УПРАВЛЕНИЕ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ ИНФРАСТРУКТУРОЙ

Санкт-Петербург 2011

Содержание

Введение

Информационные технологии сегодня являются неотъемлемой составляющей актива любого предприятия. В то же время затраты на их поддержку и развитие неизменно растут, и их доля в общей структуре расходов предприятий неизменно увеличивается. Значительная часть этих расходов приходится не собственно на приобретение конечных решений, но на создание и поддержание инфраструктуры, необходимой для надежного и эффективного функционирования этих решений.

Сложность информационно-технологической инфраструктуры, необходимой для обеспечения функционирования на должном уровне современных корпоративных информационных систем и других комплексных решений требует реализации не менее сложных и комплексных стратегий управления ИТ-инфраструктурой. Сложность решения такой задачи состоит в том, что для этого нужно достаточно радикально пересматривать общее позиционирование сервисных ИТ-служб в структуре предприятия.

Исторически сложившиеся, зачастую плохо организованные ИТ-подразделения и отдельные специалисты, решающие широкий круг вопросов, связанных с теми или иными инфраструктурными элементами не могут обеспечить эффективного управления ИТ-инфраструктурой без системного подхода к этому вопросу на уровне предприятия в целом. При этом ИТ-служба предприятия сегодня уже не может рассматриваться сугубо как вспомогательное, обеспечивающее подразделение. Уровень инвестиций и ответственности, который связан с внедрением и эксплуатацией информационных технологий на современном предприятии требует нового, значительно более серьезного взгляда на управление информационно-технологической инфраструктурой.

В рамках дисциплины "Управление информационно-технологической инфраструктурой" будет предпринята попытка сформировать у студентов направлений подготовки "Бизнес-информатика", "Прикладная информатика" и "Информационные системы и технологии" системного взгляда на вопросы управления информационно-технологической структурой предприятия. Курс состоит из трех модулей. В первом модуле рассматриваются современные стандарты, методологии и методики управления информационно-технологической инфраструктурой, созданные ведущими производителями корпоративных информационных решений и исследовательскими институтами. Второй модуль посвящен программным средствам поддержки и автоматизации управления информационно-технологической инфраструктурой. В третьем модуле рассматривается ряд частных вопросов управления информационно-технологической инфраструктурой, связанных, в частности, с организацией безопасности персональных данных и управлением лицензиями в условиях использования свободного программного обеспечения. Также в третьем модуле приводятся два примера комплексного подхода к организации информационно-технологической инфраструктуры в крупных сетевых проектах Google и Flickr.

Глава 1. Стандарты и методики управления ИТ-инфраструктурой

Место ИТ-инфраструктуры в архитектуре предприятия

Под архитектурой предприятия (EA - Enterprise Architecture), обычно понимается полное описание (модель) структуры предприятия, как системы, включающее описание ключевых элементов этой системы, связей между ними.

Архитектура предприятия определяет общую структуру и функции систем (бизнес и ИТ) в рамках всей организации в целом (включая партнеров и другие организации, формирующие так называемое «предприятие реального времени») и обеспечивает общую рамочную модель (framework), стандарты и руководства для архитектуры уровня отдельных проектов. Общее видение, обеспечиваемое архитектурой предприятия, создает возможность единого проектирования систем, адекватных, с точки зрения обеспечения потребностей организации, и способных к взаимодействию и интеграции там, где это необходимо.

В основе архитектуры предприятия заложен «Архитектурный взгляд» на системы, определенный в стандарте ANSI/IEEE 1471, как «фундаментальная организация системы, состоящая из совокупности компонент, их связей между собой и внешней средой, и принципы, которыми руководствуются при их создании и развитии».

Архитектура предприятия описывает деятельность компании с двух основных позиций:

- Бизнес-архитектура описывает предприятие с позиции логических терминов, таких, как взаимодействующие бизнес-процессы и бизнес правила, необходимая информация, структура и потоки информации.
- Архитектура информационных технологий описывает предприятие с позиции технических понятий, таких как аппаратные и компьютерные средства, программное обеспечение, защита и безопасность.

Документирование и оптимизация архитектуры информационных технологий обеспечивает нам уменьшение уровня сложности информационных систем и упрощает их интеграцию. Оптимизация бизнес-процессов компании и оптимизация функциональности информационных систем, использующихся для автоматизации бизнес-процессов, увеличивает приток инвестиций в информационные технологии. Архитектура предприятия в первую очередь объединяет архитектуру информационных технологий и бизнес - архитектуру в единое целое, обеспечивая комплексный взгляд на обе существующие области.

Архитектура предприятия является важным критическим элементом, связывающим информационные технологии, бизнес потребности предприятия и объединяет в себе процессы стратегического бизнес – планирования, прикладные информационные системы и процессы их сопровождения.

При этом архитектура предприятия неразрывно связана с основными рабочими процессами:

- стратегия и планирование на уровне предприятия;
- управление корпоративными проектами.

Разработка стратегии современного предприятия (Strategy and Planning) и управление корпоративными проектами (Enterprise program management) включают в себя направление, связанное непосредственно с информационными технологиями. Современные тенденции рассматривают ИТ проекты и стратегические инициативы как определенный актив компании, которым можно управлять аналогично финансовым активам.

Управление портфелем информационных технологий (Business and IT portfolio management) – это процесс управления инвестициями в области управления ИТ проектами. Под портфелем понимается совокупность проектов, выполняемых на общем пуле ресурсов (финансы, люди, оборудование, материалы, энергия), при этом пул ресурсов и результаты всех проектов портфеля находятся в компетенции одного центра ответственности.

Аналитики компании META Group считали, что это - область пересечения архитектуры предприятия, стратегии предприятия и управления корпоративными проектами. Стратегия и планирование при этом обеспечивают основу для выработки ИТ стратегии предприятия, в соответствии с которыми появляются проекты внедрения (модернизации) информационных систем. Управление проектами – можно рассматривать, в первую очередь, как механизм, обеспечивающий переход от текущего состояния к планируемому, или, другими словами, переход от текущей архитектуры предприятия к целевой архитектуре.

Архитектура предприятия является одним из элементов управление ИТ портфелем и предоставляет необходимую информацию о бизнес-процессах и технологиях, необходимых для их автоматизации. Архитектура предприятия не только является основой для разработки портфеля активов, но также обеспечивает весь жизненный цикл многих ИТ - активов.

Архитектура предприятия позволяет увидеть все предприятие целиком, создать цепочку, показывающую воздействие отдельных элементов стратегии развития предприятия на его бизнес-процессы, и их зависимость от информационных систем и технологических элементов.

Архитектура предприятия является инструментом управления, обеспечивающим процесс принятия решений об инвестициях в информационные технологии, стирающие грань между бизнесом и ИТ - подразделением.

Традиционно считается, что новые инициативы по внедрению информационных технологий должны проявляться в виде требований от бизнеса, и новые информационные системы должны отвечать именно этим требованиям. Но бизнес должен, в то же время, получать и учитывать «сигналы» от ИТ - подразделения, которое, соответственно, должно показывать новые возможности, появляющиеся у предприятия при внедрении новых ИС. Таким образом, архитектуру предприятия можно рассматривать как новый виток развития организационных принципов построения деятельности предприятия, обеспечивающий его эффективное функционирование.

Любому предприятию требуется планомерное развитие его структуры, бизнес-процессов, информационных систем и их интеграция между собой. Архитектура предприятия собственно и является планом развития предприятия (целевая архитектура) и документированной схемой того, что происходит в компании в текущий момент времени (текущая архитектура).

Текущая архитектура (Current architecture) - описывает существующее состояние архитектуры предприятия. Называется также архитектурой “как есть” (AS-IS) или базовым состоянием существующей архитектуры.

Текущая архитектура – это отображение объективной реальности, включающей в себя существующие компоненты (бизнес-процессы, информационные системы, технологические элементы) и их связи. Это набор моделей с неизбежными упрощениями, ограничениями и субъективными искажениями.

Процесс разработки текущей архитектуры – это, в первую очередь, процесс документирования и поддержания информации о состоянии предприятия в актуальном виде, обеспечивающий регистрацию и контроль информации обо всех элементах архитектуры предприятия, включающий в себя ведение базы данных по архитектурным объектам; ведение управленческого учета и учета состояния.

Процесс разработки текущей архитектуры аналогичен процессу ITIL/ITSM (управление конфигурацией - Configuration Management). Для упрощения работы по разработке текущей архитектуры многие компании используют базу данных конфигурационных единиц (CMDB), дополнив ее необходимой информацией.

Целевая архитектура (Target Architecture) - описывает желаемое будущее состояние предприятия или, «что должно быть сформировано» (TO-BE). Другими словами, целевая архитектура является будущей моделью предприятия.

Целевую архитектуру можно назвать идеальной моделью предприятия, в основу которой заложены:

- стратегические требования к бизнес-процессам и информационным технологиям;
- информация о выявленных «узких местах» и путях их устранения;
- анализ технологических тенденций и среды бизнес деятельности предприятия.

Целевая архитектура (модель to-be) и текущая архитектура (модель as-is) позволяют описать начальное и конечное состояние предприятия – до и после внесения изменений в его структуру, оставляя без внимания сам процесс изменений.

Процесс перехода от текущей архитектуры предприятия к целевой переводит предприятие на новую спираль развития и, таким образом, мы можем говорить, что архитектура предприятия характеризуется определенным жизненным циклом, похожим на жизненный цикл информационных систем.

Современные подходы к построению архитектуры предприятия традиционно разделяют ее на несколько слоев (предметных областей). Количество архитектурных слоев варьируется в различных методиках. Ниже мы рассмотрим слои, использующиеся в большинстве из существующих методик:

- Стратегические цели и задачи предприятия.
- Бизнес – архитектура предприятия.
- Архитектура информационных технологий (ИТ - архитектура предприятия).
    - Информационная архитектура (Enterprise Information Architecture).
    - Архитектура прикладных решений (Enterprise Solution Architecture).
    - Технологическая архитектура (Enterprise Technical Architecture).

Стратегические цели и задачи предприятия определяют основные направления развития и ставят долгосрочные задачи и цели. При разработке стратегических целей предприятия необходимо учитывать воздействие информационных технологий на формирование облика современного предприятия. В ходе разработки стратегических целей предприятия формируется (модернизируется) и стратегия развития информационных технологий.

Бизнес стратегия – определяет направление развития бизнеса в соответствии со стратегическими целями и задачами, стоящими перед предприятием, и отвечает на вопрос, почему предприятие должно развиваться именно в этом направлении. Бизнес стратегия включает в себя:

- Цели и задачи стоящие перед предприятием.
- Бизнес решения, необходимые для достижения поставленных целей и задач.
- Изменения, которые нужно провести для достижения поставленных целей и задач.

ИТ - стратегия определяет направление развития информационных технологий в соответствии с целями, задачами и бизнес стратегией предприятия, и определяет, как может быть реализована бизнес стратегия. ИТ - стратегия включает:

- Проекты, которые можно запустить для выполнения бизнес стратегии.
- Варианты решения текущих задач и проблем.
- Технологии, которые можно использовать для достижения поставленных целей.

Бизнес - архитектура предприятия (EBA - Enterprise Business Architecture) – это целевое построение организационной структуры предприятия, увязанное с его миссией, стратегией, бизнес - целями. В ходе построения бизнес - архитектуры определяются необходимые бизнес-процессы, информационные и материальные потоки, а также организационно-штатная структура.

Под бизнес - архитектурой, как правило, понимается целостная организация бизнес-процессов, организационных, культурных и социальных областей деятельности предприятия. Она учитывает профиль предприятия, его цели, варианты реализации. Архитектура бизнес-процессов определяется основными функциями организации и может меняться под влиянием внешней среды.

Бизнес - архитектура предприятия неразрывна, связана с процессом его управления. Под управлением предприятием обычно понимается деятельность компании с учетом изменений в окружающей экономической и социальной среде. Управленческий персонал распределяет финансовые, трудовые и материальные ресурсы для максимально эффективного достижения стратегических целей и задач предприятия.

В ходе разработки бизнес - архитектуры подробно рассматриваются различные модели построения предприятия, соответствующие стратегии его развития. Модели бизнес - архитектуры могут быть разделены на три класса: классические (эталонные), специализированные и специфические.

ИТ - архитектура предприятия или, другими словами, *архитектура информационных технологий* представляет собой совокупность технических и технологических решений для обеспечения эффективного функционирования бизнес - процессов предприятия в соответствии с правилами и концепциями, определяемыми бизнес - архитектурой.

Архитектура информационных технологий описывает основные информационные системы, их взаимосвязи и включает в себя их принципы развития, совершенствования и поддержки. Таким образом, мы можем говорить о том, что «архитектура является самодостаточной и полной динамической моделью системы».

Архитектура информационных технологий является неотъемлемым элементом архитектуры всего предприятия и зависит от его целей и задач, стратегии развития, сложившейся модели бизнес процессов.

В настоящее время существует множество работ, посвященных исключительно архитектуре информационных систем. Следует отметить, что практически во всех существующих методиках - архитектура информационных технологий является производной (частным случаем) архитектуры предприятия в целом, и рассматривать ее отдельно от контекста предприятия не является целесообразным.

Обобщенная ИТ - архитектура должна включать в себя как логические, так и технические компоненты. Логическая архитектура предоставляет высокоуровневое описание миссии предприятия, его функциональных и информационных требований, системных компонентов и информационных потоков между этими компонентами. Техническая архитектура определяет конкретные стандарты и правила, которые будут использоваться для реализации логической архитектуры. Традиционно ИТ - архитектуру предприятия представляют в виде трех взаимосвязанных компонентов:

- Enterprise Information Architecture (EIA) – информационная архитектура.
- Enterprise Solution Architecture (ESA) – архитектура прикладных решений.
- Enterprise Technical Architecture (ETA) – техническая архитектура.

В ходе разработки архитектуры предприятия создается модель, включающая информацию о его производственных процессах, информационных и материальных потоках, ресурсах и организационных единицах. При этом модель ИТ - архитектуры непосредственно зависит от роли, которую выполняют информационные системы на предприятии: стратегическая (ориентированная на выполнение сложившихся стратегий и операций), сдвигающая (инструмент для увеличения эффективности бизнеса), поддерживающая (ИС не играют особой роли в функционировании

предприятия), заводская (ИС являются обязательным элементом, обеспечивающим функционирование бизнеса). Модель предприятия (соответствующая ее роли) позволяет не только давать лучшее представление о структуре предприятия, но и является эффективным инструментом для анализа экономических, организационных и многих других аспектов его функционирования.

ИТ - архитектура предприятия определяет правила формирования всех компонентов ИТ, взаимосвязи между ними и бизнес - архитектурой предприятия. Это связано с тем, что документирование ИТ - архитектуры без ее увязки с бизнес - архитектурой предприятия быстро утрачивает практическую ценность.

Информационная архитектура (EIA - Enterprise Information Architecture) или, другими словами, архитектура информации – это (с точки зрения аналитиков компании Meta Group) управляемый набор методик, описывающий информационную модель предприятия и включающий в себя:

- Базы данных и хранилища данных.
- Информационные потоки (как внутри организации, так и связи с внешним миром).

Информационную архитектуру предприятия условно можно назвать уровнем потоков данных. Но, при построении информационной архитектуры предприятия нет необходимости создавать модели всех видов данных, используемых на предприятии. Достаточно обеспечить выбор наиболее важных (критичных для предприятия) данных и моделировать их на высоком уровне абстракции.

Архитектура прикладных решений (ESA - Enterprise Solution Architecture) – или, другими словами, архитектура приложений, включает в себя совокупность программных продуктов и интерфейсов между ними.

Архитектуру прикладных решений разделают на два направления:

- Область разработки прикладных систем.
- Портфель прикладных систем.

Область разработки прикладных систем описывает технологическую часть архитектуры прикладных решений и включает в себя: программные продукты; модели данных; интерфейсы (API); пользовательские интерфейсы.

Область разработки прикладных систем является техническим описанием конкретных приложений. Соответственно, информацию о данных модулях проще всего представить в виде двух следующих схем:

- Компоненты и структура системы – внутренняя структура системы, включающая в себя информацию о программных модулях и базах данных.

- Взаимодействие с другими системами (интерфейсы) – описывает взаимодействие приложения с внешними объектами (программными продуктами, пользователями).

Архитектура прикладных решений описывает ситуацию, сложившуюся в ИТ - подразделении на текущий момент времени (т.е. это картина, демонстрирующая «технологическое обеспечение» бизнес - процессов, где каждой основной бизнес - функции соответствуют определенные приложения). На основе архитектуры прикладных решений строятся планы последующего развития информационных технологий в компании, разрабатываются планы мероприятий и проектов, необходимых для достижения стратегических целей.

На данном уровне лучше всего отслеживается взаимодействие бизнес - архитектуры предприятия и ИТ - архитектуры, т.к. можно определить взаимосвязи между организационной структурой предприятия и используемыми приложениями. В этом случае для оптимизации управления приложениями их разделяют на определенные группы (домены) в соответствии с функциональными возможностями. Следует отметить, что подобное разделение позволяет проще идентифицировать владельца приложения, определять его соответствие бизнес - требованиям.

Техническая архитектура предприятия (ETA - Enterprise Technical Architecture) – это совокупность программно-аппаратных средств, методов и стандартов, обеспечивающих эффективное функционирование приложений. Другими словами, под технической архитектурой мы будем понимать полное описание инфраструктуры предприятия, включающее в себя:

- Информацию об инфраструктуре предприятия.

- Системное программное обеспечение (СУБД, системы интеграции).

- Стандарты на программно-аппаратные средства.

- Средства обеспечения безопасности (программно-аппаратные).

- Системы управления инфраструктурой.

Техническую архитектуру предприятия можно визуально представить в виде совокупности архитектурных схем приложений, используемых на предприятии. Визуально техническую архитектуру приложения, в свою очередь, можно представить в виде схемы включающей в себя информацию о серверах, сегментах СКС, компонентах системы, стандартах (использующихся в данном приложении) и взаимосвязях между ними.

Information Technology Infrastructure Library (ITIL)

В настоящее время ИТ-служба предприятия становится полноправным участником бизнеса, выступая в роли поставщика определенных услуг для бизнес-подразделений, а отношения между ними формализуются как отношения «поставщик услуг – потребитель услуг». Бизнес-подразделение формулирует свои требования к необходимому спектру услуг и их качеству, руководство предприятия определяет объем финансирования для выполнения этих требований, а подразделения ИТ-службы поддерживают и развивают информационную инфраструктуру предприятия таким образом, чтобы она была в состоянии обеспечить запрошенную услугу с заданным качеством.

Связь стратегический целей многих современных компаний с информационными технологиями привела к росту потребности в ИТ - услугах, качество которых соответствовало бы требованиям бизнеса. ИТ - подразделения стали рассматриваться как структуры, не только разрабатывающие и поддерживающие различные корпоративные приложения, но как подразделения, предоставляющие пользователям определенный набор сервисов (ИТ – сервисов).

По проекту ITIL была разработана библиотека, описывающая лучшие из применяемых на практике способов организации работы подразделений или компаний, занимающихся предоставлением услуг в области информационных технологий. Множество частных и государственных компаний в разных странах мира, включая и Россию, добились значительных успехов в повышении качества ИТ-сервисов, следуя изложенным в ITIL рекомендациям и принципам. В настоящее время ITIL становится стандартом де-факто для ИТ.

Библиотека ITIL создавалась по заказу британского правительства. В настоящее время она издается британским правительственным агентством Office of Government Commerce и не является собственностью ни одной коммерческой организации. В семи томах библиотеки описан весь набор процессов, необходимых для того, чтобы обеспечить постоянное высокое качество ИТ-сервисов и повысить степень удовлетворенности пользователей. Следует отметить, что все эти процессы нацелены не просто на обеспечение бесперебойной работы компонент ИТ-инфраструктуры. В гораздо большей степени они нацелены на выполнение требований пользователя и заказчика.

Особенностью проекта является свобода использования его результатов:

- ограничений на использование нет;
- материалы модели могут быть использованы полностью или частично;
- модель может быть использована в точном соответствии с текстом книг ITIL либо адаптирована пользователем.

При этом модель сегодня является наиболее широко распространенным в мире подходом к управлению ИТ-сервисами. Она применима к организациям любого размера и любой отраслевой принадлежности.

Вторая версия библиотеки ITIL включает 7 книг по основным разделам управления ИТ-сервисами:

Service Delivery (предоставление услуг) – содержит описание типов ИТ-услуг, предоставляемых предприятием;

Service Support (поддержка услуг) – представляет собой описание процессов, позволяющих обеспечить пользователям доступ к ИТ-услугам, необходимым для выполнения бизнес-задач;

Information & Computing Technology Infrastructure Management (управление ИТ-инфраструктурой). В книге представлено общее описание методики организации работы ИТ-службы по управлению ИТ-инфраструктурой компании;

Application Management (управление приложениями) указывает, как обеспечить соответствие программных приложений изменениям в потребностях бизнеса, а также рассматривает общий жизненный цикл приложений, включающий разработку, внедрение и сопровождение;

The Business Perspective (бизнес-перспектива) – рассматривается, как работа ИТ-инфраструктуры может влиять на бизнес компании в целом;

Planning to Implement Service Management (планирование внедрения управления услугами) – посвящена проблемам и задачам планирования, реализации и развития ITSM, необходимым для реализации поставленных целей;

Security Management (управление безопасностью) – посвящена проблемам безопасности. В ней рассматриваются проблемы разграничения доступа к информации и ИТ-сервисам, особенности оценки, управления и противодействия рискам, инциденты, связанные с нарушением безопасности и способы реагирования на них.

В третьей, версии библиотеки ITIL, представлено пять книг, названия которых отражают жизненный цикл ИТ-услуг:

Первая книга *Service Strategy* (стратегия сервисов) рассказывает о необходимости сервисного подхода, о преимуществах, которые даёт сервисная модель бизнесу, о том, как строить стратегическую политику соотнесения этой модели с внешними и внутренними стандартами организации, как рассчитать стоимость сервиса, управлять рисками и т.д.

Во второй книге *Service Design* (проектирование сервисов) рассказывается о политике проектирования сервисов (самое важное обновление во всей третьей версии ITIL): ведь абсолютно очевидно, что любой сервис должен

быть изначально спроектирован, хотя на практике организации демонстрируют примеры обратного. Результатом проектирования сервисов должен являться сервисный пакет (service package), в котором содержится подробнейшая информация о сервисе: за что он будет отвечать, как будет внедряться.

Третья книга *Service Transition* (передача сервисов) — здесь речь идёт о том, что невозможно судить о приемлемости ИТ сервиса до тех пор, пока не станет точно понятно, каким образом он будет использоваться. Часто заказчику бывает нужно нечто совершенно не похожее на то, что он сформулировал на этапе проектирования. В таком случае в уже спроектированном ИТ сервисе делаются серьёзные изменения. И необходимо, чтобы при построении новых сервисов можно было контролировать ход выполнения работы. В этой книге собраны методики перехода, оценки и тестирования сервисов.

В четвёртую книгу *Service Operation* (эксплуатация сервисов) перешли процессы сервисной поддержки (service support) из предыдущей версии библиотеки ITIL® v2. Правда, добавлено всё то, чего не хватало для поддержки сервисов во второй версии: наконец-то описана процедура сервисных запросов и процедура управления событиями.

В пятой книге *Continual Service Improvement* (непрерывное улучшение сервисов) описан семишаговый процесс поиска необходимых изменений для уже работающих сервисов. Рассказано о непременно предшествующей таким изменениям оценке двух ситуаций: той, в которой компания находится сейчас, и той, в которой планирует оказаться через некоторое время после усовершенствования сервиса.

В Европе существуют два центра сертификации специалистов по модели ITIL/ITSM − EXIN (Нидерланды – Голландский Экзаменационный Институт) и ISEB (The Information Systems Examination Board – подразделение Британского Компьютерного Общества – British Computer Society). Внедрением процессов ITIL/ITSM и обучением занимается целый ряд компаний-консультантов. В России это Hewlett-Packard Consulting, «Ай-Теко», IT-Expert.

Модель ITIL/ITSM поддерживается более чем десятком программных продуктов и пакетов. Лидерами разработки программных инструментов управления ИТ-инфраструктурой являются: Hewlett-Packard, Computer Associated, IBM, BMC Software и Microsoft. Среди российских компаний, поставщиков программных систем автоматизации управления ИТ-услугами следует отметить компании СофтИнтегро и Итилиум.

Важным элементом инфраструктуры ITIL/ITSM являются так называемые ITSM-форумы. Эти форумы представляют собой сообщества пользователей модели, консультантов, внедряющих модель, и производителей инструментального программного обеспечения. Сообщество, как правило,

имеет сайт в сети Интернет (например, ITSM ПОРТАЛ.RU), а также проводит конференции и другие мероприятия, обеспечивающие реальное общение участников. Так российское партнерство «Форум по ИТ Сервис-менеджменту» получило международную аккредитацию ITSMF и стало полноправным членом всемирного сообщества. ITSMF International представляет собой независимое сообщество профессионалов в области управления ИТ-услугами. Оно было создано в Великобритании в 1991 году и занимается пропагандой идей ITSM, разработкой стандартов в этой области и поддержкой обмена опытом в десятках стран мира. На сегодняшний день национальные отделения itSMF действуют уже в 41 стране мира. ITSMF Russia было образовано в 2005 году.

Внедрение методики управления ITSM – поэтапный процесс. Как показывает практика, решение первоочередных задач связано с рекомендациями, приведенными в первых книгах ITIL v.2 «Поддержка сервисов» и «Предоставление сервисов». Процессы группы предоставления сервисов считаются оперативными процессами, поскольку включают в себя повседневные функции ИТ-службы. Процессы группы поддержки сервисов относятся к тактическим, которые предназначены для обеспечения предоставления сервисов заданного качества.

Процессы поддержки ИТ-сервисов

Блок процессов поддержки ИТ-сервисов включает следующие процессы:

- управление инцидентами;
- управление проблемами;
- управление конфигурациями;
- управление изменениями;
- управление релизами.

Процесс управления инцидентами предназначен для обеспечения быстрого восстановление ИТ-сервиса. При этом *инцидентом* считается любое событие не являющееся частью нормального функционирования ИТ-сервиса.

Показателями качества реализации процесса являются:

- временная продолжительность инцидентов;
- число зарегистрированных инцидентов.

При реализации процесса должны выполняться следующие функции:

- прием запросов пользователей;
- регистрация инцидентов;
- категоризация инцидентов;

- приоритизация инцидентов;
- изоляция инцидентов;
- эскалация инцидентов;
- отслеживание развития инцидента;
- разрешение инцидентов;
- уведомление клиентов;
- закрытие инцидентов.

Необходимым элементом обеспечения эффективного функционирования процесса является создание службы поддержки пользователей (Help Desk), единой точки обращения по поводу различных ситуаций в ИТ-инфраструктуре, обработки и разрешении пользовательских запросов. Следует отметить, что роль службы поддержки пользователей в последнее время возрастает, что отражается в её модифицированном названии – Service Desk. Это говорит о том, что современные службы поддержки переориентируются с реактивного принципа работы, на проактивный, позволяющий анализировать ситуацию и предотвращать инциденты еще до их возникновения.

Для управления качеством процесса необходимо определить систему управления инцидентами, разработать управленческие отчеты и обеспечивать непрерывное улучшение процесса.

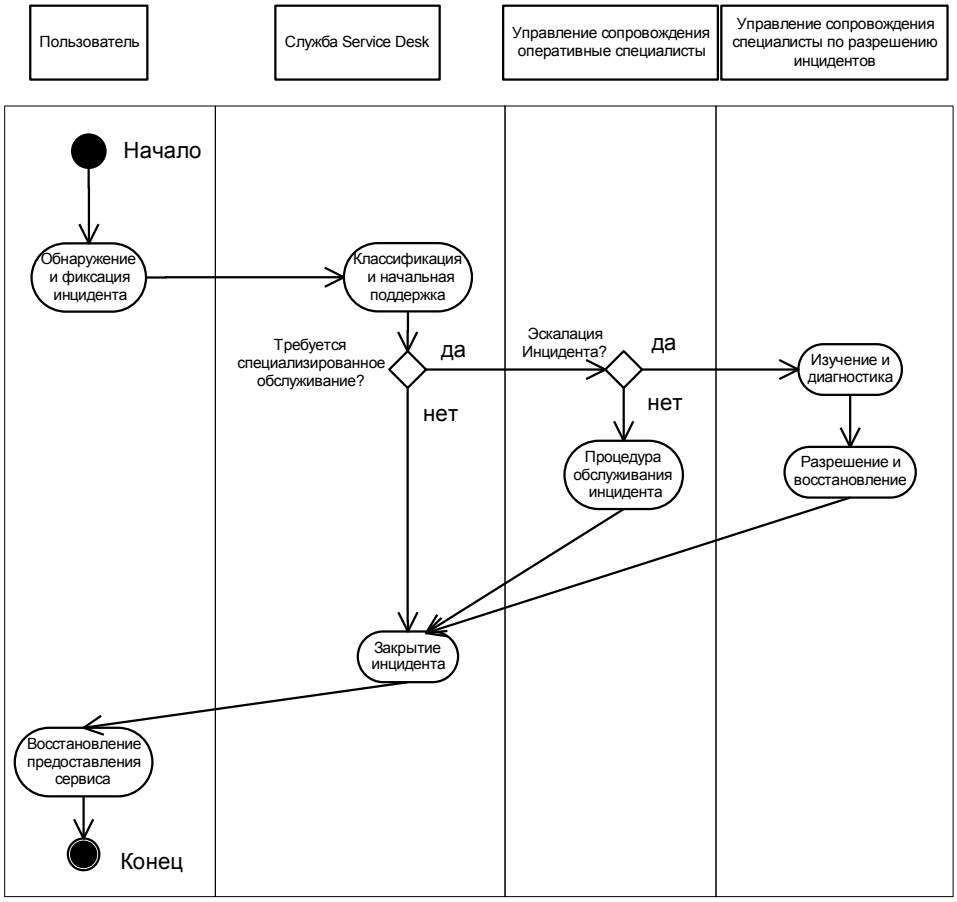

Рисунок 1.1

Пользователь ИТ-сервиса обнаруживает нарушение режима предоставления сервиса и обращается в Service Desk ИТ-службы. Сотрудник подразделения Service Desk фиксирует в регистрационном журнале инцидент, классифицирует его, определяет приоритет и при возможности осуществляет начальную поддержку. Например, при невозможности для пользователя корректно завершить транзакцию предлагается перезагрузить операционную систему и повторно провести транзакцию. Если начальной поддержки пользователю достаточно и не требуется специализированная поддержка, то осуществляется закрытие инцидента. Если необходимо специализированное обслуживание, то информация по инциденту передается в подразделение сопровождения ИТ-сервисов. В этом подразделении на основе базы знаний выясняется возможность устранения инцидента оперативным персоналом, т.е. нет необходимости эскалации инцидента на более высокий уровень обслуживания. В этом случае оперативный персонал реализует ранее документированную процедуру восстановления ИТ-сервиса.

Если для устранения инцидента отсутствует решение в базе знаний, то осуществляется эскалация на следующий уровень обслуживания, где специалисты высокого класса проводят изучение и диагностику инцидента, разрабатывают методы его устранения, восстановления заданной работоспособности ИТ-сервиса и пополняют базу знаний по инцидентам. После закрытия инцидента для пользователя предоставляется возможность доступа к ИТ-сервису с требуемыми показателями качества. Момент закрытия инцидента фиксируется в журнале службы Service Desk.

Процесс управления проблемами предназначен для минимизации негативного влияния инцидентов на бизнес и уменьшения количества инцидентов, за счет предотвращения возможных причин инцидентов. В данном контексте под *проблемой* понимают инцидент или группу инцидентов, имеющих общую неизвестную причину.

При реализации процесса должны выполняться следующие функции:

- анализ тенденций инцидентов;
- регистрация проблем;
- идентификация корневых причин инцидентов;
- отслеживание изменений проблем;
- выявление известных ошибок;
- управление известными ошибками;
- решение проблем;
- закрытие проблем.

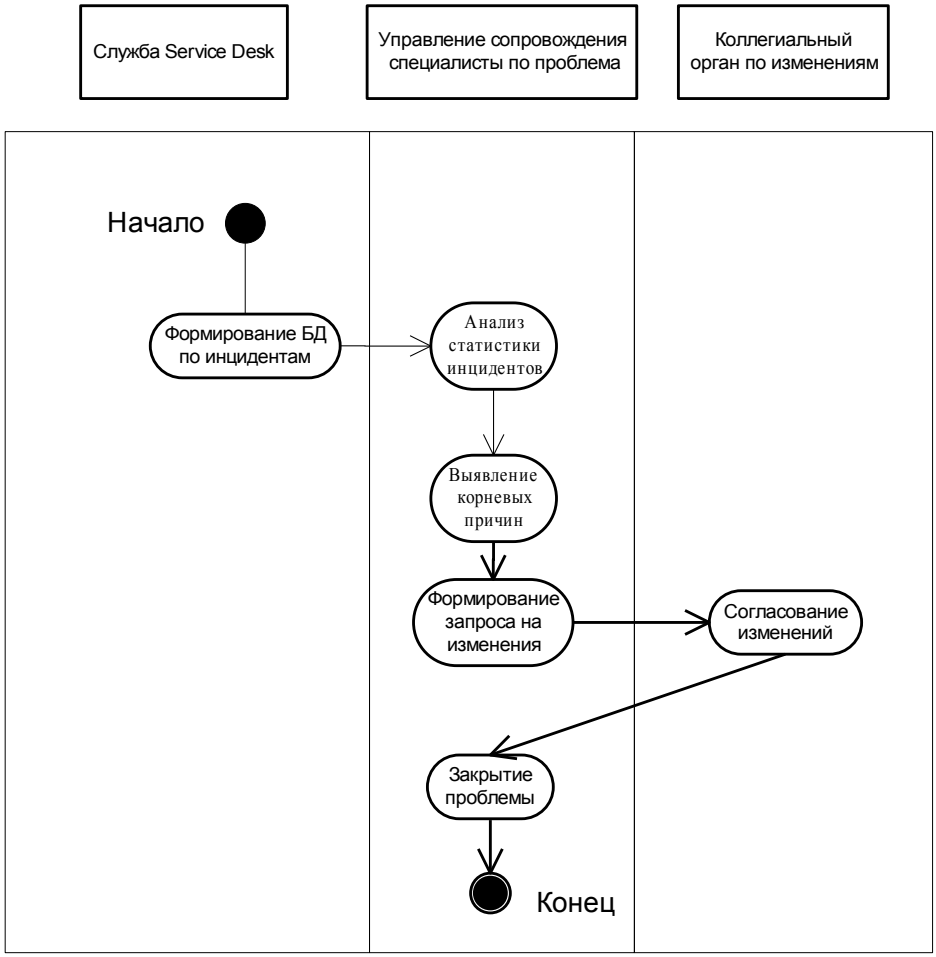

Рисунок 1.2

Для управления качеством процесса необходима организация системы управления проблемами/известными ошибками, организация превентивных процедур поддержки, организация способов верификации известных ошибок,

организация интерфейса поддержки поставщиком, разработка отчетов для управления, постоянное усовершенствование процесса.

Процесс управления конфигурациями предназначен для оказание помощи в управлении экономическим характеристиками ИТ-сервисов (комбинация требований клиентов, качества и затрат) за счет поддержания логической модели инфраструктуры ИТ и ИТ-сервисов, а также предоставление информации о них другим бизнес-процессам. Это реализуется путем идентификации, мониторинга, контроллинга и обеспечения информации о конфигурационных единицах (CI – Configuration Item) и их версиях. Конфигурационные единицы описывают системные компоненты с их конфигурационными атрибутами.

Процесс Управление конфигурациями отвечает за поддержание информации о взаимоотношениях между CI и за стандартизацию CI, мониторинг информации о статусе CI, их местоположении и всех изменениях CI. Информация о CI хранится в базе данных конфигурационных единиц (Configuration Management Data Base – CMDB). База данных управления конфигурациями представляет собой репозиторий метаданных, описывающий элементы конфигурации, их взаимосвязи и атрибуты. Элементы конфигурации представляют информационные компоненты, являющиеся объектами или субъектами процесса управления конфигурациями:

- материальными сущностями (серверная стойка, компьютер, маршрутизатор, модем, сегмент линии связи);
- системными или прикладными программными продуктами и компонентами;
- реализациями баз данных;
- файлами;
- потоками данных;
- нормативными или техническими документами;
- логическими или виртуальными сущностями (виртуальный сервер, серверный кластер, пул дисковой памяти, группа устройств).

Выбор классов и типов объектов конфигурации, их атрибутов, формируемых в CMDB, определяется разработчиком, в соответствии с требованиями предметной области. Атрибуты CI, как правило, отражают их специфические свойства и могут включать:

- идентификаторы;

- марки и названия моделей;
- серийные номера;
- сетевые адреса;
- технические характеристики;
- операционные характеристики.

Взаимосвязи CI представляют отношения, которые существуют или могут возникнуть между двумя и более CI. Как правило, язык спецификации модели CMDB – XML.

При реализации процесса управления конфигурациями должны выполняться следующие функции:

- планирование – определение стратегии, правил и целей для реализации процесса, определение инструментария и ресурсов, определение интерфейсов с другими процессами, проектами, поставщиками;
- идентификация – разработка модели данных для записи в базу конфигураций всех компонент инфраструктуры ИТ, отношений между ними, а также информации о владельцах этих компонент, их статусе и соответствующей документации.

При спецификации процесса важными понятиями являются:

- сфера охвата;
- глубина детализации;
- контроль;
- мониторинг статуса;
- верификация.

Сфера охвата (Scope) определяет, какая часть инфраструктуры будет находиться под контролем процесса. Например, можно охватывать только сервера и маршрутизаторы. Правильный выбор Сферы охвата очень важен на начальном этапе внедрения процесса Управление конфигурациями.

Глубина детализации (Level of Detail) – важный аспект, определяющий в дальнейшем отношения между CI. Отношения, как правило рассматриваются физические и логические. Физические отношения: родители - дети; соединения. Логические отношения: копия; «использует» (когда одна единица использует другую).

Контроль процесса означает, что процесс контролирует все изменения КЕ, кем бы они не производились.

Мониторинг *статуса* предполагает отслеживание реального статуса CI, содержащихся в базе: В процессе жизненного цикла информационной системы статус CI может меняться от «заказано» до «исключено из конфигурации»

Верификация предполагает проверку того, насколько информация в базе конфигураций соответствует реальности. При реализации процесса необходимо формировать отчеты руководству и другим процессам для осуществления их эффективного выполнения.

Процесс управления изменениями предназначен для обеспечения уверенности ИТ-менеджера в том, что все изменения необходимы, запланированы и согласованы. Данных процесс предполагает регистрацию всех существенные изменений в среде ИС предприятия, разрешает изменения, разрабатывает график работ по изменениям и организует взаимодействие ресурсов, всесторонне оценивает воздействие изменения на среду ИС и связанные с ним риски.

Основная задача данного процесса − проведение только обоснованных изменений в ИТ-инфраструктуре и отсев непродуманных или потенциально рискованных изменений. Для этого каждое изменение конфигурации ИС организации в обязательном порядке оформляется запросом на изменение. Запрос на изменение проходит стандартную процедуру одобрения. В зависимости от масштаба изменения решение принимается на уровне менеджера процесса, комитета по оценке изменений в рамках службы ИС, правления организации.

Конечный результат процесса — набор изменений, согласованных между собой и с существующей конфигурацией информационной системы и не нарушающих функционирования уже существующих сервисов. Все изменения в обязательном порядке регистрируются процессом управления конфигурацией.

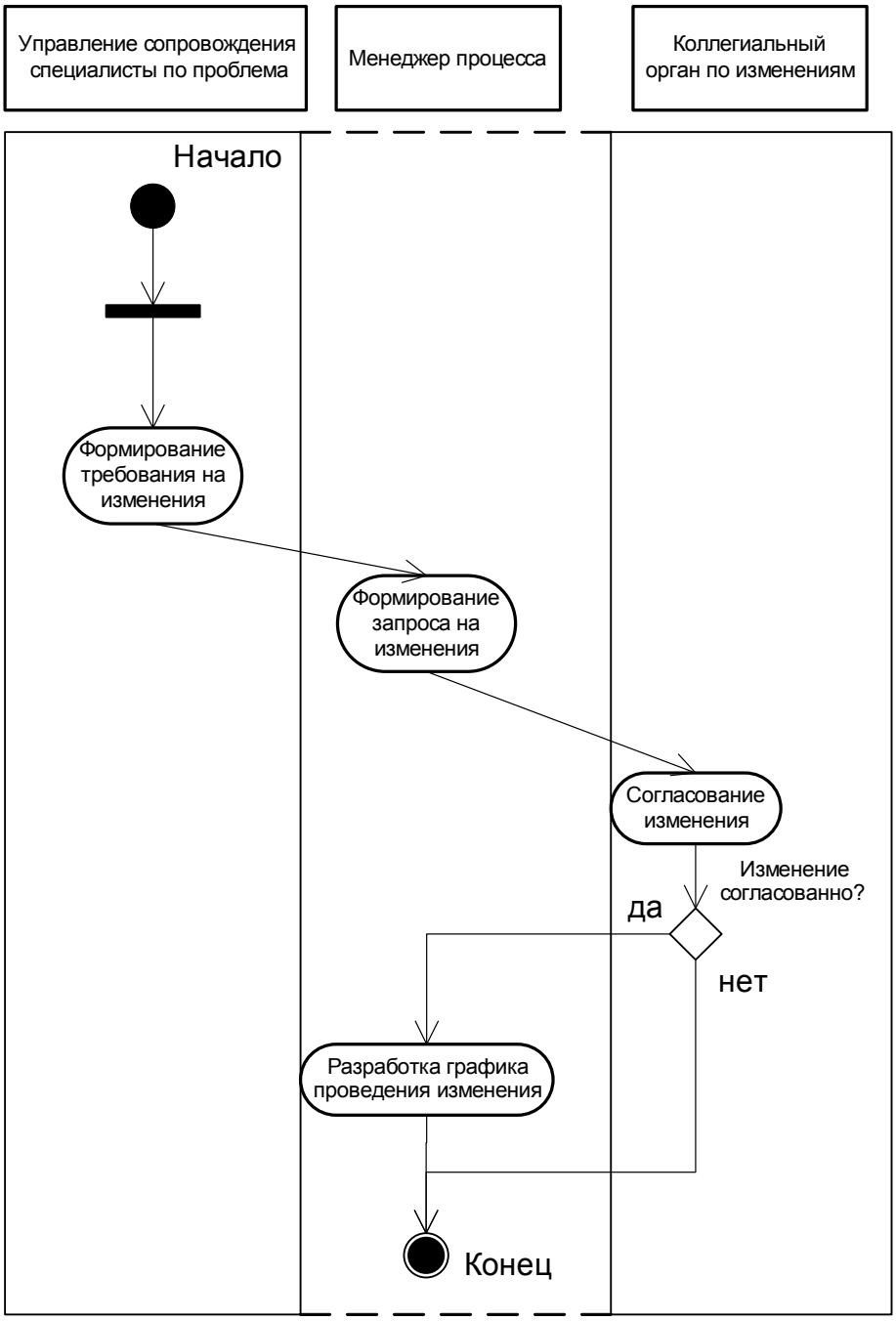

Рисунок 1.3

Процесс управления изменениями выполняет следующие функции:

- обрабатывает запросы на изменения;
- оценивает последствия изменений;
- утверждает изменения;
- разрабатывает график проведения изменений, включая восстановление при сбое;
- устанавливает процедуру обработки запроса на изменение;
- устанавливает категории и приоритеты изменений;

- управляет проектами изменений;
- организует работу комитета по оценке изменений;
- осуществляет постоянное улучшение процесса.

Важную роль в процессе управления изменениями играет коллегиальный орган по согласованию изменений. Этот орган включает в себя ИТ-директора (председателя), представителей бизнес-подразделений (представителей от финансовой службы и основных направлений бизнеса) и сотрудников ИС-службы, отвечающих по мере необходимости за следующие роли: планирование сервисов, управление изменениями, управление уровнем сервиса, управление проблемами и др. Задача коллегиального органа − возможных результатов и рисков при внесении изменений в ИТ-инфраструктуру.. Изменение отвергается как в случае незначительных результатов, так и в случае значительных рисков. В остальных случаях изменение может быть принято.

На основании положительного решения по изменениям разрабатывается график будущих изменений — детальный календарный график одобренных изменений, согласованный с заказчиками изменений, а также рядом других процессов ITSM.

Таким образом, процессы управления изменениями и конфигурациями обеспечивают целостность и согласованность информационной системы предприятия. В процессе управления изменениями эта задача решается посредством процесса одобрения изменений, предусматривающего всесторонний контроль за изменениями со стороны сотрудников ИС-службы, а при значительных изменениях — и руководства предприятия в целом. Процесс управления конфигурациями регистрирует все изменения в ИТ-инфраструктуре организации и обеспечивает все остальные процессы данными об установленных позициях оборудования и программного обеспечения, включая данные о произведенных настройках.

Процесс управления релизами предназначен для обеспечения согласованности изменений, вносимых в ИТ-инфраструктуру предприятия. Под *релизом* понимается набор новых и/или измененных позиций конфигурации, которые тестируются и внедряются совместно.

Процесс управления релизами предполагает консолидацию, структурирование и оптимизация всех изменений или обновлений, а также снижение риска при переводе сервиса на новый качественный уровень.

Процесс управления релизами состоит из трёх этапов:

- разработка;
- тестирование;

- распространение и внедрение.

Этап разработки не является обязательным для всех предприятий. Но для некоторых компаний, данный этап может являться одним из основополагающих, к ним могут относиться, например, компании по разработке программных средств.

Второй этап, этап тестирования, является важным для всех предприятий без исключения. На данном этапе необходимо определить критерии, по которым будет проводиться тестирование для каждого релиза, что позволяет определить степень определения готовности релиза к распространению и внедрению.

Если процесс Управления релизами подготавливает реализацию принятых изменений, то необходимо определить, какой процесс ответственен за их непосредственное внедрение. Руководствуясь материалами ITIL, можно сделать заключение, что в некоторых случаях, например, внедрение срочных или не значительных изменений, процесс Управления релизами осуществляет сам, на этапе внедрения. А в некоторых случаях, возможен вариант формирования целых проектов под управлением процесса управления проектами для внедрения комплексных и глобальных изменений, затрагивающих значительные ресурсы. В любом случае, это решается непосредственно в процессе внедрения самого процесса Управления релизами в каждой конкретной ситуации.

Процесс управления релизами выполняет следующие функции:

- планирование релиза;
- проектирование, разработка, тестирование и конфигурирование релиза;
- подписание релиза в развертывание;
- подготовка релиза и обучение пользователей;
- аудит оборудования и ПО до начала внедрения изменений и по завершении такового;
- размещение эталонных копий ПО в DSL;
- установка нового или усовершенствованного оборудования и ПО;
- постоянное улучшение процесса.

Для оценки качества деятельности процесса важно тщательно выбирать метрики.

По масштабу релизы подразделяются на три вида:

- большой релиз ПО и/или обновление оборудования − обычно содержит значительный объем новой функциональности, которая делает ранее сделанные исправления проблем частично или полностью избыточными. Также большой релиз обычно отменяет предшествующие малые релизы;

- малый релиз ПО и/или обновление оборудования − обычно содержит незначительные улучшения, часть из которых могли быть выполнены ранее как чрезвычайные релизы. Соответственно, эти изменения отменяются малым релизом;

- чрезвычайный релиз ПО и/или обновление оборудования — обычно содержит исправления некоторого числа известных ошибок.

По способу реализации релизы подразделяются также на три вида:

- при полном релизе все компоненты релиза разрабатываются, тестируются, распространяются и внедряются вместе. В результате увеличивается трудоемкость релиза, зато повышается вероятность того, что возможные проблемы будут обнаружены и устранены на этапе разработки и тестирования и не попадут в среду промышленной эксплуатации;

- дельта-релиз, или частичный релиз, включает в себя только новые или измененные позиции конфигурации. Например, если речь идет о программном релизе, дельта-релиз включает в себя только те модули, которые были созданы или изменены с момента прошлого релиза;

- пакетный релиз включает в себя несколько различных полных или частичных релизов, которые распространяются и внедряются совместно для снижения общего числа релизов, что облегчает работу пользователей. Сами релизы могут разрабатываться и тестироваться отдельно и быть объединенными в пакет лишь на заключительных этапах.

Особой сферой ответственности процесса управления релизами является библиотека эталонного ПО (Definitive Software Library − DSL). Все позиции DSL отражаются как записи CMDB. Эта библиотека — физическое хранилище протестированных и подготовленных к распространению копий разработанного и покупного ПО, лицензий на последнее, а также пользовательской и эксплуатационной документации. Информация о копиях ПО, хранящихся в DSL, ведется в базе данных позиций конфигурации. Наличие такой библиотеки играет важную роль в процессе управления релизами, особенно на этапе распространения и установки ПО.

Функции процесса управления релизами таковы:

- планирование релиза;
- проектирование, разработка, тестирование и конфигурирование релиза;
- подписание релиза в развертывание;
- подготовка релиза и обучение пользователей;
- аудит оборудования и ПО до начала внедрения изменений и по завершении такового;
- размещение эталонных копий ПО в DSL;
- установка нового или усовершенствованного оборудования и ПО;
- постоянное улучшение процесса.

Процессы предоставления ИТ-сервисов

Блок процессов поддержки ИТ-сервисов в соответствии с ITIL включает следующие процессы:

- процесс управления уровнем сервиса;
- процесс управления мощностью;
- процесс управления доступностью;
- процесс управления непрерывностью;
- процесс управления финансами;
- процесс управления безопасностью.

Процесс управления уровнем сервиса (Service Level Management − SLM) определяет, согласовывает и контролирует параметры ИТ-сервиса, определенные с точки зрения бизнеса, а не с точки зрения ИТ. Ключевая роль менеджера процесса – осуществление баланса между требованиями бизнеса и возможностями ИТ.

На основе каталога ИТ-сервисов данный процесс разрабатывает, согласовывает и документирует соглашение об уровне сервиса (SLA – Service Level Agreement) между менеджментом ИС-службы и бизнес-пользователями.

Основная задача процесса управления уровнем сервиса − согласование специфицированных требований к составу и параметрам ИТ-сервисов, с одной стороны, и объема ресурсов, предоставляемых ИТ-службе, − с другой. В рамках этой работы также уточняются приоритеты сервисов и ресурсов. Результатом такого согласования является формальный документ − SLA.

Соглашение об уровне сервиса необходимо периодически пересматривать поскольку информационные системы предприятия подвержены изменениям, появляются необходимость в новых сервисах, модификации или отказе от уже существующих.

Данный процесс осуществляет следующие функции:

- оценивает требования пользователей к ИТ-сервисам, распределяет их по существующим сервисам и определяет потребности в специализированных сервисах;
- согласует и документирует SLA;
- организует контроль результативности каталога сервисов в целом и уровня отдельных сервисов;
- определяет приоритетность сервисов;
- осуществляет управление версиями SLA;
- готовит планы повышения качества сервиса, направленные на повышение качества существующих сервисов, или включения в SLA новых сервисов;
- обеспечивает соответствие соглашения об уровне внутренней поддержки службы ИС (Operation Level Agreement − OLA) и субординированных контрактов ИС-службы с поставщиками оборудования, ПО и услуг;
- осуществляет постоянное улучшение процесса.

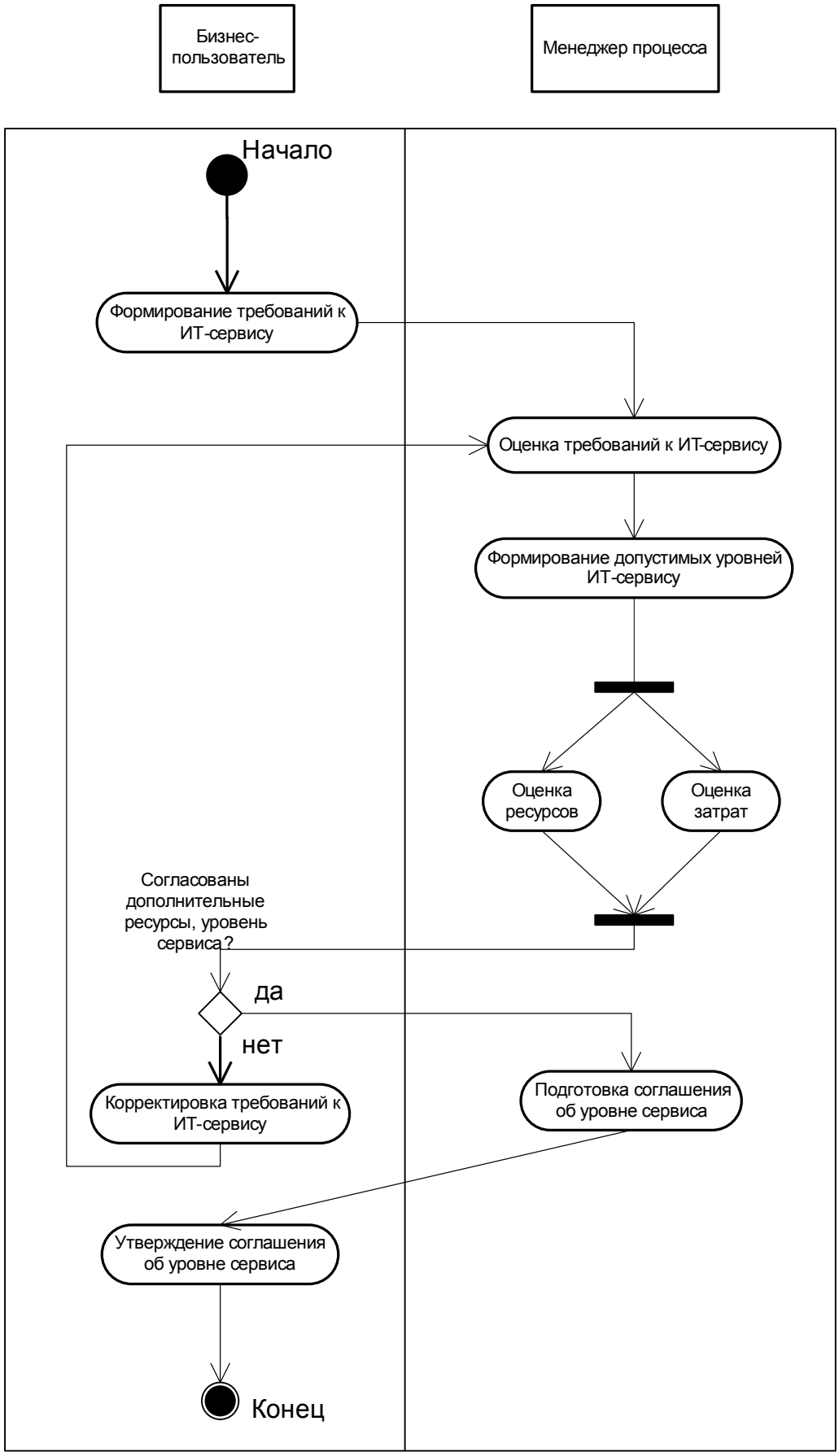

Рисунок 1.4

Бизнес-пользователь формулирует требования к ИТ-услуге. Менеджер процесса управления уровнем сервиса совместно с менеджером процесса управления мощностями уточняет данные о дополнительной потребности в

сотрудниках службы сопровождения. В рамках процесса управления затратами уточняется смета дополнительных расходов на такой сервис. Соответствующие данные передаются на рассмотрение бизнес-пользователей, при их согласии на выделение дополнительных ресурсов новый уровень сервиса и новые ресурсы фиксируются в соглашении об уровне сервиса.

Если бизнес-пользователь не согласовывает требуемые ресурсы и затраты на ИТ-сервис, то необходимо провести пересмотр требований к ИТ-сервису.

Процесс управления мощностями (Capacity Management – CAP) предназначен для оптимизации использования ресурсов ИТ-инфраструктуры в соответствии с требованиями бизнеса к уровню обслуживания и тенденциями развития инфраструктуры. Четкое определение параметров предоставления услуг и их связи с элементами инфраструктуры, формализованные требования к готовности и бесперебойности предоставления услуг, прогнозирование развития в рамках управления мощностями – все это создает основу для корректного определения стоимости предоставления каждой услуги.

Основная задача этого процесса — обеспечение устойчивой работы ИТ-сервиса с требуемым уровнем производительности при максимально возможных объемах обрабатываемых данных, оговоренных в SLA, как в текущий момент, так и будущем.

Процесс управление мощностями должен обеспечивать оптимизацию расходов, времени приобретения и размещения ИТ-ресурсов с целью обеспечения выполнения условий SLA. Данный процесс предполагает управление ресурсами, производительностью, спросом на ИТ, моделирование, планирование мощностей, управление нагрузкой и определение необходимого объема технических средств для работы приложений.

Процесс управления мощностями выполняет следующие функции:

- инвентаризует ИТ-ресурсы;
- картографирует загрузку ИТ-сервисов и требования к ней, фиксирует результаты;
- ведет анализ проблем;
- дает рекомендации в отношении аутсорсинга (в области пропускной способности);
- анализирует производительность в условиях реальной загрузки;
- определяет систему планирования пропускной способности и измерения последней;

- осуществляет постоянное улучшение процесса.

Реализация процесса управления мощностями позволяет планировать использование ресурсов и ввод в эксплуатацию оптимальным способом благодаря следующим факторам:

- рациональное управление использованием ИТ-ресурсов и технологий с целью уменьшения стоимости предоставления ИТ-услуг и снижения рисков отказов;
- структурирование процесса ввода в эксплуатацию и перераспределения ИТ-ресурсов в соответствии с потребностями бизнеса;
- анализ зависимости требований к количеству и производительности ИТ-ресурсов от специфики и вариативности бизнес-цикла;
- повышение окупаемости инвестиций за счет оптимизации использования ИТ-ресурсов, своевременного согласования требований к производительности и возможностей ИТ-ресурсов, сокращения капитальных расходов на оборудование, повышения готовности систем и увеличения производительности конечных пользователей.

Процесс управление мощностями позволяет анализировать и прогнозировать развитие ИТ-инфраструктуры предприятия за счет следующего:

- формирования в централизованном хранилище данных о производительности ИТ-ресурсов для анализа тенденций, изменений потребностей и планирования инвестиций в ИТ-инфраструктуру;
- согласования достижимого качества предоставления ИТ-услуг с учетом возможностей ИТ-ресурсов;
- моделирования и планирования сценариев оптимизации ИТ-инфраструктуры для определения требований к производительности ИТ-ресурсов при изменениях и развитии бизнеса;
- централизации и автоматизации динамического перераспределения ИТ-мощностей;
- устранения избытка или нехватки ИТ-ресурсов;
- оценки возможностей виртуализации ИТ-ресурсов;
- динамического перераспределение аппаратных и программных ресурсов на основе оперативных или прогнозируемых потребностей в производительности ИТ-ресурсов для обеспечения необходимого уровня бизнес-услуг.

Процесс управления доступностью (Availability Management – AVM) контролирует способность службы ИС обеспечить экономически

эффективный и устойчивый уровень доступности ИТ-сервисов, удовлетворяющий требованиям бизнеса.

Цель процесса управления доступностью состоит в том, чтобы оптимизировать способность ИТ-инфраструктуры, ИТ-сервисов и организаций внешних поставщиков поставлять оптимальный по стоимости уровень доступности, который позволит бизнесу удовлетворить свои бизнес цели. Эта цель достигается путём определения требований бизнеса по доступности и соответствия этих требований способностям ИТ-инфраструктуры и организаций внешних поставщиков услуг.

Под доступностью понимается способность ИТ-сервиса исполнять требуемую функцию в установленный момент или за установленный период времени. Доступность подкреплена надежностью и восстанавливаемостью ИТ-инфраструктуры и эффективностью работы организаций внешних поставщиков. Надежность ИТ-сервиса может быть точно определена как независимость от оперативного сбоя. Восстанавливаемость касается способности компонента ИТ-инфраструктуры содержаться или возвращаться к операционному состоянию.

Основная задача данного процесса − определение требований бизнеса к доступности и реализация этих требований в инфраструктуре ИТ и организации сопровождения. В тех случаях, когда требования бизнеса превышают возможности службы ИС, управление доступностью обеспечивает предоставление бизнесу возможных альтернатив и связанных с ними затрат.

Процесс управления доступностью осуществляет следующие функции:

- инвентаризация ресурсов ИТ;
- определение узких мест ИТ-сервисов с точки зрения доступности;
- анализ проблем;
- выработка рекомендаций в отношение аутсорсинга;
- анализ доступности ИТ-сервисов, в том числе при отказе оборудования, ПО, каналов связи и т.д.;
- регистрация проблем доступности, угрожающие невыполнением SLA и подготовка рекомендаций по их устранению;
- формирование системы планирования доступности и измерения последней;
- осуществление постоянного улучшения процесса.

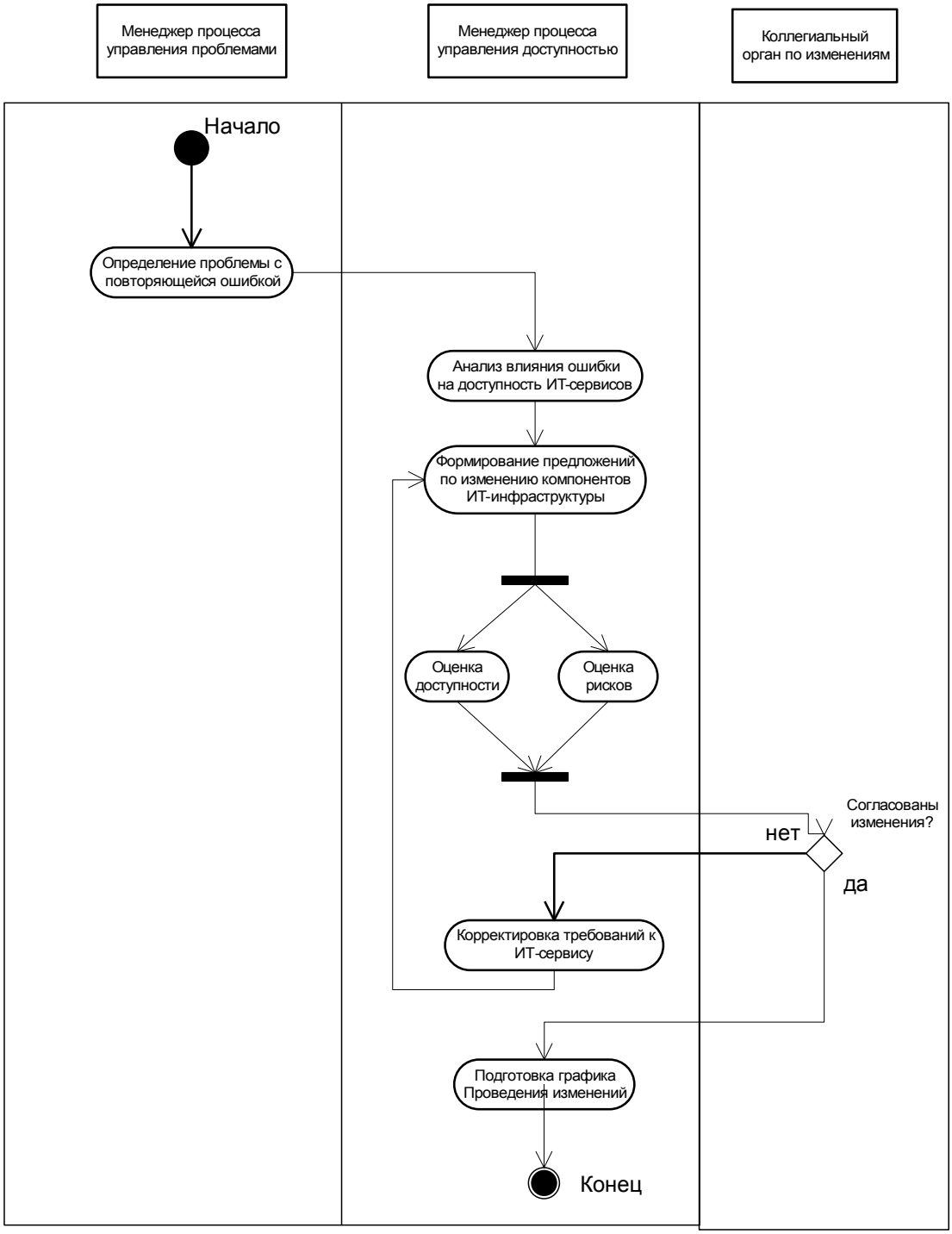

Рисунок 1.5

В рамках процесса управления доступностью сотрудник ИС-службы анализирует влияние компонентов ИТ-инфраструктуры на доступность различных сервисов и риск невыполнения SLA по этим сервисам при возникновении ошибки. На основе анализа подготавливаются предложения по изменениям ИТ-инфраструктуре. Если предложения принимаются, то подготавливается график проведения изменений.

Процесс управления непрерывностью предоставления ИТ-сервисов (IT Service Continuity Management – ITSCM) обеспечивает выполнение требований к устойчивости предоставляемых сервисов, в первую очередь необходимых для функционирования критичных бизнес-процессов.

Под устойчивостью понимается способность ИС-службы и ИТ-инфраструктуры организации поддерживать сервисы в работоспособном состоянии в случае чрезвычайных ситуаций − пожара, наводнения, других стихийных бедствий и техногенных катастроф. В SLA должны быть зафиксированы требования к предоставлению сервисов в чрезвычайных ситуациях и ресурсам для их обеспечения. Соответствующие данные должны быть предоставлены процессом управления уровнем сервиса.

Цель процесса управления непрерывностью предоставления ИТ-услуг – поддержка непрерывности бизнеса в целом. Такая поддержка означает, что, во-первых, инфраструктура и ИТ-услуги, в том числе услуги по поддержке (служба Service Desk), должны быть восстановлены за заданный период времени после возникновения чрезвычайной ситуации. Во-вторых, на время восстановления предоставление ИТ-услуг должно поддерживаться на «аварийном» уровне, приемлемом для ведения бизнеса, то есть на уровне, минимально необходимом для функционирования бизнеса. Поскольку целью процесса является поддержка бизнеса, то сфера действия процесса должна определяться в первую очередь исходя из целей бизнеса.

Согласно ITIL процесс отвечает за решение следующих основных задач:

- оценка воздействия нарушений в предоставлении ИТ-услуг при возникновении чрезвычайной ситуации;
- определение критичных для бизнеса ИТ-услуг, которые требуют дополнительных превентивных мер по обеспечению непрерывности их предоставления;
- определение периода, в течение которого предоставление ИТ-услуги должно быть восстановлено;
- определение общего подхода к восстановлению ИТ-услуги;
- разработку, тестирование и поддержку плана восстановления ИТ-услуги с достаточным уровнем детализации, который поможет пережить чрезвычайную ситуацию и восстановить нормальную работу за заданный промежуток времени.

Процесс управления финансами ИТ-службы (Financial Management) отслеживает фактические затраты в разрезе заказчиков, ИТ-сервисов и пользователей и на этой основе рассчитывает внутренние цены на услуги ИС-службы. Процесс взаимодействует с процессом управления уровнем сервиса для определения цен сервисов.

Основные цели процесса состоит в следующем:

- сформировать информацию о полных стоимостях предоставляемых ИТ-сервисов, с целью повышения производительности и эффективности работы ИТ-службы;

- упорядочить поведение клиентов, предоставляя им информацию о действительной стоимости ИТ-сервисов;
- обеспечить возврат затрат на предоставление ИТ-сервисов.

Основная задача процесса управления затратами − расчет издержек, связанных с ИТ-сервисами, цен сервисов для бизнес-пользователей и поиск путей снижения затрат.

Функциями данного процесса являются:

- прогноз затрат и выручки (последняя определяется на основании внутренних цен на услуги);
- разработка бюджета сервисов;
- анализ использования сервисов и связанных с этим издержек, поиск путей их снижения;
- калькулирование счета и выставление его бизнес-пользователям, получение платежей;
- расчет совокупной стоимости владения (ССВ) ИТ-сервисов;
- установление системы ценообразования и выставление счетов за услуги;
- установление системы управления затратами;
- установление механизма привлечения инвестиций;
- осуществление постоянного улучшения процесса.

Процесс управления финансами касается экономических вопросов предоставляемых ИТ-услуг. Например, данный процесс подготавливает информацию о расходах, возникших при предоставлении услуг. В результате при определении необходимых изменений ИТ-инфраструктуры возможен учет финансовых факторов (соотнесение расходов и доходов – цены и результата). Эта деятельность повышает информированность о расходах (где возникают издержки и какие) и может использоваться также при составлении бюджета. Управление финансами ИТ-службы описывает различные методы выставления счетов, включая определение цели выставления счетов за ИТ-услуги и определение ценообразования, а также аспекты бюджетирования.

Процесс управления безопасностью (Security Management) обеспечивает внедрение, контроль и техническую поддержку инфраструктуры безопасности, а также разработку и контроль соблюдения стандартов безопасности существующих, разрабатываемых и планируемых ИТ-сервисов. В ряде случаев он рассматривается вне рамок процессов предоставления ИТ-сервисов

Основная задача процесса управления безопасностью − планирование и мониторинг безопасности ИТ-сервисов.

Функции процесса управления безопасностью таковы:

- разработка корпоративной политики безопасности в части ИС, обеспечение необходимого уровня безопасности в этой области;
- анализ проблем безопасности и рисков в этой области;
- аудит безопасности и оценка инцидентов в этой области;
- установление процедур безопасности, включая защиту от вирусов;
- выбор систем и инструментов поддержания безопасности;
- постоянное улучшение процесса.

Таким образом, блок процессов поддержки ИТ-сервисов обеспечивает разработку новых ИТ-сервисов при обеспечении целостности и согласованности ИТ-инфраструктуры предприятия. ИТ-инфраструктура как целое оптимизируется по пропускной способности и затратам при заданном уровне производительности и устойчивости ИТ-сервисов. Вновь разработанные ИТ-сервисы передаются на одобрение в процесс управления изменениями и в случае одобрения предложений передаются в блок процессов разработки и внедрения сервисов.

В терминах функций ИС-службы блок процессов поддержки ИТ-сервисов является ядром выполнения функции планирования и организации работ, с одной стороны, и мониторинга − с другой. В функции планирования реализуются задачи планирования основного объекта управления − ИТ-сервисов. В функции координации работ процессы данного блока обеспечивают согласование потребностей бизнес-подразделений, возможностей информационных систем и стоимости сервиса для бизнес-подразделения. Результатом такого согласования становится спецификация ИТ-сервиса. В области мониторинга данные роли обеспечивают контроль процессов ИС-службы с точки зрения основных инженерных областей − безопасности, устойчивости и пропускной способности.

Соглашение об уровне сервиса

Основным документом, регламентирующим взаимоотношения ИС-службы и бизнес-подразделений предприятия, является соглашение об уровне сервиса (Service Level Agreement – SLA). В данном документе дается качественное и количественное описание ИТ-сервисов, как с точки зрения службы ИС, так и с точки зрения бизнес-подразделений.

Соглашение об уровне сервиса определяет взаимные ответственности поставщика ИТ-сервиса и пользователей этого сервиса.

Типовая модель SLA должно включать следующие разделы:

- определение предоставляемого сервиса, стороны, вовлеченные в соглашение, и сроки действия соглашения;
- доступность ИТ-сервиса;
- число и размещение пользователей и/или оборудования, использующих данный ИТ-сервис;
- описание процедуры отчетов о проблемах;
- описание процедуры запросов на изменение.

Спецификации целевых уровней качества сервиса, включая:

- средняя доступность, выраженная как среднее число сбоев на период предоставления сервиса;
- минимальная доступность для каждого пользователя;
- среднее время отклика сервиса;
- максимальное время отклика для каждого пользователя;
- средняя пропускная способность;
- описания расчета приведенных выше метрик и частоты отчетов;
- описание платежей, связанных с сервисом;
- ответственности клиентов при использовании сервиса (подготовка, поддержка соответствующих конфигураций оборудования, программного обеспечения или изменения только в соответствии с процедурой изменения);
- процедура разрешения споров, связанных с предоставлением сервиса.

Существенной частью SLA является каталог сервисов. Каталог ИТ-сервисов представляет собой документ, в котором сформулированы все ИТ-сервисы, предоставляемые пользователям, при необходимости указывается цена услуги, общий порядок обращения за услугой. Каталог включает информацию описательную и операционную.

Как правило, в описывающей части содержится следующая информация:

- имя сервиса;
- ссылки на связанные сервисы;
- описание сервисов, функций, границ предоставления сервисов, профилей пользователей;
- поддерживаемые платформы или инфраструктуры;

- характеристики доступности, производительности;
- процедуры поддержки;
- метрики;
- процедуры мониторинга.

В операционной части приводят:

- имя владелец сервиса;
- профиль клиента;
- зависимости от других сервисов;
- модель Operations Level Agreement (OLA);
- детальная информация о технической инфраструктуре, необходимой для обеспечения сервиса;
- единицы инфраструктуры, рассматриваемые как активы;
- план поддержания целостности, улучшения качества сервисов, развития возможностей;
- результаты аудита;
- информация о ценах.

SLA позволяет установить формализованные критерии оценки результатов деятельности ИС-службы, установить единообразные и обязательные для всех участников процесса процедуры оценки результатов деятельности ИС-службы.

Сервисный подход к управления ИС-службой требует определенной зрелости как для самой ИС-службы, так и для бизнес-заказчиков. При этом следует учитывать ряд факторов:

- требуется определенный уровень развития управления процессами и сервисами ИТ-службы предприятия, который предполагает, что процессы и ИТ-сервисы являются измеримы;
- бизнес должен быть готов воспринимать некоторые «стандартные услуги» ИТ-службы как набор управляемых сервисов, выдвигать адекватные требования к уровню качества их предоставления, участвовать в повышении их качества;
- обеспечение прозрачности ценообразования ИТ-сервисов, при которой ИТ-служба должна обосновывать формирование цены ИТ-сервиса и возможные пути её снижения;

- наличие исключительных ситуаций, которые трудно предусмотреть заранее, процедуры выхода из них;
- процессы, люди, взгляды подвержены изменениям. SLA, как и бизнес, должен адекватно изменяться при изменении внутренних и внешних факторов.

Следует отметить, что модель ITSM может применяться для предприятий с ИТ-службами различного размера: от 1 – 5 сотрудников до нескольких десятков сотрудников.

Для малых предприятий ролевой подход, принятый в ITSM, допускает совмещение одним и тем же сотрудником сколь угодно большого количества ролей в пределах его возможностей и компетенции. В предельном случае модель ITSM может использовать ИС-служба, состоящая из одного человека. Инструментальные программные средства, которые используются для управления ИТ-инфраструктурой, могут варьироваться в широких пределах: от офисных пакетов, в простейшем случае, до специализированных инструментальных средств при большом размере ИС-службы.

Information Technology Service Management (ITSM)

Концепция Управления ИТ-службами — Information Technology Service Management (ITSM) разработана компанией Hewlett-Packard, является подходом к построению и организации работы службы ИТ с целью наиболее эффективного решения бизнес - задач компании. При данном подходе, ИТ отдел должен не просто обслуживать ИТ - инфраструктуру, а выступать как поставщик ИТ - услуг бизнес подразделениям компании. ITSM - можно рассматривать, как эталонную модель для управления ИТ – услугами на предприятии. Для построения данной модели были использованы лучшие рекомендации из библиотеки ИТ - инфраструктуры (ITIL).

Считается, что при разработке эталонной модели ITSM был отобран весь практический опыт, описанный в публикациях ITIL, который может быть применим на предприятиях, а также опыт консультантов HP со всего мира, полученный ими на практике при разработке и внедрении решений для управления услугами, как внутри HP, так и в компаниях-клиентах HP.

В соответствии с концепцией ITSM ИТ - отдел перестает быть вспомогательным элементом для основного бизнеса компании, ответственным только за работу отдельных серверов, сетей и приложений, применяющихся в компании. ИТ – подразделение становился элементом эффективного функционирования предприятия и предоставляет бизнес подразделениям информационные услуги. Отношения между ИТ подразделением и бизнес подразделением формализуются как отношения «поставщик услуг – потребитель услуг».

В руководствах по ITSM выделяются три основных элемента концепции:

- формализация процессов функционирования информационных технологий;
- профессионализм и четкая ответственность сотрудников ИТ - отдела за определенный круг задач;
- технологическая инфраструктура обеспечения качества услуг:
    - информационные технологии, служба поддержки пользователей;
    - служба управления конфигурациями и изменениями;
    - система контроля услуг;
    - служба тестирования и внедрения новых услуг и т.д.

Примерами ИТ – процессов могут служить: установка нового ПО, ликвидация проблем в сети, процесс перехода на новую резервную систему. В концепции ITIL считается, что недокументированные процессы являются результатом неконтролируемых изменений, что впоследствии может привести к существенным сбоям в предоставлении сервиса. Неэффективные процессы ИТ подразделения также влияют на рациональность использования ресурсов и время вывода новых услуг для пользователей.

В основе использования концепции ITSM лежит разработка формализованных процессов ИТ подразделения. Для каждого процесса необходимо описать последовательность операций, необходимые ресурсы, затраты по времени, способы контроля качества.

При разработке концепции ITSM аналитики Hewlett-Packard выделили пять групп процессов:

- Привязка ИТ к бизнес процессам обеспечивает взаимодействие между ИТ подразделением и бизнес подразделениями и позволяет не только разработать дальнейшую стратегию развития информационных технологий, но и провести анализ потенциальных услуг.
    - Оценка бизнеса (Business Assessment). Процесс производит анализ существующих информационных систем и основных тенденций развития информационных технологий, что позволяет создать новые услуги, соответствующие требованиям бизнеса.
    - Управление клиентами (Customer Management) обеспечивает возможность прогнозировать их поведение и потребности, оценивать степень удовлетворенности.
    - Разработка стратегии ИТ (IT Strategy Development) один из ключевых процессов в функционировании ИТ подразделения, обеспечивающий разработку стратегии в соответствии с

требованиями бизнеса и тенденциями развития информационных технологий.

- Проектирование и управление услугами включает в себя набор бизнес процессов обеспечивающих разработку конкретных услуг в соответствии со спецификациями, определяющими качество, производительность, стоимость.
    - Планирование услуг (Service Planning). Процесс обеспечивает планирование и проектирование стандартных и специализированных сервисов, вывод из эксплуатации устаревших, анализ рисков.
    - Управление качеством услуг (Service Level Management) обеспечивает согласование уровня сервиса между поставщиком и потребителем. Процесс обеспечивает оценку требований пользователей к услугам, разработку и согласование SLA.
    - Управление доступностью (Availability Management). Процесс обеспечивает поддержку работоспособности сервисов в случае чрезвычайных ситуаций, проводит анализ проблем и рисков для обеспечения отказоустойчивости.
    - Управление производительностью (Capacity Management) – контролирует уровень нагрузки на сервисы и обеспечивает необходимый уровень производительности в соответствии с требованиями бизнеса.
    - Управление затратами (Cost Management) оценивает затраты на ИТ подразделения, рассчитывает внутренние цены на сервисы в соответствии со стоимостью их разработки и поддержки.
- Разработка сервисов и внедрение (Service Development & Deployment) – обеспечивает внедрение и ввод новых информационных систем в эксплуатацию, модернизацию уже существующих информационных систем для поддержки набора необходимых сервисов.
    - Разработка и тестирование (Build & Test). В рамках данного процесса происходит приобретение, разработка, настройка, тестирование новых информационных систем и их обновлений обеспечивающих поддержку сервисов. Цель данного процесса заключается в реализации сервиса.
    - Процесс ввода в эксплуатацию (Relies to Production) обеспечивает внедрение новых сервисов на предприятии (прошедших процедуру тестирования) для всех пользователей.

- Эксплуатация (Operation) обеспечивает управление основными текущими процессами ИТ подразделения, обеспечивающими поддержку существующих сервисов.
    - Управление операциями (Operations Management) включает в себя набор процедур, направленных на управление информационными системами и включает в себя: мониторинг ресурсов, администрирование программно - аппаратного обеспечения, обеспечение безопасности.
    - Управление инцидентами (Incident Management) обеспечивает поддержку пользователей и восстановление сервисов в случае возникновения инцидентов, отслеживает процесс разрешений инцидентов.
- Управление проблемами (Problems Management) ориентировано на минимизацию количества сбоев в программно - аппаратном обеспечении. В рамках процесса происходит анализ числа инцидентов, регистрация проблем, выявление причин возникновения и их устранение.

Предоставление сервисов является основной группой процессов в методологии ITSM, которая обеспечивает стабильность функционирования всей ИТ - инфраструктуры и включает в себя:

- Управление изменениями (Change management) обеспечивает анализ всех планируемых изменений в рамках ИТ - инфраструктуры компании, определяет их влияние на сервисы и конфигурационные единицы, оценивает риски.
- Управление конфигурацией (Configuration management) собирает, регламентирует, контролирует информацию по всем существующим конфигурационным единицам, релизам, инцидентам, проблемам.

Использование концепции ITSM существенно зависит от организации самого проекта, от того, насколько четко организовано взаимодействие между людьми, насколько они правильно понимают свои роли в функционировании ИТ подразделения; от детализации процессов и четкого понимания их целей; от технологий, использующихся для автоматизации функционирования ИТ подразделения.

Следует отметить, что проблемы в ИТ подразделениях по всему миру, связанные с разработкой, внедрением и поддержкой информационных систем привлекли внимание большого числа производителей программно - аппаратного обеспечения по всему миру.

IT Process Model (ITPM)

Модель информационных процессов ITPM (IT Process Model), возникла из модели управления архитектурой ISMA (Information Systems Management Architecture), предложенной IBM в 1979 году. Модель ITPM, отличается от ITIL не только по способу деления процессов, но и по ряду терминологических моментов. В реальности, ITPM — не модель в её практическом понимании, а среда разработки прикладной модели.

ITPM включает семь групп процессов по числу факторов, влияющих на успех любого ИТ-проекта:

- улучшение взаимодействия с клиентами;
- обеспечение управленческих систем корпоративной информа-цией;
- управление ИТ-инфраструктурой с точки зрения потребностей бизнеса;
- реализация и развертывание решений;
- обеспечение ИТ-сервисами;
- поддержка ИТ-сервисов и решений;
- управление ИТ-ресурсами и ИТ-инфраструктурой.

Успешное управление ИТ-сервисами немыслимо без четко определенных процессов взаимодействия с клиентами. ИТ-служба путем формирования разнообразных отчетов о положении дел с обслуживанием, может улучшить все формы работы с бизнес-пользователями, включая преобразование запросов в конкретные решения, обеспечение их поддержкой, что, в конечном итоге, будет способствовать повышению уровня обслуживания. Это обеспечивается составлением и соблюдением соглашений об уровне обслуживания SLA в терминах, понятных обеим сторонам.

Обеспечение управленческих систем корпоративной информацией необходимо для повышения эффективности процесса принятия решений, обеспечивающего достижение максимальной отдачи от инвестиций. Задачи построения и развития ИТ-инфраструктуры предприятия должны быть централизованы и согласованы с задачами бизнеса, а также перспективными планами подразделений (например, отдел сбыта не заинтересован в увеличении товарных запасов и старается как можно быстрее их реализовать, однако для целей маркетинга в течение всего года будут требоваться образцы продукции, которых в нужный момент на складе просто не окажется). Централизация информации позволяет высшему руководству адекватно оценивать влияние каждого фактора на общие результаты бизнеса. ИТ-служба, отвечающая за обеспечение централизации, должна понимать бизнес-цели предприятия и принципы достижения этих целей, предлагая, в частности, план взаимодействия, оценки нагрузки на ИТ-инфраструктуру и т.п.

Управление ИТ-инфраструктурой с точки зрения бизнеса предполагает оценку эффективности работы ИТ-службы по её вкладу в конечный результат деятельности бизнес-подразделений предприятия. Менеджмент ИТ-службы должен понимать цели бизнеса, способы их достижения и рассматривать деятельность ИТ-службы как обеспечивающего подразделения предприятия, способствующего достижению целей бизнес-подразделений. ИТ-директор должен ориентироваться в приоритетах выделения ресурсов для удовлетворения запросов бизнес-пользователей в соответствии со структурой бизнеса и при соблюдении корпоративных стандартов. Также требуется определять объем услуг, план мероприятий с оценкой их эффективности, а также оперативности, с которой ИТ-служба сможет отреагировать на изменения бизнесе.

Реализация и развертывание решений в ИТ-инфраструктуре предприятия должны подвергаться всестороннему анализу с точки зрения влияния на бизнес и рисков, связанных с этими решениями. Процедура внедрения решений должна быть унифицирована и выполняться примерно одинаково, как при развертывании системного программного обеспечения, так и при установке оборудования, бизнес-приложений и баз данных. Развертывание нового решения внутри уже существующей конфигурации должно осуществляться с минимальными нарушениями работоспособности последней. Особую роль в успешном внедрении играет управление изменениями: требуется идентифицировать все задачи, имеющие отношение к каждому конкретному изменению и контролировать их; необходим анализ результатов изменений; ведение базы изменении полезен также план координации всех технологических изменений внутри организации с целью выполнения максимального количества изменений при минимальных нарушениях работоспособности бизнеса. Также важна оценка рисков для бизнеса в случае возникновении сбоев при внедрении

Обеспечение услугами бизнес-пользователей является одним из основ-ных направлений реализации модели ITPM. ИТ-сервисы могут требовать для своей поддержки разных ресурсов и дисциплин работы, выполняться с разными приоритетами. Необходим мониторинг процесса доставки ИТ-сервисов для выявления потенциальных нарушений и предотвращения сбоев критически важных функций. Благодаря интеграции этот процесс может выполняться автоматически или вручную через администратора. Задача ИТ-службы — предложить структуру доставки ИТ-сервисов и план, в котором должно быть указано место и время их предоставления, а также перечень необходимых ресурсов. Для составления такого плана ИТ-служба через единую точку входа осуществляют взаимодействие с клиентом, получают все запросы на ИТ-услуги, выполняют их анализ и интеграцию для выделения ресурсов. Предоставление ИТ-сервисов должно сопровождаться управлением изменениями в запросах пользователей:

- требуется идентифицировать факторы, важные для бизнеса и способные его улучшить;

- понять, что в первую очередь требуется для бизнес-клиентов;
- определить адекватные метрики оценки степени удовлетворенности пользователя;
- наметить и реализовать план мероприятий по улучшению обслуживания.

Для поддержки ИТ-сервисов и решений задачу ИТ-служба должна проводить ежедневный мониторинг процесса доставки услуг:

- слежение за доступностью системы;
- разрешение проблем;
- измерение производительности;
- ведение базы данных по конфигурации системы;
- выполнение резервного копирования;
- оценка необходимости своевременного масштабирования систе-мы.

Управление ИТ-ресурсами и ИТ-инфраструктурой предполагает мониторинг всех критически важных ресурсов, включая технологии и квалификацию персонала, необходимую для сопровождения текущей конфигурации, а также управление финансами, выделенными на развитие ИТ-инфраструктуры предприятия. Управление ИТ-инфраструктурой подразумевает работы по инвентаризации:

- лицензии на программное обеспечение и информационные ре-сурсы;
- замеры времени, необходимого для выполнения того или иного процесса;
- соблюдение политики безопасности.

Microsoft Operations Framework и Microsoft Solution Framework

В конце 90ых годов прошлого века многие крупные компании начали разработку собственных концепций управления ИТ подразделением. Естественно корпорация Microsoft не осталась в стороне от этого процесса и в 2000 году предложила опирающуюся на ITIL методологию Microsoft Operations Framework (MOF) дополнения и изменения, внесенные в MOF по сравнению с ITIL, позволяют использовать ее в гетерогенных средах.

Следует отметить, что набор методик Microsoft в настоящий момент ориентирован на разработку конкретных программных прикладных систем и создание технологической инфраструктуры. Именно поэтому методика Microsoft Operations Framework неразрывно связана с методикой Microsoft

Solution Framework ориентированной на разработку и внедрение информационных систем.

Microsoft Operations Framework (MOF) - это методология, описывающая процесс эксплуатации информационных систем для достижения максимальной надежности и доступности.

Microsoft Solution Framework (MSF) - пакет руководств по эффективному проектированию, разработке, внедрению и сопровождению информационных систем.

Аналитики Microsoft считают, что для эффективной работы ИТ подразделения необходимо определять текущие потребности бизнес подразделения в сервисах и услугах, эффективно использовать существующие технические решения для предоставления этих услуг.

MOF и MSF дополняют друг друга, сокращая период вывода новых информационных услуг в эксплуатацию, используют общую терминологию и концепцию, обеспечивая создание «высококачественных решений».

Microsoft Operations Framework (MOF)

Microsoft Operations Framework (MOF) состоит из набора статей, руководств, служб, материалов обучающих курсов и включает в себя три основные модели: Microsoft Operations Framework позволяет получить общую структуру бизнес процессов всего ИТ подразделения, включающую внедрение информационных систем и предоставление ИТ услуг.

На своем сайте Microsoft позиционирует методику, как практическое пособие для ежедневного использования. которая помогает внедрить «надежные и эффективные по цене ИТ сервисы. Рекомендации MOF касаются вопросов персонала, процессов, технологий и стратегии управления в сложных, распределённых, гетерогенных ИТ средах. MOF можно назвать расширением приёмов и методик, предусмотренных ITIL».

В основе модели процессов MOF заложены следующие определения:

- Решения – средства и возможности, появившиеся у организации в результате применения ИТ - технологий.
- Релиз – группа изменений, которую команда, обслуживающая ИС, внедряет в рабочее окружение как единое целое.
- Управление ИТ - услугами – применение структурированного набора процессов, призванных гарантировать качество важных ИТ - услуг, для достижения уровня обслуживания, согласованного с заказчиком.

Модель процессов описывает процессы управления обслуживанием информационных систем и считает, что команда обслуживающая

информационную систему ответственна за все изменения в существующей инфраструктуре.

В методике Microsoft Operations Framework бизнес процессы ИТ подразделения упорядочены в виде «функций управления ИТ – услугами», или другими словами их называют SMF-функции.

SMF-функция (Service management function) – функция управления услугами. Эти функции свойственны большинству решений, имеющих место на протяжении жизненного цикла каждого релиза. Функции разделены на четыре группы. Каждая группа функций соответствует определенному этапу жизненного цикла услуги.

Microsoft Operations Framework 4.0 отличается от предыдущих версий и выделяет следующие четыре этапа жизненного цикла ИТ услуг:

- Этап планирование обеспечивает оптимизацию, разработку стратегии и предоставление сервисов в соответствии с требованиями бизнеса. На этапе планирования определяется, как ИТ служба будет предоставлять услуги. При этом необходимо найти баланс между качеством, надежностью и стоимостью предоставляемых услуг. Этап планирования включает в себя следующие функции: выравнивание; надежность; политика; управление финансами.

- Этап внедрение обеспечивает разработку, настройку, развертывание и оптимизацию программно - аппаратных средств, обеспечивающих предоставление сервисов. Внедрение нового сервиса можно рассматривать в виде самостоятельного проекта. В этом случае аналитики Microsoft рекомендуют воспользоваться методологией Microsoft Solutions Framework (MSF), для разработки программного обеспечения, управлением процессами Capability Maturity Model Integration (CMMI), или методикой, разработанной институтом Project Management Institute (PMI). Этап внедрения включает в себя следующие функции: предварительное планирование; планирование проекта; создание; стабилизация; развертывание.

- Этап эксплуатация обеспечивает «оптимальное использование, обслуживание и поддержку ИТ - услуг в соответствии с потребностями и ожиданиями компании». В рамках данного этапа производится мониторинг состояния каждой из существующих услуг и восстановление эксплутационного состояния услуги в случае возникновения сбоев. В рамках этого этапа ведется эксплуатация существующих программно - аппаратных комплексов и поддержка пользователей. Этап эксплуатации включает в себя следующие функции: операции; мониторинг и контроль услуг; обслуживание заказчиков; управление проблемами.

- Уровень управление описывает набор основных рекомендаций по предоставлению услуг и включает такие понятия, как управление

информационными технологиями, оценка рисков, роли и обязанности, управление изменениями и конфигурациями на всех этапах жизненного цикла услуги. Функции управления являются основой для всех этапов жизненного цикла информационных технологий, поэтому аналитики Microsoft вынесли его в отдельный уровень. Уровень управления включает в себя следующие функции: управление, риски и соответствие нормативным требованиям; изменение и конфигурация; рабочая группа.

Для оценки состояния ИТ - услуг и контроля их готовности к переходу на следующих этап используется управленческий анализ, который включает в себя следующий набор функций, распределенных по различным этапам:

- Согласование услуги (этап планирование).
- Портфолио (этап планирование).
- Утверждения плана проекта (этап внедрение).
- Готовность релиза (этап внедрение).
- Эксплутационное состояние (этап эксплуатация).
- Политика и контроль (этап управление).

Microsoft Solution Framework (MSF)

Microsoft Solution Framework (MSF) - пакет руководств по эффективному проектированию, разработке, внедрению, включает в себя следующие модели:

- Модель процессов
- Модель проектной группы
- Дисциплина управления рисками
- Дисциплина управления проектами
- Дисциплина управления подготовкой

Особенностью Microsoft Solution Framework считается высокий уровень гибкости и отсутствия жестких процедур, что позволяет решать широкий круг проблем, появляющихся при разработке и внедрении информационных систем. Аналитики Microsoft считают что «главными принципами MSF можно назвать производительность, интегрируемость и расширяемость».

Считается, что для внедрения и разработки различного программного обеспечения не существует единой оптимальной методологии. Microsoft Solution Framework ориентирован, в первую очередь, на оптимальное управление процессом разработки и внедрения.

Модель процессов описывает общую методологию разработки и внедрения информационных систем и включает в себя стадию разработки концепции проекта, плана проекта, разработку решения, внедрения релизов, тестирование. Также в модель процессов входит подготовка документации и обучение пользователей работе с новым программно – аппаратным обеспечением.

В модели процессов выделяют определенные ключевые точки проекта (в Microsoft их называют – milestones - вехи). Данные ключевые точки определяют промежуточный или конечный результат, который может быть оценен и проанализирован. Считается, что ключевые точки проекта могут изменяться в соответствии с требованиями к проекту.

Каскадная модель описывает последовательное выполнение процесса разработки и внедрения программного обеспечения. Каждый процесс (анализ, проектирование, реализация, тестирование, интеграция, поддержка) начинается строго после окончания предыдущего процесса.

Спиральная модель учитывает необходимость постоянных изменений в момент проекта. Различные этапы разработки и внедрения могут происходить одновременно, что существенно сокращает время вывода продукта.

Считается, что аналитики Microsoft объединили в себе принципы спиральной и каскадной модели разработки и внедрения программного обеспечения. Они разделили цикл спиральной модели разработки на последовательные бизнес - процессы. При этом функциональность программного продукта наращивается поэтапно (версионно). На первом этапе создается первая версия продукта, включающая базовую функциональность. В следующих версиях происходит увеличение функциональности в соответствии с требованиями бизнеса.

Microsoft Solution Framework предполагает создание «живой документации», которая изменяется по мере эволюции проекта. На этапе разработки концепции документация распространяется исключительно среди членов проектных групп. По мере подключения дополнительных специалистов к реализации проекта они получают возможность ознакомиться с проектной документацией и внести изменения в часть документов, попадающих в их зону ответственности. Измененная документация попадает на проверку всем заинтересованным сторонам и описанный процесс повторяется.

Создание базовых версий программных продуктов позволяет членом команды начать разработку в максимально короткие сроки. При этом необходимо «как можно чаще собирать текущие версии всех компонентов решения для проведения тестирования и анализа». Большие проекты рекомендуется разделять на множество маленьких. Каждый локальный проект разрабатывается и тестируется отдельной командой.

При использовании подхода Microsoft для разработки программного обеспечения необходимо использовать процесс управления конфигурациями (configuration management). Данный процесс обеспечивает мониторинг за состоянием различных версий программного продукта и его документации. Следует отметить, что управление конфигурациями в Microsoft Solution Framework, не имеет ни какого отношения к схожему по названию процессу из Microsoft Operations Framework.

Microsoft Solution Framework - закрывает весь процесс разработки решения и включает пять основных фаз, «каждая фаза заканчивается главной вехой, результаты которой становятся видимыми за пределами проектной команды».

Фаза выработки концепции описывает процесс создания проектной группы, выработка высокоуровневого взгляда на цели и условия проекта. По завершению этой фазы определяются общие задачи проекта, описывается требуемая функциональность, ограничения по времени.

Фаза планирования описывает набор работ по составлению планов проекта. Происходит подготовка спецификаций, разработка дизайна, оценка проектных затрат и сроков разработки. Функциональные спецификации и календарный план - график проекта необходимы для определения жестких рамок проекта.

Фаза разработки включает процесс подготовки определенной версии программного продукта и документации к нему. Следует отметить, что некоторая часть этой работы может быть выполнена на фазе стабилизации программного продукта.

Фаза стабилизации обеспечивает тестирование программного продукта. В соответствии с моделью команд MSF тестированием и разработкой не могут заниматься одни и те же специалисты. На данном этапе тестировщики выполняют поиск ошибок, а проектная группа занимается их устранением.

Фаза внедрения включает установку всех компонентов решения и их запуск в эксплуатацию. После приемки программного продукта в эксплуатацию ответственность переходит от проектной группы к службе поддержки программного продукта. Следует отметить, что при возникновении проблем с программным продуктом, проектная группа может принимать участие в их устранении.

Модель проектной группы описывает состав распределенной команды разработчиков, определяет ролевые функции, их области компетенции и зоны ответственности. В соответствии с MSF проектные группы строятся, как небольшие команды, члены которых распределяют ответственность между собой.

Управление рисками включает в себя непрерывное оценивание рисков и использование информации о рисках в рамках процесса принятия решений на протяжении всего жизненного цикла проекта.

Управление проектами это набор методик Microsoft, ориентированный на оптимизацию работы по проектам и взаимодействиями в проектной группе. Одной из основных особенностей методики является отсутствие в проектной команде должности проджект - менеджера. При этом ответственность за управление проектом распределена между лидерами различных ролевых кластеров внутри команды.

Управление подготовкой обеспечивает управление знаниями в рамках проекта разработки программного обеспечения. Модель определяет набор шагов, обеспечивающих, с точки зрения аналитиков Microsoft, стремление членов команды к повышению своей квалификации.

Глава 2. Средства автоматизации управления ИТ-инфраструктурой

Программные решения HP OpenView

Программные решения HP OpenView, предназначенные для централизованного управления ИТ-ресурсами предприятия, обеспечивают прозрачность управления и тесную интеграцию с бизнес-процессами.

Набор решений HP OpenView включает:

- управление бизнесом (Business Service Management – BSM);
- управление приложениями (Application Management);
- управление ИТ-службой (IT Service Management);
- управление ИТ-инфраструктурой (Infrastructure Optimization solutions);
- управление перекрестными функциями.

Управление бизнесом

Решение HP OpenView *управление бизнесом* обеспечивает связь информационных технологий предприятия с основным бизнесом. Это решение содействует повышению эффективности использования информационных технологий в бизнесе. Решение BSM позволяет прояснить как информационные технологии могут содействовать успеху ключевых бизнес-процессов предприятия, согласовать текущую деятельность ИТ-службы с потребностями бизнеса, расставить приоритеты использования ИТ-ресурсов и оптимизировать инвестиции в ИТ-инфраструктуру.

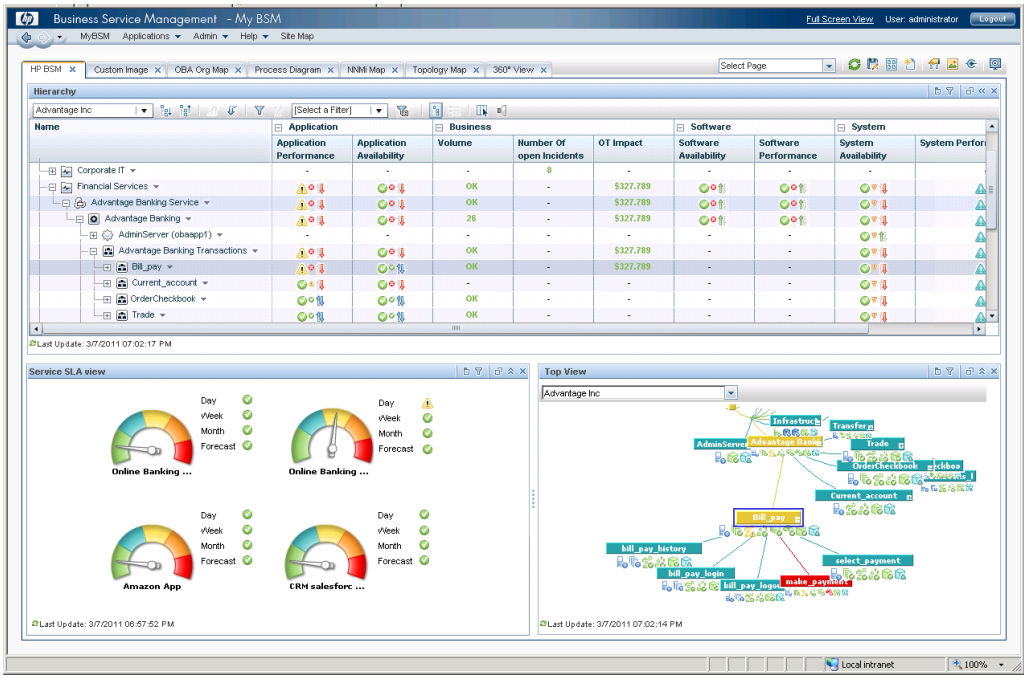

Рисунок 2.6

Управление приложениями

Решение HP OpenView *управление приложениями* дает возможность обеспечить необходимую доступность и производительность приложений, поддерживающих основные бизнес-процессы. Для этого используется мониторинг уровней обслуживания ИТ-сервисов (время отклика по транзакции, коэффициенты загрузки ресурсов информационной системы). Это позволяет идентифицировать проблемы до момента их возникновения, установить им приоритеты и с упреждением решать проблемы с меньшим количеством ресурсов.

Управление ИТ-службой

Решение HP OpenView *управление ИТ-службой* поддерживает переход ИТ-службы предприятия на процессную основу и содержит следующие программные решения:

- управление активами (Asset Management);
- управление конфигурациями (Configuration Management);
- управление объединенными событиями и производительностью (Consolidated Event and Performance Management);
- управление идентификацией (Identity Management);
- поддержка пользователей (Consolidated Service Desk).

Решение *управление активами* обеспечивает контроль и оптимизацию ИТ-ресурсов в каждой стадии жизненного цикла ИТ-сервиса. Эти решения предполагают:

- управление затратами на ИТ посредством автоматизации учета ИТ-активов, их стандартизации, управления расходами, покупками, контрактами и более эффективным использованием активов;
- управления программными активами, с целью контроля лицензий и оптимизации закупок новых лицензий;
- интеграцию управления ИТ-активами с ERP-системой, управления ИТ-сервисами и другими бизнес-системами.

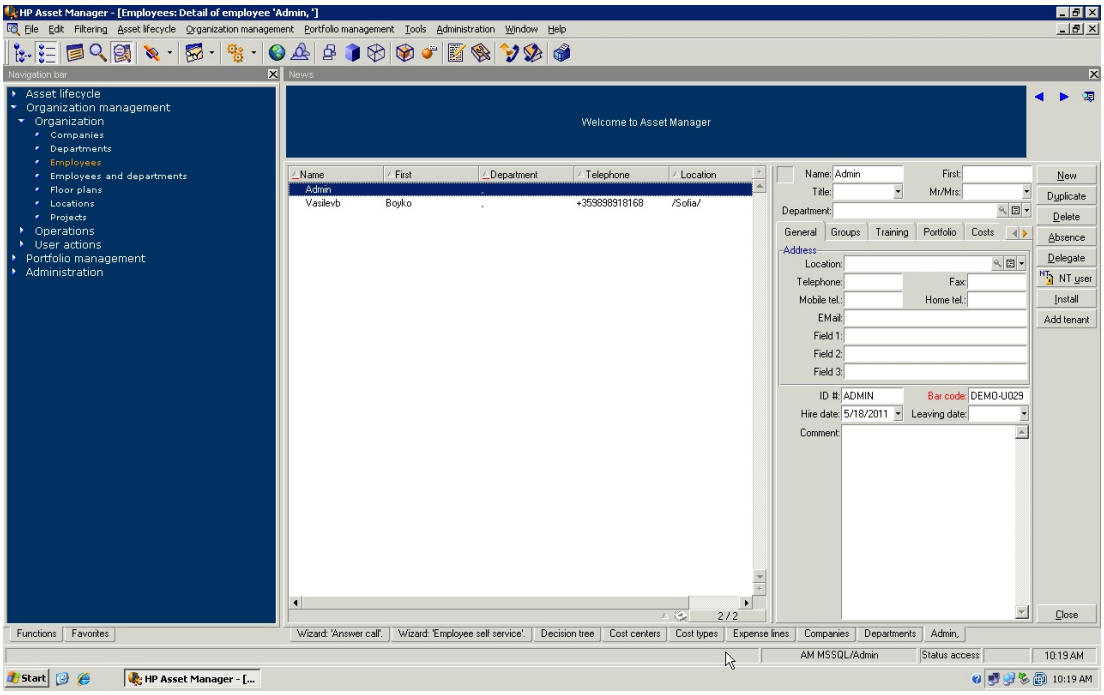

Рисунок 2.7

Решения *управление конфигурациями* обеспечивают автоматизированный учет, развертывание, непрерывное управление и обновление программного обеспечения, включая операционные системы, приложения, базы данных на всех стадиях жизненного цикла ИТ-сервисов.

Решение *управление объединенными событиями и производительностью* обеспечивает эффективное управление ИТ-сервисами в распределенных системах.

Решение *управление идентификацией* обеспечивает автоматизацию процесса создания и поддержки идентификационных данных пользователя и управление доступом как внутри, так и за пределами традиционных границ ИТ-инфраструктуры предприятия. Эти задачи решаются набором продуктов HP OpenView Select — Identity, Access, Audit, Federation.

Пакет HP OpenView Select Identity обеспечивает централизованное управление идентификационными данными и правами доступа пользователей. Это решение организует и контролирует процессы подачи/обработки заявок на предоставление доступа и операции создания, изменения и аннулирования учетных записей. Технологически продукт основан на инновационной модели управления учетными записями, реализующей сервисно-ориентированный подход к ИТ. В рамках этого подхода программные и аппаратные элементы ИТ-инфраструктуры рассматриваются не в качестве обособленных объектов управления, а как взаимосвязанные компоненты системы оказания информационных услуг.

Select Identity позволяет обрабатывать ситуации, которые не вписываются в рамки ролевой модели, не создавая дополнительных ролей или правил. Вместо них используются переменные полномочия, с помощью которых

можно обрабатывать исключительные ситуации в рамках процессов запросов и предоставления полномочий на доступ к ресурсам.

Пакет HP OpenView Select Access, позволяет организовать централизованный доступ к Internet-приложениям и Web-сервисам. Он предусматривает единый подход в определении политик авторизации и разграничении прав доступа к ресурсам на основе ролей. Решение дает возможность в полной мере реализовать преимущества технологий однократной регистрации в корпоративных средах на основе порталов и сетей интранет/экстранет.

Настраиваемые интерфейсы API значительно расширяют спектр поддерживаемых систем и позволяют интегрировать Select Access с традиционными и Web-средами. С помощью этого продукта обеспечивается также централизованное управление авторизацией в беспроводных и кабельных сетях Internet и экстранет. Решение поддерживает различные механизмы аутентификации, включая ввод регистрационного имени и пароля самим пользователем, Kerberos и Radius, аутентификацию с использованием токенов, идентификаторов SecurID и сертификатов X.509.

Select Access позволяет не только установить централизованные политики безопасности, действующие в отношении всех пользователей и приложений, но и гибко распределить администраторские обязанности и полномочия между сотрудниками. В частности, делегированию подлежат права на управление пользовательскими профилями, политиками, объектами аудита, доступ к определенным функциям системы Select Access и само право на дальнейшее делегирование полномочий. Уполномоченные пользователи могут работать только с частью таблицы Policy Matrix, которая определяется персональным уровнем доступа, остальные данные скрыты от посторонних глаз. Select Access также содержит гибко настраиваемую Web-консоль администрирования, которая полностью поддерживает режим делегирования полномочий и встраивается в корпоративный портал.

Решение HP OpenView Select Audit предназначено для автоматизированного аудита процессов управления идентификацией и доступом на соответствие законодательным и внутрикорпоративным нормам. Входящая в его состав среда моделирования позволяет сопоставить отдельные аспекты и положения нормативных требований к защите информации с имеющимися системами управления идентификацией и доступом.

С помощью Select Audit организуется сбор, регистрация и централизованное хранение полной истории администраторских и пользовательских действий, обращений к информационным ресурсам и решений о предоставлении прав доступа. Применение электронных подписей надежно защищает информацию в базе аудита от попыток фальсификации. Используя Select Audit, предприятие всегда может не только проконтролировать, но и документально подтвердить все случаи обращения к информационным ресурсам, действия пользователей и ИТ-персонала.

Механизмы обработки событий в Select Audit отвечают за автоматическую рассылку оповещений и выполнение предварительно заданных действий в критических ситуациях. Арсенал ответных действий предусматривает самые разные меры — от записи в журнале аудита до отправки предупреждения по электронной почте или создания инцидента в системе HP OpenView Service Desk путем отправки сообщения SNMP. Встроенные средства формирования отчетности позволяют в полной мере учесть особенности организации работ по обслуживанию ИТ-систем предприятия и политик проведения аудита.

HP OpenView Select Federation обеспечивает эффективное управление учетными записями без центрального репозитария идентификационных данных, реализуя принципы однократной регистрации и федеративного управления с использованием имеющихся систем идентификации — как входящих в состав решений HP OpenView, так и от сторонних поставщиков.

Для управления поддержкой пользователей предназначено решение HP OpenView Service Desk –готовое решение для автоматизации служб технической поддержки и внедрения процессов управления IT-услугами. Объединяя критически важные компоненты технической поддержки в единое решение, оно упрощает работу пользователей и операторов службы поддержки, поднимая качество обслуживания на новый уровень

Центральное место в технической поддержке занимает работа с обращениями клиентов в ИТ-службу поддержки и учет инцидентов. Первоочередная задача при осуществлении общего руководства в области информационных технологий — максимальное удовлетворение требований конечного пользователя, и HP OpenView Service Desk предлагает ряд возможностей, которые улучшают взаимодействие с клиентом.

Программа позволяет персоналу первого уровня поддержки быстро разрешать вопросы, ставшие причиной обращений, или передавать их решение на второй уровень. Интеграция инструментальных средств Service Desk предоставляет специалисту первого уровня поддержки удобный доступ к любой необходимой информации, например, об известных происшествиях, проблемах или изменениях, связанных с конкретными компонентами инфраструктуры. Благодаря этому увеличивается число устраняемых по первому обращению проблем, что повышает производительность и конечного пользователя и персонала поддержки.

Для минимизации негативных последствий инцидентов обеспечивается двунаправленная интеграция HP Service Desk с другими технологическими компонентами HP OpenView, в результате чего информация о событиях быстро и точно передается всем сторонам, которые в ней нуждаются. Поступление информации о происшествиях в Service Desk обеспечивает их обработку в надлежащем порядке, определяемом приоритетами.

Обращения в службу поддержки, инциденты, проблемы и изменения часто требуют выполнения огромного объема работы с документами. Наряд на

работу — это форма, используемая для планирования, распределения и проверки исполнения. HP OpenView Service Desk обеспечивает полную обработку и отслеживание этих форм для максимально быстрого и правильного выполнения работ. Планируемые затраты, предельную дату завершения и максимальное время на выполнение задания вносится в наряд Service Desk инициатором работы. По мере продвижения работы вы можете обновлять наряд, отражая реальное время и дату завершения, любые понесенные издержки и другие сведения. Service Desk обеспечивает просмотр состояния каждого наряда и позволяет по мере необходимости вносить уточнения в запланированные мероприятия. Отчеты о завершенной или еще выполняемой работе предоставляются в различных формах.

Управление изменениями приобретает все большую важность по мере ускорения внедрения новых технологий. В рамках HP OpenView Service Desk управление изменениями связывает операции календарного планирования, предварительной оценки, реализации и окончательного тестирования изменений информационной инфраструктуры.

В процессе управления изменениями основное внимание уделяется не столько средствам, используемым для внесения фактических изменений, сколько инструментам для управления информацией об изменениях и их последствиях для производственной среды. Практически невозможно успешно управлять сложной информационной инфраструктурой, если у операторов нет новейшей информации об используемом в данный момент программном и аппаратном обеспечении.

Соблюдение баланса между запросами ваших заказчиков и необходимым обслуживанием систем имеет решающее значение в управлении изменениями. Для выполнения этого условия Service Desk предлагает Outage Planning (планирование перерывов в работе). Используя Outage Planning, можно задавать плановое время простоя элементов конфигурации и служб. Перерыв в работе может быть связан с профилактическими мероприятиями, такими как техническое обслуживание сервера, или с не зависящими от вас обстоятельствами, например, с перерывами в подаче электроэнергии.

HP OpenView Service Desk отслеживает и контролирует элементы конфигурации (например, компоненты аппаратного обеспечения) в течение всего срока их службы. Наряду с предоставлением информации другим процессам, таким как анализ проблем и управление изменениями, управление конфигурациями, обеспечивает также простой доступ к информации о договорах на оказание услуг, а также о связях между элементами конфигурации и относящимися к ним организационными вопросами.

HP OpenView Service Desk помогает в предоставлении и документировании услуги в соответствии с обязательствами, заявленными в соглашении SLA. С его помощью легко составить таблицы, описывающие время, потраченное на решение различных пользовательских проблем. Максимальное время на

оказание поддержки зависит от гарантированного уровня обслуживания, для его соблюдения учитывается момент поступления запроса и расписание работы информационной службы. Каждому обращению в службу поддержки автоматически присваивается приоритет в зависимости от уровня обслуживания и степени серьезности обращения. При вычислении допустимых сроков обслуживания учитываются: соглашение об уровне обслуживания, заключенное с клиентом и степень серьезности обращения и последствия выбора определенного приоритета для данного уровня обслуживания.

Представления баз данных дают возможность быстрой интеграции для создания необходимых вам документов, настроенных под конкретного заказчика, например, в виде отчетов об уровне обслуживания, таблиц с показателями работы информационной службы и отчетов об управлении изменениями.

Отчеты — это ключевой способ представления управленческой информации о производительности, готовности к работе и пропускной способности ИТ-службы поддержки. HP OpenView Service Desk предлагает готовые средства создания отчетов общего назначения. Для отображения всей информации, хранимой в базе данных Service Desk, используются пригодные для распечатки табличные и графические формы, а также представления в виде пиктограмм и списков, напоминающих Проводник Microsoft Windows. Кроме того, для облегчения интеграции с внешними инструментальными средствами для создания отчетов имеются специальные представления в базе данных Service Desk. Формирование таких баз — это автоматический процесс, происходящий при установке Service Desk.

Простота использования и гибкость — центральные моменты архитектуры Service Desk. Интуитивно-понятный интерфейс пользователя, подобный интерфейсу Microsoft Outlook, предоставляет легко воспринимаемую информацию в знакомом виде, что существенно облегчает обучение конечных пользователей. Развертывание и обновление без остановки приложения, а также простота настройки приносят дополнительную выгоду, сокращая затраты на администрирование и время развертывания справочной службы.

Введение правил реагирования системы на значения полей пользовательского интерфейса обеспечивает дополнительные возможности. В зависимости от состояния или значения определенного поля в открытом диалоговом окне, например, в Service Call (телефонное обращение в службу поддержки), менеджер правил Rule Manager предпримет необходимые действия еще до того, как информация будет сохранена.

Правила позволяют выполнить следующие операции:

- интеллектуальные действия: запуск программ, в том числе с параметрами;

- обзорные действия: отображение заранее настроенных представлений, упрощающих анализ информации;
- системные действия: готовые руководства к действию или списки вопросов, предоставляемые мастером правил Checklist Wizard;
- запуск консольных приложений;
- обновление полей: изменение состояния поля.

HP OpenView Service Desk позволяет объединить в единый поток операций процессы управления конфигурациями, изменениями, обработкой инцидентов и причин сбоев.

Благодаря такому уровню интеграции ИТ-служба поддержки способна работать в упреждающем режиме. Имея под рукой всю необходимую информацию, персонал сможет четко реагировать на возникающие проблемы и разрешать их до того, как они отразятся на критически важных бизнес-процессах.

Возможность сопоставить конкретную проблему в инфраструктуре с соглашениями об уровне обслуживания (например, с использованием HP OpenView Operations) обеспечивает обработку происшествий в соответствии с SLA для конкретного элемента конфигурации.

Решения на уровне управления ИТ-инфраструктурой

Решение *управление ИТ-инфраструктурой* обеспечивает проактивное и эффективное управление вычислительной сетью ИС, программными средствами, приложениями и оборудованием для обеспечения качественного предоставления ИТ-сервисов пользователям с минимальными затратами. Данное решение предполагает управление сетями серверами и хранением данных уровня предприятие, оптимизацию производительности информационной системы и оптимизацию работы приложений конечных пользователей.

Решение HP OpenView Network Node Manager (NNM) обеспечивает высокофункциональное управление сетью предприятия, позволяя оптимизировать совокупную стоимость владения, повысить производительность и эффективность использования сетевых ресурсов. Инструменты, входящие в состав решения HP OpenView NNM, позволяют сократить сроки поиска и устранения неисправностей. Эти инструменты будут одинаково полезны как начинающим специалистам по обслуживанию сетей, так и высококвалифицированным сетевым администраторам.

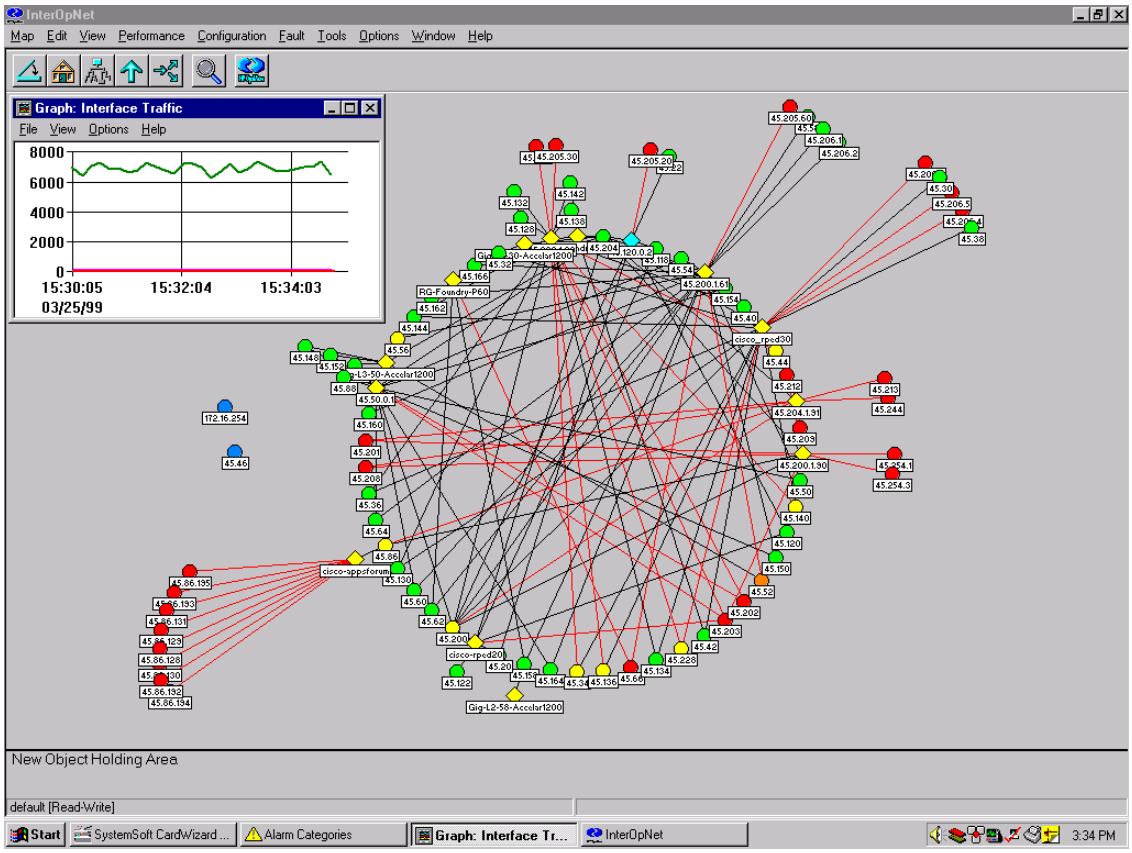

Рисунок 2.8

Графический интерфейс HP OpenView NNM содержит наглядные сведения о состоянии сети и позволяет быстро перейти к детальным спискам событий или визуальным картам сети. Карты сети наглядно отображают состояние сетевых устройств и места возникновения неполадок, что помогает своевременно обнаружить и устранить проблемы в работе сети.

HP OpenView NNM содержит обширный перечень готовых отчетов, необходимых для упреждающего анализа и выявления тенденций в работе сети. Отчеты позволяют отобразить тренды производительности и готовности сети, осуществить инвентаризацию имеющихся устройств и систем, а также получить статистику ошибок и отказов с использованием практически любого браузера. С помощью отчетов HP OpenView NNM можно получить точную картину состояния всех элементов сети и устранить потенциальные проблемы до того, как они начнут сказываться на работоспособности и производительности.

Система сетевого управления HP OpenView NNM предельно проста в установке и использовании и вместе с тем обладает достаточной гибкостью для оптимизации имеющихся сетевых ресурсов и легко расширяется по мере развития сети предприятия.

Управление ИТ-ресурсами

В семейство программных продуктов HP OpenView позволяет решать весь комплекс задач в области управления ИТ-ресурсами. В состав программного

обеспечения, кроме перечисленных ранее, входят ряд пакетов программ HP OpenView.

Пакет HP OpenView Compliance Manager ведет непрерывный мониторинг внутренних контуров управления ключевыми бизнес-процессами, вспомогательными приложениями и инфраструктурой, чтобы измерить эффективность, смягчить возможные риски, а также постоянно отслеживать соблюдение стандартов защиты и раскрытия информации. Пакет HP OpenView Compliance Manager оценивает эффективность инструментов ИТ-управления, проверяя основные области управления ИТ-процессами. Это – управление доступностью, управление защитой информации, управление инцидентами, управление изменениями, управление выпусками и управление конфигурациями.

HP OpenView Performance Insight — это инструмент для анализа производительности ИТ-среды и управления ею. Продукт предназначен для руководителей и технических специалистов служб эксплуатации, в чьи обязанности входит контроль и поддержание требуемого уровня обслуживания внутрикорпоративных или сторонних заказчиков. HP OpenView Performance Insight содержит средства построения отчетов, которые могут использоваться специалистами по планированию и эксплуатации ИТ-среды в качестве оперативного инструмента для выявления и устранения потенциальных проблем до того, как они начнут негативно сказываться на работе ИТ-среды. Кроме того, отчеты HP OpenView Performance Insight могут использоваться в качестве инструмента стратегического планирования, который позволяет получить и, что более важно, осмыслить информацию, необходимую для развития ИТ-среды предприятия в соответствии с эволюционирующими требованиями бизнеса. HP OpenView Performance Insight и HP OpenView Network Node Manager образуют единую систему поиска и устранения неисправностей в работе сети.

HP OpenView Reporter — это доступное, гибкое и простое в использовании решение для создания отчетов о работе распределенной ИТ-инфраструктуры предприятия. Продукт позволяет управлять отчетами, автоматически преобразовывать данные, полученные от приложений HP OpenView на всех поддерживаемых платформах, в ценную и удобную для дальнейшего использования управленческую информацию.

Пакет HP OpenView Dashboard позволяет быстро строить информационные панели, отражающие состояние любых бизнес-сервисов. Такие панели позволяют эффективно наблюдать за всеми параметрами интересующего бизнес-сервиса, включая источники событий и состояние систем безопасности.

HP OpenView Service Information Portal — это спроектированное для поставщиков услуг портальное приложение, позволяющее быстро создавать и настраивать под нужды клиентов удобные web-сайты с оперативными

отчетами по уровню качества используемых ими услуг. Service Information Portal отличает удобная навигация, возможность персонализации, а также надежная защита данных.

Программный пакет HP OpenView Business Process Insight обеспечивает визуальное представление бизнес-процессов предприятия. Этот пакет предлагает инструменты для мониторинга таких процессов, как, например, доставка заказов. Пользователь может оценить влияние задержек на разных этапах процесса в терминах ценности заказа, определить ключевых заказчиков, на которых отразилась задержка, и др.

Программные решения HP OpenView позволяют автоматизировать процессы поддержки пользователей, а также внутренние процессы служб ИТ-предприятий, основываясь на концепциях управления ИТ-услугами, ITIL, ITSM, а также обеспечить визуализацию ИТ-услуг средствами веб-портала.

Платформа управления ИТ-инфраструктурой IBM/Tivoli

Фирма IBM для поддержки процессов ITPM предлагает семейство продуктов IBM/Tivoli. Платформа управления Tivoli включает в себя решения по автоматизации всех аспектов управления ИТ-инфраструктурой. Компоненты Tivoli позволяют управлять практически любой информационной системой независимо от ее состава, сложности, размера и территориального расположения.

Используя вертикальный подход к управлению информационной средой компании, Tivoli предоставляет мощные инструменты для бизнес-ориентрованного управления ИТ-инфраструктурой. Программное обеспечение Tivoli позволяет:

- собирать и анализировать важнейшие данные по управлению ИТ-инфраструктурой предприятия;
- использовать лучший практический опыт проактивного управления;
- реализовать подходы к управлению с точки зрения бизнеса и технологий;
- использовать простые в понимании и развертывании решения;
- использовать новые функции автоматического управления

Программные продукты Tivoli имеют общий графический интерфейс и используют инфраструктуру Web, основанную на открытых стандартах.

Единый репозиторий Tivoli Enterprise Data Warehouse дает администратору стандартизированное представление о ресурсах системы. Репозиторий поддерживает масштабирование от нескольких записей до нескольких миллионов элементов. Технология Data Warehouse охватывает все продукты

Tivoli. Репозиторий Data Warehouse поддерживает выполнение рутинных задач управления и проведение прогнозного анализа.

Платформа Tivoli включает специализированные решения, охватывающие четыре основные области управления ИТ-инфраструктурой предприятия:

- производительность и готовность;
- операционная поддержка;
- безопасность информационных систем;
- управление хранением данных.

Вопросы производительности и готовности ИТ-инфраструктуры предприятия и эффективность бизнеса тесно связаны. На базе программного обеспечения Tivoli можно построить интегрированные решения с быстрой окупаемостью и возможностью проактивного управления уровнем обслуживания.

Решения по операционной поддержке платформы Tivoli позволяет снизить потенциальный уровень затрат, автоматизировать управление и повысить его эффективность. Это достигается за счет выполнения следующих функций:

- автоматическая инвентаризация аппаратного и программного обеспечения информационной системы;
- централизованное развертывание программного обеспечения;
- удаленное управление пользовательскими компьютерами;
- планирование и оптимальное использование корпоративных вычислительных ресурсов.

Решения по обеспечению безопасности информационных систем способствует устранению или снижению рисков, за счет последовательного применения политик безопасности, приводит к снижению потенциальных административных издержек.

Решения по управлению хранением данных обеспечивает защиту информационных активов предприятия, обеспечивает высокую степень надежности и непрерывности бизнес-процессов, упрощает управление хранением корпоративной информации.

Платформа Tivoli содержит более 80 программных продуктов для управления ИТ-инфраструктурой предприятия.

Базовые технологии поддерживаются следующими решениями:

- IBM Tivoli Enterprise Data Warehouse;
- IBM Tivoli Management Framework;

- IBM Tivoli Universal Agent.

Программный продукт Tivoli Enterprise Data Warehouse выполняет функцию основного репозитария для всех ретроспективных данных по управлению информационными системами предприятия и является базой для всех функций составления отчетов в программных решениях Tivoli. Основными характеристиками данного продукта являются:

- открытая расширяемая архитектура, позволяющая собирать и хранить данные обо всей ИТ-инфраструктуре предприятия;
- интерфейс составления отчетов на основе Web, через который пользователь может настраивать, генерировать и просматривать отчеты;
- система безопасности на уровне пользователей, определяющая права на просмотр и модификацию конкретных отчетов для каждого пользователя.

Tivoli Enterprise Data Warehouse предоставляет возможность эффективного доступа к данным системы управления, полученным из различных источников, и позволяет осуществлять всесторонний анализ накапливаемых данных по управлению информационными системами.

Программное решение Tivoli Management Framework является базовым модулем платформы управления Tivoli. Оно создает вычислительную и коммуникационную основу для функционирования остальных модулей Tivoli. Tivoli Management Framework обеспечивает:

- тесную интеграцию компонентов Tivoli;
- стандартные интерфейсы;
- средства для расширения функциональности;
- кросс-платформенность системы управления;
- возможность включения собственных приложений в единую систему управления.

Именно Tivoli Management Framework создает распределенную среду, которая обеспечивает интеграцию всех уровней информационной системы в единую систему управления, обеспечивая управление информационными системами любой сложности, позволяет быстро адаптировать информационную систему к текущим потребностям бизнеса. Внедрение Tivoli Management Framework обеспечивает интеграцию системы управления Tivoli в информационную среду предприятия.

Программный продукт IBM Tivoli Universal Agent представляет собой многофункциональный агент решения IBM Tivoli Monitoring. Основной особенностью агента является возможность сбора информации от

источников различных типов. Поддерживается большое количество платформ, на которых функционируют управляемые системы. Данные мониторинга можно просматривать в режиме реального времени при помощи Tivoli Enterprise Portal.

Основными функциями программного продукта являются:

- получение данных мониторинга от различных операционных систем и источников, в том числе приложений, баз данных и сетевых устройств;
- настройка получения интересующих параметров функциониро-вания управляемых систем;
- работа с различными типами Data Provider;
- наблюдение и посылка оповещений об изменении статуса источников данных.

Технологии IBM/Tivoli для бизнес-ориентированного управления приложениями и системами

Для реализации бизнес-ориентированного управления приложениями и системами платформа Tivoli предоставляет следующие программные решения.

Application Dependency Discovery Manager, который обеспечива-ет обнаружение и поддержание в актуальном состоянии зависимостей меж-ду функционирующими приложениями. ИТ-сервисами корпоративной информационной системы, визуализацию обнаруженных зависимостей и предоставление отчетов, планирование изменений и разработку дополнительных компонент обнаружения и анализа изменений;

Business Systems Manager обеспечивает управление критичными для бизнеса системами и принятие решений о внесении изменений в ИТ-инфраструктуру в соответствии с требованиями бизнеса, мониторинг и управление группами взаимодействующих прикладных программ, обеспечивающими информационную деятельность предприятия;

Change and Configuration Management Database представляет собой инструмент для сбора, агрегации и консолидации данных об объектах корпоративной информационной системы. Основной бизнес функцией является информационная поддержка процессов ITSM и поддержка принятий решений при изменении элементов корпоративной информационной системы;

Composite Application Manager for Websphere и Composite Application Manager Basic for Websphere являются инструментами для контроля производительности и доступности распределённых Web-систем масштаба предприятия, использующих IBM WebSphere в качестве сервера приложений

и позволяют в режиме реального времени определять причины возникновения узких мест, как в исходном коде приложения, так и в серверных ресурсах или связях с внешними системами;

Composite Application Manager for Response Time Tracking пред-ставляет собой решение для мониторинга характеристик транзакций в рас-пределённых приложениях, отслеживающее время отклика приложения и позволяющее визуализировать весь путь выполнения транзакций и оценить временные затраты для каждого из участков пути;

Composite Application Manager for SOA представляет собой решение для развертывания и управления сервис-ориентированной архитектурой корпоративной информационной системы;

Intelligent Orchestrator позволяет в автоматическом режиме быстро развертывать серверы, операционные системы, программное обеспечение промежуточного уровня, приложения и сетевые устройства. Типовые технологические процессы автоматизируют самые распространенные, часто повторяющиеся задачи развертывания и конфигурирования ресурсов;

License Compliance Manager обеспечивает минимизацию затрат на закупку и обновление лицензий на программное обеспечение за счет централизованного учета лицензий;

Service Level Advisor предназначен для формирования объектив-ной основы для оценки соответствия реально предоставляемых ИТ-сервисов тому уровню, который зафиксирован в соглашениях об уровне обслуживания SLA за счет консолидации в одной точке информации о соглашениях SLA, определения соглашений SLA, автоматического обнаружения фактов нарушения соглашений SLA, прогнозирования тенденций изменения уровня обслуживания, генерации отчётов, оповещения ответственного персонала о выявлении фактов нарушения соглашений SLA;

Storage Process Manager обеспечивает автоматизацию управле-ния процессами хранения данных в соответствии с рекомендациями ITIL и на основе методологии процессного управления IBM Tivoli Unified Process;

Unified Process Composer предоставляет детализированное опи-сание процессов управления ИТ сервисами, которое основано на лучших методиках, используемых в ИТ индустрии. Использование данного решения позволяет пользователям существенно повысить эффективность процессов управления ИТ-инфраструктурой в их организации. Решение предоставляет подробные методики, а также программные средства, позволяющие редактировать, оптимизировать и публиковать описание процессов ITSM;

Release Process Manager предназначен для управления, аудита и координации работ по выпуску программного обеспечения информационной системы. Данный продукт позволяет выстроить процесс выпуска

программного обеспечения на предприятии в соответствии с рекомендациями, изложенными в библиотеке ITIL..

Технологии IBM/Tivoli для малых и средних предприятий

Для малых и средних компаний IBM предлагает линейку программных продуктов для управления и оптимизации ИТ-инфраструктуры предприятия, которые отличается простотой установки, внедрения и управления. В линейку программных продуктов входят IBM Tivoli:

- Identity Manager Express;
- Monitoring (ITM) Express;
- Provisioning Manager (TPM) Express for Inventory;
- Provisioning Manager (TPM) Express for Software Distribution;
- Storage Manager Express;
- Continuous Data Protection (CDP) for Files.

Identity Manager Express - это решение для управления учётными записями, которое:

- предоставляет единую точку управления паролями, учётными записями пользователей и правами доступа;
- обеспечивает постоянную защиту и аудит прав доступа пользователей для повышения защищённости систем;
- способствует сокращению издержек за счет сокращения числа обращений в службу поддержки;
- обеспечивает быстрое создание и уничтожение учётных записей пользователей;
- поддерживает централизованное отслеживание доступа пользователей и формирование стандартных отчётов аудита

Monitoring (ITM) Express обеспечивает возможности мониторинга и управления и упрощает администрирование гетерогенных сред. ITM Express предоставляет централизованный портал для устранения узких мест, ликвидации проблем с производительностью и устранения сбоев. ITM Express обеспечивает доступ пользователей к большим объемам данных о готовности, которые можно использовать для раннего обнаружения и быстрого исправления проблем до того, как пострадает производительность конечных пользователей.

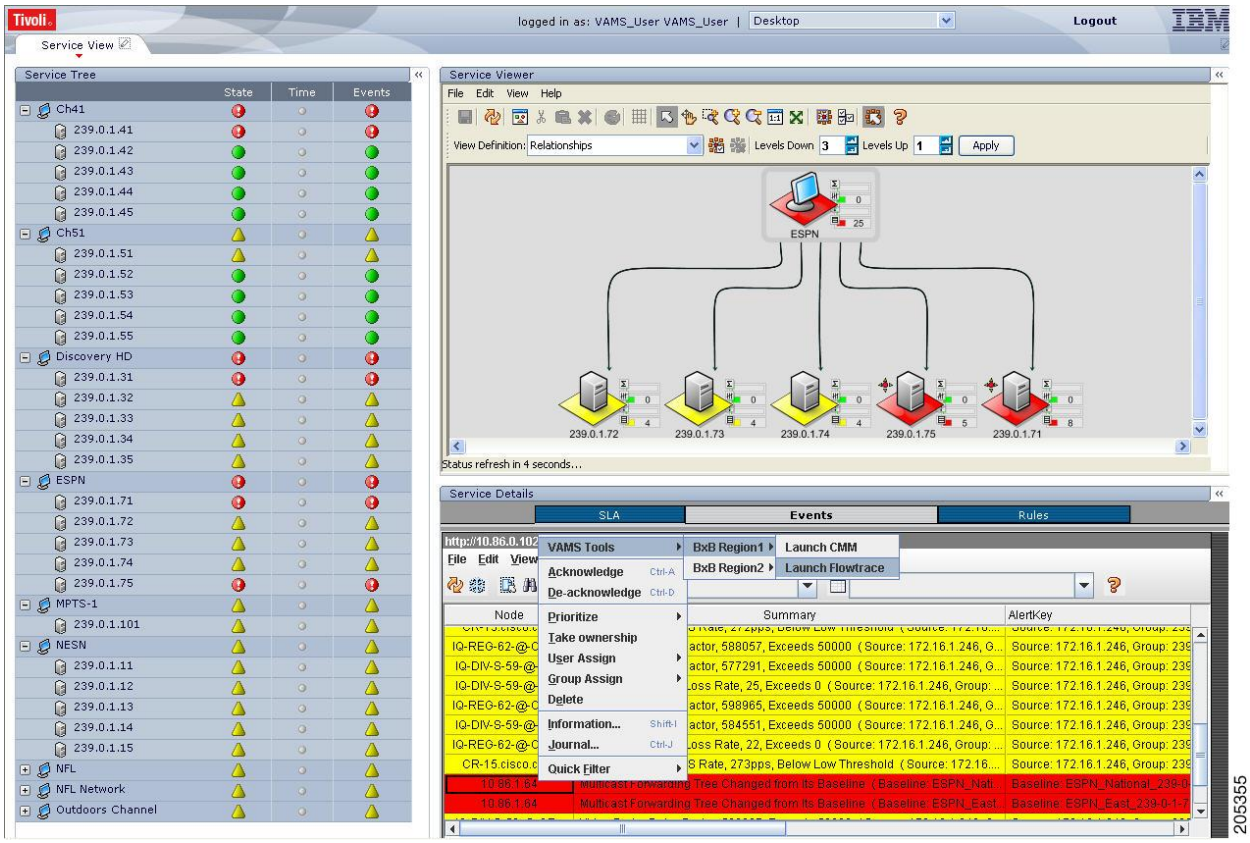

Рисунок 2.9

ITM Express обеспечивает:

- быстрое обнаружение и разрешение проблем в критически важных компонентах ИТ-инфраструктуры;
- сокращение общих эксплуатационных затрат на ИТ-инфраструктуру, благодаря простоте установки и внедрения;
- визуализацию текущих и архивных показателей производительности в табличном и графическом форматах, предоставление экспертных советов и автоматизацию процессов для повышения производительности;
- автоматическое отслеживание состояния критически важных элементов разнородной ИТ-инфраструктуры и получение предупреждений только при возникновении проблем.

Provisioning Manager (TPM) Express for Inventory применяется для управления инвентарными данными, которое обеспечивает сбор и хранение информации об активах, программном и аппаратном обеспечении. TPM Express for Inventory обеспечивает:

- постоянную точную идентификацию, отслеживание и от-чётность о программном и аппаратном обеспечении и их владельцах;
- замену медленных и дорогостоящих методов ручной инвентаризации;

- предотвращение закупки лишних или недоиспользованных ли-цензий на программное обеспечение и оборудования.

Provisioning Manager (TPM) Express for Software Distribution обеспечивает управление инвентарными данными и автоматическое развертывание программного обеспечения. TPM Express for Software Distribution позволяет:

- точно и экономично управлять активами распределённой ИТ-инфраструктурой;
- обеспечить быструю установку изменений программного обеспечения только на тех компьютерах, на которых это необходимо;
- сократить инфраструктурные издержки и обеспечить безопасность.

Storage Manager Express проедставляет недорогое и простое во внедрении и использовании решение резервного копирования и восстановления базового уровня. Данное решение обеспечивает:

- быструю установку (установка и первое резервное копирование менее чем за 1 час);
- удобный пользовательский интерфейс;
- автоматическую настройку устройств;
- поиск устройств.

Для резервного копирования реализована традиционная методология «дед-отец-сын», что помогает повысить производительность благодаря таким функциям, как:

- управление ленточными накопителями «в фоновом режиме»;
- встроенная система оперативной отчётности;
- резервное копирование клиентских систем без монтирования лент.

Continuous Data Protection (CDP) for Files предназначено для модернизации и автоматизации защиты данных в широком круге применений - от обычных пользовательских ПК до высокотехнологичных корпоративных файловых серверов. В данном решении реализовано сочетание репликации, постоянной защиты и контроля версий и традиционного планового резервного копирования в едином пакете. CDP обеспечивает:

- постоянную защиту важных файлов;
- прозрачную работу в фоновом режиме;
- восстановление на заданный момент времени.

Инструментарий управления ИТ-инфраструктурой Microsoft System Center

Для решения задач управления ИТ-инфраструктурой предприятия Microsoft предлагает набор инструментов, моделей, методик и рекомендаций, которые призваны обеспечить построение управляемых ИС высокой надежности, доступности и защищенности. Данные материалы объединены в решения Microsoft для управления – MSM (Microsoft Solutions for Management).

Методологической основой построения и сопровождения управляемых ИТ-систем является библиотека MOF. На базе основного руководства MOF разработано более 20 документов, описывающих функции управления обслуживанием SMF (Service Management Function) и инструкции по реализации конкретных действий в рамках ИТ-инфраструктуры.

В свою очередь SMF являются основой для руководств, в которых детализируются мероприятия по достижению конкретных целей при оптимизации ИТ-инфраструктуры. Руководства включены в:

- инструкции проектов усовершенствования обслуживания SIP (Service Improvement Project);
- акселераторы решений SA (Solution Accelerator).

В проектах усовершенствования обслуживания приведены рекомендации по реализации или усовершенствованию отдельных функций (совокупности функций) управления обслуживанием.

Акселераторы решений являются примерами решений по усовершенствованию ИТ-инфраструктуры предприятия на базе программного инструментария и инструкций SMF. Решения SA содержат следующее:

- решения по развертыванию новых приложений с помощью SMS для операционных систем семейства Windows;
- решения по управлению обновлению установкой оборудования на базе SMS, предлагающее рекомендации по развертыванию исправлений и пакетов обновления для серверов Windows, SQL Server, Exchange и клиентских программ настольных компьютеров.

Инструментальной основой MSM является семейство продуктов MSC (Microsoft System Center), которое решает следующие задачи:

- управление эксплуатацией и функционированием информационных систем;
- управление изменениями и конфигурацией;
- защита и хранение данных;

- контроль проблем;
- управление нагрузкой.

В семейство Microsoft System Center входят:

- Microsoft System Management Server (SMS);
- Microsoft Operations Manager (MOM);
- System Center Reporting Manager (SCRM);
- Microsoft System Center Data Protection Manager (DPM);
- Microsoft System Center Capacity Planner (CCP).

Microsoft System Management Server обеспечивает централизованное управление изменениями и конфигурациями ИТ-инфраструктуры предприятия, построенной на базе компьютеров семейства операционных систем Windows. SMS предоставляет следующие возможности:

- инвентаризацию аппаратных и программных средств корпоративной информационной системы предприятия;
- надежное развертывание системы на уровне предприятия и автоматизированная установка и обновление программ в системе;
- управление ресурсами и распространение программного обеспечения дл мобильных пользователей;
- отслеживание использования программного обеспечения на клиентских компьютерах конкретными пользователями и подготовку отчетов по использованию;
- дистанционное диагностирование проблем и неисправностей на клиентских компьютерах.

Microsoft Operations Manager обеспечивает средства управления серверной инфраструктурой в масштабах предприятия, что позволяет повысить эффективность ее эксплуатации. MOM предоставляет открытые и масштабируемые средства для управления информационными системами предприятий, комплексного управления событиями, активного контроля и оповещения, создания отчетов и анализа тенденций, а также специализированные базы знаний, содержащие сведения о функционировании систем и приложений, для повышения уровня управляемости корпоративных систем.

MOM позволяет существенно упростить выявление проблемных зон ИТ-инфраструктуры предприятия, облегчает процесс определения основных причин неполадок и способствует быстрому восстановлению работы служб и предотвращению потенциальных проблем ИТ-среды.

Operations Manager включает следующие интерфейсы пользователя:

- консоль администратора;
- консоль оператора;
- Web-консоль;
- консоль отчетов.

Консоль администратора предназначена для индивидуальной настройки MOM, просмотра серверов информационной системы, развертывания агентов на серверах и клиентах, создания и обслуживания прав доступа корпоративных пользователей, а также для создания, импорта и экспорта пакетов управления (Management Pack).

Консоль оператора обеспечивает оценку состояния ИТ-инфраструктуры предприятия, выявление неполадок и получение рекомендаций по их устранению. На нее можно добавить сведения об устранении специфических неполадок для конкретного предприятия.

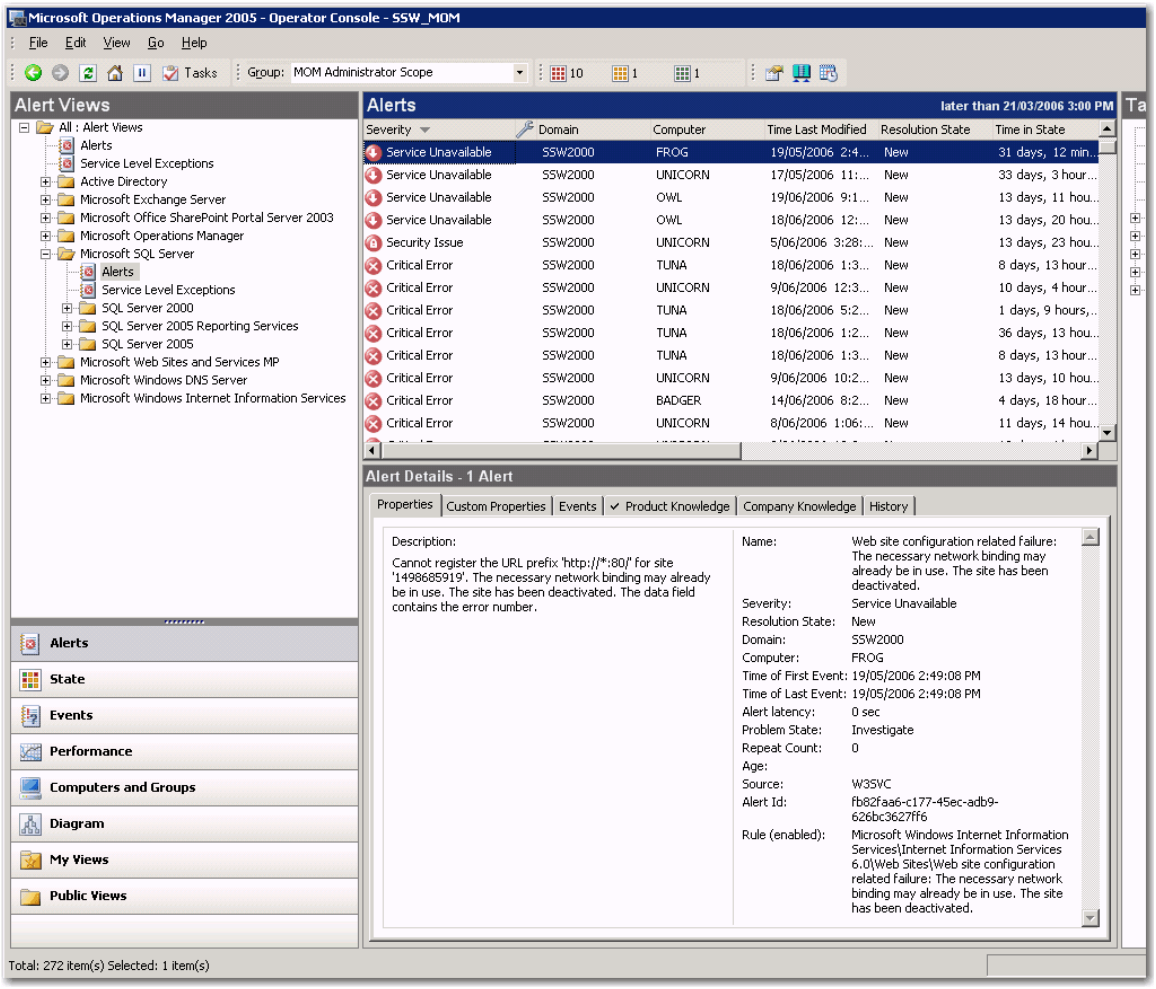

Рисунок 2.10

Представление консоли в виде нескольких областей облегчает просмотр данных, необходимых для решения возникающих проблем, позволяя избежать открытия различных диалоговых окон. Консоль имеет несколько

видов экранов (представлений). Представление State View (Просмотр состояния) обеспечивает сводный обзор состояния компьютеров в режиме реального времени в пределах управляемой среды. Представление Diagram View (Просмотр диаграммы) обеспечивает различные обзоры топологии, в которых отображается взаимосвязь между серверами – объектами мониторинга, сервисами и их состояние. Представление Alerts View (Просмотр предупреждений) содержит список проблем среды, требующих немедленного вмешательства, а также сведения о текущем состоянии и степени серьезности каждого предупреждения. В нем указано, были ли предупреждения подтверждены, расширены или устранены, и было ли нарушено соглашение об уровне обслуживания. Представление данных о производительности позволяет выбрать и отобразить один или несколько показателей производительности ряда систем за определенный период времени. Представление Events View содержит список событий, которые произошли на управляемых серверах, описание каждого события, а также сведения об источнике неполадки.

Web-консоль обеспечивает ряд функциональных возможностей консоли оператора, доступных с помощью Web -обозревателя. Это гарантирует необходимую гибкость в случае необходимости изменения статуса предупреждения, обновления базы знаний компании, просмотра состояния компьютера, а также получение уведомлений по электронной почте со ссылками на конкретные неполадки сети, требующие вмешательства.

Консоль отчетов позволяет просматривать отчеты о событиях, предупреждениях и производительности в окне Web-обозревателя. Она дает возможность подписываться на избранные отчеты и автоматически получать их новые версии. Для стандартных отчетов используется служба SQL Server Reporting Services, а специализированные отчеты могут быть созданы в инструментальной среде Visual Studio. Отчеты можно легко экспортировать в Microsoft Excel, Adobe Acrobat, а также в файлы формата HTML, TIFF, CSV или XML.

Operations Manager обладает хорошей масштабируемостью относительно количества управляемых компьютеров на каждом сервере MOM и количества управляемых серверов на каждой консоли.

В части решаемых задач и диагностики MOM позволяет настраивать, экспортировать, импортировать и запускать контекстные задачи и диагностику. Задачи могут выполняться на консоли, сервере или агенте. В число задач входят тестовый опрос компьютера, сброс кэша DNS и удаление неактивных объектов из Active Directory.

В режиме обслуживания обеспечивается предотвращение отображения предупреждений на консоли оператора, пока выполняется обслуживание системы.

Operations Manager допускает переопределение правил, что позволяет изменять стандартные параметры и пороговые значения для выбранных компьютеров или групп и задавать приоритет для предотвращения потенциальных конфликтов, вызванных многочисленными переопределениями.

MOM обеспечивает сброс автоматического предупреждения, что позволяет агенту автоматически обновлять базу данных MOM в случае исправления предупреждения без участия оператора.

Operations Manager позволяет вести детальное наблюдение за отдельными экземплярами информационной инфраструктуры. MOM распознает отдельные экземпляры в системе и выполняет наблюдение за ними. Например, MOM выявляет отдельные базы данных в пределах SQL Server, и не только SQL Server, но и в целом.

В кластерной серверной среде MOM распознает виртуальный кластерный сервер наряду с физическими серверами. Эта возможность различения серверов в пределах кластера позволяет создателям пакетов управления создавать более детализированные правила.

MOM поддерживает вложенные группы компьютеров. Логическая группировка компьютеров может быть подвернута дальнейшему разделению для обеспечения контекста управления сходными системами. Например, внутри группы компьютеров SQL Server 2005 могут быть выделены группы компьютеров для ведения платежных ведомостей или выполнения заказов, причем каждая из них будет связана с различными правилами.

Operations Manager обеспечивает ответы на предупреждения, которые могут быть выполнены агентом до того, как предупреждение будет отключено.

MOM предусматривает быстрое выяснение причин снижения уровней предоставления ИТ-сервисов за счет реализации концепции пакетов управления Management Pack. Пакеты управления представляют собой механизм консолидации накопленного опыта ИТ-экспертов в отдельно выделенной области. Использование пакетов управления позволяет сократить время и расходы на управление инцидентами при выполнении следующих операций:

- определение объектов наблюдения – фиксация инцидента;
- устранение неполадок по мере их возникновения – закрытие инцидента.

Пакеты управления содержат:

- правила наблюдения с заданными пороговыми значениями определенных метрик. Пороговые значения параметров ИТ-инфраструктуры позволяют сформировать приоритеты оповещений по конкретным событиям;

- базу знаний, содержащую сведения по устранению неполадок. Благодаря привязке базы знаний к оповещению оператор быстро получает необходимые сведения по инциденту и процедуре его устранения;

- сценарии, которые можно использовать для быстрого обнаружения причин инцидентов в ИТ-инфраструктуре. Сценарии позволяют восстанавливать требуемые уровни предоставления ИТ-сервисов как вручную, так и автоматически. При необходимости операторы могут создавать собственные специальные сценарии.

Обеспечение эффективного управления инфраструктурой предприятия поддерживается решениями по наблюдению за службами Service Monitoring Solution Accelerator (SMSA), в которых содержатся полезные советы и рекомендации, а также инструкции по внедрению и эксплуатации MOM. В состав SMSA включены следующие решения:

- маршрутизация оповещений;

- автоматическое создание заявок;

- настройка оповещений;

- отказоустойчивость системы мониторинга.

Маршрутизация оповещений дает возможность использовать подписку и отправку уведомлений по электронной почте, используя приложение Microsoft SQL Server Notification Services.

Автоматическое создание заявок позволяет полностью автоматизировать отправку запроса (заявки) в систему запросов о неполадках, используемую для управления событиями.

Настройка оповещений обеспечивает следующие возможности:

- инструкции с использованием проверенной методики по эффективному определению высокоприоритетных оповещений;

- три основных отчета MOM по настройке оповещений.

Отказоустойчивость системы мониторинга содержит руководства для ИТ-менеджеров, ориентированные на следующее:

- повышение работоспособности и стабильности служб мониторинга ИТ-инфраструктуры;

- автоматизации служб MOM на основных уровнях обслуживания;

- обеспечения различных конфигураций архитектуры, учитывающих несколько географических регионов;

- использование нескольких групп управления на основе единого хранилища данных для объединенных отчетов.

Для интеграции Operations Manager со средствами управления других производителей в MOM включены Web-службы MOM Connector Framework (MCF). Web-службы MCF обеспечивают:

- поиск и выявление оповещений MOM, которые должны быть направлены в другие системы управления;
- получение предупреждений, поступивших из других систем управления, и отображение их на консоли оператора;
- отслеживание того, какие оповещения были направлены в другие системы управления и когда они должны быть обновлены;
- синхронизация оповещений разных систем управления, позволяющая избежать повторной работы при отслеживании и обновлении оповещений.

Microsoft Operations Manager является основным компонентом инициативы Dynamic Systems Initiative, которая предполагает для ИТ-службы предприятия максимально эффективно использовать трудовые ресурсы и снижать необходимый объем работ на всех этапах жизненного цикла информационной системы.

System Center Reporting Manager обеспечивает объединение информации, формируемой Microsoft System Management Server и Microsoft Operations Manager. При этом от SMS поступает информация о конфигурации и изменениях в ИТ-инфраструктуре предприятия, а от MOM - информация о событиях и производительности. SCRM позволяет формировать отчеты, которые позволяют:

- обнаружить сервера с низким уровнем нагрузки и исключить их из эксплуатации, применив сценарий консолидации серверов;
- упростить процесс принятия решения о балансировке нагрузки, предоставив информацию о производительности серверов и выполненном ими объеме работы;
- определить, являются ли проведенные изменения (программные или аппаратные) причиной возросшего потока предупреждающих сообщений от серверов;
- сформировать статистику о производительности серверов в контексте изменений программного обеспечения ИТ-инфраструктуры предприятия.

System Center Reporting Manager предоставляет простые в построении и информативные отчеты о функционировании ИТ-инфраструктуры предприятия.

Microsoft System Center Data Protection Manager предназначен для резервного копирования на диски и восстановления данных. DPM обеспечивает постоянную и эффективную защиту данных, а также быстрое и надежное их восстановление. Для реализации функциональности DPM использует репликацию, инфраструктуру службы теневого копирования томов.

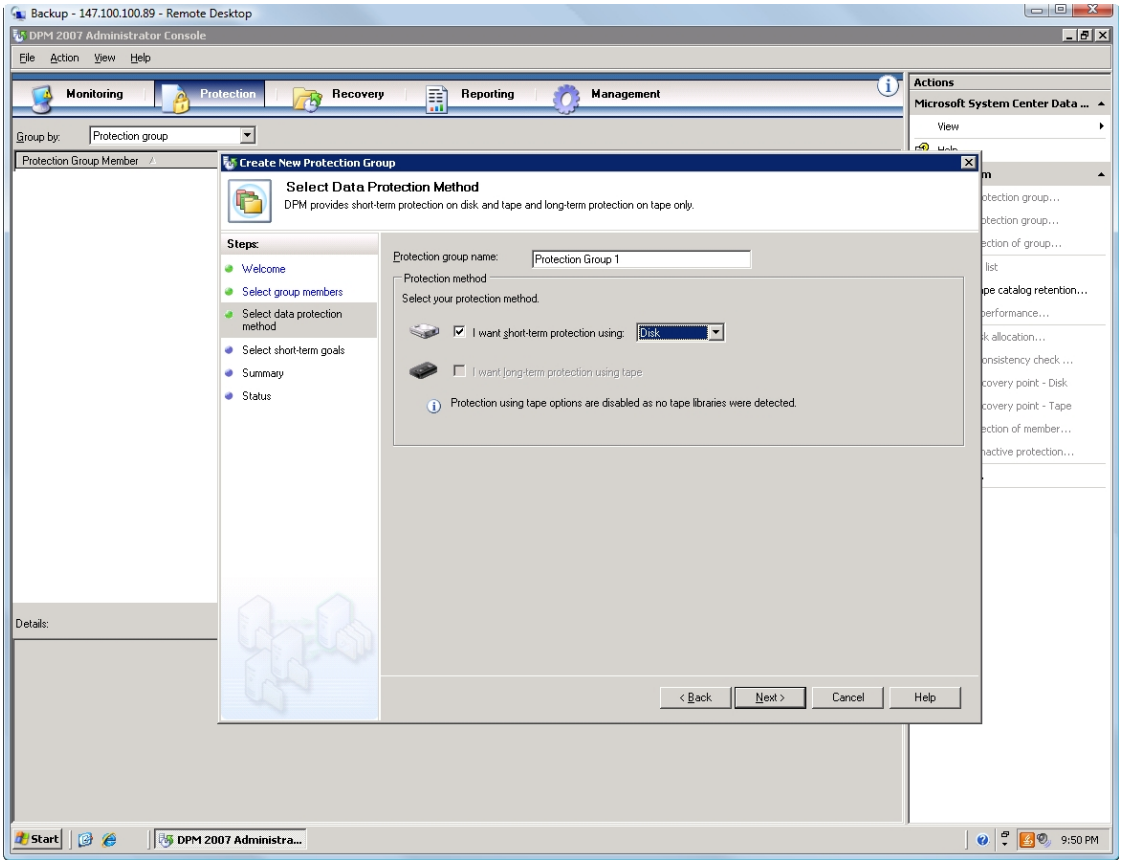

Рисунок 2.11

Data Protection Manager может применяться для малых и средних предприятий, но наиболее эффективно его применение для предприятий, в ИТ-инфраструктуре которых имеется от 5 до 49 серверов. Целесообразность применения DPM может характеризоваться следующим:

- существуют проблемы с выделением времени для остановки серверов для проведение операций резервного копирования;
- имеется достаточно частая необходимость (не менее 5 – 10 раз в месяц) восстановления файлов с магнитной ленты;
- имеется опыт работы со службой теневого копирования томов или знания возможностей Windows server 2003 в поддержке теневых копий общих папок;
- наличие директивных сроков восстановления данных, которое должно быть не более часа;

- директивное время восстановления не может быть достигнуто из-за медленной работы ленточных накопителей.

Основными достоинствами DPM являются:

- быстрое восстановление файлов (за минуты, а не за часы);
- исключение необходимости остановки производственных серверов для резервного копирования;
- сокращение периода потенциально возможной потери данных до одного часа;
- исключение неудачных попыток восстановления данных;
- мгновенная проверка целостности резервных копий;
- возможность для пользователей самостоятельно восстанавливать данные;
- быстрая организация защиты файловых серверов (за считанные минуты);
- возможность использования средств мониторинга и отчетности , содержащегося в серверном программном обеспечении.

DPM обеспечивает гибкие процедуры восстановления данных корпоративной информационной системы. Наиболее распространенные сценарии восстановления данных следующие:

- полное восстановление сервера администраторами сервера;
- восстановление файлов администраторами сервера;
- восстановление файлов службой поддержки;
- восстановление файлов пользователями.

Microsoft System Center Capacity Planner предназначен для планирования развертывания систем посредством функционирования ИТ-инфраструктуры предприятия.

CCP позволяет ИТ-персоналу решать следующие задачи:

- анализ количественных параметров развертываемой распределенной информационной системы;
- анализ использования оборудования путем эмулирования планируемой нагрузки для модели ИТ-инфраструктуры и вычисления нагрузки для каждого аппаратного ресурса (серверов, дисковых подсистем, локальных и глобальных сетей);
- анализ времени выполнения транзакций;

- анализ вариантов развертывания или модернизации аппаратного и программного обеспечения информационной системы по принципу «что – если».

Использование ССР позволяет проводить корректное планирование допустимых уровней обслуживания ИТ-сервисов, обосновывать требуемые ИТ-службе ресурсы для поддержания требуемых параметров ИТ-сервисов.

Глава 3. Частные вопросы управления ИТ-инраструктурой

Особенности управления ИТ-инфраструктурой в условиях правоприменения законодательства в области работы с персональными данными

Вступление в силу Федерального Закона №152 «О персональных данных» привело к необходимости значительно пересмотреть состав и организационные решения по управлению ИТ-инфраструктурой на большинстве предприятий. В нашем государстве была принята не инцидентная, а превентивная модель обеспечения безопасности персональных данных, которая заключается в обязательном применении сертифицированных решений для любых информационных систем, связанных с обработкой или хранением персональных данных. Закон и подзаконные акты предусматривают строго регламентированную процедуру приведения информационных систем персональных данных (ИСПДн) в соответствие законодательству. Но прежде, чем рассматривать эту процедуру имеет смысл систематизировать данные по имеющемуся законодательству в этой сфере. Именно рассматриваемые ниже документы являются основанием для принятия решений при управлении ИТ-инфраструктурой в аспекте обеспечения безопасности персональных данных.

Законодательная база организации работы с персональными данными

Конституция РФ. В соответствии со статьей 23 Конституции РФ каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Статья 24 часть 1 обязывает всех соблюдать установленный порядок сбора, хранения, использования и распространения информации о частной жизни лица, который действует в границах пользования правами и свободами, установленными частью 3 статьи 55 Конституции. Статья 24 часть 2 возлагает на органы государственной власти и местного самоуправления, на должностных лиц этих органов обязанность обеспечить возможность ознакомления каждого с документами и материалами, непосредственно затрагивающими его права и свободы.

Федеральный закон № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и защите информации». Создает правовые, организационные и экономические основания для реализации права на свободный поиск, получение, передачу, производство и распространение информации.

Федеральный закон № 152-ФЗ от 27.07.2006 г. «О персональных данных». Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов

Российской Федерации, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Постановление правительства РФ № 781 от 17.11.2007 г. «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Постановление правительства РФ № 687 от 15.09.2008 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». Настоящее положение определяет особенности организации обработки персональных данных и меры по обеспечению безопасности персональных данных при их обработке, осуществляемых без использования средств автоматизации

Приказ ФСТЭК РФ № 55, ФСБ РФ № 86 от 13.02.2008 г. и Мининформсвязи РФ № 20 «Об утверждении Порядка проведения классификации информационных систем персональных данных». Настоящий Порядок определяет проведение классификации информационных систем персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Приказ Россвязькомнадзора № 8 от 17.07.2008 г. «Об утверждении образца формы уведомления об обработке персональных данных» (с изменениями от 18.02.2009 г.). Настоящим приказом определен, рекомендуемый к использованию при направлении уведомления об обработке персональных данных, образец формы уведомления, а также даны рекомендации по его заполнению.

Приказ ФСТЭК РФ № 58 от 5.02.2010 г. «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных». Настоящее Положение устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных. Положение определяет

цели и содержание обработки персональных данных оператором или лицом, которому на основании договора оператор поручает обработку персональных данных.

Методический документ ФСТЭК РФ «Базовая модель угроз безопасности персональным данным при их обработке в информационных системах персональных данных» от 15.02.2008 г. Данный документ содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. В модели угроз дано обобщенное описание информационных систем персональных данных как объектов защиты, возможных источников угрозы безопасности персональных данных, основных классов уязвимостей информационных систем персональных данных, возможных видов деструктивных воздействий на персональные данные, а также основных способов их реализации.

Методический документ ФСТЭК РФ от 15.02.2008 г. «Методика определения актуальных угроз безопасности персональным данным при их обработке в информационных системах персональных данных». Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных предназначена для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Типовые требования ФСБ Российской Федерации по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных № 149/6/6-622 от 21.02.2008. Настоящие Требования определяют порядок организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

Методические рекомендации по обеспечению с помощью крипто средств безопасности персональных данных при их обработке в информационных системах персональных данных. Методическими рекомендациями необходимо руководствоваться в случае определения оператором необходимости обеспечения безопасности персональных данных с использованием крип-то средств, а также при обеспечении безопасности персональных данных при обработке в информационных системах, отнесенных к компетенции ФСБ России

Классификация ИСПДн

В основе предусмотренной законодательством модели обеспечения безопасности персональных данных лежит принцип классификации ИСПДн. Эта классификация осуществляется с учетом категорий и объема накапливаемых, обрабатываемых и распределяемых с их использованием ПДн с целью установления методов и способов защиты, необходимых для обеспечения безопасности ПДн. Состав и функциональное содержание методов и средств зависит от вида и степени ущерба, возникающего вследствие реализации угроз безопасности ПДн. При этом ущерб возникает за счет неправомерного или случайного:

- уничтожения,
- изменения,
- блокирования,
- копирования,
- распространения ПДн
- или от иных неправомерных действий с ними.

В зависимости от объекта, причинение ущерба которому, в конечном счете, вызывается неправомерными действиями с ПДн, рассматриваются два вида ущерба: непосредственный и опосредованный. Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту ПДн. Он возникает за счет незаконного использования (в том числе распространения) ПДн или за счет несанкционированной модификации этих данных и может проявляться в виде:

- незапланированных и/или непроизводительных финансовых или материальных затратах субъекта;
- потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием ПДн;
- нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь путем осуществления контактов с ним по различным поводам без его на то желания (например - рассылка персонифицированных рекламных предложений и т.п.).

Опосредованный ущерб, связан с причинением вреда обществу и/или государству вследствие нарушения нормальной деятельности экономических, политических, военных, медицинских, правоохранительных, социальных, кредитно-финансовых и иных государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с ПДн.

Основаниями для классификации ИСПДн являются:

- Категория обрабатываемых в информационной системе персональных данных - Хпд;
- Объем обрабатываемых персональных данных - Хнпд;
- Характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- Структура информационной системы;
- Наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- Режим обработки персональных данных;
- Режим разграничения прав доступа пользователей информационной системы;
- Местонахождение технических средств информационной системы.

По категории ПДн делятся на:

- категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4 - обезличенные и/или общедоступные персональные данные.

По объему ПДн выделяют три объема:

1. в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта РФ или РФ в целом;
2. в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики РФ, в органе государственной власти, проживающих в пределах муниципального образования;

3. в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

По характеристикам безопасности ПДн выделяются:

- Типовые ИСПДн – требуется только конфиденциальность данных.
- Специальные ИСПДн - требуется обеспечить хотя бы одну из характеристик безопасности ПДн, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий). К специальным ИСПДн в любом случае относятся:
    - информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;
    - информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

По структуре ИС можно выделить следующие типы ИСПДн:

- автономные (не подключенные к иным информационным системам) комплексы технических и программных средств;
- комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);
- комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена выделяются ИСПДн, имеющие или не имеющие такие подключения.

По режиму обработки персональных данных в информационной системе информационные системы могут быть однопользовательские и многопользовательские.

По разграничению прав доступа пользователей: системы без разграничения прав доступа и системы с разграничением прав доступа.

В зависимости от местонахождения технических средств выделяют системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

На основе рассмотренных выше классификационных признаков в дальнейшем выделают классы ИСПДн. Для специальных ИСПДн классы определяются относительно каждой характеристики безопасности.

- класс 1 (К 1) - нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов ПДн;
- класс 2 (К2) - нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к негативным последствиям для субъектов ПДн;
- класс 3 (КЗ) - нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПДн;
- класс 4 (К4) - нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, не приводит к негативным последствиям для субъектов ПДн.

Основание для определения класса является соотношения категории ПДн и объема ПДн. Для этого используется следующая матрица:

	Объем 3	Объем 2	Объем 1
категория 4	К4	К4	К4
категория 3	КЗ	КЗ	К2
категория 2	КЗ	К2	К1
категория 1	К1	К1	К1

Общая методика оценки обстановки для разработки мер по обеспечению безопасности ИСПДн

Первые шаги связаны с оценкой обстановки, реализуемой по схеме, представленной ниже.

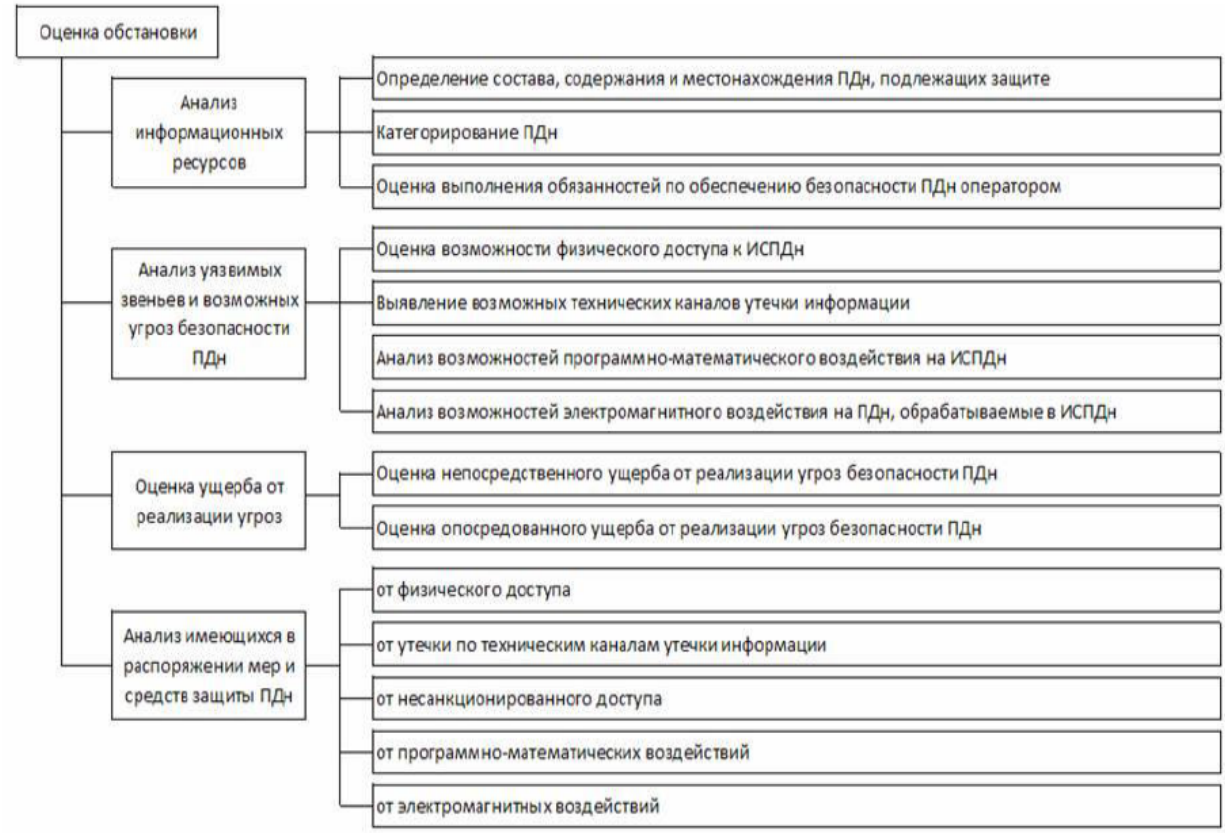

Рисунок 3.12

Дальнейшее обеспечение безопасности ПДн осуществляется в соответствии со следующим порядком:

1. Обоснование требований по обеспечению безопасности ПДн на основе выявления и оценки актуальности угроз
2. Построение частной модели угроз – на основе анализа матрицы доступа, характеристики ПДн и системной архитектуры – руководящий документ – базовая модель угроз. Она в частности содержит типовые модели угроз для распространенных компонентов ИСПДн
3. Определение исходного уровня защищенности – строго по методики через оценку ряда характеристик ИСПДн
4. Определение вероятности реализации угроз – экспертно
5. Из исходного уровня и вероятности – определение возможности реализации угрозы – по формуле
6. Оценка опасности угроз – опять экспертно
7. Определение актуальных угроз из возможности реализации и оценки опасности – по матрице – методика закончилась
8. Разработка мер противодействия актуальным угрозам – каждой угрозе противопоставляется механизм противодействия (именно

механизм, а не средство) – на основе рекомендаций по обеспечению безопасности

9. Разработка проекта СЗПДн. Он состоит из организационно-распорядительной документации, определяющей, в частности ответственныз, допуски к работе с ПДн, описание разрешительной системы доступа и т.п. и проекта технических мер. Для последнего важно понимать, что это не просто выбор из перечня сертифицированных ФСТЭК и ФСБ (для криптографических) решений, а именно полномасштабное проектирование системной архитектуры.
10. Определение порядка действий по созданию защищенной ИСПДн
11. Выполнение действий, контроль, тестирование, документирование результатов

Реализация описанного выше алгоритма связана с значительными материальными и временными затратами. Причем следует понимать, что даже проведенная сертификация построенной ИСПДн не дает долгосрочной гарантии от решения проблем связанных с законодательством в области безопасности персональных данных. Изменения в системной архитектуре и ИТ- инфраструктуре предприятия приводит к необходимости повторной сертификации и новых вложений. Поэтому можно дать ряд общих рекомендаций, выполнение которых должно предшествовать собственно описанным выше работам.

Во первых нужно постараться максимально снизить класс ИСПДн, в том числе за счет вывода части ПДн за пределы автоматизированной обработки.

Во вторых необходимо отказаться от «случайного» хранения ПДн, связанного с промежуточной обработкой, неправильной организацией работы персонала и т.п.

Также имеет смысл укрупнить информационные системы в которых производится обработка ПДн и реализовать их работу на единой и централизовано управляемой ИТ-инфраструктуре.

С точки зрения собственно инфраструктурных решений нужно понимать, что сертифицированные аппаратные решения с точки зрения суммарной стоимости владения, как правило, оказываются дешевле программных, но грамотные организационные решения могут оказаться еще выгоднее.

Особенности управления ИТ-инфраструктурой в условиях использования свободного программного обеспечения

Сегодня, все чаще при выборе тех или иных компонентов ИТ-инфраструктуры выбор падает на использование свободного программного обеспечения. Как будет показано в одном из следующих параграфов, даже очень масштабные и дорогостоящие проекты, такие как сетевой ресурс Flickr,

можно полностью реализовать на инфраструктуре, программные компоненты которой состоят только их свободного ПО. Практика применения свободного ПО сегодня в нашем государстве не так проста, как кажется на первый взгляд. И основные проблемы здесь имеют юридический характер и в частности связаны с управлением свободными лицензиями. Но прежде чем коснутся этих проблем, имеющих непосредственное отображение на управление ИТ-инфраструктурой в условиях применения свободного ПО, определимся с терминологией.

Понятие свободного ПО было введено Ричардом Столлменом для поддержки научного сообщества в области разработки ПО на принципах совместной научной работы (сложившейся практики работы американских университетов конца 70-х). В основе этого понятия четыре критерия свободного ПО, они же четыре свободы (реплика на четыре свободы Рузвельта):

0. Программу можно свободно использовать с любой целью («нулевая свобода»).

1. Можно изучать, как программа работает, и адаптировать её для своих целей («первая свобода»). Условием этого является доступность исходного текста программы.

2. Можно свободно распространять копии программы — в помощь товарищу («вторая свобода»).

3. Программу можно свободно улучшать и публиковать свою улучшенную версию — с тем, чтобы принести пользу всему сообществу («третья свобода»). Условием этой третьей свободы является доступность исходного текста программы и возможность внесения в него модификаций и исправлений.

Первая и третья свободы требуют открытости кода, но термин открытое ПО считается уже чем свободное ПО. Например программа UnRar – ее исходный код опубликован, но лицензия запрещает использовать этот код для создания Rar-совместимых архиваторов.

Также есть путаница между свободным и бесплатным ПО (двойственность английского "free"). Бесплатное не обязано быть свободным – существует масса бесплатного ПО с закрытым кодом. С другой стороны свободное ПО не обязано быть бесплатным. В качестве примера можно привести RedHat Linux. В бинарном виде он распространяется только по платной подписке, но исходные коды публикуются и в результате появляется Linux CentOS – бесплатная сборка на основе этих исходных кодов. Двойственность трактовки free для бизнеса привело к распространению термина открытое ПО, хотя как уже было сказано выше это не решает проблемы свободы, а зачастую и маскирует их.

Еще одна точка столкновения мнений связана с тем, что современное ПО – это не только коды программ, но и данные. И они в принципе не подпадают под свободы Столлмена. Это еще одна из точек ветвления свободных лицензий и отправная точка появления лицензий Creative Commons.

Следующая проблема – наследование лицензии в порождаемых продуктах, так называемый копилефт (значок как зеркальное отражение копирайта). Интересный казус – ограничение свободы проявляется через принуждение соблюдать исходные свободы.

Один из компромиссов с точки зрения терминологии понятие Free Open Source Software (FOSS), но оно пока не слишком распространено.

Теперь имеет смысл поговорить собственно о свободных лицензиях как активе в управлении ИТ-инфраструктурой. Одна из первых свободных лицензий, которая появилась еще на заре операционных систем и универсального ПО – *лицензия BSD*. Эта лицензия очень простая и обладает минимумом ограничений. Фактически она заботится только об охране честного имени автора:

- Разрешается повторное распространение и использование как в виде исходного кода, так и в двоичной форме, с изменениями или без, при соблюдении следующих условий:
- При повторном распространении исходного кода должно оставаться указанное выше уведомление об авторском праве, этот список условий и последующий отказ от гарантий.
- При повторном распространении двоичного кода должна сохраняться указанная выше информация об авторском праве, этот список условий и последующий отказ от гарантий в документации и/или в других материалах, поставляемых при распространении.
- Ни название <Организации>, ни имена ее сотрудников не могут быть использованы в качестве поддержки или продвижения продуктов, основанных на этом ПО без предварительного письменного разрешения.

Плюс как и в практически любом лицензионном соглашении на ПО в лицензии BSD содержится отказ от гарантий и ответственности за убытки, которые произошли в процессе эксплуатации ПО.

Эта лицензия является не копилефтной. Она позволяет использовать код даже в проприетарном коммерческом ПО (например многие фрагменты кода FreeBSD используются в MacOSX). Также позволяется переопубликовать код под новой лицензией. Но в чистом виде это его не позволит закрыть, так как есть эта исходная лицензия, но можно закрыть модифицированный код или

бинарники на его основе. Часто лицензия BSD является требованием госконтрактов.

Есть версии этой лицензии без третьего пункта с запретом использовать название организации и имен авторов. Раньше был еще пункт с обязательной демонстрацией имен (названий) авторов, но в последствии был упразднен в связи с громоздкостью такой рекламной вставки.

Одной из наиболее распространенных сегодня лицензий на свободное ПО является лицензия *GNU's not Unix General Public License*. В ее основе лежат собственно свободы Столлмена. Эта лицензия декларирует следующее:

- Право на копирование и распространение исходного кода.
- Право на изменение исходного кода при соблюдении условий:
- Требование добавления информации об изменениях в модифицированных файлах.
- Требование лицензирования модифицированных версий под той же лицензией.
- Возможность по требованию вывода информации об авторских правах и отсутствии гарантии
- Требование предоставления исходного кода (на выбор):
    - Исполнимый код распространяется вместе с исходным.
    - Исполнимый код распространяется вместе с гарантией предоставления исходного по требованию.
    - То же с гарантией от третьей стороны.
- Лицензия прекращает действие при любом ее нарушении.
- Указание перечня актов, обозначающих принятие лицензии.
- Запрет на дополнительные ограничения при распространении.
- Невозможность внешних ограничений изменить требования лицензии. То есть независимость от законодательства – твой закон противоречит лицензии – не используй продукты под этой лицензией.
- Отказ от гарантий и ответственности.

Важный момент, связанный с использованием лицензии GPL заключается в том, что нельзя линковать программу (библиотеку), выпущенную под этой лицензией с другой программой с несовместимой лицензией.

Чтобы это обойти выпущена *GNU Lesser General Public License*. Эта лицензия постулирует, что можно линковаться с программой под любой лицензией, если она позволяет «модификации для внутреннего использования потребителем и обратную разработку для отладки таких модификаций». В частности можно связывать с несвободным ПО – копилефт действует только на саму программу, но не на другое ПО, которое с ней только связывается.

Еще одним примером свободной лицензии является *Apache License*. В этой лицензии указано, что можно свободно распространять, изменять, распространять модифицированные версии ПО, но без указания исходного названия (защита торговой марки). Можно менять лицензию и даже закрывать код и делать его платным (не копилефт), но с обязательным уведомлением получателя об использовании исходного кода под Apache лицензией. Как уже видно из требований лицензии, она несовместима с GPL, но совместима с LGPL.

Одним из компромиссных вариантов в мире свободного ПО является Mozilla Public License (MPL). Исходный код, скопированный или изменённый под лицензией MPL, должен быть лицензирован по правилам MPL. Но этот код под лицензией MPL может быть объединен в одной программе с проприетарными файлами под другими лицензиями (частичный копилефт). Лицензия несовместима с GPL, но может быть совместима с LGPL в зависимости от способа компоновки

Таблица 4.1

Лицензия	GPL	BSD	Mozilla public license	Apache software license
Требуется указывать имя автора	Да	Да	Да	Да
Измененные файлы должны быть помечены	Да	Нет	Да	Нет
Наименование производного ПО должно отличаться от наименования продукта создателей лицензии	Нет	Нет	Нет	Да*
Производные произведения должны распространяться на условиях первоначальной лицензии	Да	Нет	Да**	Нет
Отсутствие гарантий на ПО	Да	Да	Да	Да
Предоставляется право применить другую лицензию	Нет	Не указано	Да	Не указано

* Если нет письменного разрешения создателя лицензии.

** Только исходный код

С точки зрения использования свободного ПО в ИТ-инфраструктуре имеет смысл привести ряд распространенных программных компонент ИТ-инфраструктуры, выпущенных под свободными лицензиями.

Таблица 4.2

Программа	**Лицензия**
Ядро ОС Linux	GPL
ОС FreeBSD и ее модификации OpenBSD, DragonflyBSD	BSD
Окружение рабочего стола KDE	GPL
Окружение рабочего стола GNOME	GPL
Пакет OpenOffice.org	LGPL
Почтовый клиент Mozilla Thunderbird	MPL
Среда для запуска программ, работающих в среде MS Windows Win32API Wine	LGPL
Антивирусное ПО ClamAV	GPL
Apache веб-сервер	Apache license
СУБД MySQL	GPL
СУБД PostgreSQL	BSD

Теперь можно рассмотреть подробнее проблемы, связанные с использованием FOSS в России.

Согласно IV части Гражданского Кодекса Российской Федерации, Лицензионный договор заключается только в письменной форме, а отсутствие договора в письменной форме делает его недействительным. Есть правда еще один пункт, который гласит, что «Заключение лицензионных договоров о предоставлении права *использования* ПО допускается путем заключения каждым пользователем с соответствующим правообладателем договора присоединения, условия которого изложены на *приобретаемом экземпляре* такой программы или базы данных, либо на упаковке этого экземпляра. Начало использования такой программы или базы данных пользователем, как оно определяется этими условиями, означает его согласие на заключение договора». Этот пункт немного смягчает условия, но не сильно помогает в действительности. В частности остаются вопросы – является ли процесс скачивания образа с дистрибутивом операционной системы с сайта правообладателя "приобретением"? Что значит право "использования"? Что считать экземпляром, и в частности, как быть, например, с дистрибутивами операционных систем, в которые входят тысячи отдельных программ, выпущенных под разными лицензиями.

Кроме того можно отметить еще одну серьезную проблему. Большинство свободных лицензий действительны только на английском языке, тогда как если обе стороны сделки по передаче неисключительных прав являются гражданами РФ или зарегистрированы на территории РФ (программный

продукт приобретается у российской компании) – передача авторских прав должна быть оформлена на государственном языке Российской Федерации. Это затрудняет использование продуктов под свободными лицензиями в своих разработках.

С точки зрения приобретения свободного ПО как компонента ИТ-инфраструктуры можно рекомендоать следующее документальное оформление этого акта, которое позволяет снизить вероятность проблем с контролирующими органами.

Если свободное ПО было предоставлено организации Компанией-поставщиком в рамках заключения договора гражданско-правового характера (договор поставки, подряда и т. п.) в письменной форме согласно действующему российскому законодательству, рекомендуется предоставить правоохранительным органам:

- Декларацию соблюдения прав авторов и разрешенных способов использования программных продуктов, подписанную и заверенную печатью организации-поставщика.
- Оригинал договора, подписанный сторонами и заверенный печатями организации, либо его нотариально заверенную копию.
- Оригиналы документов, подтверждающих передачу программного продукта (накладная, акт приема-передачи экземпляров программного продукта, подписанный сторонами, либо его нотариально заверенную копию).
- В случае, если условия передачи авторских прав на программный продукт сформулированы в тексте самого договора и/или акта, необходимо обратить внимание представителей правоохранительных органов на соответствующие статьи договора и/или акта.
- Документы, подтверждающие факт оплаты договора.
- Оригинал лицензионного договора на программный продукт, в случае, если такой договор подписывался сторонами отдельно.
- Распечатки оригиналов лицензионных договоров, на условиях которых распространяются свободные программные программы, на английском языке и их перевод на русский язык (желательно — нотариально заверенный).
- Упаковку от программного продукта, если данный продукт был предоставлен компанией-поставщиком в «коробочной» версии.
- Также целесообразно продемонстрировать представителям правоохранительных органов интерфейсы (экраны) компьютерных программ, входящих в Сборник, содержащие тексты лицензионных договоров.

Если экземпляры свободного ПО были получены организацией путем безвозмездного скачивания их с сайта Компании-поставщика на условиях, определенных Компанией-поставщиком (путем акцепта публичной оферты Компании-поставщика и т.д.), рекомендуется предоставить правоохранительным органам:

- Ссылку на Интернет-сайт Компании-поставщика, где размещена информация об условиях предоставления экземпляров и прав на свободное ПО, а также информация о возможности бесплатной загрузки экземпляров программного продукта с сайта производителя; либо распечатки с сайта, переведенные на русский язык. Возможно также открыть и продемонстрировать соответствующую страницу Интернет-сайта в режиме он-лайн.

- Распечатки оригиналов лицензионных договоров, на условиях которых распространяются свободные программные продукты, на английском языке и их перевод на русский язык (желательно — нотариально заверенный).

- Декларацию соблюдения прав авторов и разрешенных способов использования произведений (при наличии).

- Также целесообразно продемонстрировать представителям правоохранительных органов интерфейсы (экраны) компьютерных программ, входящих в Сборник, содержащие тексты лицензионных договоров.

Если экземпляр был приобретен, например, через Интернет-магазин, документами, подтверждающими правомочность владения в случае возмездного приобретения, могут быть:

- документы, подтверждающие передачу экземпляра пользователю – накладная, акт приема-передачи;

- документы, подтверждающие оплату, в качестве которых могут выступать: кассовый чек; платежное поручение в банк или его копия об оплате экземпляра по безналичному расчету; банковская выписка по счету; документы, подтверждающие осуществление денежного почтового перевода; документы (распечатанные или в электронном виде) из систем электронного документооборота в случаях, когда платеж осуществлялся через электронные платежные системы (например, данные «Интернет-кошелька» или его аналога); выписки от соответствующих юридических лиц – операторов электронных платежных систем.

- при получении экземпляра средствами почтовой связи – извещения о регистрируемых почтовых отправлениях, простые уведомления о вручении почтовых отправлений. Пользователь может также в устной или письменной форме предоставить правоохранительным органам

данные почтового отправления (дата, номер и т. д.) и предложить представителям указанных органов запросить данные, подтверждающие рассылку, в соответствующем почтовом отделении.

Во всех случаях рекомендуется иметь полный пакет оригиналов или нотариально заверенных копий документов не только в головном офисе организации, но и во всех филиалах и отделениях организации, где используется указанное программное обеспечение.

Рекомендуется отражать все операции по приобретению программного обеспечения на балансе предприятия.

Особенности управления ИТ-инфраструктурой с точки зрения информационной безопасности на основе стратегии Microsoft Trustworthy Computing

В параграфе, посвященном особенностям управления ИТ-инфраструктурой в условиях правоприменения законодательства в области защиты персональных данных мы уже коснулись такого вопроса управления ИТ-инфраструктурой как обеспечение информационной безопасности. Очевидно, что решения в этой области могут быть только комплексными, охватывающими все уровни компоненты ИТ-инфраструктуры, а значит требуют системного подхода к их проектированию, развертыванию и эксплуатации. В качестве примера такого системного подхода можно рассмотреть стратегию построения защищенных информационных систем (Trustworthy Computing), которую разрабатывает и поддерживает в своих программных решениях (в первую очередь в серверных версиях операционных систем Windows) компания Microsoft. Это долгосрочная стратегия, направленная на обеспечение более безопасной, защищенной и надежной работы с компьютерами для всех пользователей [2].

Концепция защищенных компьютерных построена на четырех принципах:

безопасность, которая предполагает создание максимально защищенных ИТ-инфраструктур;

конфиденциальность, которая подразумевает внедрение в их состав технологий и продуктов для защиты конфиденциальности на протяжении всего периода их эксплуатации;

надежность, которая требует повышения уровня надежности процессов и технологий разработки программного обеспечения информационных систем;

целостность деловых подходов направлена на укрепление доверия клиентов, партнеров, государственных учреждений.

Для решения вопросов обеспечения информационной безопасности компания Microsoft предоставляет следующие технологии:

- Active Directory – единый каталог, позволяющий сократить число паролей, которые должен вводить пользователь;
- двухэтапная аутентификация на основе открытых/закрытых ключей и смарт-карт;
- шифрование трафика на базе встроенных средств операционной системы IPSec (IP Security - это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов);
- создание защищенных беспроводных сетей на основе стандарта IEEE 802.1x;
- шифрование файловой системы;
- защита от вредоносного кода;
- организация безопасного доступа мобильных и удаленных пользователей;
- защита данных на основе кластеризации, резервного копирования и несанкционированного доступа;
- служба сбора событий из системных журналов безопасности.

Механизм управления групповыми политиками

Управление групповыми политиками позволяет администраторам задавать конфигурацию операционных систем серверов и клиентских компьютеров. Реализуется эта функциональность с помощью оснастки «Редактор объектов групповой политики».

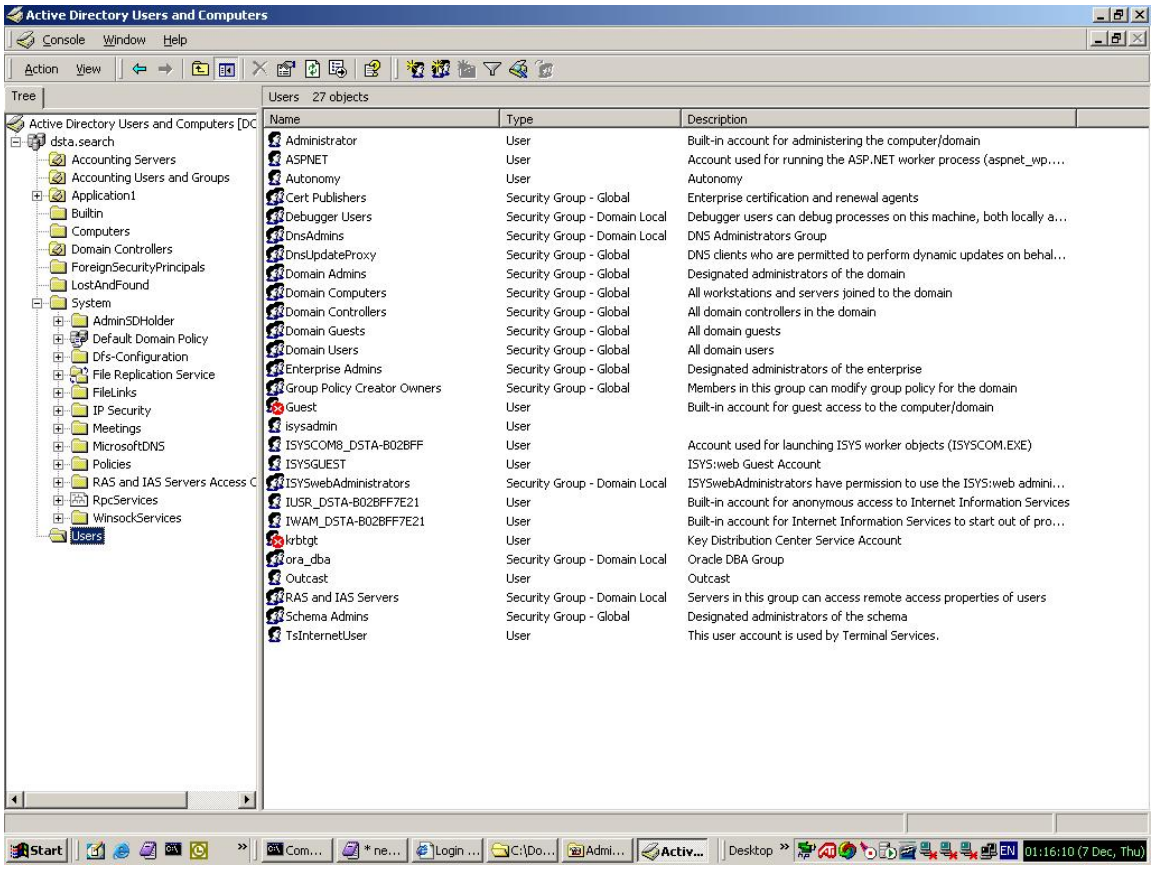

Рисунок 3.13

Для компьютеров, входящих в домен Active Directory, используются групповые политики, определяющие политики безопасности, используемые в рамках сайта, домена или набора организационных единиц (OU – organizational units).

Групповые политики и Active Directory позволяют:

- централизованно управлять пользователями и компьютерами в масштабах предприятия;
- автоматически применять политики информационной безопасности;
- понижать сложность административных задач (например, обновление операционных систем, установка приложений);
- унифицировать параметры безопасности в масштабах предприятия;
- обеспечить эффективную реализацию стандартных вычислительных средств для групп пользователей.

При управлении безопасностью информационной системы предприятия групповая политика позволяет управлять контроллерами доменов и серверами, определять наборы параметров для конкретной группы пользователей, параметры защиты, сетевой конфигурации и ряд других параметров, применяемых к определенной группе компьютеров.

Active Directory позволяет управлять через групповые политики любыми службами и компонентами на платформе Windows.

Групповые политики Active Directory позволяют администраторам централизованно управлять ИТ-инфраструктурой предприятия. С помощью групповой политики можно создавать легко управляемую ИТ-инфраструктуру. Эти возможности позволяют снизить уровень ошибок пользователей при модификации параметров операционных систем и приложений, а также совокупную стоимость владения информационной системы, связанную с администрированием распределенных сетей.

Групповая политика позволяет создать ИТ-инфраструктуру предприятия, ориентированную на потребности пользователей, сформированные в строгом соответствии с их должностными обязанностями и уровнем квалификации.

Применение групповых политик и Active Directory для сайтов, доменов и организационных единиц необходимо реализовывать с учетом следующих правил:

- объекты групповой политики (GPO) хранятся в каждом домене индивидуально;
- с одним сайтом, доменом или организационной единицей может быть сопоставлено несколько GPO;
- с несколько сайтов, доменов или организационных единиц могут использовать единственную GPO;
- любому сайту, домену или организационной единице можно сопоставить любую GPO;
- параметры, определяемые GPO, можно фильтровать для конкретных групп пользователей или компьютеров на основе их членства в группах безопасности или с помощью WMI-фильтров.

При администрировании ИТ-инфраструктуры предприятия администраторы посредством механизма групповой политики могут производить настройку приложений, операционных систем, безопасность рабочей среды пользователей и информационных систем в целом. Для этого используются следующие возможности:

- политика на основе реестра. С помощью редактора объектов групповой политики можно задать параметры в реестре для приложений, операционной системы и её компонентов;
- параметры безопасности. Администраторы могут указывать параметры локальной, доменной и сетевой защиты для компьютеров и пользователей в области действия GPO, используя шаблоны безопасности;

- ограничения на использование программ. Данные ограничения предназначены для защиты от вирусов, выполнения нежелательных программ и атак на компьютеры;
- распространение и установка программ. Обеспечивается возможность централизованного управления установкой, обновлением и удалением приложений;
- сценарии для компьютеров и пользователей. Данные средства позволяют автоматизировать операции, выполняемые при запуске и выключении компьютера, при входе и выходе пользователя;
- мобильные пользовательские профили и перенаправление папок. Профили хранятся на сервере и позволяют загружаться на тот компьютер, где пользователь входит в систему. Перенаправление папок позволяет размещать важные для пользователя папки на сервере;
- автономные папки. Данный механизм позволяет создавать копии сетевых папок, синхронизировать их с сетью и работать с ними при отключении сети;
- поддержка Internet Explorer. Эта возможность позволяет администраторам проводить управление конфигурацией Microsoft Internet Explorer на компьютерах с поддержкой групповой политики.

Для общего контроля применения групповой политики используются механизм WMI – фильтров (Windows Management Instrumentation). Данное решение позволяет администраторам создавать и модифицировать WMI – запросы для фильтрации параметров безопасности, определяемых групповыми политиками. WMI – фильтры позволяют динамически задавать область действия групповой политики на основе атрибутов целевого компьютера.

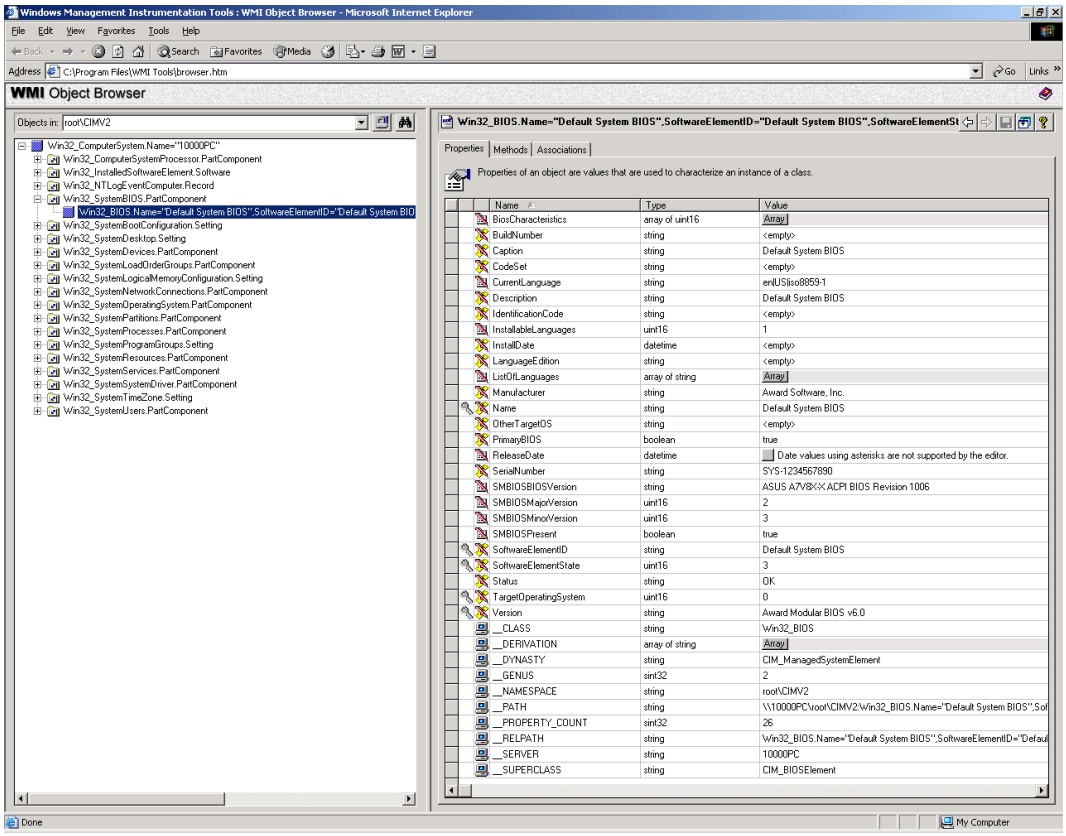

Рисунок 3.14

Применение механизма групповой политики для ИТ-инфраструктуры предприятия способствует снижению сложности решения задач развертывания обновлений, установки приложений, настройки профилей пользователей и, в целом, администрирования информационной системы. Применение групповой политики в информационной системе предприятия дает следующие преимущества:

- повышение эффективности использования инфраструктуры Active Directory;
- повышение гибкости выбора области администрирования для предприятий, различающихся по размеру и отраслевой принадлежности, при происходящих изменениях в бизнесе;
- наличие интегрированного средства управления групповой политикой на основе консоли GPMC;
- простота в использовании, которая обеспечивается удобным и понятным пользовательским интерфейсом консоли GPMC, что приводит к сокращению расходов на обучение и повышает эффективность руда администраторов;
- надежность и безопасность действий администраторов за счет автоматизации процесса ввода групповых политик в действие;
- централизованное управление конфигурациями на основе стандартизации пользовательских вычислительных сред.

Управление авторизацией и аутентификацией пользователей

Многие компоненты ИТ-инфраструктуры являются потенциально уязвимыми перед попытками неавторизованного доступа со стороны злоумышленников. Контроль и управление идентификацией пользователей может быть осуществлен на базе инфраструктуры открытых ключей.

Инфраструктура открытых ключей PKI (public key infrastructure) – это системы цифровых сертификатов, центров сертификации CA (certification authorities) и других центров регистрации RA (registration authorities), которые идентифицируют (проверяют подлинность) каждой стороны, участвующей в электронной транзакции, с применением шифрования открытым ключом (public key). Службы сертификации (Certification Services) и средства управления сертификатами позволяют построить предприятию собственную инфраструктуру открытых ключей.

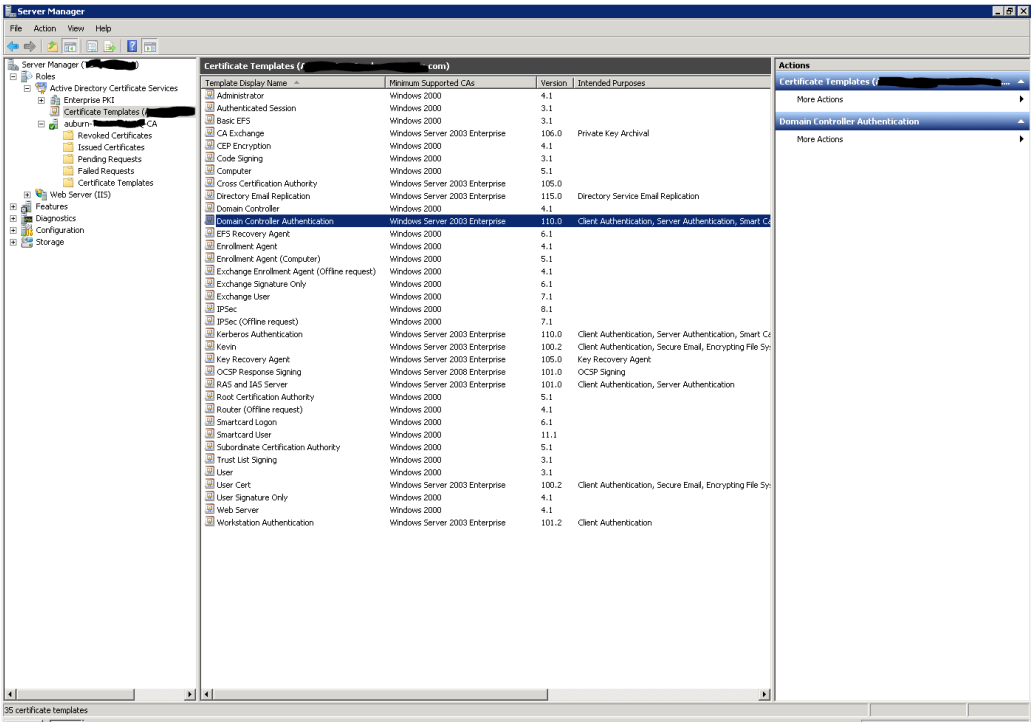

Рисунок 3.15

Применение инфраструктуры открытых ключей обеспечивает следующие преимущества для информационной системы предприятия:

- *более устойчивая к взлому защита*, которая базируется на аутентификации с высокой степенью защищенности и применении смарт-карт, использовании протокола IPSec для поддержания целостности и защиты данных от попыток несанкционированной модификации при передаче по общедоступным сетям, а также использовании шифрующей файловой системы для защиты конфиденциальных данных, хранящихся на сервере;

- *упрощение администрирования* за счет создания сертификатов, которые позволяют избавиться от применения паролей, масштабировать доверительные отношения в рамках предприятия;

- *дополнительные возможности,* которые обеспечивают безопасный обмен файлами и данными между сотрудниками предприятия по общедоступным сетям, защищенную электронную почту и безопасное соединение через Web;

- *использование сертификатов*, которые представляют собой цифровой документ, выпускаемый центром сертификации и подтверждающий идентификацию владельца данного сертификата. Сертификат связывает открытый ключ с идентификацией лица, компьютера или службы, которые имеют соответствующий закрытый ключ;

- *службы сертификации,* которые применяются при создании и управлении центрами сертификации. В корпоративной информационной системе может быть один или несколько центров сертификации, которые управляются через оснастку Центр сертификации консоли MMC;

- *шаблоны сертификатов*, которые представляют собой набор правил и параметров, применяемых к входящим запросам на сертификаты определенного типа;

- *автоматическая подача заявок на сертификаты*, которая позволяет администратору конфигурировать субъекты сертификатов для автоматического запроса сертификатов, получения выданных сертификатов и возобновления просроченных сертификатов без участия их субъектов;

- *Web-страницы подачи заявок на сертификаты*, которые позволяют подавать заявки на сертификаты через Web-браузер;

- *политики открытых ключей*, которые позволяют автоматически распространять сертификаты их субъектам, определять общие доверяемые центры сертификации и проводить управление политиками восстановления данных;

- *поддержка смарт-карт,* которая позволяет обеспечивать вход в систему через сертификаты на смарт-картах, хранение на них сертификатов и закрытых ключей. Смарт-карты предназначены для обеспечения безопасности аутентификации клиентов, входа в домен под управлением Windows Server, цифрового подписания программного кода, работы с защищенной электронной почтой на основе применения шифрования с открытыми ключами.

Управление защитой коммуникаций

Для защиты коммуникаций предназначена технология IP-безопасности, базирующаяся на протоколе IPSec (IP Security). В корпоративной информационной системе данная технология должна обеспечивать защиту от:

- изменения данных при пересылке;
- перехвата, просмотра и копирования данных;
- несанкционированного изменения определенных ролей в системе;
- перехвата и повторного использования пакетов для получения доступа к конфиденциальным ресурсам.

Протокол IPSec представляет протокол транспортного уровня с защитой данных на основе шифрования, цифровой подписи и алгоритмов хеширования. Он обеспечивает безопасность на уровне отдельных IP-пакетов, что позволяет защищать обмен данными в общедоступных сетях и обмен данными между приложениями, не имеющими собственных средств безопасности.

IPSec в Windows Server 2003 интегрирован с политиками безопасности Active Directory, что обеспечивает хорошую защищенность интрасетей и коммуникаций через Internet.

В IPSec предусмотрены криптографические механизмы хеширования и шифрования для предупреждения атак. Протокол имеет следующие средства защиты:

- аутентификация отправителя на основе цифровой подписи;
- проверка целостности данных на основе алгоритмов хеширования;
- использование алгоритмов шифрования DES и 3DES;
- защита от воспроизведения пакетов;
- свойство неотрекаемости (nonrepudiat ion), которое предполагает применение цифровой подписи для однозначного доказательства авторства сообщения;
- динамическая генерация ключей при передаче данных;
- алгоритм согласования ключей Диффи-Хелмана, который позволяет согласовывать ключ, не передавая его по сети;
- возможность задавать длину ключей.

При передаче данных с одного компьютера на другой по протоколу IPSec согласовывается уровень защиты, используемый в сеансе. В процессе согласования определяются методы аутентификации, хеширования, возможно туннелирования и шифрования. Секретные ключи для аутентификации создаются на каждом компьютере локально на основе информации, которой они обмениваются. Эта информация не передается по сети. После создания ключа выполняется аутентификация и инициируется сеанс защищенного обмена данными.

Защита от вторжений должна обеспечить профилактические меры по защите компьютеров и данных. Эти задачи решает Microsoft ISA (Internet Security and Acceleration) Server, который включает в себя межсетевой экран прикладного уровня, поддержку виртуальных частных сетей (Virtual Public Netware – VPN), Web-кэширование, фильтры прикладного уровня,защищая корпоративные информационные системы от внутренних и внешних атак. Сервер выполняет динамическую проверку потока данных и расширенную фильтрацию различных протоколов Интернета на прикладном уровне, что позволяет противостоять угрозам, не обнаруживаемым традиционными межсетевыми экранами. ISA Server 2004 позволяет:

- защитить периметр сети;
- увеличить скорость доступа к Интернету за счет кэширования Web-страниц;
- обеспечить безопасную публикацию Web-сервисов IIS;
- предоставлять доступ VPN-клиентам к ресурсам сети и сервисам, в случае исполнения роли сервера VPN;
- объединять локальные сети через VPN-соединение, в случае исполнения роли шлюза VPN;
- расширить возможности мониторинга и регистрации VPN-соединений, позволяя отслеживать и сохранять трафик на уровне отдельных приложений;
- составлять отчеты, используя встроенные средства;
- фильтровать пакеты для всех сетевых интерфейсов;
- осуществлять поддержку туннельного режима IPSec для VPN-подключений «точка – точка»;
- поддерживать режим Windows Quarantine (сетевой карантин), что повышает безопасность работы удаленных пользователей;
- поддерживать произвольную топологию и неограниченное количество сетей.

Задачи безопасности, а также надежности, масштабируемости, быстродействия при управлении Web-серверами обеспечиваются полнофункциональным Web-сервером Internet Information Services (IIS). Службы IIS базируются на архитектуре обработки запросов, которая реализует среду с изоляцией приложений. Это обеспечивает функционирование отдельных Web-приложений в собственном Web-процессе. При таком режиме работа приложений и сайтов реализуется обособлено рабочими процессами, полностью изолированными от ядра Web-сервера, что исключает их влияние друг на друга.

В IIS включены разнообразные средства управления для администрирования и конфигурирования ИТ-инфраструктуры предприятия. Системные администраторы могут изменять параметры и отлаживать приложения во время работы служб.

Решения Microsoft для обеспечения повышенной защиты от компьютерных атак и воздействия вредоносного ПО включают следующие продукты:

- Windows Defender помогает блокировать «всплывающие» браузерные окна и пресекает деятельность программ-шпионов (spyware);
- Microsoft Client Protection (MCP) помогает защитить настольные компьютеры, портативные ПК и серверы от внезапных внешних сетевых угроз;
- Certificate Lifecycle Manager— решение на основе анализа бизнес-процессов, помогающее предприятиям управлять жизненным циклом цифровых сертификатов и смарт-карт;
- Windows Malicious Software Removal Tool (MSRT) — выполняет проверку системы и удаляет самое распространенное вредоносное ПО в случае его обнаружения;
- Windows OneCare™ Live содержит антивирусный модуль, брандмауэр, систему резервного копирования и восстановления данных и другие средства защиты.

Безопасность мобильных пользователей корпоративных систем

Для безопасной работы мобильных пользователей используются следующие виды защиты:

- защита домена;
- защита мобильного устройства;
- защита беспроводных соединений.

При *защите домена* мобильные устройства должны отвечать требованиям аутентификации, применяемым на предприятии. Например, устройства, работающие под управлением Windows Mobile, поддерживают двухэтапную аутентификацию и позволяют применять стойкие пароли, биометрические технологии и сертификаты. Устройства с Windows Mobile можно интегрировать в существующую инфраструктуру открытых ключей.

Защиту мобильных устройств, работающих под управлением Windows Mobile, поддерживают средства защиты, которые позволяют защищать информацию, хранящуюся на таких устройствах. Это предотвращает несанкционированный доступ к данным в случае утери или кражи

мобильного устройства. В Windows Mobile в дополнение к поддержке строгих паролей встроены средства шифрования данных.

Для *защиты беспроводных соединений* сетевые администраторы должны контролировать процесс доступа этих устройств к корпоративной сети предприятия. Кроме того информация, передаваемая по беспроводной сети должна шифроваться.

Одним из решений по организации доступа сотрудников, находящихся вне предприятия, к корпоративной сети является организация виртуальной частной сети – VPN. Для контроля доступа к приложениям в серверной операционной системе имеется служба сетевого карантина (Windows Quarantine). Карантин используется в сети для проверки состояния клиента пред тем, как предоставить ему доступ к защищенным сетям. Карантинный фильтр на основании политики безопасности может запретить доступ и не разрешать его до тех пор пока настройки подключаемого компьютера не будут удовлетворять требованиям политики безопасности. Для применения карантина требуется, чтобы эта служба поддерживалась и клиентом и сервером аутентификации.

Сервер терминалов (Terminal Server) позволяет с удаленных клиентских компьютеров получить через сеть доступ к приложениям, установленным на сервере. Сервер терминалов обеспечивает шифрование канала связи. Для аутентификации соединений со службами терминалов и шифрования коммуникаций с сервером терминалов применяется Secure Sockets Layer (SSL) / Transport Layer Security (TLS).

SSL – протокол шифрованной передачи данных между клиентом и сервером, который требует сертификата, выданного одним из авторизованных центров. TLS — криптографический протокол, который обеспечивает безопасную передачу данных между узлами в сети Internet. SSL, используя криптографию, предоставляет возможности аутентификации и безопасной передачи данных через Internet. Часто происходит лишь аутентификация сервера, в то время как клиент остается неаутентифицированным. Для взаимной аутентификации каждая из сторон должна поддерживать инфраструктуру открытых ключей

SSL включает в себя три основных фазы:

- диалог между сторонами, целью которого является выбор алгоритма шифрования;
- обмен ключами на основе криптосистем с открытым ключом или аутентификация на основе сертификата;
- передача данных, шифруемых при помощи симметричных алгоритмов шифрования.

Для корректной работы аутентификации SSL (TLS) удаленные клиенты должны:

- работать под управлением Windows 2000 или Windows XP;
- использовать клиент протокола RDP (Remote Desktop Protocol);
- доверять корневому сертификату сервера.

Управление безопасностью хранения данных

Для защиты данных применяются технологии кластеризации, теневого копирования, а также службы управления правами и Data Protection Manager.

Служба кластеров (Cluster Service, MSCS) обеспечивает высокую отказоустойчивость и масштабируемость для баз данных, коммуникационных систем, файловых служб и служб печати. В системе реализуется режим автоматического восстановления после сбоя, при котором в случае недоступности одного узла кластера обработку начинает проводить другой узел. Совместно со службой кластеров используется служба балансировки сетевой нагрузки (Network Load Balancing Service, NLBS), которая обеспечивает балансировку нагрузки, создаваемую IP-трафиком, между кластерами. Служба NLBS повышает отказоустойчивость и масштабируемость приложений, размещаемых на серверах в Internet (Web-серверах, серверах, передающих потоковую информацию, служб терминалов).

Интеграция служб кластеризации с Active Directory позволяет проводить регистрацию в Active Directory «виртуального» объекта компьютера, поддерживать аутентификацию через Kerberos и обеспечивать тесную интеграцию с другими службами, публикующими информацию о себе в Active Directory.

Теневое копирование общих папок в Windows Server 2003 помогает предотвратить случайную потерю данных и обеспечивает экономичный способ восстановления данных, утраченных в результате ошибки пользователя. При теневом копировании регулярно, через заданный интервал времени, создается теневые копии файлов и папок, хранящиеся в общих сетевых папках. Теневая копия представляет предыдущую версию файла или паки по состоянию на определенный момент времени.

Теневые копии упрощают текущее восстановление поврежденных файлов, но они не заменяют процедуры резервного копирования, создания архивов, полнофункциональной системы восстановления данных.

Теневые копии не обеспечивают защиту от потери данных при сбоях или повреждении физического носителя. Тем не менее восстановление данных из теневых копий уменьшает количество случаев, в которых приходится прибегать к восстановлению данных из архивов.

Следует отметить, что теневые копии не предназначены для использования в качестве средств управления версиями документов. Это временные копии, автоматически создаваемые по расписанию.

Microsoft System Center Data Protection Manager (DPM) предназначен для резервного копирования на диск. DPM обеспечивает постоянную эффективную защиту данных, быстрое и надежное их восстановление. Это реализуется путем использования репликации, а также инфраструктуры службы теневого копирования томов.

Резервное копирование с использованием DPM может быть централизованным (копирование по схеме «диск-диск-лента в центре обработки данных») и децентрализованным (резервные копии передаются на центральный сервер DPM).

При восстановлении данных могут выполняться следующие сценарии:

- полное восстановление сервера администраторами сервера;
- восстановление файлов администраторами сервера;
- восстановление файлов ИТ-службой;
- восстановление файлов самими пользователями.

Примеры инфраструктурных решений, применяющихся в крупных сетевых проектах

Пример реализации инфраструктуры в Google

Сегодня Google это далеко не только поисковая система. Это огромная сервисно-ориентированная платформа для построения масштабируемых приложений, позволяющая выпускать и поддерживать множество конкурентоспособных интернет-приложений, работающих на уровне всей глобальной сети. Компания ставит перед собой цель постоянно строить все более и более производительную и масштабируемую инфраструктуру для поддержки своих продуктов. Рассмотрим основные принципы и компоненты этого инфраструктурного решения. Но сначала несколько цифр, для того, чтобы представить масштабы решения.

Система включает в себя около 1 миллиона недорогих серверов (почти 2 % всех серверов в мире).

Google включает в себя более 400 GFS кластеров. Один кластер может состоять из 1000 или даже 5000 компьютеров.

Десятки и сотни тысяч компьютеров получают данные из GFS кластеров, которые насчитывают более 10 петабайт дискового пространства. Суммарные пропускная способность операций записи и чтения между дата центрами может достигать 40 гигабайт в секунду

Система BigTable позволяет хранить миллиарды ссылок (URL), сотни терабайт снимков со спутников, а также настройки миллионов пользователей

Google визуализирует свою инфраструктуру в виде трехслойного стека:

Продукты: поиск, реклама, электронная почта, карты, видео, чат, блоги и т.п.

Распределенная инфраструктура системы: GFS, MapReduce и BigTable

Вычислительные платформы: множество компьютеров во множестве датацентров

При этом поддерживаются два принципа:

Легкое развертывание для компании при низком уровне издержек

Больше денег вкладывается в оборудование для исключения возможности потерь данных

С точки зрения ИТ-инфраструктуры нас интересуют в первую очередь решения, расположенные на втором слое.

Распределенная файловая система GFS (Google File System)

GFS является наиболее, наверное, известной распределенной файловой системой. Надежное масштабируемое хранение данных крайне необходимо для любого приложения, работающего с таким большим массивом данных, как все документы в интернете. GFS является основной платформой хранения информации в Google. GFS — большая распределенная файловая система, способная хранить и обрабатывать огромные объемы информации.

GFS строилась исходя из следующим критериев:

- Система строится из большого количества обыкновенного недорого оборудования, которое часто дает сбои. Должны существовать мониторинг сбоев, и возможность в случае отказа какого-либо оборудования восстановить функционирование системы.
- Система должна хранить много больших файлов. Как правило, несколько миллионов файлов, каждый от 100 Мб и больше. Также часто приходится иметь дело с многогигабайтными файлами, которые также должны эффективно храниться. Маленькие файлы тоже должны храниться, но для них не оптимизируется работа системы.
- Как правило, встречаются два вида чтения: чтение большого последовательного фрагмента данных и чтение маленького объема произвольных данных. При чтении большого потока данных обычным делом является запрос фрагмента размером в 1Мб и больше. Такие последовательные операции от одного клиента часто читают подряд

идущие куски одного и того же файла. Чтение небольшого размера данных, как правило, имеет объем в несколько килобайт. Приложения, критические по времени исполнения, должны накопить определенное количество таких запросов и отсортировать их по смещению от начала файла. Это позволит избежать при чтении блужданий вида назад-вперед.

- Часто встречаются операции записи большого последовательного куска данных, который необходимо дописать в файл. Обычно, объемы данных для записи такого же порядка, что и для чтения. Записи небольших объемов, но в произвольные места файла, как правило, выполняются не эффективно.

- Система должна реализовывать строго очерченную семантику параллельной работы нескольких клиентов, в случае если они одновременно пытаются дописать данные в один и тот же файл. При этом может случиться так, что поступят одновременно сотни запросов на запись в один файл. Для того чтобы справится с этим, используется атомарность операций добавления данных в файл, с некоторой синхронизацией. То есть если поступит операция на чтение, то она будет выполняться, либо до очередной операции записи, либо после.

- Высокая пропускная способность является более предпочтительной, чем маленькая задержка. Так, большинство приложений в Google отдают предпочтение работе с большими объемами данных, на высокой скорости, а выполнение отдельно взятой операции чтения и записи, вообще говоря, может быть растянуто.

Файлы в GFS организованы иерархически, при помощи каталогов, как и в любой другой файловой системе, и идентифицируются своим путем. С файлами в GFS можно выполнять обычные операции: создание, удаление, открытие, закрытие, чтение и запись.

Более того, GFS поддерживает резервные копии, или снимки (snapshot). Можно создавать такие резервные копии для файлов или дерева директорий, причем с небольшими затратами.

Архитектура GFS

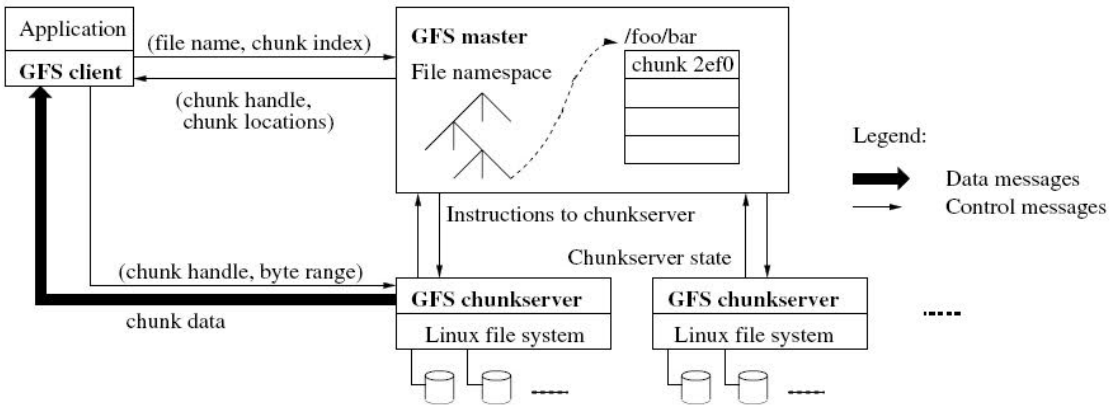

Рисунок 3.16

В системе существуют мастер-сервера и чанк-сервера, собственно, хранящие данные. Как правило, GFSкластер состоит из одной главной машины мастера (master) и множества машин, хранящих фрагменты файлов чанк-серверы (chunkservers). Клиенты имеют доступ ко всем этим машинам. Файлы в GFS разбиваются на куски — чанки (chunk, можно сказать фрагмент). Чанк имеет фиксированный размер, который может настраиваться. Каждый такой чанк имеет уникальный и глобальный 64 — битный ключ, который выдается мастером при создании чанка. Чанк-серверы хранят чанки, как обычные Linux файлы, на локальном жестком диске. Для надежности каждый чанк может реплицироваться на другие чанк-серверы. Обычно используются три реплики.

Мастер отвечает за работу с метаданными всей файловой системы. Метаданные включают в себя пространства имен, информацию о контроле доступа к данным, отображение файлов в чанки, и текущее положение чанков. Также мастер контролирует всю глобальную деятельность системы такую, как управление свободными чанками, сборка мусора (сбор более ненужных чанков) и перемещение чанков между чанк-серверами. Мастер постоянно обменивается сообщениями (HeartBeat messages) с чанк-серверами, чтобы отдать инструкции, и определить их состояние (узнать, живы ли еще).

Клиент взаимодействует с мастером только для выполнения операций, связанных с метаданными. Все операции с самими данными производятся напрямую с чанк-серверами. GFS — система не поддерживает POSIX API, так что разработчикам не пришлось связываться с VNode уровнем Linux.

Разработчики не используют кеширование данных, правда, клиенты кешируют метаданные. На чанк-серверах операционная система Linux и так кеширует наиболее используемые блоки в памяти. Вообще, отказ от кеширования позволяет не думать о проблеме валидности кеша (cache coherence).

Использование одного мастера существенно упрощает архитектуру системы. Позволяет производить сложные перемещения чанков, организовывать репликации, используя глобальные данные. Казалось бы, что наличие только одного мастера должно являться узким местом системы, но это не так. Клиенты никогда не читают и не пишут данные через мастера. Вместо этого они спрашивают у мастера, с каким чанк-сервером они должны контактировать, а далее они общаются с чанк-серверами напрямую.

Рассмотрим, как происходит чтение данных клиентом. Сначала, зная размер чанка,

имя файла и смещение относительно начала файла, клиент определяет номер чанка внутри файла. Затем он шлет запрос мастеру, содержащий имя файла и номер чанка в этом файле. Мастер выдает чанк-серверы, по одному в каждой реплике, которые хранят нужный нам чанк. Также мастер выдает клиенту идентификатор чанка.

Затем клиент решает, какая из реплик ему нравится больше (как правило та, которая ближе), и шлет запрос, состоящий из чанка и смещения относительно начала чанка. Дальнейшее чтения данных, не требует вмешательства мастера. На практике, как правило, клиент в один запрос на чтение включает сразу несколько чанков, и мастер дает координаты каждого из чанков в одном ответе.

Размер чанка является важной характеристикой системы. Как правило, он устанавливается равным 64 мегабайт, что гораздо больше, чем размер блока в обычной файловой системе. Понятно, что если необходимо хранить много файлов, размеры которых меньше размера чанка, то будем расходоваться много лишней памяти. Но выбор такого большого размера чанка обусловлен задачами, которые приходится компании Google решать на своих кластерах. Как правило, что-то считать приходится для всех документов в интернете, и поэтому файлы в этих задачах очень большого размера.

Мастер хранит три важных вида метаданных: пространства имен файлов и чанков, отображение файла в чанки и положение реплик чанков. Все метаданные хранятся в памяти мастера. Так как метаданные хранятся в памяти, операции мастера выполняются быстро. Состояние дел в системе мастер узнает просто и эффективно. Он выполняется сканирование чанк-серверов в фоновом режиме. Эти периодические сканирования используются для сборки мусора, дополнительных репликаций, в случае обнаружения недоступного чанк-сервера и перемещение чанков, для балансировки нагрузки и свободного места на жестких дисках чанк-серверов.

Мастер отслеживает положение чанков. При старте чанк-сервера мастер запоминает его чанки. В процессе работы мастер контролирует все перемещения чанков и состояния чанк-серверов. Таким образом, он обладает всей информацией о положении каждого чанка.

Важная часть метаданных — это лог операций. Мастер хранит последовательность операций критических изменений метаданных. По этим отметкам в логе операций, определяется логическое время системы. Именно это логическое время определяет версии файлов и чанков.

Так как лог операций важная часть, то он должен надежно храниться, и все изменения в нем должны становиться видимыми для клиентов, только когда изменятся метаданные. Лог операций реплицируется на несколько удаленных машин, и система реагирует на клиентскую операцию, только после сохранения этого лога на диск мастера и диски удаленных машин.

Мастер восстанавливает состояние системы, исполняя лог операций. Лог операций сохраняет относительно небольшой размер, сохраняя только последние операции. В процессе работы мастер создает контрольные точки, когда размер лога превосходит некоторой величины, и восстановить систему можно только до ближайшей контрольной точки. Далее по логу можно заново воспроизвести некоторые операции, таким образом, система может откатываться до точки, которая находится между последней контрольной точкой и текущем временем.

Взаимодействия внутри системы

Каждое изменение чанка должно дублироваться на всех репликах и изменять метаданные. В GFS мастер дает чанк во владение(lease) одному из серверов, хранящих этот чанк. Такой сервер называется первичной (primary) репликой. Остальные реплики объявляются вторичными (secondary). Первичная реплика собирает последовательные изменения чанка, и все реплики следуют этой последовательности, когда эти изменения происходят.

Механизм владения чанком устроен таким образом, чтобы минимизировать нагрузку на мастера. При выделении памяти сначала выжидается 60 секунд. А затем, если потребуется первичная реплика может запросить мастера на расширение этого интервала и, как правило, получает положительный ответ. В течение этого выжидаемого периода мастер может отменить изменения.

Рассмотрим подробно процесс записи данных. Он изображен по шагам на рисунке, при этом тонким линиям соответствуют потоки управления, а жирным потоки данных.

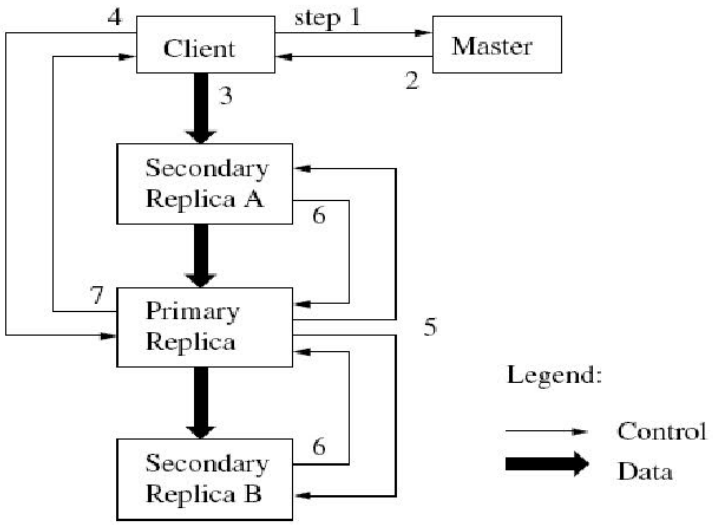

Рисунок 3.17

Клиент спрашивает мастера, какой из чанк-серверов владеет чанком, и где находится этот чанк в других репликах. Если необходимо, то мастер отдает чанк кому-то во владение.

Мастер в ответ выдает первичную реплику, и остальные (вторичные) реплики. Клиент хранит эти данные для дальнейших действий. Теперь, общение с мастером клиенту может понадобиться только, если первичная реплика станет недоступной.

Далее клиент отсылает данные во все реплики. Он может это делать в произвольном порядке. Каждый чанк-сервер будет их хранить в специальном буфере, пока они не понадобятся или не устареют.

Когда все реплики примут эти данные, клиент посылает запрос на запись первичной реплике. В этом запросе содержатся идентификация данных, которые были посланы в шаге 3. Теперь первичная реплика устанавливает порядок, в котором должны выполняться все изменения, которые она получила, возможно от нескольких клиентов параллельно. И затем, выполняет эти изменения локально в этом определенном порядке.

Первичная реплика пересылает запрос на запись всем вторичным репликам. Каждая вторичная реплика выполняет эти изменения в порядке, определенном первичной репликой.

Вторичные реплики рапортуют об успешном выполнении этих операций.

Первичная реплика шлет ответ клиенту. Любые ошибки, возникшие в какой-либо реплике, также отсылаются клиенту. Если ошибка возникла при записи в первичной реплике, то и запись во вторичные реплики не происходит, иначе запись произошла в первичной реплике, и подмножестве вторичных. В этом случае клиент обрабатывает ошибку и решает, что ему дальше с ней делать.

Из примера выше видно, что создатели разделили поток данных и поток управления. Если поток управления идет только в первичную реплику, то поток данных идет во все реплики. Это сделано, чтобы избежать создания узких мест в сети, а взамен широко использовать пропускную способность каждой машины. Так же, чтобы избежать узких мест и перегруженных связей, используется схема передачи ближайшему соседу по сетевой топологии. Допустим, что клиент передает данные чанк-серверам S1,...,S4. Клиент шлет ближайшему серверу данные, пусть S1. Он далее пересылает ближайшему серверу, пусть будет S2. Далее S2 пересылает их ближайшему S3 или S4, и так далее.

Также задержка минимизируется за счет использования конвейеризации пакетов передаваемых данных поTCP. То есть, как только чанк-сервер получил какую-то часть данных, он немедленно начинает их пересылать. Без сетевых заторов, идеальное время рассылки данных объемом B байт на R реплик будетB/T + RL, где T сетевая пропускная способность, а L — задержка при пересылке одного байта между двумя машинами.

GFS поддерживает такую операцию, как атомарное добавление данных в файл. Обычно, при записи каких-то данных в файл, мы указываем эти данные и смещение. Если несколько клиентов производят подобную операцию, то эти операции нельзя переставлять местами (это может привести к некорректной работе). Если же мы просто хотим дописать данные в файл, то в этом случае мы указываем только сами данные.GFS добавит их атомарной операцией. Вообще говоря, если операция не выполнилась на одной из вторичных реплик, то GFS, вернет ошибку, а данные будут на разных репликах различны.

Еще одна интересная вещь в GFS — это резервные копии (еще можно сказать мгновенный снимок) файла или дерева директорий, которые создаются почти мгновенно, при этом, почти не прерывая выполняющиеся операции в системе. Это получается за счет технологии похожей на copy on write. Пользователи используют эту возможность для создания веток данных или как промежуточную точку, для начала каких-то экспериментов.

Операции, выполняемые мастером

Мастер важное звено в системе. Он управляет репликациями чанков: принимает решения о размещении, создает новые чанки, а также координирует различную деятельность внутри системы для сохранения чанков полностью реплицированными, балансировки нагрузки на чанк-серверы и сборки неиспользуемых ресурсов.

В отличие от большинства файловых систем GFS не хранит состав файлов в директории. GFS логически представляет пространство имен, как таблицу, которая отображает каждый путь в метаданные. Такая таблица может эффективно храниться в памяти в виде бора (словаря этих самых путей). Каждая вершина в этом дереве (соответствует либо абсолютному пути к

файлу, либо к директории) имеет соответствующие данные для блокировки чтения и записи(read write lock). Каждое операция мастера требует установления некоторых блокировок. В этом месте в системе используются блокировки чтения-записи. Обычно, если операция работает с /d1/d2/.../dn/leaf, то она устанавливает блокировки на чтение на /d1, /d1/d2, ..., d1/d2/.../dn и блокировку, либо на чтение, либо на запись нad1/d2/.../dn/leaf. При этом leaf может быть как директорией, так и файлом.

Покажем на примере, как механизм блокировок может предотвратить создание файла /home/user/foo во время резервного копирования /home/user в /save/user. Операция резервного копирования устанавливает блокировки на чтение на /home и /save, а так же блокировки на запись на /home/user и/save/user. Операция создания файла требует блокировки на чтение /home и /home/user, а также блокировки на запись на /home/user/foo. Таким образом, вторая операция не начнет выполняться, пока не закончит выполнение первая, так как есть конфликтующая блокировка на /home/user. При создании файла не требуется блокировка на запись родительской директории, достаточно блокировки на чтение, которая предотвращает удаление этой директории.

Кластеры GFS, являются сильно распределенными и многоуровневыми. Обычно, такой кластер имеет сотни чанк-серверов, расположенных на разных стойках. Эти сервера, вообще говоря, доступны для большого количества клиентов, расположенных в той же или другой стойке. Соединения между двумя машинами из различных стоек может проходить через один или несколько свитчей. Многоуровневое распределение представляет очень сложную задачу надежного, масштабируемого и доступного распространения данных.

Политика расположения реплик старается удовлетворить следующим свойствам: максимизация надежности и доступности данных и максимизация использование сетевой пропускной способности. Реплики должны быть расположены не только на разных дисках или разных машинах, но и более того на разных стойках. Это гарантирует, что чанк доступен, даже если целая стойка повреждена или отключена от сети. При таком расположении чтение занимает время приблизительно равное пропускной способности сети, зато поток данных при записи должен пройти через различные стойки.

Когда мастер создает чанк, он выбирает где разместить реплику. Он исходит из нескольких факторов:

Желательно поместить новую реплику на чанк-сервер с наименьшей средней загруженностью дисков. Это будет со временем выравнивать загруженность дисков на различных серверах.

Желательно ограничить число новых создаваемых чанков на каждом чанк-сервере. Несмотря на то, что создание чанка сама по себе быстрая операция, она подразумевает последующую запись данных в этот чанк, что уже

является тяжелой операцией, и это может привести к разбалансировке объема трафика данных на разные части системы.

Как сказано выше, желательно распределить чанки среди разных стоек.

Как только число реплик падает ниже устанавливаемой пользователем величины, мастер снова реплицирует чанк. Это может случиться по нескольким причинам: чанк-сервер стал недоступным, один из дисков вышел из строя или увеличена величина, задающая число реплик. Каждому чанку, который должен реплицироваться, устанавливается приоритет, который тоже зависит от нескольких факторов. Во-первых, приоритет выше у того чанка, который имеет наименьшее число реплик. Во-вторых, чтобы увеличить надежность выполнения приложений, увеличивается приоритет у чанков, которые блокируют прогресс в работе клиента

Мастер выбирает чанк с наибольшим приоритетом и копирует его, отдавая инструкцию одному из чанк-серверов, скопировать его с доступной реплики. Новая реплика располагается, исходя из тех же причин, что и при создании.

Во время работы мастер постоянно балансирует реплики. В зависимости от распределения реплик в системе, он перемещает реплику для выравнивания загруженности дисков и балансировки нагрузки. Также мастер должен решать, какую из реплик стоит удалить. Как правило, удаляется реплика, которая находится на чанк-сервере с наименьшим свободным местом на жестких дисках.

Еще одна важная функция, лежащая на мастере — это сборка мусора. При удалении файла, GFS не требует мгновенного возвращения освободившегося дискового пространства. Он делает это во время регулярной сборки мусора, которая происходит как на уровне чанков, так и на уровне файлов. Авторы считают, что такой подход делает систему более простой и надежной.

При удалении файла приложением, мастер запоминает в логах этот факт, как и многие другие. Тем не менее, вместо требования немедленного восстановления освободившихся ресурсов, файл просто переименовывается, причем в имя файла добавляется время удаления, и он становится невидимым пользователю. А мастер, во время регулярного сканирования пространства имен файловой системы, реально удаляет все такие скрытые файлы, которые были удалены пользователем более трех дней назад (этот интервал настраивается). А до этого момента файл продолжает находиться в системе, как скрытый, и он может быть прочитан или переименован обратно для восстановления. Когда скрытый файл удаляется мастером, то информация о нем удаляется также из метаданных, а все чанки этого файла отцепляются от него.

Мастер помимо регулярного сканирования пространства имен файлов делает аналогичное сканирование пространства имен чанков. Мастер определяет чанки, которые отсоединены от файла, удаляет их из метаданных и во время регулярных связей с чанк-серверами передает им сигнал о возможности

удаления всех реплик, содержащих заданный чанк. У такого подхода к сборке мусора много преимуществ, при одном недостатке: если место в системе заканчивается, а отложенное удаление увеличивает неиспользуемое место, до момента самого физического удаления. Зато есть возможность восстановления удаленных данных, возможность гибкой балансировки нагрузки при удалении и возможность восстановления системы, в случае каких-то сбоев.

Устойчивость к сбоям и диагностика ошибок

Авторы системы считают одной из наиболее сложных проблем частые сбои работы компонентов системы. Количество и качество компонентов делают эти сбои не просто исключением, а скорее нормой. Сбой компонента может быть вызван недоступностью этого компонента или, что хуже, наличием испорченных данных. GFS поддерживает систему в рабочем виде при помощи двух простых стратегий: быстрое восстановление и репликации.

Быстрое восстановление — это, фактически, перезагрузка машины. При этом время запуска очень маленькое, что приводит к маленькой заминке, а затем работа продолжается штатно. Про репликации чанков уже говорилось выше. Мастер реплицирует чанк, если одна из реплик стала недоступной, либо повредились данные, содержащие реплику чанка. Поврежденные чанки определяется при помощи вычисления контрольных сумм.

Еще один вид репликаций в системе, про который мало было сказано — это репликация мастера. Реплицируется лог операций и контрольные точки (checkpoints). Каждое изменение файлов в системе происходит только после записи лога операций на диски мастером, и диски машин, на которые лог реплицируется. В случае небольших неполадок мастер может перезагрузиться. В случае проблем с жестким диском или другой жизненно важной инфраструктурой мастера, GFS стартует нового мастера, на одной из машин, куда реплицировались данные мастера. Клиенты обращаются к мастеру по DNS, который может быть переназначен новой машине. Новый мастер является тенью старого, а не точной копией. Поэтому у него есть доступ к файлам только для чтения. То есть он не становится полноценным мастером, а лишь поддерживает лог операций и другие структуры мастера.

Важной частью системы является возможность поддерживать целостность данных. Обычный GFS кластер состоит из сотен машин, на которых расположены тысячи жестких дисков, и эти диски при работе с завидным постоянством выходят из строя, что приводит к порче данных. Система может восстановить данные с помощью репликаций, но для этого необходимо понять испортились ли данные. Простое сравнение различных реплик на разных чанк-серверах является неэффективным. Более того, может происходить несогласованность данных между различными репликами, ведущая к различию данных. Поэтому каждый чанк-сервер должен самостоятельно определять целостность данных.

Каждый чанк разбивается на блоки длиной 64 Кбайт. Каждому такому блоку соответствует 32-битная контрольная сумма. Как и другие метаданные эти суммы хранятся в памяти, регулярно сохраняются в лог, отдельно от данных пользователя.

Перед тем как считать данные чанк-сервер проверяет контрольные суммы блоков чанка, которые пересекаются с затребованными данными пользователем или другим чанк-сервером. То есть чанк-сервер не распространяет испорченные данные. В случае несовпадения контрольных сумм, чанк-сервер возвращает ошибку машине, подавшей запрос, и рапортует о ней мастеру. Пользователь может считать данные из другой реплики, а мастер создает еще одну копию из данных другой реплики. После этого мастер дает инструкцию этому чанк-серверу об удалении этой испорченной реплики.

При добавлении новых данных, верификация контрольных сумм не происходит, а для блоков записывается новые контрольные суммы. В случае если диск испорчен, то это определится при попытке чтения этих данных. При записи чанк-сервер сравнивает только первый и последний блоки, пересекающиеся с границами, в которые происходит запись, поскольку часть данных на этих блоках не перезаписывается и необходимо проверить их целостность.

Организация работы с данными при помощи MapReduce

MapReduce является программной моделью и соответствующей реализацией обработки и генерации больших наборов данных. Пользователи могут задавать функцию, обрабатывающую пары ключ/значение для генерации промежуточных аналогичных пар, и сокращающую функцию, которая объединяет все промежуточные значения, соответствующие одному и тому же ключу. Многие реальные задачи могут быть выражены с помощью этой модели. Программы, написанные в таком функциональном стиле автоматически распараллеливаются и адаптируются для выполнения на обширных кластерах. Система берет на себя детали разбиения входных данных на части, составления расписания выполнения программ на различных компьютерах, управления ошибками, и организации необходимой коммуникации между компьютерами. Это позволяет программистам, не обладающим опытом работы с параллельными и распределенными системами, легко использовать все ресурсы больших распределенных систем.

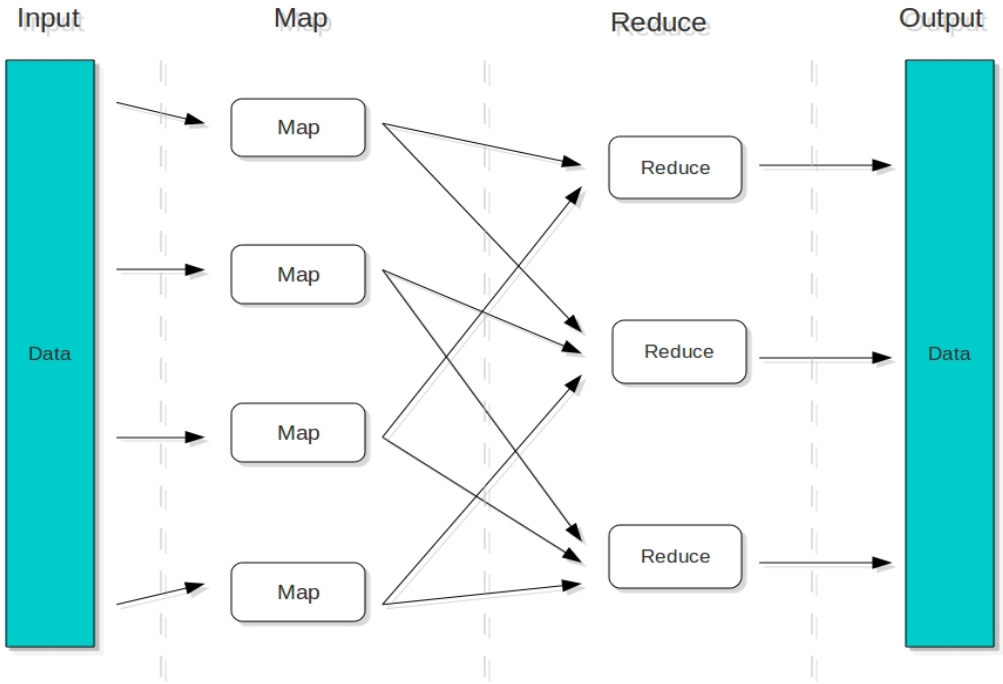

Рисунок 3.18

Преимущества использования MapReduce?

Эффективный способ распределения задач между множеством компьютеров

Обработка сбоев в работе

Работа с различными типами смежных приложений, таких как поиск или реклама. Возможно предварительное вычисление и обработка данных, подсчет количества слов, сортировка терабайт данных и так далее

Вычисления автоматически приближаются к источнику ввода-вывода

MapReduce использует три типа серверов:

- Master: назначают задания остальным типам серверов, а также следят за процессом их выполнения
- Map: принимают входные данные от пользователей и обрабатывают их, результаты записываются в промежуточные файлы
- Reduce: принимают промежуточные файлы от Map-серверов и сокращают их указанным выше способом

Например, мы хотим посчитать количество слов на всех страницах. Для этого нам необходимо передать все страницы, хранимые в GFS, на обработку в MapReduce. Этот процесс будет происходить на тысячах машин одновременно с полной координацией действий, в соответствии с автоматически составленным расписанием выполняемых работ, обработкой потенциальных ошибок, и передачей данных выполняемыми автоматически.

Последовательность выполняемых действий выглядела бы следующим образом: GFS → Map → перемешивание → Reduce → запись результатов обратно в GFS.

Технология MapReduce состоит из двух компонентов: соответственно map и reduce. Map отображает один набор данных в другой, создавая тем самым пары ключ/значение, которпыми в нашем случае являются слова и их количества. В процессе перемешивания происходит аггрегирование типов ключей. Reduction в этом случае просто суммирует все результаты и возвращает финальный результат.

В процессе индексирования Google подвергает поток данных обработке около 20 разных механизмов сокращения. Сначала идет работа над всеми записями и аггрегированными ключами, после чего результат передается следующему механизму и второй механизм уже работает с результатами работы первого, и так далее.

Транспортировка данных между серверами происходит в сжатом виде. Идея заключается в том, что ограничивающим фактором является пропускная способность канала и ввода-вывода, что делает резонным потратить часть процессорного времени на компрессию и декомпрессию данных.

Хранение структурированных данных в BigTable

BigTable является крупномасштабной, устойчивой к потенциальным ошибкам, самоуправляемой системой, которая может включать в себя терабайты памяти и петабайты данных, а также управлять миллионами операций чтения и записи в секунду. BigTable представляет собой распределенный механизм хэширования, построенный поверх GFS, а вовсе не реляционную базу данных и, как следствие, не поддерживает SQL-запросы и операции типа Join. Она предоставляет механизм просмотра данных для получения доступа к структурированным данным по имеющемуся ключу. GFS хранит данные не поддающиеся пониманию, хотя многим приложениям необходимы структурированные данные. Коммерческие базы данных попросту не могут масштабироваться до такого уровня и, соответственно, не могут работать с тысячами машин одновременно.

С помощью контролирования своих низкоуровневых систем хранения данных, Google получает больше возможностей по управлению и модификации их системой. Например, если им понадобится функция, упрощающая координацию работы между датацентрами, они просто могут написать ее и внедрить в систему. Подключение и отключение компьютеров к функционирующей системе никак не мешает ей просто работать. Каждый блок данных хранится в ячейке, доступ к которой может быть предоставлен как по ключу строки или столбца, так и по временной метке. Каждая строка может храниться в одной или нескольких таблицах. Таблицы реализуются в виде последовательности блоков по 64 килобайта, организованных в формате данных под названием SSTable.

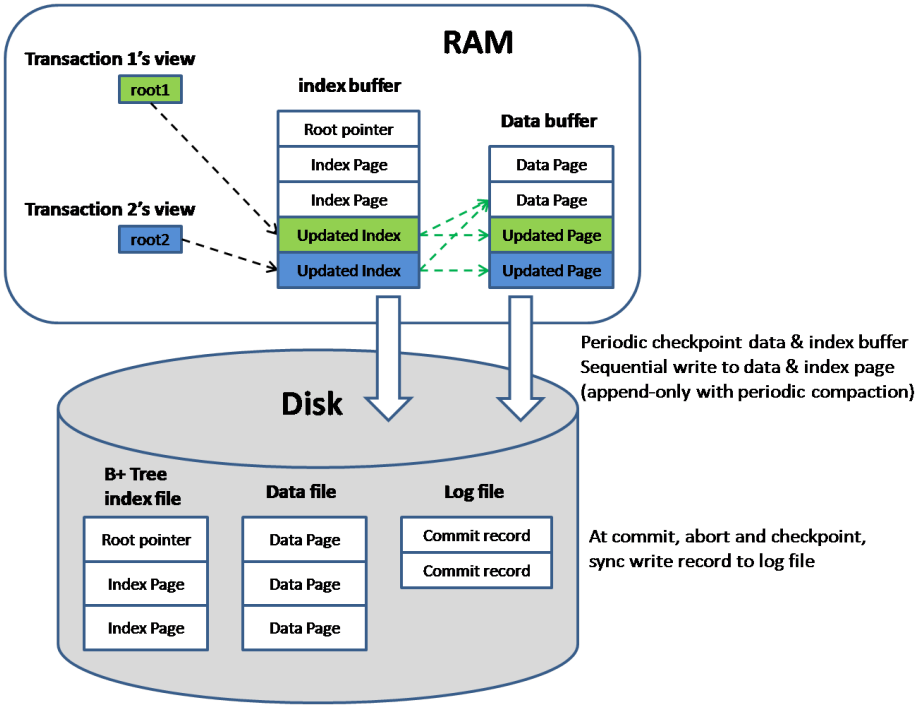

Рисунок 3.19

В BigTable тоже используется три типа серверов:

Master: распределяют таблицы по Tablet-серверам, а также следят за расположением таблиц и перераспределяют задания в случае необходимости.

Tablet: обрабатывают запросы чтения/записи для таблиц. Они раделяют таблицы, когда те превышают лимит размера (обычно 100-200 мегабайт). Когда такой сервер прекращает функционирование по каким-либо причинам, 100 других серверов берут на себя по одной таблице и система продолжает работать как-будто ничего не произошло.

Lock: формируют распределенный сервис ограничения одновременного доступа. Операции открытия таблицы для записи, анализа Master-сервером или проверки доступа должны быть взаимноисключающими.

Локальная группировка может быть использована для физического хранения связанных данных вместе, чтобы обеспечить лучшую локализацию ссылок на данные. Таблицы по возможности кэшируются в оперативной памяти серверов.

Пример реализации инфраструктуры для проекта Flickr

Flickr является мировым лидером среди сайтов размещения фотографий. Перед Flickr стоит крайне непростая задача, они должны контролировать огромное количество ежесекундно обновляющегося контента, непрерывно пополняющиеся пользователи, постоянный поток новых предоставляемых пользователям возможностей, и при этом поддерживать постоянно высокий уровень производительности.

Статистика

Более четырех миллиардов запросов в день

Примерно 35 миллионов фотографий в кэше прокси-сервера Squid

Около двух миллионов фотографий в оперативной памяти Squid

Всего приблизительно 470 миллионов изображений, каждое представлено в 4 или 5 размерах

38 тысяч запросов к memcached (12 миллионов объектов)

2 петабайта дискового пространства

Более 400000 фотографий добавляются ежедневно

Использующиеся программные компоненты

Примечательно, что на проекте Flickr используется практически только свободное программное обеспечение.

Платформа GNU/Linux (RedHat)

СУБД MySQL

Web-сервер Apache

Скрипты программной логики, написанные на языке PHP и Perl

Средства сегментирования (Shards) (прим.: разбиение системы на части, обслуживающие каждая свою группу пользователей; называть можно было по-разному, но давайте остановимся на этом варианте перевода)

Memcached для кэширования часто востребованного контента

Squid в качестве обратного прокси-сервера для html-страниц и изображений

Шаблонизатор Smarty

PEAR для парсинга e-mail и XML

ImageMagick для обработки изображений

SystemImager для развертывания элементов конфигурации

Ganglia для мониторинга распределенных систем

Subcon для хранения важных системных конфигурационных файлов в SVN-репозитории для легкого развертывания на машины в кластере

Cvsup для распространения и обновления коллекций файлов по сети.

Типовое оборудование для серверов:

EMT64 под управлением RHEL 4 с 16 Gb оперативной памяти.

6 жестких дисков с 15000rpm, объединены в RAID-10.

Размер для пользовательских метаданных достигает 12 терабайт (это не включает фотографии).

Используются 2U корпуса.

Системная архитектура

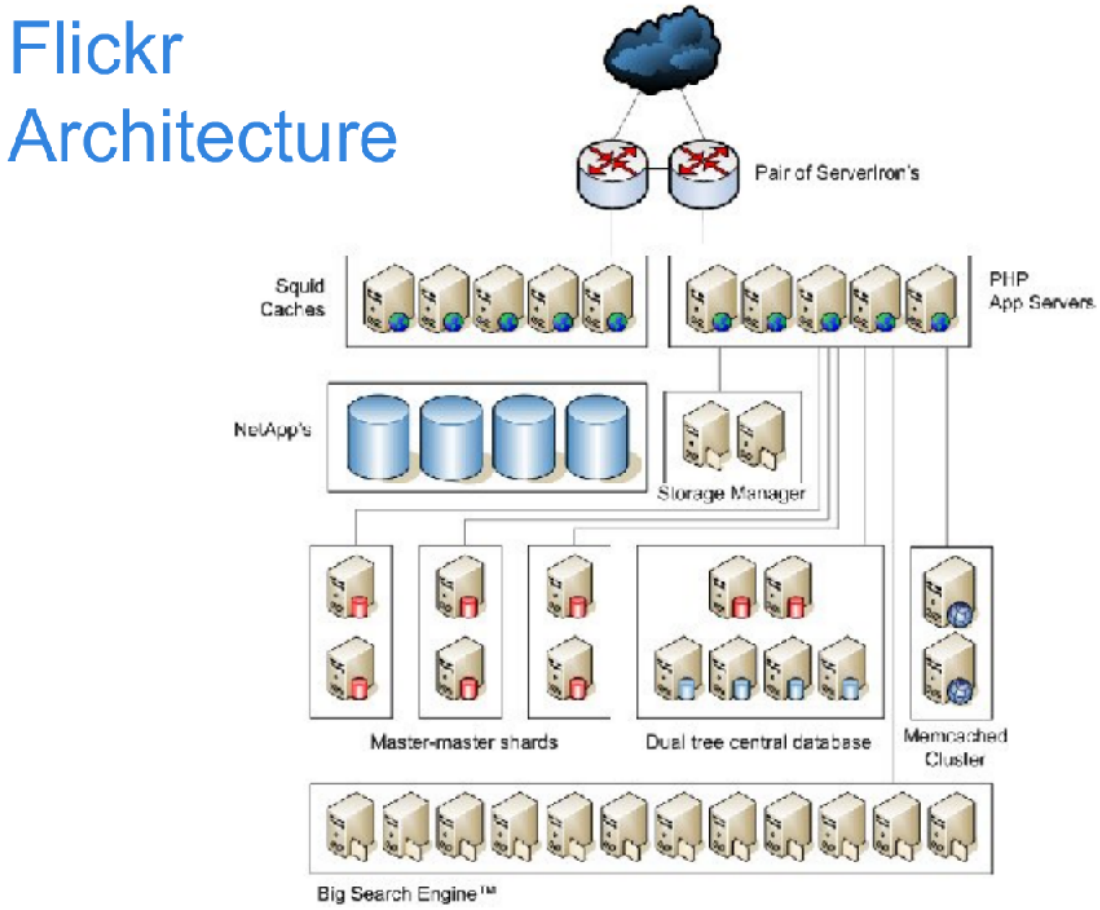

Рисунок 3.20

Рассмотрим наиболее характерные решения.

Входные запросы поступают на сдублированные контроллеры приложений Brocade ServerIron ADX. Они обеспечивают коммутацию приложений и балансировку трафика, основываясь на принципе виртуальных ферм серверов:

Коммутатор приложений получает все клиентские запросы

Выбор “лучшего” сервера производится на основании механизма Real-Time Health и наличия требуемой производительности

Последовательно повышается коэффициент использования для всех серверов

Интеллектуальное распределение загрузки осуществляется для всех доступных ресурсов

Метод конфигурируется и выбирается пользователем

Обеспечивается защита серверной фермы от атак и от неправильной эксплуатации

Клиенты подсоединяются к серверам приложений используя виртуальный IP (VIP). VIP адреса настраиваются на коммутаторе приложений

Коммутатор приложений осуществляет трансляцию адресов после выбора нужного сервера, причем сами адреса серверов скрыты.

Обслуживание сессий ведется согласно последовательности:

Запись о каждой пользовательской сессии создается в таблице

Каждая сессия назначается определенному серверу

Все сообщения в рамках сессии посылаются к одному серверу

Таблицы сессий синхронизируются между двумя коммутаторами

За счет дублирования коммутаторов нет простоя сервиса когда коммутатор вышел из строя: второй коммутатор обнаруживает отказ и начинает обслуживать сессии пользователей

Структура Dual Tree является индивидуальным набором модификаций для MySQL, позволяющим масштабировать систему путем добавления новых мастер-серверов без использования кольцевой архитектуры. Эта система позволяет экономить на масштабировании, так как варианты мастер-мастер требовали бы удвоенных вложений в оборудование.

Центральная база данных включает в себя таблицу пользователей, состоящую из основных ключей пользователей (несколько уникальных идентификационных номеров) и указатель на сегмент, на котором может быть найдена остальная информация о конкретном пользователе.

Все, за исключением фотографий, хранится в базе данных. Для статического контента используются выделенные сервера. Фотографии хранятся в системе хранения данных. После загрузки изображения система выдает различные его размеры, на чем ее работа заканчивается. Метаданные и ссылки на файловые системы, где расположены фотографии, хранятся в базе данных.

В основе масштабируемости лежит репликация. Для поиска по определенной части базы данных создается отдельная копия этого фрагмента. Активная

репликация производится по принципу мастер-мастер. Автоматическое инкрементирование идентификационных номеров используется для поддержания системы в режиме одновременной активности обоих серверов в паре. При этом привязывание новых учетных записей к сегментам системы происходит случайным образом. Миграция пользователей проводится время от времени для того, чтобы избавиться от проблем, связанных с излишне активными пользователями. Необходима сбалансированность в этом процессе, особенно в случаях с большим количеством фотографий.

Каждый сегмент содержит данные о более чем 400 тысячах пользователей. В системе заложены федеративные принципы сегментации: "Мои данные хранятся на моем сегменте, но запись о Вашем комментарии хранится на Вашем сегменте". При этом реализуется глобальное кольцо, принцип работы которого схож с DNS: "Необходимо знать куда Вы хотите пойти и кто контролирует то место, куда Вы собираетесь пойти". Логика, реализованная в виде PHP скриптов устанавливает соединение с сегментом и поддерживает целостность данных.

Каждый сервер в рамках одного сегмента в обычном состоянии нагружен ровно на половину. Выключите половину серверов в каждом сегменте и система продолжит функционировать без изменений. Это значит, что один сервер внутри сегмента может взять на себя всю нагрузку второго, в то время как второй сервер может по каким либо причинам быть отключен от системы, например для проведения технических работ. Обновление оборудования производится очень просто: отключается половина сегмента, она же обновляется, подключается обратно, процесс повторяется для оставшейся половины.

Периоды пиковой нагрузки также нарушают правило 50% нагрузки. В такие моменты система получает 6-7 тысяч запросов в секунду, в то время как на данный момент система может работать на пятидесятипроцентном уровне нагрузки только при четырех тысячах запросов в секунду.

В среднем при загрузке одной страницы выполняется 27-35 SQL-запросов. Списки избранных фотографий обрабатываются в реальном времени, ровно как и доступ через API к базе данных. Все требования к нагрузке в реальном времени выполняются без каких-либо недостатков.

Организация резервного копирования данных реализована с помощью процесса ibbackup, который выполняется регулярно посредством cron daemon'a, причем на каждом сегменте он настроен на разное время. Каждую ночь делается снимок со всего кластера баз данных. Запись или удаление нескольких больших файлов с резервными копиями одновременно на реплицирующую систему хранения может сильно сократить производительность системы в целом на последующие несколько часов из-за процесса репликации. Выполнение этого на активно работающей системе хранения фотографий затруднительно.

Использованные источники

1. Bernard, Scott A.; Introduction to Enterprise Architecture; Publisher: authorHOUSE™; 2005
2. Google Lab: BigTable. - http://labs.google.com/papers/bigtable.html
3. Google Lab: MapReduce: упрощенная обработка данных на больших кластерах - http://labs.google.com/papers/mapreduce.html
4. Google Lab: интерпретирование данных. Параллельный анализ с помощью Sawzall. - http://labs.google.com/papers/sawzall.html
5. Google Lab: Файловая система Google (GFS) - http://labs.google.com/papers/gfs.html
6. HP OV Service Desk / http://www.hp.ru/openview/products/servicedesk/
7. ITIL – библиотека передового опыта организации ИТ-служб / http://www.cio-world.ru/weekly/251017/page3.html
8. Management Software: HP OpenView / http://h20229.www2.hp.com/
9. META Group. Executive Insights. Enterprise Architecture Desk Reference, 2002.
10. Microsoft® Operations Framework 4.0. Published at 2008, April.
11. MSF for Agile Software Development Process Guidance. Published at 2006, November.
12. MSF for CMMI® Process Improvement. Published at 2006, November.
13. Rob England, Introduction to Real ITSM, ISBN 1438243065 9781438243061, год 2008
14. System Center Reporting Manager 2006 Overview // http://www.microsoft.com/systemcenter/scrm/evaluation/overview/default.mspx
15. Tivoli / http://www-128.ibm.com/developerworks/ru/tivoli/
16. White Paper, The HP IT Service Management Reference Model, http://www.hp.com/hps/hpc/itsm/briefs/wp_v2-1.pdf
17. Долженко А.И., Управление информационными системами, Ростов-на-Дону, 2007
18. Информация о Data Protection Manager // http://www.microsoft.com/rus/systemcenter/dpm/evaluation/default.mspx

19. Как работает Google от David Carr в Baseline Magazine. - http://www.baselinemag.com/c/a/Infrastructure/How-Google-Works-1/

20. Олейник А.И., Сизов А.В., ИТ-Инфраструктура, Москва, 2009

21. Построение масштабируемых веб-сайтов от Call Handerson'a из Flickr

22. Потоцкий М.А. ITSM, как современный подход к ИТ - менеджменту, «Директор ИС», № 05 2002.

23. Решение HP OpenView Network Node Manager (NNM) / http://www.hp.ru/openview/nnm/

24. Решения IBM Tivoli для растущих компаний / http://www-306.ibm.com/software/ru/tivoli/smb/products.html#express

25. Решения Microsoft для повышения эффективности ИТ-инфраструктуры / Microsoft. – М.: Русская редакция, 2005.

26. Системы управления ИТ инфраструктурой на базе IBM Tivoli / http://www.r-style.com/rubrs.asp?rubr_id=214&art_id=954

27. Технологии IBM для управления информационными системами / http://www.tivoli.computel.ru/article?id=a0018

28. Федерация Flickr: Тур по архитектуре Flickr - http://www.bytebot.net/blog/archives/2007/04/25/federation-at-flickr-a-tour-of-the-flickr-architecture

29. Центр безопасности Microsoft / http://www.microsoft.com/rus/security/default.mspx