Лекция 2
«**Проектная документация на ИС**»

Овчинников П.Е.
МГТУ «СТАНКИН»,
ст.преподаватель кафедры ИС

11.09.2017

Документация на АС

ГОСТ 34.601-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

1. Формирование требований к АС
2. Разработка концепции АС
3. Техническое задание
4. Эскизный проект
5. Технический проект
6. Рабочая документация
7. Ввод в действие
8. Сопровождение АС

РД 50-34.698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов

1.1. Требования к содержанию документов, разрабатываемых при создании АС, установлены настоящими указаниями, а также соответствующими государственными стандартами Единой системы программной документации (ЕСПД), Единой системы конструкторской документации (ЕСКД), Системы проектной документации для строительства (СПДС) и ГОСТ 34.602.

Виды и комплектность документов регламентированы ГОСТ 34.201.

ГОСТ 34.601-90
РД 50-34.698-90

Документация НИР

ГОСТ 7.32-2001 СИБИД. Отчет о научно-исследовательской работе. Структура и правила оформления

Структурными элементами отчета о НИР являются:
- **титульный лист;**
- **список исполнителей**;
- **реферат;**
- содержание;
- определения;
- обозначения и сокращения;
- **введение;**
- **основная часть;**
- **заключение;**
- список использованных источников;
- приложения.

Обязательные структурные элементы выделены полужирным шрифтом. Остальные структурные элементы включают в отчет по усмотрению исполнителя НИР с учетом требований разделов 5 и 6.

ГОСТ 7.32-2001

Документация на АС

ГОСТ 34.201-89 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем

1.3. Виды документов, разрабатываемых на стадиях "Эскизный проект", "Технический проект", "Рабочая документация", приведены в табл.1.

Вид документа	Код документа	Назначение документа
Ведомость	В	Перечисление в систематизированном виде объектов, предметов и т.д.
Схема	С	Графическое изображение форм документов, частей, элементов системы и связей между ними в виде условных обозначений
Инструкция	И	Изложение состава действий и правил их выполнения персоналом
Обоснование	Б	Изложение сведений, подтверждающих целесообразность принимаемых решений
Описание	П	Пояснение назначения системы, ее частей, принципов их действия и условий применения
Конструкторский документ		По ГОСТ 2.102
Программный документ		По ГОСТ 19.101

ГОСТ 34.201-89

Документация на АС

ГОСТ 34.201-89 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем

ГОСТ 34.201-89

Виды обеспечения АС

ГОСТ 34.003-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

1.1 **автоматизированная система;** АС:
Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.3 **организационное обеспечение автоматизированной системы**
Совокупность документов, устанавливающих организационную структуру, права и обязанности пользователей и эксплуатационного персонала АС в условиях функционирования, проверки и обеспечения работоспособности АС

2.4 **методическое обеспечение автоматизированной системы**
Совокупность документов, описывающих технологию функционирования АС, методы выбора и применения пользователями технологических приемов для получения конкретных результатов при функционировании АС

2.5 **техническое обеспечение автоматизированной системы**
Совокупность всех технических средств, используемых при функционировании АС

ГОСТ 34.003-90

Виды обеспечения АС

ГОСТ 34.003-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

2.6 **математическое обеспечение автоматизированной системы**
Совокупность математических методов, моделей и алгоритмов, примененных в АС

2.7 **программное обеспечение автоматизированной системы**
Совокупность программ на носителях данных и программных документов, предназначенная для отладки, функционирования и проверки работоспособности АС

2.8 **информационное обеспечение автоматизированной системы**
Совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в АС при ее функционировании

2.9 **лингвистическое обеспечение автоматизированной системы**
Совокупность средств и правил для формализации естественного языка, используемых при общении пользователей и эксплуатационного персонала АС с комплексом средств автоматизации при функционировании АС

ГОСТ 34.003-90

Виды обеспечения АС

ГОСТ 34.003-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

2.10 **правовое обеспечение автоматизированной системы**
Совокупность правовых норм, регламентирующих правовые отношения при функционировании АС и юридический статус результатов ее функционирования.

Примечание. Правовое обеспечение реализуют в организационном обеспечении АС.

2.11 **эргономическое обеспечение автоматизированной системы**
Совокупность реализованных решений в АС по согласованию психологических, психофизиологических, антропометрических, физиологических характеристик и возможностей пользователей АС с техническими характеристиками комплекса средств автоматизации АС и параметрами рабочей среды на рабочих местах персонала АС

ГОСТ 34.003-90

Информационная безопасность

ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

Информационная безопасность включает в себя три основных измерения:
- **конфиденциальность**,
- **доступность** и
- **целостность**.

С целью обеспечения длительного непрерывного успеха в бизнесе и уменьшения нежелательных воздействий информационная безопасность предусматривает применение соответствующих мер безопасности, которые включают в себя рассмотрение широкого диапазона угроз, а также управление этими мерами.

Информационная безопасность достигается посредством применения соответствующего набора средств управления, определенного с помощью **процесса управления рисками** и управляемого с использованием СМИБ, включая политику, процессы, процедуры, организационные структуры, программное и аппаратное обеспечение, чтобы защитить идентифицированные информационные активы.

Стандарты в области ИБ
http://docs.cntd.ru/document/1200102762

Информационная безопасность

ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

2.19 **информационная безопасность (information security):** сохранение конфиденциальности (2.9), целостности (2.25) и доступности (2.7) информации.
Примечание - Также сюда могут быть включены другие свойства, такие как подлинность (2.6), подотчетность (2.2), неотказуемость (2.27) и достоверность (2.33).

2.9 **конфиденциальность (confidentiality):** Свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов (2.31).
2.25 **целостность (integrity):** Свойство сохранения правильности и полноты активов (2.3).
2.7 **доступность (availability):** Свойство быть доступным и готовым к использованию по запросу авторизованного субъекта.
2.6 **подлинность (authenticity):** Свойство, гарантирующее, что субъект или ресурс идентичен заявленному.
2.2 **подотчетность (accountability):** Ответственность субъекта за его действия и решения.
2.27 **неотказуемость (non-repudiation):** Способность удостоверять имевшее место событие (2.15) или действие и их субъекты так, чтобы это событие (2.15) или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение.
2.33 **достоверность (reliability):** Свойство соответствия предусмотренному поведению и результатам.

Стандарты в области ИБ
http://docs.cntd.ru/document/1200102762

Кибербезопасность

ГОСТ Р МЭК 62443-2-1-2015 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики

Организации, применяющие IACS (системы промышленной автоматики и контроля), начали применять готовые коммерческие технологии (COTS), разработанные для бизнес-систем, используемых в их повседневных процессах, в результате чего возрос риск кибератак, направленных на оборудование IACS. Как правило, такие системы в среде IACS по многим причинам не настолько робастны, как системы, специально спроектированные как IACS для подавления кибератак. Подобные недостатки могут привести к последствиям, которые отразятся на уровне охраны труда, промышленной безопасности и охраны окружающей среды (HSE).

3.1.13 **система управления кибербезопасностью** (cyber security management system): Программа, разработанная организацией для поддержания кибербезопасности всех имущественных объектов данной организации на заданном уровне конфиденциальности, целостности и доступности, независимо от того, относятся ли данные объекты к бизнес-процессам или системам IACS организации.

http://docs.cntd.ru/document/1200102762

Аутентификация

ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

2.5 **аутентификация (authentication):** Обеспечение гарантии того, что заявленные характеристики объекта правильны.

Р 50.1.056-2005 Техническая защита информации. Основные термины и определения

3.5.11 **аутентификация (подлинности субъекта доступа):** Действия по проверке подлинности субъекта доступа в информационной системе

ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации

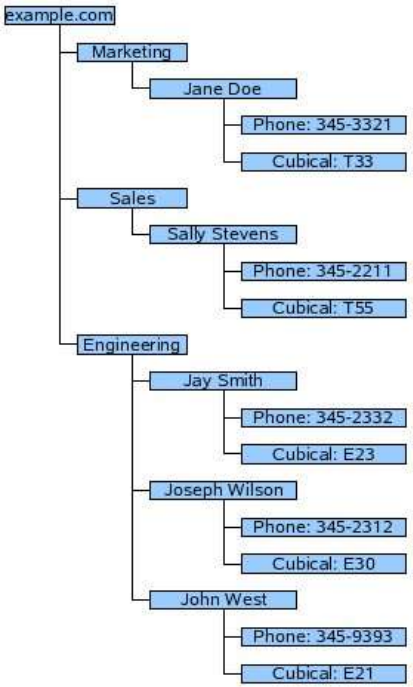
3.6 **биометрическая идентификация:** Преобразование совокупности примеров биометрических образов человека, позволяющее описать их стационарную и случайную составляющие, например, в виде математического ожидания и дисперсий контролируемых параметров или, например, в виде параметров обученной сети искусственных нейронов

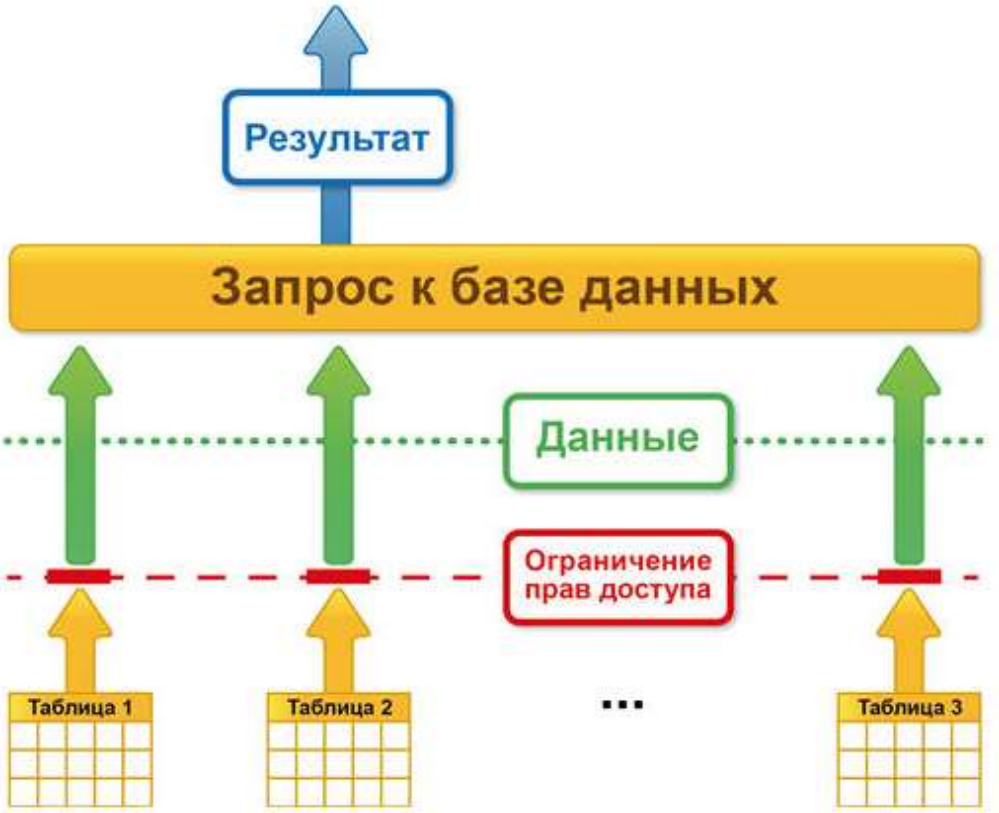
http://docs.cntd.ru/document/1200102762
http://docs.cntd.ru/document/1200048922
Биометрическая аутентификация

Авторизация

Р 50.1.056-2005 Техническая защита информации. Основные термины и определения

3.5.10 **санкционирование доступа; *авторизация*:** Предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ





http://docs.cntd.ru/document/1200044768
http://v8.1c.ru/overview/Term_000000579.htm
https://ru.wikipedia.org/wiki/Active_Directory

Угрозы, атаки, уязвимости

ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

2.45 **угроза** (threat): Возможная причина нежелательного инцидента, который может нанести ущерб системе или организации.

2.4 **атака** (attack): Попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к **активу** (2.3) или его несанкционированного использования.

2.46 **уязвимость** (vulnerability): Слабое место **актива** (2.3) или **меры и средства контроля и управления** (2.10), которое может быть использовано **угрозой** (2.45).

http://docs.cntd.ru/document/1200102762

Нарушители

Модель нарушителя — (в информатике) абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

Модель нарушителя определяет:
• **категории** (типы) нарушителей, которые могут воздействовать на объект
• **цели**, которые могут преследовать нарушители каждой категории, возможный количественный состав, используемые инструменты, принадлежности, оснащение, оружие и проч.
•типовые **сценарии** возможных действий нарушителей, описывающие последовательность (алгоритм) и способы действий групп и отдельных нарушителей

Модель нарушителей может иметь разную степень детализации.
• **Содержательная модель** нарушителей отражает систему принятых руководством объекта, ведомства взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий, преследуемые цели и общий характер действий в процессе подготовки и совершения акций воздействия.
• **Сценарии воздействия** нарушителей определяют классифицированные типы совершаемых нарушителями акций с конкретизацией алгоритмов и этапов, а также способов действия на каждом этапе.
• **Математическая модель воздействия** нарушителей представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей

Модель нарушителя

Защита

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

защита информации; ЗИ: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

• **правовая защита информации:** Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

• **техническая защита информации;** ТЗИ: Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

• **криптографическая защита информации:** Защита информации с помощью ее криптографического преобразования

• **физическая защита информации:** Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

http://docs.cntd.ru/document/1200058320

Парирование

ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

3.6.1 **обеспечение информационной безопасности** организации; обеспечение ИБ организации: Деятельность, направленная на **устранение (нейтрализацию, парирование)** внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз.

3.1.15 **критически важная система информационной инфраструктуры;** *ключевая система информационной инфраструктуры*; КСИИ: Информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление или информационное обеспечение критическим объектом или процессом, или используется для официального информирования общества и граждан, нарушение или прерывание функционирования которой (в результате деструктивных информационных воздействий, а также сбоев или отказов) может привести к чрезвычайной ситуации со значительными негативными последствиями.

3.1.16 **критический объект:** Объект или процесс, нарушение непрерывности функционирования которого может нанести значительный ущерб.

http://docs.cntd.ru/document/1200075565
http://cyberrus.com/wp-content/uploads/2015/01/vkb_05_01.pdf

Доверенная среда

ГОСТ Р 54583-2011 Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Основы доверия к безопасности информационных технологий. Часть 3 Анализ методов доверия

2.4 **орган обеспечения доверия** (assurance authority): Лицо или организация, уполномоченные принимать решения (например, по выбору, спецификации, принятию, контролю за исполнением), связанные с обеспечением доверия к объекту, что однозначно приводит к формированию уверенности в безопасности объекта.

2.9 **среда** (environment): Условия, в которых выполняются процессы жизненного цикла (то есть люди, оборудование и другие ресурсы), и связанные с этими условиями характеристики доверия (например, репутация, сертификация).

Примечание - В настоящем стандарте "доверие к среде" означает то же, что "доверие к продукту" и "доверие к процессу".

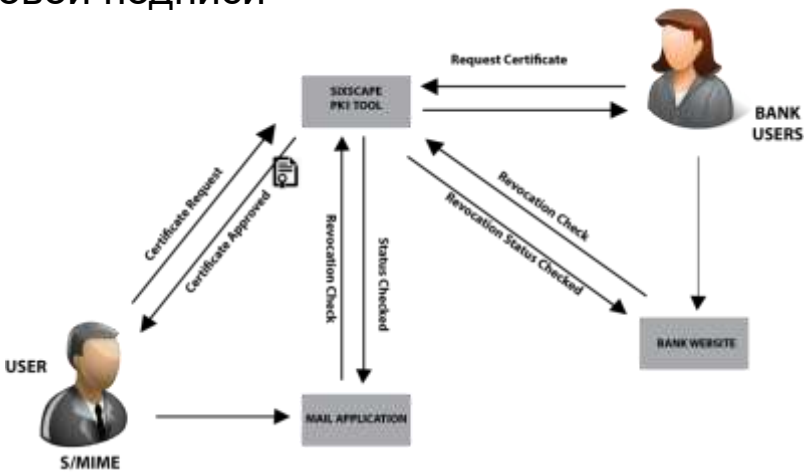
http://docs.cntd.ru/document/gost-r-54583-2011

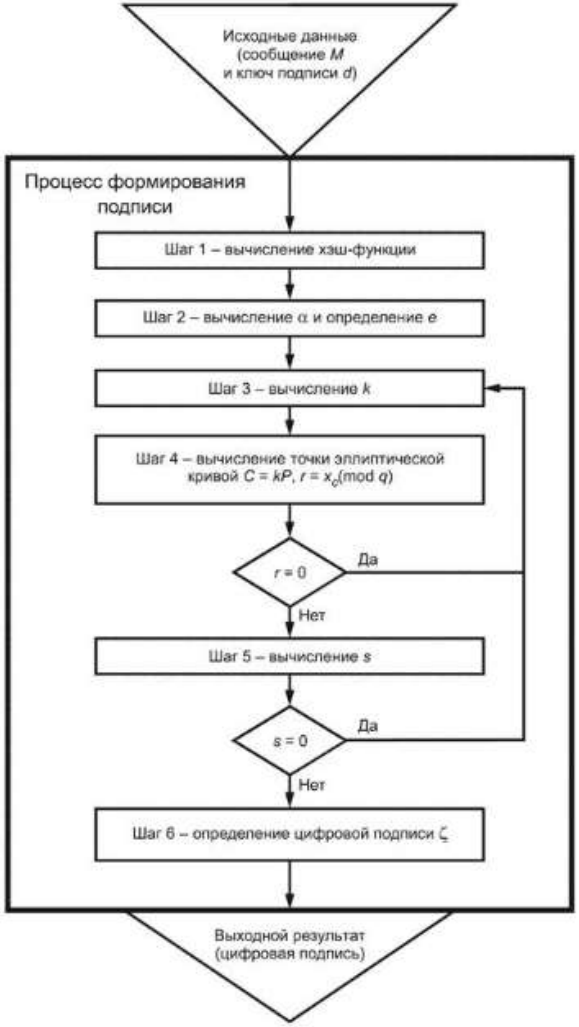
Криптография

ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ключ подписи (signature key): Элемент секретных данных, специфичный для субъекта и используемый только данным субъектом в процессе формирования цифровой подписи

ключ проверки подписи (verification key): Элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи





http://docs.cntd.ru/document/1200095034
PKI

Лекция 2
«Проектная документация на ИС»

Часть 2.

Основные стандарты в области разработки моделей и алгоритмов информационных процессов автоматизированных систем

Национальные, межгосударственные и международные стандарты

1. Схемы алгоритмов, программ, данных и систем (ГОСТ 19.701-90, ИСО 5807-85)
2. UML
3. Операграммы (ГОСТ Р 51167-98, ГОСТ Р 51168-98)
4. Функциональные модели SADT (Р 50.1.028-2001, IDEF0)

1. Схемы алгоритмов, программ, данных и систем

Схемы	Назначение
Схемы данных	Отображают путь данных, определяют этапы обработки и применяемые носители данных.
Схемы программ	Отображают последовательность операций в программе .
Схемы работы системы	Отображают управление операциями и поток данных в системе.
Схемы взаимодействия программ	Отображают путь активации программ и взаимодействий с соответствующими данными.
Схемы ресурсов системы	Отображают конфигурацию блоков данных и обрабатывающих блоков, которая требуется для решения задачи или набора задач.

Схема данных

Схема работы программы

Схема работы системы

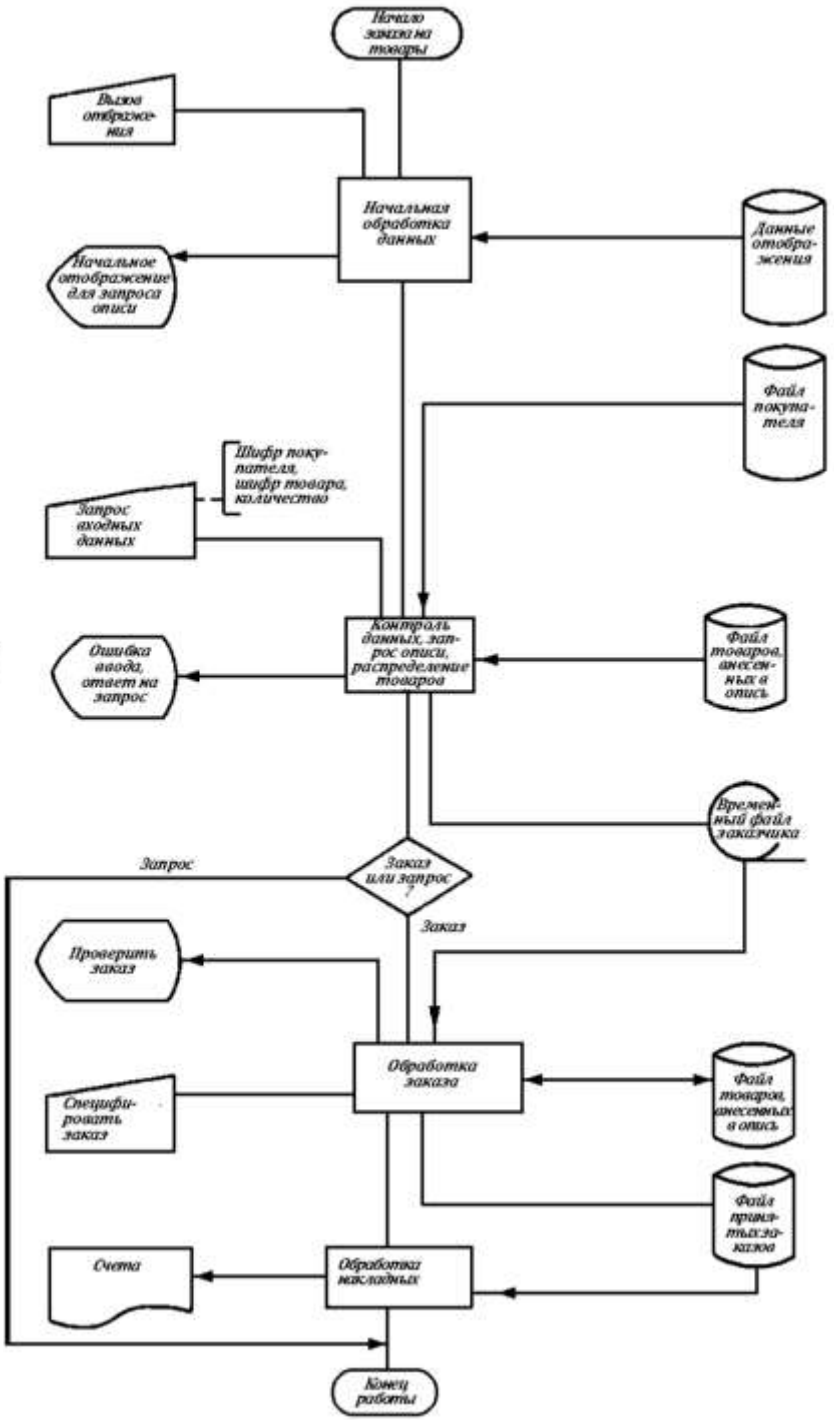


Схема взаимодействия программ

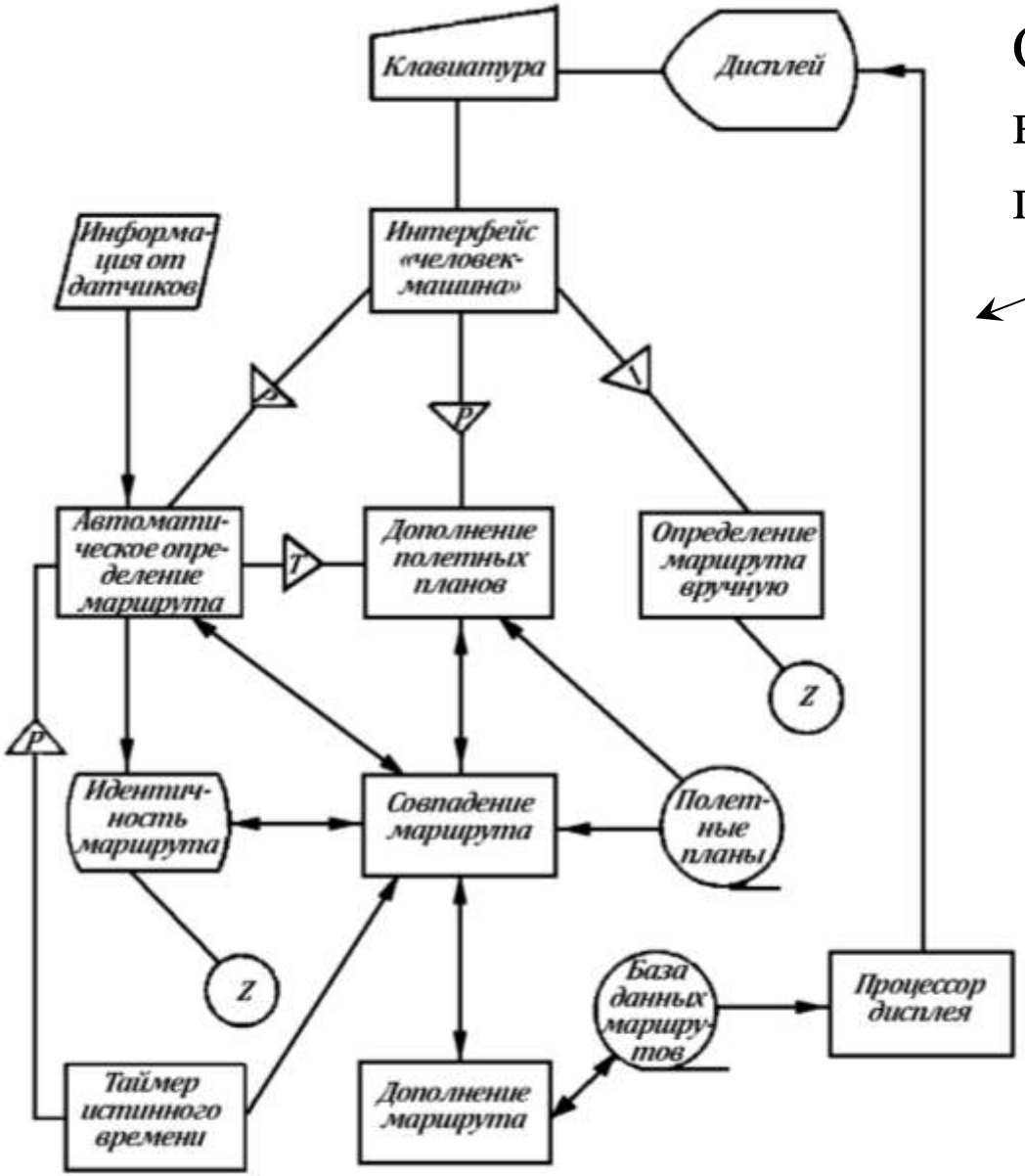
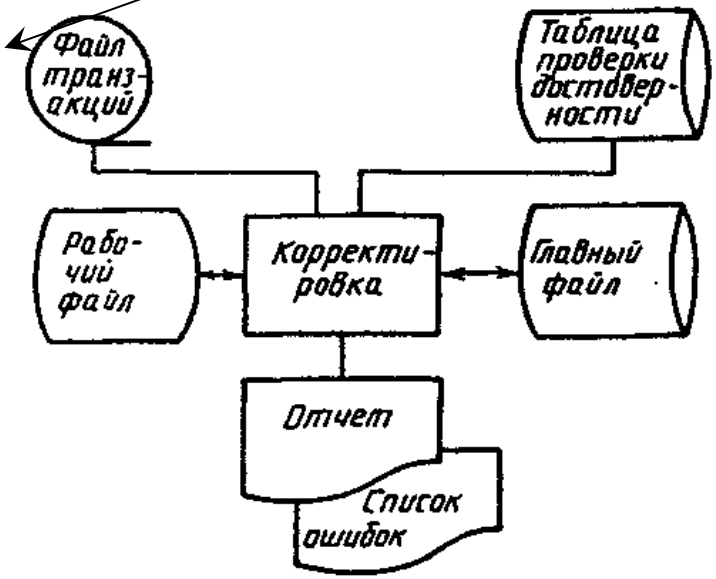


Схема ресурсов системы



2. UML


Диаграммы
Структурные
Классов
Компонентов
Составной структуры
Взаимодействия
Пакетов
Развёртывания
Объектов
Профилей
Поведения
Деятельности
Состояний
Прецедентов
Взаимодействия
Коммуникации
Обзора взаимодействия
Последовательности
Синхронизации

Диаграмма классов

Классы, их атрибуты, операторы, взаимосвязь

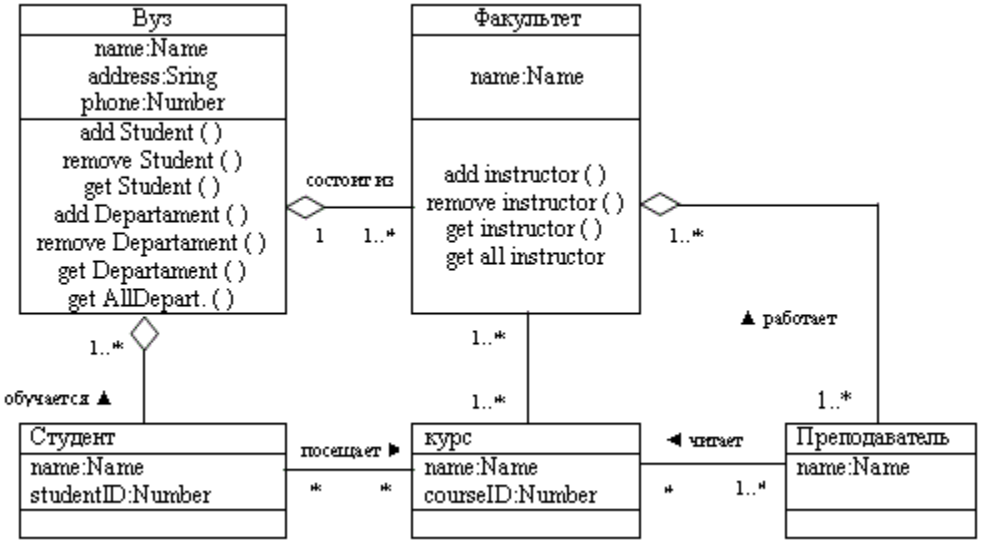


Диаграмма составной структуры

Внутренняя структура классов

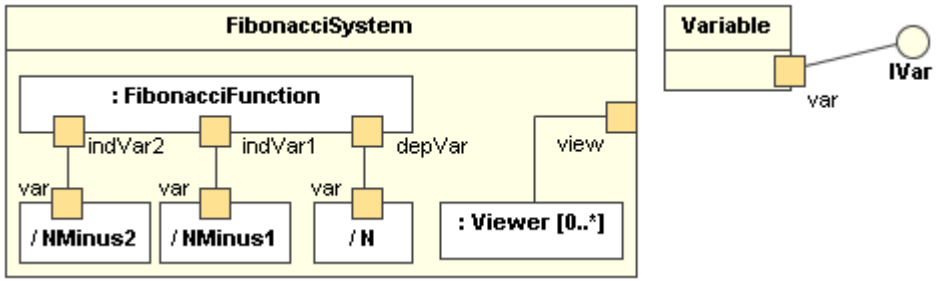


Диаграмма компонентов

Компоненты системы, их взаимосвязь

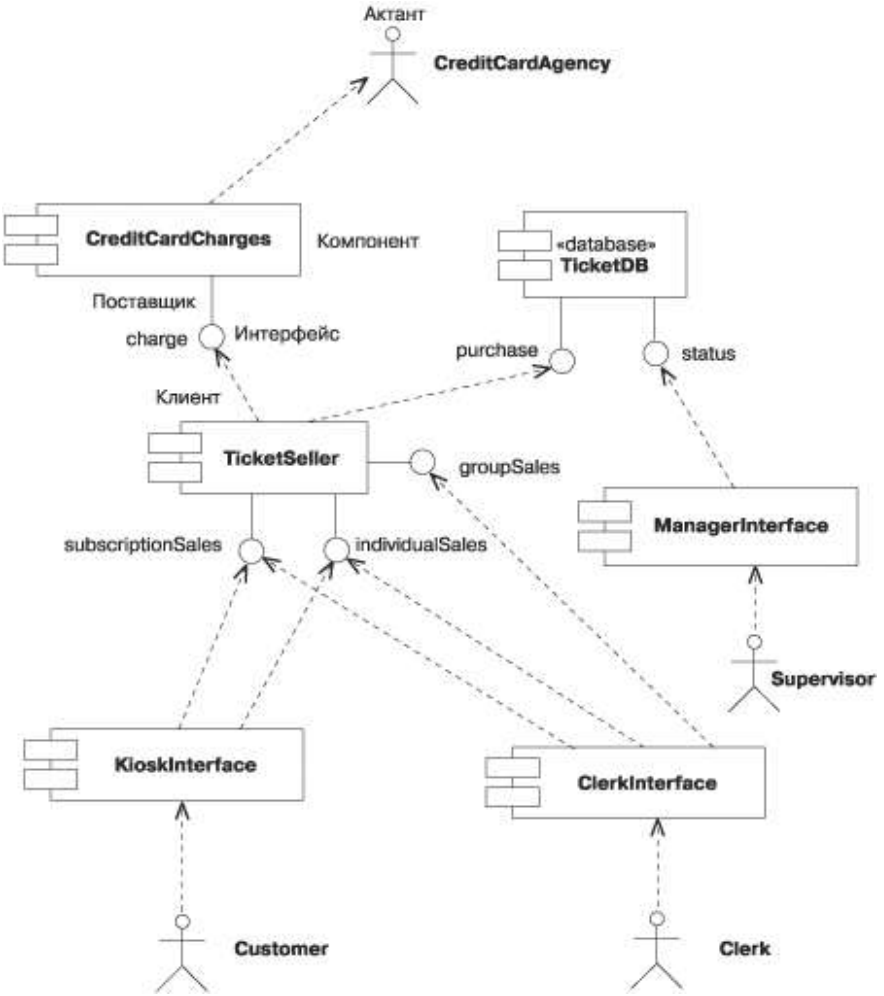


Диаграмма взаимодействия

Объекты, участвующие во взаимодействии, их связи

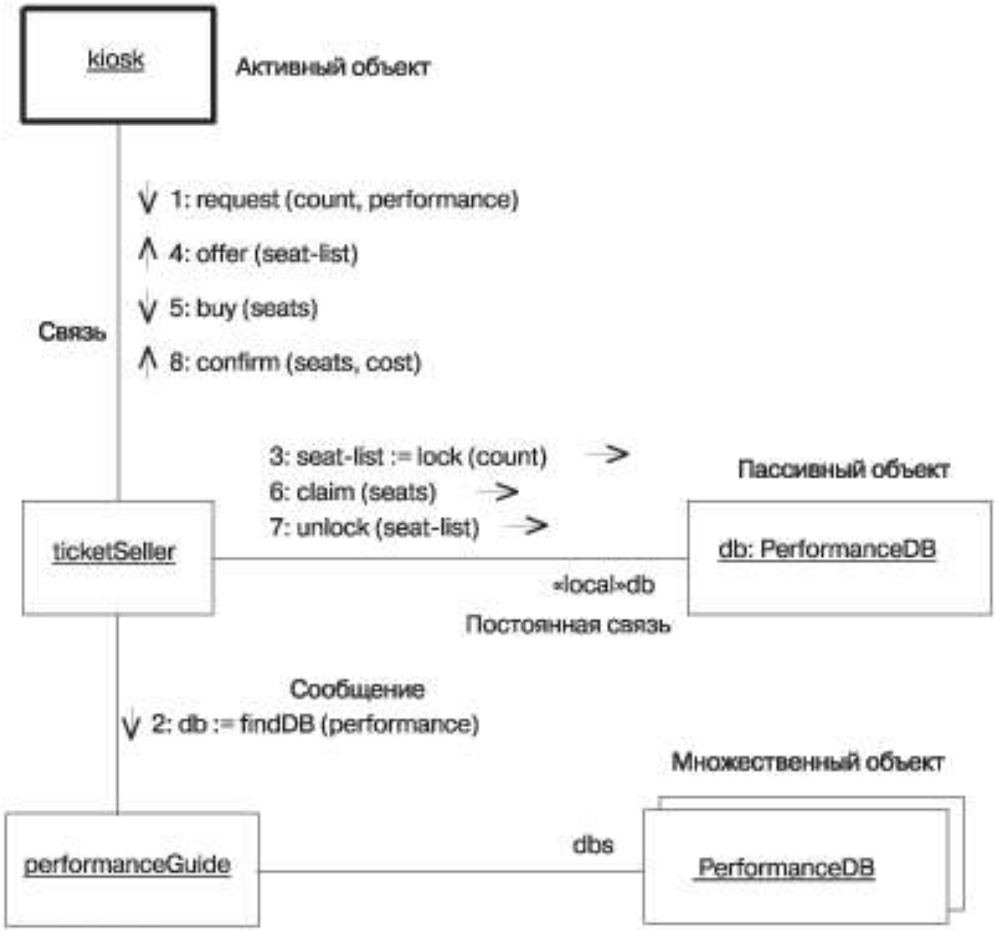


Диаграмма пакетов

Зависимости между пакетами

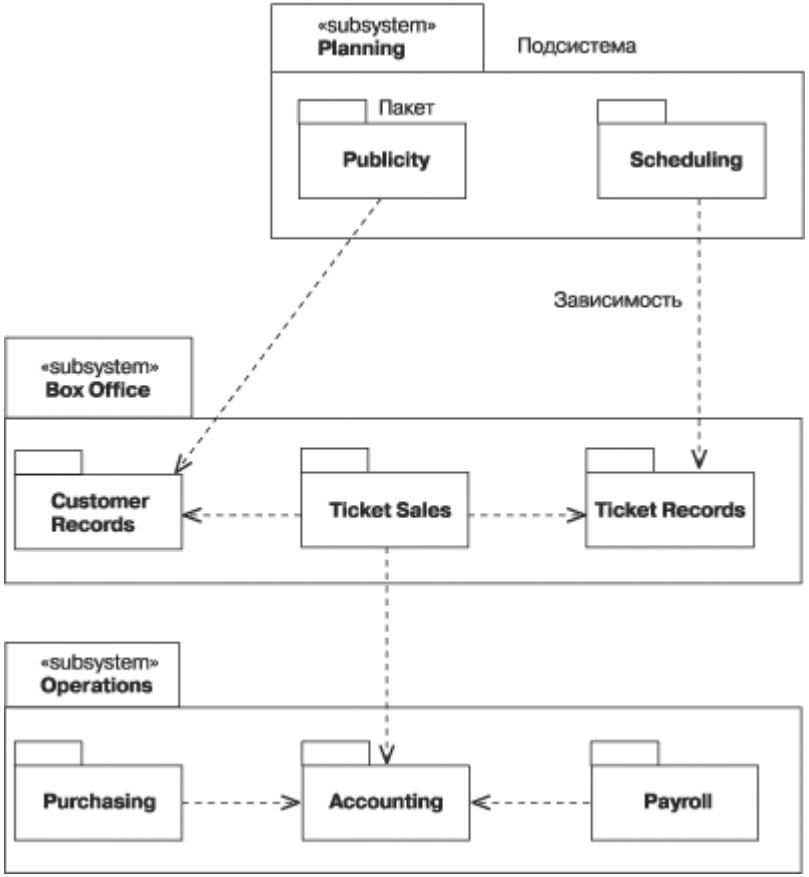
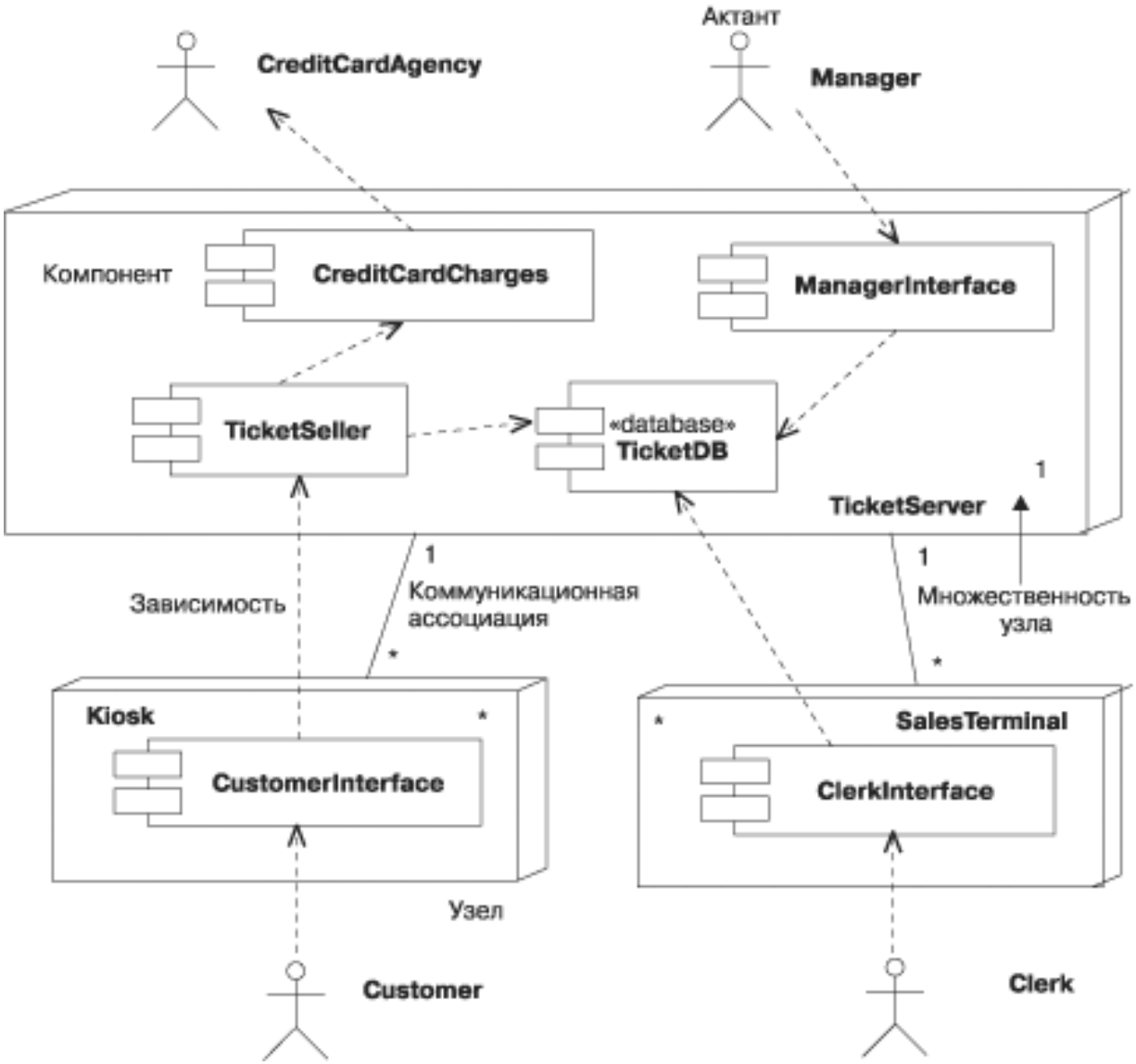


Диаграмма развёртывания

Конфигурация узлов, где производится обработка информации



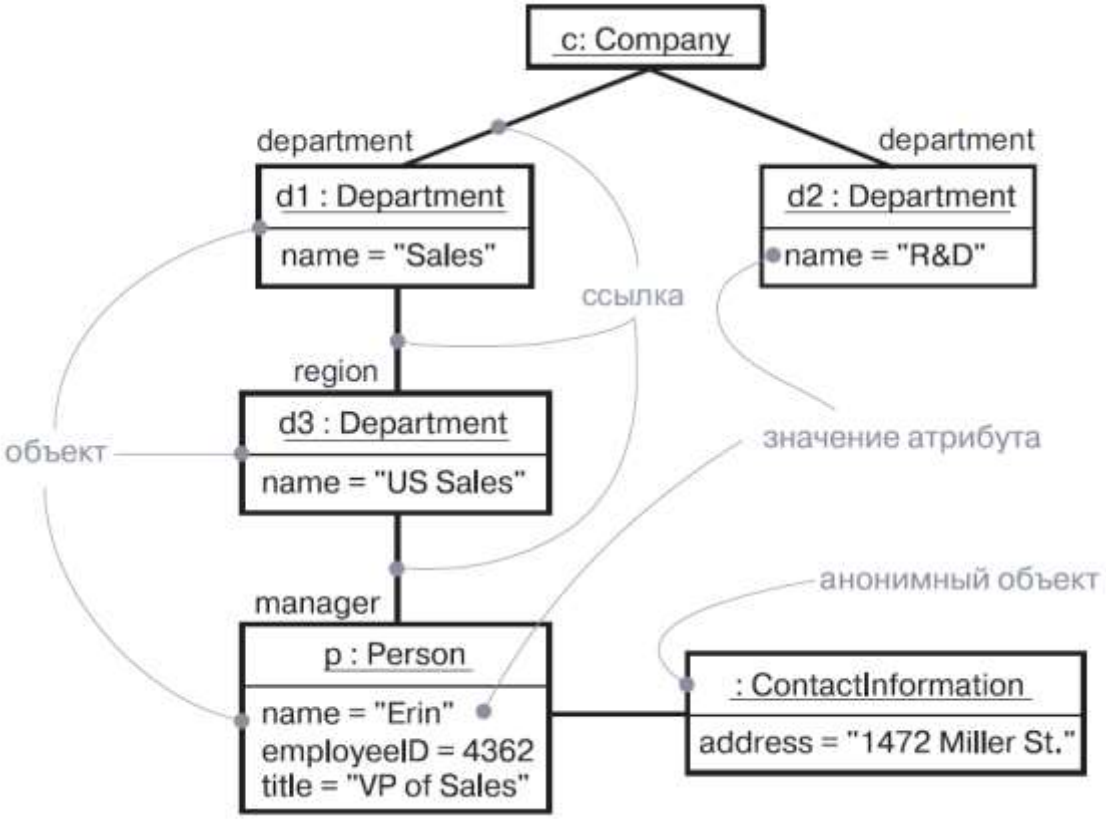


Диаграмма объектов

Экземпляры классов (объекты) с указанием текущих значений их атрибутов и связей между объектами.

Диаграмма профилей

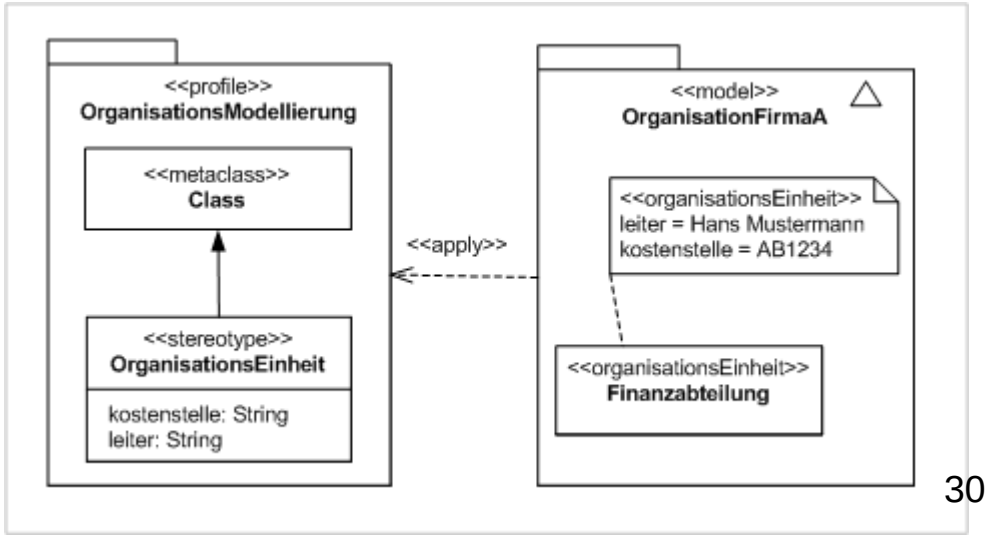


Диаграмма деятельности

Разложение некоторой деятельности на её составные части

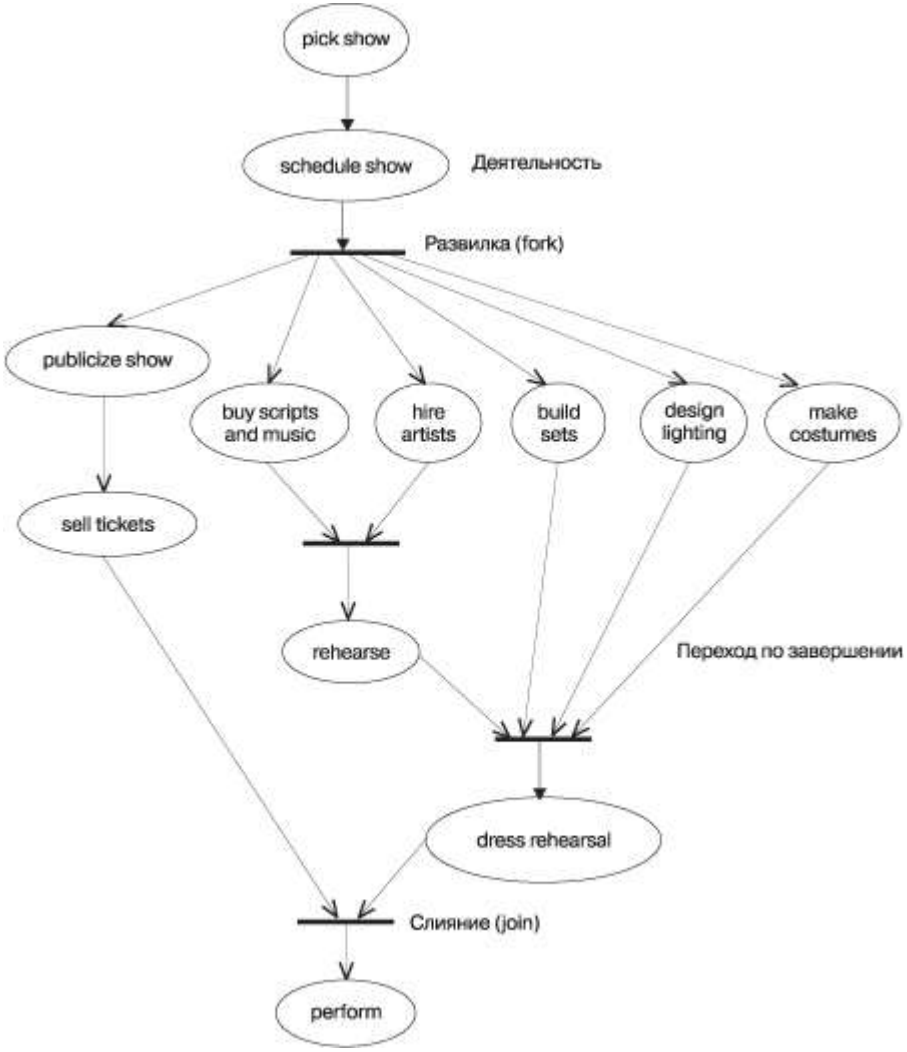
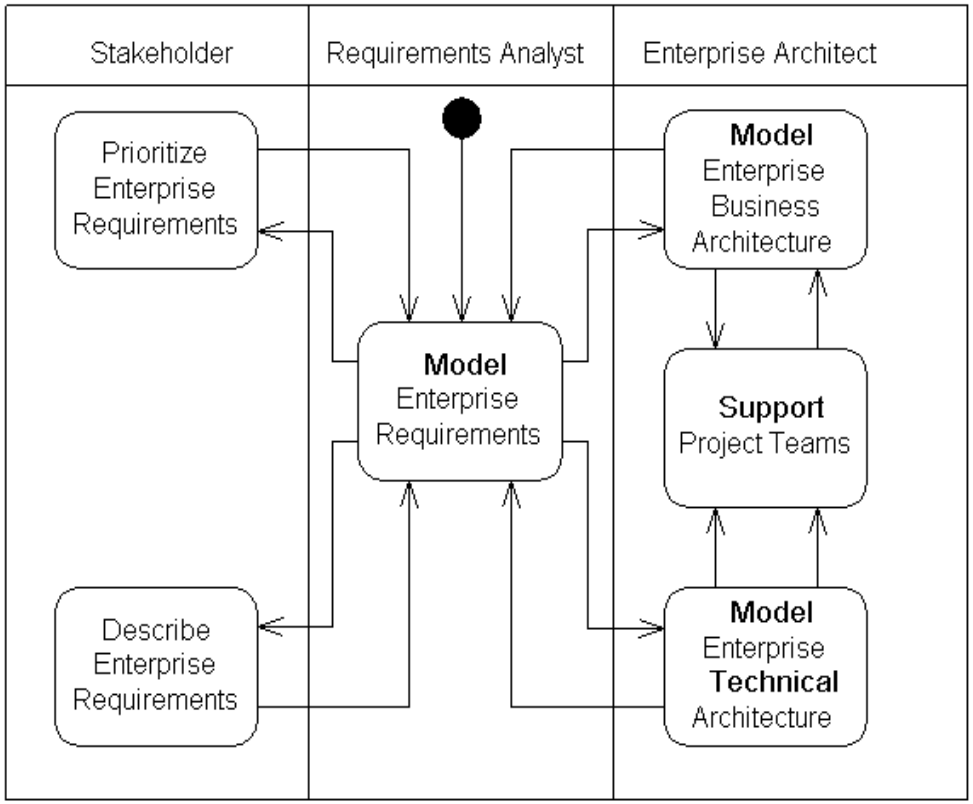


Диаграмма деятельности

(«плавательные дорожки»)



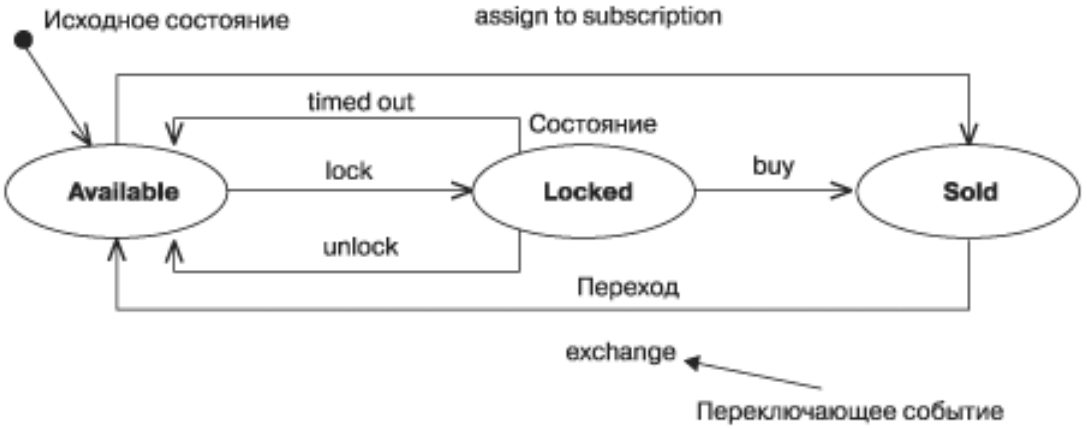


Диаграмма состояний

Все возможные состояния системы под воздействием различных действий или событий

Диаграмма прецедентов

Отношения между действующими лицами и прецедентами

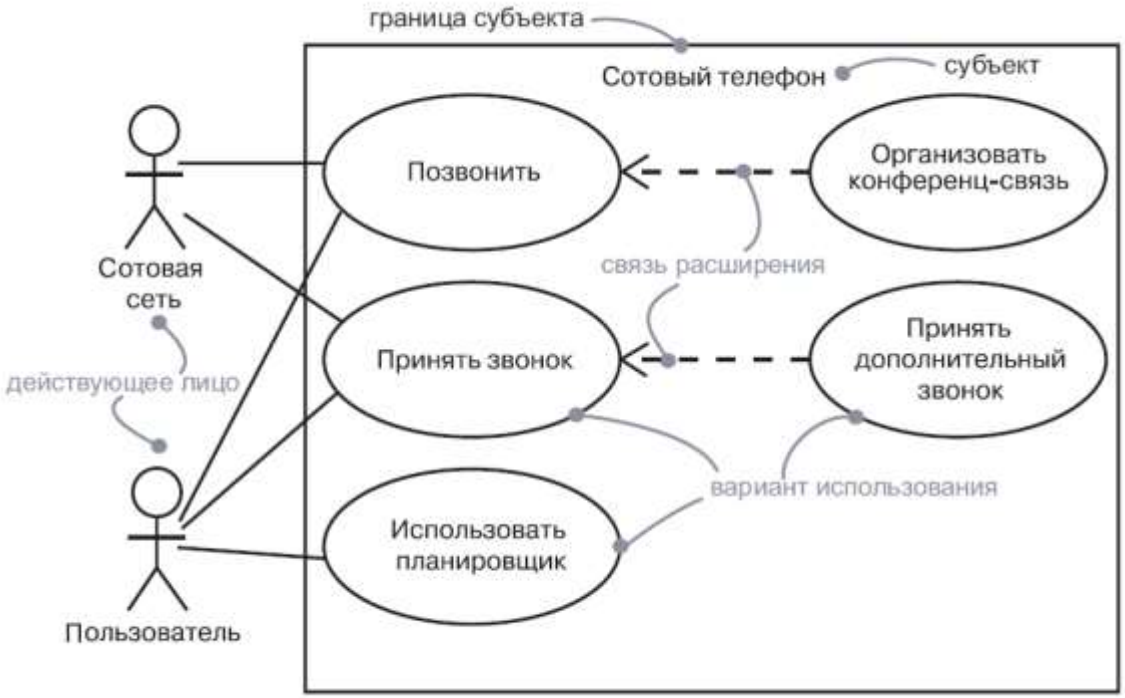


Диаграмма коммуникации

Взаимодействия между частями составной структуры или ролями кооперации

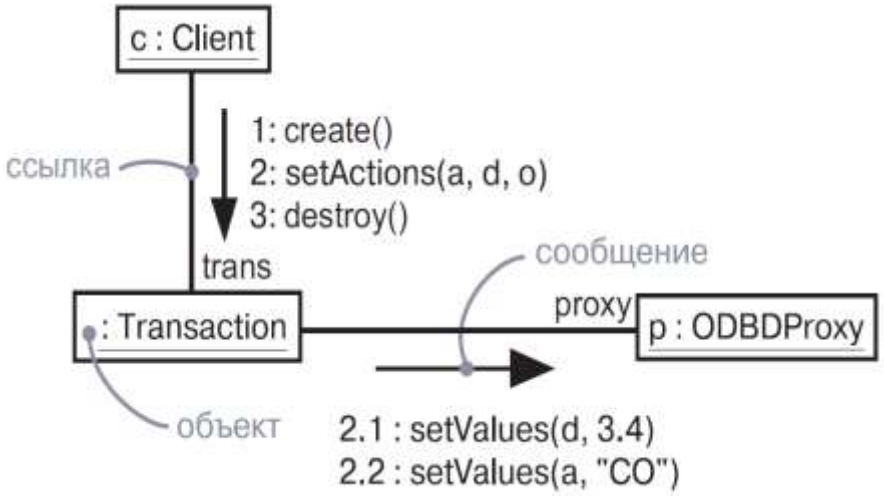


Диаграмма обзора взаимодействия

Диаграмма деятельности + диаграмма последовательности

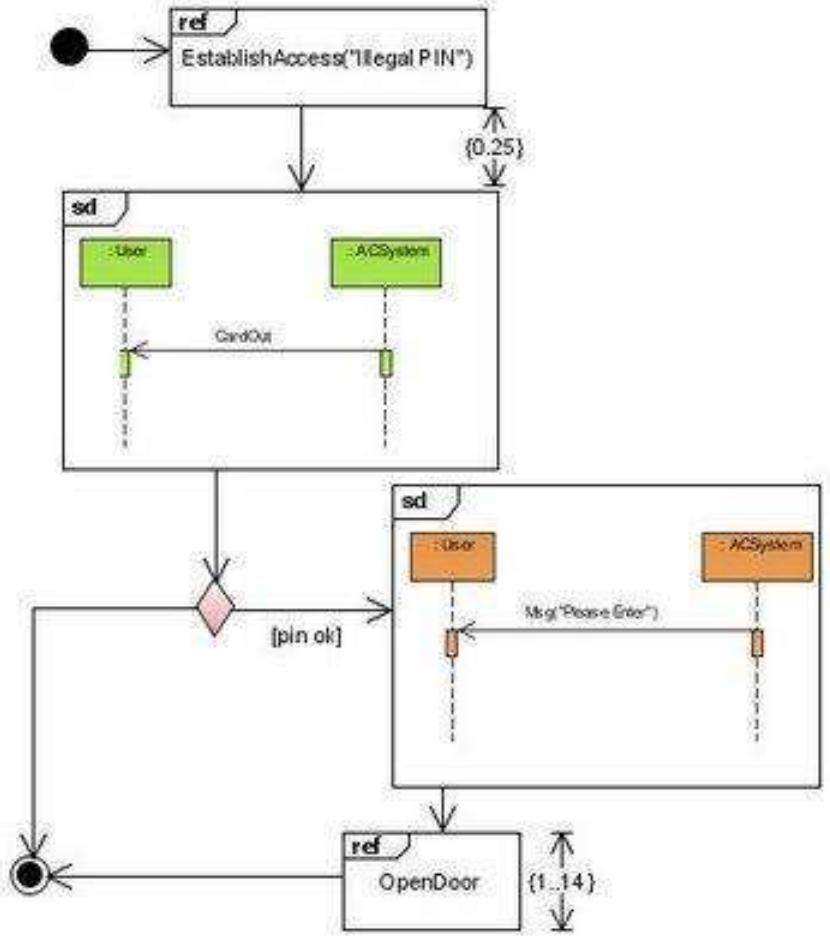
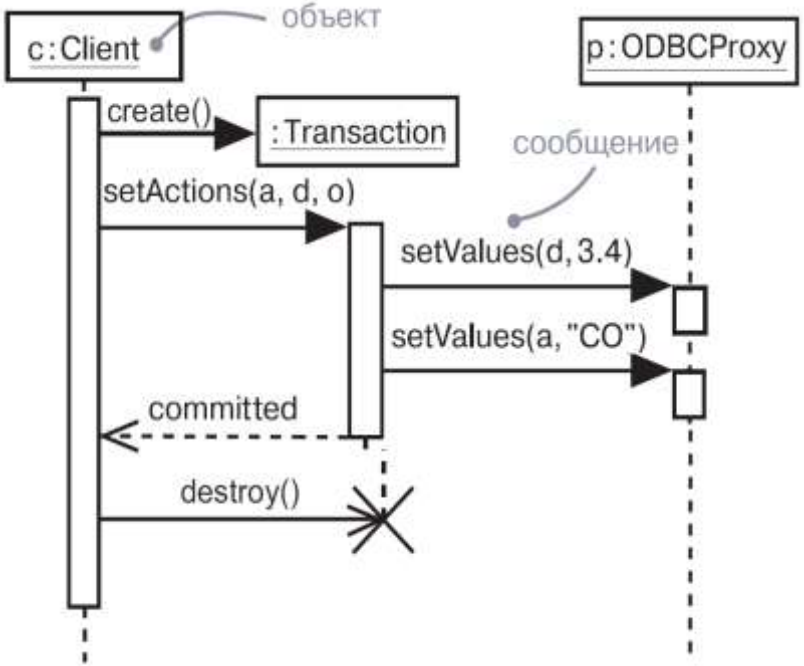


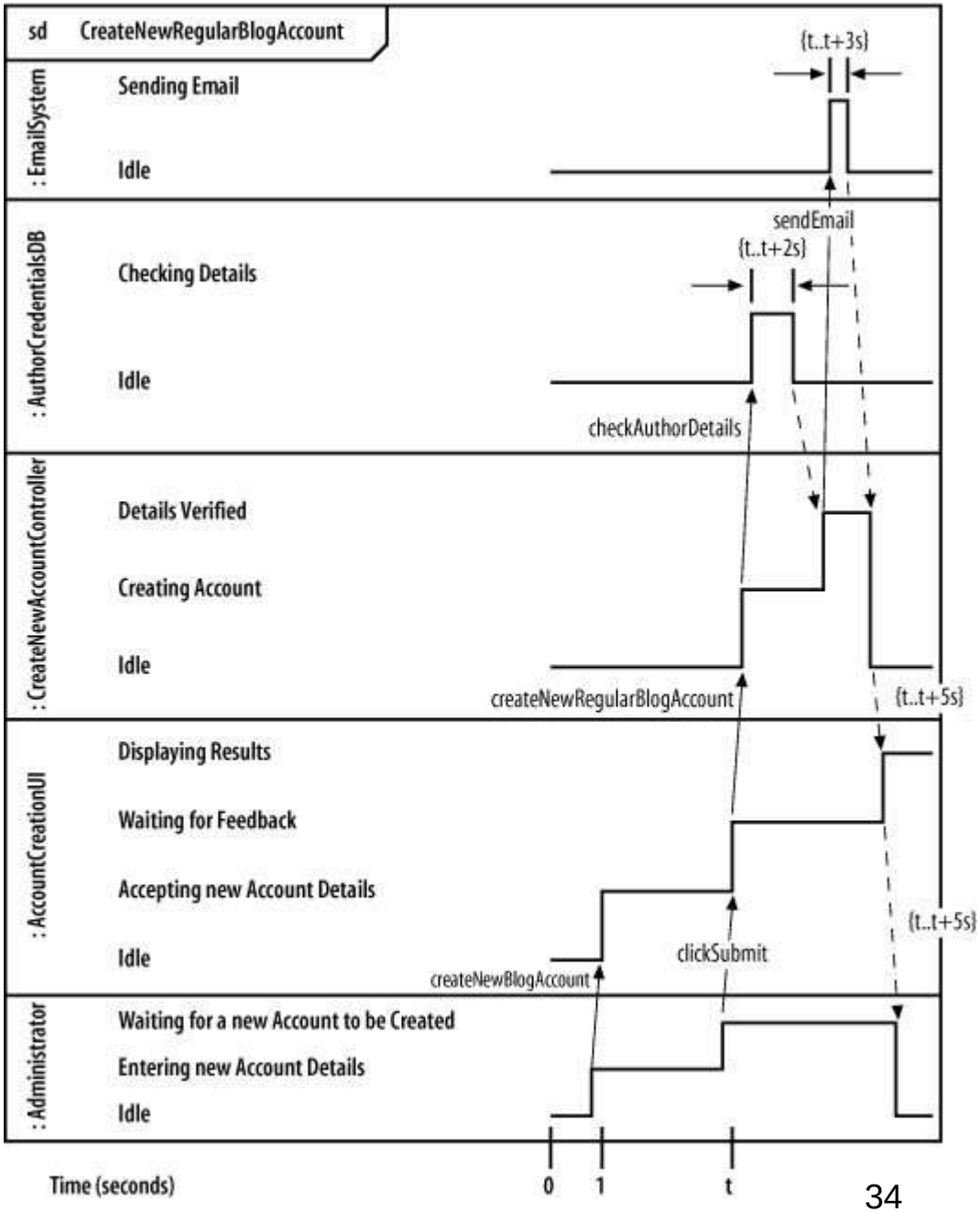
Диаграмма синхронизации

Взаимодействие объектов с учётом определенных временных рамок

Диаграмма последовательности

Взаимодействия объектов, упорядоченные по времени их проявления





3. Операграммы

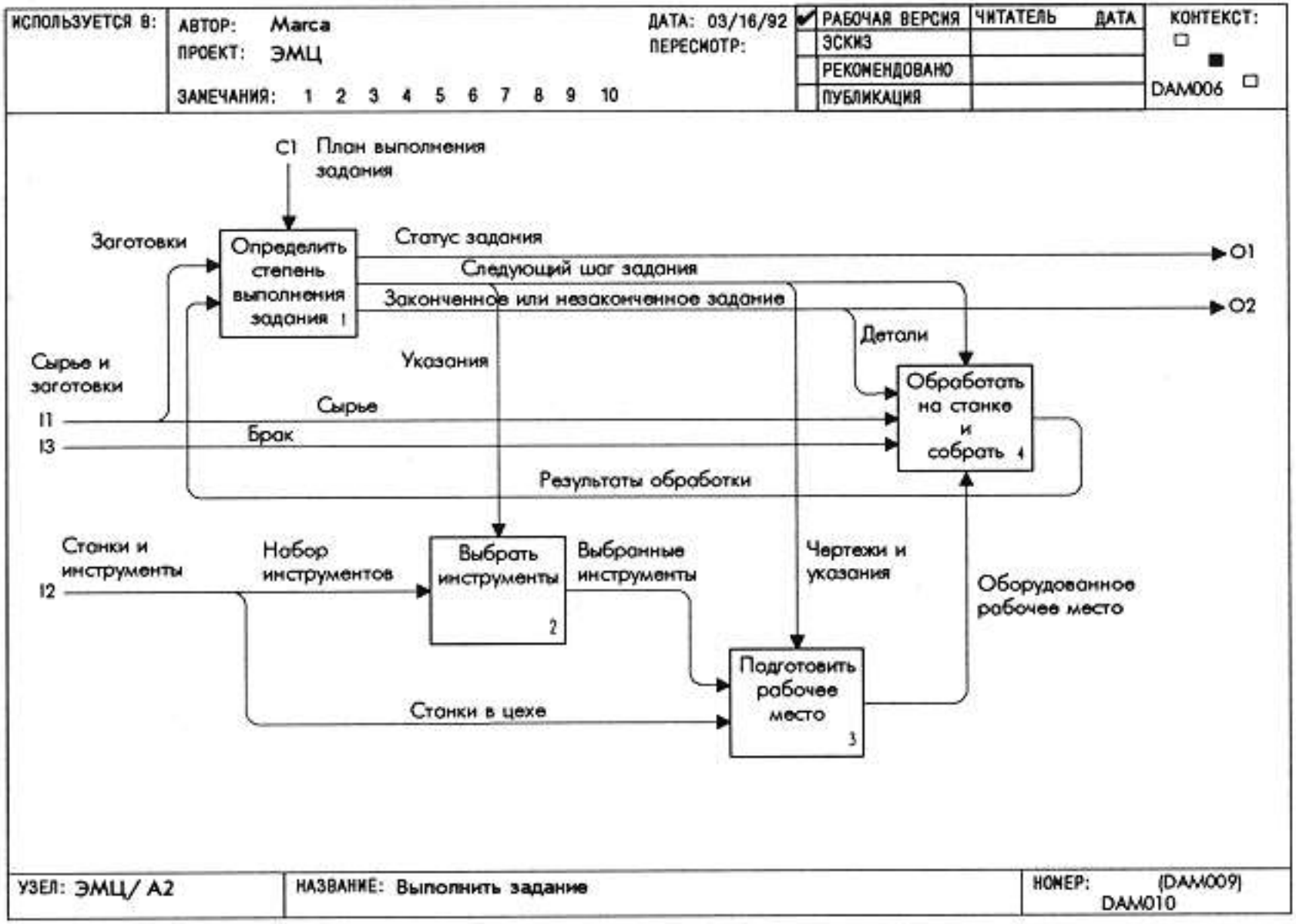
Планирование и контроль хода выполнения технологических процессов переработки данных

Этап процесса	Пользо-ватель	Служба сопро-вождения	Програм-мист	Комиссия по приемке
1 Формирование и передача предварительного извещения об изменениях в программном изделии(ПИ)				
2 Сообщение о возможных изменениях ПИ				
3 Разработка предложений об изменениях в ПИ				
4 Формирование новой версии ПИ				
5 Анализ физических характеристик ПИ, полученных в результате изменения ПИ				
6 Сообщение о внесении изменений				
7 Внесение изменений в тестовую версию				
8 Тестирование ПИ				
9 Внесение изменений в пользовательскую версию				
10 Внесение изменений в документацию пользовательской версии				
11 Испытание ПИ. Составление акта приемки ПИ				
12 Тиражирование новой версии ПИ				
13 Передача новой версии ПИ пользователю				

4. Функциональные модели SADT

- Представление сложных систем путем построения моделей
- SADT-модель - функциональное описание системы, у которого есть единственный субъект, цель и одна точка зрения, соответствующая методологии и нотации IDEF0
- Цель - набор вопросов, на которые должна ответить модель.
- Точка зрения - позиция, с которой описывается система

В РФ только этот вид моделей из всего набора, определённого в IDEF, включён в официальную нормативную базу.



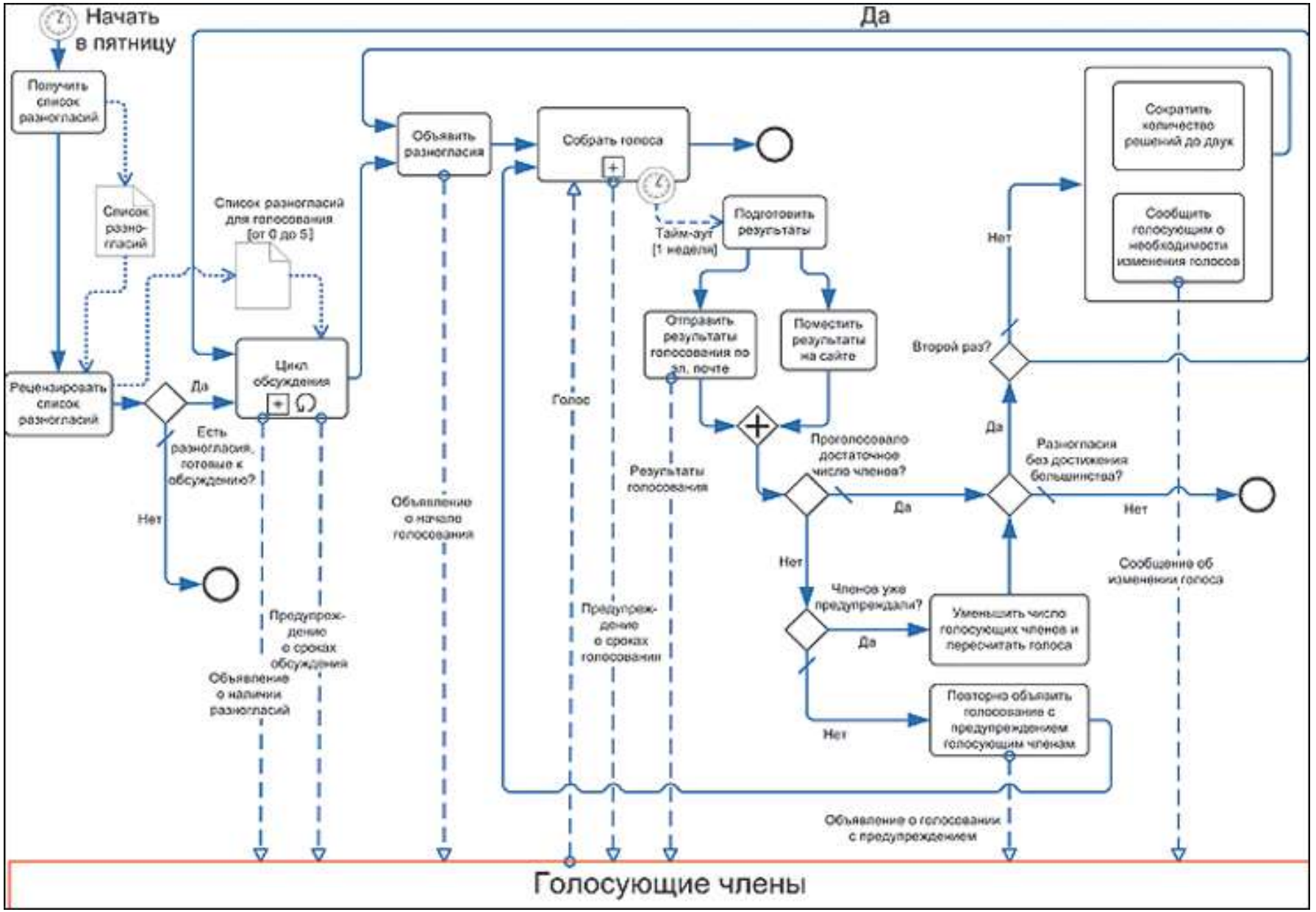
SADT диаграмма

Рекомендации независимых организаций

1. BPMN (Business Process Model and Notation)
2. IDEF (Integration Definition Metodology)
3. DFD (Data Flow diagram)

1. BPMN

- Введён в действие и поддерживается консорциумом OMG (Object Management Group)
- Создание нотации, понятной всем участникам бизнес-сферы
- Возможность симметричного преобразования между схемами BPMN и описанием бизнес-процессов на языке BPEL (business process execution language)



BPMN диаграмма

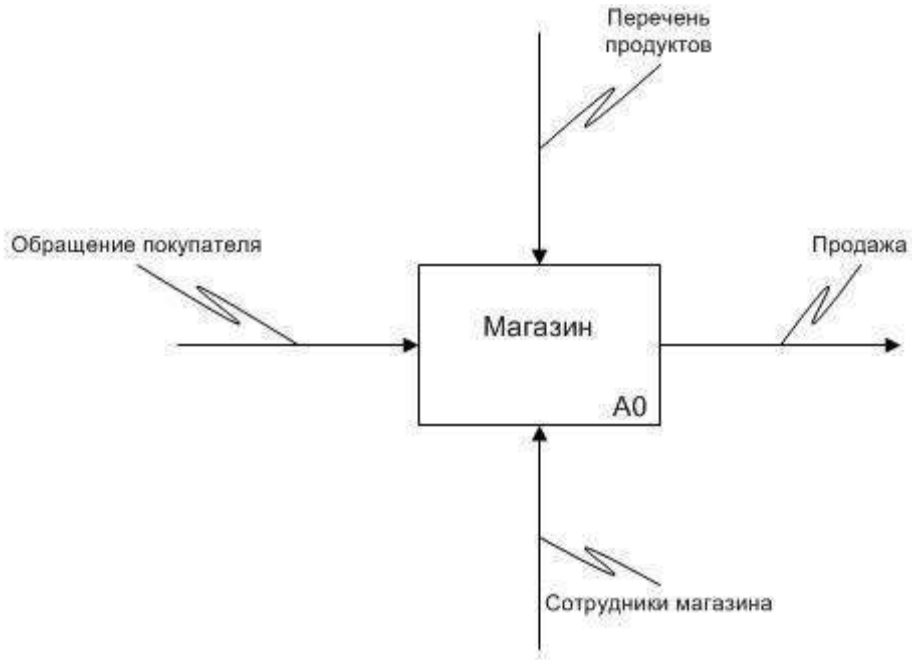
2. IDEF

Нотация	Назначение
IDEF0	Структурированное отображение функций производственной системы/среды, информации и объектов, связывающих эти функции .
IDEF1	Отображение и анализ структуры и взаимосвязей информационных потоков в системе.
IDEF1X	Отображение структуры информации, необходимой для поддержки функций производственной системы/среды.
IDEF2 Не используется	Динамическое моделирование развития систем.
IDEF3	Сбор информации о состоянии моделируемой системы.
IDEF4	Отображение структуры объектов и заложенных принципов их взаимодействия.
IDEF5	Развитие и оптимизация системы.
IDEF6	Облегчение получения «знаний о способе» моделирования, их представления и использования при разработке систем управления предприятиями.

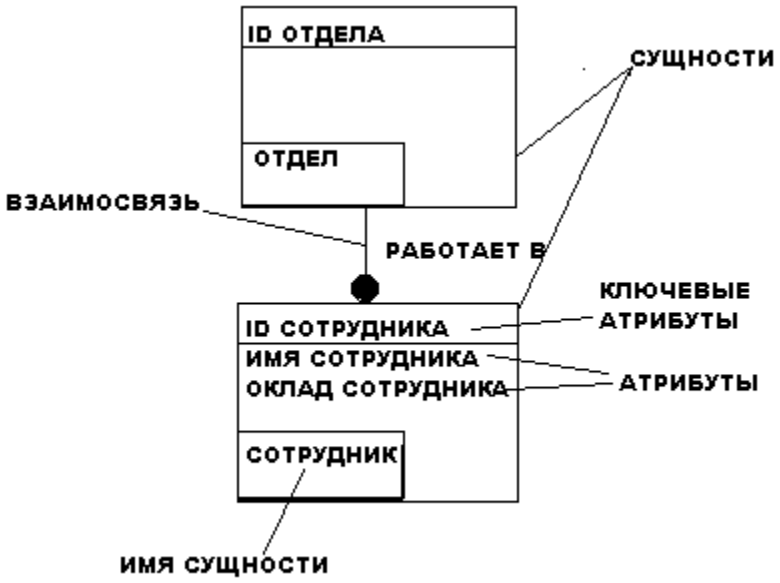
IDEF

IDEF7	Аудит информационных систем.
IDEF8	Разработка интерфейсов взаимодействия оператора и системы (пользовательских интерфейсов).
IDEF9	Исследование бизнес ограничений.
IDEF10	Моделирование архитектуры выполнения.
IDEF11	Information Artifact Modeling.
IDEF12	Организационное моделирование.
IDEF13	Трёхсхемное проектирование преобразования данных.
IDEF14	Проектирования компьютерных сетей.

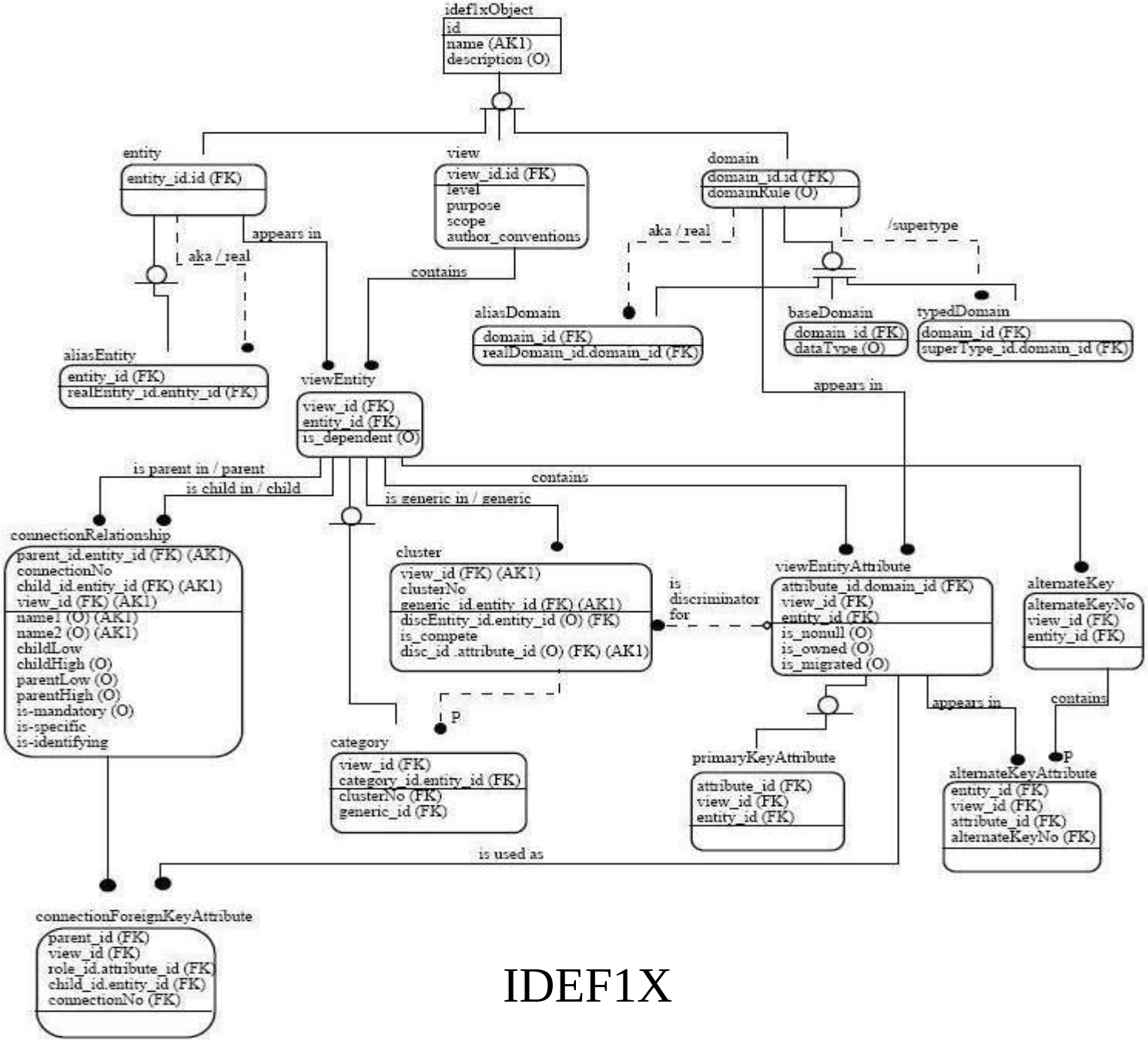
Методы IDEF7, IDEF10, IDEF11, IDEF 12 и IDEF13 не разработаны полностью.


Перечень продуктов
Обращение покупателя
Продажа
Магазин
A0
Сотрудники магазина

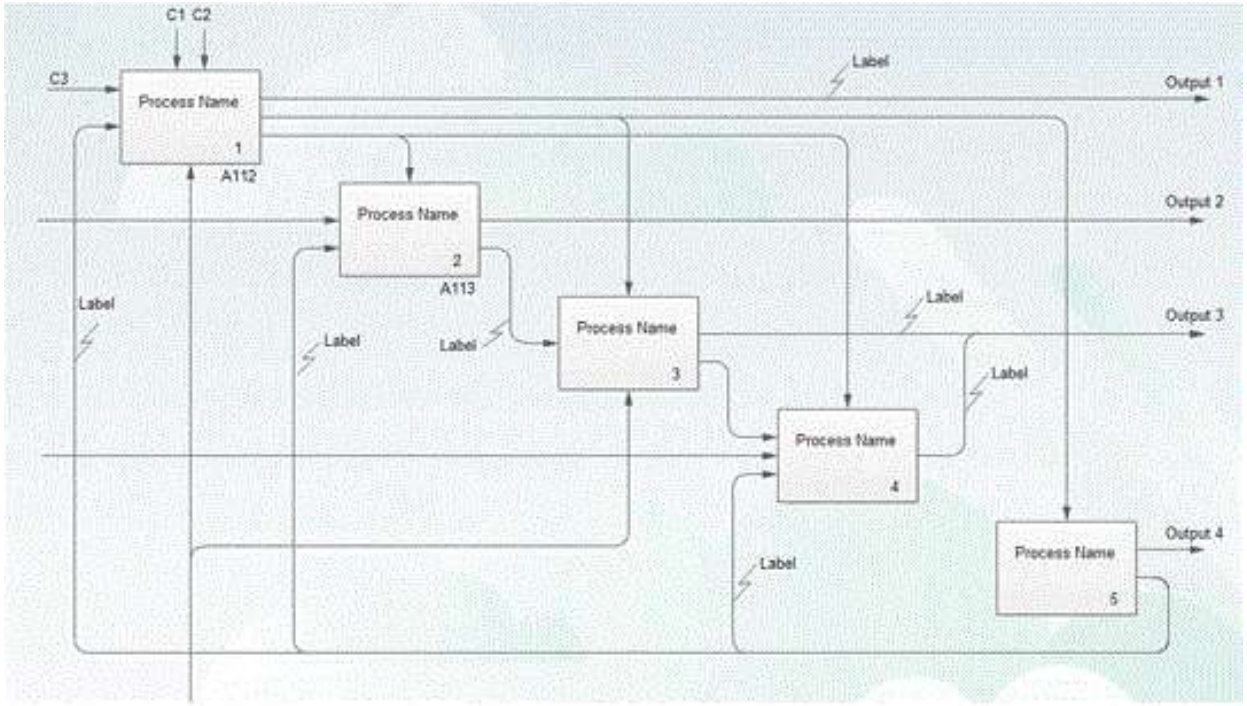
IDEF0


ID ОТДЕЛА
ОТДЕЛ
СУЩНОСТИ
ВЗАИМОСВЯЗЬ
РАБОТАЕТ В
КЛЮЧЕВЫЕ АТРИБУТЫ
ID СОТРУДНИКА
ИМЯ СОТРУДНИКА
ОКЛАД СОТРУДНИКА
АТРИБУТЫ
СОТРУДНИК
ИМЯ СУЩНОСТИ

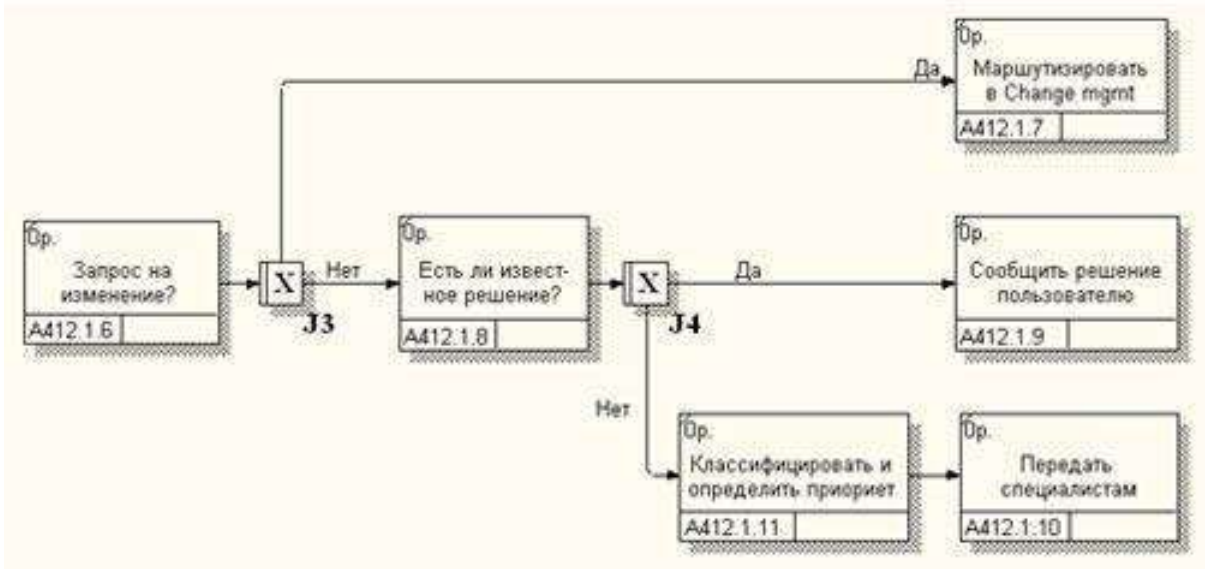
IDEF1


idef1xObject
id
name (AK1)
description (O)
entity
entity_id.id (FK)
view
view_id.id (FK)
level
purpose
scope
author_conventions
domain
domain_id.id (FK)
domainRule (O)
appears in
aka / real
contains
aka / real
/supertype
aliasDomain
domain_id (FK)
realDomain_id.domain_id (FK)
baseDomain
domain_id (FK)
dataType (O)
typedDomain
domain_id (FK)
superType_id.domain_id (FK)
aliasEntity
entity_id (FK)
realEntity_id.entity_id (FK)
viewEntity
view_id (FK)
entity_id (FK)
is_dependent (O)
appears in
is parent in / parent
is child in / child
is generic in / generic
contains
connectionRelationship
parent_id.entity_id (FK) (AK1)
connectionNo
child_id.entity_id (FK) (AK1)
view_id (FK) (AK1)
name1 (O) (AK1)
name2 (O) (AK1)
childLow
childHigh (O)
parentLow (O)
parentHigh (O)
is-mandatory (O)
is-specific
is-identifying
cluster
view_id (FK) (AK1)
clusterNo
generic_id.entity_id (FK) (AK1)
discEntity_id.entity_id (O) (FK)
is_compete
disc_id .attribute_id (O) (FK) (AK1)
is discriminator for
viewEntityAttribute
attribute_id.domain_id (FK)
view_id (FK)
entity_id (FK)
is_nonull (O)
is_owned (O)
is_migrated (O)
alternateKey
alternateKeyNo
view_id (FK)
entity_id (FK)
P
category
view_id (FK)
category_id.entity_id (FK)
clusterNo (FK)
generic_id (FK)
primaryKeyAttribute
attribute_id (FK)
view_id (FK)
entity_id (FK)
appears in
contains
P
alternateKeyAttribute
entity_id (FK)
view_id (FK)
attribute_id (FK)
alternateKeyNo (FK)
is used as
connectionForeignKeyAttribute
parent_id (FK)
view_id (FK)
role_id.attribute_id (FK)
child_id.entity_id (FK)
connectionNo (FK)

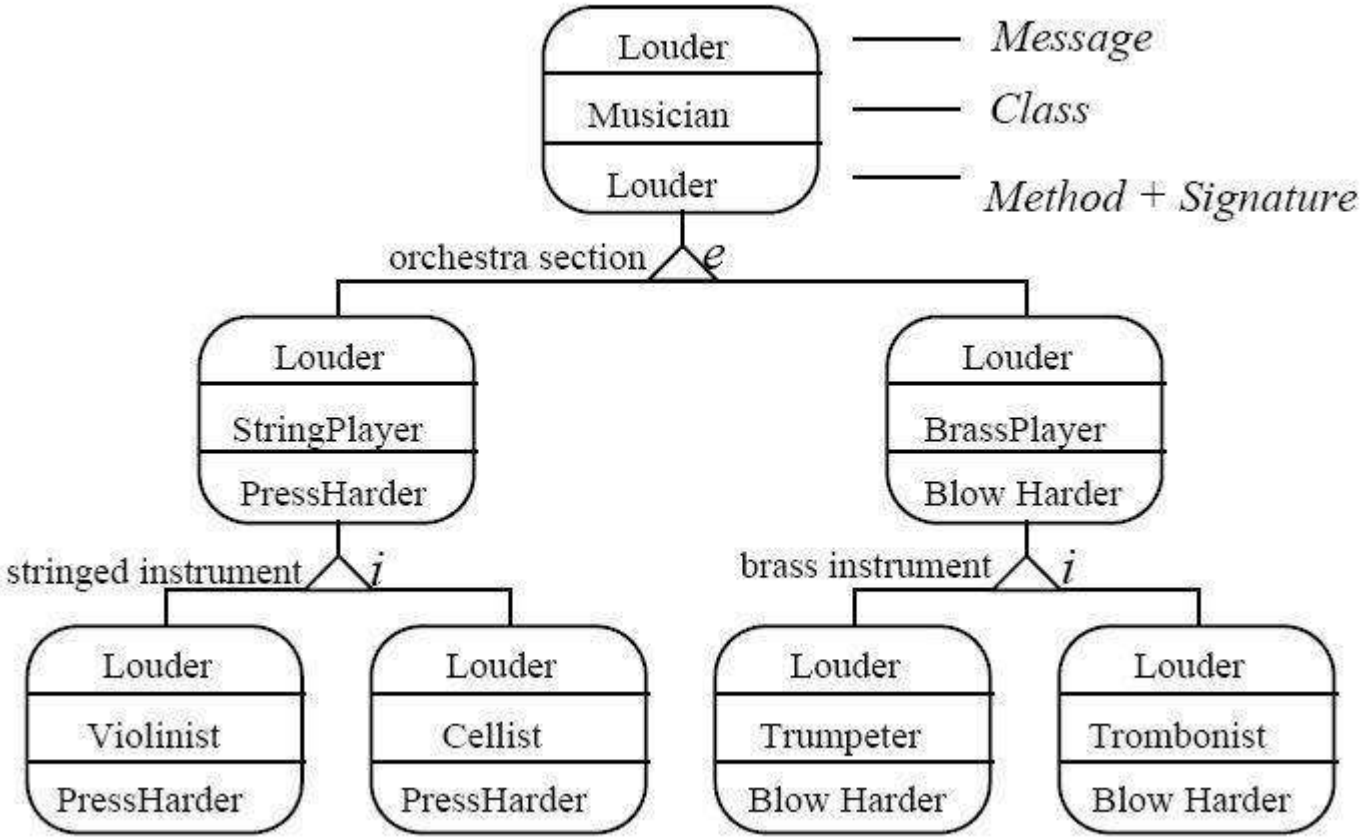
IDEF1X


C1 C2
C3
Process Name
1
A112
Label
Output 1
Process Name
2
A113
Output 2
Label
Label
Label
Process Name
3
Label
Output 3
Label
Process Name
4
Output 4
Process Name
5
Label

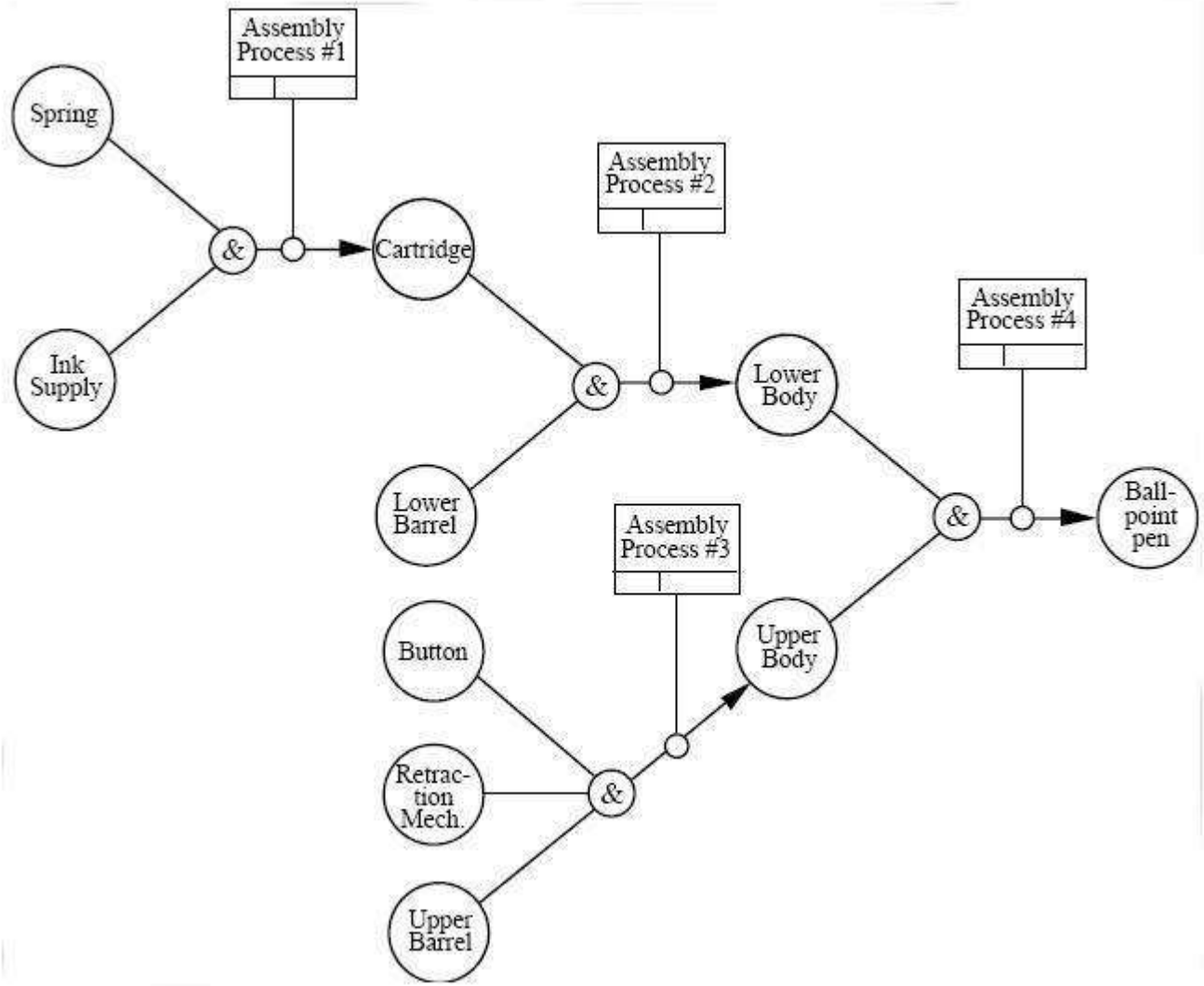
IDEF2


Op.
Запрос на изменение?
A412.1.6
X
J3
Нет
Op.
Есть ли извест-ное решение?
A412.1.8
X
J4
Да
Op.
Маршутизировать в Change mgmt
A412.1.7
Да
Op.
Сообщить решение пользователю
A412.1.9
Нет
Op.
Классифицировать и определить приоритет
A412.1.11
Op.
Передать специалистам
A412.1.10

IDEF3


Louder
Musician
Louder
Message
Class
Method + Signature
orchestra section
e
Louder
StringPlayer
PressHarder
Louder
BrassPlayer
Blow Harder
stringed instrument
i
brass instrument
i
Louder
Violinist
PressHarder
Louder
Cellist
PressHarder
Louder
Trumpeter
Blow Harder
Louder
Trombonist
Blow Harder

IDEF4


Assembly Process #1
Spring
Ink Supply
&
Cartridge
Assembly Process #2
Assembly Process #4
&
Lower Body
Lower Barrel
&
Ball-point pen
Assembly Process #3
Button
Upper Body
Retrac-tion Mech.
&
Upper Barrel

IDEF5

3. DFD

- Иерархия функциональных процессов, связанных потоками данных.
- Демонстрация, как каждый процесс преобразует свои входные данные в выходные, а также выявление отношений между этими процессами.

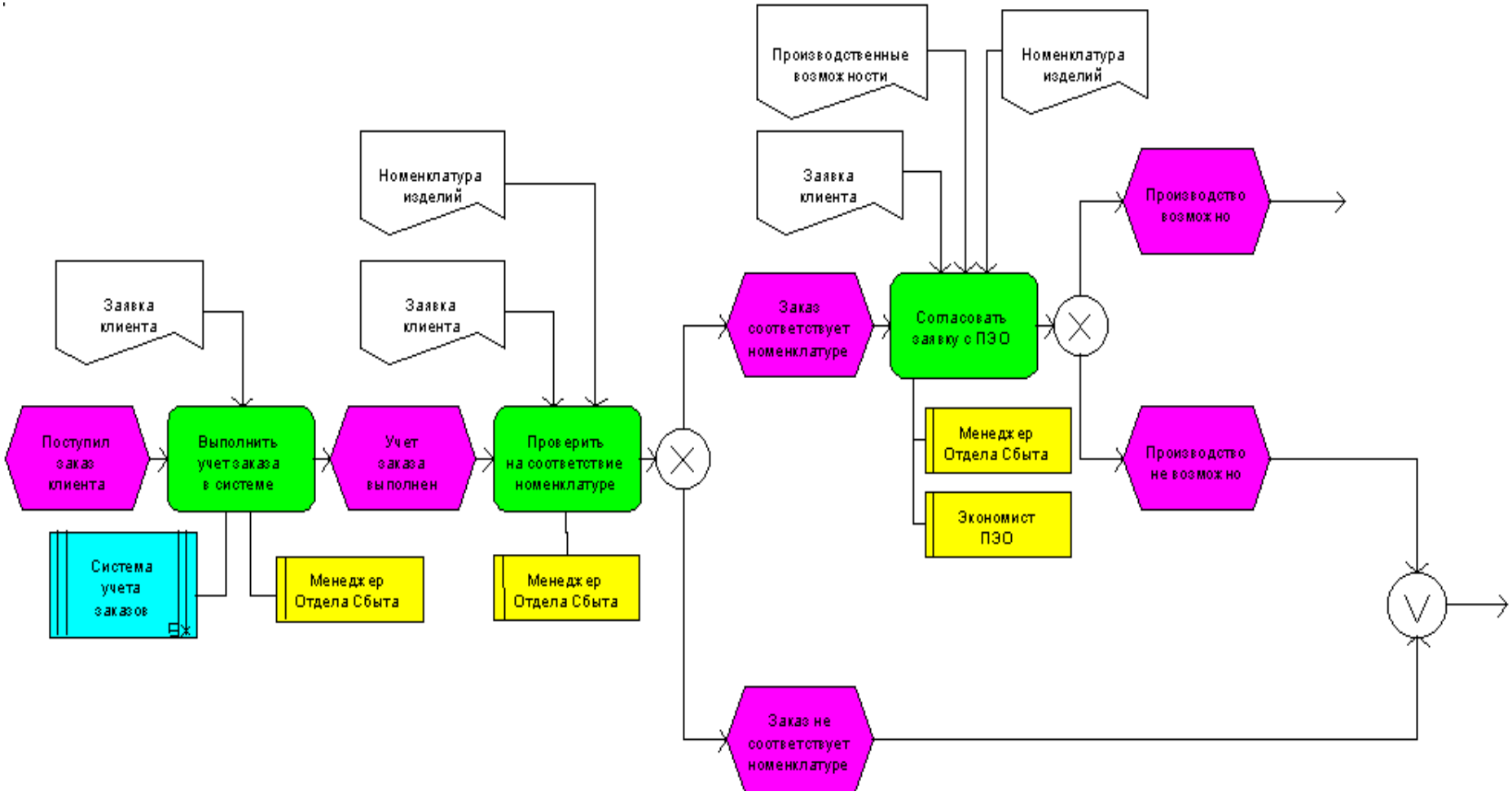
DFD диаграмма

Стандарты и рекомендации вендоров

1. ARIS
2. Oracle
3. BAAN
4. 1C

1. ARIS

Нотация	Описание
ARIS eEPC (extended Event Driven Process chain)	Описание цепочки процесса, управляемого событиями. Относится к классу нотаций workflow (описания потоков работ), которые предназначены для описания деятельности в динамике.
ARIS Information Flow	Используется при построении схем потоков данных или документов между функциями бизнес-процессов предприятия.

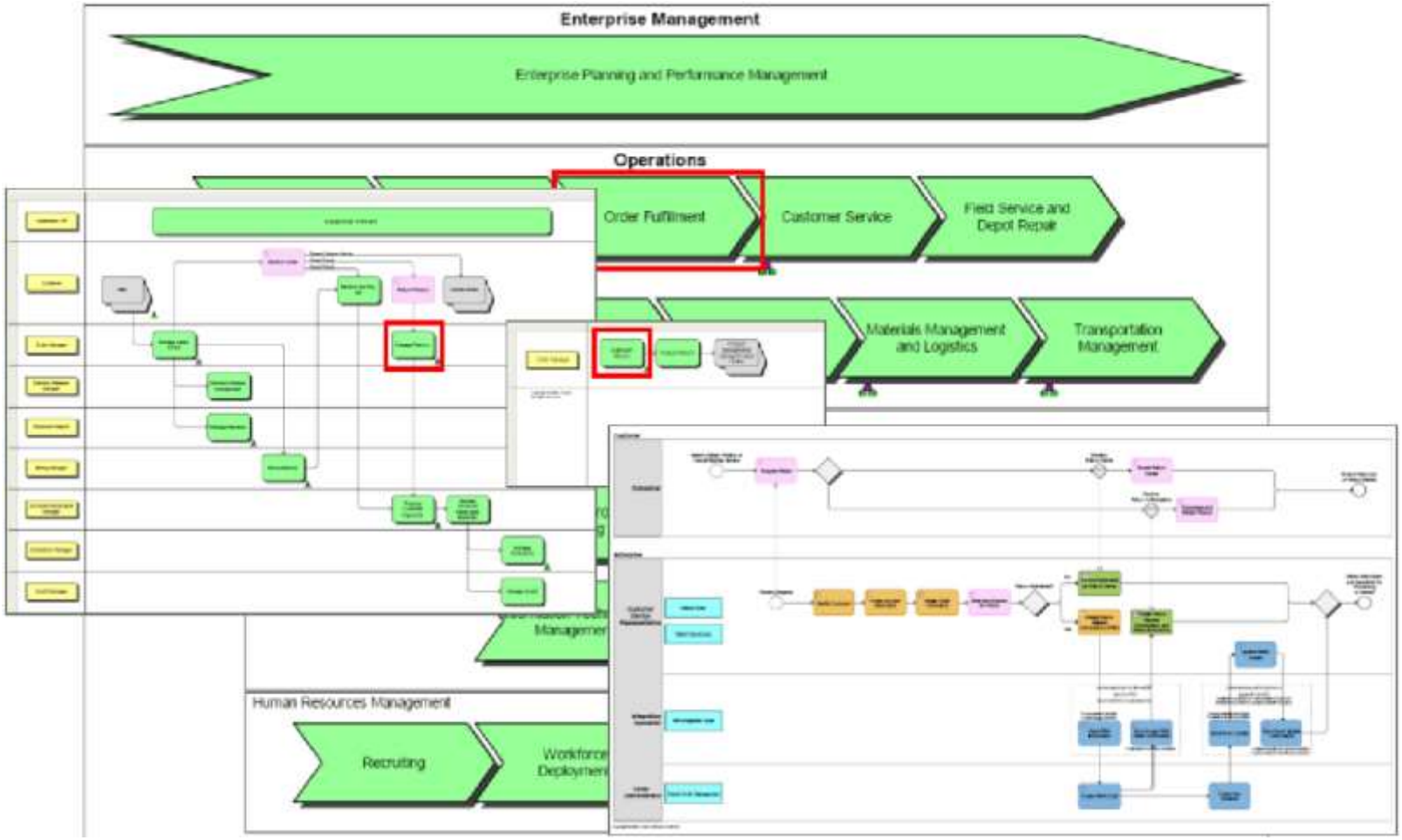

Производственные возможности
Номенклатура изделий
Заявка клиента
Производство возможно
Номенклатура изделий
Заявка клиента
Заявка клиента
Заказ соответствует номенклатуре
Согласовать заявку с ПЭО
Менеджер Отдела Сбыта
Экономист ПЭО
Производство не возможно
Поступил заказ клиента
Выполнить учет заказа в системе
Учет заказа выполнен
Проверить на соответствие номенклатуре
Система учета заказов
Менеджер Отдела Сбыта
Менеджер Отдела Сбыта
Заказ не соответствует номенклатуре

ARIS eEPC

ARIS
InformationFlow

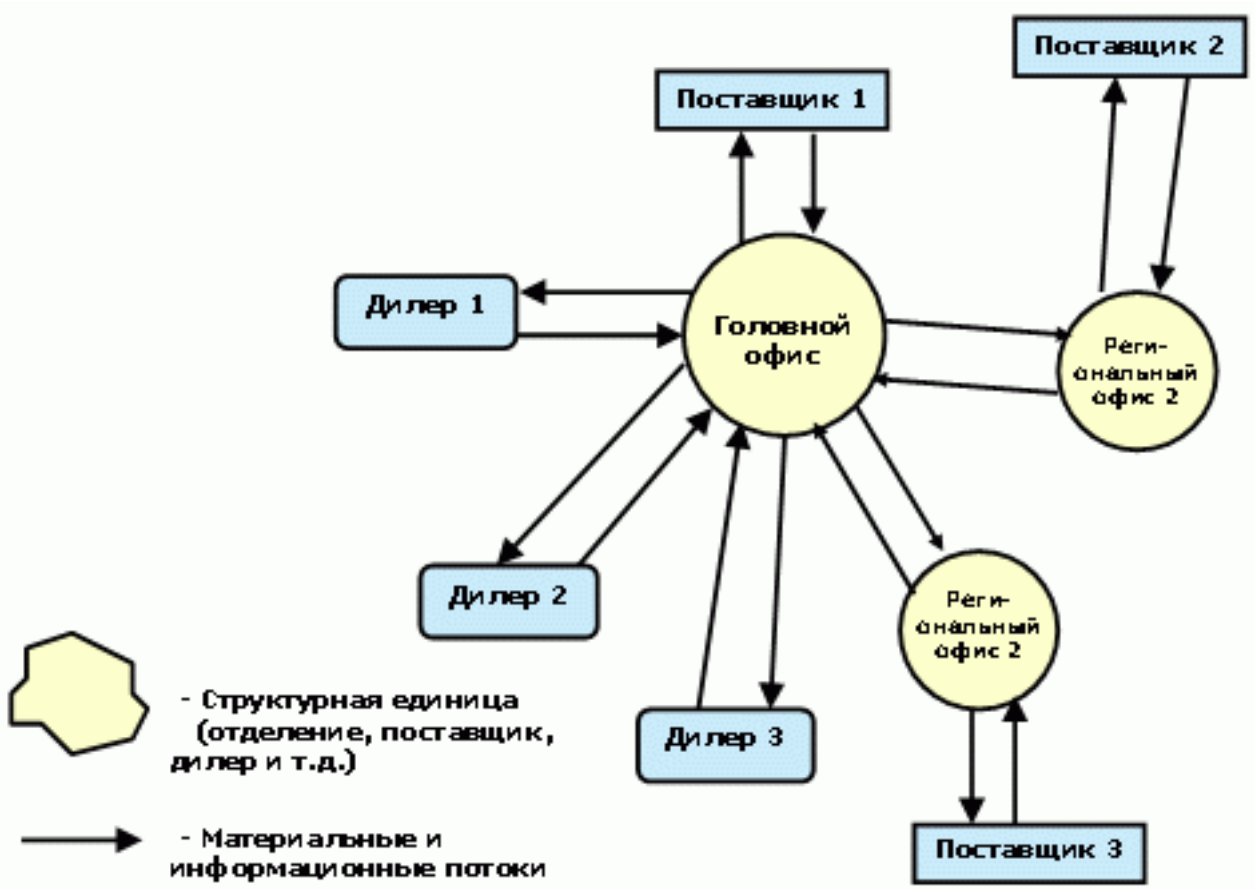
2. Oracle

5 уровней декомпозиции, для каждого из которых применяется своя методология и нотация:



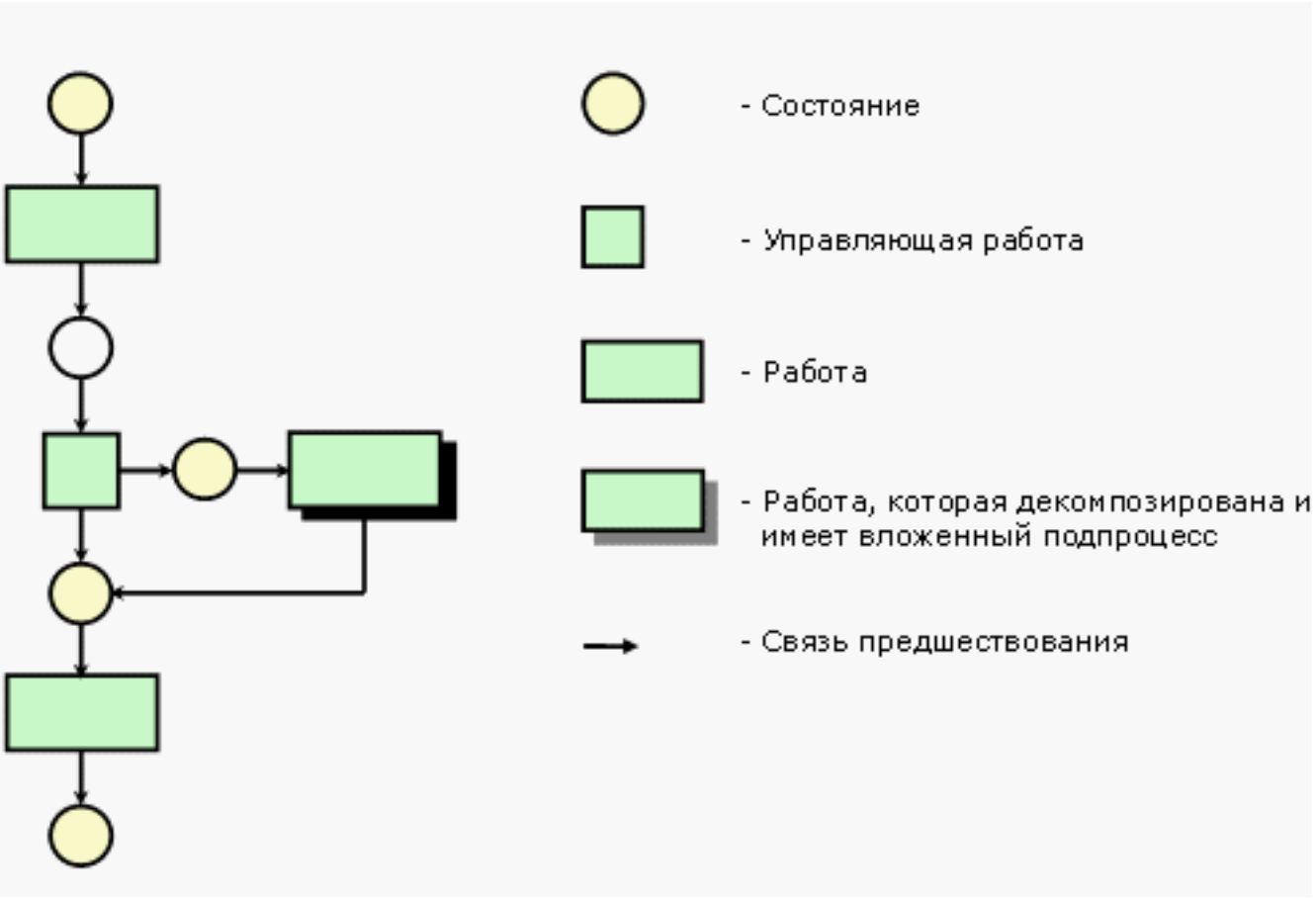
3. BAAN

Модель	Назначение
ESM (метаструктуры предприятия)	Описание географически распределенной организационной структуры предприятия. Описание географических подразделений компании, материальных и информационных потоков между ними.
BSM (управления предприятия)	Отображение бизнес-процессов структурных подразделений, материальных и информационных потоков между ними.
BPM (бизнес-процессов)	Описание бизнес-процессов компании.
BFM (функций)	Построение дерева функций компании.
BOM (организационной структуры)	Описание подразделений и должностей организации, связей линейного и функционального подчинения. Отображение ролей, которые играет должность в бизнес-процессах.
ERM (информационная)	Описание структуры информации, используемой при реализации бизнес-процессов. Проектирование баз данных.

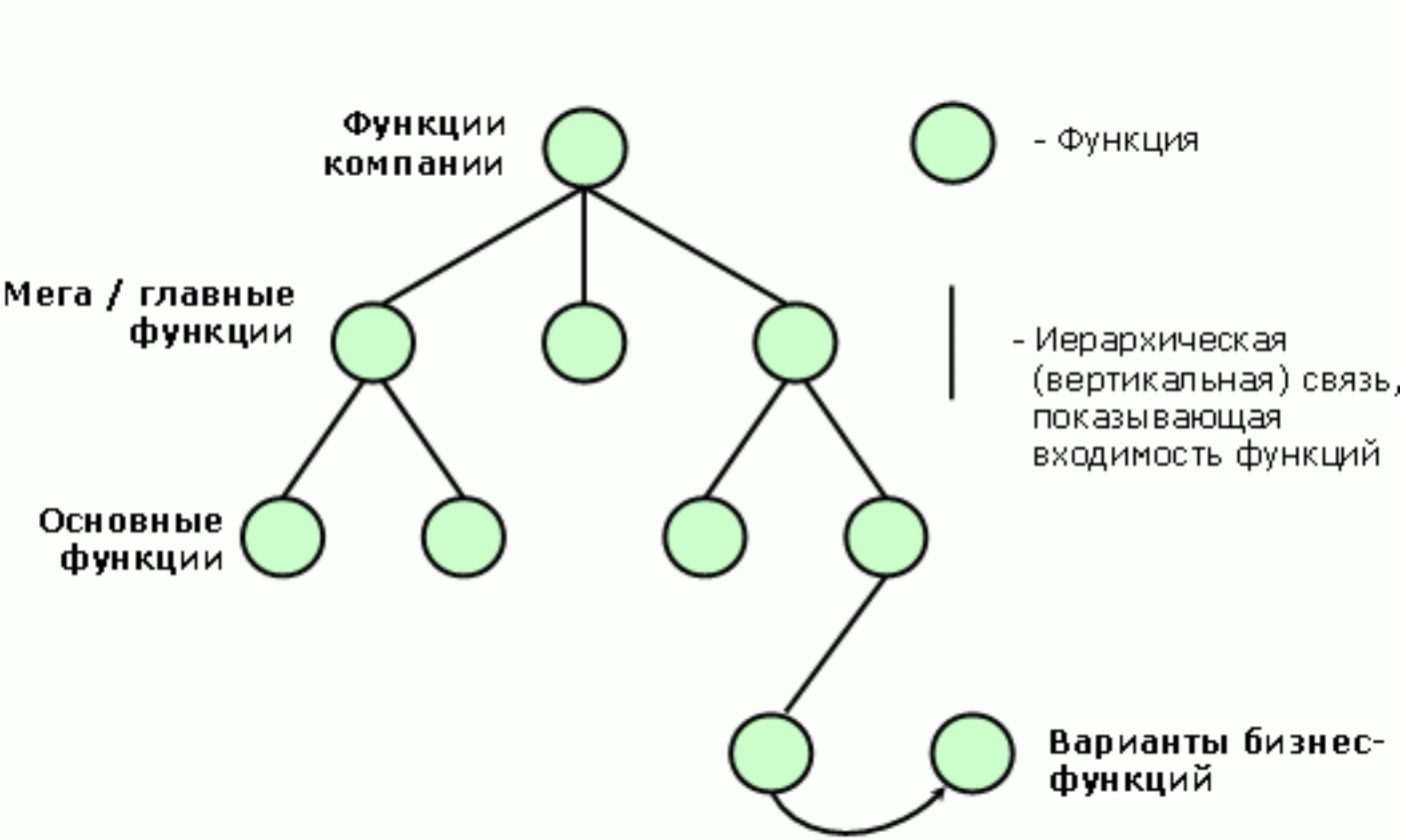


Модель метаструктуры предприятия

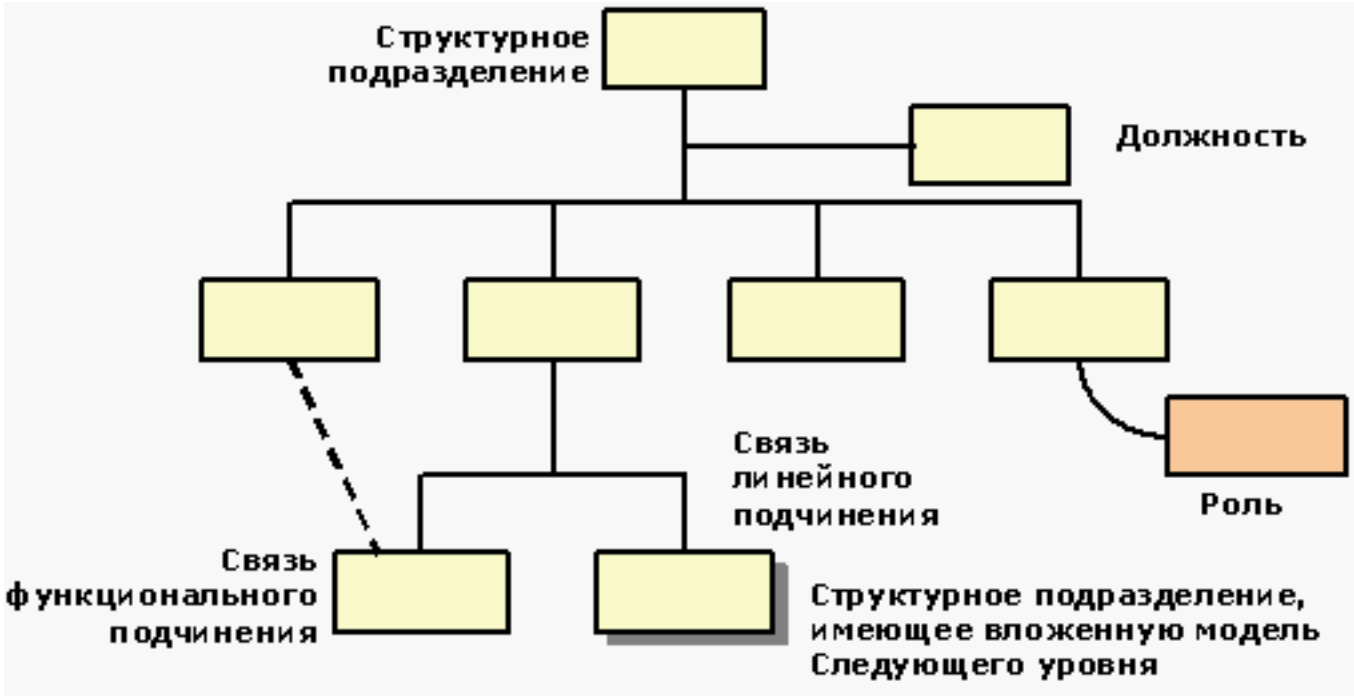
Модель управления предприятием



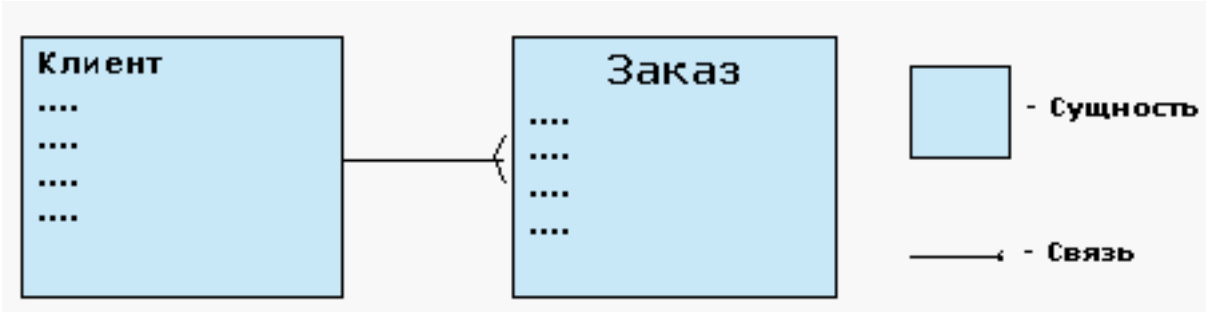
Модель бизнес-процессов



Модель функций



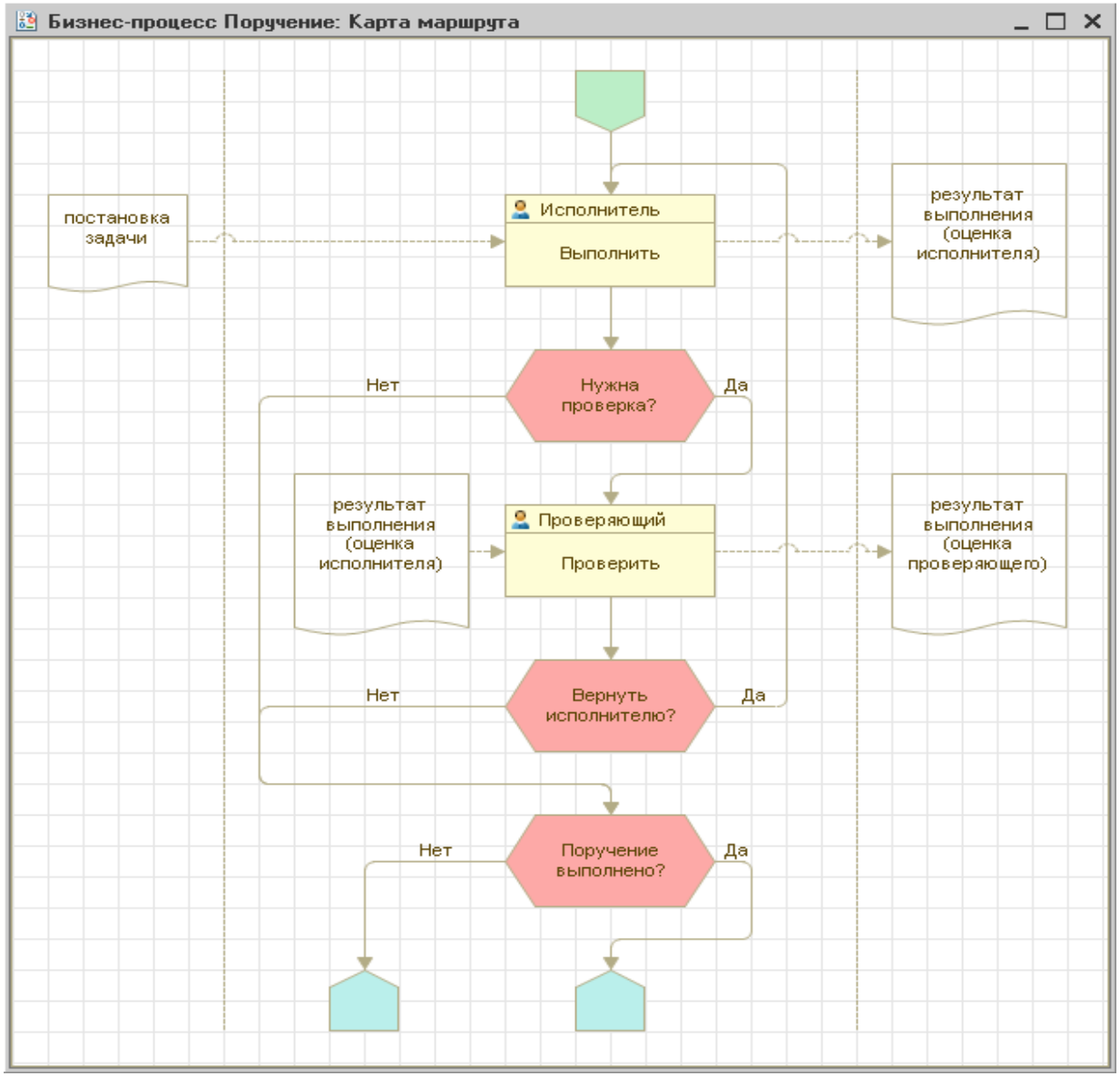
Модель организационной структуры



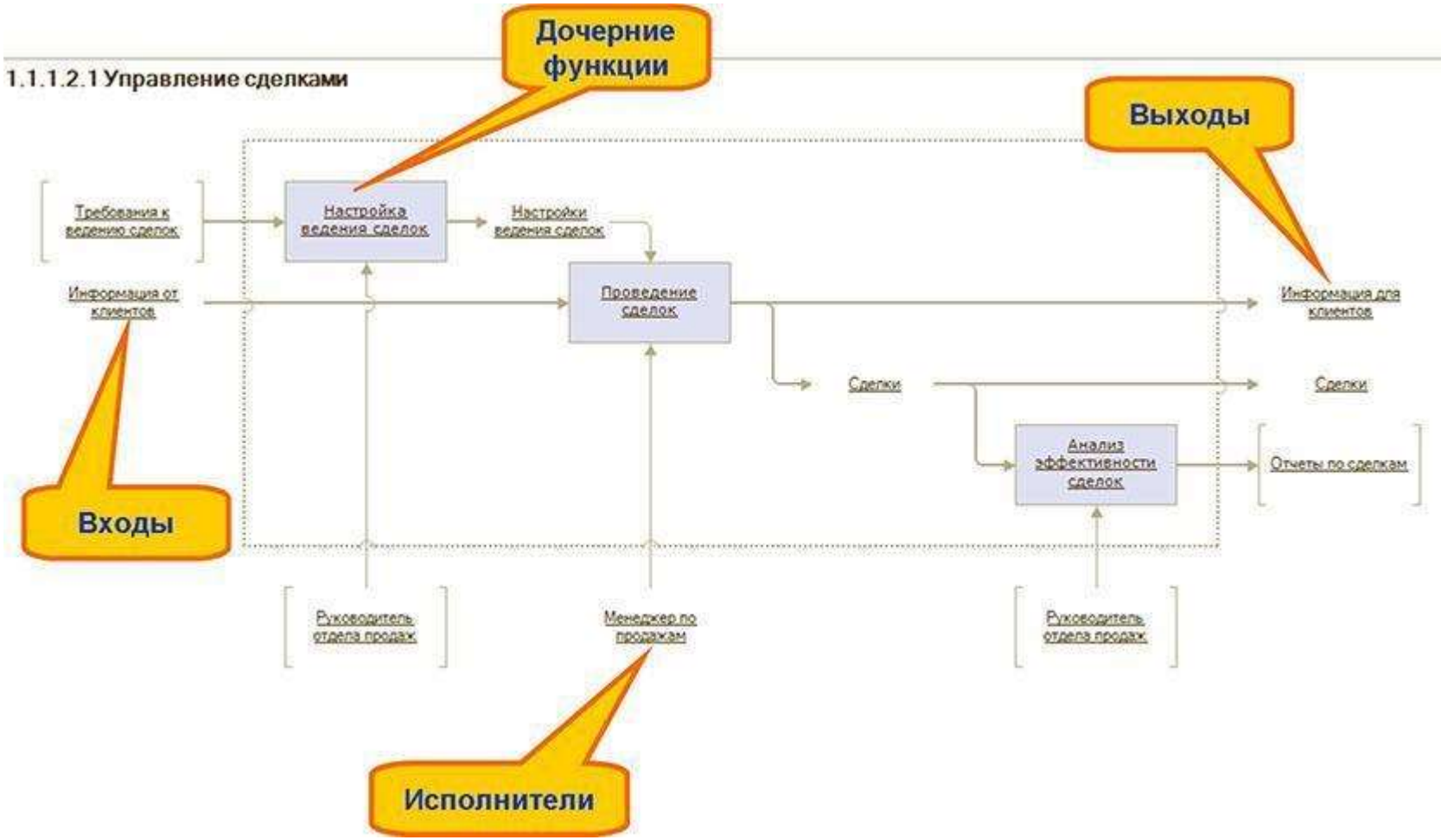
Информационная модель

4. 1С

- В состав стандартных объектов платформы 1С:Предприятие 8 входят объекты «Бизнес-процесс», для описания которых используется нотация, близкая к нотации 19.701-90.
- При проектировании прикладных решений с использованием специальных программных средств используется нотация IDEF0 с упрощённым оформлением.



Блок-схема бизнес-процесса



Упрощённая IDEF0 диаграмма