Проектная документация на ИС

Лекция 3

Стадии, документы, виды обеспечения

Овчинников П.Е.

МГТУ «СТАНКИН»,

ст.преподаватель кафедры ИС

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 (отменен!!!)

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.

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.

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.

ГОСТ Р МЭК 62443-2-1-2015

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

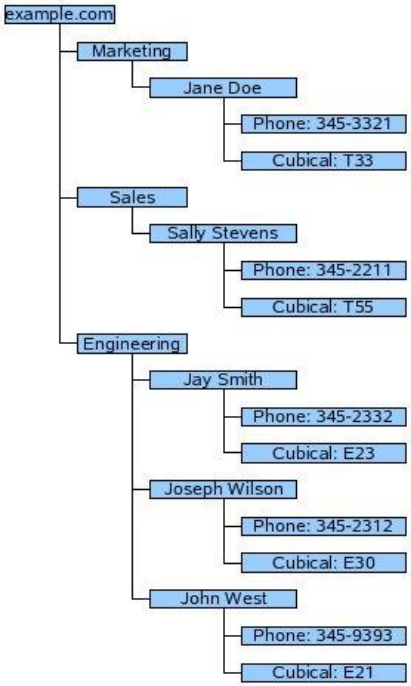
3.6 **биометрическая идентификация:** Преобразование совокупности примеров биометрических образов человека, позволяющее описать их стационарную и случайную составляющие, например, в виде математического ожидания и дисперсий контролируемых параметров или, например, в виде параметров обученной сети искусственных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

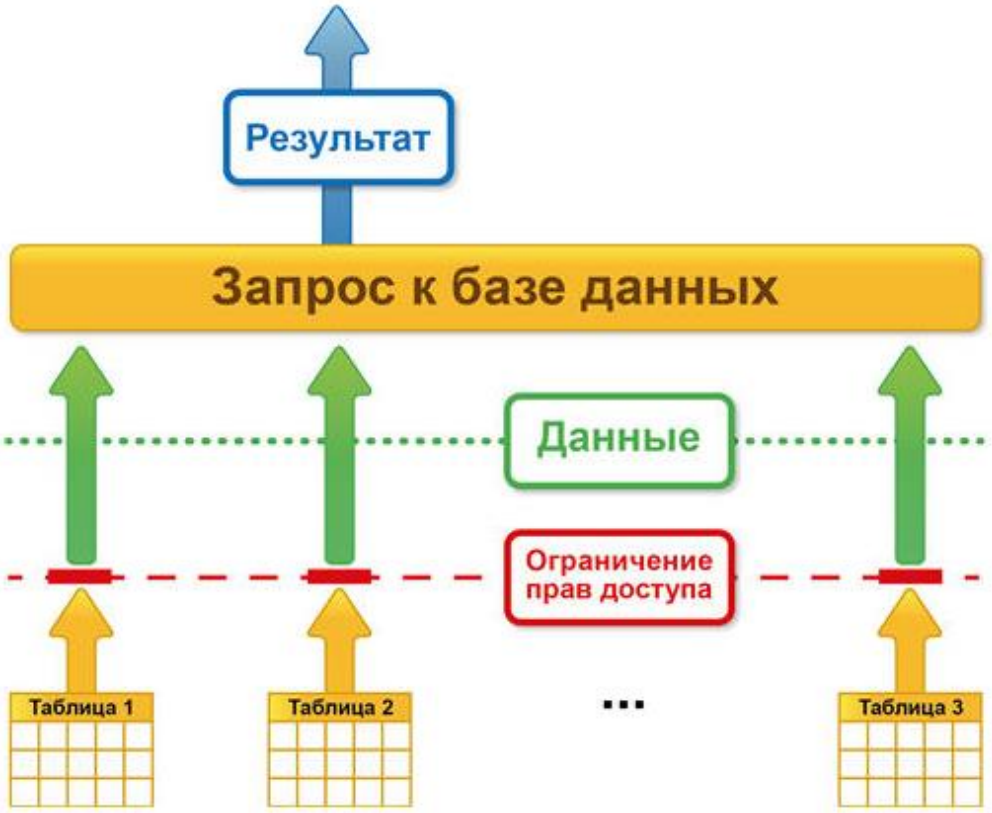
ГОСТ Р ИСО/МЭК 27000-2012
Р 50.1.056-2005
Биометрическая аутентификация

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





Р 50.1.056-2005
Права доступа в 1С:Предприятие
Active Directory (Википедия)

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).

ГОСТ Р ИСО/МЭК 27000-2012

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

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

ГОСТ Р 50922-2006

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.

ГОСТ Р 53114-2008
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".

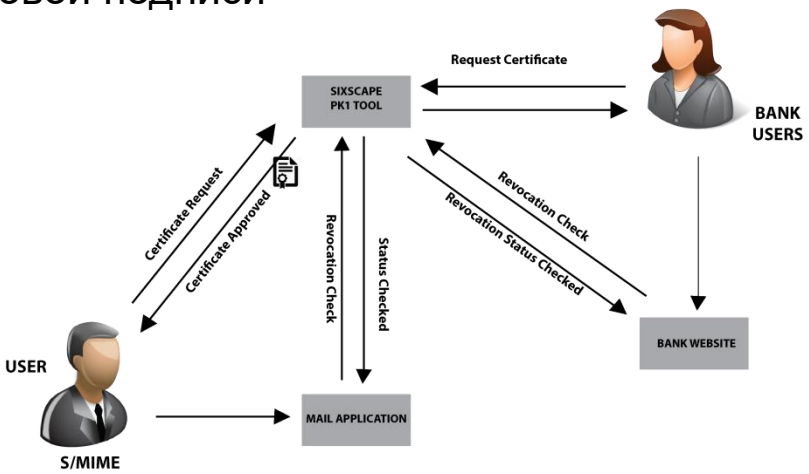
ГОСТ Р 54583-2011

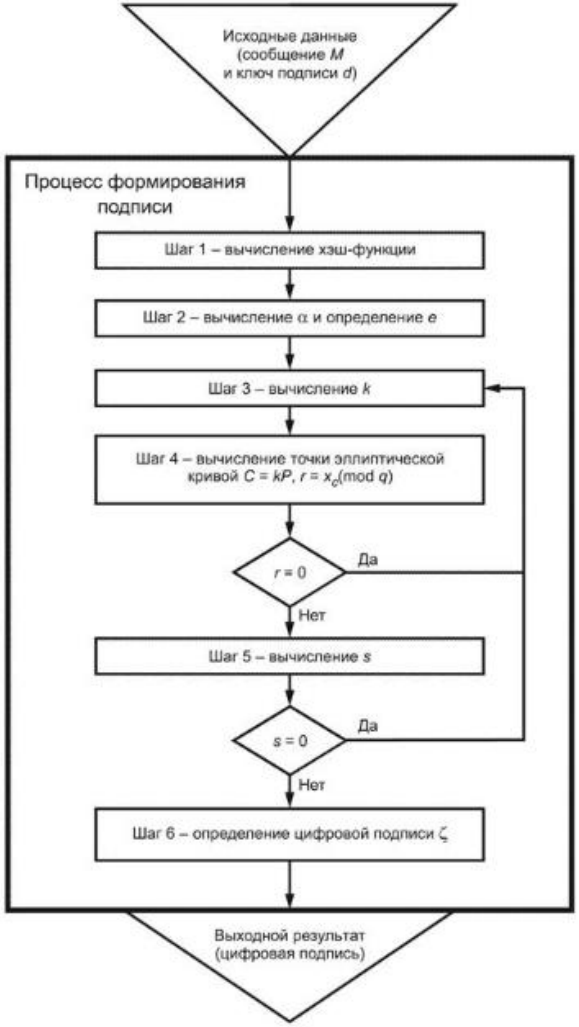
Криптография

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





[ГОСТ Р 34.10-2012]
[PKI]

От VUCA-миру к демо-версии новой реальности

Виды цифровых персональных данных граждан

BIS SUMMIT 2020

Типы данных	Кто собирает и использует	Зачем
• Лица • Окружение • Геоданные • Номера автомобилей • Связи • Тексты • Интересы • Голос • Пульс • Давление	• Госслужбы, муниципальные власти • Транспортные компании • Мобильные операторы • Интернет-компании	• Оптимизация процессов • Анализ потребностей людей в услугах, вакансиях, товарах • Обеспечение безопасности • Реклама и продажа товаров
	• Рекламщики • Мошенники • Экстремисты • Пропагандисты, политики • Спецслужбы	• Воровство паролей, логинов, денег, секретов • Шантаж, вербовка • Влияние на конкретных лиц и массы

4

От VUCA-миру к демо-версии новой реальности

Что можно вычислить по открытым данным

BIS SUMMIT 2020

Личные характеристики	Интересы, психология	Места, маршруты	Личную активность
• Ф.И.О. • Возраст • Лицо, фигура, приметы • Отпечатки пальцев, сигнатура голоса • Рост, вес, комплекция • Пульс, давление, температура • Болезни	• Хобби • Привычки • Пристрастия • Взгляды • Опасения • Фобии • Навязчивые идеи • Зависимости	• Адреса семьи • Места отдыха или частого пребывания • Офис • Ежедневные маршруты • Адреса друзей	• Используемые устройства • Приложения • Переписка • Поисковые запросы • Клики • Сайты • Посты, комментарии • Лайки • Покупки • Уровень расходов

Нужны законы, регулирующие сбор и использование ВЫЧИСЛЯЕМЫХ данных

[BIS Summit-2020]

От VUCA-миру к демо-версии новой реальности

Деструктивная информация

BIS SUMMIT 2020

В настоящий момент в социальных медиа действуют различные деструктивные течения и движения

- **СКУЛШУТИНГ, МАССОВЫЕ И СЕРИЙНЫЕ УБИЙСТВА**
- **КИБЕРБУЛЛИНГ** (травля в Интернете)
- **СУИЦИДАЛЬНЫЕ ГРУППЫ**
- **УЛЬТРАДВИЖЕНИЕ**
- **НАРКОМАНИЯ**
- **ШОК-КОНТЕНТ**

[BIS Summit-2020]

Задание на ВКР: Цель, Объект, Предмет

1. Описание задания на выполнение ВКР

1.1. Тип ВКР – исследовательская работа.

1.2. Цель исследования – обеспечить технологическую поддержку процессов автоматизированного комплектования сборочных единиц вычислительной техники.

1.3. Объект исследования – процессы выбора комплектующих при формировании заказов и сборке вычислительной техники.

1.4. Предмет исследования – программное и информационное обеспечение.

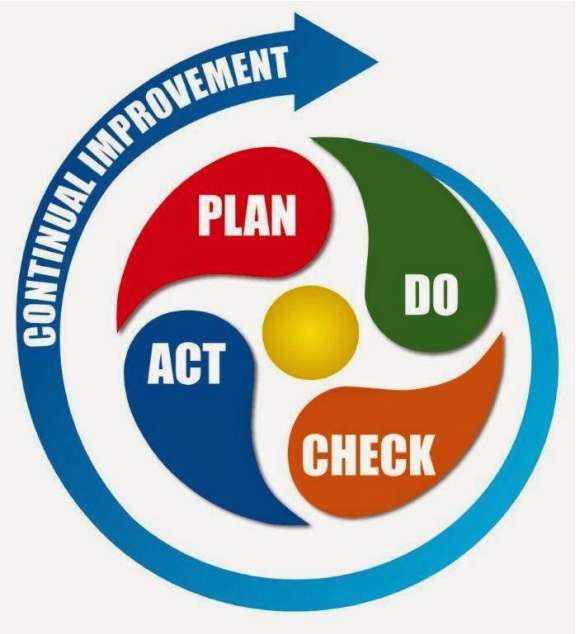
1.5. Методы исследования – системный анализ, процессный подход, функциональное моделирование, многокритериальное оценивание, прототипирование.

1.6. Задачи исследования:

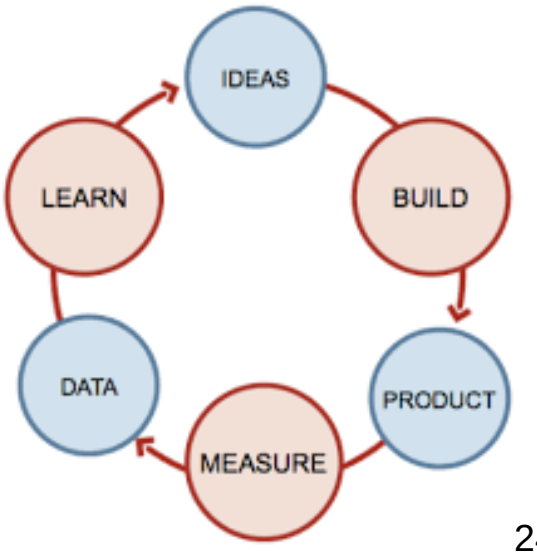
1.6.1. Проанализировать современные средства и сервисы для автоматизированного комплектования сборочных единиц.
1.6.2. Разработать комплекс функциональных моделей, моделей потоков и моделей базы данных информационной системы.
1.6.3. Обосновать выбор программных средств и программной среды для

Модели «как есть» и «как будет»

PDCA (англ. «Plan-Do-Check-Act» - планирование-действие-проверка-корректировка) циклически повторяющийся процесс принятия решения, используемый в управлении качеством. Также известен как цикл Деминга (Deming cycle), цикл Шухарта (Shewhart cycle)



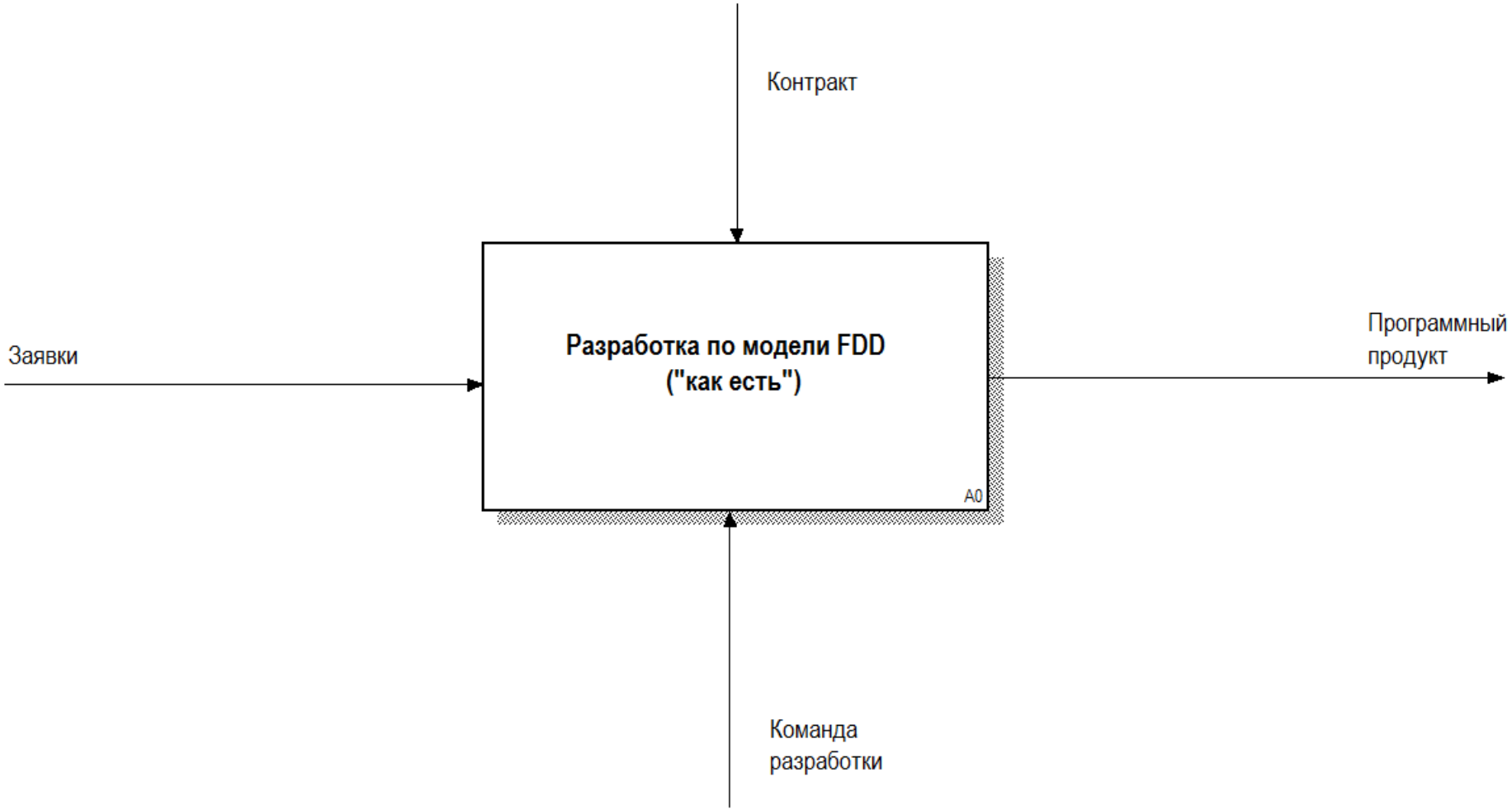
Customer Development Methodology (клиент-ориентированная методология) позволяет сфокусироваться не на разработке конкретного функционала продукта, а на понимании потребителей и их проблем



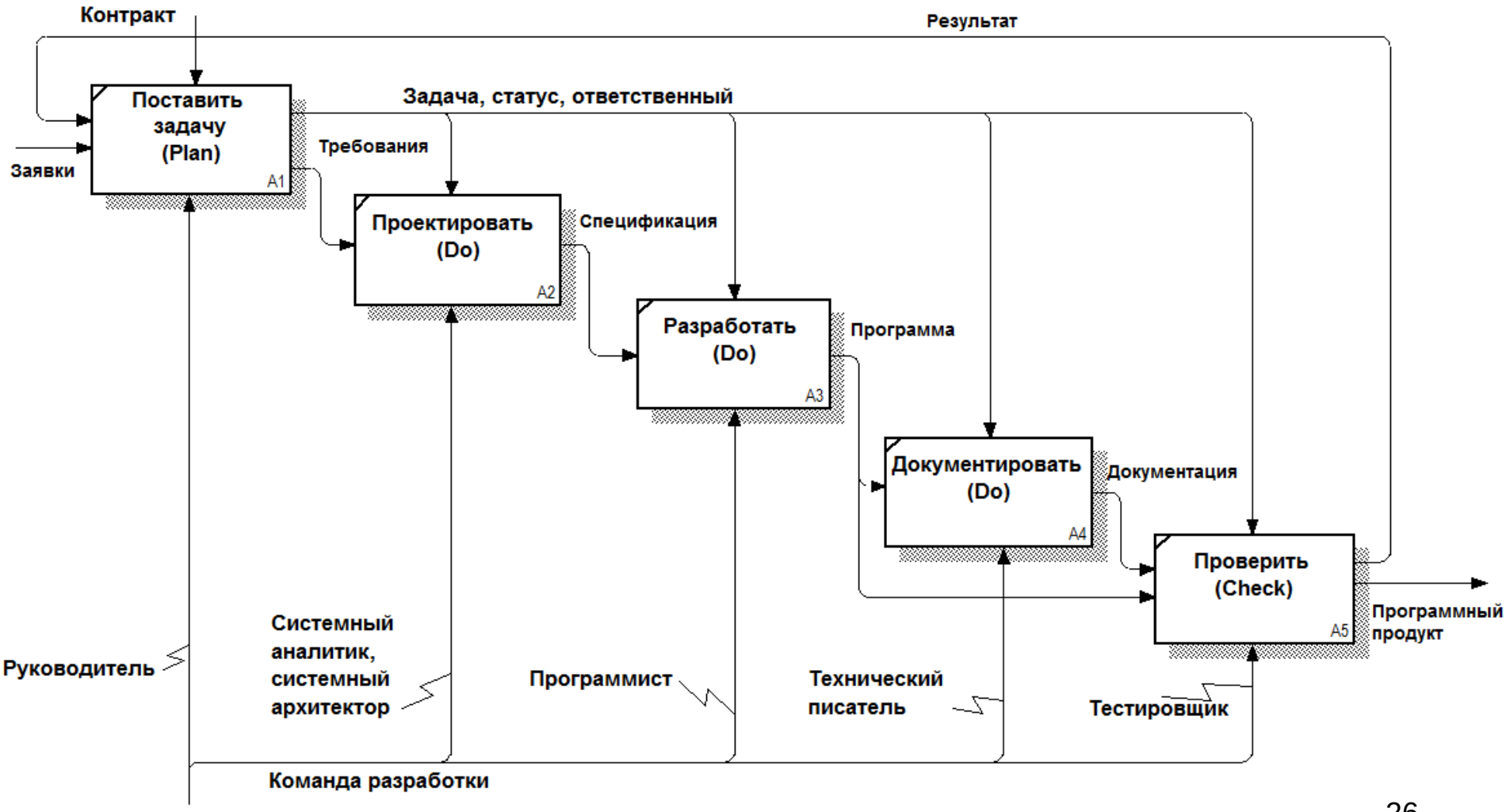
http://www.up-pro.ru/encyclopedia/deming-cycle.html
http://www.intuit.ru/studies/courses/3467/709/lecture/21817

Структурно-функциональный подход в ВКР (задача: определить контекст)

Модель FDD

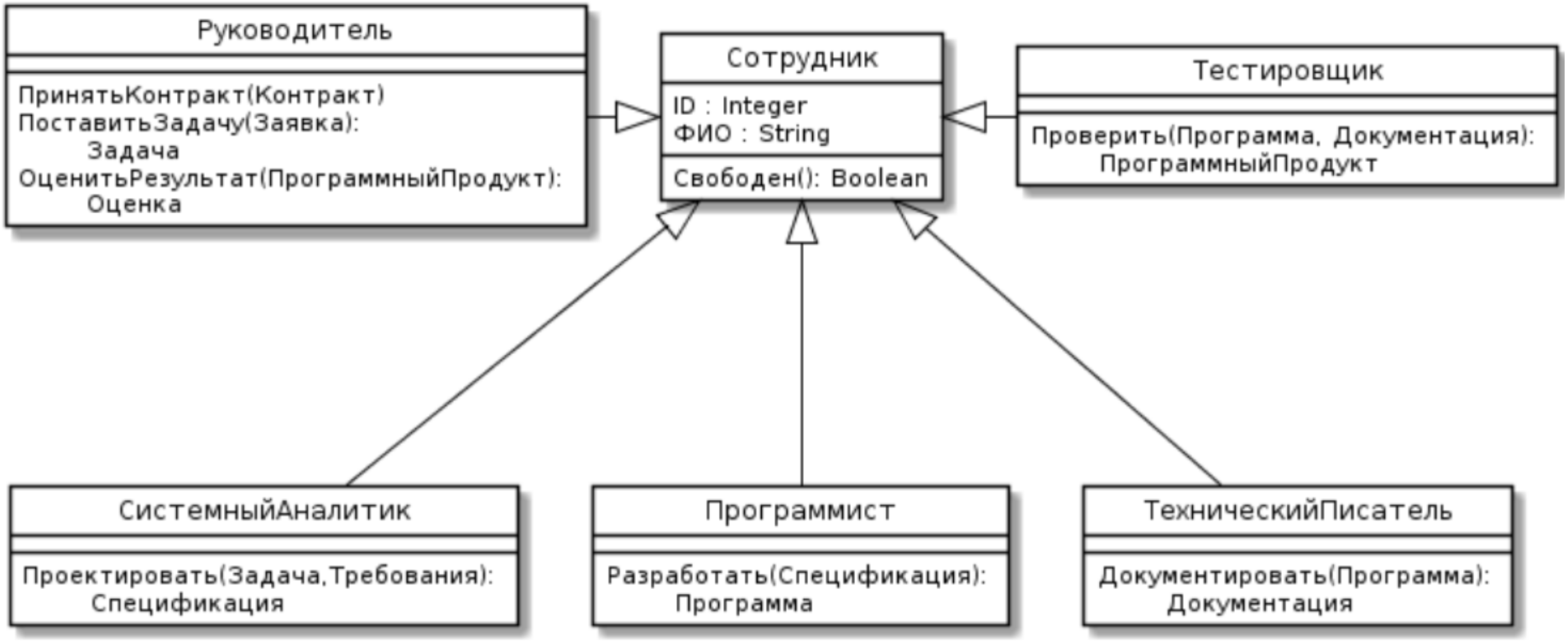


Структурно-функциональный подход в ВКР (задача: определить участников) Модель FDD и команда



Структурно-функциональный подход в ВКР (задача: определить участников)

Модель FDD и команда

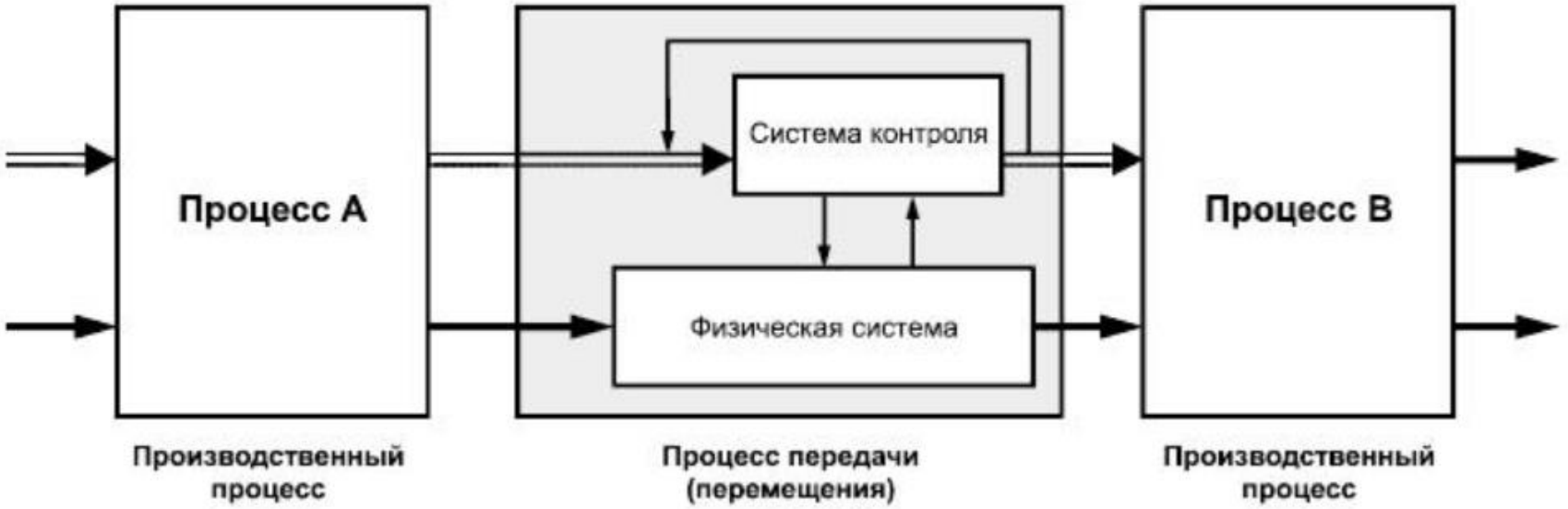


http://www.intuit.ru/studies/courses/3467/709/lecture/21825
http://www.intuit.ru/studies/courses/3467/709/lecture/21825?page=2

Терминология: поток

ГОСТ Р ИСО 15531-43-2011 Системы промышленной автоматизации и интеграция. Данные по управлению промышленным производством. Часть 43. Информация для управления производственными потоками. Модель данных для мониторинга и обмена производственной информацией

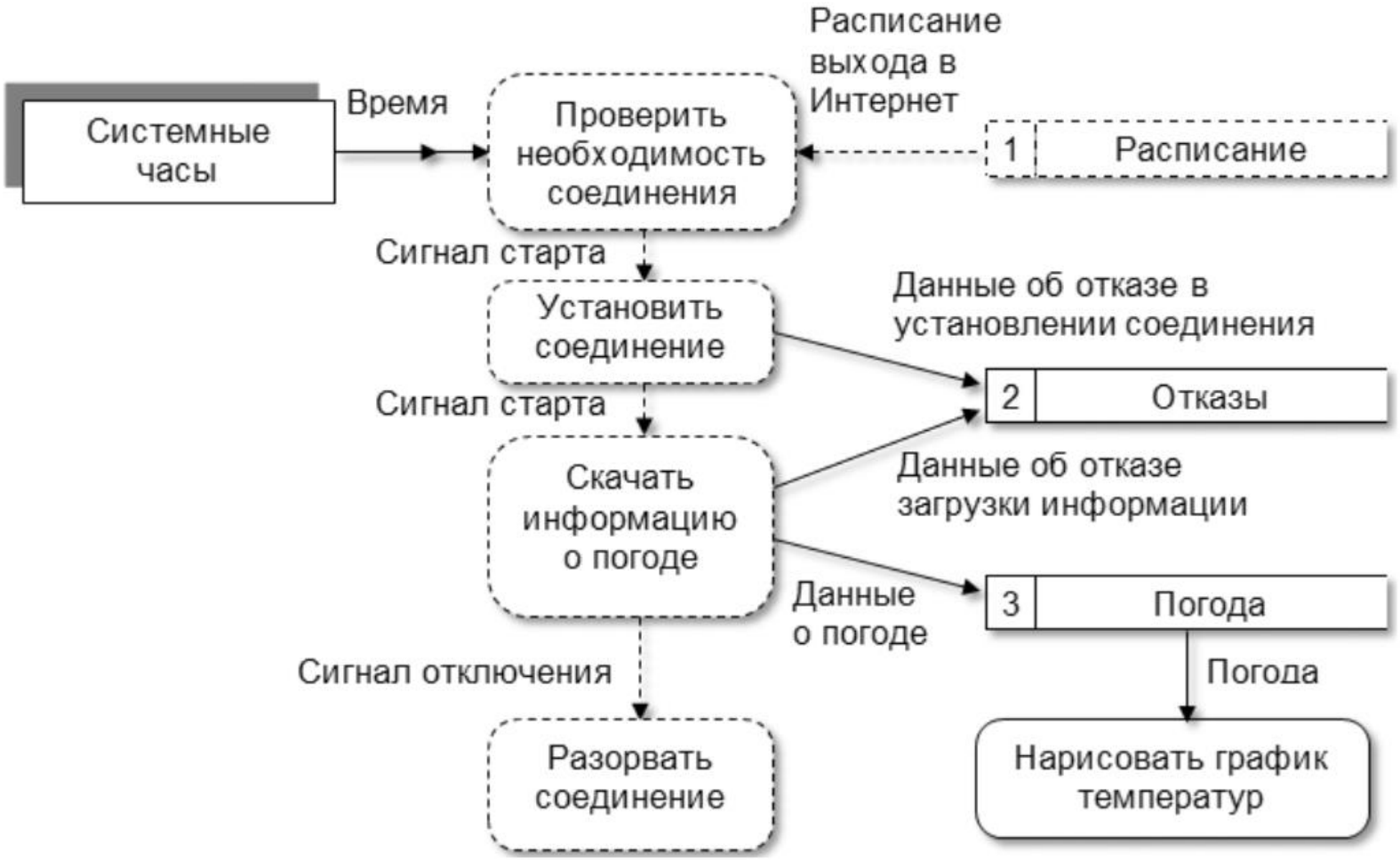
поток (flow): Движение множества физических или информационных объектов в пространстве и времени.



ГОСТ Р ИСО 15531-43-2011

Структурно-функциональный подход в ВКР (задача: определить потоки данных)

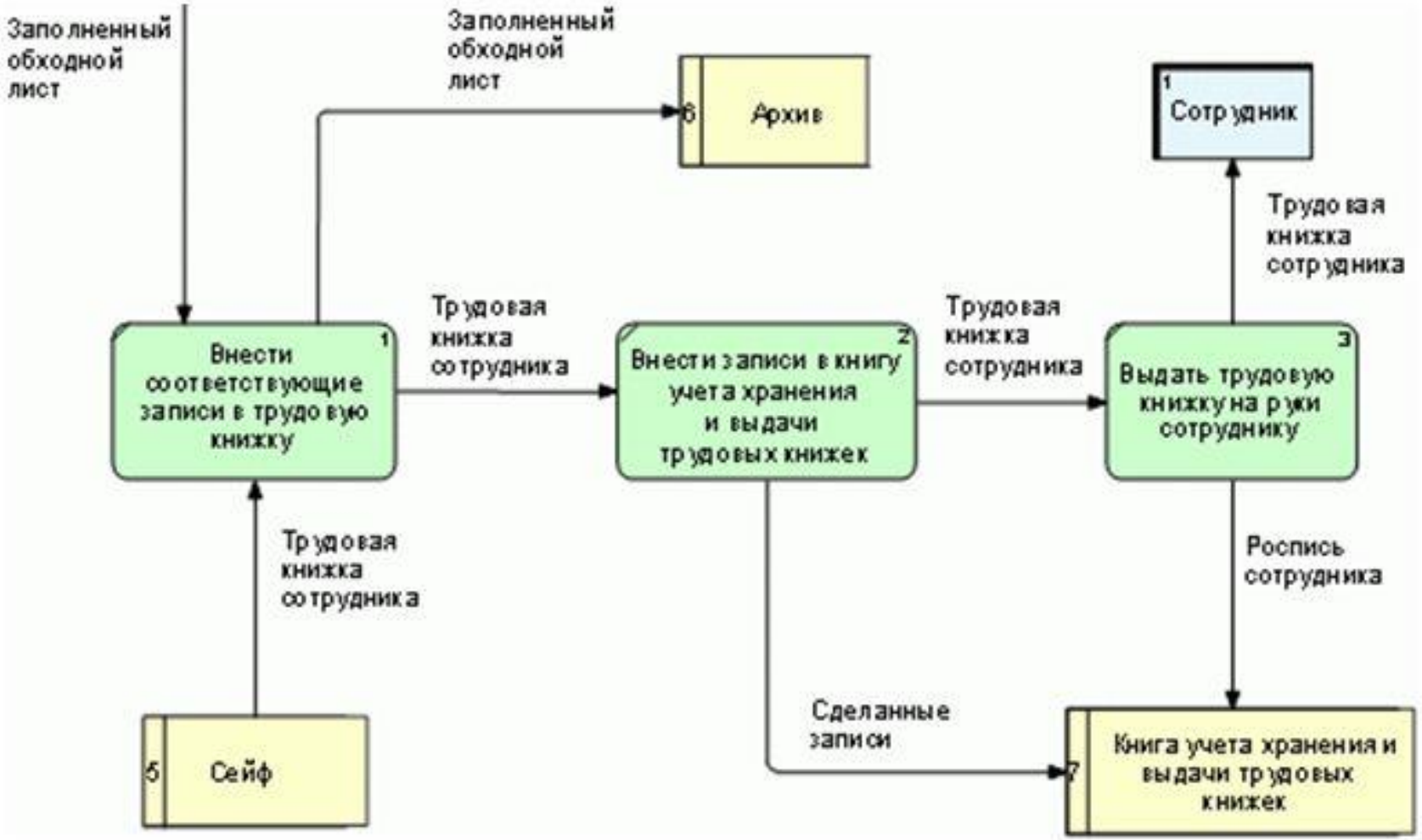
DFD - Нотация Гейна-Сарсона



DFD - Расширения

Структурно-функциональный подход в ВКР (задача: определить потоки данных)

DFD - Нотация Гейна-Сарсона

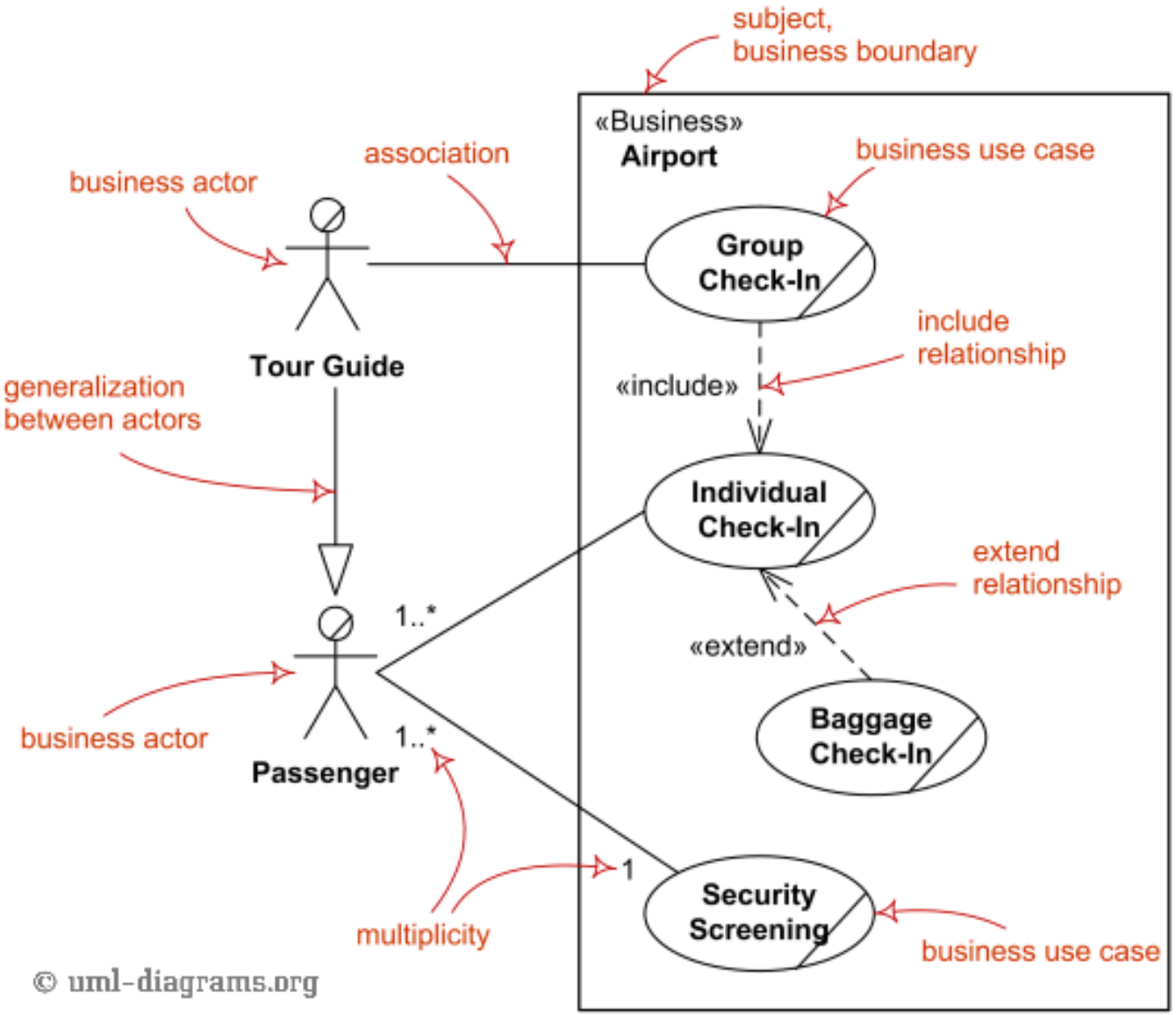


BPWin, RAMUS

Курсовой проект

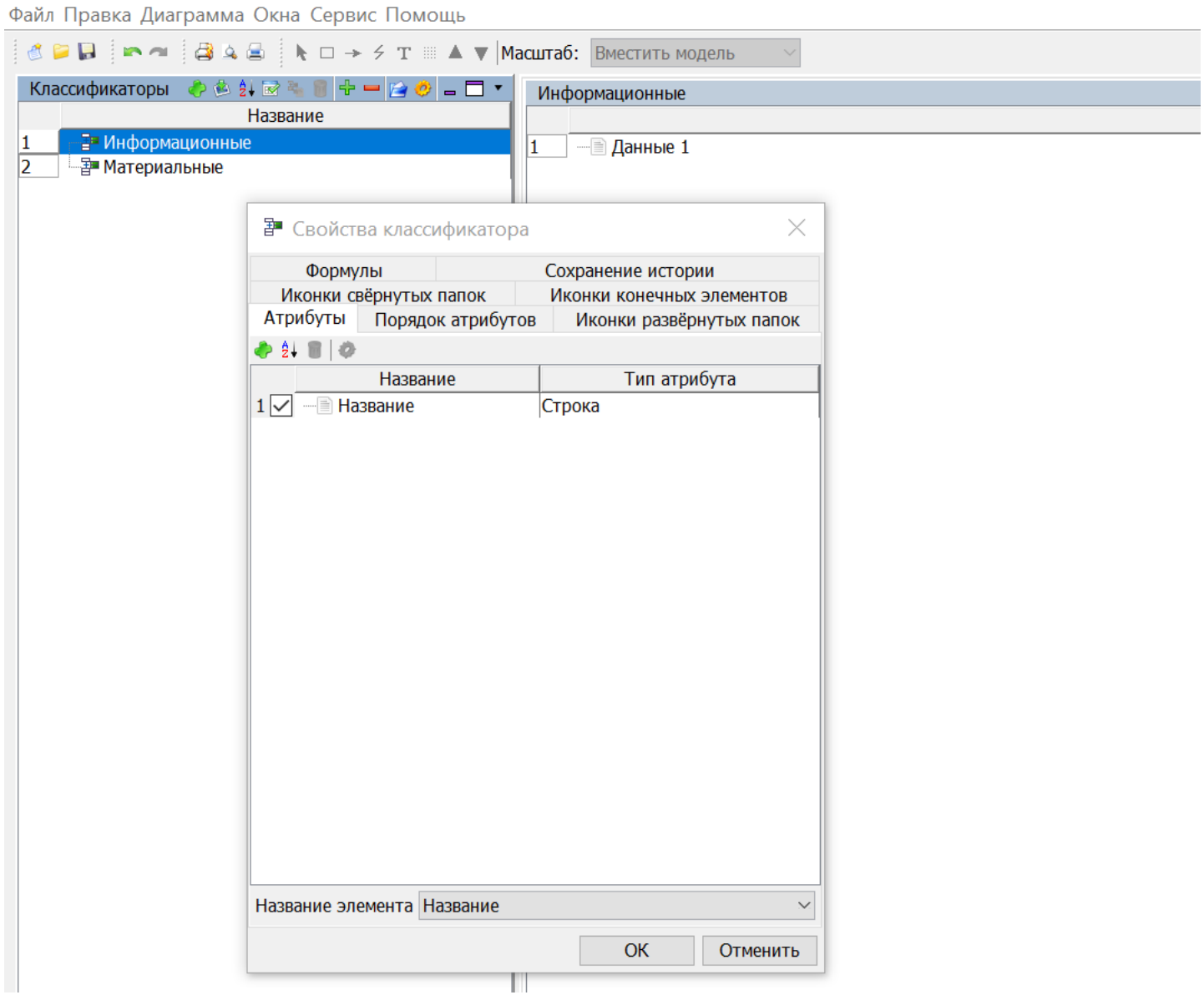
Материалы курса

ООП: UML Use Case



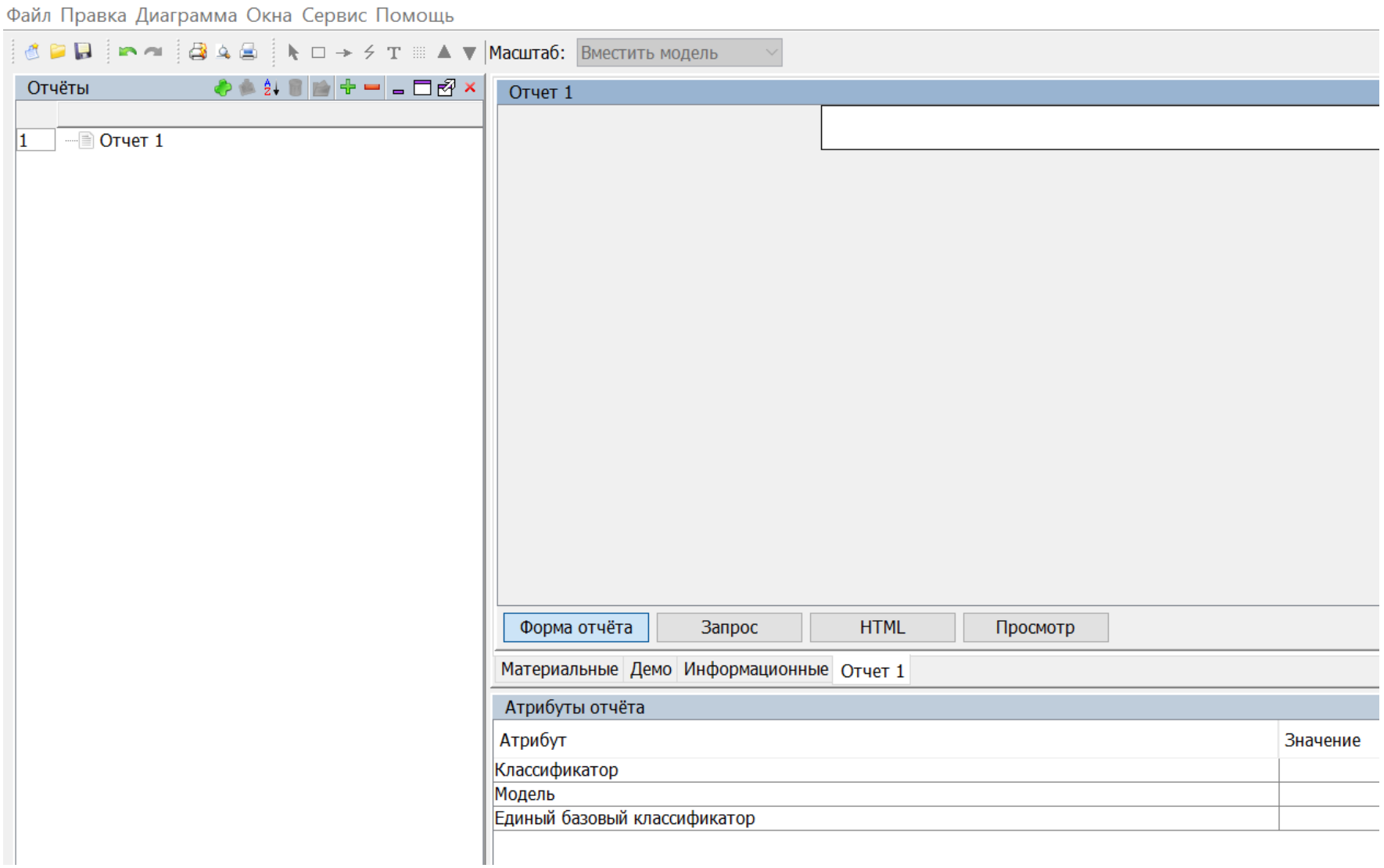
http://www.uml-diagrams.org/use-case-diagrams.html

РАМУС: Классификаторы

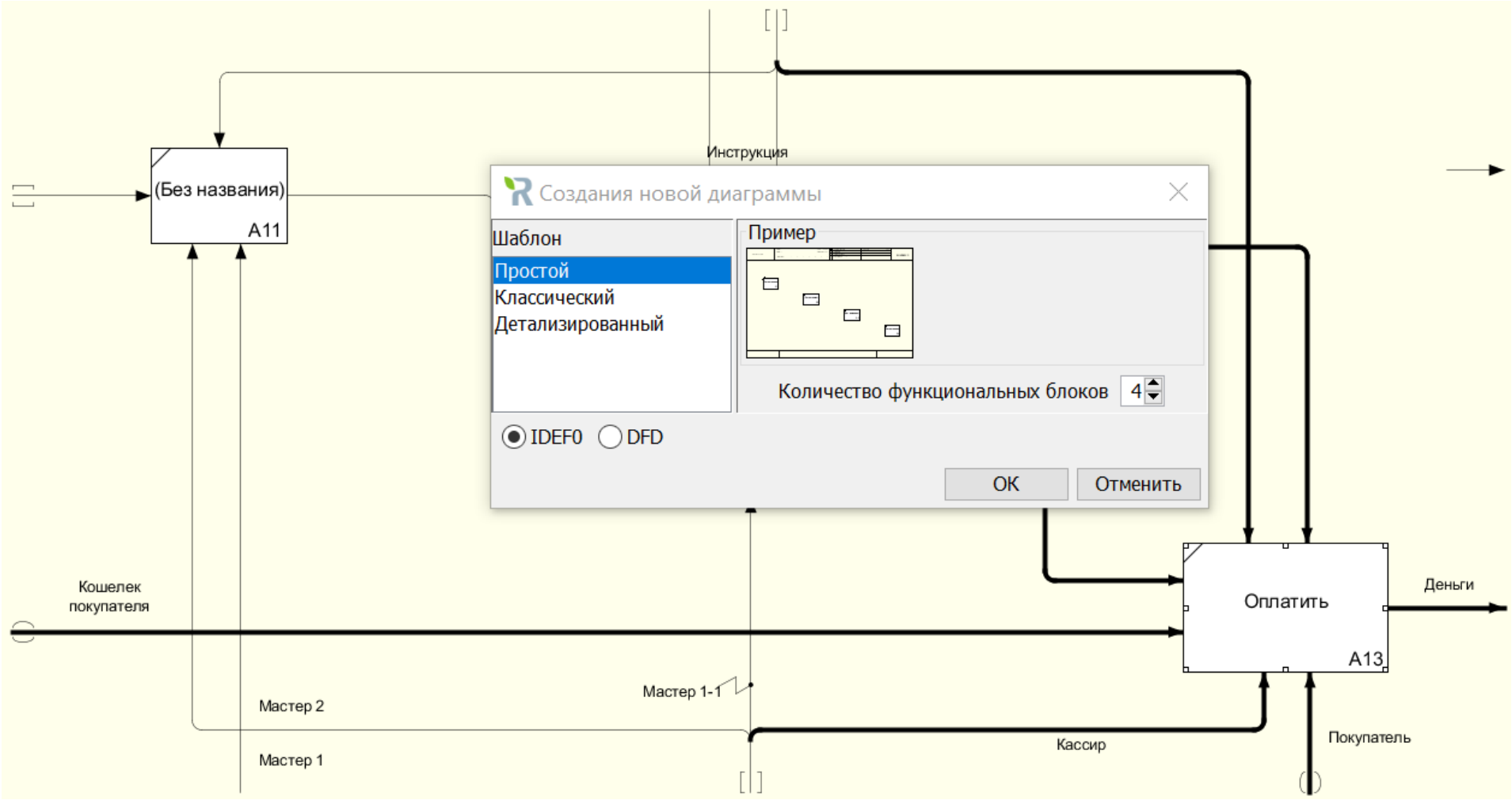


BPWin, RAMUS

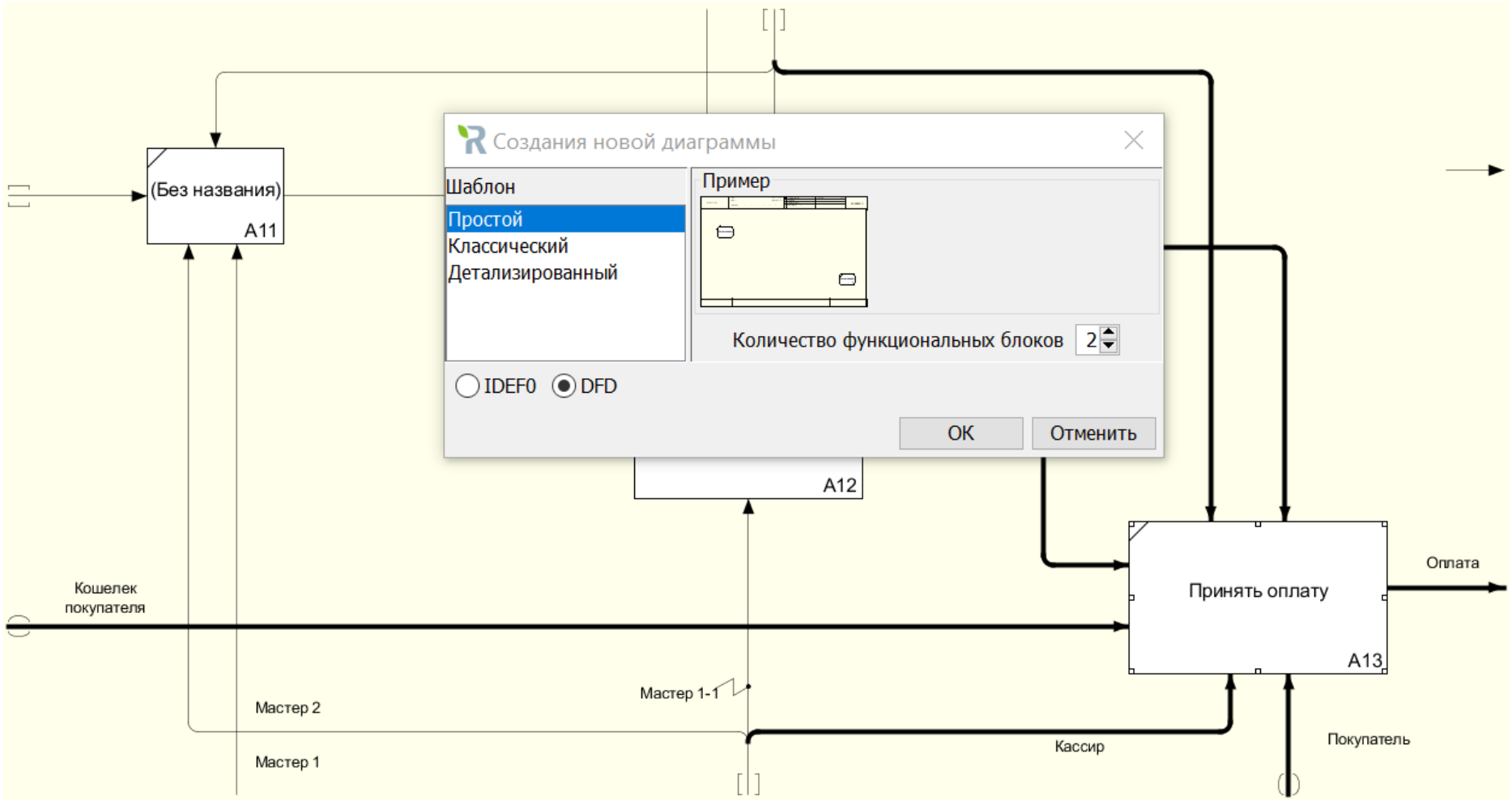
РАМУС: Отчеты



РАМУС: Декомпозиция в DFD



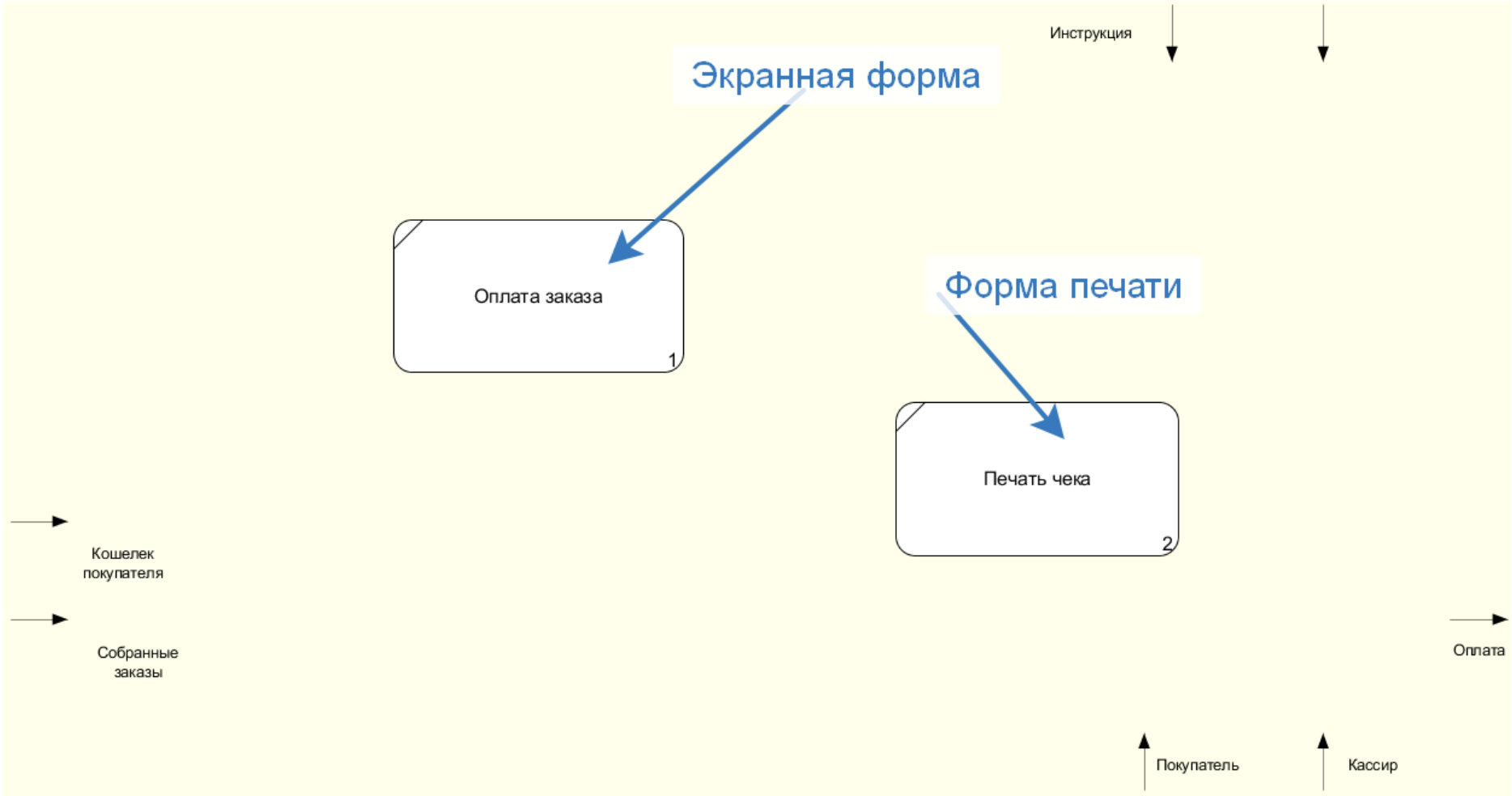
РАМУС: Декомпозиция в DFD



РАМУС: Декомпозиция в DFD

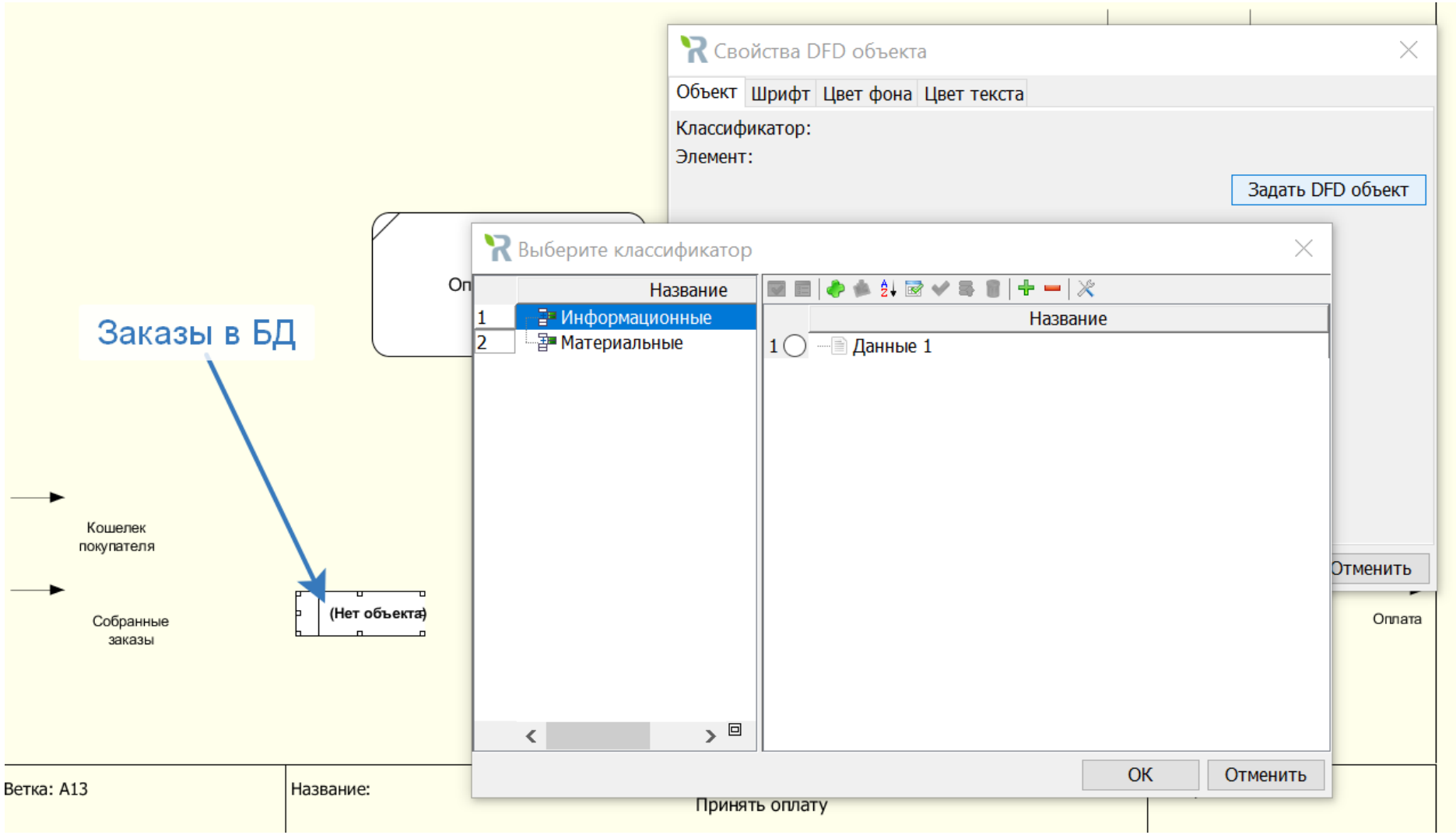
BPWin, RAMUS

РАМУС: Декомпозиция в DFD



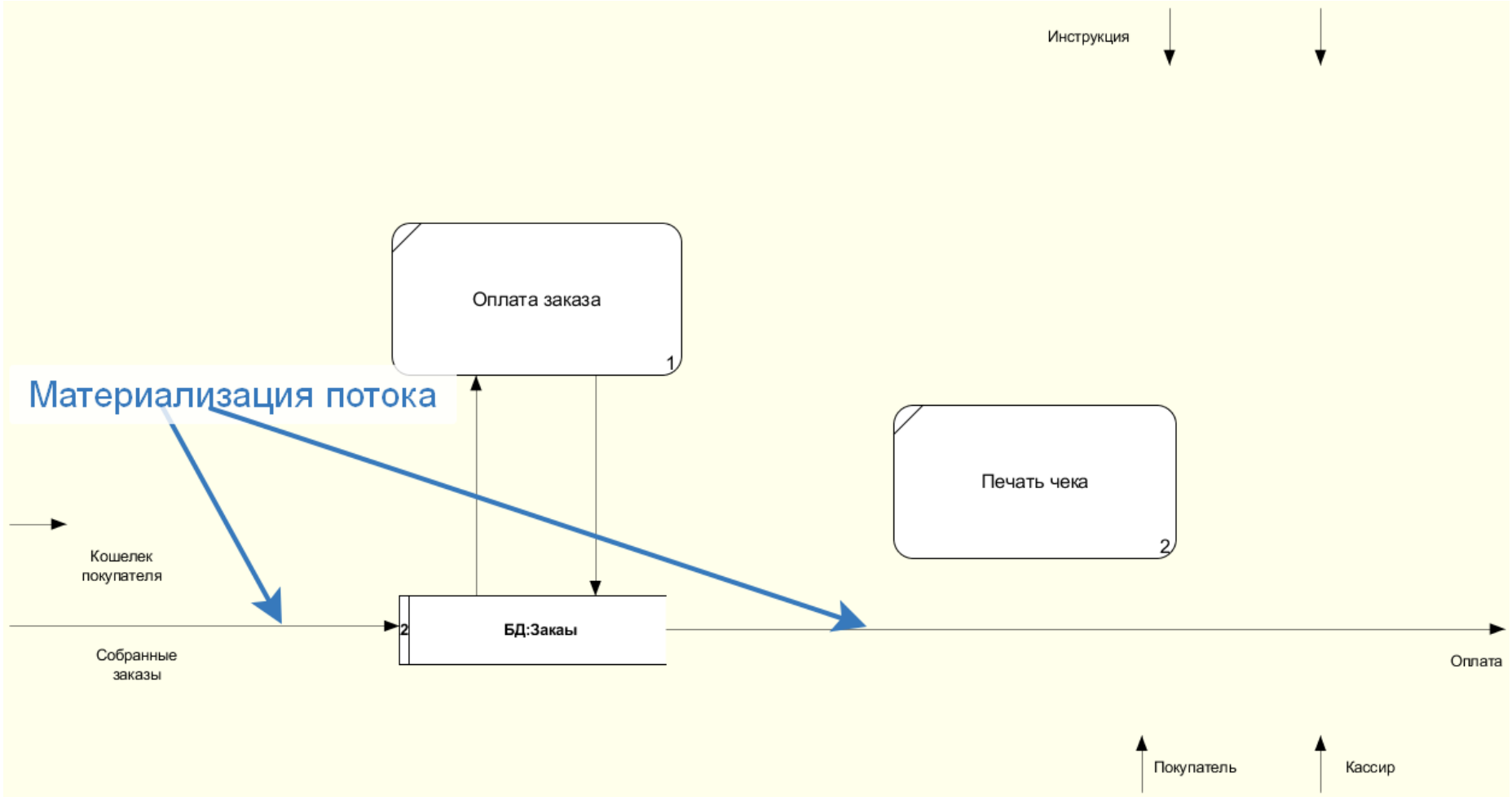
BPWin, RAMUS

РАМУС: Декомпозиция в DFD



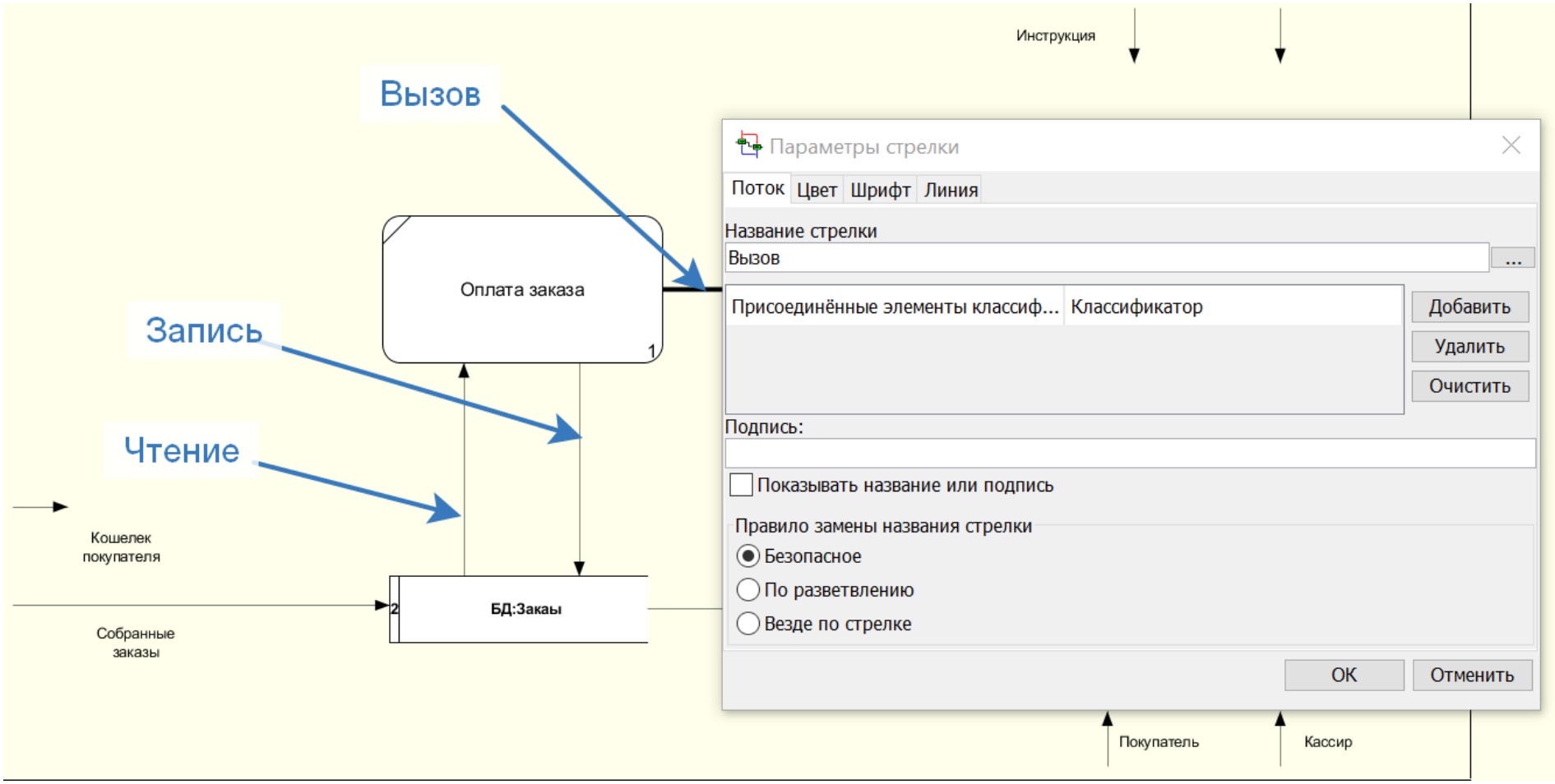
[BPWin, RAMUS]

РАМУС: Декомпозиция в DFD



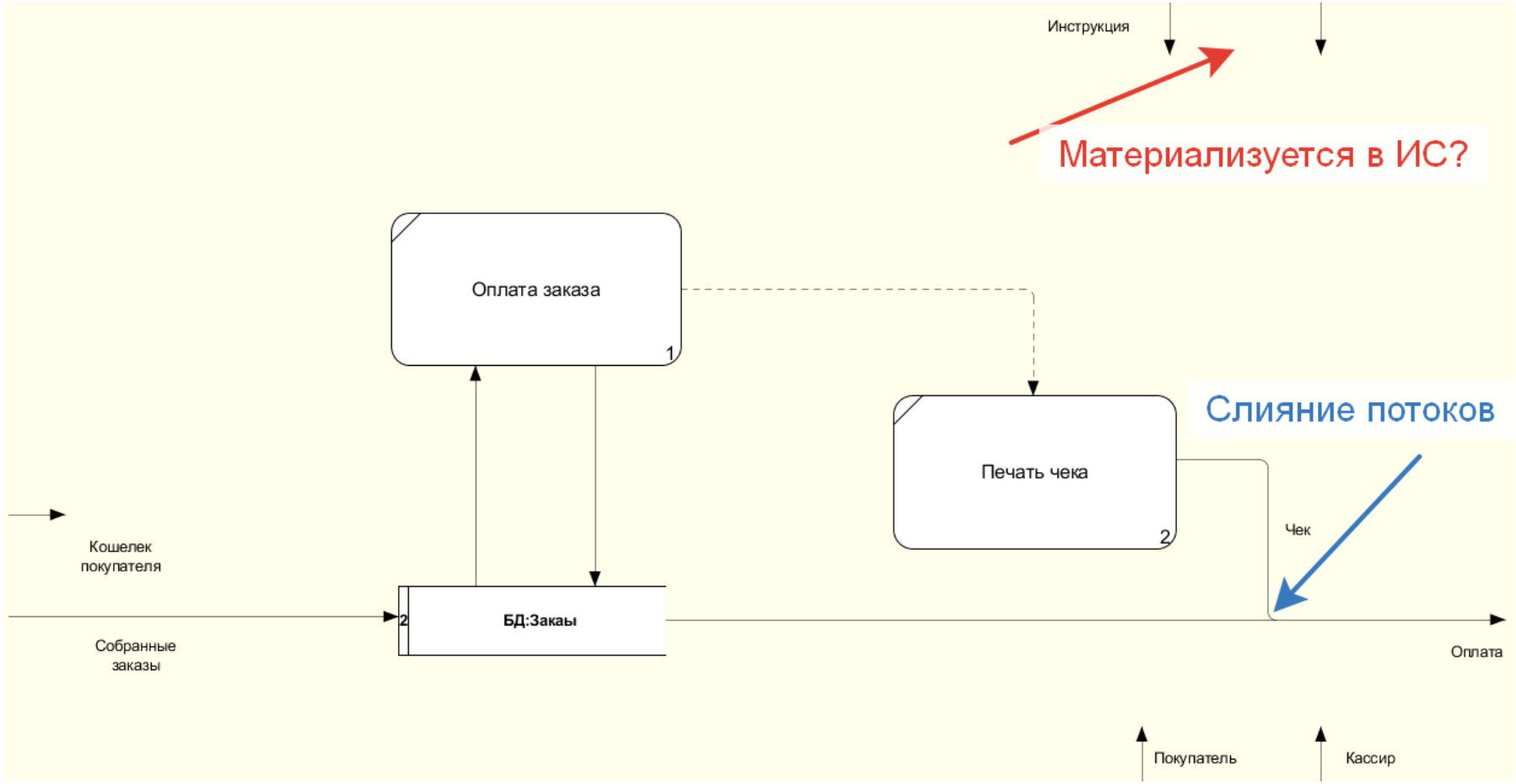
BPWin, RAMUS

РАМУС: Декомпозиция в DFD



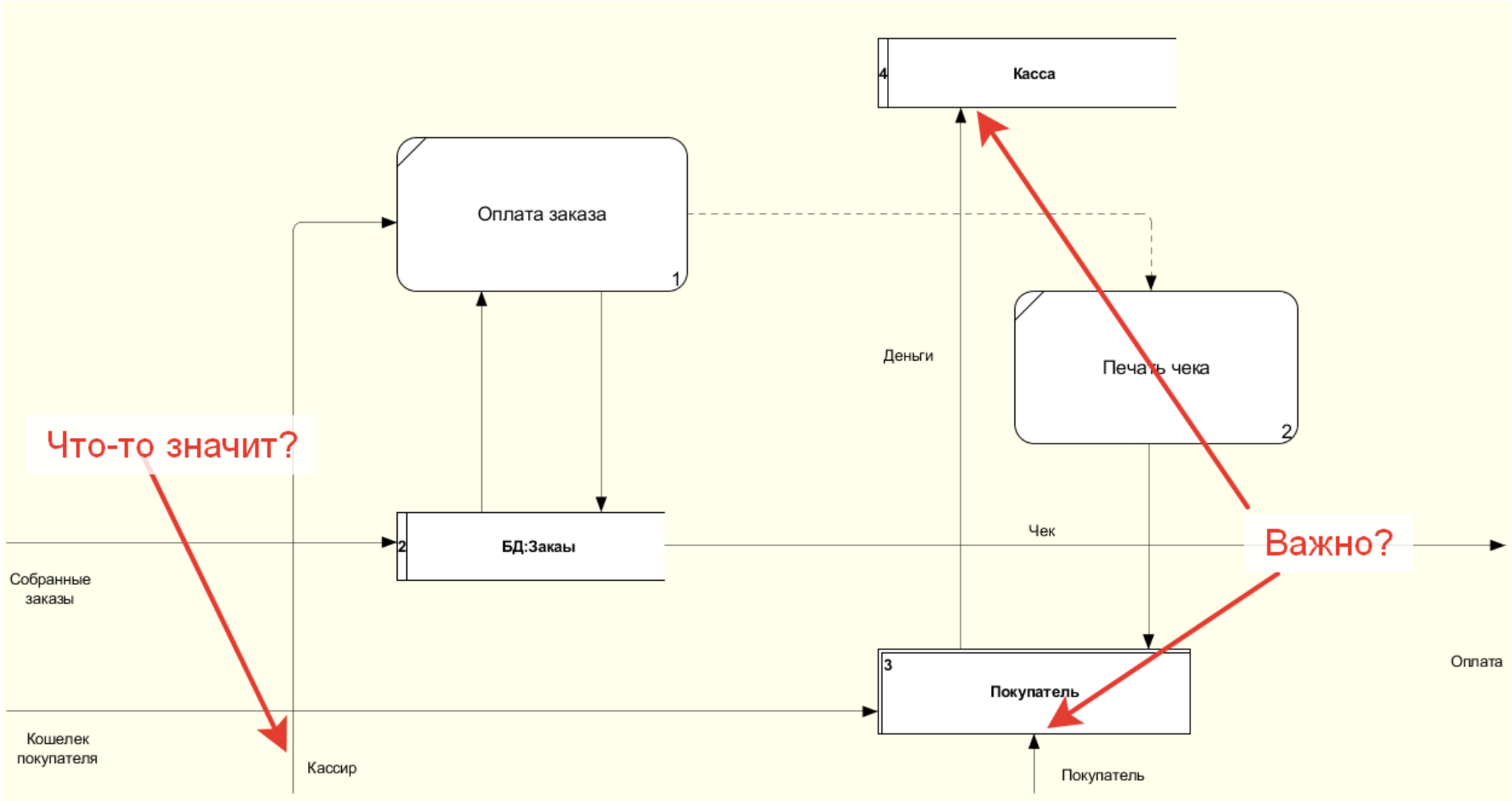
[BPWin, RAMUS]

РАМУС: Декомпозиция в DFD



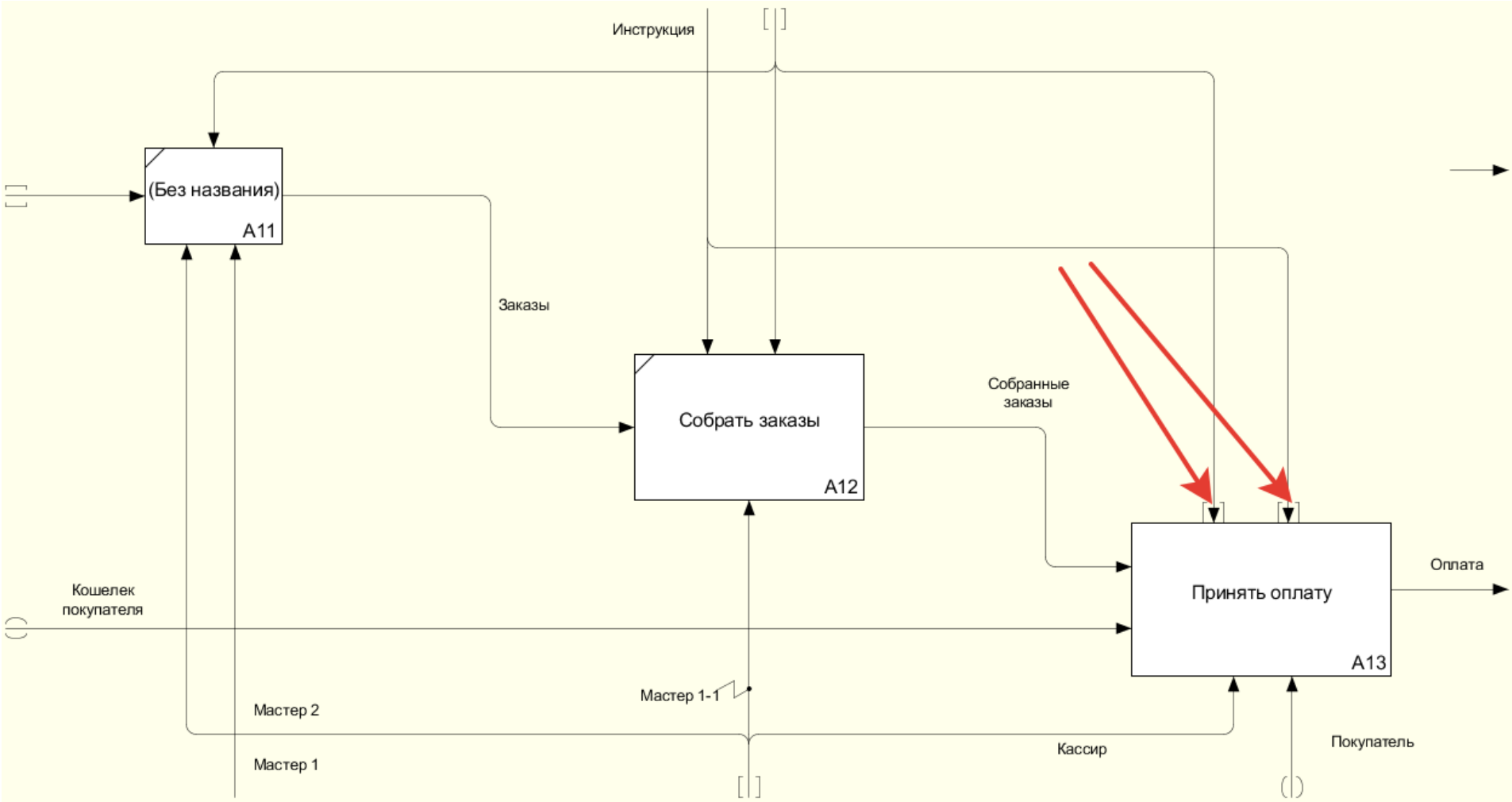
BPWin, RAMUS

РАМУС: Декомпозиция в DFD

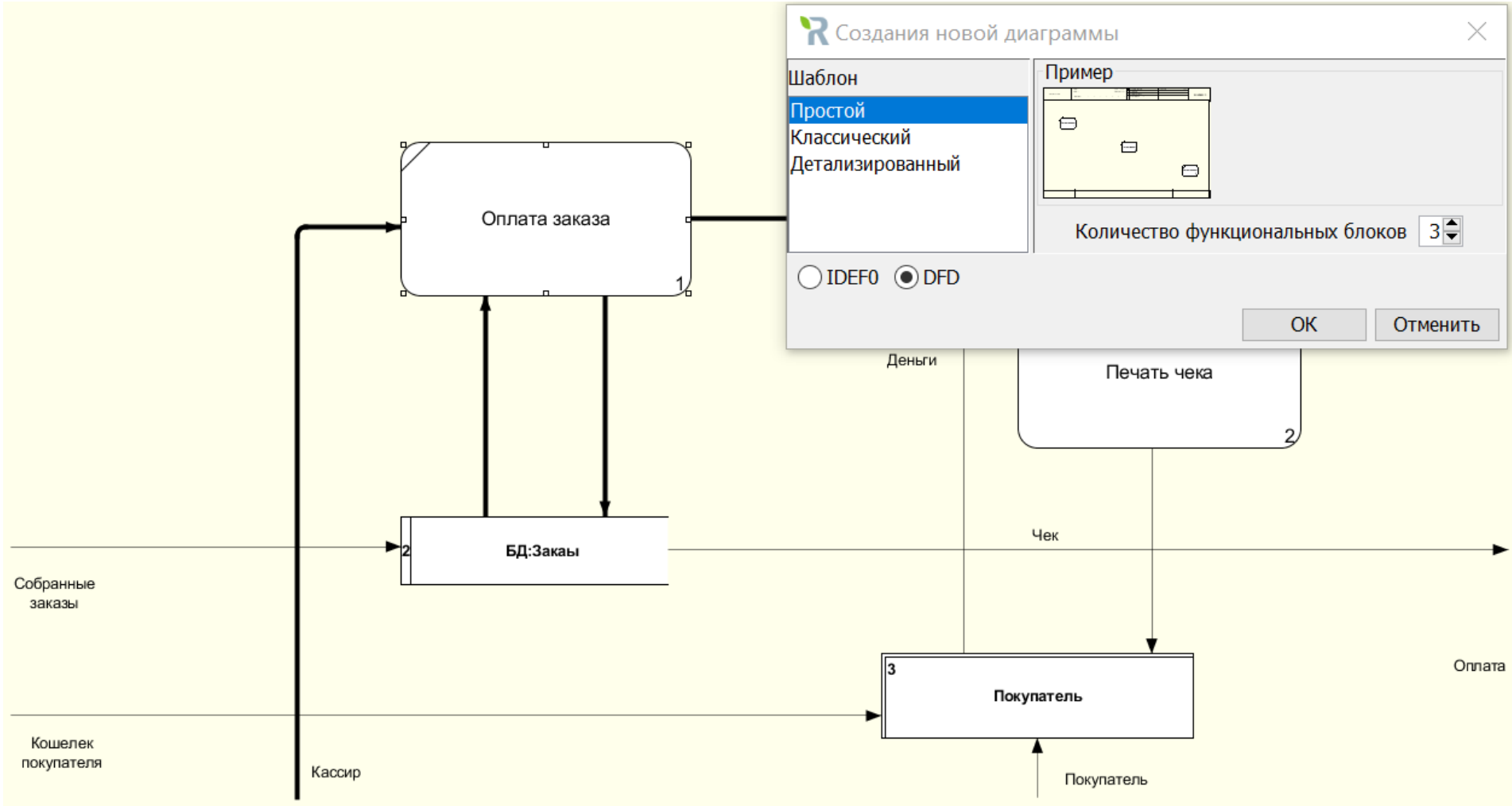


BPWin, RAMUS

РАМУС: Декомпозиция в DFD



РАМУС: Декомпозиция в DFD



[BPWin, RAMUS]