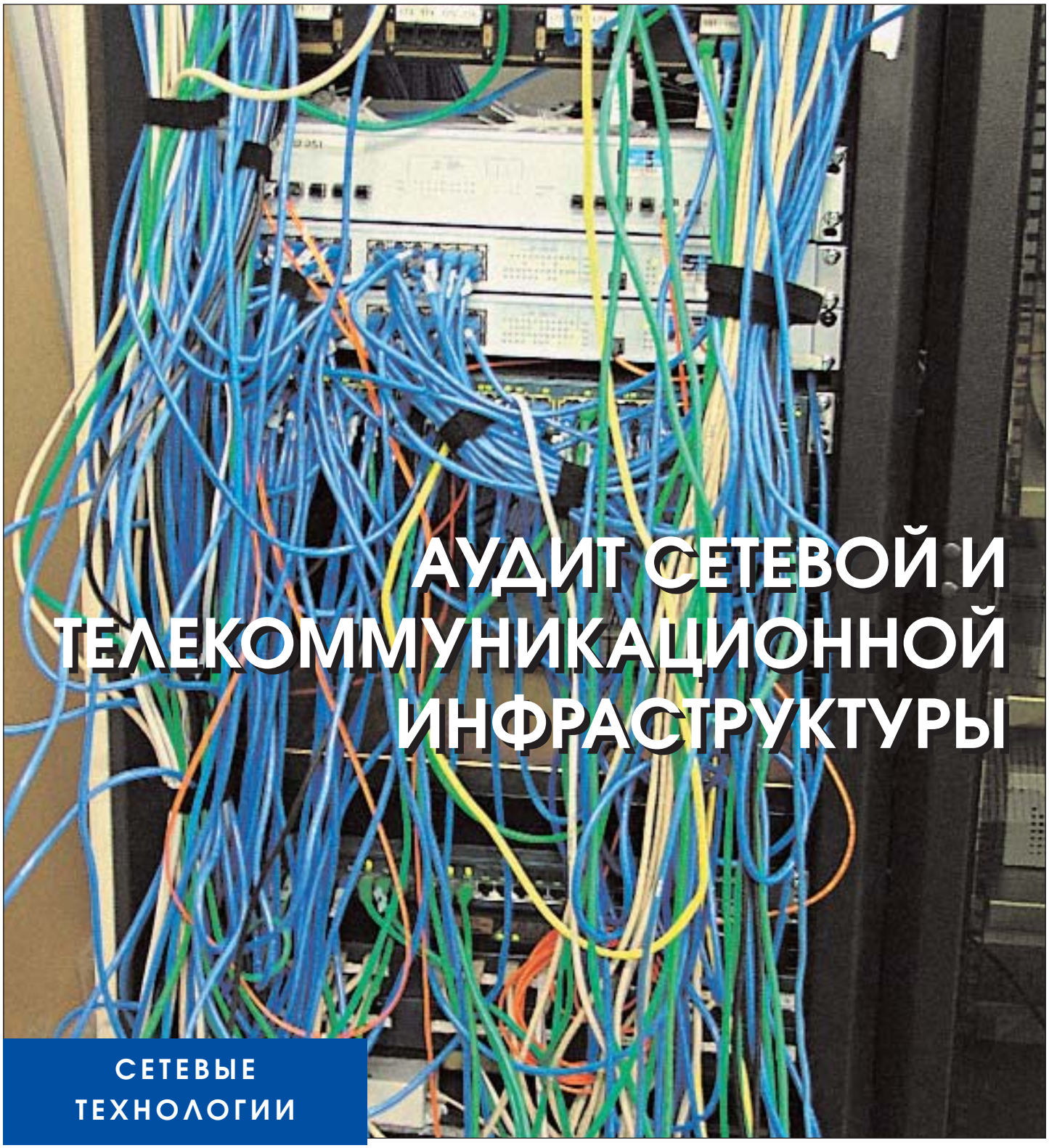
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 4 (143)/2005



АУДИТ СЕТЕВОЙ И ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

СЕТЕВЫЕ ТЕХНОЛОГИИ

АУДИТ СЕТЕВОЙ И ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Максим Клочков,
инженер-консультант отдела сетевых проектов

СОДЕРЖАНИЕ

Общие сведения об аудите

Место информационных технологий в современном бизнесе

В последнее время структура компаний и их бизнес-процессы становятся все более сложными, соответственно, усложняются и технологии управления ими. Передачу и обработку информации уже невозможно представить без развитой информационной инфраструктуры[1].

Современная экономика бурно развивается. Чтобы сохранить эффективность бизнеса, менеджменту компаний приходится постоянно адаптировать бизнес-процессы к меняющимся требованиям рынка. Понятно, что в таких условиях информационная инфраструктура, задействованная в автоматизации этих бизнес-процессов, должна быть достаточно гибкой.

Когда уровень информационных технологий перестает соответствовать потребностям бизнеса, возникают такие проблемы как несвоевременное получение, неадекватность или неудобная организация информации, необходимой для выработки управленческих решений.

Особая ситуация складывается в тех компаниях, основным бизнесом которых является передача информации — операторах связи, информационных агентствах. Здесь развитая информационная инфраструктура является важнейшим конкурентным преимуществом, а ее неадекватное функционирование может полностью уничтожить бизнес компании.

Большинство российских компаний молоды (10—15 лет), причем их создание и рост совпали

[1] Информационная инфраструктура (ИИ) — комплекс структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия. ИИ включает совокупность информационных центров, банков данных и знаний, систем связи; обеспечивает доступ потребителей к информационным ресурсам.

с бумом на рынке информационных технологий. Именно в период возникновения и становления современного российского бизнеса компьютеры начали устанавливать на большинстве рабочих мест, а затем объединять в сети. Появились и мощные приложения, рассчитанные на работу в сетевой среде.

Существенным преимуществом в положении служб информационных технологий российского бизнеса оказалось то обстоятельство, что информационная инфраструктура, как правило, создавалась с нуля, без необходимости сохранения совместимости с приложениями, не рассчитанными на работу в современной распределенной сетевой среде. И все же, при быстром развитии технологий информационная инфраструктура большинства крупных компаний находится в состоянии непрерывной модернизации. Тем не менее, по ряду причин (недостаток финансирования, недооценка важности, недостаточная квалификация персонала) ее отставание от потребностей бизнеса нарастает.

Для оценки состояния информационной инфраструктуры компании и выработки методов достижения соответствия этого состояния потребностям бизнеса служит аудит информационной инфраструктуры.

Аудит как метод сохранения и повышения эффективности информационной инфраструктуры

Модернизация информационной инфраструктуры обычно начинается с аудита, затем следуют выработка целей и плана ее развития, реализация которого восстанавливает необходимый уровень информационных технологий и делает дальнейшее развитие информационной инфраструктуры целенаправленным и управляемым процессом.

Периодический аудит информационной инфраструктуры дает представление о соответствии ее состояния и развития конкретным частным задачам и целям всего бизнеса. Кроме того, аудит помогает оценить состояние отдельных элементов инфраструктуры и связанные с ними риски, а значит, позволяет определить, какие элементы информационной инфраструктуры должны совершенствоваться в первую очередь. К настоящему времени разработаны различные методики аудита информационной инфраструктуры. Большинство из них ориентированы на оценку соответствия потребностей бизнеса предприятия состоянию его информационной инфраструктуры (см., например, методику COBIT на http://www.isaca.org).

Основным недостатком существующих стандартов является неполная детальность описания работ по аудиту отдельных элементов информационной инфраструктуры. Подобные пробелы восполняются производителями оборудования, консалтинговыми компаниями и системными интеграторами.

Методики аудита

Рассмотрим кратко особенности методик аудита информационной инфраструктуры, предлагаемых различными компаниями.

Производители сетевого и телекоммуникационного оборудования разрабатывают методики, позволяющие оценить готовность сети заказчика к внедрению тех или иных продуктов или комплексных решений, предлагаемых этими производителями. Например, компаниями Cisco Systems и Avaya Communications созданы методики, направленные на оценку готовности сети к внедрению систем IP-телефонии (см. врезки).

Крупные консалтинговые компании (например, входящие в так называемую «большую четверку») предлагают ИТ-аудит, позволяющий оценить риски, связанные с информационной инфраструктурой: недостаточной надежностью, безопасностью или функциональностью информационной инфраструктуры в целом либо ее отдельных элементов.

Системные интеграторы, каковым является и компания «Инфосистемы Джет», предлагают аудит, направленный на оценку качества сети, выявление проблем ее функционирования и выработку рекомендаций, обеспечивающих устранение этих проблем.

Компания «Инфосистемы Джет» традиционно предлагает сетевые решения, применение которых позволяет добиться конечной цели создания сетевой инфраструктуры — эффективного выполнения задач бизнеса средствами сети. Сервисный центр компании обеспечивает сопровождение внедренных сетевых решений на всех этапах их жизненного цикла.

В компании разработана собственная методика аудита сетевой и телекоммуникационной инфраструктуры (ТИ). Аудит выполняется как в виде отдельной услуги, так и в составе работ по сопровождению сети заказчика. Отдельная методика разработана для аудита безопасности информационной инфраструктуры.

Компания «Инфосистемы Джет», специализируясь на внедрении комплексных решений в

области информационных технологий, по желанию заказчика берет на себя выполнение рекомендаций, вырабатываемых при аудите сетевой и телекоммуникационной инфраструктуры.

Что получает заказчик в результате аудита?

Кратко сформулировать цели аудита телекоммуникационной инфраструктуры можно следующим образом.

- Выявление проблем функционирования ТИ и составление рекомендаций по их устранению.
  Предоставление заказчику информации о выявленных проблемах с ТИ и рекомендаций по их устранению.
- Оценка качества ТИ.
  Заказчику предоставляются данные о соответствии ТИ его деловым потребностям, решаемым задачам, стандартам (межгосударственным, национальным, международным и внутрикорпоративным), рекомендациям производителей оборудования и общим принципам создания аналогичных систем. Может быть оценена интегральная стоимость ТИ и совокупная стоимость владения.
- Инвентаризация и документирование ТИ.
  Заказчик получает комплект эксплуатационной документации, облегчающей решение задач текущей эксплуатации (добавление и удаление пользователей, внедрение новых приложений и т. п.), а также поиск и устранение проблем.

О необходимости аудита ТИ заставляют задуматься конкретные проблемы, препятствующие повседневной деятельности персонала. Например, крайне медленная загрузка приложений, нужных для работы, или файлов с данными. Частые сбои в работе ТИ создают угрозу своевременному выполнению каких-либо важных текущих задач (это может быть сдача баланса бухгалтерией или проведение важных платежей).

Многие сети, развернутые в настоящее время у текущих и потенциальных заказчиков компании «Инфосистемы Джет», развивались достаточно стихийно. Оборудование закупалось для удовлетворения сиюминутных потребностей, без какой-либо долговременной стратегии. Персонал, обслуживающий ТИ, менялся, при этом документирование конфигурации ТИ не проводилось или не поддерживалась актуальность документации. В результате потенциальный заказчик аудита оказался владельцем большой, сложной, дорогой, но недостаточно надежной и производительной сети, к тому же и плохо управляемой. Желание навести здесь порядок становится вполне понятным. Например, при вступлении в должность нового руководителя службы информационных технологий аудит часто становится для него единственной возможностью получить адекватное представление о своей области ответственности.

Если компания пользуется услугами ИТ-аутсорсинга (например, заключает контракт на сервисное обслуживание сети в сторонней организации), то аудит, проведенный перед заключением контракта, даст обслуживающей организации четкое представление об объеме работ и позволит оценить риски, связанные с обслуживанием сети. Аудит поможет оптимально сформировать условия договора, выявить критически важные элементы ТИ, обслуживание которых должно быть приоритетным, определить необходимые режимы обслуживания (24x7, 8x5 и т. п.). При отработке сервисных запросов результаты аудита помогают ускорить выявление источника проблемы и, в конечном итоге, снизить время неработоспособности ТИ или элементов ТИ.

Периодическое проведение аудитов в ходе исполнения длительного контракта по обслуживанию сложной развивающейся сети позволит сохранять актуальность представлений о ней как у обслуживающей организации, так и у заказчика, что также способствует повышению качества обслуживания. Если для обслуживания сети предусмотрена сложная структура с разделением полномочий, то аудит может упростить управление такой структурой, сделав ее более прозрачной, выявив уровни ответственности и границы разделения полномочий. Перед глубокой модернизацией большой сложной ТИ целесообразно провести ее аудит. Это поможет оптимально спланировать модернизацию, сохранить инвестиции, обеспечить гладкое внедрение новых технологий. Результаты аудита в этом случае станут частью исходных данных для концепции, эскизного проекта, технического проекта модернизации ТИ.

Аудит может быть полезен и в ситуации, когда возникает необходимость внедрить новые сетевые приложения, пользуясь существующей ТИ (без ее изменений или с минимальными изменениями). Примерами таких приложений могут служить системы управления предприятием (SAP/R3, Oracle Applications), системы передачи мультимедийной информации (IP-телефония, видеоконференцсвязь) и т. п. В этом случае аудит обеспечит уверенность в достаточности ресурсов сети для работы новых приложений.

Иногда разработчики или подрядчики по внедрению каких-либо информационных систем требуют предварительных оценок параметров ТИ «в цифрах». Например, для внедрения IP-телефонии важно знать реально достижимую пропускную способность каналов связи и максимальную величину задержки прохождения IP-пакетов. Ответы на подобные вопросы тоже может дать аудит ТИ.

Кто является заказчиком аудита?

Как правило, заказчиком аудита ТИ является достаточно крупная компания с развитой телекоммуникационной инфраструктурой. В такой организации работает большое количество сотрудников, все используют ПК с сетевыми приложениями (почта, Интернет, IP-телефония, средства групповой работы, такие как Microsoft Exchange или Lotus Domino/Notes, ERP-системы, такие как SAP/R3). Наличие отделений или филиалов (возможно, расположенных в разных городах) усложняет структуру сети и создает дополнительные проблемы при эксплуатации. Их решению также может способствовать проведение аудита.

Совершенно необходимым становится аудит ТИ для компаний, чей бизнес напрямую зависит от бесперебойного функционирования ТИ. Примерами организаций, обладающих перечисленными признаками, можно назвать крупные государственные учреждения, операторы связи, крупные банки.

Особым заказчиком работ по аудиту являются фирмы-разработчики прикладного ПО и подрядчики, внедряющие прикладное ПО. Многие разработчики прикладных информационных систем, использующих сеть, никак не учитывают возможности современных ТИ и не вырабатывают формализованные критерии оценки ТИ на применимость совместно с разрабатываемой системой. Это приводит к проблемам при внедрении таких ИС или при их расширении.

Чтобы избежать проблем, разработчику на этапе разработки ПО целесообразно заказать аудит приложения для выявления его потребностей в сетевых ресурсах. Подрядчику по внедрению прикладного ПО весьма полезно заказать аудит ТИ заказчика уже при сборе исходных данных.

Аудит необходим и в ситуации конфликта между заказчиком и подрядчиком по внедрению прикладной системы, поскольку помогает выяснить, является ли ТИ источником проблем при внедрении приложения. В результате проведения аудита разработчик ИС получит данные, на основании которых сможет сформировать требования к ТИ.

С одной стороны, это снизит риски проблем при внедрении телекоммуникационной инфраструктуры, с другой — стимулирует заказчика к приведению ТИ в состояние, при котором указанные требования будут удовлетворяться. Выполнить данную работу можно как силами подрядчика, проводившего аудит, так и силами самого заказчика. Кроме того, ее можно заказать любой другой организации, обладающей достаточными возможностями и опытом.

Почему аудит лучше заказывать внешней организации?

Итак, потенциальным заказчиком аудита является относительно крупная компания с развитой телекоммуникационной инфраструктурой, функционирование которой часто критически важно для бизнеса компании в целом. Обычно в таких организациях есть собственная развитая служба поддержки ИТ, в которой работают высококвалифицированные специалисты.

Возникает вопрос, зачем заказчику привлекать к аудиту внешнего подрядчика? Почему бы не выполнить эту работу силами собственных квалифицированных специалистов?

Основные преимущества обращения к внешнему подрядчику следующие.

- У стороннего подрядчика нет прямой заинтересованности в результатах аудита, поэтому объективность его выводов выше.
- Специалисты подрядчика не обладают никакими предварительными знаниями о сети заказчика и вынуждены получать информацию о ней, интервьюируя персонал, анализируя предоставленные заказчиком документы, изучая конфигурацию устройств. Таким образом, они получают актуальное представление о состоянии сети.
- Специалисты заказчика, эксплуатирующие сеть, могут иметь неадекватное представление о ней, не догадываясь об этом, и, соответственно, не проверить какую-то информацию, считая ее очевидной.
- Подрядчик непрерывно взаимодействует с различными заказчиками, поэтому у него больше опыта и наработана более высокая квалификация.
- У подрядчика имеется проработанная технология, а также большой опыт выполнения аналогичных проектов, поэтому аудит будет проведен быстрее, качественнее, а затраты могут оказаться даже ниже.

Методика проведения аудита телекоммуникационной инфраструктуры

Общие сведения

Построение и модернизация информационной инфраструктуры представляет собой, в основном, проектную деятельность.

Действительно, создание кабельной системы, ЛВС, серверного комплекса, системы хранения данных, системы резервного копирования, а также разработка и внедрение прикладного ПО почти всегда направлены на достижение уникального результата. Такая деятельность организуется по принципам проектного управления.

Грамотно организованная эксплуатация информационной инфраструктуры, напротив, осуществляется обычно по принципу конвейера. Профилактика, сервисное обслуживание, добавление, удаление и перемещение рабочих мест, а также другие работы, связанные с эксплуатацией, как правило, регламентируются инструкциями. Даже в тех случаях, когда регламенты не зафиксированы в виде документов, фактически указанные операции всегда сводятся к небольшому набору совершенно определенных действий, регламентирование которых не составляет серьезной проблемы.

Аудит, как одна из работ, связанных с эксплуатацией ТИ, также хорошо поддается регламентированию и стандартизации. Компания «Инфосистемы Джет» выполняет технический аудит (в том числе и аудит ТИ) для широкого круга заказчиков по единой методике, но с обязательной адаптацией к нуждам конкретного клиента.

В процессе аудита вырабатываются рекомендации по модернизации и развитию ТИ. Результаты представляются в виде аналитического отчета. Рекомендации могут предполагать немедленную реализацию (перенастройка оборудо-

Рис. 1. Этапы аудита

вания, приобретение нового оборудования) или быть долговременными (разработка концепции развития ТИ или концепции сервисного обслуживания). В последнем случае отчет об аудите является частью исходных данных концепции развития ТИ или проекта ее модернизации.

Порядок проведения аудита

Вне зависимости от объекта обследования проведение аудита включает три основных этапа:

1) постановка задачи и уточнение границ работ;
2) сбор данных;
3) анализ данных и оформление результатов.

Постановка задачи и уточнение границ работ

Выше упоминалось, что компания «Инфосистемы Джет» выполняет обязательную адаптацию стандартной методики аудита к нуждам конкретного заказчика. Такая адаптация проводится именно на данном этапе.

В ходе этого этапа выявляются элементы ТИ, подлежащие обследованию, такие как активное сетевое оборудование, кабельные системы, системы управления сетью и другие. Фиксируется их количество, расположение, определяется круг лиц, непосредственно эксплуатирующих ТИ, отвечающих за ее эксплуатацию и использующих ее в работе. На этапе сбора данных с этими сотрудниками проводятся интервью. Постановка задачи завершается разработкой, согласованием и утверждением технического задания (ТЗ).

ТЗ на аудит разрабатывается в соответствии с ГОСТ 34.602-89 «Техническое задание на создание информационной системы». Несмотря на то, что указанный стандарт описывает ТЗ на создание информационных систем, он подходит и для разработки ТЗ на аудит. Адаптация стандарта — минимальная.

В ТЗ на аудит обязательно фиксируются требования к обследуемой системе, состав и содержание работ по аудиту и требования к разрабатываемым документам. Если в ходе аудита выполняется документирование ТИ, то в него включают состав и содержание разрабатываемой документации. Если аудит направлен на решение определенных проблем, то в ТЗ фиксируются работы по выявлению их причин и порядок представления результатов этих работ. Кроме того, в ТЗ вносят сроки проведения работ, а при необходимости — план-график.

ТЗ согласуется с заказчиком, утверждается и с этого момента определяет все дальнейшие работы.

Часто для проведения аудита необходим доступ к информации, которую заказчик считает конфиденциальной. В этом случае параллельно с ТЗ разрабатывается соглашение о конфиденциальности и организуется взаимодействие со службой безопасности заказчика.

Сбор данных

На этом этапе обычно проводят интервьюирование персонала заказчика, осмотр и инвентаризацию оборудования, сбор конфигурационной и операционной информации, измерения различных параметров сети.

Сбор данных может включать следующие типовые работы:

- интервьюирование персонала заказчика;
- анализ представленных документов;
- приборные измерения;
- сбор конфигурационной и операционной информации;
- осмотр оборудования.

Детальный перечень выполняемых работ обычно определяется ТЗ на аудит.

Интервьюирование персонала направлено на выявление представлений заказчика о назначении ТИ, ее текущем состоянии и требованиях к ней. К интервьюированию обязательно привлекаются сотрудники:

- непосредственно эксплуатирующие сетевое оборудование, например, системные администраторы и инженеры поддержки;
- использующие сеть для решения своих задач, например, пользователи персональных компьютеров и администраторы прикладных систем;
- отвечающие за работоспособность сети, надежность и качество ее работы, например, начальник службы эксплуатации или директор по информационным технологиям.

Всем перечисленным категориям персонала задаются вопросы о проблемах, которые им приходится решать. Видение одной и той же проблемы может существенно различаться с точки зрения, например, пользователя и системного администратора. На этапе сбора информации сведения, сообщенные сотрудниками, тщательно фиксируются. Позже, при анализе данных, будет выработана целостная точка зрения на обозначенную проблему и даны рекомендации по ее устранению или снижению ее проявления.

Персонал, отвечающий за работу сети, в ходе интервью отвечает на вопросы о деловых потребностях компании, решаемых посредством

ТИ, о требованиях к ТИ, о соответствии ее характеристик этим требованиям.

Пользователи рассказывают о качестве функционирования ТИ и о последствиях плохой работы ТИ для их повседневной деятельности.

Компанией «Инфосистемы Джет» разработаны специальные опросные листы для проведения технического аудита. Если аудит необходимо провести в короткие сроки и за небольшие деньги, заказчик может заполнить опросные листы самостоятельно. Когда же речь идет о глубоком всестороннем аудите, интервьюирование обязательно выполняется инженером-аналитиком подрядчика. Опытный специалист в ходе беседы задаст дополнительные и уточняющие вопросы, вскроет противоречия в высказываниях различных представителей заказчика, поможет им выработать единую точку зрения.

План интервьюирования включается в ТЗ. В качестве приложения к ТЗ могут выступать опросные листы, адаптированные под конкретного заказчика. Обычно они содержат вопросы следующей тематики:

- требования, предъявляемые к сети;
- порядок обслуживания сети;
- активное сетевое оборудование;
- программное обеспечение;
- кабельные системы;
- вспомогательные и смежные системы;
- условия установки и эксплуатации оборудования.

Вся документация на ТИ, предоставленная заказчиком, собирается для дальнейшего анализа. Особое внимание обращается на журналы внесения изменений в систему и журналы обслуживания заявок пользователей.

Осмотр оборудования обычно включает оценку следующих параметров:

- температура, влажность и запыленность в помещении, где установлено оборудование;
- наличие вентиляции, кондиционирования, охранной и пожарной сигнализации;
- способ установки оборудования;
- состояние кабельных линий;
- качество электропитания (наличие ИБТ, заземления и т. д.).

По желанию заказчика к документации на ТИ, подготавливаемой в ходе аудита, могут быть приложены фотографии установленного сетевого оборудования.

На рис. 2 показано правильно смонтированное и подключенное оборудование. Следует обратить внимание, что в данном случае:

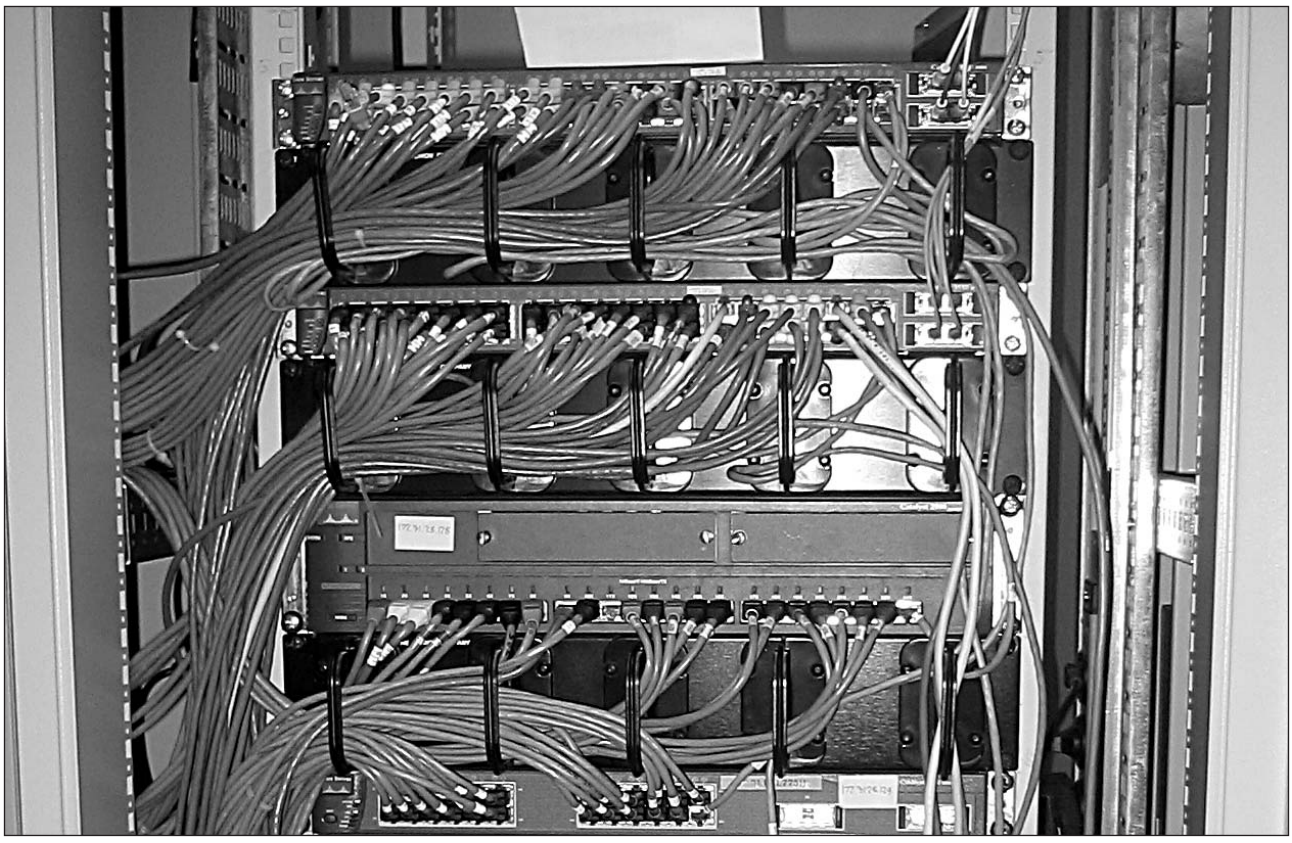


Рис. 2. Правильно смонтированное и подключенное оборудование

- оборудование смонтировано в монтажный шкаф;
- запыленность отсутствует;
- кабели промаркированы и уложены в органайзеры.

На рис. 3 приведена фотография оборудования, эксплуатирующегося в тяжелых условиях. Здесь можно видеть, что:

- часть оборудования не рассчитана на стоечный монтаж;
- присутствует запыление;
- не все кабели промаркированы и аккуратно уложены.

Сбор конфигурационной информации выполняется, прежде всего, в целях восстановления полной актуальной схемы ТИ. Одновременно с этим проверяется и доступность устройства посредством различных средств управления (с консоли, по протоколу telnet, по http, через систему сетевого управления и другими способами).

Кроме конфигурационных файлов сохраняются файлы журналов сетевого оборудования и системы сетевого управления, результаты исполнения команд, показывающих параметры работы устройств, и другие данные. Перечень сохраняемых данных обычно также включается в техническое задание и зависит, прежде всего, от применяемого оборудования и систем управления.

Данные, собираемые на больших сложных сетях, могут занимать очень большой объем. Их анализ «вручную» может быть затруднен, поэтому в таких случаях применяются средства автоматизированной обработки, например, Cisco Output Interpreter (см. ниже). Объем данных, подлежащих анализу, можно искусственно ограничить. Например, если аудит ТИ направлен лишь на поиск критических ошибок, то ограничивают важность (severity) рассматриваемых сообщений журналов. Когда ищут ошибки в какой-то подсистеме, то ограничиваются рассмотрением ошибок только из определенного источника (facility).

Приборные измерения выполняются в тех случаях, когда необходимо определить параметры работы сети, а внутренних средств диагностики сетевого оборудования недостаточно. Объектом данных исследований всегда являются каналы связи. Измерениям поддаются такие параметры как загрузка, количество ошибок (с распределением по типам), распределение пакетов по определенным признакам (размеру, протоколам, портам). Средства измерений и анализа трафика позволяют собрать сетевой трафик, полностью восстановить отдельные сессии, построить диа-

Рис. 3. Оборудование, эксплуатирующееся в тяжелых условиях

граммы распределения фреймов или пакетов по различным признакам. Полученные сведения дают возможность ответить, например, на такие вопросы:

- Насколько сильно загружена сеть?
- Какие приложения загружают сеть сильнее всего?
- Какие пользователи загружают сеть сильнее всего?
- Много ли передается по сети ошибочной или иной бесполезной информации?

По окончании этапа сбора данных компания, проводящая аудит, владеет набором документов, детально описывающих ТИ. При необходимости эти документы могут быть переданы заказчику, но практическая их ценность невелика по следующим причинам:

- Методика, по которой проводит аудит компания «Инфосистемы Джет», предусматривает разделение сбора и анализа данных. Как правило, эту работу выполняют разные люди. Собранные данные, таким образом, не проверяются на полноту и корректность.
- Основной сценарий применения собранных данных — это формирование на их основе выводов и рекомендаций. Для других целей, например, в качестве эксплуатационной документации на ТИ, они не подходят.

Отчетные документы о проделанной работе и документы, направленные на реализацию целей аудита, разрабатываются на следующем этапе, при анализе данных.

В некоторых случаях при проведении аудита ТИ на этапе сбора данных выполняется профилирование приложений, то есть определение требований приложений к ТИ и описание их в виде количественных параметров.

Профилирование обязательно выполняется в тех случаях, когда одной из целей аудита является оценка готовности сети к внедрению специфических приложений, требования к ТИ которых не определены или есть сомнения в адекватности этих требований. Профиль приложения является частью исходных данных, собираемых при аудите ТИ.

Профилирование предусматривает следующие шаги:

- Составление перечня типовых операций, выполняемых пользователями приложения.
- Организация отдельного стенда (или опытного участка в существующей сети), на котором эти операции могут быть выполнены. При выполнении операций по сети должен пересылаться реальный объем данных. Стенд снабжается средствами записи и последующего анализа сетевого трафика, а также средствами имитации загрузки.
- Выполнение на стенде типовых операций. Каждая типовая операция выполняется, записывается сессия, анализируется объем переданных данных. При необходимости имитируется нагруженная сеть, оценивается комфортность выполнения операций. Как правило, оценивается влияние нагрузки на наиболее частые операции и на наиболее длительные, сильно нагружающие сеть.
- Формирование требований к ТИ. На основе собранных данных формируются требования приложений ТИ, выраженные в виде количественных параметров.

Этап сбора данных завершается формированием комплекта документов, описывающих сеть заказчика.

Анализ данных и оформление результатов аудита

Эти работы также определяются ТЗ. При их выполнении проводится проверка собранных данных на полноту и корректность, анализ полученной информации, формирование выводов и рекомендаций, оформление и презентация результатов. В ходе анализа может быть принято решение о сборе дополнительных данных.

Этап анализа данных и оформления результатов обычно включает следующие типовые работы:

- проверка собранных данных;
- анализ структуры ТИ;
- анализ конфигурационных файлов;
- анализ операционного состояния ТИ;
- подготовка аналитического отчета;
- подготовка эксплуатационной документации;
- презентация результатов.

Собранные данные проверяются на полноту (отражают ли они ситуацию с ТИ полностью, все ли элементы охвачены, все ли связи учтены), корректность (имеются ли противоречивые или заведомо неверные данные), достаточность (приводит ли их анализ к достижению целей аудита). При необходимости собирается заново часть данных или дополнительная информация.

Структура ТИ и конфигурационные файлы анализируются совместно. ТИ проверяется на соответствие:

- решаемым задачам, т. е. определяется, в какой степени она обеспечивает работу прило-

жений, автоматизирующих бизнес-процессы предприятия;
- стандартам; например, кабельные сети стандартизованы на международном уровне, сети операторов связи должны удовлетворять нормам Минсвязи и т. п.;
- рекомендациям производителей; например, компания Cisco Systems предлагает достаточно детально проработанные принципы построения сетей и четко позиционирует свое оборудование как магистральное, уровня распределения или уровня доступа. Соответственно, проверяется, как различное оборудование используется в сети заказчика;
- общепринятым принципам построения сетей; например, уровень ошибок должен быть не выше определенного или количество производителей используемого оборудования ТИ должно быть сведено к минимуму.

Кроме того, анализируются такие характеристики сети, как расширяемость (сколько еще пользователей/подключений выдержит ТИ без существенной модернизации), управляемость (каковы трудозатраты на типовые операции по обслуживанию сети), производительность (сколько времени занимает типовая операция пользователя), безопасность.

Проведение аудита ТИ иллюстрируется рисунком 1 (стр. 6).

При анализе структуры обязательно проверяются следующие показатели:
- наличие точек единого отказа, т. е. таких элементов сети, отказ которых приводит к невозможности предоставления сервиса всем или большинству ее пользователей;
- наличие узких мест, например, коммутаторов или каналов связи с недостаточной производительностью, которые при этом сильно загружены и влияют на производительность сети в целом;
- оптимальность прохождения потоков трафика, например, равномерность загрузки параллельных каналов, отсутствие петель, отсутствие маршрутов с неоправданно большим количеством промежуточных узлов.

При анализе конфигурации обязательно проверяются следующие параметры:
- соответствие конфигурации сетевых устройств задачам, решаемым сетью в целом;
- наличие или отсутствие ненужных сетевых протоколов и служб;
- оптимальность настроек параметров различных сервисов и протоколов.

При анализе служебных сервисов и протоколов обязательно проверяются следующие параметры:
- наличие и частота сообщений об ошибках работы каких-либо протоколов или служб, а также степень влияния этих ошибок на функционирование сети в целом;
- статистические данные о работе различных сетевых протоколов и служб, например, частота обновления информации в таблице маршрутизации или количество ошибок на интерфейсе.

Аудит безопасности позиционируется компанией «Инфосистемы Джет» как отдельный продукт. Тем не менее, рекомендация по его проведению может быть включена, например, в отчет о техническом аудите ТИ и подкреплена необходимыми аргументами.

Аналитический отчет является основным отчетным документом об аудите. Его структура, как правило, согласуется еще на этапе разработки ТЗ. Он включает описание текущего состояния ТИ, выводы о соответствии ТИ решаемым задачам, рекомендации по модернизации и развитию.

Содержание отчета в значительной степени зависит от предполагаемого применения. Например, рекомендации могут стать основой концепции модернизации ТИ. Или же аргументы, изложенные в отчете, можно использовать в качестве обоснования проекта полной перестройки ТИ.

Содержание эксплуатационной документации в значительной степени зависит от структуры ТИ заказчика, а также организационной структуры его компании. Минимальный комплект документов должен включать схему топологии сети и таблицу конфигураций устройств.

Аналитический отчет, как правило, бывает достаточно объемным. При необходимости может быть подготовлена презентация, фиксирующая основные положения этого документа. В презентацию обычно включают:
- перечень проблем, обнаруженных в ТИ;
- оценку последствий этих проблем;
- предлагаемые меры по устранению проблем с выделением первоочередных мер и оценкой длительности и стоимости их реализации.

Этап завершается передачей заказчику разработанных документов.

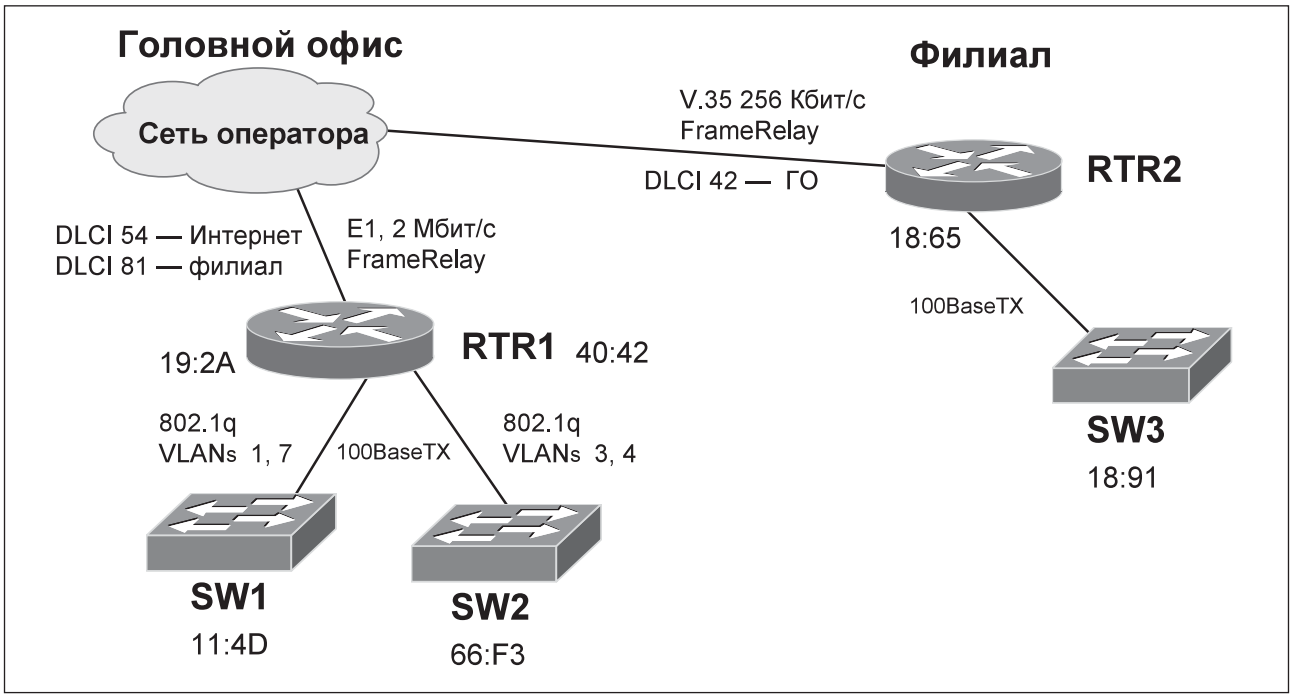


Рис. 4. Схема топологии сети (канальный уровень)

Представление результатов аудита

Минимальный комплект эксплуатационной документации на ТИ обычно включает следующие документы:

- схему топологии сети;
- таблицу конфигурации сетевых устройств;
- таблицу конфигурации устройств, подключаемых к сети.

Более полный комплект предусматривает дополнительные документы:

- отдельные схемы топологии сети на канальном и сетевом уровне;
- инструкции обслуживающему персоналу;
- таблицы коммутации;
- профили пользователей;
- профили приложений.

Схема топологии графически изображает сетевые устройства и связи между ними. В простых случаях можно обойтись одной схемой, которая содержит информацию как канального, так и сетевого уровня.

Для сложных сетей рекомендуется разработать и поддерживать две схемы топологии — на канальном и на сетевом уровне.

Возникает вопрос: когда можно ограничиться одной схемой, а в каких случаях следует разработать две? Основным критерием является существенное различие топологий канального и сетевого уровня. Например, если в сети имеются виртуальные сети, туннели, применяются технологии MPLS, целесообразно разрабатывать две схемы.

Образец схемы топологии сети на канальном уровне приведен на рис. 4. В качестве примера взята сеть небольшой компании, имеющей филиал. Связь с филиалом и выход в Интернет обеспечивается одним и тем же провайдером по технологии Frame Relay.

На схеме представлены следующие данные:

- сетевые устройства (маршрутизаторы, коммутаторы);
- их имена (RTR1, RTR2, SW1 и т. п.);
- каналы связи, их тип (E1, 100BaseTX и т. п.);
- сведения о виртуальных каналах (DLCI, VLAN);
- MAC-адреса (два последних октета, например, 11:4D).

Следует обратить внимание на то, что изображенные на схеме связи в точности повторяют структуру физических соединений в реальной сети.

В сложных сетях целесообразно не показывать все перечисленные данные на схеме, а вынести часть их (MAC-адреса, каналы связи, номера портов) в таблицы коммутации.

Пример схемы топологии той же сети на сетевом уровне приведен на рис. 5.

В нее включены:

- сетевые устройства (маршрутизаторы, коммутаторы);

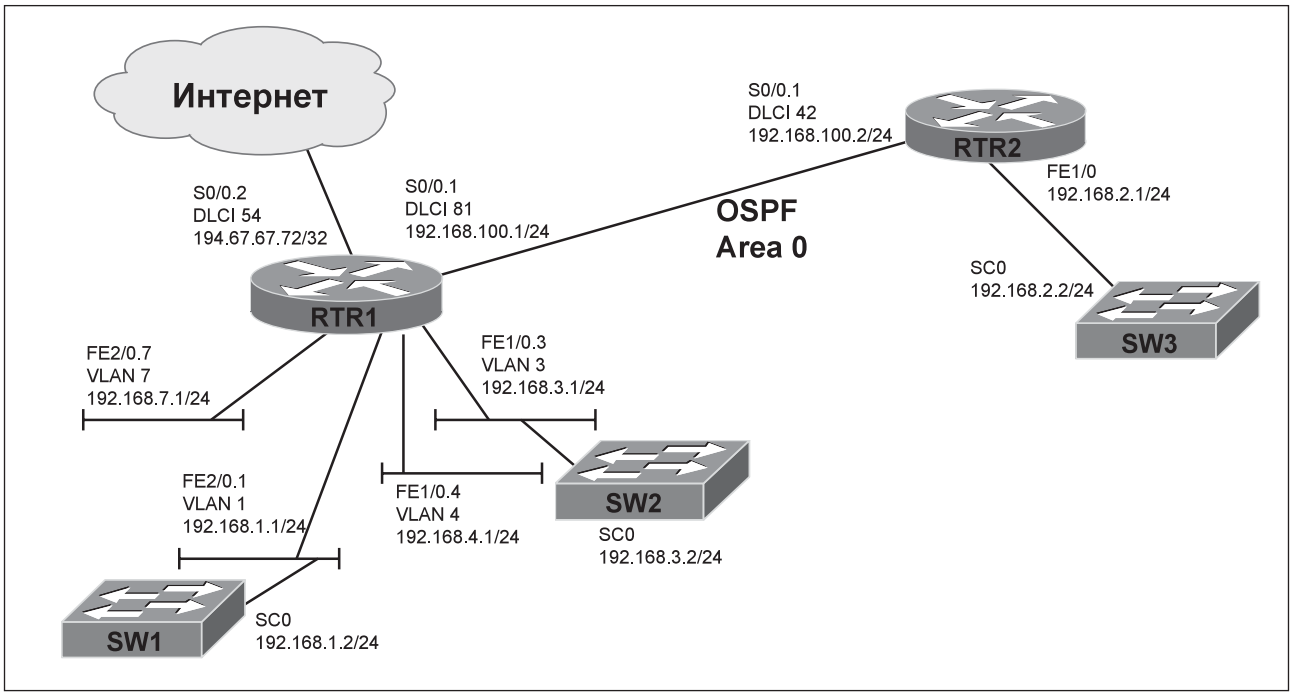


Рис. 5. Схема топологии сети (сетевой уровень)

- их имена (например, SW1, RTR1);
- сегменты, IP-адреса и маски (например, 192.168.4.1/24);
- имена интерфейсов (например, FE2/0, SC0);
- информация протоколов маршрутизации (OSPF Area 0).

Связи, изображенные на схеме, показывают путь прохождения IP-пакетов между сегментами.

Образец таблицы конфигурации сетевых устройств представлен в таблице 1 (для примера взята сеть, изображенная на схемах).

Для сложных сетей, в которых количество устройств велико, рекомендуется разработать два отдельных документа — инвентаризационный журнал и таблицу конфигураций сетевых устройств. В инвентаризационный журнал вносят данные об именах устройств, их расположении и, возможно, условиях эксплуатации, а в таблицу конфигураций — только имена и сведения, относящиеся к сетевому уровню.

Пример таблицы конфигураций устройств, подключаемых к сети, представлен в таблице 2.

Такая таблица может использоваться в простых сетях с небольшим количеством рабочих мест. В более сложных сетях рекомендуется разработать так называемые профили пользователей и профили приложений, а в таблице устройств, подключаемых к сети, ссылаться на эти профили.

Фрагмент типового описания профилей пользователей показан в таблице 3, а профилей приложений — в таблице 4.

В зависимости от потребностей конкретного заказчика описания профилей пользователей и приложений могут включать не только перечисленную в таблицах информацию, но и другие сведения. Рекомендации о включаемых в профили сведениях также могут присутствовать в аналитическом отчете об аудите.

Инструкции обслуживающему персоналу необходимы в том случае, если сетью управляет не один администратор, а подразделение, и в особенности — если подразделений несколько.

Инструкции должны обеспечивать:

- разделение ответственности между подразделениями и сотрудниками;
- механизм передачи запросов на обслуживание и эскалации проблем;
- регламентацию типовых операций;
- механизм поддержания документации в актуальном состоянии.

Таблица 1. Конфигурация сетевых устройств

Имя устройства	Размещение	Интерфейс	Layer 2	Layer 3	Маршрутизация
RTR1	Головной офис, комн. 520	S0/0.1	FR, DLCI 81	192.168.100.1/24	OSPF Area 0
		S0/0.2	FR, DLCI 54	194.67.67.72/32	Default 194.67.67.1
		FE1/0.3	802.1q, VLAN 3	192.168.3.1/24	
		FE1/0.4	802.1q, VLAN 4	192.168.4.1/32	
		FE2/0.1	802.1q, VLAN 1	192.168.1.1/24	
		FE2/0.7	802.1q, VLAN 7	192.168.7.1/24	
RTR2	Филиал, комн. 310	FE1/0		192.168.2.1/24	OSPF Area 0
		S0/0.1	FR, DLCI 42	192.168.100.2/24	
SW1	Головной офис, комн. 520	SC0		192.168.1.2/24	Default 192.168.1.1
SW2	Головной офис, комн. 520	SC0		192.168.3.2/24	Default 192.168.3.1
SW3	Филиал, комн. 310	SC0		192.168.2.2/24	Default 192.168.2.1

Таблица 2. Устройства, подключаемые к сети

Имя устройства	Платформа, ОС	IP-адрес, маска	Службы
Main-server	Sun Fire 450 , Solaris 9	192.168.3.59/24	DNS, DHCP, SMB, SQL
Internet-server	Sun Fire 450 , Solaris 9	192.168.7.105/24	SMTP, IMAP4, HTTP, HTTP-proxy
Pc-1	Pentium IV, Linux	192.168.3.5/24	cvs, gcc, почта, браузер
Pc-2	Pentium IV, Windows XP	192.168.4.104/24	MS Office, Adobe Photoshop, почта, браузер

Таблица 3. Профили пользователей

Название	Задачи	Приложения	Требования к платформе	Требования к ТИ
Юристы	Консультирование клиентов Комментирование договоров	MS Office «Гарант» «Консультант» Почта=Браузер	Проц. 1 ГГц, память 512 MB, диск 80 Гб Windows XP	Подключение 100 Мбит/с Работа с 9:00 до 21:00 с пн. по пт. К-т готовности 0.9
Секретари	Прием и регистрация телефонных звонков	MS Office Клиент БД (браузер)	Проц. 800 МГц, память 256 MB диск 40 Гб=Windows XP	Подключение 10 Мбит/с Работа с 9:00 до 21:00 с пн. по пт. К-т готовности 0.99
Программисты	Разработка ПО	MS Visual C++ Почта, Браузер	Проц. 1 ГГц, память 512 MB, диск 80 Гб Windows XP	Подключение 1 Гбит/с Работа с 9:00 до 21:00 с пн. по пт. К-т готовности 0.9
Системные администраторы	Устранение проблем со всеми системными и прикладными средствами	Почта Браузер все прочие (при отладке)	Проц. 1 ГГц, память 512 MB, диск 80 Гб, Windows XP	Подключение 100 Мбит/с Работа круглосуточно К-т готовности 0.9

Таблица 4. Профили приложений

Название	Программный продукт	Требования к ТИ	Характеристики
MS Office	MS Office XP Professional	Периодический обмен с файловым сервером. Достаточная скорость - 100 Мбит/с	Протокол - IP. Исп. порты: 137, 139 Объем трафика: до 10 Мбайт единовременно при сохранении файлов
Почта	Lotus Notes	Периодический обмен с почтовым сервером. Достаточная скорость - 100 Мбит/с	Протокол - IP. Исп. порты: TCP 110, 143, 25 Объем трафика: обычно 1-2 Мбайт при открытии или отправке сообщения
Браузер	MS Internet Explorer 6.0	Периодический обмен с различными сетевыми хостами. Достаточная скорость - 10 Мбит/с	Протокол - IP. Исп. порты: TCP 80 Объем трафика: ок. 100 Кбит/с при просмотре страниц
Клиент БД «Телефонные звонки»	MS Internet Explorer 6.0 +приложение «Телефонные звонки» (на Java)		Протокол - IP=Исп. порты: TCP 80, 8080, 7120 Постоянный обмен с сервером приложений на скорости около 64 Кбит/с

Методика аудита, предлагаемая компанией Cisco Systems

Ведущий производитель сетевого и телекоммуникационного оборудования, компания Cisco Systems, в 2003 г. включила в свой учебный курс «Cisco Internetwork Troubleshooting» и в экзамен, соответствующий этому курсу, сведения, позволяющие проводить базовый аудит компьютерной сети. Указанный экзамен сдают все кандидаты на звание Cisco Certified Network Professional (CCNP).

Методика Cisco Systems определяет состав и содержание минимально необходимой документации на компьютерную сеть, а также порядок составления такой документации.

Этот комплект включает:

- схему топологии сети (topology diagram);
- таблицу конфигурации сетевых устройств (network configuration table);
- таблицу конфигурации устройств, подключаемых к сети (end system configuration table).

На схеме топологии сети графически изображаются сетевые устройства и наносятся, как минимум, следующие данные:

- имена устройств;
- IP-адреса, маски подсетей;
- идентификаторы интерфейсов;
- протоколы маршрутизации.

Таблица конфигурации сетевых устройств должна содержать следующие необходимые данные:

- данные канального уровня (VLAN, DLCI);
- данные сетевого уровня (интерфейсы, IP-адреса, маски);
- параметры протоколов маршрутизации;
- информацию о физическом размещении устройств.

В таблице конфигурации устройств, подключаемых к сети, обязательно должны быть:

- платформа и операционная система;
- IP-адрес (при необходимости — маска подсети, адрес шлюза);
- перечень служб (приложений).

Документирование незнакомой ТИ компания Cisco рекомендует проводить в следующем порядке:

- Получить физический доступ к сетевому оборудованию. Следует составить перечень всего имеющегося оборудования, определить, каким образом оно управляется.
- Получить доступ к управлению сетевым оборудованием. Получить доступ к консоли или запустить средства управления оборудованием, ввести необходимые пароли, чтобы можно было выявить сетевые интерфейсы и их настройки.
- Идентифицировать и документировать сетевые интерфейсы. Определить данные сетевого (IP-адреса, маски) и, при необходимости, канального уровня (DLCI, VC, VLAN), составить таблицу конфигурации сети.
- Выполнить схемы топологии сети. Графически изобразить сетевые устройства, их соединения. При необходимости составить отдельные схемы топологии на различных уровнях модели ISO/OSI.
- Идентифицировать и документировать устройства, подключенные к сети. Определить параметры подключенных устройств, свести данные в таблицу конфигураций.

Более подробно о методике компании Cisco можно прочитать по ссылке http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014f924.shtml.

Кроме методики документирования сети, компания Cisco Systems предлагает автоматизированное средство оценки ее дизайна — «IP Telephony Readiness Assessment». Оно ориентировано на оценку дизайна сети с точки зрения внедрения приложений IP-телефонии, но может использоваться и для оценки «здоровья» сети в целом. Средство является веб-ориентированным интерактивным приложением. В ходе работы этого приложения пользователю задаются вопросы о состоянии сети и предлагается выбрать один из вариантов ответов. По окончании тестирования пользователю выдается пакет рекомендаций, ранжированных по срочности исполнения.

Стоит сказать еще об одном средстве автоматизированного аудита — Cisco Output Interpreter. Оно позволяет найти ошибки и «подозрительные места» в конфигурационных файлах, файлах журналов, трассировках стека устройств и других диагностических файлах, генерируемых оборудованием Cisco.

Указанные средства доступны партнерам компании и клиентам, которые приобрели пакет сервисного обслуживания оборудования Cisco SMARTnet.

Методики аудита, предлагаемые компанией Avaya

Компания Avaya имеет в своем составе подразделение Professional Services, которое оказывает, в числе других, и услуги технического аудита.

Методика компании Avaya предусматривает два этапа аудита сети:

а) определение уровня готовности инфраструктуры клиента (CIRS);

б) анализ и оптимизация сети (NANO).

Услуга CIRS представляет собой дистанционную оценку состояния сети, завершающуюся разработкой отчетных документов.

Услуга NANO предусматривает проведение на месте необходимых оценок, моделирование трафика, тестирование сети, анализ результатов и выработку рекомендаций по устранению имеющихся причин недостаточной пропускной способности сети.

Кроме аудита сетей, компания Avaya предлагает также аудит систем телефонной связи и операторских центров.

Описанные методики предназначены, прежде всего, для оценки готовности сети заказчика к внедрению решений компании Avaya (например, систем IP-телефонии, систем управления опереторскими центрами и др.).

Технические средства аудита

Специалисты компании «Инфосистемы Джет» используют при аудите ТИ ряд технических средств, которые можно разбить на две группы. В первую входят различные анализаторы сетевого трафика:

- Аппаратный сетевой анализатор Acterna DA-3400. Позволяет анализировать множество сетевых протоколов на высокой скорости (Gigabit Ethernet), может имитировать загрузку сегментов сети, допускает подключение в разрыв сетевого кабеля.
  Подробное описание анализатора Acterna DA-3400 можно найти по ссылке http://www.acterna.com/global/products/descriptions/DA-3400/index.html.
- Анализаторы Ethereal (один из лучших бесплатных продуктов), Observer (коммерческий продукт). Устанавливаются на ПК, применяются, как правило, в связке со средствами захвата и отражения трафика (SPAN-порты коммутаторов Cisco).
  Описание этих анализаторов можно найти на сайтах http://www.networkinstruments.com/products/observer.html и http://www.ethereal.com/ соответственно.

Вторая группа включает средства автоматизированного анализа сообщений об ошибках и анализа файлов журналов.

- Средство Cisco Output Interpreter обеспечивает автоматизированный поиск ошибок в конфигурациях, сообщений о проблемах в файлах журналов. Представляет собой web-средство на сайте Cisco в разделе для партнеров.
- Анализатор Sawmill обеспечивает анализ журналов одновременно из нескольких источников и позволяет находить корреляции между сообщениями об ошибках.
  Описание этого продукта можно найти на сайте http://www.sawmill.net/.

Что дальше?

Итак, в результате проведенного аудита заказчик получает документы:

- Аналитический отчет.
- Комплект эксплуатационной документации.

Прежде всего, следует обратить внимание на рекомендации, содержащиеся в аналитическом отчете. Отметим, что Компания «Инфосистемы Джет» не ограничивается их разработкой. Специалисты компании готовы оказать помощь в выполнении большинства из них.

Все выдаваемые рекомендации классифицируются на неотложные и долговременные. Неотложные следует реализовать как можно скорее, это немедленно даст заметный результат: будут устранены наиболее злободневные проблемы, сопровождающие эксплуатацию ТИ заказчика.

Методику классификации рекомендаций иллюстрирует рис. 7. В результате проведения аудита выявляются расхождения между потреб-

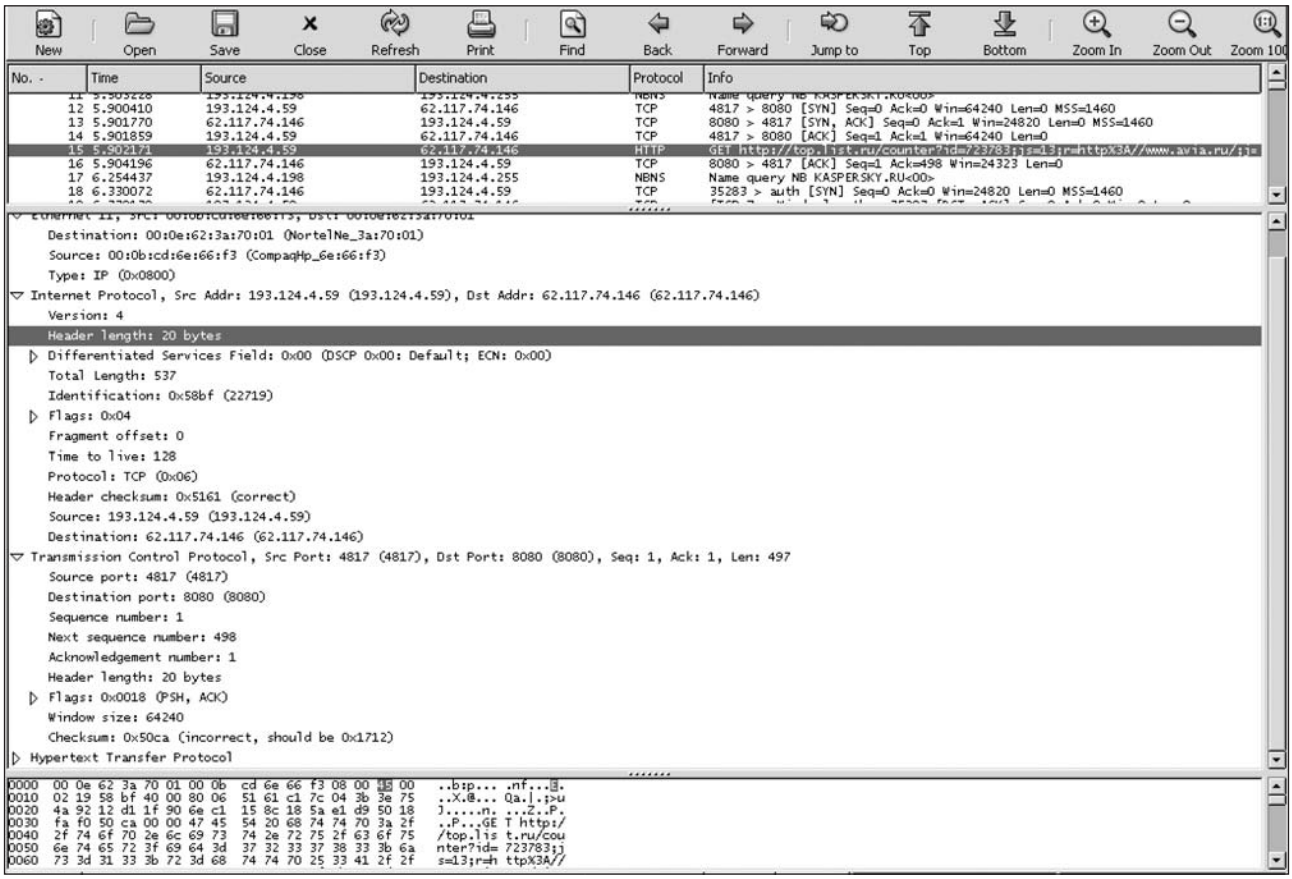


Рис. 6. Анализатор трафика Ethereal. Пример рабочего экрана.

ностями заказчика и характеристиками использующейся ТИ. Рекомендации, включенные в отчет, направлены на устранение этих расхождений. Реализация всех или части рекомендаций может быть представлена как проект модернизации ТИ.

На этапе аудита оценивается степень воздействия на сеть тех или иных рекомендаций, и, соответственно, степень соответствия сети потребностям заказчика после их выполнения. Также уже на этапе аудита может быть оценена стоимость реализации проекта модернизации ТИ и рисков, связанных с этим проектом.

Модернизации, воздействие которых на сеть существенно, а стоимость внедрения минимальна, и рекомендуются в качестве неотложных.

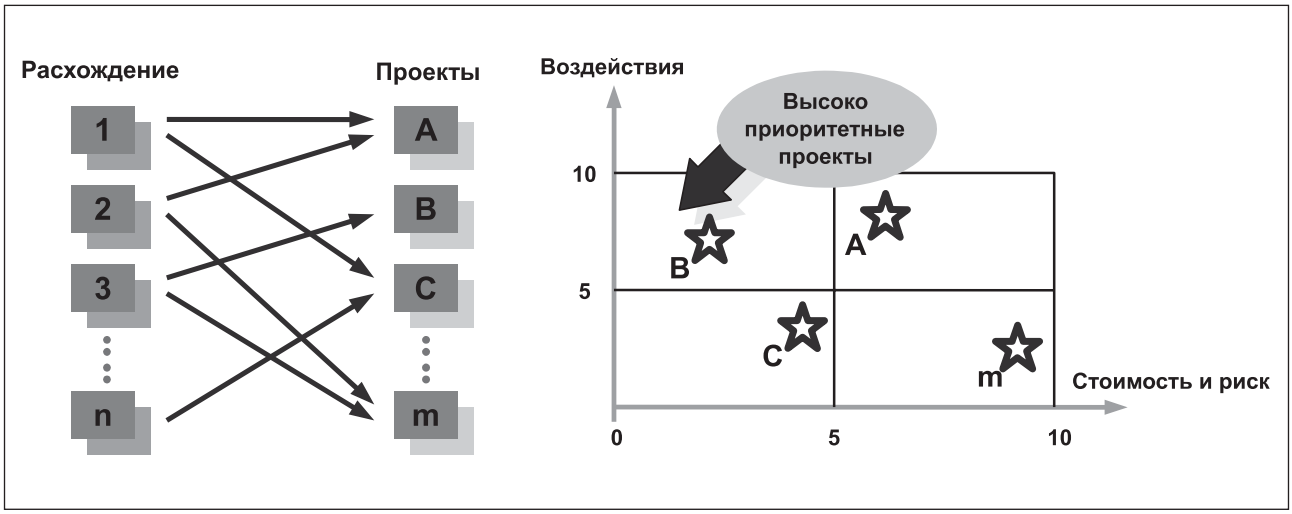


Рис. 7. Принятие решений о модернизации ТИ

Примеры неотложных рекомендаций.

- Обновление версий программного обеспечения, наложение пакетов исправлений. Эти меры предлагаются обычно в тех случаях, когда заведомо известно, что используемые программные продукты содержат ошибки, которые могут быть причиной обозначаемых заказчиком проблем.
- Изменение параметров настойки оборудования. Например, изменение времени ожидания со значения по умолчанию на большее или изменение алгоритма приоритизации трафика. Во многих случаях реализация таких рекомендаций дает значительный немедленный эффект при минимальных затратах.
- Настройка централизованного сбора информации с сетевого оборудования и серверов. Такая мера существенно упрощает работу системного администратора и позволяет ему быстрее выявлять причины проблем с сетью.

Долговременные рекомендации обычно предполагают разработку стратегии развития ТИ, зафиксированной в виде концепции модернизации, часто предусматривают длительную, поэтапную программу приведения характеристик сети в соответствие деловым потребностям заказчика. Сведения, содержащиеся в отчете об аудите, в этом случае являются исходными данными концепции или проекта.

Примеры долговременных рекомендаций.

- Применить резервирование. Обычно рекомендуется установить резервный коммутатор или организовать резервную линию связи. Эти меры полезны в тех случаях, когда простой сети в значительной степени влияет на деятельность предприятия. Может быть предложено как «горячее», так и «холодное» резервирование (помещение резервного оборудования на склад).
- Внедрить систему управления сетью. В тех случаях, когда в сети много оборудования и локализовать неисправность затруднительно, система управления поможет ускорить устранение проблем.
- Перейти к иной технологии связи с оператором телематических услуг. Иногда достаточно лишь немного повысить скорость каналов связи для существенного ускорения работы приложений и повышения общей производительности труда сотрудников.

Здесь приведены примеры рекомендаций лишь технического характера, но во многих случаях наибольшего эффекта можно достичь комбинацией технических и организационных мер. Типовые организационные меры могут включать:

- разработку порядка подключения новых пользователей или площадок;
- разработку порядка внесения изменений в эксплуатационную документацию;
- заключение сервисных договоров на определенных условиях.

Качество аудита, как и любых работ, зависит, в первую очередь, от квалификации подрядчика. Однако заказчик должен понимать, что в немалой степени оно зависит и от его готовности предоставить подрядчику все необходимые сведения, поскольку их полнота и актуальность непосредственно влияют на результат. Описание работ, содержащееся в данной статье, поможет заказчику подготовиться к аудиту своей сети и, в конечном счете, способствовать обеспечению высокого качества работ в целом.

Реализованные проекты

Компания «Инфосистемы Джет» реализовала ряд проектов по аудиту ТИ предприятий. Представим наиболее значительные из них.

Торговая компания. Аудит проводился для оценки готовности ТИ к внедрению централизованной системы торговли. Было выполнено профилирование приложения, разработан пакет рекомендаций по повышению эффективности работы сети. Реализация рекомендаций обеспечила стабильную работу ТИ и приложения на 25 объектов. В настоящее время в сеть объединено 60 объектов, приложение работает стабильно.

Оператор мобильной связи. Аудит в этой компании проводился, чтобы на основе его результатов можно было разработать ТИ для вновь открываемых региональных офисов. Особенности данной ТИ заключаются в необходимости обеспечения централизованного учета и тарификации телефонных переговоров. Было проведено профилирование приложений, разработана методика расчета пропускной способности каналов связи. Организация каналов связи с использованием этой методики обеспечивает стабильную работу приложений в масштабах всей сети компании.

Государственная структура. Аудит проводился для оценки готовности ТИ к внедрению нового приложения с высокими требованиями к качеству обслуживания. Особенности ТИ заказчика: каналы с низкой пропускной способностью (Frame Relay 64-128 Кбит/с). Было проведено профилирование приложения, оценены потоки данных, разработана политика обеспечения качества обслуживания. Внедрение этой политики позволило обеспечить стабильную работу приложений.

Крупный банк. Был проведен аудит телекоммуникационной инфраструктуры на трех площадках, направленный на устранение конкретных проблем (снижение производительности и нестабильная работа подсистемы связи площадок).

Финансовая компания. Аудит проводился для оценки степени соответствия ТИ требованиям, предъявляемым сетевыми приложениями (прежде всего, IP-телефонией Cisco AVVID). Были разработаны рекомендации, выполнение которых позволяет при сравнительно небольших затратах обеспечить соответствие ТИ предъявляемым требованиям.

Несколько советов по эксплуатации ТИ

Здесь приведены некоторые рекомендации, составленные в разное время для разных заказчиков. Они могут быть полезны любому клиенту и для любой сети.

Установите в сети сервер службы времени (NTP). Настройте все сетевое оборудование и все серверы так, чтобы системное время всех устройств было синхронизовано. Такая мера существенно облегчает анализ журналов.

Настройте сетевое оборудование и серверы так, чтобы сообщения системного журнала копировались на отдельный сервер. Предусмотрите архивирование данных сообщений. Максимально защитите этот сервер от НСД. При атаке злоумышленнику будет сложнее скрыть следы своей деятельности.

Используйте централизованную аутентификацию доступа к сетевому оборудованию, например, через сервер RADIUS. Синхронизируйте базу сервера RADIUS со службой каталогов. Так проще контролировать доступ к сетевым устройствам.

Выделите для управляющих интерфейсов всех устройств отдельную виртуальную сеть. Ограничьте доступ в нее.

Выделите в рабочем графике системного администратора специальное время для просмотра всех журналов и предупреждений.

Регламентируйте и автоматизируйте все типовые операции (например, добавление пользователей или перемещение рабочих мест). Включите в регламенты порядок обновления эксплуатационной документации.

Внесите все имена и IP-адреса в DNS. Применяйте два сервера DNS — для внутренних нужд и для внешних ресурсов.

Поддерживайте сетевую инфраструктуру сбалансированной. Защищайте все данные одинаково надежно и тщательно.

Стройте сетевую инфраструктуру так, чтобы в ней было минимальное количество точек единого отказа, а отказы приводили бы к выходу из строя не всей ситемы, а лишь ее части.

Применяйте протокол Spanning Tree (и его расширения) только тогда, когда хорошо представляете себе его работу.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Лапина И.К. *(lapina@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (095) 411 76 01
факс (095) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати **32555**