Министерство образования и науки Российской Федерации
Государственное образовательное учреждение высшего профессионального образования
«Томский государственный университет систем управления и радиоэлектроники»

УТВЕРЖДАЮ

Заведующий кафедрой
«Управление инновациями»

_____ /*А.Ф.Уваров*
(подпись) *(ФИО)*
"_____" _____ 2011 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ЛАБОРАТОРНЫМ РАБОТАМ

по дисциплине

«Информационные технологии в управлении качеством и защита информации»

Составлены кафедрой «Управление инновациями»

Для студентов, обучающихся
по специальности 220500 «Управление качеством».

Форма обучения очная

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

" 01 " ноября 2011 г.

Томск 2011 г.

Введение

Изучению дисциплины «Информационные технологии в управлении качеством и защита информации» (уровень дисциплины федеральный (ГОСовский)) отводится одно из важнейших мест при подготовке дипломированных специалистов по специальности 220500 «Управление качеством».

По курсу «Информационные технологии в управлении качеством и защита информации» предусмотрены лабораторные работы в двух семестр, ориентированные на практическое закрепление лекционного материала. Лабораторные работы направлены на формирование у студентов навыков моделирования бизнес-процессов организаций (предприятий) различного уровня; формирование знаний о классах и критериях существующих угроз информационной безопасности; терминологией и основными понятиями теории безопасности информации; ознакомление с международной и российской нормативно-правовой базой в области защиты информации.

На изучение курса «Информационные технологии в управлении качеством и защита информации» согласно учебному плану специальности 220500 «Управление качеством» отводится два семестра. Курс логически разбит на два блока. Лабораторные работы первого блока изучаются в осеннем семестре и направлены на формирование навыков моделирования простых бизнес-процессов предприятия в различных нотациях. Данное разбиение курса является целесообразным и полностью коррелирует с выполнением студентами курсовой работы по данной дисциплине в осеннем семестре.

В первый блок входит 6 лабораторных работ, длительностью 4 академических часа и один академический час 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 написании курсовых работ. Таким образом, максимально оптимизируется учебный процесс при посещении студентами лекций, лабораторных работ и написание курсовой работы.

Во второй блок входит 8 лабораторных работ, ориентированных на формирование навыков разработки 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.

Перед текстом каждой лабораторной работы указаны два типа литературных источников. Источники первого типа являются ссылками на литературу, фрагменты которой использовались при разработке данных методических рекомендаций. Ссылки на

эти источники приводятся в тексте лабораторных работ. Литература данного типа входит в текст лабораторных работ, используется только на аудиторных занятиях и не требует дополнительного самостоятельного изучения. Источники второго типа являются дополнительными, предназначенными для самостоятельной работы студентов. При помощи дополнительной литературы студенты могут более тщательно проработать теоретический материал лабораторных работ и подготовиться к защите лабораторных работ. Кроме того дополнительная литература будет полезной при подготовке к итоговому тестированию за семестр.

Требования к знаниям студентов

Для полноценного изучения дисциплины «Информационные технологии в управлении качеством и защита информации» студентам обязательным условием является освоение ряда дисциплин:

1. Информатика;
2. Информационное обеспечение, базы данных
3. Менеджмент и маркетинг.

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

1. Моделирование систем;
2. Основы обеспечения качества;
3. Всеобщее управление качеством;
4. Делопроизводство.

Ход выполнения лабораторных работ

Лабораторные работы содержат три основные части:

1. Теоретическая часть
2. Практическая часть
3. Вопросы для самоконтроля.

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 вопросы для самоконтроля.

Правила работы в компьютерном классе

Для наиболее эффективной работы в компьютерном классе 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 BPWin.

Оборудование: компьютеры с операционной системой Windows XP и выше, наличие любой программы поддерживающей нотацию BPMN (в данной лабораторной работе использовалась программа BPWin).

При подготовке лабораторной работы использованы материалы: 1) Грекул В.И. Проектирование информационных систем. – Интернет-университет информационных технологий ИНТУИТ. - URL: http://www.intuit.ru/department/se/devis/1/3.html/. (Режим доступа: требуется регистрация); 2) Методы и модели информационного менеджмента. Под ред. А.В. Кострова. – М.: Финансы и статистка, 2007

Дополнительная литература: 1) Елиферов В.Г., Репин В.В. Процессный подход к управлению. Моделирование бизнес-процессов. – М.: Стандарты и качество, 2009. 408 с. 2) Справочные материалы по информационным технологиям. BPWin. URL: http://itteach.ru/bpwin/ (Режим доступа: свободный); 3) Сериков А.В., Титов Н.В. Компьютерное моделирование бизнес-процессов. – М.: Бурун-книга, 2007. – 304 с.

Теоретическая часть

BPwin имеет достаточно простой и интуитивно понятный интерфейс пользователя. При запуске BPwin по умолчанию появляется основная панель инструментов, палитра инструментов (вид которой зависит от выбранной нотации) и, в левой части, навигатор модели — Model Explorer [1].

При создании новой модели возникает диалог, в котором следует указать, будет ли создана модель заново или она будет открыта из файла либо из репозитория ModelMart, затем внести имя модели и выбрать методологию, в которой будет построена модель.

Модель в BPwin 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.

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.

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.

Модель может содержать четыре типа диаграмм [2]:

- ✓ контекстную диаграмму (в каждой модели может быть только одна контекстная диаграмма);
- ✓ диаграммы декомпозиции;
- ✓ диаграммы дерева узлов;
- ✓ диаграммы только для экспозиции (FEO).

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.

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.

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. 1.9 все работы еще не были декомпозированы.

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

В IDEF0 различают пять типов стрелок:

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.

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.

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.

Механизм (Mechanism) — ресурсы, которые выполняют работу, например персонал предприятия, станки, устройства и т. д. Стрелка механизма рисуется как входящая в нижнюю грань работы. По усмотрению аналитика стрелки механизма могут не изображаться в модели.

Вызов (Call) — специальная стрелка, указывающая на другую модель работы. Стрелка вызова рисуется как исходящая из нижней грани работы. В BPwin стрелки вызова используются в механизме слияния и разделения моделей.

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.

Связь по входу (**output-input**), когда стрелка выхода вышестоящей работы (далее — просто выход) направляется на вход нижестоящей.

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.

Обратная связь по входу (output-input feedback), когда выход нижестоящей работы направляется на вход вышестоящей. Такая связь, как правило, используется для описания циклов.

Обратная связь по управлению (output-control feedback), когда выход нижестоящей работы направляется на управление вышестоящей. Обратная связь по управлению часто свидетельствует об эффективности бизнес-процесса.

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.

Практическая часть

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

Требования к построению учебной модели:

а) Контекстная диаграмма «Деятельности компании Titan» 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.

б) Заполнить свойства диаграммы: General, Status, Model Name, Viewpoint, Purpose, Source.

в) Создать отчет по диаграмме Model Report и сохранить его в txt файл.

построение контекстной диаграммы;

г) Создать диаграмму декомпозиции для работы «Деятельность компании Titan», содержащую работы «Продажи и маркетинг», «Обработка и тестирование компьютеров», «Отгрузка и получение»;

д) Разработать данные (стрелки) внутренние и внешние, обеспечивающие взаимодействие между работами;

е) 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»;

ж) По итогам созданных диаграмм сделать диаграмму дерева узлов и просмотреть правильность построения иерархии.

е) Защитить полученную модель, ответить на вопросы для самоконтроля.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1) Охарактеризуйте современные концепции управления организациями;
2) Перечислите известные методологии структурного системного анализа и проектирования;
3) Перечислите известные языки описания бизнес-процессов;
4) Что понимается под термином «CASE-средства»;
5) Что представляет собой IDEF0-модель?
6) Что понимается под термином «декомпозиция»?
7) Каков синтаксис описания систем в IDEF0?
8) Что такое работа?
9) Сколько блоков декомпозиции рекомендуется создавать при моделировании и почему?
10) Какое смысловое значение имеет расположение работ на диаграммах декомпозиции от верхнего левого угла к правому нижнему?
11) Какова функция стрелок на диаграммах IDEF0?
12) Назовите назначение ICOM-кодов в BPWin?
13) Наличие какой связи свидетельствует о высокой эффективности бизнес-процесса?
14) Объяснить смысл стрелок с квадратными и круглыми скобками на диаграмме IDEF0?

Лабораторная работа № 2.

ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ СРЕДСТВАМИ ПАКЕТА BPWIN

Цель работы: изучение функций стоимостного анализа пакета BPWin для количественной оценки качества созданной модели;

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

При подготовке лабораторной работы использованы материалы: 1) Грекул В.И. Проектирование информационных систем. – Интернет-университет информационных технологий ИНТУИТ. - URL: http://www.intuit.ru/department/se/devis/1/3.html/. (Режим доступа: требуется регистрация); 2) Методы и модели информационного менеджмента. Под ред. А.В. Кострова. – М.: Финансы и статистка, 2007

Дополнительная литература: 1) Елиферов В.Г., Репин В.В. Процессный подход к управлению. Моделирование бизнес-процессов. – М.: Стандарты и качество, 2009. 408 с. 2) Справочные материалы по информационным технологиям. BPWin. URL: http://itteach.ru/bpwin/ (Режим доступа: свободный)/ 3) Сериков А.В., Титов Н.В. Компьютерное моделирование бизнес-процессов. – М.: Бурун-книга, 2007. – 304 с.

Теоретическая часть

Обычно моделирование бизнес-процессов начинается с построения функциональной модели 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.

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 [1].

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.)

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.

Параметры стоимостного анализа задаются на вкладке «ABC Units» окна Model Properties.

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

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.

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. 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.*

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*).

Практическая часть

Пример построения IDEF0-модели бизнес-процесса телевизионной службы новостей и решение задачи ФСА

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 [2].

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 [2]

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 [2].

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 BPWin построить контекстную диаграмму «Функционирование службы информации» (рис. 2.1)

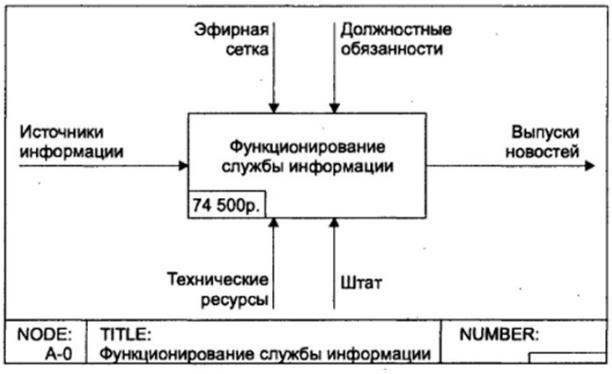


Рис. 2.1. Контекстная диаграммы «Функционирование службы информации»

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

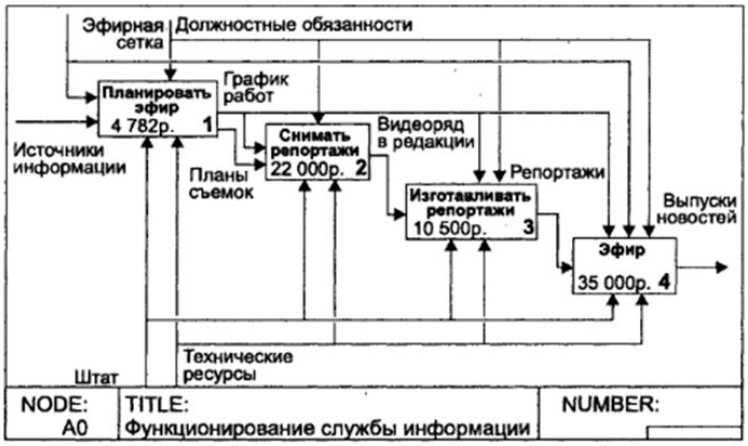


Рис. 2.2. Декомпозиция контекстной диаграммы

Задание № 3. Построить диаграмму «Планировать эфир».

На данном этапе происходит поиск информационных поводов, которые могут стать темами для будущих сюжетов новостей (рис. 2.3).

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. 2.3.) 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.

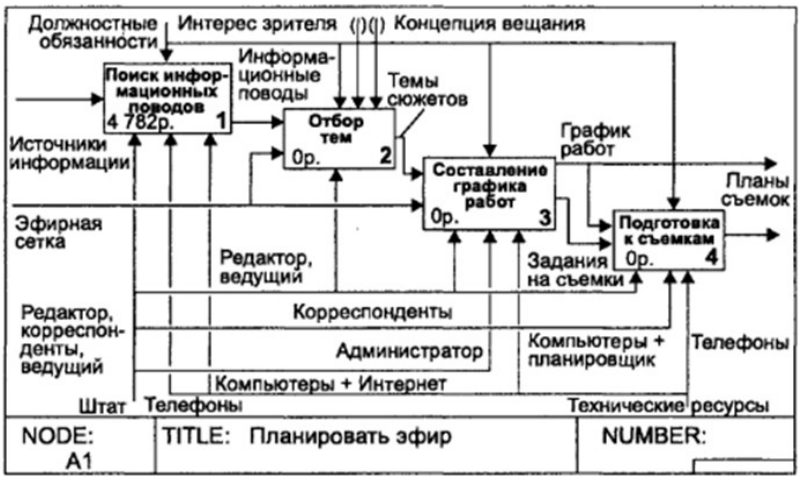


Рис. 2.3. Диаграмма «Планировать эфир»

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

На основе рис. 2.4. построить диаграмму «Поиск информационных поводов», самостоятельно проанализировать работы и стрелки на диаграмме.

Рис. 2.4. 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. 2.5.)

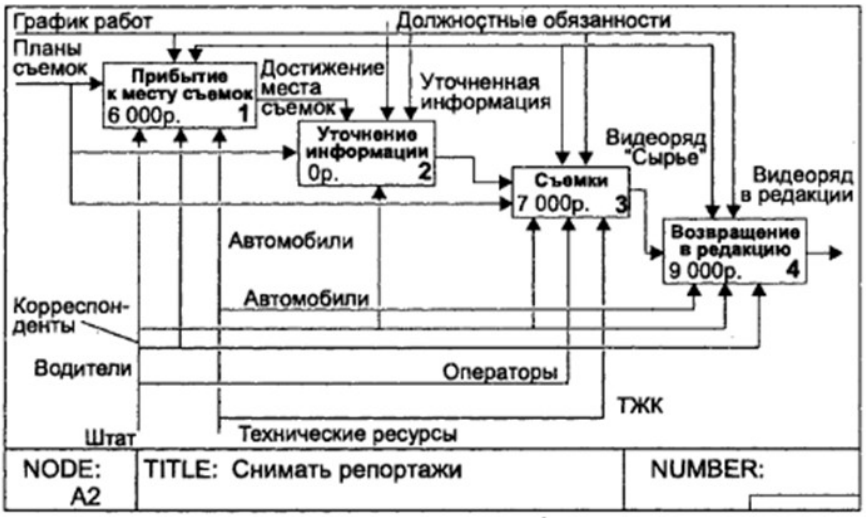


Рис. 2.5. Диаграмма «Снимать репортажи»

Задание № 6. Построить диаграмму «Изготавливать репортажи».

Диаграмма на рис. 2.6. 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.

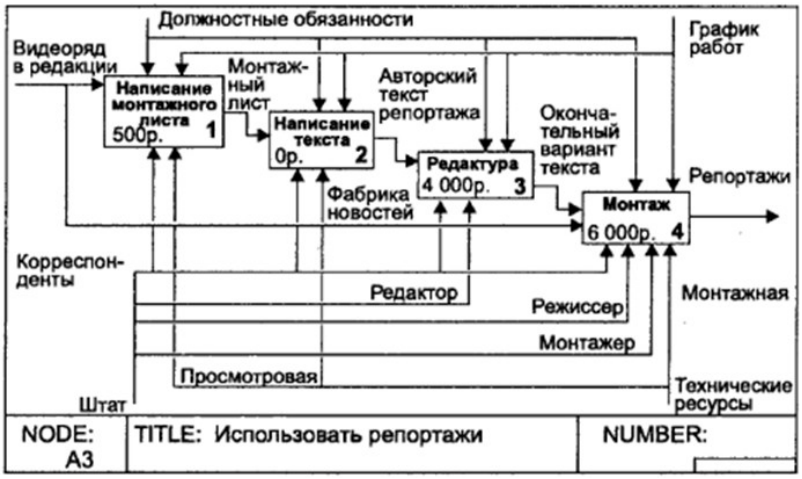


Рис. 2.6. Диаграмма «Изготавливать репортажи»

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. 2.7.).

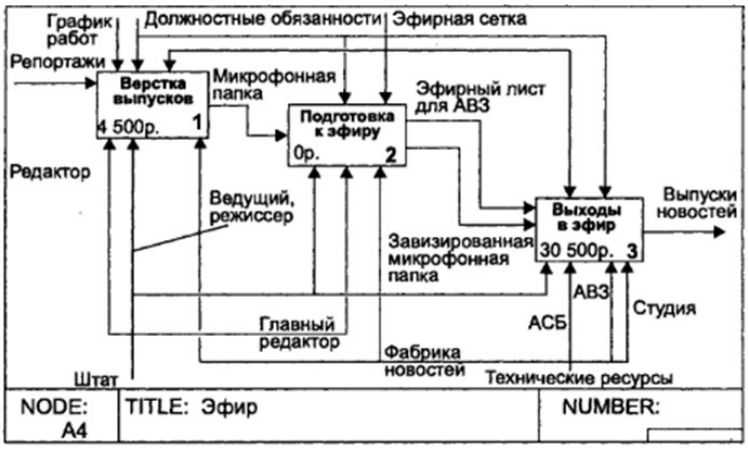


Рис. 2.7. Диаграмма «Эфир»

Задание № 8. Провести функционально-стоимостный анализ работы телевизионной службы новостей.

Одна из методик выполнения ФСА – методика анализа расходов. Финансирование работы телевизионной службы информации осуществляется за счет выделения средсв из общего бюджета предприятия (телевидения). Описание стоимостных характеристик бизнес-процесса внутри информационной службы позволяет сделать анализ расходов и оценить эффективность ее работы. Кроме того, такая модель может помочь руководителям, службе маркетинга и бухгалтерии оптимизировать структуру и функционирование информационной службы. Далее приводится описание экономических характеристик диаграмм модели работы телевизионной службы информации в расчете на один месяц (суммы взяты условно). В таблице 2.1. показаны центры затрат (черным курсивом) и стоимость каждой работы в рамках центра затрат.

Таблица 2.1.

Функционирование службы информации	***Поиск информации в газетах***
Override Decomposition (74500 руб.)	*Override Decomposition* (0 руб.)
Аренда помещения – 4000 руб.	*Compute from Decomposition (142 р.)*
Обслуживание и амортизация оргтехники – 1500 р.	Подписка на газету «АиФ» - 34,80
Оклад водителя – 7000 р.	Подписка на газету «Владимирские ведомости» - 18 р.
Оклад монтажера – 5000 р.	Подписка на газету «Комсомольская правда» - 36 р.
Оклад начальника службы информации – 7000 р.	Подписка на газету «Молва» - 14 р.
Оклад корреспондента – 8000 р.	Подписка на газету «Призыв» - 22 р.
Оклад оператора – 7000 р.	Подписка на газету «Хронометр» - 17 р.
Оклад редактора – 4000 р.	***Поиск информации в интернете***

Оклад режиссера – 4000 р.	*Override Decomposition* (0 руб.)
Оплата за интернет – 7000 р.	*Compute from Decomposition (4750 р.)*
Оплата сотовой связи – 6000 р.	Подписка на ленту новостей «Интерфакс»- 1480 р.
Оплата телефонной связи – 3000 р.	Подписка на ленту новостей «РИА «Новости»»- 1560 р.
Оплата услуг ЖКХ – 3000 р.	Подписка на ленту новостей «Итар-ТАСС»- 1530 р.
Оплата электроэнергии – 6000 р.	***Рассмотрение памятных дат***
Расходы на канцтовары, бумагу – 2000 р.	*Override Decomposition* (0 руб.)
Compute from Decomposition (72282 р.)	*Compute from Decomposition (70 р.)*
Снимать репортажи	Покупка справочников – 70 р.
Override Decomposition (0 руб.)	***Съемки***
Compute from Decomposition (6000 р.)	*Override Decomposition* (0 руб.)
Расходы на бензин – 6000 р.	*Compute from Decomposition (7000 р.)*
	Гонорар оператора – 6000 р.
	Обслуживание и амортизация ТЖК – 1000 р.

Возвращение в редакцию	***Редактура***
Override Decomposition (0 руб.)	*Override Decomposition* (0 руб.)
Compute from Decomposition (9000 р.)	*Compute from Decomposition (70 р.)*
Обслуживание и ремонт автомобилей – 3000 р.	Гонорар редактора – 4000 р.
Расходы на бензин – 6000 р.	***Монтаж***
Написание монтажного листа	*Override Decomposition* (0 руб.)
Override Decomposition (0 руб.)	*Compute from Decomposition (6000 р.)*
Compute from Decomposition (500 р.)	Гонорар корреспондента – 5000 р.
Обслуживание и амортизация просмотровой – 500 р.	Обслуживание и амортизация монтажных комплексов – 1000 р.
Верстка выпусков	***Выходы в эфир***
Override Decomposition (0 руб.)	*Override Decomposition* (0 руб.)
Compute from Decomposition (4500 р.)	*Compute from Decomposition (500 р.)*
Гонорар ведущего – 4500 р.	Гонорар режиссера – 3500 р.
	Обслуживание и амортизация АВЗ – 4000 р.
	Обслуживание и амортизация АСБ – 5000 р.
	Обслуживание студии и амортизация студийной техники – 3000 р.
	Оплата эфирного сигнала – 15000 р.

Таким образом, рассчитанные расходы на функционирование службы информации составили в общем 146 782 руб.

Результаты стоимостного анализа могут существенно повлиять на очередность выполнения работ. Предположим, что для оценки качества изделия необходимо провести три работы:

- ✓ внешний осмотр — стоимость 50 руб.;
- ✓ пробное включение — стоимость 150 руб.;
- ✓ испытание на стенде — стоимость 300 руб.

Предположим также, что с точки зрения технологии очередность проведения работ несущественна, а вероятность выявления брака одинакова (50%). Пусть необходимо проверить восемь изделий. Если проводить работы в убывающем по стоимости порядке, то затраты на получение готового изделия составят:

300 руб. (испытание на стенде)*8 +150 руб. (пробное включение) *4 + 50 руб. (внешний осмотр) *2 = 3100 руб.

Если проводить работы в возрастающем по стоимости порядке, то на получение готового изделия будет затрачено:

50 руб. (внешний осмотр) *8 +150 руб. (пробное включение) *4 + 300 руб. (испытание на стенде) *2 = 1600 руб.

Следовательно, с целью минимизации затрат первой должна быть выполнена наиболее дешевая работа, затем — средняя по стоимости и в конце — наиболее дорогая.

Результаты стоимостного анализа наглядно представляются на специальном отчете BPwin, настройка которого производится в диалоговом окне Activity Cost Report (меню Tools/Reports/Activity Cost Report). Отчет позволяет документировать имя, номер, определение и стоимость работ, как суммарную, так и раздельно по центрам затрат.

Результаты отображаются и непосредственно на диаграммах. В левом нижнем углу прямоугольника работы может показываться либо стоимость (по умолчанию), либо продолжительность, либо частота проведения работы. Настройка отображения осуществляется в диалоге Model Properties (меню Model/Model Properties), закладка Display (ABC Data, ABC Units).

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

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?

Лабораторная работа № 3

ИЗУЧЕНИЕ НОТАЦИИ BPMN И ИНТЕРФЕЙСА TIBCO BUSINESS STUDIO ДЛЯ МОДЕЛИРОВАНИЯ БИЗНЕС-ПРОЦЕССОВ

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)

При подготовке лабораторной работы использованы материалы: 1) Кознов Д.В. Визуальное моделирование: теория и практика. - Интернет-университет информационных технологий. ИНТУИТ. URL: ***http://www.intuit.ru/department/se/vismodtp/9/****. (Режим доступа: требуется регистрация); 2) BPMN. URL: http://ru.wikipedia.org/wiki/BPMN/ (Режим доступа: свободный).*

Дополнительная литература: 1) Все о системном проектировании. URL: http://idefinfo.ru/content/view/434/55// (Режим доступа: свободный) 2) Управление бизнес-процессами URL: http://process.siteedit.ru/page6 (Режим доступа: свободный); 3) White S., Miers D. BPMN Modeling and reference guide. – USA: Future Strategues Inc., 2008. 226 p.

Теоретическая часть

Новая концепция бизнеса - ориентация на бизнес-процессы

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) [1].

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 [2].

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

- ✓ **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 3.1.

Таблица 3.1. 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

а) ДЕЙСТВИЯ (activities)

Процесс состоит из цепочки действий. Действия бывают следующих видов:

- задача - рис. 3.41, а и б ;
- свернутый подпроцесс - рис. 3.2, в и г ;
- развернутый подпроцесс - рис. 3.3, д.

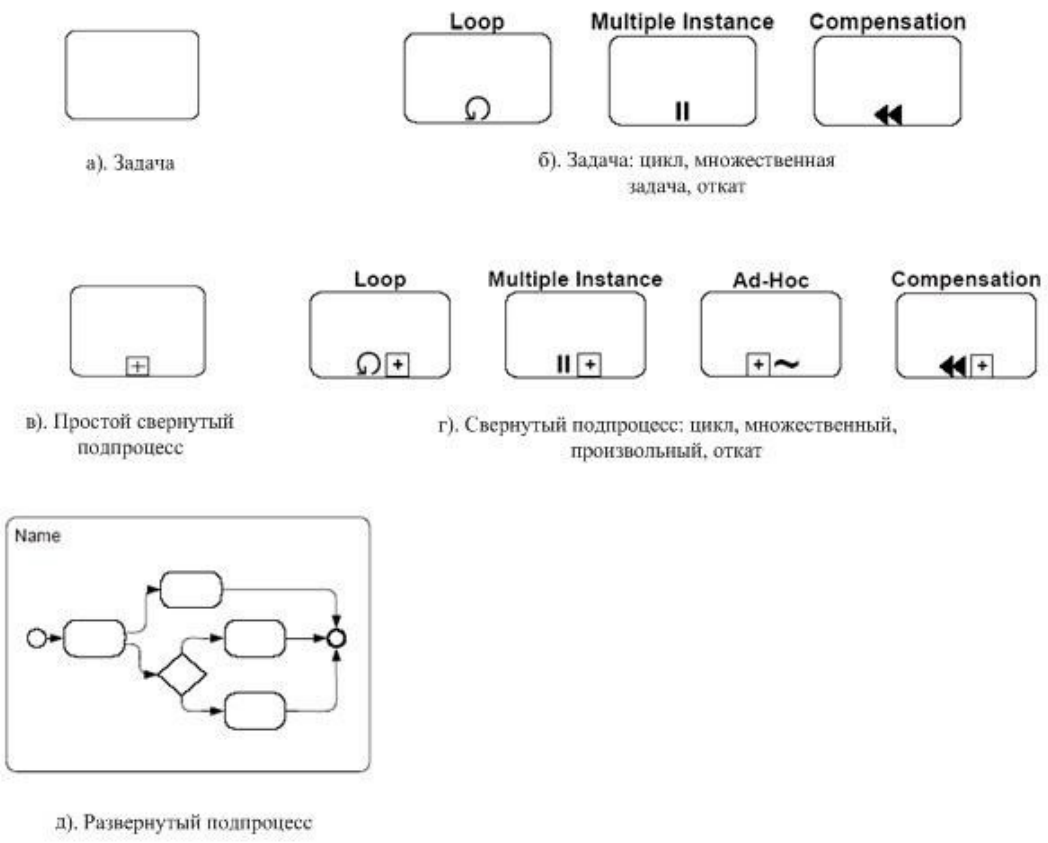


Рис. 3.1. Виды действий

***задача (task*)** - это атомарное действие процесса, неделимое на более элементарные части. На диаграмме задача изображается, как показано на рис. 3.1, а. На рис. 3.1, б приводится три вида задач, которые могут быть заданы в BPMN - циклическая задача, множественная задача и откат.

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.

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).

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. 3.2.

Рис. 3.2. Пример задачи с откатом

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

- ✓ ***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 **ПОДПРОЦЕСС** ***(subprocess)***. Он позволяет разбить сложные процессы на более мелкие. Подпроцессы бывают ***свернутые*** (collapsed subprocesses) - см. рис. 3.1, в и г - и ***развернутые*** (expanded subprocesses) - см. рис. 3.1, 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. 3.1, 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. 3.3.

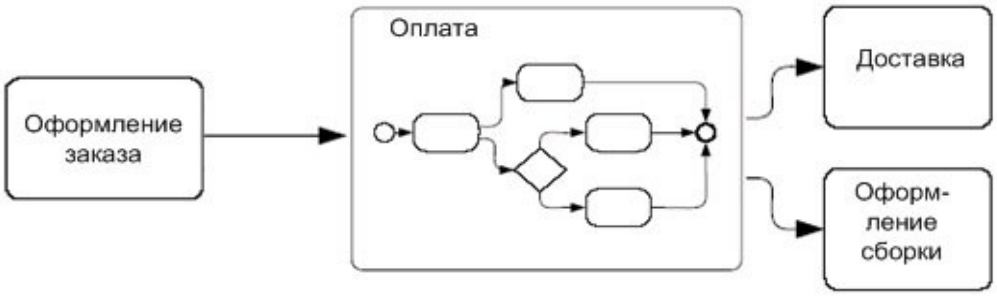


Рис. 3.3. Пример развернутого подпроцесса

б) ПОРТЫ (gateways)

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. 3.4.

На рис. 3.4, 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. 3.4, 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. 3.4, б показан оператор распараллеливания и соединения потоков управления. Как следует из этого рисунка, он может быть изображен с ромбиком и без.

На рис. 3.4, 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).

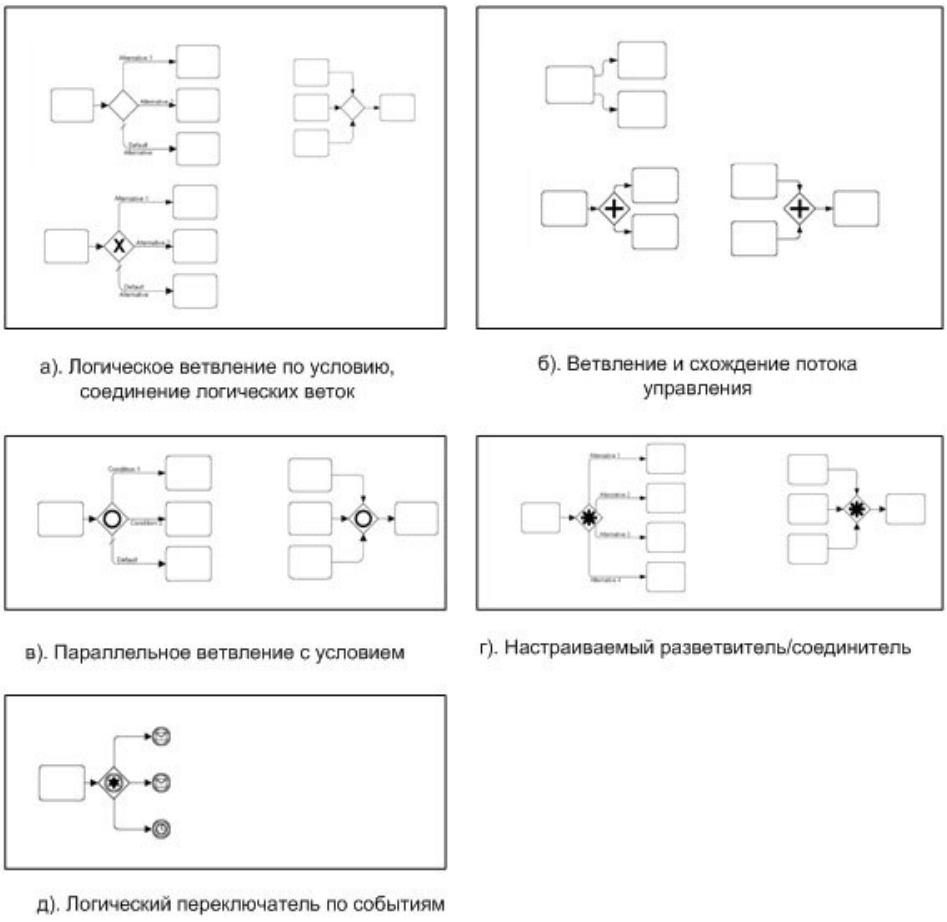


Рис. 3.4. Порты

На рис. 3.4, 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. 3.4 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.

На диаграммах BPMN событие изображается, как показано на рис. 3.5, 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. 3.5. События

Эти типы событий по-разному изображаются на BPMN-спецификациях, как показано на рис. 3.5, б. В контексте этих трех типов события могут различаться по видам - см. рис.3.5, 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.

СВЯЗИ (connecting objects)

На рис. 3.6. показаны связи разного вида, существующие в BPMN:

- ✓ ***поток исполнения*** (sequence flow) - рис. 3.6 а; это самый распространенный вид связи, с его помощью обозначается порядок выполнения действий процесса;
- ✓ ***поток сообщений*** (message flow) - рис. 3.6 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. 3.6 в представлена ассоциация отката; на рис. 3.6 г показана ассоциация исключения;

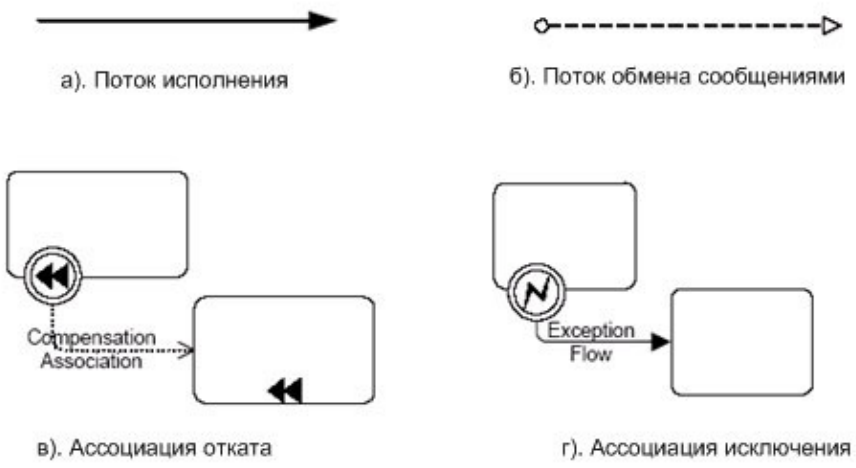


Рис. 3.6. Виды связей

УЧАСТНИКИ (swimlanes) бизнес-процесса

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. 3.7 а.

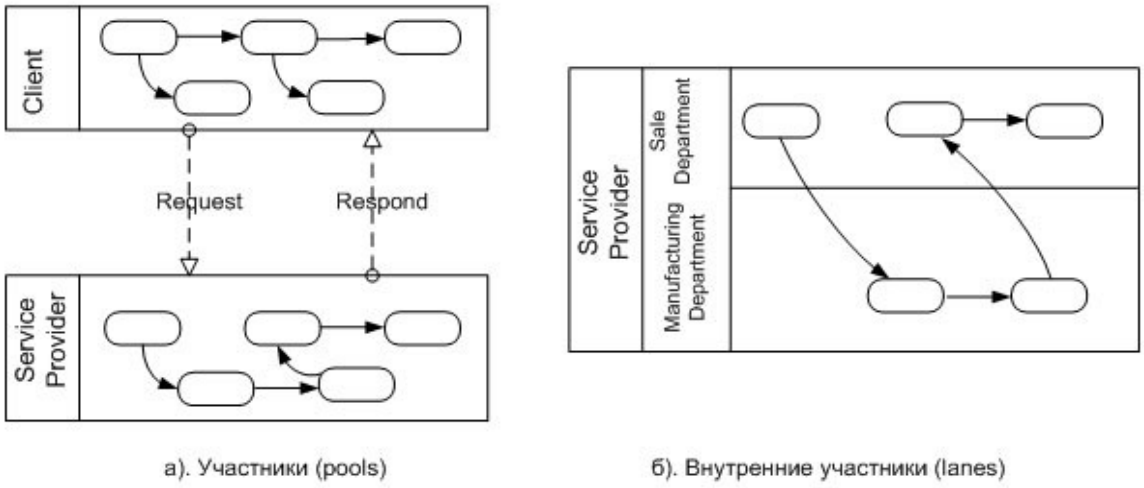


Рис. 3.7. Участники бизнес-процесса

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.

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. 3.7 б показан пример внутренних участников. Так, в компании под названием Service Provider из примера на рис. 3.7 а имеется два отдела - отдел продаж (Sale Department) и производственный отдел (Manufacturing Department). Бизнес-процесс этой компании на рис. 3.7 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

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. 3.8):

Окно состоит из вкладки Диаграммы процессов, куда добавляются элементы модели. Структуры диаграммы (рис. 3.8 левая часть) и палитры инструментов Palette (рис. 3.8 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. 3.8. внизу)

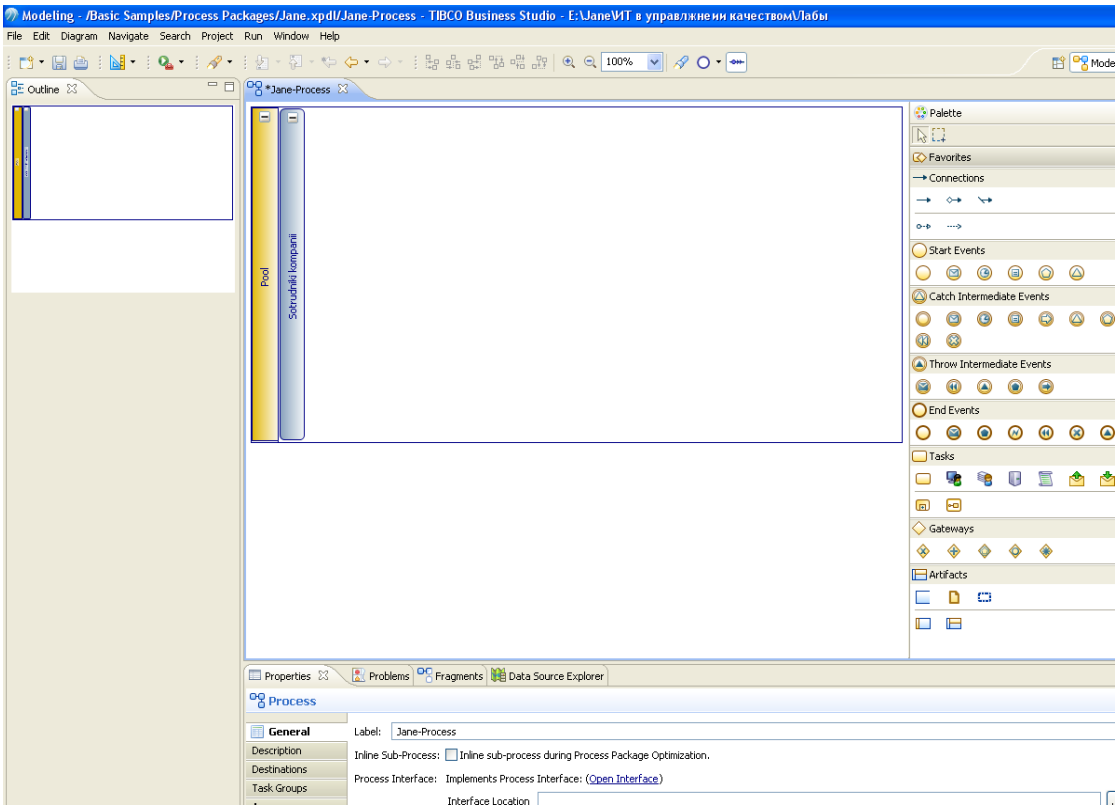


Рис. 3.8. Интерфейс программы TIBCO Business Studio

ЗАДАНИЕ:

1. При помощи программы TIBCO Business Studio создать диаграмму процесса «Обработка запроса о товарах» представленную на рис. 3.9.

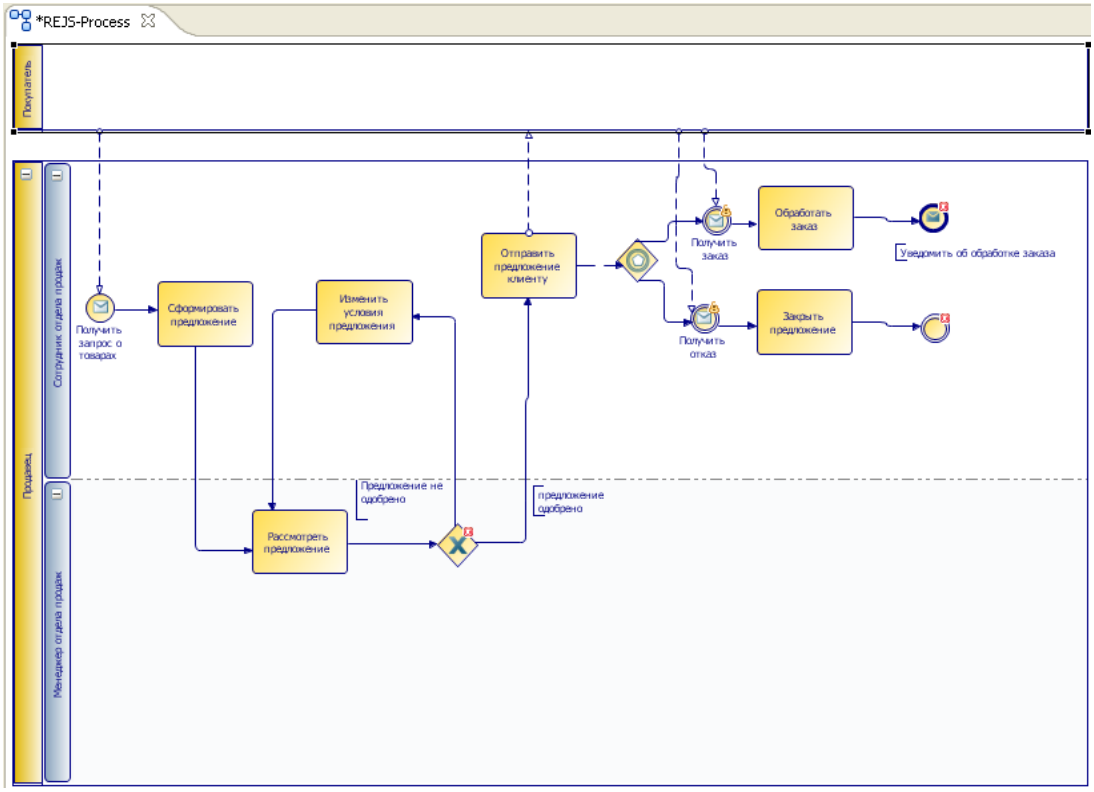


Рис. 3.9. Модель процесса «Обработка запроса о товарах»

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

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

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 № 4

МОДЕЛИРОВАНИЕ БИЗНЕС-ПРОЦЕССОВ СРЕДСТВАМИ TIBCO BUSINESS STUDIO

Цель: закрепить навыки разработки и проектирования моделей бизнес-процессов организации.

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

При подготовке лабораторной работы использованы материалы: 1) Кознов Д.В. Визуальное моделирование: теория и практика. - Интернет-университет информационных технологий. ИНТУИТ. URL: ***http://www.intuit.ru/department/se/vismodtp/9/****. (Режим доступа: требуется регистрация); 2) BPMN. URL: http://ru.wikipedia.org/wiki/BPMN/ (Режим доступа: свободный).*

Дополнительная литература: 1) Все о системном проектировании. URL: http://idefinfo.ru/content/view/434/55// (Режим доступа: свободный) 2) Управление бизнес-процессами URL: http://process.siteedit.ru/page6 (Режим доступа: свободный); 3) White S., Miers D. BPMN Modeling and reference guide. – USA: Future Strategues Inc., 2008. 226 p.

Теоретическая часть

Моделирование бизнес-процессов используется для донесения широкого спектра информации до различных категорий пользователей. Диаграммы бизнес-процессов позволяют описывать сквозные бизнес-процессы, но в то же время помогают читателям быстро понимать процесс и легко ориентироваться в его логике. В сквозной BPMN-модели можно выделить три типа подмоделей:

- ✓ Частные (внутренние) бизнес-процессы;
- ✓ Абстрактные (открытые) бизнес-процессы;
- ✓ Процессы взаимодействия (глобальные).

Частные (внутренние) бизнес-процессы

Частные бизнес-процессы описывают внутреннюю деятельность организации. Они представляют бизнес-процессы в общепринятом понимании (business processes или workflows). При использовании ролей частный бизнес-процесс помещается в отдельный пул. Поэтому поток управления находится внутри одного пула и не может пересекать его границ. Поток сообщений, напротив, пересекает границы пулов для отображения взаимодействия между разными частными бизнес-процессами.

Абстрактные (открытые) бизнес-процессы

Служат для отображения взаимодействия между двумя частным бизнес-процессами (то есть между двумя участниками взаимодействия) В открытом бизнес процессе показываются только те действия, которые участвуют в коммуникации с другими процессами. Все другие, «внутренние», действия частного бизнес-процесса не показываются в абстрактном процессе. Таким образом, абстрактный процесс показывает окружающим последовательность событий, с помощью которой можно взаимодействовать

с данным бизнес-процессом. Абстрактные процессы помещаются в пулы и могут моделироваться как отдельно, так и внутри большей диаграммы бизнес-процесса для отображения потока сообщений между действиями абстрактного процесса с другими элементами. Если абстрактный процесс и соответствующий частный процесс находятся в одной диаграмме, то действия, отображённые в обоих процессах, могут быть связаны ассоциациями.

Процессы взаимодействия (глобальные)

Процесс взаимодействия отображает взаимодействия между двумя и более сущностями. Эти взаимодействия определяются последовательностью действий, обрабатывающих сообщения между участниками. Процессы взаимодействия могут помещаться в пул. Эти процессы могут моделироваться как отдельно, так и внутри большей ДБП для отображения ассоциаций между действиями и другими сущностями. Если процесс взаимодействия и соответствующий частный процесс находятся в одной диаграмме, то действия, отображённые в обоих процессах, могут быть связаны ассоциациями.

Рассмотрим пример из окружающего мира, который может использоваться прообразом для создания модели. Например**, стойка регистрации на рейс** (англ. *check-in counter*) — пункт оформления пассажира для посадки на рейс авиакомпании в аэропорту. Стойка регистрации оборудована весами для взвешивания багажа и ручной клади, компьютером, оснащённым системой бронирования авиабилетов и регистрации, и принтером для распечатки посадочных талонов. Стойки регистрации размещаются рядами с указанием нумерации в специально отведённой зоне вылета или специальном зале вылета аэропорта. Обычно за стойками проходит лента багажного транспортёра. Номер стойки регистрации на оформляющийся рейс указывается в терминале на табло расписания вылетов и объявляется по громкой связи. Крупные авиакомпании обычно имеют выделенные постоянные стойки регистрации на свои рейсы, обозначенные соответствующими вывесками с логотипами и названиями авиакомпаний. Кроме того, авиакомпании выделяют специальные стойки для регистрации пассажиров первого и бизнес-класса, а также иногда имеются отдельные стойки для регистрации на рейс участников бонусных программ. На стойке регистрации уполномоченный сотрудник аэропорта или авиакомпании производит сверку данных авиабилета с данными системы бронирования соответствующей авиакомпании, проверяет документ, удостоверяющий личность пассажира, принимает к транспортировке багаж, выдаёт пассажиру посадочный талон с указанием места на борту и выхода на посадку.

В целях экономии расходов авиакомпании и времени ожидания в очереди пассажиры с электронными билетами без багажа могут воспользоваться для регистрации на свой рейс специальными автоматами.

Словесное описание бизнес-процесса

Когда пассажир прибывает в аэропорт, его приоритетной задачей является регистрация на рейс. Сотрудник на стойке регистрации приветствует клиента и берёт у него документы: билет на рейс и паспорт. Если документы клиента не в порядке (например, истёк срок действия паспорта), он не может быть зарегистрирован на рейс и процесс завершается. При этом клиент получает документы обратно.

Если паспорт и билет в порядке, то сотрудник авиакомпании регистрирует клиента на рейс и распечатывает посадочный талон. При этом он взаимодействует с информационной системой авиакомпании. Сотрудник отдаёт пассажиру посадочный талон и паспорт, после чего уточняет, нет ли в багаже пассажира запрещённых грузов (например, воспламеняющихся веществ). Если таковые есть, то они изымаются из багажа. Сотрудник авиакомпании забирает багаж и ручную кладь пассажира и регистрирует её. При этом сотрудник снова взаимодействует с информационной системой авиакомпании. Если выясняется, что есть перевес, то сотрудник уведомляет об этом пассажира и сообщает, сколько необходимо заплатить. После получения денег от пассажира, сотрудник регистрирует оплату в системе.

В итоге, пассажир получает багажную квитанцию. Сотрудник желает пассажиру приятного полёта, и процесс завершается.

Практическая часть

ЗАДАНИЕ: на основе словесного описания бизнес-процесса «Регистрация на рейс» построить его модель, используя методологию нотации BPMN.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1) Сколько типов подмоделей можно выделить в сквозной модели BPMN?
2) Назовите типы подмоделей, выделяемых в сквозной модели BPMN?
3) Какую функцию при моделировании выполняют абстрактные бизнес-процессы?
4) Что описывают частные бизнес-процессы?
5) Для чего используются процессы взаимодействия при моделировании?
6) Назовите несколько реальных примеров из окружающего мира, для которых можно разработать модель.
7) Назовите отличия нотации BPMN от нотации IDEF0 рассмотренной ранее?

8) Можно ли было бы построить модель процесса «Регистрация на рейс» в нотации IDEF0?
9) Что представляла бы собой модель процесса «Регистрация на рейс» в нотации IDEF0 (при условии что это возможно в принципе)?

Лабораторная работа № 5
ИЗУЧЕНИЕ НОТАЦИИ UML ДЛЯ ПОСТРОЕНИЯ ДИАГРАММЫ ДЕЯТЕЛЬНОСТИ

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).

При подготовке лабораторной работы использованы материалы: 1) Бабич А.В. Введение в UML. – Итернет-университет информационных технологий ИНТУИТ. URL: ***http://www.intuit.ru/department/se/intuml/1/2.html*** *(Режим доступа: требуется регистрация); 2) Леоненков А.В. Нотация и семантика языка UML. Лекция 11. «Элементы графической нотации диаграммы деятельности». – Интернет-университет информационных технологий ИНТУИТ. – URL:* ***http://www.intuit.ru/department/pl/umlbasics/11/4.html*** *(Режим доступа: требуется регистрация).*

Дополнительная литература: 1) Фаулер М. UML. Краткое руководство по стандартному языку объектного моделирования. – СПб.: Символ-Плюс, 2011. – 192 с. 2) Киммел П. UML. Универсальный язык программирования. – М.: НТ-Пресс, 2008. – 272 с. 3) Буч Г., Рамбо Дж., Якобсон И. Введение в UML от создателей языка. – М.: ДМК Пресс, 2011. – 496 с.

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. 5.1). Она в полной мере демонстрирует типичный процесс создания продукта, или "решения" [1].

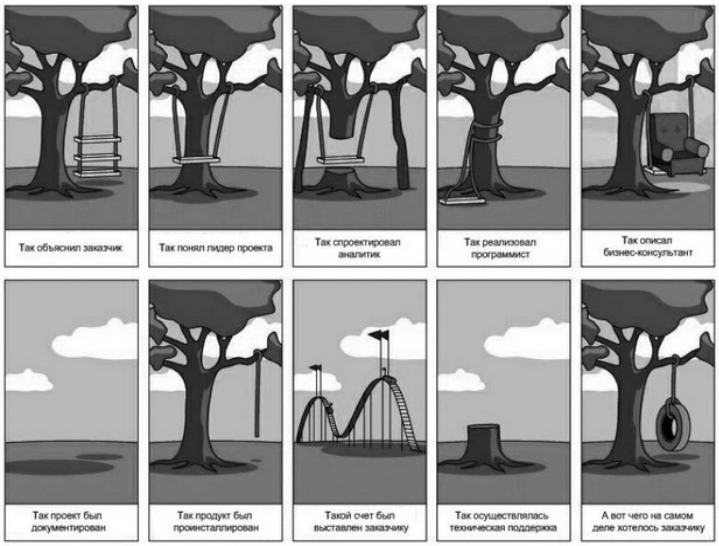


Рис. 5.1. Демонстрация разных взглядов заказчика и исполнителя на проблему.

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.

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

- ✓ Диаграмма классов;
- ✓ Диаграмма компонентов;
- ✓ Диаграмма композитной/составной структуры;
- ✓ Диаграмма развёртывания;
- ✓ Диаграмма объектов;
- ✓ Диаграмма пакетов;
- ✓ Диаграмма деятельности;
- ✓ Диаграмма автомата;
- ✓ Диаграмма вариантов использования;
- ✓ Диаграммы коммуникации и последовательности;
- ✓ Диаграмма обзора взаимодействия;
- ✓ Диаграмма синхронизации.

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 [2].

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. 5.2 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.

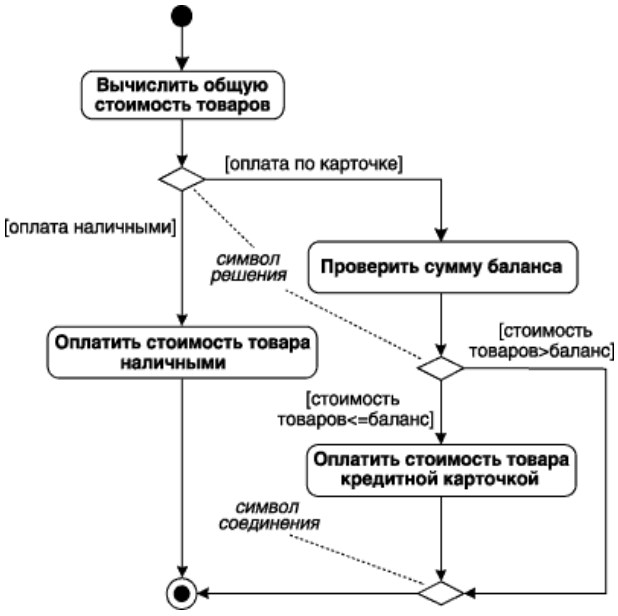


Рис. 5.2. Различные варианты ветвлений на диаграмме деятельности

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. 5.2. 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. 5.2) 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. 5.3а), которые изображаются отрезками вертикальных, реже - горизонтальных, линий. Слияние (join), наоборот, имеет несколько входящих переходов и один выходящий (рис. 5.3 б). Параллельные переходы на диаграмме деятельности можно изображать в удлиненной форме, а входящие и выходящие переходы вертикальными стрелками.

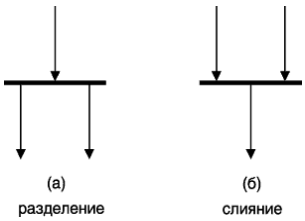


Рис. 5.3. Графическое изображение разделения и слияния параллельных потоков управления на диаграмме деятельности

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. 5.4.) [2].

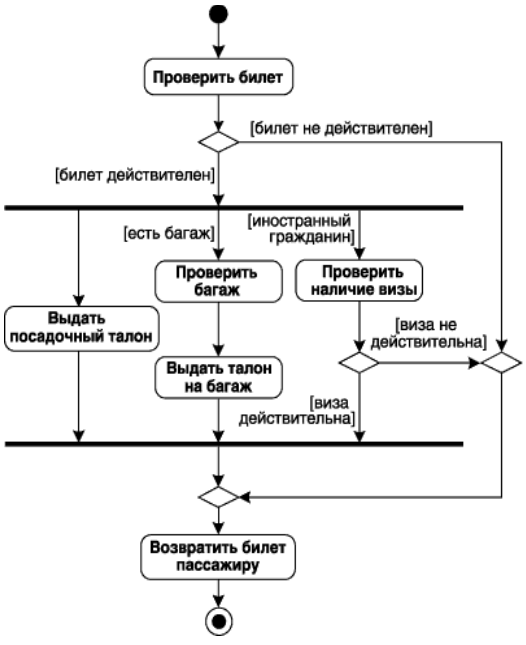


Рис. 5.4. Диаграмма деятельности для примера регистрации пассажиров в аэропорту

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. 5.5.). 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.

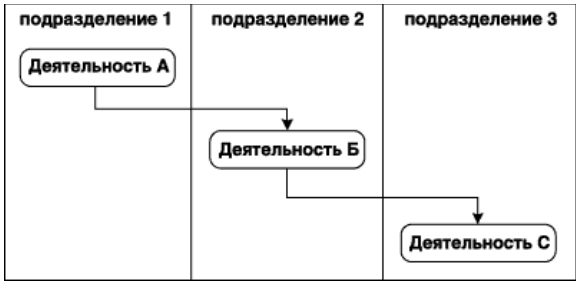


Рис. 5.5. Вариант диаграммы деятельности с дорожками

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. 5.6.). 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 [2].

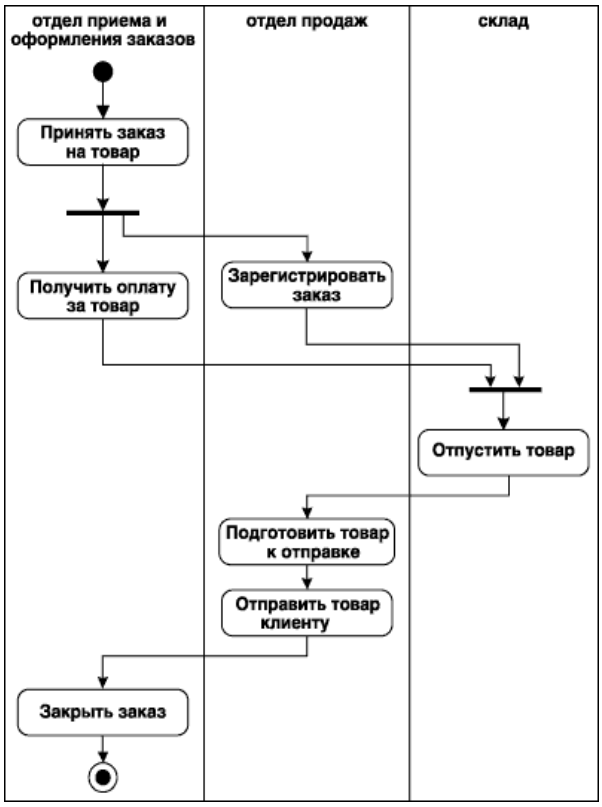


Рис. 5.6. Фрагмент диаграммы деятельности для торговой компании

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. 5.7).

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].

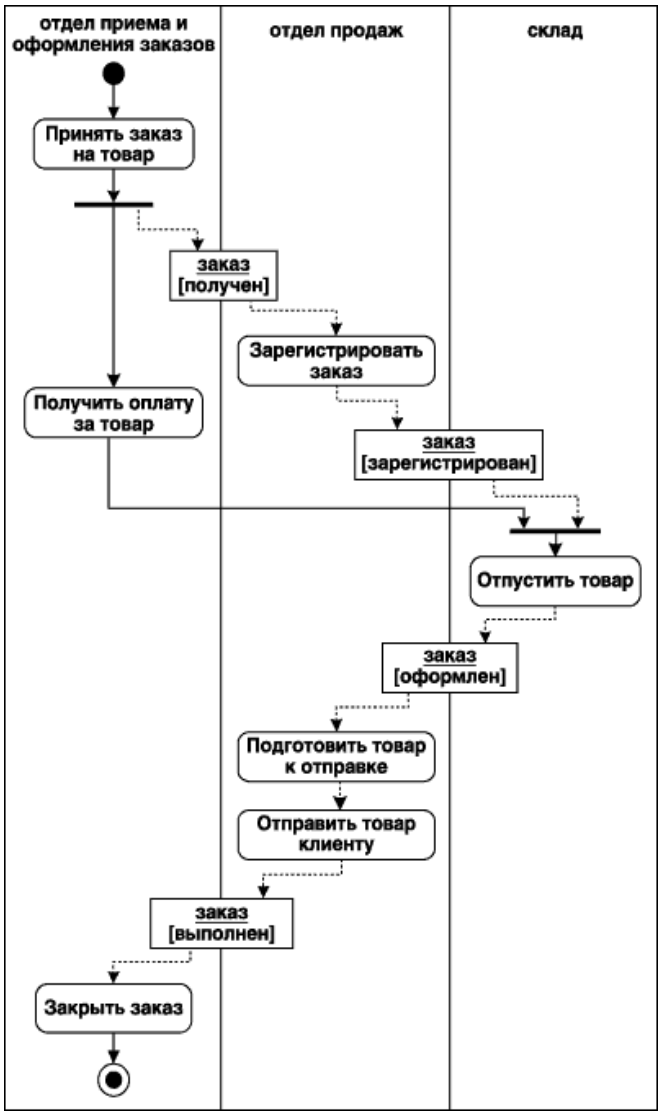


Рис. 5.7. Фрагмент диаграммы деятельности торговой компании с объектом-заказом

Практическая часть.

На основе представленного материала разработать диаграммы деятельности, показанные на рис. 5.4, 5.6 и 5.7 средствами программного продукта Software Ideas Modeler.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

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) Какие виды диаграмм (кроме диаграммы деятельности) позволяет реализовать UML?

Лабораторная работа № 6
ИЗУЧЕНИЕ НОТАЦИИ UML ДЛЯ ПОСТРОЕНИЯ ДИАГРАММЫ ВАРИАНТОВ ИСПОЛЬЗОВАНИЯ

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).

При подготовке лабораторной работы использованы материалы: 1) Леоненков А. В. Нотация и семантика языка UML. Лекция 3. «Элементы графической нотации диаграммы вариантов использования». - Интернет-университет информационных технологий ИНТУИТ.- URL: http://www.intuit.ru/department/pl/umlbasics/3/2.html (Режим доступа: требуется регистрация). 2) Леоненков А.В. Самоучитель по UML. - URL: http://khpi-iip.mipk.kharkiv.edu/library/case/leon/ (Режим доступа: свободный); 3) Пущин М.Н. Проектирование информационных систем: Учеб. пособие. – М.: Изд-во МИЭТ, 2008. – 234 с.; 4) Калашник Ю.В. Постреляционные технологии Cache в системе управления университетом. URL: http://ifets.ieee.org/russian/depository/v6_i2/html/4.html (Режим доступа: свободный).

Дополнительная литература: 1) Фаулер М. UML. Краткое руководство по стандартному языку объектного моделирования. – СПб.: Символ-Плюс, 2011. – 192 с. 2) Киммел П. UML. Универсальный язык программирования. – М.: НТ-Пресс, 2008. – 272 с. 3) Буч Г., Рамбо Дж., Якобсон И. Введение в UML от создателей языка. – М.: ДМК Пресс, 2011. – 496 с.

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 [1].

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: 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 [1].

Отдельный вариант использования обозначается на диаграмме эллипсом, внутри которого содержится его краткое название (рис. 6.1.а) или имя в форме глагола (рис. 6.1.б) с пояснительными словами.

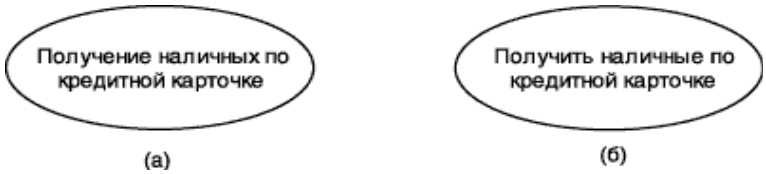


Рис. 6.1. Графическое обозначение варианта использования

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. 6.2) [2].

Рис. 6.2. 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.

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.

На диаграмме вариантов использования интерфейс изображается в виде маленького круга, рядом с которым записывается его имя (рис. 6.3, 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, ISecurelnformation, ISensor (рис. 6.3, б) [2].

Рис. 6.3. 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. 6.4, а). Кроме этого, интерфейсы могут соединяться с

вариантами использования пунктирной линией со стрелкой (рис. 6.4, б), означающей, что вариант использования предназначен для спецификации только того сервиса, который необходим для реализации данного интерфейса.

Рис. 6.4. 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. 6.5). 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 [2].

Рис. 6.5. 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.

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

- ✓ 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 [1, 2].

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. 6.6).

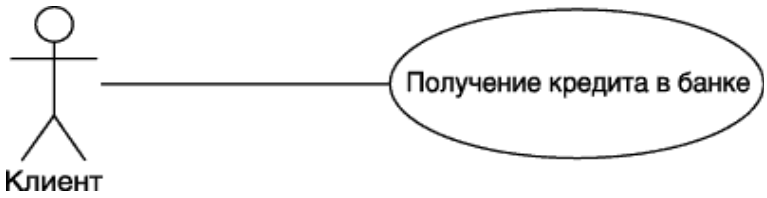


Рис. 6.6. Пример графического представления отношения ассоциации между актером и вариантом использования

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. 6.7.

Рис. 6.7. 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 [1, 2].

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. 6.7) 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.

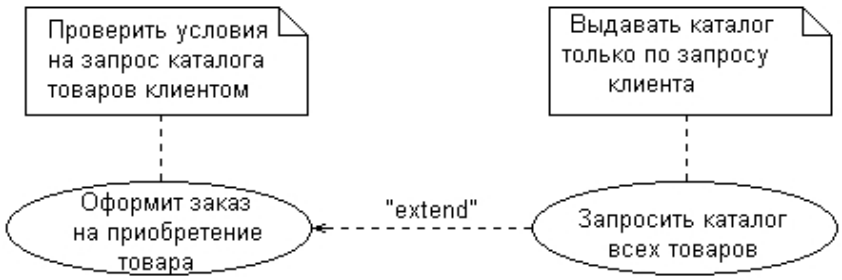


Рис. 6.8. Графическое изображение отношения расширения с примечаниями условий выполнения вариантов использования

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. 6.8)

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. 6.9). Эта линия со стрелкой имеет специальное название — стрелка "обобщение".

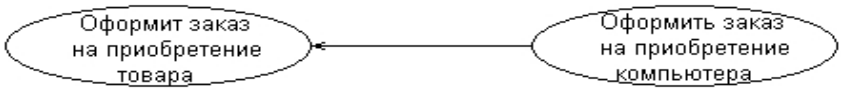


Рис. 6.9. Пример графического изображения отношения обобщения между вариантами использования

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. 6.10).

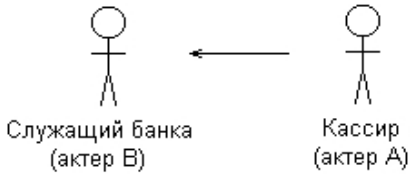


Рис. 6.10. Пример графического изображения отношения обобщения между актерами

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 [1, 2].

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. 6.11.

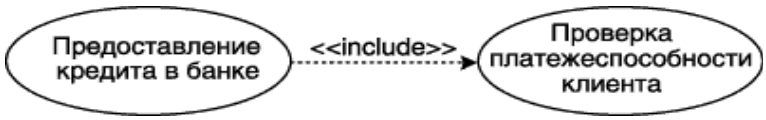


Рис. 6.11. Пример графического изображения отношения включения между вариантами использования

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.

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

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 - Банком, который осуществляет выполнение соответствующих транзакций. Каждый из этих актеров взаимодействует с банкоматом, хотя главный актер Клиент, поскольку именно он инициирует функциональность банкомата [1].

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. 6.12) [1, 2].

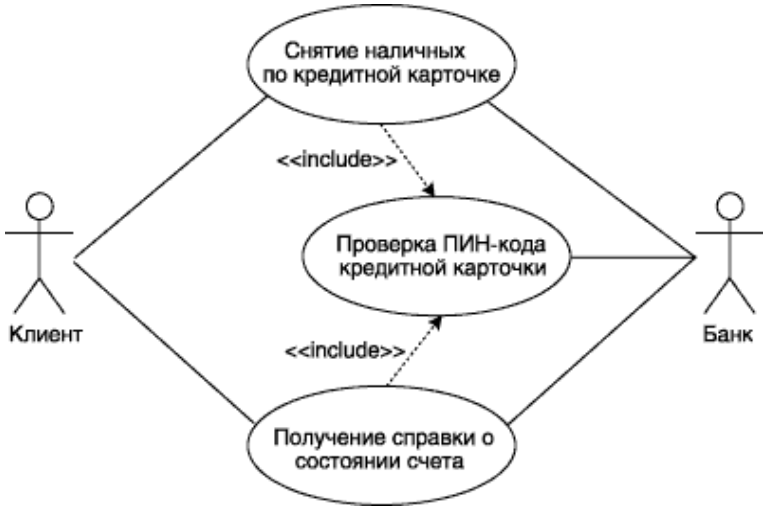


Рис. 6.12. Диаграмма вариантов использования для модели банкомата

ЗАДАНИЕ 1: Используя средства программы Software Ideas Modeler построить диаграмму вариантов использования, показанную на рис. 6.12.

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. 6.1.) указывается имя рассматриваемого варианта использования, имена взаимосвязанных с ним актеров, цель выполнения варианта, условный тип и ссылки на другие варианты использования.

Таблица 6.1. 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. 6.2) 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 6.2. 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	16. Банкомат отображает сообщение о

карточку	готовности к работе

В третьем разделе сценария (табл. 6.3) описывается последовательность действий, выполняемых при возникновении исключительных ситуаций или исключений.

Таблица 6.3. 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 [3].

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 использвания **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. 6.13. показан пример диаграммы вариантов использования для построения автоматизированной информационной системы «Управление университетом» (Пример рисунка взят с ресурса [4]).

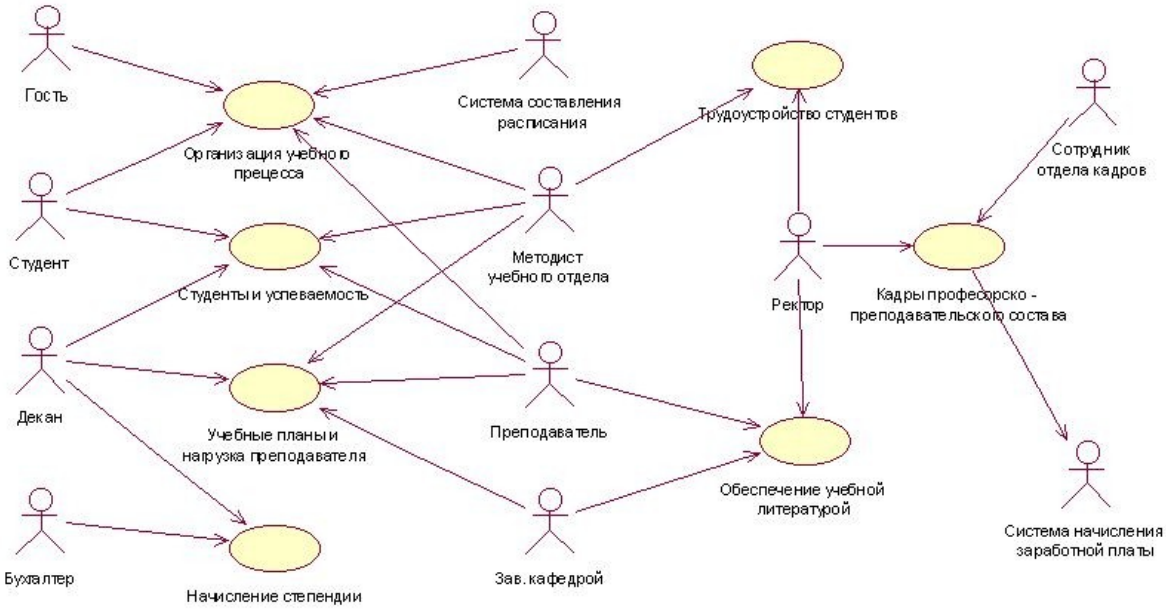


Рис. 6.13. Диаграмма вариантов использования АИС «Управление университетом»

ЗАДАНИЕ 3: Построить диаграмму, показанную на рис. 6.13.

6) **ЗАДАНИЕ 4:** Разработать собственную диаграмму вариантов использования на основе примеров из жизни.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1) Охарактеризовать стандартные виды отношений 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

КОНТРОЛЬНОЕ ТЕСТИРОВАНИЕ ЗА СЕМЕСТР ПО ТЕМАМ ЛЕКЦИЙ И ЛАБОРАТОРНЫХ РАБОТ № 1-6 НАХОДИТСЯ В ПРИЛОЖЕНИИ А К МЕТОДИЧЕСКИМ РЕКОМЕНДАЦИЯМ.

БЛОК «ЗАЩИТА ИНФОРМАЦИИ»

Лабораторная работа № 7

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).

При подготовке лабораторной работы использованы материалы: 1) Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft. – Интернет-университет информационных технологий ИНТУИТ. - URL: http://www.intuit.ru/department/itmngt/riskanms/4/7.html. (Режим доступа: требуется регистрация)

Дополнительная литература: 1) Управление рисками и безопасностью. Учеб пособ. под ред. Черешкина Д. – М.: Ленанд, 2009. – 288 с.

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.) [1].

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") [1].

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 [1].

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.

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.

Методика Microsoft

Проведение оценки рисков в соответствии с методикой Microsoft

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

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:

- ✓ **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. 7.1).

Для угроз указывается уровень воздействия в соответствии с концепцией многоуровневой защиты (уровни - физический, сети, хоста, приложения, данных) [1].

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. 7.1. 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. 7.2.

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. 7.2. 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.

Исходя из значения класса актива и оценки подверженности актива воздействию по таблице приведенной на рис. 7.3. 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. 7.3. 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.

		Уровни в списке с обобщенными сведениями о рисках		
Влияние (из предыдущей таблицы)	Выс.	Средн.	Выс.	Выс.
	Средн.	Низк.	Средн.	Выс.
	Низк.	Низк.	Низк.	Средн.
		Низк.	Средн.	Выс.
		Уровень вероятности		

Рис. 7.4. Определение итогового уровня риска

Полученные оценки заносятся в таблицу, пример которой приведен на рис. 7.5.

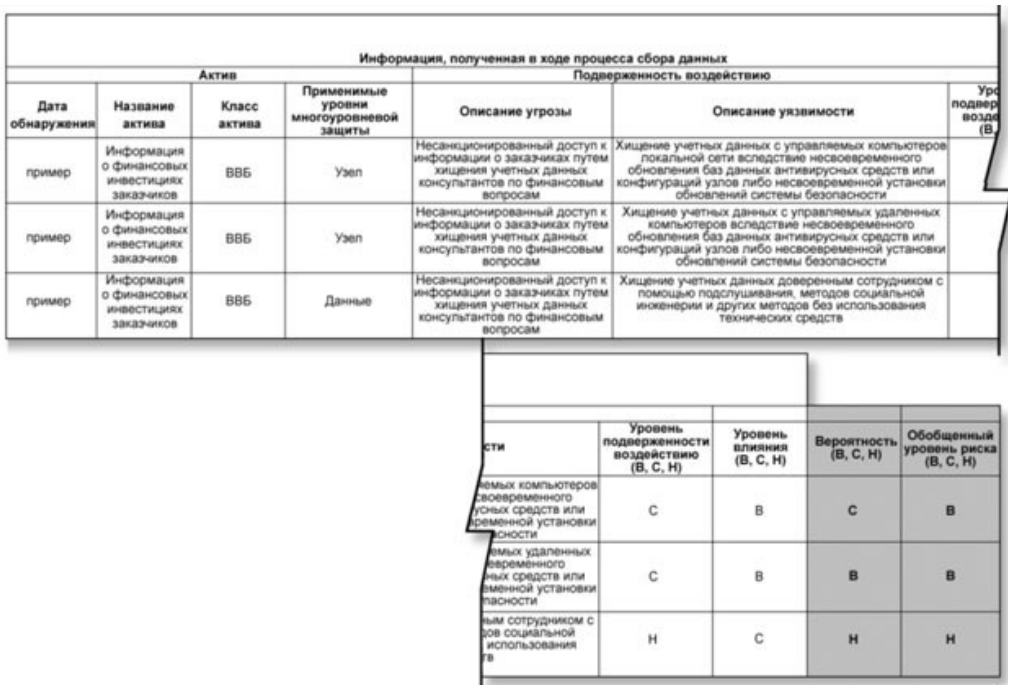
Для детального изучения (составления "перечня на уровне детализации") отбираются риски, отнесенные по результатам оценки на обобщенном уровне к одной из трех групп:

- 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 временного ных средств или еменной установки пасности	С	В	В	В
ным сотрудником с дов социальной использования тв	Н	С	Н	Н

Рис. 7.5. Пример перечня рисков на обобщенном уровне

Уровень подверженности воздействию оценивается по пятибалльной шкале. Шкала для угрозы целостности и конфиденциальности приведена на рис. 7.6. Для угрозы отказа в обслуживании – на рис. 7.7. В качестве итогового уровня подверженности воздействию предлагается выберите максимальное значение.

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. 7.6. 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. 7.7. 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. 7.8 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. 7.8. 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. 7.9, с последующим переходом к результирующей оценке (рис. 7.10). 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. 7.9. 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. 7.10. Оценка уровня вероятности

Рис. 7.11 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. 7.11. Оценка эффективности текущего контроля

Полученные значения суммируются и заносятся в шаблон для уровня детализации.

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

Рис.7.12. Результирующая оценка

Пример заполненного шаблона представлен на рис. 7.13.

Прим. 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".

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. 7.13. 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. 7.14.

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

- ✓ 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).

Рис. 7.14. 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. 7.15 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. 7.15. 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. 7.16. 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. 7.17.

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. 7.17. 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.

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. [1]

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).

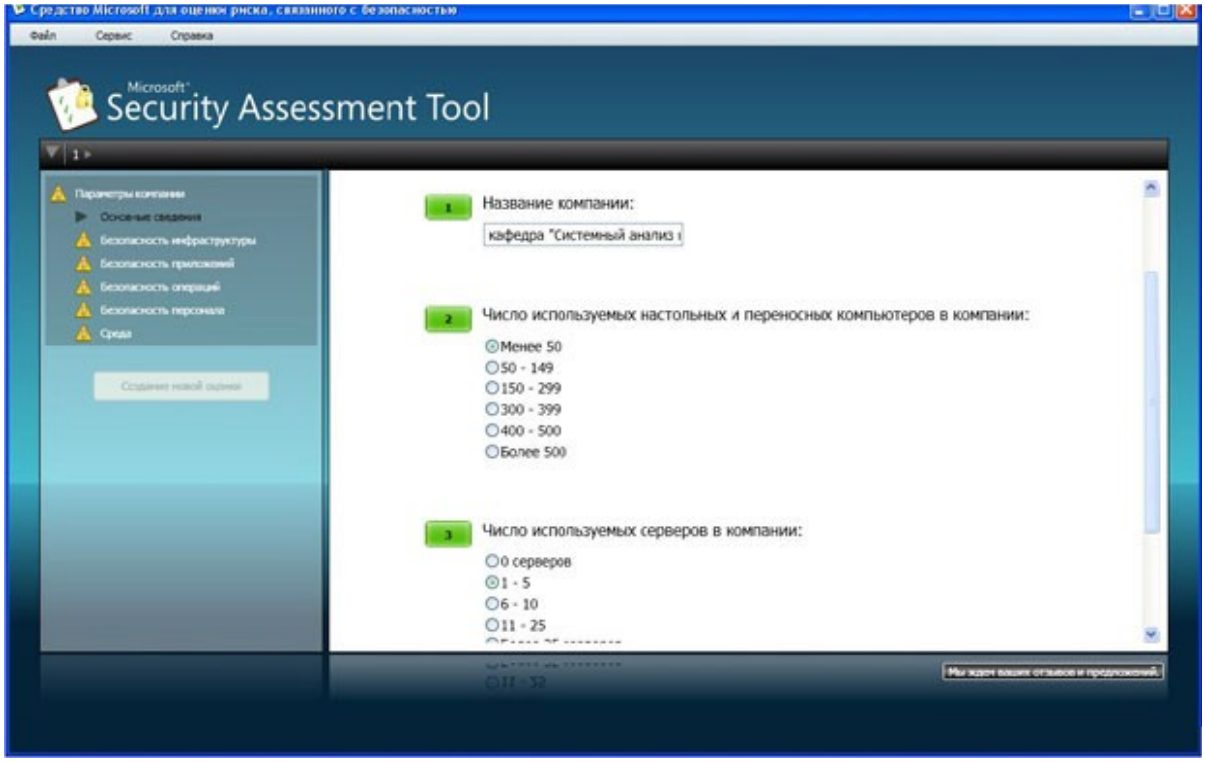


Рис. 7.18. Информация о компании

Вопросы этого этапа разбиты на 6 групп. Первая (рис. 7.18) 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. 7.19). Стоит сказать, что и перевод вопросов второго этапа выполнен существенно лучше.

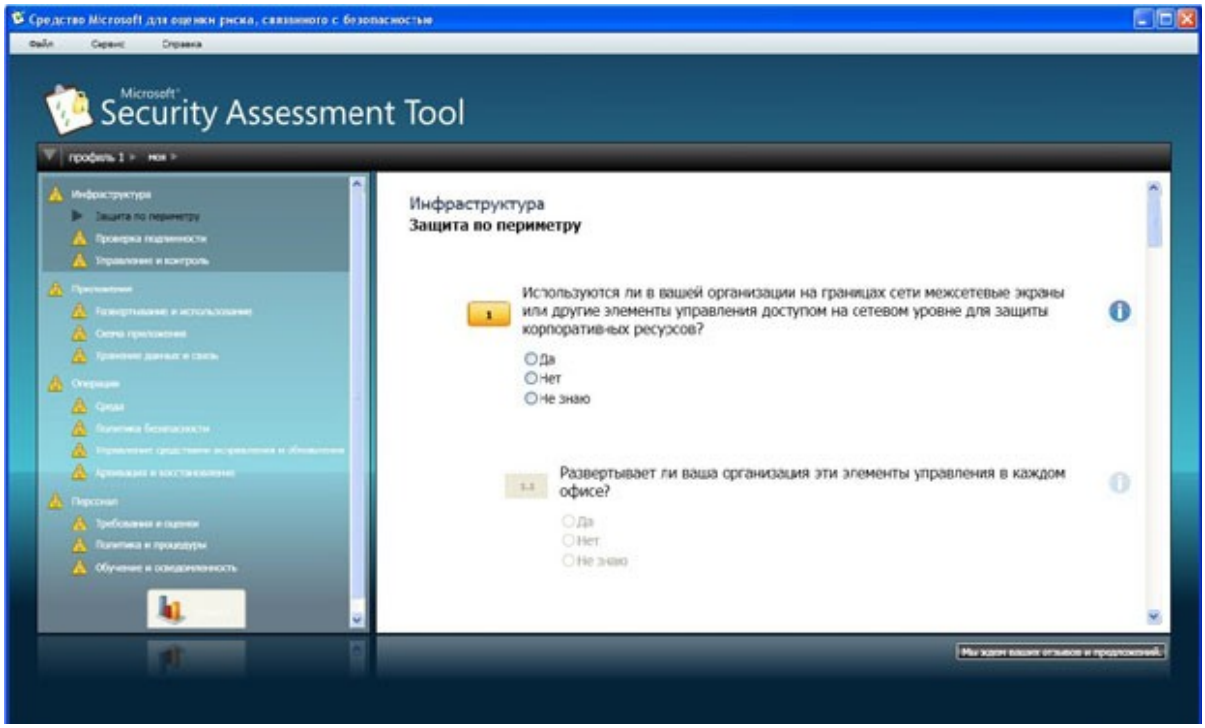


Рис. 7.19. Анализ используемых механизмов защиты

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. 7.1

Таблица 7.1. 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.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

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?

Лабораторная работа № 8.
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.

При подготовке лабораторной работы использованы материалы: 1) Энциклопедия безопасности Касперского. URL: http://www.securelist.com/ru/threats/detect (Режим доступа: свободный); 2) 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. - URL: http://www.intuit.ru/department/itmngt/riskanms/3/5.html (Режим доступа: требуется регистрация).

Дополнительная литература: 1) Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. – М.: Академия, 2011. – 336 с. 2) Сычев Ю.Н. Основы информационной безопасности. Учебно-практическое пособие. – М.: Издат. центр ЕАОИ, 2007. – 300 с. 4)

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 [1]:

- ✓ 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 [1].

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.

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.

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.

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).

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 [2].

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. 8.1) [2]. 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. 8.2 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.

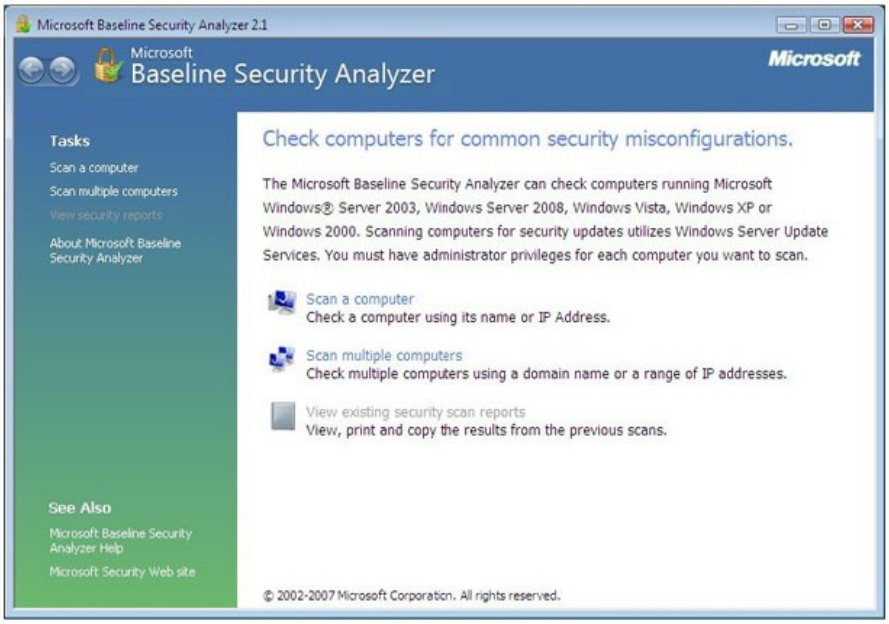


Рис. 8.1. Выбор проверяемого компьютера

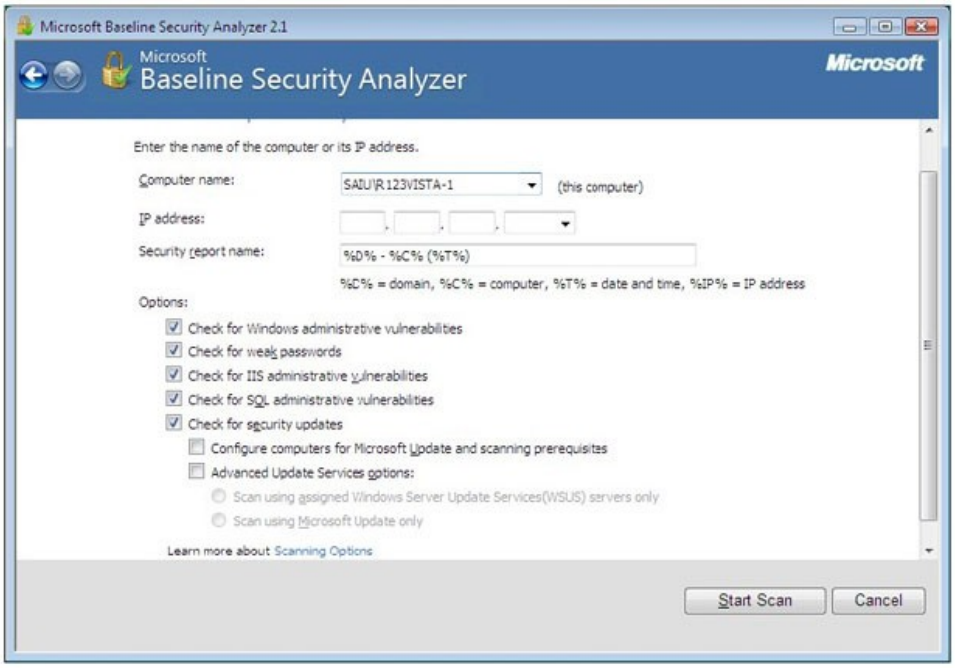


Рис. 8.2. Задание параметров проверки

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. 8.2 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. 8.3 примере уровень риска оценивается как "серьезный" (Severe risk) [2].

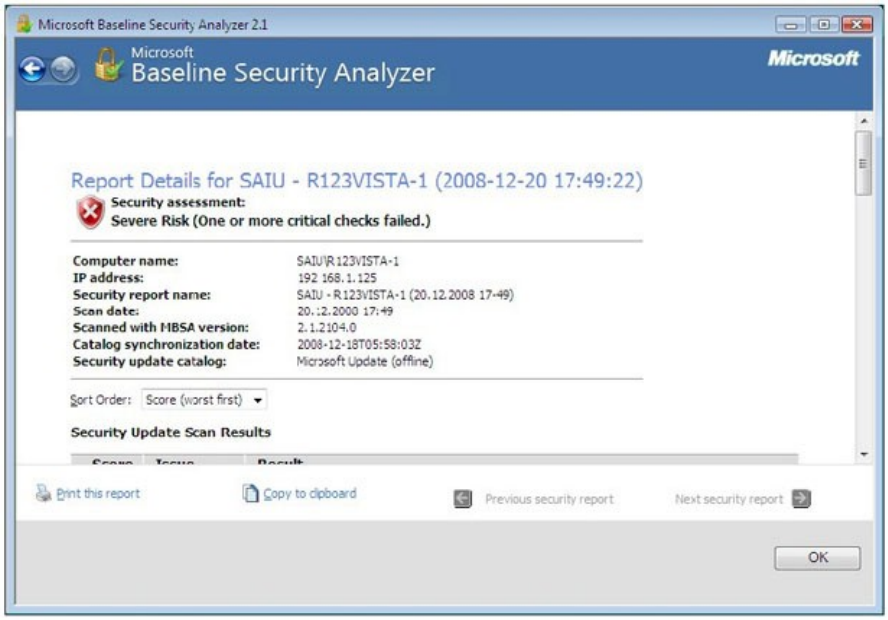


Рис. 8.3. Заголовок отчета

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. 8.4) 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. 8.5). Описывается уязвимость, указывается ее уровень критичности, даются рекомендации по исправлению. На рис. 8.6 представлено подробное описание результатов (ссылка **result details**) проверки паролей. Указывается, что 3 учетные записи имеют пароли, неограниченные по сроку действия [2].

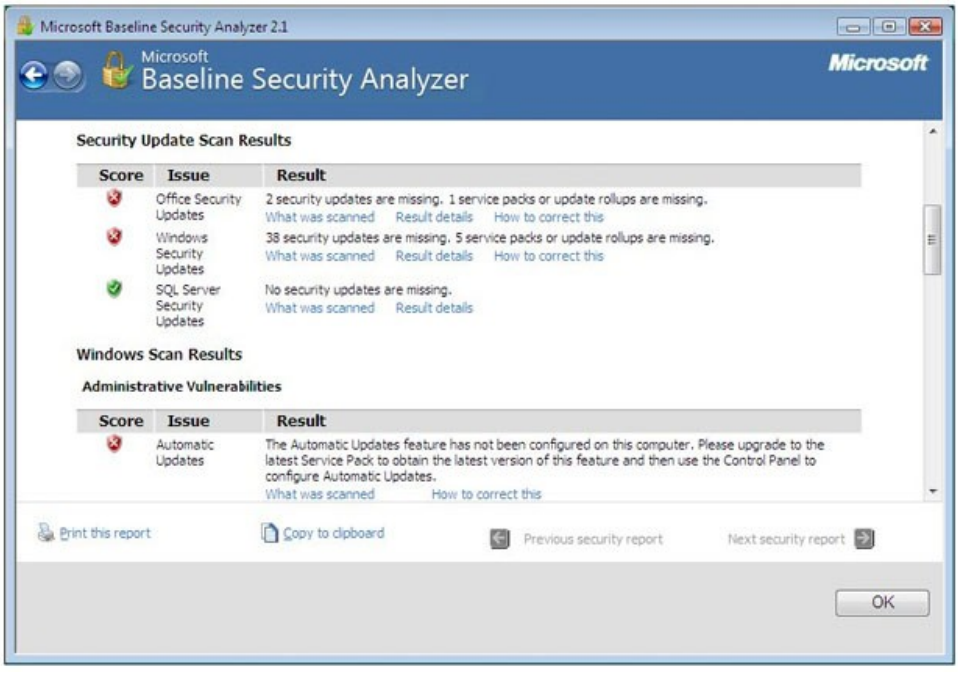


Рис. 8.4. Перечень неустановленных обновлений (по группам)

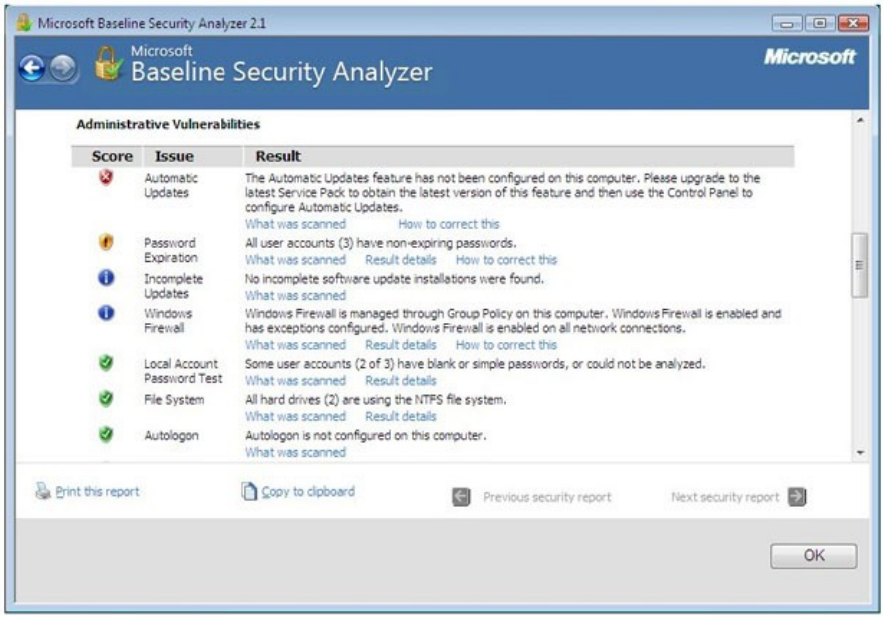


Рис. 8.5. Уязвимости, связанные с администрированием операционной системы

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 **"/?"**.

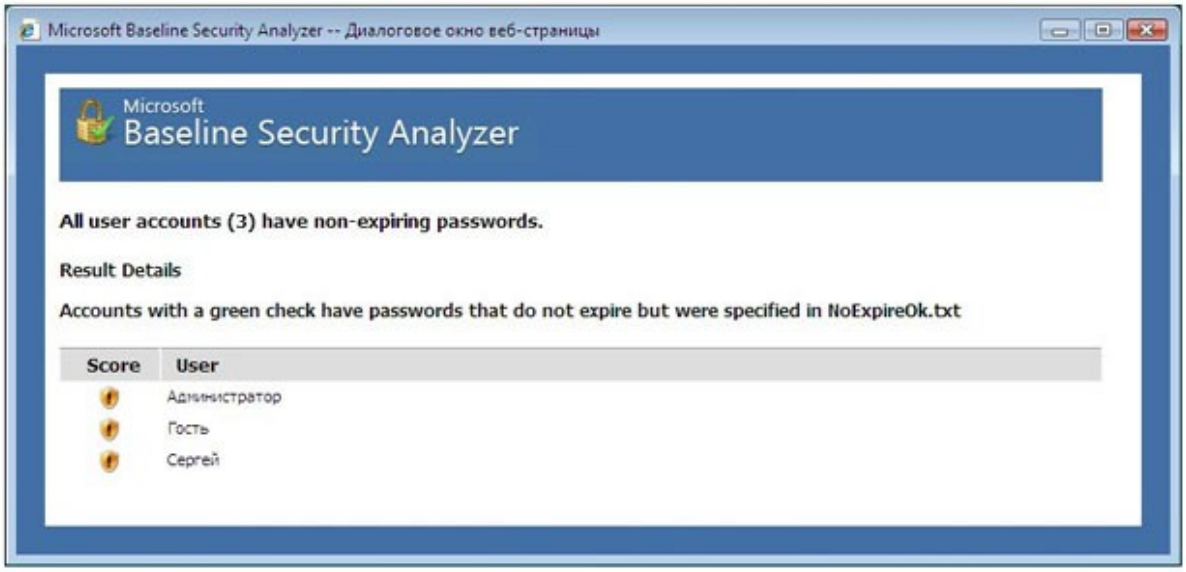


Рис. 8.6. Результаты проверки паролей

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 [2]

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**.

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. 8.7.

Значения выбранного параметра можно изменить (рис. 8.8).

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**).

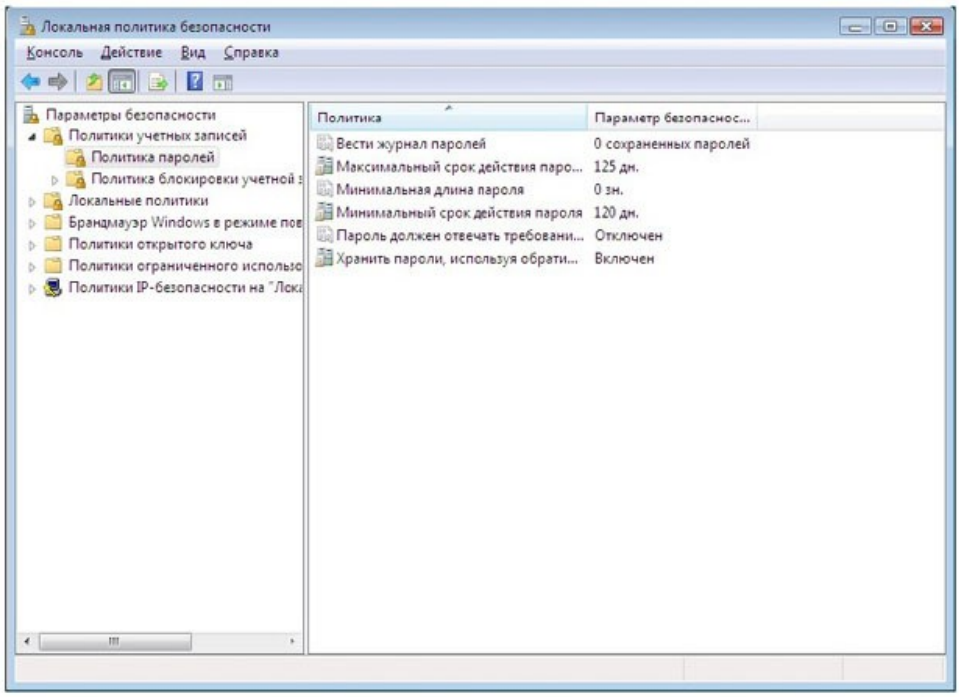


Рис. 8.7. Настройка политики паролей

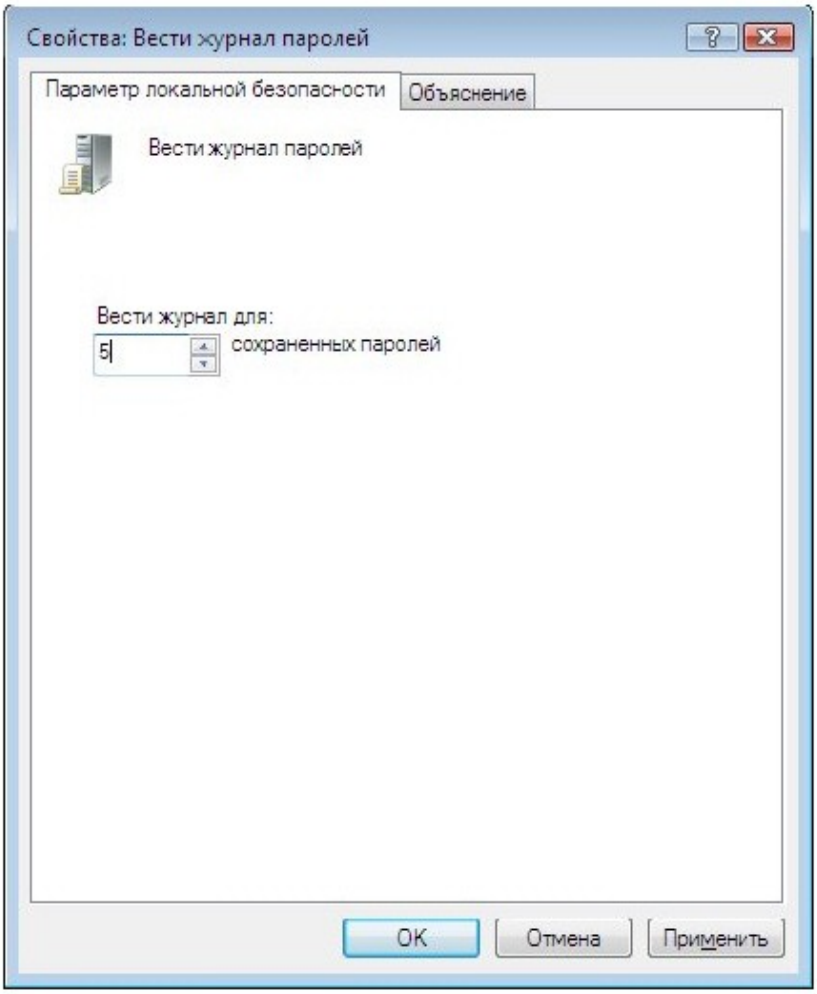


Рис. 8.8. Установка требования ведения журнала паролей

Задания

1. Выполните проверку Вашего компьютера с помощью Microsoft Baseline security analyzer. В отчете о выполнении лабораторной работы необходимо указать следующее [2]:
   - ✓ как оценен уровень уязвимости Вашего компьютера;
   - ✓ какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей;
   - ✓ опишите наиболее серьезные уязвимости каждого типа, выявленные на Вашем компьютере.
2. Проведите анализ результатов - какие уязвимости можно устранить, какие - нельзя из-за особенностей конфигурации ПО или использования компьютера.
3. Выполните удаленную проверку соседнего компьютера из сети лаборатории. Опишите наиболее серьезные уязвимости.
4. Выполните проверку нескольких компьютеров с помощью утилиты mbsacli. Для этого, предварительно создайте текстовый файл с перечнем имен компьютеров или ip-адресов и запускайте mbsacli с ключом /listfile, после которого указывается имя файла с перечнем компьютеров. В результате Вы получите сообщение примерно следующего содержания:

   2. Computer Name, IP Address, Assessment, Report Name
   3. ----------

   HOME\MYNBOOK, 127.0.0.1, Severe Risk, HOME - MYNBOOK (06.12.2008 13-51)

Для того, чтобы увидеть подробные результаты проверки, надо повторно запустить mbsacli с ключом /ld, после которого указывается имя отчета. Вывод можно перенаправить в текстовый файл для дальнейшей обработки. Например:

mbsacli /ld "HOME - MYNBOOK (06.12.2008 13-51)" > c:\test\report1.txt

После выполнения задания проанализируйте результаты, кратко опишите их в отчете по лабораторной работе.

1. Опишите действующую на вашем компьютере политику паролей.
2. Измените ее в соответствии с рассмотренными в теоретической части курса рекомендациями по администрированию парольной системы.
3. Если в ходе проверки утилитой bsa были выявлены уязвимости связанные с управлением паролями пользователей, опишите пути их устранения или обоснуйте необходимость использования действующих настроек.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

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. Что включает в себя локальная политика паролей?
6. Для чего необходимо владеть информацией о локальной политике паролей предприятия?

Лабораторная работа № 9.
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 3Com Network Supervisor, наличие доступа к ресурсам глобальной сети Internet.

При подготовке лабораторной работы использованы материалы: 1) 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. - URL: http://www.intuit.ru/department/itmngt/riskanms/3/5.html (Режим доступа: требуется регистрация);

Дополнительная литература: 1) Галатенко В.А. Основы информационной безопасности. – М.: Интернет университет информационных технологий ИНТУИТ, 2008. – 208 с.; 2) Основы защиты информации. Учеб. пособие в 3-х ч. Под ред. Шелупанова А.А. – Томск: В-Спектр, 2007. 3) Сычев Ю.Н. Основы информационной безопасности. Учебно-практическое пособие. – М.: Издат. центр ЕАОИ, 2007. – 300 с.

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 [1].

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. 7.1).

Рис. 7.1. Компоненты модели LifeCycle Security

Перечень выделяемых уровней незначительно различается в различных документах. Возможные варианты представлены на рис. 7.2 [1].

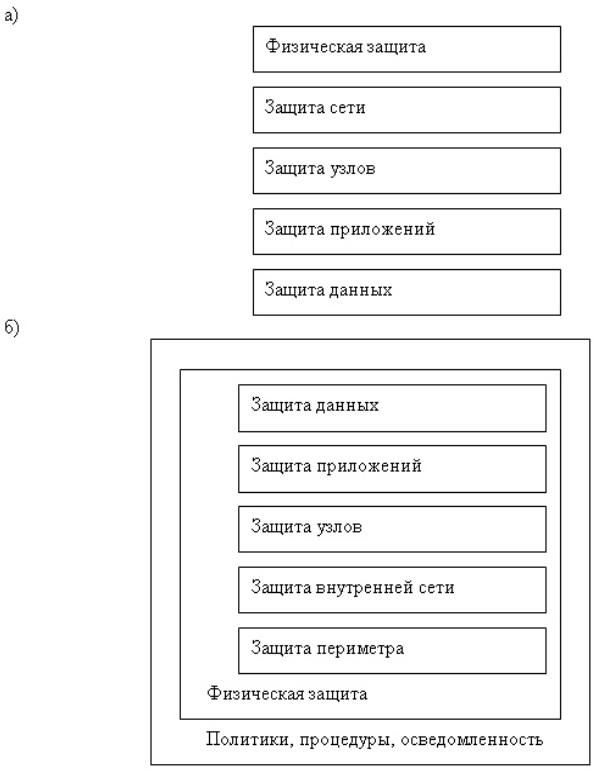


Рис. 7.2. Модель многоуровневой защиты

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).

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.

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.

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.

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.

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.

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.

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.

В продолжение темы инвентаризации активов информационной системы (ИС), является целесообразным рассмотреть средства, позволяющие получить данные о составе и топологии сети. В качестве примера в данной лабораторной работе будет использоваться утилита 3Com Network Supervisor, которую можно бесплатно получить с сайта компании 3Com (ссылка для скачивания: www.3com.com). Аналогичные по функциональности продукты есть и у других производителей сетевого оборудования.

При запуске программы предлагается выбор - строить новую карту сети или открыть существующую. При выборе создания новой карты надо указать, какая подсеть документируется (рис. 7.3). На рисунке выбрана локальная подсеть, т.е. та ip-сеть, к которой относится компьютер, на котором выполняется 3Com Network Supervisor [1].

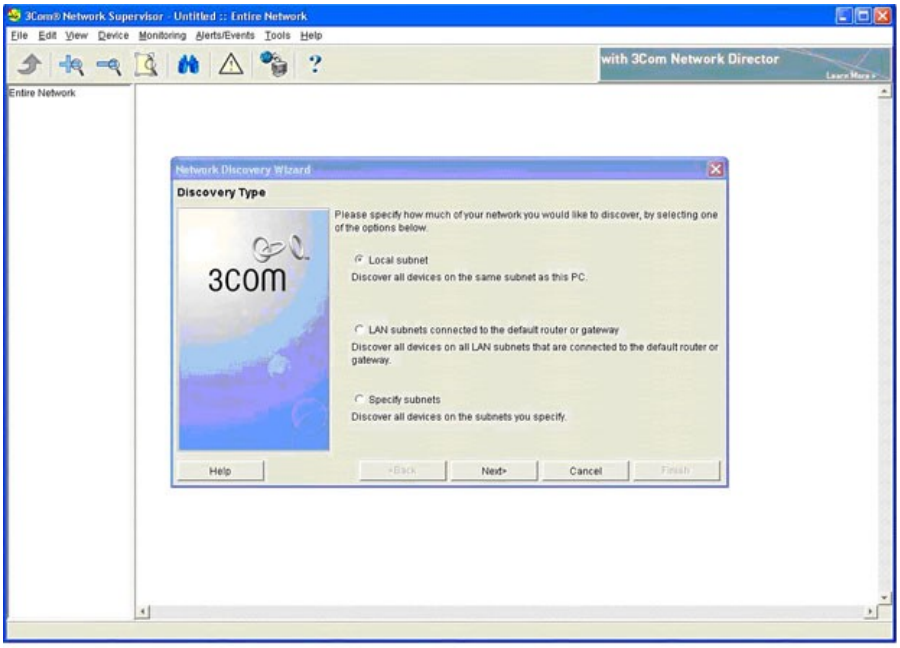


Рис. 7.3. Выбор документируемой сети

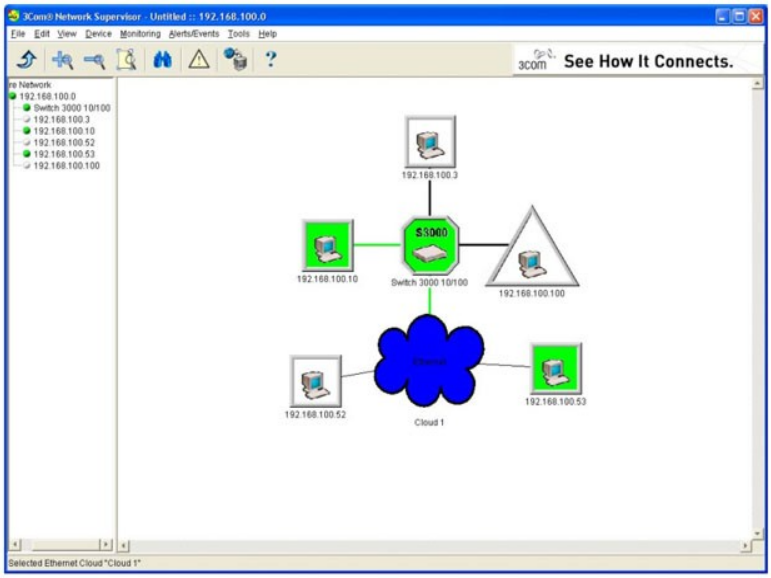


Рис. 7.4. Карта сети 192.168.100.0. Cloud 1 скрывает неуправляемый коммутатор

На рис. 7.4. представлен пример карты сети, которую строит утилита. Надо отметить, что наиболее информативна такая карта будет в том случае, если в сети используется управляемое сетевое оборудование 3Com, поддерживающее, в частности, протокол SNMP. В то же время, польза от составления карты будет и в случае отсутствия в сети подобного оборудования. Для того, чтобы это продемонстрировать, были сделаны следующие настройки. Каждому из компьютеров были присвоены ip-адреса из двух сетей класса C - 192.168.1.0 и 192.168.100.0. Управляемому коммутатору 3Com SuperStack II Switch 3000 назначен адрес 192.168.100.6, т.е. он "виден" только при построении карты сети 192.168.100.0. DNS серверы доступны только в сети 192.168.1.0, поэтому на рисунках, относящихся ко второй сети, компьютеры идентифицируются только ip-адресами. Карта сети 192.168.1.0 представлена на рис. 7.5 [1].

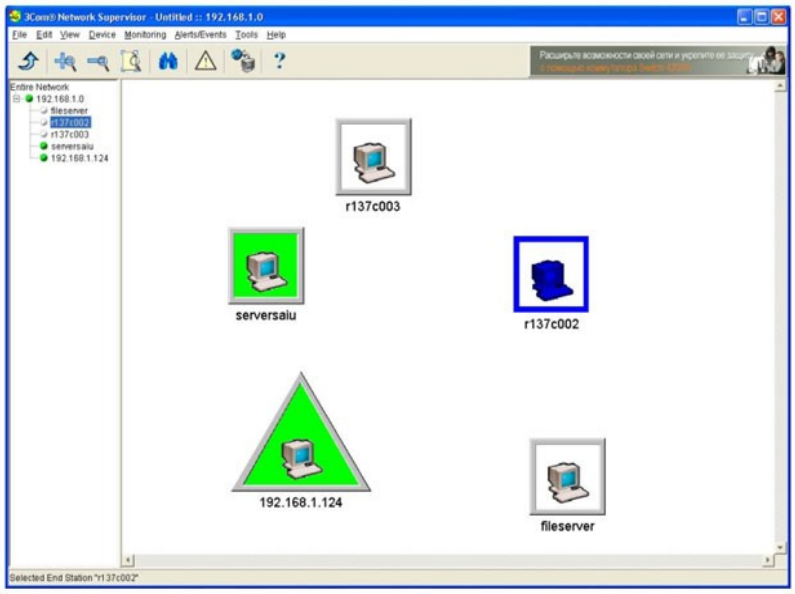


Рис. 7.5. Карта сети 192.168.1.0. Информация от управляемого коммутатора недоступна

Для выбранного узла можно потребовать провести мониторинг загрузки различных сетевых сервисов или обратиться к средствам удаленного администрирования, использующим протоколы http, telnet или ssh (рис. 7.6, 7.7).

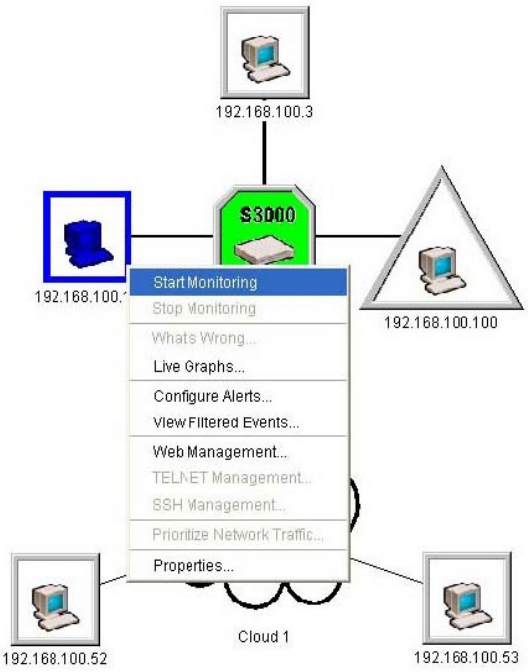


Рис. 7.6. Функции, доступные для выбранного узла

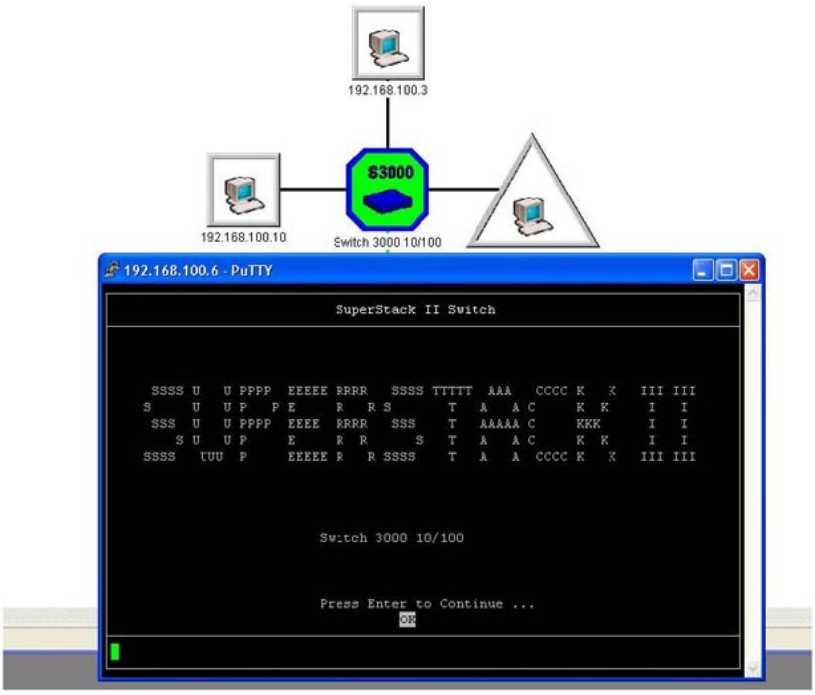


Рис. 7.7. Запуск удаленного терминала для администрирования коммутатора Switch 3000

Функция поиска (кнопка панели инструментов с изображением бинокля) позволяет, в частности, отобразить информацию о типах используемых сетевых подключений (рис. 7.8 и 7.9) [1].

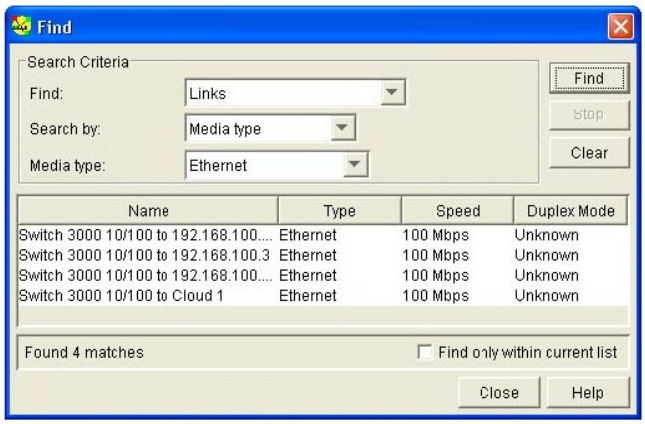


Рис. 7.8. Соединения по типам подключений. Ethernet

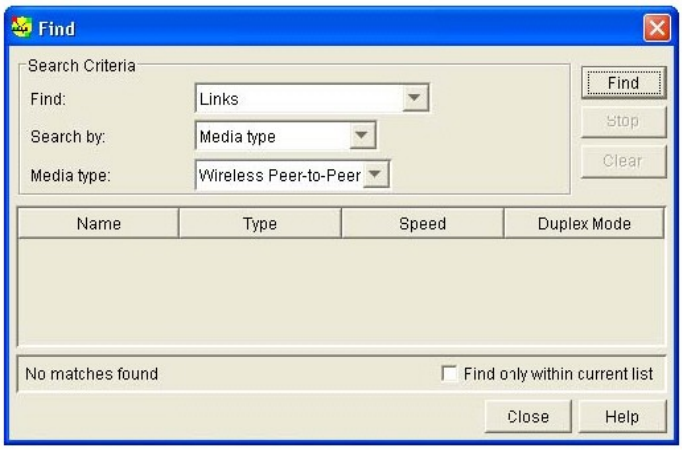


Рис. 7.9. Соединения по типам подключений. Беспроводные подключения (отсутствуют)

Собранная информация может отображаться в виде отчетов, формируемых в формате HTML. Опция доступна через меню **Tools пункт Reports**. Для задач, связанных с инвентаризацией системы, наибольший интерес представляют отчеты **Inventory Report** и **Topology Report**. Примеры "содержательной части" отчетов приведены в табл.7.1-7.3 [1].

Таблица 7.1. Inventory Report для сети 192.168.100.0

IP Address	Device Type	MAC Address	Device Name	Last Discovery Time
Core Devices				
192.168.100.6	3Com SuperStack II Switch 3000	08-00-4e-50-6d-b3	Switch 3000 10/100	3 Октябрь 2007 г. 22:09
None Core Devices				
192.168.100.10	Generic IP device	00-e0-4c-e9-59-39	192.168.100.10	3 Октябрь 2007 г. 22:09
192.168.100.100	Generic IP device	00-14-85-d6-50-7d	192.168.100.100	3 Октябрь 2007 г. 22:09
192.168.100.3	Generic IP device	00-11-d8-82-56-d2	192.168.100.3	3 Октябрь 2007 г. 22:09
192.168.100.52	Generic IP device	00-40-f4-70-4f-8f	192.168.100.52	3 Октябрь 2007 г. 22:09
192.168.100.53	Generic IP device	00-30-84-88-09-a7	192.168.100.53	3 Октябрь 2007 г. 22:09

Таблица 7.2. Inventory Report для сети 192.168.1.0

IP Address	Device Type	MAC Address	Device Name	Last Discovery Time
Core Devices				
IP Address	**Device Type**	**MAC Address**	**Device Name**	**Last Discovery Time**
None Core Devices				
192.168.1.10	Generic IP device	00-e0-4c-e9-59-39	serversaiu	3 Октябрь 2007 г. 22:35
192.168.1.124	Generic IP device	00-14-85-d6-50-7d	192.168.1.124	3 Октябрь 2007 г. 22:35
192.168.1.3	Generic IP device	00-11-d8-82-56-d2	fileserver	3 Октябрь 2007 г. 22:35
192.168.1.52	Generic IP device	00-40-f4-70-4f-8f	r137c002	3 Октябрь 2007 г. 22:35

192.168.1.53	Generic IP device	00-30-84-88-09-a7	r137c003	3 Октябрь 2007 г. 22:35

Таблица 7.3. Topology Report для сети 192.168.100.0

IP Address	Type	Unit	Port	Linked To	IP Address	Type	Unit	Port
192.168.100.6	3Com SuperStack II Switch 3000	1	6		192.168.100.3	Generic IP device	N/A	N/A
192.168.100.6	3Com SuperStack II Switch 3000	1	5		192.168.100.100	Generic IP device	N/A	N/A
192.168.100.6	3Com SuperStack II Switch 3000	1	12		192.168.100.10	Generic IP device	N/A	N/A
192.168.100.6	3Com SuperStack II Switch 3000	1	4		Unknown	Unknown	N/A	N/A
Unknown	Unknown	N/A	N/A		192.168.100.53	Generic IP device	N/A	N/A
Unknown	Unknown	N/A	N/A		192.168.100.52	Generic IP device	N/A	N/A

Отчет по топологии сети 192.168.1.0 состоит из записи "Нет данных", т.к. данные о топологии программа 3Com Network Supervisor получить не смогла (в этой сети управляемый коммутатор "невидим", т.к. его адрес принадлежит другой ip-сети).Через свойства управляемого коммутатора доступна информация о том, к какому порту какой узел подключен и графики загрузки (рис. 7.10, 7.11) [1].

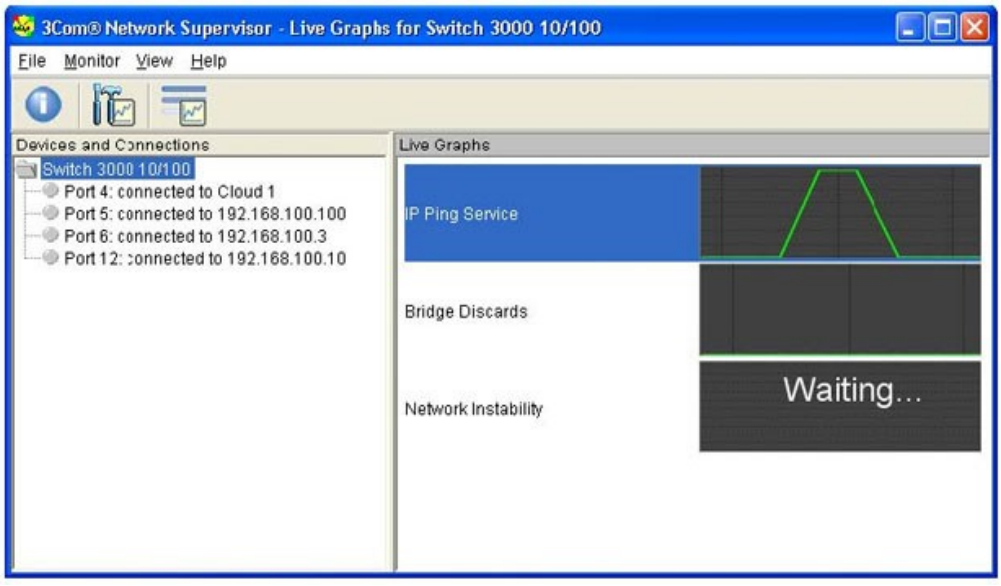


Рис. 7.10. Данные о подключениях и графики

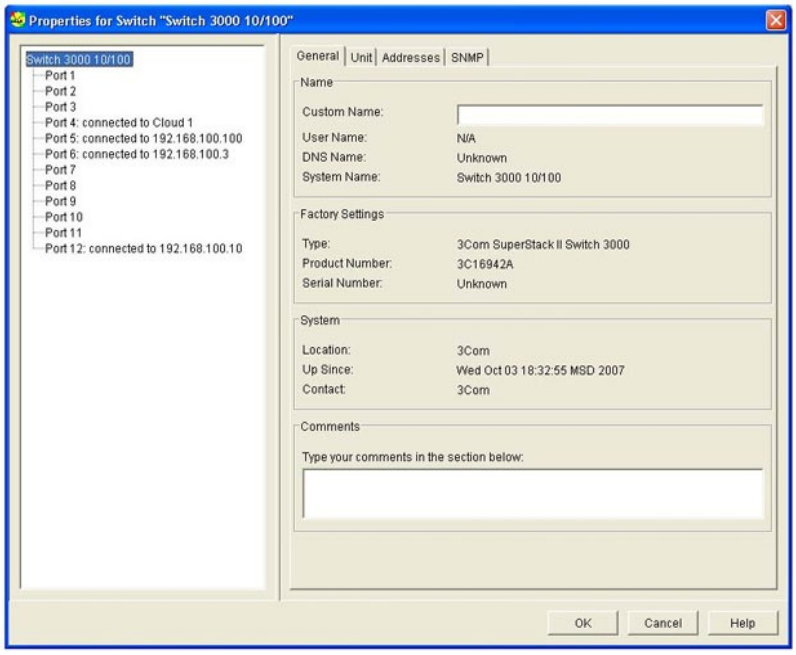


Рис. 7.11. Свойства коммутатора

Практическая часть

1) С помощью 3Com Network Supervisor постройте карту сети учебной лаборатории. Опишите узлы сети, используемые типы соединений, доступные средства удаленного администрирования.

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

3) При помощи ресурсов сети Интернет найти информацию об утилитах для построения топологий и карты сети других разработчиков. Составить перечень параметров для сравнения и представить в виде таблицы, с указанием в каких программах данные параметры имеются, а в каких нет.

Отчет представить преподавателю в текстовом файле формата *.doc.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

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?

Лабораторная работа № 10.

ИЗУЧЕНИЕ МЕЖДУНАРОДНЫХ 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.

При подготовке лабораторной работы использованы материалы: 1) Нестеров С.А. Анализ и управление рисками в операционных системах на базе операционных систем Microsoft. Лекция 2. «Современные стандарты в области информационной безопасности , использующие концепцияю управления рисками» - Интернет-университет информационных технологий ИНТУИТ. - URL: http://www.intuit.ru/department/itmngt/riskanms/3/5.html (Режим доступа: требуется регистрация). 2) Безопасность информационных технологий. Руководящий документ Гостехкомиссии России № 187 от 19.06.02. 3) ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Библиотека ГОСТов. – URL: http://vsegost.com/Catalog/57/5736.shtml (Режим доступа: свободный)

Дополнительная литература: 1) Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. – М.: Академия, 2011. – 336 с.; 2) Международные стандарты информационной безопасности. URL: http://ypn.ru/177/international-standards-of-information-technologies-security/ (Режим доступа: свободный); 3) ISO 27000 - Международные стандарты управления информационной безопасностью/ URL: http://www.iso27000.ru/standarty/iso-27000-mezhdunarodnye-standarty-upravleniya informacionnoi-bezopasnostyu-1/ (Режим доступа: свободный).

Теоретическая часть

В соответствии с международными и национальными стандартами обеспечение информационной безопасности в любой компании предполагает следующее [1]:

- ✓ 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 [1].

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. 10.1 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.

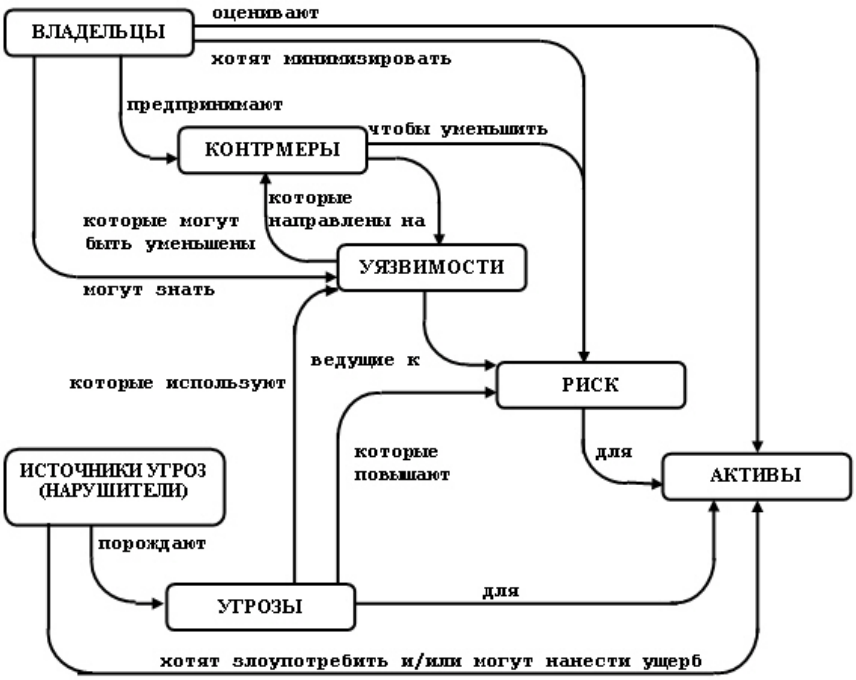


Рис. 10.1. Понятия безопасности и их взаимосвязь в соответствии с ГОСТ Р ИСО/МЭК 15408-2002

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 [2].

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 [1, 2]:

- ✓ 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. 2.2.

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 [1].

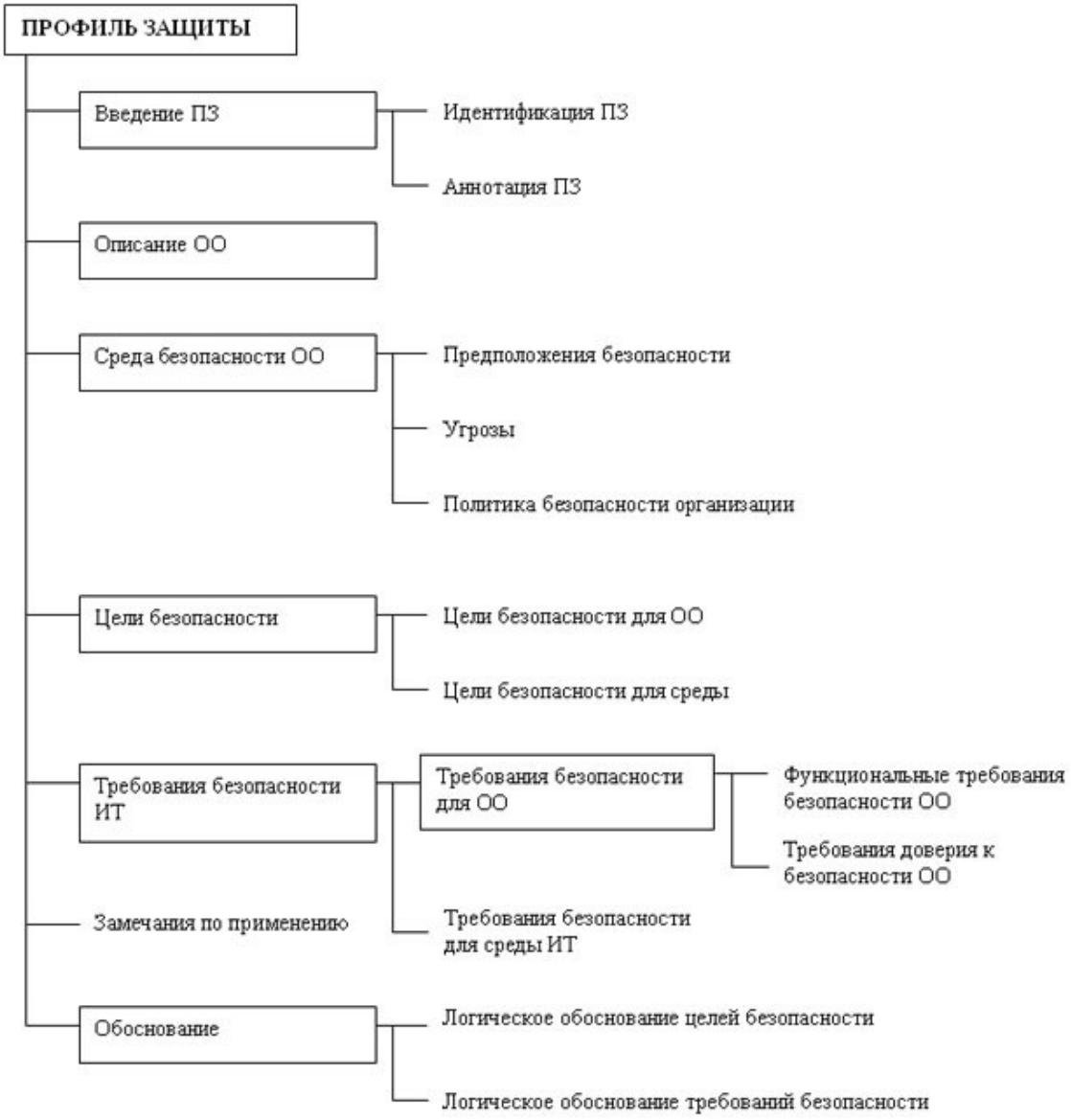


Рис. 10.2. Структура профиля защиты

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 [1, 2].

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 [3].

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. 10.3 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.

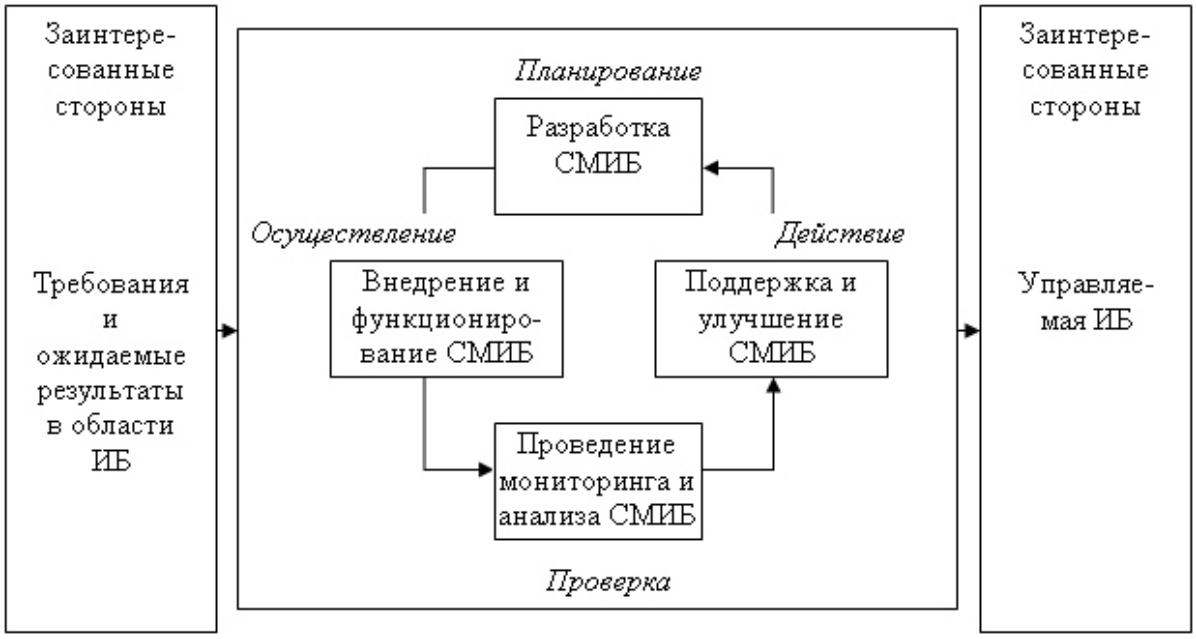


Рис. 2.3. Этапы построения и использования СМИБ

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

На основе лекционного материала, материала методических рекомендаций к лабораторной работе и ресурсов сети Интернет разработайте требования к хранению, использованию, утилизации информации для предприятия, описанного ранее в курсовой работе. Проработайте требования для специалистов по подбору кадров с целью внесения пунктов об информационной безопасности в трудовой договор новых сотрудников.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1) Что предполагает информационное обеспечение любой компании в целом?
2) Дайте объяснение (устное описание) схемы на рис. 10.1
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 № 11.

ШИФРОВАНИЕ ТЕКСТА КАК МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ

Цель работы: изучить метод перестановки для шифрования открытого текста.

Оборудование: компьютер с операционной системой Windows, текстовый редактор Microsoft Word.

При подготовке лабораторной работы использованы материалы: 1) 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. URL: http://www.234555.ru/publ/12-1-0-408 (Режим доступа свободный).

Дополнительная литература: 1) Гашков С. Б., Применко Э. А., Черепнев М. А. Криптографические методы защиты информации. – М.: Академия, 2010. – 304 с.; 2) Информационная безопасность. Методы шифровнаия. Под ред. Е.Сухарева. – М.: Радиотехника, 2011. - 208 с. 3)

Теоретическая часть

Шифрование является одним из эффективных способов защиты текстовой информации. При шифровании существуют следующие понятия [1].

Открытый текст – информация, содержание которой может быть понятно любому субъекту.

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.

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.

Криптосистема – совокупность алгоритмов, реализуемых функциями E и D, множества ключей k, $'k$ и шифротекстов.

Криптограмма (загадочное письмо или тайнопись) – наука о защите информации с помощью шифрования.

Криптоанализ – наука о методах дешифрования.

Криптостойкость – характеристика надёжности шифротекста от вскрытия.

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.

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

$$1 \le i \le n,\ C_i = P_{k[i]}, \qquad (1)$$

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; $k = \{k_1, k_2, k_3, \ldots Pk_i, k_n\}$ – ключ шифрования.

При расшифровании используется обратная перестановка:

$$P_{k[i]} = C_i. \quad (2)$$

Как видно из приведенных выражений, ключ должен удовлетворять условиям: $k_i \neq k_j$, $1 \leq k_i \leq n$

Рассмотрим пример шифрования слова «Пример» методом перестановки. Зададим ключ, который должен быть равен 6-ти символам (количеству символов в шифруемом слове) в виде $k = \{1, 2, 3, 4, 5, 6\}$.

11.1. 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

Применим формулу (1) с выбранным ключом k к слову «Пример». Получим следующие выражения:

$C_1 = P_{k[1]} = P_1 = $ 'П'; $C_2 = P_{k[2]} = P_4 = $ 'м'; $C_3 = P_{k[3]} = P_6 = $ 'р';

$C_4 = P_{k[4]} = P_2 = $ 'р'; $C_5 = P_{k[5]} = P_3 = $ 'и'; $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 (2):

$P_{k[1]} = P_1 = C_1 = $ 'П'; $P_{k[2]} = P_4 = C_2 = $ 'м'; $P_{k[3]} = P_6 = C_3 = $ 'р';

$P_{k[4]} = P_2 = C_4 = $ 'р'; $P_{k[5]} = P_3 = C_5 = $ 'и'; $P_{k[6]} = P_5 = C_6 = $ 'е';

Таким образом, получим $P = \{P_1, P_2, P_3, P_4, P_5, P_6\} = \{\text{Пример}\}$.

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 [1]:

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.

Этап а

р	и	р	п	э
	я	о	р	т

Этап б

э	п	р	р	и
т	р		о	я

ш		в	и	о
и		а	м	т
ф		н	е	

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) одно слово открытого текста ключом, длина которого равна длине шифруемого слова.

3. Придумать символьный пароль, преобразовать его в ключ и зашифровать (расшифровать) фразу открытого текста с помощью этого ключа [1].

Выберите предложение открытого текста для шифрования в соответствии с номером своего варианта (таблица 11.2)

11.2. Таблица выбора заданий по вариантам

Вариант №	№ шифруемой строки	Вариант №	№ шифруемой строки	Вариант №	№ шифруемой строки
1	1	7	7	13	13
2	2	8	8	14	14
3	3	9	9	15	15
4	4	10	10	16	16
5	5	11	11	17	17
6	6	12	12	18	18

Строки для создания шифра

1. Существует три разновидности угроз.

2. Угроза нарушения конфиденциальности заключается в следующем.

3. Информация становится известной тому, кто не располагает полномочиями доступа к ней.

4. Она имеет место всякий раз, когда получен доступ к некоторой секретной информации.

5. Информация хранится в вычислительной системе или передается от одной системы к другой.

6. В связи с угрозой нарушения конфиденциальности, используется термин «утечка».

7. Угроза нарушения целостности включает в себя любое умышленное изменение информации.

8. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена.

9. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения.

10. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью.

11. Целостность информации это существование информации в неискаженном виде.

12. Чаще субъектов интересует обеспечение более широкого свойства – достоверности информации.

13. Угроза отказа служб возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы.

14. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен.

15. Или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того чтобы он стал бесполезным.

16. В этих случаях говорят, что ресурс исчерпан.

17. Естественные угрозы – угрозы, вызванные воздействиями на АС и её компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.

18. Искусственные угрозы это угрозы информационной безопасности АС, вызванные деятельностью человека.

Оформление результатов выполнения лабораторной работы [1]

Ответы к заданиям оформляются в текстовом редакторе Microsoft Word и сохраняются в файл. Название файла формируется из фамилии и номера лабораторной работы, например Иванов_11.doc.

Исходное слово для шифрования:

Ключ шифрования:

Результат шифрования

Символьный пароль

Цифровой пароль _ _ _ _ _ _ _ _ _ _

Фраза для шифрования

Этап а

Этап б

Результат шифрования

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1) Охарактеризовать информацию и её свойства.
2) Что является предметом и объектом защиты информации?
3) Чем определяется ценность информации? Приведите классификацию конфиденциальной информации.
4) Охарактеризовать свойства достоверности и своевременности информации.
5) Что понимается под угрозой информации? Назвать разновидности угроз информации.

6) Привести классификацию угроз информации.
7) Какие основные направления и методы реализации угроз вам известны?
8) Пояснить классификацию злоумышленников.
9) Охарактеризовать причины и виды утечки информации.
10) Назвать и привести примеры каналов утечки информации.
11) Перечислить задачи государства в области безопасности информации.
12) Охарактеризовать основные законы РФ, регулирующие отношения в области информационных технологий.
13) Назвать государственные органы, обеспечивающие безопасность информационных технологий, и решаемые ими задачи.
14) Пояснить, что такое шифрование и в чём заключается сущность метода перестановки.

Лабораторная работа № 12.
ИССЛЕДОВАНИЕ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ АЛГОРИТМА RSA

Цель работы: изучить принцип действия электронной цифровой подписи;

Оборудование: компьютер с операционной системой Windows.

При подготовке лабораторной работы использованы материалы: 1) 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. URL: http://www.234555.ru/publ/12-1-0-408 (Режим доступа свободный).

Дополнительная литература: 1) Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации. В 2-х т. Т.2. Информационная безопасность. – М.: Арий, 2008. – 444 с. 2) Молдовян Н.А. Теоретический минимум и основы цифровой подписи. – Спб.: БВХ-Петербург, 2010. – 304 с. 3) Гашков С. Б., Применко Э. А., Черепнев М. А. Криптографические методы защиты информации. – М.: Академия, 2010. – 304 с. 4)

Теоретическая часть

Технология применения электронной цифровой подписи (ЭЦП) предполагает наличие сети абонентов, обменивающихся подписанными электронными документами. При обмене электронными документами по сети значительно снижается затраты, связанные с их обработкой, хранением и поиском [1].

Одновременно при этом возникает проблема, как аутентификации автора электронного документа, так и самого документа, т.е. установление подлинности автора и отсутствие изменений в полученном электронном сообщении.

В алгоритмах ЭЦП как и в асимметричных системах шифрования используются однонаправленные функции. ЭЦП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. ЭЦП представляет собой относительно небольшой объем дополнительной цифровой информации, передаваемой вместе с подписанным текстом.

Концепция формирования ЭЦП 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 подписи, которая реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Система ЭЦП содержит две процедуры:

- ✓ Формирование цифровой подписи;
- ✓ Проверку цифровой подписи;

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи – открытый ключ отправителя [1].

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 [1].

Обобщенная схема формирования и проверки электронной цифровой подписи приведена на рис. 12.1.

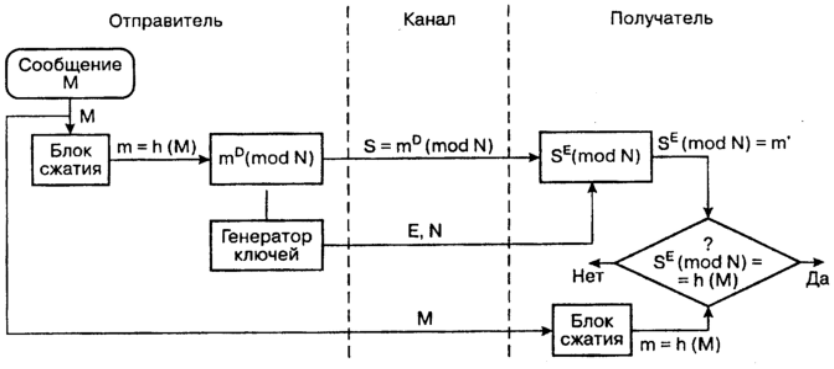


Рис. 12.1. Схема RSA электронной цифровой подписи [1]

Практическая часть

Изучение алгоритма RSA электронной цифровой подписи

Определение открытого «e» и секретного «d» ключей [1]

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.

Задание: На основе теоретического материала, указанного алгоритма и рассмотренного примера сформировать электронную цифровую подпись (значение чисел выдается преподавателем).

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1) Откуда получил название алгоритм RSA?
2) Рассказать основной принцип, на котором основан алгоритм RSA.
3) Назовете процедуры, которые составляют систему электронной цифровой подписи.
4) Основное назначение электронной цифровой подписи и условие ее существования.
5) На чем основана концепция формирования ЭЦП?
6) Дать пояснения к блок-схеме алгоритма RSA.

Лабораторная работа № 13.
БРАНДМАУРЫ И МЕТОДЫ ЗАЩИТЫ КОМПЬЮТЕРА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Цели работы: а) изучить принцип действия брандмауэра и обозревателя Internet Explorer как средств защиты от несанкционированного доступа; б) получить навык проведения анализа защищенности информационных ресурсов.

Оборудование: компьютер с операционной системой Windows, наличие обозревателя Internet Explorer, возможность регулировать включение брандмаура Windows.

При подготовке лабораторной работы использованы материалы: 1) 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. URL: http://www.234555.ru/publ/12-1-0-408 (Режим доступа свободный). 2) Межсетевой экран. URL: http://ru.wikipedia.org/wiki (Режим доступа: свободный).

Дополнительная литература: 1) Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации. В 2-х т. Т.1. Несанкционированное получение информации. – М.: Арий, 2008. – 464 с. 2) Шаньгин В.Ф. Методы и средства защиты компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2010. – 544 с. 3) Шелупанов А., Зайцев А. Технические средства и методы защиты информации. – М.: Горячая линия-Телеком, 2009. – 616 с.

Теоретическая часть

Брандмауэр – сочетание программного и аппаратного обеспечения, образующее систему защиты от несанкционированного доступа из внешней глобальной сети во внутреннюю сеть (интрасеть). Брандмауэр предотвращает прямую связь между внутренней сетью и внешними компьютерами, пропуская сетевой трафик через прокси-сервер, находящийся снаружи сети. Прокси-сервер определяет, следует ли разрешить файлу попасть во внутреннюю сеть. Брандмауэр называется также шлюзом безопасности [1].

Можно считать брандмауэр пограничным постом, на котором проверяется информация (часто называемая трафик), приходящая из Интернета или локальной сети. В ходе этой проверки брандмауэр отклоняет или пропускает информацию на компьютер в соответствии с установленными параметрами.

Когда к компьютеру пытается подключиться кто-то из Интернета или локальной сети, такие попытки называют «непредусмотренными запросами». Когда на компьютер поступает непредусмотренный запрос, брандмауэр Windows блокирует подключение. Если на компьютере используются такие программы, как программа передачи мгновенных сообщений или сетевые игры, которым требуется принимать информацию из Интернета или локальной сети, брандмауэр запрашивает пользователя о блокировании или разрешении подключения. Если пользователь разрешает подключение, брандмауэр Windows создает исключение, чтобы в будущем не тревожить пользователя запросами по поводу поступления информации для этой программы [2].

Если идёт обмен мгновенными сообщениями с собеседником, который собирается прислать файл (например, фотографию), брандмауэр Windows запросит подтверждение о снятии блокировки подключения и разрешении передачи фотографии на компьютер. А при желании участвовать в сетевой игре через Интернет с друзьями пользователь может добавить эту игру как исключение, чтобы брандмауэр пропускал игровую информацию на компьютер. Хотя имеется возможность отключать брандмауэр Windows для отдельных подключений к Интернету или локальной сети, это повышает вероятность нарушения безопасности компьютера.

Чтобы открыть компонент «Брандмауэр Windows», нажмите кнопку Пуск, выберите пункты Настройка, Панель управления, Сеть и подключения к Интернету и Брандмауэр Windows [1].

В обозревателе Internet Explorer имеется несколько возможностей, позволяющих обеспечить защиту конфиденциальности, а также повысить безопасность личных данных пользователя. Параметры конфиденциальности позволяют защитить личные данные пользователя — с помощью этих параметров можно понять, как просматриваемые веб-узлы используют эти данные, а также задать значения параметров конфиденциальности, которые будут определять, разрешено ли веб-узлам сохранять файлы «cookie» на компьютере.

В число параметров конфиденциальности Internet Explorer входят следующие:

- ✓ Параметры конфиденциальности, определяющие обработку на компьютере файлов «cookie».
- ✓ Файлы «cookie» — это созданные веб-узлом объекты, которые сохраняют на компьютере определенные сведения, например о предпочтениях пользователя при посещении данного узла. Кроме того, эти файлы могут также сохранять личные данные пользователя, такие как имя и адрес электронной почты.
- ✓ Оповещение безопасности, выдаваемые пользователю при попытке получить доступ к веб-узлу,не соответствующему заданным параметрам конфиденциальности.
- ✓ Возможность просмотра политики конфиденциальности P3P для веб-узла.

Средства безопасности позволяют предотвратить доступ других пользователей к таким сведениям, на доступ к которым у них нет разрешения. Это, например, сведения о кредитной карточке, вводимые при покупках в Интернете. Эти средства безопасности могут также защитить компьютер от небезопасного программного обеспечения.

В число параметров безопасности Internet Explorer входят следующие.

- ✓ Возможность блокирования большинства всплывающих окон.
- ✓ Возможность обновления, отключения или повторного включения надстроек для веб-обозревателя.
- ✓ Средства повышения безопасности, предупреждающие пользователя о попытке веб-узла загрузить файлы или программы на компьютер.
- ✓ Цифровые подписи, которые подтверждают, что файл поступил действительно от указанного лица или издателя и с момента включения цифровой подписи в этот файл никем не внесены изменения.

- ✓ Безопасное подключение с использованием 128-разрядного ключа, которое применяется для связи с безопасными веб-узлами.

Поиск уязвимостей в системе защиты

Противостояние атакам – важное свойство защиты. Казалось бы, если в сети установлен межсетевой экран (firewall), то безопасность гарантирована, но это распространенное заблуждение может привести к серьёзным последствиям [1].

Например, межсетевой экран (МЭ) не способен защитить от пользователей, прошедших аутентификацию. А квалифицированному хакеру не составляет труда украсть идентификатор и пароль авторизованного пользователя. Кроме того, межсетевой экран не только не защищает от проникновения в сеть через модем или иные удалённые точки доступа, но и не может обнаружить такого злоумышленника.

При этом система защиты, созданная на основе модели адаптивного управления безопасностью сети (Adaptive Network Security, ANS), способна решить все или почти все перечисленные проблемы. Она позволяет обнаруживать атаки и реагировать на них в режиме реального времени, используя правильно спроектированные, хорошо управляемые процессы и средства защиты.

Компания Yankee Group опубликовала в июне 1998 г. отчёт, содержащий описание процесса обеспечения адаптивной безопасности сети. Этот процесс должен включать в себя анализ защищённости, т.е. поиск уязвимостей, обнаружение атак, а также использовать адаптивный (настраиваемый) компонент, расширяющий возможности двух первых функций, и управляющий компонент.

Анализ защищённости осуществляется на основе поиска уязвимых мест во всей сети, состоящей из соединений, узлов (например, коммуникационного оборудования), хостов, рабочих станций, приложений и баз данных. Эти элементы нуждаются как в оценке эффективности их защиты, так и в поиске в них неизвестных уязвимостей. Процесс анализа защищённости предполагает исследование сети для выявления в ней слабых мест и обобщение полученных сведений, в том числе в виде отчёта. Если система, реализующая данную технологию, содержит адаптивный компонент, то устранение найденной уязвимости будет осуществляться автоматически. При анализе защищённости обычно идентифицируются:

- ✓ люки в системах (back door) и программы типа «троянский конь»;
- ✓ слабые пароли;
- ✓ восприимчивость к проникновению из внешних систем и к атакам типа «отказ в обслуживании»;
- ✓ отсутствие необходимых обновлений (parch, hotfix) операционных систем;

- ✓ неправильная настройка межсетевых экранов, WEB-серверов *и баз данных.*

Обнаружение атак – это процесс оценки подозрительных действий в корпоративной сети, реализуемый посредством анализа журналов регистрации операционной системы и приложения (log-файлов)либо сетевого трафика. Компоненты ПО обнаружения атак размещаются на узлах или в сегментах сети и оценивают различные операции, в том числе с учётом известных уязвимостей. Адаптивный компонент ANS позволяет модифицировать процесс анализа защищенности, предоставляя самую последнюю информацию о новых уязвимостях. Он также модифицирует компонент обнаружения атак, дополняя его последней информацией о подозрительных действиях и атаках. Примером адаптивного компонента может служить механизм обновления баз данных антивирусных программ, которые являются частным случаем систем обнаружения атак.

Управляющий компонент предназначен для анализа тенденций, связанных с формированием системы защиты организации и генерацией отчётов. К сожалению, эффективно реализовать все описанные технологии в одной системе пока не удаётся, поэтому пользователям приходится применять совокупность систем защиты, объединённых единой концепцией безопасности. Пример таких систем – семейство продуктов SAFEsuite, разработанных американской компанией Internet Security Systems (ISS). В настоящее время комплект ПО SAFEsuite поставляется в новой версии SAFEsuite Enterprise, в которую входит также ПО SAFEsuite Decisions, обеспечивающее принятие решений по проблемам безопасности.

Система анализа защищённости Internet Scanner предназначена для проведения регулярных всесторонних или выборочных тестов сетевых служб, операционных систем, используемого прикладного ПО, маршрутизаторов, межсетевых экранов, WEB-серверов и т.п.

Другим примером системы анализа защищенности является программа SuperScan, позволяющая сканировать открытые порты узлов с известными IP-адресами. Для начала сканирования достаточно в поле Start указать IP-адрес сканируемого узла. Для более глубокого сканирования необходимо указать минимальную скорость сканирования, передвинув движок на отметку Min.

Практическая часть

1. Определить все доступные узлы в локальной сети [1].
2. Просканировать порты сервера компьютерной сети (компьютерного класса).

Результаты поиска уязвимостей в системе защиты

узла _____ IP: ___ . ___ . ___ . ___

Символьное имя узла *IP адрес узла*

Оформить результаты лабораторной работы в виде таблицы

№ п.п.	№ порта	Наименование	№ п.п.	№ порта	Наименование
1			7		
2			8		
3			9		
4			10		
5			11		
6			12		

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1) Может ли брандмауэр блокировать компьютерным вирусам и «червям» доступ на компьютер?
2) Может ли брандмауэр запретить пользователю открывать сообщения электронной почты с опасными вложениями?
3) Может ли брандмауэр блокировать спам или несанкционированные почтовые рассылки?
4) Может ли брандмауэр запросить пользователя о выборе блокировки или разрешения для определённых запросов на подключение?
5) Перечислите параметры, определяющие работу брандмауэра.
6) Какой параметр брандмауэра обеспечивает наивысшую защиту компьютера?
7) Что такое брандмауэр, его назначение.
8) Какими возможностями обладает Интернет обозреватель для защиты личных данных пользователей?
9) Перечислите параметры безопасности Internet Explorer.
10) Для чего нужно проводить анализ защищенности сети?

Лабораторная работа № 14.

ТИПЫ КОМПЬЮТЕРНЫХ ВИРУСОВ И МЕТОДЫ БОРЬБЫ С НИМИ

Цель работы: получить навыки подбора антивирусного ПО для домашнего и офисного пользования

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

При подготовке лабораторной работы использованы материалы: 1) Энциклопедия безопасности Касперского. URL: http://www.securelist.com/ru/threats/detect/ (Режим доступа: свободный).

Дополнительная литература: 1) Гошко С.В. Технологии борьбы с компьютерными вирусами. - М.: Солон-Пресс, 2009. - 352 с. 2) Михайлов А.В. Компьютерные вирусы и борьба с ними. - М: Даилог-МИФИ, 2011. - 104 с.

Теоретическая часть

Компьютерный вирус – это небольшая саморазмножающаяся программа, мешающая нормальной работе компьютера [1].

Процесс внедрения вирусом своей копии в другую программу, файлы или системную область диска называется **заражением,** а программа или иной объект, содержащий вирус — **зараженным.**

Основные источники вирусов и последствия их действия

Основными источники вирусов являются:

- ✓ съемный диск или DVD-диск, на котором находятся зараженные вирусом файлы;
- ✓ компьютерная сеть, в том числе система электронной почты и Internet;
- ✓ жесткий диск, на который попал вирус в результате работы с зараженными программами;
- ✓ вирус, оставшийся в оперативной памяти после предшествующего пользователя.

При заражении безвредными вирусами происходит уменьшение объема свободной оперативной памяти или памяти на дисках. Заражение неопасными вирусами приводит также к уменьшению объема свободной оперативной памяти или памяти на дисках или непонятным системным сообщениям, музыкальным и визуальным эффектам и т.д.

Опасные вирусы производят замедление загрузки и работы компьютера, непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов, ошибки при загрузке операционной системы, невозможность сохранять файлы в нужных каталогах. Очень опасные вирусы являются причиной исчезновения файлов, форматирования жесткого диска, невозможности загрузки файлов или операционной системы.

Классификация вирусов

Вирусы классифицируются по нескольким признакам:

1. ***По способу заражения***: резидентные и нерезидентные;
2. ***По среде обитания***: файловые, сетевые, бутовые (загрузочные);
3. ***По деструктивным возможностям***: опасные и неопасные;

По «среде обитания» вирусы можно разделить на несколько типов.

Резидентные вирусы – это вирусы, которые оставляют себя или часть себя в оперативной памяти и перехватывают любые операции ввода/вывода. При выключении компьютера уничтожаются вместе с очищением памяти.

Нерезидентные вирусы – характеризуются тем, что активны только при запуске зараженного файла, как только файл закрывается, вирус сворачивается.

Опасные – характеризуются, как правило, спонтанными аудиоэффектами, притормаживают работу ОС, привязаны к датам, как правило, одноразовые.

Загрузочные вирусы

Рассмотрим схему функционирования простого загрузочного вируса, заражающего диски.

Вспомним, что происходит при включении компьютера. В первую очередь начинает работу программа BIOS, которая тестирует компьютерную систему. После того как выясняется, что все компоненты компьютера функционируют нормально, управление передается небольшой программе-загрузчику операционной системы (ЗОС), которая должна загрузить операционную систему с диска и передать ей управление.

Таким образом, нормальная схема начальной загрузки следующая:

BIOS(ПЗУ) → ЗОС(диск) → Операционная система (диск) (1)

Теперь рассмотрим вирус. В загрузочных вирусах выделяют две части — так называемую голову и так называемый хвост. Хвост, вообще говоря, может быть пустым.

Пусть имеется не зараженный компьютер и дискета с активным резидентным вирусом. Как только этот вирус обнаружит, что в дисководе появилась подходящая жертва — в нашем случае еще не зараженный винчестер — он приступает к заражению. Заражая диск, вирус производит следующие действия:

- выделяет некоторую область диска и помечает ее как недоступную операционной системе; это можно сделать по-разному, в простейшем и традиционном случае занятые вирусом секторы помечаются как сбойные ***(bad),*** иногда вирусы даже форматируют на диске дополнительную дорожку;
- копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор;
- замещает программу начальной загрузки в загрузочном секторе (настоящем) своей головой;
- организует цепочку передачи управления согласно схеме:

Голова вируса → Хвост вируса → Оригинальный загрузочный сектор. (2)

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору. В цепочке (1) появляется новое звено:

BIOS(ПЗУ) Вирус → ЗОС(диск) → Операционная система.

Файловые вирусы

Простые файловые вирусы

В отличие от загрузочных вирусов, которые практически всегда резидентные, файловые вирусы совсем не обязательно резидентные. Файловые вирусы поражают исполняемые файлы.

Шифрованные и **полиморфные вирусы**

К данному типу вирусов относятся те, у которых часть кода зашифрована. При запуске вирус расшифровывается (разворачивается) в памяти и только потом выполняется.

Полиморфные вирусы имеют один и тот же зашифрованный код вируса, который можно расшифровать разными расшифровщиками. Кроме того имеется алгоритм для их автоматической генерации.

Стелс-вирусы

Некоторые загрузочные и файловые вирусы предпринимают специальные действия для «маскировки» — скрытия своего присутствия в зараженных объектах. Такие вирусы получили название «стеле-вирусов». Наиболее просто стелс-механизм реализуется в операционной системе MS-DOS. Способов маскировки (стелсирования) имеется довольно много, но все они реализуют одну идею — «сделать вид, что с зараженным объектом все нормально».

Макро-вирусы

Данные вирусы являются макросами, хранящимися во внешних файлах программного обеспечения (документах Microsoft Office, Autocad, CorelDRAW и пр.) и при открытии документа исполняются внутренними интерпретаторами данных программ. Широкое распространение они получили благодаря огромным возможностям интерпретатора языка Visual Basic, интегрированного в Microsoft Office. Излюбленным местом обитания этих вирусов являются офисы с большим документооборотом.

Макрос, написанный на языке VBA и интегрированный в документ, например, Word или Excel, обладает всеми теми же возможностями, что и обычное приложение. Он может отформатировать ваш винчестер или просто удалить информацию, украсть какие-то файлы или пароли и отправить их по электронной почте. Фактически вирусы этого класса способны парализовать работу целого офиса, а то даже и не одного

Троянские программы и **утилиты скрытого администрирования**

Одними из наиболее распространенных вирусов данного типа являются **Trojan и Backdoor программы.** Отличие этих двух типов программ заключается в том, что троянская программа выполняет активные действия (уничтожение данных, сбор данных и отправка через Internet, выполнение каких-либо действий в определенное время), в то время как Backdoor-программы открывают удаленный доступ к компьютеру и ожидают команды злоумышленника. Для простоты будем называть оба этих класса троянскими программами.

Главное отличие «троянов» от всех перечисленных выше творений человеческого разума — это то, что троянские программы не размножаются сами. Они единожды устанавливаются на компьютер и долгое время (как правило, либо до момента обнаружения, либо до переустановки операционной системы по какой-либо причине) выполняют свои функции.

Компьютерный антивирус – программа для поиска и уничтожения компьютерных вирусов.

Различают следующие типы компьютерных антивирусов:

1. Детекторы (полифаги)

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Для этого они используют так называемые «маски». Маской вируса называют некоторую постоянную последовательность программного кода, специфичную для этого вируса. Если антивирусная программа обнаружит такую последовательность в каком-либо файле, то файл считается зараженным и подлежит лечению. Некоторые программы-детекторы также выполняют эвристический анализ файлов и системных областей дисков, что часто (но отнюдь не всегда) позволяет обнаруживать новые, не известные программе-детектору вирусы.

2. Ревизоры

Программы-ревизоры запоминают сведения о состоянии файлов и системных областей дисков, т.е. принцип работы ревизора основан на подсчете контрольных сумм файлов и некоторой другой: длины файлов, даты их последней модификации и т.д. Эти сведения сохраняются в базе данных антивируса. При последующих запусках ревизоры сравнивают состояния данных, содержащихся в базе данных с реально подсчитанными. При выявлении несоответствий об этом сообщается пользователю. Недостаток ревизоров состоит в том, что они не могут обнаружить вирус в новых файлах (на съемных дисках, при распаковке файлов из архива, в электронной почте), поскольку в их базе данных отсутствует информация об этих файлах.

3. Сторожа

Программы-сторожа (или блокировщики) располагаются резидентно в оперативной памяти компьютера и проверяют на наличие вирусов запускаемые файлы и вставляемые в дисковод съемные диски. При наличии вируса об этом сообщается пользователю. Кроме того, многие программы-сторожа перехватывают те действия, которые используются вирусами для размножения и нанесения вреда (скажем, попытку записи в загрузочный сектор или форматирование жесткого диска), и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции. Программы-сторожа позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

Практическая часть

1) Посетить сайты наиболее известных разработчиков антивирусных программ:
   а) Антивирус Касперского (http://www.kaspersky.ru/),
   б) Доктор Web (http://www.drweb.com/),
   в) NOD32 (http://www.esetnod32.ru/),
   д) Avast! (http://www.avast-russia.com/).

2) Исходя из информации, представленной на сайтах разработчиков анитивирусного ПО, проанализировать виды угроз, от которых гарантированно предоставляется защита. Анализ проводить по параметрам защиты от: 1) мошеннического ПО; 2) хакерских атак; 3) фишинга; 4) спама.

Результаты представить в виде статистической гистограммы, используя средства программного продукта MS Excel.

На основе полученных результатов выбрать антивирусное ПО для реализации политики безопасности компании. Привести обоснование выбора в виде сравнительного отчета выбранного продукта с остальными продуктами, по следующим показателям: а) стоимость; б) надежность; в) устойчивость; г) простота использования; д) наличие спецпредложений.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1) Что такое компьютерный вирус и компьютерный антивирус?
2) Повысится ли устойчивость компьютера к воздействию вируса, если установить два антивирусных продукта одновременно?
3) Какие существуют классификации вирусов?
4) Какие существуют разновидности файловых вирусов?

5) Каков принцип функционирования загрузочных вирусов?
6) Каковы внешние проявления наличия вируса в компьютере?
7) Перечислить типы антивирусного ПО?

КОНТРОЛЬНОЕ ТЕСТИРОВАНИЕ ЗА СЕМЕСТР ПО ТЕМАМ ЛЕКЦИЙ И ЛАБОРАТОРНЫХ РАБОТ № 7-14 НАХОДИТСЯ В ПРИЛОЖЕНИИ В К МЕТОДИЧЕСКИМ РЕКОМЕНДАЦИЯМ.

ПРИЛОЖЕНИЕ А

КОНТРОЛЬНОЕ ТЕСТИРОВАНИЕ 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