Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Томский государственный университет систем управления и радиоэлектроники»
(ТУСУР)

УТВЕРЖДАЮ

Заведующий кафедрой
«Управление инновациями»

_____ */А.Ф.Уваров*
(подпись) *(ФИО)*
"_____" _____ 2013 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ЛАБОРАТОРНЫМ РАБОТАМ

по дисциплине

«Информационные технологии в управлении качеством и защита информации»

Составлены кафедрой «Управление инновациями»

Для студентов, обучающихся
по направлению подготовки бакалавров
221400.62 «Управление качеством»

Форма обучения: очная

Составитель
Доцент каф. УИ, к.ф.-м.н. Годенова Е.Г.

" 18 " января 2013 г.

Томск 2013 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Изучению дисциплины «Информационные технологии в управлении качеством и защита информации» отводится одно из важнейших мест при подготовке бакалавров по направлению 221400.62 «Управление качеством». Об этом, в частности, свидетельствует тот факт, что согласно ФГОС направления «Управление качеством» данная дисциплина отнесена к разделу базовых дисциплин профессионального блока подготовки бакалавров.

Целью курса «Информационные технологии в управлении качеством и защита информации» является формирование у студентов целостного представления о роли современных информационных технологий в управлении качеством организаций и обеспечении безопасности информационных ресурсов предприятий.

Задачи курса:

- ✓ ознакомить обучающихся с рядом графических нотаций, применяемых для разработки альбомов бизнес-процессов организаций;
- ✓ сформировать у обучающихся навыки работы с рядом современных программных продуктов для визуализации, оценки и анализа эффективности деятельности организаций;
- ✓ ознакомить обучающихся с международными стандартами информационной безопасности, российской нормативно-правовой базой в области защиты информации;
- ✓ освоить базовые понятия и навыки по разработке политики безопасности компании;
- ✓ ознакомить студентов с методологией построения комплексной защиты информационной среды предприятия.

В результате изучения дисциплины студент должен:

Знать: основные информационные технологии в управлении качеством;

Уметь: использовать технологии проектирования моделей данных на различных уровнях: концептуальном, логическом и физическом;

Владеть: методами защиты информации.

По курсу «Информационные технологии в управлении качеством и защита информации» предусмотрены лабораторные работы в двух семестрах, ориентированные на практическое закрепление лекционного материала и самостоятельной работы студентов. Лабораторные работы направлены на формирование у студентов навыков разработки моделей бизнес-процессов организаций (предприятий) различного уровня; знаний о классах и критериях существующих угроз информационной безопасности; понимание

важности защиты конфиденциальной информации, практических умений по защите документооборота и файлов от различных форм несанкционированного доступа и непреднамеренного воздействия, навыков разработки управленческих мер по защите информации организации.

На изучение курса «Информационные технологии в управлении качеством и защита информации» согласно учебному плану направления 221400.62 «Управление качеством» отводится два семестра. Курс логически разбит на два блока. Лабораторные работы первого блока «Информационные технологии в управлении качеством» проводятся в осеннем семестре и направлены на приобретение студентами компетенций в области разработки моделей бизнес-процессов предприятия, как простого уровня, так и комплекса моделей. При этом в ходе выполнения лабораторных работ студенты осваивают три различные нотации визуального моделирования бизнес-процессов. Второй блок «Защита информации» содержит курс лабораторных работ, направленных на формирование компетенций в области защиты документооборота, разработки управленческих документов по защите информации, защиты файлов от несанкционированного доступа и использования. Данное разбиение курса является логическим и целесообразным с точки зрения последовательности изложения материала и взаимодействия с другими дисциплинами учебного плана.

В первый блок входит 8 лабораторных работ. Восьмая лабораторная работа является итоговой работой семестра, при выполнении которой студенты должны продемонстрировать компетенции, полученные ими на лекциях, за время самостоятельной работы и лабораторных работ. Один академический час отводится на написание итогового тестирования за семестр. Тестовые задания представлены в приложении А к данным методическим рекомендациям. В ходе выполнения лабораторных работ студенты осваивают три нотации моделировании бизнес-процессов, которые рекомендуются в дальнейшем для применения при выполнении итоговой работы. Таким образом, максимально оптимизируется учебный процесс при посещении студентами лекций, лабораторных работ и самостоятельной работе.

Во второй блок входит 9 лабораторных работ по защите информации (физической, криптографической и т.д.), выполнение которых позволит студентом приобрести компетенции для выполнения итоговой работы по разработке политики безопасности компании. Изучение блока приходится на весенний семестр. По окончанию цикла лабораторных работ предусмотрено итоговое тестирование. Материалы тестов находятся в Приложении В к данным методическим рекомендациям.

ТРЕБОВАНИЯ К ЗНАНИЯМ СТУДЕНТОВ

Для полноценного освоения студентами дисциплины «Информационные технологии в управлении качеством и защита информации» рекомендуется изучение следующих дисциплин:

1) информатика;
2) информационные технологии;
3) теоретические основы информатики;
4) статистические методы в управлении качеством;
5) информационное обеспечение, базы данных
6) средства и методы управления качеством.

Для наиболее продуктивного выполнения лабораторных работ рекомендуется, но не является обязательным условием, изучение дисциплин:

1) основы обеспечения качества;
2) всеобщее управление качеством;
3) делопроизводство.

Ход выполнения лабораторных работ

Каждая лабораторная работа посвящена определенной теме и может быть организована в любой форме по усмотрению преподавателя. Однако каждая из комплекса лабораторных работ содержит три основные части:

1) теоретическая часть;
2) практическая часть;
3) контрольные вопросы по теме.

Для выполнения лабораторной работы студенту необходимо изучить теоретический материал, описанный в теоретической части работы. После изучения теоретического материала студент должен получить допуск к лабораторной работе у преподавателя. Далее студенты выполняют задания лабораторной работы, описанные в практической части. В конце занятия необходимо защитить результаты лабораторной работы, ответив на контрольные вопросы.

Правила работы в компьютерном классе

Поскольку компьютерный класс является местом повышенной опасности и характеризуется большим скоплением технических средств, студентам рекомендуется выполнять следующие правила поведения:

1. не входить в компьютерный класс в верхней одежде;

2. за каждым студентом в компьютерном классе закрепляется определенное рабочее место, которое он поддерживает в чистоте и порядке.

3. во время работы на рабочем столе должны находиться только тетрадь и раздаточный материал.

4. не есть и не пить на рабочем месте перед компьютером;

5. не играть во время лабораторной работы в компьютерные игры, и не использовать ресурсы сети Internet в личных целях, не связанных с лабораторной работой;

6. не устанавливать самостоятельно программное обеспечение на лабораторные компьютеры без согласия преподавателя или инженера лаборатории;

БЛОК «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ КАЧЕСТВОМ»

ЛАБОРАТОРНАЯ РАБОТА № 1
Моделирование бизнес-процесса предприятия с использованием методологии IDEF0

Цель работы: изучение нотации IDEF0 для моделирования бизнес-процессов предприятия средствами пакета Ramus Educational;

Оборудование: компьютеры с операционной системой Windows XP и выше, наличие программы Ramus Educational.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Ramus Educational имеет достаточно простой и интуитивно понятный интерфейс пользователя [1]. При запуске Ramus Educational появляется диалоговое окно, в котором можно создать новый проект, либо открыть уже имеющийся. Для создания нового проекта необходимо выбрать соответствующий переключатель и нажать кнопку «Далее». На экране появиться Мастер «Свойства проекта», где можно выбрать нотацию моделирования и задать свойства проекта. В окне справа появляется описание выбранного окна. Программа Ramus Educational поддерживает две методологии - IDEF0 и DFD, каждая из которых решает свои специфические задачи (рис. 1.1).

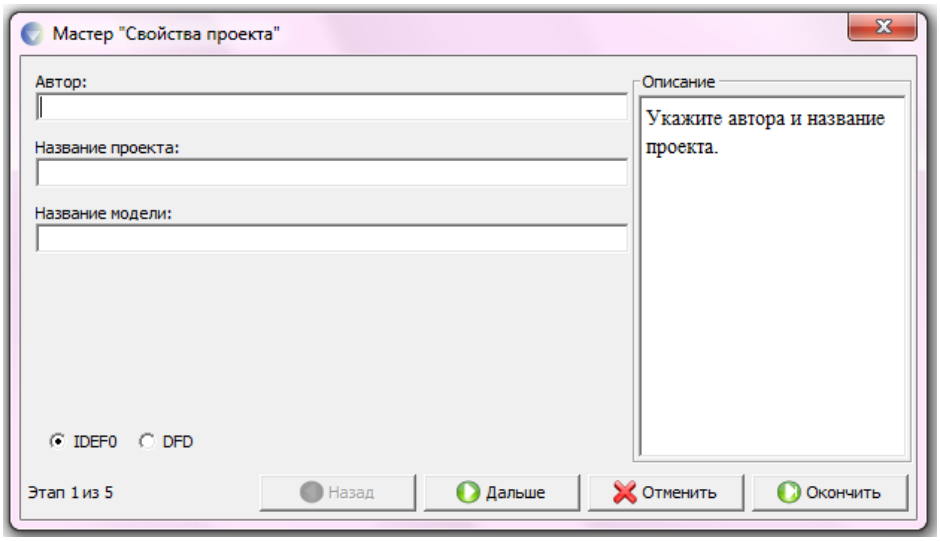


Рис. 1.1. Диалоговое окно мастера «Свойства проекта»

Состав палитры инструментов изменяется автоматически, когда происходит переключение с одной нотации на другую. При дальнейшей настройке свойств проекта нужно указать организацию, для которой разрабатывается данная модель и краткое описание модели. После описания свойств модели можно описать ресурсы,

задействованных в проекте. В программе Ramus Educational они называются словом Классификатор (см. рис. 1.2). Последний шаг создания модели позволяет выбрать собственников проекта из созданных классификаторов. Как правило, собственником проекта считается лицо, ответственное за внедрение и разработку этого проекта в бизнес-процессы фирмы. После нажатия кнопки окончить появляется рабочая область проекта.

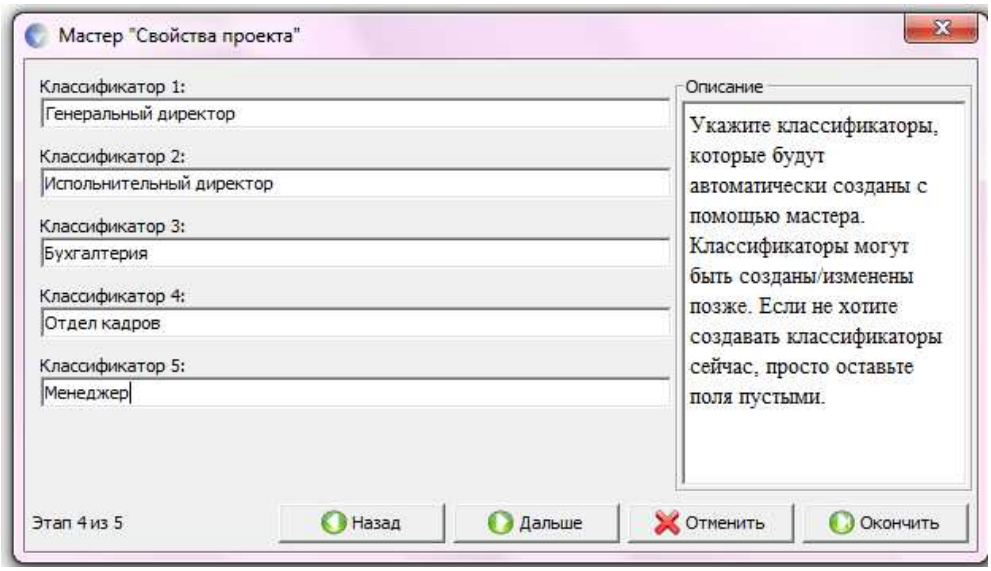


Рис. 1.2. Диалоговое окно для описания классификаторов

Модель в Ramus Educational рассматривается как совокупность работ, каждая из которых оперирует с некоторым набором данных. Работа изображается в виде прямоугольников, данные — в виде стрелок. Если щелкнуть по любому объекту модели левой кнопкой мыши, появляется контекстное меню, каждый пункт которого соответствует редактору какого-либо свойства объекта.

Построение модели IDEF0

На начальных этапах создания модели необходимо понять, как работает организация, которую собираются автоматизировать. Руководитель хорошо знает работу в целом, но не в состоянии вникнуть в детали работы каждого рядового сотрудника. Рядовой сотрудник хорошо знает, что творится на его рабочем месте, но может не знать, как работают коллеги. Поэтому для описания работы предприятия необходимо построить модель, которая будет адекватна предметной области и содержать в себе знания всех участников бизнес-процессов организации [2].

Наиболее удобным языком моделирования бизнес-процессов является IDEF0, где система представляется как совокупность взаимодействующих работ или функций. Такая чисто функциональная ориентация является принципиальной — функции системы

анализируются независимо от объектов, которыми они оперируют. Это позволяет более четко смоделировать логику и взаимодействие процессов организации.

Процесс моделирования системы в IDEF0 начинается с создания контекстной диаграммы — диаграммы наиболее абстрактного уровня описания системы в целом, содержащей определение субъекта моделирования, цели и точки зрения на модель.

Под субъектом понимается сама система, при этом необходимо точно установить, что входит в систему, а что лежит за ее пределами, другими словами, определить, что будет в дальнейшем рассматриваться как компоненты системы, а что как внешнее воздействие. На определение субъекта системы будут существенно влиять позиция, с которой рассматривается система, и цель моделирования — вопросы, на которые построенная модель должна дать ответ. Другими словами, вначале необходимо определить область моделирования. Описание области как системы в целом, так и ее компонентов является основой построения модели. Хотя предполагается, что в ходе моделирования область может корректироваться, она должна быть в основном сформулирована изначально, поскольку именно область определяет направление моделирования. При формулировании области необходимо учитывать два компонента — широту и глубину. Широта подразумевает определение границ модели — что будет рассматриваться внутри системы, а что снаружи. Глубина определяет, на каком уровне детализации модель является завершенной. При определении глубины системы необходимо помнить об ограничениях времени — трудоемкость построения модели растет в геометрической прогрессии с увеличением глубины декомпозиции. После определения границ модели предполагается, что новые объекты не должны вноситься в моделируемую систему [2].

Цель моделирования

Цель моделирования определяется из ответов на следующие вопросы [3]:

- ✓ Почему этот процесс должен быть смоделирован?
- ✓ Что должна показывать модель?
- ✓ Что может получить клиент?

IDEF0-модель предполагает наличие четко сформулированной цели, единственного субъекта моделирования и одной точки зрения. Для задания атрибутов модели и указания статуса разработки необходимо выбрать пункт меню Диаграмма / Свойства модели (рис. 1.3). В закладке Атрибуты можно задать ресурсы, используемые в процессе, а Статус — стадию разработки модели (черновой вариант, рабочий, окончательный и т. д.).

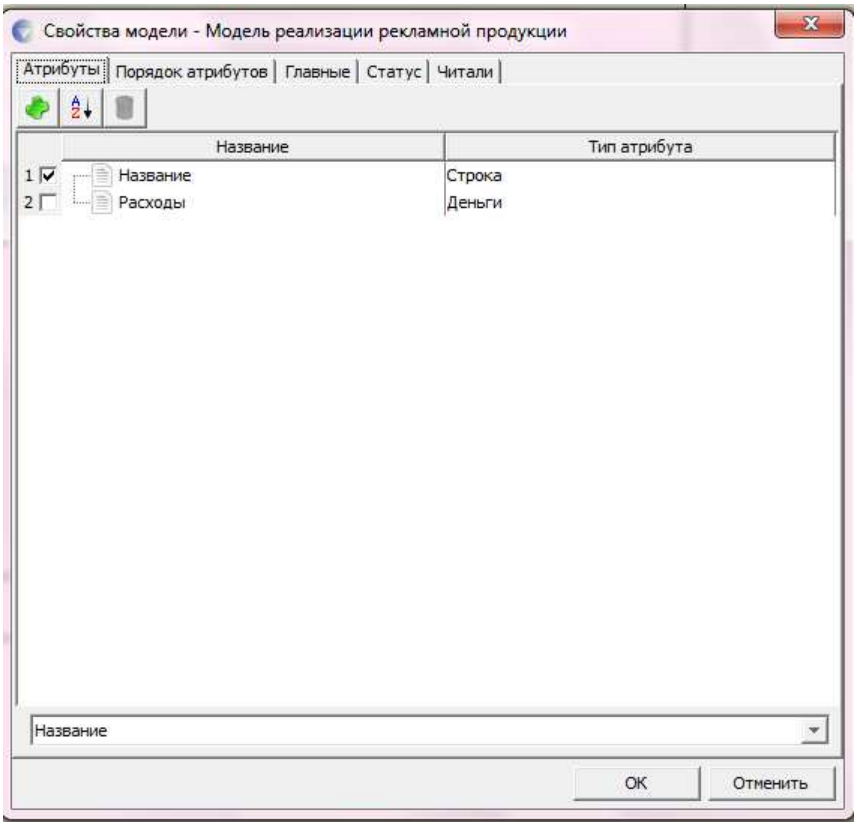


Рис. 1.3. Диалог задания свойств модели

Модели AS-IS и TO-BE

Обычно сначала строится модель существующей организации работы — AS-IS (как есть). Анализ функциональной модели позволяет понять, где находятся наиболее слабые места, в чем будут состоять преимущества новых бизнес-процессов и насколько глубоким изменениям подвергнется существующая структура организации бизнеса. Детализация бизнес-процессов позволяет выявить недостатки организации даже там, где функциональность на первый взгляд кажется очевидной. Найденные в модели AS-IS недостатки можно исправить при создании модели TO-BE (как будет) — модели новой организации бизнес-процессов [1].

Технология проектирования ИС подразумевает сначала создание модели AS-IS, ее анализ и улучшение бизнес-процессов, то есть создание модели TO-BE, и только на основе модели TO-BE строится модель данных, прототип и затем окончательный вариант ИС.

Иногда текущая AS-IS и будущая TO-BE модели различаются очень сильно, так что переход от начального к конечному состоянию становится неочевидным. В этом случае необходима третья модель, описывающая процесс перехода от начального к конечному состоянию системы, поскольку такой переход — это тоже бизнес-процесс.

Как правило, результат описания модели можно получить в отчете Model Report или Отчет. Однако данная программа является учебной и не позволяет реализовать функцию построения отчета.

Основу методологии IDEF0 составляет графический язык описания бизнес-процессов. Модель в нотации IDEF0 представляет собой совокупность иерархически упорядоченных и взаимосвязанных диаграмм. Каждая диаграмма является единицей описания системы и располагается на отдельном листе.

Контекстная диаграмма является вершиной древовидной структуры диаграмм и представляет собой самое общее описание системы и ее взаимодействия с внешней средой. После описания системы в целом проводится разбиение ее на крупные фрагменты. Этот процесс называется ***функциональной декомпозицией***, а диаграммы, которые описывают каждый фрагмент и взаимодействие фрагментов, называются диаграммами ***декомпозиции.*** После декомпозиции контекстной диаграммы проводится декомпозиция каждого большого фрагмента системы на более мелкие и так далее, до достижения нужного уровня подробности описания. После каждого сеанса декомпозиции проводятся сеансы экспертизы — эксперты предметной области указывают на соответствие реальных бизнес-процессов созданным диаграммам. Найденные несоответствия исправляются, и только после прохождения экспертизы без замечаний можно приступать к следующему сеансу декомпозиции. Так достигается соответствие модели реальным бизнес-процессам на любом и каждом уровне модели. Синтаксис описания системы в целом и каждого ее фрагмента одинаков во всей модели [2].

Работы (Activity) обозначают поименованные процессы, функции или задачи, которые происходят в течение определенного времени и имеют распознаваемые результаты. Работы изображаются в виде прямоугольников. Все работы должны быть названы и определены. Имя работы должно быть выражено отглагольным существительным, обозначающим действие (например, "Деятельность компании", "Прием заказа" и т.д.). Работа "Деятельность компании" может иметь, например, следующее определение: "Это учебная модель, описывающая деятельность компании" (рис. 1.4) [2].

Рис. 1.4. Пример контекстной диаграммы [2]

Для внесения работы в рабочую область диаграммы необходимо щелкнуть соответствующий элемент на панели инструментов (см. рис. 1.5).

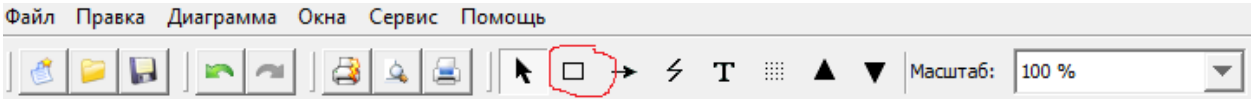


Рис. 1.5. Палитра инструментов для добавления функциональных элементов модели

Для внесения имени работы следует щелкнуть по работе правой кнопкой мыши, выбрать в меню ***Редактировать активный элемент*** и в появившемся диалоге внести имя работы. Для описания других свойств работы служит диалог Параметры стрелки (рис. 1.6).

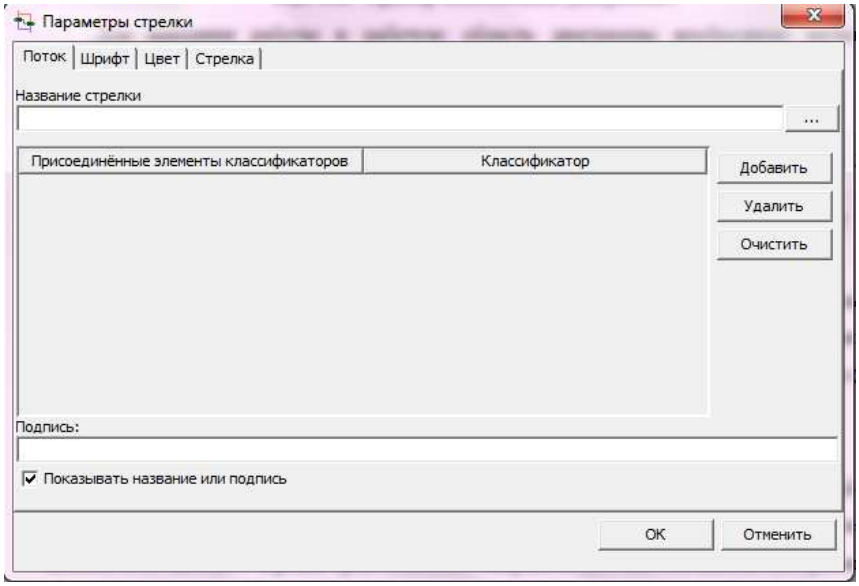


Рис. 1.6. Диалоговое окно Параметры стрелки

Диаграммы декомпозиции содержат родственные работы, т. е. дочерние работы, имеющие общую родительскую работу. Для создания диаграммы декомпозиции следует щелкнуть по кнопке с черным треугольником направленным вниз на панели инструментов (см. рис. 1.5). При этом возникает диалог Создания новой диаграммы (рис. 1.7), в котором следует указать нотацию новой диаграммы и количество работ на ней. Остановимся пока на нотации IDEF0 и щелкнем на OK. Появляется диаграмма декомпозиции (рис.1.9).

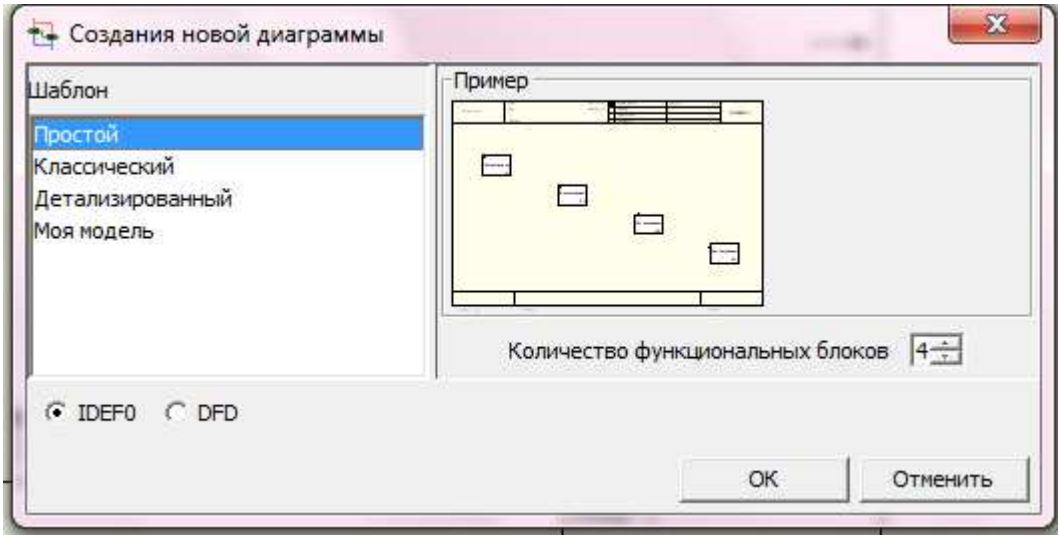


Рис. 1.7. Диалог создания новой диаграммы

Допустимый интервал числа работ — 2-8. Декомпозировать работу на одну работу не имеет смысла: диаграммы с количеством работ более восьми получаются перенасыщенными и плохо читаются. Для обеспечения наглядности и лучшего понимания моделируемых процессов рекомендуется использовать от трех до шести блоков на одной диаграмме. Пример диаграммы декомпозиции показан на рис. 1.8. [2].

Если оказывается, что количество работ недостаточно, то работу можно добавить в диаграмму, щелкнув сначала по кнопке с нарисованным прямоугольником на палитре инструментов, а затем по свободному месту на диаграмме.

Работы на диаграммах декомпозиции обычно располагаются по диагонали от левого верхнего угла к правому нижнему.

Такой порядок называется порядком доминирования. Согласно этому принципу расположения в левом верхнем углу помещается самая важная работа или работа, выполняемая по времени первой. Далее вправо вниз располагаются менее важные или выполняемые позже работы. Такое размещение облегчает чтение диаграмм, кроме того, на нем основывается понятие взаимосвязей работ (см. ниже).

Каждая из работ на диаграмме декомпозиции может быть в свою очередь декомпозирована. На диаграмме декомпозиции работы нумеруются автоматически слева направо. Номер работы показывается в правом нижнем углу. В левом верхнем углу

изображается небольшая диагональная черта, которая показывает, что данная работа не была декомпозирована. Так, на рис. 1.8 все работы еще не были декомпозированы.

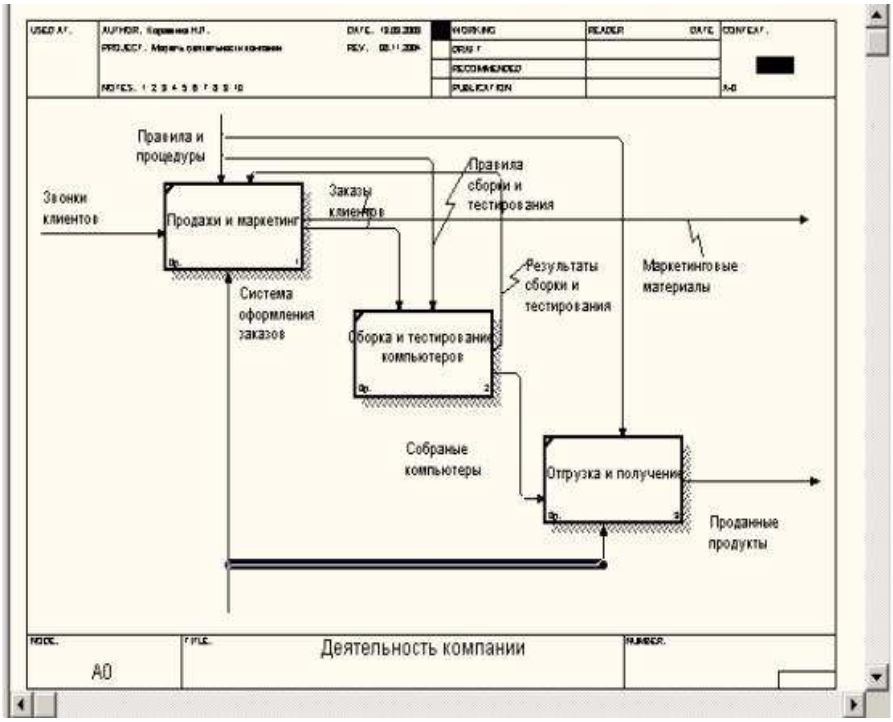


Рис. 1.8. Пример диаграммы декомпозиции [2]

Стрелки (Arrow) описывают взаимодействие работ и представляют собой некую информацию, выраженную существительными.(Например, "Звонки клиентов", "Правила и процедуры", "Бухгалтерская система") [2].

В IDEF0 различают пять типов стрелок:

1. Вход (Input) — материал или информация, которые используются или преобразуются работой для получения результата (выхода). Допускается, что работа может не иметь ни одной стрелки входа. Каждый тип стрелок подходит к определенной стороне прямоугольника, изображающего работу, или выходит из нее. Стрелка входа рисуется как входящая в левую грань работы. При описании технологических процессов (для этого и был придуман IDEF0) не возникает проблем определения входов. Действительно, "Звонки клиентов" на рис. 1.4 — это нечто, что перерабатывается в процессе "Деятельность компании" для получения результата. При моделировании ИС, когда стрелками являются не физические объекты, а данные, не все так очевидно. Например, при "Приеме пациента" карта пациента может быть и на входе и на выходе, между тем качество этих данных меняется. Другими словами, в нашем примере для того, чтобы оправдать свое назначение, стрелки входа и выхода должны быть точно определены с тем, чтобы указать на то, что данные действительно были переработаны (например, на выходе — "Заполненная карта

пациента"). Очень часто сложно определить, являются ли данные входом или управлением. В этом случае подсказкой может служить информация о том, перерабатываются/изменяются ли данные в работе или нет. Если изменяются, то, скорее всего, это вход, если нет — управление [3].

2. Управление (Control) — правила, стратегии, процедуры или стандарты, которыми руководствуется работа. Каждая работа должна иметь хотя бы одну стрелку управления. Стрелка управления рисуется как входящая в верхнюю грань работы. На рис. 1.4 стрелка "Правила и процедуры" — управление для работы "Деятельность компании". Управление влияет на работу, но не преобразуется работой. Если цель работы — изменить процедуру или стратегию, то такая процедура или стратегия будет для работы входом. В случае возникновения неопределенности в статусе стрелки (управление или вход) рекомендуется рисовать стрелку управления [3].

3. Выход (Output) — материал или информация, которые производятся работой. Каждая работа должна иметь хотя бы одну стрелку выхода. Работа без результата не имеет смысла и не должна моделироваться. Стрелка выхода рисуется как исходящая из правой грани работы. На рис. 1.4 стрелки "Маркетинговые материалы" и "Проданные продукты" являются выходом для работы "Деятельность компании" [3].

4. Механизм (Mechanism) — ресурсы, которые выполняют работу, например персонал предприятия, станки, устройства и т. д. Стрелка механизма рисуется как входящая в нижнюю грань работы. На рис. 1.4. стрелка "Бухгалтерская система" является механизмом для работы "Деятельность компании". По усмотрению аналитика стрелки механизма могут не изображаться в модели [3].

5. Вызов (Call) — специальная стрелка, указывающая на другую модель работы. Стрелка вызова рисуется как исходящая из нижней грани работы. На рис. 1.9. стрелка "Другая модель работы " является вызовом для работы "Изготовление изделия". Стрелка вызова используется для указания того, что некоторая работа выполняется за пределами моделируемой системы [3].

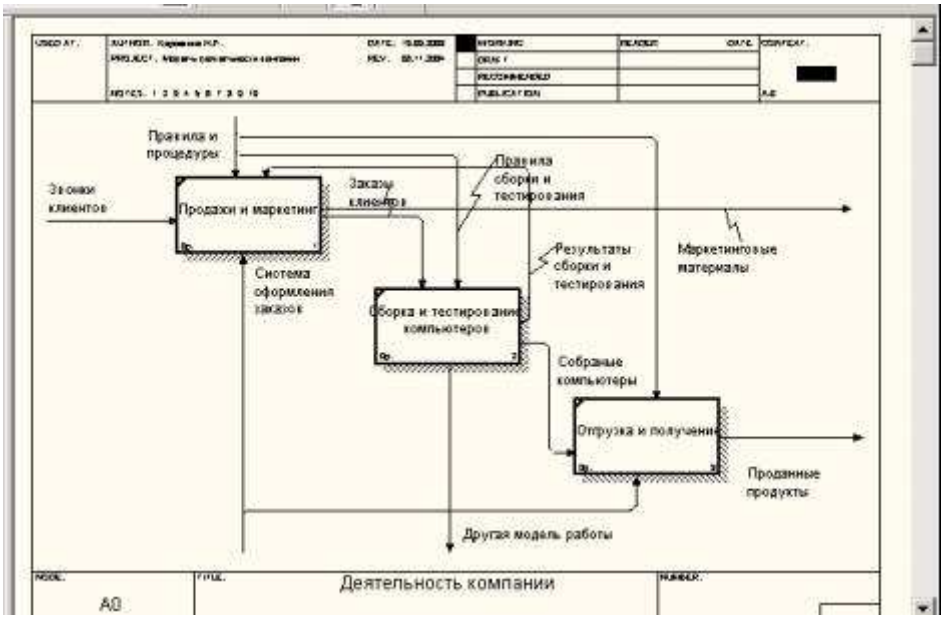


Рис. 1.9. Стрелка вызова, появляющаяся при расщеплении модели [2]

Граничные стрелки. Стрелки на контекстной диаграмме служат для описания взаимодействия системы с окружающим миром. Они могут начинаться у границы диаграммы и заканчиваться у работы, или наоборот. Такие стрелки называются граничными [2, 3].

Для внесения граничной стрелки входа следует:

✓ щелкнуть по кнопке с символом стрелки ;

✓ в палитре инструментов перенести курсор к левой стороне экрана, пока не появится начальная штриховая полоска;

✓ щелкнуть один раз по полоске (откуда выходит стрелка) и еще раз в левой части работы со стороны входа (где заканчивается стрелка);

✓ вернуться в палитру инструментов и выбрать опцию редактирования стрелки;

✓ щелкнуть правой кнопкой мыши на линии стрелки, во всплывающем меню выбрать Name и добавить имя стрелки в закладке Name диалога IDEF0 Arrow Properties.

Стрелки управления, входа, механизма и выхода изображаются аналогично.

ICOM-коды. Диаграмма декомпозиции предназначена для детализации работы. В отличие от моделей, отображающих структуру организации, работа на диаграмме верхнего уровня в IDEF0 — это не элемент управления нижестоящими работами. Работы нижнего уровня — это то же самое, что работы верхнего уровня, но в более детальном изложении. Как следствие этого границы работы верхнего уровня — это то же самое, что границы диаграммы декомпозиции. ICOM (аббревиатура от Input, Control, Output и Mechanism) —

коды, предназначенные для идентификации граничных стрелок. Код ICOM содержит префикс, соответствующий типу стрелки (I, C, O или M), и порядковый номер [2].

Такие программы как BPwin вносят ICOM-коды автоматически. Для отображения ICOM-кодов следует включить опцию ICOM codes на закладке Display диалога Model Properties (меню Model/Model Properties) (рис.1.10). Программа Ramus Educational является учебной и не обладает такими возможностями.

Словарь стрелок редактируется при помощи специального редактора Arrow Dictionary Editor, в котором определяется стрелка и вносится относящийся к ней комментарий (рис.1.11). Словарь стрелок решает очень важную задачу. Диаграммы создаются аналитиком для того, чтобы провести сеанс экспертизы, т. е. обсудить диаграмму со специалистом предметной области. В любой предметной области формируется профессиональный жаргон, причем очень часто жаргонные выражения имеют нечеткий смысл и воспринимаются разными специалистами по-разному. В то же время аналитик — автор диаграмм должен употреблять те выражения, которые наиболее понятны экспертам. Поскольку формальные определения часто сложны для восприятия, аналитик вынужден употреблять профессиональный жаргон, а чтобы не возникло неоднозначных трактовок, в словаре стрелок каждому понятию можно дать расширенное и, если это необходимо, формальное определение.

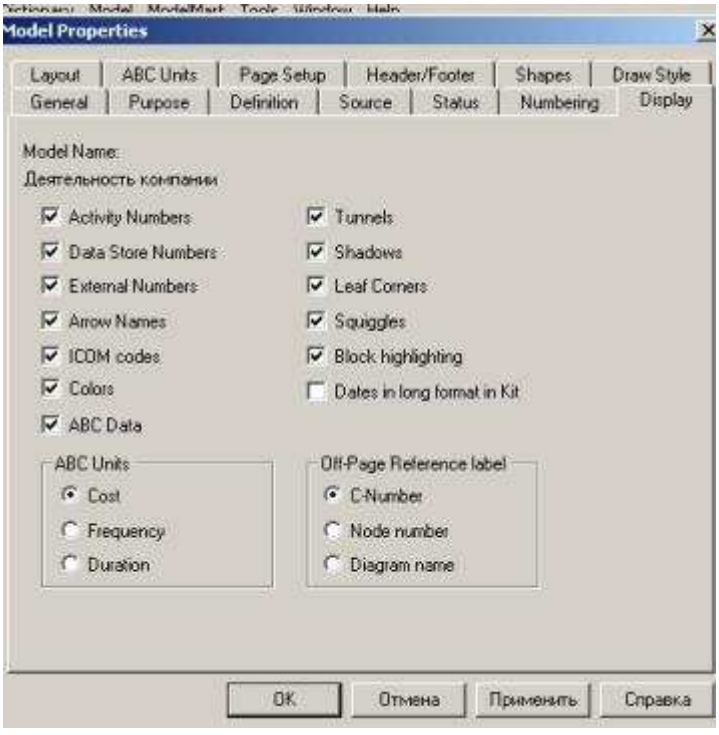


Рис. 1.10. Включение опции ICOM codes на закладке Display [2]

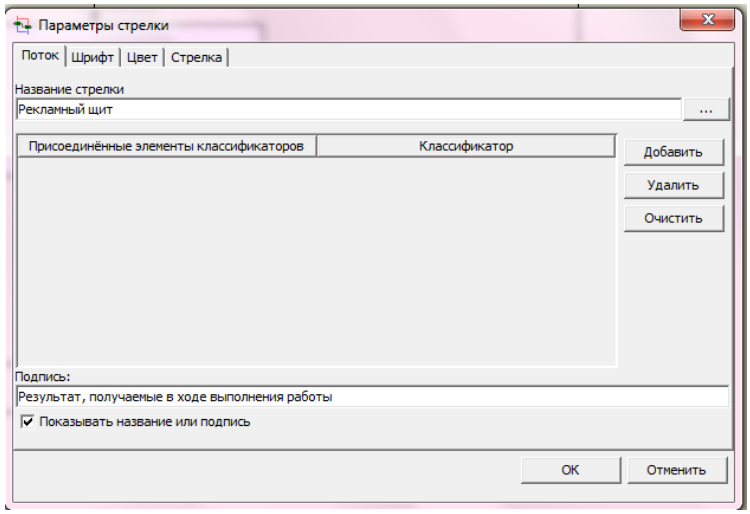


Рис. 1.11. Редактирование словаря стрелок

Несвязанные граничные стрелки (unconnected border arrow). При декомпозиции работы входящие в нее и исходящие из нее стрелки (кроме стрелки вызова) автоматически появляются на диаграмме декомпозиции (миграция стрелок), но при этом не касаются работ. Такие стрелки называются несвязанными и воспринимаются как синтаксическая ошибка [2].

На рис. 1.12 приведен фрагмент диаграммы декомпозиции с несвязанными стрелками, генерирующийся при декомпозиции работы **"Сборка настольных компьютеров"**. Для связывания стрелок входа, управления или механизма необходимо перейти в режим редактирования стрелок, щелкнуть по наконечнику стрелки и потом по соответствующему сегменту работы. Для связывания стрелки выхода необходимо перейти в режим редактирования стрелок, щелкнуть по сегменту выхода работы и затем по стрелке [2].

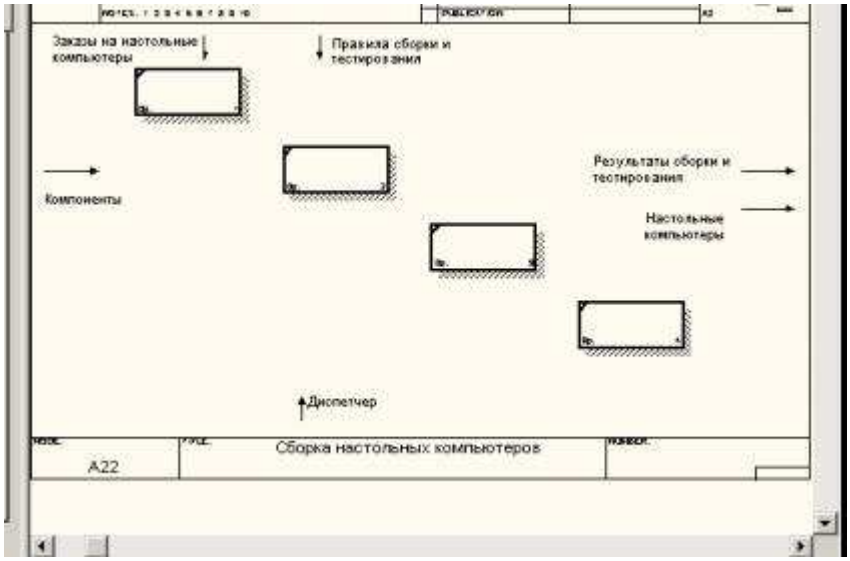


Рис. 1.12. Пример несвязанных стрелок [2]

Внутренние стрелки. Для связи работ между собой используются внутренние стрелки, то есть стрелки, которые не касаются границы диаграммы, начинаются у одной и кончаются у другой работы.

Для рисования внутренней стрелки необходимо в режиме рисования стрелок щелкнуть по сегменту (например, выхода) одной работы и затем по сегменту (например, входа) другой. **В IDEF0 различают пять типов связей работ** [2]:

Связь по входу (output-input), когда стрелка выхода вышестоящей работы (далее — просто выход) направляется на вход нижестоящей (например, на рис. 1.13 стрелка **"Собранные компьютеры"** связывает работы **"Сборка и тестирование компьютеров"** и **"Отгрузка и получение"**).

Рис. 1.13. Связь по входу [2]

Связь по управлению (output-control), когда выход вышестоящей работы направляется на управление нижестоящей. Связь по управлению показывает доминирование вышестоящей работы. Данные или объекты выхода вышестоящей работы не меняются в нижестоящей. На рис. 1.14 стрелка "**Заказы клиентов**" связывает работы "**Продажи и маркетинг**" и "**Сборка и тестирование компьютеров**".

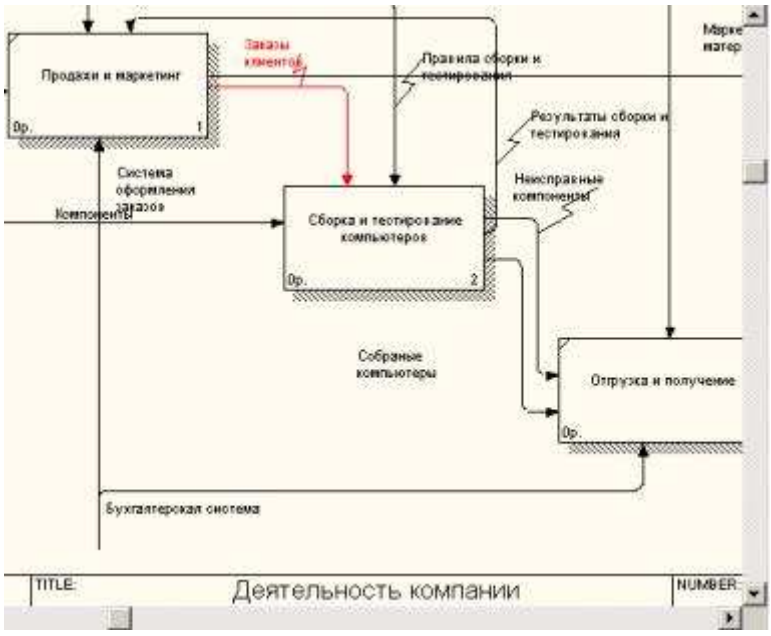


Рис.1.14. Связь по управлению [2]

Обратная связь по входу (output-input feedback) когда выход нижестоящей работы направляется на вход вышестоящей. Такая связь, как правило, используется для описания циклов. На рис. 7.15 стрелка "**Результаты тестирования**" связывает работы "**Тестирование компьютеров**" и "**Отслеживание расписания и управление сборкой и тестированием**".

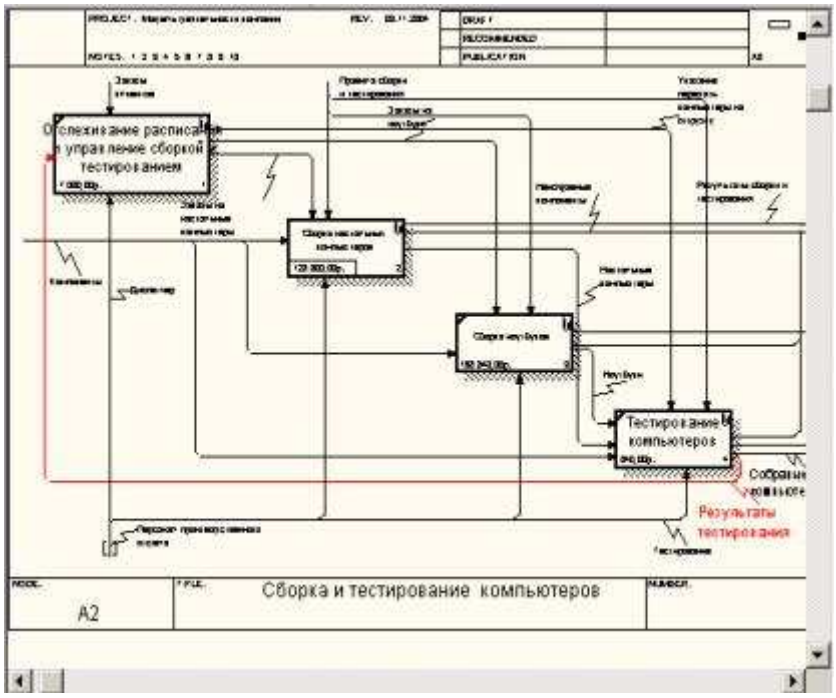


Рис. 1.15. Обратная связь по входу [2]

Обратная связь по управлению (output-control feedback), когда выход нижестоящей работы направляется на управление вышестоящей (стрелка "**Результаты сборки и тестирования**", рис. 1.16). Обратная связь по управлению часто свидетельствует об эффективности бизнес-процесса. На рис. 1.16 объем продаж может быть повышен путем непосредственного регулирования процессов сборки и тестирования компьютеров (выхода) работы "**Сборки и тестирование компьютеров**".

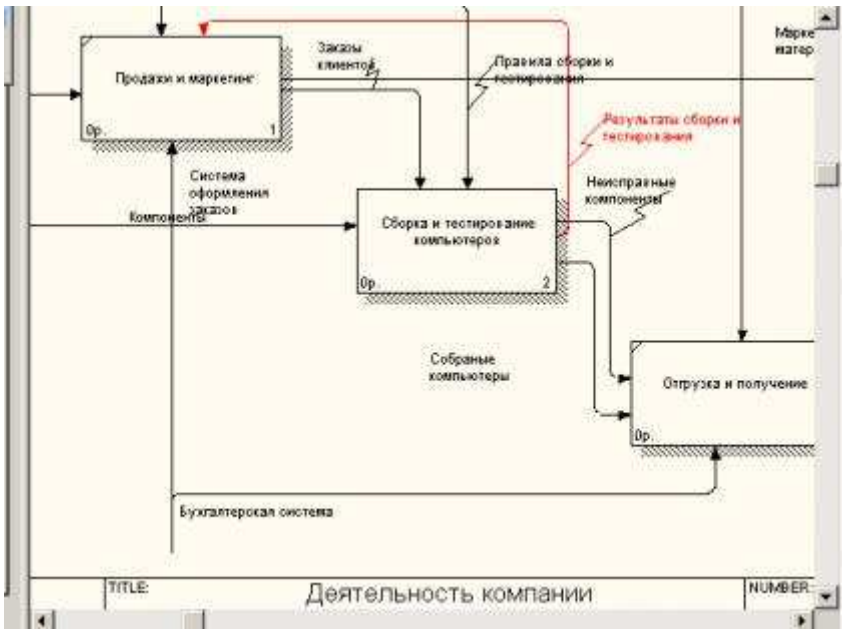


Рис. 1.16. Обратная связь по управлению [2]

Связь выход-механизм (output-mechanism), когда выход одной работы направляется на механизм другой. Эта взаимосвязь используется реже остальных и показывает, что одна работа подготавливает ресурсы, необходимые для проведения другой работы (рис. 1.17).

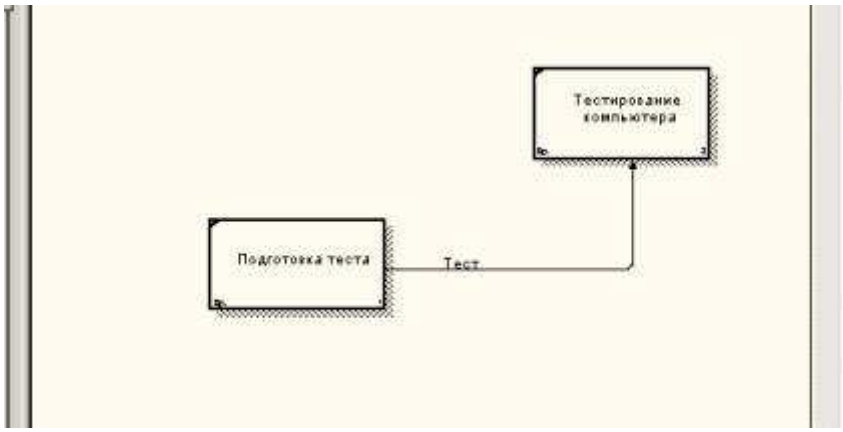


Рис. 7.17. Связь выход-механизм [2]

Разветвляющиеся и сливающиеся стрелки. Одни и те же данные или объекты, порожденные одной работой, могут использоваться сразу в нескольких других работах. С другой стороны, стрелки, порожденные в разных работах, могут представлять собой одинаковые или однородные данные или объекты, которые в дальнейшем используются или перерабатываются в одном месте. Для моделирования таких ситуаций в IDEF0 используются разветвляющиеся и сливающиеся стрелки. Для разветвления стрелки нужно в режиме редактирования стрелки щелкнуть по фрагменту стрелки и по соответствующему сегменту работы. Для слияния двух стрелок выхода нужно в режиме редактирования

стрелки сначала щелкнуть по сегменту выхода работы, а затем по соответствующему фрагменту стрелки.

Смысл разветвляющихся и сливающихся стрелок передается именованием каждой ветви стрелок. Существуют определенные правила именования таких стрелок. Рассмотрим их на примере разветвляющихся стрелок. Если стрелка именована до разветвления, а после разветвления ни одна из ветвей не именована, то подразумевается, что каждая ветвь моделирует те же данные или объекты, что и ветвь до разветвления (рис. 1.18).

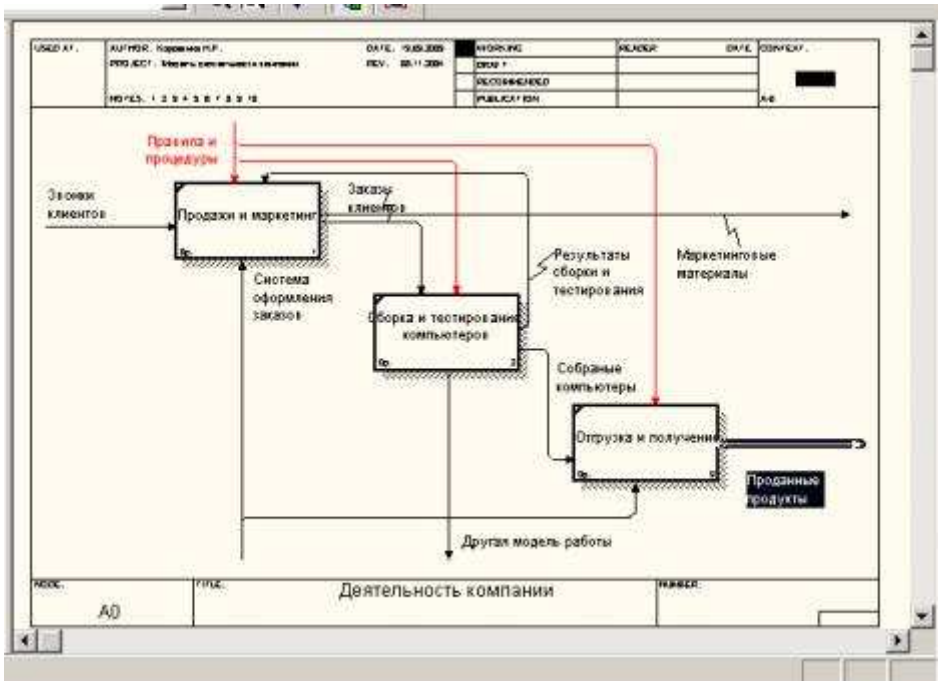


Рис. 1.18. Пример именования разветвляющейся стрелки [2]

Если стрелка именована до разветвления, а после разветвления какая-либо из ветвей тоже именована, то подразумевается, что эти ветви соответствуют именованию. Если при этом какая-либо ветвь после разветвления осталась неименованной, то подразумевается, что она моделирует те же данные или объекты, что и ветвь до разветвления (рис. 1.19).

Примечание! *Недопустима ситуация, когда стрелка до разветвления не именована, а после разветвления не именована какая-либо из ветвей.*

Правила именования сливающихся стрелок полностью аналогичны — ошибкой будет считаться стрелка, которая после слияния не именована, а до слияния не именована какая-либо из ее ветвей. Для именования отдельной ветви разветвляющихся и сливающихся стрелок следует выделить на диаграмме только одну ветвь, после чего вызвать редактор имени и присвоить имя стрелке. Это имя будет соответствовать только выделенной ветви.

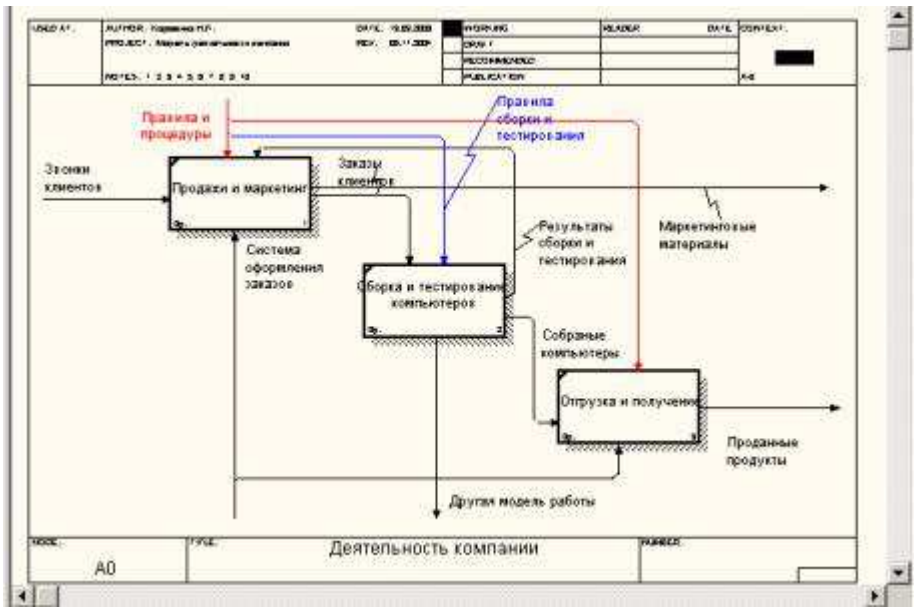


Рис. 1.19. Пример именования разветвляющейся стрелки [2]

Туннелирование стрелок. Вновь внесенные граничные стрелки на диаграмме декомпозиции нижнего уровня изображаются в квадратных скобках и автоматически не появляются на диаграмме верхнего уровня (рис. 1.20).

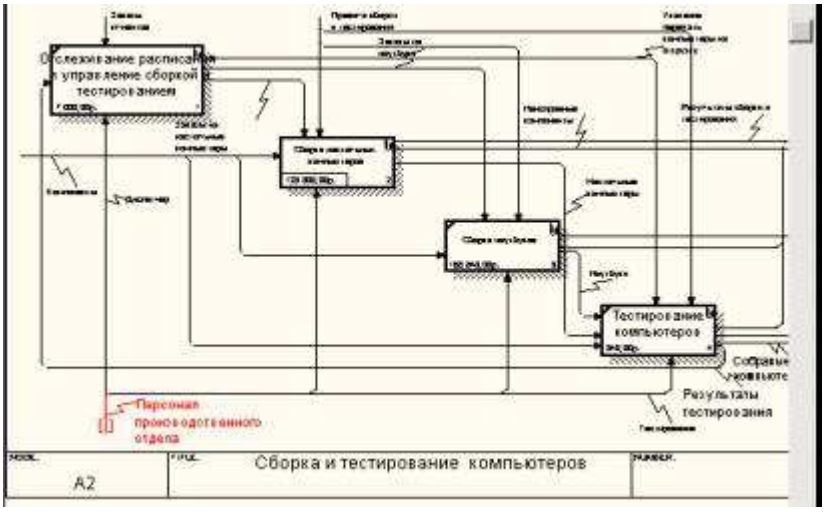


Рис. 1.20. Неразрешенная (unresolved) стрелка [2]

Для их "перетаскивания" наверх нужно щелкнуть правой кнопкой мыши по квадратным скобкам граничной стрелки и в контекстном меню выбрать команду Arrow Tunnel (рис. 1.20).

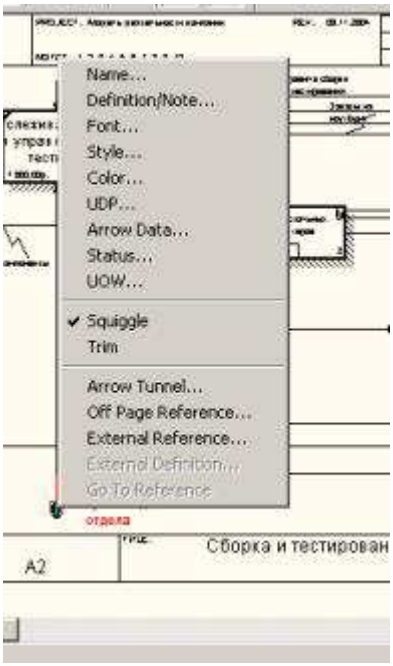


Рис. 1.20. Выбор команды из контекстного меню [2]

Появляется диалог Border Arrow Editor (рис. 1.21).

Если щелкнуть по кнопке Resolve Border Arrow, стрелка мигрирует на диаграмму верхнего уровня, если по кнопке Change To Tunnel — стрелка будет туннелирована и не попадет на другую диаграмму. Туннельная стрелка изображается с круглыми скобками на конце (рис. 1.22).

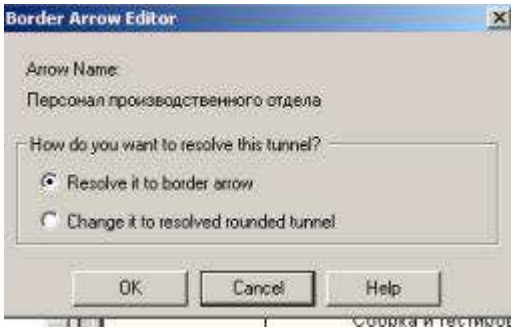


Рис. 1.21. Диалог Border Arrow Editor [2]

Туннелирование может быть применено для изображения малозначимых стрелок. Если на какой-либо диаграмме нижнего уровня необходимо изобразить малозначимые данные или объекты, которые не обрабатываются или не используются работами на текущем уровне, то их необходимо направить на вышестоящий уровень (на родительскую диаграмму). Если эти данные не используются на родительской диаграмме, их нужно направить еще выше, и т. д. В результате малозначимая стрелка будет изображена на всех уровнях и затруднит чтение всех диаграмм, на которых она присутствует. Выходом является туннелирование стрелки на самом нижнем уровне. Такое туннелирование называется "не-в-родительской-диаграмме" [2].

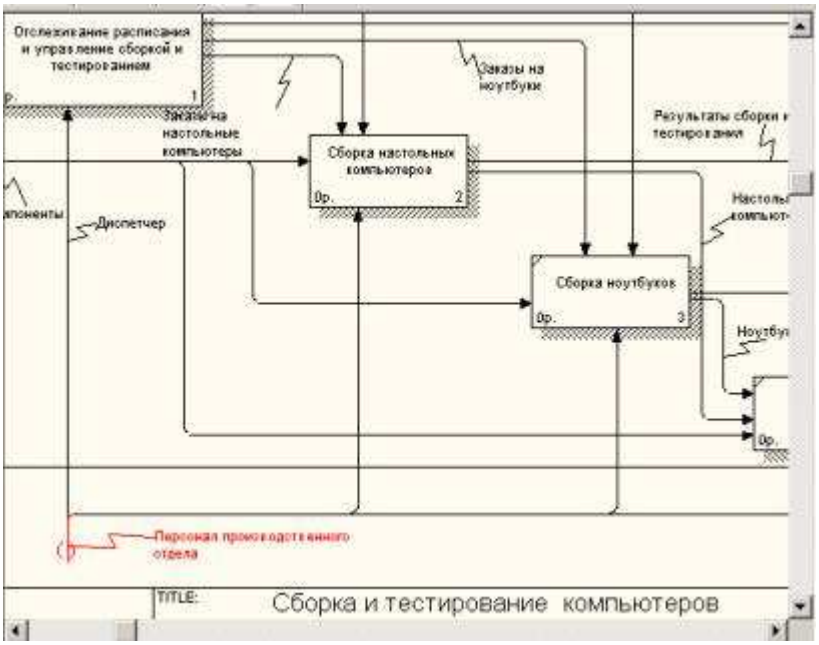


Рис. 1.22. Типы туннелирования стрелок [2]

Другим примером туннелирования может быть ситуация, когда стрелка механизма мигрирует с верхнего уровня на нижний, причем на нижнем уровне этот механизм используется одинаково во всех работах без исключения. (Предполагается, что не нужно детализировать стрелку механизма, т. е. стрелка механизма на дочерней работе именована до разветвления, а после разветвления ветви не имеют собственного имени). В этом случае стрелка механизма на нижнем уровне может быть удалена, после чего на родительской диаграмме она может быть туннелирована, а в комментарии к стрелке или в словаре можно указать, что механизм будет использоваться во всех работах дочерней диаграммы декомпозиции. Такое туннелирование называется "не-в-дочерней-работе" (рис. 1.22).

Нумерация работ и диаграмм. Все работы модели нумеруются. Номер состоит из префикса и числа. Может быть использован префикс любой длины, но обычно используют префикс А. Контекстная (корневая) работа дерева имеет номер А0. Работы i декомпозиции А0 имеют номера А1, А2, А3 и т. д. Работы декомпозиции нижнего уровня имеют номер родительской работы и очередной порядковый номер, например работы декомпозиции А3 будут иметь номера А31, А32, А33, А34 и т. д. Работы образуют иерархию, где каждая работа может иметь одну родительскую и несколько дочерних работ, образуя дерево. Такое дерево называют деревом узлов, а вышеописанную нумерацию — нумерацией по узлам. Диаграммы IDEF0 имеют двойную нумерацию. Во-первых, диаграммы имеют номера по узлу. Контекстная диаграмма всегда имеет номер А-0, декомпозиция контекстной диаграммы — номер А0, остальные диаграммы декомпозиции — номера по

соответствующему узлу (например, A1, A2, A21, A213 и т. д.). BPwin автоматически поддерживает нумерацию по узлам, т. е. при проведении декомпозиции создается новая диаграмма и ей автоматически присваивается соответствующий номер.

Каркас диаграммы

На рис. 1.23 показан типичный пример диаграммы декомпозиции с граничными рамками, которые называются каркасом диаграммы.

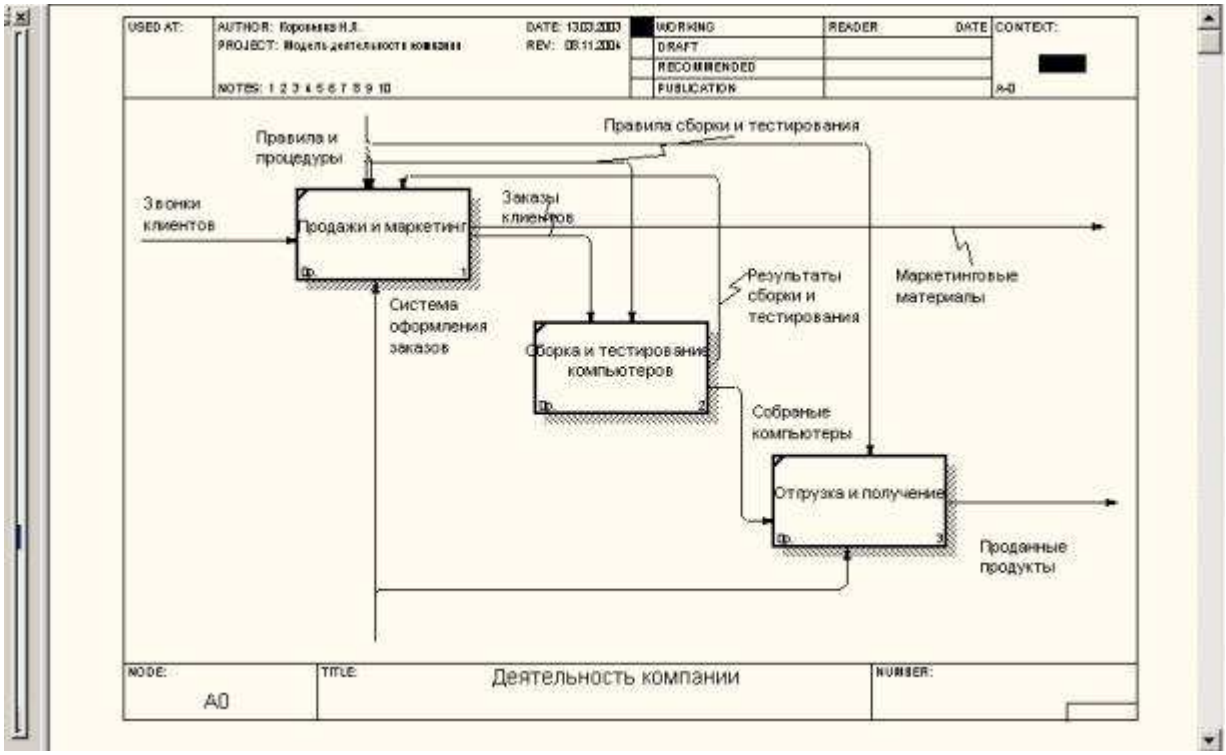


Рис. 1.23. Пример диаграммы декомпозиции с каркасом [2]

Каркас содержит заголовок (верхняя часть рамки) и подвал (нижняя часть). Заголовок каркаса используется для отслеживания диаграммы в процессе моделирования. Нижняя часть используется для идентификации и позиционирования в иерархии диаграммы. Смысл элементов каркаса приведен в табл. 1.1 и 1.2.

Таблица 1.1. Поля заголовка каркаса (слева направо)

Поле	Смысл
Used At	Используется для указания на родительскую работу в случае, если на текущую диаграмму ссылались посредством стрелки вызова
Autor, Date, Rev, Project	Имя создателя диаграммы, дата создания и имя проекта, в рамках которого была создана диаграмма. REV-дата последнего редактирования диаграммы
Notes 123456789 10	Используется при проведении сеанса экспертизы. Эксперт должен (на бумажной копии диаграммы) указать число замечаний, вычеркивая цифру из списка каждый раз при внесении нового замечания
Status	Статус отображает стадию создания диаграммы, отображая все этапы публикации

Working	Новая диаграмма, кардинально обновленная диаграмма или новый автор диаграммы
Draft	Диаграмма прошла первичную экспертизу и готова к дальнейшему обсуждению
Recommended	Диаграмма и все ее сопровождающие документы прошли экспертизу. Новых изменений не ожидается
Publication	Диаграмма готова к окончательной печати и публикации
Reader	Имя читателя (эксперта)
Date	Дата прочтения (экспертизы)
Context	Схема расположения работ в диаграмме верхнего уровня. Работа, являющаяся родительской, показана темным прямоугольником, остальные – светлым. На контекстной диаграмме (A-0) показана надпись TOP. В левом нижнем углу показывается номер по узлу родительской диаграммы: 

Таблица 1.2. Поля подвала каркаса (слева направо)

Поле	**Смысл**
Node	Номер узла диаграммы (номер родительской работы)
Title	Имя диаграммы. По умолчанию — имя родительской работы
Number C-Number	уникальный номер версии диаграммы
Page	Номер страницы, может использоваться как номер страницы при формировании папки

ПРАКТИЧЕСКАЯ ЧАСТЬ

Основываясь на теоретическом материале к лабораторной работе и лекциях построить учебную модель процесса сборки и продажи компьютеров компании Quil в нотации IDEF0.

Требования к построению учебной модели:

а) создать модель «Описание бизнес-процессов компании Quil»;

б) задать автора модели и классификаторы;

в) указать какие из классификаторов являются руководителями проекта;

г) создайте контекстную диаграмму «Деятельности компании Quil», которая должна содержать пять стрелок: звонки клиентов, правила и процедуры, бухгалтерская система, маркетинговые материалы, проданные продукты. Исходя из названий стрелок, определить их тип и расположить в соответствии с требованиями нотации IDEF0.

д) заполнить свойства модели: Главные, Статус, Читали.

е) создать диаграмму декомпозиции для работы «Деятельность компании Quil», содержащую работы «Продажи и маркетинг», «Обработка и тестирование компьютеров», «Отгрузка и получение»;

ж) разработать данные (стрелки) внутренние и внешние, обеспечивающие взаимодействие между работами;

з) к каждой из стрелок добавить описание в поле подпись и по возможности классификаторы.

и) создать диаграмму декомпозиции для работы «Сборка и тестирование компьютеров», содержащую работы «Отслеживание расписания управления сборкой и тестированием», «Сборка микросхем для ноутбуков», «Сборка ноутбуков», «Тестирование компьютеров»;

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Перечислите известные языки описания бизнес-процессов;
2) Что понимается под термином «CASE-средства»;
3) Что представляет собой IDEF0-модель?
4) Что понимается под термином «декомпозиция»?
5) Каков синтаксис описания систем в IDEF0?
6) Что такое работа?
7) Сколько блоков декомпозиции рекомендуется создавать при моделировании и почему?
8) Какое смысловое значение имеет расположение работ на диаграммах декомпозиции от верхнего левого угла к правому нижнему?
9) Какова функция стрелок на диаграммах IDEF0?
10) Назовите назначение ICOM-кодов в BPWin?
11) Наличие какой связи свидетельствует о высокой эффективности бизнес-процесса?
12) Какие виды связи могут быть реализованы в нотации IDEF0?
13) Объяснить смысл стрелок с квадратными и круглыми скобками на диаграмме IDEF0?
14) Может ли диаграмма не иметь стрелок входа, выхода, управления и ресурсов соответственно?

ЛАБОРАТОРНАЯ РАБОТА № 2

Применение нотации IDEF0 при проектировании бизнес-процессов

Цель работы: изучение принципов ФСА в нотации IDEF0, построение бизнес-модели работы телевизионной службы в указанной нотации.

Оборудование: компьютеры с операционной системой Windows XP и выше, наличие программы Ramus Educational.

Форма проведения занятия: интерактивное занятие с применением IT-методов (2 ч).

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Как было рассмотрено ранее, обычно сначала строится функциональная модель существующей организации работы — AS-IS (как есть). После построения модели AS-IS проводится анализ бизнес-процессов, потоки данных и объектов перенаправляются и улучшаются, в результате строится модель TO-BE. Как правило, строится несколько моделей TO-BE, из которых по какому-либо критерию выбирается наилучшая. Проблема состоит в том, что таких критериев много и непросто определить важнейший. Для того чтобы определить качество созданной модели с точки зрения эффективности бизнес-процессов, необходима система метрики, т. е. качество следует оценивать количественно [2].

Функционально-стоимостный анализ (ФСА) – методология непрерывного совершенствования продукции, производственных технологий, организационных структур. Задачей ФСА является снижение всех видов затрат при одновременном сохранении или повышении качества. Функционально-стоимостный подход к рассмотрению объекта обоснован тем, что потребителя интересует не объект сам по себе, а его функции, качество их выполнения и затраты на приобретение этого качества. Основным критерием совершенства (конкурентоспособности) объекта с позиции ФСА является его потребительская стоимость, определяемая соотношением качества (полезности) объекта и затрат потребителя [3] .

В частности с помощью ФСА можно решать задачи:

- ✓ анализа затрат (выявление зон неоправданно высоких затрат на всем жизненном цикле объекта);
- ✓ оценки решений (программное обеспечение для количественной оценки новых идей и проектов);
- ✓ оценки конкурентоспособности (определение конкурентоспособной цены и т.д.) [3].

BPwin предоставляет аналитику два инструмента для оценки модели — стоимостный анализ, основанный на работах (Activity Based Costing, ABC), и свойства, определяемые пользователем (User Defined Properties, UDP). Функциональное оценивание – ABC – это технология выявления и исследования стоимости выполнения той или иной функции (действия). Исходными данными для функционального оценивания являются затраты на ресурсы (материалы, персонал и т.д.). В сравнении с традиционными способами оценки затрат, при применении которых часто недооценивается продукция, производимая в

незначительном объеме, и переоценивается массовый выпуск, ABC обеспечивает более точный метод расчета стоимости производства продукции, основанный на стоимости выполнения всех технологических операций, выполняемых при ее выпуске. Стоимостный анализ **представляет собой соглашение об учете, используемое для сбора затрат, связанных с работами, с целью определить общую стоимость** процесса. Стоимостный анализ основан на модели работ, потому что количественная оценка невозможна без детального понимания функциональности предприятия. Обычно ABC применяется для того, чтобы понять происхождение выходных затрат и облегчить выбор нужной модели работ при реорганизации деятельности предприятия (Business Process Reengineering, BPR). С помощью стоимостного анализа можно решить такие задачи, как определение действительной стоимости производства продукта, определение действительной стоимости поддержки клиента, идентификация наиболее дорогостоящих работ (тех, которые должны быть улучшены в первую очередь), обеспечение менеджеров финансовой мерой предлагаемых изменений и т.д. ABC-анализ может проводиться только тогда, когда модель работы последовательная (следует синтаксическим правилам IDEF0), корректная (отражает бизнес), полная (охватывает всю рассматриваемую область) и стабильная (проходит цикл экспертизы без изменений), другими словами, когда создание модели работы закончено [3].

Параметры стоимостного анализа задаются на вкладке «ABC Units» окна Model Properties (рис. 2.2) [3].

Model Name – отображает название текущей модели;

Currency description – для задания единицы измерения денежных средств из списка. Выбранное название единицы измерения денег будет показано в отчетах и в таблице стоимости в диалоговом окне Свойства Работы (Activity Properties). Если в списке выбора отсутствует необходимая валюта (например, рубль), то ее можно добавить. По умолчанию символ валюты извлекается из настроек Windows.

Symbol placement – определение символа единицы измерения денег.

Symbol – вид денежного символа, который отображается возле значения стоимости работы на диаграмме;

Number of decimals in diagrams – количество значащих цифр после запятой (0-9), которые показаны на диаграмме на значении стоимости работ. Например, стоимость работы с двумя десятичными разрядами представляется так: $ 2.35.

Number of decimals in report – количество значащих цифр после запятой (0-9) применительно к отчетам.

Time unit – временной интервал, который используется при определении таких стоимостных факторов, как продолжительность и частота.

Decimals in frequency values – десятичное число (0-9) для использования в стоимостном значении частоты. Можно установить стоимостное значение частоты в таблице стоимости в диалоговом окне свойств работы.

Decimals in duration values – аналогично предыдущему пункту, но в отношении продолжительности.

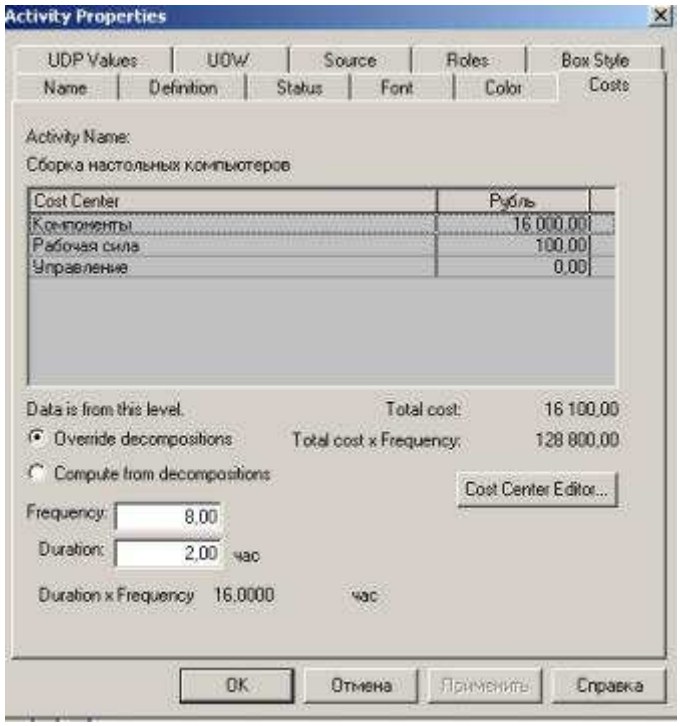


Рис. 2.2. Задание стоимости работ в диалоге Activity Properties/Cost [2]

Далее описываются ***центры затрат (cost centers)***. Для внесения центров затрат необходимо вызвать диалог ***Cost Center Editor*** из меню Model (рис. 2.3). Если в процессе назначения стоимости возникает необходимость внесения дополнительных центров затрат, диалог Cost Center Editor вызывается прямо из диалога Activity Properties/Cost соответствующей кнопкой.

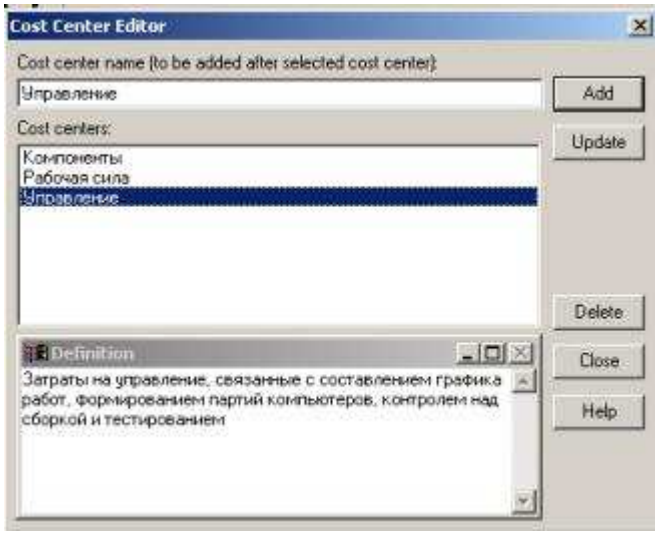


Рис. 2.3. Диалог Cost Center Editor [2]

Каждому центру затрат следует дать подробное описание в окне ***Definition***. Список центров затрат упорядочен. Порядок в списке можно менять при помощи стрелок, расположенных справа от списка. Задание определенной последовательности центров затрат в списке, во-первых, облегчает последующую работу при присвоении стоимости работам, а во-вторых, имеет значение при использовании единых стандартных отчетов в разных моделях. Хотя BPwin сохраняет информацию о стандартном отчете в файле BPWINRPT.INI, информация о центрах затрат и UDP сохраняется в виде указателей, т. е. хранятся не названия центров затрат, а их номера. Поэтому, если нужно использовать один и тот же стандартный отчет в разных моделях, списки центров затрат должны быть в них одинаковы.

Общие затраты по работе рассчитываются как сумма по всем центрам затрат. При вычислении затрат вышестоящей (родительской) работы сначала вычисляется произведение затрат дочерней работы на частоту работы (число раз, которое работа выполняется в рамках проведения родительской работы), затем результаты складываются. Если во всех работах модели включен режим ***Compute from Decompositions***, подобные вычисления автоматически проводятся по всей иерархии работ снизу вверх (рис 2.4). Этот достаточно упрощенный принцип подсчета справедлив, если работы выполняются последовательно.

Обычно все расходы, рассмотренные в модели, можно разбить на две части. В первую войдут затраты, не связанные с конкретными этапами бизнес-процесса. Это, например, оклады сотрудников, оплата за электроэнергию и т.д. Их относят к контекстной диаграмме. Для внесения этих характеристик в модель их описывают в таблице на вкладке ***Costs***, причем переключатель ***Data is from level*** устанавливают в положение ***Override Decomposition*** [2].

Рис. 2.4. Вычисление затрат родительской работы [2]

Многие диаграммы нижнего уровня можно описать стоимостными характеристиками, присущими данному этапу модели. Так, отметив эти издержки в ***Costs***, установив переключатель ***Data is from level*** в положение ***Compute from decompositions***, можно учесть расходы на диаграммах более высоких уровней. Таким образом, на контекстной диаграмме можно просмотреть общие расходы на этапы нижнего уровня (***Override Decomposition***), а также расходы, переданные «вверх» от декомпозиций нижнего уровня **(*Compute from decompositions***).

Свойства, определяемые пользователем (UDP)

ABC позволяет оценить стоимостные и временные характеристики системы. Если стоимостных показателей недостаточно, имеется возможность внесения собственных метрик — свойств, определенных пользователем — (***User Defined Properties***, UDP). UDP позволяют провести дополнительный анализ, хотя и без суммирующих подсчетов [3].

Для описания UDP служит диалог User-Defined Property Editor (меню Model/UDP Definition Editor) (рис. 2.5.). В верхнем окне диалога вносится имя UDP, в списке выбора Datatype описывается тип свойства. Имеется возможность задания 18 различных типов UDP, в том числе управляющих команд и массивов, объединенных по категориям. Для внесения категории следует задать имя категории в окне ***New Keyword*** и щелкнуть по кнопке ***Add Category***. Для присвоения свойства категории необходимо выбрать UDP из списка, затем категорию из списка категорий и щелкнуть по кнопке ***Update***. Одна категория может объединять несколько свойств, в то же время одно свойство может входить в несколько категорий. Свойство типа ***List*** может содержать массив предварительно определенных значений. Для определения области значений UDP типа List следует задать значение свойства в окне New Keyword и щелкнуть по кнопке ***Add Member***. Значения из списка можно редактировать и удалять.

Рис. 2.5. Диалог описания UDP [2]

Каждой работе можно поставить в соответствие набор UDP. Для этого следует щелкнуть правой кнопкой мыши по работе и выбрать пункт меню UDP. В закладке UDP ***Values*** диалога IDEF0 Activity Properties можно задать значения UDP. Результат задания можно проанализировать в отчете ***Diagram Object Report*** (меню Tools/Report/Diagram Object Report) [2].

Проведение экспертизы модели

Цикл автор-читатель. Цикл автор-читатель (рис. 2.6) предназначен для обеспечения обратной связи при построении модели. Он включает определенные формализованные процедуры, предписывающие правила координации деятельности участников создания модели. В работе над моделью принимают участие специалисты разных профилей – аналитики (авторы), эксперты предметной области (читатели), библиотекари и комитет технического контроля. Обычно библиотекарь выделяется для больших проектов. Цикл автор - читатель содержит следующие этапы [2].

На очередном этапе декомпозиции аналитик создает диаграмму на основе общих знаний, анализа документации и опроса экспертов. Общие знания не позволяют создать диаграмму достаточно корректно, поэтому она нуждается в уточнении и дополнении.

Все коммуникации при создании модели контролируются библиотекарем. Он ответственен за прохождение папок и архивирование диаграмм модели. После создания диаграмма посылается библиотекарю для помещения в архив.

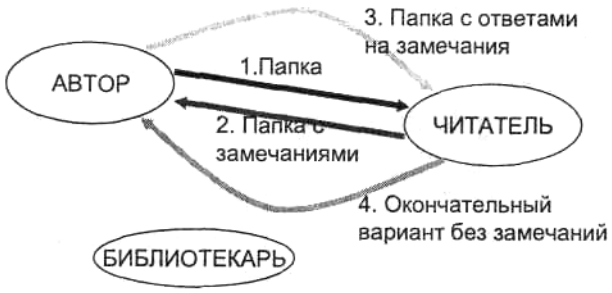


Рис. 2.6. Цикл автор-читатель [3]

Автором формируется папка и передается для распространения библиотекарю (одна копия направляется автору). В папку должна входить текущая диаграмма. Кроме того, в папку могут включаться сопутствующие отчеты, в том числе словарь стрелок и работ, диаграмма верхнего уровня, дерево узлов и любая необходимая дополнительная документация. На папке регистрируются входящие данные - дата, автор, данные читателя и т. д., после чего папка направляется эксперту предметной области (читателю).

Читатель рецензирует папку и записывает свои комментарии. Замечания вносятся в диаграмму по определенным правилам. Если читатель решил внести замечание, он должен указать номер замечания, затем внести текст замечания и в каркасе диаграммы в разделе Notes зачеркнуть цифру, соответствующую номеру замечания (рис. 2.7).

После рецензирования папки возвращаются библиотекарю. Библиотекарь должен обеспечивать проведение рецензирования в срок. Затем папки регистрируются и направляются автору.

Автор вносит ответ на замечания и, если он согласен с замечаниями, вносит изменения в модель. На практике зачастую сеанс экспертизы проводится в форме устного собеседования между автором и экспертом. В этом случае особенно важно вносить замечания эксперта и комментарии автора в диаграмму для документирования всех идей, возникших в результате моделирования.

Если это необходимо, проводится дополнительная экспертиза у того же или у другого эксперта.

Рис. 2.7. Внесение замечаний в диаграмму [3]

После прохождения нескольких циклов число замечаний обычно уменьшается, и диаграмма становится стабильной. В процессе изменения диаграмма может менять свой статус, который должен быть отражен в каркасе. Когда автор считает, что диаграмма уже достаточно проработана и достигла уровня ***Recommended***, он пересылает ее на утверждение в комитет технического контроля, где она проходит окончательную экспертизу. После внесения замечаний и окончательных изменений диаграмма (или набор диаграмм) окончательно утверждается, получает статус ***Publication*** и может быть распечатана и распространена среди участников проекта.

ПРАКТИЧЕСКАЯ ЧАСТЬ

ЧАСТЬ I

Пример построения IDEF0-модели бизнес-процесса телевизионной службы новостей

Описание проблемы: в телевизионных компаниях служба информации – это, как правило, структурное подразделение, занимающееся подготовкой и выпуском программ и новостей в эфир. В зависимости от масштабов и зоны вещания телерадиокомпаний варьируются штат, техническое оснащение, частота выходов в эфир. Однако практически во всех службах действуют общие принципы функционирования, призванные обеспечить оперативную выдачу информации в эфир и наполняемость выпусков [3].

Редакции новостей центральных (федеральных) каналов хорошо организованы и технически обеспечены. Региональные информационные службы (как государственные, так и частные) зачастую ограничены в ресурсах, что не может не сказываться на качестве

репортажей. Кроме того, подчас оставляет желать лучшего и порядок работы. Причина – недостаток квалифицированных кадров при неуклонном росте числа телерадиокомпаний, появляющихся в российских регионах. В сложившейся ситуации для оптимизации затрат, а также технических ресурсов и штата в соответствии с потребностями отделов актуально моделирование бизнес-процессов.

Процесс построения модели процесса «Функционирование службы информации»

Перед началом моделирования необходимо определить основные составляющие компоненты контекстной диаграммы, с построения которой начинается процесс создания бизнес-модели [3].

***Цель работы службы информации*:** выдача в эфир выпусков новостей;

***Сырье для работы*:** источники информации (справочники, газеты, ленты новостей интернета, звонки телезрителей)

***Исполнители*:** а) штатные сотрудники (журналисты, редакторы, операторы и режиссеры) и б) технические ресурсы (компьютеры, камеры, аппаратно-студийный блок, аппаратная видеозаписи и т.д.).

Задание № 1: Средствами пакета Ramus Educational построить контекстную диаграмму «Функционирование службы информации» (рис. 2.8)

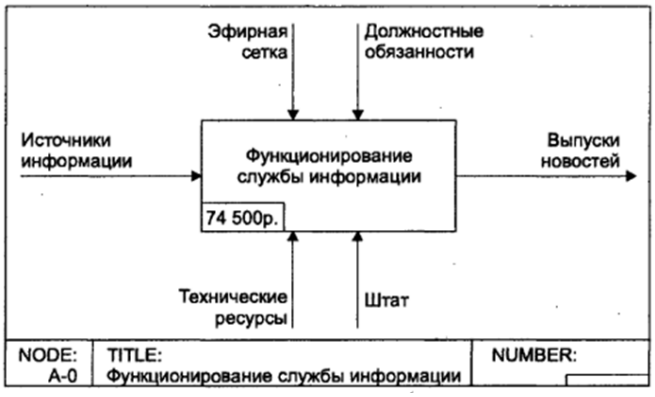


Рис. 2.8. Контекстная диаграммы «Функционирование службы информации»

Задание № 2: Построить диаграмму декомпозиции «Функционирование службы информации».

В работе службы информации можно выделить четыре основных этапа подготовки выпусков новостей: планирование эфира, съемки сюжетов, монтаж сюжетов, выход в эфир. Так как планирование основано на расписании выпусков новостей, то эфирная сетка является входом, который используется для получения результата на данном этапе – составление графика работ и планов съемок. Кроме того, эфирная сетка является управлением для последнего этапа работы «Эфир», так как она регламентирует эфирное расписание. Декомпозиция контекстной диаграммы представлена на рис. 2.9. Очевидно,

что эта диаграмма недостаточно детализирована, чтобы понять как функционирует служба информации, поэтому требуется более подробное описание.

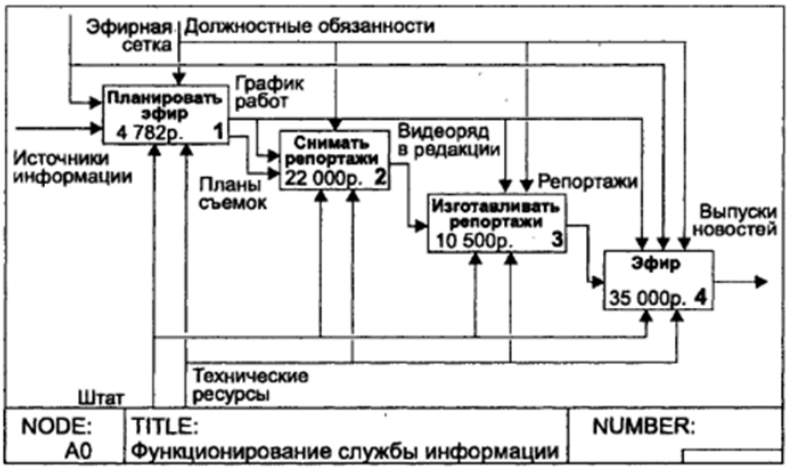


Рис. 2.9. Декомпозиция контекстной диаграммы

Задание № 3. Построить диаграмму «Планировать эфир».

На данном этапе происходит поиск информационных поводов, которые могут стать темами для будущих сюжетов новостей (рис. 2.10).

Каждый вечер накануне эфирного дня, а также утром редактор выпусков вместе с ведущими и корреспондентами просматривает газеты, ленты новостей интернета и поиска информации. Из всех найденных сообщений выбираются те, которые способны заинтересовать зрителей и соответствуют общей концепции вещания. На диаграмме декомпозиции (рис. 2.10) такие критерии указываются стрелками, «*помещенными в тоннель*». Составляется график, в котором определены временные пределы съемок, написания текста и монтажа. При этом назначаются исполнители – журналисты, операторы, водители. Корреспонденты консультируются с редактором о том, как лучше сделать сюжет, собирают информацию по теме, договариваются об интервью по телефону и составляют план съемок.

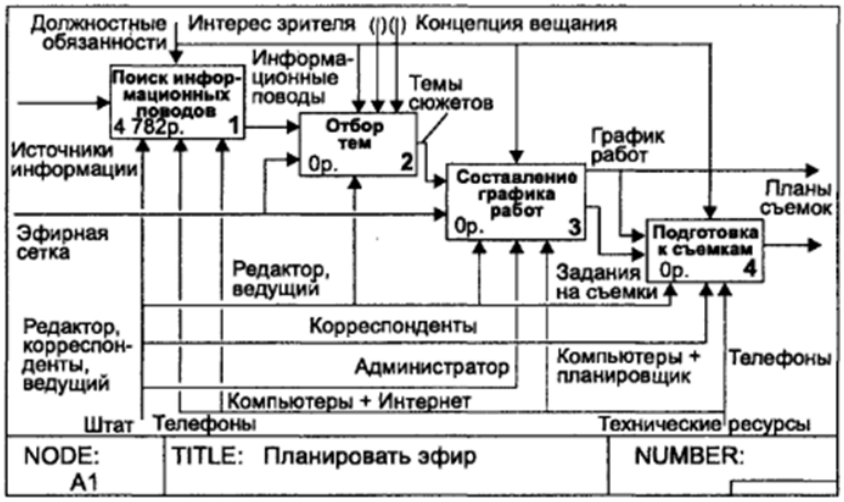


Рис. 2.10. Диаграмма «Планировать эфир»

Задание № 4. Построить диаграмму «Поиск информационных поводов».

На основе рис. 2.11. построить диаграмму «Поиск информационных поводов», самостоятельно проанализировать работы и стрелки на диаграмме.

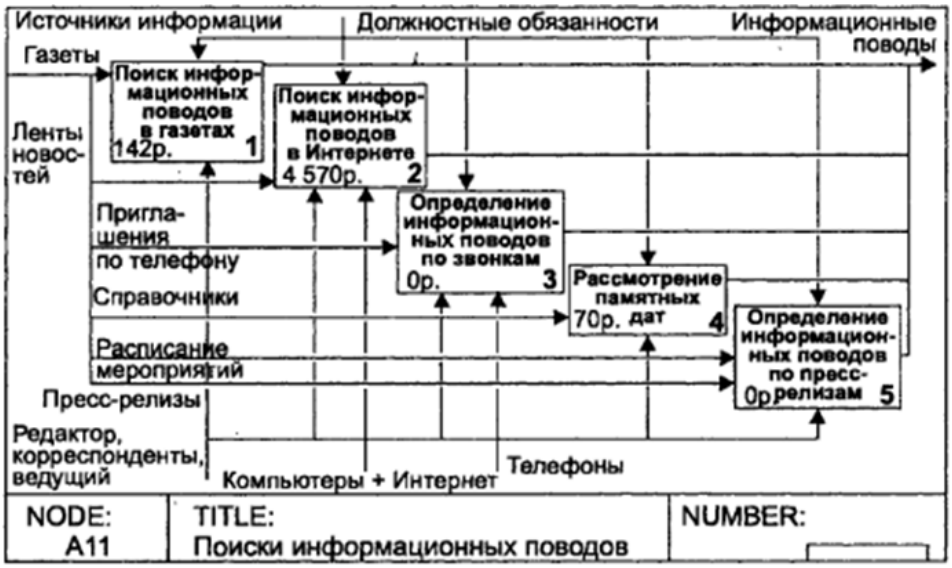


Рис. 2.11. Диаграмма «Поиск информационных поводов»

Задание № 5. Построить диаграмму «Снимать репортажи».

Съемка новостей осуществляется на основе плана, а также временных ограничений. Съемочная группа выезжает на место, корреспондент уточняет предварительную информацию, записывает интервью, оператор снимает «картинки», используя телевизионный журналистский комплект (ТЖК) – камеру, микрофон, штатив и светильник. После завершения работы съемочная группа возвращается в редакцию (рис. 2.12.)

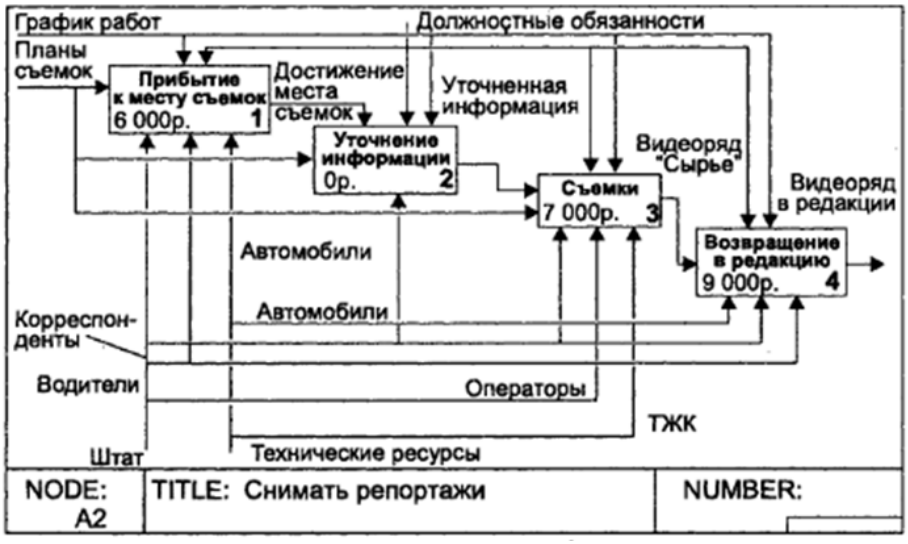


Рис. 2.12. Диаграмма «Снимать репортажи»

Задание № 6. Построить диаграмму «Изготавливать репортажи».

Диаграмма на рис. 2.13. дает понимание, какие штатные сотрудники участвуют в создании сюжета после съемок. Прежде всего, журналист просматривает видео в

просмотровой и расписывает монтажный лист – содержание видеоряда и интервью. Для видео он пишет текст, который в случае необходимости правит редактор. Сюжет монтируется по проверенному тексту. Иногда во время монтажа журналиста консультирует режиссер.

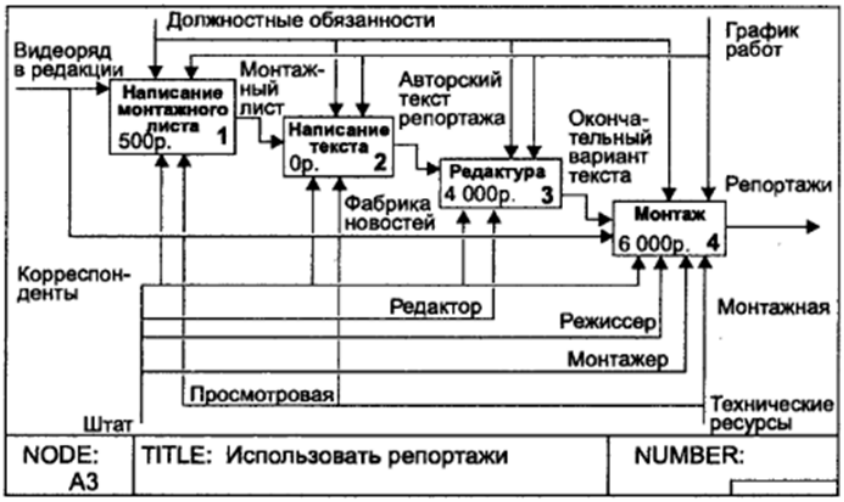


Рис. 2.13. Диаграмма «Изготавливать репортажи»

Задание № 7. Построить диаграмму «Эфир».

Верстка выпуска предполагает определение порядка следования репортажей, написание подводок, проверку на соответствие временным лимитам. При этом используется сетевая компьютерная программа СУБД «Фабрика новостей». Заполняется микрофонная папка, которая визируется главным редактором. Режиссер проверяет готовность сюжетов и составляет эфирный лист с порядком следования сюжетов и номерами кассет для сотрудников аппаратно-студийного блока (АСБ) и аппаратной видеозаписи (АВЗ). Во время эфира ведущий находится в студии, техническая поддержка осуществляется АСБ, сюжеты запускаются в АВЗ (рис. 2.14).

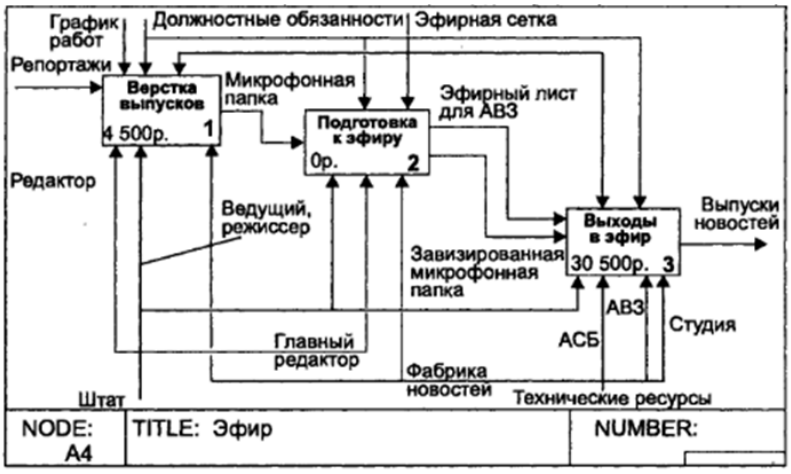


Рис. 2.14. Диаграмма «Эфир»

Задание № 8 (данное задание является творческим и выполняется по желанию студента).

Попробуйте придумать и описать какой-либо процесс или вашу деятельность «Процесс моего обучения в вузе». Разработайте контекстную диаграмму и 3-4 диаграммы декомпозиции.

ЧАСТЬ II

Используя ресурсы сети интернет, пакет Office каждый из студентов формирует одно задание по данной теме. Суть задания – разработать модель бизнес-процесса, составить карту процесса, провести ФСА. Сфера деятельности предприятия может быть любой, но обязательно прописана в задании. Для описания сферы деятельности предприятия можно использовать ресурсы сети Интернет.

Задание должно содержать:

1. Название предприятия;
2. Описание деятельности;
3. Описание проблемы для создания модели;
4. Описание точки зрения;
5. Описание участников;
6. Описание бизнес-процесса для построения модели;
7. Описание области моделирования.

Задание может быть составлено в текстовом документе, презентации и проч. по желанию студента (использование технических средств обязательно).

Далее задания по кругу выдаются остальным студентам для реализации. По итогам занятия автор задания и преподаватель оценивают степень и качество его выполнения.

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Какие существуют критерии для определения момента завершения моделирования;
2) Чем отличается метод функционально стоимостного анализа от традиционных финансовых методов;
3) Что необходимо предпринять, в случае если стоимостных показателей системы ABC недостаточно?
4) Что означает выбор переключателя *Data is from level* в положения *Override Decomposition* и *Compute from Decomposition?*
5) При каком условии можно начинать функционально-стоимостный анализ?
6) Какие характеристики необходимо указать, прежде чем приступать к анализу стоимости работы?
7) Какова основная задача ФСА?
8) Что является основным критерием совершенствования с позиции ФСА?
9) Какие задачи можно решить при помощи метода ФСА?

ЛАБОРАТОРНАЯ РАБОТА № 3
Построение диаграммы деятельности в нотации UML

Цель работы: получить навык разработки диаграммы деятельности с помощью нотации унифицированного языка моделирования UML.

Оборудование: компьютеры с операционной системой Windows XP и выше, наличие любой программы поддерживающей нотацию UML (в данной лабораторной работе используется Software Ideas Modeler).

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Унифицированный язык объектно-ориентированного моделирования ***Unified Modeling Language (UML)*** – это стандартная нотация визуального моделирования программных систем, принятая консорциумом Object Managing Group (OMG) осенью 1997 г. Введение в UML по ходу данной лабораторной работы начнем с известной картинки уже достаточно долго живущей в Интернете (рис. 3.1). Она в полной мере демонстрирует типичный процесс создания продукта, или "решения" [4].

Здесь четко видны все проблемы программной инженерии, в частности проблемы с коммуникацией и пониманием, вызванные отсутствием четкой спецификации создаваемого продукта. Авторы UML определяют его как графический язык моделирования общего назначения (т. е. его можно применять для проектирования чего угодно - от простой качели, как на рисунке, до сложного аппаратно-программного комплекса или даже космического корабля), предназначенный для спецификации, визуализации, проектирования и документирования всех артефактов, создаваемых в ходе разработки.

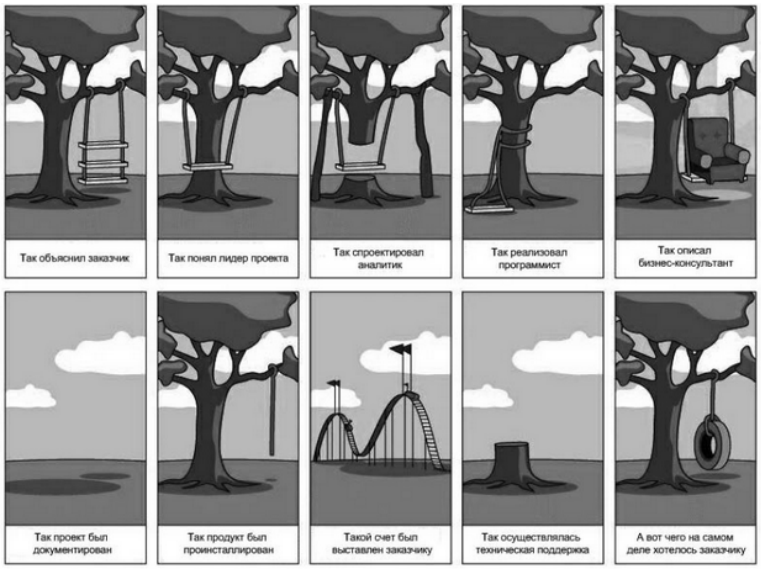


Рис. 3.1. Демонстрация разных взглядов заказчика и исполнителя на проблему

UML позволяет строить различные типы диаграмм, их выбор определяется исходными целями моделирования:

Для моделирования бизнес-процессов, технологических процессов, последовательных и параллельных вычислений используется диаграмма деятельности. ***Диаграмма деятельности (Activity diagram)*** — диаграмма, на которой показано разложение некоторой ***деятельности*** на её составные части [5].

Каждая диаграмма деятельности должна иметь единственное начальное и конечное состояния. При этом каждая деятельность начинается в начальном состоянии и заканчивается в конечном состоянии. Саму диаграмму деятельности принято располагать таким образом, чтобы действия следовали сверху вниз или слева направо. В этом случае начальное состояние будет изображаться в верхней или левой части диаграммы, а конечное - в ее нижней или правой части. В интересах удобства визуального представления на диаграмме деятельности допускается изображать несколько конечных состояний. В этом случае все их принято считать эквивалентными друг другу. Если из состояния действия выходит единственный переход, то его можно никак не помечать. Если же таких переходов несколько, то при моделировании последовательной деятельности запускается только один из них. При этом для всех выходящих из некоторого состояния деятельности переходов должно выполняться требование истинности только одного из них. Подобный случай встречается тогда, когда последовательно выполняемая деятельность должна разделиться на альтернативные ветви в зависимости от значения промежуточного результата. Такая ситуация получила название ветвления, а для ее обозначения применяется специальный символ решения.

Графически ветвление на диаграмме деятельности обозначается символом решения (decision), изображаемого в форме ***небольшого ромба***, внутри которого нет никакого текста (рис. 3.2 вверху). В этот ромб может входить только одна стрелка от того состояния действия, после выполнения которого поток управления должен быть продолжен по одной из взаимно исключающих ветвей. Принято входящую стрелку присоединять к верхней или левой вершине символа решения. Выходящих стрелок может быть две или более, но для каждой из них явно указывается соответствующее сторожевое условие в форме булевского выражения.

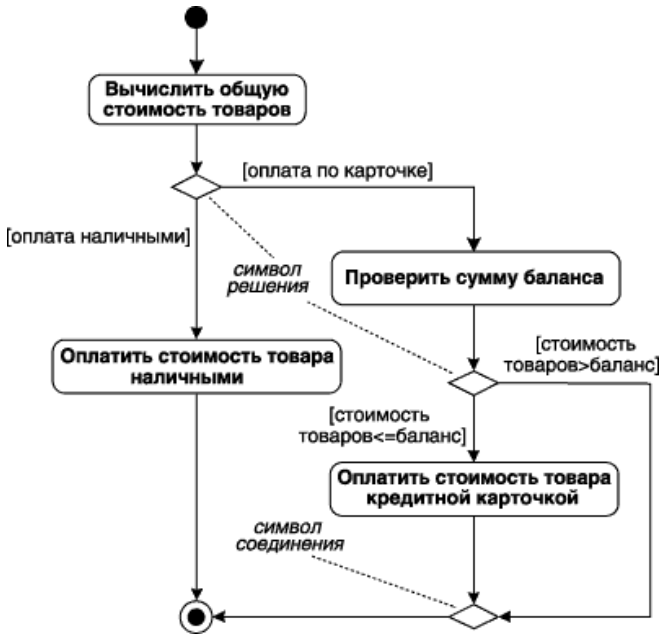


Рис. 3.2. Различные варианты ветвлений на диаграмме деятельности

Для ***графического объединения альтернативных ветвей*** на диаграмме деятельности рекомендуется также использовать ***аналогичный символ в форме ромба***, который в этом случае называют соединением (***merge***). Наличие этого символа, внутри которого также не записывается никакого текста, упрощает визуальный контроль логики выполнения процедурных действий на диаграмме деятельности (рис. 3.2. внизу). Входящих стрелок у символа соединения может быть несколько, они исходят от состояний действия, принадлежащих к одной из взаимно исключающих ветвей. Выходить из ромба соединения может только одна стрелка, при этом ни входящие, ни выходящая стрелки не должны содержать сторожевых условий. Исключением является ситуация, когда с целью сокращения диаграммы объединяют символ решения с символом соединения. Нарушение этих правил делает диаграмму деятельности несостоятельной (ill formed).

Диаграмма деятельности (рис. 3.2) моделирует ситуацию, возникающую в супермаркетах при оплате товаров. Как правило, заплатить за покупки можно либо наличными, либо по кредитной карточке. Если покупателем выбран вариант оплаты по кредитной карточке, то проверяется сумма баланса предъявленной к оплате кредитной карточки. При этом оплата происходит только в том случае, если общая стоимость приобретаемых товаров не превышает суммы баланса этой карточки. В противном случае оплаты не происходит, и товар остается у продавца.

Обычно распараллеливание вычислений существенно повышает общее быстродействие программных систем, поэтому необходимы графические примитивы для представления параллельных процессов. В диаграммах деятельности с этой целью используется специальный символ для ***разделения и слияния параллельных вычислений***

или потоков управления. Это прямая черточка, аналогичная обозначению параллельных переходов для диаграмм состояний. На диаграммах деятельности такая черточка изображается отрезком горизонтальной, реже - вертикальной, линии, толщина которой несколько шире линий простых переходов диаграммы деятельности. При этом ***разделение (fork) имеет*** один входящий переход и несколько выходящих (рис. 3.3а), которые изображаются отрезками вертикальных, реже - горизонтальных, линий. ***Слияние (join)***, наоборот, имеет несколько входящих переходов и один выходящий (рис. 3.3 б). Параллельные переходы на диаграмме деятельности можно изображать в удлиненной форме, а входящие и выходящие переходы вертикальными стрелками.

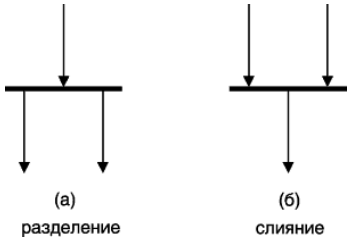


Рис. 3.3. Графическое изображение разделения и слияния параллельных потоков управления на диаграмме деятельности

Рассмотренных переходов оказывается достаточно для моделирования различных по сложности ситуаций. Для иллюстрации особенности изображения ветвления и параллельных деятельностей можно рассмотреть пример регистрации пассажиров в аэропорту (рис. 3.4.) [5].

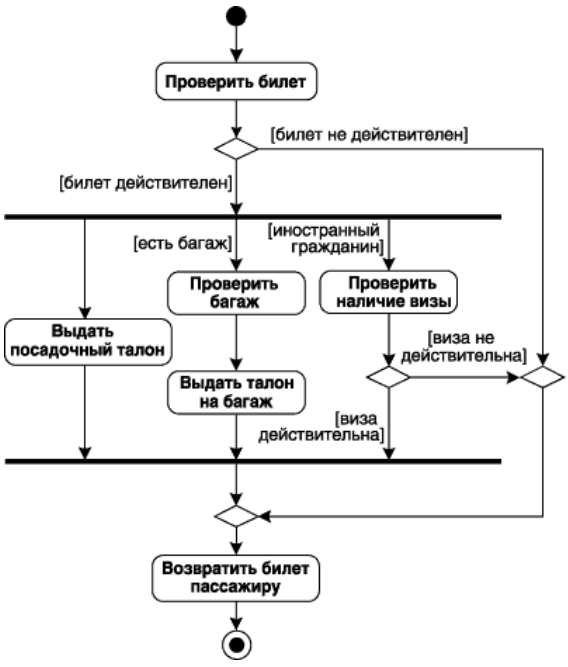


Рис. 3.4. Диаграмма деятельности для примера регистрации пассажиров в аэропорту

Первоначально выполняется деятельность по проверке билета. В случае если билет не действителен, он возвращается пассажиру, при этом никаких дополнительных действий

не выполняется. Если же билет действителен, то пассажиру выдается посадочный талон. В дополнение к этому проверяется гражданство и наличие багажа у пассажира. Если есть багаж, то его проверка может быть выполнена параллельно, по результатам которой пассажиру выдается талон на багаж. Если пассажир является иностранным гражданином, то дополнительно проверяется наличие у него визы. Если виза действительна, то проверка завершается успешно, и пассажир с возвращенным ему билетом может проследовать на посадку.

Если же виза окажется не действительной, то для этого пассажира посадка на данный рейс оказывается невозможной. В этом случае ему не выдается посадочный талон и талон на багаж, в случае его наличия, поскольку происходит прекращение всех выполняемых сотрудниками аэропорта действий.

Дорожки

Как правило, применительно к бизнес-процессам желательно выполнение каждого действия ассоциировать с конкретным подразделением компании. В этом случае подразделение будет нести ответственность за реализацию определенных действий, а сам бизнес-процесс представляется в виде переходов действий из одного подразделения к другому. Для моделирования этих особенностей в языке UML предложена специальная конструкция, получившая название дорожки.

Дорожка (swimlane) - графическая область диаграммы деятельности, содержащая элементы модели, ответственность за выполнение которых принадлежит отдельным подсистемам.

В данном случае имеется в виду визуальная аналогия с плавательными дорожками в бассейне, если смотреть на соответствующую диаграмму деятельности сверху. При этом все состояния на диаграмме деятельности делятся на группы, разграниченные вертикальными линиями. Две соседних линии и образуют дорожку, а группа состояний между этими линиями выполняется организационным подразделением (отделом, группой, отделением, филиалом) или сотрудником компании (рис. 3.5). В последнем случае принято указывать должность сотрудника, ответственного за выполнение определенных действий.

Названия подразделений или должностей явно указываются в верхней части дорожки. Пересекать линию дорожки могут только переходы, которые в этом случае обозначают выход или вход потока управления в соответствующее подразделение компании. Порядок следования дорожек не несет какой-либо семантической информации и определяется соображениями удобства.

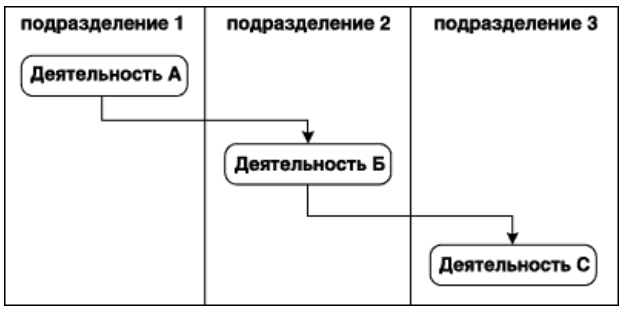


Рис. 3.5. Вариант диаграммы деятельности с дорожками

В качестве примера рассмотрим фрагмент диаграммы деятельности торговой компании, обслуживающей клиентов в форме заказов. Подразделениями компании обычно являются отдел приема и оформления заказов, отдел продаж и склад. Этим подразделениям будут соответствовать три дорожки на диаграмме деятельности, каждая из которых специфицирует зону ответственности подразделения. В этом случае диаграмма деятельности заключает в себе не только информацию о последовательности выполнения рабочих действий, но и о том, какое подразделение торговой компании должно выполнять, то или иное действие (рис. 3.6). Из указанной диаграммы деятельности видно, что после принятия заказа от клиента отделом приема и оформления заказов осуществляется распараллеливание деятельности на два потока (переход-разделение). Первый из них остается в этом же отделе и связан с получением оплаты от клиента за заказанный товар. Второй инициирует выполнение действия по регистрации заказа в отделе продаж (модель товара, размеры, цвет, год выпуска и пр.). Однако выдача товара со склада начинается только после того, как будет получена от клиента оплата за товар (переход-слияние). Затем выполняется подготовка товара к отправке и его отправка клиенту в отделе продаж. После завершения этих деятельностей заказ закрывается в отделе приема и оформления заказов [5].

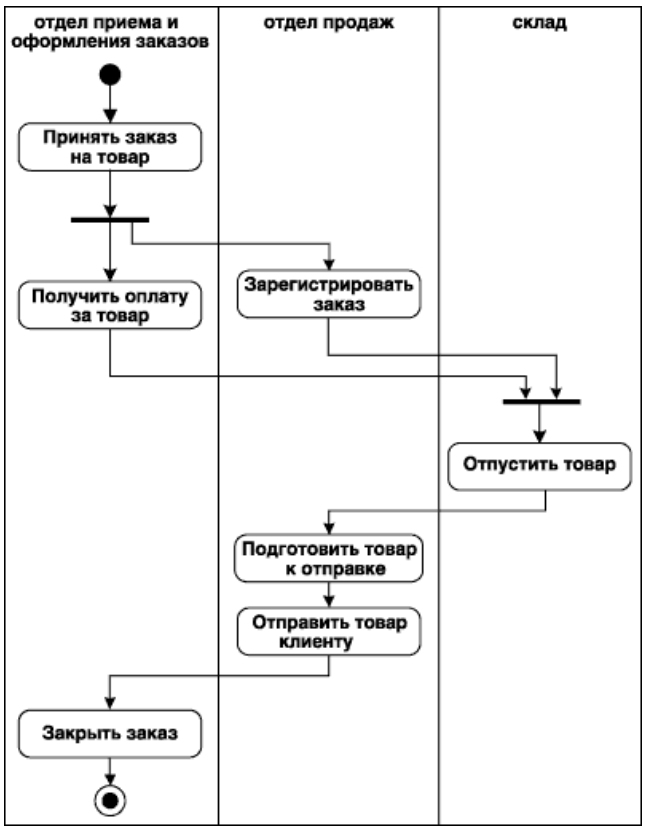


Рис. 3.6. Фрагмент диаграммы деятельности для торговой компании

Объекты на диаграмме деятельности

Действия на диаграмме деятельности могут производиться над теми или иными объектами. Эти объекты либо инициируют выполнение действий, либо определяют результат этих действий. При этом действия специфицируют вызовы, которые передаются от одного объекта графа деятельности другому. Поскольку в таком ракурсе объекты играют определенную роль в понимании процесса деятельности, иногда возникает необходимость явно указать их на диаграмме деятельности.

Базовым графическим представлением объекта в нотации языка UML является ***прямоугольник класса,*** с тем отличием, что имя объекта подчеркивается. На диаграммах деятельности после имени может указываться характеристика состояния объекта в прямых скобках. Такие прямоугольники объектов присоединяются к состояниям действия отношением зависимости пунктирной линией со стрелкой. Соответствующая зависимость определяет состояние конкретного объекта после выполнения предшествующего действия.

На диаграмме деятельности с дорожками расположение объекта может иметь дополнительный смысл. А именно, если объект расположен на границе двух дорожек, то это может означать, что переход к следующему состоянию действия в соседней дорожке ассоциирован с нахождением документа в некотором состоянии. Если же объект

расположен внутри дорожки, то и состояние этого объекта целиком определяется действиями данной дорожки.

Применительно к диаграммам деятельности объекты, как правило, являются экземплярами классов сущностей или бизнес - сущностей. Стоит также заметить, что на диаграмме деятельности один и тот же объект может быть изображен несколько раз, при этом для исключения несогласованности диаграммы необходимо указывать для них различные характеристики состояния.

В предыдущем примере с торговой компанией центральным объектом процесса продажи является заказ или вернее состояние его выполнения. Вначале до обращения клиента заказ как объект отсутствует и возникает лишь после контакта с клиентом. В результате фиксируется полученный заказ, после чего он регистрируется в отделе продаж. Затем он передается на склад, где после получения оплаты за товар оформляется окончательно. Наконец, после того, как товар отправлен клиенту, эта информация вносится в заказ, и он считается выполненным. Эта информация может быть представлена графически в виде модифицированного варианта диаграммы деятельности торговой компании (рис. 3.7).

Достоинством диаграммы деятельности является возможность визуализировать отдельные аспекты поведения рассматриваемой системы или реализации отдельных операций классов в виде процедурной последовательности действий. Таким образом, полная модель системы может содержать одну или несколько диаграмм деятельности, каждая из которых описывает последовательность реализации либо наиболее важных вариантов использования (типичный ход событий и все исключения), либо нетривиальных операций классов.

В заключение следует заметить, что диаграмма деятельности, так же как и другие виды канонических диаграмм, не содержат средств выбора оптимальных вариантов конфигурации собственно диаграмм. При разработке сложных проектов проблема выбора оптимальных решений применительно к диаграммам деятельности становится весьма актуальной. Рациональное расходование средств, затраченных на разработку и эксплуатацию системы, повышение ее производительности и надежности зачастую определяют конечный результат всего проекта [2].

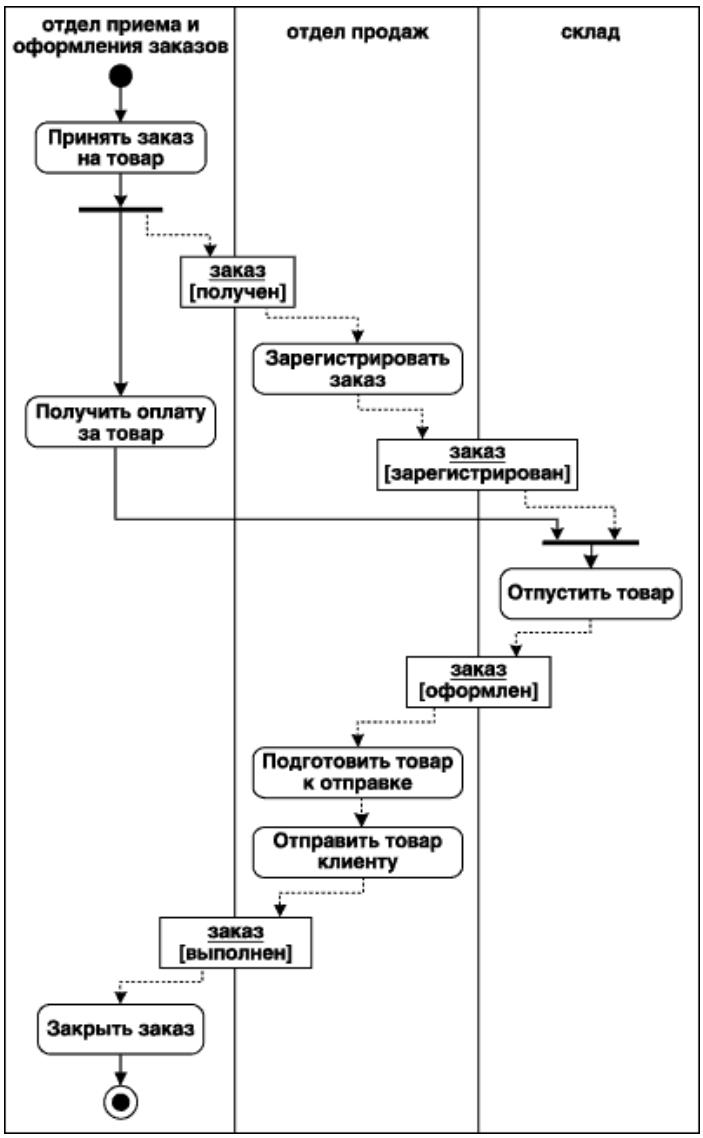


Рис. 3.7. Фрагмент диаграммы деятельности торговой компании с объектом-заказом

ПРАКТИЧЕСКАЯ ЧАСТЬ

1) На основе представленного материала разработать диаграммы деятельности, показанные на рис. 3.4, 3.6 и 3.7 средствами программного продукта Software Ideas Modeler.

2) Используя семантику языка UML, опишите деятельность по приготовлению вашего любимого блюда.

3) Постройте диаграмму деятельности «Продажа и прокат видео» на основе следующего описания [6]:

«Магазин продает видеокассеты, DVD-диски, аудио-кассеты, CD-диски и т.д., а также предлагает широкой публике прокат видеокассет и DVD-дисков. Товары поставляются несколькими поставщиками. Каждая партия товара предварительно заказывается магазином у некоторого поставщика и доставляется после оплаты счета. Вновь

поступивший товар маркируется, заносится в базу данных и затем распределяется в торговый зал или прокат.

Видеоносители выдаются в прокат на срок от 1 до 7 дней. При прокате с клиента взимается залоговая стоимость видеоносителя. При возврате видеоносителя возвращается залоговая стоимость минус сумма за прокат. Если возврат задержан менее чем на 2 дня, взимается штраф в размере суммы за прокат за 1 день*кол-во дней задержки. При задержке возврата более чем на 2 дня - залоговая сумма не возвращается. Клиент может взять одновременно до 4 видеоносителей (прокат-заказ). На каждый видеоноситель оформляется квитанция.

Клиенты могут стать членами видео-клуба и получить пластиковые карточки. С членов клуба не берется залог (за исключением случая описанного ниже), устанавливается скидка на ставку проката и покупку товаров. Члены клуба могут делать предварительные заказы на подбор видеоматериалов для проката или покупки. Каждый член клуба имеет некоторый статус. Первоначально – «новичок». При возврате в срок 5 прокат-заказов, статус меняется на «надежный». При задержке хотя бы одного видеоносителя более чем на 2 дня, статус «новичок» или «надежный» меняется на «ненадежный» и клиенту высылается предупреждение. При повторном нарушении правил статус меняется на «нарушитель». Члены клуба со статусом «надежный» могут брать до 8 видеоносителей единовременно, все остальные – 4. С членов клуба со статусом «нарушитель» берется залоговая сумма.

Клиенты при покупке товара или получении видеоносителя в прокат могут расплачиваться наличными или кредитной картой».

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Как расшифровывается аббревиатура UML?
2) Как графически изобразить начало и конец процесса на диаграмме деятельности?
3) Каков смысл использования дорожек на диаграммах деятельности UML?
4) Сколько начальных и конечных состояний может иметь диаграмма деятельности в UML?
5) Каким образом изобразить ветвление (выбор альтернативы) на диаграмме деятельности?
6) Что является базовым графическим представлением объекта в нотации языка UML?
7) Каким образом, использование нотации UML могло бы помочь в решении проблемы, показанной на рис. 3.1?
8) В чем состоит недостаток диаграмм деятельности?

ЛАБОРАТОРНАЯ РАБОТА № 4

Построение диаграммы вариантов использования в нотации UML

Цель работы: получить навык разработки диаграммы вариантов использования с помощью нотации унифицированного языка моделирования UML.

Оборудование: компьютеры с операционной системой Windows XP и выше, наличие любой программы поддерживающей нотацию UML (в данной лабораторной работе используется бесплатно распространяемая программа Softaware Ideas Modeler).

Форма проведения занятия: интерактивное занятие с использованием метода презентации (1 ч).

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Визуальное моделирование в UML можно представить как некоторый процесс поуровневого спуска от наиболее обшей и абстрактной концептуальной модели исходной системы к логической, а затем и к физической модели соответствующей программной системы. Для достижения этих целей вначале строится модель в форме, так называемой ***диаграммы вариантов использования*** (***use case diagram***), которая описывает функциональное назначение системы или, другими словами, то, что система будет делать в процессе своего функционирования. Диаграмма вариантов использования является исходным концептуальным представлением или концептуальной моделью системы в процессе ее проектирования и разработки [7].

Разработка диаграммы вариантов использования преследует цели:

- ✓ определить общие границы и контекст моделируемой предметной области на начальных этапах проектирования системы.
- ✓ сформулировать общие требования к функциональному поведению проектируемой системы.
- ✓ разработать исходную концептуальную модель системы для ее последующей детализации в форме логических и физических моделей.
- ✓ подготовить исходную документацию для взаимодействия разработчиков системы с ее заказчиками и пользователями.

Суть данной диаграммы состоит в следующем [8]: проектируемая система представляется в виде множества сущностей или актеров, взаимодействующих с системой с помощью, так называемых вариантов использования. При этом ***актером (actor)*** или действующим лицом называется любая сущность, взаимодействующая с системой извне. Это может быть человек, техническое устройство, программа или любая другая система, которая может служить источником воздействия на моделируемую систему так, как определит сам разработчик. В свою очередь, ***вариант использования (use case)*** служит

для описания сервисов, которые система предоставляет актеру. Другими словами, каждый вариант использования определяет некоторый набор действий, совершаемый системой при диалоге с актером. При этом ничего не говорится о том, каким образом будет реализовано взаимодействие актеров с системой.

В самом общем случае, диаграмма вариантов использования представляет собой граф специального вида, который является графической нотацией для представления конкретных вариантов использования, актеров, возможно, некоторых интерфейсов, и отношений между этими элементами. **Базовыми элементами диаграммы являются вариант использования и актер.**

Вариант использования (use case) - внешняя спецификация последовательности действий, которые система или другая сущность могут выполнять в процессе взаимодействия с актерами. Каждый вариант использования определяет последовательность действий, которые должны быть выполнены проектируемой системой при взаимодействии ее с соответствующим актером. Диаграмма вариантов может дополняться пояснительным текстом, который раскрывает смысл или семантику составляющих ее компонентов. Такой пояснительный текст получил название примечания или сценария.

Отдельный вариант использования обозначается на диаграмме эллипсом, внутри которого содержится его краткое название (рис. 4.1.а) или имя в форме глагола (рис. 4.1.б) с пояснительными словами.

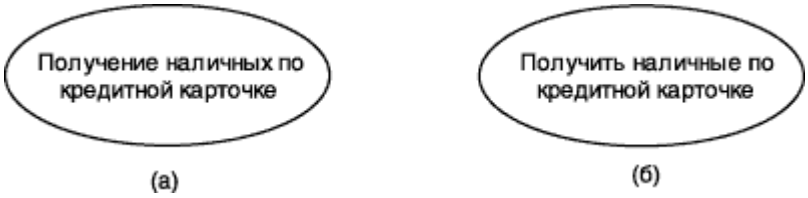


Рис. 4.1. Графическое обозначение варианта использования

Цель варианта использования заключается в том, чтобы определить законченный аспект или фрагмент поведения некоторой сущности без раскрытия внутренней структуры этой сущности. В качестве такой сущности может выступать исходная система или любой другой элемент модели, который обладает собственным поведением, подобно подсистеме или классу в модели системы.

Каждый вариант использования соответствует отдельному сервису, который предоставляет моделируемую сущность или систему по запросу пользователя (актера), т.е. определяет способ применения этой сущности. Сервис, который инициализируется по запросу пользователя, представляет собой законченную последовательность действий. Это

означает, что после того как система закончит обработку запроса пользователя, она должна возвратиться в исходное состояние, в котором готова к выполнению следующих запросов.

Варианты использования описывают не только взаимодействия между пользователями и сущностью, но также реакции сущности на получение отдельных сообщений от пользователей и восприятие этих сообщений за пределами сущности. Варианты использования могут включать в себя описание особенностей способов реализации сервиса и различных исключительных ситуаций, таких как корректная обработка ошибок системы. Множество вариантов использования в целом должно определять все возможные стороны ожидаемого поведения системы. Для удобства множество вариантов использования может рассматриваться как отдельный пакет.

Примерами вариантов использования могут являться следующие действия: проверка состояния текущего счета клиента, оформление заказа на покупку товара, получение дополнительной информации о кредитоспособности клиента, отображение графической формы на экране монитора и другие действия.

Актер (actor) - согласованное множество ролей, которые играют внешние сущности по отношению к вариантам использования при взаимодействии с ними. При этом актеры служат для обозначения согласованного множества ролей, которые могут играть пользователи в процессе взаимодействия с проектируемой системой. Каждый актер может рассматриваться как некая отдельная роль относительно конкретного варианта использования. Стандартным графическим обозначением актера на диаграммах является фигурка "человечка", под которой записывается конкретное имя актера (рис. 4.2).

Рис. 4.2. Графическое обозначение актера

В некоторых случаях актер может обозначаться в виде прямоугольника класса с ключевым словом <<actor>> и обычными составляющими элементами класса. Имена актеров должны записываться заглавными буквами и следовать рекомендациям использования имен для типов и классов модели. При этом символ отдельного актера связывает соответствующее описание актера с конкретным именем. Имена абстрактных актеров, как и других абстрактных элементов языка UML, рекомендуется обозначать курсивом.

Примечание: *имя актера должно быть достаточно информативным с точки зрения семантики. Вполне подходят для этой цели наименования должностей в компании (например, продавец, кассир, менеджер, президент). Не рекомендуется давать актерам*

имена собственные (например, "О.Бендер") или моделей конкретных устройств (например, "маршрутизатор Cisco 3640"), даже если это с очевидностью следует из контекста проекта. Дело в том, что одно и то же лицо может выступать в нескольких ролях и, соответственно, обращаться к различным сервисам системы. Например, посетитель банка может являться как потенциальным клиентом, и тогда он востребует один из его сервисов, а может быть и налоговым инспектором или следователем прокуратуры. Сервис для последнего может быть совершенно исключительным по своему характеру [8].

Примерами актеров могут быть: клиент банка, банковский служащий, продавец магазина, менеджер отдела продаж, пассажир авиарейса, водитель автомобиля, администратор гостиницы, сотовый телефон и другие сущности, имеющие отношение к концептуальной модели соответствующей предметной области.

Так как в общем случае актер всегда находится вне системы, его внутренняя структура никак не определяется. Для актера имеет значение только его внешнее представление, т.е. то, как он воспринимается со стороны системы. Актеры взаимодействуют с системой посредством передачи и приема сообщений от вариантов использования. Сообщение представляет собой запрос актером сервиса от системы и получение этого сервиса. Это взаимодействие может быть выражено посредством ассоциаций между отдельными актерами и вариантами использования или классами. Кроме этого, с актерами могут быть связаны интерфейсы, которые определяют, каким образом другие элементы модели взаимодействуют с этими актерами.

Два и более актера могут иметь общие свойства, т. е. взаимодействовать с одним и тем же множеством вариантов использования одинаковым образом. Такая общность свойств и поведения представляется в виде рассматриваемого ниже отношения обобщения с другим, возможно, абстрактным актером, который моделирует соответствующую общность ролей.

Интерфейс (interface) служит для спецификации параметров модели, которые видимы извне без указания их внутренней структуры. В языке UML интерфейс является классификатором и характеризует только ограниченную часть поведения моделируемой сущности. Применительно к диаграммам вариантов использования, интерфейсы определяют совокупность операций, которые обеспечивают необходимый набор сервисов или функциональности для актеров. Интерфейсы не могут содержать ни атрибутов, ни состояний, ни направленных ассоциаций. Они содержат только операции без указания особенностей их реализации. Формально интерфейс эквивалентен абстрактному классу без атрибутов и методов с наличием только абстрактных операций [9].

На диаграмме вариантов использования интерфейс изображается в виде маленького круга, рядом с которым записывается его имя (рис. 4.3, а). В качестве имени может быть существительное, которое характеризует соответствующую информацию или сервис (например, "датчик", "сирена", "видеокамера"), но чаще строка текста (например, "запрос к базе данных", "форма ввода", "устройство подачи звукового сигнала"). Если имя записывается на английском, то оно должно начинаться с заглавной буквы I, например, ***ISecureInformation, ISensor*** (рис. 4.3, б).

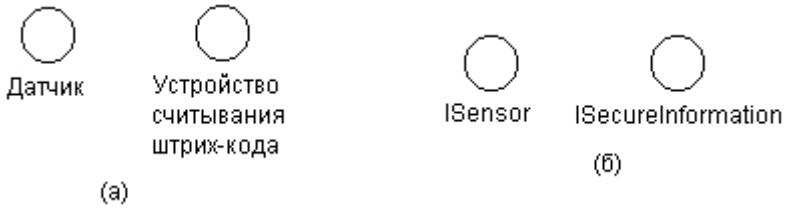


Рис. 4.3. Графическое изображение интерфейсов на диаграммах вариантов использования

Графический символ отдельного интерфейса может соединяться на диаграмме сплошной линией с тем вариантом использования, который его поддерживает. Сплошная линия в этом случае указывает на тот факт, что связанный с интерфейсом вариант использования должен реализовывать все операции, необходимые для данного интерфейса, а возможно и больше (рис. 4.4, а). Кроме этого, интерфейсы могут соединяться с вариантами использования пунктирной линией со стрелкой (рис. 4.4, б), означающей, что вариант использования предназначен для спецификации только того сервиса, который необходим для реализации данного интерфейса.

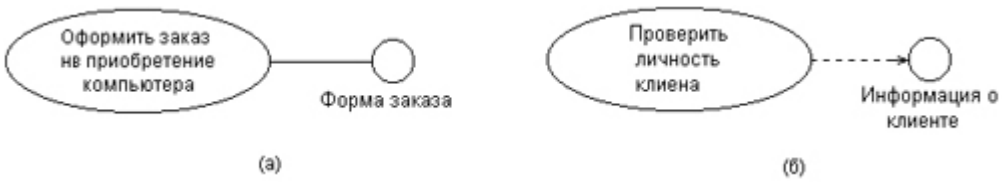


Рис. 4.4. Графическое изображение взаимосвязей интерфейсов с вариантами использования

Важность интерфейсов заключается в том, что они определяют стыковочные узлы в проектируемой системе, что совершенно необходимо для организации коллективной работы над проектом. Более того, спецификация интерфейсов способствует "безболезненной" модификации уже существующей системы при переходе на новые технологические решения. В этом случае изменению подвергается только реализация операций, но никак не функциональность самой системы. А это обеспечивает совместимость последующих версий программ с первоначальными при спиральной технологии разработки программных систем.

Примечания (notes) в языке UML предназначены для включения в модель произвольной текстовой информации, имеющей непосредственное отношение к контексту разрабатываемого проекта. В качестве такой информации могут быть комментарии разработчика (например, дата и версия разработки диаграммы или ее отдельных компонентов), ограничения (например, на значения отдельных связей или экземпляры сущностей) и помеченные значения. Применительно к диаграммам вариантов использования примечание может носить самую общую информацию, относящуюся к общему контексту системы.

Графически примечания обозначаются прямоугольником с "загнутым" верхним правым уголком (рис. 4.5). Внутри прямоугольника содержится текст примечания. Примечание может относиться к любому элементу диаграммы, в этом случае их соединяет пунктирная линия. Если примечание относится к нескольким элементам, то от него проводятся, соответственно, несколько линий. Разумеется, примечания могут присутствовать не только на диаграмме вариантов использования, но и на других канонических диаграммах.

Рис. 4.5. Примеры примечаний в языке UML

Отношения на диаграмме вариантов использования

Между компонентами диаграммы вариантов использования могут существовать различные отношения, которые описывают взаимодействие экземпляров одних актеров и вариантов использования с экземплярами других актеров и вариантов. Один актер может взаимодействовать с несколькими вариантами использования. В этом случае этот актер обращается к нескольким сервисам данной системы. В свою очередь один вариант использования может взаимодействовать с несколькими актерами, предоставляя для всех них свой сервис. Следует заметить, что два варианта использования, определенные для одной и той же сущности, не могут взаимодействовать друг с другом, поскольку каждый из них самостоятельно описывает законченный вариант использования этой сущности. Более того, варианты использования всегда предусматривают некоторые сигналы или

сообщения, когда взаимодействуют с актерами за пределами системы. В то же время могут быть определены другие способы для взаимодействия с элементами внутри системы [10].

Отношение (relationship) — семантическая связь между отдельными элементами модели. В языке UML имеется несколько стандартных видов отношений между актерами и вариантами использования [8]:

- ✓ отношение ассоциации (association relationship)
- ✓ отношение расширения (extend relationship)
- ✓ отношение обобщения (generalization relationship)
- ✓ отношение включения (include relationship)

При этом общие свойства вариантов использования могут быть представлены тремя различными способами, а именно с помощью отношений расширения, обобщения и включения.

Отношение ассоциации – одно из фундаментальных понятий в языке UML и в той или иной степени используется при построении всех графических моделей систем в форме канонических диаграмм. Применительно к диаграммам вариантов использования ассоциация служит для обозначения специфической роли актера при его взаимодействии с отдельным вариантом использования. Другими словами, ассоциация специфицирует семантические особенности взаимодействия актеров и вариантов использования в графической модели системы. На диаграмме вариантов использования, так же как и на других диаграммах, отношение ассоциации обозначается сплошной линией между актером и вариантом использования. Эта линия может иметь некоторые дополнительные обозначения, например, имя и кратность (рис. 4.6) [8].

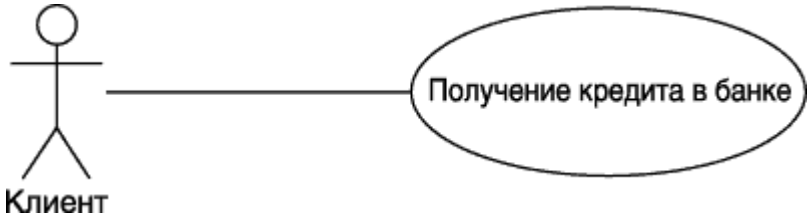


Рис. 4.6. Пример графического представления отношения ассоциации между актером и вариантом использования

В контексте диаграммы вариантов использования отношение ассоциации между актером и вариантом использования может указывать на то, что актер инициирует соответствующий вариант использования. ***Такого актера называют главным***. В других случаях подобная ассоциация может указывать на актера, которому предоставляется справочная информация о результатах функционирования моделируемой системы. ***Таких актеров часто называют второстепенными.***

Отношение расширения (extend) определяет взаимосвязь базового варианта использования с другим вариантом использования, функциональное поведение которого задействуется базовым не всегда, а только при выполнении дополнительных условий. В языке UML отношение расширения является зависимостью, направленной к базовому варианту использования и соединенной с ним в так называемой точке расширения. Отношение расширения между вариантами использования обозначается как отношение зависимости в форме пунктирной линии со стрелкой, направленной от того варианта использования, который является расширением для базового варианта использования. Данная линия со стрелкой должна быть помечена стереотипом <<extend>> ("расширяет"), как показано на рис. 4.7. [8].

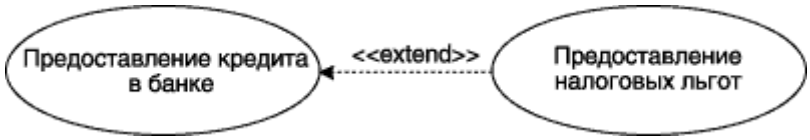


Рис. 4.7. Пример графического изображения отношения расширения между вариантами использования

Отношение расширения отмечает тот факт, что один из вариантов использования может присоединять к своему поведению некоторое дополнительное поведение, определенное для другого варианта использования. Данное отношение включает в себя некоторое условие и ссылки на точки расширения в базовом варианте использования. Чтобы расширение имело место, должно быть выполнено определенное условие данного отношения. Ссылки на точки расширения определяют те места в базовом варианте использования, в которые должно быть помещено соответствующее расширение при выполнении условия.

Один из вариантов использования может быть расширением для нескольких базовых вариантов, а также иметь в качестве собственных расширений несколько других вариантов. Базовый вариант использования может дополнительно никак не зависеть от своих расширений.

Семантика отношения расширения определяется следующим образом. Если экземпляр варианта использования выполняет некоторую последовательность действий, которая определяет его поведение, и при этом имеется точка расширения на экземпляр другого варианта использования, которая является первой из всех точек расширения у исходного варианта, то проверяется условие данного отношения. Если условие выполняется, исходная последовательность действий расширяется посредством включения действий экземпляра другого варианта использования. Следует заметить, что условие отношения расширения проверяется лишь один раз — при первой ссылке на точку

расширения, и если оно выполняется, то все расширяющие варианты использования вставляются в базовый вариант.

В представленном выше примере (рис. 4.7) при оформлении заказа на приобретение товара только в некоторых случаях может потребоваться предоставление клиенту каталога всех товаров. При этом условием расширения является запрос от клиента на получение каталога товаров. Очевидно, что после получения каталога клиенту необходимо некоторое время на его изучение, в течение которого оформление заказа приостанавливается. После ознакомления с каталогом клиент решает либо в пользу выбора отдельного товара, либо отказа от покупки вообще. Сервис или вариант использования "Оформить заказ на приобретение товара" может отреагировать на выбор клиента уже после того, как клиент получит для ознакомления каталог товаров.

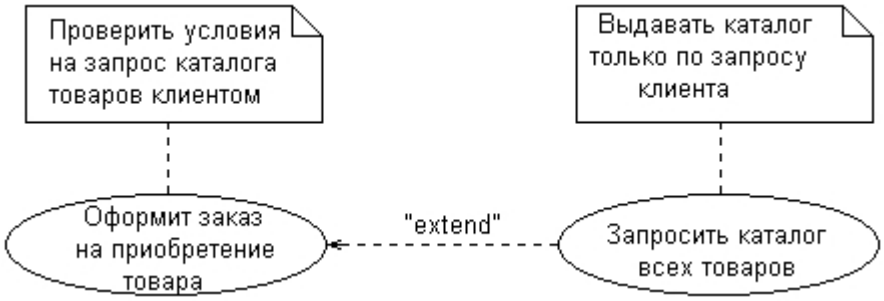


Рис. 4.8. Графическое изображение отношения расширения с примечаниями условий выполнения вариантов использования

Точка расширения может быть как отдельной точкой в последовательности действий, так и множеством отдельных точек. Важно представлять себе, что если отношение расширения имеет некоторую последовательность точек расширения, только первая из них может определять множество отдельных точек. Все остальные должны определять в точности одну такую точку. Какая из точек должна быть первой точкой расширения, т.е. определяться единственным расширением. Такие ссылки на расположение точек расширения могут быть представлены различными способами, например, с помощью текста примечания на естественном языке (рис. 4.8)

Отношение обобщения служит для указания того факта, что некоторый вариант использования А может быть обобщен до варианта использования В. В этом случае вариант А будет являться специализацией варианта В. При этом В называется предком или родителем по отношению А, а вариант А — потомком по отношению к варианту использования В. Следует подчеркнуть, что потомок наследует все свойства и поведение своего родителя, а также может быть дополнен новыми свойствами и особенностями поведения. Графически данное отношение обозначается сплошной линией со стрелкой в форме незакрашенного треугольника, которая указывает на родительский вариант

использования (рис. 4.9). Эта линия со стрелкой имеет специальное название — стрелка "обобщение" [8].

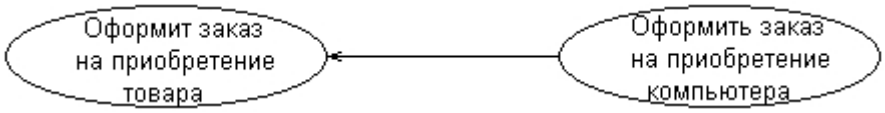


Рис. 4.9. Пример графического изображения отношения обобщения между вариантами использования

Отношение обобщения между вариантами использования применяется в том случае, когда необходимо отметить, что дочерние варианты использования обладают всеми атрибутами и особенностями поведения родительских вариантов. При этом дочерние варианты использования участвуют во всех отношениях родительских вариантов. В свою очередь, дочерние варианты могут наделяться новыми свойствами поведения, которые отсутствуют у родительских вариантов использования, а также уточнять или модифицировать наследуемые от них свойства поведения.

Применительно к данному отношению, один вариант использования может иметь несколько родительских вариантов. В этом случае реализуется множественное наследование свойств и поведения отношения предков: С другой стороны, один вариант использования может быть предком для нескольких дочерних вариантов, что соответствует таксономическому характеру отношения обобщения.

Между отдельными актерами также может существовать отношение обобщения. Данное отношение является направленным и указывает на факт специализации одних актеров относительно других. Например, отношение обобщения от актера А к актеру В отмечает тот факт, что каждый экземпляр актера А является одновременно экземпляром актера В и обладает всеми его свойствами. В этом случае актер В является родителем по отношению к актеру А, а актер А, соответственно, потомком актера В. При этом актер А обладает способностью играть такое же множество ролей, что и актер В. Графически данное отношение также обозначается стрелкой обобщения, т. е. сплошной линией со стрелкой в форме незакрашенного треугольника, которая указывает на родительского актера (рис. 4.10).

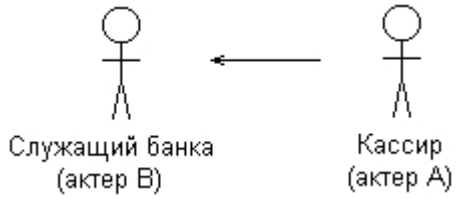


Рис. 4.10. Пример графического изображения отношения обобщения между актерами

Отношение включения (include) в языке UML — это разновидность отношения зависимости между базовым вариантом использования и его специальным случаем. При

этом отношением зависимости (dependency) является такое отношение между двумя элементами модели, при котором изменение одного элемента (независимого) приводит к изменению другого элемента (зависимого). Отношение включения устанавливается только между двумя вариантами использования и указывает на то, что заданное поведение для одного варианта использования включается в качестве составного фрагмента в последовательность поведения другого варианта использования. Данное отношение является направленным бинарным отношением в том смысле, что пара экземпляров вариантов использования всегда упорядочена в отношении включения [8].

Так, например, отношение включения, направленное от варианта использования "**Предоставление кредита в банке**" к варианту использования "**Проверка платежеспособности клиента**", указывает на то, что каждый экземпляр первого варианта использования всегда включает в себя функциональное поведение или выполнение второго варианта использования. В этом смысле поведение второго варианта использования является частью поведения первого варианта использования на данной диаграмме. Графически данное отношение обозначается как отношение зависимости в форме пунктирной линии со стрелкой, направленной от базового варианта использования к включаемому варианту использования. При этом данная линия помечается стереотипом <<include>>, как показано на рис. 4.11 [8].

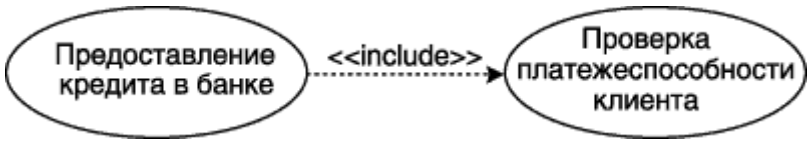


Рис. 4.11. Пример графического изображения отношения включения между вариантами использования

Семантика этого отношения определяется следующим образом. Процесс выполнения базового варианта использования включает в себя как собственное подмножество последовательность действий, которая определена для включаемого варианта использования. При этом выполнение включаемой последовательности действий происходит всегда при инициировании базового варианта использования [8].

Один вариант использования может входить в несколько других вариантов, а также содержать в себе другие варианты. Включаемый вариант использования является независимым от базового варианта в том смысле, что он предоставляет последнему инкапсулированное поведение, детали реализации которого скрыты от последнего и могут быть легко перераспределены между несколькими включаемыми вариантами использования. Более того, базовый вариант зависит только от результатов выполнения

включаемого в него варианта использования, но не от структуры включаемых в него вариантов.

ПРАКТИЧЕСКАЯ ЧАСТЬ

ЧАСТЬ I

1) Запустить программу Software Ideas Modeler;

2) Создайте новый проект, выбрав тип диаграммы «Диаграмма вариантов использования»;

3) Для иллюстрации особенностей спецификации функциональных требований на диаграмме вариантов использования рассмотрим модель обычного банкомата. Процесс функционирования этой системы хорошо знаком владельцам кредитных карточек, поэтому не требует дополнительного описания. Особенность отечественных банкоматов состоит в том, что в них отсутствует возможность перевода средств с одного счета на другой. Рассматриваемая система имеет двух актеров, один из которых является клиентом банкомата, а другой - Банкомат, который осуществляет выполнение соответствующих транзакций. Каждый из этих актеров взаимодействует с банкоматом, хотя главный актер Клиент, поскольку именно он инициирует функциональность банкомата [8].

Основные функциональные требования к банкомату заключаются в предоставлении клиенту возможности снятия наличных по кредитной карточке и получении справки о состоянии счета. Именно эти функциональные требования специфицируются отдельными вариантами использования, которые служат ключевыми элементами соответствующей концептуальной модели. Поскольку для выполнения этих вариантов использования необходимо аутентифицировать кредитную карточку, они оба обращаются к дополнительному сервису "Проверка ПИН-кода кредитной карточки". Как следует из существа выдвигаемых к банкомату функциональных требований, этот сервис может выступать в качестве отдельного варианта использования разрабатываемой диаграммы и соединяться с первыми двумя вариантами отношением включения. Соответствующая диаграмма вариантов использования может включать в себя только указанных двух актеров и три варианта использования (рис. 4.12).

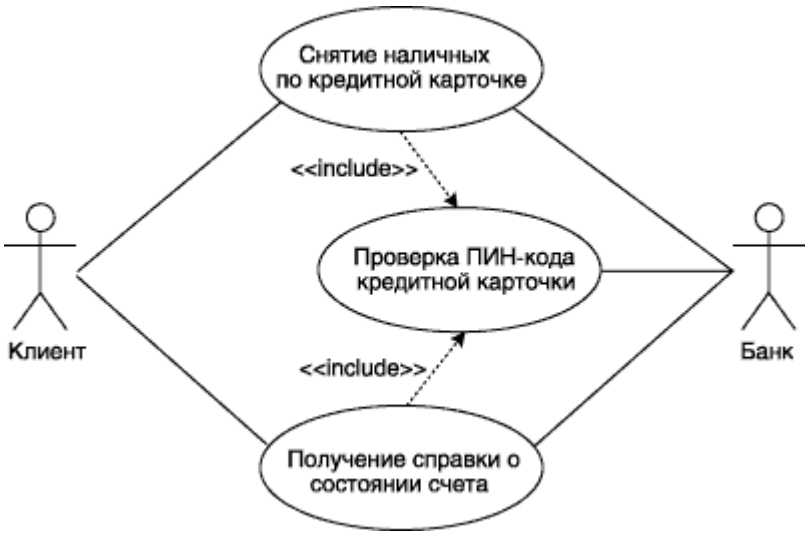


Рис. 4.12. Диаграмма вариантов использования для модели банкомата

Задание № 1. Используя средства программы Software Ideas Modeler построить диаграмму вариантов использования, показанную на рис. 4.12.

На следующем этапе разработки модели вариантов использования для рассматриваемой системы банкомата следует дополнить данную диаграмму текстовым сценарием. Этот сценарий будет дополнять диаграмму, раскрывая содержание и логическую последовательность отдельных действий, которые выполняются системой и актерами в процессе снятия наличных по кредитной карточке. В этом случае сценарий удобно представить в виде трех таблиц, каждая из которых описывает отдельный раздел шаблона.

В главном разделе сценария (табл. 4.1.) указывается имя рассматриваемого варианта использования, имена взаимосвязанных с ним актеров, цель выполнения варианта, условный тип и ссылки на другие варианты использования.

Таблица 4.1. Главный раздел сценария выполнения варианта использования "Снятие наличных по кредитной карточке"

Вариант использования	Снятие наличных по кредитной карточке
Актеры	Клиент, Банк
Цель	Получение требуемой суммы наличными
Краткое описание	Клиент запрашивает требуемую сумму. Банкомат обеспечивает доступ к счету клиента. Банкомат выдает клиенту наличные.
Тип	Базовый
Ссылки на другие варианты использования	Включает в себя ВИ: • Проверка ПИН-кода кредитной карточки • Идентифицировать кредитную карточку

В следующем разделе сценария (табл. 4.2) описывается последовательность действий, приводящая к успешному выполнению рассматриваемого варианта использования. При

этом инициатором действий должен выступать актер Клиент. Для удобства последующих ссылок каждое действие помечается порядковым номером в последовательности.

Таблица 4.2. Раздел Типичный ход событий сценария выполнения варианта использования "Снятие наличных по кредитной карточке"

Действия актеров	Отклик системы
1. Клиент вставляет кредитную карточку в устройство чтения банкомата **Исключение №1**: Кредитная карточка недействительна	2. Банкомат проверяет кредитную карточку 3. Банкомат предлагает ввести ПИН-код
4. Клиент вводит персональный PIN-код **Исключение №2**: Клиент вводит неверный ПИН-код	5. Банкомат проверяет ПИН-код 6. Банкомат отображает опции меню
7. Клиент выбирает снятие наличных со своего счета	8. Система делает запрос в Банк и выясняет текущее состояние счета клиента 9. Банкомат предлагает ввести требуемую сумму
10. Клиент вводит требуемую сумму 11. Банк проверяет введенную сумму **Исключение №3**: Требуемая сумма превышает сумму на счете клиента	12. Банкомат изменяет состояние счета клиента, выдает наличные и чек
13. Клиент получает наличные и чек	14. Банкомат предлагает клиенту забрать кредитную карточку
15. Клиент получает свою кредитную карточку	16. Банкомат отображает сообщение о готовности к работе

В третьем разделе сценария (табл. 4.3) описывается последовательность действий, выполняемых при возникновении исключительных ситуаций или исключений.

Таблица 4.3. Раздел Исключения сценария выполнения варианта использования "Снятие наличных по кредитной карточке"

Исключение №1. Кредитная карточка недействительна или неверно вставлена	
Действия актера	**Отклик системы**
	3. Банкомат отображает информацию о неверно вставленной кредитной карточке 14. Банкомат возвращает клиенту его кредитную карточку
15. Клиент получает свою кредитную карточку	
Исключение №2. Клиент вводит неверный ПИН-код	
	6. Банкомат отображает информацию о неверном ПИН-коде
4. Клиент вводит новый ПИН-код	
Исключение №3. Требуемая сумма превышает сумму на счете клиента	

	12. Банкомат отображает информацию о превышении кредита
10. Клиент вводит новую требуемую сумму	

Можно дополнить данный сценарий, аналогичным образом описав не только варианты использования "Получение справки о состоянии счета" и "Проверка Пин-кода кредитной карточки", но и рассмотрев другие исключения, например отказ клиента от получения наличных после проверки ПИН-кода и т.п. При этом полнота сценариев и модели вариантов использования будут определяться теми функциональными требованиями, которые сформулированы в рамках конкретного проекта разработки соответствующего банкомата.

Отдельные небольшие по своему объему сценарии могут быть размещены на диаграмме в форме примечаний.

Примечание (note) предназначено для включения в модель произвольной текстовой информации, имеющей непосредственное отношение к контексту разрабатываемого проекта.

В качестве такой информации могут быть комментарии разработчика (например, дата и версия разработки диаграммы или ее отдельных компонентов), ограничения (например, на значения отдельных связей или экземпляры сущностей) и помеченные значения. Применительно к диаграммам вариантов использования примечание может иметь уточняющую информацию, относящуюся к контексту тех или иных вариантов использования.

4) Рассмотрим модель функционирования мобильного телефона. Достоинством этого проекта является то, что он не требует специального описания предметной области, поскольку предполагает интуитивное знакомство читателей с особенностями функционирования телефона

Задание № 2. Построить диаграмму вариантов использования для оператора мобильной связи.

Для этого необходимо выполнить действия:

1. Добавить актеров с именами **Сотовый оператор** и **Пользователь;**
2. Добавить вариант использования **Исходящее соединение**;
3. Добавить вариант использования **Получение информации о состоянии счета;**
4. Добавить варианты использования **Идентификация пользователя** и **Блокирование Sim-карты телефона;**

5. Добавить направленную ассоциацию от актера **Пользователь** к варианту использования **Получение информации о состоянии счета**;
6. Добавить направленную ассоциацию от актера **Пользователь** к варианту использования **Исходящее соединение**;
7. Добавить направленную ассоциацию от варианта использования **Исходящее соединение** к актеру **Сотовый оператор;**
8. Добавить направленную ассоциацию от варианта использования **Получение информации** о состоянии счета к актеру **Сотовый оператор;**
9. Добавить отношение зависимости со стереотипом «include», направленное от варианта использования **Получение информации о состоянии счета** к варианту использования **Идентификация пользователя**;
10. Добавить отношение зависимости со стереотипом «include», направленное от варианта использования **Исходящее соединение** к варианту использования **Идентификация пользователя**;
11. Добавить отношение зависимости со стереотипом «extend», направленное от варианта использования **Блокирование SIM-карты** к варианту использования **Идентификация пользователя;**
12. Продумать как наиболее эффективно и грамотно расположить элементы на диаграмме;
13. Описать сценарий базовых вариантов использования на основе примера из задания № 1.

5) Диаграммы вариантов использования очень эффективны при разработке архитектуры информационных систем. На рис. 4.13. показан пример диаграммы вариантов использования для построения автоматизированной информационной системы «Управление университетом».

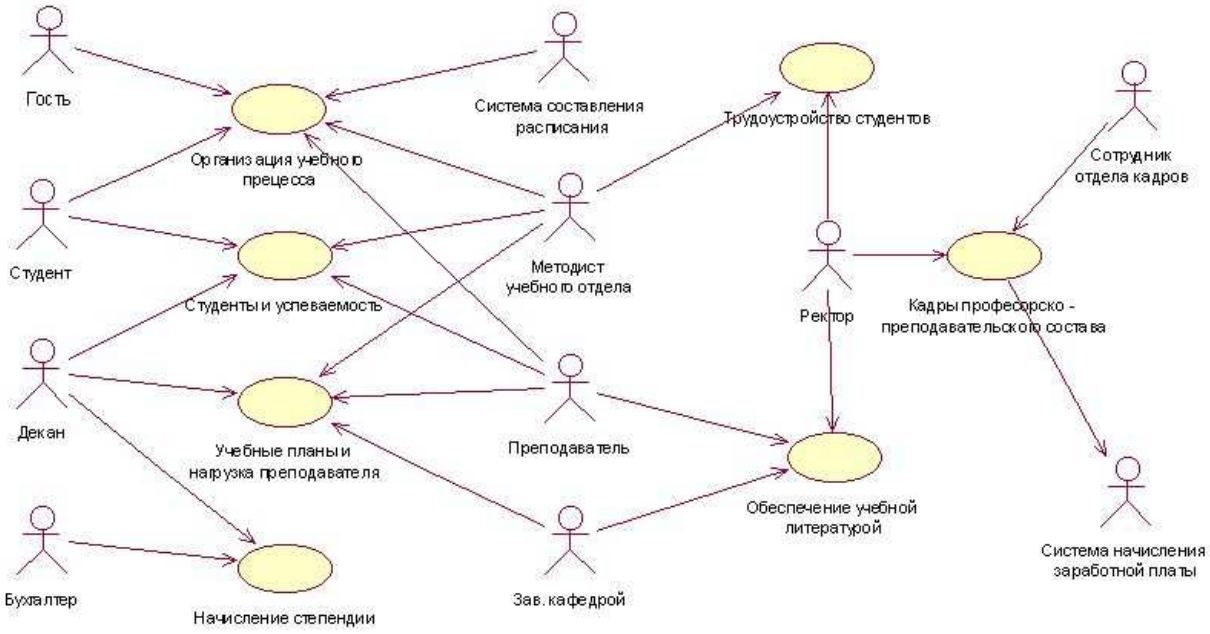


Рис. 4.13. Диаграмма вариантов использования АИС «Управление университетом»

Задание № 3. Построить диаграмму, показанную на рис. 4.13.

Задание № 4. Разработать собственную диаграмму вариантов использования на основе примеров из жизни.

ЧАСТЬ II

Студентам предварительно было выдано задание для самостоятельной работы: подготовка карты процессов и презентации данной карты. Презентация оформляется в формате ppt в соответствии с идеями студента. Каждый из студентов представляет свою карту процессов, рассказывает о сложностях, с которыми он столкнулся при ее разработке. Остальные студенты из группы задают ему вопросы и делятся впечатлениями о его презентации.

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Какие виды отношений могут существовать между актерами и вариантами использования?
2) Каких актеров называют главными, а каких второстепенными?
3) В чем состоит суть диаграммы вариантов использования?
4) Объяснить графическую нотацию и смысл актера на диаграмме вариантов использования;
5) Объяснить графическую нотацию и смысл элемента «Вариант использования» на диаграмме вариантов использования;
6) В каком случае на диаграмме вариантов использования применяется отношение включения?

7) В каком случае на диаграмме вариантов использования применяется отношение обобщения?
8) В каком случае на диаграмме вариантов использования применяется отношение ассоциации?
9) В каком случае на диаграмме вариантов использования применяется отношение расширения?
10) Для чего служит элемент «интерфейс» на диаграмме вариантов использования и как он изображается графически?

ЛАБОРАТОРНАЯ РАБОТА № 5

Построение диаграммы последовательностей в нотации UML

Цель работы: получить навык разработки диаграмм последовательности с помощью нотации унифицированного языка моделирования UML.

Оборудование: компьютеры с операционной системой Windows XP и выше, наличие любой программы поддерживающей нотацию UML (в данной лабораторной работе используется бесплатно распространяемая программа Softaware Ideas Modeler).

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Диаграмма последовательности (sequence diagram) - диаграмма, на которой показаны взаимодействия объектов, упорядоченные по времени их проявления [11].

Особенности взаимодействия элементов моделируемой системы могут быть представлены на диаграммах кооперации и последовательности. Диаграммы кооперации используются для спецификации динамики поведения систем, хотя время в явном виде в них отсутствует. Однако временной аспект поведения может иметь существенное значение при моделировании синхронных процессов, описывающих взаимодействие объектов. Именно для этой цели в языке UML используются диаграммы последовательности [11].

На диаграмме последовательности неявно присутствует ось времени, что позволяет визуализировать временные отношения между передаваемыми сообщениями. С помощью диаграммы последовательности можно представить взаимодействие элементов модели как своеобразный временной график "жизни" всей совокупности объектов, связанных между собой для реализации варианта использования программной системы, достижения бизнес-цели или выполнения какой-либо задачи [11].

Изображение объектов на диаграмме последовательности

На диаграмме последовательности, как и на диаграммах рассмотренных ранее, также изображаются объекты, которые непосредственно участвуют во взаимодействии, при этом

никакие статические связи с другими объектами не визуализируются. Для диаграммы последовательности ключевым моментом является именно динамика взаимодействия объектов во времени. При этом диаграмма последовательности имеет как бы ***два измерения***. Одно - слева направо в виде вертикальных линий, каждая из которых изображает линию жизни отдельного объекта, участвующего во взаимодействии. Второе измерение диаграммы последовательности - вертикальная временная ось, направленная сверху вниз [11].

Каждый объект графически изображается в форме прямоугольника и располагается в верхней части своей линии жизни (рис. 5.1). Внутри прямоугольника записываются собственное имя объекта со строчной буквы и имя класса, разделенные двоеточием. При этом вся запись подчеркивается, что является признаком объекта, который, как указывалось ранее, представляет собой экземпляр класса [11].

Если на диаграмме последовательности отсутствует собственное имя объекта, то при этом должно быть указано имя класса. Такой объект считается ***анонимным***. Может отсутствовать и имя класса, но при этом должно быть указано собственное имя объекта. Такой объект считается ***сиротой***. Роль классов в именах объектов на диаграммах последовательности, как правило, не указывается [11].

Крайним слева на диаграмме изображается объект - инициатор моделируемого процесса взаимодействия (объект a на рис. 5.1). Правее - другой объект, который непосредственно взаимодействует с первым. Таким образом, порядок расположения объектов на диаграмме последовательности определяется исключительно соображениями удобства визуализации их взаимодействия друг с другом [11].

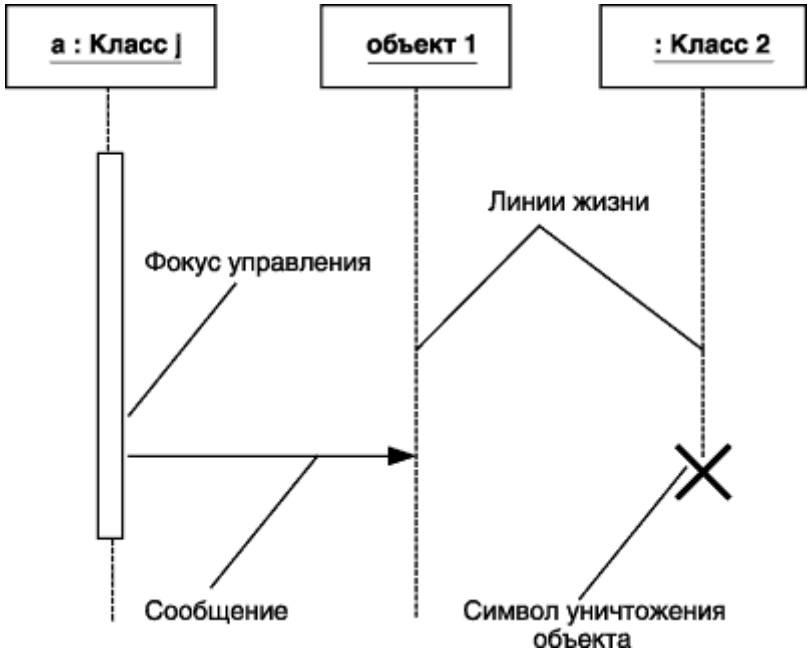


Рис. 5.1. Графические элементы диаграммы последовательности

Начальному моменту времени соответствует самая ***верхняя часть диаграммы***. При этом процесс взаимодействия объектов реализуется посредством сообщений, которые посылаются одними объектами другим. Сообщения изображаются в виде горизонтальных стрелок с именем сообщения и образуют определенный порядок относительно времени своей инициализации. Другими словами, сообщения, расположенные на диаграмме последовательности выше, передаются раньше тех, которые расположены ниже. При этом масштаб на оси времени не указывается, поскольку диаграмма последовательности моделирует лишь временную упорядоченность взаимодействий типа "раньше-позже" [11].

Линия жизни объекта (object lifeline) - вертикальная линия на диаграмме последовательности, которая представляет существование объекта в течение определенного периода времени [11].

Линия жизни объекта изображается пунктирной вертикальной линией, ассоциированной с единственным объектом на диаграмме последовательности. Линия жизни служит для обозначения периода времени, в течение которого объект существует в системе и, следовательно, может потенциально участвовать во всех ее взаимодействиях. Если объект существует в системе постоянно, то и его линия жизни должна продолжаться по всей рабочей области диаграммы последовательности от самой верхней ее части до самой нижней (объект 1 и анонимный объект Класса 2 на рис. 5.1) [11].

Отдельные объекты, закончив выполнение своих операций, могут быть уничтожены, чтобы освободить занимаемые ими ресурсы. Для таких объектов линия жизни обрывается в момент его уничтожения. Для обозначения момента уничтожения объекта в языке UML применяется специальный символ в форме латинской буквы "X". На рис. 5.2 этот символ используется для уничтожения анонимного объекта, образованного от Класса 3. Ниже этого символа пунктирная линия не изображается, поскольку соответствующего объекта в системе уже нет, и этот объект должен быть исключен из всех последующих взаимодействий [11].

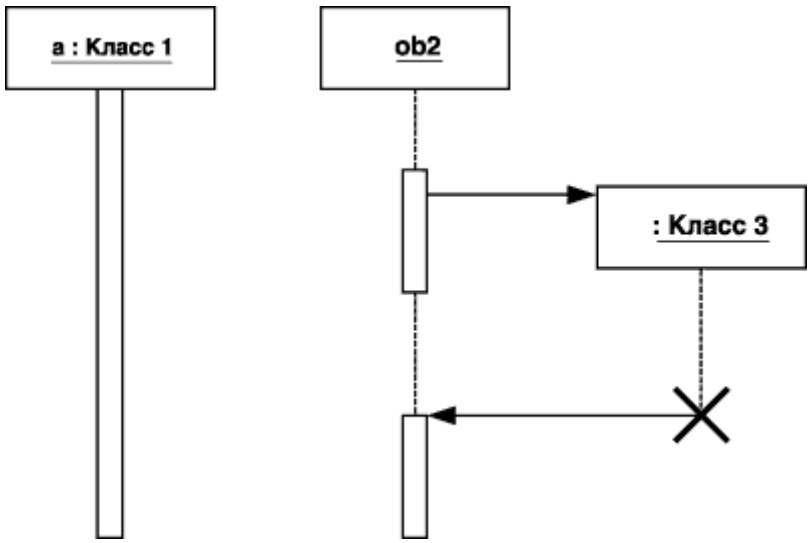


Рис. 5.2. Графическое изображение линий жизни и фокусов управления объектов

Не обязательно создавать все объекты в начальный момент времени. Отдельные объекты в системе могут создаваться по мере необходимости, существенно экономя ресурсы системы и повышая ее производительность. В этом случае прямоугольник такого объекта изображается не в верхней части диаграммы последовательности, а в той, которая соответствует моменту создания объекта (анонимный объект, образованный от Класса 3 на рис. 5.2). При этом прямоугольник объекта вертикально располагается в том месте диаграммы, которое по оси времени совпадает с моментом его возникновения в системе. Объект создается со своей линией жизни а, возможно, и с фокусом управления [11].

В процессе функционирования объектно-ориентированных систем одни объекты могут находиться в активном состоянии, непосредственно выполняя определенные действия, или в состоянии пассивного ожидания сообщений от других объектов. Фокус управления - символ, применяемый для того, чтобы явно выделить подобную активность объектов на диаграммах последовательности [11].

Фокус управления (focus of control) - специальный символ на диаграмме последовательности, указывающий период времени, в течение которого объект выполняет некоторое действие, находясь в активном состоянии [11].

Фокус управления изображается в форме вытянутого узкого прямоугольника (объект а на рис. 5.1), верхняя сторона которого обозначает начало получения фокуса управления объекта (начало активности), а ее нижняя сторона - окончание фокуса управления (окончание активности). Этот прямоугольник располагается ниже обозначения соответствующего объекта и может заменять его линию жизни (объект а на рис. 5.2), если на всем ее протяжении он активен [11].

Периоды активности объекта могут чередоваться с периодами его пассивности или ожидания. В этом случае у такого объекта фокусы управления изменяют свое изображение

на линию жизни и наоборот (объект сирота ob2 на рис.5.2). Важно понимать, что получить фокус управления может только объект, у которого в этот момент имеется линия жизни. Если же объект был уничтожен, то вновь возникнуть в системе он уже не может. Вместо него может быть создан лишь экземпляр этого же класса, который, строго говоря, будет другим объектом [11].

В отдельных случаях инициатором взаимодействия в системе может быть актер или внешний пользователь. При этом актер изображается на диаграмме последовательности самым первым объектом слева со своим фокусом управления (рис. 5.3). Наиболее часто актер и его фокус управления будут существовать в системе постоянно, отмечая характерную для пользователя активность в инициировании взаимодействий с системой. Актер может иметь собственное имя либо оставаться анонимным [11].

В отдельных случаях объект может посылать сообщения самому себе, инициируя так называемые **рефлексивные** сообщения. Для этой цели служит специальное изображение (сообщение у объекта a на рис. 5.3). Такие сообщения изображаются в форме сообщения, начало и конец которого соприкасаются с линией жизни или фокусом управления одного и того же объекта. Подобные ситуации возникают, например, при обработке нажатий на клавиши клавиатуры при вводе текста в редактируемый документ, при наборе цифр номера телефона абонента [11].

Если в результате рефлексивного сообщения создается новый подпроцесс или нить управления, то говорят о рекурсивном или вложенном фокусе управления. На диаграмме последовательности рекурсия обозначается небольшим прямоугольником, присоединенным к правой стороне фокуса управления того объекта, для которого изображается данное рекурсивное взаимодействие (анонимный объект Класса 2 на рис. 5.3) [11].

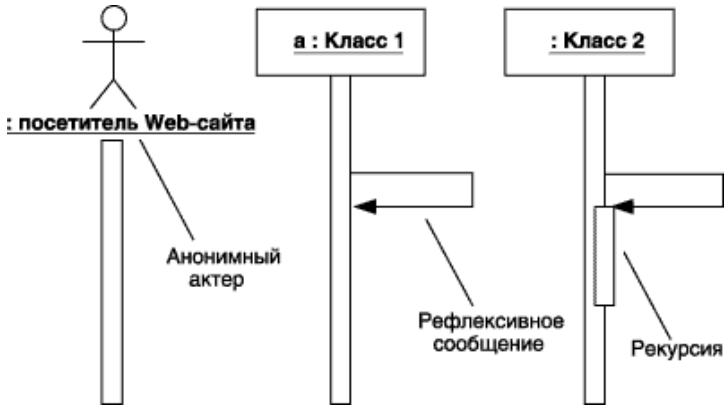


Рис. 5.3. Графическое изображение актера, рефлексивного сообщения и рекурсии на диаграмме последовательности

Сообщения на диаграмме последовательности

Как правило, сообщения в UML изображаются в виде стрелок с указателем. Стрелки сообщений изображаются аналогично рассмотренным ранее диаграммам, но применительно к диаграммам последовательности сообщения имеют дополнительные семантические особенности. При этом на диаграмме последовательности все сообщения упорядочены по времени своей передачи в моделируемой системе, хотя номера у них могут не указываться [11].

На диаграммах последовательности могут присутствовать три разновидности сообщений, каждое из которых имеет свое графическое изображение (рис. 5.4).

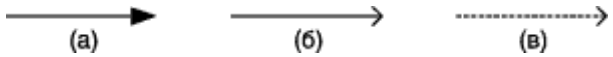


Рис. 5.4. Графическое изображение различных видов сообщений между объектами на диаграмме последовательности

Первая разновидность сообщения (рис. 5.4, а) наиболее распространена и используется для вызова процедур, выполнения операций или обозначения отдельных вложенных потоков управления. Начало этой стрелки, как правило, соприкасается с фокусом управления того объекта-клиента, который инициирует это сообщение. Конец стрелки соприкасается с линией жизни того объекта, который принимает это сообщение и выполняет в ответ определенные действия. При этом принимающий объект может получить фокус управления, становясь в этом случае активным. Передающий объект может потерять фокус управления или остаться активным [11].

Вторая разновидность сообщения (рис. 5.4, б) используется для обозначения простого асинхронного сообщения, которое передается в произвольный момент времени. Передача такого сообщения обычно не сопровождается получением фокуса управления объектом-получателем [11].

Третья разновидность сообщения (рис. 5.4, в) используется для возврата из вызова процедуры. Примером может служить простое сообщение о завершении вычислений без предоставления результата расчетов объекту-клиенту. В процедурных потоках управления эта стрелка может быть опущена, поскольку ее наличие неявно предполагается в конце активизации объекта. В то же время считается, что каждый вызов процедуры имеет свою пару - возврат вызова. Для непроцедурных потоков управления, включая параллельные и асинхронные сообщения, стрелка возврата должна указываться явным образом [11].

Обычно сообщения изображаются горизонтальными стрелками, соединяющими линии жизни или фокусы управления двух объектов на диаграмме последовательности. При этом неявно предполагается, что время передачи сообщения достаточно мало по сравнению с процессами выполнения действий объектами. Считается также, что за время передачи сообщения с соответствующими объектами не может произойти никаких

событий. Другими словами, состояния объектов не изменяются. Если же это предположение не может быть признано справедливым, то стрелка сообщения изображается под наклоном, так чтобы конец стрелки располагался ниже ее начала [11].

Каждое сообщение на диаграмме последовательности ассоциируется с определенной операцией, которая должна быть выполнена принявшим его объектом. При этом операция может иметь аргументы или параметры, значения которых влияют на получение различных результатов. Соответствующие параметры операции будет иметь и вызывающее это действие сообщение. Более того, значения параметров отдельных сообщений могут содержать условные выражения, образуя ветвление или альтернативные пути основного потока управления.

Ветвление потока управления

Одна из главных особенностей диаграммы последовательности - возможность визуализировать простое ветвление процесса. Для изображения ветвления используются две или более стрелки, выходящие из одной точки фокуса управления объекта (объект ob1 на рис. 5.5). При этом рядом с каждой из них должно быть явно указано соответствующее условие ветви в форме булевского выражения [11].

Количество ветвей может быть произвольным, однако наличие ветвлений может существенно усложнить интерпретацию диаграммы последовательности. Предложение-условие должно быть явно указано для каждой ветви и записывается в форме обычного текста, псевдокода или выражения языка программирования. Это выражение всегда должно возвращать некоторое булевское выражение. Запись этих условий должна исключать одновременную передачу альтернативных сообщений по двум и более ветвям. В противном случае на диаграмме последовательности может возникнуть конфликт ветвления [11].

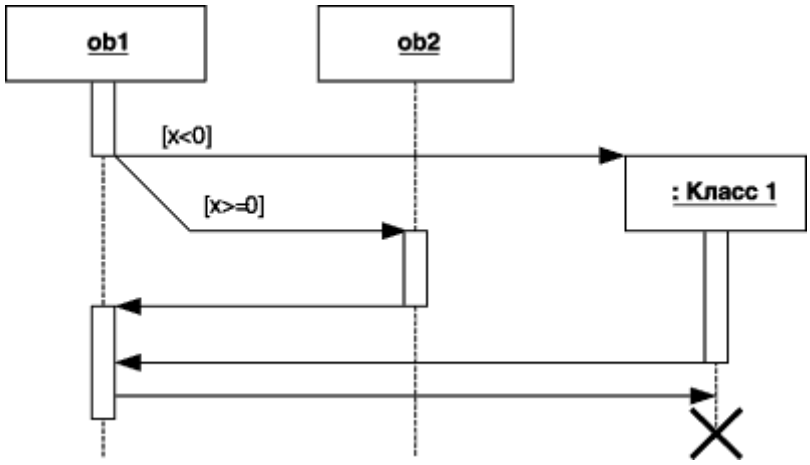


Рис. 8.5. Графическое изображение бинарного ветвления потока управления на диаграмме последовательности

С помощью ветвления можно изобразить и более сложную логику взаимодействия объектов между собой (объект ob1 на рис. 5.6). Если условий более двух, то для каждого из них необходимо предусмотреть ситуацию единственного выполнения. Описанный ниже пример относится к моделированию взаимодействия программной системы обслуживания клиентов в банке. В этом примере диаграммы последовательности объект ob1 вызывает выполнение действий у одного из трех других объектов [11].

Условием ветвления может служить сумма снимаемых клиентом средств со своего текущего счета. Если эта сумма превышает 1500$, то могут потребоваться дополнительные действия, связанные с созданием и последующим разрушением объекта Класса 1. Если же сумма превышает 100$, но не превышает 1500$, то вызывается операция или процедура объекта ob3. И, наконец, если сумма не превышает 100$, то вызывается операция или процедура объекта ob2. При этом объекты ob1, ob2 и ob3 постоянно существуют в системе. Последний объект создается от Класса 1 только в том случае, если справедливо первое из альтернативных условий. В противном случае он может быть никогда не создан [11].

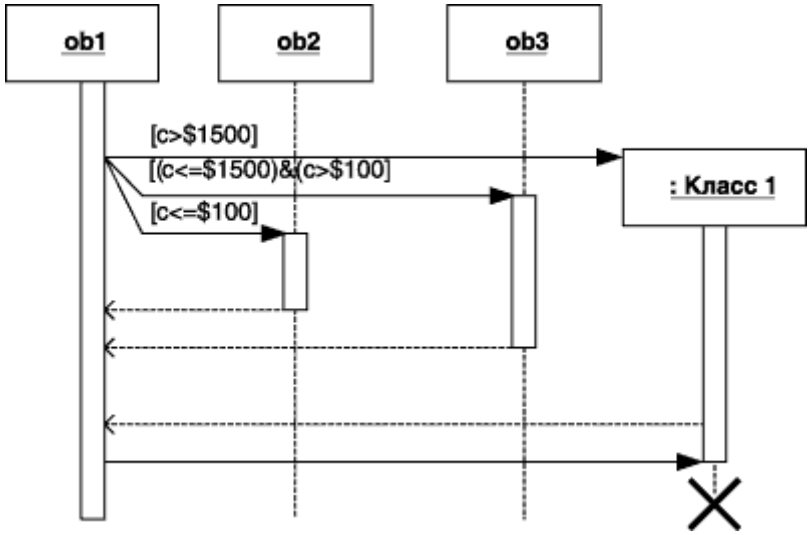


Рис. 5.6. Графическое изображение тернарного ветвления потока управления на диаграмме последовательности

Объект ob1 имеет постоянный фокус управления, а все остальные объекты - получают фокус управления только для выполнения ими соответствующих операций.

Рекомендации по построению диаграмм последовательности

Построение диаграммы последовательности целесообразно начинать с выделения из всей совокупности классов только тех, объекты которых участвуют в моделируемом взаимодействии. После этого все объекты наносятся на диаграмму, с соблюдением порядка инициализации сообщений. Здесь необходимо установить, какие объекты будут существовать постоянно, а какие временно - только на период выполнения ими требуемых действий [11].

Когда объекты визуализированы, можно приступать к спецификации сообщений. При этом необходимо учитывать те операции, которые имеют классы соответствующих объектов в модели системы. При необходимости уточнения этих операций следует использовать их стереотипы. Для уничтожения объектов, которые создаются на время выполнения своих действий, нужно предусмотреть явное сообщение. Наиболее простые случаи ветвления процесса взаимодействия можно изобразить на одной диаграмме с использованием соответствующих графических примитивов. В более сложных случаях для моделирования каждой ветви управления может потребоваться отдельная диаграмма последовательности. Следует помнить, что каждый альтернативный поток управления затрудняет понимание построенной модели [11].

Общим правилом является визуализация особенностей реализации каждого варианта использования на отдельной диаграмме последовательности. В этой ситуации отдельные диаграммы должны рассматриваться совместно как одна модель взаимодействия. Необходимость синхронизации сложных потоков управления, как правило, требуют введение в модель дополнительных ограничений [11].

ПРАКТИЧЕСКАЯ ЧАСТЬ

Диаграммы последовательности могут быть использованы для моделирования последовательности действий совершенно обыденной жизни. Например, покупка книг у поставщика библиотекой, показанная на рис. 5.7.

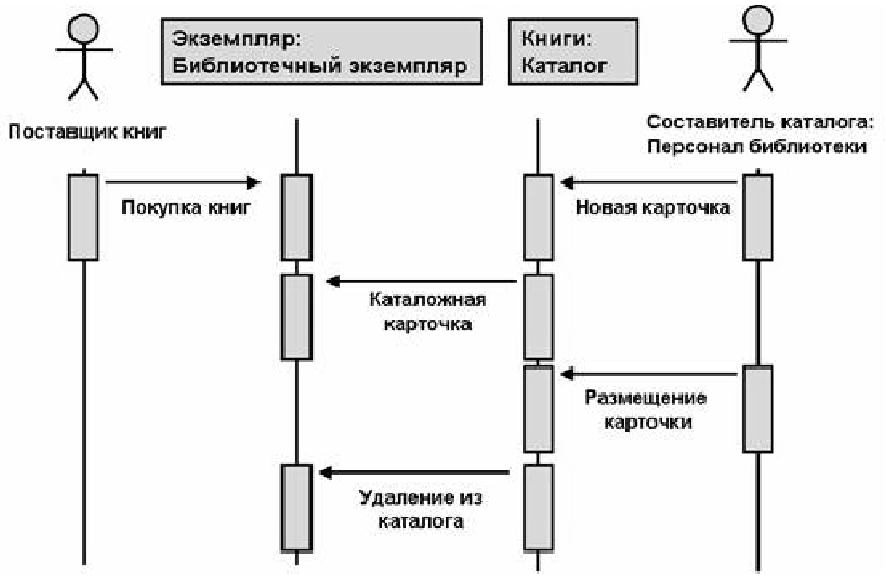


Рис. 5.7. Последовательность действий по покупке книг библиотекой

В узкоспециализированных сферах деятельности диаграммы последовательностей также находят применение. Особо часто, диаграммы, построенные в нотации UML используют для описания свойств программного обеспечения. Так на рис. 5.8. показано

применение диаграммы последовательностей для обзора метода разработки Web-приложений Ajax[1].

На рис. 5.9. приводится пример диаграммы последовательностей. На которой изображен порядок действий по прохождению годового интервью (ГИ) сотрудниками фирмы. Инициатором этого процесса является генеральный директор, который согласует дату интервью с департаментом по работе с персоналом (ДРП). ДРП согласует график с руководителями департаментов и утверждает его. Далее составляются анкеты, на вопросы которой должны ответить сотрудники предприятия. После ответов сотрудников их анкеты обрабатываются и получается сводный итоговый отчет, который поступает генеральному директору. На основе этого отчета будут предприняты уже дальнейшие действия по работе предприятия, которые можно будет отразить на другой диаграмме.

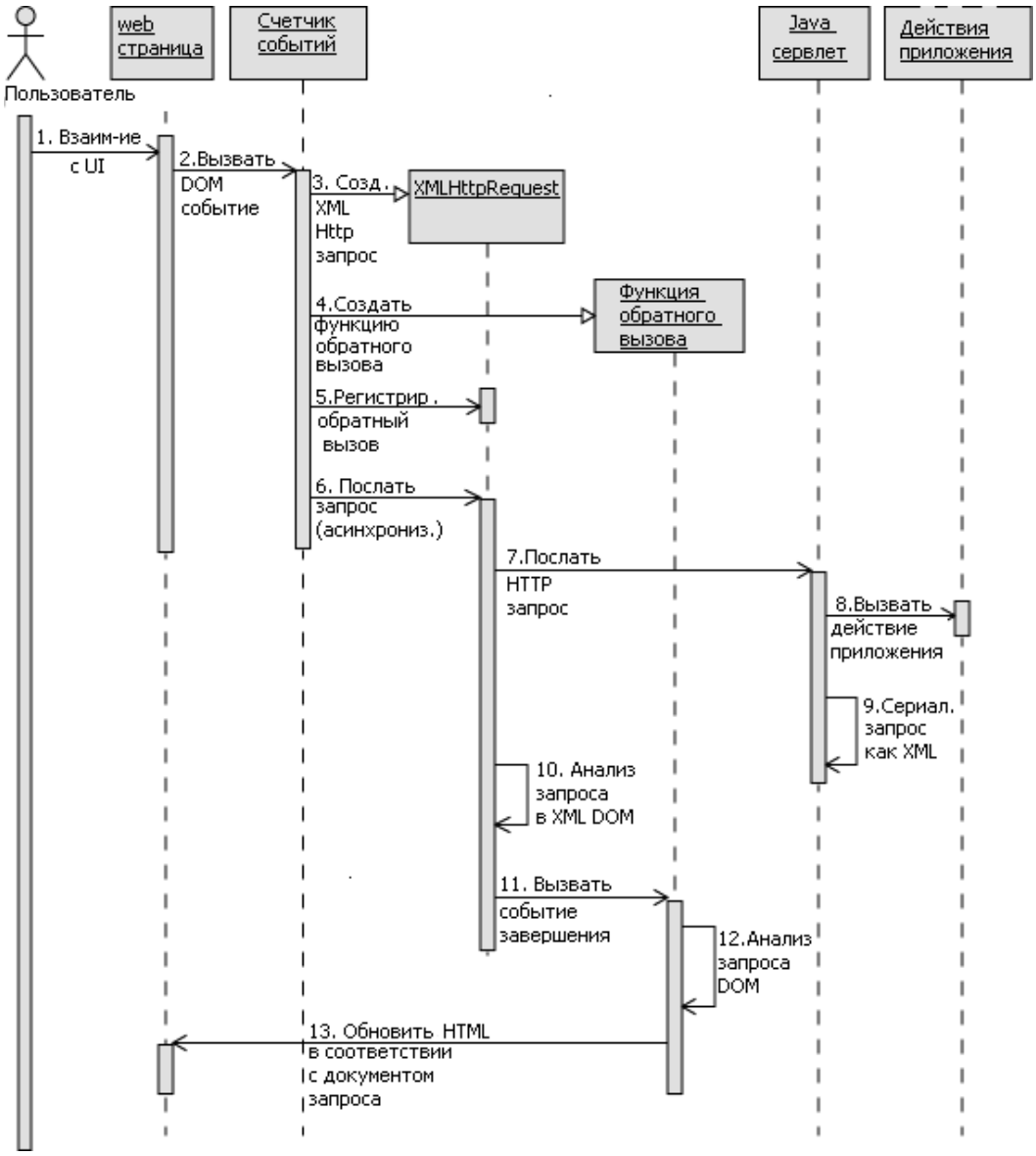


Рис. 5.8. Обзор Ajax при помощи диаграммы последовательностей

[1] Ajax для Java разработчиков: Часть 1: строим динамическое приложение на языке Java. [Электронный ресурс]. Режим доступа: http://www.ibm.com/developerworks/ru/library/j-ajax1/ (Дата обращения 19.01.2013 г.)

Задание.

1) При помощи программы постройте диаграммы, изображенные на рис. 5.7-5.9.;

2) К диаграммам на рис. 5.7 и 5.8. дайте текстовое описание, подобное тому, какое приводится в тексте работы для диаграммы 5.9.

3) Разработайте и постройте диаграмму последовательности по сдачи экзаменационной сессии;

4) Самостоятельно в команде придумайте диаграмму последовательности по своему выбору и защитите ее перед остальной группой.

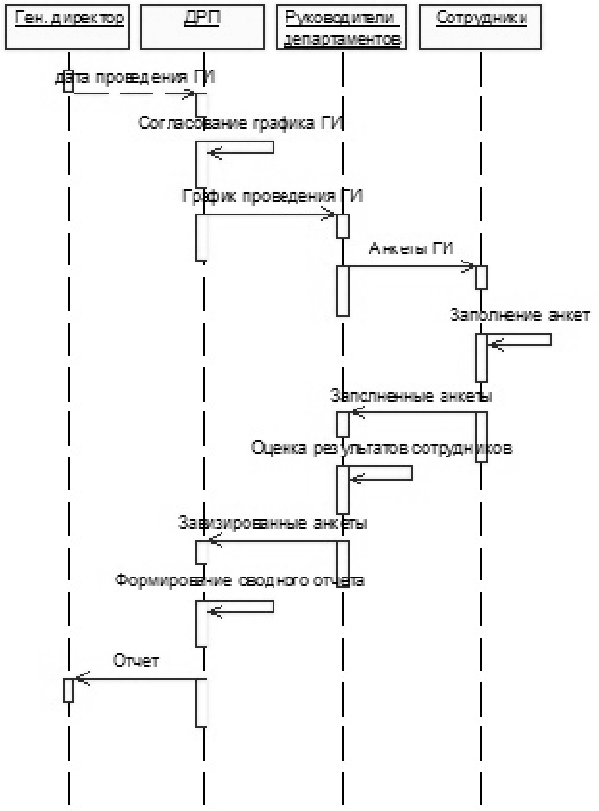


Рис. 5.9. Вид диаграммы последовательности для прохождения годового интервью сотрудниками фирмы [12]

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Сколько измерений может иметь диаграмма последовательности?
2) Как изображаются объекты на диаграммах последовательности?
3) Что называют линией жизни объекта?
4) Каков порядок передачи сообщений на диаграмме последовательностей?
5) Как изобразить на диаграмме последовательностей прекращение деятельности какого-либо объекта?

6) Какой объект на диаграмме последовательностей называют сиротой, а какой анонимом?
7) С какой целью строят диаграммы последовательностей?
8) Что называют фокусом управления?
9) Что называют рефлексивным сообщением?
10) В каком случае на диаграмме последовательностей может возникнуть конфликт ветвления?

ЛАБОРАТОРНАЯ РАБОТА № 6
Изучение интерфейса программы TIBCO BUSINESS STUDIO и нотации BPMN

Цель: изучить систему условных обозначений (нотацию) BPMN для построения модели бизнес-процесса предприятия.

Оборудование: компьютеры с операционной системой Windows XP и выше, наличие программы, поддерживающей нотацию BPMN (в данной лабораторной работе используется программа TIBCO Business Studio).

Форма проведения занятия: интерактивное занятие с использованием метода case-study (2 ч).

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

В 70-80-х годах прошлого века началось массовое снижение конкурентоспособности американских бизнес-компаний. В частности, японские компании стали успешно конкурировать с американскими прямо на внутреннем рынке США. В поисках путей повышения эффективности американского бизнеса в начале 1990-х годов в США появилась новая парадигма организации бизнеса, ориентированная на процессы. В результате, в лексикон бизнеса и IT-технологий вошли такие термины, как бизнес-процесс (business process), реинжиниринг бизнеса (business reengineering), реинжиниринг бизнес-процессов (business process reengineering), моделирование бизнес-процессов (business process modeling). Далее мы рассмотрим известный язык визуального моделирования бизнес-процессов - ***BPMN (Business Process Management Notation)*** [13].

Нотация BPMN

Процесс с точки зрения бизнеса - это отдельная деятельность (часть бизнес-процесса), выполняемая компанией или организацией. В терминологии BPMN процесс является сложным действием, которое, в свою очередь, состоит из действий, переходов между ними и т. д. Процесс можно вызывать, приостанавливать, прерывать, также он может завершаться сам, процессы могут выполняться параллельно и обмениваться сообщениями [13].

Моделирование в BPMN осуществляется посредством диаграмм с небольшим числом графических элементов. Это помогает пользователям быстро понимать логику процесса. Выделяют четыре основные категории элементов [13] :

- ✓ ***Объекты потока управления***: события, действия и логические операторы;
- ✓ ***Соединяющие объекты***: поток управления, поток сообщений и ассоциации;
- ✓ ***Роли***: пулы и дорожки;
- ✓ ***Артефакты***: данные, группы и текстовые аннотации.

Элементы этих четырёх категорий позволяют строить простейшие диаграммы бизнес процессов (ДБП). Для повышения выразительности модели спецификация разрешает создавать новые типы объектов потока управления и артефактов.

Т.о., процесс в BPMN может состоять из нескольких конструкций, описанных в таблице 6.1. [14].

Таблица 6.1. Конструкции BPMN

Сущности (flows objects):	**Связи** (connecting objects) - соединяют разные действия и данные в единый поток исполнения, могут быть следующих видов:	**Участники** (swimlanes) процесса:	**Артефакты** (artifacts) процесса
▪ действие (activity); ▪ порт (gateway); ▪ событие (event);	▪ поток исполнения (sequence flow) - переход от одного действия к другому; ▪ поток сообщений (message flow) - обмен сообщениями между разными участниками процесса; ▪ ассоциация (association) - опредяет переход между действиями в особенных ситуациях (например, при возникновении исключений); может использоваться для "прикрепления" комментариев, данных и пр.;	▪ внешние (pools); ▪ внутренние (lanes);	▪ данные (data object), группы (groups), комментарии (annotations).

Рассмотрим эти конструкции подробнее.

СУЩНОСТИ включают в себя:

а) Действия (activities) [13];

Процесс состоит из цепочки действий. Действия бывают следующих видов:

- ✓ задача - рис. 6.1, а и б;
- ✓ свернутый подпроцесс - рис. 5.2, в и г;
- ✓ развернутый подпроцесс - рис. 5.3, д.

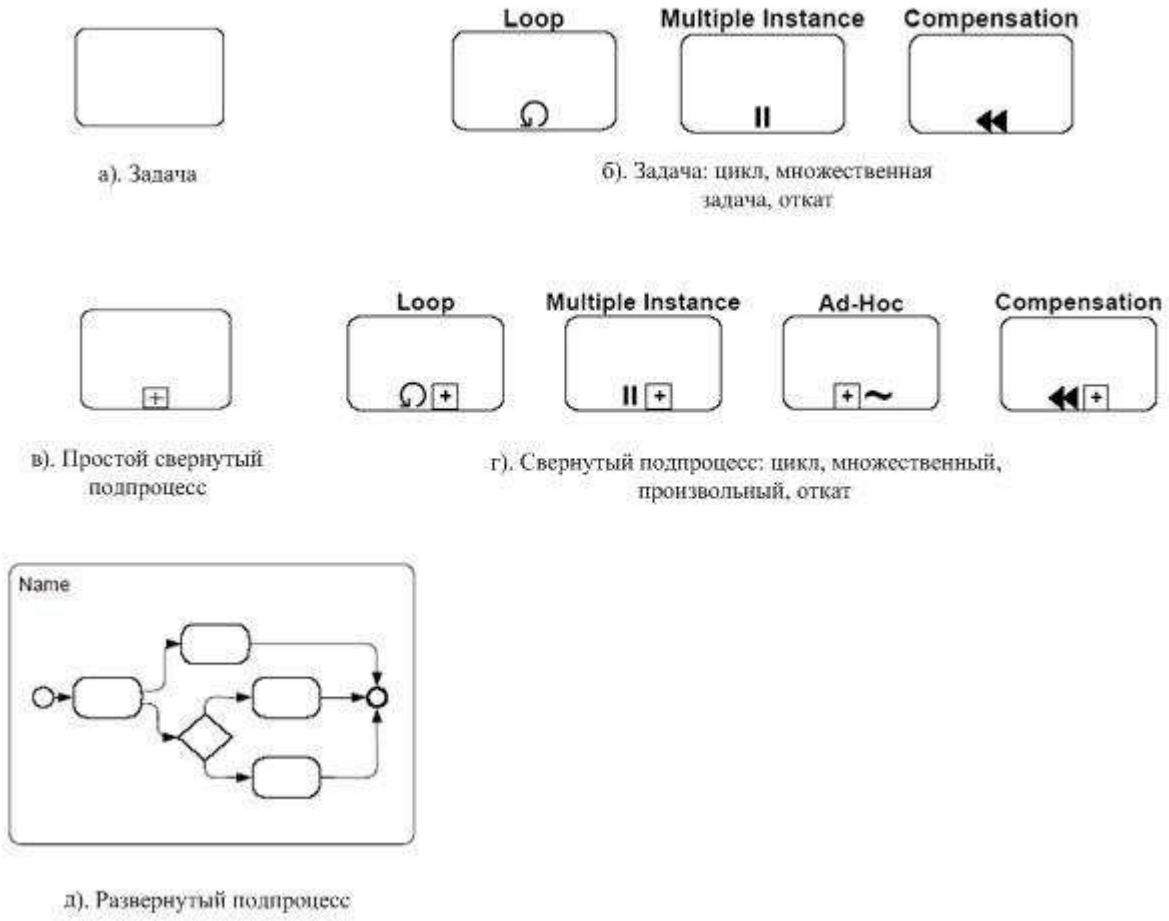


Рис. 6.1. Виды действий

Задача (task) - это атомарное действие процесса, неделимое на более элементарные части. На диаграмме задача изображается, как показано на рис. 6.1, а. На рис. 6.1, б приводится три вида задач, которые могут быть заданы в BPMN - циклическая задача, множественная задача и откат [13].

Циклическая задача (loop) - это задача, которая выполняется в цикле. В параметрах этой задачи можно указать, какой цикл имеется в виду - с пред- или постусловием, определить это условие и указать некоторые дополнительные свойства цикла [13].

Множественная задача (multiple instance) - это циклическая задача, которая выполняет в цикле целый набор однотипных задач. Текстовыми параметрами можно задать условие цикла, количество однотипных задач, а также порядок их выполнения (последовательный или параллельный) [13].

Откат (compensation) - задача, которая вызывается в случае отмены другой задачи, например, клиент отказался от забронированного отеля - тогда система должна освободить соответствующую бронь; пример приводится на рис. 6.2. [13].

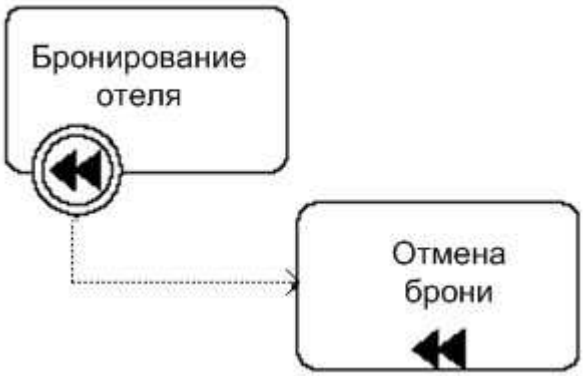


Рис. 6.2. Пример задачи с откатом

Кроме того, у задачи есть атрибут, который может иметь одно из следующих значений [13]:

- ✓ ***Service*** – задача является сторонним программным сервисом, вызываемым WE (это значение имеют по умолчанию все задачи); например, вызывается Web-сервис, вычисляющий погоду, курс валюты или еще что-нибудь;
- ✓ ***Receive*** – задача является ожиданием внешнего для данного бизнес-процесса события, часто является началом бизнес-процесса;
- ✓ ***Send*** – задача является посылкой сообщения во внешний для данного бизнес-процесса контекст;
- ✓ ***User*** – задача выполняется человеком или группой, при этом используется некоторая сторонняя IT-технология или сервис; в параметрах можно задать как исполнителей так и используемую ими ПО;
- ✓ ***Script*** – задача является скриптом, который WE выполняет полностью автоматически;
- ✓ ***Manual*** – задача, которая выполняется без помощи WE или друго IT- технологии или сервиса, например, посредством личного общения менеджера с заказчиком;
- ✓ ***Reference*** – задача является ссылкой на другую задачу;
- ✓ ***None*** – значение данного атрибута не задано.

Эти значения не имеют графического представления и могут быть отражены, например, в имени задачи. Список этих атрибутов может быть расширен.

Еще одним типом действия является **подроцесс *(subprocess)***. Он позволяет разбить сложные процессы на более мелкие. Подпроцессы бывают ***свернутые*** (collapsed subprocesses) - см. рис. 6.1, в и г - и ***развернутые*** (expanded subprocesses) - см. рис. 6.1, д. Так же как и задачи, подпроцессы могут быть циклическими, множественными и с откатом, но кроме того, могут иметь еще маркер ***произвольный*** (ad hoc) - см. рис. 6.1, г. Он

означает, что задачи и другие подпроцессы, входящие в состав данного, исполняются в произвольном порядке.

Свернутый подпроцесс является ссылкой на другую диаграмму, где он определяется в виде задач и, возможно, других подпроцессов.

Развернутый подпроцесс позволяет задать на диаграмме второй этаж (а, возможно, третий и т. д. - все зависит от того, насколько модель "глубока"). Это означает, что прямо на родительской диаграмме один или несколько процессов детализированы, как показано на рис. 6.3. [13]

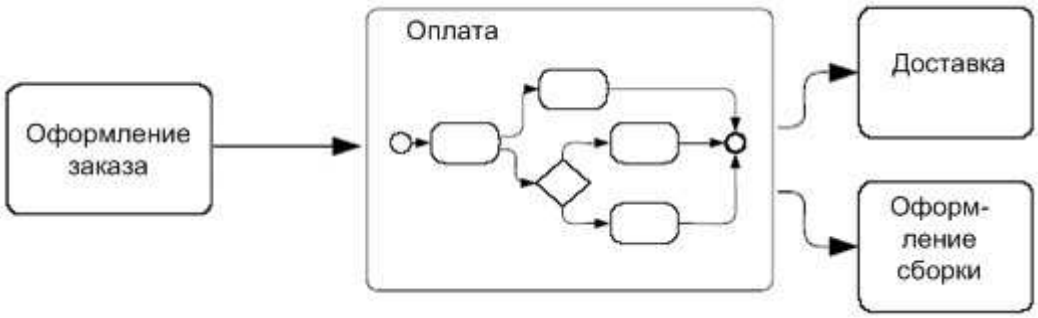


Рис. 6.3. Пример развернутого подпроцесса

б) Порты (gateways) [13]**;**

Этот вид конструкций позволяет управлять потоком выполнения процесса - ветвить его (в логическом смысле и в смысле распараллеливания) и соединять. Таким образом, почти каждый вид порта может быть использован в двух вариантах - как разветвитель и как соединитель. Общий список портов BPMN показан на рис. 6.4.

На рис. 6.4, а показан традиционный оператор логического ветвления по условию. BPMN предлагает два варианта для его изображения - обычный ромбик и ромбик с крестиком внутри. Первый вариант удобен, если никаких других типов ромбиков на диаграмме нет, второй - если на диаграмме есть иные, экзотические ромбики (см. рис. 6.4, б, в, г, д). В этом случае ромб с крестиком используется, чтобы разные ромбы можно было легко отличать друг от друга. Логический соединитель означает объединение разных логических веток. Например, пусть есть оператор switch с разными ветками, но вот он заканчивается, и какая бы ветка не выполнилась в этом операторе, далее поток управления одинаков для всех случаев.

На рис. 6.4, б показан оператор распараллеливания и соединения потоков управления. Как следует из этого рисунка, он может быть изображен с ромбиком и без.

На рис. 6.4, в показан оператор, разветвляющий поток управления по всем веткам, логические условия которых оказались, выполнены к моменту проверки. Когда этот оператор используется в качестве соединителя, он ждет все те потоки из множества

направленных к нему, которые были до этого запущены, а не вообще все потоки, определенные в спецификации как входящие в него. Ведь часть из тех потоков, которые показаны на диаграмме как входящие в него, могли быть не запущены (например, при использовании этого же оператора как разветвителя).

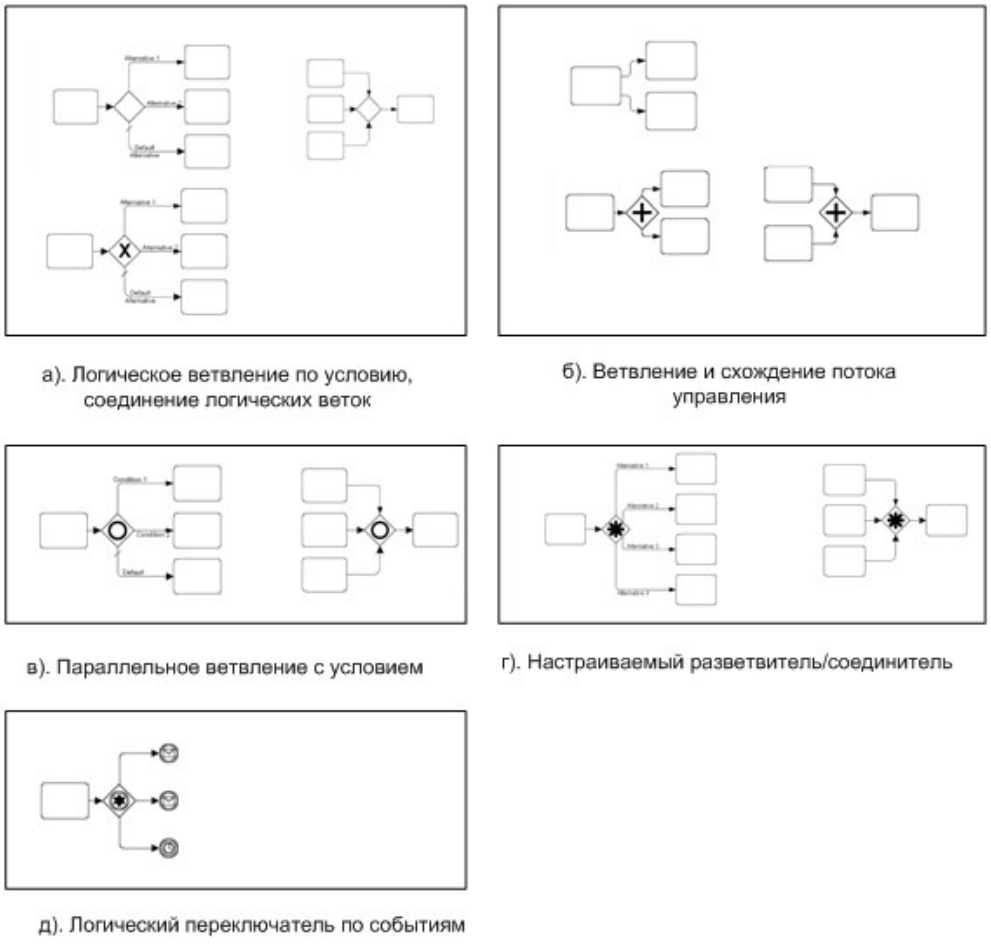


Рис. 6.4. Порты

На рис. 6.4, г показан сложный разветвитель. Он введен для того, чтобы можно было задавать более сложную семантику ветвления потоков управления, чем было определено выше (BPMN не специфицирует эту семантику). Возможно, что новое условие будет некоторой комбинацией представленных выше операторов. Таким образом, этот оператор должен обязательно сопровождаться некоторым выражением, точно определяющим его семантику. То же самое можно сказать и про использование этого оператора как соединителя - требуется задать специальное выражение, которое определит условие для множества всех потоков, заданных на спецификации как входящих в этот оператор. Например, можно определить такой порт как соединитель, соединяющий на диаграмме три параллельных потока, с условием, что он "пропускает" выполнение процесса дальше, если дождался любых двух из трех.

Наконец, на рис. 6.4 д показан разветвитель, который переключает поток управления в зависимости от получения того или иного события. Сами события обозначены в начале соответствующей ветки. В качестве соединителя этот оператор не используется.

в) Событие (event) - это некоторое происшествие, возникшее во время исполнения процесса. Событиями могут быть инициация/завершение процесса, прием/посылка сообщения, завершение какой-либо задачи или подпроцесса и т. д. Не все события одинаково интересны с точки зрения бизнес-процесса и, значит, достойны специального обозначения на диаграммах. Но многие события способны влиять на порядок выполнения процесса, активировать и прерывать те или иные его действия. Вот их-то в BPMN и предлагают специально выделять [13].

На диаграммах BPMN событие изображается, как показано на рис. 6.5, а. Внизу, сразу под символом события, указывается его имя или источник. События бывают трех типов:

- ✓ начальное (start) - событие, с которого начинается процесс или подпроцесс;
- ✓ промежуточное (intermidiate), которое случается в "середине" процесса;
- ✓ конечное (end), наступление которого означает завершение процесса или подпроцесса.

Рис. 6.5. События

Эти типы событий по-разному изображаются на BPMN-спецификациях, как показано на рис. 6.5, б. В контексте этих трех типов события могут различаться по видам - см. рис.6.5, в:

- ✓ прием/посылка сообщения (message);
- ✓ истечение определенного промежутка времени (timer);
- ✓ исключение (error) - происшествие исключительного события, например, ошибки при обработке данных;
- ✓ отмена (cancel) - отмена действия или транзакции: возврат объемлющего процесса или подпроцесса к состоянию, которое было до начала исполнения этого действия/транзакции;
- ✓ компенсация (compensation)- выполнение специальных отменяющих действий, например при отказе заказчика от услуги;
- ✓ выполнение правила (rule) - событие, которое обозначает, что в бизнес-процесе выполнилось какое-либо бизнес-правило, например, ставка акций компании поднялась выше определенной суммы, и в результате этого нужно сделать что-то особое, определенное (например, собрать совет акционеров компании);
- ✓ связь (link) - способ переключаться между двумя процессами (как правило, подпроцессами одного общего) или как оператор goto в рамках одного процессора; в первом случае первый подпроцесс должен иметь конечное событие такого типа с пометкой, в какой подпроцесс "прыгать" дальше; а тот, второй подпроцесс, должен либо стартовать с события, также помеченного как link, либо ожидать такое же промежуточное событие; и в том и в другом случае целевые события link должны иметь идентификатор, связывающий их с тем, исходным событием link;
- ✓ множественный триггер (multiple) - "ловит" (в качестве начального или промежуточного события) одно событие из списка событий, связанных с ним; в качестве заключительного события порождает весь список связанных с ним событий.
- ✓ конец (terminate) - имеет только тип "конец", обозначает, что все действия процесса и экземпляры (если их запущено более одного) завершаются.

События могут "цепляться" к границе действия, а могут быть узлами, которые соединяются связями потока управления. Далее они могут обозначать ожидание события, а могут быть его источником (например, событие посылки сообщения). Существуют многочисленные правила, которые определяют детали того, где и при каких условиях может размещаться то или иное событие.

г) СВЯЗИ (connecting objects) [13]**;**

На рис. 6.6. показаны связи разного вида, существующие в BPMN:

- ✓ ***поток исполнения*** (sequence flow) - рис. 6.6 а; это самый распространенный вид связи, с его помощью обозначается порядок выполнения действий процесса;
- ✓ ***поток сообщений*** (message flow) - рис. 6.6 б; с помощью этой связи определяются сообщения, которыми обмениваются действия; многие сущности бизнес-процесса могут обмениваться сообщениями - конструкции pools друг с другом, задачи, подпроцессы и т. д.; сообщения являются способом общения между собой параллельно работающих сущностей, поэтому сущности могут обмениваться сообщениями, лишь находясь в разных pools ;
- ✓ ***ассоциации*** (association) - это способ отобразить различные вспомогательные связи в модели бизнес-процессов; на рис. 6.6 в представлена ассоциация отката; на рис. 6.6 г показана ассоциация исключения;

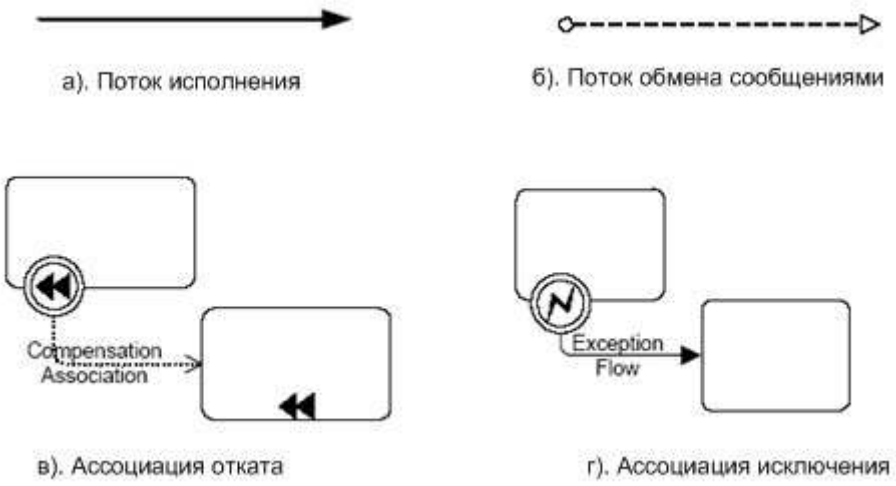


Рис. 6.6. Виды связей

д) УЧАСТНИКИ (swimlanes) бизнес-процесса [13]**;**

Таких участников в BPMN бывает два вида.

Первый вид - ***участник бизнес-процесса*** (pool). Это бизнес-сущность (например, компания), участвующая в бизнес-процессе, или некоторая бизнес-роль - покупатель, продавец, дилер и т. д. В одном бизнес-процессе может быть много компаний, но часть из них может быть представлена бизнес-ролями. Это означает, что в этом общем бизнес-процессе не существенны детали их индивидуальных, внутренних бизнес-процессов, а важна только стандартная реакция, определяемая теми ролями, которые они играют. Одну и ту же роль могут играть разные компании, выполняющие лишь определенные правила взаимодействия. Как бизнес-роль (покупатель, продавец некоторой биржи), так и уникальная компания (например, Центробанк РФ) являются в BPMN участниками бизнес-процесса. Пример показан на рис. 6.7 а.

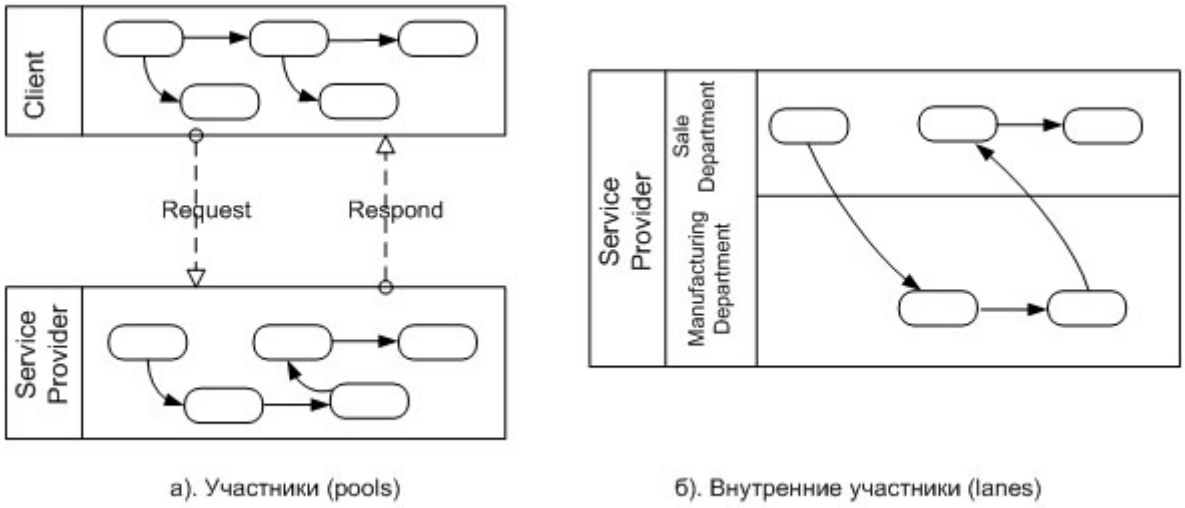


Рис. 6.7. Участники бизнес-процесса

На этом рисунке представлены два участника бизнес-процесса - Client и Service Provider. В каждом из них определен свой бизнес-процесс. Эти участники взаимодействуют друг с другом, обмениваясь сообщениями. Эти сообщения можно было "протащить" до отдельных задач, но можно оставить и так: здесь не ставилась цель вдаваться в детали семантики сообщений [13].

Участник бизнес-процесса может содержать других участников, например, функциональные подразделения внутри компании. В BPMN для этого есть конструкция lane. Этот термин переведен на русский язык как внутренний участник. На рис. 6.7 б показан пример внутренних участников. Так, в компании под названием Service Provider из примера на рис. 6.7 а имеется два отдела - отдел продаж (Sale Department) и производственный отдел (Manufacturing Department). Бизнес-процесс этой компании на рис. 6.7 б распределен по этим двум участникам.

Внутренний участник - это еще один способ декомпозиции бизнес-процесса, наряду с подпроцессами. Пользуясь терминологией теории графов можно сказать, что подпроцессы - это декомпозиция "в глубину", а внутренние участники - декомпозиция "в ширину". В случае подпроцессов создаются "этажи" описания бизнес-процесса, а в случае использования внутренних участников "плоское плотно" действий разбивается на группы, каждая из которых не скрывается за одним подпроцессом, а помещается в отдельную секцию на диаграмме - внутреннего участника.

ПРАКТИЧЕСКАЯ ЧАСТЬ

ЧАСТЬ I

1) Запустить программу TIBCO Business Studio. При первом запуске указать свою папку в качестве директории, в которую будут сохраняться файлы диаграмм;

2) Выбрать пункт меню File -> New -> Process Package;

3) Указать название диаграммы и путь, который предлагает программа по умолчанию;

4) Нажать Next;

5) Откроется окно программы (рис. 6.8):

Окно состоит из вкладки Диаграммы процессов, куда добавляются элементы модели. Структуры диаграммы (рис. 6.8 левая часть) и палитры инструментов Palette (рис. 6.8 справа). Соответствующий участник процесса добавляется путем щелчка на палитре инструментов и последующего щелчка на поле для построения диаграммы. Свойства каждого из добавленных элементов можно изменить на панели Properties (рис. 6.8. внизу).

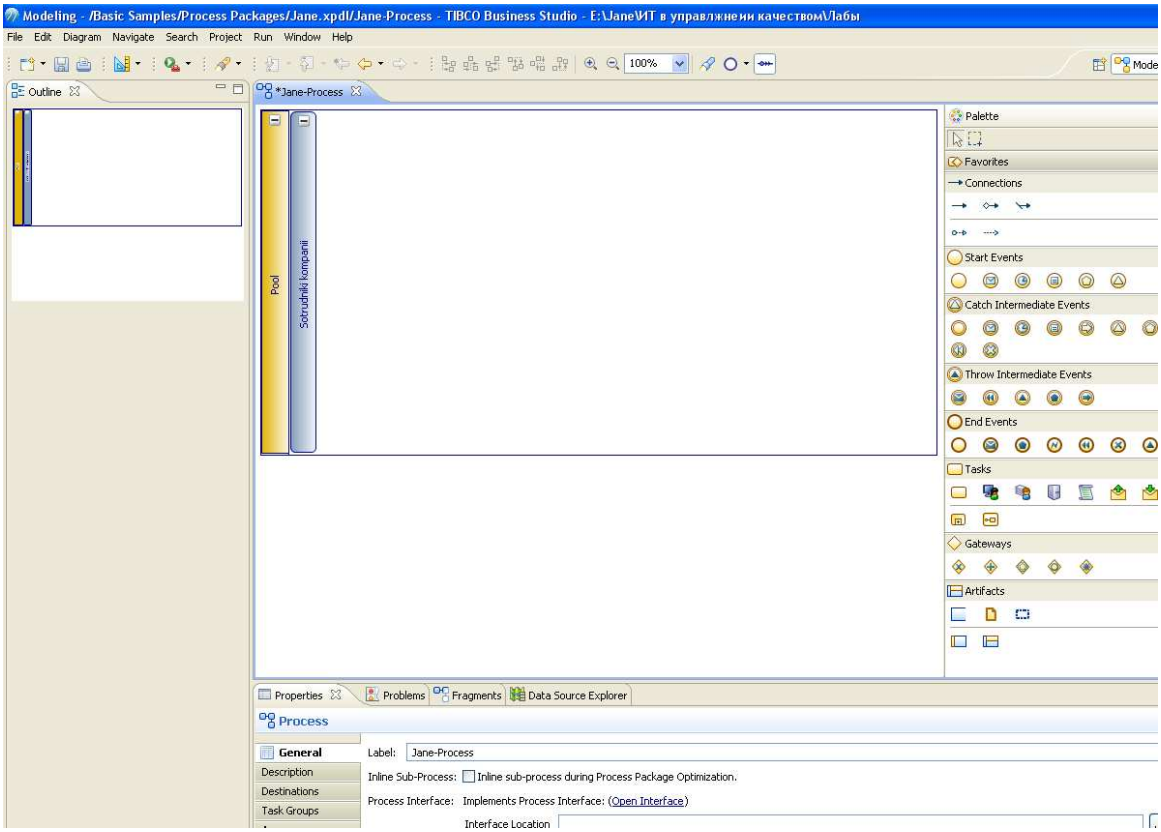


Рис. 6.8. Интерфейс программы TIBCO Business Studio

Задание.

1. При помощи программы TIBCO Business Studio создать диаграмму процесса «Обработка запроса о товарах» представленную на рис. 6.9. [14].

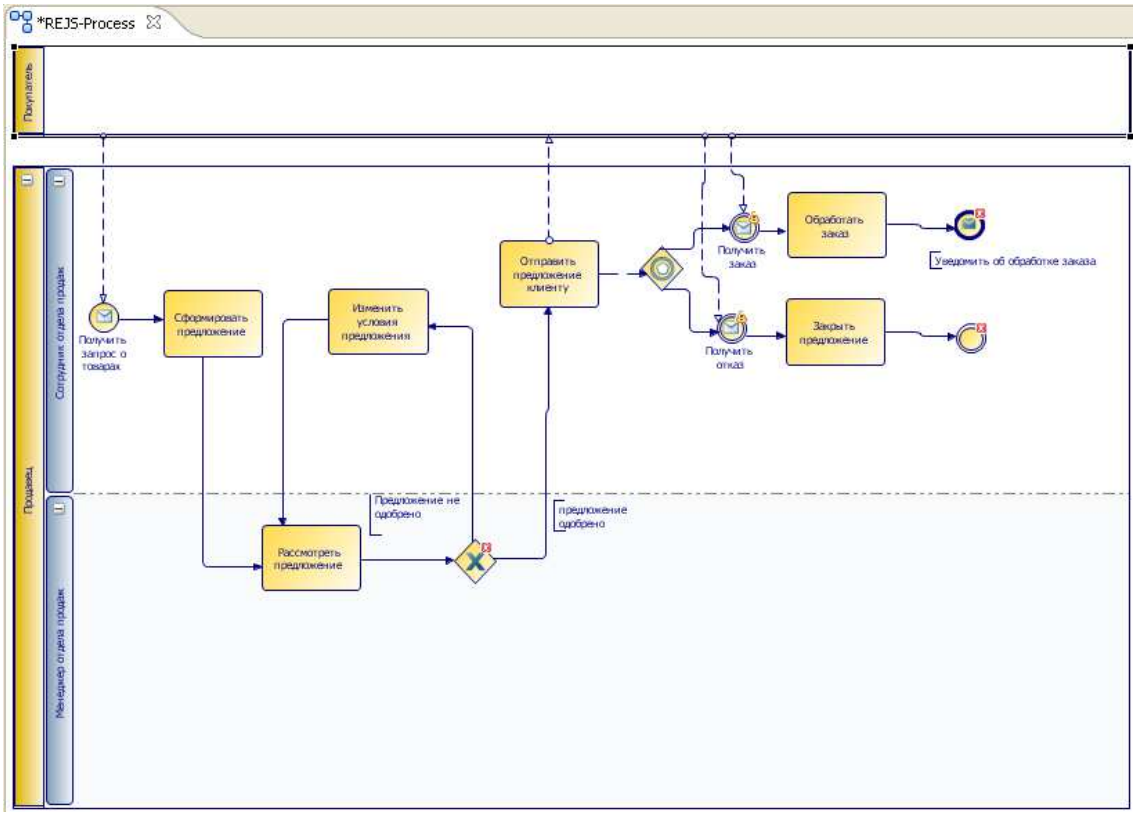


Рис. 6.9. Модель процесса «Обработка запроса о товарах»

2. Дать текстовое описание полученной диаграммы, исходя из логики хода действий.

3. Разработать модель бизнес-процесса по бронированию авиабилетов и гостиницы для туристов в деятельности турфирмы. При этом рассмотреть 4-х участников процесса: туриста, турфирму, авиакассу и гостиницу и показать отношения между ними.

ЧАСТЬ II

Преподаватель собирается все кейсы, разработанные студентами при выполнении самостоятельной работы. Преподаватель перемешивает кейсы и каждый из студентов вытягивает себе по 2 кейса. Далее дается 30 минут на решение. После того, как студенты решили кейсы, каждый из них по очереди озвучивает проблему и ее решение. Остальные студенты слушают ответ и предлагают другие методы решения. Все методы обсуждаются, и всеобщим голосованием выбирается лучший. Кроме того, от студентов требуется подготовить обоснование важности разработки бизнес-процессов предприятия и озвучить его с последующим обсуждением.

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Какие бывают виды сущностей (connecting objects) в BPMN?
2) Что такое действие?
3) Что такое задача?
4) Что такое подпроцесс?

5) Какие виды связей бывают у сущностей бизнес-процессов?
6) Какие сущности бизнес-процессов могут обмениваться сообщениями, и какие не могут? Почему?
7) Что такое участник бизнес-процесса?
8) Что такое порт (gateway), зачем он нужен?

ЛАБОРАТОРНАЯ РАБОТА № 7
Моделирование бизнес-процессов предприятия BPMN

Цель: при помощи нотации моделирования бизнес-процессов BPMN необходимо описать процесс приема нового сотрудника на работу в медицинское учреждение.

Форма проведения занятия: интерактивное занятие с использованием метода презентации (1 ч).

ПРАКТИЧЕСКАЯ ЧАСТЬ

ЧАСТЬ I

Описание проблемы: директор клиники «Евромед» желает автоматизировать процесс приема на работу сотрудников и довести его до всех участников данного процесса.

Методы получения информации: интервью, изучение нормативных документов и должностных инструкций.

Работа строится на основе серии проведенных интервью и их анализа. В результате интервью и анализа документов **были выявлены 8 участников данного процесса**: директор частной медицинской клиники «Евромед», руководитель структурного подразделения (в которое устраивается работник), начальник кадрово-правового отдела (КПО), зам. начальника кадрово-правового отдела (КПО), бухгалтер, юрисконсультант, эпидемиолог, инженер по охране труда. Процесс включает около 16-20 функций и длится примерно 3 месяца. Между участниками процесса идет активный обмен документами.

Процесс трудоустройства на основании серии интервью **можно описать так** [15]:

1. руководитель структурного подразделения сообщает о трудностях в выполнении работы, которые обусловлены отсутствием необходимых человеческих ресурсов и просит принять еще одного или нескольких сотрудников.

2. директор либо подтверждает необходимость устройства нового сотрудника, либо нет, и тогда процесс заканчивается.

3. если директор подтвердил необходимость устройства нового сотрудника, то зам. начальника КПО составляет список вакансий, в котором указаны и требования к кандидатам на должность.

4. заместитель начальника КПО при участии начальника КПО и руководителя подразделения оценивают кандидита.

5. если кандидат подходит, то зам. начальника КПО знакомит его с необходимыми документами, если не подходит, то процесс завершается.

6. после того, как кандидат ознакомлен с необходимыми документами, зам. начальника КПО принимает документы для трудоустройства за подписью начальника структурного подразделения и бухгалтера.

7. начальник КПО проверяет документы на прием, если все верно, то передает директору для заключения трудового договора, если не верно, то возвращает кандидата вновь на стадию приема документов.

8. директор рассматривает вопрос заключения трудового договора. Здесь может быть три взаимоисключающих сценария развития событий: а) директор отказывает в заключении договора и процесс заканчивается; б) директор дает предписание начальнику ТПО еще раз проверить документы на трудоустройство до тех пор, пока директора не устроит их качество; в) директор одобряет заключение трудового договора;

9. после одобрения директором заключения трудового договора руководитель структурного подразделения знакомит нового сотрудника с должностной инструкцией, а начальник ТПО готовит приказ о трудоустройстве, юрисконсультант готовит трудовой договор.

10. после того, как юрисконсультант подготовит трудовой договор, зам. начальника ТПО выполняет допуск нового сотрудника к работе. Процесс допуска к работе объединяет в себе две задачи: санэпидемконтроль, который проводит эпидемиолог и вводный инструктаж, который проводит инженер по охране труда.

11. после получения допуска к работе руководитель структурного подразделения составляет индивидуальный план работы на испытательный срок, который длится 3 месяца. На этот срок работнику выделяется наставник.

12. через 3 месяца руководитель подразделения оценивает работу сотрудника.

13. на основании оценки руководителем структурного подразделения директор принимает решение о продлении трудового договора.

14. если решение о продлении трудового договора положительное, то юрисконсультант подготавливает дополнительное соглашение, где установлен новый срок договора, в противном случае зам. начальника ТПО возвращает сотруднику его документы и на работу его не устраивают.

ЧАСТЬ II

Студентам предварительно было выдано задание для самостоятельной работы: подготовка карты процессов и презентации данной карты. Кроме того, аналогичную карту процессов необходимо разработать на аудиторном занятии под модель процесса описанного выше (процесс трудоустройства нового сотрудника). Презентация оформляется в формате ppt в соответствии с идеями студента. Возможна работа в парах. Далее каждый из студентов представляет свою карту процессов, рассказывает о сложностях, с которыми он столкнулся при ее разработке. Остальные студенты из группы задают ему вопросы и делятся впечатлениями о его презентации. По ходу представления презентаций студенты ставят оценки за каждый ответ на специальном бланке. Оценки являются анонимными. По итогам занятия оценки суммируются, вычисляется средний балл и озвучивается студентам.

ЛАБОРАТОРНАЯ РАБОТА № 8
Разработка комплекса моделей бизнес-процессов предприятия

Цель: при помощи одной из рассмотренных нотаций моделирования бизнес-процессов разработать комплекс моделей бизнес-процессов предприятия.

Оборудование: компьютер с программным обеспечением (Ramus Educational, Tibco Business Studio, Software Ideas Modeler).

Форма проведения занятия: работа в команде из 3-4 человек с последующим обсуждением проекта в рамках круглого стола (4 ч);

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

При выполнении комплекса лабораторных работ 1-7, посвященных моделированию бизнес-процессов, были рассмотрены единичные примеры различного рода диаграмм и нотаций. Как правило, такой подход не приемлем для предприятия. Бизнес-процессы реальных организаций разрабатываются в комплексе. Так, чтобы итоговый комплекс моделей бизнес-процессов охватывал все сферы деятельности данного предприятия, и кроме того, описывал не только основные процессы, но и вспомогательные (работу бухгалтерии, отдела кадров и т.д.), а также взаимодействие между этими процессами.

На сайте http://www.businessstudio.ru/ приводится большое количество примеров, построенных при помощи функционального моделирования IDEF0. Знакомство с этими примерами, поможет понять суть данной работы и увидеть примерный результат своей работы, который необходимо получить при работе в команде. Нотация моделирования для реализации проекта может быть любой.

ПРАКТИЧЕСКАЯЧ ЧАСТЬ

В команде из 2-3 человек (оптимально все же число 3) один должен быть лидером. Лидер определяется командой и несет ответственность за выполнение всего проекта в нужные сроки. Предприятие для построения комплекса моделей полностью определяется выбором студентов. Это может быть предприятие где проходилась производственная практика, или реализовывался проект ГПО. Кроме того, можно найти предприятие в структуре МСБИ «Дружба».

При выполнении работы должен быть сформирован отчет, содержащий:

1) информацию о предприятии;
2) организационная структура отделов;
3) методы получения информации для работы (интервью, анкеты, анализ документов);
4) описание основных, вспомогательных и управленческих процессов (можно в форме карты процессов);
5) модели бизнес-процессов и описание к ним;
6) выводы по результатам моделирования;
7) рекомендации руководителю предприятия.

После представления отчета, организуется представление проектов командами в форме круглого стола. Каждая команда представляет свой проект в виде презентации, отвечает на вопросы, рассказывает, с какими трудностями она столкнулась при выполнении работы. Также для защиты требуется подготовить обоснование важности разработки бизнес-процессов предприятия, представленной командой. Остальные студенты должны критически оценить это обоснование и приводить команде контраргументы. Команда отвечает на эти контраргументы.

По итогам занятия обсуждаются проекты, защита, убедительность обоснования. Преподаватель присваивает номинации:

1. «Лучший проект»;
2. «Лучшая командная работа»;
3. «Лучшее умение противостоять возражениям»;
4. «Лучшее умение выступать публично»;
5. и прочее по желанию преподавателя.

После выступления обсуждаются методы исследования, отношение со стороны компании к разработке бизнес-процессов и прочее. Кроме того, от команды ожидается пожелание для младших курсов при выполнении данной работы.

ПРИМЕР КОНТРОЛЬНОГО ТЕСТИРОВАНИЯ ЗА СЕМЕСТР ПО ТЕМАМ ЛЕКЦИЙ И ЛАБОРАТОРНЫХ РАБОТ № 1-7 НАХОДИТСЯ В ПРИЛОЖЕНИИ А К ДАННЫМ МЕТОДИЧЕСКИМ РЕКОМЕНДАЦИЯМ.

БЛОК «ЗАЩИТА ИНФОРМАЦИИ»

ЛАБОРАТОРНАЯ РАБОТА № 9

Изучение Международных и отечественных стандартов в области информационной безопасности

Цель работы: изучить существующие стандарты международного и отечественного уровня в области защиты информации.

Оборудование: компьютер с операционной системой Windows, текстовый редактор Microsoft Word, наличие доступа к ресурсам глобальной сети Интернет.

Форма проведения занятия: интерактивное занятие с использованием методов круглого стола и презентации (4 ч);

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

В соответствии с международными и национальными стандартами обеспечение информационной безопасности в любой компании предполагает следующее [16]:

- ✓ определение целей обеспечения информационной безопасности компьютерных систем;
- ✓ создание эффективной системы управления информационной безопасностью;
- ✓ расчет совокупности детализированных качественных и количественных показателей для оценки соответствия информационной безопасности поставленным целям;
- ✓ применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния;
- ✓ использование методик управления безопасностью, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Рассмотрим наиболее известные международные стандарты в области защиты информации [16].

ISO/IEC 15408. Критерии оценки безопасности информационных технологий

Международный стандарт ISO 15408 был разработан на основе стандарта "Общие критерии безопасности информационных технологий" вер.2.1. В 2002 году этот стандарт был принят в России как ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий", часто называемый в литературе "Общие критерии". Ранее в отечественных нормативных документах в области ИБ понятие риска не вводилось. На рис. 9.1

представлена определяемая стандартом взаимосвязь высокоуровневых понятий в области ИБ. Безопасность связана с защитой активов ИС от угроз. За сохранность рассматриваемых активов отвечают их владельцы, для которых эти активы имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельца. Владельцы будут воспринимать подобные угрозы как потенциал воздействия на активы, приводящего к понижению их ценности для владельца.

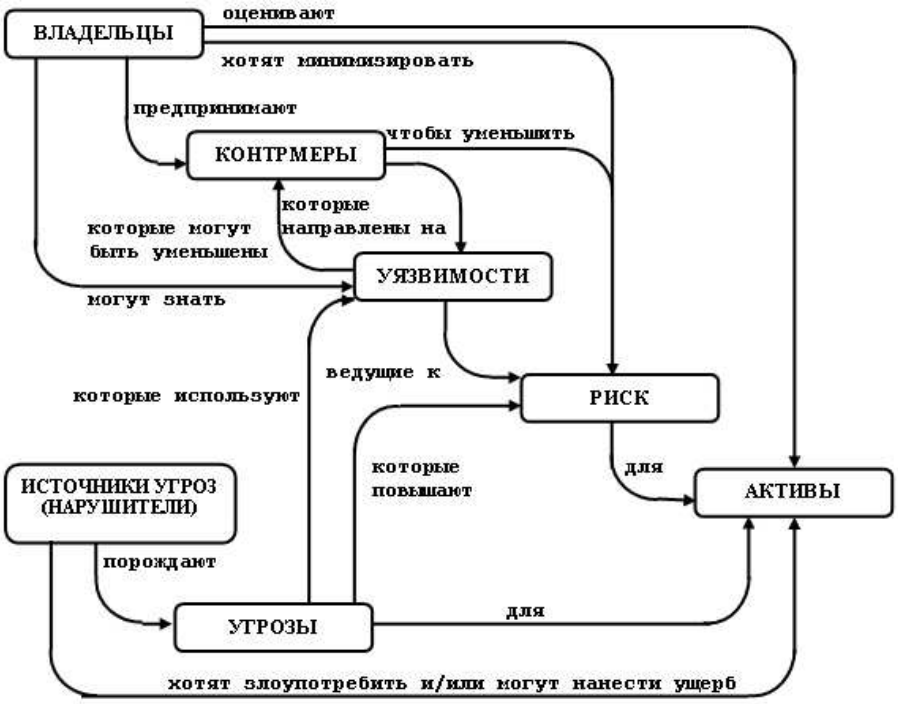


Рис. 9.1. Понятия безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-2002

Владельцы активов будут анализировать возможные угрозы, чтобы решить, какие из них действительно присущи их среде. В результате анализа определяются риски. Анализ может помочь при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня [16].

Контрмеры предпринимают для уменьшения уязвимостей и выполнения политики безопасности владельцев активов (прямо или косвенно распределяя между этими составляющими). Но и после введения этих контрмер могут сохраняться остаточные уязвимости. Такие уязвимости могут использоваться нарушителями, представляя уровень остаточного риска для активов. Владельцы будут стремиться минимизировать этот риск, задавая дополнительные ограничения.

Стандарт разработан таким образом, чтобы удовлетворить потребности трех групп специалистов: разработчиков, экспертов по сертификации и пользователей объекта оценки.

Под объектом оценки (ОО) понимается "подлежащие оценке продукт информационных технологий (ИТ) или система с руководствами администратора и пользователя". К таким объектам относятся, например, операционные системы, прикладные программы, ИС и т.д.

"Общие критерии" предусматривают наличие двух типов требований безопасности - функциональных и доверия. Функциональные требования относятся к сервисам безопасности, таким как идентификация, аутентификация, управление доступом, аудит и т.д. Требования доверия к безопасности относятся к технологии разработки, тестированию, анализу уязвимостей, поставке, сопровождению, эксплуатационной документации и т.д.

Описание обоих типов требований выполнено в едином стиле: они организованы в иерархию "класс - семейство - компонент - элемент". Термин "класс" используется для наиболее общей группировки требований безопасности, а элемент - самый нижний, неделимый уровень требований безопасности.

В стандарте выделены 11 классов функциональных требований [16, 17]:

- ✓ аудит безопасности;
- ✓ связь (передача данных);
- ✓ криптографическая поддержка (криптографическая защита);
- ✓ защита данных пользователя;
- ✓ идентификация и аутентификация;
- ✓ управление безопасностью;
- ✓ приватность (конфиденциальность);
- ✓ защита функций безопасности объекта;
- ✓ использование ресурсов;
- ✓ доступ к объекту оценки;
- ✓ доверенный маршрут/канал.

Основные структуры "Общих критериев" - это профиль защиты и задание по безопасности. Профиль защиты определяется как "независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя". Профиль состоит из компонентов или пакетов функциональных требований и одного из уровней гарантированности. Структура профиля защиты представлена на рис. 9.2.

Профиль определяет "модель" системы безопасности или отдельного ее модуля. Количество профилей потенциально не ограничено, они разрабатываются для разных областей применения (например, профиль "Специализированные средства защиты от несанкционированного доступа к конфиденциальной информации").

Профиль защиты служит основой для создания задания по безопасности, которое можно рассматривать как технический проект для разработки ОО. Задание по безопасности может включать требования одного или нескольких профилей защиты. Оно описывает также уровень функциональных возможностей средств и механизмов защиты, реализованных в ОО, и приводит обоснование степени их адекватности. По результатам проводимых оценок, создаются каталоги сертифицированных профилей защиты и продуктов (операционных систем, средств защиты информации и т.д.), которые затем используются при оценке других объектов"

Стандарты ISO/IEC 17799/27002 и 27001

Международные стандарты ISO/IEC 17799 (новая версия вышла под номером 27002) и 27001 посвящены вопросам управления информационной безопасностью, и так как они взаимосвязаны, рассматривать их будем в одном разделе. Первая часть стандарта описывает рекомендуемые меры в области управления информационной безопасностью и, в целом, не предназначался для проведения сертификации систем на его соответствие.

В 1999 году была опубликована вторая часть стандарта, на соответствие которому может проводиться сертификация.

В России на данный момент действуют стандарты ГОСТ Р ИСО/МЭК 17799-2005 "Информационная технология. Практические правила управления информационной безопасностью" (аутентичный перевод ISO/IEC 17799:2000) и ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" (перевод ISO/IEC 27001:2005). Несмотря на некоторые внутренние расхождения, связанные с разными версиями и особенностями перевода, наличие стандартов позволяет привести систему управления информационной безопасностью в соответствие их требованиям и, при необходимости, сертифицировать [16].

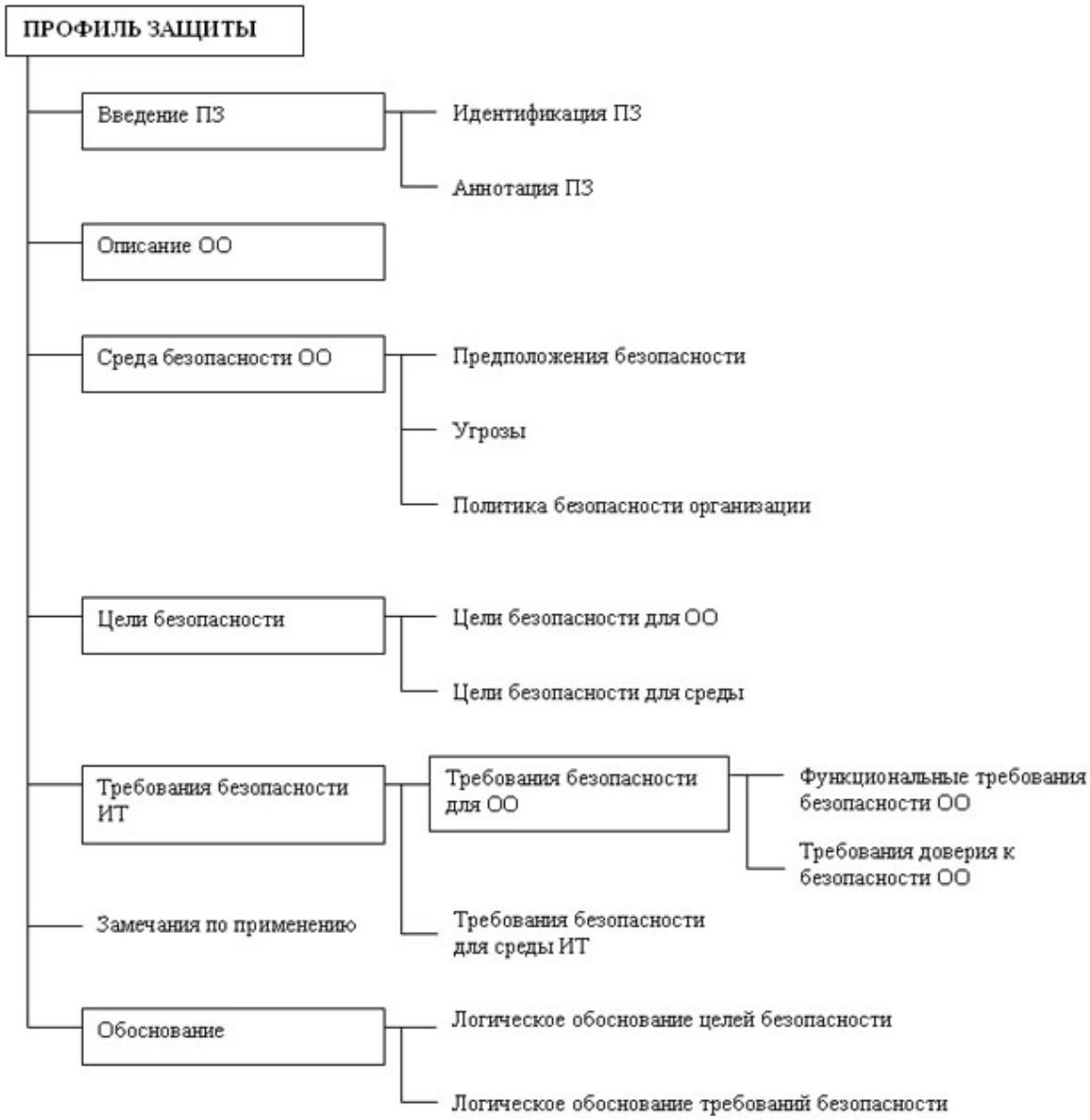


Рис. 9.2. Структура профиля защиты

ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью"

Данный стандарт рассматривает вопросы информационной безопасности, в том числе, и с точки зрения экономического эффекта [16, 17].

Указываются три группы факторов, которые необходимо учитывать при формировании требований в области информационной безопасности. Это:

- ✓ оценка рисков организации. Посредством оценки рисков происходит выявление угроз активам организации, оценка уязвимости соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий;

- ✓ юридические, законодательные, регулирующие и договорные требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг;
- ✓ специфический набор принципов, целей и требований, разработанных организацией в отношении обработки информации.

После того, как определены требования, идет этап выбора и внедрения мероприятий по управлению информационной безопасностью, которые обеспечат снижение рисков до приемлемого уровня.

Кратко перечислим разделы стандарта и предлагаемые в них мероприятия по защите информации. Первая их группа касается политики безопасности. Требуется, чтобы она была разработана, утверждена руководством организации, издана и доведена до сведения всех сотрудников. Она должна определять порядок работы с информационными ресурсами организации, обязанности и ответственность сотрудников. Политика периодически пересматривается, чтобы соответствовать текущему состоянию системы и выявленным рискам.

Следующий раздел затрагивает организационные вопросы, связанные с обеспечением информационной безопасности. Стандарт рекомендует создавать управляющие советы (с участием высшего руководства компании) для утверждения политики безопасности, назначения ответственных лиц, распределения обязанностей и координации внедрения мероприятий по управлению информационной безопасностью в организации. Также должен быть описан процесс получения разрешений на использование в организации средств обработки информации (в т.ч. нового программного обеспечения и аппаратуры), чтобы это не привело к возникновению проблем с безопасностью.

Следующий раздел стандарта посвящен вопросам классификации и управления активами. Для обеспечения информационной безопасности организации необходимо, чтобы все основные информационные активы были учтены и закреплены за ответственными владельцами. Начать предлагается с проведения инвентаризации. В качестве примера приводится следующая классификация:

- ✓ информационные активы (базы данных и файлы данных, системная документация и т.д.);
- ✓ активы программного обеспечения (прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты);
- ✓ физические активы (компьютерное оборудование, оборудование связи, носители информации, другое техническое оборудование, мебель, помещения);
- ✓ услуги (вычислительные услуги и услуги связи, основные коммунальные услуги).

Далее предлагается классифицировать информацию, чтобы определить ее приоритетность, необходимость и степень ее защиты. При этом, можно оценить соответствующую информацию с учетом того, насколько она критична для организации, например, с точки зрения обеспечения ее целостности и доступности. После этого предлагается разработать и внедрить процедуру маркировки при обработке информации. Для каждого уровня классификации следует определять процедуры маркировки для того, чтобы учесть следующие типы обработки информации:

- ✓ копирование;
- ✓ хранение;
- ✓ передачу по почте, факсом и электронной почтой;
- ✓ передачу голосом, включая мобильный телефон, голосовую почту, автоответчики;
- ✓ уничтожение.

Следующий раздел рассматривает вопросы безопасности, связанные с персоналом. Стандартом определяется, чтобы обязанности по соблюдению требований безопасности распределялись на стадии подбора персонала, включались в трудовые договоры и проводился их мониторинг в течение всего периода работы сотрудника. В частности, при приеме в постоянный штат, рекомендуется проводить проверку подлинности представляемых претендентом документов, полноту и точность резюме, представляемые им рекомендации. Рекомендуется, чтобы сотрудники подписывали соглашение о конфиденциальности, уведомляющее о том, какая информация является конфиденциальной или секретной. Должна быть определена дисциплинарная ответственность сотрудников, нарушивших политику и процедуры безопасности организации. Там, где необходимо, эта ответственность должна сохраняться и в течение определенного срока после увольнения с работы.

Следующий раздел стандарта посвящен вопросам физической защиты и защиты от воздействия окружающей среды. Указывается, что "средства обработки критичной или важной служебной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами контроля проникновения. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия".

Рекомендуется провести разделение сред разработки, тестирования и промышленной эксплуатации программного обеспечения (ПО). Правила перевода ПО из статуса разрабатываемого в статус принятого к эксплуатации должны быть определены и документально оформлены.

Должен быть определен порядок проведения вспомогательных операций, к которым относится резервное копирование программного обеспечения и данных регистрация событий и ошибок и, где необходимо, мониторинг состояния аппаратных средств. Мероприятия по резервированию для каждой отдельной системы должны регулярно тестироваться для обеспечения уверенности в том, что они удовлетворяют требованиям планов по обеспечению непрерывности бизнеса.

Следующий раздел стандарта посвящен вопросам контроля доступа.

Требуется, чтобы правила контроля доступа и права каждого пользователя или группы пользователей однозначно определялись политикой безопасности. Пользователи и поставщики услуг должны быть оповещены о необходимости выполнения данных требований.

При использовании парольной аутентификации, необходимо осуществлять контроль в отношении паролей пользователей. В частности, пользователи должны подписывать документ о необходимости соблюдения полной конфиденциальности паролей. Требуется обеспечить безопасность процесса получения пароля пользователем и, если это используется, управления пользователями своими паролями (принудительная смена пароля после первого входа в систему и т.д.).

Желательно предусматривать сигнал тревоги на случай, когда пользователь может стать объектом насилия (если такое событие оценивается как вероятное). При этом необходимо определить обязанности и процедуры реагирования на сигнал такой тревоги.

Для обнаружения отклонения от требований политики контроля доступа и обеспечения доказательства на случай выявления инцидентов нарушения информационной безопасности необходимо проводить мониторинг системы. Результаты мониторинга следует регулярно анализировать. Журнал аудита может использоваться для расследования инцидентов, поэтому достаточно важной является правильная установка (синхронизация) компьютерных часов.

Очередной раздел стандарта называется "Разработка и обслуживание систем". Уже на этапе разработки информационных систем необходимо обеспечить учет требований безопасности. А в процессе эксплуатации системы требуется предотвращать потери, модификацию или неправильное использование пользовательских данных. Для этого в прикладных системах рекомендуется предусмотреть подтверждение корректности ввода и вывода данных, контроль обработки данных в системе, аутентификацию сообщений, протоколирование действий пользователя.

Следующий раздел стандарта посвящен вопросам управления непрерывностью бизнеса. На начальном этапе предполагается идентифицировать события, которые могут

быть причиной прерывания бизнес-процессов (отказ оборудования, пожар и т.п.). При этом нужно провести оценку последствий, после чего разработать планы восстановления. Адекватность планов должна быть подтверждена тестированием, а сами они должны периодически пересматриваться, чтобы учитывать происходящие в системе изменения.

Заключительный раздел стандарта посвящен вопросам соответствия требованиям. В первую очередь, это касается соответствия системы и порядка ее эксплуатации требованиям законодательства. Сюда относятся вопросы соблюдения авторского права (в том числе, на программное обеспечение), защиты персональной информации (сотрудников, клиентов), предотвращения нецелевого использования средств обработки информации.

Сами информационные системы должны соответствовать политике безопасности организации и используемым стандартам. Безопасность информационных систем необходимо регулярно анализировать и оценивать. В то же время, требуется соблюдать меры безопасности и при проведении аудита безопасности, чтобы это не привело к нежелательным последствиям (например, сбой критически важного сервера из-за проведения проверки).

ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

Разработчики стандарта отмечают, что он был подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ). СМИБ (англ. -information security management system; ISMS) определяется как часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности [16].

Стандарт предполагает использование процессного подхода для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ организации. Он основан на модели "Планирование (Plan) - Осуществление (Do) - Проверка (Check) - Действие (Act)" (PDCA), которая может быть применена при структурировании всех процессов СМИБ. На рис. 9.3 показано, как СМИБ, используя в качестве входных данных требования ИБ и ожидаемые результаты заинтересованных сторон, с помощью необходимых действий и процессов выдает выходные данные по результатам обеспечения информационной безопасности, которые соответствуют этим требованиям и ожидаемым результатам.

На этапе разработки системы менеджмента информационной безопасности организация должна осуществить следующее:

- ✓ определить область и границы действия СМИБ;
- ✓ определить политику СМИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий;
- ✓ определить подход к оценке риска в организации;
- ✓ идентифицировать риски;
- ✓ проанализировать и оценить риски;
- ✓ определить и оценить различные варианты обработки рисков;
- ✓ выбрать цели и меры управления для обработки рисков;
- ✓ получить утверждение руководством предполагаемых остаточных рисков;
- ✓ получить разрешение руководства на внедрение и эксплуатацию СМИБ;
- ✓ подготовить Положение о применимости.

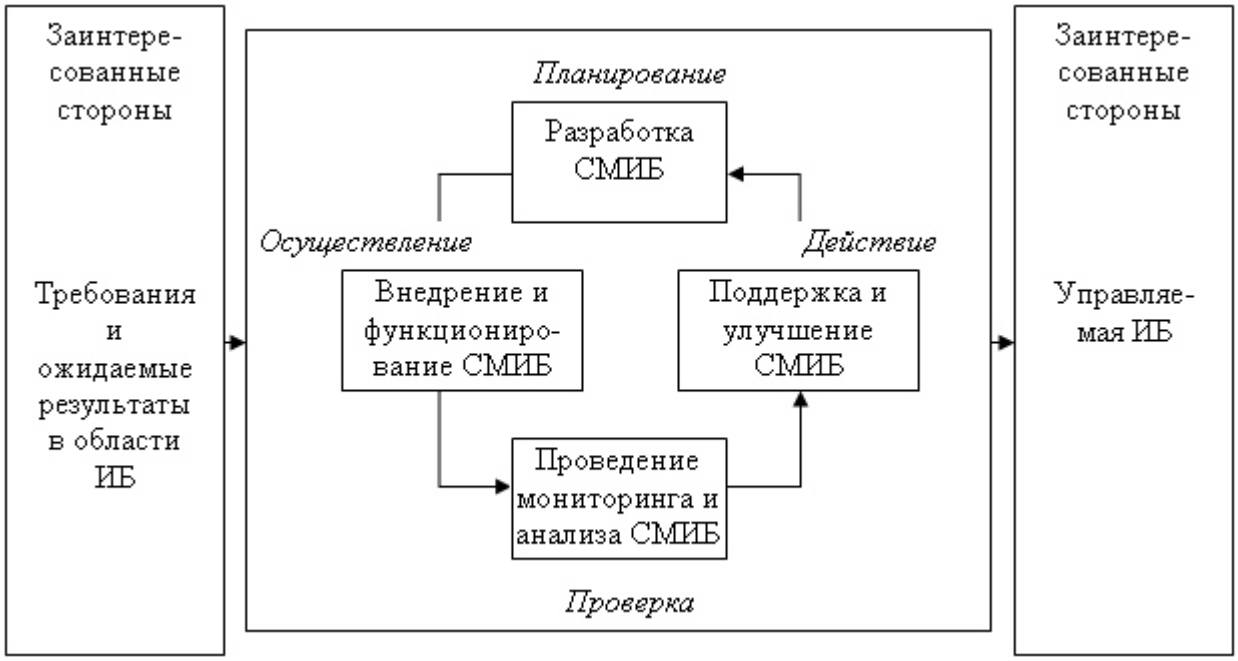


Рис. 9.3. Этапы построения и использования СМИБ

Далее в стандарте приводятся требования к документации, которая в частности должна включать положения политики СМИБ и описание области функционирования, описание методики и отчет об оценке рисков, план обработки рисков, документирование связанных процедур. Также должен быть определен процесс управления документами СМИБ, включающий актуализацию, использование, хранение и уничтожение.

Для предоставления свидетельств соответствия требованиям и результативности функционирования СМИБ необходимо вести и поддерживать в рабочем состоянии учетные записи и записи о выполнении процессов. В качестве примеров называются журналы регистрации посетителей, отчеты о результатах аудита и т.п.

Стандарт определяет, что руководство организации ответственно за обеспечение и управление ресурсами, необходимыми для создания СМИБ, а также организацию подготовки персонала.

В приложении к стандарту перечисляются рекомендуемые меры управления, взятые из ранее рассмотренного стандарта ISO/IEC 17799:2005.

ПРАКТИЧЕСКАЯ ЧАСТЬ

Для данной лабораторной работы требуется предварительная подготовка материала по темам, выданным преподавателем. Каждая тема представляет собой краткий обзор определенного стандарта в области информационной безопасности. В теоретической части данной работы показаны примеры представления материала на круглый стол.

На круглом столе обсуждаются вопросы уровня информационной безопасности на текущий момент. Какие существуют стандарты информационной безопасности, насколько они применяются в российских компаниях, с какой целью они применяются, когда проводилась актуализация стандарта.

По ходу изложения доклада, остальные участники круглого стола должны делать пометки, готовить вопросы докладчику, а также оценить степень развернутости темы.

По окончанию докладов все участники вступают в дискуссию по вопросу о том, какой стандарт наиболее оптимален для разработки общей и специализированной политики безопасности организации.

По итогу занятия студенты оцениваются исходя из следующих критериев: а) количество вопросов, заданных докладчику; б) степень подготовки доклада; в) степень ответа на вопросы; г) степень участия в дискуссии.

Допускается подготовка одной темы двумя студентами.

Темы для подготовки докладов

Номер темы	Наименование темы
1	Стандарт ISO/IEC 15408. Критерии оценки безопасности информационных технологий;
2	Стандарт ISO/IEC 27001:2005 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования»
3	Стандарт ГОСТ Р ИСО/МЭК 17799:2005 "Информационная технология. Практические правила управления информационной безопасностью"
4	Стандарт ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология.

	Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".
5	Стандарт BS 7799-1:2005
6	Стандарты безопасности в сети Интернет;
7	Стандарты безопасности для беспроводных сетей;
8	ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Что предполагает информационное обеспечение любой компании в целом?
2) Дайте объяснение (устное описание) схемы на рис. 9.1
3) Назвать 5-6 из 11 существующих функциональных требований стандарта ISO/IEC 1508
4) Для чего служить профиль защиты согласно стандарту ISO/IEC 15408?
5) Какой из рассмотренных стандартов рассматривает вопросы информационной безопасности с точки зрения экономического эффекта?

ЛАБОРАТОРНАЯ РАБОТА № 10
Изучение существующих методик оценки рисков

Цель работы: получить навык выявления рисков в системе безопасности предприятия, изучить существующие методики управления рисками, их достоинства и недостатки.

Оборудование: компьютер с операционной системой Windows, программа Microsoft Security Assessment (MSAT).

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Существует несколько разновидностей методик для оценки рисков, которые в основном отличаются уровнем оценки. Выделяют три типа методик:

- ✓ методики, использующие оценку риска на качественном уровне (например, по шкале "высокий", "средний", "низкий"). К таким методикам, в частности, относится FRAP;
- ✓ количественные методики (риск оценивается через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch;
- ✓ методики, использующие смешанные оценки (такой подход используется в CRAMM, методике Microsoft и т.д.) [19].

Методика CRAMM

Это одна из первых методик анализа рисков в сфере ИБ - работа над ней была начата в середине 80-х гг. центральным агентством по компьютерам и телекоммуникациям (ССТА) Великобритании. В основе метода CRAMM лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит как для крупных, так и для малых организаций, как правительственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (profiles). Для коммерческих организаций имеется Коммерческий профиль (Commercial Profile), для правительственных организаций - Правительственный профиль (Government profile). Правительственный вариант профиля, также позволяет проводить аудит на соответствие требованиям американского стандарта ITSEC ("Оранжевая книга") [19].

Методика FRAP

Методика "Facilitated Risk Analysis Process (FRAP)" предлагаемая компанией Peltier and Associates (сайт в Интернет http://www.peltierassociates.com/) разработана Томасом Пелтиером (Thomas R. Peltier) и опубликована в (фрагменты данной книги доступны на сайте, приведенное ниже описание построено на их основе). В методике, обеспечение ИБ ИС предлагается рассматривать в рамках процесса управления рисками. Управление рисками в сфере ИБ - процесс, позволяющий компаниям найти баланс между затратами средств и сил на средства защиты и получаемым эффектом. Управление рисками должно начинаться с оценки рисков: должным образом оформленные результаты оценки станут основой для принятия решений в области повышения безопасности системы. После завершения оценки, проводится анализ соотношения затрат и получаемого эффекта (англ. cost/benefit analysis), который позволяет определить те средства защиты, которые нужны, для снижения риска до приемлемого уровня [19].

Методика OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - методика поведения оценки рисков в организации, разрабатываемая институтом Software Engineering Institute (SEI) при университете Карнеги Меллон (Carnegie Mellon University). Полное описание методики доступно в Интернет на сайте www.cert.org/octave.

Особенность данной методики заключается в том, что весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов. Для этого создается смешанная группа, включающая как технических специалистов, так и

руководителей разного уровня, что позволяет всесторонне оценить последствия для бизнеса возможных инцидентов в области безопасности и разработать контрмеры [19].

Методика Risk Watch

Компания RiskWatch разработала собственную методику анализа рисков и семейство программный средств, в которых она в той либо иной мере реализуется. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности:

- ✓ RiskWatch for Physical Security - для анализа физической защиты ИС;
- ✓ RiskWatch for Information Systems - для информационных рисков;
- ✓ HIPAA-WATCH for Healthcare Industry - для оценки соответствия требованиям стандарта HIPAA (US Healthcare Insurance Portability and Accountability Act), актуальных в основном для медицинских учреждений, работающих на территории США;
- ✓ RiskWatch RW17799 for ISO 17799 - для оценки соответствия ИС требованиям стандарта международного стандарта ISO 17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются ожидаемые годовые потери (Annual Loss Expectancy, ALE) и оценка возврата инвестиций (Return on Investment, ROI). RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. В основе продукта RiskWatch находится методика анализа рисков, которая состоит из четырех этапов [19].

Методика Microsoft. Проведение оценки рисков в соответствии с методикой Microsoft

Процесс управления рисками, предлагаемый корпорацией Майкрософт, разбивает этап оценки рисков на следующие три шага [19]:

1. ***Планирование***. Разработка основы для успешной оценки рисков.
2. ***Координированный сбор данных***. Сбор информации о рисках в ходе координированных обсуждений рисков.
3. ***Приоритизация рисков***. Ранжирование выявленных рисков на основе непротиворечивого и повторяемого процесса.

Для проведения оценки требуется собрать данные о:

- ✓ Активах организации.
- ✓ Угрозах безопасности.
- ✓ Уязвимостях.

- ✓ Текущей среде контроля (прим. в принятой авторами перевода руководства терминологии средства и меры защиты информации называются элементами контроля, соответственно, среда контроля - совокупность элементов).
- ✓ Предлагаемые элементы контроля.

Активами считается все, что представляет ценность для организации. К материальным активам относится физическая инфраструктура (например, центры обработки данных, серверы и имущество). К нематериальным активам относятся данные и другая ценная для организации информация, хранящаяся в цифровой форме (например, банковские транзакции, расчеты платежей, спецификации и планы разработки продуктов).

Процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, определяет следующие три качественных класса активов [19]:

✓ ***высокое влияние на бизнес (ВВБ)*** - влияние на конфиденциальность, целостность и доступность этих активов может причинить организации значительный или катастрофический ущерб. Например, к этому классу относятся конфиденциальные деловые данные.

✓ ***среднее влияние на бизнес (СВБ)*** - влияние на конфиденциальность, целостность и доступность этих активов может причинить организации средний ущерб. Средний ущерб не вызывает значительных или катастрофических изменений, однако нарушает нормальную работу организации до такой степени, что это требует проактивных элементов контроля для минимизации влияния в данном классе активов. К этому классу могут относиться внутренние коммерческие данные, такие как перечень сотрудников или данные о заказах предприятия.

✓ ***низкое влияние на бизнес (НВБ)*** - активы, не попадающие в классы ВВБ и СВБ, относятся к классу НВБ. К защите подобных активов не выдвигаются формальные требования, и она не требует дополнительного контроля, выходящего за рамки стандартных рекомендаций по защите инфраструктуры. Например, это могут быть общие сведения о структуре организации.

Далее определяется перечень угроз и уязвимостей и выполняется оценка уровня потенциального ущерба, называемого степенью подверженности актива воздействию. Оценка ущерба может проводиться по различным категориям:

- ✓ конкурентное преимущество.
- ✓ законы и регулятивные требования.
- ✓ операционная доступность.
- ✓ репутация на рынке.

Оценку предлагается проводить по следующей шкале:

- ✓ ***высокая подверженность воздействию***. Значительный или полный ущерб для актива.
- ✓ ***средняя подверженность воздействию***. Средний или ограниченный ущерб.
- ✓ ***низкая подверженность воздействию***. Незначительный ущерб или отсутствие такового.

Следующий шаг - оценка частоты возникновения угроз:

- ✓ ***высокая***. Вероятно возникновение одного или нескольких событий в пределах года.
- ✓ ***средняя***. Влияние может возникнуть в пределах двух-трех лет.
- ✓ ***низкая***. Возникновение влияния в пределах трех лет маловероятно.

Данные собираются в приведенный ниже шаблон (рис. 10.1).

Для угроз указывается уровень воздействия в соответствии с концепцией многоуровневой защиты (уровни - физический, сети, хоста, приложения, данных) [19].

Шаблон сбора данных

Определите активы, за разработку, поддержку, управление и сопровождение которых несет ответственность ваша группа

Название актива	Классификация актива (высокое, среднее или низкое влияние на деятельность)
1.	

Для каждого актива укажите следующие значения

Многоуровневая защита	Чего необходимо избежать (угрозы)	Пути возникновения (уязвимости)	Уровень подверженности воздействию (В, С, Н)	Описания текущих элементов контроля	Вероятность (В, С, Н)	Назначение контроля, потенциальные новые
Физический уровень						
Приложения						
Узлы						
Сеть						
Данные						

Рис. 10.1. Снимок экрана шаблона

В столбце текущие элементы контроля описываются использующиеся средства и меры защиты, противостоящие данной угрозе. На основе собранных данных заполняется таблица, пример которой представлен на рис. 10.2.

Актив				Подверженность воздействию			
Дата обнаружения	Название актива	Класс актива	Применимые уровни многоуровневой защиты	Описание угрозы	Описание уязвимости	Уровень подверженности воздействию (В, С, Н)	Уровень влияния (В, С, Н)
Дата	Информация о финансовых инвестициях заказчиков	ВВБ	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых компьютеров локальной сети вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	С	В
Дата	Информация о финансовых инвестициях заказчиков	ВВБ	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых удаленных компьютеров вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	С	В
Дата	Информация о финансовых инвестициях заказчиков	ВВБ	Данные	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных доверенным сотрудником с помощью подслушивания, методов социальной инженерии и других методов без использования технических средств	Н	С

Рис. 10.2. Пример заполненного шаблона

Следующий шаг этапа оценки рисков - приоритизация рисков, т.е. создание упорядоченного по приоритетам списка рисков. Формирование данного списка сначала предлагается выполнить на обобщенном уровне, после чего описания наиболее существенных рисков детализируются [19].

Исходя из значения класса актива и оценки подверженности актива воздействию по таблице приведенной на рис. 10.3. определяется уровень влияния.

		Образец подверженности воздействию		
Класс актива	Выс.	Средн.	Выс.	Выс.
	Средн.	Низк.	Средн.	Выс.
	Низк.	Низк.	Низк.	Средн.
		Низк.	Средн.	Выс.
		Уровень подверженности воздействию		

Рис. 10.3. Определение уровня влияния по классу актива и уровню подверженности воздействию

Итоговый уровень риска определяется исходя из уровня влияния и оценки частоты возникновения риска, для которой используется шкала:

- ✓ ***Высокая***. Вероятно возникновение одного или нескольких влияний в течение года;
- ✓ ***Средняя***. Влияние может хотя бы один раз возникнуть в течение двух или трех лет;

✓ ***Низкая***. Возникновение влияния в течение трех лет маловероятно.

Рис. 10.4. Определение итогового уровня риска

Полученные оценки заносятся в таблицу, пример которой приведен на рис. 10.5.

Для детального изучения (составления "перечня на уровне детализации") отбираются риски, отнесенные по результатам оценки на обобщенном уровне к одной из трех групп:

✓ риски высокого уровня;

✓ граничные риски: риски среднего уровня, которые необходимо снижать;

✓ противоречивые риски: риск является новым и знаний об этом риске у организации недостаточно или различные заинтересованные лица оценивают этот риск по-разному.

Формирование перечня рисков на уровне детализации является последней задачей процесса оценки рисков. В этом перечне каждому риску в итоге сопоставляется оценка в числовой (денежной) форме.

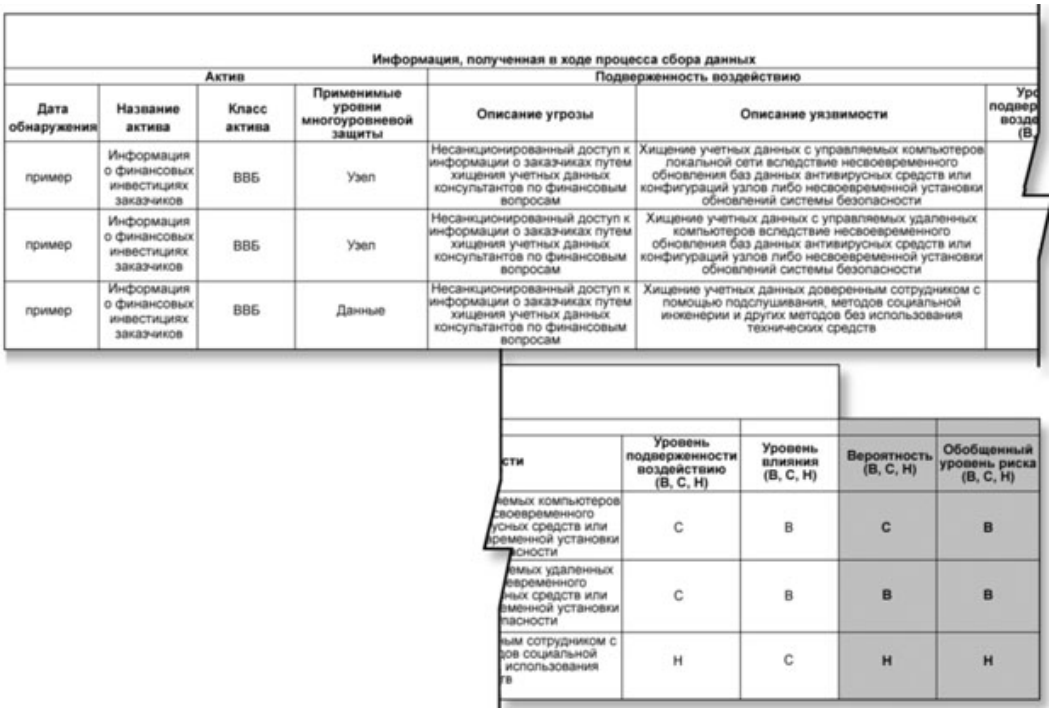
Вновь определяются:

✓ величина влияния и подверженности воздействию;

✓ текущие элементы контроля;

✓ вероятности влияния;

✓ уровень риска.



Информация, полученная в ходе процесса сбора данных						
Актив				Подверженность воздействию		
Дата обнаружения	Название актива	Класс актива	Применимые уровни многоуровневой защиты	Описание угрозы	Описание уязвимости	Ур подвер возде (В,
пример	Информация о финансовых инвестициях заказчиков	ВВБ	Узел	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых компьютеров локальной сети вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	
пример	Информация о финансовых инвестициях заказчиков	ВВБ	Узел	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых удаленных компьютеров вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	
пример	Информация о финансовых инвестициях заказчиков	ВВБ	Данные	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных доверенным сотрудником с помощью подслушивания, методов социальной инженерии и других методов без использования технических средств	

сти	Уровень подверженности воздействию (В, С, Н)	Уровень влияния (В, С, Н)	Вероятность (В, С, Н)	Обобщенный уровень риска (В, С, Н)
емых компьютеров своевременного урных средств или временной установки асности	С	В	С	В
емых удаленных евременного ных средств или еменной установки пасности	С	В	В	В
ым сотрудником с дов социальной использования тв	Н	С	Н	Н

Рис. 10.5. Пример перечня рисков на обобщенном уровне

Уровень подверженности воздействию оценивается по пятибалльной шкале. Шкала для угрозы целостности и конфиденциальности приведена на рис. 10.6. Для угрозы отказа в обслуживании – на рис. 10.7. В качестве итогового уровня подверженности воздействию предлагается выберите максимальное значение [19].

Уровень подверженности воздействию	Конфиденциальность или целостность актива
5	Серьезные повреждения или полный выход актива из строя (например, видимые снаружи и влияющие на прибыльность или успешность ведения бизнеса)
4	Серьезные повреждения, не приводящие к полному выходу актива из строя (например, влияющие на прибыльность или успешность ведения бизнеса и, возможно, видимые снаружи)
3	Средние повреждения или ущерб (например, влияющие на внутренние рекомендации по ведению бизнеса и способные вызвать увеличение эксплуатационных затрат или уменьшение доходов)
2	Незначительные повреждения или ущерб (например, влияющие на внутренние рекомендации по ведению бизнеса, но не вызывающие существенного роста затрат)
1	Небольшие изменения в активе или отсутствие изменений

Рис. 10.6. Уровни подверженности воздействию для угроз конфиденциальности и целостности

Уровень подверженности воздействию	Дата выпуска	Описание
5	Прекращение работы	Большие эксплуатационные затраты или нарушение коммерческих обязательств
4	Прерывание работы	Значительное увеличение эксплуатационных затрат или задержка при выполнении коммерческих обязательств
3	Задержки в работе	Заметное влияние на величину эксплуатационных затрат и производительность.
2	Отвлечение от работы	Измеримое влияние на деятельность компании отсутствует; небольшое увеличение эксплуатационных затрат или затрат на инфраструктуру
1	Не влияет на обычный ход бизнес-операций	Измеримое влияние на эксплуатационные затраты, производительность и коммерческие обязательства отсутствует

Рис. 10.7. Уровни подверженности воздействию для доступности

После определения уровня подверженности воздействию производится оценка величины влияния. Каждому уровню подверженности воздействию сопоставляется значение в процентах, отражающее величину ущерба, причиненного активу, и называемое фактором подверженности воздействию. Майкрософт, рекомендует использовать линейную шкалу подверженности воздействию от 100 до 20%, которая может изменяться в соответствии с требованиями организации. Кроме того, каждой величине влияния сопоставляется качественная оценка: высокая, средняя или низкая. На рис. 10.8 показаны возможные значения для каждого класса влияния.

Класс влияния	Значение класса влияния (З)
ВВБ	10
СВБ	5
НВБ	2

Уровень подверженности воздействию	Фактор подверженности воздействию (ФПВ)	Уровень влияния (З * ФПВ)	Диапазон влияния	Обобщенное сравнение
5	100%		7 - 10	Выс.
4	80%		4 - 6	Средн.
3	60%		0 - 3	Низк.
2	40%			
1	20%			

Рис. 10.8. Определение величин влияния

Далее описываются "элементы контроля", используемые в организации для снижения вероятностей угроз и уязвимостей, определенных в формулировке влияния.

Следующая задача - определение вероятности влияния. Результирующий уровень вероятности определяется на основании двух значений. Первое значение определяет вероятность существования уязвимости в текущей среде. Второе значение определяет вероятность существования уязвимости исходя из эффективности текущих элементов контроля. Каждое значение изменяется в диапазоне от 1 до 5. Определение оценки проводится на основе ответов на вопросы, перечень которых представлен на рис. 10.9, с последующим переходом к результирующей оценке (рис. 10.10). При этом разработчики руководства указывают, что оценка вероятности взлома имеет субъективный характер и предлагают при проведении оценки уточнять приведенный перечень.

Определения вероятностей для уязвимостей
Высокая
Большое число злоумышленников — любители и компьютерные хулиганы
Удаленное выполнение
Возможность использования анонимного доступа
Общеизвестный метод взлома
Автоматизированность
5, если выполняется хотя бы одно из условий
Средняя
Среднее число злоумышленников — специалисты и эксперты
Невозможность удаленного выполнения
Необходимость наличия привилегий уровня пользователя
Метод взлома не является общеизвестным
Атака не автоматизирована
3, если выполняется хотя бы одно из условий
Низкая
Небольшое число злоумышленников — необходима внутренняя информация
Невозможность удаленного выполнения
Необходимость наличия привилегий уровня администратора
Метод взлома не является общеизвестным
Атака не автоматизирована
1, если выполняются все условия

Рис. 10.9. Оценка уязвимости

Результирующая оценка уязвимости	
Атрибуты подверженности воздействию (выберите из числа указанных выше)	
высокая	5
средняя	3
низкая	1
уровень вероятности (1, 3 или 5)	

Рис. 10.10. Оценка уровня вероятности

Рис. 10.11 приведена шкала оценки эффективности текущих мер и средств защиты. Меньший результат означает большую эффективность элементов контроля и их способность уменьшать вероятность взлома.

Насколько эффективны текущие элементы контроля?	
Да — 0, Нет — 1	
Эффективно ли определена и реализована ответственность?	1,0
Эффективно ли осуществляется информирование?	1,0
Эффективно ли определены и реализованы процессы?	1,0
Эффективно ли существующие технологии или элементы контроля снижают угрозы?	1,0
Обеспечивают ли существующие методы аудита обнаружение злоупотреблений и недостатка контроля?	1,0
Сумма атрибутов контроля (0–5) =	

Рис. 10.11. Оценка эффективности текущего контроля

Полученные значения суммируются и заносятся в шаблон для уровня детализации.

Сумма уровней уязвимости и эффективности контроля (0–10) =	

Рис.10.12. Результирующая оценка

Пример заполненного шаблона представлен на рис. 10.13.

Примечание. Рисунок взят из перевода описания, в который закралась неточность - в предпоследнем столбце первой строки следует читать "Уязвимость: 5, Контроль: 1", в предпоследнем столбце второй строки - "Уязвимость: 5, Контроль: 5" [19].

Базовый риск (текущий)									
Актив		Подверженность воздействию							
Название актива	Уровень класса влияния	Многоуровневая защита	Описание угрозы	Описание уязвимости	Уровень подверженности воздействию (1–5)	Уровень подверженности воздействию (1–10)	Описания текущих элементов контроля	Уровень вероятности с контролем (1–10)	Уровень риска с контролем (0–100)
Информация о финансовых инвестициях заказчиков	10 (ВВБ)	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых компьютеров локальной сети вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	4 (80%)	8	1. Каждый консультант имеет доступ только к информации о своих клиентах. Таким образом, подверженность воздействию составляет менее 100%. 2. Уведомления об обновлениях и исправлениях, отправляемые по электронной почте. 3. В локальной сети каждые несколько часов выполняется установка требуемых обновлений, что уменьшает временной интервал, в течение которого узлы локальной сети уязвимы перед взломом.	Уязвимость: 5 Контроль: 1 Всего = 6	48
Информация о финансовых инвестициях заказчиков	10 (ВВБ)	Узлы	Несанкционированный доступ к информации о заказчиках путем хищения учетных данных консультантов по финансовым вопросам	Хищение учетных данных с управляемых удаленных компьютеров вследствие несвоевременного обновления баз данных антивирусных средств или конфигураций узлов либо несвоевременной установки обновлений системы безопасности	4 (80%)	8	1. Каждый консультант имеет доступ только к информации о своих клиентах. Таким образом, подверженность воздействию составляет менее 100%. 2. Уведомления об обновлениях и исправлениях, отправляемые по электронной почте. — Отсутствует решение, позволяющее обеспечить соответствие требованиям за пределами локальной сети.	Контроль: 5 Всего = 10	80

Рис. 10.13. Перечень рисков на уровне детализации (SRMGTool3)

На приведенном выше рисунке показаны уровни риска и соответствующие элементы данных. Уровень риска определяется как произведение оценок уровня влияния (со значением от 1 до 10) и уровня вероятности (со значением от 0 до 10). В результате уровень риска может принимать значения от 0 до 100. Переход от числовой оценки к оценке по шкале "высокий", "средний" или "низкий" можно сделать в соответствии с таблицей, представленной на рис. 10.14.

В заключение процедуры оценки рисков, проводится количественный анализ. Чтобы определить количественные характеристики, необходимо выполнить следующие задачи [19]:

- ✓ сопоставить каждому классу активов в организации денежную стоимость.
- ✓ определить стоимость актива для каждого риска.
- ✓ определить величину ожидаемого разового ущерба (single loss expectancy - SLE).
- ✓ определить ежегодную частоту возникновения (annual rate of occurrence - ARO).

✓ определить ожидаемый годовой ущерб (annual loss expectancy - ALE).

Уровень влияния × Уровень вероятности = Уровень риска			
Диапазоны уровня влияния		Диапазоны вероятности	
Выс.	10 -- 7	10 -- 7	
Средн.	6 -- 4	6 -- 4	
Низк.	3 -- 0	3 -- 0	

Влияние												
В	10	0	10	20	30	40	50	60	70	80	90	100
	9	0	9	18	27	36	45	54	63	72	81	90
	8	0	8	16	24	32	40	48	56	64	72	80
	7	0	7	14	21	28	35	42	49	56	63	70
	6	0	6	12	18	24	30	36	42	48	54	60
С	5	0	5	10	15	20	25	30	35	40	45	50
	4	0	4	8	12	16	20	24	28	32	36	40
	3	0	3	6	9	12	15	18	21	24	27	30
	2	0	2	4	6	8	10	12	14	16	18	20
Н	1	0	1	2	3	4	5	6	7	8	9	10
		0	1	2	3	4	5	6	7	8	9	10
		Н					С					В
							Вероятность					

Общий риск	Уровень риска
	Выс.
	Средн.
	Низк.

Рис. 10.14. Результирующее качественное ранжирование

Количественную оценку предлагается начать с активов, соответствующих описанию класса ВВБ. Для каждого актива определяется денежная стоимость с точки зрения его материальной и нематериальной ценности для организации. Также учитывается:

✓ стоимость замены.

✓ затраты на обслуживание и поддержание работоспособности.

✓ затраты на обеспечение избыточности и доступности.

✓ влияние на репутацию организации.

✓ влияние на эффективность работы организации.

✓ годовой доход.

✓ конкурентное преимущество.

✓ внутренняя эффективность эксплуатации.

✓ правовая и регулятивная ответственность.

✓ процесс повторяется для каждого актива в классах СВБ и НВБ.

Каждому классу активов сопоставляется одно денежное значение, которое будет представлять ценность класса активов. Например, наименьшее среди активов данного класса. Данный подход уменьшает затраты времени на обсуждение стоимости конкретных активов.

После определения стоимостей классов активов необходимо определить и выбрать стоимость каждого риска.

Следующей задачей является определение степени ущерба, который может быть причинен активу. Для расчетов предлагается использовать ранее определенный уровень подверженности воздействию, на основе которого определяется фактор подверженности

воздействию (рекомендуемая формула пересчета - умножение значения уровня (в баллах) на 20%).

Последний шаг состоит в получении количественной оценки влияния путем умножения стоимости актива на фактор подверженности воздействию. В классической количественной модели оценки рисков это значение называется величиной ожидаемого разового ущерба (SLE). На рис. 10.15 приведен пример реализации такого подхода.

Величина высокого влияния на деятельность = $ M			Уровень подверженности воздействию	Фактор подверженности воздействию, %
			5	100
Класс актива			4	80
Значение ВВБ	$ M		3	60
Значение СВБ	$ M/2		2	40
Значение НВБ	$ M/4		1	20
Оценочное значение риска =	Значение класса актива × Фактор подверженности воздействию (%) = Ожидаемый разовый ущерб			

Рис. 10.15. Количественная оценка ожидаемого разового ущерба

Описание риска	Значение класса актива	Уровень подверженности воздействию	Величина подверженности воздействию	Ожидаемый разовый ущерб
Риск для узла локальной сети	$ 10	4	80%	$ 8
Риск для удаленного узла	$ 10	4	80%	$ 8

Рис. 10.16. Пример определения ожидаемого разового ущерба (суммы указаны в миллионах долларов)

Далее делается оценка ежегодной частоты возникновения (ARO). В процессе оценки ARO используются ранее полученные качественные оценки рис. 10.17.

Качественный уровень	Описание	Диапазон ежегодной частоты возникновения	Примеры описаний
Высокий	Очень вероятно	>= 1	Влияние раз в год или чаще
Средний	Вероятно	От 0,99 до 0,33	Не менее одного раза каждые 1–3 года
Низкий	Маловероятно	< 0,33	Реже, чем один раз в 3 года

Рис. 10.17. Количественная оценка ежегодной частоты возникновения

Для определения ожидаемого годового ущерба (ALE) значения SLE и ARO перемножаются.

$$ALE = SLE \times ARO$$

Величина ALE характеризует потенциальные годовые убытки от риска. Хотя данный показатель может помочь в оценке ущерба заинтересованным лицам, имеющим финансовую подготовку, группа управления рисками безопасности должна напомнить, что

влияние на организацию не ограничивается величиной годовых издержек - возникновение риска может повлечь за собой причинение ущерба в полном объеме.

Подводя итог, можно еще раз отметить, что процесс управления рисками безопасности, предлагаемый корпорацией Майкрософт, использует комбинированный подход включающий оценку рисков на качественном уровне на начальном этапе и количественную оценку - на заключительном [19].

ПРАКТИЧЕСКАЯ ЧАСТЬ

В ходе данной лабораторной работы мы познакомимся с разработанной Microsoft программой для самостоятельной оценки рисков, связанных с безопасностью - Microsoft Security Assessment Tool (MSAT). Она бесплатно доступна на сайте Microsoft по ссылке http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=cd057d9d-86b9-4e35-9733-7acb0b2a3ca1. [19]

В ходе работы, пользователь, выполняющий роль аналитика, ответственного за вопросы безопасности, отвечает на две группы вопросов.

Первая из них посвящена бизнес-модели компании, и призвана оценить риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Создается так называемый профиль риска для бизнеса (ПРБ).

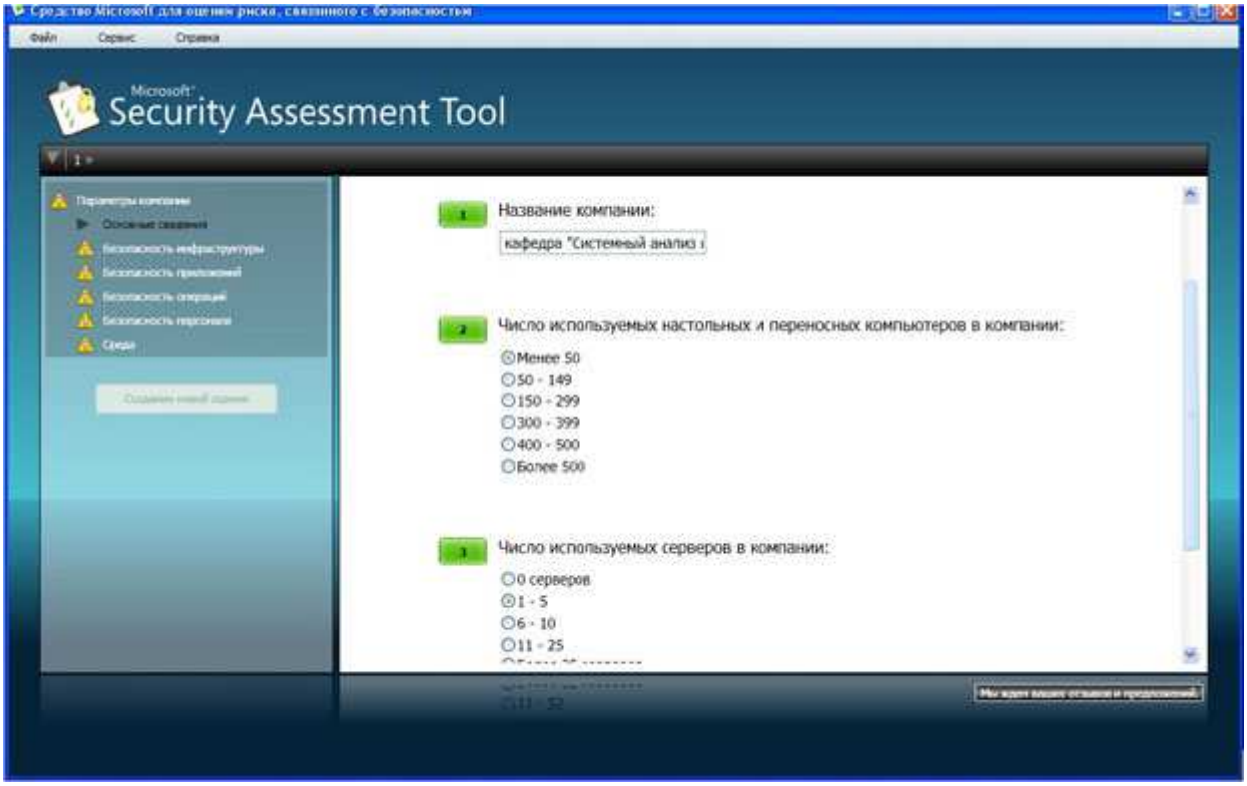


Рис. 10.18. Информация о компании

Вопросы этого этапа разбиты на 6 групп. Первая (рис. 10.18) касается общих сведений о компании - название, число компьютеров, серверов и т.д. Вторая группа

вопросов озаглавлена "Безопасность инфраструктуры". Примеры вопросов - "использует ли компания подключение к Интернет", "размещаются ли службы, используемые как внешними, так и внутренними клиентами, в одном и том же сегменте" и т.д. Остальные группы - "Безопасность приложений", "Безопасность операций", "Безопасность персонала", "Среда".

Надо отметить, что при локализации не все вопросы первого этапа были качественно переведены с английского. Чего стоит вопрос: "Прошла ли ваша организация через "копирование и замена" касающиеся любого основного компонента технологии, за последние 6 месяцев ?"! Однако во всех случаях можно из контекста понять, о чем идет речь (в приведенном примере вопрос был, относительно того, менялись ли используемые технологии обработки информации).

Когда проведен первый этап оценки, полученная информация обрабатывается (для этого требуется подключение к Интернет), после чего начинается второй этап анализа. Для технических специалистов он будет более интересен, т.к. касается используемых в компании политик, средств и механизмов защиты (рис. 10.19). Стоит сказать, что и перевод вопросов второго этапа выполнен существенно лучше.

Рис. 10.19. Анализ используемых механизмов защиты

Вопросы организованы в соответствии с концепцией многоуровневой (эшелонированной) защиты. Сначала рассматривается защита инфраструктуры (защита периметра, аутентификация…), затем вопросы защиты на уровне приложений, далее проводится анализ безопасности операций (определена ли политика безопасности,

политика резервного копирования и т.д.), последняя группа вопросов касается работы с персоналом (обучение, проверка при приеме на работу и т.д.).

Во многом тематика вопросов соответствует разделам стандартов ISO 17799 и 27001, рассмотренных в теоретической части курса.

После ответа на все вопросы программа вновь обращается к удаленному серверу и генерирует отчеты. Наибольший интерес для технических специалистов представляет "Полный отчет". В частности, он содержит предлагаемый список приоритетных действий. Фрагмент списка представлен в табл. 10.1

Таблица 10.1. Список предлагаемых действий

Список приоритетных действий	
Предмет анализа	**Рекомендация**
Высокий приоритет	
Операции > Управление средствами исправления и обновления > Управление средствами исправления	Наличие политики исправлений и обновлений для операционных систем является полезным начальным шагом, однако необходимо разработать такую же политику и для приложений. Разработайте такую политику, пользуясь сведениями, доступными в разделе, посвященном передовым методикам. Сначала установите исправления для внешних приложений и приложений Интернета, затем для важных внутренних приложений и, наконец, для не особо важных приложений.

Задание. На основе представленного материала опишите политику безопасности предприятия, модель которого разрабатывалась вами в теме курсовой работы прошлого семестра (особенности организации процесса защиты информации, применяемые методы и средства). С помощью программы MSAT проведите оценку рисков для предприятия.

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Назовите методики для оценки рисков по уровню?
2) Опишите особенности методики CRAMM?
3) Опишите особенности методики FRAP?
4) Опишите особенности методики OCTAVE?
5) Опишите особенности методики Microsoft?
6) Каким образом можно оценить возможные потери от нарушения информационной безопасности?
7) Каким образом определить величину ожидаемого разового ущерба SLE?

8) По какой формуле определяется ожидаемый годовой ущерб ALE?

9) Каким образом определить ежегодную частоту возникновения ARO?

10) Каким образом определяется класс влияния актива на бизнес?

ЛАБОРАТОРНАЯ РАБОТА № 11

Разработка плана аудита информационной безопасности

Цель: разработать план аудита информационной безопасности организации на основе стандартов информационной безопасности и типа организации;

Оборудование: компьютеры с доступом к сети Интернет;

Форма проведения занятия: интерактивное занятие с использованием метода работы в малых группах (2 ч);

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Аудит информационной безопасности — системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности [20].

Информационная безопасность — состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере [20].

Виды и цели аудита

Различают внешний и внутренний аудит.

Внешний аудит — это, как правило, разовое мероприятие, проводимое по инициативе руководства организации или акционеров. Внешний аудит рекомендуется (а для ряда финансовых учреждений и акционерных обществ требуется) проводить регулярно.

Внутренний аудит представляет собой непрерывную деятельность, которая осуществляется на основании документа, обычно носящего название “Положение о внутреннем аудите“, и в соответствии с планом, подготовка которого осуществляется подразделением внутреннего аудита и утверждается руководством организации. Аудит безопасности информационных систем является одной из составляющих ИТ—аудита.

Как правило, наиболее общими ***целями проведения аудита*** безопасности являются:

✓ анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;

- ✓ оценка текущего уровня защищенности ИС;
- ✓ локализация узких мест в системе защиты ИС;
- ✓ оценка соответствия ИС существующим стандартам в области информационной безопасности;
- ✓ выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС [20].

Однако, цели аудита информационной безопасности могут определяться заказчиком и, исходя из насущных проблем организации, ее специфики, могут быть сформулированы более конкретно:

- ✓ анализ программного обеспечения в компании на наличие лицензий;
- ✓ исследование работоспособности резервных копий;
- ✓ проверка защищенности финансовых программ (клиент-банк, 1С и других);
- ✓ оценка уровня защищенности информационной системы заказчика;
- ✓ выявление и анализ рисков безопасности;
- ✓ обнаружение проблемных мест в информационной системе;
- ✓ оценка соответствия системы стандартам безопасности;
- ✓ подготовка рекомендаций по внедрению новых решений или повышению эффективности существующих;
- ✓ и многое другое [21].

По виду аудита – внутреннему и внешнему – различают и аудиторов. Как правило, внутренние аудиторы – это сотрудники организации, тогда как внешние аудиторы вызываются организацией из специализированных фирм, уполномоченных решать подобные задачи. В число дополнительных задач, стоящих перед внутренним аудитором, помимо оказания помощи внешним аудиторам, могут также входить:

- ✓ разработка политик безопасности и других организационно - распорядительных документов по защите информации и участие в их внедрении в работу организации;
- ✓ постановка задач для ИТ-персонала, касающихся обеспечения защиты информации;
- ✓ участие в обучении пользователей и обслуживающего персонала ИС вопросам обеспечения информационной безопасности;
- ✓ участие в разборе инцидентов, связанных с нарушением информационной безопасности;
- ✓ прочие задачи [20].

Основные этапы аудита безопасности

Работы по аудиту безопасности ИС включают в себя ряд последовательных этапов, которые в целом соответствуют этапам проведения комплексного ИТ—аудита автоматизированной системы, включающего в себя:

- ✓ инициирование процедуры аудита;
- ✓ сбор информации аудита;
- ✓ анализ данных аудита;
- ✓ выработку рекомендаций;
- ✓ подготовку аудиторского отчета.

На этапе ***инициирования процедуры аудита*** должны быть решены следующие организационные вопросы [20]:

1) права и обязанности аудитора должны быть четко определены и документально закреплены в его должностных инструкциях, а также в положении о внутреннем (внешнем) аудите;

2) аудитором должен быть подготовлен и согласован с руководством план проведения аудита;

3) в положении о внутреннем аудите должно быть закреплено, в частности, что сотрудники компании обязаны оказывать содействие аудитору и предоставлять всю необходимую для проведения аудита информацию.

На этапе инициирования процедуры аудита должны быть определены границы проведения обследования. План и границы проведения аудита обсуждаются на рабочем собрании, в котором участвуют аудиторы, руководство компании и руководители структурных подразделений [20].

Этап ***сбора информации аудита*** является наиболее сложным и длительным. Это связано в основном с отсутствием необходимой документации на информационную систему и с необходимостью плотного взаимодействия аудитора со многими должностными лицами организации [20].

Компетентные выводы относительно положения дел в компании с информационной безопасностью могут быть сделаны аудитором только при условии наличия всех необходимых исходных данных для анализа. Первый пункт аудиторского обследования начинается с получения информации об организационной структуре пользователей ИС и обслуживающих подразделений. Назначение и принципы функционирования ИС во многом определяют существующие риски и требования безопасности, предъявляемые к системе. Далее, аудитору требуется более детальная информация о структуре ИС. Это позволит уяснить, каким образом осуществляется распределение механизмов безопасности по структурным элементам и уровням функционирования ИС.

Используемые аудиторами методы анализа данных определяются выбранными подходами к проведению аудита, которые могут существенно различаться.

Первый подход, самый сложный, базируется на анализе рисков. Опираясь на методы анализа рисков, аудитор определяет для обследуемой ИС индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной ИС, среды ее функционирования и существующие в данной среде угрозы безопасности [20].

Второй подход, самый практичный, опирается на использование стандартов информационной безопасности. Стандарты определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Стандарты могут определять разные наборы требований безопасности, в зависимости от уровня защищенности ИС, который требуется обеспечить, ее принадлежности (коммерческая организация либо государственное учреждение), а также назначения (финансы, промышленность, связь и т. п.). От аудитора в данном случае требуется правильно определить набор требований стандарта, соответствие которым нужно обеспечить [20].

Третий подход, наиболее эффективный, предполагает комбинирование первых двух. Базовый набор требований безопасности, предъявляемых к ИС, определяется стандартом. Дополнительные требования, в максимальной степени учитывающие особенности функционирования данной ИС, формируются на основе анализа рисков [20].

Рекомендации, выдаваемые аудитором по результатам анализа состояния ИС, определяются используемым подходом, особенностями обследуемой ИС, состоянием дел с информационной безопасностью и степенью детализации, используемой при проведении аудита. В любом случае, рекомендации аудитора должны быть конкретными и применимыми к данной ИС, экономически обоснованными, аргументированными (подкрепленными результатами анализа) и отсортированными по степени важности. При этом мероприятия по обеспечению защиты организационного уровня практически всегда имеют приоритет над конкретными программно-техническими методами защиты. В то же время наивно ожидать от аудитора, в качестве результата проведения аудита, выдачи технического проекта подсистемы информационной безопасности, либо детальных рекомендаций по внедрению конкретных программно-технических средств защиты информации. Это требует более детальной проработки конкретных вопросов организации защиты, хотя внутренние аудиторы могут принимать в этих работах самое активное участие [20].

Аудиторский отчет является основным результатом проведения аудита. Его качество характеризует качество работы аудитора. Он должен, по крайней мере, содержать

описание целей проведения аудита, характеристику обследуемой ИС, указание границ проведения аудита и используемых методов, результаты анализа данных аудита, выводы, обобщающие эти результаты и содержащие оценку уровня защищенности АС или соответствие ее требованиям стандартов, и, конечно, рекомендации аудитора по устранению существующих недостатков и совершенствованию системы защиты [20].

ПРАКТИЧЕСКАЯ ЧАСТЬ

На основании теоретического материала, ресурсов сети Интернет необходимо разработать план проведения аудита. При выполнении данной лабораторной работы, необходимы компетенции, полученные при изучении стандартов информационной безопасности и оценке рисков организации. На основании этих компетенций план аудита, может быть составлен в соответствии с третьим подходом, описанным в теоретической части данной работы.

За основу для составления плана аудита можно использовать типовые решения, например, на сайте http://efsol.ru/it-services/restaurant.html.

Работа организуется следующим образом:

1) группа разбивается на 2 или 4 команды (в зависимости от числа человек в академической группе);

2) одна команда является представителями организации, заказывающей аудит. Вторая команда – внешними аудиторами.

3) Команда-организация должна выбрать внутреннего аудитора, разработать организационную структуру своей организации, описать структуру используемых ИС и прочих технических особенностей; Сформулировать проблему и представить цели аудита команде аудиторов;

4) Команда аудиторов тем временем изучает необходимый стандарт информационной безопасности и готовит план аудита. В план аудита нужно включить набор требований, на соответствие которых нужно проверить работу ИС организации.

5) План аудита предоставляется команде-организации и согласуется с ними;

6) Далее «проводится» аудит на основе подготовленного плана

7) Затем команды меняются местами;

8) Преподаватель оценивает работу команд, организует обсуждение занятия (его плюсы и минусы).

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

9) Какие виды аудита информационной безопасности различают?

10) Каковы цели аудита информационной безопасности?
11) Каковы основные этапы аудита информационной безопасности?
12) Какие подходы к проведению аудита существуют и в чем их особенности?
13) Что является результатом аудита информационной безопасности?
14) Чем общая формулировка целей аудита может отличаться от целей, поставленных заказчиком аудита?

ЛАБОРАТОРНАЯ РАБОТА № 12
Анализ внутренней сети

Цель работы: получить навык проведения анализа локальной сети для формирования политики безопасности предприятия.

Оборудование: компьютер с операционной системой Windows, наличие системной утилиты 10-Strike LanState Pro, наличие доступа к ресурсам глобальной сети Internet.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Роль анализа рисков для создания корпоративной системы защиты информации в компьютерной сети предприятия можно наглядно показать на примере модели Lifecycle Security (название можно перевести как "жизненный цикл безопасности"), разработанной компанией Axent, впоследствии приобретенной Symantec [22].

Lifecycle Security - это обобщенная схема построения комплексной защиты компьютерной сети предприятия. Выполнение описываемого в ней набора процедур позволяет системно решать задачи, связанные с защитой информации, и дает возможность оценить эффект от затраченных средств и ресурсов. С этой точки зрения, идеология Lifecycle Security может быть противопоставлена тактике "точечных решений", заключающейся в том, что все усилия сосредотачиваются на внедрении отдельных частных решений (например, межсетевых экранов или систем аутентификации пользователей по смарт-картам). Без предварительного анализа и планирования, подобная тактика может привести к появлению в компьютерной системе набора разрозненных продуктов, которые не стыкуются друг с другом и не позволяют решить проблемы предприятия в сфере информационной безопасности.

Lifecycle Security включает в себя 7 основных компонентов, которые можно рассматривать как этапы построения системы защиты (рис. 12.1).

Рис. 12.1. Компоненты модели LifeCycle Security

Примечание: ***assess risk*** – *оценка риска;* ***design security roadmap*** - *построение политики безопасности;* ***select & implement solutions*** – *принятие и исполнение решений;* ***conduct training*** – *проведение тренингов;* ***monitor security*** – *слежение за безопасностью,* ***implement incident responses & recovery –*** *фиксация воздействий и лечение.*

Перечень выделяемых уровней незначительно различается в различных документах. Возможные варианты представлены на рис. 12.2 [22].

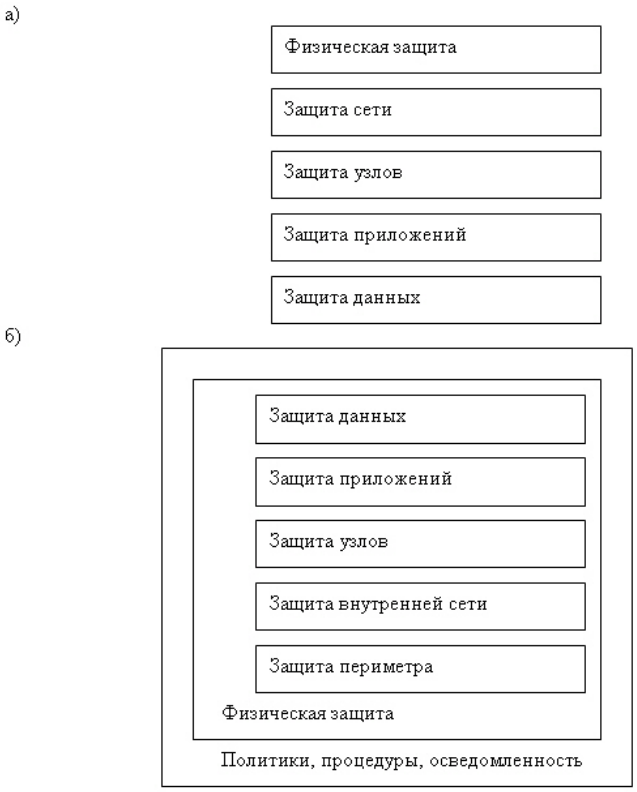


Рис. 12.2. Модель многоуровневой защиты

Политика безопасности должна описывать все аспекты работы системы с точки зрения обеспечения информационной безопасности. Поэтому ***уровень политики***

безопасности можно рассматривать как базовый. Этот уровень также подразумевает наличие документированных организационных мер защиты (процедур) и порядка информирования о происшествиях, обучение пользователей в области информационной безопасности и прочие меры аналогичного характера (например, рекомендуемые стандартом ISO/IEC 17799) [22].

Уровень физической защиты включает меры по ограничению физического доступа к ресурсам системы - защита помещений, контроль доступа, видеонаблюдение и т.д. Сюда же относятся средства защиты мобильных устройств, используемых сотрудниками в служебных целях [22].

Уровень защиты периметра определяет меры безопасности в "точках входа" в защищаемую сеть из внешних, потенциально опасных. Классическим средством защиты периметра является межсетевой экран (англ. термин - firewall), который на основании заданных правил определяет, может ли проходящий сетевой пакет быть пропущен в защищаемую сеть. Другие примеры средств защиты периметра - системы обнаружения вторжений, средства антивирусной защиты для шлюзов безопасности и т.д. [22].

Уровень защиты внутренней сети "отвечает" за обеспечение безопасности передаваемого внутри сети трафика и сетевой инфраструктуры. Примеры средств и механизмов защиты на этом уровне - создание виртуальных локальных сетей (VLAN) с помощью управляемых коммутаторов, защита передаваемых данных с помощью протокола IPSec и т.д. Нередко внутри сети также используют средства, характерные для защиты периметра, например, межсетевые экраны, в том числе и персональные (устанавливаемые на защищаемый компьютер). Связано это с тем, что использование беспроводных сетевых технологий и виртуальных частных сетей (VPN) приводит к "размыванию" периметра сети. Например, если атакующий смог подключиться к точке беспроводного доступа внутри защищаемой сети, его действия уже не будут контролироваться межсетевым экраном, установленным "на границе" сети, хотя формально атака будет производиться с внешнего по отношению к нашей сети компьютера. Поэтому иногда при анализе рассматривают "***уровень защиты сети***", включающий и защиту периметра, и внутренней сети [22].

Следующим на схеме идет ***уровень защиты узлов***. Здесь рассматриваются атаки на отдельный узел сети и, соответственно, меры защиты от них. Может учитываться функциональность узла и отдельно рассматриваться защита серверов и рабочих станций. В первую очередь, необходимо уделять внимание защите на уровне операционной системы - настройкам, повышающим безопасность конфигурации (в том числе, отключению не использующихся или потенциально опасных служб), организации установки исправлений

и обновлений, надежной аутентификации пользователей. Исключительно важную роль играет антивирусная защита [22].

Уровень защиты приложений отвечает за защиту от атак, направленных на конкретные приложения - почтовые серверы, web-серверы, серверы баз данных. В качестве примера можно назвать SQL-инъекции - атаки на сервер БД, заключающиеся в том, что во входную текстовую строку включаются операторы языка SQL, что может нарушить логику обработки данных и привести к получению нарушителем конфиденциальной информации. Сюда же можно отнести модификацию приложений компьютерными вирусами. Для защиты от подобных атак используются настройки безопасности самих приложений, установка обновлений, средства антивирусной защиты [22].

Уровень защиты данных определяет порядок защиты обрабатывающихся и хранящихся в системе данных от несанкционированного доступа и других угроз. В качестве примеров контрмер можно назвать разграничение доступа к данным средствами файловой системы, шифрование данных при хранении и передаче [22].

В процессе идентификации рисков определяется, что является целью нарушителя, и на каком уровне или уровнях защиты можно ему противостоять. Соответственно выбираются и контрмеры. Защита от угрозы на нескольких уровнях снижает вероятность ее реализации, а значит, и уровень риска. Одним из первоочередных действий для создания системы защиты является инвентаризация всех информационных активов организации. Корпоративная сеть является связующим звеном всех компонентов ИС, а значит наиболее целесообразно начинать инвентаризацию информационных активов с анализа внутренней сети. Таким образом, в данном практическом задании мы рассмотрим программный продукт, позволяющий получить данные о составе и топологии сети. ***Топология*** - это физическая конфигурация сети в совокупности с ее логическими характеристиками. Топология - это стандартный термин, который используется при описании основной компоновки сети. В качестве примера в данной практической работе будет использоваться утилита 10-Strike LanState Pro. **10-Strike LANState** - программа для администраторов сетей Microsoft Windows. Полностью функционирует под ОС WINDOWS NT / 2000 / XP / Server 2003 / Vista / 7.

Основное предназначение: строит и отображает в наглядном представлении карту сети с условными обозначениями, связями и областями, с возможностью отслеживания в реальном времени состояния устройств (работает/не работает), состояния портов удаленных машин (открыт/закрыт), состояния различных служб, файлов и т.д. Включает в себя ряд полезных функций для получения информации об удаленных машинах:

- ✓ IP - адреса;

- ✓ MAC - адреса (номера сетевых адаптеров);
- ✓ Текущий пользователь;
- ✓ Принадлежность к домену, серверу;
- ✓ Установленная операционная система;
- ✓ Список дисков;
- ✓ Текущие дата и время;
- ✓ Доступные сетевые ресурсы;
- ✓ Текущие подключения;
- ✓ Системный реестр;
- ✓ Службы и устройства;
- ✓ Учетные записи;
- ✓ Группы пользователей;
- ✓ Открытые порты;
- ✓ Выполняемые процессы;
- ✓ Журналы событий;
- ✓ Полная информация о домене или рабочей группе;
- ✓ Список установленного ПО;
- ✓ SNMP-информация (англ.. *Simple Network Management Protocol* — простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур UDP/TCP. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие).

Позволяет:

- ✓ моделировать в графическом виде локальную сеть, автоматически рисовать условные соединительные линии, области, помещения с названиями и телефонами, а затем сохранять полученный результат в виде карты, графического изображения и выводить на печать;
- ✓ получать разнообразную информацию из сетевых устройств по SNMP-протоколу;
- ✓ отслеживать использование ваших сетевых ресурсов пользователями сети с поддержкой "черного списка";
- ✓ просматривать загруженность вашей сетевой карты (входящий/исходящий трафик);
- ✓ управлять допусками к ресурсам вашего компьютера;
- ✓ пинговать любой компьютер сети (ICMP и TCP);
- ✓ выполнять трассировку маршрутов пакетов в сети;

- ✓ получать имя компьютера по адресу хоста;
- ✓ посылать обычные и анонимные сообщения любому компьютеру сети или группе пользователей;
- ✓ выключать, включать и перезагружать компьютер сети (при соответствующих правах на удаленной машине);
- ✓ осуществлять мониторинг различных сетевых сервисов на удаленных компьютерах, оповещать о событиях выполнением нескольких функций, в том числе отправкой SMS и E-MAIL, перезапуском служб и компьютера;
- ✓ выполнять с устройствами действия через настраиваемое контекстное меню;
- ✓ сканировать сеть по IP-адресам (максимально широкий диапазон);
- ✓ осуществлять поиск устройств в сети и на карте;
- ✓ создавать HTML-отчеты по составу системы удаленных компьютеров (информация о системе).
- ✓ создавать HTML-отчеты по устройствам на карте с отображением их основных сетевых атрибутов (таблица соответствия DNS имен, IP и MAC-адресов);
- ✓ ведение логов доступа к сетевым ресурсам, сигнализации, отправленных/принятых сообщений;
- ✓ открывать и осуществлять навигацию по нескольким картам.

При запуске программы предлагается выбор - строить новую карту сети или открыть существующую. При запуске Мастера построения новой карты надо указать, какая подсеть документируется. При загрузке программы LanState Pro по умолчанию загружается стандартная картина топологии сети (рис. 12.3).

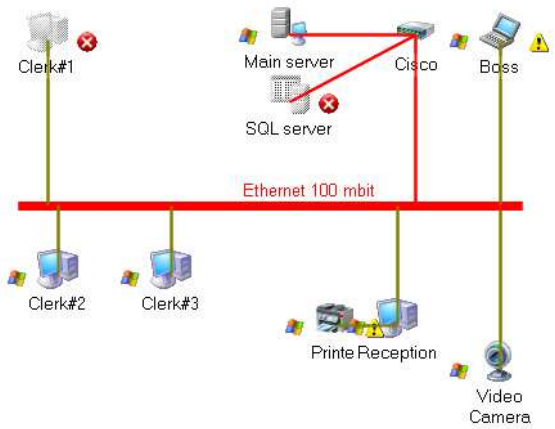


Рис. 12.3. Стандартный пример топологии сети

Описание карты сети на рисунке 12.3: *на рисунке представлена локальная вычислительная сеть Ethernet 100 Мбит/с. В сеть входят четыре рабочих компьютера с*

сетевыми именами Clerk#1, Clerk#2, Clerk#3 и Reception, к которому подключен принтер. Кроме того, в сети имеется ноутбук Boss и сетевая камера. На момент проверки компьютер с именем Clerk#1 был недоступен. Сеть содержит два сервера: главный (Main server) и сервер баз данных (SQL server).. На рисунке также видно наличие коммутатора (свитча) Cisco. Мастер создания топологии сети позволяет строить сеть на основе диапазона IP-адресов или на основе Импорта из ближайшего окружения. При этом необходимо наличие этого окружения, иначе карта сети будет пустой.

На рис. 12.4 показана карта внутренней сети СБИ, полученная путем использования Мастера построения сети. Как видно из рис. 12.4., помимо двух сетевых принтеров в сети имеется принтер, подключенный непосредственно к компьютеру, с которого производилась проверка сети - Xerox Phaser 3100 MFP.

Данная утилита позволяет получать широкий круг отчетов по состоянию сети. Для этого используется пункт меню Отчеты. Для того чтобы узнать имя компьютера по его IP-адресу нужно использовать пункт меню Сервис.

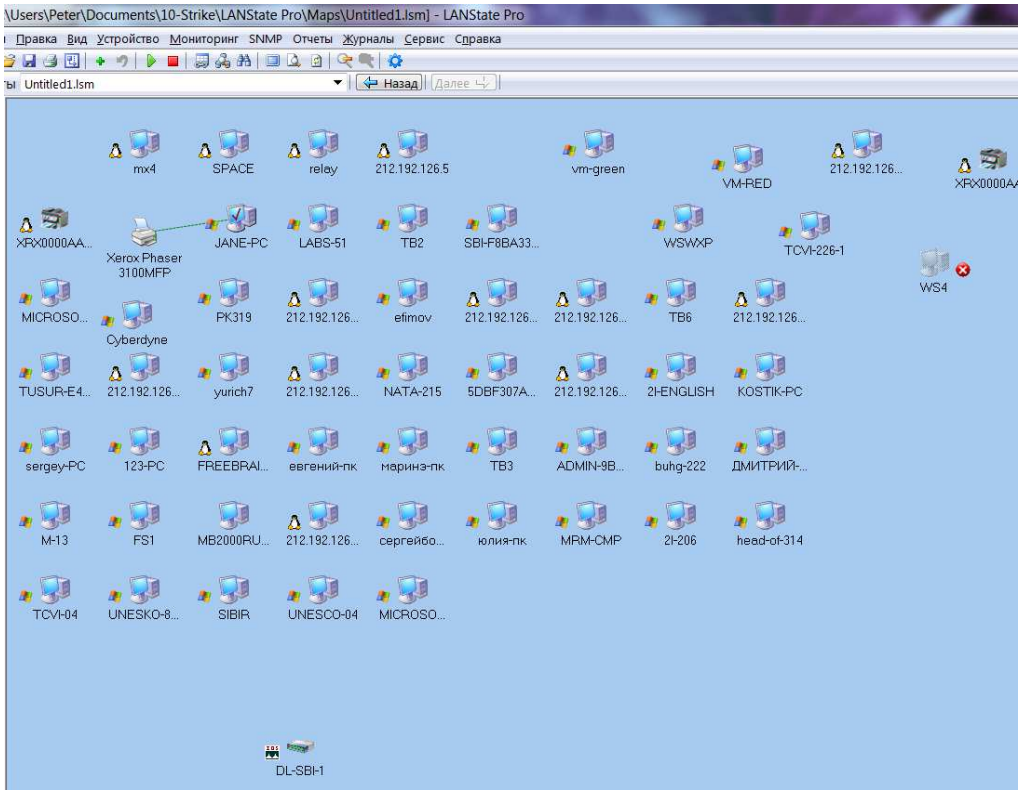
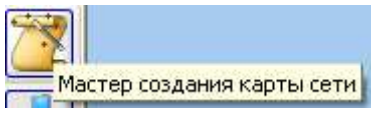


Рис. 12.4. Результат работы Мастера построения новой карты сети во внутренней сети СБИ

ПРАКТИЧЕСКАЯ ЧАСТЬ

1) Запустите утилиту 10-Strike LanState Pro;
2) Постройте карту сети двумя способами:

а) при помощи Мастера создания карты сети 

при этом задать условия сканирования: диапазон в 124 IP-адреса;. Из найденных устройств на карту добавить 20 любых устройств. Сохранить результат в Карта1.

б) при помощи Импорта устройств из сетевого окружения. Опишите в чем отличие этих методов и сохраните карты под разными именами. Сохранить результат в Карта 2.

3) В справке найдите рекомендации для задания наиболее оптимальных параметров поиска устройств;

4) Далее работать с файлом Карта1. Выделить на карте любое устройство и выбрать в контекстном меню пункт Выравнивание. Изучить возможности данного меню. Выровнять полученные компьютеры по таблице и по окружности.

5) Создайте отчет по практическому занятию, в котором укажите:

а) Какие операционные системы установлены на компьютерах сети;

б) Какие общие ресурсы используются в данной сети;

в) Перечислите используемые сетевые устройства и укажите, какие последствия могут возникнуть при выходе из строя (или некорректной работе) каждого из них.

г) Сколько принтеров используется в данной сети, какие из них являются сетевыми?

д) Создайте список устройств карты и сохраните полученный отчет;

е) Создайте отчет о компонентах системы любого рабочего компьютера (в отчете укажите какого) и сохраните его в личную папку;

ж) При помощи пункта меню Сетевой трафик, определите, с каким интерфейсом происходит максимальный обмен пакетами.

з) определите MAC-адрес и IP-адрес компьютера, заданного преподавателем.

и) определите имя и IP-адрес вашего рабочего компьютера.

к) Используя меню Статистика определите Имя карты; Количество объектов на карте; Количество различных типов устройств на карте; Количество отвечающих на пинг устройств; Количество SNMP-устройств.

6. Используя данные сети интернет изучите какие топологии сети существуют и при помощи инструмента 

, создайте эффективную, по вашему мнению, карту сети, объединив компьютеры в группы по определенным функциям.

7 Общий отчет в формате doc, сохраните в личную папку.

8. В отчете приведите примеры, к какому из найденных устройств необходимо применять физический уровень защиты, уровень периметра, узлов, приложений и т.д.

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) В чем заключается смысл понятия Lifecycle Security?
2) К какому уровню защиты относится уровень политики безопасности?
3) Какие меры включает в себя уровень физической защиты?
4) Какие меры включает в себя уровень защиты периметра?
5) Какие меры выполняются на уровне защиты узлов?
6) Какие меры выполняются на уровне защиты внутренней сети?
7) Какие меры входят в уровень защиты данных?
8) Дайте определение топологии сети.
9) Для чего необходимо строить карту сети?

ЛАБОРАТОРНАЯ РАБОТА № 13

Выявление уязвимостей в компьютерных системах и построение локальной политики паролей

Цель работы: получить навык выявления уязвимостей операционной системы и разработки локальной политики паролей.

Оборудование: компьютер с операционной системой Windows, программа Microsoft Baseline Security analyzer, наличие доступа к ресурсам глобальной сети Internet.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Термин «уязвимость» часто упоминается в связи с компьютерной безопасностью, во множестве самых различных контекстов.

В общем случае, уязвимость ассоциируется с нарушением политики безопасности, вызванным неправильно заданным набором правил или ошибкой в обеспечивающей безопасность компьютера программе. Стоит отметить, что теоретически все компьютерные системы имеют уязвимости. Но то, насколько велик потенциальный ущерб от вирусной атаки, использующей уязвимость, позволяет подразделять уязвимости на активно используемые и не используемые вовсе.

Предпринималось много попыток четко определить термин «уязвимость» и разделить два его значения. MITRE, исследовательская группа, финансируемая федеральным правительством США, занимающаяся анализом и разрешением критических проблем с безопасностью, разработала следующие определения:

[...] Уязвимость — это состояние вычислительной системы (или нескольких систем), которое позволяет [23]:

- ✓ исполнять команды от имени другого пользователя;
- ✓ получать доступ к информации, закрытой от доступа для данного пользователя;
- ✓ показывать себя как иного пользователя или ресурс;
- ✓ производить атаку типа «отказ в обслуживании».

Предпринималось много попыток четко определить термин «уязвимость» и разделить два его значения.

Считается, что атака, производимая вследствие слабой или неверно настроенной политики безопасности, лучше описывается термином «открытость» (exposure).

Открытость — это состояние вычислительной системы (или нескольких систем), которое не является уязвимостью, но:

- ✓ позволяет атакующему производить сбор защищенной информации;
- ✓ позволяет атакующему скрывать свою деятельность;
- ✓ содержит возможности, которые работают корректно, но могут быть легко использованы в неблаговидных целях;
- ✓ является первичной точкой входа в систему, которую атакующий может использовать для получения доступа или информации.

Когда хакер пытается получить неавторизованный доступ к системе, он производит сбор информации (расследование) о своем объекте, собирает любые доступные данные и затем использует слабость политики безопасности («открытость») или какую-либо уязвимость. Существующие уязвимости и открытости являются точками, требующими особенно внимательной проверки при настройке системы безопасности против неавторизованного вторжения.

Примеры распространенных уязвимостей

Наиболее распространенная в настоящее время на подключенных к интернету компьютерах операционная система Microsoft Windows содержит множественные опасные уязвимости. Чаще всего хакерами используются уязвимости в IIS, MS SQL и Internet Explorer, а также системах обработки файлов и сервисах сообщений самой операционной системы [23].

Уязвимость в IIS, подробно описанная в Microsoft Security Bulletin MS01-033, является одной из наиболее часто используемых уязвимостей Windows. В последние годы было написано множество сетевых червей, пользующихся данной уязвимостью, но одним из наиболее известных является CodeRed. CodeRed был впервые обнаружен 17 июля 2001 года, и, по некоторым оценкам, заразил около 300 тысяч компьютеров, помешал работе

множества предприятий и нанес значительный финансовый ущерб компаниям по всему миру. Хотя Microsoft и выпустила вместе с бюллетенем MS01-033 патч, закрывающий используемую червем уязвимость, некоторые версии CodeRed до сих пор продолжают распространяться [23].

Сетевой червь Spida, обнаруженный спустя почти год после появления CodeRed, использовал для своего распространения открытость в MS SQL. Некоторые стандартные инсталляции MS SQL не защищали паролем системный эккаунт «SA», позволяя любому человеку с доступом к системе через сеть запускать на ней на исполнение произвольные команды. При использовании этой уязвимости, червь открывает эккаунту «Guest» полный доступ к файлам компьютера, после чего производит загрузку самого себя на заражаемый сервер [23].

Сетевой червь Slammer, обнаруженный в конце января 2003 года, использовал более простой способ заражения компьютеров под управлением Windows с работающим сервером MS SQL, а именно — уязвимость при переполнении буфера в одной из подпроцедур обработки UDP-пакетов. Поскольку червь был достаточно мал — всего 376 байт — и использовал протокол UDP, предназначенный для быстрой пересылки малых объемов данных, Slammer распространялся с невероятной скоростью. По некоторым оценкам, Slammer поразил порядка 75 тысяч компьютеров по всему миру за первые 15 минут эпидемии [23].

Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer.

Настройка локальной политики паролей

Microsoft Baseline Security analyzer - программа, позволяющая проверить уровень безопасности установленной конфигурации операционной системы (ОС) Windows 2000, XP, Server 2003, Vista Server 2008. Также проверяется и ряд других приложений разработки Microsoft. Данное средство можно отнести к разряду систем анализа защищенности. Оно распространяется бесплатно и доступно для скачивания с web-сервера Microsoft (адрес страницы данной утилиты на момент подготовки описания был: http://technet.microsoft.com/ru-ru/security/cc184924(en-us).aspx) [22].

В процессе работы BSA проверяет наличие обновлений безопасности операционной системы, офисного пакета Microsoft Office(для версий XP и более поздних), серверных приложений, таких как MS SQL Server, MS Exchange Server, Internet Information Server и т.д. Кроме того, проверяется ряд настроек, касающихся безопасности, например, действующая политика паролей [22].

Интерфейс программного продукта

При запуске открывается окно, позволяющее выбрать объект проверки - один компьютер (выбирается по имени или ip-адресу), несколько (задаваемых диапазоном ip-адресов или доменным именем) или просмотреть ранее сделанные отчеты сканирования системы (рис. 13.1) [22]. При выборе сканирования отдельного компьютера по умолчанию подставляется имя локальной станции, но можно указать имя или ip-адрес другого компьютера.

Можно задать перечень проверяемых параметров. На рис. 13.2 представлен выбор вариантов проверки:

- ✓ проверка на наличие уязвимостей Windows, вызванных некорректным администрированием;
- ✓ проверка на "слабые" пароли (пустые пароли, отсутствие ограничений на срок действия паролей и т.д.);
- ✓ проверка на наличие уязвимостей web-сервера IIS, вызванных некорректным администрированием;
- ✓ аналогичная проверка в отношении СУБД MS SQL Server;
- ✓ проверка на наличие обновлений безопасности.

Рис. 13.1. Выбор проверяемого компьютера

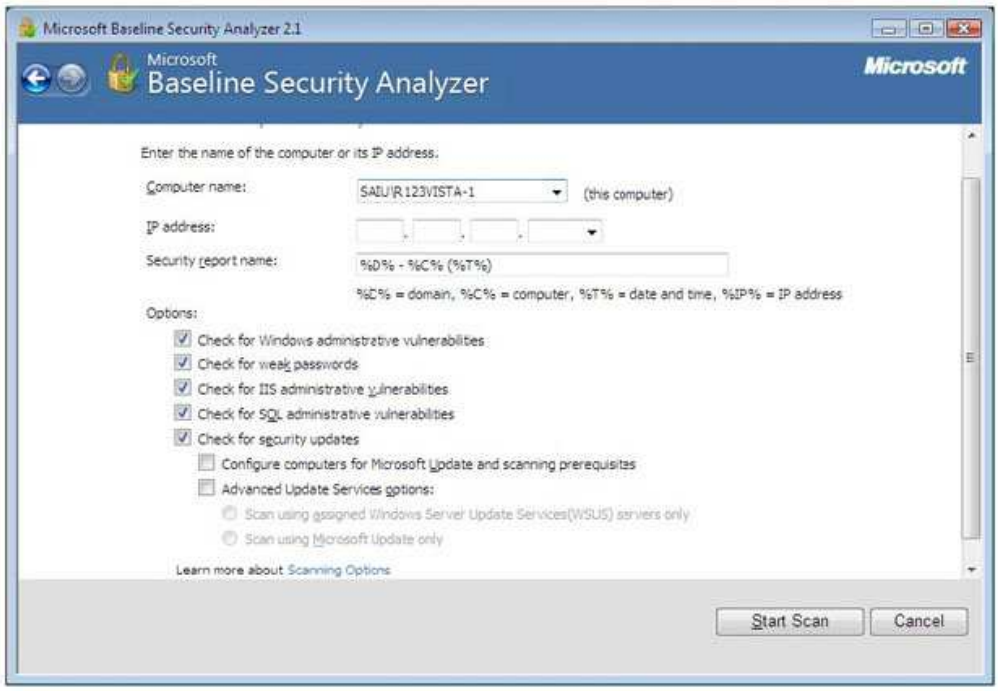


Рис. 13.2. Задание параметров проверки

Перед началом работы программа обращается на сервер Microsoft для получения перечня обновлений для ОС и известных уязвимостей. Если на момент проведения проверки компьютер не подключен к Интернет, база уязвимостей не будет обновлена, программа об этом сообщит и дальнейшие проверки выполняться не будут. В подобных случаях нужно отключать проверку обновлении безопасности (сбросив соответствующую галочку на экране рис. 13.2 или с помощью ключа при использовании утилиты командной строки, о чем речь пойдет ниже).

Для успешной проверки локальной системы необходимо, чтобы программа выполнялась от имени учетной записи с правами локального администратора. Иначе проверка не может быть проведена и о чем будет выдано сообщение: "You do not have sufficient permissions to perform this command. Make sure that you are running as the local administrator or have opened the command prompt using the 'Run as administrator' option".

По результатам сканирования формируется отчет, вначале которого дается общая оценка уровня безопасности конфигурации проверяемого компьютера. В приведенном на рис. 13.3 примере уровень риска оценивается как "серьезный" (Severe risk) [22].

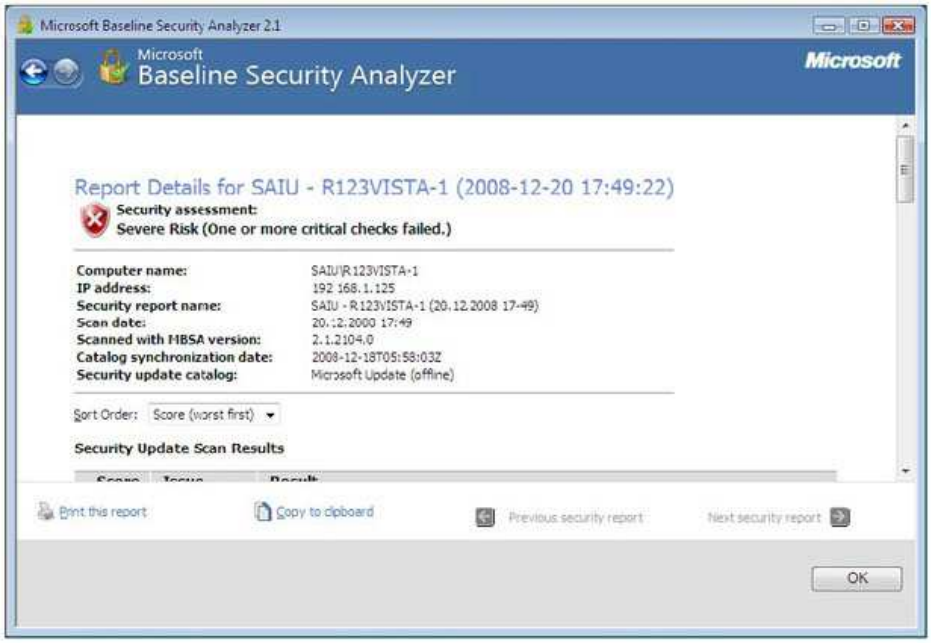


Рис. 13.3. Заголовок отчета

Далее приводится перечень обнаруженных уязвимостей, разбитый на группы: результаты проверки установки обновлений, результаты проверки Windows и т.д. Надо отметить, что выпускаемые Microsoft обновления бывают различных типов:

Security updates - собственно обновления безопасности, как правило, посвященные исправлению одной уязвимости программного продукта;

Update rollups - набор исправлений безопасности, который позволяет одновременно исправить несколько уязвимостей. Это упрощает обслуживание процесса обновления программного обеспечения (ПО);

Service packs - набор исправлений, как связанных, так и несвязанных с безопасностью. Установка Service pack, как правило, исправляет все уязвимости, обнаруженные с момента выхода предыдущего Service pack, таким образом устанавливать промежуточные обновления уже не надо.

В описании рассматриваемого результата проверки (рис. 13.4) можно выбрать ссылку ***Result details*** и получить более подробное описание найденных проблем данной группы. При наличии подключения к Интернет, перейдя по приводимой в отчете ссылке, можно получить информацию об отсутствующем обновлении безопасности и скачать его из сети.

Нужно отметить, что установка обновлений для систем с высокими требованиями в области непрерывности работы, требует предварительной тщательной проверки совместимости обновлений с использующимися приложениями. Подобная проверка обычно производится на тестовых системах с близкой конфигурацией ПО. В то же время, для небольших организаций и пользователей домашних компьютеров такая проверка зачастую неосуществима. Поэтому надо быть готовым к тому, чтобы восстановить систему

после неудачного обновления. Для современных ОС семейства Windows это можно сделать, например, используя специальные режимы загрузки ОС - безопасный режим или режим загрузки последней удачной конфигурации.

Также надо отметить еще одну особенность. На данный момент **baseline security analyzer** не существует в локализованной русскоязычной версии. И содержащиеся там ссылки на пакеты обновлений могут указывать на иные языковые версии, что может создать проблемы при обновлении локализованных продуктов.

Аналогичным образом проводится работа по анализу других групп уязвимостей (рис. 13.5). Описывается уязвимость, указывается ее уровень критичности, даются рекомендации по исправлению. На рис. 13.6 представлено подробное описание результатов (ссылка **result details**) проверки паролей. Указывается, что 3 учетные записи имеют пароли, неограниченные по сроку действия [22].

Рис. 13.4. Перечень неустановленных обновлений (по группам)

Рис. 13.5. Уязвимости, связанные с администрированием операционной системы

Кроме версии программы с графическим интерфейсом, существует также утилита с интерфейсом командной строки. Называется она mbsacli.exe и находится в том же каталоге, куда устанавливался Baseline security analyzer, например, **"C:\Program Files\Microsoft Baseline Security Analyzer 2"**. У утилиты есть достаточно много ключей, получить информацию, о которых можно запустив ее с ключом **"/?"**.

Рис. 13.6. Результаты проверки паролей

Запуск без ключей приведет к сканированию локального компьютера с выводом результатов на консоль. Чтобы сохранить результаты сканирования, можно перенаправить вывод в какой-либо файл. Например: mbsacli > mylog.txt. Следует еще раз обратить внимание на то, что при настройках по умолчанию сначала утилита обращается на сайт Майкрософт за информацией об обновлениях. Если соединение с Интернет отсутствует, то утилиту надо запускать или с ключом /nd (указание "не надо скачивать файлы с сайта Майкрософт") или с ключом /n Updates (указание "не надо проводить проверку обновлений").

Запуск с ключом /xmlout приводит к запуску утилиты в режиме проверки обновлений (т.е. проверка на уязвимости, явившиеся результатом неудачного администрирования, проводиться не будет), при этом, отчет формируется в формате xml. Например:

```
mbsacli /xmlout > c:\myxmlog.xml
```

ПРАКТИЧЕСКАЯ ЧАСТЬ

Локальная политика паролей

Рассмотрим, какие настройки необходимо сделать, чтобы пароли пользователей компьютера были достаточно надежны. В теоретической части курса мы рассматривали рекомендации по администрированию парольной системы. Потребовать их выполнения можно с помощью политики безопасности. Настройка делается через **Панель управления Windows [**22**]**.

Откройте **Панель управления** → **Администрирование** → **Локальная политика безопасности**. Выберите в списке **Политика учетных записей** и **Политика паролей**. Для Windows Vista экран консоли управления будет выглядеть так, как представлено на рис. 13.7.

Значения выбранного параметра можно изменить (рис. 13.8).

Надо понимать, что не все требования политики паролей автоматически подействуют в отношении всех учетных записей. Например, если в свойствах учетной записи стоит "Срок действия пароля не ограничен", установленное политикой требование максимального срока действия пароля будет игнорироваться. Для обычной пользовательской учетной записи, эту настройку лучше не устанавливать. Но в некоторых случаях она рекомендуется. Например, если в учебном классе нужна "групповая" учетная запись, параметры которой известны всем студентам, лучше поставить для нее **"Срок действия пароля не ограничен"** и **"Запретить смену пароля пользователем"**.

Свойства учетной записи можно посмотреть в **Панель управления** → **Администрирование** → **Управление компьютером**, там выберите **Локальные**

пользователи и группы и **Пользователи** (или запустив эту же оснастку через **Пуск** → **Выполнить** → **lusrmgr.msc**).

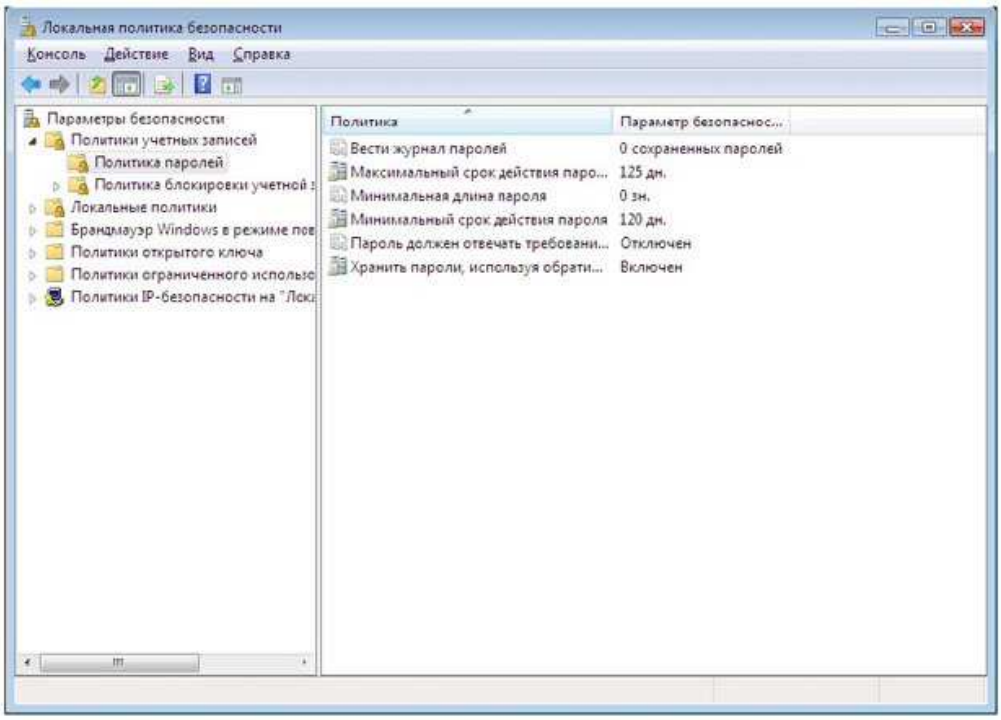


Рис. 13.7. Настройка политики паролей

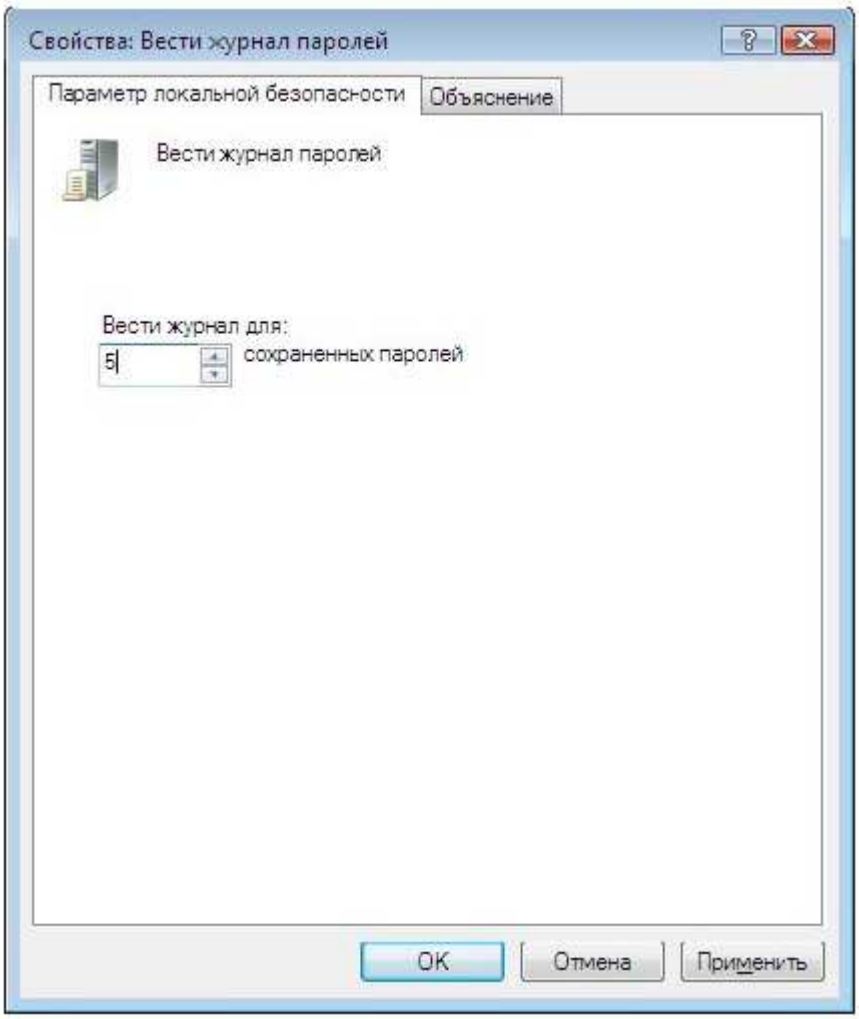


Рис. 13.8. Установка требования ведения журнала паролей

Задания

1. Запустите режим командной строки путем выполнения операции **Пуск -> Выполнить**. В появившейся строке напишите команду **cmd** и нажмите Enter. Для дальнейшей работы необходимо определить ip-адрес своего компьютера. Для этого пропишите в появившемся черном окне команду **ipconfig.** В тетради запишите ip-адрес своего компьютера, который появится на черном экране.

2. Запустите **Microsoft Baseline security analyzer**. Выберите команду **Scan a computer**. В окошке «IP-адрес» пропишите свой адрес, записанный в тетради. Снимите галочку **Check for security updates** (проверять наличие обновлений) перед выполнением проверки. Нажмите клавишу **Start Scan.**

3. Выполните проверку Вашего компьютера с помощью Microsoft Baseline security analyzer.

4. Подготовьте отчет в тетради или в текстовом файле формата doc (при условии последующего вывода на печать). В отчете следует указать, как оценен уровень уязвимости Вашего компьютера и какие проверки проводились; в какой области обнаружено наибольшее количество уязвимостей; отчет оформить в виде таблицы 13.1. В данной таблице отчет составлен на основании уязвимостей, найденных на тестовом компьютере. Список найденных уязвимостей показан на рис. 13.9.

Таблица 13.1 – Отчет о группах уязвимостей

Группа уязвимостей	Проверяемые уязвимости	Число замечаний и их наименование
Administrative Vulnerabilities		
Additional System Information	Auditing Shares Services Windows version	4 This check was skipped because the computer is not joined to a domain. Some potentially unnecessary services are installed. 6 share(s) are present on your computer. Computer is running Microsoft Windows XP
Internet Information Services (IIS) Scan Results	-	Not found
SQL Server Scan Results	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer
Administrative Vulnerabilities		Not found
Security assessment	Strong Security	The selected checks were passed.

(оценка уровня безопасности)		

Примечание: допускается собственная форма представления отчета/

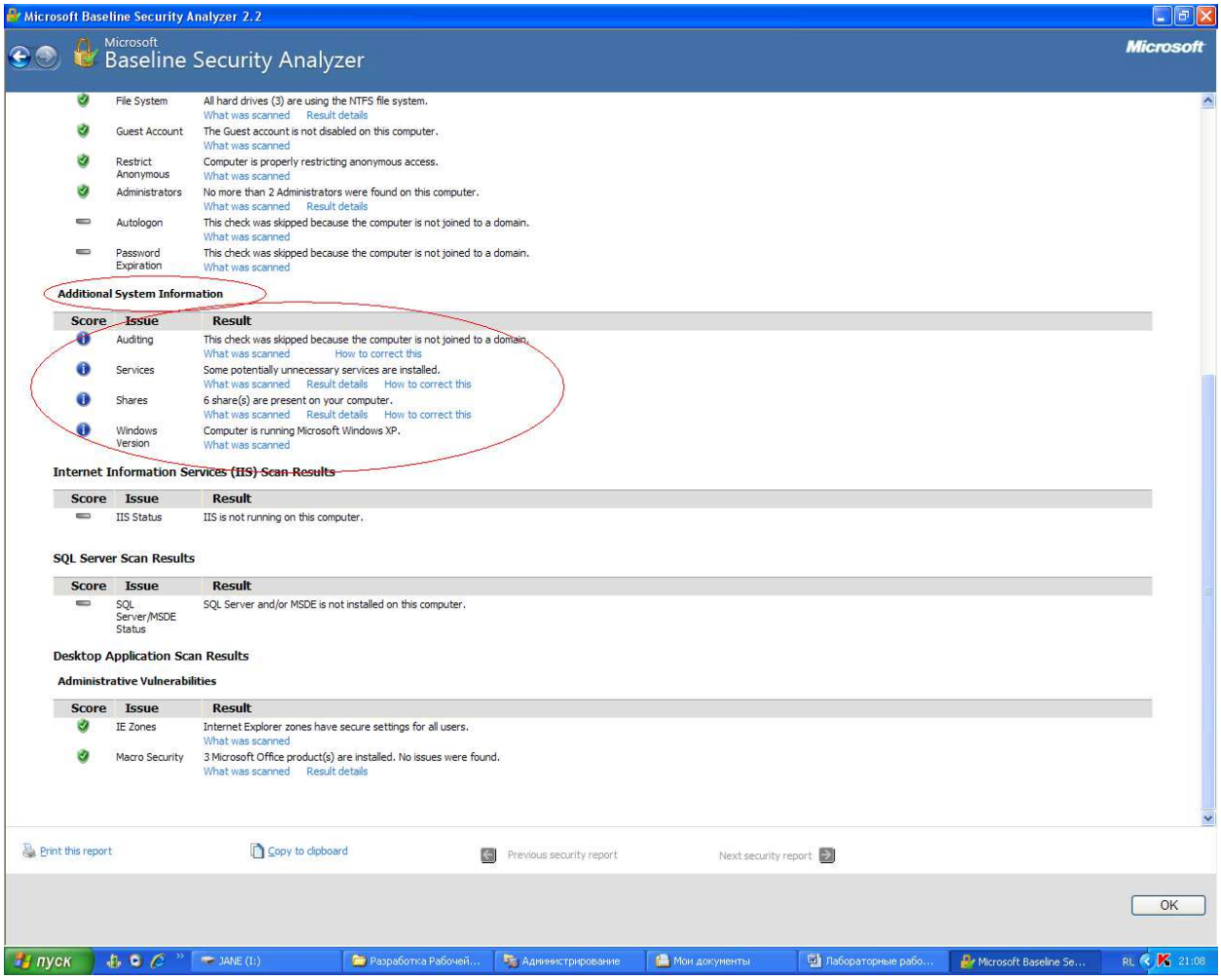


Рис. 13.9. Пример результата анализа уязвимостей локального компьютера

5. Опишите наиболее серьезные уязвимости каждого типа, выявленные на Вашем компьютере.

6. Проведите анализ результатов: какие уязвимости можно устранить, какие - нельзя из-за особенностей конфигурации ПО или использования компьютера.

7. По аналогичной схеме попытайтесь выполнить удаленную проверку соседнего компьютера из сети лаборатории. Опишите наиболее серьезные уязвимости.

8. Опишите действующую на вашем компьютере политику паролей.

9. Если в ходе проверки утилитой bsa были выявлены уязвимости связанные с управлением паролями пользователей, опишите пути их устранения или обоснуйте необходимость использования действующих настроек

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Что подразумевается под термином «Уязвимость операционной системы»?
2) В чем состоит основное отличие терминов «уязвимость» и «открытость»?
3) Приведите несколько примеров наиболее известных в мире последствий использования хакерами уязвимостей ОС?
4) Какие меры применяются для устранения уязвимостей ОС?
5) Какие типы обновлений позволяет устанавливать программа Microsoft Baseline Security Analyzer?
6) Что включает в себя локальная политика паролей?
7) Позволяют ли свойства программы Microsoft Baseline Security Analyzer работать в режиме командной строки, если да, то каким образом просмотреть список ее ключей?
8) Для чего необходимо владеть информацией о локальной политике паролей предприятия?

ЛАБОРАТОРНАЯ РАБОТА № 14

Исследование надежности системы идентификации пользователя

Цель занятия: изучение порядка выбора и хранения паролей, изучение порядка передачи паролей по сети, формирование навыков подписывания файлов цифровой подписью и передачу файлов по сети в зашифрованном виде.

Оборудование к занятию: компьютеры с операционной системой Windows, программное обеспечение - криптографическая программа GnuPG, встроенный калькулятор Windows.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

PGP – это криптографическая (шифровальная) программа с высокой степенью надежности, которая позволяет пользователям обмениваться информацией в электронном виде в режиме полной конфиденциальности [24].

Главное преимущество этой программы состоит в том, что для обмена зашифрованными сообщениями пользователям нет необходимости передавать друг другу тайные ключи т.к. эта программа построена на ином принципе работы – публичной криптографии или обмене открытыми (публичными) ключами, где пользователи могут открыто посылать друг другу свои публичные ключи с помощью сети Интернет и при этом не беспокоиться о возможности несанкционированного доступа каких-либо третьих лиц к их конфиденциальным сообщениям.

В PGP применяется принцип использования двух взаимосвязанных ключей: открытого и закрытого. К закрытому ключу имеете доступ только вы, а свой открытый ключ вы распространяете среди своих корреспондентов.

Великолепным преимуществом этой программы до недавнего времени было то, что она являлась бесплатной и любой пользователь, имеющий доступ к Интернету, мог ее «скачать» на свой компьютер за очень короткое время. Создатель PGP Филипп Циммерман открыто опубликовал код программы, который неоднократно был исследован специалистами крипто-аналитиками высочайшего класса и ни один из них не нашел в программе каких-либо слабых мест. PGP шифрует сообщение таким образом, что никто кроме получателя сообщения, не может ее расшифровать. За годы существования и развития PGP свет увидел целый стандарт OpenPGP —стандарт, выросший из программы PGP, получившей в Интернете к середине 90-х повсеместное распространение как надёжное средство шифрования электронной почты. Став стандартом де-факто, PGP начал встраиваться во множество приложений и систем.

Однако в 2010 г. компания Symantec выкупила PGP и программа перестала быть бесплатной. Исходный открытый код программы в настоящее время поддерживается энтузиастами со всего мира и эта программа имеет уже другое название GnuPG (GNU Privacy Guard, *Страж приватности GNU*) — это свободный некоммерческий аналог PGP, как и PGP, основанный на IETF-стандарте [25].

Электронные сообщения, в том виде и формате, который существует на сегодняшний день, легко могут быть прочитаны и архивированы любым человеком, имеющим доступ к серверу Интернет провайдера. В настоящий момент спецслужбам проще и дешевле подключиться к электронным адресам большого количества лиц, нежели к телефонным разговорам. Здесь вообще ничего делать не надо. Все сделает компьютер. Агенту спецслужбы или другому заинтересованному человеку остается только сесть за компьютер и просмотреть все ваши сообщения. Научно-технический прогресс облегчил задачу таким людям, однако, этот же самый прогресс предоставил возможность пользователям сети Интернет скрыть свои сообщения от третьих лиц таким образом, что даже суперкомпьютер стоимостью несколько десятков миллионов долларов не способен их расшифровать [25].

Принцип работы GnuPG

Когда пользователь шифрует сообщение с помощью GnuPG, то программа сначала сжимает текст, что сокращает время на отправку сообщения и увеличивает надежность шифрования. Большинство приемов криптоанализа (взлома зашифрованных сообщений) основаны на исследовании «рисунков», присущих текстовым файлам, что помогает взломать ключ. Сжатие ликвидирует эти «рисунки» и таким образом повышает надежность зашифрованного сообщения. Затем GnuPG генерирует сессионный ключ, который

представляет собой случайное число, созданное за счет движений вашей мышки и нажатий на клавиши клавиатуры [25].

Как только данные будут зашифрованы, сессионный ключ зашифровывается с помощью публичного ключа получателя сообщения, который отправляется к получателю вместе с зашифрованным текстом.

Расшифровка происходит в обратной последовательности. Программа PGP получателя сообщения использует закрытый ключ получателя для извлечения временного сессионного ключа, с помощью которого программа затем дешифрует зашифрованный текст.

Количественные характеристики систем парольной защиты информации

Пароли являются наиболее распространенным и доступным средством аутентификации. Самым слабым звеном в парольной аутентификации остается человек [26].

В большинстве систем пользователи самостоятельно выбирают пароли или получают их от системных администраторов. Зачастую люди не считают или не могут физически запоминать пароли, поэтому в качестве таковых используют номера телефонов, даты рождения, клички домашних животных, имена друзей-подруг, названия любимых фильмов или торговых марок [26].

Для снижения деструктивного влияния человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей.

К числу основных требований при выборе паролей относятся: установление минимальной длины пароля; использование в пароле различных групп символов; установление максимального и минимального сроков действий пароля; ведение журнала истории паролей; ограничение числа попыток ввода пароля; принудительная смена пароля при первой регистрации пользователя в системе и др.

Соблюдение перечисленных и других требований обеспечивают высокий уровень защиты информационных ресурсов в компьютерной системе. Стойкость парольной системы может быть оценена количественно. Для этого используются следующие параметры:

A – мощность алфавита паролей, т. е. то множество знаков, которое может применяться при вводе пароля (определяется количеством букв одного регистра в алфавите);

L – длина пароля;

S – мощность пространства паролей, т. е. множество всех возможных паролей в системе;

V – скорость подбора пароля;

T – срок действия пароля;

P – вероятность подбора пароля в течение срока его действия.

Для вычисления мощности пространства паролей в зависимости от алфавита паролей и их длины используют соотношения [26]:

$$S = A^L, \quad (1)$$

$$P = VT/S \quad (2)$$

Очевидно, что с увеличением длины пароля вероятность его подбора уменьшается; при удлинении срока жизни пароля, а также скорости перебора пароля вероятность его подбора увеличивается.

На практике возникают разные ситуации для задания параметров паролей, связанные с пожеланиями владельца информационных ресурсов фирмы, руководства организации. Например, заказчик может задать значение вероятности подбора пароля. В этом случае нужен подбор значений других параметров, входящих в соотношения (1) и (2).

Практически задачу можно свести к выбору длины пароля, если заданы мощность алфавита паролей A, скорость перебора пароля V и срок действия пароля T. Тогда длину пароля можно рассчитать по следующим соотношениям:

$$S = VT/P, \quad (3)$$

$$L = LnS / LnA \quad (4)$$

Анализ параметров системы парольной защиты информации, а также соотношений (3) и (4) приводит к следующим логическим выводам: скорость подбора V зависит от заданных алгоритмов перебора, и на практике эта величина обычно постоянная, мощность алфавита паролей A – также величина постоянная.

Срок действия пароля T и вероятность подбора пароля P в течение срока его действия – переменные величины.

Общие параметры для количественной оценки стойкости парольных систем представлены в табл. 14.1 [26].

Таблица 14.1. – Количественная оценка стойкости парольных систем

Параметр	**Способ определения**
Мощность алфавита паролей *A* Длина пароля *L*	Могут варьироваться для обеспечения заданного значения $S(S=A^L)$
Мощность пространства паролей *S*	Вычисляется на основе заданных значений *P, T* или *V*
Скорость подбора паролей *V*: 1.Для интерактивного режима определяется как скорость обработки одной попытки регистрации	1. Может быть искусственно увеличена для защиты от данной угрозы.

проверяющей стороной. 2.Для режима off-line (на основе свертки пароля) определяется как скорость вычисления значения свертки для одного пробного пароля	Задается используемым алгоритмом вычисления свертки. Алгоритм, имеющий медленные реализации, повышает стойкость по отношению к данной угрозе.
Срок действия пароля (задает промежуток времени, по истечении которого пароль должен быть обязательно сменен) *T*	Определяется исходя из заданной вероятности *P*, или полагается заданным для дальнейшего определения *S*.
Вероятность подбора пароля в течение срока его действия (подбор продолжается непрерывно в течение всего срока действия пароля) *P*	Выбирается заранее для дальнейшего определения *S* или *T*

Решение прямой и обратной задачи

В качестве иллюстрации к таблице 14.1. рассмотрим задачу на определение минимальной мощности пространства паролей (зависящей от параметров *A* и *L)* в соответствии с заданной вероятностью подбора пароля в течение его срока действия и обратную задачу [26].

Прямая задача

Задана вероятность $P=10^{-6}$. Необходимо найти минимальную длину пароля, которая обеспечит его стойкость в течение одной недели непрерывных попыток подобрать пароль при заданном значении мощность алфавита A [26].

Пусть скорость интерактивного подбора паролей V=10 паролей/мин. Тогда в течение недели можно перебрать

10*60*24*7= 100800 паролей (в 1 неделе 7 суток, в сутках 24 часа, в часе 60 мин)

Далее, учитывая, что параметры S, *V, T* и P связаны соотношением

$$P=V*T/S,$$

получаем: $S=100*800/10^{-6} = 1{,}008 * 10^{11} \approx 10^{11}$.

Если алфавит содержит A=26 символов, то применяя формулу (4) получим минимальную длину пароля:

$$L = \ln(10^{11}) / \ln 26 = 11 \cdot \ln 10 / \ln 26 = 7{,}77 \approx 8$$

Таким образом, минимальная длина пароля, которая обеспечит его стойкость в течение одной недели непрерывных попыток со скоростью 10 паролей в минуту для алфавита, состоящего из 26 букв составляет 8 символов.

Обратная задача

Пусть скорость перебора паролей $V = 100\,000 = 10^5$ паролей в секунду. Срок действия (жизни) пароля T = 30 суток. Длина пароля L = 8 символов [26].

Согласно формулам (1) и (2) рассчитаем соответствующие вероятности подбора пароля при мощности алфавита A равного 36 символам.

Вероятность подбора пароля вычисляется по формуле (2) $P = VT/S$. Поскольку V и T заданы, то для определения вероятности не хватает величины мощности пространства паролей S. Для нахождения величины S будем использовать формулу (1) $S = A^L$. *Для условий задачи величина S будет следующей:*

$S = 36^8 = 2821109907456 = 2{,}8 \times 10^{12} \approx 3 \times 10^{12}$.

Используя найденное значение S, находим вероятность подбора пароля для заданных условий задачи:

$$P = (10^5 \times 30 \times 24 \times 60 \times 60) / (3 \times 10^{12}) = 864 \times 10^{-4} \approx 9 \times 10^{-2} = 0{,}09$$

Таким образом, получаем значение вероятности подбора пароля при длине пароля 8 символов в течении 30 суток со скоростью 100 000 паролей в секунду составляет 9%.

Естественно, существуют способы повышения стойкости пароля. Для удобства чтения они сведены в таблицу 14.2.

Таблица 14.2. - Требования к выбору и использованию паролей

Требования к выбору пароля	**Получаемый эффект**
Установление максимальной длины пароля	Усложняет задачу злоумышленнику при попытке подсмотреть пароль или подобрать пароль методом «тотального опробования»
Использование в пароле различных групп символов	Усложняет задачу злоумышленнику при попытке подобрать пароль методом «тотального опробования»
Проверка и отбраковка пароля по словарю	Усложняет задачу злоумышленнику при попытке подобрать пароль по словарю
Установление максимального срока действия пароля	Усложняет задачу злоумышленнику при попытке подобрать пароль методом «тотального опробования», в том числе без непосредственного обращения к системе зашиты (режим off-line)
Установление минимального срока действия пароля	Препятствует попыткам пользователя заменить пароль на старый после его смены по предыдущему требованию
Введение журнала истории паролей	Обеспечивает дополнительную степень защиты по предыдущему требованию
Применение эвристического алгоритма, бракующего пароли на основании данных журнала истории	Усложняет задачу злоумышленнику при попытке подобрать пароль по словарю или с использованием эвристического алгоритма
Ограничение числа попыток ввода пароля	Препятствует интерактивному подбору паролей злоумышленником
Поддержка режима принудительной смены пароля пользователя	Обеспечивает эффективность требования, ограничивающего максимальный срок действия пароля
Использование задержки при вводе неправильного пароля	Препятствует интерактивному подбору паролей злоумышленником
Запрет на выбор пароля самим пользователем и автоматическая генерация	Исключает возможность подобрать пароль по словарю. Если алгоритм генерации

паролей	известен злоумышленнику, последний может подбирать пароли только методом «тотального опробования»
Принудительная смена пароля при первой регистрации пользователя в системе	Защищает от неправомерных действий системного администратора, имеющего доступ к паролю в момент создания учетной записи

ПРАКТИЧЕСКАЯ ЧАСТЬ

1) Программа GnuPG не требует установки и работает в режиме Portable. Запустите файл с расширением exe из папки местоположения программы;

2) В папке с программой вы найдете ярлык Инструкция, который откроет в браузере файл с инструкцией по работе с данной программой;

3) Обратите внимание, что для шифрования и подписывания файлов нужно первоначально создать пару секретный\публичный ключи;

4) При пересылке зашифрованных файлов указывается публичный ключ ПОЛУЧАТЕЛЯ!!! Таким образом, для того, чтобы вам могли отправлять файлы нужно сначала отправить свой публичный ключ вашим собеседникам.

5) Для создания пары ключей необходимо зайти в пункт меню Менеджер ключей;

6) В открывшемся окне выберите пункт меню Ключ -> Генерировать ключ.

7) При этом появится окно «генерировать ключ», где необходимо внести вашу идентификационную информацию, см. пример на рис. 14.1. Чем короче срок действия ключа тем лучше, однако, срок следует выбирать исходя из соображений того, как скоро ваше сообщение может прочитать собеседник. После нажатия клавиши ОК начинается процесс генерации ключа.

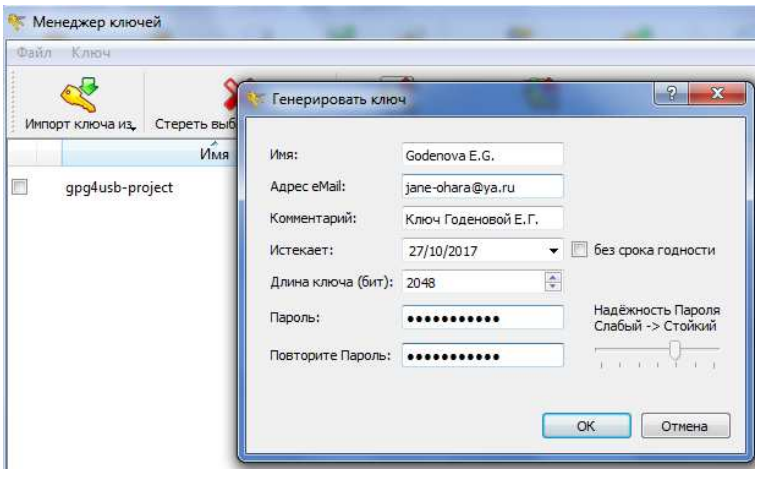


Рис. 14.1. – Пример заполнения данных для генерации ключа

8) Ваш ключ появится в правой части окна программы. Обратите внимание, что отличить ваш ключ от других можно по характерному значку ключа рядом с названием ключа, что означает секретность данного ключа. Публичные ключи, полученные от других пользователей, такого значка не имеют.

9) Для того, чтобы послать свой публичный ключ собеседнику необходимо зайти в меню Менеджер ключей, установить галочку напротив нужного ключа и выбрать экспорт в файл. В открывшемся окне указать место, куда следует сохранить ключ. Затем вы можете отправить этот ключ своему собеседнику.

10) Для того чтобы отправлять зашифрованные сообщения своему собеседнику вам необходим его публичный ключ. Собеседник может прислать свой ключ по электронной почте. Для того, чтобы внести полученный ключ в общий список нужно выбрать пункт меню Импорт ключа – Из файла. Указать путь к файлу и загрузить его. Все! Теперь можно отправлять собеседнику зашифрованные сообщения.

Задание.

1) Создайте свою пару ключей секретный / публичный;

2) Экспортируйте свой публичный ключ в файл и отправьте одному собеседнику;

3) Зашифруйте текст как показано в инструкции и пришлите его одному собеседнику;

4) Зашифруйте файл как показано в инструкции и пришлите его одному собеседнику;

5) Аналогичным образом получите зашифрованный текст и зашифрованный файл и расшифруйте их.

6) Сделайте скриншоты программы с шифрованием и расшифрованием теста и файла и вставьте в отчет по работе.

7) Напишите в левой части окна программы свою биографию и подпишите своим секретным ключом (пункт меню Подписать).

8) Сохраните подписанный текст в файл и перешлите собеседнику по электронной почте.

9) Получите подписанный файл от собеседника и проверьте его подпись (пункт меню Проверить);

10) Посмотрите детали цифровой подписи и сделайте скриншот окна в отчет по работе.

11) В отчете опишите отличие секретного и публичного ключа так, как вы это поняли.

12) Решите прямую (вычислите минимальную длину пароля) и обратную (вычислить вероятность подбора пароля) задачи при условиях, заданных преподавателем. Расчеты можно представить в суммарном отчете или на отдельном листе бумаги.

13) Файл отчета зашифруйте для собеседника Преподаватель, используя его публичный ключ, и пришлите на электронную почту.

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Каким образом найти минимальную длину пароля, зная вероятность подбора пароля и срок действия?
2) Каков принцип работы программы GnuPGP?
3) Принцип использования, каких двух ключей применяется в GnuPGP?
4) Каким образом происходит расшифровка сообщения в программе GnuPGP?
5) К какому эффекту приведет установление минимального срока действия пароля?
6) От какой действия возникает эффект защиты от неправомерных действий системного администратора, имеющего доступ к паролю в момент создания учетной записи?
7) Перечислите количественные оценка стойкости парольных систем;
8) По каким формулам вычисляется вероятность подбора паролей и мощность пространства паролей?

ЛАБОРАТОРНАЯ РАБОТА № 15
Средства защиты и удостоверения подлинности электронных документов

Цель занятия: изучить и практически освоить стандартные средства, обеспечивающие защиту и контроль подлинности текстовых офисных документов, электронных таблиц и их фрагментов.

Оборудование к занятию: компьютеры с офисным пакетом Open Office, программа создания самоподписанных сертификатов Abylon Selfcert.

Форма проведения занятия: интерактивное занятие с использованием методов работы в малых группах и деловой игры (2 ч).

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Зачастую при решении повседневных дел приходится сталкиваться с большим количеством электронных документов. Различные анкеты, договора, бланки, запросы оформляются средствами известных офисных пакетов. Вопрос получения вами или вашим адресатом нужного документа в неизменном виде всегда очень важен. Как правило, современные офисные пакеты содержат несколько вариантов защиты от

несанкционированного доступа к тесту документа. Так, версии MS Office от 2003 и выше содержат следующие возможности по защите электронных документов:

- ✓ опечатывание документа с помощью цифрового сертификата;
- ✓ запрос пароля при открытии или изменении документа;
- ✓ рекомендация доступа только для чтения;
- ✓ защита полей электронной формы от случайного изменения;
- ✓ разрешить только добавление примечаний и записей исправления;
- ✓ защита форматирования.

Некоторые из указанных функций доступны также в свободном программном обеспечении Open Office.

Как известно, большая часть документооборота ведется в форме стандартных текстовых документов, электронных таблиц и баз данных. Все эти документы могут стать объектами деятельности злоумышленника, причем как внешнего, так и внутреннего. В данной лабораторной работе рассматриваются средства защиты документов, имеющиеся в стандартном наборе настроек офисных пакетов. Работа состоит из двух частей: защита текстовых документов и защита электронных таблиц.

ПРАКТИЧЕСКАЯ ЧАСТЬ

Часть I. Защита текстовых документов и их фрагментов

1) Создайте новый документ Open Office. Writer и сохраните его в личной папке.

2) Скопируйте в новый документ любую статью по информационной безопасности из сети Интернет и напишите критический отзыв к этой статье.

3) Данный документ сохраните в формате Фамилия_критика.odt;

4) Далее требуется защитить документ от незаконного использования и изменения средствами Open Office. Writer

5) ***Защита документа от редактирования***. Любой документ можно защищать от внесения в него изменений посторонними лицами. Для этого необходимо сохранять документ в режиме «Только чтение». Сохраните ваш документ в режиме «Только чтение» при помощи меню Файл → Свойства → Безопасность. Далее поставить галочку напротив пункта «Открывать только для чтения» и нажать клавишу Защитить. Ввести пароль для защиты.

6) Описать, для чего можно применять вид защиты, описанный в пункте 5.

7) ***Защита документа от несанкционированного открытия.*** Если документ нужно не просто защитить от редактирования, а вообще сделать недоступным для просмотра посторонними лицами, его можно сохранить с условием ввода пароля при открытии.

8) ***Выберите пункт меню Сервис***→ Параметры →Безопасность → Параметры → Рекомендовать сохранение с паролем. Имейте ввиду, что данная настройка сохраняется на все последующие документы, если ее не сбросить. Найдите еще один способ сохранения документа с паролем и опишите его.

9) Создайте новый документ с описанием необходимости использования данного пункта меню. Установите пароль на открытие документа с критическим отзывом и отправьте на проверку преподавателю.

10) Помимо защиты всего документа, иногда существует необходимость ***защиты отдельных фрагментов текста***. Для этого в Open Office существует возможность защиты разделов текста. Самостоятельно найдите возможность защиты разделов и создайте документ с защищенными от редактирования разделами текста.

Цифровая подпись документа

Цифровая подпись - шифрованная электронная подпись, подтверждающая подлинность макроса или документа. Наличие цифровой подписи подтверждает, что макрос или документ был получен от владельца подписи и не был изменен.

Цифровой сертификат - вложение в файл, проект макроса или сообщение электронной почты, подтверждающее его подлинность, обеспечивающее шифрование или предоставляющее поддающуюся проверке подпись.

Цифровую подпись можно создать с помощью программы **Selfcert.exe**. Зачастую данная программа распространяется производителями ПО бесплатно. В данной работе используется программа Abylon Selfcert. Поскольку самоподписанный сертификат может создать кто угодно, то он не имеет особой ценности. Однако для людей, не пересылающих особо ценную информацию, он может быть полезен.

1) Запустите программу Abylon Selfcert. Возникнет диалоговое окно с вопросом, ответьте Yes. На рис. 15.1. показано окно программы, где требуется внести данные для создания сертификата. После внесения всех данных нажмите кнопку **Create**. При этом появится вопрос о пути, по которому сохранить файл. Укажите свою личную папку.

2) После создания сертификата появится окно с вопросом об импорте сертификата в хранилище сертификатов. Поскольку данный сертификат является сампоподписанным и не будет храниться на сервере центра сертификации, то хранилищем может являться любая папка на компьютере. На рис. 15.2. показано окно работы мастера Импорта.

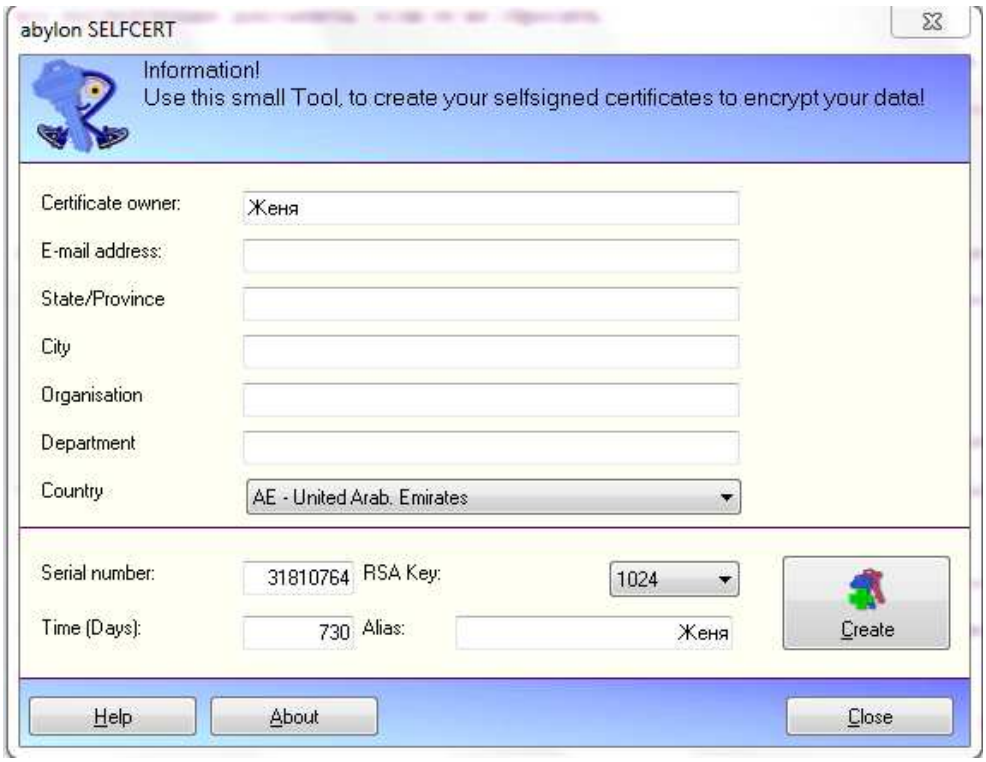


Рис. 15.1. Окно программы Abylon Selfcert для создания самоподписанного сертификата

В процессе импорта можно установить нужный уровень безопасности.

3) Создайте новый текстовый документ.

4) Откройте сайт http://wiki.i-rs.ru/wiki/RU/security/digital_signature и на основе представленной там информации опишите в новом документе виды электронной подписи в Open Office. Результат опишите **СВОИМИ СЛОВАМИ** в форме научной статьи. **Скопированный текст не принимается!** Возможно использование других ресурсов.

5) Подпишите сформированный документ цифровой подписью при помощи созданного сертификата. Для этого выберите пункт меню Файл → Цифровая подпись → Подписать документ. В окне выберите свой сертификат.

ЗАПОМНИТЕ! ПОСЛЕ СОХРАНЕНИЯ ВСЕ ЦИФРОВЫЕ ПОДПИСИ УДАЛЯЮТСЯ! ДОКУМЕНТ ПОДПИСЫВАЕТ ПОСЛЕ ВСЕХ РЕДАКЦИЙ.

6) Для выполнения данного задания необходимо разбиться на малые группы по 2-3 человека. Каждая группа должна подготовить обзор программных средств защиты электронного документооборота компании (например, представленных на сайте http://signal-com.ru/ru/prod/documents/index.php). Составьте обзорную характеристику достоинств и недостатков этих программных продуктов. Резюмируйте, какой продукт вы выбрали бы для своей компании;

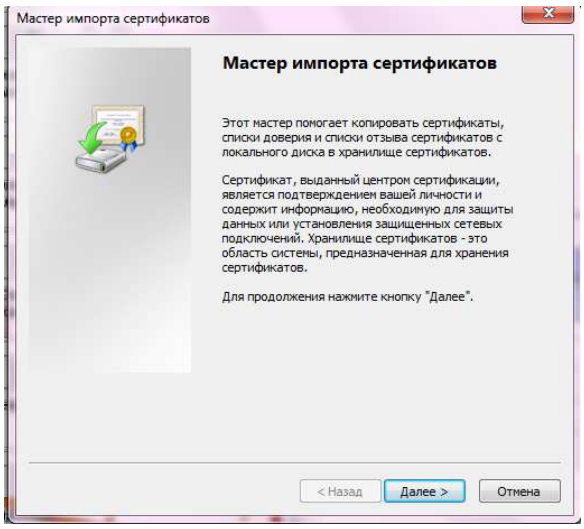


Рис. 15.2. Мастер импорта сертификатов

7) Далее работа происходит в форме деловой игры «Продавец программного обеспечения». Малая группа должна представить свой обзор другим студентам, которые являются «потенциальными покупателями», с тем, чтобы они захотели купить эту продукцию. Для представления обзора, т.е. рекламы продукта, студенты могут использовать вспомогательные технические средства (компьютер, планшет и проч.). По мере представления «продавцами» своего продукта, «потенциальные покупатели» должны находить минусы в представляемом продукте, а «продавцы» обосновывать эти минусы и обращать в плюсы;

8) Далее группы меняются местами и по очереди представляют свой обзор;

9) По окончании занятия 5-7 минут отводится на обсуждение со студентами данного метода проведения занятия, его достоинства и недостатки, а также рекомендации по усовершенствованию.

Часть II. Защита электронных таблиц и их фрагментов

1) Создайте новый документ Open Office Calc и подготовьте электронную ведомость по указанному образцу (рис. 13.3).

	A	B	C	D	E	F	G
1	**Электронная ведомость**						
2	№№ п.п.	ФИО	Баллы			Сумма баллов	Отметка о зачете
3			Аттестация	Работа в семестре	Зачет		
4	1	2	3	4	5	6	7
5	1	Антонова И.	12	15	60	87	Зачтено
6	2	Борисов В.	18	16	12	46	Не зачтено
7	3	Васильев А.	16	17	24	57	Зачтено
8	4	Григорьева М.	8	18	23	49	Не зачтено
9	5	Яковлева Н.	2	10	40	52	Зачтено
10							

Рис. 13.3. Пример создания фрагмента электронной таблицы

Введите данные в ячейки «шапки» таблицы, выполните необходимое форматирование и объединение ячеек.

В графу 2 (ФИО) введите 5-7 произвольных фамилий.

В графы 3 (Аттестация) и 4 (Работа в семестре) введите произвольные баллы от 0 до 20.

В графу 6 (Сумма баллов) введите формулу, вычисляющую сумму баллов в графах 3, 4 и 5.

В графу 7 введите с помощью встроенной функции ЕСЛИ формулу, формирующую текст «Зачтено», если значение соответствующего поля графы 6 больше или равно 50, и текст «Не зачтено» в противном случае.

2) Для диапазона данных графы 5 (в примере E5:E9) выполните операции:

Выделить ячейки диапазона данных → Команда Формат → Ячейки… → Вкладка Защита → Снять флажок Защищенное→ ОК

3) Выполните защиту документа (листа электронной таблицы):

Команда Сервис → Защитить документ → Лист… → Ввести пароль для отключения защиты листа → Подтвердить пароль → ОК

4) Введите данные зачета – баллы от 0 до 60. Проверьте, как меняются значения граф 6 и 7.

5) Попробуйте отредактировать данные в ячейках (C5:C9) или (D5:D:9). Что при этом происходит? Попробуйте снять защиту листа и попробовать еще раз отредактировать данные в указанных ячейках:

Команда Сервис → Защитить документ → Лист… → Ввести пароль для отключения защиты листа → ОК

6) Внесите правки в ячейки и снова установите защиту.

7) Сохраните документ Open Office Calc в своей личной папке.

8) Подпишите документ Open Office Calc цифровой подписью с использованием ранее созданного Вами цифрового сертификата и закройте его окно.

9) По аналогии с защитой текстового документа установите запрос пароля при сохранении документа.

10) Разработайте анкету для опроса сотрудников, чтобы они могли вносить данные в строго определенные поля и никуда больше?

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Что такое цифровая подпись электронного документа?
2) Что такое цифровой сертификат?
3) Какую опасность, и при каких условиях, могут содержать документы Excel?
4) Какие способы защиты документа вы знаете?

5) Каким образом можно защитить документ при помощи пароля?
6) Какие виды защиты документов типа Word, Open Office существуют?
7) Что такое цифровая подпись?
8) Что такое цифровой сертификат?
9) Какие виды цифровых подписей возможны в Open Office?
10) Чем отличается защита документов в разных программных пакетах?

ЛАБОРАТОРНАЯ РАБОТА № 16
Шифрование текста как метод защиты информации

Цели занятия: изучить метод перестановки для шифрования открытого текста, изучить метод многоалфавитной одноконтурной обыкновенной подстановки для шифрования открытого текста.

Оборудование: не требуется специализированного оборудования. Работа выполняется в письменном виде.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Шифрование является одним из эффективных способов защиты текстовой информации. При шифровании существуют следующие понятия [27].

Открытый текст – информация, содержание которой может быть понятно любому субъекту [27].

Шифрование – процесс преобразования открытого текста в шифротекст или криптограмму с целью сделать его содержание непонятным для посторонних лиц. В общем виде процесс шифрования описывается выражением вида $C=E_k(P)$ где С – шифротекст; Е – функция шифрования; k – ключ шифрования; P – открытый текст [27].

Расшифрование – процесс обратного преобразования шифротекста в открытый текст. В общем виде процесс расшифрования описывается выражением вида $P=D_{k'}(C)$ где D – функция расшифрования; k' – ключ расшифрования [27].

Криптосистема – совокупность алгоритмов, реализуемых функциями E и D, множества ключей k, $'k$ и шифротекстов [27].

Криптограмма (загадочное письмо или тайнопись) – наука о защите информации с помощью шифрования [27].

Криптоанализ – наука о методах дешифрования [27].

Криптостойкость – характеристика надёжности шифротекста от вскрытия [27].

Криптостойкость шифра характеризуют двумя величинами:

1) минимальным объёмом шифротекста, статическим анализом которого можно его вскрыть и получить открытый текст без знания ключа;

2) числом MIPS-часов (лет) – временем работы условного криптоаналитического компьютера производительностью 1 000 000 операций в секунду, необходимым для вскрытия шифротекста.

Данная работа состоит из двух частей. В первой части необходимо выполнить задание на шифрование текста по методу обыкновенной перестановки, во второй части – по методу многоалфавитной одноконтурной обыкновенной перестановки.

Часть I. Шифрование по методу обыкновенной перестановки

В настоящее время известно множество методов шифрования, одним из которых является метод перестановки. В соответствии с этим методом биты (или символы) открытого текста переставляются в соответствии с задаваемым ключом шифрования правилом [27]:

$$1 \le i \le n,\ C_i = P_{k[i]}, \qquad (1.1)$$

где $P = \{P_1, P_2, P_3, \ldots P_i, P_n\}$ – открытый текст; n – длина открытого текста (количество символов текста); $C = \{C_1, C_2, C_3, \ldots C_i, C_n\}$ – шифротекст; $k = \{k_1, k_2, k_3, \ldots k_i, k_n\}$ – ключ шифрования.

При расшифровании используется обратная перестановка:

$$P_{k[i]} = C_i. \qquad (1.2)$$

Как видно из приведенных выражений, ключ должен удовлетворять условиям: $k_i \neq k_j$, $1 \le k_i \le n$

Рассмотрим пример шифрования слова «Пример» методом перестановки. Зададим ключ, который должен быть равен 6-ти символам (количеству символов в шифруемом слове) в виде $k = \{1, 2, 3, 4, 5, 6\}$. В данном примере зададим следующий ключ $k = \{1, 4, 6, 2, 3, 5\}$. Для удобства запишем все данные для шифрования в одну таблицу (таблица 1.2).

Таблица 1.2. Данные для шифрования

Символы открытого текста	П	Р	И	М	Е	Р
	P_1	P_2	P_3	P_4	P_5	P_6
Цифровые символы ключа	1	4	6	2	3	5
	k_1	k_2	k_3	k_4	k_5	k_6

Запишем открытый текст в виде Р = {П Р И М Е Р}, далее необходимо получить шифротекст в виде С = $\{C_1, C_2, C_3, C_5, C_6\}$.

Применим формулу (1.1) с выбранным ключом k к слову «Пример». Получим следующие выражения:

$$C_1 = P_{k[1]} = P_1 = 'П'; \quad C_2 = P_{k[2]} = P_4 = 'м'; \quad C_3 = P_{k[3]} = P_6 = 'р';$$

$$C_4 = P_{k[4]} = P_2 = 'р'; \quad C_5 = P_{k[5]} = P_3 = 'и'; \quad C_6 = P_{k[6]} = P_5 = 'е';$$

В конечном итоге получим шифротекст С = Пмррие

Очевидно, что применив другой ключ, получим другой вид шифрованного текста.

При дешифровании используем обратную операцию по формуле (1.2):

Выпишем данные для дешифрования в виде таблицы 1.3:

Таблица 1.3. Данные для дешифрования

Символы шифротекста	П	м	р	р	и	е
	C_1	C_2	C_3	C_4	C_5	C_6
Цифровые символы ключа	1	4	6	2	3	5
	k_1	k_2	k_3	k_4	k_5	k_6
Порядок формирования дешифруемого текста	P_1	P_2	P_3	P_4	P_5	P_6

Следует учесть, что при расшифровании необходимо получить не только исходное значение зашифрованного символа, но и его порядковый номер P_i в исходном тексте.

$$P_{k[1]} = P_1 = C_1 = 'П'; \quad P_{k[2]} = P_4 = C_2 = 'м'; \quad P_{k[3]} = P_6 = C_3 = 'р';$$

$$P_{k[4]} = P_2 = C_4 = 'р'; \quad P_{k[5]} = P_3 = C_5 = 'и'; \quad P_{k[6]} = P_5 = C_6 = 'е';$$

Таким образом, получим $P = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ = {Пример}.

Если требуется зашифровать достаточно длинный текст длиной n, то его можно разбить на блоки, длина которых равна длине ключа m. Открытый текст записывают в таблицу с числом столбцов, равным длине ключа (каждый блок открытого текста записывается в столбец таблицы). Затем столбцы полученной таблицы переставляются в соответствии с ключом перестановки, а шифротекст считывается из строк таблицы последовательно.

Пусть требуется зашифровать открытый текст «этот пример шифрования». Длина текста (вместе с пробелами n = 22). Выберем ключ шифрования в виде $k = \{3, 5, 4, 2, 1\}$ ($m = 5$).

Разбиваем строку «этот пример шифрования» на пять блоков, каждый из который располагаем в таблицу:

э	п	р	р	и
т	р		о	я

о	и	ш	в	
т	м	и	а	
	е	ф	н	

Переставляем столбцы полученной таблицы в соответствии с ключом *k = {3, 5, 4, 2, 1}*. Получим

р	и	р	п	э
	я	о	р	т
ш		в	и	о
и		а	м	т
ф		н	е	

Считываем последовательно текст из строк таблицы. Получим следующий шифр: *рирпэ яортш виои амтф не*.

Для расшифрования шифротекст записывают в таблицу того же размера по строкам, затем производится обратная перестановка столбцов в соответствии с ключом, после чего расшифрованный текст считывается из таблицы по столбцам. Ниже приведены этапы расшифровывания: а) запись шифротекста в таблицу; б) перестановка столбцов в соответствии с ключом; в) считывание символов по столбцам. [27]

Этап а

р	и	р	п	э
	я	о	р	т
ш		в	и	о
и		а	м	т
ф		н	е	

Этап б

э	п	р	р	и
т	р		о	я
о	и	ш	в	
т	м	и	а	
	е	ф	н	

Результатом считывания данных таблицы этапа б будет фраза «этот пример шифрования».

Если в качестве ключа перестановки использовать последовательность не цифр, а произвольных символов (например, пароль пользователя), то его необходимо предварительно преобразовать в последовательность целых чисел от 1 до *m*.

Например, пользователь ввел пароль «Петров».

Отсортируем символы в алфавитном порядке.

Получим Петров=>веопрт. Каждому символу присвоим порядковый номер:

в е о п р т

1 2 3 4 5 6

Заменим символы введённого пароля цифрами и получим ключ: 426531.

ПРАКТИЧЕСКАЯ ЧАСТЬ

1) Изучить теоретические основы метода перестановки.
2) Зашифровать (расшифровать) слово открытого текста ключом, длина которого равна длине шифруемого слова (задание выдается преподавателем).
3) Зашифровать и расшифровать фразу (выдается преподавателем) при помощи ключа.
4) Придумать символьный пароль, преобразовать его в ключ и зашифровать (расшифровать) фразу из задания № 3 с помощью этого ключа.

Ответы к заданиям оформляются в письменном виде или в текстовом редакторе Microsoft Word с последующим сохранением в файл. Название файла формируется из фамилии и номера лабораторной работы, например Иванов_11.doc. В тексте ответа должны быть приведены все промежуточные расчеты.

Исходное слово для шифрования:

Ключ шифрования:

Результат шифрования

Символьный пароль

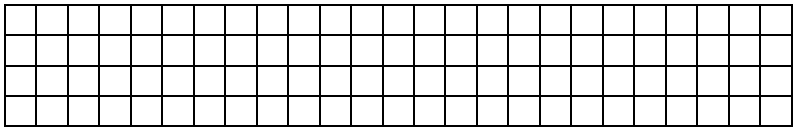
Цифровой пароль _ _ _ _ _ _ _ _ _ _ _

Фраза для шифрования

Этап а

Этап б

Результат шифрования



Часть II. Шифрование по методу многоалфавитной одноконтурной обыкновенной перестановки

В течение столетий использование простого одноалфавитного шифра замены было достаточным, чтобы обеспечить секретность. Последующее развитие частного анализа, вначале арабами, а затем в Европе, разрушило его стойкость. Трагическая казнь Марии Стюарт, королевы Шотландии, явилась драматической иллюстрацией слабостей одноалфавитной замены. Ряд ученых эпохи возрождения трудились над созданием нового шифра, однако только в 1549 г. Французский дипломат Блез де Виженер смог объединить труды многих людей и представить миру новый методы шифрования при помощи многоалфавитной одноконтурной перестановки.

Стойкость шифра Виженера состоит в том, что для зашифрования сообщения в нем используется не один, а несколько различных шифроалфавитов (для английского языка – 26, для русского – 33). Шифрование начинается с так называемого квадрата Виженера, пример которого показан в таблице 16.4.: алфавит открытого текста с последующими 26 шифроалфавитами, каждый из которых сдвинут на одну букву относительно предыдущего алфавита [28].

Верхний ряд квадрата, со строчными буквами, представляет буквы алфавита открытого текста. Вы можете зашифровать каждую букву открытого текста с помощью любого из 26 шифроалфавитов. Например, есил используется шифроалфавит номер 2, то буква а зашифровывается как С, если же используется шифроалфавит номер 12, тогда а преобразуется в М [28].

Чтобы показать, как применяется ключевое слово с квадратом Виженера для защифровывания короткого сообщения, зашифруем следующую короткую фразу **divert troops to east ridge** с помощью ключевого слова **WHITE**.

Таблица 16.4. - Квадрат Виженера

Открытый алфавит	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Прежде всего, ключевое слово записывается над сообщением буква за буквой, и его повторяют до тех пор, пока каждой букве в сообщении не будет сопоставлена буква ключевого слова. Далее приступаем к созданию шифротекста, что делается следующим образом [28]:

1) чтобы зашифровать первую букву d, определим вначале букву ключа над ней, W, которая в свою очередь задает строку в квадрате Виженера. Именно строка, начинающаяся с буквы W, - двадцать вторая строка, - и является шифроалфвавитом, который будет использован для шифрования буквы d открытого текста.

2) смотрим, где столбец с буквой d в первой строке пересекается со строкой, начинающейся с буквы W – это будет буква Z. Следовательно, буква d в открытом тексте будет буквой Z в шифротексте.

3) точно также шифруем букву I открытого текста - это будет буква P шифротекста.

4) широтекст записывается под исходным текстом буква под буквой, пример показан на рис. 16.1.

Ключевое слово	W H I T E W H I T E W H I T E W H I T E W H I T E W H I
Исходный текст сообщения	d i v e r t t r o o p s t o e a s t r i d g e
Зашифрованный текст сообщения	Z P D X V P A Z H S L Z B H I W Z B K M Z N M

Рис. 16.1. Пример записи ключевого слова, исходного текста и шифротекста.

На рис. 16.2 приведен квадрат Виженера с пятью выделенными строками (т.е. пятью шифроалфавитами), которые определяются ключевым словом WHITE [28].

Открытый алфавит	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Рис. 16.2. Методика шифрования с использованием квадрата Виженера.

Одним из главных достоинств шифра Виженера является то, что он неуязвим для частотного анализа. Это обусловлено тем, что одна и та же буква в открытом тексте, может быть зашифрована многими другими буквами в шифротексте.

Помимо того, что шифр Виженера неуязвим для частотного анализа, он подразумевает использование гигантского количества ключей. Отправитель и получатель могут договориться об использовании любого слова из словаря, любой комбинации слов или даже придумать свои слова. А криптоаналитик, не сможет дешифровать сообщение перебором всех возможных ключей, так как число возможных вариантов просто огромно [28].

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Дать определение шифротекста
2) Дать определение открытого текста
3) Дать определение криптосистемы

4) Дать определение криптоанализа
5) Что такое криптостойкость и чем она характеризуется?
6) В чем заключается метод шифрования текста перестановкой?
7) Какие еще существуют методы шифрования текста?
8) Где можно использовать шифрование текста?
9) Объяснить, почему получил свое название метод шифрования «Одноконтурная многоалфавитная обыкновенная перестановка».
10) Объяснить суть шифрования по методу Виженера?
11) Чем определяется стойкость шифра по методу Виженера?

ЛАБОРАТОРНАЯ РАБОТА № 17

Исследование электронной цифровой подписи на основе алгоритма RSA

Цель работы: изучить принцип действия электронной цифровой подписи;

Оборудование: компьютер с операционной системой Windows, наличие доступа в сеть Интернет.

Форма проведения занятия: интерактивное занятие с использованием метода case-study (2 ч).

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Электронная цифровая подпись (ЭЦП) используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. При таком обмене электронными документами существенно снижаются затраты на обработку и хранение документов, ускоряется их поиск. Но возникает проблема аутентификации автора электронного документа и самого документа, т. е. установления подлинности автора и отсутствия изменений в полученном электронном документе [29].

Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к которым относятся [29]:

- ✓ ***активный перехват*** — нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;
- ✓ ***маскарад*** — абонент *C* посылает документ абоненту *B* от имени абонента *A;*
- ✓ ***ренегатство*** — абонент *A* заявляет, что не посылал сообщения абоненту *B,* хотя на самом деле послал;
- ✓ ***подмена*** — абонент *B* изменяет или формирует новый документ и заявляет, что получил его от абонента *A;*
- ✓ ***повтор*** — абонент *C* повторяет ранее переданный документ, который абонент *A*

посылал абоненту *B*.

Эти виды злоумышленных действий могут нанести существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, частным лицам, применяющим в своей деятельности компьютерные информационные технологии.

Проблему проверки целостности сообщения и подлинности автора сообщения позволяет эффективно решить методология электронной цифровой подписи [29].

Основные процедуры цифровой подписи

Функционально цифровая подпись аналогична обычной рукописной подписи и обладает ее основными достоинствами [29]:

- ✓ удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- ✓ не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
- ✓ гарантирует целостность подписанного текста.

Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом.

Электронная цифровая подпись основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности цифровой подписи. Электронная цифровая подпись реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа.

Система ЭЦП включает две основные процедуры [29]:

- ✓ формирования цифровой подписи;
- ✓ проверки цифровой подписи.

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки — открытый ключ отправителя.

Процедура формирования цифровой подписи

На подготовительном этапе этой процедуры абонент *A* — отправитель сообщения — генерирует пару ключей: секретный ключ k_A и открытый ключ K_A. Открытый ключ K_A вычисляется из парного ему секретного ключа k_A. Открытый ключ K_A рассылается остальным абонентам сети (или делается доступным, например, на разделяемом ресурсе) для использования при проверке подписи. Для формирования цифровой подписи отправитель *A* прежде всего вычисляет значение хэш-функции *h(M)* подписываемого текста *M* (рис. 17.1). [29]

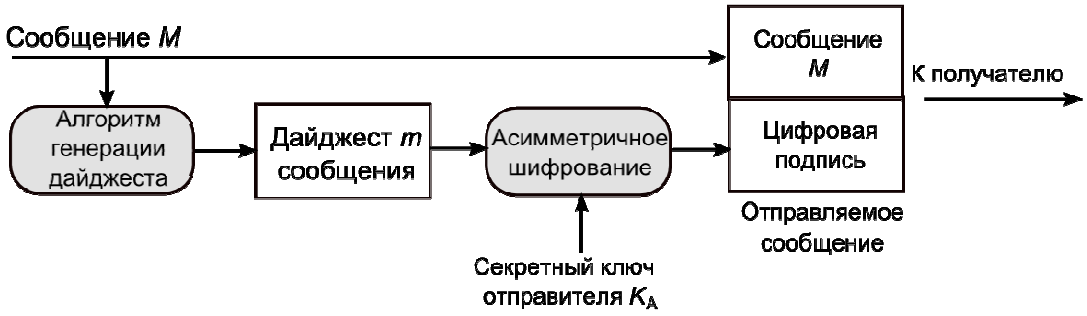


Рис. 17.1. Схема формирования электронной цифровой подписи

Хэш-функция служит для сжатия исходного подписываемого текста *M* в дайджест – относительно короткое число, состоящее из фиксированного небольшого числа битов и характеризующее весь текст *M* в целом. Далее отправитель *A* шифрует дайджест *m* своим секретным ключом k_A. Получаемая при этом пара чисел представляет собой цифровую подпись для данного текста *M*. Сообщение *M* вместе с цифровой подписью отправляется в адрес получателя [29].

Процедура проверки цифровой подписи

Абоненты сети моет проверить цифровую подпись полученного сообщения *M* с помощью открытого колюча отправителя K_A этого сообщения (рис. 17.2). [29]

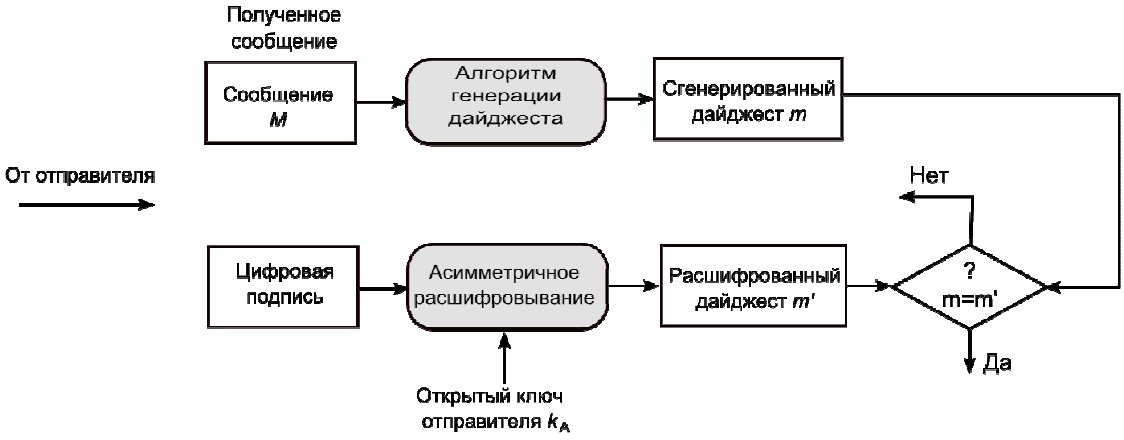


Рис. 17.2. Схема проверки электронной цифровой подписи

При проверке ЭЦП абонент *B* — получатель сообщения *M* — расшифровывает принятый дайджест *m* открытым ключом K_A отправителя *A*. Кроме того, получатель сам

вычисляет с помощью хэш-функции $h(M)$ дайджест m' принятого сообщения M и сравнивает его с расшифрованным. Если эти два дайджеста m и m' совпадают, то цифровая подпись является подлинной. В противном случае либо подпись подделана, либо изменено содержание сообщения [29].

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания. Поэтому необходимо защитить секретный ключ подписывания от несанкционированного доступа. Секретный ключ ЭЦП аналогично ключу симметричного шифрования рекомендуется хранить на персональном ключевом носителе в защищенном виде.

Электронная цифровая подпись представляет собой уникальное число, зависящее от подписываемого документа и секретного ключа абонента. В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей [29].

Помещаемая в подписываемый файл (или в отдельный файл электронной подписи) структура ЭЦП обычно содержит дополнительную информацию, однозначно идентифицирующую автора подписанного документа. Эта информация добавляется к документу до вычисления ЭЦП, что обеспечивает и ее целостность. Каждая подпись содержит следующую информацию:

- ✓ дату подписи;
- ✓ срок окончания действия ключа данной подписи;
- ✓ информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы);
- ✓ идентификатор подписавшего (имя открытого ключа);
- ✓ собственно цифровую подпись.

Важно отметить, что, с точки зрения конечного пользователя, процесс формирования и проверки цифровой подписи отличается от процесса криптографического закрытия передаваемых данных следующими особенностями.

При формировании цифровой подписи используется закрытый ключ отправителя, тогда как при зашифровывании применяется открытый ключ получателя. При проверке цифровой подписи используется открытый ключ отправителя, а при расшифровывании — закрытый ключ получателя.

Проверить сформированную подпись может любое лицо, так как ключ проверки подписи является открытым. При положительном результате проверки подписи делается заключение о подлинности и целостности полученного сообщения, т. е. о том, что это сообщение действительно отправлено тем или иным отправителем и не было

модифицировано при передаче по сети. Однако, если пользователя интересует, не является ли полученное сообщение повторением ранее отправленного или не было ли оно задержано на пути следования, то он должен проверить дату и время его отправки, а при наличии — порядковый номер [29].

Аналогично асимметричному шифрованию, необходимо обеспечить невозможность подмены открытого ключа, используемого для проверки ЭЦП. Если предположить, что злоумышленник *n* имеет доступ к открытым ключам, которые хранит на своем компьютере абонент В, в том числе к открытому ключу K_A абонента *A*, то он может выполнить следующие действия:

- ✓ прочитать из файла, в котором содержится открытый ключ K_A, идентификационную информацию об абоненте *A;*
- ✓ сгенерировать собственную пару ключей k_n и K_n, записав в них идентификационную информацию абонента *A;*
- ✓ подменить хранящийся у абонента *B* открытый ключ K_A своим открытым ключом K_n, но содержащим идентификационную информацию абонента *A*.

После этого злоумышленник *n* может посылать документы абоненту *B*, подписанные своим секретным ключом k_n. При проверке подписи этих документов абонент *B* будет считать, что документы подписаны абонентом *A* и их ЭЦП верна, т.е. они не были модифицированы кем-либо. До выяснения отношений непосредственно с абонентом А у абонента В может не появиться сомнений в подлинности полученных документов. Открытые ключи ЭЦП можно защитить от подмены с помощью соответствующих цифровых сертификатов.

Сегодня существует многообразие видов алгоритмов ЭЦП, в данной практической работе будет рассмотрен алгоритм RSA для формирования ЭЦП.

Применение алгоритма RSA для формирования ЭЦП

Алгоритм RSA (слово образовано от заглавных букв создателей алгоритма Rivest, Shamir и Adleman) – криптографический алгоритм с открытым ключом. RSA стал первым алгоритмом такого типа, пригодным и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений. Безопасность системы RSA определяется вычислительной трудностью разложения на множители больших целых чисел. Недостатком алгоритма цифровой подписи RSA является уязвимость ее к мультипликативной атаке. Другими словами, алгоритм ЭЦП на основе RSA позволяет хакеру без знания секретного ключа сформировать подписи под теми

документами, в которых результат хэширования можно вычислить как произведение результата хэширования уже подписанных документов [27].

Обобщенная схема формирования и проверки электронной цифровой подписи приведена на рис. 17.3.

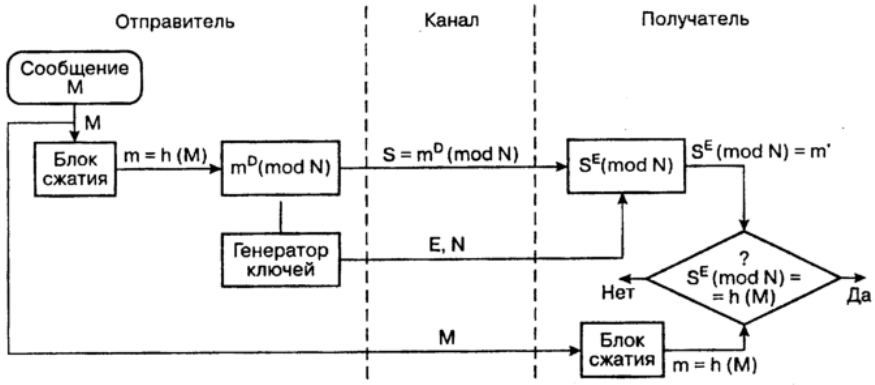


Рис. 17.3. Схема RSA электронной цифровой подписи [27]

ПРАКТИЧЕСКАЯ ЧАСТЬ

ЧАСТЬ I

Изучение алгоритма RSA электронной цифровой подписи

Определение открытого «e» и секретного «d» ключей [27]

Действие отправителя

1. Выбрать два взаимно простых числа p и q;
2. Определить их произведение $n = p \cdot q$;
3. Определить функцию Эйлера $\varphi(n) = (p - 1)(q - 1)$;
4. Выбрать секретный ключ d с учетом условий: $1 < d \leq \varphi(n)$; $НОД(d, \varphi(n)) = 1$;
5. Определить значение открытого ключа e: $e < n$, $e \cdot d \equiv 1 \pmod{\varphi(n)}$.

Формирование электронной цифровой подписи

1. Вычислить хэш-сообщение M: $m = h(M)$;
2. Для получения ЭЦП шифруем хэш-значение m с помощью секретного ключа d и отправляем получателю цифровую подпись $S = m^d \pmod{n}$ и открытый текст сообщения M.

Аутентификация сообщения – проверка подлинности подписи

1. Расшифровкать цифровую подпись S с помощью открытого ключа e и вычислить ее хэш-значения $m' = S^e \pmod{n}$
2. Вычислить хэш-значение принятого открытого текста M

$$m = h(M)$$

3. Сравнить хэш-значения m и m', если $m = m'$, то цифровая подпись S - достоверна.

Пример вычисления хэш-сообщения M: m=h(M)

а) Хэшируемое сообщение M представим как последовательности целых чисел 312. В соответствии с приведенным выше алгоритмом формирования ЭЦП на основе RSA выбираем два взаимно простых числа $p = 3$ и $q = 11$, вычисляем значение $n = p \cdot q = 3 \cdot 11 = 33$, выбираем значение секретного ключа $d = 7$ и вычисляем значение открытого ключа $e = 3$. Вектор инициализации H_0 выбираем равным 6 (выбор производится случайным образом).

Хэш-код сообщения $M = 312$ формируется следующим образом:

$$H_1 = (M_1 + H_0)^2 \pmod n = (3+6)^2 \pmod{33} = 81 \pmod{33} = 15;$$

$$H_2 = (M_2 + H_1)^2 \pmod n = (1+15)^2 \pmod{33} = 256 \pmod{33} = 25;$$

$$H_3 = (M_3 + H_2)^2 \pmod n = (2+25)^2 \pmod{33} = 729 \pmod{33} = 3,\ m = 3.$$

б) Для получения ЭЦП шифруем хэш-значение m с помощью секретного ключа d и отправляем получателю цифровую подпись

$$S = m^d \ (mod\ n)$$ и открытый текст сообщения M

$$S = 3^7 \ (mod\ 33) = 2187 \ (mod\ 33) = 9$$

в) Проверка подлинности ЭЦП

Расшифровка S (т.е. вычисление её хэш-значения m') производится с помощью открытого ключа e.

$$m' = S^e \pmod n = 9^3 \pmod{33} = 729 \pmod{33} = 3$$

г) Сравниваем значения m и m', если $m = m'$, то подпись достоверна.

Примечание: Самое сложное в данной задаче – это определение открытого ключа e. Данный ключ необходимо находить при помощи обратного алгоритма Евклида. Рассмотрим пример для простых чисел p=7, q=11, d = 37.

$e = d^{-1} \bmod (p-1)(q-1)$

$e = 37^{-1} \bmod 60$

$60 = 37 \cdot \underline{1} + 23$

$37 = 23 \cdot \underline{1} + 14$

$23 = 14 \cdot \underline{1} + 9$

$14 = 9 \cdot \underline{1} + 5$

$9 = 5 \cdot \underline{1} + 4$

$5 = 4 \cdot \underline{1} + 1$

$4 = 1 \bullet \underline{4} + 0$

Выписываем в таблицу частные всех операций алгоритма (подчеркнутые числа):

X - частное

X	1	1	1	1	1	1	4
y	1	2	3	5	8	13	60

Вычисляем значения Y по формулам:

$x_1 = y_1$ = первому частному

$y_2 = y_1 \bullet x_2 + x_2$

$y_n = y_{n-1} \bullet x_n + y_{n-2}$

Последнее число в таблице 60 = 13 • 4 + 8 считается для проверки. Предпоследнее перед ним — 13 – это и есть мультипликативное обратное в кольце чисел, .т.е. значение открытого ключа.

Как правило, при больших значениях чисел n и q вычисление открытого ключа становится непосильной вычислетельной задачей, к тому же совершенно бессмысленной. На сегодняшний день имеется множество программ генерирующих пару открытый/секретный ключ. При выполнении данного задания предлагается воспользоваться для этой цели ресурсами сайта http://www.langenhoven.com/code/emailencrypt/keygen.php .

На основе теоретического материала и рассмотренного примера сформировать электронную цифровую подпись методом RSA (значение чисел *p, q, M* и H_0 выдается преподавателем индивидуально для каждого студента). При выполнении расчетов можно пользоваться встроенным стандартным калькулятором Windows и табличным процессором MS Excel (OpenOffice).

При оформлении отчета необходимо указать в правом верхнем углу ФИО студента. Отчет должен содержать следующие вычисления:

1) Рассчитанное значение функции Эйлера;
2) Секретный ключ *d*, выбранный исходя из требований алгоритма RSA;
3) Рассчитанное значение открытого ключа *e*;
4) Значение хэш-кода сообщения *M*;
5) Электронную цифровую подпись *S*;
6) Проверку подлинности ЭЦП (проверить выполнение условия m = m'.

ЧАСТЬ II

1) Студенты предварительно (в рамках самостоятельной работы) готовят кейсы по теме «Злоумышленные действия над электронным документооборотом», в которых они должны придумать реальные ситуации по 5 видам злоумышленных действий – активный перехват, маскарад, ренегатство, подмена, повтор.

2) Преподаватель раздает кейсы остальным студентам в произвольном порядке. Далее дается время на обдумывание задачи и представление ее решения. В решении должно содержаться предложение относительного того, какие методы защиты документов необходимо было применить для предотвращения возникшей ситуации злоумышленного характера.

3) Решение обсуждается, заслушивают иные мнения и варианты решения.

4) Делается коллективный вывод о лучшем решении.

КОНТРОЛЬНЫЕ ВОПРОСЫ ПО ТЕМЕ

1) Объясните процесс формирования ЭЦП.
2) Объясните процесс проверки ЭЦП.
3) Что является целью аутентификации электронных документов?
4) Какие угрозы могут стоять перед электронным документом?
5) Что такое дайджест сообщения?
6) Откуда получил название алгоритм RSA?
7) Рассказать основной принцип, на котором основан алгоритм RSA.
8) Назовете процедуры, которые составляют систему электронной цифровой подписи.
9) Основное назначение электронной цифровой подписи и условие ее существования.
10) На чем основана концепция формирования ЭЦП?
11) Дать пояснения к блок-схеме алгоритма RSA.

ПРИМЕР КОНТРОЛЬНОГО ТЕСТИРОВАНИЯ ЗА СЕМЕСТР ПО ТЕМАМ ЛЕКЦИЙ И ЛАБОРАТОРНЫХ РАБОТ № 9-17 НАХОДИТСЯ В ПРИЛОЖЕНИИ В К МЕТОДИЧЕСКИМ РЕКОМЕНДАЦИЯМ.

ПРИЛОЖЕНИЕ А

ПРИМЕР КОНТРОЛЬНОГО ТЕСТИРОВАНИЯ ЗА 7 СЕМЕСТР

Вопрос № 1

Какой из подходов управления бизнес-процессами является традиционным и устаревшим?

а) ERP (Enterprise Resourse Planning)
б) SCM (Supply Chain Management)
в) CRM (Customer Relationship management)
г) CSRP (Customer synchronized resource planning)

Вопрос № 2

Какое из представленных средств не является средством структурного и объектно-ориентированного анализа бизнес-процессов?

а) IDEF
б) UDP
в) DFD
г) BPMN

Вопрос № 3

Что представляет собой нотация IDEF0?

а) унифицированный язык моделирования
б) диаграмму потоков данных
в) систему условных обозначений для моделирования бизнес-процессов
г) методологию функционального моделирования

Вопрос № 4

Что представляет собой нотация BPMN?

а) унифицированный язык моделирования
б) диаграмму потоков данных
в) систему условных обозначений для моделирования бизнес-процессов
г) методологию функционального моделирования

Вопрос № 5

Что представляет собой нотацияUML?

а) унифицированный язык моделирования
б) диаграмму потоков данных
в) систему условных обозначений для моделирования бизнес-процессов
г) методологию функционального моделирования

Вопрос № 6

Что представляет собой нотация Data WorkFlow?

а) унифицированный язык моделирования
б) диаграмму потоков данных
в) систему условных обозначений для моделирования бизнес-процессов
г) методологию функционального моделирования

Вопрос № 7

Какой из представленных типов модели отображает «снимок» состояния дел организации?

а) TO IS
б) AS IS
в) TO BE
г) AS BE

Вопрос № 8

Разделение объекта на блоки и дуги в нотации IDEF0 называется …?

а) декомпозицией
б) реструктуризацией
в) деструктуризацией
г) разбивкой

Вопрос № 9

Главная диаграмма в нотации IDEF0, показывающая общее положение дел в выбранном отделе предприятия называется …?

а) верховной
б) контекстной
в) наивысшей
г) main

Вопрос № 10

Разделение объекта на блоки и дуги в нотации IDEF0 называется …?

а) декомпозицией
б) реструктуризацией
в) деструктуризацией
г) разбивкой

Вопрос № 11

Схема кодирования дуг ICOM в нотации IDEF0 означает следующее…?

а) I – introduction, C – control, O – output, M - mechanism
б) I – input, C – combination, O – output, M - mechanism
в) I – input, C – control, O – output, M - mechanical
г) I – input, C – control, O – output, M - mechanism

Вопрос № 12

Что из представленного не является видом информационного менеджмента?

а) управление публикациями
б) управление публикациями
в) управление инвестициями
г) управление документацией

Вопрос № 13

Какая из представленных компаний разработала концепцию управления эксплуатацией информационной системой на основе ITIL?

а) Microsoft
б) IBM
в) Apple
г) Hewlett-Packard

Вопрос № 14

Какая из указанных задач не является задачей информационного менеджмента?

а) управление кредитами в среде информационной системы
б) Развитие и обслуживание информационных систем
в) планирование в среде информационной системы
г) управление финансами в области информационных систем

Вопрос № 15

Какая из представленных конструкций относится только к нотации BPMN?

а) актер
б) артефакты
в) сущность
г) комментарии

Вопрос № 16

Какой из объектов не входит в конфигурацию «Сущности» в нотации BPMN?

а) действие (activity)
б) порт (gateway)
в) участники (swimlanes)
г) событие (event)

Вопрос № 17

Как называется задача, которая в нотации BPMN вызывается в случае отмены другой задачи?

а) циклическая
б) откат
в) множественная
г) I мультивариативная

Вопрос № 18

Какой тип диаграммы невозможно построить средствами нотации UML?

а) компонентов
б) пакетов
в) деятельности
г) преобразования

Вопрос № 19

Какой тип диаграмм используется в UML для моделирования бизнес-процессов, технологических процессов, последовательных и параллельных вычислений?

а) синхронизации
б) вариантов использования
в) деятельности
г) пакетов

Вопрос № 20

Какое второе название имеет диаграмма прецедентов в UML?

а) синхронизации
б) вариантов использования
в) деятельности
г) пакетов

ПРИЛОЖЕНИЕ В

КОНТРОЛЬНОЕ ТЕСТИРОВАНИЕ ЗА 8 СЕМЕСТР

Вопрос № 1

Что из перечисленного не входит в понятие уязвимости вычислительной системы?

а) исполнение команды от имени другого пользователя

б) получение доступ к информации, закрытой от доступа для данного пользователя

в) произведение атак типа «отказ в обслуживании»

г) выполнение макроса Excel при запуске

Вопрос № 2

Какое сетевой червь, обнаруженный в январе 2003 г. поразил порядка 75 тысяч компьютеров по всему миру за первые 15 минут его инициализации?

а) Slammer

б) CodeRed

в) Spida

г) LOVEYOU

Вопрос № 3

Обобщенная схема построения комплексной защиты компьютерной сети предприятия называется - …?

а) Life-saving Security

б) Lifecycle Tools

в) Life-office Security

г) Lifecycle Security

Вопрос № 4

Уровень защиты периметра в модели многоуровневой защиты определяет …?

а) обеспечение безопасности передаваемого внутри сети трафика и сетевой инфраструктуры

б) меры по ограничению физического доступа к ресурсам системы

в) меры безопасности в "точках входа" в защищаемую сеть из внешних, потенциально опасных

г) наличие документированных организационных мер защиты (процедур) и порядка информирования о происшествиях, обучение пользователей в области информационной безопасности

Вопрос № 5

Уровень политики безопасности в модели многоуровневой защиты включает …?

а) обеспечение безопасности передаваемого внутри сети трафика и сетевой инфраструктуры

б) меры по ограничению физического доступа к ресурсам системы

в) меры безопасности в "точках входа" в защищаемую сеть из внешних, потенциально опасных

г) наличие документированных организационных мер защиты (процедур) и порядка информирования о происшествиях, обучение пользователей в области информационной безопасности

Вопрос № 6

Уровень физической защиты в модели многоуровневой защиты включает …?

а) обеспечение безопасности передаваемого внутри сети трафика и сетевой инфраструктуры

б) меры по ограничению физического доступа к ресурсам системы

в) меры безопасности в "точках входа" в защищаемую сеть из внешних, потенциально опасных

г) наличие документированных организационных мер защиты (процедур) и порядка информирования о происшествиях, обучение пользователей в области информационной безопасности

Вопрос № 7

Уровень защиты внутренней сети в модели многоуровневой защиты отвечает за…?

а) обеспечение безопасности передаваемого внутри сети трафика и сетевой инфраструктуры

б) меры по ограничению физического доступа к ресурсам системы

в) меры безопасности в "точках входа" в защищаемую сеть из внешних, потенциально опасных

г) наличие документированных организационных мер защиты (процедур) и порядка информирования о происшествиях, обучение пользователей в области информационной безопасности

Вопрос № 8

Какой из международных стандартов безопасности был принят в России как ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий"

а) ISO/IEC 17799
б) ISO 15408
в) ISO/IEC 27002
г) ISO/IEC 27001

Вопрос № 9

Какой из классов функциональных требований не входит в перечень стандарта ISO 15408 по требованиям безопасности?

а) оценка рисков
б) управление безопасностью
в) аудит безопасности
г) идентификация и аутентификация

Вопрос № 10

Основой для создания задания по безопасности, которое можно рассматривать как технический проект для разработки объекта оценки служит ….

а) уровень защиты
б) критерии защиты
в) каталог защиты
г) профиль защиты

Вопрос № 11

В общем виде процесс шифрования описывается выражением вида $C=E_k(P)$, здесь C – это ….?

а) ключ шифрования
б) шифротекст
в) функция шифрования
г) открытый текст

Вопрос № 12

В общем виде процесс шифрования описывается выражением вида $C=E_k(P)$, здесь E – это ….?

а) ключ шифрования
б) шифротекст
в) функция шифрования
г) открытый текст

Вопрос № 13

В общем виде процесс шифрования описывается выражением вида $C=E_k(P)$, здесь k – это ….?

а) ключ шифрования
б) шифротекст
в) функция шифрования
г) открытый текст

Вопрос № 14

В общем виде процесс шифрования описывается выражением вида $C=E_k(P)$, здесь P – это ….?

а) ключ шифрования
б) шифротекст
в) функция шифрования
г) открытый текст

Вопрос № 15

Как называется наука о методах дешифрования?

а) криптоанализ
б) криптойстойкость
в) криптограмма
г) криптосистема

Вопрос № 16

На чем основана концепция электронной цифровой подписи?

а) на обратимости асимметричных шифров
б) на обратимости криптограмм
в) на обратимости симметричных шифров
г) на обратимости хэш-функций

Вопрос № 17

Что является недостатком алгоритма цифровой подписи RSA?

а) вычислительной трудностью разложения на множители больших целых чисел
б) уязвимость к мультипликативной атаке
в) пригодность и для шифрования, и для цифровой подписи
г) использование однонаправленных функций

Вопрос № 18

По способу заражения вирусы бывают ….?

а) резидентными б) сетевыми
в) файловыми г) опасными

Вопрос № 19

По деструктивным возможностям вирусы бывают ….?

а) резидентными б) сетевыми
в) файловыми г) опасными

Вопрос № 20

Стелс-вирусы относятся к классу ….

а) файловых б) бутовых
в) сетевых г) загрузочных

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ И ИСТОЧНИКОВ

1. Официальный русскоязычный сайт проекта Ramus. Ramus Educational. [Электронный ресурс]. Режим доступа: http://ramussoftware.com/index.php?option=com_content&view=article&id=10&Itemid=16 (Дата обращения 18.01.2013 г.);

2. Грекул В.И. Проектирование информационных систем. Лекция № 7 «Моделирование бизнес-процессов средствами BPWin». Интернет-Университет информационных технологий – ИНТУИТ. [Электронный ресурс]. Режим доступа: http://www.intuit.ru/department/se/devis/7/ (Дата обращения 18.01.2013 г.);

3. Методы и модели информационного менеджмента / Д.В. Александров, Р.И. Макаров, Е.Р. Хорошева; под. ред. А.В. Кострова. – М.: Финансы и статистика, 2007. - 336 с.;

4. Бабич А.В. Введение в UML. – Итернет-Университет информационных технологий - ИНТУИТ. [Электронный ресурс]. Режим доступа: http://www.intuit.ru/department/se/intuml/1/2.html (Дата обращения 18.01.2013 г.);

5. Леоненков А.В. Нотация и семантика языка UML. Лекция 11. «Элементы графической нотации диаграммы деятельности». – Интернет-университет информационных технологий ИНТУИТ. [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/department/pl/umlbasics/11/4.html (Дата обращения 18.01.2013 г.);

6. Стасышина Т.Л. Диаграммы прецедентов. [Электронный ресурс]. - Режим доступа: http://ciu.nstu.ru/kaf/persons/1914/study/baz_dannh/4.kursovoiy_proekt/ (Дата обращения 18.01.2013 г.);

7. Фаулер М. UML. Краткое руководство по стандартному языку объектного моделирования / М. Фаулер. – СПб.: Символ-Плюс, 2011. – 192 с.;

8. Леоненков А. В. Нотация и семантика языка UML. Лекция 3 «Элементы графической нотации диаграммы вариантов использования». Интернет-университет информационных технологий - ИНТУИТ. [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/department/pl/umlbasics/3/2.html (Дата обращения 18.01.2013 г.).;

9. Киммел П. UML. Универсальный язык программирования / П. Киммел. – М.: НТ-Пресс, 2008. – 272 с.;

10. Буч Г., Рамбо Дж., Якобсон И. Введение в UML от создателей языка / Г. Буч, Дж. Рамбо, И. Якобсон. – М.: ДМК Пресс, 2011. – 496 с.;

11. Леоненков А. В. Нотация и семантика языка UML. Лекция 8 «Элементы графической нотации диаграммы последовательности». Интернет-университет

информационных технологий - ИНТУИТ. [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/department/pl/umlbasics/8/ (Дата обращения 18.01.2013 г.);

12. Рожкова Е. Case-средства. Сравнительный анализ. ARIS-rational. [Электронный ресурс]. Режим доступа: http://ocnova.ru/?p=334. (Дата обращения 19.01.2013 г.);

13. Кознов Д.В. Визуальное моделирование: теория и практика. Лекция № 9 «Визуальное моделирование бизнес-процессов». Интернет-Университет информационных технологий - ИНТУИТ. [Электронный ресурс]. Режим доступа: http://www.intuit.ru/department/se/vismodtp/9/ (Дата обращения 18.01.2013 г.);

14. BPMN. Материал из Википедиии свободной энциклопедии. [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/BPMN. (Дата обращения 18.01.2013 г.);

15. Семухина А.С., Никифоров Д.А. Пример автоматизации некоторых поддерживающих бизнес-процессов в медицинском учреждении // Электронный научный журнал «Системная интеграция и здравоохранение». [Электронный ресурс]. Режим доступа www.sys-int.ru. №4(10). 2010. С. 76-84.(Дата обращения 18.01.2013 г.);

16. Нестеров С.А. Анализ и управление рисками в операционных системах на базе операционных систем Microsoft. Лекция 2. «Современные стандарты в области информационной безопасности, использующие концепцию управления рисками» - Интернет-университет информационных технологий - ИНТУИТ. [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/department/itmngt/riskanms/2/ (Дата обращения 18.01.2013 г);

17. Безопасность информационных технологий. Руководящий документ Гостехкомиссии России № 187 от 19.06.02;

18. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Библиотека ГОСТов. – Режим доступа: http://vsegost.com/Catalog/57/5736.shtml (Дата обращения 20.01.2013 г.);

19. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft. Лекция 4 «Методики и программные продукты для оценки рисков». Интернет-университет информационных технологий - ИНТУИТ. [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/department/itmngt/riskanms/4/ (Дата обращения 18.01.2013 г.);

20. Аудит информационной безопасности. Материал из Википедии свободной энциклопедии. [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/Аудит_информационной_безопасности (Дата обращения 20.01.2012 г.);

21. Эффективные решения. Информационная безопасность. Аудит информационной безопасности. [Электронный ресурс]. Режим доступа: http://efsol.ru/it-services/audit_its.html (Дата обращения 20.01.2013 г.);

22. Нестеров С.А. Анализ и управление рисками в операционных системах на базе операционных систем Microsoft. Лекция 3. «Методики построения систем защиты информации». Интернет университет информационных технологий - ИНТУИТ. [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/department/itmngt/riskanms/3/ (Дата обращения 18.01.2013 г.);

23. Энциклопедия безопасности Касперского. // Программные уязвимости Режим доступа: http://www.securelist.com/ru/threats/vulnerabilities?chapter=142 (Дата обращения 18.01.2013 г.);

24. Установка и применение программы PGP. [Электронный ресурс]. Режим доступа: http://www.gloffs.com/pgp.htm (Дата обращения 18.01.2013 г.);

25. OpenPGP в России. [Электронный ресурс]. Режим доступа: https://www.pgpru.com/faq/obschie#h46-3 (Дата обращения 18.01.13 г.);

26. Заркумова Р.Н. Исследование количественных характеристик системы парольной защиты информации. Сборник научных трудов НГТУ. – 2010. - № 2(60). С. 83-88.;

27. Балабанов П.В., Пономарев С.В. Системы автоматизированного расчёта в управлении качеством и при защите информации : лабораторные работы / сост.: П.В. Балабанов, С.В. Пономарёв. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2009. – 32 с. [Электронный ресурс]. – Режим доступа: http://www.234555.ru/publ/12-1-0-408 (Дата обращения 18.01.2013).

28. Сингх С. Книга шифров. Тайная история шифров и их расшифровки / С. Сингх. – М.: АСТ: Астрель, 2009. 447 с.

29. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. – М. : ИД «ФОРУМ» : ИНФРА-М, 2010. – 592 с.