

Администрирование информационных систем

Смирнов Михаил
СПбГУ
2009

- Автоматизация
- Модель предприятия
- Архитектура предприятия
- Информационная безопасность

Введение

- повышение степени организационной и финансовой самостоятельности;
- выход на зарубежный рынок;
- стремление ряда западных компаний производить свои товары в России;
- завершение периода “островковой” автоматизации;
- возрастающая ориентация предприятий на бизнес-процессы, т.е. деятельности, имеющие ценность для клиента;
- появление на рынке как зарубежных, так и отечественных систем автоматизации, опыта их внедрения и использования и др.

Автоматизация – предпосылки

- единая информационная среда предприятия;
- режим реального времени;
- независимость от законодательства;
- интеграция с другими приложениями (в том числе с уже работающими на предприятии системами);
- поэтапное внедрение и т.п.

Ключевые слова

- **Короткое и “легкое” обследование предприятия** и дальнейшее лоббирование одной из интегрированных систем управления предприятием под красивыми лозунгами настройки и адаптации под конкретного заказчика
- **Детальное обследование предприятия** и разработка на его основе собственной системы управления, дублирующей существующие на предприятии технологии, что только усугубляет ситуацию

Автоматизация - подходы

От целей бизнеса к проекту		Объекты (что?)	Действия (как?)	Дислокация (где?)	Люди (кто?)	Время (когда?)	Мотивы (почему?)	
	Планировщик							Сфера действия
	Владелец предприятия							Модель предприятия
	Проектировщик							Системная модель
	Разработчик							Техническая модель
	Субподрядчик							Компоненты архитектуры
		Данные	Функции	Сеть	Организация	Расписание	Стратегия	
Элементы архитектуры предприятия								

Метод Захмана

	Люди (кто?)	Время (когда?)	Мотив (почему?)
Позиция планировщика Объектов/сфер а действия	<p>Перечень организаций, важных для бизнеса предприятия.</p> <p>Список организаций, с которыми данное предприятие несет определенную ответственность за выполняемую работу. Этот перечень имеет достаточно высокий уровень агрегирования и определяет масштабы или границы модели предприятия (см. строки ниже).</p>	<p>Перечень событий, существенных для бизнеса предприятия.</p> <p>Список событий, по которым предприятие отвечает во времени. Этот перечень также имеет достаточно высокий уровень агрегирования и определяет важные для предприятия масштабы или границы модели функционирования предприятия во времени (см. строки ниже).</p>	<p>Перечень бизнес-целей и бизнес-стратегий предприятия.</p> <p>Список главных целей, объектов, стратегий и критических факторов успеха бизнеса данного предприятия, определяющих мотивации его деятельности. Этот перечень, как и предыдущие, также имеет достаточно высокий уровень агрегирования и определяет важные для предприятия масштабы или границы модели предприятия (см. строки ниже).</p>

Пример описания

Позиция собственника	Модель потока работ.	Главное расписание (график).	Бизнес-план.
Модель предприятия	<p>Данная модель определяет обязанности и спецификации работ, выполняемых на данном предприятии. Обычно организационная диаграмма отражает распределение обязанностей, а остальные сопутствующие документы описывают процессы производства изделий. Чтобы быть окончательно законченной организационная диаграмма должна дополняться процессами по производству изделий, включая управление работами, координацию работы и собственно проведение работ.</p>	<p>Модель бизнеса, представленная во времени. Отражает текущее состояние во времени, а также основные предшествующие события. Обычно используется одна из двух наиболее распространенных нотаций модели: сетевые графики в виде ПЕРТ-диаграмм и модель Senge или интеллектуальная модель.</p>	<p>Бизнес-план моделирует бизнес-цели и стратегию предприятия, которые составляют основную мотивацию для деятельности предприятия и принятия решений. Хотя теоретически бизнес-план в первую очередь ориентирован на проблемы управления, в нем должно уделяться значительное внимание вопросам мотивации деятельности.</p>

Пример-2

Позиция проектировщика Модель информационной системы	Архитектура человеческого интерфейса. Логические системы, отражающие поток работ, который в свою очередь включает спецификации ролей и ответственности участников: менеджмент, администрацию, работников высокой квалификации (или знание-ориентированных работников), разработчиков, специалистов по маркетингу и т.д., а также логические спецификации процессов разработки изделий (например, текст, графика, видео и т.д.).	Структура рабочих процессов. Системы логических спецификаций, привязанных к определенным моментам времени (т.е., события системы) и периоды времени, необходимые рабочие процессы (т.е., циклы обработки). Эта модель описывает события, происходящие в системе, как триггерные переходы от одного допустимого состояния (т.е. «точка во времени») к другому состоянию и динамика этого перехода. Такая модель обычно представляется в виде диаграммы состояний (например, по методологии SSADM, разработанной в Великобритании) или в нотациях объектно-ориентированной диаграммы состояния Harel. Помимо этого могут использоваться и сети Петри, также позволяющие отобразить последовательность выполнения процессов.	Бизнес-правила. Логическая модель реализации бизнес-правил предприятия в терминах намерений и ограничений. В настоящее время общепринятой нотации записи бизнес-правил не существует.
---	---	---	---

Пример-3

<p>Позиция разработчика. Технологическая модель</p>	<p>Представление архитектуры.</p> <p>Данный документ является физическим выражением потока работ, осуществляемых на предприятии конкретными служащими, а также их эргономические требования и форматы представления результатов работы.</p>	<p>Структура контроля.</p> <p>Представление физических событий, происходящих в системе и циклов обработки. Оно должно содержать контрольные точки моментов передачи «управления» от одного обрабатывающего модуля к другому.</p>	<p>Правила проекта.</p> <p>Правила проекта являются физической реализацией спецификации бизнес-правил. Эти правила, представленные в виде соответствующих входящих элементов отражаются в моделях данных, в процедурных кодах и в детализированных спецификациях технических требований.</p>
--	--	---	---

Пример-4

Позиция субподрядчиков	Архитектура системы защиты	Синхронизация.	Спецификации.
<p>Детализированные спецификации</p>	<p>В соответствии с контекстом технических требований к выполнению потока работ идентифицируется перечень служащих предприятия, которые могут иметь доступ к системе или к рабочим процессам.</p>	<p>Содержит определение разрешенных прерываний и временные циклы процессов.</p>	<p>Содержат контекстные технические требования, предъявляемые со стороны бизнес-правил.</p>

Пример-5

- Двигатели архитектуры - внешние стимулы, которые побуждают архитектуру предприятия к изменениям.
- Стратегические направления - Гарантирует, что все принятые решения согласуются с общим направлением развития архитектуры.
- Текущая Архитектура - Представляет текущее состояние предприятия.
- Целевая архитектура - Представляет целевое (намечаемое) состояние для предприятия в рамках контекста стратегических направлений.
- Переходные процессы – Фиксируют изменения, сопровождающие переход от текущей архитектуры к целевой архитектуре, происходящий в соответствии со стандартами.
- Архитектурные сегменты - Сосредотачиваются на подгруппах или на отдельных предприятиях в пределах общего числа предприятий.
- Архитектурные модели - Обеспечивают документацию и базу для управления и осуществления изменений в предприятии.
- Стандарты - Включают стандарты (часть которых может быть сделана обязательными), руководства и накопленный передовой опыт, которые, в первую очередь, направлены на обеспечение интероперабельности

Уровни архитектуры

Подход к обеспечению ИБ должен быть комплексным, сочетающим меры следующих уровней:

- законодательного (законы, нормативные акты, стандарты);
- административного (действия общего характера, предпринимаемые руководством организации);
- процедурного (меры безопасности, реализуемые персоналом);
- программно-технического (конкретные технические меры).

Информационная безопасность

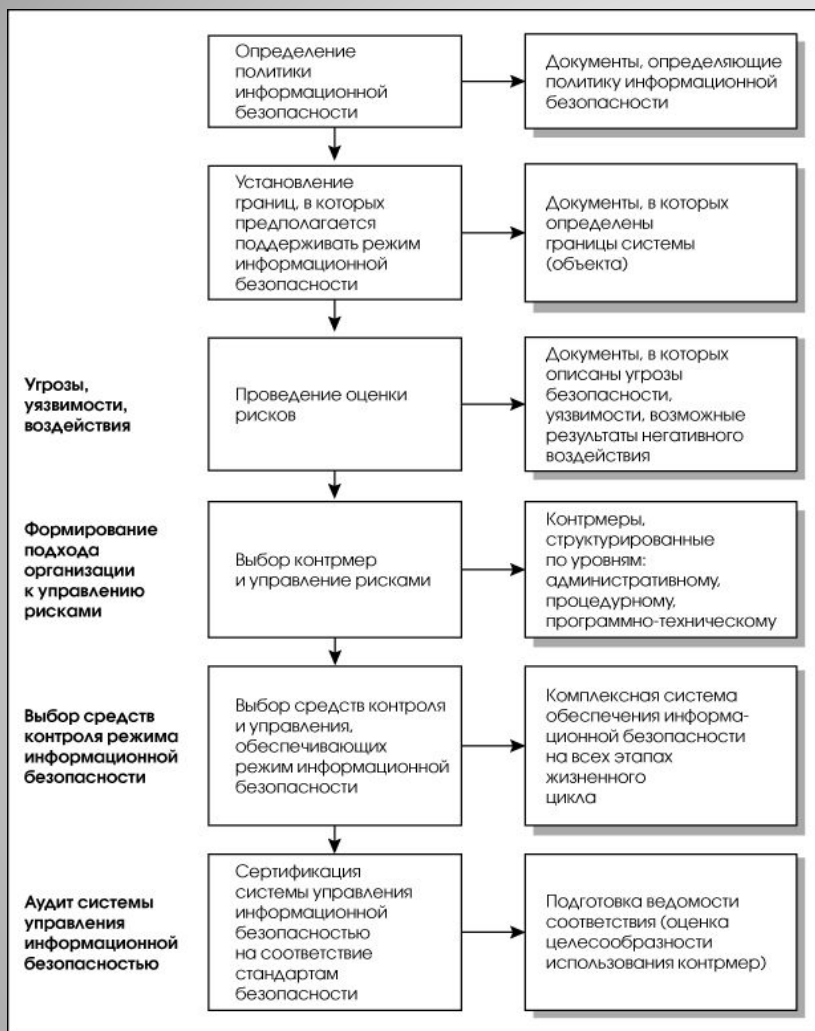
- Режим ИБ в подобных системах обеспечивается:

- на процедурном уровне — путем разработки и выполнения разделов инструкций для персонала, посвященных ИБ, а также мерами физической защиты;
- на программно-техническом уровне — применением апробированных и сертифицированных решений, стандартного набора контрмер: резервное копирование, антивирусная защита, парольная защита, межсетевые экраны, шифрование данных и т.д.

ИБ в ИТ



Требования к ИБ



- Определение политики ИБ.
- Определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания.
- Оценка рисков.
- Управление рисками.
- Выбор контрмер, обеспечивающих режим ИБ.
- Аудит системы управления ИБ.

Обеспечение ИБ. Основные этапы

- Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:
 - управление доступом к средствам вычислительной техники (СВТ), программам и данным;
 - антивирусную защиту;
 - вопросы резервного копирования;
 - проведение ремонтных и восстановительных работ;
 - информирование об инцидентах в области ИБ.
- Определение подходов к управлению рисками: хватает базового уровня защищенности или требуется проводить полный анализ рисков.
- Структуризацию контрмер по уровням.
- Порядок сертификации на соответствие стандартам в области ИБ.

Определение политики ИБ

- Структура организации. Описание существующей структуры и изменений, которые предполагается внести в связи с разработкой (модернизацией) автоматизированной системы.
- Размещение средств СВТ и поддерживающей инфраструктуры.
- Ресурсы информационной системы, подлежащие защите. Рекомендуется рассмотреть ресурсы автоматизированной системы следующих классов: СВТ, данные, системное и прикладное ПО. Все ресурсы представляют ценность с точки зрения организации. Для их оценки должна быть выбрана система критериев и методология получения оценок по этим критериям.
- Технология обработки информации и решаемые задачи. Для решаемых задач должны быть построены модели обработки информации в терминах ресурсов.

**Определение сферы (границ)
системы управления ИБ и
конкретизация целей ее создания**

- Поставлена задача оценки рисков
- Определены требования к методике оценки рисков.
- Минимальным требованиям к режиму ИБ соответствует базовый уровень ИБ.
 - Область использования - типовые проектные решения.
- Повышенные требования
 - когда нарушения режима ИБ чреваты тяжелыми последствиями

Постановка задачи оценки рисков

- Регистрация удачных и неудачных попыток входа в систему;
- Регистрация изменений, вносимых в процессе администрирования базы данных;
- Использование системных сервисов;
- Отправка сообщения администратору безопасности при попытке несанкционированного доступа к регистрационным журналам, процесс-нарушитель должен быть блокирован;
- Записи о событиях в регистрационном журнале должны содержать информацию о типе (классе) события, дате и времени начала и окончания, удачном/неудачном завершении, пользователе.

Минимальные требования (на примере протоколирования)

- определить ценность ресурсов;
- к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;
- оценить вероятности угроз;
- определить уязвимости ресурсов.

Повышенные требования к режиму ИБ

- уменьшение риска;
- уклонение от риска;
- изменение характера риска (перенос риска);
- принятие риска.

Управление рисками

- стратегия управления.

- Выбор контрмер, обеспечивающих режим ИБ
 - комплекс мер, структурированных по уровням (организационному, программно-техническому) и отдельным аспектам безопасности.
- Аудит системы управления ИБ
 - проверка соответствия выбранных контрмер декларированным в политике безопасности целям
 - В результате должен быть создан документ "Ведомость соответствия", в котором содержится анализ эффективности контрмер. Основные разделы этого документа:
 - границы проводимого аудита;
 - методика оценки;
 - соответствие существующего режима ИБ требованиям организации и используемым стандартам;
 - несоответствия и их категории;
 - общие замечания, выводы, рекомендации.

Результат работы с рисками