АНАЛИЗ СЕТЕВОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

Щербаков С.В., Коннов А.Л., канд. техн. наук, доцент
Оренбургский государственный университет

Сетевая инфраструктура представляет собой совокупность различного оборудования, программного обеспечения, которая формирует особую среду для эффективного процесса обмена данными, а также для работы бизнес-приложений.

В настоящее время будущее каждой компании напрямую связано с возможностью её оперативного реагирования на тенденции развития рынка. Именно поэтому современная компания обязана функционировать как хорошо отлаженный механизм. Она должна быть управляемой. Степень такой управляемости организации зависит от того, как хорошо в ней поставлен сбор, обработка и хранение информации, необходимой для принятия решения. Если информационная система (ИС) организована должным образом, то компания в состоянии решать поставленные задачи. В основе такой ИС лежит сетевая инфраструктура. Когда в организации установлено более одного персонального компьютера (ПК), которые не объединены в одну общую локальную сеть, это приводит к возникновению многочисленных проблем. Все они связаны с поиском, восстановлением и передачей информации, отсутствием возможности пользоваться данными дома либо во время командировок, совместной работой над различной документацией, подключением к сети интернет при помощи периферийного оборудования. Это и многое другое существенно уменьшает эффективность работы любой организации. Но правильная организация и эксплуатация объектов сетевой инфраструктуры легко решает данные проблемы. Именно поэтому любой руководитель компании обязан обращать на это своё внимание. Сетевая инфраструктура предприятия представляет собой комплекс следующих устройств. В локальную сеть входит программное обеспечение аппаратных средств, которые объединены в одну общую платформу. К активному оборудованию относятся коммутаторы, маршрутизаторы и конверторы интерфейсов. Пассивные устройства представляют собой различные монтажные шкафы, кабели, коммутационные панели, кабельные каналы, розетки информационного типа. Периферийное оборудование и компьютеры включает рабочие станции, копиры, серверы, сканеры и принтеры. Самое основное место в СИ занимает локальная вычислительная сеть (ЛВС). С её помощью осуществляется объединение вычислительных и локальных ресурсов с возможностью организации раздельного доступа к ним. Благодаря локальной сети осуществляется связь всех компьютерных установок. Она может быть как проводной или беспроводной, так и комбинированной. Такая сеть может располагаться в одном помещении на различных этажах, в разных помещениях, а также на большом расстоянии друг от друга. Для связи всех её пользователей используются специальные устройства – коммутаторы (свитчи) и маршрутизаторы. Все возможности локальной сети могут использоваться одновременно, независимо от

того, где находятся рабочие места. С её помощью открывается моментальный доступ к нужной информации, возможность обмениваться данными и мультимедийными носителями, а также подсоединяться к существующей на предприятии сети интернет. Именно поэтому внедрение сетевой инфраструктуры очень важно для любой компании. Надёжность и производительность локальной сети, независимо от того, будет она кабельной или беспроводной, зависит ещё и от того, какие в ней применяются технологии, активное оборудование и сетевое программное обеспечение. Если вы хотите правильно и эффективно спроектировать такую сеть, то обязательно производить анализ информационных потоков вашей организации, при этом учитывая перспективу развития самой инфраструктуры. Для каждой организации правильное построение СИ является залогом безопасного и эффективного использования информации. После того как была сформирована база такой системы, происходит внедрение сетевых сервисов. С их помощью обеспечивается надёжность и доступность всех ресурсов компании. Эффективность ведения бизнеса определяется доступностью пользовательских сервисов, систем видео и голосовой связи, а также систем унифицированных коммуникаций. Немаловажным значением обладает и защита сетевой инфраструктуры. Ведь при возникновении чрезвычайной ситуации велика вероятность потери не только самого оборудования, но и информации. Многие такие аварии и катастрофы угрожают целостности самого бизнеса. Они являются предсказуемыми с определённым процентом вероятности. Такие события могут быть как природные (наводнение, землетрясение и т.п.), так и механические (разрыв водопроводных коммуникаций, выход из строя жёсткого диска и другие). Отсутствие специальной программы, с помощью которой осуществляется восстановление работоспособности сетевой инфраструктуры, ставит под большую угрозу дальнейшую деятельность организации. Особенно это касается предпринимателей малого и среднего бизнеса. Во многих компаниях такое планирование чрезвычайных мероприятий фокусируется уже на стадии ИТ. Такая программа сохранения непрерывности любых бизнес-операций, а также послеаварийного восстановления способна стать, пожалуй, самым ценным и эффективным вкладом отдела ИТ в успешное процветание самой компании. Существует так называемое горячее запасное оборудование, которое готово моментально включиться в работу при аварийной ситуации. К примеру, вы можете дублировать самые важные данные занесением их на специально предназначенную базу. А вот холодное – представляет собой устройства, которые можно оперативно подготовить к выполнению тех либо иных задач. Это может быть набор не подключённых серверов, на которых установлено всё необходимое для работы программное обеспечение сетевой инфраструктуры. Таким образом, вы сможете без проблем и очень быстро переключиться с неисправного оборудования и продолжить работу. К примеру, если в вашей фирме имеется совсем небольшой отдел IT, а именно: несколько серверов, немного больше ПК, интернет, сетевое оборудование и т.п. Все эти устройства довольно часто обслуживает один администратор. Его рабочий день должен проходить следующим образом. Вначале необходимо проверить работу серверов, убедиться в ис-

правной работе интернета, почты и прочих приложений, произвести пробное подключение к каждому из серверов, проверить свободное пространство, ОЗУ и другие мощности, убедиться в работе сетевой оргтехники и проверить задание резервного копирования. Многие могут спросить: затем такая постоянная ежедневная проверка? Тут всё просто. Если вы вовремя не обнаружите ошибку либо проблему в работе оборудования, то это может привести к необратимому процессу, который способен стать настоящей катастрофой для вашей фирмы. К примеру, если внезапно закончится свободное место для резервного копирования данных, то и восстанавливать вам нечего будет потом. Но не каждый администратор добросовестно относится к своей работе и может просто забыть произвести плановую проверку. В таком случае руководителям компании помогут специальные системы мониторинга, которые будут выполнять всю работу автоматически. Вам достаточно только указать, что и когда нужно проверять. Что может мониторить такая система. Это рабочие станции, сервера на базе различных операционных систем, доступность сайтов, серверные и клиентские приложения, а также службы, принтеры, сканеры и прочее сетевое оборудование, отправка уведомления и отчёты на e-mail адрес либо в sms, построение графиков и многое другое. Очень важным вопросом также является и конфигурирование и поддержка сетевой инфраструктуры. Ведь с каждым годом мощность серверов и скоростей увеличивается. Это влечёт за собой необходимость своевременного и профессионального обслуживания, а также потребность в оперативном решении текущих и перспективных задач. Чем выше требования предъявляются к СИ, тем больше нужно использовать различного эффективного и функционального оборудования. Кроме этого требуются более глубокие познания и опыт построения сетей на таких устройствах. Это следует помнить, знать и своевременно решать. Также на предприятии периодически следует проводить и аудит сетевой инфраструктуры. Данный комплекс мероприятий направлен на определение состояния, в котором в данный момент находится СИ организации, проводится поиск самых уязвимых мест. По результатам такого аудита составляется специальный отчёт, в котором будет отображено текущее состояние сетевой инфраструктуры и предложена организация эксплуатации сетевой инфраструктуры. Данная проверка нужна в следующих случаях. Перед модернизацией и после нее, для определения истинной причины возникшей проблемы, для оценки качества и эффективности сервиса, во время передачи функций администрирования. Обслуживание и создание эффективной ИТ инфраструктуры организации – это необходимое условие успешного ведения бизнеса. Сетевая инфраструктура становится с каждым днём сложнее. В неё входит огромное количество оборудования и программного обеспечения, обслуживать которое должен довольно большой штат сотрудников. Именно поэтому многие фирмы начинают задумываться: производить им поддержку самостоятельно либо же воспользоваться внешним обслуживанием аутсорсингом. Аутсорсинг сетевой инфраструктуры – это превосходный способ сохранения и страхования ваших инвестиций в IT. Данная процедура позволяет снизить расходы, которые связаны с развитием и функционированием корпоративной сети,

а также существенно повысить качество IT услуги. Преимущества перехода на аутсорсинг заключаются в следующем. Наблюдается сокращение издержек на сопровождение СИ. В данном случае поставщик услуг IT аутсорсинга берёт на себя второстепенные обязательства. Сам же управляющий персонал может сконцентрировать своё внимание на решении других задач, которые более важны. Таким образом, компания добивается конкурентного преимущества. Также имеет место снижение рисков в проектах. Расширение и модернизация СИ, внедрение бизнес-приложений и IT сервисов – всё это выполняют узкоспециализированные профессионалы. Таким образом удаётся минимизировать вероятность ошибок, которые довольно часто могут возникать у специалистов более широкого профиля. Увеличение качества самого обслуживания. Передача всех обязанностей, связанных с технической поддержкой и сопровождением, одному поставщику даёт возможность стандартизировать обслуживание и гарантировать высокое качество работы.

Список литературы

1.Олифер В.Г., Олифер Н.А. О-54 Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е издание – Спб., Питер, 2010. -944 с.: ил. ISBN 978-5-49807-389-7.

2.Аутсорсинг: создание высокоэффективных и конкурентоспособных организаций: Учеб. пособие / Гос. Университет Управления; Под ред. Б.А. Аникина. - М.: ИНФРА-М, 2003. - 187 с.: 60x88 1/16. - (Высшее образование). ISBN 5-16-001602-3.