сотрудникам корпорации), а также внешним пользователям, не являющимся сотрудниками корпорации. Это способствует популяризации сети и положительно сказывается на сокращении сроков окупаемости затрат на ее создание, внедрение и совершенствование. По мере развития КВС расширяется перечень предоставляемых ею услуг и повышается их интеллектуальный уровень. Расширению контингента пользователей КВС способствует то обстоятельство, что Internet и Intranet легко интегрируются.

Типовая структура КВС приведена на рис. 16.1. Здесь выделено оборудование сети, размещенное в центральном офисе корпорации и в ее региональных отделениях. В центральном офисе имеется локальная сеть и учрежденческая автоматическая телефонная станция (УАТС) с подключенными к ней телефонными аппаратами (Т). Через мультиплексор-коммутатор и модемы ЛВС И УАТС имеют выход на территориальную сеть связи (ТСС) типа Frame Relay или X.25, где используются выделенные телефонные линии связи. Такое же оборудование сети имеется в каждом региональном отделении (РО-1, ..., РО-N). Удаленные персональные компьютеры (УПК) через сервер доступа и ТСС имеют прямую связь с ЛВС центрального офиса.

Для установления Intranet необходимы следующие компоненты:

• компьютерная сеть для совместного использования ресурсов, или сеть взаимосвязанных ЛВС и УПК;

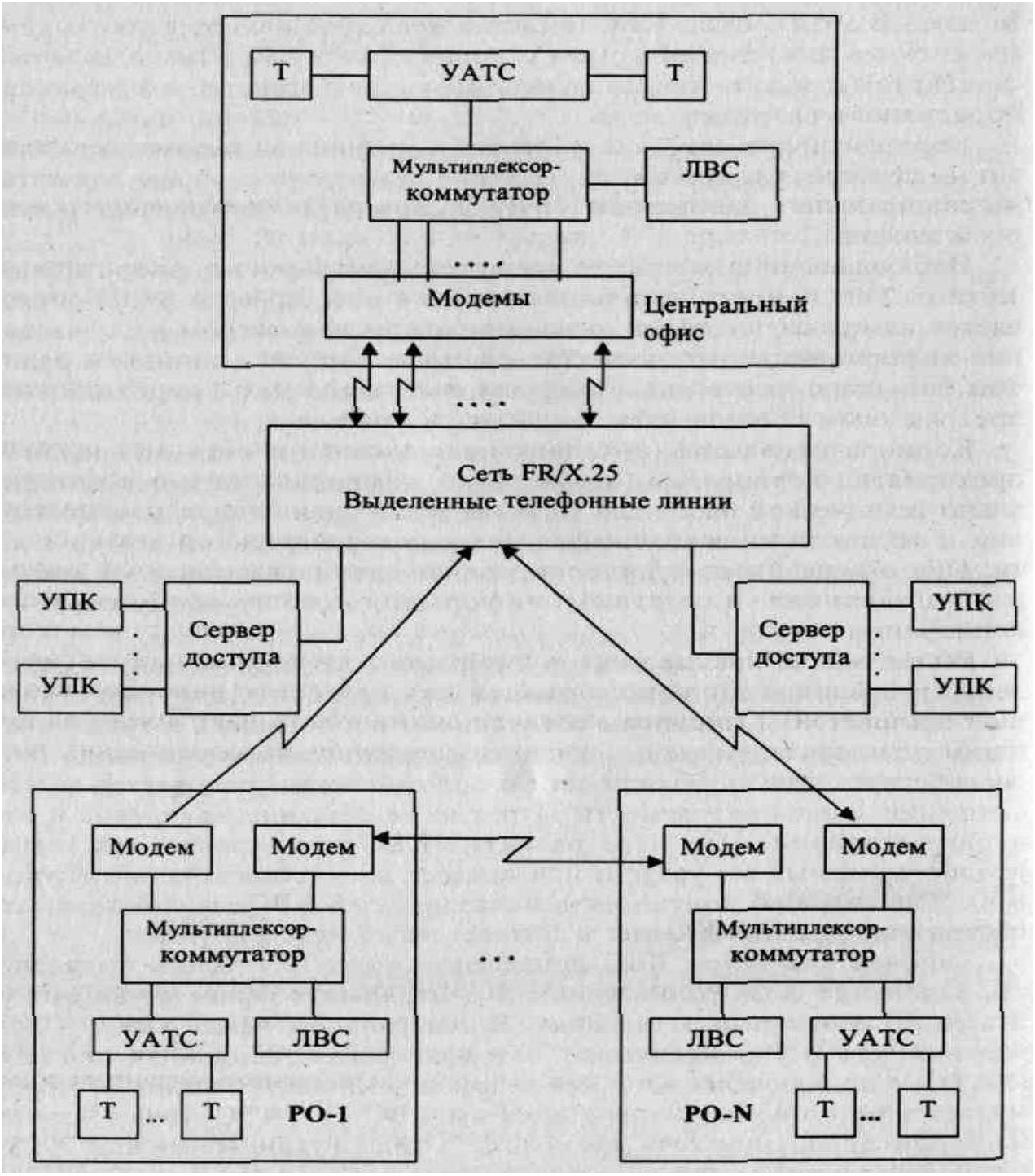

Рис. 16.1. Типовая структура КВС

• сетевая операционная система, поддерживающая протокол TCP/ IP (Unix, Windows NT, Netware, OS/2);

• компьютер-сервер, который может работать как сервер Internet;

• программное обеспечение сервера, поддерживающее запросы броузеров в формате протокола передачи гипертекстовых сообщений (HTTP);

• компьютеры-клиенты, на которых имеется сетевое программное обеспечение, позволяющее посылать и принимать пакетные данные по протоколу TCP/IP;

• программное обеспечение броузера для различных компьютеров-клиентов

(Netscape Navigator, Microsoft Internet Explorer). Эти требования к оборудованию и программному обеспечению Intranet дополняются требованиями к знанию технологии составления документов на языке описания гипертекста (HTML).

Эффективность использования КВС зависит от успешного решения как технологических, так и организационных вопросов, причем по мере эксплуатации сети, когда технологические вопросы получили должное разрешение, все большее значение приобретают организационные вопросы. Ключевыми факторами успешного и эффективного функционирования КВС являются рациональное распределение информации, необходимой для планирования, организации и осуществления производственно-хозяйственной деятельности корпорации, обеспечение сотрудников корпорации системами управления документооборотами и предоставление доступа к различным корпоративным базам данных, воспитание культуры совместного использования информации (это может оказаться наиболее сложной проблемой). Основное внимание должно быть направлено на потребности пользователей, а не на расширение технологических возможностей сети.

16.2.Программное обеспечение КВС

Структура и функции программного обеспечения корпоративных сетей обусловлены тем, что эти сети основаны на технологии Internet, сформировавшейся прежде всего вокруг протокола TCP/IP. Корпоративная сеть состоит из определенного числа взаимосвязанных компьютеров или ЛВС, использующих одну или более сетевых технологий, таких, как Ethernet или Token Ring. Для управления работой сети необходима сетевая операционная система (СОС), реализующая принцип сетевой модели «клиент — сервер». Наиболее популярными СОС являются Windows NT компании Microsoft и NetWare компании Novell.

Система Windows NT для передачи данных использует протоколы TCP/IP или IPX/SPX. Подобно TCP/IP протокол IPX/SPX определяет набор правил для координации сетевой связи между двумя системами. Если сеть не поддерживает протокол TCP/IP, то необходимо использовать программы-шлюзы для трансляции TCP/IP в используемый протокол сетевой операционной системы.

Система NetWare позволяет соединять компьютеры в сети типа Ethernet или Token Ring, используя модель «клиент — сервер». Программное обеспечение сервера NetWare выполняется на всех главных компьютерных платформах типа UNIX, DOS, Windows, Macintosh. Для того чтобы компьютер-клиент имел доступ к сети, на нем должно быть установлено программное обеспечение клиента системы NetWare. После этого клиенты могут совместно использовать файлы и ресурсы принтеров, а также выполнять ряд различных приложений с помощью сервера. Программное обеспечение стороны клиента системы NetWare создано и успешно используется для UNIX, DOS, Macintosh, OC/2 и Windows.

При формировании Intranet на локальной компьютерной сети, работающей под управлением NetWare, для каждого клиента не требуется IP-адрес. Вместо этого используется приложение-шлюз (специальная программа) для трансляции IPX в IP и обратно. IP-адрес присваивается только Web-серверу NetWare. Последовательность трансляции и ретрансляции такова: программное обеспечение клиента транслирует протоколы TCP/IP, генерированные Web-броузером, в протокол IPX, после чего сообщения «путешествуют» по сети на стороне клиента, пока не достигнут Web-

сервера NetWare; на этом сервере осуществляется ретрансляция, т.е. сообщения формата IPX преобразуются в формат TCP/IP и отправляются к другим серверам сети. Таким образом, программы трансляции IPX в IP и обратно позволяют пользователям системы NetWare формировать корпоративную сеть, не выполняя в сети набор программ протоколов TCP/IP.

В корпоративных сетях широко используется язык описания гипертекстовых документов HTML, который, не будучи языком программирования, представляет собой мощное средство обработки документов. Для создания HTML-документов необходим текстовый редактор, а для их просмотра — броузер. Пользуясь HTML, следует включать в свой документ специальные символы — теги (коды), которые предоставляют броузеру определенную информацию для вывода содержимого документа на экран. Каждый HTML-документ имеет две части: головную, содержащую заголовок документа, и тело, состоящее из содержимого документа. Язык HTML обеспечивает связь документов ссылками, причем есть возможность создавать ссылки на различные секции того же или других документов, что обеспечивает пользователям более быстрый доступ к необходимой им информации. Если установлена вспомогательная программа Internet — Assistant for Word, то можно преобразовать имеющиеся документы Word в формат HTML.

Эффективность функционирования корпоративной сети во многом определяется возможностями пользователей взаимодействовать с их Web-страницами. Среди различных методов расширения интерактивных возможностей корпоративных сетей, создания интерактивных Web-страниц в настоящее время чаще всего используются ***CGI-сценарии*** (CGI — Common Gateway Interface — интерфейс общего шлюза). CGI-сценарий представляет собой программу, которая осуществляет связь с Web-сервером для обработки и предоставления данных. Обычно он применяется в узлах для создания интерактивных HTML-форм (бланков), заполняемых пользователями, которые затем передаются на сервер для обработки. При использовании CGI-сценария пользователь взаимодействует с броузером при заполнении формы, после чего броузер должен взаимодействовать с сервером для обработки содержимого формы. Следовательно, после того как пользователь заполнит и представит форму, броузер посылает информацию на сервер, который в свою очередь выполняет сценарий (набор запрограммированных команд) обработки содержимого формы. В зависимости от заданного сценария сервер может послать ответ обратно на броузер, который отобразит результат пользователю.

HTML-форма аналогична стандартному HTML-документу с добавлением тегов <FORM> и </FORM> и связи с CGI-сценарием. Для разработки разнообразных интерактивных HTML-форм можно использовать набор стандартных CGI-сценариев.

Таким образом, включение в корпоративную сеть интерактивных функций упрощает служащим и клиентам использование ресурсов сети, и прежде всего базы данных, программа которой обычно постоянно находится на Web-сервере.

Эффективным средством создания корпоративной сети является ***Front Page*** — интегрированный пакет фирмы Microsoft для размещения материалов на Web. Он включает HTML-редактор, программу для работы с Web-документами, персональный Web-сервер и набор расширения сервера. Front Page — это новый инструмент, упрощающий разработку Intranet. Среда разработки Front Page работает

под управлением Windows, но ее также можно установить на сервер, функционирующий под управлением Unix.

В отличие от автономных инструментов для работы в формате HTML, инструментальных средств поиска или продуктов для дискуссионных групп Front Page включает все эти компоненты в один программный пакет, причем его базовые компоненты разделены на две части: сторону клиента и сторону сервера. Программное обеспечение стороны клиента предназначено для предоставления пользователям инструментальных средств, необходимых при составлении статических и динамических страниц в формате HTML, а также средств, позволяющих проводить поиск и работу в дискуссионной группе. Инструментальные средства стороны сервера включают Front Page

Personal Web Server и программные расширения сервера, обеспечивающие независимость компонентов стороны клиента от сервера (с помощью этих средств пользователи могут сами разрабатывать и проверять свои материалы, размещаемые на Web).

Intranet как модель группового сотрудничества не нова. В 1989 г. пакетом Lotus Notes фирмы Lotus Corporation (США) установлен стандарт для совместного использования информации и внутрикорпоративного сотрудничества. Lotus Notes — это фирменное программное обеспечение типа «клиент — сервер», которое поддерживает связь в группе, электронную почту, дискуссии, дублирование базы данных и среду разработки приложений. Оно разрабатывается и совершенствуется уже в течение 12 лет и более 3 млн пользователей имеют на него лицензии.

Сравнивая конкурирующие средства Lotus Notes и Intranet, можно обнаружить, что для каждого из них характерны свои преимущества и недостатки.

Основные ***преимущества Lotus Notes (или просто Notes) перед корпоративными сетями*** заключаются в следующем [4]:

- Notes — вполне законченное изделие, на его создание и совершенствование фирма Lotus затратила многие годы, и в настоящее время оно доминирует среди программных продуктов для рабочих групп типа «клиент — сервер». Notes управляет корпоративной информацией, собирая и сохраняя ее в центральных устройствах памяти;
- Notes автоматически прослеживает версии документа, в то время как в большинстве корпоративных сетей задача просмотра и сохранения документов передается пользователю, что при наличии тысяч документов, содержащихся в Intranet, представляется довольно непростым делом;
- в Notes организована многоуровневая безопасность информации, что существенно надежнее, чем в предназначенных для Intranet программных пакетах (если необходима секретность при работе с документами, то современные программные продукты для Intranet могут не соответствовать поставленным требованиям);
- Notes располагает набором программ, реализующих готовые к использованию средства координации совместной работы;
- Notes предоставляет пользователям возможность быстрой разработки новых баз данных и, кроме того, обеспечивает синхронизацию содержимого различных баз данных.

Преимущества корпоративных сетей, основанных на Web-подходе, перед

пакетом Notes:

- корпоративные сети в большей степени масштабируемы, т.е. после установки Intranet можно без особых трудностей и затрат наращивать ее возможности, чего нельзя сказать о пакете Notes: он масштабируется гораздо сложнее, так как предлагает меньшее количество программных решений;
- изменение и улучшение технологий Intranet .осуществляется намного быстрее, чем Notes, так как этим занимаются тысячи программистов, а развитием Notes занята только IBM;
- программное обеспечение Notes значительно дороже;
- использование Notes автоматически связано с необходимостью привязки компании к фирменным технологиям Lotus (что многими воспринимается как существенный недостаток), а также к точке зрения только одной фирмы на прикладное программное обеспечение для рабочих групп. При работе с Intranet можно выбирать любых поставщиков продукции, удовлетворяющей предъявляемым требованиям;
- для разработки приложений под Notes программисты компании должны использовать базы данных Notes и соответственно преобразовать уже существующие приложения.

Хотя Notes и Intranet дополняют (а не исключают) друг друга, по соображениям издержек приходится выбирать что-то одно. Какую из этих технологий необходимо развернуть в своей компании, зависит от ее потребностей. Предпочтение следует отдать Notes, если в качестве критериев выбора принимаются такие: наличие высокоинтегрированного набора инструментальных средств, наличие многоуровневой системы безопасности, возможность координации совместной работы, необходимость ограничения числа служащих по управлению данными и поддержке приложений, необходимость в сложной системе управления документооборотом.

Выбор будет в пользу Intranet, если: необходимо иметь развитую и эффективную электронную систему размещения и распределения документов, когда их создание и обслуживание осуществляются в различных подразделениях компании; имеющиеся в Intranet средства e-mail и конференц-связи Web вполне удовлетворяют потребности в организации совместной работы; ограничения по количеству служащих, занятых управлением данными, не накладываются (пользователи сами управляют документами); необходимо разрабатывать сложные заказные приложения корпоративной сети; есть возможность появления в продаже усовершенствованных версий программного обеспечения Intranet. В настоящее время наблюдается тенденция к сближению прикладных программных продуктов для рабочих групп (таких, как Notes) и основанных на Intranet решений. Фирма Lotus подтвердила, что будущее принадлежит открытым системам. Новое программное обеспечение Inter Notes Web Publisher, являющееся неотъемлемой частью Notes, позволяет пользователям Notes автоматически связываться с серверами Notes, используя Web-броузер, а также транслировать документы Notes в Web-страницы.

Для сокращения времени на создание и запуск корпоративной сети необходимо решить вопрос: что из готового программного обеспечения следует приобрести, а что нужно разработать собственными силами? В настоящее время на

рынке имеются четыре группы современных программных средств для Intranet: поисковые серверы; программное обеспечение для дискуссионных групп; системы управления документами и программы координации совместной работы.

Средства поискового сервера помогают быстро и эффективно находить нужную информацию в корпоративной сети. Программное обеспечение для дискуссионных групп, способствующее совместной работе над проектами, может работать на различных платформах (такие программы отличаются по своим характеристикам и стоимости установки). Большинство систем управления документами, помогающие пользователям находить нужные документы и управляющие внесением изменений в документы, основаны на фирменных-технологиях. Они сложнее и дороже программ для поиска и дискуссионных групп. Программы координации совместной работы, позволяющие пользователям автоматизировать текущие производственные процессы, могут быть расширениями системы управления документами. Они также сложны и требуют обучения сотрудников. Интегрированные программные продукты лучше всего подходят для крупных организаций с большими информационно-технологическими ресурсами.

Развитие программного обеспечения корпоративных сетей, как и сети Internet, связано с широким использованием достаточно нового языка программирования — Java, основное назначение которого — предоставление пользователям возможности выполнять программы прямо на Web-страницах. С помощью Java программисты могут создавать небольшие приложения (апплеты) со встроенными мультимедийными средствами, такими, как текст, изображения, звук и видеоматериалы. Апплеты Java независимы от платформы, т.е. если создан апплет для использования под Windows, он может выполняться на любом броузере, например на броузере, работающем под Unix. Разработчики языка Java при его формировании имели в виду и проблемы безопасности: ограничения, содержащиеся в Java, затрудняют создание вирусов на этом языке.

16.3. Сетевое оборудование КВС

В настоящее время сетевое оборудование выпускается многими фирмами, каждая из которых энергично рекламирует свою продукцию, что создает дополнительные трудности при его выборе. Есть несколько критериев, которыми следует руководствоваться при выборе сетевого оборудования. К ним относятся:

- характеристика фирмы — производителя сетевого оборудования, ее известность на рынке сбыта как производителя высококачественной продукции;
- функциональные возможности изделия, его выходные технико-эксплуатационные характеристики и условия эксплуатации;
- наличие стандартов по изделию;
- возможность подбора оборудования, производимого одной и той же фирмой.

Ниже даются краткие сведения по основному сетевому оборудованию КВС, используемому в сетях X.25 и FR.

Модемы — это наиболее массовый вид оборудования в сетях. Они различаются между собой по способу модуляции, пропускной способности, способу коррекции ошибок, способу сжатия данных. Для различных скоростей работы модемов, различных способов коррекции ошибок и сжатия данных разработаны

стандарты.

При построении сети на базе телефонных каналов широко используются модемы серии 326xV.34 SDC (Synchronous Data Compression) фирмы Motorola — мирового лидера в производстве высокоскоростных аналоговых устройств. Эти модемы являются одной из лучших реализаций стандарта V.34. Они позволяют передавать по 2 — 4-провод-ным выделенным каналам связи данные со скоростью до 28,8 Кбит/с, в качестве дополнительного средства повышения скорости и достоверности данных реализован режим синхронной компрессии (при этом скорость возрастает до 128 Кбит/с), что делает эти модемы идеальными для сетей X.25/ Frame Relay.

Модемы стандарта V.34 включают в свой состав последние достижения в технологии модуляции, в том числе: предварительное тестирование линии, предварительный выбор способа кодирования, адаптивное управление мощностью сигнала, многомерное решетчатое кодирование. Это позволяет достичь максимально возможной скорости передачи, что особенно важно при использовании телефонных линий невысокого качества.

Модемы семейства 326x успешно применяются для соединений между собой маршрутизаторами и удаленными локальными сетями, в качестве альтернативы дорогим цифровым сетям передачи данных, для ответственных приложений, требующих надежной и устойчивой связи. Они прошли испытания на всей территории России и отлично зарекомендовали себя на отечественных каналах связи.

К наиболее распространенным модемам для передачи данных и факса производства фирмы Motorola относятся следующие [20]:

- модемы серии 3400 PRO PC — для передачи данных и факса по 2-проводным коммутируемым линиям со скоростью от 300 бит/с до 28,8 Кбит/с; скорость передачи в синхронном режиме до 115,2 Кбит/с, скорость передачи факса от 2400 до 14400 бит/с;
- модемы серии PREMIER 33,6, их характеристики близки к характеристикам серии 3400 PRO PC. Большой популярностью пользуются технические средства для построения корпоративных сетей связи, производимые компанией **RAD** DATA COMMUNICATIONS. Среди них — модемы для проводных выделенных линий связи, в частности синхронные модемы для работы на 4-проводных линиях в дуплексном режиме:
- ASM-20, скорость от 32 до 256 Кбит/с, радиус действия на проводе-сечением 0,5 мм равен 7,5 км при скорости передачи 64 Кбит/с;
- ASM-40, скорость от 64 до 2048 Кбит/с, радиус действия может достигать до 20 км;
- MTM-20, скорость от 32 до 64 Кбит/с, радиус действия — до 14 км при скорости передачи 32 Кбит/с.

Мультиплексоры — это многофункциональные устройства, используемые в качестве устройств доступа к сетям, а также для построения узлов корпоративной сети. В настоящее время в сетях с коммутацией пакетов чаще всего используются мультиплексоры CX-1000 фирмы Memotec, MPRouter 6520 фирмы Motorola, Kilomux-3000 фирмы RAD.

Рассмотрим характеристики мультиплексора/коммутатора CX-1000,

предназначенного для организации передачи голоса/данных в сетях FR. Фирма-производитель Memotec — широко известная североамериканская транснациональная компания, работающая на рынке сетевого оборудования с 1969 г. Изделие CX-1000 имеет модульную конструкцию, что позволяет создавать узел сети с необходимым набором функций и требуемым числом портов в одном шасси.

С учетом возможности одновременной передачи данных, оцифрованного голоса и факсимильных сообщений изделие CX-1000 имеет много уникальных особенностей [20]:

- минимальная скорость оцифровки голоса равна 4,8 бит/с, причем реализован механизм подавления пауз, позволяющий экономить до 50 % полосы пропускания канала, отводимой под передачу голоса;
- механизм голосовой компрессии, используемый в изделии, устойчив к потерям кадров, т.е. голосовое соединение не разрывается и качество передачи голоса остается удовлетворительным;
- в голосовой модуль изделия заложены возможности автоматического распознавания и передачи сигналов факсимильных аппаратов, что позволяет использовать порты голосовой платы для подключения этих аппаратов без изменения конфигурации модуля;
- голосовой модуль поддерживает все существующие аналоговые и цифровые интерфейсы телефонного оборудования. В сочетании с развитыми встроенными функциями коммутации голосовых соединений это дает возможность реализовать территориально-распределенную ведомственную телефонную сеть с подключенными к ней телефонно-факсимильными аппаратами, учрежденскими и городскими АТС.

В состав мультиплексора CX-1000 входит большой набор функциональных модулей, каждый из которых включает одну процессорную плату и несколько плат ввода-вывода.

К основным функциональным модулям относятся:

- FR-600 — модуль коммутации/доступа Frame Relay, выполняющий функции центра коммуникации сети FR и устройства доступа к ней. Модуль выполняет процедуры протоколов управления FR, решает задачи маршрутизации, поддерживая четырехуровневую систему абсолютных и относительных приоритетов информационных потоков, широковещательную передачу, фрагментацию и компрессию данных;
- AC-600 — модуль передачи голоса/факса по сети FR через модуль FR-600. Он поддерживает функции коммутации телефонных соединений и обеспечивает автоматический выбор свободного канала из группы, автоматическое соединение, переадресацию вызова и т.д. Модуль обеспечивает подключение как обычных аналоговых телефонных аппаратов, так и учрежденских и городских АТС, построение ведомственной распределенной телефонной сети, наложенной на сеть передачи данных. Оцифровка голоса осуществляется со скоростью 4,8 и 8 Кбит/с, автоматическое распознавание и передача сигналов факсимильного обмена — со скоростью от 2,4 до 9,6 Кбит/с. При использовании этого модуля уменьшается вероятность несанкционированного доступа к голосовым сообщениям, так как вся информация оцифровывается, кодируется и уплотняется в общий поток, что исключает возможность прямого прослушивания телефонных переговоров в канале связи;

• CL-600 — модуль удаленного моста-маршрутизатора, обеспечивающий взаимодействие удаленных ЛВС через сеть FR (типы ЛВС Ethernet или Token Ring, количество — до 256). Маршрутизация выполняется для протоколов IP и IPX;

• PX-674 — модуль коммутации пакетов сетей X.25, FR. Может функционировать в качестве центра коммутации пакетов сети X.25, а также осуществлять инкапсуляцию данных в кадры FR для передачи их по сети (через модуль FR 600);

• DI-600 — модуль интерфейса E1/T1, обеспечивающий использование цифровых групповых каналов учреждения и городских АТС (24 канала T1 или 20 каналов E1) для передачи голосового трафика в сеть FR, осуществляя при этом компрессию оцифрованного голосового трафика (скорость передачи речи — 5,8 и 8 Кбит/с). Модуль полностью совместим с модулем AC-600, он выполняет практически те же функции: коммутацию голоса, автоматическое распознавание и передачу сигналов факсимильного обмена, подавление пауз, автоматическое соединение, переадресацию вызова, автоматический вызов свободного канала из группы;

• MC-600 D — низкоскоростной модуль компрессии данных, поддерживающий практически все известные типы сетевых архитектур и протоколов (скорость портов до — 128 Кбит/с);

• HC-600 — высокоскоростной модуль компрессии, функционально аналогичный модулю MC600D (скорость портов — до 2048 Кбит/с);

• FX-600 — новый многофункциональный модуль, отличающийся универсальностью: он может одновременно выполнять функции моста-маршрутизатора локальной сети, коммутатора FX, центра коммутации пакетов для протоколов X.25, а также предоставлять широкий набор сервисных услуг (разграничение доступа, создание пользовательских групп, учет графика и т.д.).

Оборудование опорных узлов КВС. Кроме многофункциональных устройств типа CX-1000, в сетях связи КВС могут использоваться устройства с ограниченным числом выполняемых функций для создания опорных узлов. Характеристики некоторых из этих устройств указаны ниже.

1. Региональный концентратор серии RC 6500 Plus производства фирмы Motorola, предназначенный для создания высокопроизводительных узлов связи в сетях FR и X.25. Его основные функции: обеспечение коммутации пакетов в сетях X.25/FR и доступ абонентов к этим сетям по выделенным и коммутируемым линиям связи, поддержка от 12 до 54 последовательных синхронных/асинхронных портов. Каждый порт может быть сконфигурирован как устройство доступа к сети FR, как коммутатор пакетов X.25 или пакетов FR, как сборщик/разборщик пакетов с поддержкой стандартов X.28 и X.29.

На базе концентратора RC 6500 Plus можно создавать компактные высокопроизводительные узлы коммутации пакетов, конструктивно объединенные с модемами, мультиплексорами и другим оборудованием канала передачи данных.

2. Удаленный многопротокольный мост/маршрутизатор *с* гибкой расширяемой конфигурацией ***серии 6520*** (Multimedia Perupheru Router фирмы Motorola), имеющий до 17 портов, что позволяет использовать его для больших отделений корпорации. Изделие имеет специализированный процессор для сжатия данных и программное обеспечение, реализующее широкий набор протоколов.

3. Многопротокольный мост/маршрутизатор серии 6560, представляющий собой более совершенный вариант изделия серии 6520. Он поддерживает скорость во всех каналах до 2 Мбит/с, число портов увеличено до 19, процессор обеспечивает сжатие данных для 15, 75 и 508 каналов.

Система видеоконференц-связи. Организация видеоконференц-связи (ВКС) имеет исключительно важное значение для обеспечения оперативного обмена информацией и принятия обоснованных, приемлемых для всех участников видеоконференции решений, касающихся производственно-хозяйственной деятельности корпорации.

Из ряда систем ВКС выделим систему OnLAN фирмы RADVision, получившую известность и предназначенную для организации ВКС в локальных или территориально-распределенных сетях. Она относится к классу настольных систем ВКС и может быть установлена на любой персональный компьютер, совместимый с IBM PC. При работе через распределенную сеть можно использовать каналы с пропускной способностью 64 Кбит/с. Обеспечиваемая скорость обмена информацией — от 64 до 384 Кбит/с с частотой смены кадров 15 кадров/с и 30 кадров/с при использовании различных стандартов. Система обеспечивает поддержку стандартных телефонных услуг: набор номера вызываемого абонента с клавиатуры или с помощью системного телефона, соединения, регулировку громкости звука, разъединение. Для передачи звука используется компрессия. Все оборудование станции соответствует стандарту ITU-T, регламентирующему передачу видеоизображения и голоса в распределенных сетях, что обеспечивает совместимость системы OnLAN с видеоконференциями других производителей.

Оборудование системы OnLAN для проведения ВКС состоит из видеостанции (рабочего места для конечного пользователя) и маршрутизатора видеопотока.

Видеостанция включает плату компрессии-декомпрессии (Codec), к которой подключается видеокамера, активные колонки и набор соединительных кабелей. Используются видеокамеры с системой дистанционного позиционирования и дистанционного управления такими функциями, как панорама и увеличение. Программное обеспечение видеостанции позволяет осуществлять работу с независимо масштабируемыми окнами принимаемого и передаваемого изображения.

Маршрутизатор видеопотока при организации ВКС играет ключевую роль. Он устанавливает соединения между видеостанциями, обеспечивает соединение различных сегментов локальной сети, осуществляет маршрутизацию видеопотока между локальными сетями и территориальной сетью. Один маршрутизатор видеопотока может обеспечить одновременное проведение четырех сессий. Маршрутизатор может использоваться для организации ВКС в нескольких локальных сетях, взаимодействующих через территориально-распределенную сеть.

Системы управления сетью. Надежное функционирование сети обеспечивается ее системой управления. В настоящее время ряд фирм выпускает системы управления, по своим функциональным возможностям мало отличающиеся друг от друга. Рассмотрим системы управления сетью фирмы Motorola.

Система управления 9000-PC предназначена для управления малыми и средними сетями на базе устройств производства фирмы Motorola и других поставщиков оборудования, поддерживающих протокол SNMP. Программное

обеспечение системы 9000-PC создает полную и надежную систему управления по этому протоколу на базе персонального компьютера. Система позволяет управлять, конфигурировать и тестировать изделия фирмы Motorola, поддерживающие протокол SNMP.

Система управления 9000-VX фирмы Motorola обеспечивает управление модемами и устройствами сетевого доступа этой фирмы, а также оборудованием других фирм, поддерживающих протокол SNMP. Она может быть использована для управления как существующими сетями, так и сетями будущего. Система управления реализована на базе наиболее популярной платформы управления HP Open View, графические возможности которой позволяют отображать общую топологию и каждый элемент сети в отдельности.

16.4. Безопасность КВС

Вопросы обеспечения безопасности информации КВС, ее информационных и программных ресурсов (или: вопросы безопасности КВС) приобретают особое значение, если принять во внимание конфиденциальный характер информации, зачастую представляющий собой фирменную тайну. Структура Intranet, как и структура Internet, во многих случаях обеспечивает свободный поток информации и не содержит адекватных средств ее защиты от несанкционированного доступа, что позволяет злоумышленникам получать информацию прямо из корпоративной сети. Поэтому, создавая корпоративную сеть, необходимо разработать и реализовать стратегию обеспечения безопасности, позволяющую защитить сеть от внешних и внутренних несанкционированных посетителей.

16.4.1. Принципы построения системы обеспечения безопасности КВС

В рамках построения защищенной корпоративной сети принципиально возможен выбор одной из двух концепций [57]:

- создание надежной системы обеспечения безопасности (СОБ) корпоративной сети, построенной на базе каналов связи и средств коммутации ТСС общего пользования, в которой применяются открытые протоколы Internet;
- отказ от средств Internet, создание корпоративной сети на базе специализированной или выделенной сети связи с использованием конкретной сетевой технологии, в частности ATM, FR, ISDN. Эти концепции представляют полярные взгляды на решение проблемы обеспечения безопасности КВС и, как следствие, имеют определенные недостатки. Первая концепция связана с большими затратами на обеспечение надежной защиты информации при подключении КВС к Internet. Вторая предлагает отказаться от услуг Internet и реализуемых в ней технологий, убедительно доказавших свою жизнеспособность и эффективность. Очевидно, что решение проблемы обеспечения безопасности КВС представляет собой некоторый компромисс между этими концепциями.

Отличительными особенностями КВС можно считать централизованное управление сетью связи и заданный уровень защищенности сети, определяемый конфиденциальностью обрабатываемой информации и учитывающий характеристики средств и каналов связи. Компромиссное решение по созданию СОБ корпоративной сети, использующей каналы Internet, может базироваться на двух основных принципах [57]:

• использование закрытого протокола при установлении соединения «клиент — сервер», обеспечивающего защищенное взаимодействие абонентов по виртуальному каналу связи;

• доступность открытых протоколов (команд Internet) для взаимодействия по защищенному виртуальному каналу после установления соединения.

16.4.2. Функциональные требования к СОБ корпоративной сети

К основным функциональным требованиям относятся следующие.

1. ***Многоуровневость*** СОБ, предусматривающая наличие нескольких рубежей защиты, реализованных в разных точках сети.

2.*Распределенность* средств защиты по разным элементам сети с обеспечением автономного управления каждым из этих средств.

3.*Разнородность или разнотипность* применяемых средств защиты. Предпочтение должно отдаваться аппаратным средствам, так как они не поддаются прямому воздействию из внешней сети. Однако на разных уровнях защиты должны использоваться и программные средства. Требование разнотипности относится и к использованию различных механизмов защиты: нельзя ограничиваться, например, одной криптографической защитой или построением сверхзащищенной технологии аутентификации, необходимо реализовать и другие механизмы защиты.

4. ***Уникальность защиты,*** являющаяся ее краеугольным камнем. Степень защищенности КВС можно оценить сложностью и, главное, оригинальностью алгоритма защиты, деленному на количество реализаций такого алгоритма.и на время его использования. Это означает, что с течением времени любой механизм защиты будет вскрыт, особенно если он многократно тиражирован, т.е. представлен для исследования большому количеству хакеров. Следовательно, предпочтение следует отдать собственному механизму защиты, уникальность которого ослабит интерес со стороны хакеров, поскольку их в гораздо большей степени привлекают массовые, типовые решения (для них можно создать стандартные средства вскрытия, допускающие тиражирование).

5. ***Непрерывность развития*** **СОБ,** т.е. постоянное наращивание возможностей и модификация системы защиты с течением времени. Развитие должно быть заложено в самом механизме защиты. Разработка СОБ — это не одноразовое действие, а постоянный процесс.

6. ***Распределение полномочий,*** в соответствии с которым ни один человек персонально не имеет доступ ко всем возможностям системы. Такие возможности открываются только группе уполномоченных лиц. Один из аспектов этого требования заключается в том, что сменный дежурный администратор сети не может обладать теми же полномочиями по конфигурированию системы защиты, которыми обладает администратор по управлению безопасностью сети.

7. ***Прозрачность и простота*** средств защиты. Это требование трудно реализовать на практике, оно достаточно противоречиво. Для эксплуатации СОБ лучше иметь много простых и понятных средств, чем одно сложное и трудновоспринимаемое средство. Однако для защиты от хакеров предпочтительными могут оказаться сложные и «непрозрачные» решения.

8. ***Физическое разделение*** (подключение к различным связным ресурсам) серверов и рабочих мест, т.е. организация подсетей рабочих мест и серверов.

9. ***Обеспечение предотвращения несанкционированного доступа*** к информационным ресурсам КВС со стороны внутренних и внешних недоброжелателей. Для этого следует предусмотреть такие мероприятия:

- снабдить КВС межсетевыми средствами защиты от несанкционированного доступа, которые должны обеспечить сокрытие структуры защищаемых объектов, в частности IP-адресов (шифрование этих адресов недопустимо при использовании средств коммутации ТСС общего пользования);
- обеспечить закрытие и несовместимость протоколов верхних уровней (5-го и 7-го уровней модели ВОС) с протоколами телекоммуникационных служб Internet при установлении соединения и открытие при обмене информацией;
- обеспечить защиту от возможной подмены алгоритма взаимодействия клиента с сервером при установлении соединения между ними;
- исключить сервер Internet (коммуникационный сервер доступа к Internet) из подсети функциональных серверов КВС; он должен иметь собственную группу рабочих станций, исключенных из подсети функциональных рабочих мест КВС.

10. ***Организация централизованной службы административного управления сети,*** включающей службы управления: эффективностью функционирования; конфигурацией и именами; учетными данными; при отказах и сбоях. Создание единого центра управления сетью связи (ЦУС).

11. ***Организация централизованной службы административного управления безопасностью сети,*** обеспечивающая высокий уровень защищенности КВС. Создание выделенного центра управления безо-

пасностью (ЦУБ) сети, основные функции которого: сбор информации о зарегистрированных нарушениях, ее обработка и анализ с целью удаленного управления всеми техническими средствами защиты информации. Функции ЦУБ и ЦУС не должны быть совмещены на одном рабочем месте администратора сети, хотя они и являются службами сетевого управления. Необходимо предусмотреть алгоритм взаимодействия между ними, с тем чтобы предотвратить принятие прямо противоположных решений, принимаемых администраторами для управления и защиты ВКС в процессе ее функционирования.

Ориентация на эти требования и их реализация обеспечивают безопасность информации в КВС, т.е. создают такие условия ввода-вывода, хранения, обработки и передачи, при которых гарантируется достаточная степень защиты от утечки, модификации и утраты, а также свободный доступ к данным только их владельца и его доверенных лиц. Удовлетворение перечисленных требований позволяет формировать ***систему обеспечения безопасности*** корпоративной сети, которая представляет собой совокупность правил, методов и аппаратно-программных средств, создаваемых при ее проектировании, непрерывно совершенствуемых и поддерживаемых в процессе эксплуатации для предупреждения нарушений нормального функционирования при проявлении случайных факторов или умышленных действий, когда возможно нанесение ущерба пользователям путем отказа в обслуживании, раскрытия или модификации защищаемых процессов, данных или технических средств.

Количественная оценка прочности защиты (вероятности ее преодоления) может осуществляться с помощью временного фактора. Если время контроля и передачи сообщения в ЦУБ о несанкционированном доступе меньше ожидаемого

времени, затрачиваемого нарушителем на преодоление средств защиты и блокировки доступа к информации, то вероятность преодоления этих средств приближается к единице, в противном случае прочность защиты выше. Средства защиты обеспечивают приемлемую прочность, если ожидаемые затраты времени на их преодоление будут больше времени жизни информации, подлежащей защите.

16.4.3. Классификация средств защиты

Рассмотрим классификационную структуру средств защиты, причем деление их на группы будет осуществляться в зависимости от способа реализации [25;38].

1. ***Организационные методы обеспечения безопасности.*** Они являются первым (или последним) рубежом защиты сети и представляют собой некоторый набор инструкций, определяющий обязательные для всех пользователей порядок и правила использования компьютеров сети, а также ограничения по правилам доступа в компьютерные помещения.

2. ***Технологические методы обеспечения безопасности.*** **Они** могут рассматриваться как основа защиты любой системы. Любое технологическое решение реализуется организационно, аппаратно или программно. Примеры технологических решений: фильтрация пакетов, мониторинг и аудит системы, автоматическое ведение журналов регистрации, система «обратного дозвона» при наличии в сети удаленных пользователей (система не устанавливает соединение по запросу удаленного пользователя, а только регистрирует запрос на соединение и сама производит обратный вызов абонента по указанному им адресу).

3. ***Программные средства защиты.*** Это наиболее распространенные средства, так как с их помощью могут быть реализованы практически все идеи и методы защиты, и, кроме того, по сравнению с аппаратными средствами они имеют невысокую стоимость. С помощью программных методов обеспечения безопасности реализованы почти все межсетевые экраны и большинство средств криптографической защиты. Основным их недостатком является доступность для хакеров, особенно это касается широко распространенных на рынке средств защиты. Поэтому желательна разработка собственных оригинальных программных средств защиты.

4. ***Аппаратные средства защиты.*** Такие средства принадлежат к наиболее защищенной части системы. С их помощью также могут быть реализованы любые концепции защиты, но стоимость реализации оказывается на порядок выше по сравнению с аналогичными по назначению программными средствами. При наличии выбора предпочтение следует отдавать аппаратным средствам защиты, так как они исключают любое вмешательство в их работу непосредственно из сети. Изучение работы этих средств возможно только при наличии непосредственного физического доступа к ним. Другим преимуществом аппаратных средств является большая их производительность по сравнению с программными средствами защиты (особенно в случае их использования в устройствах криптографической защиты).

5. ***Аппаратно-программные (гибридные) методы защиты.*** Это средства, основанные на использовании технологических устройств, допускающих некоторую настройку параметров их работы программными методами. Они представляют собой компромисс между предыдущими двумя способами и совмещают высокую производительность аппаратно реализованных систем и гибкость настройки

программных. Типичными представителями такого рода устройств является аппаратно реализованные маршрутизаторы фирмы Cisco, которые допускают их настройку в качестве пакетных фильтров.

По способу реализации программного управления аппаратные средства можно разделить на два вида: предусматривающие свою

программную настройку с помощью сетевого компьютера, к которому они подключены, и требующие программирования своей работы с помощью специального устройства, отличного от используемого в сети компьютера. Вторые обладают тем очевидным преимуществом, что после соединения с компьютером сети их программа не может быть изменена.

16.4.4. Способы разработки средств защиты

Существуют различные варианты разработки средств защиты для СОБ корпоративной сети: коммерческая реализация средств защиты, самостоятельная разработка, индивидуальный заказ средств защиты, смешанный (гибридный) подход к реализации этих средств. Приведем краткую характеристику этих вариантов.

Коммерческая реализация средств защиты в настоящее время остается единственным доступным полнофункциональным решением для аппаратных и программных средств. При использовании таких средств следует обращать внимание на их сертификацию соответствующими органами и приобретать только лицензионные версии. Общим и очевидным недостатком является неопределенная степень защиты по отношению к возможностям фирмы-производителя. В связи с этим там, где это возможно (при разработке, например, организационных и технологических средств), следует воспринимать общие рекомендации, но не всегда использовать конкретные рекомендуемые решения. При использовании коммерческих продуктов следует хотя бы их настройку производить самостоятельно (несмотря на значительные трудозатраты), не полагаясь на конфигурацию поставки или различные установки по умолчанию.

Самостоятельная разработка средств защиты является во всех отношениях предпочтительным вариантом. Именно так должны разрабатываться организационные и технологические методы защиты. При самостоятельной разработке аппаратных и программных средств серьезным недостатком является трудность сертификации конечного продукта. Разработка программ существенно упрощается при использовании инструментальных средств программирования.

В рамках такого варианта разработки средств защиты рациональной представляется самостоятельная разработка тех дополнений этих средств, которые необходимы, но отсутствуют в готовом продукте. В этом случае получается дополнительный рубеж защиты, в том числе и от фирмы — производителя данного продукта.

2. ***Индивидуальный заказ средств защиты*** крупным производителям мог бы стать идеальным вариантом, но в настоящее время трудно найти организацию, готовую реализовать такой заказ в полном объеме, так как конкурировать с возможностями фирмы Microsoft нереально. Разработанный продукт может оказаться несовместимым с очередной версией операционной системы этой фирмы и с ее компонентами, которые развиваются удивительными темпами, исключающими возможность их полноценного предварительного тестирования и

изучения.

Смешанный подход к реализации средств защиты основан на том, что следует, не полагаясь на опыт поставщика, самостоятельно разобраться во всех возможностях настройки предлагаемого изделия и самостоятельно ее произвести, хотя это и связано с существенными трудозатратами. Такой подход почти всегда реален и реализуем.

Рассматриваемые ниже конкретные методы и средства защиты, используемые в корпоративных сетях, разделены на традиционные и специфические сетевые. Традиционные методы и средства зарождались и использовались еще до появления ТВС как в отдельных компьютерах, так и в многопользовательских средствах, построенных на одном компьютере. Сетевые методы и средства появились только с развитием сетевых технологий. Они не заменяют, а дополняют традиционные методы.

16.4.5.Традиционные методы и средства обеспечения безопасности КВС

К традиционным методам и средствам обеспечения безопасности относятся следующие.

1. ***Парольная защита*** основана на том, что для использования какого-либо ресурса необходимо задать некоторую комбинацию символов, или пароль, открывающий доступ к этому ресурсу. С помощью паролей защищаются файлы, личные или фирменные архивы, программы и отдельные компьютеры (пароль на включение компьютера). Недостатки такой защиты: слабая защищенность коротких (менее 8 символов) паролей, которые на современных компьютерах раскрываются простым перебором, и необходимость частой смены паролей. В сетях пароли используются как самостоятельно, так и в качестве основы для различных методов аутентификации.

В практике использования паролей выработался целый «свод законов», основные из которых следущие:

- в качестве пароля не может использоваться слово из какого бы то ни было языка;
- длина пароля не может быть менее 8 символов;
- один и тот же пароль не может быть использован для доступа к разным средствам;
- старый пароль не должен использоваться повторно;
- пароль должен меняться как можно чаще.

2. ***Идентификация пользователей*** представляет собой некоторое развитие системы парольной защиты на более современном техническом уровне. Она основана на применении для идентификации пользователей специальных электронных карт, содержащих идентифицирующую конкретного пользователя информацию (подобно банковским кредитным карточкам). Системы идентификации пользователей реализуются аппаратно и являются более надежными, чем парольная защита.

3. ***Аутентификация пользователей*** — это развитие систем парольной защиты и идентификации для использования в сетях. Аутентификация — это процедура проверки пользователя, аппаратуры или программы для получения доступа к определенной информации или ресурсу. По отношению к пользователю

система аутентификации обычно требует указания имени и предъявления пароля или электронной карты. Поскольку частая смена паролей, а тем более электронных карт, крайне неудобна, многие переходят на использование одноразового динамического пароля, который генерируется аппаратными или программными средствами.

4. ***Криптографические методы защиты*** являются необходимыми во всех случаях обеспечения безопасности, независимо от того, применяются они в сети или вне ее. Они основаны на шифровании информации и программ. Шифрование программ обеспечивает гарантию невозможности внесения в них изменений. Криптографическая защита данных осуществляется как при их хранении, так и при передаче по сети, причем хранение данных в зашифрованном виде существенно повышает степень их защищенности. В настоящее время доступны как программная, так и высокопроизводительная аппаратная реализация средств криптографии.

5. ***Привязка программ и данных к конкретному компьютеру (сети или ключу)*** — метод, весьма динамичный по развитию реализующих его средств защиты. Основная идея метода — включение в данные или в программу конкретных параметров или характеристик конкретного компьютера, которое делает невозможным чтение данных или исполнение программ на другом компьютере. Применительно к сети различные модификации этого метода могут требовать либо выполнения всех операций на конкретном компьютере, либо наличия активного соединения сети с конкретным компьютером. Возможности использования метода «привязки» могут значительно повысить защищенность сети.

6. Разграничение прав доступа пользователей к ресурсам сети — метод, основанный на использовании таблиц или наборов таблиц, определяющих права пользователей и построенных по правилам «разрешено все, кроме» или «разрешено только». Таблицы по идентификатору или паролю пользователя определяют его права доступа к дискам, разделам диска, конкретным файлам или их группам, операциям записи, чтения или копирования, системному принтеру и другим ресурсам сети. Возможность такого разграничения доступа определя-

ется, как правило, возможностями используемой операционной системы и заложены именно в ней. Большинство современных СОС предусматривают разграничение доступа, но в каждой из них эти возможности реализованы в разном объеме и разными способами.

7. ***Использование заложенных в ОС возможностей защиты*** — это обязательное правило. Однако большинство ОС либо имеют минимальную защиту, либо предоставляют возможности ее реализации дополнительными средствами.

Исторически сложилось так, что в США большинство потребителей в локальных сетях используют UNIX, а в России — Novel NetWare 3.x/4.x. Создаваемые в настоящее время локальные сети в России и за рубежом все в большей степени ориентируются на продукцию фирмы Microsoft — Windows NT 4.0/5.0, которая обеспечивает также подключение к Internet и позволяет реализовать унификацию интерфейсов и способов представления и передачи информации.

Windows NT является единственной коммерческой операционной системой, сертифицированной на класс защиты, который предусматривает:

- возможность владельца ресурса (например, файла) контролировать доступ к

нему;

- защиту объектов средствами ОС от повторного использования другими процессами;
- идентификацию пользователей с помощью уникальных имен и паролей, используемых для отслеживания деятельности пользователей;
- возможность аудита событий, связанных с безопасностью;
- защиту ОС самой себя от изменений.

Необходимо учитывать, что защищенность локальной сети (в том числе и являющейся частью КВС) определяется ее слабым звеном. Поэтому неоднородные сети, в которых используются разные ОС и платформы, всегда представляют повышенную опасность. Даже защита Windows NT значительно ослабляется, если в сети есть клиенты, например, Windows 95/98, не говоря об операционных системах других производителей.

16.4.6. Специфические сетевые методы и средства обеспечения безопасности КВС

Прежде всего введем понятие промежуточной сети (perimeter network), которая представляет собой совокупность оборудования (включая межсетевые экраны, маршрутизаторы, концентраторы, мосты и т.д.), расположенного между двумя объединенными сетями. Основные типы устройств защиты промежуточной сети — это пакетные фильтры, прокси-системы и системы контроля текущего состояния, которые обычно реализуются в межсетевых экранах [4].

1. ***Межсетевые экраны (брандмауэры)*** — это программные, аппаратные или программно-аппаратные механизмы защиты сети от внешнего мира, которые служат барьером, ограничивающим распространение информации из одной сети в другую.

Межсетевые экраны (МЭ) разделяются на ***открытые***, функционирующие на основе открытых протоколов Internet и предназначенные для подключения к КВС открытых серверов Internet, и ***корпоративные***, позволяющие организовать в КВС защищенное взаимодействие «клиент — сервер» с закрытыми серверами корпоративной сети, в том числе по виртуальным каналам сетей общего пользования.

Корпоративные МЭ делятся на ***внутренние*** и ***внешние.*** Внешние МЭ, работающие на виртуальном канале парами (входной и выходной МЭ), предназначены для разграничения прав доступа к виртуальному каналу связи и согласования параметров его защищенности при взаимодействии «клиент — сервер». Внутренние МЭ обеспечивают разграничение прав доступа к ресурсам информационного сервера.

Основные функции МЭ корпоративной сети [4]:

- физическое отделение рабочих станций и серверов КВС от каналов сети связи общего назначения (деление на подсети);
- согласование качества обслуживания между межсетевыми средствами защиты глобальной сети при установлении соединения;
- разграничение прав доступа пользователей КВС к серверам по нескольким критериям;
- регистрация всех событий, связанных с доступом к серверам КВС;
- контроль за целостностью программного обеспечения и данных, а также

отслеживание прерывания такого контроля во время сеанса обмена данными;

- обеспечение многоэтапной идентификации и аутентификации всех сетевых элементов;
- сокрытие IP-адресов информационных серверов.

В дополнение к службам контроля за доступом, аутентификации одноуровневых объектов и доступа к источникам данных межсетевой экран КВС на уровне взаимодействия «клиент — сервер» должен использовать средства защиты, реализующие функции таких служб безопасности: засекречивания соединения, засекречивания выборочных полей и потока данных, контроля за целостностью соединения и выборочных полей, защиты от отказов с подтверждением отправления и доставки.

Существует несколько типов межсетевых экранов, отличающихся назначением и принципами построения. Основные из них — пакетные фильтры, прокси-системы, устройства контроля текущего состояния.

Пакетные фильтры (аппаратные или программные) предназначены для ограничения входящего и исходящего трафика между адресатами (взаимодействующими абонентами) сети, реализуя при этом определенный набор правил, задаваемых при их настройке.

Примером типичного аппаратного фильтра может служить фильтрующий маршрутизатор, в который встроены функции ограничения трафика на входе и выходе. Такие фильтры достаточно гибки и обладают высокой пропускной способностью.

Программный фильтр обычно устанавливается на сетевом сервере, выполняющем роль маршрутизирующего шлюза. Он работает медленнее аппаратного фильтра, но предоставляет более удобную и гибкую систему настройки.

Прокси-система, или шлюзы прикладного уровня, реализуют идею прокси-сервера (сервера-посредника), который выступает в роли посредника между двумя сетями — внешней и внутренней (при использовании прокси-сервера корпоративная сеть и Internet физически не соединены). Их преимущества: сохранение инкогнито компьютера конечного пользователя (сокрытие IP-адреса этого компьютера от хакера) и экономия адресного пространства (для внутренней сети может использоваться любая схема адресации, включая использование официально не зарегистрированных IP-адресов).

Основной недостаток прокси-систем — поддержка только тех протоколов, для которых они разработаны. Кроме того, они обладают недостаточными «прозрачностью» и производительностью в случае использования высокоскоростных соединений.

Устройства контроля текущего состояния обеспечивают отслеживание соединения по его установлению. Они повышают безопасность сети и значительно производительнее прокси-систем. В отличие от фильтров такие устройства не просто ориентируются на заголовок IP-пакета, но и проверяют информацию о приложении, чтобы убедиться, что это действительно тот пакет, который объявлен в заголовке.

2. ***Средства усиления защиты сети*** — это некоторые устройства промежуточной сети и отдельные технологические решения.

К ним относятся:

- переключаемые мосты на концентраторе, которые, контролируя направление трафика в сети и производя дополнительную фильтрацию пакетов, создают еще один барьер для хакеров;
- шлюзы уровня виртуального канала позволяют пользователям соединяться и обмениваться пакетами с сервером, при этом каждый пакет в отдельности не проверяется, а после проверки адресных данных принимаются сразу несколько пакетов; могут использоваться для полного запрета прямых контактов компьютеров внутренней сети с внешней сетью;
- изоляция протоколов, основанная на использовании протокола TCP/ IP только для связи с Internet. Во внутренней (локальной) сети используются другие протоколы, несовместимые с TCP/IP, а доступ в Internet осуществляется через шлюз прикладного уровня;
- создание виртуальной частной сети, если предусматривается подключение удаленных пользователей к КВС. Применение такой технологии основано на аутентификации удаленных пользователей и шифровании всего сетевого трафика;
- реализация межсетевого экрана на внутреннем сервере. Такой экран является последним рубежом защиты, он располагается после выделенного сетевого экрана.

3. ***Мониторинг и аудит сети*** составляют основу обеспечения безопасности. Мониторинг (контроль текущего состояния и параметров работы сети) и аудит (регулярный анализ журналов регистрации для выявления происходящих в сети процессов и активности пользователей) — это обязательные составные части работы сетевого администратора. Большинство сетевых ОС имеют встроенные или дополнительно поставляемые программы, обеспечивающие проведение этой работы. Для этой же цели могут использоваться дополнительные средства: аппаратные или программные перехватчики пакетов (анализируют собранные пакеты на наличие в них информации, которой может воспользоваться злоумышленник), аппаратно реализованные анализаторы сети (измеряют и контролируют трафик в сети).

4. ***Архитектурные методы защиты,*** к которым относятся решения, принимаемые на уровне топологии и архитектуры сети и повышающие ее защищенность в целом. Различают решения, принимаемые на уровне топологии и архитектуры внутренней сети (корпоративной, локальной), и решения на уровне промежуточной сети, связывающей внутреннюю сеть с внешней, например с сетью Internet.

На уровне топологии и архитектуры внутренней сети могут приниматься такие решения:

- физическая изоляция закрытого сегмента внутренней сети, содержащего конфиденциальную информацию, от внешней сети. Связь с внешней сетью поддерживается через открытый сегмент внутренней сети;
- функциональное разделение внутренней сети на подсети, при котором в каждой подсети работают пользователи (сотрудники компании), объединенные по профессиональным интересам;
- сеансовое (кратковременное) подключение внутренней сети к сегменту сети, подключенному к Internet, с помощью' коммутатора и/или переключаемого

моста (любое кратковременное соединение с внешней сетью более безопасно, чем постоянное соединение). Многие меры обеспечения безопасности на уровне архитектуры промежуточной сети связаны с реализацией компонентов многоуровневой защиты. Если промежуточная сеть включает маршрутизатор, компьютер, выделенный для межсетевого экрана, и концентратор, соединенный непосредственно с сервером внутренней сети, то средства защиты могут быть реализованы на каждом из этих устройств. Например, на маршрутизаторе — фильтрация пакетов, на компьютере — межсетевой экран, на концентраторе — переключаемый мост и виртуальная ЛВС, на сервере внутренней сети — еще один межсетевой экран.

Следует еще раз подчеркнуть, что при построении системы обеспечения безопасности КВС предпочтение следует отдавать аппаратным или аппаратно-программным средствам защиты. Чисто программные средства не обеспечивают такой же надежной защиты.