3.1. Методы системной диагностики организаций

Системная диагностика является начальным этапом стратегического ИТ-аудита, она базируется на архитектурной концепции и подразумевает диагностику как бизнес-слоя, так и системного слоя архитектуры. Бессмысленно осуществлять диагностику ИТ без выявления таких аспектов как степень покрытия бизнес-процессов существующими информационными системами, уровень удовлетворенности бизнес-пользователей имеющимися информационными технологиями и т.п.

3.1.1. Методы выявления и сбора информации

Этап выявления и сбора информации (обследование) является важнейшим и определяющим этапом диагностики, на его основе осуществляется вся последующая деятельность. Необходимо отметить, что каждый из участвующих в диагностике специалистов должен обследовать не более 2-3 бизнес-процессов организации для того, чтобы тщательно в них разобраться. Современная организация является сложной системой, состоящей из крупных взаимоувязанных подсистем, а возможности человека в одновременном охвате большого количества таких подсистем ограничены, поэтому здесь в полной мере должен использоваться принцип "разделяй и властвуй".

Во время обследования должны быть собраны следующие материалы:

1. стратегические цели и перспективы развития;
2. данные по организационно-штатной структуре организации;
3. информация о принятых технологиях деятельности;
4. результаты интервьюирования сотрудников (от руководителей до исполнителей нижнего звена);
5. предложения сотрудников по усовершенствованию деятельности;
6. нормативно-справочная документация;
7. данные по имеющимся в организации средствам и системам автоматизации.

Во время обследования должны быть собраны следующие материалы:

1. анкетирование
2. сбор документов
3. интервьюирование.

Анкетирование применяется на начальном этапе обследования и предваряет применение других методов. Анкеты позволяют составить грубое представление о процессах и информационных системах организации, что позволит спланировать первоначальное распределение работ группы аналитиков. Анкеты должны рассылаться руководителям структурных

подразделений и содержать графы для идентификации фамилии и должности анкетируемого, отдельно излагается просьба приложить шаблоны документов, с которыми работают сотрудники соответствующего подразделения. Список вопросов должен быть ограничен (не более 15-20) с тем, чтобы вся анкета не занимала более двух листов. Авторам приходилось видеть анкеты размером в 50 страниц, содержащие до 500 тщательно продуманных вопросов, но не встречался ни один человек, добровольно (а, следовательно, также тщательно и с пользой для дела) на них ответивший.

Примерный вариант анкеты приведен ниже:

- ФИО руководителя подразделения, телефон
- Координаты контактного лица (к кому в отсутствие или при занятости руководителя можно обращаться)
- Каковы (с позиций Вашего подразделения) должны быть цели внедрения ИТ
- Основные функции подразделения
- Какая информация поступает из других подразделений (заявки, запросы, отчеты и т.п.)
- Какая информация передается в другие подразделения
- Какая информация формируется ("рождается") в подразделении
- С какими внешними организациями (банк, заказчик, поставщик и т.п.) взаимодействует подразделение и какой информацией обменивается
- Физическое представление информационных потоков и хранилищ (документ, дискета, сеть, журнал, картотека и т.п.)
- Время хранения информации
- Штатная структура и квалификация кадров
- Техническое оснащение подразделения (компьютеры, сеть, модем и т.п.)
- Используемые программные продукты
- Подпись
- Приложение 1: Положение о подразделении
- Приложение 2: Набор шаблонов и форм основных документов, используемых подразделением

Сбор документов должен осуществляться на всех этапах проведения обследования, соответствующие формы, бланки и т.п. в дальнейшем сослужат неоценимую службу при разработке информационной модели предприятия (выявлении сущностей информационной модели и наполнении их атрибутикой). В дальнейшем целесообразно подготовить альбом форм с разбивкой их по бизнес-процессам. Такой альбом будет являться хорошим вспомогательным результатом диагностики - своими силами подобная работа обычно не проводится.

Интервьюирование является важнейшим и необходимым методом обследования, только с его помощью возможно разобраться во всех тонкостях применяемых в организации технологий. Современная организация является сложнейшей системой, как оно функционирует, не представляет ни один его сотрудник. Конечно, руководство владеет ситуацией в целом, с другой стороны, клерк досконально знает свою деятельность, но полной картины не имеет никто. И только интервьюирование представителей всех звеньев организационно-штатной структуры позволит выявить и, в дальнейшем, формализовать эту картину.

С другой стороны, интервьюирование является и наиболее сложной задачей: необходимо найти контакт с сотрудником и направить беседу в необходимое для целей диагностики русло.

Какую же информацию необходимо выявлять прежде всего во время интервьюирования? Во-первых, необходимо ограничить контекст диагностируемой системы - с этой целью должны быть выявлены все внешние объекты, с которыми диагностируемая организация взаимодействует, технологии взаимодействия со стороны организации, а также информационные (и, возможно, материальные) потоки, обеспечивающие эти взаимодействия. Во-вторых, должны быть детально выявлены реальные технологии работы организации - нормативно-справочная документация описывает их неполно. В-третьих, должны быть определены реальные функции подразделений и их взаимосвязи и взаимозависимости, поскольку положения о подразделениях такую информацию не содержат. В-четвертых, должны быть выявлены и специфицированы все информационные хранилища (в том числе и бумажные: картотеки, архивы и т.п.). В-пятых, должна быть оценена аппаратно-техническая база организации, а также исследовано работающее на ней программное обеспечение. Наконец, в-шестых, должны быть собраны статистические данные по бизнес-процессам организации: они со временем сослужат хорошую службу при анализе и выборе соответствующих информационных систем.

Опыт показывает, что длительность обследования, как правило, не зависит от размера организации (конечно, не имеются в виду территориально распределенные структуры) и составляет 5-7 рабочих дней (оптимальной группой специалистов численностью 6-8 человек). Однако, следует отметить, что часто возникает необходимость в проведении дополнительного обследования: какие-то моменты были не до конца выяснены, где-то возникли нестыковки, что-то было просто упущено. Обычно дополнительное обследование занимает 1-2 дня, и при его проведении очень полезно обсудить с интервьюированными уже наработанные результаты.

3.1.2. Диагностика информационных технологий

Результаты ИТ-диагностики должны быть ориентированы на руководителей организаций, которых, в первую очередь, интересует:

1. агрегация данных (а не обилие конкретных значений);
2. динамика, перспективы, тенденции (а не статика);
3. корпоративные решения (а не решения для подразделений);
4. минимальные затраты на поиск требуемой информации;
5. полнота и непротиворечивость информации;
6. аналитические срезы для поддержки принятия решений.

С другой стороны, результаты диагностики должны быть сопоставлены с современным уровнем развития информационных технологий, обеспечивающим следующие требования:

1. функциональную полноту;
2. масштабируемость – технология должна учитывать растущие потребности организации;
3. гибкость – технология должна настраиваться на изменения бизнес-процессов и внешней среды;
4. стандартизацию и мобильность – компоненты технологии должны функционировать на различных аппаратных и системных платформах, а также быть взаимозаменяемыми компонентами аналогичной функциональности;
5. информационную безопасность;
6. экономическую эффективность;
7. независимость – с одной стороны, организация не должна попадать в зависимость от поставщиков, с другой – не содержать собственного штата разработчиков.

С учетом вышесказанного, целью диагностики является оценка функциональности и техническая оценка имеющихся в организации ИТ на предмет перспектив дальнейшего развития и использования в составе корпоративной системы. В ходе диагностики должна быть получена характеристика состояния информатизации, включающая идентификацию существующих информационных систем и поддерживаемых ими бизнес-процессов, описание технологической архитектуры и используемых программно-технических средств, квалификацию пользователей и степень их удовлетворенности. Также должны быть рассмотрены вопросы взаимодействия со смежными системами, обеспечения информационной безопасности комплекса, аппаратного обеспечения, условий эксплуатации и состояния эксплуатирующей службы.

В качестве ресурсной части также необходимо рассмотреть квалификационный и численный состав всей ИТ-службы, а также ее структуру.

Текущее состояние информатизации должно быть проанализировано с точки зрения эффективности ее использования и перспектив развития. При этом должны быть идентифицированы пробелы в покрытии ИТ наиболее существенных бизнес-процессов, а также оценена степень соответствия существующей системы управления развитием и использованием информационных технологий основным требованиям развития бизнеса.

Итоговый документ (отчет по диагностике) должен содержать общую характеристику объекта аудита и техническую оценку по каждой из анализируемых систем. Общая характеристика объекта должна включать следующие разделы:

1. перечень имеющихся в организации прикладных программных комплексов и их общие описания;
2. структура ИТ-службы, ее цели и задачи, роли и численность персонала, обслуживающего каждую из программных систем;
3. состояние и состав эксплуатируемого системного программного обеспечения;
4. состояние и состав аппаратного обеспечения;
5. обеспечение информационной безопасности эксплуатируемых систем.

По каждой из анализируемых программных систем должно быть представлено:

1. состав подсистем и перечень функций системы;
2. схемы информационных взаимодействий с другими системами;
3. степень покрытия бизнес-процессов организации функциональностью системы;
4. направления и приоритетность развития функциональности системы;
5. оценка методологии создания системы;
6. оценка архитектурных решений, использованных в системе (общая оценка архитектуры, оценка информационной модели – схемы базы данных, оценка реализации базовых функциональных элементов);
7. оценка характеристик системы (масштабируемость системы, устойчивость к внесению изменений, степень интегрируемости системы в комплексное решение, степень документированности и отчуждаемости системы);
8. общая оценка системы и выводы о ее возможном использовании при построении корпоративной системы.

В качестве "путеводной карты" при проведении диагностики необходимо использовать требования к системе, аккумулированные в

Техническом задании на нее. Следует отметить, что требования разбиваются на две самостоятельные группы – требования к функциям и нефункциональные требования. В число последних входят:

1. правовые и законодательные требования;
2. качественные характеристики создаваемой системы, включая требования к ее практичности, надежности, производительности и возможностей поддержки;
3. требования по безопасности;
4. другие требования, например, касающиеся операционных систем и сред, совместимости и проектных ограничений.

Техническое задание (ТЗ) на систему (и, по необходимости, частные технические задания на ее компоненты – подсистемы) создается на основе ГОСТ 34.602-89 – "Техническое задание на создание автоматизированной системы" и включает в себя следующие основные разделы:

1. общие сведения
2. назначение и цели создания системы
3. характеристика объекта автоматизации
4. требования к системе
5. состав и содержание работ по созданию системы
6. порядок контроля и приемки системы
7. требования по подготовке и вводу в действие
8. требования к документированию
9. источники разработки
10. глоссарий.

Раздел Общие сведения содержит справочную информацию, включая полное наименование системы, условное обозначение системы, шифр (номер) договора, названия предприятий разработчика и заказчика (пользователя) системы и их реквизиты, перечень документов, на основании которых создается система, плановые сроки начала и окончания работы по созданию системы, сведения об источниках и порядке финансирования работ.

В разделе Характеристика объекта автоматизации приводятся общие сведения об организации согласно ее Уставу, перечень основных видов деятельности и бизнес-процессов, перечень бизнес-процессов, подлежащих автоматизации, характеристики видов обеспечения – организационного (организационные документы, организационная структура, нормативное обеспечение, квалификация персонала), методического, программного, технического, лингвистического, математического, правового и информационного.

Раздел Требования к системе включает следующие три подраздела: требования к системе в целом, требования к функциям, требования к видам обеспечения. В подразделе Требования к системе в целом содержатся:

1. перечень компонент (подсистем), их назначение и основные характеристики, требования к структуре системы;
2. требования к интеграции компонент (включая требования к способам и средствам связи для информационного обмена между компонентами системы и требования к функциональной интеграции в рамках бизнес-процессов);
3. требования к характеристикам взаимосвязей создаваемой системы со смежными системами, требования к ее совместимости, способы информационного обмена;
4. требования к режимам функционирования системы;
5. требования к диагностированию системы;
6. требования к численности и квалификации персонала системы и режиму его работы (включая обслуживающий персонал, пользователей и, по необходимости, частные требования по отдельным подсистемам);
7. требования к надежности и сохранности информации (технических средств, базового системного программного обеспечения, специализированного функционального программного обеспечения, средств защиты информации, средств резервного копирования информации и носителей резервных копий и т.п., включая требования к парированию отказов и восстановлению после аварийных ситуаций);
8. требования к безопасности и защите информации (включая перечень угроз информационной безопасности, требования к архитектуре и функциям обеспечения защиты информации, требования к организационному обеспечению защиты);
9. требования к стандартизации и унификации.

Подраздел Требования к функциям содержит требования к компонентам (подсистемам) системы в случае общего ТЗ или детальные функциональные требования в случае частного ТЗ на конкретную подсистему. Подраздел Требования к видам обеспечения включает детальное описание требований к математическому, информационному, лингвистическому, программному, техническому и организационному обеспечению.

Раздел Порядок контроля и приемки системы определяет виды, состав, объем и методы испытаний системы (предварительные испытания, опытная эксплуатация, приемочные испытания), требования к оформлению соответствующей документации (программы и методики испытаний, протокола предварительных испытаний, акта приемки в опытную эксплуатацию, журнала опытной эксплуатации, протокола приемочных испытаний, акта о приемке системы в промышленную эксплуатацию и др.), требования к организации приемки типовых компонент системы.

Раздел Требования по подготовке и вводу в действие описывает требования к организации работ по внедрению системы на предприятии, осуществляемые в связи с этим изменения в организационно-штатной структуре (прежде всего, по развитию ИТ-службы), нормативно-методическом обеспечении (регламенты подразделений, должностные инструкции сотрудников), персонале (комплектование и обучение), а также требования по внедрению типовых компонент системы.

Раздел Требования к документированию содержит состав комплекта документации и структуру документов по системе. По типовым компонентам, используемым в системе, предоставляется документация, входящая в комплект поставки. Эксплуатационная документация по разрабатываемым компонентам представляется в соответствии с требованиями ГОСТ 34.201-89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем", а также РД 50-34.698-90 "Методические указания. Информационная технология. Требования к содержанию документов". Возможный перечень этих документов приведен ниже:

1. Частное техническое задание - в соответствии с ГОСТ 34.602-89;
2. Описание информационного обеспечения - в соответствии с РД 50-34.698-90 п.5.3. (при необходимости);
3. Описание программного обеспечения - в соответствии с РД 50-34.698-90 п.6.1.;
4. Инструкцию по обозначениям и кодированию (при необходимости);
5. Альбом выходных форм;
6. Руководство администратора подсистемы;
7. Руководство пользователя - в соответствии с РД 50-34.698-90 п.3.4.;
8. Программа и методика испытаний - в соответствии с РД 50-34.698-90 п.2.14.

В перечень проектной документации также должны входить следующие документы, отражающие ход работ по проекту и обеспечивающие качество их выполнения:

1. План разработки (детализированный календарный план работ, содержащий виды работ, даты начала и завершения работ, отметки о выполнении работ);
2. План управления конфигурацией, содержащий описание следующих процессов управления проектной документацией: порядок разработки и хранения, порядок внесения изменений, ведение версионности, рассылка, порядок внутреннего согласования;

3. План качества проекта определяющий перечень и порядок проведения мероприятий, направленных на обеспечение качества (внутренние аудиты, тестирование, анализ результатов).

3.1.3. Аудит ИТ-процессов

Процессы управления информационными технологиями целесообразно рассматривать с точки зрения применения методов лучшего мирового опыта. С данных позиций наибольшее распространение получили следующие подходы к управлению ИТ: COBIT и ITIL/ITSM. Оба подхода ориентированы на удовлетворение потребностей бизнес-подразделений ИТ-службой, базируются на процессном подходе и оперируют измеримыми показателями деятельности.

Стандарт COBIT охватывает 34 ИТ-процесса, сгруппированных по следующим направлениям:

1. планирование и организация (10 процессов);
2. проектирование и внедрение (7 процессов);
3. эксплуатация и сопровождение (13 процессов);
4. мониторинг (4 процесса).

В совокупности перечисленные 4 группы содержат 302 объекта контроля. Все ресурсы, используемые объектами контроля, оцениваются с точки зрения их соответствия критериям, которые логически вытекают из бизнес-задач организации. Перечень этих критериев (эффективность, технический уровень, безопасность, целостность, пригодность, согласованность, надежность) совпадает с критериями оценки деятельности организации в целом. Для количественной и качественной оценки по критериям широко используется сравнение с лучшими мировыми показателями (на основании модели зрелости). Все это в совокупности обеспечивает полную, объективную и актуальную информацию о текущем состоянии ИТ, возможных решениях по изменению ситуации, перспективах и рисках их реализации.

В современных условиях происходит смещение акцентов в управлении ИТ, связанное с тем, что, фактически, подразделения организации потребляют не информационные системы, а ИТ-услуги, оценка которых должна производится не только по предоставляемой функциональности, но и по качеству обслуживания. При этом серьезно меняется модель управления ИТ, объектом управления становится услуга (а не информационная система),

целью – решение бизнес-задачи (а не обеспечение технических возможностей использования ИС).

Основные идеи этого подхода были воплощены в типовой модели бизнес-процессов ИТ-службы ITIL/ITSM (IT InfrastructureLibrary / IT ServiceManagement). Инициированный правительством Великобритании проект ITIL воплощает в себе основные принципы передовой практики организации ИТ-процессов, сформированные на основе анализа успешных решений (результаты этого анализа издаются в виде постоянно обновляемой библиотеки обобщенных ИТ-процессов). Разработанная компанией Hewlett-Packard на основе принципов ITIL модель ITSM представляет собой описание целостной системы взаимосвязанных ИТ-процессов.

Основные отличия управления ИТ-услугами от управления информационными системами заключаются в следующем:

1. бизнес формулирует требования к ИТ-услугам, а ИТ-служба обеспечивает их реализацию;
2. информационные системы для ИТ-службы имеют статус ресурса;
3. финансовый результат ИТ-службы определяется традиционным для бизнес-единицы образом: доходы за счет предоставления услуг минус расходы по их разработке, внедрению и сопровождению;
4. контроль деятельности ИТ-службы осуществляется на основе показателей, имеющих ценность с позиций клиента;
5. прозрачность деятельности ИТ-службы обеспечивается за счет формализации управленческих процедур в виде пакета документов, являющихся нормативной базой для всех ИТ-процессов.

Модель ITSM группирует ИТ-процессы в 5 тематических блоков:

1. Блок стратегического управления включает в себя следующие процессы:
    1. процесс анализа потребностей бизнеса, основной задачей которого является согласование целей и приоритетов между подразделениями предприятия и ИТ-службой;
    2. процесс управления клиентами, определяющий и согласовывающий требования по конкретным услугам, необходимым подразделениям;
    3. процесс разработки стратегии развития ИТ, организующий интегрированный корпоративный процесс по развитию информационных технологий для обеспечения их соответствия основным целям и потребностям бизнеса предприятия.
2. Блок планирования и управления услугами включает в себя следующие процессы:

1. процесс планирования услуг, основной задачей которого является проектирование спецификаций услуг;
2. процесс управления качеством сервиса, согласующий спецификации по составу и параметрам услуг и предоставляемые ИТ-службой ресурсы, а также создающий и согласующий регламентирующий взаимоотношения документ (договор) - Соглашение об уровне сервиса;
3. процесс управления инфраструктурой, включающий управление безопасностью, управление устойчивостью (способностью поддерживать услуги в чрезвычайных ситуациях), а также управление пропускной способностью;
4. процесс управления затратами, осуществляющий расчет издержек, пользовательских цен, а также поиск путей снижения затрат.

3. Блок разработки и внедрения услуг включает в себя следующие процессы:
    1. процесс разработки и тестирования, основной задачей которого является реализация услуги в соответствии с ее спецификациями;
    2. процесс ввода в эксплуатацию, обеспечивающий инфраструктуру функционирования новой услуги, осуществляющий подготовку справочных руководств и обучение специалистов по технической поддержки сервиса.
4. Блок оперативного управления включает в себя следующие процессы:
    1. процесс управления операциями, осуществляющий регламентные работы по поддержанию ИТ-инфраструктуры предприятия (функции системного администратора);
    2. процесс управления инцидентами, обеспечивающий восстановление услуги путем обработки инцидентов – событий, не являющихся частью нормального ее функционирования, приводящих (потенциально) к отказу услуги или снижению ее качества;
    3. процесс управления проблемами, предназначенный для устранения причин возникновения инцидентов.
5. Блок управления изменениями и конфигурациями включает в себя следующие процессы:
    1. процесс управления изменениями, задачами которого являются регистрация изменений, разрешение и отсев изменений, оценка воздействия изменений на ИТ-среду и т.п.;
    2. процесс управления конфигурацией, поддерживающий в актуальном состоянии данные по конфигурации информационных систем.

Переход к сервисной модели ИТ в 2002 году был отражен в стандарте BS 15000 "Управление ИТ-сервисом", недавно получившем официальный международный статус ISO 20000. Стандарт ISO 20000 конкретизирует

процессный подход, развиваемый в ITIL, применительно к менеджменту ИТ-услуг. Он определяет требования и взаимосвязанные процессы, необходимые для создания и эффективного использования системы менеджмента. Стандарт состоит из двух частей:

1. ISO 20000-1 "Information technology — Service management. Part 1: Specification" представляет собой описание требований к системе менеджмента ИТ-услуг и состоит из 10 разделов: Область применения, Термины и определения, Требования к системе управления, Планирование и применение управления услугой, Планирование и внедрение новых или измененных услуг, Процесс оказания услуг, Процессы взаимосвязей, Процессы разрешения проблем, Процессы контроля, Процесс управления релизом.
2. ISO 20000-2 "Information technology — Service management. Part 2: CodeofPractice" воплощает практические рекомендации по процессам, требования к которым сформулированы в первой части.

В конце 2000 года международный институт стандартов ISO на базе первой части британского BS 7799 "Управление информационной безопасностью. Практические рекомендации по управлению информационной безопасностью" (InformationSecurityManagement – CodeofPracticeforinformationSecurityManagement) разработал и выпустил международный стандарт менеджмента безопасности ISO/IEC 17799 "Информационные технологии. Управление информационной безопасностью" (InformationTechnology – InformationSecurityManagement). Стандарт является совокупностью практических правил по управлению информационной безопасностью, разработанных на основе передового мирового опыта и описывает:

1. требования к политике информационной безопасности;
2. организационные меры безопасности;
3. классификация и контроль информационных ресурсов;
4. кадровые аспекты информационной безопасности;
5. физическую защиту информационных ресурсов;
6. управление технологическим процессом;
7. управление доступом;
8. требования к безопасности компонентов систем в ходе их разработки, эксплуатации и сопровождения;
9. правила обеспечения непрерывности работы и восстановления;
10. требования к соответствию систем информационной безопасности нормативным и руководящим документам.

Следует отметить, что ISO 17799 не является техническим стандартом и не зависит от конкретного средства защиты или технологии. Он описывает концептуальные основы управления информационной безопасностью.

Кроме того, в международной практике широко применяется вторая часть стандарта BS 7799 – "Управление информационной безопасностью. Технические требования" (InformationSecurityManagement – RequirementsSpecification). Она определяет возможные меры по обеспечению защиты в соответствии с требованиями первой части стандарта и по предотвращению реализации угроз информационной безопасности (так называемое управление рисками информационной безопасности).