МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

КРУГЛЯК Ю. О.

СУЧАСНА ТЕОРІЯ УПРАВЛІННЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Конспект лекцій

Одеса
Одеський державний екологічний університет
2015

УДК 681.518
К84

Рекомендовано методичною радою Одеського державного екологічного університету Міністерства освіти і науки України як конспект лекцій (протокол №9 від _25.06. 2015 р.)

Кругляк Ю. О.
Сучасна теорія управління в інформаційних системах: конспект лекцій. Одеса, Одеський державний екологічний університет, 2015. 190 с.

В курсі розглядаються основи управління IT-інфраструктурою підприємства, що базуються на понятті інформаційного сервісу, модель управління інформаційними системами (ITSM), бібліотека ITIL, моделі процесів ITSM RM компанії Hewlett-Packard, MOF компанії Microsoft, рівні зрілості IT інфраструктури підприємства (Microsoft), методологія Microsoft з проектування і експлуатації інформаційних систем, рішення Microsoft з побудови ефективних і раціональних IT-інфраструктур.

Конспект лекцій призначений для студентів V курсу спеціальності «Інформаційні управляючі системи та технології», напрям підготовки 6.050101 «Комп'ютерні науки».

ISBN 978-966-186-088-8

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Важная роль информационных технологий (ИТ) в успешном ведении основного бизнеса предприятий – это сегодня почти очевидный факт. В то же время затраты на поддержку и развитие информационных систем (ИС) неизменно растут, и доля их в общей структуре расходов предприятий неизменно увеличивается. В результате перед руководителями многих предприятий встает очень непростая проблема: необходимо повысить качество обслуживания при одновременном сокращении затрат.

Сложность решения такой задачи состоит в том, что для этого нужно достаточно радикально пересматривать общее позиционирование сервисных ИТ-служб в структуре предприятия. Одна сторона вопроса заключается в том, что ИТ-инфраструктура предприятий зачастую формировалась хаотично, оперативно отвечая на те или иные запросы со стороны основного бизнеса. В результате ИТ-службы имеют весьма запутанную структуру как с технической, так и с экономической точки зрения. Вторая сторона проблемы в том, что ИТ-службы исторически рассматриваются как вспомогательные, сугубо бюджетные подразделения. Как следствие, руководство компаний не может четко выявить взаимосвязь между инвестициями в развитие и поддержку ИС и повышением эффективности основного бизнеса.

В условиях возрастающей конкуренции ИТ-службы многих предприятий наряду с дефицитом выделяемых им бюджетов столкнулись с требованиями со стороны руководства о предоставлении отчетов по расходам и сведений об ожидаемой прибыли от инвестиций в ИТ-инфраструктуру предприятия. Это подтверждается целым рядом исследований по всему миру. Результаты этих исследований говорят также о том, что ИТ-менеджеры не всегда могут четко определить, какие преимущества получают внутренние или внешние клиенты ИТ-служб от той или иной услуги.

Следует отметить, что задача установления четких связей между ИТ-операциями и соответствующим бизнесом в общем случае достаточно сложна. Но развитие ИТ-служб должно идти именно в этом направлении

По оценкам Meta Group, ситуация на рынке такова, что сегодня около 75% ИТ-служб – это не более чем поставщики инфраструктуры, ориентированные исключительно на ее технологическое развитие вне связи с деятельностью предприятий в целом. В то же время предприятия хотят получать экономически эффективные ИТ-услуги, отвечающие их индивидуальным потребностям и способные помочь им в решении ключевых бизнес-задач. Поэтому ИТ-службы должны стать не просто поставщиками ИТ-инфраструктуры, а настоящими сервис-провайдерами, а затем и стратегическими партнерами руководства предприятий, предоставляющими широкий спектр услуг, эффективность которых поддается достаточно простой оценке со стороны их потребителей.

Решение задачи повышения эффективности работы ИТ-служб предприятий часто связывают с применением специального программного обеспечения (ПО) для автоматизации управления. Программное обеспечение для управления ИТ-инфраструктурой должно рассматриваться в первую очередь как вспомогательное средство поддержки методологии, автоматизации ее применения. В настоящее время на рынке предлагается достаточно много продуктов, нацеленных на решение таких задач. Однако среди ПО мирового уровня, наверное, в первую очередь нужно отметить пакеты, поставляемые компаниями Hewlett Packard (OpenView), IBM (Tivoli), Microsoft.

В предлагаемом лекционном курсе рассматривается современная методология и передовые инструментальные средства управления информационными технологиями на предприятии.

1 ИТ-СЕРВИС – ОСНОВА ДЕЯТЕЛЬНОСТИ СОВРЕМЕННОЙ ИС СЛУЖБЫ

1.1 Понятие ИТ-сервиса

Системы управления информационными технологиями (ИТ) предприятий и организаций (далее по тексту используется термин «предприятие») являются достаточно сложными, поскольку требуют учета интересов множества участников, вовлеченных в создание и использование ИТ-ресурсов (спонсоров создания информационной системы, конечных пользователей и разработчиков).

Понятие «информационные технологии» является общеупотребительным, в то же время отсутствует общепризнанное определение этого понятия. Мы будем придерживаться определения, данного в энциклопедии *Wikipedia* (*en.wikipedia.org/wiki/Main_Page*): «***Информационные технологии (ИТ)***, или информационные и коммуникационные технологии (ИКТ), — *это технологии, применяемые для обработки информации. В частности, они используют компьютеры и программное обеспечение для преобразования, хранения, защиты, передачи и извлечения информации в любом месте и в любое время*» [1]. С учетом этого определения ***ИТ-менеджмент*** *охватывает управление всеми компьютерными и коммуникационными ресурсами предприятия*. Его основная задача состоит в создании и поддержании в работоспособном состоянии приложений и инфраструктуры, на которой они исполняются. Подобный менеджмент можно разделить на три уровня: операционный, тактический и стратегический. На стратегическом уровне обеспечивается установление соответствия между информационными функциями системы и ее контентом, что сводится к атрибуции задач на поле информационной политики, определению содержания информационных функций и ИТ-поддержке. На операционном и тактическом уровнях ИТ-менеджмента должны обеспечиваться заданные уровни работоспособности и надежности эксплуатации приложений информационной системы (ИС) на продолжении всего жизненного цикла системы.

Создание системы управления ИТ, как и любой другой системы управления, предполагает определение управляемых объектов и управляющих воздействий (рис. 1.1).

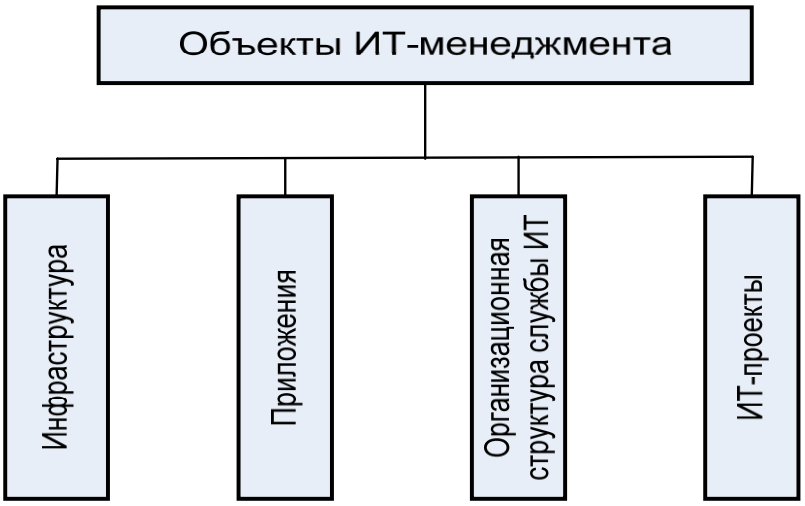

Рисунок 1.1 – Объекты информационного менеджмента

Объектами ИТ-менеджмента являются:

- инфраструктура;
- приложения;
- организационная структура службы ИС;
- ИТ-проекты.

Инфраструктура ИТ включает техническое и системное программное обеспечение. Техническое обеспечение ИТ состоит из серверов, персональных компьютеров, систем хранения данных, сети и коммуникационных приложений. Программное обеспечение характеризуется операционными системами, инструментальными средами разработки, программами поддержки ИТ-менеджмента и средствами обеспечения информационной безопасности.

Приложения обеспечивают поддержку бизнес-процессов предприятия и работоспособность отдельных автоматизированных рабочих мест.

Организационная структура службы ИС определяет состав подразделений, распределение между ними функций и задач. Служба ИСдолжна обеспечивать разработку, ввод в действие и эксплуатацию информационной системы посредством координированных действий, которые обеспечивают непрерыв-

ность функционирования существующей системы в соответствии с согласованными правилами и процедурами на протяжении жизненного цикла ИС.

ИТ-проекты представляют собой проекты внедрения новых информационных систем, а также модернизацию существующих. При этом модернизация (изменения, дополнения) рассматривается как результат действий, выполненных по запросу и относящихся к функциональным или нефункциональным требованиям, которые не были определены изначально при разработке и внедрении системы.

В настоящее время бизнес характеризуется высокой динамикой (слияния, поглощения, смена стратегических целей). Это обуславливает тот факт, что информационные системы предприятий находятся в условиях постоянных изменений, вызванных следующими факторами:

- перемены внутри предприятий и в окружающей бизнес-среде;
- развитие технологий, появление принципиально новых технических решений;
- появление новых информационных технологий;
- социальные изменения.

Кроме того, современное состояние бизнеса в отношении информационных технологий характеризуется достаточно жестким контролем инвестиций, выделяемых на ИТ, и возросшими требованиями к ИТ со стороны бизнеса. С учетом этого, на первый план выходят требования к информационным системам, которые определяют систему информационного менеджмента, способную видоизменять ИТ предприятия или организации синхронно с изменением бизнеса [2]. В соответствии с этими требованиями основная роль ИТ на предприятии определяется как информационное обслуживание её подразделений с целью повышения эффективности бизнеса. Информационное обслуживание бизнеса состоит в предоставлении информационных сервисов (ИТ-сервисов) заданного качества подразделениям предприятия.

ИТ-сервис в корпоративной среде – это ИТ-услуга, которую ИТ-подразделение (департамент, отдел, служба) или внешний провайдер предос-

тавляет бизнес-подразделениям предприятия для поддержки их бизнес-процессов.

Примерами корпоративных ИТ-сервисов могут быть электронная почта, сетевая инфраструктура, системы хранения данных, бизнес-приложения (начисление заработной платы, формирование счетов), бизнес-функции (списание/начисление денежных средств на счете клиента).

Набор ИТ-сервисов, необходимых организации, индивидуален и в значительной степени зависит от отрасли, размеров организации, уровня автоматизации, квалификации персонала, стратегии развития и т. п. Корпоративные ИТ-сервисы можно разбить на три большие группы:

- поддержка ИТ-инфраструктуры;
- поддержка бизнес-приложений;
- поддержка пользователей.

В общем случае ИТ-сервис характеризуется рядом параметров [3]:

- функциональность;
- время обслуживания;
- доступность;
- надежность;
- производительность;
- конфиденциальность;
- масштаб;
- затраты.

Функциональность определяет решаемую задачу (информатизацию бизнес-операции, бизнес-функции, бизнес-процесса) и предметную область её использования.

Время обслуживания определяет период времени, в течение которого ИТ-подразделение поддерживает данный сервис, т.е. несет ответственность за его непрерывное функционирование. Время обслуживания измеряется долей суток и долей календарной недели, в течение которых ИТ-подразделение поддерживает ИТ-сервис. Например, время обслуживания 24×7 означает, что ИТ-сервис

поддерживается 24 часа в сутки 7 дней в неделю, 5×8 − 5 дней в неделю по рабочим дням по 8 часов в день, т.е. в течение рабочего дня.

Доступность определяет долю согласованного времени обслуживания, которая измеряется в процентах, и характеризует в течение какого времени ИТ-сервис доступен;. Например, доступность 95% при согласованном времени обслуживания 8×5 означает, что сервис простаивает 2 часа в неделю (5% от 40 часов).

Надежность определяется средним временем наработки на отказ ИТ-сервиса, т.е. средним периодом времени между двумя сбоями в предоставлении ИТ-сервиса. Например, если в условиях предыдущего примера (время обслуживания 8×5, доступность 95%) в неделю в среднем происходит два сбоя ИТ-сервиса, среднее время наработки на отказ составляет 19 часов.

Производительность характеризует способность информационной системы соответствовать требованиям своевременности. Для различных ИТ-сервисов показателями производительности могут быть время реакции (время выполнения бизнес-транзакции) или пропускная способность системы. Например, при задании времени реакции системы пользователь может потребовать чтобы время проводки по счету клиента было не более 5 сек., а при задании производительности – количество транзакций по счету клиента было не менее 20 в течении 1 часа т.е. 20 транзакции/ч. Для задания производительности ИТ-сервиса следует использовать бизнес-операции (бизнес-функции), существенные для конечного пользователя, − ввод документов, подготовку отчетов и т.д.

Конфиденциальность определяет вероятность несанкционированного доступа к данным и/или их несанкционированное изменение. Количественные измерения данного показателя обычно не проводятся. Вместо этого ИС, обеспечивающие ИТ-сервис, классифицируются по степени конфиденциальности. Принадлежность ИС к тому или иному классу подтверждается независимой сертификацией. Конфиденциальность ИТ-сервиса в целом определяется классом безопасности наиболее слабой из обеспечивающих сервис ИС, а также кор-

ректируется с учетом качества инструкций для конечных пользователей и их обучения.

Масштаб характеризует объем и сложность работ по поддержке ИТ-сервиса. Единого измерителя масштаба не существует, к его показателям относятся число рабочих мест, количество удаленных сайтов, сложность используемых приложений и т.п.

Затраты – стоимость всей совокупности ресурсов, вовлеченных в сопровождение ИТ-сервиса, а также потерь от простев ИТ-сервиса. В ресурсы включаются стоимость оборудования, ПО, используемых ресурсов и каналов связи, внешних услуг, заработная плата сотрудников организации (включая связанные с ней расходы) и т.п.

Параметры сервиса определяются не только свойствами ИС, которые его обеспечивают. Существенное значение имеет качество работы самой службы ИС, а также уровень регламентации деятельности службы ИС и конечных пользователей ИТ-сервисов..

Важным фактором эффективности деятельности службы ИС является инструментальная поддержка автоматизации процессов управления информационными технологиями предприятия, которая в значительной степени может способствовать снижению затрат на управление и мониторинг ИС с целью предоставления ИТ-сервисов требуемого качества.

1.2 Функциональные области управления службой ИС

Информационная система предприятия предназначена для информационной поддержки бизнес-процессов.

В наши дни основой успешного бизнеса является бесперебойное функционирование информационных систем, обеспечивающих конкурентоспособность и прибыльность компании. Основная задача службы ИС − обеспечение бизнес-процессов информационным обслуживанием заданного качества с использованием соответствующих информационных технологий. Поддержка ин-

формационных процессов осуществляется посредством ИТ-сервисов с заданными характеристиками.

Служба ИС предприятия, как правило, организует свою работу по четырем функциональным направлениям [3]:

- планирование и организация;
- разработка, приобретение и внедрение;
- предоставление и сопровождение ИТ-сервиса;
- мониторинг.

В рамках направления «Планирование и организация» решаются задачи разработки стратегии в области ИТ, координации развития ИТ организации, планирования ресурсов службы ИС (бюджет, человеческие ресурсы, внешние услуги и др.), управления рисками, управления качеством.

Основной задачей направления «Разработка, приобретение и внедрение» − внедрение новых ИС.

Функциональное направление «Предоставление и сопровождение сервиса ИТ» обеспечивает формализацию требований подразделений-заказчиков к ИТ-сервисам, согласование требований к сервисам с соответствующими ресурсами службы ИС и предоставление конечным пользователям сервисов ИТ, соответствующих согласованным требованиям.

Основная задача направления «Мониторинг» − аудит процессов службы ИС.

Организационная структура службы ИС зависит от многих факторов:

- масштаб службы ИС − более крупные службы ИС обычно имеют более сложную и разветвленную организационную структуру;
- отраслевую принадлежность, с которой связано наличие или, напротив, отсутствие определенных структурных подразделений;
- распределение организации по территории − наличие территориально удаленных подразделений и филиалов существенно меняет организационную структуру службы ИС.

Этот перечень отнюдь не исчерпывающий, в него входят и другие факторы, например состав используемых в организации ИС.

Для малых предприятий организационная структура службы ИС, описанная в [3], представлена на рис. 1.2.

Функции планирования в ней выполняются руководителем службы ИС. Именно по этой причине такая структура пригодна только для службы ИС небольшого размера − в более крупных службах ИС объем работ по планированию требует обособления отдельных функций планирования.

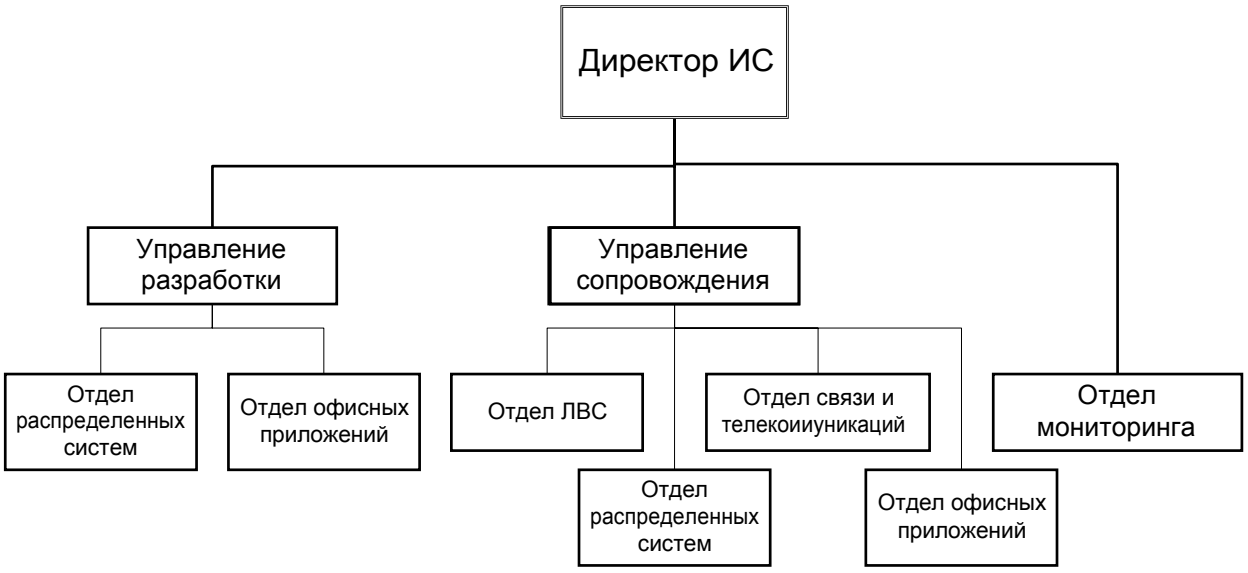

Рис. 1.2. Пример плоской структуры службы ИС

Непосредственно подчиняются директору ИС: 1) управление разработкой, выполняющее функции разработки, приобретения и внедрения информационных систем, и 2) управление сопровождением, выполняющее функции предоставления и сопровождения ИТ-сервисов. Организационное разделение разработки и эксплуатации имеет принципиальное значение. Успешная эксплуатация ИС в течение сколько-нибудь длительного времени возможна лишь тогда, когда она не требует постоянного вмешательства разработчика. Это обеспечивается соблюдением существующих методологий разработки и тестирования ИС, а также надлежащей пользовательской и эксплуатационной документацией. Тестирование ИС и документации на нее на соответствие требованиям устойчивой эксплуатации обеспечивается в ходе передачи системы в эксплуатацию. Этот

процесс и определяет важность разделения двух функциональных направлений. Передача ИС от одного управления службы ИС другому, равноправному первому, обеспечивает всестороннее тестирование созданной ИС и документации на нее. Напротив, внутри одного управления передача в эксплуатацию осуществляется обычно формально, с учетом возможности последующих доработок. Таким образом, во втором случае качество эксплуатируемой ИС обычно оказывается ниже.

В рамках процесса разработки одна и та же группа − проектная команда, подчиненная одному руководителю, − должна последовательно выполнить все функции процесса разработки применительно к определенной ИС. Следовательно, распределение функций разработки по различным подразделениям не имеет смысла. Напротив, имеет смысл выделить различные проектные группы для различных видов ИС, требующих от сотрудников различных знаний и навыков.

В результате в нашем примере выделены два отдела разработки − отдел офисных систем и отдел распределенных систем. Офисные системы представляют собой разработки в среде пакета *MS Office*, распределенные системы − многопользовательские системы, специализированные для выполнения отдельных задач. В малых организациях типичным примером таких задач и соответственно ИС являются бухгалтерские системы. Отдел офисных систем решает задачи «малой автоматизации» задач пользователей в среде *MS Office*. Отдел распределенных систем занимается внедрением бухгалтерской системы, а после того как внедрение завершено, расширением ее функциональности − внедрением дополнительных модулей, написанием отчетов и других программ в среде данной распределенной системы. Наконец, в штате управления разработкой необходим хотя бы один менеджер проектов. В простейшем случае им может быть руководитель управления разработкой, однако совмещение этих двух позиций может стать узким местом проектов этого управления. Таким образом, директор ИС должен отслеживать ситуацию с управлением проектами и при

необходимости расширить управление разработкой за счет одного или нескольких менеджеров проектов.

В управлении сопровождением выделяют группы специалистов сходной квалификационной базы. Отделами, состоящими из сотрудников сходной квалификации, проще управлять, поскольку однородность упрощает найм персонала, диспетчирование работ, бюджетирование и др. Типичный набор отделов в управлении сопровождением в плоской структуре включает отдел ЛВС (локальной вычислительной сети), отдел распределенных систем, отдел связи и телекоммуникаций, отдел офисных приложений. Первый отдел осуществляет поддержку локальной сети, включая сервер и его ОС, второй − поддержку распределенных систем, например бухгалтерской, третий − связь, телефонизацию и доступ в Интернет, четвертый − поддержку оборудования рабочих мест − компьютеров, принтеров и т.д., а также офисных приложений.

Функции мониторинга в плоской структуре выполняет отдел мониторинга (*Service Desk*), непосредственно подчиненный директору ИС. В этот отдел поступают сообщения пользователей об инцидентах, он же сообщает об инциденте соответствующим отделам службы сопровождения и контролирует ход работ по разрешению инцидента. Наконец, в этом отделе накапливается большой объем статистики инцидентов и времени их разрешения. Функции мониторинга более высокого уровня − контроль планов работ, графиков проектов, бюджета службы ИС в целом и отдельных ее подразделений − выполняет директор ИС.

Увеличение размера организации и объема работ службы ИС ведет к усложнению её организационной структуры. В этом случае могут применяться развернутые и дивизиональные структуры службы ИС.

Функциональная модель управления и основанная на ней организационная структура службы ИС длительное время представляли собой основной и единственный подход к управлению в этой области. Однако со временем выявился ряд ограничений функционального подхода, снижавших эффективность управления службой ИС.

Функции службы ИС должны обеспечивать создание конечного продукта − ИТ-сервисов, поддерживающих выполнение определенных бизнес-процессов.

Функциональность ИТ-сервиса затрагивает большое количество функций службы ИС. На этапе планирования ИТ-сервиса функциональность согласовывается со стратегией, стандартами и планами в рамках стратегических функций службы ИС: контролируется соответствие создаваемого сервиса ИТ-стратегии предприятия, принятым стандартам и нормам службы ИТ, а также наличие средств в бюджете предприятия. На этапе разработки и внедрения функциональность ИТ-сервиса обеспечивается всеми функциями направления разработки и внедрения. Наконец, на этапе эксплуатации ИТ-сервиса функциональность обеспечивается управлением данными, оборудованием и системным программным обеспечением и поддержкой конечных пользователей. Соответствующие функции отдела сопровождения и эксплуатации обеспечивают учет связанных с сопровождением ИТ-сервиса расходов, а функции отдела мониторинга − соблюдение условий соглашений между заказчиком и службой ИС, с одной стороны, и службой ИС и внешними поставщиками − с другой.

Время обслуживания, доступность, надежность и производительность сервиса определяется в ходе согласования требований к ИТ-сервису с заказчиком и далее контролируется функциями мониторинга. Обеспечиваются эти параметры функциями поддержки конечных пользователей (устранение возникших сбоев) и управления данными, оборудованием и системным ПО (предотвращение возникновения сбоев и/или снижение их количества). Данные по производительности операций, существенных для конечного пользователя, могут быть получены на основании статистики использования прикладных систем.

Конфиденциальность ИТ-сервиса на этапе планирования формулируются в рамках функции определения политики безопасности отдельных сервисов. На этапе создания ИТ-сервиса в рамках функций разработки, приобретения и внедрения сервиса реализуется необходимая инфраструктура безопасности − разделение полномочий на доступ к операциям и документам, присвоение прав

пользователям, шифрование данных и т.д. Наконец, на этапе эксплуатации сервиса осуществляются обучение пользователей и контроль выполнения требований безопасности на рабочих местах конечных пользователей.

Масштаб сервиса определяется на этапе планирования сервиса в рамках функции планирования сервиса ИТ. Если некие сервисы ИТ реализуются совместно в рамках общего проекта, эти сервисы должны планироваться совместно. Обеспечение доступа к ИТ-сервису на всех серверах и рабочих местах реализуется в рамках функций приобретения, разработки и внедрения. Изменения масштаба сервиса контролируются в рамках функций планирования и организации.

Цена ИТ-сервиса определяется в процессе планирования сервиса. На этапе разработки и внедрения ИТ-сервиса контролируется выполнение бюджета соответствующего проекта и уточняется сумма первоначальных затрат на приобретение и/или разработку и внедрение. На этапе эксплуатации контролируется величина текущих затрат на сервис и их соответствие бюджету организации.

Таким образом, между функциями службы ИС и параметрами ИТ-сервиса нет прямого и однозначного соответствия. Качество ИТ-сервиса в целом и каждый параметр сервиса ИТ в частности определяются несколькими функциями ИТ. Одна и та же функция службы также может относиться к нескольким сервисам ИТ или даже ко всем сервисам ИТ, существующим в организации. Это обстоятельство создает для управления службой ИС, организованной по чисто функциональному принципу, целый ряд проблем.

Во-первых, обеспечение конечного результата − качества ИТ-сервиса − требует координации различных функций службы ИС. В ряде случаев эту координацию может осуществить вышестоящий руководитель. Однако многие задачи по такой координации требуют полномочий высокого уровня, вплоть до уровня директора ИТ. В результате руководители высокого уровня оказываются перегруженными большим потоком задач, не имеющих отношения к их постоянной деятельности и непосредственным обязанностям.

Во-вторых, управление подразумевает ответственность, и коль скоро параметры сервиса определяют качество последнего, следует назначить лиц, ответственных за эти параметры. При этом сфера ответственности не должна превышать полномочий ответственного лица. Из проведенного анализа прямо следует, что в целом содержание, доступность, надежность, производительность и конфиденциальность ИТ-сервиса находятся исключительно в сфере полномочий директора ИТ. Такой объем обязанностей директора ИТ возможен в плоской структуре службы ИС, но абсолютно нереалистичен для развернутой или дивизиональной структуры. В результате лицо, ответственное за качество сервиса, при функциональной организации службы ИС отсутствует.

В-третьих, проблемой является «точка контакта» − телефон и/или адрес электронной почты, по которому следует обращаться в случае необходимости. Наличие такой «точки контакта» особенно удобно в случае возникновения у пользователя потребности в новом или измененном ИТ-сервисе, а также при необходимости сообщить о сбое. При этом «точка контакта» может быть использована не только для регистрации запроса пользователя, но и для обработки его − назначения запроса специалисту, контроля хода выполнения работ, информации пользователя. Однако в функциональной организации эту дополнительную обработку организовать затруднительно. Специалисты, обрабатывающие запрос пользователя, не находятся в подчинении службы мониторинга (Service Desk) и не ответственны перед этой службой.

Таким образом, функциональная организация обеспечивает лишь текущую деятельность службы ИС, а не решение всех необходимых управленческих задач. С точки зрения обеспечения конечного результата − ИТ-сервиса необходимого качества − основными проблемами являются:

- координация функций;
- трудности обеспечения ответственности;
- трудности обеспечения единой «точки контакта».

Эти трудности успешно преодолеваются при процессном подходе к управлению службой ИС.

Процесс подразумевает наличие цели, критерия результата, ресурсов и определенной последовательности работ (т.е. шагов процесса). Применительно к процессам службы ИТ целью является предоставление заказчику ИТ-сервиса приемлемого уровня качества. Эта общая задача может быть разделена на две более частных:

- определение и согласование параметров ИТ-сервиса;
- обеспечение соответствия фактических параметров ИТ-сервиса достигнутым соглашениям.

Каждая из этих целей, в свою очередь, распадается на несколько целей следующего порядка, каждой из которых соответствует свой процесс.

Управление процессами предполагает следующие шаги:

- определение цели процесса и показателей достижения этой цели (количественных или качественных);
- назначение ответственного за процесс, задачей которого является достижение цели процесса;
- регламентация процесса в целом и составляющих его работ;
- при необходимости − автоматизация процесса посредством инструментальных средств, разработанных в самой организации либо закупленных извне.

Проблемы ответственности за результат процесса и координации разрешается в явном виде посредством назначения ответственного лица – менеджера процесса. Проблема единой «точки контакта» также вполне разрешима в рамках регламента процесса, обязательного для всех сотрудников службы ИС независимо от их функционального подчинения.

Управление процессами изменяет лишь управленческие функции службы ИС, не затрагивая функции собственно разработки и сопровождения ИТ-сервисов. Изменения состоят в систематическом целенаправленном решении задач координации функций в ходе выполнения процессов службы ИС. Для этого достаточно формализовать соответствующий процесс, т.е. назначить менеджера процесса, определить роли участников процесса и установить правила

его выполнения, т.е. последовательность выполнения операций процесса, обязанности в рамках ролей, правила эскалации и т.д.

Как следствие переход к процессной модели управления обычно не требует ни дополнительного персонала, ни изменений в организационной структуре. Участники процесса выполняют свои должностные обязанности в рамках существующей организационной структуры; часть этих обязанностей, относящаяся к данному процессу, формализована в виде ролей процесса. Если все процессы службы ИС формализованы, то совокупность ролей совпадает с должностными обязанностями сотрудника (рис. 1.3).

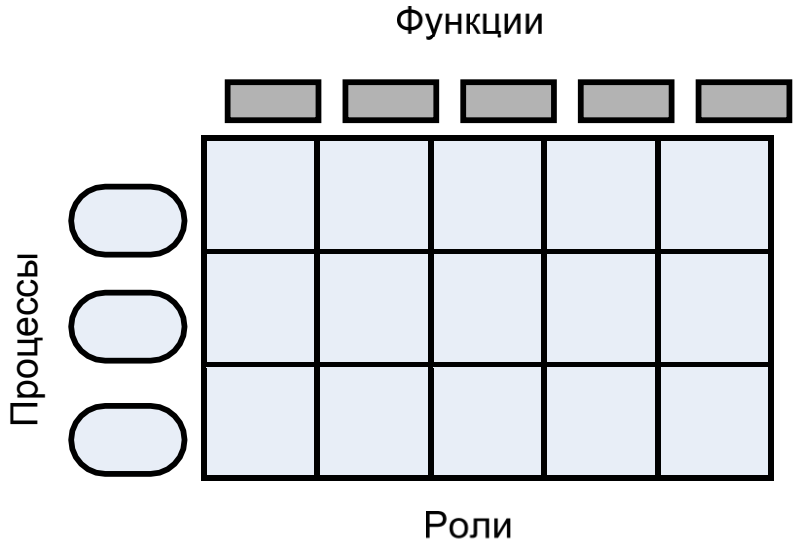

Рис. 1.3. Процессы, функции, роли в процессной модели управления

В такой системе менеджер процесса является начальником без подчиненных: он координирует деятельность не подчиненных ему сотрудников, относящихся к различным подразделениям существующей организационной структуры. Сам менеджер процесса тоже имеет должность в рамках существующей организационной структуры.

Использование процессов в рамках существующей функциональной структуры весьма удобно. В ходе работы по этой схеме процессная модель и функциональная структура организации взаимодействуют между собой и усиливают преимущества друг друга.

Совместное использование обеих моделей также упрощает внедрение процессной модели. Процессная модель влияет не на полномочия функциональных менеджеров, а на формы осуществления этих полномочий. Процессные менеджеры принимают на себя задачу координации функций, которая в чисто функциональной модели решается на излишне высоком уровне.

Переход к процессной модели можно осуществить двумя путями:

- первый состоит в формализации опыта данной организации;
- второй предполагает использование передового опыта управления службой ИС, который реализован в типовых моделях бизнес-процессов этой службы.

На сегодняшний день общей методологической основой таких моделей является подход ITIL/ITSM, основанный на сборе и систематизации передовой практики управления службой ИС в течение последних 20 лет.

Использование типовых моделей бизнес-процессов службы ИС имеет целый ряд преимуществ.

Во-первых, типовая модель представляет в концентрированном виде опыт управления службой ИС в тысячах и даже десятках тысяч компаний. Соответственно, отказ от использования этого массива знаний по меньшей мере нецелесообразен.

Во-вторых, переход к процессной модели управления для всех задач службы ИС одновременно, в рамках одного проекта маловероятен. В этом случае процессная модель дает менеджеру образ будущего, который становится ориентиром в ходе отдельных шагов внедрения.

В-третьих, типовая модель процессов службы ИС всегда опирается на некую систему понятий, на некий язык. Использование этого языка значительно облегчает достижение взаимопонимания участников процесса.

В-четвертых, типовая модель процессов поддержана разработчиками программного обеспечения автоматизации управления службой ИС и инфраструктурой ИТ. В результате программное обеспечение реализует именно эти

процессы. Реализация собственных процессов потребует разработки собственного ПО.

Наконец, стандартная модель процессов обычно внедряется во многих организациях. В результате образуется сообщество пользователей, которое является ценным источником информации по внедрению модели.

В этой теме были рассмотрены основные понятия ИТ-менеджмента, ИТ-сервиса, характеристики ИТ-сервиса, основы процессной модели управления ИС-службой в ее взаимосвязи с ИТ-сервисами, с одной стороны, и функциональной моделью, с другой стороны.

1.3 Темы рефератов

1. Поясните понятие ИТ-менеджмента и раскройте его содержание.
2. Перечислите основные объекты ИТ-менеджмента и охарактеризуйте их.
3. Что определяет инфраструктура ИТ-предприятия?
4. Чем обусловлены постоянные изменения в ИС предприятий?
5. Раскройте понятие «ИТ-сервис».
6. Приведите примеры корпоративных ИТ-сервисов и охарактеризуйте их.
7. Перечислите и поясните основные характеристики ИТ-сервисов.
8. Как задается и чем определяется характеристика «время обслуживания» для ИТ-сервиса?
9. Как задается и чем определяется характеристика «производительность» для ИТ-сервиса?
10. Почему в организационной структуре службы ИС целесообразно выделять подразделения разработки и сопровождения ИС?
11. Поясните основные функциональные направления службы ИС.
12. Какие факторы и почему влияют на организационную структуру службы ИС?
13. Какая существует связь и почему между функциями службы ИС и параметрами ИТ-сервиса?
14. Какие возможны варианты перехода от функциональной к процессной модели службы ИС предприятия?
15. Какие имеются преимущества использования типовых моделей бизнес-процессов службы ИС?

1.4 Литература

1. Экономическая информатика: Введение в экономический анализ информационных систем. Учебник. – М.:ИНФРА-М, 2005, 958 с.

2 ITIL/ITSM − КОНЦЕПТУАЛЬНАЯ ОСНОВА ПРОЦЕССОВ ИС-СЛУЖБЫ

2.1 Общие сведения о библиотеке ITIL (IT Infrastructure Library)

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.

Отражением трансформации роли и места ИТ-службы в структуре предприятий является концепция и модель управления качеством информационных услуг (Information Technology Service Management – ITSM, управление ИТ-услугами) [1]. Бизнес-процессы сегодня неразделимы с программными приложениями, техническими ресурсами и деятельностью персонала ИТ-служб, поэтому качество работы последних становится важнейшим фактором, определяющим эффективность деятельности предприятия в целом.

Модель ITSM является открытой для изменения со стороны пользователей и описывает совокупность процессов службы ИС. Это позволяет настраивать процессы ITSM для конкретного применения. Существует большое количество инструментальных средств, реализующих модели процессов ITSM, разработанных компаниями-консультантами и производителями программного обеспечения управления инфраструктурой ИТ. Модель ITSM не дает ИТ-менеджеру службы ИС однозначных рекомендаций как конкретно строить систему управления информационной инфраструктурой предприятия. В то же время концепция ITSM содержит модель типовых процессов службы ИС, поня-

тийный аппарат, на основе которых целесообразно строить модели процессов для ИТ-службы.

Модель ITSM, разработанная в рамках проекта ITIL (IT Infrastructure Library - библиотека инфраструктуры информационных технологий, произносится как *«айти́л»*), описывающая процессный подход к предоставлению и поддержке ИТ-услуг [2, 3]. Данная модель получила наибольшую известность в силу того, что предоставление и поддержка ИТ-услуг является первичной задачей ИТ-службы предприятия.

В отличие от более традиционного функционального подхода к организации ИТ-службы, ITSM рекомендует сосредоточиться на клиенте и его потребностях, на ИТ-услугах, предоставляемых пользователю информационными технологиями, а не на них самих. При этом процессная организация предоставления услуг и наличие заранее оговоренных уровней параметров эффективности позволяет ИТ-службе предоставлять качественные ИТ-услуги, измерять и улучшать их качество.

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 [2]. 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 ком-

понент 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.

Текущая версия библиотеки ITIL включает 7 книг по основным разделам управления ИТ-сервисами [3]:

- 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, разрабатываемой версии библиотеки ITIL (проект ITIL Refresh), представлено пять книг, названия которых отражают жизненный цикл ИТ-услуг:

- «Стратегии обслуживания» (Service Strategies);
- «Проектирование услуг» (Service Design);
- «Внедрение услуг» (Service Introduction);
- «Оказание услуг» (Service Operation);
- «Непрерывное совершенствование услуг» (Continuous Service Improvement).

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 и на сегодняшний день объединяет около 200 представителей из более чем 45 российских компаний.

С более подробной информацией по библиотеке ITIL можно познакомиться на сайтах, приведенных в табл. 2.1, 2.2.

Таблица 2.1 – Англоязычные сайты

Web-адрес	Описание
www.itil-officialsite.com/	Оффициальный сайт ITIL
www.itil.org/en/index.php	Сайт на английском и немецком, общие сведения
www.itil.org.uk	Информация по ITL
www.pinkelephant.com	Компания — эксперт в области ITIL, создает ITIL v3
www.itilmonkey.com/	Статьи по ITIL
www.itilcommunity.com/	Форум по ITIL
www.itilpedia.com/	Ссылки и информация
www.itsm-portal.com/	Статьи по ITIL
www.ogc.gov.uk	Статьи по ITIL
www.itservicetoday.com/	Статьи по ITIL
manageengine.adventnet.com/	Статьи о Service Desk
www.asktheserviceexpert.com/	Статьи от Robin Yearsley
www.isoiec20000certification.com/	Статьи ISO 20000

Продолжение табл.2.1

Web-адрес	Описание
www.itsmwatch.com	Статьи, форум
www.toolselector.com/	Статьи, форум, ссылки и многое др.
www.bita-center.com/	Ссылка на bita-сайт (business-to-it-allignment).
en.wikipedia.org/wiki/Itil	Новости, анонсы
www.itilsurvival.com	Много ссылок на платные ресурсы
www.becta.org.uk/fits	FITS — Framework for ICT Technical Support, построен на принципах ITIL
www.becta.org.uk/tsas/	«Облегченная» ITIL, предназначенная для британских школ
www.itserviceblog.com/	Блоги по тематике ITIL
en.itsmportal.net/	Портал по ITSM (статьи, книги, советы, форум)
dritil.blogspot.com/	Статьи и блоги по тематике ITIL
www.itilworx.com/	Статьи по тематике ITIL
www.informit.com	IT Management Reference Guide
service.mirror42.com	Библиотека KPI
www.itservicetoday.com	Сайт об ITSM — IT Service Today;

Таблица 2.1 – Англоязычные сайты

Web-адрес	Описание
www.itsmportal.ru/	Информационный портал по управлению ИТ
www.akmeev.ru/	Сайт Руслана Акмеева, информация про MOF и ITIL, таблица взаимодействия процессов и ролей
easmf.ru/	Евразийский форум по управлению сервисами
www.networkdoc.ru/forum	Форум по ITIL
krylov.lib.ru/index.html	Страница Евгения Крылова, статьи по ITIL

Внедрение методики управления ITSM – поэтапный процесс. Как показывает практика, решение первоочередных задач связано с рекомендациями, приведенными в первых книгах «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.

2.2 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. К инцидентам относятся, например, невозможность загрузить операционную систему, сбой электропитания, сбой жесткого диска на рабочей станции пользователя, появление компьютерного вируса в локальной сети офиса, отсутствие тонера или бумаги для печатающего устройства и т.д. 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.

На рис. 2.1 приведена диаграмма активности для процесса Управление инцидентами. 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.

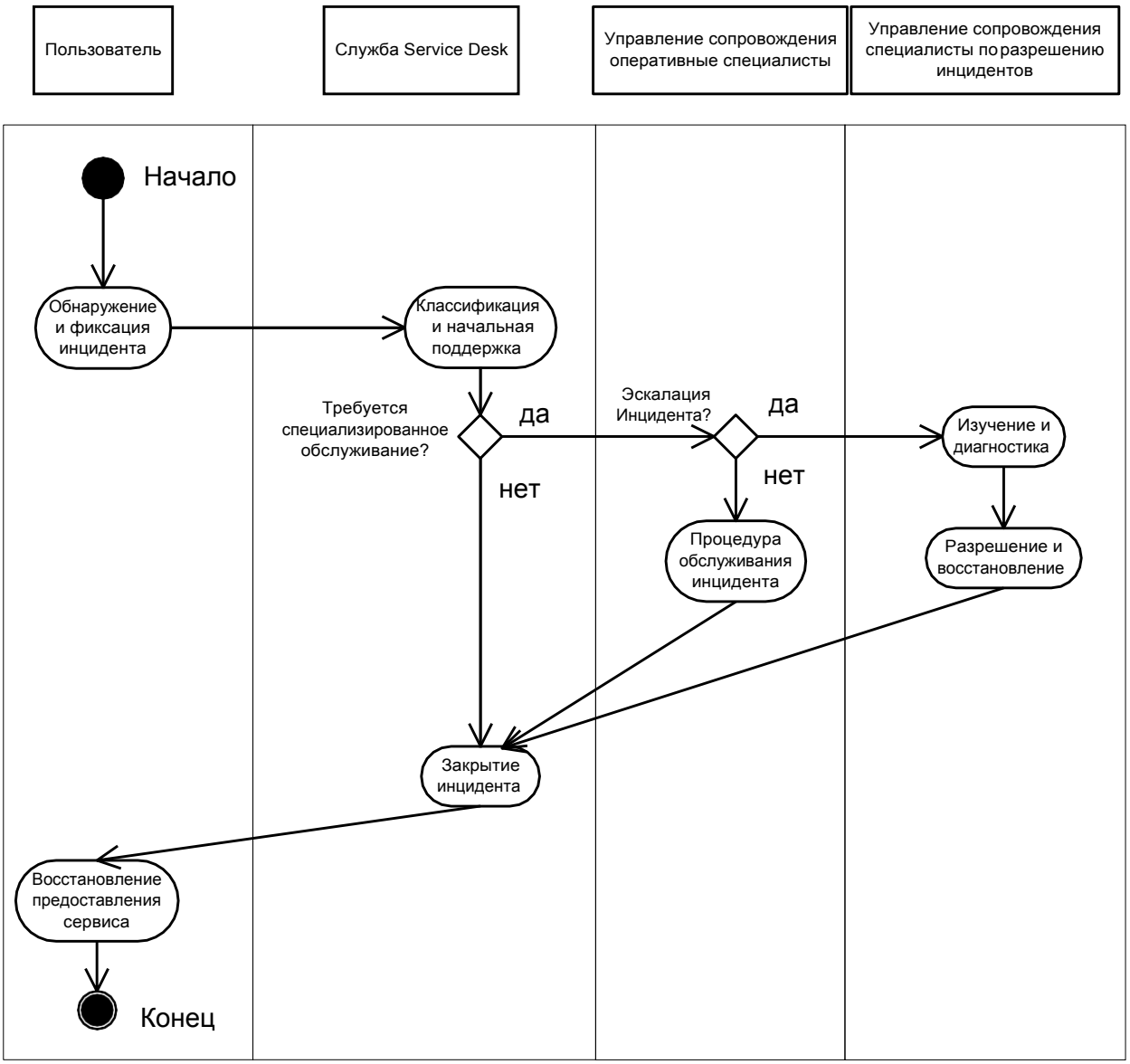

Рисунок 2.1 – Диаграмма активности процесса управления инцидентами

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.

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.

На рис. 2.2 приведена диаграмма активности для процесса Управление проблемами.

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.

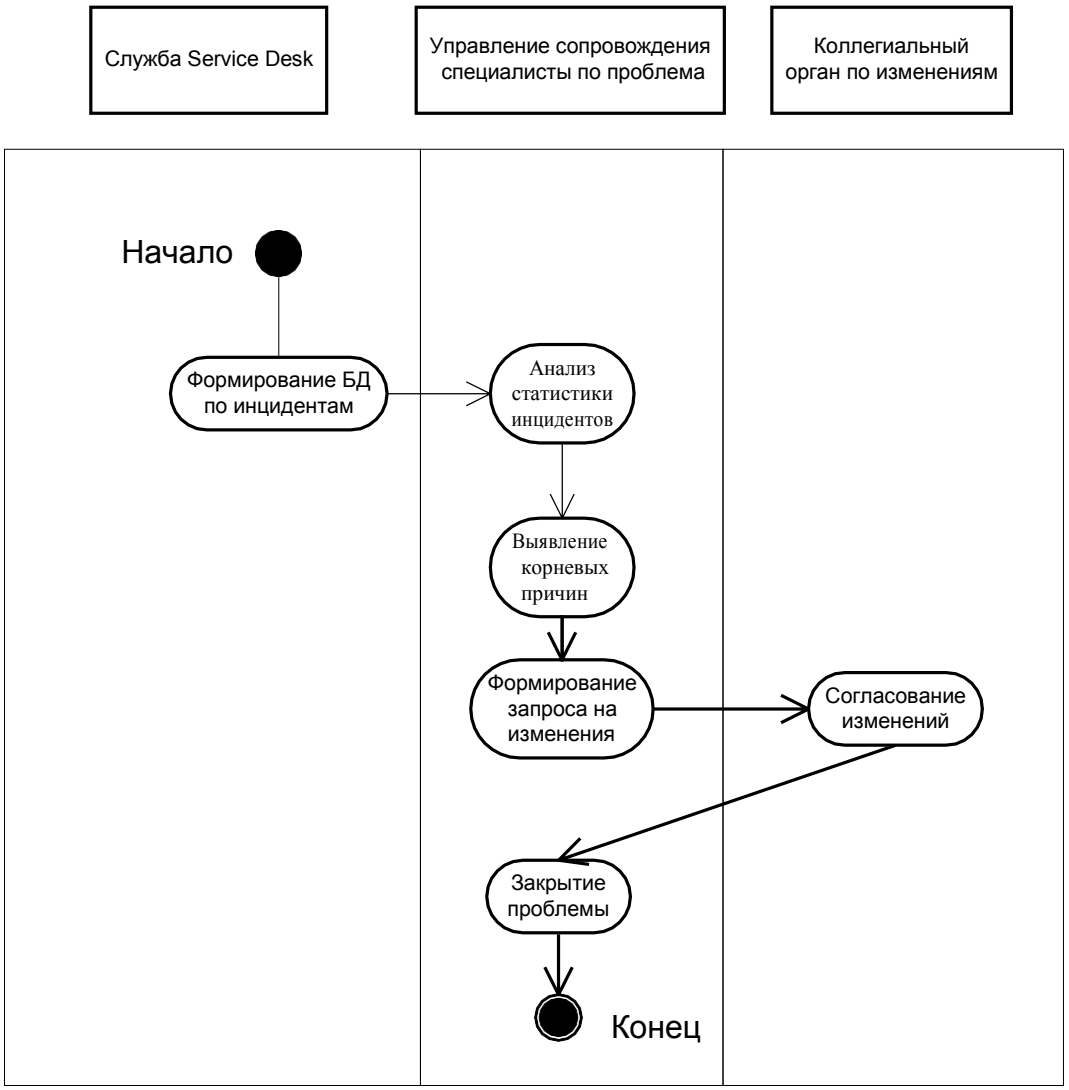

Рисунок 2.2 – Диаграмма активности процесса управления проблемами

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. На рис.2.3 приведен пример модели классификации конфигурации [4].

```
Конфигурация
     Элемент конфигурации (CI)
          Ресурс ИТ
               Стока  серверная
               Узел технологический
                    Компьютер
                    Сервер
                    Настольный ПК
                    Ноутбук
                    КПК
                    Устройство хранения данных
                    Концентратор
                    Коммутатор
               Устройство комплектующее
                    Жесткий диск
                    Процессор
                    Плата сетевая
                    Потр
               ПО системное
                    Операционная система
                    ПО серверное
                    СУБД
                    ПО управляющее
               ПО прикладное
                    Пакет прикладных программ
                    Конфигурация программы
                         Файл конфигурации
                         IP-адрес
                         Имя хост-машины
                         DNS
                         Сетевой интерфейс
                    База данных
                    Сервис
                         Бизнес-сервис
                         Технологический сервис
                         Web-сервис
               Сотрудник
                    Администратор
                    Системный инженер
                    Пользователь
               Документ
                    Бизнес-документ
                    Регламент
                    Техническое описание
                    Контракт
```

Рисунок 2.3 – Классификация элементов конфигурации

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;
- соединенная.

Логические отношения:

- копия;
- «использует», когда одна единица использует другую. Например, программа использует сервер.

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. Диаграмма активности процесса управления изменениями приведена на рис. 2.4.

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.

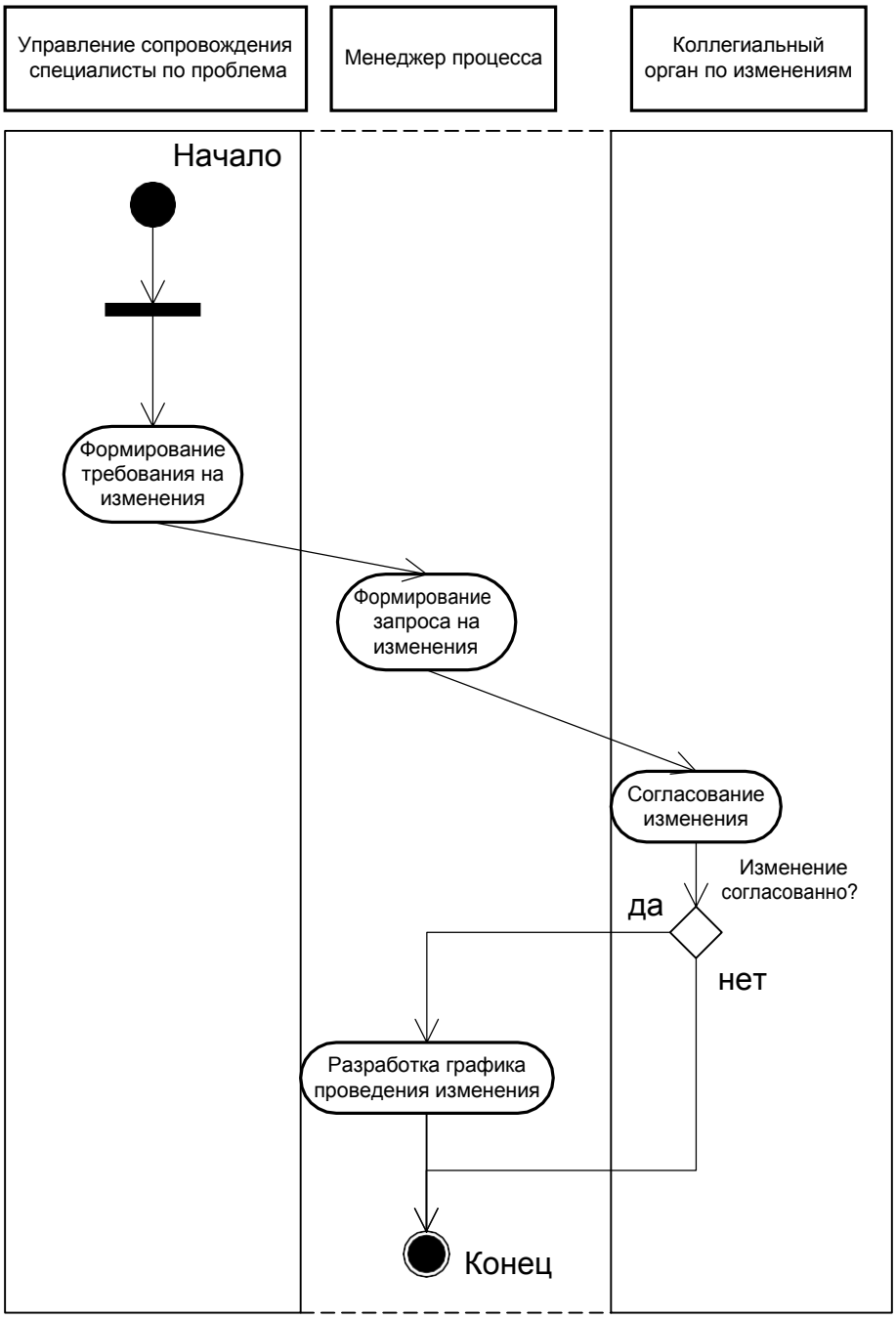

Рисунок 2.4 – Диаграмма активности процесса управления изменениями

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.

2.3 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.

Диаграмма активности процесса управления уровнем сервиса приведена на рис. 2.5. Бизнес-пользователь формулирует требования к ИТ-услуге (установить поддержку электронной почты в режиме 24 × 7). 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.

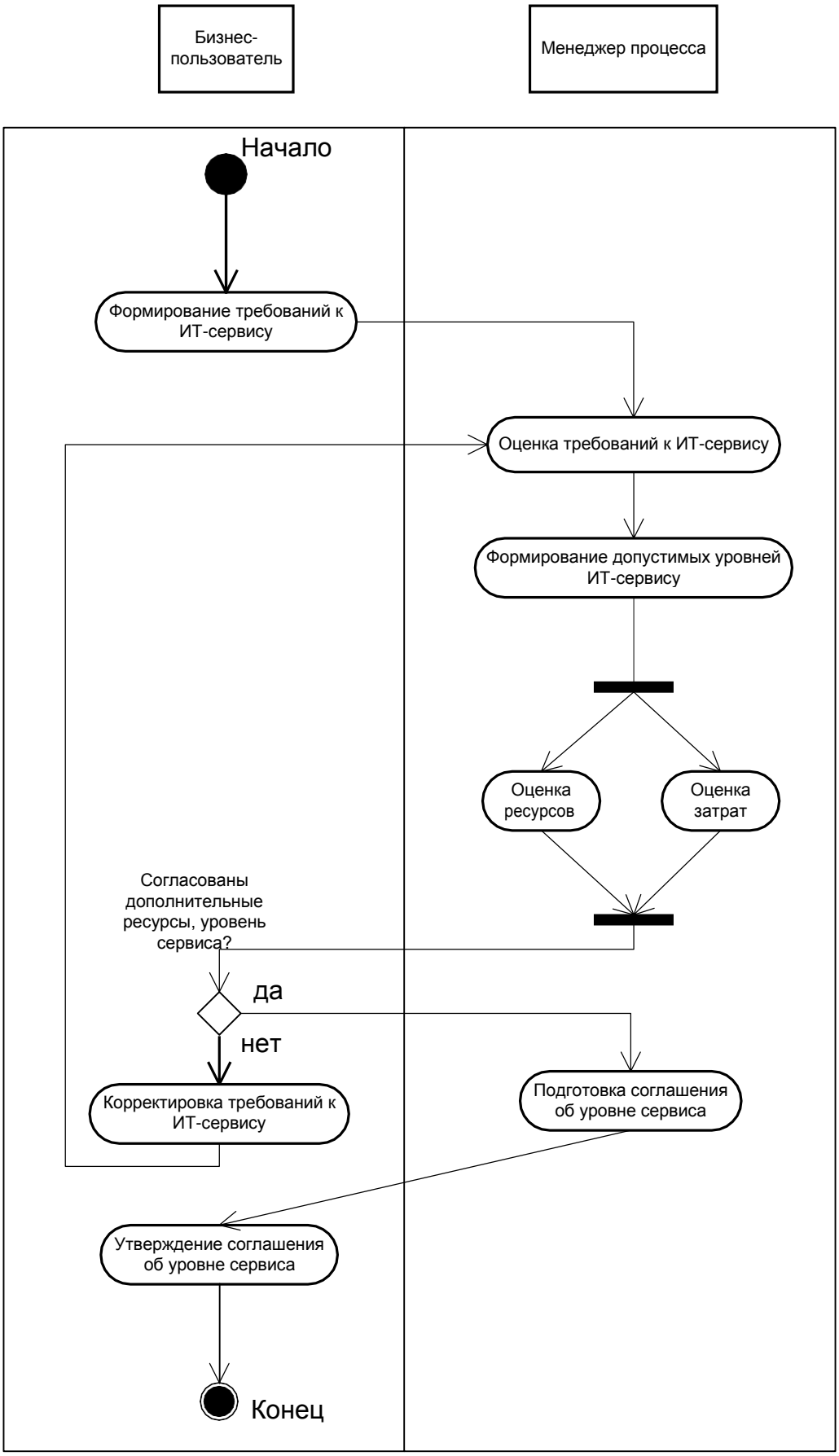

Рисунок 2.5 – Диаграмма активности процесса управления уровнем сервиса

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

Возможный вариант диаграммы активности процесса управления доступностью приведен на рис. 2.6. На уровне процесса управления проблемами обнаружена известная ошибка. 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.

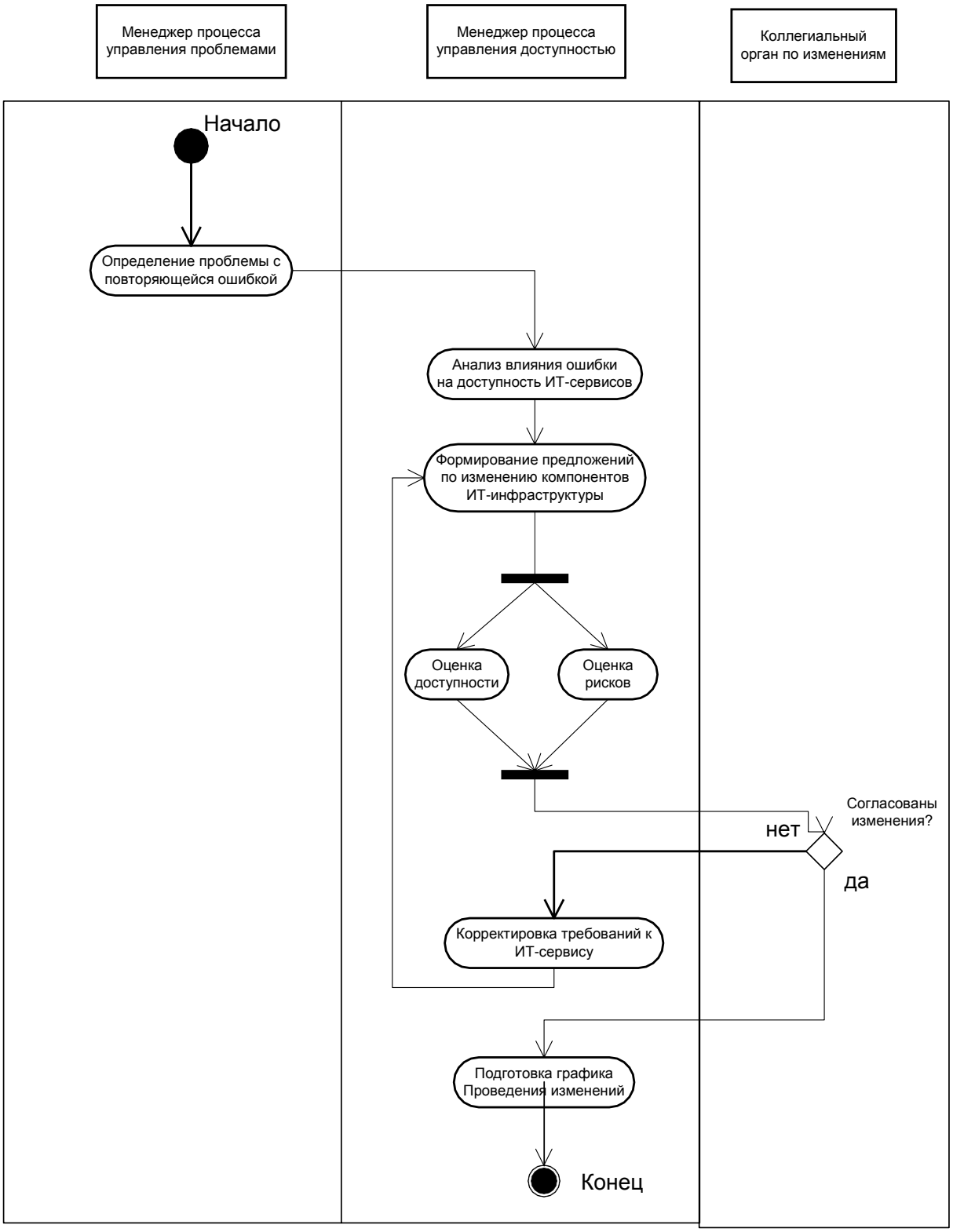

Рисунок 2.6 – Диаграмма активности процесса управления доступностью

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 зафиксирова-

ны 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 [5]:

- 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.

Основная цель 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 финансо-

вых 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.

2.4 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.

В этой теме были рассмотрены методологические основы управления ИТ-инфраструктурой предприятия, базирующиеся на библиотеке передового опыта ITIL и модели ITSM. Для оперативных и стратегических процессов ИТ-службы проанализированы задачи и предложены диаграммы активности. Рассмотрена роль соглашения об уровне сервиса для ИТ-службы предприятия.

2.5 Темы рефератов

1. Как характеризуется роль ИС-службы в современном бизнесе?
2. Чем модель ITSM отличается от традиционного функционального подхода к организации ИТ-службы?
3. Перечислите и поясните особенности проекта ITIL.
4. Какие разделы управления ИТ-сервисами описаны в текущей версии библиотеки ITIL? Опишите разделы подробно.
5. Какие направления управления ИТ-услугами описаны в проекте ITIL Refresh? Опишите направления подробно.
6. Какие процессы включены в блок поддержки ИТ-сервисов? Опишите процессы подробно.
7. Какие процессы включены в блок предоставления ИТ-сервисов? Опишите этот блок подробно.
8. Поясните назначение процесса управления инцидентами.
9. Поясните понятие «инцидент». Приведите примеры.
10. Приведите и опишите основные функции процесса управления инцидентами.
11. Поясните назначение процесса управления проблемами. Примеры.
12. Поясните понятие «проблема». Приведите примеры.
13. Приведите и опишите основные функции процесса управления проблемами.
14. Поясните назначение процесса управления конфигурациями. Примеры.
15. Поясните понятие «конфигурационная единица». Приведите примеры.
16. Для чего используется БД конфигурационных единиц – CMDB?
17. Что могут описывать атрибуты конфигурационных единиц в CMDB?
18. Какие важные понятия описываются в спецификации процесса управления конфигурациями?
19. Поясните назначение процесса управления изменениями. Примеры.

20. Приведите основные функции процесса управления изменениями. Характеристики.
21. Поясните назначение процесса управления релизами. Примеры.
22. Поясните понятие «релиз». Приведите примеры.
23. Как классифицируются релизы по показателю масштаба изменений?
24. Приведите основные функции процесса управления релизами.
25. Поясните назначение и содержание библиотеки эталонного ПО DSL.
26. Поясните назначение процесса управления уровнем сервиса.
27. Поясните понятие «соглашение об уровне сервиса SLA».
28. Приведите основные функции процесса управления уровнем сервиса.
29. Поясните назначение процесса управления мощностями.
30. Приведите основные функции процесса управления мощностями.
31. Поясните назначение процесса управления доступностью.
32. Поясните понятие «доступность ИТ-сервиса». Примеры.
33. Приведите основные функции процесса управления доступностью.
34. Поясните назначение процесса управления непрерывностью.
35. Приведите основные функции процесса управления непрерывностью.
36. Поясните назначение процесса управления финансами ИТ-службы.
37. Приведите основные функции процесса управления финансами ИТ-службы.
38. Поясните назначение процесса управления безопасностью.
39. Поясните возможность применения модели ITSM на предприятиях различного масштаба.
40. Поясните сущность реактивного принципа работы службы ИТ-поддержки.
41. Поясните сущность проактивного принципа работы службы ИТ-поддержки.

2.6 Литература

1. Н. Дубова. ITSM – новая идеология управления ИТ: www.osp.ru/os/2000/10/178254/.
2. А. Александров. CMDB: Досье для управления ИТ: www.osp.ru/os/2006/10/3910054/.
3. А. Кожухов. Управление непрерывностью ИТ-услуг, Корпоративные системы, № 9, 2006: www.iemag.ru/analitics/detail.php?ID=16170.

3 РЕШЕНИЯ HEWLETT-PACKARD ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

3.1 Модель информационных процессов ITSM Reference Model

Корпорация Hewlett-Packard (HP) – одна из компаний, полностью взявшая на вооружение рекомендации ITIL. Ее применение позволило HP не только войти в число ведущих поставщиков услуг консалтинга и внедрения, но и стать одним из крупнейших провайдеров услуг по обучению основам ITIL и сертификации этих знаний.

Для практического применения ITIL компания HP разработала собственный вариант методологии, получивший название «Типовой модели HP ITSM» (IT Service Management Reference Model – ITSM Reference Model). Ее первый вариант был опубликован в сентябре 1997 г., следующий - в январе 2000 г. Действующая сегодня версия HP ITSM 3.0 выпущена в июне 2003 г. Подчеркнем, что HP ITSM построена в точном соответствии с ITIL и не противоречит ее положениям.

Следует также отметить, что ITSM Reference Model носит лишь рекомендательный характер. Однако одна из ключевых идей этой методологии состоит в том, что, несмотря на разнообразие информационных систем, их работа на 80% может быть построена на базе стандартизованных процессов и регламентов. Поэтому адаптация методологии к конкретным, специфическим задачам предприятия требует настройки не более 20% системы ИТ-сервиса.

Методология HP — ITSM Reference Model в общем жизненном цикле обслуживания ИС выделяется пять основных групп процессов [1, 2]:

- согласование задач бизнеса и ИТ (Business – IT Alignment);
- планирование и управление ИТ-сервисами (Service Design & Management);
- разработка и внедрение ИТ-сервисов (Service Development & Deployment);

– оперативное управление ИТ-сервисами (Service Operations);

– обеспечение ИТ-сервисами (Service Delivery Assurance).

При этом первые четыре блока принято рассматривать как следующие друг за другом в рамках жизненного цикла работы ИТ-службы, а в центр помещать пятый блок, отвечающий за предоставление услуг (рис. 3.1).

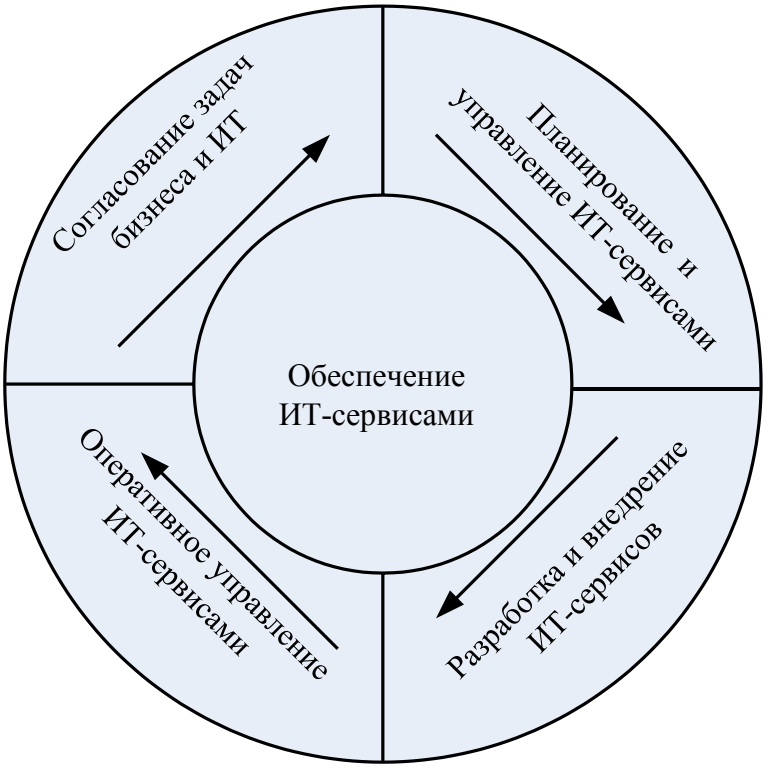

Рисунок 3.1. Блоки процессов модели ITSM Reference Model

Блок процессов *согласование задач бизнеса и ИТ* обеспечивает реализацию ИТ-стратегии в соответствии с целями бизнеса и создает основу для количественной оценки эффективности затрат на ИТ. В данный блок входят следующие процессы.

– анализ потребностей бизнеса (IT business assessment);

– разработка стратегии развития ИТ предприятия (IT strategy & architecture planning);

– управление клиентами (Customer management);

– планирование ИТ-сервисов (Service planning).

При разработке портфеля ИТ-сервисов процессы этого блока согласуют ИТ-стратегию предприятия с бизнес-целями, который обеспечивает макси-

мальный эффект для бизнеса. Разработка эффективного портфеля ИТ-сервисов требует, чтобы информационные технологии определяли важные для бизнеса ИТ-сервисы и согласовывали ИТ-функции и бизнес-функции с доступными возможностями информационных технологий, потребностями бизнеса и приоритетами обслуживания бизнеса. Эти процессы позволяют ИТ-службе согласовывать ИТ-стратегию, архитектуру, организационную структуру и портфель ИТ-сервисов с бизнес-целями – и, в конечном счете, отображать стратегию в согласованные уровни обслуживания ИТ-сервисов.

Процесс *анализ потребностей бизнеса* подразумевает анализ рынка ИТ-услуг с точки зрения применения информационных технологий. Этот процесс предполагает проведение оценки того как ИТ-сервисы могут способствовать повышению эффективности деятельности предприятия, выявление важности ИТ-сервисов для бизнес-подразделений и оценки ресурсов для предоставления ИТ-сервисов. В частности, здесь определяется приоритет тех или иных сервисов с точки зрения пользователей и оценивается стоимость ИТ-сервисов.

Процесс *разработки стратегии развития ИТ предприятия* позволяет сформировать ИТ-стратегию на основе оценки бизнеса и спланировать ИТ-архитектуру. Согласование требований бизнеса и возможностей информационных технологий позволяет обосновать план внедрения ИТ-сервисов, важных для бизнеса предприятия, определить общие количественные показатели работы ИТ-службы и сформировать последовательный план развития ИТ-стратегии и ИТ-архитектуры.

Процесс *управления клиентами* позволяет ИТ-службе организовывать свою деятельность на партнерских отношениях с бизнес-пользователями информационной системы. Различные функции процесса позволяют отслеживать потребности клиентов, прогнозировать изменения их требований, доводить до клиентов существующие уровни обслуживания ИТ-сервисов, оценивать удовлетворенность клиентов и участвовать в совместном решении задач.

Процесс *планирования ИТ-сервисов* позволяет сформировать необходимые этапы внедрения сервисов, оценить риски, связанные с этим, наметить пути максимизации возврата инвестиций.

Блок процессов *планирования и управления ИТ-сервисами* формирует детализированную информацию по проектированию новых ИТ-сервисов, управлению доступностью и качеством этих сервисов, а также поддержания нужного баланса между качеством и стоимостью. Данный блок включает следующие процессы:

- управление безопасностью (Security management);
- управление непрерывностью (Continuity management);
- управление готовностью (Availability management);
- управление производительностью (Capacity management);
- финансовое управление (Financial management).

Процесс *управление безопасностью* позволяет определять уровень безопасности, проводить мониторинг и управлять безопасностью корпоративной информации. Процесс формализует задачи обеспечения, управления и поддержания безопасности ИТ-инфраструктуры предприятия. Он является неотъемлемой частью общего корпоративного плана безопасности предприятия.

Процесс *управления непрерывностью* должен обеспечить ИТ-службе способность предоставлять заданный уровень услуг даже в результате серьезных внешних потрясений бизнеса.

Процесс *управления готовностью* управляет возможностью реального получения ИТ-сервисов пользователями в соответствии с согласованными уровнями обслуживания.

Процесс *управления производительностью* подразумевает, что ИТ-службы способны справляться с потоком поступающих заданий на предоставление ИТ-сервисов в соответствии с согласованными уровнями обслуживания.

Процесс *управления финансами* позволяет ИТ-службе определять стоимость предоставляемых ИТ-сервисов и покрывать свои расходы за счет платы со стороны потребителей.

Блок *процессов разработки и внедрения ИТ-сервисов* обеспечивает создание и тестирование новых сервисов и используемых ими инфраструктурных компонентов, включая установку оборудования и ПО, разработку приложений, обучение и т. п. Сюда входят два типа процессов:

- разработка и тестирование (Service build and test);
- ввод в эксплуатацию (Release to production).

Процесс *разработки и тестирования* выполняют разработку и проверку работоспособности и функциональности внедряемых ИТ-сервисов.

Процесс *ввода в эксплуатацию* обеспечивает развертывание новые или модернизированные компонентов и функции ИТ-сервисов для определенных пользователей с учетом их конкретных потребностей.

Блок процессов *оперативное управление ИТ-сервисами* обеспечивает ежедневный мониторинг предоставляемых ИТ-сервисов, управление запросами пользователей, отслеживание удовлетворенности клиентов и оценку общего уровня качества выполняемых сервисных работ. В данный блок входят следующие процессы:

- оперативное управление (Operation management);
- управление инцидентами (Incident and service request management);
- управление проблемами (Problem management).

Процесс *оперативного управления* позволяет управлять постоянным процессом предоставления ИТ-сервисов в соответствии с заданными уровнями обслуживания.

Процесс *управления инцидентами* обеспечивает фиксацию всех инцидентов в информационной системе и быстрое реагирование на нужды потребителей.

Процесс *управления проблемами* фокусируется на задаче снижения числа инцидентов на основе анализа и прогноза работы информационной системы и заблаговременного устранения потенциальных проблем или более оперативного их разрешения.

Блок процессов *обеспечение ИТ-сервисами* описывает предоставление соглашений и информации, процедуры взаимодействия для выполнения соглашений об уровне сервиса. Центральное положение этой группы на рис. 3.1 отражает ее связующую роль в ITSM. В состав этой группы входят три типа процессов:

- управление конфигурациями (Configuration management);
- управление изменениями (Change management);
- управление уровнями услуг (Service-level management).

Процесс *управления конфигурациями* отвечает за регистрацию и отслеживание состояния каждого компонента ИТ-инфраструктуры. Все сведения о компонентах (технические характеристики, состояние и различные взаимосвязи) хранятся в локальной базе данных Configuration Management Database.

Процесс *управления изменениями* гарантирует, что ИТ-службы используют стандартные методы и процедуры для управления всеми изменениями в информационной среде предприятия.

Процесс *управления уровнями услуг* позволяет выделять отдельные специфические услуги для потребителей в рамках стандартного спектра предоставляемого сервиса.

При внедрении процессного управления ИТ-службы предприятия методология HP ITSM [3, 4] выделяет три основные стадии эволюции ИТ-служб:

- управление инфраструктурой (Managing the infrastructure);
- управление сервисами (Managing the services);
- управление деловыми характеристиками ИТ (Managing the business value of IT).

Стадия *управление инфраструктурой* предполагает реализацию следующих процессов:

- управление операциями;
- управление конфигурацией;
- управление изменениями;
- управление инцидентами и сервисными запросами.

Стадия *управление сервисами* рекомендует внедрение следующих процессов:

- создание и тестирование сервисов;
- сервис-ориентированное управление;
- управление проблемами;
- управление непрерывностью;
- управление готовностью;
- управление объемами услуг;
- управление финансами.

Стадия *управление деловыми характеристиками ИТ* определяет уровень стратегического бизнес-партнера руководства компании и ИТ-службы. Одна из важнейших характеристик этой стадии – полная интеграция ИТ-процессов в общую бизнес-модель организации. Как результат, такой статус подразумевает, что руководители предприятия должны четко понимать, как те или иные инвестиции в ИТ могут способствовать развитию основного бизнеса компании. На этой стадии должны быть реализованы остальные процессы ITSM Reference Model:

- бизнес-оценка;
- управление отношениями с пользователями;
- планирование ИТ-стратегии и развития архитектуры;
- планирование развития сервисов.

Реализация методологии ITSM Reference Model напрямую связана с общей задачей повышения уровня управления качеством работы компаний. В качестве ориентиров могут быть выбраны стандарты ISO 9000, но для ИТ-подразделений лучше использовать модель CMM (Capability Maturity Model, модель уровня зрелости), в большей степени ориентированную на ИТ-отрасль.

3.2 Программные решения HP OpenView

Программные решения HP OpenView, предназначенные для централизованного управления ИТ-ресурсами предприятия, обеспечивают прозрачность управления и тесную интеграцию с бизнес-процессами [5]. 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.

3.2.1 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.

3.2.2 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.

3.2.3 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.

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.

Более подробно рассмотрим решения по идентификации и поддержке пользователей.

3.2.3.1 Управление идентификацией – Identity Management

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 централизо-

ванное управление авторизацией в беспроводных и кабельных сетях Internet и экстранет. Решение поддерживает различные механизмы аутентификации, включая ввод регистрационного имени и пароля самим пользователем, Kerberos[1] и Radius[2], аутентификацию с использованием токенов, идентификаторов SecurID и сертификатов X.509[3].

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 дей-

---

[1] **Kerberos** - протокол аутентификации, при помощи которого компьютер, собирающийся установить связь с другим компьютером, может подтвердить свою «личность».

[2] **RADIUS** (***R**emote **A**uthentication in **D**ial-**I**n **U**ser **S**ervice*) — протокол AAA (authentication, authorization и accounting), разработанный для передачи сведений между программами-сервисами (NAS, Network Access Server) и системой биллинга

[3] **X.500** — серия стандартов для службы распределенного каталога сети. Каталоги X.500 предоставляют централизованную информацию обо всех именованных объектах сети (ресурсах, приложениях и пользователях).

ствий, 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.

3.2.3.2 Решение HP OpenView Service Desk

Решение HP OpenView Service Desk – это готовое решение для автоматизации служб технической поддержки и внедрения процессов управления IT-услугами [6]. 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.

В основе эффективного управления на основе SLA лежит четкое понимание зависимости различных служб, лежащих в основе информационной инфра-

структуры. HP OpenView Service Desk включает расширения, которые помогают оператору сориентироваться благодаря:

– отображению служб в группах по типам;

– возможности иерархической классификации служб, точно описывающей зависимости между ними.

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;

– 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 предоставляет стандартное решение для создания объединенной службы поддержки, основанное на лучших отраслевых технологиях.

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.

3.2.4 Управление 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 [7]. 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.

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.

3.3 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 [8].

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 ос-

новные 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 на-

страивать под нужды клиентов удобные веб-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 Open View 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 Open View 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.

В этой теме были рассмотрены методология компании Hewlett-Packard, представленная моделью ITSM Reference Model и программные средства автоматизации управления ИТ-инфраструктурой предприятия HP Open View.

3.4 Темы рефератов

1. В каком году опубликован первый вариант типовой модели HP ITSM Reference Model?
2. Какие основные группы процессов определены в методологии HP ITSM Reference Model?
3. Поясните основное назначение блока процессов «Согласования задач бизнеса и ИТ».
4. Поясните основное назначение блока процессов «Планирование и управление ИТ-сервисами».
5. Поясните основное назначение блока процессов «Разработка и внедрение ИТ-сервисов».
6. Поясните основное назначение блока процессов «Оперативное управление ИТ-сервисами».
7. Поясните основное назначение блока процессов «Обеспечение ИТ-сервисами».
8. Назовите и поясните основные стадии внедрения процессного управления ИТ-службы предприятия.
9. Какие процессы внедряются на стадии «Управление ИТ-инфраструктурой»?
10. Какие процессы внедряются на стадии «Управление сервисами»?
11. Какие процессы внедряются на стадии «Управление деловыми характеристиками ИТ»?
12. Назовите набор основных решений HP Open View, предназначенных для централизованного управления ИТ-ресурсами предприятия.
13. Охарактеризуйте решение HP Open View «Управление бизнесом».
14. Охарактеризуйте решение HP Open View «Управление приложениями».
15. Охарактеризуйте решение HP Open View «Управление ИТ-инфраструктурой».
16. Охарактеризуйте решение HP Open View «Управление ИТ-службой».

17. Охарактеризуйте решение HP Open View «Управление идентификацией».
18. Охарактеризуйте решение HP Open View «Service Desk».
19. Охарактеризуйте решение HP Open View «Network Node Manager».
20. Поясните назначение пакета программ HP Open View Compliance Manager.
21. Поясните назначение пакета программ HP Open View Perfomance Insight.
22. Поясните назначение пакета программ HP Open View Reporter.
23. Поясните назначение пакета программ HP Open View Dashboard.
24. Поясните назначение пакета программ HP Open View Information Portal.
25. Поясните назначение пакета программ HP Open View Business Process Insight.

3.5 Литература

1. ITSM Reference Model: ftp.hp.com/pub/services/itsm/info/itsm_rmwp.pdf.
2. Введение в ИТ сервис-менеджмент – принципы управления ИТ-услугами и сервисами: www.itexpert.ru/rus/biblio/articles/200406222006/200406222044/.
3. Развитие ITIL: www.itsmportal.ru/articles/itil/2004-02-04-00_00_00-31.html.
4. HP Open View: https://en.wikipedia.org/wiki/HP_OpenView.

4 РЕШЕНИЯ IBM ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

4.1 Модель информационных процессов ITPM

Модель информационных процессов ITPM (IT Process Model), возникшая 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 [1]. 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 информацией;
- 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 основных 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 системы.

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 ресурсы;

– замеры времени, необходимого для выполнения того или иного процесса;

– соблюдение политики безопасности.

4.2 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 [2]:

- 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 [2].

4.2.1 Базовые технологии IBM/Tivoli

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 систе-

му 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 функционирования управляемых систем;

– работа с различными типами Data Provider;

– наблюдение и посылка оповещений об изменении статуса источников данных.

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

Для реализации бизнес-ориентированного управления приложениями и системами платформа Tivoli предоставляет следующие программные решения [3]:

– *Application Dependency Discovery Manager*, который обеспечивает обнаружение и поддержание в актуальном состоянии зависимостей между 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* представляет собой решение для мониторинга характеристик транзакций в распределённых 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 техно-

логические 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 объективной 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 управления процессами хранения данных в соответствии с рекомендациями ITIL и на основе методологии процессного управления IBM Tivoli Unified Process;

– *Unified Process Composer* предоставляет детализированное описание 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..

4.2.3 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 [4], которые отличается простотой установки, внедрения и управления. В линейку программных продуктов входят IBM Tivoli:

- Identity 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. 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 отчётность о программном и аппаратном обеспечении и их владельцах;

– замену медленных и дорогостоящих методов ручной инвентаризации;

– предотвращение закупки лишних или недоиспользованных лицензий 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.

В данной теме были рассмотрены модель информационных процессов ITPM и семейство продуктов IBM/Tivoli, которые позволяют управлять

практически любой информационной системой независимо от ее состава, сложности, размера и территориального расположения.

4.3 Темы рефератов

1. Как соотносятся модель ITPM (IT Process Model) и библиотека ITIL?
2. Какие группы процессов определены в ITPM?
3. Поясните сущность процесса «Улучшение взаимодействия с клиентами».
4. Поясните сущность процесса «Обеспечение управленческих систем корпоративной информацией».
5. Поясните сущность процесса «Управление ИТ-инфраструктурой с точки зрения бизнеса».
6. Поясните сущность процесса «Реализация и развертывание решений».
7. Поясните сущность процесса «Обеспечение ИТ-сервисами».
8. Поясните сущность процесса «Поддержка ИТ-сервисов и решений».
9. Поясните сущность процесса «Управление ИТ-ресурсами и ИТ-инфраструктурой».
10. Что позволяет реализовать ПО Tivoli в плане бизнес-ориентированного управления ИТ_инфраструктурой предприятия?
11. Какие области управления ИТ-инфраструктурой предприятия включают специализированные решения платформы Tivoli?
12. Какие функции операционной поддержки Tivoli позволяют снизить потенциальный уровень затрат, автоматизировать управление и повысить его эффективность?
13. Какие решения IBM Tivoli поддерживают базовые технологии?
14. Поясните основные функции ПП Tivoli Enterprise Data Warehouse.
15. Поясните основные функции ПП Tivoli Management Framework.
16. Поясните основные функции ПП Tivoli Universal Agent.

17. Какие основные решения IBM Tivoli поддерживают технологии для бизнес-ориентированного управления приложениями и системами?
18. Поясните основные функции ПП Tivoli Business Systems Manager.
19. Поясните основные функции ПП Tivoli Change and Configuration Management Database.
20. Поясните основные функции ПП Tivoli Service Level Adviser.
21. Поясните основные функции ПП Tivoli Storage Process Manager.
22. Поясните основные функции ПП Tivoli Unified Process Composer.
23. Какие решения IBM Tivoli предназначены для управления и оптимизации ИТ-инфраструктуры малых предприятий?
24. Поясните основные функции ПП Tivoli Identity Express.
25. Поясните основные функции ПП Tivoli Monitoring (ITM) Express.

4.4 Литература

1. IBM Tivoli: www.ibm.com/software/tivoli.
2. Программное обеспечение IBM Tivoli: www.tivoli.computel.ru/products/.

5 ПОДХОД MICROSOFT К ПОСТРОЕНИЮ УПРАВЛЯЕМЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

5.1 Методологическая основа построения управляемых ИС

Информационная инфраструктура современного предприятия характеризуется большим количеством настольных и переносных компьютеров, серверов, систем хранения данных, телекоммуникационных устройств, операционных систем и бизнес-приложений. В этих условиях задача обеспечения требуемого уровня предоставления ИТ-сервисов со стороны ИТ-службы для бизнес-подразделений является достаточно сложной. При общей тенденции бизнеса к сокращению непроизводственных издержек снижение совокупной стоимости владения ИТ-инфраструктурой предприятия является крайне актуальным.

Построение эффективной системы управления ИТ-инфраструктурой предприятия может быть реализовано с использованием стандартизированного набора программно-аппаратных средств, удовлетворяющих требованиям ИТ-инфраструктуры и бизнеса. Эффективная архитектура управления ИТ-инфраструктурой предприятия должна быть масштабируемой, гибкой, обеспечивать мониторинг и формирование отчетов о различных аспектах функционирования информационной системы.

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) [1].

Методологической основой построения и сопровождения управляемых ИТ-систем является библиотека MOF [2]. 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.

5.2 Инструментарий управления ИТ-инфраструктурой

Инструментальной основой MSM является семейство продуктов MSC (Microsoft System Center) [3], 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) 2003;
- Microsoft Operations Manager (MOM) 2005;
- System Center Reporting Manager (SCRM) 2006;
- Microsoft System Center Data Protection Manager (DPM) 2006;
- Microsoft System Center Capacity Planner (CCP) 2006.

5.2.1 Microsoft System Management Server 2003

Microsoft System Management Server 2003 обеспечивает централизованное управление изменениями и конфигурациями ИТ-инфраструктуры предприятия, построенной на базе компьютеров семейства операционных систем Windows [4]. SMS 2003 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 2005 обеспечивает средства управления серверной инфраструктурой в масштабах предприятия, что позволяет повысить эффективность ее эксплуатации [5]. MOM 2005 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 2005 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 2005 включает следующие интерфейсы пользователя:

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

Консоль администратора предназначена для индивидуальной настройки MOM 2005, 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. 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 2005. Отчеты можно легко экспортировать в Microsoft Excel, Adobe Acrobat, а также в файлы формата HTML, TIFF, CSV или XML.

Operations Manager 2005 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 2005 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 2005 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 2005 обеспечивает сброс автоматического предупреждения, что позволяет агенту автоматически обновлять базу данных MOM в случае исправления предупреждения без участия оператора.

Operations Manager 2005 позволяет вести детальное наблюдение за отдельными экземплярами информационной инфраструктуры. MOM 2005 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 2005 распознает виртуальный кластерный сервер наряду с физическими серверами. Эта возможность различения серверов в пределах кластера позволяет создателям пакетов управления создавать более детализированные правила.

MOM 2005 поддерживает вложенные группы компьютеров. Логическая группировка компьютеров может быть подвернута дальнейшему разделению для обеспечения контекста управления сходными системами. Например, внутри группы компьютеров SQL Server 2000 могут быть выделены группы компьютеров для ведения платежных ведомостей или выполнения заказов, причем каждая из них будет связана с различными правилами.

Operations Manager 2005 обеспечивает ответы на предупреждения, которые могут быть выполнены агентом до того, как предупреждение будет отключено.

MOM 2005 предусматривает быстрое выяснение причин снижения уровней предоставления ИТ-сервисов за счет реализации концепции пакетов управления Management Pack [6]. Пакеты управления представляют собой механизм консолидации накопленного опыта ИТ-экспертов в отдельно выделенной об-

ласти. 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 2005. 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 2005 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 2005 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 2005 со средствами управления других производителей в MOM 2005 включены Web-службы MOM Connector Framework (MCF). Web-службы MCF обеспечивают:

- поиск и выявление оповещений MOM 2005, 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 2005 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.

5.2.2 System Center Reporting Manager 2006

System Center Reporting Manager 2006 обеспечивает объединение информации, формируемой Microsoft System Management Server 2003 и Microsoft Operations Manager 2005 [7]. При этом от SMS 2003 поступает информация о конфигурации и изменениях в ИТ-инфраструктуре предприятия, а от MOM 2005 - информация о событиях и производительности. SCRM 2006 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 2006 предоставляет простые в построении и информативные отчеты о функционировании ИТ-инфраструктуры предприятия.

5.2.3 Microsoft System Center Data Protection Manager 2006

Microsoft System Center Data Protection Manager предназначен для резервного копирования на диски и восстановления данных [8]. 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.

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.

5.2.4 Microsoft System Center Capacity Planner 2006

Microsoft System Center Capacity Planner 2006 предназначен для планирования развертывания систем посредством функционирования ИТ-инфраструктуры предприятия [9].

CCP 2006 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 CCP 2006 позволяет проводить корректное планирование допустимых уровней обслуживания ИТ-сервисов, обосновывать требуемые ИТ-службе ресурсы для поддержания требуемых параметров ИТ-сервисов.

В этой теме были рассмотрены набор инструментов, моделей, методик и рекомендаций Microsoft для решения задач управления ИТ-инфраструктурой предприятия, которые призваны обеспечить построение управляемых ИС высокой надежности, доступности и защищенности.

5.3 Темы рефератов

1. Поясните область применения набора инструментов, моделей, методик и рекомендаций Microsoft Solutions for Management.
2. Что описывают акселераторы решений SA (Solution Accelerator)?
3. Какие задачи решает семейство продуктов Microsoft System Center?
4. Какие программные решения входят в Microsoft System Center?
5. Поясните назначение MS System Management Server 2003.
6. Поясните назначение MS Operation Manager 2005.
7. Поясните назначение MS System Center Reporting Manager 2006.
8. Поясните назначение MS System Center Data Protection Manager 2006.
9. Поясните назначение MS System Center Capacity Planner 2006.
10. Поясните основные возможности MS System Management Server 2003.
11. Какие интерфейсы пользователя включает MS Operation Manager 2005.
12. Поясните назначение консоли администратора Operation Manager 2005.
13. Поясните назначение консоли оператора MS Operation Manager 2005.
14. Поясните назначение веб-консоли MS Operation Manager 2005.
15. Поясните назначение консоли отчетов MS Operation Manager 2005.
16. Для чего предназначены пакеты управления Management Pack?
17. Что содержат пакеты управления Management Pack?
18. Для чего предназначены решения по наблюдению за службами Service Monitoring Solution Accelerator (SMSA)?
19. Какие решения включены в состав SMSA?
20. Для чего предназначены вэб-службы MOM Connector Framework?
21. Что обеспечивают веб-службы MCF?
22. Что позволяют выявить отчеты System Center Reporting Manager 2006?
23. При каких условиях целесообразно применять MS System Center Data Protection Manager 2006?
24. Назовите основные достоинства MS System Center Data Protection Manager 2006.
25. Приведите наиболее распространенные сценарии восстановления данных с помощью MS System Center Data Protection Manager 2006.

5.4 Литература

1. "Карманный справочник" по Microsoft Operations Framework (MOF) на русском языке: www.akmeev.ru/node/39.
2. Microsoft Operations Framework: www.technet.microsoft.com/en-us/solutionaccelerators/dd320379.aspx.
3. Обзор MS System Center 2012: www.social.technet.microsoft.com/Search/en-US?query=system%20center%202012&ac=3.

6 ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ИТ-ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

6.1 Уровни зрелости ИТ-инфраструктуры предприятия

Сервисный подход к управления ИС-службой требует определенной зрелости как для самой ИС-службы, так и для бизнес-заказчиков.

Уровень зрелости бизнес-процессов предприятия можно оценить на основе модели зрелости процесса разработки ПО (Capability Maturity Model — CMM) Института программной инженерии при американском университете Карнеги-Меллон (Software Engineering Institute, SEI) [1], которая была разработана в 1991г. С течением времени было выпущено целое семейство моделей: SW-CMM — для программных продуктов, SE-CMM — для системной инженерии, Acquisition CMM — для закупок, People CMM — для управления людскими ресурсами, ICMM —для интеграции продуктов. В 2002 году SEI опубликовал новую модель CMMI (Capability Maturity Model Integration), объединяющую ранее выпущенные модели и учитывающую требования международных стандартов.

Базовым понятием модели CMM/CMMI считается зрелость компании. Незрелой называют компанию, где процесс конструирования ПО и принимаемые решения зависят только от таланта конкретных разработчиков. Результатом является высокий риск превышения бюджета или срыва сроков окончания проекта.

В зрелой компании работают ясные процедуры управления проектами и построения программных продуктов. По мере необходимости эти процедуры уточняются и развиваются. Оценки длительности и затрат разработки точны, основываются на накопленном опыте. Кроме того, в компании имеются и действуют корпоративные стандарты на процессы взаимодействия с заказчиком, процессы анализа, проектирования, программирования, тестирования и внедре-

ния программных продуктов. Все это создает среду, обеспечивающую качественную разработку программного обеспечения.

В модели CMM/CMMI определены пять уровней зрелости предприятий:

- начальный;
- повторяемый;
- определенный;
- управляемый;
- оптимизирующий.

Начальный уровень (уровень 1) означает, что процесс на предприятии не формализован, отсутствует четкое планирование и контроль. Результаты деятельности предприятия во многом случайны. и сильно зависят от личных качеств отдельных сотрудников.

Повторяемый уровень (уровень 2) предполагает внедрение формальных процедур для выполнения основных элементов процесса разработки ПО. Результаты выполнения процесса соответствуют заданным требованиям и стандартам. Основное отличие от уровня 1 состоит в том, что выполнение процесса планируется и контролируется. Применяемые средства планирования и управления дают возможность повторения ранее достигнутых успехов.

Определенный уровень (уровень 3) требует, чтобы все элементы процесса были определены, стандартизованы и задокументированы. Основное отличие от уровня 2 заключается в том, что элементы процесса уровня 3 планируются и управляются на основе единого стандарта предприятия. Качество разрабатываемого ПО уже не зависит от способностей отдельных личностей.

Управляемый уровень (уровень 4) на предприятии принимаются количественные показатели качества как программных продуктов, так и процесса. Это обеспечивает более точное планирование проекта и контроль качества его результатов. Основное отличие от уровня 3 состоит в более объективной, количественной оценке продукта и процесса.

Оптимизирующий уровень (уровень 5) подразумевает, что главной задачей компании становится постоянное улучшение и повышение эффективности

существующих процессов, ввод новых технологий. Основное отличие от уровня 4 заключается в том, что технология создания и сопровождения программных продуктов планомерно и последовательно совершенствуется.

Каждый уровень CMM характеризуется областью ключевых процессов (ОКП), причем считается, что каждый последующий уровень включает в себя все характеристики предыдущих уровней.

По аналогии с понятием «уровень зрелости предприятия» используется понятие «уровень зрелости ИТ-инфраструктуры». Компания Gartner предлагает для оценки зрелости ИТ-службы использовать пять уровней [2]:

- хаотичный;
- реактивный;
- проактивный;
- сервис;
- польза.

Хаотичный уровень характеризуется множественными службами поддержки, неразвитой службой эксплуатации.

При *реактивном* уровне зрелости проводится отслеживание событий, имеется единая консоль и служба поддержки, осуществляется управление топологией сети, выполняется резервное копирование и инвентаризация;

Проактивный уровень предусматривает управление производительностью, изменениями, проблемами, конфигурациями, доступностью. При этом должна обеспечиваться автоматизация управления ИС-службой и планирование заданий;

Уровень зрелости *сервис* обеспечивает планирование нагрузок и емкостей, управление уровнями обслуживания;

Уровень зрелости ИТ-службы *польза* предполагает обеспечение качества предоставления ИТ-сервисов посредством использования бизнес-метрик.

Эффективность информационных систем и их ИС-служб может по разному оцениваться для различных предприятий. Данное обстоятельство влияет на подходы к повышению эффективности деятельности ИС-служб. Компания

IBM сформировала четыре профиля предприятий для оптимизации ИТ-инфраструктуры [3]:

- commodity (товар);
- utility (ресурс**);**
- partner (партнер**);**
- enabler (поддержка**).**

В профиле *commodity* предприятие рассматривает ИТ-сервисы как свои основные инвестиции для автоматизации фундаментальных административных функций с минимальными расходами. При оптимизации ИТ-инфраструктуры в организациях с таким профилем основное внимание уделяется сокращению расходов.

Для профиля *utility* компании, изначально сфокусированные на расходах, но признающие важность построения отношений с клиентами. Для этих предприятий оптимизация ИТ-инфраструктуры служит средством исполнения соглашений об уровне сервиса, сокращения времени реагирования, готовности и других параметров, связанных с обслуживанием клиентов.

Профиль *partner* предполагает рассмотрение ИТ-инфраструктуры предприятия с точки зрения влияния на бизнес. Хотя сокращение расходов всегда актуально, основное внимание уделяется получению экономического эффекта от инвестиций в информационные технологии. В этих ситуациях бизнес-подразделения вместе с ИТ-службой работают над улучшением общего качества ИТ-сервиса и достижением конечных целей деятельности предприятия.

В компаниях данного профиля *enabler* ИТ-инфраструктура служит важным элементом стратегии развития бизнеса. ИТ-инициативы в них выступают основной движущей силой развития бизнеса и рассматриваются как необходимое условие конкурентоспособности.

В методологии компании Microsoft по оптимизации ИТ-инфраструктуры выделяют уровни зрелости ИТ-инфраструктуры предприятий. Модель зрелости ИТ-инфраструктуры, разработанная Microsoft, включает четыре уровня [4]:

- базовый;
- стандартизированный;
- рационализированный;
- динамический.

Базовый уровень зрелости ИТ-инфраструктуры характеризуется наличием большого количества процессов, выполняемых вручную, минимальной централизацией управления, отсутствием стандартов и политик безопасности, резервного копирования, управления образами систем. Руководство предприятия и ИС-службы слабо ориентируется в возможностях существующей ИТ-инфраструктуре и её потенциальных возможностях по повышению эффективности бизнеса. При этом расходы на управление ИТ-инфраструктурой высоки,. так же высоки риски обеспечения качества предоставления ИТ-сервисов.

Предприятия с базовым уровнем зрелости ИТ-инфраструктуры могут повысить эффективность бизнеса при переходе на стандартизированный уровень, за счет уменьшения расходов путем реализации следующих направлений:

- разработки стандартов и политик, а также стратегии их применения;
- снижения рисков, связанных с безопасностью, за счет создания эшелонированной обороны;
- автоматизации многих ручных и длительно выполняемых операций;
- внедрения передового опыта.

Стандартизированный уровень зрелости ИТ-инфраструктуры предполагает введение точек управления на базе стандартов и политик администрирования настольных компьютеров и серверов, определение правил подключения машин к сети, управление ресурсами на основе Active Directory, формирование политик безопасности и управления доступом. Предприятия с ИТ-инфраструктурой данного уровня зрелости достаточно эффективно могут управлять инцидентами, но упреждающие действия по разрешению проблем ещё не проводятся. Процессы управления изменениями разрешаются частично

и осуществляется первоначальное формирование базы данных позиций конфигурации.

Повышение эффективности управления ИС службой предприятия возможно путем расширения уровня контроля над инфраструктурой, а также политикой безопасности для упреждающего реагирования на различные ситуации — от изменения рыночной конъюнктуры до стихийных бедствий.

На *рационализированном уровне* зрелости ИТ-инфраструктуры предприятия затраты на управление настольными компьютерами, серверами и коммутационным оборудованием сетей сводятся к минимуму, а процессы поддержки и предоставления ИТ-сервисов начинают играть важную роль в поддержке и расширении бизнеса. При обеспечении информационной безопасности основное внимание уделяется профилактическим мерам, и на любые угрозы безопасности предприятие реагирует быстро и предсказуемо.

На предприятии применяется полностью автоматизированное развертывание, с минимальным участием операторов. Количество образов программных систем (images) минимально, и процесс управления настольными компьютерами минимизирован. ИС-служба поддерживает базу данных позиций конфигурации в исчерпывающей информацией.

Динамический уровень зрелости ИТ-инфраструктуры предприятия предполагает понимание стратегической ценности для эффективного ведения бизнеса и получения конкурентных преимуществ. Данный уровень предполагает, что все расходы ИС-службы прозрачны и находятся полным контролем, пользователям доступны необходимые в их работе данные, организована эффективная совместная работа на уровне как сотрудников, так и отделов, а мобильные пользователи получают практически тот же уровень обслуживания, что и в офисах.

Процессы поддержки и предоставления ИТ-сервисов автоматизированы. Это реализуется с помощью специализированных и встроенных в систему программных средств, что позволяет управлять информационными системами в соответствии с изменяющимися требованиями бизнеса. Инвестиции в инфор-

мационные технологии дают быструю и заранее просчитываемую отдачу для бизнеса.

Для данного уровня зрелости ИТ-инфраструктуры предприятия характерно эффективное управление процессами поддержки и предоставления ИТ-сервисов и постоянная оптимизация уровней поддержки сервисов.

Предприятия с динамическим уровнем зрелости ИТ-инфраструктуры имеют возможность внедрять новые ИТ-технологии, необходимых для поступательного развития бизнеса, выигрыш от которых значительно перевешивает дополнительные расходы.

6.2 Методология Microsoft по эксплуатации ИС

Библиотека передового опыта организации управления ИТ-инфраструктурой предприятия представляет общие рекомендации и различные организации вносят свой вклад в развитие этого направления. Microsoft на основе обобщения документации ITIL, стандарта ISO 15504, описывающего критерии оценки зрелости процессов, опыта заказчиков и партнеров Microsoft, опыта организации эксплуатации во внутренних ИТ-подразделениях Microsoft разработала библиотеку документов Microsoft Operations Framework (MOF) [5].

В состав MOF входят следующие документы и руководства

- модель процессов эксплуатации (MOF Process Model for Operations);
- модель групп эксплуатации (MOF Team Model for Operations);
- дисциплина управления рисками эксплуатации (Risk Management Discipline for Operations);
- функции управления услугами (SMF – Service Management Functions).

Модель процессов эксплуатации и *функции управления услугами* описывают высокоуровневые операции, выполняемые при эксплуатации информационных систем, и основываются на четырех принципах:

- структуризация;

– быстрый цикл развития, итеративный подход;

– управление посредством периодических контрольных мероприятий;

– интегрированное управление рисками.

Принцип *структуризации* упрощает интеграцию процессов, управление жизненным циклом информационной системы и сопоставление ролей с выполняемыми функциями.

Принцип *быстрого цикла развития* способствует повышению качества работы информационной системы предприятия посредством эффективного проведения изменений при всесторонней оценке рисков.

Принцип *контрольных мероприятий* обеспечивает регулярную оценку оперативной деятельности по эксплуатации ИТ-инфраструктуры и предоставлению ИТ-сервисов, а также результативности и эффективности действий по внесению изменений в информационную систему.

Принцип *интегрированного управления рисками* предполагает распространение процедур управления рисками во все операционные процессы и роли, а также формирование упреждающей политики управления рисками.

Модель процессов MOF сформирована из четырех категорий-квадрантов [5], в которых объединены ключевые задачи эксплуатации информационных систем (рис. 6.1).

В модели выделены следующие квадранты:

– изменения;

– эксплуатация;

– поддержка;

– оптимизация.

Квадрант «Изменения» (MOF Changing Quadrant) предназначен для формализации и упорядочивания процессов изменения ИТ-инфраструктуры и ИТ-сервисов. В нем описаны следующие процессы:

– управление изменениями;

– управление релизами;

– управление конфигурациями.

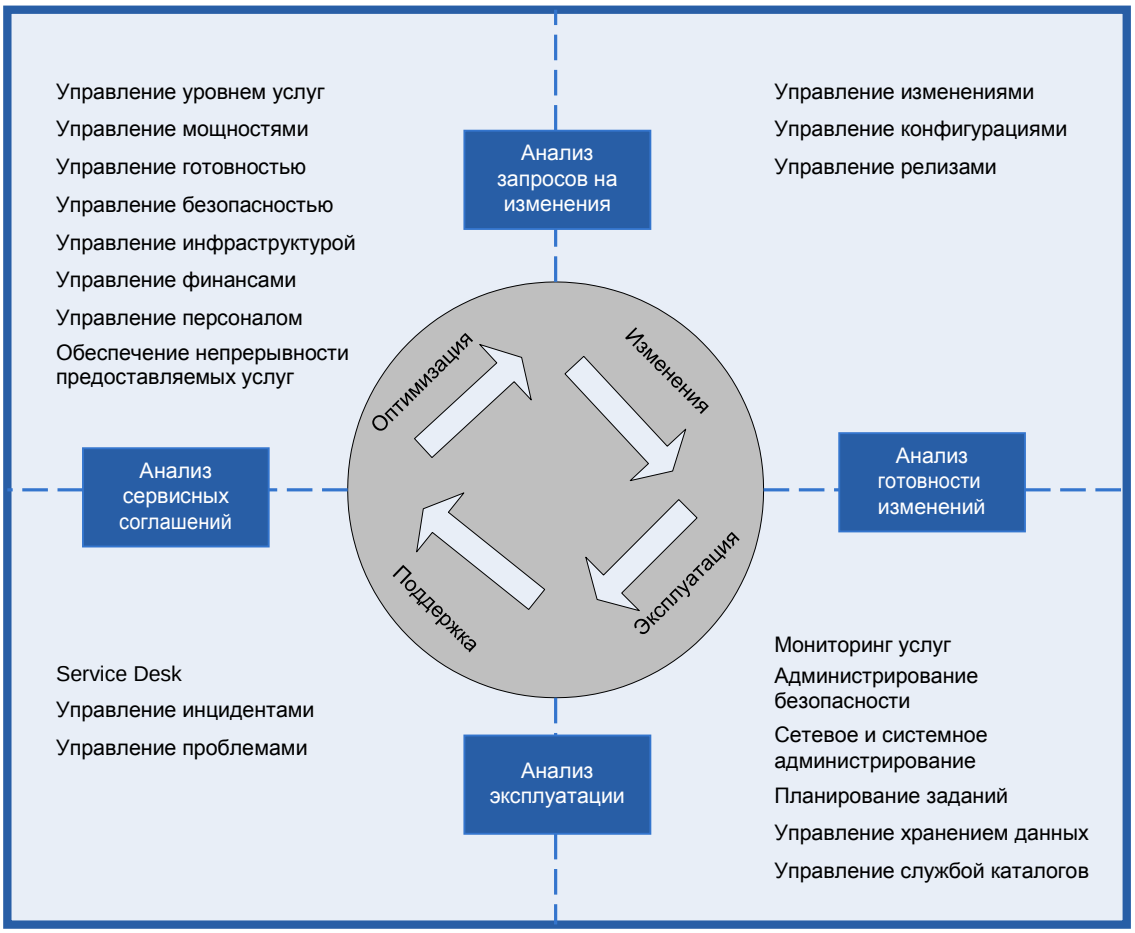

Рисунок 6.1. Модель процессов MOF

Функциональность квадранта «Изменения» в отличие от аналогичных процессов ITIL отличается более детальной проработкой диаграмм процессов и инструкций по их применению.

Квадрант «Эксплуатация» (MOF Operating Quadrant) описывает процессы технической инфраструктуры информационной системы (рис.6.2).

Для квадранта «Эксплуатация » выделены два уровня процессов. На верхнем уровне находятся следующие процессы:

– системное администрирование;

– администрирование безопасности;

– мониторинг ИТ-сервисов.

Данные процессы описывают принципы организации процессов эксплуатации технических и программных систем.

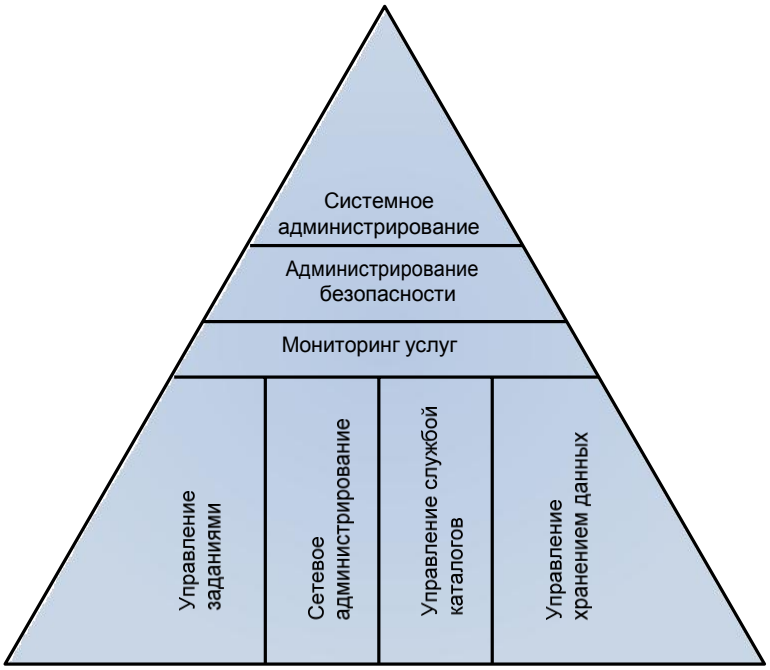

Рисунок 6.2. Квадрант «Эксплуатация»

На втором уровне находятся следующие процессы:

- управление заданиями;
- сетевое администрирование;
- управление службой каталога;
- управление хранением данных.

Эти процессы описывают процессы эксплуатации конкретных подсистем.

Следует отметить, что процессы квадранта «Эксплуатация» ориентированы на использование продуктов Microsoft.

Квадрант «Поддержка» (MOF Supporting Quadrant) описывает процессы поддержки пользователей и ИС-службы. В нем описаны следующие процессы:

- Service Desk;
- управление инцидентами;
- управление проблемами.

Документация по процессам данного квадранта в целом соответствует содержанию аналогичных процессов ITIL, но в некоторых случаях детализируются диаграммы процессов и рекомендации по их применению.

Квадрант «Оптимизация» (MOF Optimizing Quadrant) описывает процессы предоставления ИТ-сервисов и оптимизации их предоставления. В данном квадранте описаны следующие процессы:

- управление уровнем предоставления ИТ-сервисов;
- финансовый ИТ-менеджмент;
- управление мощностями;
- управление готовностью;
- управление непрерывностью предоставления ИТ-сервисов;
- управление персоналом ИТ-подразделений;
- управление безопасностью;
- оптимизация ИТ-инфраструктуры.

Если первые пять процессов, в основном, соответствуют с небольшими дополнениями процессам ITIL, то процесс «Управление персоналом» базируется на опыте Microsoft по управлению персоналом, мотивации, обучения и удержания квалифицированных кадров. Содержание процессов «Управление безопасностью» и «Оптимизация ИТ-инфраструктуры» содержат описание передового опыта обеспечения безопасности и оптимизации ИТ-инфраструктуры.

*Модель групп эксплуатаци*и формализует и описывает распределение ролей между участниками процесса эксплуатации ИС и обеспечение взаимодействия с внешними и внутренними группами проектирования. В модели групп MOF описаны следующие роли:

- группа управления изменениями в ИТ-среде;
- группа управления физической инфраструктурой и инструментами управления инфраструктурой (операциями);
- группа поддержки;
- группа управления портфелем ИТ-сервисов;
- группа управления ИТ-инфраструктурой;
- группа безопасности;

– группа взаимодействия с поставщиками услуг и продуктов (партнеры).

Как правило роли распределяют между подразделениями ИТ-службы предприятия, но иногда они назначаются бизнес-подразделениям, внешним консультантам и партнерам.

Для малых предприятий в рамках организационной структуры ИТ-службы возможны совмещения некоторых ролей сотрудниками. Рекомендации по совмещению ролей приведены в табл. 6.1 [7]. Ячейки таблицы помечены символами, имеющими следующий смысл: Д – допустимо совмещение ролей; Н/Д – не допустимо совмещение ролей; Н/Р – не рекомендуется совмещение ролей.

Таблица 6.1. Возможности совмещения ролей участниками процесса эксплуатации ИС

	Безопасность	Управление изменениями	Управление инфраструктурой	Поддержка	Партнеры	Управление операциями	Управление ИТ-сервисами
Безопасность		Н/Р	Д	Н/Д	Н/Р	Д	Н/Р
Управление изменениями	Н/Р		Д	Н/Д	Д	Д	Н/Р
Управление инфраструктурой	Д	Д		Д	Д	Д	Н/Р
Поддержка	Н/Д	Н/Д	Д		Д	Д	Д
Партнеры	Н/Р	Д	Д	Д		Д	Н/Р
Управление операциями	Д	Д	Д	Д	Д		Д
Управление ИТ-сервисами	Н/Д	Н/Д	Н/Д	Д	Н/Р	Д	

Дисциплина управления рисками эксплуатации описывает процессы выявления риска и принятия решений по устранению риска. При этом риском считается возможность нарушения предоставления ИТ-сервиса, а управление рис-

ками – это регулярная деятельность, обеспечивающая актуальность мер по минимизации выявленных рисков или предупреждению в каждый момент выполнения операций по эксплуатации.

В дисциплине определены следующие этапы управления рисками:

- выявление;
- анализ и определение приоритетов;
- планирование;
- мониторинг и отчетность;
- управление;
- обучение.

На этапе «Выявление» идентифицируют существующие риски и фиксируют их как можно раньше.

Этап анализа и определения приоритетов определяют потенциальные угрозы от рисков и устанавливают приоритеты с целью выделения ограниченных ресурсов на снижение наиболее существенных рисков.

Этап «Планирование» предполагает разработку плана действий для снижения влияния рисков на эксплуатацию ИС и внесение изменений в другие процессы управления ИТ-инфраструктурой с целью снижения уровня рисков.

Этап «Мониторинг и отчетность» состоит в отслеживании статуса конкретных рисков, исполнении соответствующих им планов, подготовки отчетов для персонала и руководства о статусе наиболее опасных рисков и планов действий по управлению ими.

Этап управления рисками предполагает исполнение плана действий по конкретным рискам и формирование соответствующей отчетности.

На этапе «Обучение» осуществляется накопление и применение опыта управления рисками.

В данной теме были рассмотрены модели уровней зрелости бизнес-процессов предприятия Capability Maturity Model, уровни зрелости ИТ-инфраструктуры, предложенные компанией Gartner, профили предприятий для

оптимизации ИТ-инфраструктуры, разработанные компанией ИБМ, уровни зрелости ИТ-инфраструктуры предприятий, определенные в методологии компании Microsoft, а также библиотеку документов Microsoft Operations Framework, ориентированную на оптимизацию процессов эксплуатации ИС.

6.3 Темы рефератов

1. Какие уроки зрелости предприятий определены в модели CMM/CMMI?
2. Как характеризуется начальный уровень зрелости предприятия по модели CMM/CMMI?
3. Как характеризуется повторяемый уровень зрелости предприятия по модели CMM/CMMI?
4. Как характеризуется определенный уровень зрелости предприятия по модели CMM/CMMI?
5. Как характеризуется управляемый уровень зрелости предприятия по модели CMM/CMMI?
6. Как характеризуется оптимизирующий уровень зрелости предприятия по модели CMM/CMMI?
7. Какие уровни зрелости ИТ-инфраструктуры предприятия предложены компанией Gartner?
8. Какие профили предприятий для оптимизации ИТ-инфраструктуры определены компанией ИБМ?
9. Как характеризуется профиль commodity в модели IBM?
10. Как характеризуется профиль utility в модели IBM?
11. Как характеризуется профиль partner в модели IBM?
12. Как характеризуется профиль enabler в модели IBM?
13. Какие уровни зрелости ИТ-инфраструктуры предприятия предложены компанией Microsoft?
14. Как характеризуется базовый уровень зрелости ИТ-инфраструктуры компании Microsoft?
15. Как характеризуется стандартизированный уровень зрелости ИТ-инфраструктуры компании Microsoft?
16. Как характеризуется рационализированный уровень зрелости ИТ-инфраструктуры компании Microsoft?
17. Как характеризуется динамический уровень зрелости ИТ-инфраструктуры компании Microsoft?
18. Какие документы и руководства входят в состав библиотеки документов Microsoft Operations Framework (MOF)?
19. На каких принципах основывается модель процессов эксплуатации и функции управления услугами MOF?
20. Какие категории квадрантов входят в модель процессов MOF?
21. Какие процессы описаны в квадранте «Изменения» модели MOF?
22. Какие роли участников процесса эксплуатации ИС определены в модели групп эксплуатации MOF?

6.4 Литература

1. К. Мильман, С. Мильман. CMMI – шаг в будущее: www.osp.ru/os/2005/05-06/185610/.
2. Уровни зрелости ИТ-инфраструктуры предприятия: www.iteam.ru/publications/it/section_91/article_3182/.
3. Решения Microsoft для повышения эффективности ИТ-инфраструктуры Microsoft/Русская редакция, М., 2005.

7 ТЕХНОЛОГИЯ MICROSOFT ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Процесс обеспечения безопасности относится к оперативным процессам и соответствии с библиотекой ITIL [1] и входит в блок процессов поддержки ИТ-сервисов. Нарушение безопасности информационной системы предприятия может привести к ряду негативных последствий, влияющих на уровень предоставления ИТ-сервисов:

- снижение уровня доступности вследствие отсутствия доступа или низкой скорости доступа к данным, приложениям или службам;
- полная или частичная потеря данных;
- несанкционированная модификация данных;
- получение доступа посторонних пользователей к конфиденциальной информации.

Анализ причин нарушения информационной безопасности показывает, что основными являются следующие:

- ошибки конфигурирования программных и аппаратных средств ИС;
- случайные или умышленные действия конечных пользователей и сотрудников ИТ-службы;
- сбои в работе программного и аппаратного обеспечения ИС;
- злоумышленные действия посторонних по отношению к информационной системе лиц.

Компания Microsoft разрабатывает стратегию построения защищенных информационных систем (Trustworthy Computing) — 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 состав и технологий и продуктов средств 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* для укрепления доверия клиентов, партнеров, государственных учреждений.

Данные принципы реализуются в программных продуктах Microsoft. Компания Microsoft предлагает обеспечивать безопасность операционных систем семейства Windows с помощью технологии единого каталога (Active Directory) и групповых политик. Использование групповой политики и Active Directory позволяет централизовано управлять параметрами безопасности как для одного пользователя или компьютера, так и для группы пользователей, управлять безопасностью серверов и рабочих станций.

Для решения вопросов обеспечения информационной безопасности компания Microsoft предоставляет следующие технологии [3]:

- 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.

7.1 Групповые политики

Управление групповыми политиками в Microsoft Windows Server 2003 позволяет администраторам задавать конфигурацию операционных систем серверов и клиентских компьютеров [4]. Реализуется эта функциональность с помощью оснастки «Редактор объектов групповой политики», общий вид которой приведен на рис. 7.1

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).

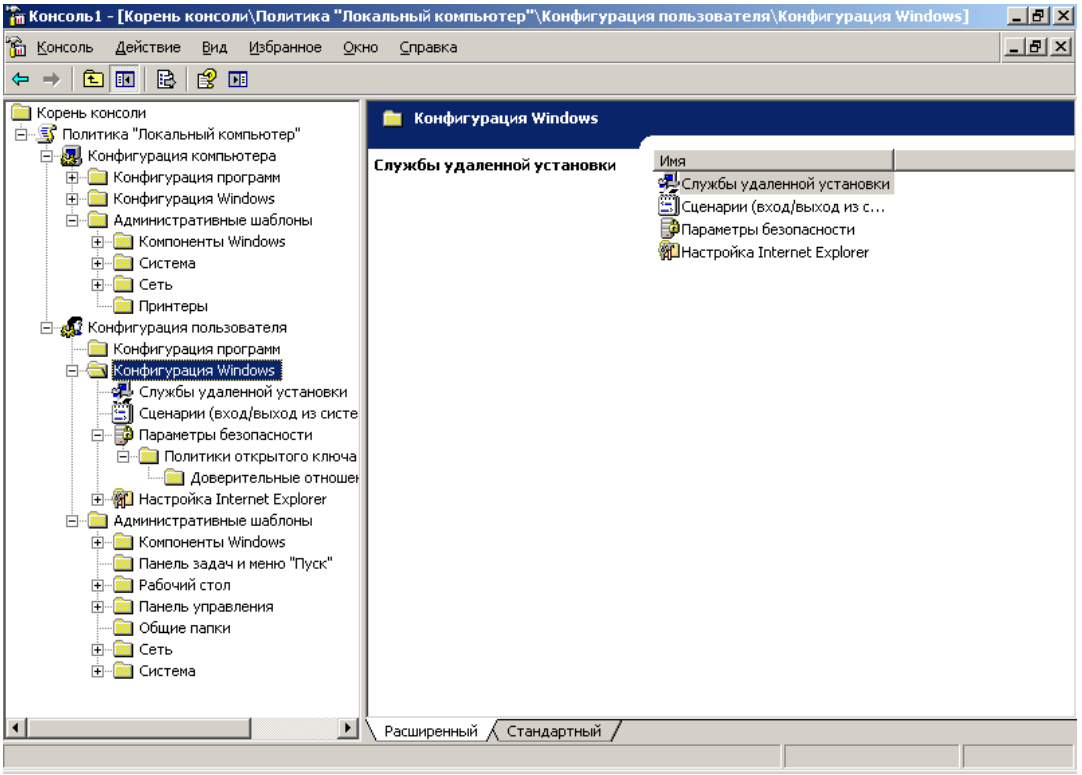

Рисунок 7.1. Оснастка «Редактор объектов групповой политики»

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 управляемую ИТ-инфраструктуру информационной системы. 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, сформированных 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 (например администратор может удалить из главного меню значок «Моя музыка», что представлено на рис. 7.2);
- параметры безопасности. Администраторы могут указывать параметры локальной, доменной и сетевой защиты для компьютеров и пользователей в области действия GPO, используя шаблоны безопасности (рис 7.3);

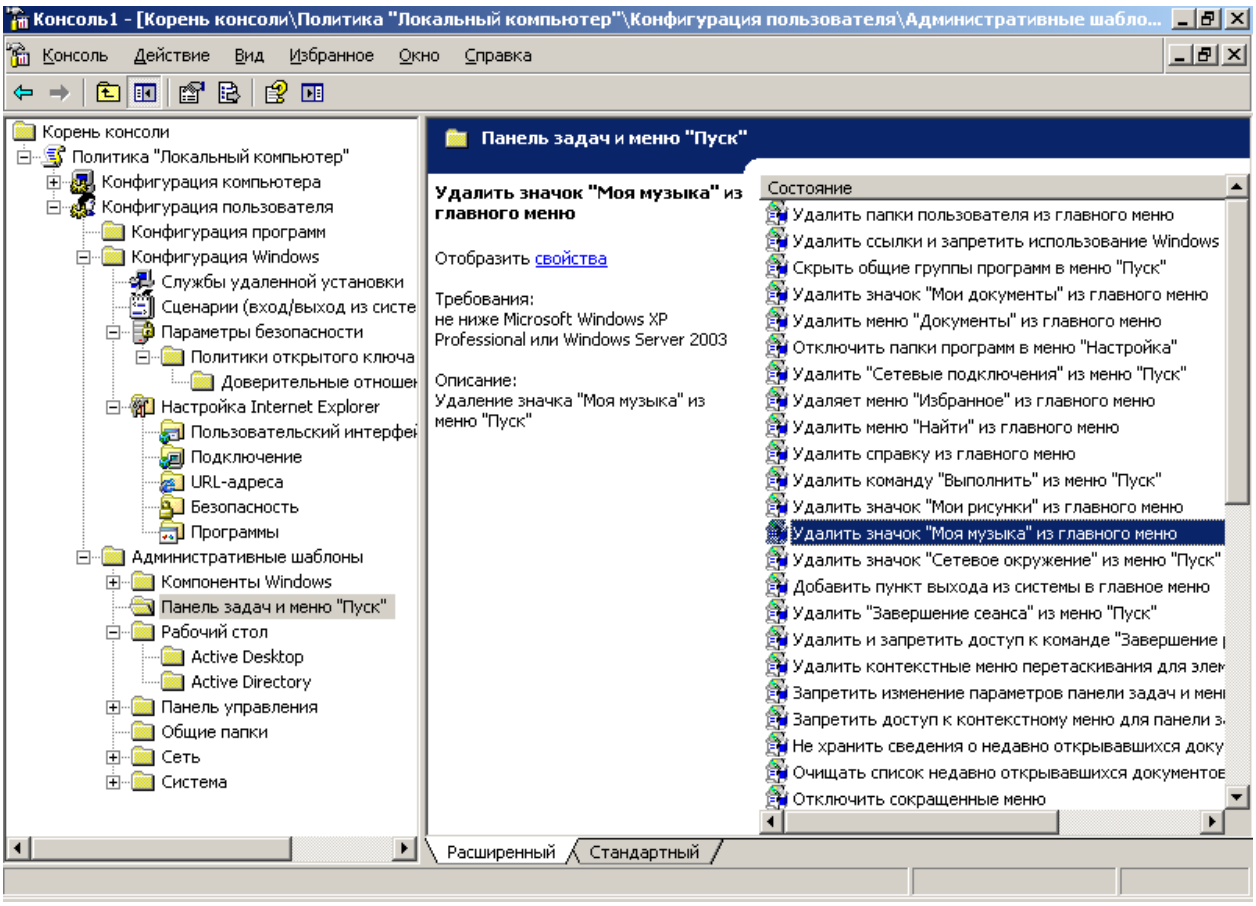

Рисунок 7.2. Удаление значка из главного меню профиля пользователя

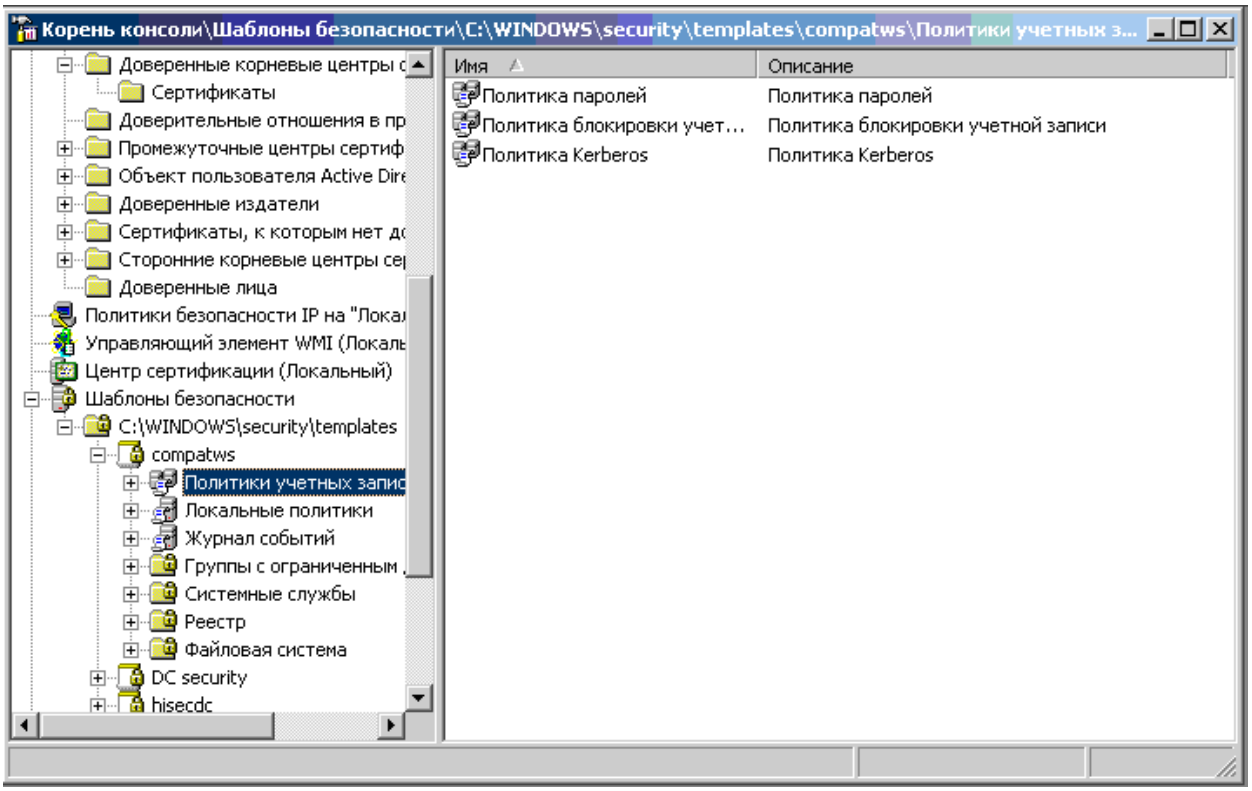

Рисунок 7.3. Оснастка Политика учетных записей шаблонов безопасности

- 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.

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.

7.2 Безопасный доступ в сеть

ИТ-инфраструктура предприятия может включать интрасети, сайты в интернете и экстрасети. Многие компоненты такой 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). В Microsoft Server 2003 политику открытых ключей можно задавить с помощью оснастки MMC - Политика открытого ключа (рис. 7.4)

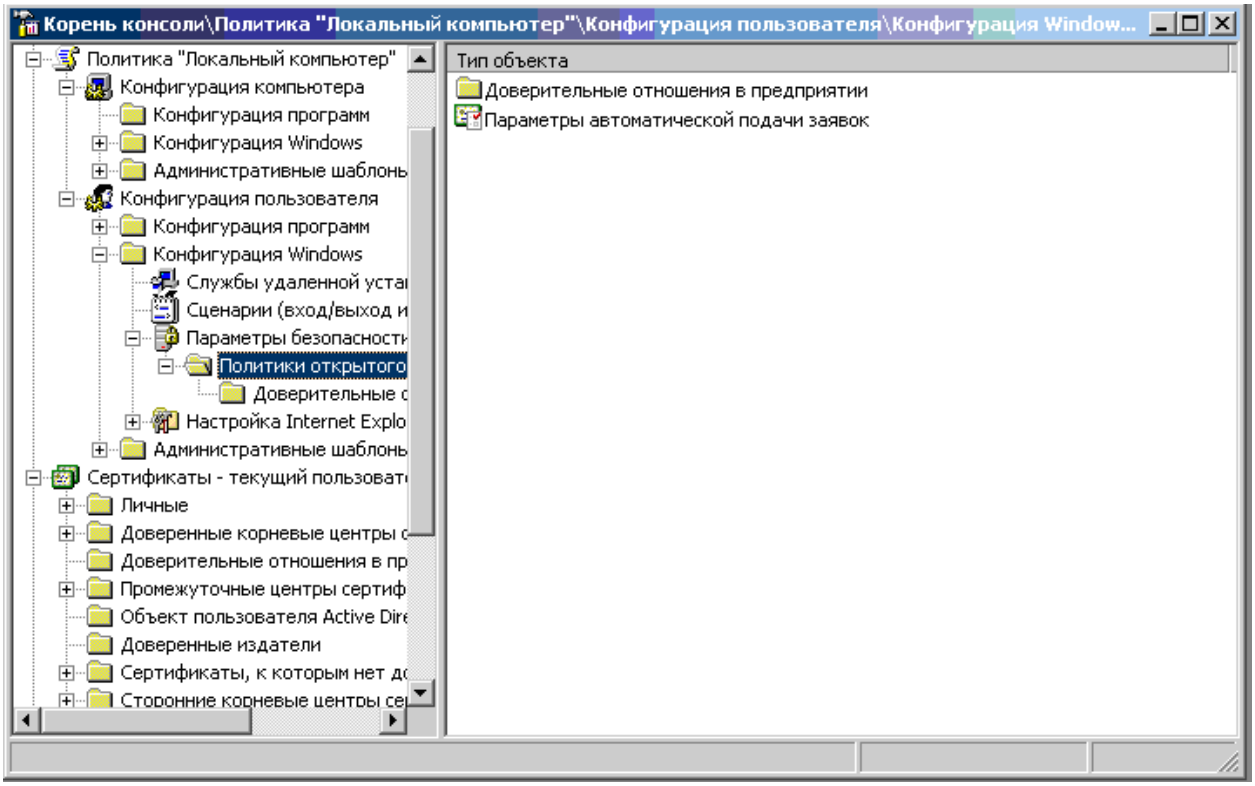

Рисунок 7.4. Оснастка Политика открытого ключа

В Windows Server 2003 центр сертификации предполагает применение электронных цифровых подписей. Службы сертификации (Certification Services) и средства управления сертификатами позволяют построить предприятию собственную инфраструктуру открытых ключей.

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 до-

веряемые 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.

7.3 Аутентификация пользователей

В операционной системе Windows Server 2003 применяются следующие стандартные протоколы аутентификации:

– *интерактивный ввод*, при котором идентификация пользователя проверяется по учетной записи на локальном компьютере или в Active Directory;

– *аутентификация в сети* предполагает идентификацию пользователя любой сетевой службой, к которой обращается пользователь, с использованием протокола Kerberos V5, сертификатов открытых ключей, SSL (Security Sockets Layer) и TLS-кэш (Transport Layer Security);

– единый вход, который дает возможность обращаться к сетевым ресурсам без повторного ввода учетных данных.

В Windows Server 2003 поддерживается аутентификация с применением смарт-карт, что позволяет создавать корпоративные сети с высоким уровнем защищенности. Смарт-карта – это устройство внешне похожее на кредитную карту, на котором хранятся пароли, открытые и закрытые ключи и другие личные данные пользователя.

Для активизации смарт-карты пользователь должен вставить её в устройство чтения, подключенное к компьютеру, и ввести свой PIN-код (персональный идентификационный номер). PIN-код обрабатывается локально и не передается по сети. После нескольких неудачных попыток ввода PIN-кода смарт-карта блокируется.

Ввод PIN-кода обеспечивает аутентификацию только по отношению к смарт-карте, а не к домену. Для аутентификации в домене применяется сертификат открытого ключа, хранящийся на смарт-карте. При запросе на вход сначала происходит обращение к локальной системе безопасности клиентского компьютера. Далее происходит обращение к службе аутентификации домена с использованием сертификата пользователя. Удостоверение сертификата подтверждается цифровой подписью с применением закрытого ключа пользователя.

7.4 Защита 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.

7.5 Защита от вторжений и вредоносного ПО

Защита от вторжений должна обеспечить профилактические меры по защите компьютеров и данных. Эти задачи решает Microsoft ISA (Internet Security and Acceleration) Server 2004. ISA Server 2004 включает межсетевой экран при-

кладного уровня, поддержку виртуальных частных сетей (Virtual Public Netware – VPN), Web-кэширование, фильтры прикладного уровня. ISA Server 2004 защищает 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.

Сервер Microsoft ISA Server 2004 реализует функциональные возможности трехуровневого межсетевого экрана, средства управления частными виртуальными сетями и службы Web-кэширования. ISA Server 2004 позволяет повысить безопасность и производительность корпоративной информационной сети,

а также снизить эксплуатационные расходы. Сервер ISA Server 2004 имеет ряд достоинств:

- *более совершенные средства защиты*, которые реализуют динамическую фильтрацию пактов и каналов. Алгоритм динамической фильтрации избирательно открывает доступ пакетов данных в защищенные области сети. По мер необходимости служба динамической фильтрации открывает порты, а по завершению сеанса связи – закрывает;
- *простота использования* за счет поддержки многоуровневой архитектуры, унификации управления VPN, понятных шаблонов, усовершенствованных средств устранения неполадок, возможности экспорта конфигурации в форматах XML, мониторинга активных соединений в режиме реального времени;
- *быстрое и надежное получение доступа* к виртуальной частной сети за счет встроенной поддержки туннельного режима IPSec для VPN-подключений, быстрое Web-кэширование и высокопроизводительный пакетный фильтр.

Задачи безопасности, а также надежности, масштабируемости, быстродействия при управлении Web-серверами обеспечиваются полнофункциональным Web-сервером Internet Information Services (IIS) 6.0. Службы IIS 6.0 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 6.0 включены разнообразные средства управления для администрирования и конфигурирования ИТ-инфраструктуры предприятия. Системные администраторы могут изменять параметры и отлаживать приложения во время работы служб. Службы IIS 6.0 поддерживают стандарты XML, SOAP и IPv6.

Для защиты от вирусов корпоративных информационных систем Microsoft предлагает технологию Microsoft Antigen, которая позволяет защитить серверы поддержки коммуникаций и коллективной работы. Эти решения серверного уровня предоставляют средства фильтрации файлов и контента, а также позволяют применять несколько механизмов сканирования одновременно. Комплекс антивирусных средств Microsoft Antigen помогают обеспечить антивирусную защиту на уровне серверов с использованием нескольких механизмов сканирования.

Продукты семейства Antigen - это приложения для серверов коллективной работы и передачи сообщений, которые обеспечивают защиту от атак злоумышленников, вирусов и нежелательных сообщений [5].

Использование многоядерной технологии антивирусного сканирования позволяет продуктам Antigen успешно бороться с возникающими угрозами.

Тесная интеграция с Microsoft Exchange Server, Microsoft SharePoint и Microsoft Live Communications Server обеспечивает надежную защиту и централизованное управление всей системой защиты без снижения производительности серверов, на которых установлены продукты Antigen.

Фильтрация содержания и файлов обеспечивает соблюдение единой корпоративной политики по правилам передачи и хранения документов, а также применения допустимой лексики как внутри компании, так и при отправке сообщений поставщикам и клиентам.

Продукты семейства Antigen имеют следующие преимущества:

- *многоуровневая защита*, которая обеспечивает выбор необходимых антивирусных ядер защиты различных модулей и уровней для обеспечения максимальной защиты ИТ-инфраструктуры предприятия;
- *оптимизация сервера*, позволяющая в зависимости от роли сервера, его загрузки и мощности можно выбрать оптимальный вариант защиты – количество ядер, используемых для проверки на различных уровнях;

– *контроль содержания*, что поддерживает формировании единой корпоративной политики по правилам передачи и хранения документов, а также возможность исключить применение недопустимой лексики при передаче сообщений между подразделениями и при отправке сообщений за пределы предприятия.

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

– Windows Defender (бета-версия 2) предназначено для компьютерной защиты. Оно 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.

В табл. 7.1 и 7.2 приведены ресурсы по обеспечению безопасности ИТ-инфраструктуры корпоративных систем.

Таблица 7.1. Русскоязычные ресурсы по обеспечению безопасности

Наименование ресурса	Web-ссылка
Ресурс Microsoft, посвященный безопасности	www.microsoft.com/rus/security
Центр рекомендаций по обеспечению безопасности для пользователей	www.microsoft.com/rus/securityguidance
Рекомендации по обеспечению безопасности для ИТ-специалистов	www.microsoft.com/rus/technet/security
Сайт Security at Home для клиентов	www.microsoft.com/rus/athome/security
Сайт программы Malicious Software Removal Tool	www.microsoft.com/rus/security/malwareremove/default.mspx
Сведения о системах Windows и Linux	www.microsoft.com/rus/getthefacts

Таблица 7.2. Англоязычные ресурсы по обеспечению безопасности

Наименование ресурса	Web-ссылка
Ресурс о безопасности для разработчиков ПО	msdn.microsoft.com/security
Ресурсы по обеспечению безопасности для партнеров	https://partner.microsoft.com/security
Пакет обновления 1 (SP1) для Windows Server 2003	www.microsoft.com/windowsserver2003/downloads/servicepacks/spl
Пакет обновления 1 (SP1) для Windows XP	www.microsoft.com/athome/security/protect/windowsxp/choose.mspx
Microsoft Windows Defender (бета-версия 2)	www.microsoft.com/athome/security/spyware/software
Стратегия Microsoft по борьбе с программами-шпионами	www.microsoft.com/athome/security/spyware/strategy.mspx
Критерии Microsoft для определения программ-шпионов	www.microsoft.com/athome/security/spyware/software/isv
Система Microsoft Antigen	www.microsoft.com/windowsserversystern/solutions/security/sybari.mspx
Обеспечение безопасности всего цикла разработки	msdn.microsoft.com/security/sdl

Продолжение табл. 7.2

Наименование ресурса	Web-ссылка
Исследовательский центр Microsoft Security Response Center	www.microsoft.com/security/msrc
Microsoft Windows OneCare Live (бета-версия)	https://beta.windowsonecare.com
Центр интернет-обслуживания WindowsLive Safety Center (бета-версия)	safety.live.com

7.6 Безопасность мобильных пользователей корпоративных систем

Для обеспечения сотрудников постоянным доступом к ресурсам корпоративной сети в неё включают мобильные устройства. С помощью мобильных устройств сотрудники предприятия могут обращаться к корпоративной информации, своей почте и бизнес-приложениям с любого места, находящегося за межсетевым экраном корпоративной сети. Для поддержки мобильных пользователей необходимо реализовать в системе стандарты безопасности, позволяющие корпоративные сетевые ресурсы и конфиденциальную информацию.

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. Устройства, работающие под управлением Windows Mobile 2003, поддерживают двухэтапную аутентификацию и позволяют применять стойкие пароли, биометрические технологии

и сертификаты. Устройства с Windows Mobile 2003 можно интегрировать в существующую инфраструктуру открытых ключей.

Защиту мобильных устройств, работающих под управлением Windows Mobile 2003, 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 2003 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 Windows Server 2003 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.

Некоторые мобильные устройства, такие как КПК и смартфоны, работающие под управлением Windows Mobile 2003, имеют возможность синхронизации данных. Эти мобильные устройства оптимизированы для синхронизации с серверами Microsoft Exchange. Для синхронизации данных Exchange КПК и смартфоны, управляемые Windows Mobile могут использовать Exchange Server 2003 ActiveSync. На каждом устройстве с Windows Mobile указывают сервер Exchange и задают параметры безопасности. Для соединения с сетью, в которой работает Exchange Server 2003 ActiveSync, мобильное устройство должно иметь

информацию по учетной записи пользователя и имени доступных серверов. Это позволяет создать шифруемый канал коммуникационной связи между мобильным пользователем и корпоративной сетью.

7.7 Службы терминалов

Сервер терминалов (Terminal Server) операционной системы Windows Server 2003 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. Различие между SSL 3.0 и TLS 1.0 незначительные, поэтому далее в тексте термин «SSL» будет относиться к ним обоим. 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.

7.8 Защита данных

Для защиты данных применяются технологии кластеризации, теневого копирования, а также службы управления правами и Data Protection Manager [6].

Кластер определяет группу компьютеров, которые совместно выполняют одинаковый набор приложений и которые представляются клиентам и приложениям как единая система. Компьютеры объединяются в кластер с помощью программных соединений и используют средства автоматического восстановления после сбоев и балансировки сетевой нагрузки.

Windows Server 2003 имеет две службы кластеризации:

- *служба кластеров* (Cluster Service, MSCS), которая 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;
- 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.

Посредством теневых копий файловый сервер под управлением Windows Server 2003 может эффективно поддерживать на выбранных томах предыдущие версии всех файлов. Пользователь имеет возможность просматривать предыдущие версии файла.

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,
- Восстановления файлов ИТ-службой,
- Восстановление файлов самими пользователями.

В заключение следует отметить, что компания Microsoft разработала программное средство для оценки системы безопасности Security Assessment Tool (MSAT). Этот инструментарий позволяет собирать данные о системе безопасности ИТ-инфраструктуры предприятия и получать рекомендации по ее усовершенствованию.

В этой теме была рассмотрена стратегия, технология и решения компании Microsoft по построению защищенных ИС.

7.9 Темы рефератов

1. К каким негативным последствиям, влияющим на уровень прелоставления ИТ-сервисов, могут привести нарушения безопасности ИС предприятия?
2. Назовите основные причины нарушения информационной безопасности для предприятия.
3. Какие технологии предоставляет Microsoft для решения вопросов обеспечения информационной безопасности?
4. Что позволяют обеспечить групповые политики и Active Directory в плане информационной безопасности предприятия?
5. С учетом каких правил необходимо применять групповые политики и Active Directory для сайтов, доменов и организационных единиц?
6. Какие возможности механизма групповой политики используются при администрировании ИТ-инфраструктуры предприятия при настройке приложений, операционных систем, безопасности рабочей среды пользователей и ИС в целом?
7. Для чего используются WMI-фильтры?
8. Какие преимущества дает применение групповой политики в ИС предприятия?
9. Поясните назначение инфраструктуры открытых ключей PKI.
10. Какие преимущества для ИС предприятия дает применение инфраструктуры открытых ключей?
11. Какие стандартныен протоколы аутентификации применяются в ОС Windows Server 2003?
12. Поясните назначение смарт-карты и преимущества аутентификации с ее использованием.
13. От каких угроз необходимо обеспечить защиту в корпоративной ИС?
14. Для чего предназначен протокол IPSec и какие он имеет средства защиты?
15. Для чего предназначен, достоинства и что обеспечивает сервер ISA Server 2004?
16. Какое назначение имеет веб-сервер Internet Information Services (IIS)?
17. Для чего предназначены и преимущества ПП семейства Antigen?
18. Какие виды защиты используются для обеспечения безопасной работы мобильных пользователей?
19. Поясните назначение сервера терминалов ОС Windows Server 2003.
20. Какие основные фазы должен реализовать протокол SSL?
21. Поясните сущность технологии кластеризации и теневого копирования.

7.10 Литература

1. Ч. Рассел. Microsoft Windows Server 2003. Справочник администратора. «ЭКОМ», М., 2006.

8 ПЛАТФОРМЫ ДЛЯ ЭФФЕКТИВНОЙ КОРПОРАТИВНОЙ РАБОТЫ

В настоящее время требования, предъявляемые к корпоративным информационным системам, сводятся не только к обеспечению эффективной индивидуальной работы пользователей, но и к возможности коллективной работы при условии доступа к нужной информации в любом месте и в любое время.

Поддержка индивидуальной и коллективной работы пользователей корпоративных информационных систем может быть реализована на базе следующих решений [1]:

- интегрированные средства коммуникаций;
- рабочие области коллективной деятельности;
- мгновенный доступ к информации и людям;
- автоматизация бизнес-процессов.

Интегрированные средства коммуникаций. Сотрудники предприятий для доступа к информации используют городские и сотовые телефоны, смартфоны, КПК, персональные компьютеры, ноутбуки и Internet-киоски. ИТ-инфраструктура предприятия должна обеспечивать взаимодействие всех перечисленных устройств.

Решения Microsoft упрощают и интегрируют разнообразные средства коммуникаций, доступные группам и индивидуальным сотрудникам. Электронная почта, мгновенный обмен сообщениями, голосовая почта, телефоны, мобильные устройства и средства проведения конференций через Internet объединяются унифицированным программным обеспечением. Функции такого ПО должны быть доступны независимо от места нахождения пользователей или типа сетевого соединения. Microsoft предоставляет интеллектуальное ПО, которое управляет коммуникациями, с учетом возможностей линий связи, в реальном масштабе времени. Данное программное обеспечение способствует созданию эффективных коммуникаций как внутри предприятия, так и с партнерами, поставщиками и клиентами.

Рабочие области коллективной деятельности. Для поддержки коллективной работы Microsoft предлагает использовать службу Windows SharePoint Services, которая устанавливается в Microsoft Windows Server 2003. Данная служба предоставляет надежные и простые в использовании рабочие области для групп, легко интегрируется с Microsoft Office System, позволяя ИТ-службе создавать рабочие области коллективной работы. Эти области облегчают проведение совещаний, управление проектами, создание документов и др. Windows SharePoint Services можно интегрировать с корпоративными бизнес-приложениями и, следовательно, получать к ним доступ посредством привычного пользователю интерфейса.

Мгновенный доступ к информации и людям. Корпоративным пользователям требуются эффективные средства поиска информации во множестве источников. Для решения данной задачи Microsoft предлагает использовать портальные технологии и управление контентом. С помощью функциональности MySites в SharePoint пользователи могут создавать свои сайты под личные задачи. Такой сайт является единой точкой доступа к документам пользователя, новостям, электронной почте и другим приложениям.

Автоматизация бизнес-процессов. При автоматизации внутренних бизнес-процессов предприятия появляется необходимость исключения бумажного документооборота из информационных потоков. Решения Microsoft позволяют использовать привычные программы, такие как Microsoft Office, для обращения к корпоративной информации и приложениям. При интеграции ERP-систем с программами Microsoft Office сотрудники предприятия могут обращаться к бизнес-приложениям прямо из Microsoft Office. Поддержка XML в Microsoft Office System предоставляет большие возможности по формированию индивидуальных схем информационных потоков и позволяет применять гибкие средства управления процессами на основе документов.

Основные элементы ИТ-инфраструктуры, которые позволяют реализовать эффективную поддержку коллективной работы следующие:

- *Exchange Server 2007* – поддержка доступа к электронной почте и информации практически из любого места, с любого устройства и в любое время;
- *технологии Microsoft SharePoint* – доступные, простые в эксплуатации и масштабируемые средства поддержки коллективной работы (от совместной деятельности в рамках отдела до взаимодействия между предприятиями). Эти технологии включают Microsoft Office SharePoint Portal Server (SPPS) 2003 и Windows SharePoint Services (SPS):
    - *Microsoft Office SharePoint Portal Server 2007* – надежный, масштабируемый, простой в использовании и управлении портал для поддержки коллективной работы, который служит связующим звеном между людьми и информацией. SPPS 2003, построенный на платформе Microsoft Windows SPS, позволяет организациям интегрировать бизнес-процессы и приложения, а также полный набор средств персонализации и коллективной работы пользователей;
    - *Microsoft Windows SharePoint Services 2.0* позволяет создавать Web –сайты, через которые члены группы могут обмениваться документами и совместно работать над проектами;
- *InfoPath 2007* – гибкое и эффективное средство создания динамических форм и их заполнения в рамках группы или организации, которое способствует успешному ведению бизнеса, расширяя возможности коллективной работы и улучшая процесс принятия решений. Информацию, собираемую с помощью InfoPath 2007, можно передавать в Web-сервисы и бизнес-приложения, так как InfoPath 2007 поддерживает любые пользовательские XML-схемы;

- *ISA Server 2004* – межсетевой экран и прокси-сервер, который обеспечивает безопасный доступ к данным и защищает конфиденциальную информацию, хранящуюся в корпоративной сети;
- *Microsoft Office 2007* – средства работы с документами, тесно интегрированные со средствами совместной работы SharePoint;
- *служба управления правами Windows* (Windows Rights Management Services, WRMS) – обеспечивает надежную защиту и контроль доступа на уровне отдельных документов;
- *Microsoft Office Live Communications Server 2007* в сочетании с Office Communicator 2007 – мощное, масштабируемое корпоративное решение для мгновенного обмена сообщениями, проведения аудио- и видеоконференций по IP-сетям в режиме реального времени с функциональностью определения присутствия. Live Meeting – отдельный Web-сервис, не требующий для установки в организации выделенного сервера и позволяющий проводить конференции через Internet;
- *платформа Windows Server 2003* со службой каталогов Active Directory – основа ИТ-инфраструктуры, обеспечивающей максимальную эффективность работы сотрудников.

8.1 Exchange Server 2007

Microsoft Exchange Server 2007 — надежная система обмена сообщениями со встроенными средствами защиты от нежелательной почты и вирусов. С помощью Exchange 2007 пользователи организации получают доступ к электронной почте, голосовой почте, календарям и контактам с использованием широкого спектра устройств и из любого места нахождения[2,3].

Данный сервер характеризуется повышенной безопасностью и надежностью. Он позволяет обеспечить доступ к корпоративной информации сотрудникам предприятия практически из любого места и в любой момент времени.

В Microsoft Exchange Server 2007 существует пять ролей сервера, которые можно установить и настроить на компьютере, на котором работает Microsoft Windows Server 2003:

- клиентский доступ;
- граничный транспорт;
- транспортный сервер-концентратор;
- сервер почтовых ящиков;
- единая система обмена сообщений.

Роль сервера «Клиентский доступ» поддерживает клиентские приложения Microsoft Web-клиент Outlook и Microsoft Exchange ActiveSync, протоколы POP3[4], IMAP4[5] и службы, такие как автообнаружение и Web-службы. Данная роль принимает подключения к серверу Exchange 2007 от различных клиентов. Программные клиенты, такие как Microsoft Outlook Express и Eudora[6], используют подключения POP3 и IMAP4, а аппаратные, такие как мобильные устройства, используют ActiveSync, POP3 или IMAP4 для связи с сервером Exchange.

Роль *пограничного транспортного сервера* развертывается в демилитаризованной зоне предприятия как автономный сервер. Созданный для уменьшения площади атаки, пограничный транспортный сервер обрабатывает весь почтовый поток, соприкасающийся с Internet, обеспечивая передачу по протоколу SMTP и работу служб промежуточных узлов организации Exchange. Дополнительные уровни защиты и безопасности сообщения обеспечиваются рядом агентов, запущенных на пограничном транспортном сервере и выполняющих операции с сообщениями при их обработке компонентами транспорта сообщения. Эти агенты поддерживают средства, которые обеспечивают защиту от вирусов и нежелательной почты и применяют правила транспорта для управления потоком сообщений.

---

[4] **POP3** (*Post Office Protocol Version 3* — протокол почтового отделения, версия 3) — это сетевой протокол, используемый для получения сообщений электронной почты с сервера.

[5] **IMAP** (*Internet Message Access Protocol*) — Internet - протокол прикладного уровня для доступа к электронной почте. Текущая версия протокола имеет обозначение IMAP4rev1 (IMAP, версия 4, ревизия 1). Протокол поддерживает передачу пароля пользователя в зашифрованном виде.

[6] **Eudora Mail** — клиент электронной почты, который появился еще на заре Internet, когда электронная почта была чуть ли не единственным средством общения

Роль *транспортного сервера-концентратора*, развернутая внутри леса службы каталогов Active Directory, управляет всем потоком почты на предприятии, применяет правила транспорта и политики ведения журнала и доставляет сообщения в почтовый ящик получателя. Сообщения, отправляемые в Internet, передаются узловым транспортным сервером к роли сервера граничного транспорта, развернутой на периметре сети. Сообщения, получаемые из Internet, прежде чем передаются серверу узлового транспорта, обрабатываются сервером граничного транспорта. Если сервера граничного транспорта нет, можно настроить сервер узлового транспорта для непосредственной передачи сообщений из Internet. На сервере узлового транспорта можно также установить и настроить агенты сервера граничного транспорта, которые обеспечат в организации защиту от нежелательной почты и компьютерных вирусов.

Роль *сервера почтовых ящиков* обеспечивает хранение баз данных почтовых ящиков пользователей. Если в почтовой системе планируется хранить почтовые ящики пользователей, общие папки или и то, и другое, роль сервера почтовых ящиков является обязательной. В Exchange Server 2007 роль сервера почтовых ящиков интегрирована со службой каталогов Active Directory. Роль сервера почтовых ящиков расширяет возможности информационных сотрудников, обеспечивая улучшенные функции календаря, управление ресурсами и автономную загрузку адресных книг.

Роль *сервера единого обмена сообщениями* объединяет голосовые сообщения, факс и электронную почту в одной папке входящих сообщений, к которой можно получить доступ с телефона и компьютера. Единая система обмена сообщениями объединяет Exchange Server 2007 с телефонной сетью организации и предоставляет функции единой системы обмена сообщениями для основной части линейки продуктов Exchange Server.

При взаимодействии Exchange 2007 с несколькими клиентами безопасность обеспечивается межсетевыми экранами в сочетании с сервером Microsoft ISA Server, который играет роль шлюза и дополнительно защищает Exchange и другие компоненты на серверной стороне.

Взаимодействие с Outlook. Exchange Server 2007 может работать с Outlook 2000/2002/2003/2007. При организации взаимодействия Outlook 2007 с Exchange 2007 обеспечивается устойчивая работа при ненадежных, низкоскоростных или некачественных соединениях.

Outlook 2007 поддерживает:

- режим кэширования данных Exchange, позволяющий получать доступ к сообщениям в отсутствии соединения с сервером Exchange;
- соединения без использования VPN, на базе протокола RPC[7] поверх HTTPS[8].

Программное средство Outlook Web Access является эффективным и безопасным. Оно поддерживает:

- средства проверки правописания;
- поддержка списка задач;
- блокирование HTML-кода и вложений, чтобы избежать отправки уведомления о том, что пользователь открыл сообщение, и последующего получения спама;
- автоматическое завершение сеанса связи (если пользователь забыл завершить сеанс связи, по истечении определенного периода простоя сеанс завершается автоматически);
- поддержка S/MIME[9] для Outlook Web Access позволяет использовать цифровые подписи и шифровать сообщения электронной почты.

Мобильные устройства на базе Windows, такие как КПК, поставляются со встроенными программами Microsoft ActiveSync и Pocket Outlook, что позволяет синхронизировать сообщения электронной почты, календарь и списки контактов непосредственно с Exchange 2007.

---

[7] **RPC** (*Remote Procedure Call*) — технология, позволяющая компьютерным программам вызывать функции или процедуры в другом адресном пространстве (как правило, на удалённых компьютерах).
[8] **HTTPS** – расширение протокола HTTP, поддерживающее шифрование
[9] **S/MIME** (Secure / Multipurpose Internet Mail Extensions) стандарт для шифрования и подписи в электронной почте с помощью открытого ключа

Пользователи Exchange 2007 посредством Outlook Mobile Access могут получать доступ к почтовым ящикам с мобильных устройств, оснащенных браузерами с поддержкой HTML, xHTML[10] (WAP 2.x[11]) и cHTML[12].

Гибкие средства доступа к данным и новые технологии непрерывного доступа позволяют пользователям повысить производительность труда и самостоятельно определять время и способ взаимодействия:

- сотрудники, совершающие деловые поездки имеют широкие возможности доступа к данным и взаимодействия с портативных компьютеров через Outlook 2007 и беспроводные сети;
- удаленные сотрудники могут работать на дому, в удаленном офисе, в организации заказчика, в точках беспроводного доступа по стандарту 802.11[13] и получать безопасный доступ к данным Exchange через или Outlook Web Access [4] или Outlook на любом компьютере, подключенном к Internet. Outlook Web Access расширяет возможности, позволяя работать с Exchange в отсутствие собственного портативного компьютера;
- сотрудники в командировке могут работать с Outlook 2007 прямо из гостиничного номера или аэропорта по коммутируемой линии и синхронизировать электронную почту. После сеанса синхронизации с Exchange можно продолжать работу в автономном режиме до следующей возможности сетевого подключения. Outlook 2007 и Exchange 2007 обеспечивают одинаковую эффективность труда как при наличии сетевого подключения, так и в автономном режиме.

---

[10] **XHTML** (*Extensible **H**yper**t**ext **M**arkup **L**anguage* — Расширяемый язык разметки гипертекста)— язык разметки веб-страниц, по возможностям сопоставимый с HTML, однако является подмножеством XML.

[11] **WAP** (*Wireless Application Protocol*) - «протокол беспроводного доступа» - это средство получения доступа к ресурсам Internet посредством только мобильного телефона, не прибегая к помощи компьютера и/или модема. По сути это технический стандарт, описывающий способ, с помощью которого информация из Internet передается на дисплей мобильного телефона

[12] **CHTML** является определенным подмножеством спецификаций HTML 2.0, HTML 3.2, HTML 4.0, ориентированным на устройства с ограниченными возможностями отображения информации — таких, как смартфоны, коммуникаторы, мобильные телефоны, КПК.

[13] **Стандарт IEEE 802.11**, разработка которого была завершена в 1997 г., является базовым стандартом и определяет протоколы, необходимые для организации беспроводных локальных сетей (WLAN).

8.2 Технология Microsoft SharePoint

Office SharePoint Server 2007 — это серверное приложение в составе System Microsoft Office 2007 [5]. Оно предназначено для обеспечения совместной работы, предоставления средств управления контентом, внедрения бизнес-процессов и представления доступа к информации, важной для организационных целей и процессов.

При помощи шаблонов узлов и других средств Office SharePoint Server 2007 можно быстро и эффективно создавать узлы, поддерживающие:

- публикацию определенного контента;
- управление контентом и записями
- потребности в бизнес-аналитике.

Например, возможно создание узлов уровня организации, таких как корпоративные порталы в интрасети или Web-узлы, либо специализированных узлов, таких как хранилища содержимого или рабочие области для собраний. Эти узлы позволяют совместно работать и обмениваться сведениями пользователям как внутри организации, так и за ее пределами. Кроме того, Office SharePoint Server 2007 можно использовать для проведения эффективных поисков людей, документов и данных, для разработки бизнес-процессов на основе форм и участия в них, а также для доступа к большим объемам бизнес-данных и их анализа.

Некоторые преимущества использования Office SharePoint Server 2007 описаны ниже.

Эффективная совместная работа с другими пользователями на предприятии. Например, можно использовать календари для просмотра запланированных событий группы, использовать библиотеки документов для хранения документов группы, отдела или организации. Также можно обсуждать вопросы с использованием блогов или записывать и сохранять сведения на вики-страницах, представляющих собой управляемые пользователями базы знаний.

Создание личных узлов, на которых пользователи могут управлять сведениями и предоставлять их для доступа другим пользователям. Например, можно создать личный узел для централизованного просмотра и управления всеми своими документами, задачами, ссылками, календарем Microsoft Office Outlook 2007, сведениями о коллегах и другими личными сведениями.

Поиск людей и данных в бизнес-приложениях. Например, при поиске на личных узлах в интрасети можно найти обладателя определенных навыков или интересов, даже не зная его имени. Также можно находить данные в корпоративной базе данных или бизнес-приложении, таком как CRM-приложение (приложение для управления взаимоотношениями с клиентами).

Управление документами, записями и Web-содержимым. Например, организация может разработать процесс прекращения действия документов по прошествии определенного времени.

Размещение бизнес-форм на основе XML, интегрированных с базами данных или другими бизнес-приложениями. Например, для местного отделения государственного учреждения можно разработать формы заявлений в Microsoft Office InfoPath 2007 и разместить их в Office SharePoint Server 2007, чтобы затем пользователи могли заполнять эти формы непосредственно в обозревателе. Введенные данные будут отправляться в базу данных в сети учреждения.

Простота публикации отчетов, списков и ключевых индикаторов производительности при помощи связывания с бизнес-приложениями, такими как SAP, Siebel и Microsoft SQL Server 2005.

Технологии SharePoint реализуются набором служб Microsoft Windows SharePoint Services 2.0 [6], которые позволяют создавать и поддерживать Web-сайты, с помощью которых члены группы могут взаимодействовать, обмениваться документами и совместно работать над проектами.

Microsoft Office 2007 позволяет еще эффективнее использовать Microsoft Windows SharePoint Services 2.0, в том числе обращаться к сайту так, будто он является частью локальной системы, сохранять файлы в библиотеки, редактировать документы в любом из приложений Office, перемещать любую инфор-

мацию на такой сайт и др. С помощью Web-сервисов продукты и технологии SharePoint легко используют информацию практически из любого корпоративного приложения.

Microsoft Windows SharePoint Services 2.0, например, существенно облегчает операции резервного копирования и восстановления, если соответствующие данные распределены по множеству разнообразных систем хранения. Все документы, списки, представления и конфигурационная информация размещаются в хранилищах под управлением SQL Server. Это упрощает управление операциями копирования и восстановления, а такие обеспечивает высокую масштабируемость и поддержку персонализированных представлений Web-портала для пользователей.

Microsoft Windows SharePoint Services является технологической платформой для SharePoint Portal Server 2007. SharePoint Portal Server 2007 является серверным продуктом с дополнительной функциональностью для создания надежного, масштабируемого, простого в использовании и управлении портала Для поддержки коллективной работы SharePoint Portal Server 2007 и Office SharePoint Server 2007 обеспечивают новый уровень совместной работы над документами. Функции управления документами, встроенные в Office SharePoint Server 2007, могут быть задействованы в любых решениях на основе продуктов и технологий SharePoint. Так, файловый сервер из обычного хранилища документов превращается в полноценный корпоративный портал с поддержкой поиска, категоризации, рассмотрения документов и получения оповещений об изменениях в них.

Использование Office SharePoint Server 2007 дает следующие преимущества:

- повышение эффективности работы групп:
    - упрощение и ускорение обмена данными и результатами работы групп за счет сотрудничества в режиме реального времени;

- экономия средств за счет упрощения взаимодействия внутри группы;
- более простое управление процессами с помощью надежного контроля версий;
- упрощения управления проектом за счет применения усовершенствованных средств и функций;

– повышение эффективности процесса в рамках организации:

- рациональнее администрирование узлов, хранилищ и систем безопасности;
- удобство коллективной работы в рамках групп за счет интеграции с Microsoft Outlook и Office;
- простые и мощные средства настройки;
- улучшенные средства обобщения данных за счет использования XML и Microsoft InfoPath;
- повышение уровня безопасности и снижение рисков за счет автоматизации защитных мероприятий;
- более высокая безопасность работы в Internet;

– более совершенная платформа для развития организации:

- улучшенное использование и доступность данных из разных систем;
- применение Microsoft Office System в качестве эффективного набора средств для коллективной работы;
- развитие организации за счет использования стандартных API-интерфейсов;
- преимущества поэтапного развертывания;

SharePoint Portal Server 2007 по сравнению с Office SharePoint Server 2007 предоставляет следующие дополнительные возможности:

– создание, развертывание и управление порталами для небольших групп, подразделений крупных организаций или целых предпри-

ятий с сотнями тысяч пользователей, десятками тысяч сайтов и миллионами документов;

- поиск любой информации в документах, имеющихся в организации, независимо от их местонахождения — на файловых серверах, Web-сайтах, в других системах хранения документов или в корпоративных приложениях;
- поддержка адаптируемых структур для создания, организации и поиска всех источников информации в рамках предприятия, в том числе на сайтах отделов и подразделений, Web-сайтах проектов, над которыми работают группы, персональных Web-сайтах и т. д.;
- персонализированная категоризация и доставка сведений из портала и другой корпоративной информации на основе настраиваемых профилей пользователей и аудиторий, определенных данной организации.

Для качественной поддержки большого числа сайтов SharePoint в Office SharePoint Server 2007 имеются стандартные средства для создания и управления сайтами. В SharePoint Portal Server 2007 включены средства развертывания и администрирования сайтов для крупных предприятий:

- каталог сайтов;
- сконфигурированные решения по интеграции корпоративных решений;
- динамически настраиваемые карты сайтов;
- средства управления крупномасштабной топологией серверов;
- возможность совместной работы множества серверов индексации и поиска.

В Microsoft Windows SharePoint Services реализована функция персонализации, которая обеспечивает поддержку аудитории – динамической группы пользователей с одним или несколькими общими свойствами (бизнес-функции, отдел, группа пользователей). Принадлежность пользователя к определенной аудитории определяет Web-компоненты, фильтры информации.

SharePoint Portal Server 2007 — как точка соединения пользователей, групп, проектов, информации и баз знаний позволяет эффективнее работать всему предприятию.

Microsoft Windows SharePoint Services 2.0 поддерживает:

- совместную работу над документами;
- обмен информацией на уровне групп и проектов;
- управление виртуальными группами;
- взаимодействие между индивидуальными лицами;
- интегрированные средства определения присутствия (с Live Communications Server 2005):
- списки и библиотеки документов:
- контроль версий документов, процедуру взятия файлов на редактирование и их возврат;
- оповещения об изменениях;
- установку дополнительных Web-компонентов;
- общие календари и средства поддержки дискуссий;
- создание Web-сайтов и управление ими пользователями;
- интеграцию с Microsoft Office;
- повышение производительности труда индивидуальных лиц и групп;
- повторное использование имеющейся информации при создании новых документов;
- разграничение доступа к информации на основе ролей;
- продуктивную среду для коллективной работы;
- упрощение использования, развертывания и настройки.

SharePoint Portal Server 2007 включает в себя все возможности Microsoft Windows SharePoint Services 2.0 и дополнительно обеспечивает:

- структуризацию сайтов в рамках всего предприятия;

- создание сайтов SharePoint с применением каталога сайтов (Site Directory);
- централизованное администрирование всех порталов и сайтов групп в организации;
- единый вход в корпоративные приложения;
- контекстный поиск любых данных и информации в рамках всей организации;
- утверждение документов;
- повышение эффективности работы организации;
- более эффективные средства поиска и выборки информации из любого источника в рамках организации или за ее пределами;
- большее увеличение производительности труда благодаря расширенным возможностям повторного использования имеющейся информации при создании новых документов и благодаря более эффективному взаимодействию групп.

8.3 Интеграция приложений Microsoft Office с технологиями SharePoint

Для поддержки коллективной работы и взаимодействия между сотрудниками предприятия используется Office 2007 в сочетании с Microsoft Windows SharePoint. Это позволяет по-новому организовать взаимодействие удаленных сотрудников, в любое время получить мнение специалиста по любому вопросу и ускорить процессы утверждения и пересмотра документов. Это обеспечивается следующими функциями:

- *область задач рабочей области* позволяет при редактировании документа в приложении Office увидеть через сервер, на котором выполняются службы Office SharePoint Server 2007, состояние проводимой совместной работы;

- *сайты рабочей области документов* обеспечивают интеллектуальную организацию совместной работы над документами и улучшенное управление версиями. Пользователи получают средства общего доступа к документу в режиме реального времени, назначения задач и сроков их выполнения, а также могут легко увидеть, на каком этапе находится работа над документом;
- *сайты рабочей области совещаний* расширяют возможности организации совещаний, получения информации и добавления участников, находящихся в различных местах;
- *технология мгновенного обмена сообщениями* интегрирована с приложениями Office 2007, что позволяет моментально получать сведения о присутствии и начинать диалог непосредственно из документов или Outlook (при наличии Live Communications Server 2005);
- *общие контакты и календари*, доступ к которым облегчен для членов группы, упрощают процесс координации и планирования совещаний;
- *технология управления правами на доступ к информации* (Information Rights Management, IRM[14]) обеспечивает более эффективный контроль над важной деловой информацией.

Взаимодействие приложений Office 2007 и Office SharePoint Server 2007 обеспечивает общая рабочая область при условии, что в системе установлены приложения Microsoft Office или Web-браузер. Office SharePoint Server 2007 предоставляет приложениям Office 2007 средства для работы над общим документом, ознакомления с ходом работы, поиска другого члена группы в сети и добавления комментариев или результатов в общую рабочую область.

Область задач общей рабочей области. При открытии документа, хранящегося на сайте Share-Point (равно как и документа, находящегося на обычном сайте, сайте рабочей области совещаний или документов), в соответст-

[14] **Служба управления правами (Microsoft® Windows® Rights Management Services, RMS) ОС Windows Server™ 2003** представляет собой технологию защиты информации, которая используется с такими RMS-совместимыми приложениями, как Microsoft Office 2007.

вующем приложении Office 2007 появляется специальная область задач со сведениями о сайте, например, список лиц, ведущих совместную деятельность в рабочей области, их местонахождение в сети, перечень задач, другие документы библиотеки общей рабочей области, связи (ссылки) и т. д. Область задач общей рабочей области появляется при открытии документа с сайта SharePoint в Word 2007, Excel 2007, PowerPoint 2007, Microsoft Project 2007, Visio 2007 и OneNote 2007.

Область задач также позволяет добавлять в рабочую область новых членов, создавать, назначать и отмечать задачи как завершенные, загружать дополнительные документы, просматривать другие документы в библиотеке, вставлять связанные с документом ссылки или переходить по ним. Благодаря интеграции области задач с технологией мгновенного обмена сообщениями можно, щелкнув знакомый значок, увидеть, кто находится в сети, и отправлять сообщения членам группы, Эта область переносит контекст документа в рабочую среду пользователя.

Рабочая область документа. Совместная работа над документом часто начинается с отправки его другим членам группы по электронной почте. Иногда, если документ хранится только на одном сервере требуется создание его локальной (автономной) копии. Автономная копия используется при отсутствии связи в сети.

Использование электронной почты и работа с автономными копиями приводит к тому, что у документов появляется несколько версий, а процесс сведения всех изменений занимает достаточно много времени. Кроме того, работая с электронной почтой, трудно отслеживать действия других членов группы.

Сайты рабочей области документов упрощают повседневную коллективную работу над документами в нескольких отношениях. Как и сайты SharePoint, они собирают для участников проекта в одном месте необходимые сведения: перечни задач, крайние сроки, соответствующие документы, ссылки и контакты. Они также интегрируются с приложениями Office 2007 через область задач, отображаемую вместе с документом, что облегчает доступ к этим ресурсам. В

отличие от электронной почты, при использовании которой автор сообщения может даже не знать, начал ли работу хоть один из тех, к кому была обращена подобная просьба, область задач общей рабочей области и сайты рабочих областей документов позволяют каждому участнику видеть состояние задачи в целом и то, как продвигается работа над документами.

Рабочая область совещаний. Рабочая область совещаний рассчитана на тех, кто занимается подготовкой, проведением и сопровождением совещаний. Эта область создает в сети безопасное место для централизации переписки, документов и материалов, относящихся к совещанию. Она упрощает организацию и проведение совещаний, делает их более удобными и эффективными, помогает экономить время и повышает результативность совещаний.

Созданная с помощью Office SharePoint Server 2007 и Web-компонентов, рабочая область совещаний в основе своей представляет пользовательский узел с простыми средствами объединения сотрудников для разовых или регулярных совещаний.

Для администратора рабочая область совещаний упрощает процедуру их планирования, координации участников, оснащения всей необходимой документацией и сопровождающими материалами, облегчает работу с удаленными сотрудниками, решение вопросов информационного обеспечения, задач сопровождения, возникающих по ходу совещания, а также распространение заметок и действий, созданных, например, в Microsoft OneNote.

Рабочая область совещаний поддерживает следующие функции:

- распространение материалов в соответствии с повесткой;
- организация совместного доступа к визуальным материалам, информации, графикам проведения и действиям;
- организация регулярных совещаний;
- отчет о недоработках текущего совещания;
- обновление дополнительных материалов без отправки повторного запроса;

- запись простых заметок по ходу совещания или получение более развернутых, например, из OneNote;
- подключение к работе удаленных участников;
- интеграция представлений календаря совещаний из списка SharePoint;
- создание и обеспечение сайта рабочей области, а также управление им;
- интеграция рабочей области с любым сайтом SharePoint;
- редактирование данных рабочей области в Excel, PowerPoint и Word.

Office SharePoint Server 2007 и Outlook 2007. В Office 2007 с данными Office SharePoint Server 2007 можно работать прямо в Outlook, что позволяет повысить эффективность использования общих данных, объединяя их с собственными. Так, можно расположить график обзоров продукции на сайте SharePoint, чтобы с ним могли ознакомиться все члены группы. Они могут сравнить этот график с собственным, открыв обновляемый календарь списка SharePoint рядом с календарями Outlook. События из списка SharePoint отражаются и работают так же, как и встречи в Outlook. Их можно перетаскивать из календаря SharePoint в собственный календарь Outlook.

Организации малого бизнеса могут использовать службы SharePoint в качестве небольшого сервера рабочей группы, предоставляющего совместный доступ к контактам и календарям без сервера Exchange.

Данные из Windows SPS кэшируются на локальном компьютере, поэтому они доступны в автономном режиме.

Списки календарей, событий и контактов можно открывать в пользовательском интерфейсе Outlook в режиме только для чтения. Данные из Office SharePoint Server 2007 отображаются и работают так же, как и календари и списки контактов Outlook.

Контакты и календари — обычные списки для хранения как личных, так и групповых сведений. Outlook 2007 и Office SharePoint Server 2007 позволяют

просматривать сразу несколько личных и общих календарей. Общий календарь и общий список контактов можно просмотреть прямо в Outlook. Так что их сведения доступны в любой момент.

Специальные оповещения повышают результативность работы, так как позволяют держать участников группы в курсе последних новостей.

Списки SharePoint. Списки SharePoint предназначены для коллективной работы с данными и методы их сбора и анализа. Списки SharePoint предоставляют следующие возможности:

- *сетка* в Office SharePoint Server 2007 помогает реализовать сходные с Excel функции;
- с*овместная работа над списком нескольких пользователей.* Один и тот же список могут редактировать сразу несколько пользователей. Службы Windows SPS выявляют конфликты и предлагают варианты их разрешения;
- *простота редактирования.* Можно перетаскивать мышью столбцы и строки, а также перемещать данные по списку;
- *интеграция Office и технологий SharePoint.* Доступны преимущества обеих систем: приложения Office могут работать со списками SharePoint;
- *новые списки.* Добавлены следующие списки: библиотека фотографий с широкими возможностями хранения и просмотра картинок, а также библиотеки деловых документов, позволяющие создавать, редактировать и хранить на общем сайте группы решения, построенные на основе XML;
- *усовершенствованные списки*. Существующие списки усовершенствованы, в частности, поддерживают новые параметры безопасности, позволяющие делегировать разрешения на уровне списка.

8.4 Microsoft Office InfoPath 2007

Microsoft Office InfoPath 2007— гибкое и эффективное средство сбора информации в динамические формы, ее распространения и повторного использования в рамках группы или предприятия [7]. InfoPath 2007 способствует успешному ведению бизнеса, расширяя возможности коллективной работы и улучшая процесс принятия решений. Информацию, собираемую с помощью InfoPath 2007, можно интегрировать с Web-сервисами и разнообразными бизнес-процессами, так как InfoPath 2007 поддерживает любые пользовательские XML-схемы. InfoPath 2007 может стать частью как формализованных, так и не формализованных бизнес-процессов в современных организациях.

Эффективный сбор информации важен для принятия более обоснованных решений. InfoPath 2007 обеспечивает следующие преимущества:

- облегчает сбор нужных данных, параллельно выполняя их проверку на допустимость, выводя на экран подсказки и форматируя собранную информацию по заданным правилам;
- классифицирует собираемую информацию, позволяя добавлять разделы на формы;
- работает с формами как в онлайновом, так и в автономном режимах, что дает возможность вводить данные и управлять ими в любом месте и в любое время;
- предоставляет привычную среду и инструментарий Microsoft Office, что резко сокращает расходы на обучение.

InfoPath 2007 как точка соединения людей, информации и процессов упрощает группам и предприятиям повторное использование собранных данных:

- позволяет обмениваться информацией и повторно использовать ее между различными системами и процессами за счет поддержки Web-сервисов;
- улучшает условия коллективной работы в группах, так как может взаимодействовать с Office SharePoint Server 2007.

Кроме того, InfoPath 2007 упрощает разработку и развертывание динамических форм в рамках всего предприятия. Эти формы можно публиковать в общем сетевом каталоге, на Web-сервере, в библиотеке форм Windows SharePoint Services или пересылать по электронной почте.

8.5 Служба управления правами Windows

Любая организация неизбежно сталкивается с проблемой защиты ценной информации от небрежного обращения и злонамеренного использования. Участившиеся случаи кражи информации и появление новых законодательных нормативов защиты данных требуют совершенствования защиты электронной информации.

Речь идет о защите таких категорий информации, как динамические отчеты, составляемые на основе баз данных и хранящиеся в информационном портале предприятия, конфиденциальные сообщения электронной почты, документы стратегического планирования, финансовые прогнозы, контракты, отчеты оборонных ведомств и другие секретные данные. Активное применение компьютеров в создании и использовании такой информации, расширение возможностей взаимодействия через сети и Internet, появление более мощных мобильных устройств — все это делает вопрос защиты корпоративных данных крайне актуальным.

Благодаря службе управления правами Windows (Windows Rights Management Services, или Windows RMS) можно усилить защиту данных всех типов в интрасетях и до определенной степени даже в Internet [8]. Это новая технология принудительного применения политик, которая позволяет защищать данные на уровне файлов. Такая защита обеспечивается независимо от того, куда перемещается файл. В Office 2007 на основе этой службы реализована система управления правами на доступ к информации (Information Rights Management, IRM). Она позволяет определять права редактирования документа и защищать его содержимое, указывая лица, уполномоченные на внесение изменений. Кро-

ме того, можно ограничить применение в документах функций вырезки, копирования, вставки, печати и отправки электронных сообщений, предоставляя пользователям и организациям расширенный контроль над важными информационными ресурсами.

Стандартная топология. Стандартная топология системы управления правами включает один или несколько физических серверов, образующих корневой узел или кластер Windows RMS. Корневой узел обеспечивает работу служб сертификации и лицензирования. При развертывании нескольких серверов их можно объединять в кластер с общим для всех URL-адресом.

Все запросы сертификатов и лицензий, созданных на основе стандарта XrML[15], передаются в корневой кластер по общему URL-адресу, определенному для этой группы серверов. Существует множество реализаций механизма виртуальной адресации: циклический алгоритм DNS, служба балансировки нагрузки сети Windows, аппаратные решения и т. п. Виртуальная адресация обеспечивает равномерное распределение нагрузки по всем серверам и повышает отказоустойчивость за счет устранения зависимости от одного сервера, ответственного за лицензирование и публикацию.

Для хранения сведений о конфигурации и политиках Windows RMS требуется база данных SQL, например Microsoft SQL Server 20005. Применять MSDE рекомендуется только для конфигурации с одним сервером. База данных конфигурации служит для хранения, совместного использования и извлечения конфигурационных и иных данных. Для каждого кластера серверов Windows RMS создается одна база данных конфигурации. База данных конфигурации и база данных журнала могут быть размещены на одном из физических серверов кластера или на отдельном сервере в виде удаленного экземпляра базы данных SQL Server.

[15] **Стандарт XrML** определяет язык описания прав, с помощью которых доверенные системы в доверенной среде могут формулировать политики в области электронной информации

8.6 Система управления правами на доступ к информации в Office 2007

Система управления правами на доступ к информации в Office 2007 и SharePoint Server 2007 предоставляет предприятиям и сотрудникам ИТ-службы расширенный контроль над информационными ресурсами. Эта система действует на уровне файлов и позволяет ограничивать список лиц, имеющих права на доступ и использование документов и электронных сообщений, а также защищает электронную интеллектуальную собственность от несанкционированной распечатки, пересылки и копирования.

IRM — это технология защиты информации, с помощью которой может быть разрешен совместный доступ к документам, и их отправка по электронной почте. При этом сохраняется контроль за тем, кто имеет права на их использование и в каких целях. Если документ или электронное сообщение защищены этой технологией, ограничения на доступ и использование вступают в силу независимо оттого, где находятся данные.

Поддержка IRM в Office 2007 удовлетворяет две потребности предприятий и сотрудников ИС-службы:

- *защита электронной интеллектуальной собственности*. Большинство предприятий полагаются в этом вопросе на межсетевые экраны, системы безопасного входа и другие технологии защиты сети. Основной недостаток таких технологий в том, что законные пользователи имеют доступ к информации и могут получать ее вместе с неуполномоченными на это лицами, что создает потенциальную угрозу для политики безопасности предприятия. Технология IRM защищает от несанкционированного доступа и использования саму информацию;
- *защита, контроль и поддержание целостности информации*. Работающие с информацией специалисты часто имеют дело с конфиденциальными или исключительно важными сведениями. При этом в вопросе неразглашения этих сведений остается полагаться только

на порядочность персонала. Система IRM, отключив соответствующие функции для защищенного объекта, исключает любую попытку пересылки, копирования или вывода на печать конфиденциальных сведений.

Технологии IRM позволяют ИТ-руководителям усовершенствовать существующие политики организации, касающиеся конфиденциальности документов, операций и электронной почты. Для руководителей организаций и служб безопасности существенно снижается актуальный на сегодня риск передачи важной корпоративной информации тем, кому она не предназначена.

Технология защиты в Office 200 SharePoint Portal Server 2007 может быть легко активирована. Интеграция с Active Directory предоставляет уровень защиты документов, который выше, чем установка паролей на документы. Кроме того, программа просмотра IRM (IRM Viewer) гарантирует, что каждый пользователь Windows сможет работать с защищенными IRM документами независимо от наличия Office 2007 на его компьютере, что позволяет компаниям организовывать совместный доступ к объектам интеллектуальной собственности за пределами компании, сохраняя действенность политик безопасности.

Система управления правами доступа к информации в электронных сообщениях Outlook. Средства IRM можно использовать в Outlook для предотвращения пересылки, копирования и вывода сообщений электронной почты на печать. Защищенные сообщения во время передачи автоматически шифруются, а если отправитель задал ограничения, то в Outlook будут отключены соответствующие команды. Вложенные в защищенные сообщения документы Office тоже автоматически защищаются.

Технология IRM в документах Excel, Word и PowerPoint. Для документов Office 2007 можно установить защиту как на уровне отдельных пользователей, так и на уровне групп (если разрешения задаются на уровне групп, то для их расширения требуется Active Directory). Для каждого пользователя или группы может быть указан набор разрешений в соответствии с ролью, определенной владельцами документа: читатель, рецензент или редактор. В зависимости от

роли система IRM для активации назначенных прав отключит определенные команды. Владельцы могут также запретить печать и установить сроки истечения действия прав. После этого срока открыть документ уже не удастся.

8.7 Эффективное взаимодействие в режиме реального времени.

Эффективная коллективная работа поддерживается серверами и службами Microsoft Office – Live Communications Server (LCS), Live Meeting и Communicator. Это средства мгновенного обмена сообщениями (instant messaging, IM), проведения аудио- и видеоконференций по IP-сетям в режиме реального времени с функциональностью определения присутствия. Благодаря таким средствам глобальный доступ к любому человеку или информационному ресурсу становится реальностью. Можно мгновенно и эффективно обмениваться идеями, информацией, принимать решения. Без всяких задержек, без расходов на поездки, без длительных согласований.

Взаимодействие в режиме реального времени (real-time communications, RTC) позволяет:

- предприятиям, развертывающим Live Communications Server, получать выгоду за счет уменьшения совокупной стоимости владения инфраструктурой коммуникаций. С помощью функции определения присутствия сотрудники видят, кто из контактов находится на месте, и это избавляет их от поиска нужных людей ;
- сократить потребность в обращениях по электронной почте и междугородной телефонной связи. Уменьшение трафика, связанного с электронной почтой, снижает потребность в сетевых ресурсах, хранилищах почтовой информации и технической поддержке соответствующих систем, а значит, способствует и сокращению расходов;
- позволяют членам групп обмениваться информацией, слышать и видеть своих коллег посредством встроенных средств аудио- и видеоконференций, а также мгновенного обмена сообщениями. Когда

эти средства объединяются с технологией определения присутствия, шансы на соединение с нужными людьми резко возрастают. Это дает возможность предприятию экономить на междугородных телефонных звонках.

Live Communications Server позволяет членам группы связываться с коллегами, партнерами, поставщиками и заказчиками в режиме реального времени, своевременно обмениваться важной для бизнеса информацией и вести совместную работу с другими организациями так же легко, как и с коллегами. Это ускоряет принятие решений и повышает их качество.

8.8 Live Communications Server 2007

Microsoft Office Live Communications Server 2007 обеспечивает высокую надежность, управляемость, защиту конфиденциальной информации и общую безопасность [10]. Этот продукт представляет для бизнеса эффективный контроль за конфиденциальной информацией в рамках всей организации.

Функциональность мгновенного обмена сообщениями (IM) и определения присутствия является в Live Communications Server 2007 частью масштабируемого корпоративного решения, которое обеспечивает высокую безопасность и бесшовную интеграцию с другими продуктами Microsoft. Оно также предоставляет расширяемую платформу разработки на основе промышленных стандартов. Это простое в управлении и надежное решение позволяет организации сэкономить на расходах, повысить эффективность бизнеса, увеличить производительность труда и усилить защиту интеллектуальной собственности.

IM – это возможность передачи текстовых сообщений в режиме реального времени по IP-сети, например по Internet или корпоративной сети, а определение присутствия – возможность выяснить, доступен ли коллега на одном или нескольких устройствах. Live Communications Server обеспечивает совместное использование приложений и коллективную работу над данными между одноранговыми (равноправными) хостами (узлами) в сети, проведение аудио- и ви-

деоконференций, кардинально ускоряя все операции, выполняемые сотрудниками ИТ-службы. IM и другие средства взаимодействия в режиме реального времени не ограничены рамками организации, и их действие может быть распространено на доверенных партнеров, заказчиков и поставщиков, а с добавлением Public IM Connectivity — и на пользователей общедоступных услуг IM.

Public IM Connectivity — это возможность соединения существующей базы пользователей Live Communications Server с общедоступными службами мгновенного обмена сообщениями. Пользователи общедоступных сетей и Live Communications Server могут взаимодействовать в режиме реального времени так же, как с коллегами своего предприятия.

Live Communications Server 2007, легко интегрируемый с Microsoft Office System и системами Windows Server, бесшовно стыкуется с существующими бизнес-процессами и ИТ-инфраструктурой.

Основными преимуществами Live Communications Server 2007 являются:

- *экономия расходов и более высокая производительность*, за счет мгновенного обмена сообщениями и определения присутствия, что способствует сокращению расходов и ускоренному принятию более обоснованных решений;
- *интеграция с Microsoft Office Communicator 2007* предоставляет возможности о применения простых средств поиска контактов с помощью службы адресной книги Live Communications Server. Сотрудники могут искать коллег по глобальному для корпорации списку адресов (GAL), а также на основе локальных сведений об адресах, хранящихся на их компьютерах. Интеграция с Microsoft Office Outlook и Microsoft Exchange Server позволяет получать информацию «свободен/занят» по любым контактам прямо из расписания или графика работ, а также выводить собственные сообщения «вне офиса» непосредственно в Office Communicator 2005. Расширенные средства определения присутствия, в том числе возможность составлять «пользовательские заметки», дают более информативные

сведения другим контактам о том, как лучше всего связаться с вами. Эти данные показываются независимо оттого, подключен пользователь или работает в автономном режиме. При наличии должной инфраструктуры шлюза с офисными телефонными системами (Private Branch Exchange. PBX) или общедоступными коммутируемыми телефонными сетями (Public Switched Telephone Networks, PSTN) Office Communicator 2007 обеспечивает интеграцию с офисными телефонными системами, что позволяет управлять офисным телефоном непосредственно с компьютера для инициации телефонных вызовов и даже для перенаправления входящих вызовов по другим номерам, если данного сотрудника нет на рабочем месте. Конференц-связь с партнерами можно организовать прямо из Office Communicator 2007, что существенно облегчает взаимодействие между сотрудниками информационных отделов.

При наличии Live Communications Server 2007 и партнерских решений в области интеграции с телефонными сетями Office Communicator 2007 поддерживает некоторые варианты офисной связи, в частности управление вызовами, перехват звонков, их пересылку, а также сеансы Microsoft Office Live Meeting.

8.9 Microsoft Office Live Meeting 2007

Программное решение Live Meeting предоставляет возможности для совместной работы с коллегами, заказчиками и поставщиками, где бы они ни находились [11]. Live Meeting обеспечивает проведение онлайновых совещаний, дистанционного обучения и просмотра репортажей о различных мероприятиях в Internet. Оно позволяет, не покидая офис, совместно работать с группами, состоящими хоть из трех человек, хоть из тысяч.

Live Meeting предоставляет интерактивные средства, интегрируется с существующими системами и офисными приложениями, а также поддерживает привычный и простой в использовании интерфейс. Все это улучшает условия

коллективной работы с участием удаленных сотрудников и позволяет проводить эффективные совещания в компаниях любых масштабов. Конфиденциальность совещаний гарантируется тем, что Live Meeting всегда использует шифрование с применением SSL. Live Meeting предоставляет следующие возможности:

- задействовать функциональность Microsoft Office PowerPoint для поддержки презентаций с любыми видами анимации и эффектами перехода между слайдами;
- производить обмен любыми документами «на лету» для просмотра и правки. Средство просмотра документов высокого разрешения позволяет участникам совещания увеличивать или уменьшать масштаб показываемых документов без потери качества текста и графики;
- совместно управлять программным обеспечением на рабочем столе без потери обратной связи с участниками. Участники совещания могут запрашивать разрешение на такое управление, а докладчики (presenters) — быстро передавать управление любому участнику;
- использования набора средств интерактивного взаимодействия. Например, диспетчер вопросов (Question Manager) позволяет любому докладчику просматривать вопросы и отвечать на них как в индивидуальном порядке, так и всем участникам одновременно. К другим средствам относятся Real-Time Polls (опросы в режиме реального времени), Mood Indicator (индикатор настроения), Chat (чат), Annotations (комментарии), Whiteboard (электронная доска), Text Slide (текстовый слайд) и Web Slide (веб-слайд);
- рисовать от руки, делать пометки и набирать текст полностью имитирует условия работы на обычных совещаниях, где люди сидят лицом к лицу.

Интеграция с Microsoft Office и существующими системами. За счет интеграции с существующими системами Live Meeting позволяет вести совмест-

ную работу в удобной и привычной среде онлайновых совещаний или семинаров.

Как часть Microsoft Office System, Live Meeting позволяет созывать совещания непосредственно из приложений Microsoft Office, например из Outlook, Word, Excel. PowerPoint, Project и Visio, или из приложений мгновенного обмена сообщениями, в том числе из Microsoft Windows Messenger, MSN Messenger и Office Communicator. Организаторы могут планировать совещания с помощью Outlook (даже при работе в автономном режиме), посылать индивидуальные приглашения докладчикам и слушателям.

Клиенты BT, InterCall и MCI могут управлять вызовами для проведения голосовых конференций непосредственно из Live Meeting, что позволяет напрямую звонить участникам, включать или выключать звук на их телефонных линиях, выбирать нужных участников и т. д.

В качестве альтернативы голосовым конференциям Internet Audio Broadcast позволяет докладчикам транслировать потоковую аудиоинформацию через Internet, и тогда, чтобы участвовать в такой конференции, достаточно наличия динамиков на компьютере.

Привычные и простые в использовании средства для организаторов и участников совещаний. Поскольку Live Meeting полностью соответствует «букве и духу» Microsoft Office и упрощает наиболее распространенные задачи, связанные с совещаниями, участники со всего мира смогут легко пользоваться этой программой. А поскольку Live Meeting можно размещать в Web как службу конференций (conferencing service), вы получаете возможность легко и быстро развертывать Live Meeting за границы своего отдела или даже компании — хоть по всему миру.

Новички могут быстро войти в курс дела, используя краткие справочные материалы по наиболее распространенным задачам, связанным с проведением совещаний. Материалы совещания могут быть адаптированы в зависимости от роли участника.

Поддержка кулуаров совещания (Meeting Lobby). Отправляя гостей в кулуары, а не прямо на совещание, организатор совещания получает дополнительный механизм контроля участников и может разрешать или отклонять запросы входа на совещание.

Портал Live Meeting в интрасети позволяет автоматизировать ряд административных функций, в том числе создание и настройку учетных записей, сброс и смену паролей. Пользователи могут автоматически входить по своим учетным записям. Этот портал поставляется в комплекте с обучающими и справочными документами и обеспечивает широкие возможности в адаптации под структуру и требования конкретной интрасети.

Политики безопасности обеспечивают шифрование паролей и возможность назначать крайние сроки актуальности того или иного информационного наполнения, по истечении которых оно автоматически удаляется.

В этой теме были рассмотрены решения, предлагаемые компанией Microsoft по интегрированным средствам коммуникаций, рабочим областям коллективной деятельности, мгновенному доступу к информации и людям, автоматизации бизнес-процессов.

8.10 Темы рефератов

1. На базе каких решений может быть реализована поддержка индивидуальной и коллективной работы пользователей корпоративных ИС?
2. Поясните назначение интегрированных средств коммуникаций.
3. Поясните назначение рабочих областей коллективной деятельности.
4. Поясните назначение решения по мгновенному доступу к информации и людям.
5. Поясните назначение решения по автоматизации бизнес-процессов.
6. Приведите основные элементы ИТ-инфраструктуры, которые позволяют реализовать эффективную поддержку коллективной работы.
7. Поясните назначение Microsoft Exchange Server 2007.
8. Какие существуют роли для Microsoft Exchange Server 2007?
9. Поясните назначение для Microsoft Exchange Server 2007 роли «клиентский доступ».
10. Поясните назначение для Microsoft Exchange Server 2007 роли «граничный транспорт».
11. Поясните назначение для Microsoft Exchange Server 2007 роли «транспортный сервер-концентратор».
12. Поясните назначение для Microsoft Exchange Server 2007 роли «сервер почтовых ящиков».
13. Поясните назначение для Microsoft Exchange Server 2007 роли «единая система обмена сообщений».
14. Поясните особенности и преимущества взаимодействия Outlook и Exchange Server.
15. Поясните назначение и преимущества MS Office SharePoint Server 2007.
16. Поясните назначение и преимущества MS Windows SharePoint Services 2.0.
17. Что позволяет реализовать интеграция приложений MS Office с технологиями SharePoint?
18. Поясните назначение области задач общей рабочей области MS Office и SharePoint Server.
19. Поясните назначение сайтов рабочей области документов SharePoint Server.
20. Поясните возможности интеграции Office SharePoint Server 2007 и Outlook 2007.
21. Поясните назначение и преимущества MS Office InfoPath 2007.
22. Поясните назначение службы управления правами Windows – RMS.

23. Поясните назначение системы управления правами на доступ к информации в Office 2007 и SharePoint Server 2007.
24. Поясните назначение технологии защиты информации IRM.
25. Какие потребности предприятия и сотрудников ИС-службы удовлетворяет поддержка IRM в Office 2007.
26. Поясните назначение службы и основные преимущества MS Office – Live Communications Server.
27. Поясните назначение службы и перечислите основные возможности MS Office – Live Meeting.
28. Что позволяет получить предприятиям взаимодействие в режиме реального времени (RTC)?
29. Поясните назначение службы мгновенного обмена сообщениями (IM).

8.11 Литература

1. Решения Microsoft для повышения эффективности ИТ-инфраструктуры. Русская редакция Microsoft, М., 2005.

ЗАКЛЮЧЕНИЕ

В современных условиях сложность ИС предприятий возрастает, а методы и технологии эффективного управления их ИТ-инфраструктурой динамически развиваются. Это является следствием появления новых архитектурных подходов к построению ИС (сервис-ориентированные архитектуры/SOA, архитектуры, управляемые событиями/EDA), новых программных систем управления бизнес-процессами, ориентированных на процессное управление бизнесом, новых программных платформ, инструментальных средств и приложений, а также новых, более жестких требований пользователей в отношении предоставляемых им информационных сервисов. В результате развития методов и технологий создаются новые программные решения для управления ИТ-инфраструктурой предприятия.

Все это определяет остроту вопроса подготовки ИТ-менеджеров – специалистов по реализации эффективного управления ИТ-инфраструктурой предприятия. Достойной целью каждого специалиста, который предполагает работать в области управления ИТ-инфраструктурой предприятия является получение сертификата Service Manager’a. Квалификация ИТ-менеджера определяется статусом IT Service Manager’a, который на сегодняшний день является наивысшей ступенью в табели о рангах специалистов в области управления ИТ-сервисами. Сертификат Service Manager’a признается во всем мире как гарантия того, что его владелец обладает не только теоретическими знаниями в области управления услугами ИТ, но проявляет и качества менеджера, позволяющие ему эффективно внедрять установки, заложенные в библиотеке ITIL.

Этот курс лекций имел своей целью представить студентам обзор существующих подходов к эффективному управлению ИТ-инфраструктурой предприятия, акцентировать их внимание на важной и перспективной сфере деятельности ИТ-менеджера и тем самым помочь сделать первый шаг в достижении статуса IT Service Manager’a.

Навчальне електронне видання

КРУГЛЯК ЮРІЙ ОЛЕКСІЙОВИЧ

СУЧАСНА ТЕОРІЯ УПРАВЛІННЯ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Конспект лекцій

Видавець і виготовлювач
Одеський державний екологічний університет
вул. Львівська, 15, м. Одеса, 65016
тел./факс: (0482) 32-67-35
E-mail: info@odeku.edu.ua
Свідоцтво суб'єкта видавничої справи
ДК № 5242 від 08.11.2016