МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН

КАЗНУ им. АЛЬ-ФАРАБИ

ХАКИМОВА ТИЫШТИК

ИННОВАЦИОННЫЕ МЕТОДЫ ОБУЧЕНИЯ ИНФОРМАТИКИ

АЛМАТЫ 2012 г.

УДК 372.851.02
УДК 372.800.4.02 УДК 004

Рекомендовано постановлением заседании кафедры
«Информатики», механико-математического факультета КазНУ им.аль-Фараби

Рецензенты:

Урмашев Б.А.-кандидат физико-математических наук, доцент зав. кафедры
«Информатики», Казахского национальный университет им.аль-Фараби
Хасенова Г.И. –кандидат технических наук, профессор,
зав. кафедры «Автоматизации и вычислительной техники», Каспийского общественного университета

ХакимоваТ.. ИННОВАЦИОННЫЕ МЕТОДЫ ОБУЧЕНИЯ ИНФОРМАТИКИ - Алматы, 2012,169с.

Учебное пособие предназначено для студентов университетов, обучающихся по кредитной технологии обучения использующих современные инновационные технологий. / к.п.н., доцент Хакимовой Т.Х.– Алматы: КазНУ имени аль-Фараби, 2012. – 169 с.

Данное учебное пособие способствует приобретению практических навыков работы на современных ЭВМ.

Материал, изложенный в пособий, предназначен для использования современных информационных технологии в учебном процессе таких: Безопасность информации и защита информации,Криптографические системы защиты информации, Мультимедийные технологии, Интернет технологии, Дистанционные технологии обучения предоставляют возможность самостоятельного решения проблем обработки информации, связанных с автоматизацией производства, используя новые информационные технологии.

Предлагаемое учебное пособие составлено на основе типовой и рабочей программы по предмету «Информатика» и предназначено для студентов первых курсов, а также может быть полезно магистрантам и аспирантам, и подготовки студентов к промежуточному государственному контролю.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Для успешного вхождения в число 50-ти наиболее конкурентоспособных государств, необходимо менять методы обучения информационной технологии в учебном процессе по кредитной системе обучения. Кредитная технология обучения пришла в систему высшего образования сравнительно недавно, поэтому многие педагогические коллективы и студенты ощущают постоянную нехватку современной литературы по кредитной технологии и методике обучения. В сложившейся ситуации задача заключается в том, чтобы подготовить высококвалифицированных специалистов, которые уверенно могут ориентироваться в современных условиях стремительного развития информационных технологий. В частности, это означает, что специалист должен владеть соответствующими программными продуктами и его приложениями различного типа.

Уровень освоения теоретических знаний и практических навыков обучающихся определяет степень профессионализма его дальнейшей деятельности. В результате обучения расширяется кругозор, развивается мышление, формируется научное мировоззрение, а полученный багаж знаний по основам информатики способствует самостоятельной творческой работе.

Материал, изложенный в пособий, предназначен для использования современных информационных технологии в учебном процессе таких: Безопасность информации и защита информации,Криптографические системы защиты информации,Мультимедийные технологии,Интернет технологии,Дистанционные технологии обучения предоставляют возможность самостоятельного решения проблем обработки информации, связанных с автоматизацией производства, используя новые информационные технологии.

Использование многофункциональных возможностей компьютерной техники при подготовке научных рефератов и дипломной работы делает образовательный процесс в вузе интересным и доступным. В связи с появлением на рынке новых IT, новых типов ЭВМ, меняется и программное обеспечение. Однако очень мало литературы по методике обучения IT – технологии. Поэтому своевременный выход данной инновационной книги является очень актуальным в условиях вхождения нашего Государства в ВТО. И для успешной реализации программы Президента РК необходимо побольше выпускать учебников по новым педагогическим технологиям и методике преподавания информатике.

ГЛАВА 1. КРЕДИТНАЯ ТЕХНОЛОГИЯ ОБУЧЕНИЯ

Основная идея общеобразовательного подхода заключается в том, что очень важно вовремя дать студентам представление об информационных процессах, об общности информационных процессов в природе, обществе и технике, об информационных ресурсах как факторе социального и культурного развития общества, об информации как социальном феномене.

Актуальным является умение личности ставить цели развития и оперативное добывание и структурирование из всего информационного потока достоверной и полезной информации, необходимой для реализации поставленных целей, т.е. “осознанный контроль за поиском информации будет подчинен целям, определяемым личностью для своего прогрессивного развития.

Государственный образовательный стандарт высшего профессионального образования, в котором определены государственные требования к минимуму содержания и уровню подготовки выпускников университетов, дает характеристику базового образования по информатике, оставляя при этом значительный простор для дифференцированного профильного развития этого курса.

Образование, и обучение в частности, тесно связано с понятием «профессиональная ориентация», поскольку в результате обучения человек может получить возможность реализовать свои интересы, способности, склонности в выбранной сфере профессиональной деятельности.

1.1.Современная технология обучения

Основными задачами современных информационных технологий обучения являются разработка интерактивных сред управления процессом познавательной деятельности и доступа к современным информационно-образовательным ресурсам (мультимедиа учебникам и учебникам, построенным на основе гипертекста, различным базам данных, обучающим сайтам и другим источникам).

Современные информационные технологии обучения – совокупность современной компьютерной техники, средств телекоммуникационной связи, инструментальных программных средств, обеспечивающих интерактивное программно-методическое сопровождение современных технологий обучения. Главные направления инновационных преобразований в педагогической системе:

- педагогическая система в целом;
- учебные заведения;
- педагогическая теория;
- педагог;
- обучаемые;
- педагогическая технология;
- содержание;
- формы, методы, средства;
- управление;
- цели и результаты.

По глубине преобразований в этих подсистемах можно судить о сущности, качестве и целесообразности инновационных нововведений.

В создании и выполнении современного обучения необходимо системное проектирование преподавания учебных дисциплин и учения с учетом возможностей технического обеспечения. Переход на новую форму обучения требует пересмотра всей научно-методической обеспеченности дисциплин специальности, разработку новых инновационных методик обучения и воспитания студентов. В отличие от традиционно

представляемого учебного материала в виде линейных структур современное гипертекстовое представление учебной информации, позволяет значительно увеличить объем материала, расширив как тематику, так и спектр его представления, облегчая поиск, интерпретацию, выбор нужного аспекта. Также гипертекстовую обучающую систему отличает удобная среда обучения, в которой легко находить нужную информацию, возвращаться к уже пройденному материалу и т.д.

Компьютерные технологии обучения – совокупность методов, приемов, способов, средств создания педагогических условий работы на основе компьютерной техники, средств телекоммуникационной связи и интерактивного программного продукта, моделирующих часть функций педагога по представлению, передаче и сбору информации, организации контроля и управления познавательной деятельностью. Компьютерные технологии обучения предоставляют большие возможности в развитии творчества педагогов и обучающихся. Применение компьютерных технологий обучения позволяет видоизменить процесс обучения, реализовать модель личностно-ориентированного обучения. Обучающимся необходимо усвоить такие базовые понятия, как технология, технологическая среда, технологический процесс, способы преобразовательной деятельности и др. Кроме того, будущие специалисты должны иметь представление о прогрессивных технологиях материального и духовного производства и основных формах жизнедеятельности человека. Широкое использование демонстрационного материала, как слайды, электронные учебники и комплексы технических средств обучения (ТСО) обеспечивает высокий уровень самостоятельной познавательной деятельности студентов.

Качественным образованием может считаться такое образование, которым удовлетворен потребитель, т.к. у него, как будущего специалиста за время учебы должны выработаться такие качества, как активность, умение отстаивать свое мнение, самостоятельность, умение вести себя в коллективе и способность креативного мышления, т.е. способность предлагать что-то оригинальное. Прогресс в области развития персональных электронно-вычислительных машин сыграл важную роль в преобразовании учебно-воспитательного процесса. ЭВМ представляет возможности для контроля знаний и для выполнения тренировочных упражнений, компьютеры повышают эффективность педагогического процесса. Применение электронных учебников, компьютерных обучающих программ хорошо развивает логику и абстрактное мышление. Фундаментальные знания в области новых информационных технологий подразумевают владение коммуникативными навыками – сбор, анализ, синтез информации. Информационные технологии включают программированное обучение, интеллектуальное обучение, экспертные системы, гипертекст и мультимедиа.

1.2.Внедрение кредитной технологии обучения в учебный процесс

Переход на новые образовательные технологии обусловлен необходимостью улучшения качества подготовки специалистов, разработки нового поколения учебных планов и программ. Внедрение кредитной технологии затрагивает всю идеологию образования. Преподаватель теперь не только передает знания, а главным образом учит, как надо учиться, добывать знания, приобретать навыки и умения самому практически делать. Усиливается роль самостоятельной работы студента, повышаются требования к качеству преподавания, обучение становится демократичным, обеспечивается открытость обучения. Для решения проблем методик развивающего характера требуется использовать активные методы обучения. Подобные методы отличаются высокой вовлеченностью обучаемых в учебный процесс, побуждают студентов быть активными. На занятиях с использованием этих методов студенты самостоятельно принимают решения (известно, что знания, которые обучающиеся добывают самостоятельно, запоминаются на более длительное время, чем знания, преподнесенные им как факт). Указанные методы обучения обеспечивают направленную активность психических процессов обучаемых: стимулируют мышление при использовании проблемных ситуаций, обеспечивают запоминание главного на уроках,

возбуждают интерес к изучаемому предмету и вырабатывают потребность к самостоятельному приобретению знаний. Новая технология, которая активно внедряется в системе образования - это по сути революция в системе высшего профессионального образования, которая призвана повышать уровень самообразования и творческого освоения знаний на основе индивидуализации, выборности образовательной траектории в рамках строгой регламентации учебного процесса и учёта объёма знаний в виде кредитов. Введение кредитной технологии обучения в вузах Казахстана вызвано мировыми тенденциями в реформировании национальных систем образования с целью создания единой международной системы взаимозачетов с последующей реализацией условий, необходимых для академического обмена студентами, преподавателями, специалистами.

Реформирование системы высшего образования в республике осуществляется с учетом мировых тенденций, передовых педагогических моделей. В этой связи в 2002/2003 учебном году Министерство образования и науки приняло решение, поддержанное вузами, о переходе отечественной магистратуры на международную систему организации академического образования. Ее основой как раз таки и является кредитная технология — методика организации учебного процесса, используемая ведущими университетами зарубежных стран. Так, толчком к развитию американской системы кредитования явилось внедрение в 1869 году в Гарвардском университете предметов по выбору. Еще раньше «движение за свободу обучения» возникло в Германии. Разнообразные системы кредитов используются и в других странах Европы. При составлении университетских учебных планов и программ там используются в качестве унифицированной единицы измерения объема учебной работы студента - академические кредиты. В переводе с латыни: ***credit — доверие***. В учебном процессе под этим понятием подразумевается следующее: каждая учебная дисциплина имеет свой индекс трудоемкости, это число часов в неделю, отводимое для ее изучения во время аудиторных занятий, лабораторных работ, семинаров, самостоятельной работы студента. В основе введения кредитной технологии в Казахстане лежит настоятельная потребность в конвертируемости вузовских дипломов, кодификации, унификации, каталогизации учебных курсов и программ, что, безусловно, позволит снять барьеры между университетами разных стран. Кредитная технология обучения способствует международному признанию национальной образовательной программы Республики Казахстан, поможет вузам выйти на мировой уровень.

Введение инновационного образования позволить подготовить специалиста нового типа, профессионально подготовленного к работе по избранной специальности. Специалист всегда будет востребован, если будет владеть новыми технологиями, свободно использовать возможности сети Интернет.

1.3. Возможности использования интерактивных методов по информатике

В связи с внедрением кредитной технологии обучения предлагаются новые подходы к системе подготовки квалифицированного специалиста, обладающего творческими способностями к решению профессиональных задач, отвечающих современным государственным и международным стандартам. Внедрение кредитной системы обучения в организацию учебного процесса с использованием интерактивных методов по предмету «Информатика» должно обеспечить качество образования.

Достоинством ***кредитной технологии*** обучения является возможность подготовки специалистов на уровне мировых стандартов, гибкое планирование учебного процесса, установление оптимального соотношения аудиторной и самостоятельной работ, привитие студенту навыков и потребности к самостоятельному творческому овладению знаниями, а также организация совместного обучения студентов и взаимное признание кредитов и дипломов.

В новой системе программа обучения должен формироваться в основном студентом, т.к. многие дисциплины, также как и преподавателей, студенту придется выбирать самому. Изменения, происходящие в системе высшего образования, требуют от студента гибкости

мышления, опережающий характер, профессионализм, компетентность, умение общаться, нестандартность подхода к решению возникших проблем.

Цель кредитной системы обучения по информатике - развитие у студентов навыков принятия решений на основе определенных знаний, а также развитие качеств творческой личности, способной решать самостоятельно информационные задачи, возникающие в ходе профессиональной деятельности.

Уровень освоения теоретических знаний и практических навыков обучающихся определяет степень профессионализма его дальнейшей деятельности. В результате обучения расширяется кругозор, развивается мышление, формируется научное мировоззрение, а полученный багаж знаний по основам информатики способствует самостоятельной творческой работе. В процессе преподавания информатики можно использовать следующие основные интерактивные методы: структурированные занятия, выявление ошибок при составлении программ, работа в Интернете, групповые дискуссии и презентации.

1.4. Методы обучения информатике

Внедрение кредитной системы обучения в организацию учебного процесса с использованием интерактивных методов по предмету «Информатика» должно обеспечить качество образования,активизировать познавательную деятельность студентов, развивать у них качество творческой личности, способной решать самостоятельно проблемы обработки информации в информационном пространстве, возникающие в ходе профессиональной деятельности.

Преподавание информатики является неотъемлемой частью общего блока профессиональной подготовки будущих специалистов. В результате изучения базового курса информатики студенты должны освоить разделы: «Информатика», «Безопасность информации и защита информации», «Криптографические системы защиты информации», «Мультимедийные технологии», «Интернет технологии» и «Дистанционные технологии», также должны уметь использовать ресурсы Интернета для организации самостоятельной работы.

Целью курса «Информатика» является систематизированное изложение основ информатики и обучение студентов работе с операционными системами и их приложениями, обучение общей методике построения алгоритмов, позволяющих быстро осваивать различные языки программирования.

В связи с требованиями информационного общества серьезным изменениям должна подвергнуться и методика обучения дисциплины «Информатика». Необходимо пересмотреть и изменить психологические и педагогические аспекты обучения, т.к. в сфере образования появилась необходимость в подготовке специалиста-исследователя, способного творчески воспринимать новые научные идеи и умеющего управлять современными технологическими процессами. Успешное функционирование современного производства обеспечивается высококвалифицированными специалистами, которые овладели техническими знаниями и производственными навыками. Качество продукции закладывается при разработке проекта, обеспечивается при ее изготовлении.

При обучении основам информатики для повышения эффективности педагогического процесса, необходимо опираться на прогрессивные научно-технические достижения сферы информационных технологий. Особую актуальность при обучении данного базового предмета приобретает использование ***интерактивных методов*** – это деловые игры, анализ конкретных ситуации, проблемные лекции, активное программированное обучение, обмен опытом, т.е. это модель открытого обсуждения, развивающая умение спорить, дискутировать. Основные задачи метода ***активного обучения***

– это привитие таких умений, как решение профессиональных проблем и предвидение сложных реальных обстоятельств.

Для повышения эффективности педагогического процесса при обучении информатике необходимо опираться на методические требования к построению предмета, это - усвоение содержания, ясность и твердость понимания. Необходимо дать квалифицированное образование в области вычислительной техники, программного обеспечения, опираясь на прогрессивные, мультимедийные научно-технические достижения.

Компьютерному обучению особенно присущи два новшества: ***интерактивное видео и мультимедиа.*** В традиционном обучении для того, чтобы найти материал на нужную тему, обычно требуется прочитать общую литературу или статьи в энциклопедии, использовать ссылки на более специальный материал, и вообще просматривать источники до тех пор, пока не убедишься, что весь материал, относящийся к вопросу, изучен. Однако такой метод имеет определенные ограничения. В процессе поиска той или иной специальной информации, возможно, потребовалось бы просмотреть огромное количество материала, не относящегося к делу.

Мультимедийные системы исключают такую неэффективную работу, прогресс в технологии хранения информации дает возможность размещать целые библиотеки документов, звуков, видео изображений на лазерных дисках, с которыми может работать компьютер. Сообщения можно оформлять в виде гипердокумента, может быть послан через сеть или модем на компьютер по адресу. Мультимедийная технология вызвала значительный интерес, потому что она способствует тому, что обучающийся может управлять тем, что он изучает, увеличивает групповое взаимодействие, обеспечивает немедленный доступ к базе данных материалов и даёт возможность получить немедленный результат.

Интерактивное видео может быть в двух формах: компьютер, связанный с видеомагнитофоном или с проигрывателем видеодисков. Основное преимущество обоих типов состоит в том, что эффективность компьютерных программ может быть увеличена с помощью более качественного визуального и звукового сопровождения. Например, вопросы тренировки и практики могли бы сопровождаться изображением соответствующего метода. Преимущество видеокассет состоит в том, что большинству классов требуется только интерфейс и программное обеспечение, и это дает педагогу возможность построить занятия, основанные на использовании компьютера.

Оборудование видеодисками имеет дополнительное преимущество получения произвольного доступа. Любой эпизод может быть вызван на экран в любой момент времени, студент может изучить информационную систему, тратя столько времени, сколько ему хочется. Таким образом, легко осуществляется разветвление в зависимости от потребностей и интереса обучающегося.

Информационная технология (information technology) – совокупность методов, производственных и программно-технологических средств, объединенных в технологическую цепочку, обеспечивающую сбор, хранение, обработку, распространение, отображение и использование информации. Информационные технологии предназначены для снижения трудоемкости процессов использования информационных ресурсов.

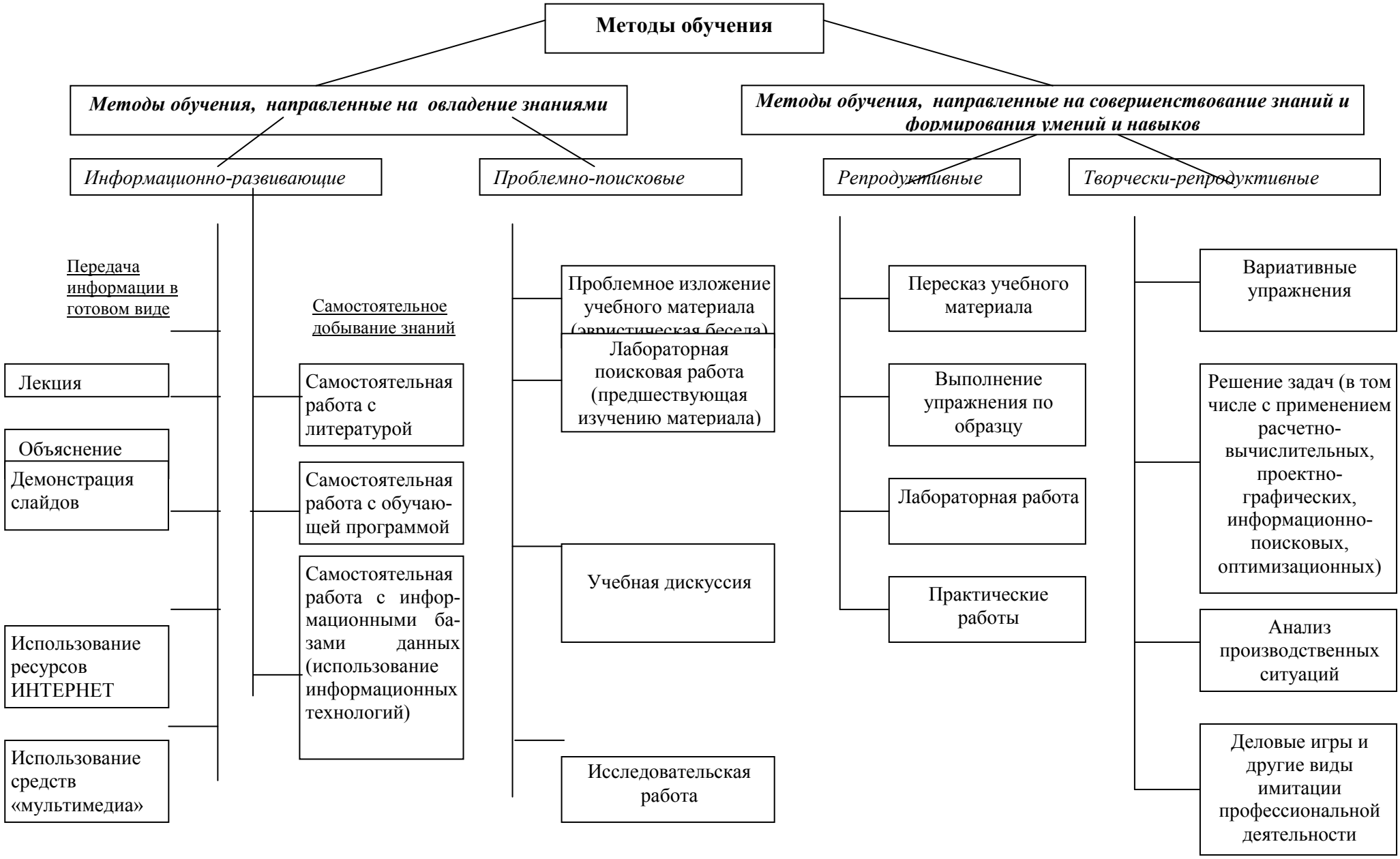
В результате изучения дисциплины «Информатика» студенты должны:

- уверенно работать на компьютере, как пользователь ПК;
- уметь разрабатывать алгоритмы и программы на современных языках программирования для решения технических и экономических задач;
- уметь разрабатывать БД для представления значений, описывающих технологические процессы;
- уметь составлять электронные таблицы для задач;
- при решении задач - применять компьютерное моделирование;
- уметь пользоваться ресурсами INTERNET, в локальных и глобальных телекоммуникационных компьютерных сетях .

- уметь предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; о безопасности информации и защита информации
- уметь возможность представления информации пользователю во взаимодействии различных форм (текст, графика, анимация, звук, видео) в интерактивном режиме.
- уметь системно-организованную совокупность средств передачи данных, информационных ресурсов, протоколов взаимодействия, аппаратно-программного и организационно-методического обеспечения, и ориентируется на удовлетворение образовательных потребностей пользователей.

Широкое применение информационных технологий способно резко повысить эффективность интерактивных методов обучения (схема 1) для всех форм организации учебного процесса: на этапе самостоятельной подготовки студентов, на лекциях, а также на практических занятиях.

Схема 1 – Классификация методов интерактивного обучения информатике



Основными задачами современных информационных технологий обучения являются разработка интерактивных сред управления процессом познавательной деятельности и доступа к современным информационно-образовательным ресурсам (мультимедиа учебникам и учебникам, построенным на основе гипертекста, различным базам данных, обучающим сайтам и другим источникам).

1. Мировоззренческие задачи - это дальнейшее формирование философского воззрения студента, понимание системно-информационной картины мира осознание единства законов функционирования информации в природе и обществе, подготовка к дальнейшей практической деятельности.
2. Методологические задачи - это дальнейшее изучение основ информатики, усвоение методов, принципов, законов, идей информатики.

Повышение эффективности учебного процесса в целом, дальнейшее формирование общеучебных умений и навыков, индивидуализация учебного процесса за счет использования системы упражнений и задач .

3. Прикладные задачи - это дальнейшее освоение и применение средств информатики, применения компьютера в качестве инструмента познания.

Рисунок Задачи курса

1.5. Роль самостоятельной работы студентов при кредитной технологии обучения

Кредитная (доверительная) система обучения делает основную ставку на самостоятельную подготовку студентов, знания добываются самими обучающимися в процессе активной деятельности, а преподаватель выполняет функцию наставника, направляющего студента и дающего ему ориентиры. Данный процесс обучения способствует развитию мышления у обучающихся, овладению умением и навыками, затруднения при решении задач побуждают к самостоятельной работе. Решение проблемы активизирует продуктивное мышление, формирует творческий подход к обучению.

Самостоятельная работа студентов (СРС) наряду с аудиторной представляет одну из форм учебного процесса и является существенной его частью. Для его успешного выполнения необходимы планирование и контроль со стороны преподавателей, а также планирование объема самостоятельной работы в учебных планах специальностей профилирующими кафедрами, учебной частью, методическими службами учебного заведения.

Ввиду наличия вариантов определения самостоятельной работы в педагогической литературе мы будем придерживаться следующей формулировки:

- ***самостоятельная работа*** – это планируемая работа студентов, выполняемая по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. СРС предназначена не только для овладения каждой дисциплиной, но и для формирования навыков самостоятельной работы вообще, в учебной, научной, профессиональной деятельности, способности принимать на себя ответственность, самостоятельно решить проблему, находить конструктивные решения, выход из кризисной ситуации и т.д. Значимость СРС выходит далеко за рамки отдельного предмета, в связи, с чем выпускающие кафедры должны разрабатывать стратегию формирования системы умений и навыков самостоятельной работы. При этом следует исходить из уровня самостоятельности абитуриентов и требований к уровню самостоятельности выпускников с тем, чтобы за период обучения искомый уровень был достигнут.

Согласно новой образовательной парадигме независимо от специализации и характера работы любой начинающий специалист должен обладать фундаментальными знаниями, профессиональными умениями и навыками деятельности своего профиля, опытом творческой и исследовательской деятельности по решению новых проблем, опытом социально-оценочной деятельности. Две последние составляющие образования формируются именно в процессе самостоятельной работы студентов. Кроме того, задачей кафедр является разработка дифференцированных критериев самостоятельности в зависимости и вида деятельности .

Самостоятельная работа студентов (СРС) – это особый вид учебной деятельности обучающихся, которая направлена на самостоятельное выполнение дидактической задачи, формирование интереса к познавательной деятельности и пополнение знаний с помощью изучения и конспектирования первоисточников.

СРС включает внеаудиторное время без участия преподавателя в соответствии с предложенным перечнем заданий, где студент должен связать работу с реализацией практических задач, которые обеспечивают развитие логического мышления, творческой активности, исследовательского подхода в освоении учебного материала.

Общий объем часов самостоятельной работы обучающихся очной формы обучения в бакалавриате составляет 66% от общей трудоемкости дисциплины, до половины которых отводится на самостоятельную работу студентов под руководством преподавателя (СРСП). При заочной форме обучения объем самостоятельной работы обучающихся должен составлять не менее 80% от общего объема отведенных кредитов.

В зависимости от уровня обучения, самостоятельная работа обучающегося и соответственно самостоятельная работа обучающегося под руководством преподавателя подразделяется на СРС (СРСП) – для студента, СРМ (СРМП) – для магистранта, СРД (СРДП) – для докторанта.

Процесс самостоятельной работы обучающихся должен быть основан на использовании инновационных технологий. Аудиторная форма СРСП предполагает работу обучающихся с учебником и первоисточником, выполнение групповых заданий, индивидуальную аналитическую деятельность в рамках поставленной задачи. СРСП проводится по каждой дисциплине в течение всего академического периода согласно графику с указанием даты, времени, аудитории и тьюторов. Занятия в рамках СРСП могут иметь консультативные и интерактивные формы, соотношение которых определяется сложностью изучаемого курса, объемом отведенных на его изучение аудиторных часов, уровнем

подготовленности обучающихся. Занятия в рамках СРСП также предназначены для обучающихся, имеющих низкий текущий рейтинг, желающих получить дополнительные консультации, испытывающих трудности при выполнении полученных заданий по дисциплине.

Для повышения эффективности педагогического процесса при обучении студентов по предмету «Информатика», необходимо опираться на прогрессивные научно-технические достижения, дать квалифицированное образование в области вычислительной техники. В частности, при обучении разделов операционных систем, текстовых редакторов и табличного процессора необходимо передавать следующие знания:

- принципы работы с командами ОС WINDOWS – для грамотного применения при работе с пакетом прикладных программ, используя многозадачность ОС;
- назначение и основные функции текстового редактора MS WORD – для использования при выполнении курсовых и дипломных работ;
- способы использования табличных процессоров MS EXCEL – для работы с данными, созданными СУБД;
- способы использования базы данных;
- умение работать с прикладными программами – для эскизного проекта в дипломной работе;
- алгоритмические язык программирование: СИ,Turbo PASCAL.
- при решении задач - применять компьютерное моделирование;
- пользоваться ресурсами INTERNET, в локальных и глобальных телекоммуникационных компьютерных сетях .
- предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; о безопасности информации и защита информации
- возможность представления информации пользователю во взаимодействии различных форм (текст, графика, анимация, звук, видео) в интерактивном режиме.
- системно-организованную совокупность средств передачи данных, информационных ресурсов, протоколов взаимодействия, аппаратно-программного и организационно-методического обеспечения, и ориентируется на удовлетворение образовательных потребностей пользователей.

Изменения, происходящие в системе высшего образования, требуют от студента гибкости мышления - опережающий характер, профессионализм, компетентность, умение общаться, нестандартность подхода к решению возникших проблем.

Уровень освоения теоретических знаний и практических навыков обучающихся определяет степень профессионализма его дальнейшей деятельности. В результате обучения расширяется кругозор, развивается мышление, формируется научное мировоззрение, а полученный багаж знаний по основам информатики способствует самостоятельной творческой работе.

Использование компьютерной подготовки в курсовом и дипломном проектировании делает образовательный процесс разнообразно интересным в его освоении, с точки зрения практической работы и содержательным в аспекте теоретической деятельности. Выпускник, должен освоить основы экономики, организации и планирования производства на базе компьютерной подготовки. Широта использования полученных знаний и практических навыков в высшей школе охватывает практически все сферы профессиональной деятельности будущего специалиста.

Так, как основу обучения составляют знание, умение и навыки, то можно утверждать, что обучение и есть воспитание. Получение фундаментальных систематизированных знаний и умение их применять – это и есть образование, а передача знаний и опыта – это воспитание, с помощью которого формируются определенные взгляды и ориентации на сферу применения полученных знаний.

Из-за высоких темпов научно-технического прогресса, знания, полученные в высших учебных заведениях, быстро устаревают. Поэтому каждому специалисту необходимо постоянно углублять свое образование, овладевать новыми навыками и подходами. Студент может успешно учиться, если будет проявлять познавательную активность и упорство в овладении изучаемым материалом.

Поскольку традиционное обучение во многом не отвечает современным требованиям, существует объективная необходимость применения новых методов обучения, которые позволяют формировать творческих знающих специалистов, способных самостоятельно решать сложные профессионально–производственные и научные проблемы, активное развивающее проблемно–контекстное обучение формирует профессиональное творческое мышление студента.

Всестороннее развитие личности происходит в активной деятельности, направленной на решение познавательных и практических задач. Например, лабораторная (практическая) работа по основам информатики закрепляет лекционный материал и в то же время требует от обучающихся глубокого творческого анализа, т.к. организация лабораторных работ студентов по применению знаний компьютерной технологий на практике включает в себе следующие приемы:

- Правильную постановку задачи;
- Определение необходимой модели;
- Построение алгоритма задач;
- Руководство ходом выполнения алгоритма;
- Методы преобразования детали;
- Программное обеспечение;
- Подведение итога.

Научно-технический прогресс, приводя к существенным изменениям в технике и в производстве, предъявляет одинаково высокие требования и к тем, кто создает машины, и к тем, кто ими управляет.

Знания, умение и навыки по базовой дисциплине «Информатика» в основном приобретаются через самостоятельную работу. По кредитной технологии обучения самостоятельная работа студентов под руководством преподавателя (СРСП) основана на использовании инновационных технологий и предполагает работу обучающихся с учебником, активным раздаточным материалом и первоисточником, предварительно подготовленным преподавателем.

Средства информационных технологии играют особую роль в развитии, умений самообразовательной деятельности студентов, т.к. многокомпонентная среда – мультимедиа позволяет обучающимся использовать текст, графику и видео в интерактивном режиме и тем самым расширяет области применения компьютера в учебном процессе.

В таблице 1 приведена характеристика форм организации учебного процесса по дисциплине «Информатика».

Таблица 1. Формы организации учебного процесса по информатике

Формы обучения (ФО)		***Формы контроля (ФК)***	
Формы обучения, направленные на теоретическую подготовку	*Формы обучения, направленные на практическую подготовку*	*Традиционные формы контроля:*	*Инновационные формы контроля:*

• лекция • научный семинар • контролируемая самостоятельная работа (СРСП) • самостоятельная внеаудиторная работа (СРС) • научная конференция • консультация	• практическое занятие • лабораторная работа • групповые дискуссии • все виды практики • деловая игра • структурированное занятие • исследования (проекты)	• контрольная работа • текущий контроль • индивидуальное собеседование • переводные и семестровые экзамены	• тестирование • рубежный контроль • рейтинговый итоговый контроль • кейс-стадий • комплексный экзамен по специальности

Современные средства обучения (компьютеры, телекоммуникационные средства связи, необходимое интерактивное программное и методическое обеспечение) предоставляют возможность интенсификации занятий различных форм обучения, но имеют наибольшее значение для организации самоподготовки обучающихся в роли методического и информационного обеспечения самостоятельной работы. Безусловно, современный компьютер и интерактивное программно-методическое обеспечение требуют изменения формы общения преподавателя и обучающегося, превращая обучение в деловое сотрудничество, а это существенно усиливает мотивацию обучения, приводит к необходимости поиска новых модели занятий, проведение итогового контроля (доклады, отчеты, публичные защиты групповых проектных работ), повышает индивидуальность и интенсивность обучения. ***Предмет технологии обучения*** – создание систем обучения и профессиональной подготовки. Существуют пять основных способов использования программ традиционного компьютерного обучения, причем каждый служит для осуществления различных функций и задач: консультации, практика, учебные игры, моделирование и способы решения задач.

Если человека постоянно приучать усваивать знания и умения в готовом виде, можно и притупить его природные творческие способности, «разучить» думать самостоятельно. В максимальной степени процесс мышления проявляется и развивается при решении **проблемных задач**. Выделяют основные условия успешного проблемного обучения:

1) необходимо вызвать интерес обучающихся к содержанию проблемы;

2) обеспечить посильность работы для студентов с возникающими проблемами;

3) информация, которую обучающийся получит при решении проблемы, должна быть значимой, важной в учебно–профессиональном плане.

Проблемное обеспечение ставит своей задачей:

- развития мышления и способностей студентов, развитие творческих умений;
- усвоение студентами знаний, умений, добытых в ходе активного поиска и самостоятельного решения проблем, в результате эти знания, умения более прочные, чем при традиционном обучении;
- воспитание активной творческой личности студента, умеющего видеть, ставить и разрешать нестандартные, профессиональные проблемы.

Выделяют три основных метода проблемного обучения: проблемное изложение, частично – поисковая деятельность и самостоятельная исследовательская деятельность.

Наиболее ***простой метод – проблемное изложение учебного материала*** на лекции, когда преподаватель ставит проблемные вопросы, выстраивает проблемные задачи и сам их решает; студенты лишь мысленно включаются в процесс поиска решения. Например, лекцию по изучению темы: «Решение задач с помощью табличного процессора EXCEL» по информатике можно начать с проблемы, с которой часто сталкиваются: нахождение оптимального решения поставленной задачи.

Выпускники, должны освоить основы экономики, организации и планирования производства на базе компьютерной подготовки. Широта использования полученных знаний и практических навыков в высшей школе охватывает практически все сферы профессиональной деятельности будущего специалиста.

ГЛАВА 2. ТЕХНОЛОГИИ ПРЕПОДАВАНИЯ ИНФОРМАТИКИ С ПРИМЕНЕНИЕМ ИННОВАЦИОННЫХ МЕТОДОВ

2.1.Технология информационной безопасности.

План:

Понятие национальной безопасности и виды безопасности. Роль и место системы обеспечения ИБ в системе национальной безопасности РК. Обоснование проблемы защиты информации в информационных системах. Концепция информационной безопасности.

Теоретический материал:

Словосочетание информационная безопасность в разных контекстах может иметь различный смысл. Состояние защищенности национальных интересов в информационной сфере определяется совокупностью сбалансированных интересов личности, общества и государства.

Под информационной безопасностью будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

К информационной безопасности относят также проблемы формирования культурного, духовно-нравственного наследия, исторических традиций, патриотизма и гуманизма. Эти компоненты общественной жизни - важнейшая часть менталитета, характера и душевного строя народов.

Все виды национальной безопасности тесно взаимосвязаны и взаимно дополняют друг друга: каждый из видов безопасности, может достаточно ярко проявляться в сфере действия другого, дополняя или ослабляя его влияние.

Экономическая безопасность. Это защищенность жизненно важных интересов личности, общества и государства в эк. сфере от внутренних и внешних угроз. Также это состояние, в котором народ может суверенно, без вмешательства и давления извне, определять пути и формы своего экономического развития.

Опасности могут быть: международные (глобальные и региональные в смысле регионов мира), национальные, локальные (или региональные в смысле регионов страны) и частные (фирм и личности).

Пути экономической безопасности

1. Отказ от навязывания моделей развития, от экономического и политического принуждения;
2. Уважение законности существования различных форм собственности и интересов;
3. Признание принципов равноправия государств вне зависимости от социального и политического строя;
4. Свобода выбора пути, развития и форм организации эк. жизни;
5. Суверенитет государств над природными ресурсами и экономическим потенциалом в своих странах.

Концепция экономической безопасности

Обеспечивает сотрудничество государств в решении глобальных проблем человечества и станет основой мирного сосуществования в безъядерном и ненасильственном мире, гарантией прогресса в деле ликвидации экономической отсталости и слаборазвитости.

Объекты : государство, его экономическая система и все его природные богатства, общество с его институтами, учреждениями, фирмами и личностью.

Субъекты : функциональные и отраслевые министерства и ведомства, налоговые и таможенные службы, банки, фонды и страховые компании, производители и продавцы продукции, работ и услуг и т.д.

Предмет - определение и мониторинг факторов, подрывающих устойчивость социально-экономической системы и государства в краткосрочной перспективе.

Военная безопасность. Военная политика проводится на основании положений, разработанных в военной доктрине РК (совокупность официальных взглядов, определяющих военно-политические, военно-стратегические и военно-экономические основы обеспечения военной безопасности РК).

В военной доктрине конкретизируются применительно к военной сфере установки Концепции национальной безопасности РК.

Цели: Предотвращение, локализация и нейтрализация военных угроз РК

Правовая основа Военной доктрины: Конституция РК; и др. законы; Международные договоры РК в области обеспечения военной безопасности.

Руководство обеспечения военной безопасности РК осуществляет Президент РК, который является Верховным Главнокомандующим Вооруженными Силами РК.

Экологическая безопасность. В результате активного воздействия цивилизации на окружающую среду степень ее загрязнения возрастает с каждым годом.

Особенно сильно это негативное влияние в: местах экологических катастроф; местах нерационального использования минеральных ресурсов и вредных отходов производства. Охрана атмосферного воздуха и водные объекты

Это ключевая проблема оздоровления окружающей природной среды. Атмосферный воздух занимает особое положение среди других компонентов биосферы.

Загрязняющие отрасли: теплоэнергетика; предприятия металлургии; нефтедобыча и нефтехимия; автотранспорт; производство стройматериалов. и др.

Информационная безопасность. Это состояние надежной защищенности культурного достояния страны, интеллектуальной собственности хозяйствующих субъектов и граждан, специальных сведений, составляющих государственную и профессиональную тайну.

Вопросы информационной безопасности занимают особое место и в связи с возрастающей ролью в жизни общества требуют к себе все большего внимания. Успех практически любой деятельности в немалой степени зависит от умения распоряжаться такой ценностью, как информация.

Информацию без преувеличения можно отнести к одному из решающих ресурсов развития. Она в современном мире активно влияет на все сферы жизнедеятельности не только отдельных государств, но и всего мирового сообщества. Однако в определенных случаях информация может быть использована не только во благо, но и во вред интересам личности, общества и государства. Поэтому роль информационной безопасности в системе национальной безопасности не только существенно возрастает, но и выходит на первый план.

Национальный информационный ресурс стал одним из главных источников экономической мощи как государства в целом, так и отдельных финансовых, научно-исследовательских и производственных субъектов. В этой связи необходимо сформулировать государственные интересы в информационной сфере, провести оценку эффективности существующей системы безопасности и наметить первоочередные меры по ее совершенствованию.

Определение приоритетов в обеспечении информационной безопасности Республики Казахстан основывается на выявлении соответствующих угроз в информационной сфере, поиске путей их преодоления, разработке механизмов обеспечения информационной безопасности и т.д. Основой для реализации приоритетов информационной безопасности является устойчивое и бесконфликтное развитие государства, развитое гражданское общество, способное контролировать и корректировать государственные позиции в информационной сфере, гарантированная безопасность общества и личности.

Целями защиты информации являются:

- предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям;
- предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;
- обеспечение правового режима документированной информации как объекта собственности;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
– сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

Концепция информационной безопасности Республики Казахстан разработана на основании Конституции Республики Казахстан и законов Республики Казахстан: "О национальной безопасности Республики Казахстан", "О государственных секретах", "О борьбе с терроризмом", "Об электронном документе и электронной цифровой подписи", "Об информатизации" ,"О противодействии экстремизму" и др. (www.zakon.kz)

Современный период развития цивилизованного общества характеризует процесс информатизации. Широкая информатизация всех сфер жизнедеятельности общества принципиально изменяет роль информации и информационных технологий и приводит к глобальным изменениям в информационной сфере мирового сообщества.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышает зависимости общества от степени безопасности используемых им информационных технологий. Актуальность и важность проблемы обеспечения информационной безопасности обусловлена следующими факторами:

- высокие темпы роста парка персональных компьютеров, применяемых в самых разных сферах деятельности;
- резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;
- увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;
- сосредоточение в единых базах данных информации различного назначения и различной принадлежности;
- бурное развитие программных средств, не удовлетворяющих даже минимальным требованиям безопасности;
- повсеместное распространение сетевых технологий и объединение локальных сетей в глобальные;
- развитие глобальной сети Internet, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире.

Несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных и компьютерных систем, к сожалению, не уменьшается.

Концепция информационной безопасности

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Цель мероприятий в области информационной безопасности - защитить интересы субъектов информационных отношений. Интересы эти многообразны, но все они концентрируются вокруг трех основных аспектов:

- доступность (возможность за разумное время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного прочтения).

При этом все средства, методы и мероприятия, используемые для защиты информации объединяются в единый целостный механизм - систему защиты.

С учетом сложившейся практики обеспечения информационной безопасности выделяют следующие **направления защиты информации:**

1. **Правовая защита** - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

2. **Организационная защита** - это регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.
3. **Инженерно-техническая защита** - это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.
По функциональному назначению средства инженерно- технической защиты классифицируются на следующие группы:
• *физические средства*, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств и финансов и информации от противоправных воздействий;
• *аппаратные средства* - приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации. В практике деятельности предприятия
находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих производственную деятельность.
Основная задача аппаратных средств - обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства, применяемые в производственной деятельности;
• *программные средства*, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных;
• *криптографические средства* - специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Для реализации защиты информации создается система безопасности.
Под **Системой безопасности** будем понимать организационную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятий, государства от внутренних и внешних угроз.
В рамках системы безопасности присутствует система защиты информации.
Система защиты информации (СЗИ) – это организованная совокупность специальных органов средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

К сожалению необходимость комплексного обеспечения безопасности информационных технологий пока не находит должного понимания у пользователей современных ИС. В то же время построение систем защиты информации не ограничивается простым выбором тех или иных средств защиты.
Для создания таких систем необходимо иметь определенные теоретические знания, а именно:
· что представляет собой защищенная информационная система,
· что такое система защиты информации и какие требования предъявляются к ней,
· какие существуют угрозы и причины нарушения безопасности информационных технологий,
· какие функции защиты и каким образом должны быть реализованы, как они противодействуют угрозам и устраняют причины нарушения безопасности,
· как построить комплексную систему защиты информации,
· как достичь высокого уровня безопасности при приемлемых затратах на средства защиты информации и многое, многое другое.

Контрольные вопросы:
1 Дать определения понятиям: информация, информационная безопасность, система защиты.
2 Понятие национальной безопасности и виды безопасности.
3 Охарактеризуйте, концепцию информационной безопасности РК
4 Что понимается под защитой информации в информационных системах?
5 Назовите аспекты информационной безопасности?

2.2. Безопасность информации и защита информации

Цель: изучить существующие меры обеспечения безопасности информации

План:

Характеристические свойства систем защиты информации. Методы защиты информации. Характеристические свойства систем обеспечения безопасности информации. Методы и средства обеспечения безопасности информации

Теоретический материал:

Система защиты информации (СЗИ) – это организованная совокупность специальных органов средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз. С позиций системного подхода к защите информации предъявляются определенные требования. Защита информации **должна быть:**

1. Непрерывной.
2. **Плановой**. Каждая служба разрабатывает план защиты информации в сфере своей компетенции.
3. **Целенаправленной**. Защищается то, что должно защищаться в интересах конкретной цели.
4. **Конкретной**. Защищаются конкретные данные, объективно подлежащие защите.
5. **Активной.**
6. **Надежной.**
7. **Универсальной**. Распространяется на любые каналы утечки информации.
8. **Комплексной**. Применяются все необходимые виды и формы защиты.

Для реализации данных требований СЗИ может иметь следующее **обеспечение:**

1. **Правовое.**
2. **Организационное**. Различные виды служб.
3. **Аппаратное**. Технические средства защиты информации.
4. **Информационное**. Сведения, данные, показатели.
5. **Программное**. Программы.
6. **Математическое**. Математические методы.
7. **Лингвистическое.** Языковые средства общения.
8. **Нормативно-методическое**. Регламент деятельности служб, практические методики.

Способы - это порядок и приемы использования сил и средств для достижения поставленной цели по защите конфиденциальной информации.

Способы защиты информации - это совокупность приемов, сил и средств, обеспечивающих конфиденциальность, целостность, полноту и доступность информации, и противодействие внутренним и внешним угрозам.

Обеспечение информационной безопасности достигается системой мер, направленных:

− на **предупреждение угроз.** Предупреждение угроз — это превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;

− на **выявление угроз.** Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;

− на **обнаружение угроз.** Обнаружение имеет целью определение реальных угроз и конкретных преступных действий;

− на **локализацию** преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;

− на **ликвидацию** последствий угроз и преступных действий и восстановление статус- кво.

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.

Предупреждение угроз возможно и путем получения (если хотите — и добывания) информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний. Для этих целей необходима работа сотруд

ников службы безопасности с информаторами в интересах наблюдения и объективной оцени
ситуации как внутри коллектива сотрудников, особенно главных участков ее фирмы, так и вне, среди конкурентов и преступных формирований.

В предупреждении угроз весьма существенную роль играет информационно-аналитическая деятельность службы безопасности на основе глубокого анализа криминогенной обстановки и деятельности конкурентов и злоумышленников.

Выявление имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны крими-нальных структур или конкурентов на рынке производства и сбыта товаров и продукции.

Обнаружение угроз - это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов
хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих u1089 секретов.

Пресечение или локализация угроз - это действия, направленные на устранение дейст-вующей угрозы и конкретных преступных действий. Например, пресечение подслушивания
конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий имеет целью восстановление состояния предшествовавшего наступлению угрозы.

Принцип максимальной дружественности - не надо вводить запреты там, где можно без них обойтись (на всякий случай); вводить ограничения нужно с минимальными неудобствами для пользователя. Следует обеспечить совместимость создаваемой СЗИ с используемой ОС, программными и аппаратными средствами ИС.

Принцип прозрачности - СЗИ должна работать в фоновом режиме, быть незаметной и не мешать пользователям в основной работе, выполняя при этом все возложенные на нее функции.

Принцип превентивности - последствия реализации угроз безопасности информации могут потребовать значительно больших финансовых, временных и материальных затрат по сравнению с затратами на создание комплексной системы защиты.

Принцип оптимальности - Оптимальный выбор соотношения различных методов и способов парирования угроз безопасности при принятии решения позволит в значительной степени сократить расходы на создание системы защиты и поддержание процесса ее функционирования.

Принцип адекватности - применяемые решения должны быть дифференцированы в зависимости от вероятности возникновения угроз безопасности, прогнозируемого ущерба от ее реализации, степени конфиденциальности информации и ее стоимости.

Принцип системного подхода - заключается во внесении комплексных мер по защите информации на стадии проектирования ЗИС, включая организационные и инженерно-технические мероприятия. Важность этого принципа состоит в том, что оснащение средствами защиты изначально незащищенной ИС является более дорогостоящим, чем оснащение средствами защиты проектируемой ИС.

Принцип комплексности - в ЗИС должен быть предусмотрен комплекс мер и механизмов защиты - организационных, физических, технических, программно-технических.

Принцип непрерывности защиты - функционирование системы защиты не должно быть периодическим. Защитные мероприятия должны проводиться непрерывно и в объеме предусмотренном политикой безопасности.

Принцип адаптивности - система защиты должна строиться с учетом возможного изменения конфигурации ИС, числа пользователей, степени конфиденциальности и ценности информации. Введение новых элементов ИС не должно приводить к снижению достигнутого уровня защищенности.

Принцип доказательности - При создании системы защиты необходимо пользоваться существующими формальными моделями безопасных систем для доказательства эффективности защиты к атакам некоторых типов, входящих в рамки разработанных формальных моделей. Другим аспектом этого принципа является логическая привязка логического и физического рабочих мести друг к другу, а также применение специальных аппаратно-программных средств идентификации, аутентификации и подтверждения подлинности информации (например ЭЦП). К этому же принципу можно отнести необходимость использования сертифицированных СЗИ и сертифицирования ЗИС в целом.

Концептуальность подхода к решению задачи защиты информации в ИС предусматривает ее решение на основе единой концепции (совокупности научно обоснованных решений, необходимых и достаточных для оптимальной организации защиты информации в ИС).

Обеспечение информационной безопасности КС является непрерывным процессом, целенаправленно проводимым на всех этапах ее жизненного цикла с комплексным применением всех имеющихся методов и средств.

Существующие методы и средства защиты информации можно подразделить на четыре основные группы:

• методы и средства организационно-правовой защиты информации;
• методы и средства инженерно-технической защиты информации;
• криптографические методы и средства защиты информации;
• программно-аппаратные методы и средства защиты информации.

Без этих методов невозможно построить целостную комплексную ЗИС.

Перечисленные выше меры по обеспечению безопасности ЗИС могут рассматриваться как последовательность барьеров на пути потенциального нарушителя, стремящегося преодолеть систему защиты. Соответственно этим барьерам выделяются следующие рубежи защиты.

Первый рубеж защиты, встающий на пути человека, пытающегося совершить НСД к информации, является чисто правовым. Нарушитель несет ответственность перед законом. Правовые нормы предусматривают определенную ответственность за компьютерные преступления. С учетом такого рубежа становится понятным, что требуется соблюдение юридических норм при передаче и обработки информации. К правовым мерам защиты информации относятся действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией ограниченного использования (доступа) и ответственность за их нарушение. Это является существенным фактором сдерживания для потенциальных нарушителей.

Второй рубеж защиты образуют морально-этические меры. Этический момент в соблюдении требований защиты имеет весьма большое значение. К морально-этическим мерам относится создание таких традиций норм поведения и нравственности, которые способствуют соблюдению правил уважения к чужой информации и нарушение которых приравнивается к несоблюдению правил поведения в обществе. Эти нормы большей частью не являются обязательными и их несоблюдение не карается штрафными санкциями, но их несоблюдение ведет к падению престижа человека, группы лиц или организации в целом. Моральные нормы бывают как неписаными так и оформленными в некий свод правил поведения.

Третьим рубежом защиты являются административные меры, которые относятся к организационным мерам и регламентируют

- Процессы функционирования ЗИС
- Использования ресурсов
- Деятельность персонала
- Порядок взаимодействия пользователей с системой

Данные меры направлены на то, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Административные меры включают:

- Разработку правил обработки информации в ЗИС
- Совокупность действий при проектировании и оборудовании вычислительных центров и других объектов ЗИС (учет стихийных угроз и охрана помещений и т.п.)
- Совокупность действий при подборе и подготовке персонала (проверка новых сотрудников, ознакомление их с порядком работы с конфиденциальной информацией, ответственностью за нарушение правил ее обработки и т.п.)
- Организацию надежного пропускного режима
- Организацию учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией
- Распределение реквизитов разграничения доступа (паролей и информации авторизации и т.п.)
- Организацию скрытого контроля за работой пользователей и персонала ЗИС
- Совокупность действий при проектировании, разработке, ремонте и модификации оборудования и программного обеспечения (сертификация используемых технических и

программных средств, строгое санкционирование, рассмотрение и утверждение всех изменений, проверка, на удовлетворение требованиям защиты, документальная фиксация всех изменений и т.п.)

До тех пор пока не будут реализованы действенные меры административной защиты остальные меры не будут эффективны.

Четвертый рубеж защиты определяется применением физических мер защиты, к которым относятся разного рода механические, электро- и электронно-механические устройства или сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам ЗИС и защищаемой информации.

Пятый рубеж защиты определяется применением аппаратно-программных средств защиты - электронным устройствам и программам, которые реализуют самостоятельно или в комплексе с другими средствами следующие способы защиты:

- Идентификацию (распознавание) и аутентификацию (поверка подлинности) субъектов (пользователей, процессов) ЗИС
- Разграничение доступа к ресурсам ЗИС
- Контроль целостности данных.
- Обеспечение конфиденциальности данных
- Регистрацию и анализ событий, происходящих в ЗИС
- Резервирование ресурсов и компонентов ЗИС Большинство из этих способов защиты реализуется с использованием криптографических методов.

Одними из основных понятий теории защиты информации являются понятия «безопасность информации» и «защищенные ИС». **Безопасность (защищенность) информации в ИС** - это такое состояние всех компонент информационной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне.

Информационные системы, в которых обеспечивается безопасность информации, называются защищенными.

Безопасность информации в ИС (информационная безопасность) является одним из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы.

Информационная безопасность достигается проведением руководством соответствующего уровня **политики информационной безопасности**. Основным документом, на основе которого проводится политика информационной безопасности, является **программа информационной безопасности**. Этот документ разрабатывается и принимается как официальный руководящий документ высшими органами управления государством, ведомством, организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в ИС. В программах информационной безопасности содержатся также общие требования и принципы построения систем защиты информации в ИС.

Под **системой защиты информации в ИС** понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности.

Контрольные вопросы:

1 Назовите основные принципы организации защиты?
2 Проанализируйте механизмы и свойства защиты информации.
3 Перечислите рубежи защиты?
4 Что составляет основу политики безопасности?

2.3 . Современные компьютерные угрозы и методы борьбы с ними

Цель: изучить существующие компьютерные угрозы

План:

Информационные угрозы. Компьютерные вирусы и вредоносные программные средства. Методы взлома компьютерных систем. Противодействие информационным угрозам

Теоретический материал:

Одним из важнейших аспектов проблемы обеспечения безопасности компьютерных систем является определение, анализ и классификация возможных угрозы безопасности.

Под угрозой безопасности вычислительной системы понимаются воздействия на систему, которые прямо или косвенно могут нанести ущерб ее безопасности. Разработчики требований безопасности и средств защиты выделяют три вида угроз: угрозы нарушения конфиденциальности обрабатываемой информации, угрозы нарушения целостности обрабатываемой информации и угрозы нарушения работоспособности системы (отказа в обслуживании).

Угрозы конфиденциальности направлены на разглашение секретной информации, т. е. информация становится известной лицу, которое не должно иметь к ней доступ. Иногда для обозначения этого явления используется понятие «несанкционированный доступ» (НСД), особенно популярное у отечественных специалистов. Традиционно противостоянию угрозам этого типа уделялось максимальное внимание, и фактически подавляющее большинство исследований и разработок было сосредоточено именно в этой области, так как она непосредственно относится к задаче охраны государственных и военных секретов.

Угрозы целостности представляют собой любое искажение или изменение неуполномоченным на это действие лицом хранящейся в вычислительной системе или передаваемой информации. Целостность информации может быть нарушена как злоумышленником, так и в результате объективных воздействий со стороны среды эксплуатации системы. Наиболее актуальна эта угроза для систем передачи информации — компьютерных сетей и систем телекоммуникаций.

Угрозы нарушения работоспособности (отказ в обслуживании) направлены на создание ситуаций, когда в результате преднамеренных действий снижается работоспособность вычислительной системы, либо ее ресурсы становятся недоступными.

В общем случае программное обеспечение любой универсальной компьютерной системы состоит из трех основных компонентов: операционной системы, сетевого программного обеспечения (СПО) и системы управления базами данных (СУБД). Поэтому все попытки взлома защиты компьютерных систем можно разделить на три группы:

- атаки на уровне операционной системы;
- атаки на уровне сетевого программного обеспечения;
- атаки на уровне систем управления базами данных.

Атаки на уровне систем управления базами данных

Защита СУБД является одной из самых простых задач. Это связано с тем, что СУБД имеют строго определенную внутреннюю структуру, и операции над элементами СУБД заданы довольно четко. Есть четыре основных действия — поиск, вставка, удаление и замена элемента. Другие операции являются вспомогательными и применяются достаточно редко. Наличие строгой структуры и четко определенных операций упрощает решение задачи защиты СУБД. В большинстве случаев хакеры предпочитают взламывать защиту компьютерной системы на уровне операционной системы и получать доступ к файлам СУБД с помощью средств операционной системы. Однако в случае, если используется СУБД, не имеющая достаточно надежных защитных механизмов, или плохо протестированная версия СУБД, содержащая ошибки, или если при определении политики безопасности администратором СУБД были допущены ошибки, то становится вполне вероятным преодоление хакером защиты, реализуемой на уровне СУБД.

Кроме того, имеются два специфических сценария атаки на СУБД, для защиты от которых требуется применять специальные методы. В первом случае результаты арифметических операций над числовыми полями СУБД округляются в меньшую сторону, а разница суммируется в некоторой другой записи СУБД (как правило, эта запись содержит личный счет хакера в банке, а округляемые числовые поля относятся к счетам других клиентов банка). Во втором случае хакер получает доступ к полям записей СУБД, для которых доступной является только статистическая информация. Идея хакерской атаки на

СУБД — так хитро сформулировать запрос, чтобы множество записей, для которого собирается статистика, состояло только из одной записи.

Атаки на уровне операционной системы

Защищать операционную систему, в отличие от СУБД, гораздо сложнее. Дело в том, что внутренняя структура современных операционных систем чрезвычайно сложна, и поэтому соблюдение адекватной политики безопасности является значительно более трудной задачей.

Успех реализации того или иного алгоритма хакерской атаки на практике в значительной степени зависит от архитектуры и конфигурации конкретной операционной системы, являющейся объектом этой атаки. Однако имеются атаки, которым может быть подвергнута практически любая операционная система:

- кража пароля;
- подглядывание за пользователем, когда тот вводит пароль, дающий право на работу с операционной системой (даже если во время ввода пароль не высвечивается на экране дисплея, хакер может легко у шип, пароль, просто следя за перемещением пальцев пользователя по клавиатуре);
- получение пароля из файла, в котором этот пароль был сохранен пользователем, не желающим затруднять себя вводом пароля при подключении к сети (как правило, такой пароль хранится в файле в незашифрованном виде);
- поиск пароля, который пользователи, чтобы не забыть, записывают па календарях, в записных книжках или на оборотной стороне компьютерных клавиатур (особенно часто подобная ситуация встречается, если администраторы заставляют пользователей применять трудно запоминаемые пароли);
- кража внешнего носителя парольной информации (дискеты или электронного ключа, на которых хранится пароль пользователя, предназначенный для входа в операционную систему);
- полный перебор всех возможных вариантов пароля;
- подбор пароля по частоте встречаемости символов и биграмм, с помощью словарей наиболее часто применяемых паролей, с привлечением знаний о конкретном пользователе — его имени, фамилии, номера телефона, даты рождения и т. д., с использованием сведений о существовании эквивалентных паролей, при этом из каждого класса опробуется всего один пароль, что может значительно сократить время перебора;
- сканирование жестких дисков компьютера (хакер последовательно пытается обратиться к каждому файлу, хранимому на жестких дисках компьютерной системы; если объем дискового пространства достаточно велик, можно быть вполне уверенным, что при описании доступа к файлам и каталогам администратор допустил хотя бы одну ошибку, в результате чего все такие каталоги и файлы будут прочитаны хакером; для сокрытия следов хакер может организовать эту атаку под чужим именем: например, под именем пользователя, пароль которого известен хакеру);
- сборка "мусора" (если средства операционной системы позволяют восстанавливать ранее удаленные объекты, хакер может воспользоваться этой возможностью, чтобы получить доступ к объектам, удаленным другими пользователями: например, просмотрев содержимое их "мусорных" корзин);
- превышение полномочий (используя ошибки в программном обеспечении или в администрировании операционной системы, хакер получает полномочия, превышающие полномочия, предоставленные ему согласно действующей политике безопасности);
- запуск программы от имени пользователя, имеющего необходимые полномочия, или в качестве системной программы (драйвера, сервиса, демона и т. д.);
- подмена динамически загружаемой библиотеки, используемой системными программами, или изменение переменных среды, описывающих путь к таким библиотекам;
- модификация кода или данных подсистемы защиты самой операционной системы;
- отказ в обслуживании (целью этой атаки является частичный или полный вывод из строя операционной системы);
- захват ресурсов (хакерская программа производит захват всех имеющихся в операционной системе ресурсов, а затем входит в бесконечный цикл);
- бомбардировка запросами (хакерская программа постоянно направляет операционной системе запросы, реакция на которые требует привлечения значительных ресурсов компьютера);
- использование ошибок в программном обеспечении или администрировании.

Если в программном обеспечении компьютерной системы нет ошибок и ее администратор строго соблюдает политику безопасности, рекомендованную разработчиками операционной системы, то атаки всех перечисленных пики, малоэффективны. Дополнительные меры, которые должны быть предприняты для повышения уровня безопасности, в значительной степени зависят от конкретной операционной системы, под управлением которой работаем данная компьютерная система. Тем не менее, приходится признать, что вне зависимости от предпринятых мер полностью устранить угрозу взлома компьютерной системы на уровне операционной системы невозможно. Поэтому политика обеспечения безопасности должна проводиться так, чтобы, даже преодолев защиту, создаваемую средствами операционной системы, хакер не смог нанести серьезного ущерба.

Атаки на уровне сетевого программного обеспечения

СПО является наиболее уязвимым, потому что канал связи, по которому передаются сообщения, чаше всего не защищен, и всякий, кто может иметь доступ к этому каналу, соответственно, может перехватывать сообщения и отправлять свои собственные. Поэтому на уровне СПО возможны следующие хакерские атаки:

- прослушивание сегмента локальной сети (в пределах одного и того же сегмента локальной сети любой подключенный к нему компьютер в состоянии принимать сообщения, адресованные другим компьютерам сегмента, а следовательно, если компьютер хакера подсоединен к некоторому сегменту локальной сети, то ему становится доступен весь информационный обмен между компьютерами этого сегмента);
- перехват сообщений на маршрутизаторе (если хакер имеет привилегированный доступ к сетевому маршрутизатору, то он получает возможность перехватывать все сообщения, проходящие через этот маршрутизатор, и хотя тотальный перехват невозможен из-за слишком большого объема, чрезвычайно привлекательным для хакера является выборочный перехват сообщений, содержащих пароли пользователей и их электронную почту);
- создание ложного маршрутизатора (путем отправки в сеть сообщений специального вида хакер добивается, чтобы его компьютер стал маршрутизатором сети, после чего получает доступ ко всем проходящим через него сообщениям);
- навязывание сообщений (отправляя в сеть сообщения с ложным обратным сетевым адресом, хакер переключает на свой компьютер уже установленные сетевые соединения и в результате получает права пользователей, чьи соединения обманным путем были переключены на компьютер хакера);
- отказ в обслуживании (хакер отправляет в сеть сообщения специальною вида, после чего одна или несколько компьютерных систем, подключенных к сети, полностью или частично выходят из строя).

Поскольку хакерские атаки на уровне СПО спровоцированы открытостью сетевых соединений, разумно предположить, что дли отражения этих атак необходимо максимально защитить каналы связи и тем самым затруднить обмен информацией по сети для тех, кто не является легальным пользователем. Ниже перечислены некоторые способы такой защиты:

- максимальное ограничение размеров компьютерной сети (чем больше сеть, тем труднее ее защитить);
- изоляция сети от внешнего мира (по возможности следует ограничивать физический доступ к компьютерной сети извне, чтобы уменьшить вероятность несанкционированного подключения хакера);
- шифрование сетевых сообщений (тем самым можно устранить угрозу перехвата сообщений, правда, за счет снижения производительности СПО и роста накладных расходов);
- электронная цифровая подпись сетевых сообщений (если все сообщения, передаваемые по компьютерной сети, снабжаются электронной цифровой подписью, и при этом неподписанные сообщения игнорируются, то можно забыть про угрозу навязывания сообщений и про большинство угроз, связанных с отказом в обслуживании);
- использование брандмауэров (брандмауэр является вспомогательным средством защиты, применяемым только в том случае, если компьютерную сеть нельзя изолировать от других сетей, поскольку брандмауэр довольно часто не способен отличить потенциально опасное сетевое сообщение от совершенно безвредного, и в результате типичной является ситуация, когда брандмауэр не только не защищает сеть от хакерских атак, но и даже препятствует ее нормальному функционированию).

На пресс-конференции «Вирусные итоги 2005 года», проведенной 24.01.2006 «Лабораторией Касперского», Евгений Касперский так охарактеризовал текущую ситуацию с распространением вредоносных программ: «Раньше было плохо, сейчас стало совсем плохо. Десять лет назад вирусы писали для удовольствия, а сегодня этим занимаются, чтобы заработать деньги»[7].

Противодействие информационным угрозам

Перечисленные выше методы хакерской атаки на компьютерную систему являются наиболее типичными и описаны в общей форме. Самые распространенные из этих методов будут рассмотрены ниже более подробно, поскольку их применение в конкретных случаях имеет свои особенности, которые требуют применения дополнительных защитных мер. А пока для обобщенной модели взлома компьютерных систем можно сформулировать универсальные правила, которых следует придерживаться, чтобы свести риск к минимуму.

- Не отставайте от хакеров: будьте всегда в курсе последних разработок из области компьютерной безопасности. Оформите подписку на несколько специализированных журналов, в которых подробно освещаются вопросы зашиты компьютерных систем от взлома. Регулярно просматривал материалы, помещаемые на хакерских серверах Internet (например. astalavista.box.sk).
- Руководствуйтесь принципом разумной достаточности: не стремитесь построить абсолютно надежную защиту. Ведь чем мощнее зашита, тем больше ресурсов компьютерной системы она потребляет и тем труднее использовать ее.
- Храните в секрете информацию о принципах действия защитных механизмов компьютерной системы. Чем меньше хакеру известно об этих принципах, тем труднее будет для него организовать успешную атаку.
- Постарайтесь максимально ограничить размеры защищаемой компьютерной сети и без крайней необходимости не допускайте ее подключения к Internet.
- Перед тем как вложить денежные средства в покупку нового программного обеспечения, поищите информацию о нем, имеющуюся на хакерских серверах Internet.
- Размещайте серверы в охраняемых помещениях. Не подключайте к ним клавиатуру и дисплеи, чтобы доступ к этим серверам осуществлялся только через сеть.
- Абсолютно все сообщения, передаваемые по незащищенным каналам связи, должны шифроваться и снабжаться цифровой подписью.
- Если защищаемая компьютерная сеть имеет соединение с незащищенной сетью, то все сообщения, отправляемые в эту сеть или принимаемые из нее, должны проходить через брандмауэр, а также шифроваться и снабжаться цифровой подписью.
- Не пренебрегайте возможностями, которые предоставляет аудит. Интервал между сеансами просмотра журнала аудита не должен превышать одних суток.
- Если окажется, что количество событий, помешенных в журнал аудита, необычайно велико, изучите внимательно все новые записи. поскольку не исключено, что компьютерная система подверглась атаке хакера, который пытается замести следы своего нападения, зафиксированные в журнале аудита.
- Регулярно производите проверку целостности программного обеспечения компьютерной системы. Проверяйте ее на наличие программных закладок.
- Регистрируйте все изменения политики безопасности в обычном бумажном журнале. Регулярно сверяйте политику безопасности с зарегистрированной в этом журнале. Это поможет обнаружить присутствие программной закладки, если она была внедрена хакером в компьютерную систему.
- Пользуйтесь защищенными операционными системами.
- Создайте несколько ловушек для хакеров (например, заведите на диске файл с заманчивым именем, прочитать который невозможно с помощью обычных средств, и если будет зафиксировано успешное обращение к этому файлу, значит в защищаемую компьютерную систему была внедрена программная закладка).
- Регулярно тестируйте компьютерную систему с помощью специальных программ, предназначенных для определения степени ее защищенности от хакерских атак.

Цель защиты систем обработки информации — противодействие угрозам безопасности. Следовательно, безопасная или защищенная система — это система, обладающая средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Контрольные вопросы:

1 Как классифицируются угрозы безопасности информации?
2 Какими могут быть атаки на уровне систем управления базами данных?
3 Каким атакам может быть подвергнута любая операционная система?
4 Почему сетевое программное обеспечение наиболее уязвимо?
5 Основные типы компьютерных вирусов.
7 Действие программного вируса (этапы).
8 Средства антивирусной защиты.
9 Перечислите основные методы противодействия угрозам безопасности?

2.4. Анализ программной и аппаратной платформы ИС

Цель: Изучение архитектуру ИС

План:

Архитектура электронных систем обработки данных. Архитектура программного обеспечения. Системные и прикладные средства обработки данных. Аппаратные и программные средства информационной защиты.

Теоретический материал:

Информационная система **(ИС)** — организационно-техническая система, реализующая информационные технологии и включающая аппаратное, программное и другие виды обеспечения, а также соответствующий персонал.

Под информационной системой можно также понимать автоматизированную систему, предназначенную для организации, хранения, пополнения, поддержки и предоставления пользователям информации в соответствии с их запросами.

Целью любой информационной системы, независимо от области ее применения, программного и аппаратного обеспечения, является предоставление полной, достоверной и своевременной информации.

Информационные системы можно разделить на две основные группы: системы информационного обеспечения и системы, имеющие самостоятельное целевое назначение и область применения.

Системы (или подсистемы) информационного обеспечения входят в состав любой ИС. Они — важнейшие компоненты интенсивно развиваемых в настоящее время систем интегральной автоматизации производственных систем, систем автоматизированного проектирования (САПР), автоматизированных систем научных исследований и др.

К числу ИС самостоятельного значения относятся информационно-поисковые (ИПС), информационно-справочные (ИСС) и информационно-управляющие системы. Информационно-поисковые и информационно-справочные системы предназначены для хранения и представления пользователю информации (данных, фактографических записей, текстов, документов и т.п.) в соответствии с некоторыми формально задаваемыми характеристиками.

Для ИПС и ИСС характерны два этапа функционирования:

- сбор и хранение информации;
- поиск и выдача информации пользователю.

Движение информации в таких системах осуществляется по замкнутому контуру от источника к потребителю. При этом ИПС или ИСС выступает лишь как средство ускорения поиска необходимых данных.

В зависимости от режима организации поиска ИПС и ИСС могут быть разделены на документальные, библиографические, библиотечные, фактографические.

Основой для изучения теории ИС являются исходные положения теории информационных процессов (ИП). Под ИП в технике понимается совокупность взаимосвязанных и взаимообусловленных

процессов выявления, анализа, ввода и отбора информации, ее передачи и обработки, хранения, поиска, выдачи и принятия решений и т.д.

Кроме того, ИС характеризуют:

- наличие прямых, обратных, многоканальных и разветвленных связей, а также процессов управления;
- сложность, понимаемая как принципиальная невозможность в полной мере, без дополнительных условий и ограничений, иметь адекватное формализованное описание;
- обилие разнообразных составляющих информационного процесса, распределенных в пространстве, непрерывно сменяющих друг друга во времени.

Информация — сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (их свойствах, характеристиках) в некоторой предметной области, используемые (необходимые) для оптимизации принимаемых решений в процессе управления данными объектами. Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов и т.п.) на носителях различных типов.

Обработка информации в ИС — любая совокупность операций (прием, сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием технических средств ИС.

Специфичным для ИС является понятие структуры, которое раскрывает схему связей и взаимодействия между элементами.

Физическая структура ИС — это схема связей физических элементов, таких, как технические средства, аппаратура узлов, собственно узлы, вычислительная техника, устанавливаемая в них. К основным компонентам физической структуры можно отнести узлы, каналы и линии связи.

Логическая структура ИС определяет принципы установления связей, алгоритмы организации процессов и управления ими, логику функционирования программных средств. В общем виде она определяет соединение и взаимодействие двух принципиально различных по назначению и функциям составных частей архитектуры ИС: множества автономных информационных подсистем (узлов) и множества средств их связи и взаимодействия (физических средств соединений).

Обобщенная геометрическая модель физической структуры ИС определяет *топологическую структуру* ИС.

Более конкретный состав аппаратно-программных средств и схема их связей называются также ***конфигурацией*** **ИС**.

Под ***архитектурой ИС*** будем понимать согласованность всевозможных структур ИС. Так, при некоторой логической структуре, соответствующей принятой архитектуре ИС, может быть построено множество физических структур, влияющих на свойства и возможности системы. В свою очередь, логическая структура ИС в достаточной мере определяет свойства архитектуры ИС в целом.

Информационный узел — это техническая или организационно-техническая система определенной сложности, осуществляющая те или иные заданные процессы (например, обработка и накопление поступающей информации, распределение по каналам и др.).

Узлы, в которых информация выходит за пределы системы или поступает в систему, называют конечными пунктами. Здесь устанавливаются технические средства, называемые терминалами (“абонентский” пункт).

Внутренние сетевые узлы — это обычно транзитные или в общем случае коммуникационные связные узлы. Соединение отдельных информационных узлов осуществляется с помощью различных каналов связи (проводных, беспроводных, комбинированных).

Группы людей или отдельные лица, пользующиеся услугами ИС называют **пользователями.**

ИС можно разделить на системы больших масштабов (глобальные), средних (региональные или зональные) и малых (местные или локальные). Малые локальные системы могут объединяться, образуя ассоциации сетей. Таким образом создаются системы более крупного масштаба, в частности региональные, а при дальнейшем объединении и глобальные ИС.

В зависимости от уровня развития архитектуры можно выделить:

коммуникационные системы, т.е. такие, в которых применяемые средства рассчитаны на обеспечение связи и осуществление обмена информацией между территориально разделенными пользователями и терминалами;

информационно-вычислительные системы (ИВС), предоставляющие по запросам отдельных пользова-телей и систем те или иные информационные, вычислительные ресурсы и услуги.

Структура ИС и принципы ее функционирования

Основой современных ИС, как правило, являются территориально распределенные компьютерные системы (вычислительные сети) интенсивно взаимодействующие. Основу аппаратных (технических) средств таких систем составляют ЭВМ (группы ЭВМ), периферийные, вспомогательные устройства и средства связи, сопрягаемые с ЭВМ. Состав программных средств определяется возможностями ЭВМ и характером задач, решаемых при обработке информации.

Основными особенностями распределенных ИС являются:

- территориальная удаленность компонентов системы друг от друга и интенсивный обмен информацией между ними;
- широкий спектр используемых информационных технологий;
- интеграция данных различного назначения, принадлежащих разным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в удаленных узлах сети;
- абстрагирование пользователей и владельцев данных от физических структур и места размещения данных;
- использование режимов распределенной обработки данных;
- участие в процессе функционирования ИС большого количества пользователей и персонала различных категорий;
- одновременный доступ к ресурсам ИС большого числа пользователей (субъектов) различных категорий;
- высокая степень разнородности используемых средств вычислительной техники и связи, а также их программного обеспечения;
- отсутствие специальной аппаратной поддержки средств защиты в большинстве типов технических средств, широко используемых в ИС.

Системное и прикладное программное обеспечение

Программное обеспечение ПК можно разделить на три основных части:

1) операционная система;
2) сервисные программы (утилиты);
3) прикладные программы.

Операционная система — это совокупность программных средств, обеспечивающая выполнение двух главных задач:

- поддержку работы всех программ, обеспечение их взаимодействия с аппаратурой;
- предоставление пользователям возможности общего управления ЭВМ.

В рамках первой задачи ОС обеспечивает взаимодействие программ с внешними устройствами и друг с другом, распределение ОП, выявление событий, возникающих в процессе работы и соответствующую реакцию на них. Общее управление машиной осуществляется пользователем на основе командного языка ОС, с помощью которого могут осуществляться такие операции, как разметка дисков, копирование файлов, запуск программ, установка режимов работы внешних устройств и др.

Наиболее распространены следующие ОС: MS DOS фирмы MicrosoftCorp., PC DOS фирмы IBM, Windows, а также ОС UNIX.

ОС запускается при включении ПК. ОС состоит из следующих частей:

- базовая система ввода/вывода (BIOS);
- загрузчик ОС. Как уже отмечалось, загрузчик ОС, находящийся в загрузочной записи диска, — это короткая программа, которая загружает в память модули ОС (на дискете), либо выбирает логический диск на ЖД, с которого выполняется за грузка модулей ОС;

- дисковые файлы IO.SYS и MS DOS.SYS (либо IBM BIO.COM и IBM DOS.COM). Загружаются в память и остаются в ней постоянно. Файл IO.SYS представляет собой дополнение к BIOS. Файл MSDOS.COM реализует основные высокоуровневые услуги DOS;
- командный процессор DOS. Обрабатывает команды, вводимые пользователем. Находится в дисковом файле COMMAND.COM на диске, с которого загружается ОС;
- внешние команды DOS. Это программы, поставляемые вместе с ОС в виде отдельных файлов. Выполняют действия обслуживающего характера (форматирование дискет, проверку дисков и др.);
- драйверы устройств. Это специальные программы, дополняющие систему ввода/вывода DOS и обеспечивающие обслуживание новых устройств или нестандартное использование имеющихся. Драйверы загружаются в память при загрузке ОС, их имена указываются в специальном файле CONFIG.SYS.

Следует отметить основные преимущества распределенных ИС по сравнению с другими типами вычислительных структур.

1. **Надежность**. Наличие множества распределенных компонентов, расположенных в различных местах делает ИС невосприимчивой к локальным сбоям, когда один из компонентов отказывает или становится недоступным для связи с другими.
2. **Эффективность**. Многофункциональные элементы размещаются в местах наиболее частого использования и обеспечивают более быстрый доступ к данным, сокращая время отклика и стоимость связи.
3. **Гибкость**. Можно постепенно увеличить вычислительную мощность благодаря объединению нужного числа вычислительных систем малой и средней мощности.

Программно-аппаратные меры, то есть меры, направленные на контроль компьютерных сущностей - оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности.

Центральным для программно- аппаратного уровня является понятие сервиса безопасности. В число таких сервисов входят:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

Эти сервисы должны функционировать в открытой сетевой среде с разнородными компонентами, то есть быть устойчивыми к соответствующим угрозам, а их применение должно быть удобным для пользователей и администраторов. Например, современные средства идентификации/аутентификации должны быть устойчивыми к пассивному и активному прослушиванию сети и поддерживать концепцию единого входа в сеть.

Протоколирование и аудит должны быть всепроникающими и многоуровневыми, с фильтрацией данных при переходе на более высокий уровень. Это необходимое условие управляемости. Желательно применение средств активного аудита, однако нужно осознавать ограниченность их возможностей и рассматривать эти средства как один из рубежей эшелонированной обороны, причем не самый надежный. Следует конфигурировать их таким образом, чтобы минимизировать число ложных тревог и не совершать опасных действий при автоматическом реагировании.

Все, что связано к криптографией, сложно не столько с технической, сколько с юридической точки зрения; для шифрования это верно вдвойне. Данный сервис является инфраструктурным, его реализации должны присутствовать на всех аппаратно-программных платформах и удовлетворять

жестким требованиям не только к безопасности, но и к производительности. Пока же единственным доступным выходом является применение свободно распространяемого ПО.

Надежный контроль целостности также базируется на криптографических методах с аналогичными проблемами и методами их решения. Возможно, принятие Закона об электронной цифровой подписи изменит ситуацию к лучшему, будет расширен спектр реализаций. К счастью, к статической целостности есть и некриптографические подходы, основанные на использовании запоминающих устройств, данные на которых доступны только для чтения. Если в системе разделить статическую и динамическую составляющие и поместить первую в ПЗУ или на компакт-диск, можно в корне пресечь угрозы целостности. Разумно, например, записывать регистрационную информацию на устройства с однократной записью; тогда злоумышленник не сможет "замести следы".

Экранирование - идейно очень богатый сервис безопасности. Его реализации - это не только межсетевые экраны, но и ограничивающие интерфейсы, и виртуальные локальные сети. Экран инкапсулирует защищаемый объект и контролирует его внешнее представление. Современные межсетевые экраны достигли очень высокого уровня защищенности, удобства использования и администрирования; в сетевой среде они являются первым и весьма мощным рубежом обороны. Целесообразно применение всех видов МЭ - от персонального до внешнего корпоративного, а контролю подлежат действия как внешних, так и внутренних пользователей.

Анализ защищенности - это инструмент поддержки безопасности жизненного цикла. С активным аудитом его роднит эвристичность, необходимость практически непрерывного обновления базы знаний и роль не самого надежного, но необходимого защитного рубежа, на котором можно расположить свободно распространяемый продукт.

Обеспечение отказоустойчивости и безопасного восстановления - аспекты высокой доступности. При их реализации на первый план выходят архитектурные вопросы, в первую очередь - внесение в конфигурацию (как аппаратную, так и программную) определенной избыточности, с учетом возможных угроз и соответствующих зон поражения. Безопасное восстановление - действительно последний рубеж, требующий особого внимания, тщательности при проектировании, реализации и сопровождении.

Туннелирование - скромный, но необходимый элемент в списке сервисов безопасности. Он важен не столько сам по себе, сколько в комбинации с шифрованием и экранированием для реализации виртуальных частных сетей.

Управление - это инфраструктурный сервис. Безопасная система должна быть управляемой. Всегда должна быть возможность узнать, что на самом деле происходит в ИС (а в идеале - и получить прогноз развития ситуации). Возможно, наиболее практичным решением для большинства организаций является использование какого-либо свободно распространяемого каркаса с постепенным "навешиванием" на него собственных функций.

Контрольные вопросы:

1 Дайте понятие объекта защиты информации.
2. Что относят к информационным процессам?
3. Что понимают под информационной системой?
4. Что называют информационными ресурсами?
5 Примеры комплексов программно-аппаратных средств и преимущества использования**.**

2.5. Модели безопасности информационных систем

Цель: Изучить основные виды политик безопасности и их основные положения.

План:

Формальные модели. Модели безопасности и политика безопасности. Критерии и классы защищенности средств ВТ и АИС. Стандарты по оценке защищенных систем

Теоретический материал:

Одними из важнейших понятий в теории обеспечения безопасности информации являются политика безопасности и, модель безопасности. Политика безопасности определяет множество требований по обеспечению безопасности информации, которые должны быть выполнены в конкретной реализации системы обеспечения безопасности информации. В свою очередь, любая реализация системы

обеспечения безопасности информации основывается на определенной модели безопасности. Под моделью безопасности понимается формальное математическое описание механизмов защиты информации в терминах «сущность», «субъект», «объект», «ресурс», «операция», «доступ», «уровень безопасности», «степень доверия», не привязанное, однако, к конкретной реализации системы обеспечения безопасности информации.

Политика безопасности –

1) интегральная (качественная) характеристика, описывающая свойства защищенности информации в КС в заданном пространстве угроз.
2) совокупность норм и правил, регламентирующих процесс обработки информации, обеспечивающих защиту от определенного множества угроз и составляющих необходимое условие безопасности системы.

Модель безопасности - формальное (математическое, алгоритмическое, схемотехническое и т.п.) выражение политики безопасности.

Модель безопасности служит для:
-выбора и обоснования базовых принципов архитектуры, определяющих механизмы реализации средств защиты информации
-подтверждения свойств (защищенности) разрабатываемой системы путем формального доказательства соблюдения политики (требований, условий, критериев) безопасности.
-составления формальной спецификации политики безопасности разрабатываемой системы
Модель безопасности включает:
-модель компьютерной системы
-критерии, принципы или целевые функции защищенности и угроз
-формализованные правила, алгоритмы, механизмы безопасного функционирования КС
Большинство моделей безопасности основывается на *субъектно-объектной модели КС*:
Компьютерная система представляется конечным множеством элементов, разделяемых на два подмножества:
-множество **субъектов – *S***
-множество **объектов – *O***

Субъект - активная сущность КС, которая может изменять состояние системы путем порождения процессов над объектами и субъектами, в т.ч., порождая новые объекты и инициализируя порождение новых субъектов
Объект - пассивная сущность КС, процессы над которой могут в определенных случаях быть источником порождения новых субъектов

Отличия пользователя от субъекта
Пользователь - лицо, внешний фактор, управляющий одним или несколькими субъектами, воспринимающий объекты и получающий информацию о состоянии КС через субъекты, которыми он управляет
Свойства субъектов:
1) угрозы информации исходят от субъектов, изменяющих состояние объектов в КС
2) субъекты-инициаторы могут порождать через объекты-источники новые объекты
3) субъекты могут порождать потоки (передачу) информации от одних объектов к другим

Множество объектов можно разделить на два непересекающихся подмножества: объекты-источники и объекты-данные.
Определение 1. Объект O_i называется ***источником*** для субъекта S_m если существует субъект S_j , в результате воздействия которого на объект O_i возникает субъект S_m. S_j – *активизирующий* субъект для субъекта S_m, S_m – *порожденный* субъект.
Create(S_j , O_i)→ S_m

Функционирование КС – ***нестационарный*** процесс, но в субъектно-объектной модели КС действует ***дискретное время*** t_i. В любой момент t_i множество субъектов, объектов-источников, объектов-данных ***фиксировано.***

Определение 2. Объект O_i в момент времени t_k ассоциирован с субъектом S_m , если состояние объекта повлияло на состояние субъекта в момент времени t_{k+1}. (т.е. субъект S_m использует информацию, содержащуюся в объекте O_i).

Можно выделить множество ***функционально-ассоциированных объектов*** и множество ***ассоциированных объектов-данных*** с субъектом S_m в момент времени t_k.

Следствие 2.1. В момент порождения объект-источник является ассоциированным с порожденным субъектом.

Определение 3. ***Потоком*** информации между объектом O_i и объектом O_j называется называется произвольная операция над объектом O_j, осуществляемая субъектом S_m и зависящая от объекта O_i.

Stream(Sm , Oi) → Oj

Свойства потока информации:

1) потоки информации возмоны только между объектами (а не между субъектом и объектом)
2) объекты могут быть как ассоциированы, так и не ассоциированы с субъектом S_m
3) операция порождения потока локализована в субъекте и сопровождается изменением состояния ассоциированных (отображающих субъект) объектов
4) операция Stream может осуществляться в виде "чтения", "записи", "уничтожения", "создания" объекта

Определение 4. ***Доступом*** субъекта к объекту O_j называется порождение субъектом S_m потока информации между объектом O_j и некоторым другим объектом (не обязательно объект O_j ассоциирован с субъектом S_m).

Будем считать, что все множество потоков информации P (объединение всех потоков во все t_k) разбито на два подмножества:

потоки P_L , характеризующие ***легальный доступ,*** и потоки P_N, характеризующие ***несанкционированный доступ.***

Определение 5. ***Правила разграничения доступа***, задаваемые политикой безопасности - формально описанные потоки, принадлежащие множеству P_L .

Аксиомы защищенности компьютерных систем:

Аксиома 1. В любой момент времени любой субъект, объект и процесс должны быть ***персонифицированы*** и ***аутентифицированы***

Аксиома 2. В защищенной системе должна присутствовать активная компонента (субъект, процесс или объект-источник), контролирующая процессы субъектов над объектами – монитор безопасности.

Аксиома 3. Для осуществления процессов субъектов над объектами необходима (должна существовать) дополнительная информация (и наличие содержащего ее объекта), помимо информации, идентифицирующей субъекты и объекты.

Аксиома 4. Все вопросы безопасности информации в КС описываются доступами субъектов к объектам

Аксиома 5. Субъекты в КС могут быть порождены только активной компонентой (субъектами же) из объектов

Аксиома 6. Система безопасна, если субъекты не имеют возможности нарушать (обходить) правила и ограничения

Политики безопасности компьютерных систем:

1) **Политика *избирательного* (*дискреционного*) доступа** - множество $\boldsymbol{P_L}$ задается явным образом внешним по отношению к системе фактором в виде указания дискретного набора троек "субъект-поток(операция)-объект"

2) **Политика *полномочного* (*мандатного*) доступа** - множество $\boldsymbol{P_L}$ задается неявным образом через предоставление субъектам неких полномочий (допуска, мандата) порождать определенные потоки над объектами с определенными характеристиками конфиденциальности (метками, грифами секретности)

3) **Политика *тематического* (*типизованного*) доступа** - множество $\boldsymbol{P_L}$ задается неявным образом через разделение всех субъектов и объектов на фиксированное количество тематических групп с запретом потоков информации между субъектами и объектами, принадлежащими разным группам

Критерии и классы защищенности средств вычислительной техники и автоматизированных систем.

Появление материалов проекта международного стандарта ISO 15408 по Общим критериям оценки безопасности информационных технологий , принятом в 1999 году, является качественно новым этапом в развитии нормативной базы оценки безопасности ИТ. В нём наиболее полно представлены критерии для оценки механизмов безопасности программно-технического уровня.

При проведении работ по анализу защищенности АС, а также средств вычислительной техники (СВТ) "Общие критерии" целесообразно использовать в качестве основных критериев, позволяющих оценить уровень защищенности АС (СВТ) с точки зрения полноты реализованных в ней функций безопасности и надежности реализации этих функций.

Средства вычислительной техники (СВТ).

Согласно руководящему документу «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

Оценка класса защищенности СВТ (сертификация СВТ)

Оценка класса защищенности СВТ проводится в соответствии с Положением о сертификации средств и систем вычислительной техники и связи по требованиям защиты информации, Временным положением по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники и другими документами.

Автоматизированные системы.

Согласно руководящему документу «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Классификация автоматизированных систем и требования по защите информации» деление АС на соответствующие классы по условиям их

функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации. Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

Основными этапами классификации АС являются:

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД.

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

Требования по защите информации от НСД для АС

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

Стандарты по оценке защищенных систем: «Оранжевая книга» и «Критерии оценки безопасности информационных технологий».

Специалистам в области информационной безопасности почти невозможно обойтись без знаний соответствующих стандартов и спецификаций.

Стандарт - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг.

Выделяются две существенно отличающиеся друг от друга группы стандартов и спецификаций:

- оценочные стандарты, предназначенные для оценки и классификации информационных систем и средств защиты по требованиям безопасности;

- спецификации, регламентирующие различные аспекты реализации и использования средств и методов защиты.

Первым оценочным стандартом, получившим международное признание стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем, более известный под названием ***"Оранжевая книга"***.

В "Оранжевой книге" заложен понятийный базис информационной безопасности. Понятия*:* безопасная и доверенная системы, политика безопасности, уровень гарантированности, подотчетность, доверенная вычислительная база, монитор обращений, ядро *и* периметр безопасности, добровольное (дискреционное) и принудительное (мандатное) управление доступом, безопасность повторного использования объектов, принципы классификации по требованиям безопасности.

Стандарт **ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий" (*"Общие критерии"* (ОК)).**

ОК содержат два основных вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям (сервисам) безопасности и реализующим их механизмам;

- требования доверия, соответствующие пассивному аспекту; они предъявляются к технологии и процессу разработки и эксплуатации.

ОК способствуют формированию двух базовых видов нормативных документов - это профиль защиты и задание по безопасности.

Профиль защиты - типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса.

Задание по безопасности - совокупность требований к конкретной разработке.

Профили защиты, в отличие от заданий по безопасности, носят универсальный характер: они характеризуют определенный класс изделий вне зависимости от специфики условий применения. Именно официально принятые профили защиты образуют используемую на практике нормативную базу в области информационной безопасности.

Контрольные вопросы:

1 Политика безопасности и процедуры ее выполнения
2 Модели безопасности и их применение.
3 Охарактеризуйте целевую направленность Общих Критериев.
4 Требования и концепции Общих Критериев.

2.6. Криптографические системы защиты информации

Цель: Дать понятие и необходимости криптографии, а также шифрования.

План:

Основные понятия, задачи и методы криптографии. Модель криптографической системы. Шифры перестановки. Шифры замены. Гаммирование. Генераторы случайных чисел. Классификация современных криптосистем. Симметричные криптосистемы

Теоретический материал:

Шифрование - криптографическое преобразование конечной совокупности данных (текста, сообщения, файла, блока) в форме ограниченного по времени процесса, при котором:

--преобразованию подвергается каждый символ (единичный элемент) данных;

--результат преобразования каждого символа определяется шифром и местоположением символа в исходной совокупности данных

Шифр -совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования

Ключ -конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма

Криптография -научная дисциплина и отрасль производственно-технологической деятельности по разработке методов криптографического преобразования информации, созданию и эксплуатации криптографических систем

Криптоанализ -совокупность методов, приемов и средств по раскрытию (взлому) по зашифрованным данным (тексту, сообщению, файлу) их открытой формы (содержания, смысла) без знания и владения соответствующими шифрами или кодами

Криптостойкость -характеристика шифра, определяющая его стойкость к взлому (обычно определяется периодом времени или объемом вычислительных затрат, необходимых для осуществления успешной криптоаналитической атаки)

Системы подстановок. Наиболее простой метод шифрования. Символы шифруемого текста заменяются другими символами, взятыми из одного(моноалфавитная подстановка) или нескольких(полиалфавитрая подстановка) алфавитов.

Наиболее простой метод - прямая замена символов шифруемого сообщения другими буквами того же самого или другого алфавита.

Однако такой шифр имеет низкую стойкость. Зашифрованный текст имеет те же самые статистические характеристики, что и исходный, поэтому зная стандартные частоты появления символов в том языке, на котором написано сообщение, и подбирая по частотам появления символы в зашифрованном сообщении, можно восстановить таблицу замены. Для этого требуется лишь достаточно длинный зашифрованный текст, для того, чтобы получить достоверные оценки частот появления символов. Поэтому простую замену используют лишь в том случае, когда шифруемое сообщение достаточно коротко!

Стойкость метода равна 20 - 30, трудоемкость определяется поиском символа в таблице замены. Для снижения трудоемкости при шифровании таблица замены сортируется по шифруемым символам, а для расшифровки формируется таблица дешифрования, которая получается из таблицы замены сортировкой по заменяющим символам. Полиалфавитные подстановки повышают стойкость шифра.

Полиалфавитная одноконтурная обыкновенная подстановка. Для замены символов используются несколько алфавитов, причем смена алфавитов проводится последовательно и циклически: первый символ заменяется на соответствующий символ первого алфавита, второй - из второго алфавита, и т.д. пока не будут исчерпаны все алфавиты. После этого использование алфавитов повторяется.

Рассмотрим шифрование с помощью таблицы Вижинера - квадратной матрицы с n¤ элементами, где n - число символов используемого алфавита. В первой строке матрицы содержится исходный алфавит, каждая следующая строка получается из предыдущей циклическим сдвигом влево на один символ.

Для шифрования необходимо задать ключ - слово с неповторяющимися символами. Таблицу замены получают следующим образом: строку "Символы шифруемого текста" формируют из первой строки матрицы Вижинера, а строки из раздела "Заменяющие символы" образуются из строк матрицы Вижинера, первые символы которых совпадают с символами ключевого слова.

При шифровании и дешифровании нет необходимости держать в памяти всю матрицу Вижинера, поскольку используя свойства циклического сдвига, можно легко вычислить любую строку матрицы по ее номеру и первой строке.

При шифровании символы из первой строки заменяются символами остальных строк по правилу

a(1,i)->a(k,i), где k - номер используемой для шифрования строки.

Используя свойства циклического сдвига влево элементы k-ой строки можно выразить через элементы первой строки

$$a(k,i)=\begin{cases} a(1,i+k-1), & \text{если } i<=n-k+1 \\ a(1,i-n+k-1), & \text{если } i>n-k+1 \end{cases} \quad (1.1)$$

При дешифровании производится обратная замена a(k,i) -> a(1,i), поэтому необходимо решить следующую задачу: пусть очередной дешифруемый символ в тексте - a(1,j) и для дешифрования используется k-я строка матрицы Вижинера. Необходимо найти в k-ой строке номер элемента, равного a(1,j). Очевидно,

$$a(1,j)=\begin{cases} a(k,j-k+1), & \text{если } j>=k \\ a(k,n-k+j+1), & \text{если } j<k \end{cases}$$

Таким образом при дешифровании по k-ой строке матрицы Вижинера символа из зашифрованного текста, значение которого равно a(1,j), проводится обратная подстановка

$$a(1,j) \rightarrow \begin{cases} a(1,j-k+1), & \text{если } j>=k \\ a(1,n-k+j+1), & \text{если } j<k \end{cases}$$

Стойкость метода равна стойкости метода подстановки, умноженное на количество используемых при шифровании алфавитов, т.е. на длину ключевого слова и равна 20*L, где L - длина ключевого слова. С целью повышения стойкости шифрования предлагаются следующие усовершенствования таблицы Вижинера:

- Во всех, кроме первой строках таблицы буквы располагаются в произвольном порядке.
- В качестве ключа используются случайные последовательности чисел, которые задают номера используемых строк матрицы Вижинера для шифрования.

Частным случаем полиалфавитной подстановки является монофоническая замена, в котором количество и состав алфавитов выбирается таким образом, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми. При таком положении затрудняется криптоанализ зашифрованного текста с помощью его статистической обработки.

Выравнивание частот появления символов достигается за счет того, что для часто встречающихся символов исходного текста предусматривается большее число заменяющих символов, чем для редко встречающихся. Шифрование проводится также, как при простой замене с той лишь разницей, что после шифрования каждого знака соответствующий ему столбец алфавитов циклически сдвигается вверх на одну позицию.

Таким образом столбцы алфавитов как бы образуют независимые друг от друга кольца, поворачиваемые вверх на один знак каждый раз после шифрования соответствующего знака исходного алгоритма. Полиалфавитная многоконтурная замена заключается в том, что для шифрования используются несколько наборов (контуров) алфавитов, используемых циклически, причем каждый контур в общем случае имеет свой индивидуальный период применения. Частным случаем многоконтурной полиалфавитной подстановки является замена по таблице Вижинера, если для шифрования используется несколько ключей, каждый из которых имеет свой период применения. Общая модель шифрования подстановкой может быть представлена в следующем виде:

Математическое описание шифра, пусть X и У. g: $X \rightarrow Y$ – взаимнооднозначное отображение X в У. Шифр замены действует так: x1,x2,…, xn преобразуется в шифрованный текст f(x1)f(x2)...f(xn).

Выражение, который устанавливающее связь между алфавитами A и B имеет вид: $F(y[i])=(F(x[i])+h) \bmod K$

Где К- количество знаков в алфавитах, h – постоянная величина сдвига

y[i] – знак алфавита шифротекста Y, x[i]) – знак исходного алфавита X
Чтобы увеличить надежность, используется – перемешенного алфавита(рандомизирование).

Стойкость простой полиалфавитной подстановки оценивается величиной 20*n, где n - число различных алфавитов, используемых для замены. Усложнение полиалфавитной подстановки существенно повышает ее стойкость. Монофоническая подстановка может быть весьма стойкой (и даже теоретически нераскрываемой), однако строго монофоническую подстановку реализовать на практике трудно, а любые отклонения от монофоничности снижают реальную стойкость шифра.

Шифрование простой перестановкой Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Выбирается размер блока шифрования n столбцов и m строк. Выбирается ключевая последовательность, которая формируется из натурального ряда 1,2,...,n случайной перестановкой. Шифруемый текст записывается последовательными строками под числами ключевой последовательности, образуя блок шифрования размером n*m.

Предположим, что требуется зашифровать сообщение: "НА ПЕРВОМ КУРСЕ ТЯЖЕЛО УЧИТЬСЯ ТОЛЬКО ПЕРВЫЕ ЧЕТЫРЕ ГОДА ДЕКАНАТ".

Н	А	_	П	Е	Р	В	О
М	_	К	У	Р	С	Е	_
Т	Я	Ж	Е	Л	О	_	У
Ч	И	Т	Ь	С	Я	_	Т
О	Л	Ь	К	О	_	П	Е
Р	В	Ы	Е	_	Ч	Е	Т
Ы	Р	Е	_	Г	О	Д	А
_	Д	Е	К	А	Н	А	Т

В таблице символом "_" обозначен пробел. В результате преобразований получится шифровка:
НМТЧРЫ_А_ЯИЛВРД_КЖТЬЫЕЕПУЕЬКЕ_КЕРЛСО_ГАРСОЯ_ЧОНВЕ__ПЕДАО_УТЕТАТ

Ключом в данном случае является размер матрица, порядок записи открытого текста и считывания шифрограммы. Естественно, что ключ может быть другим. Например, запись открытого текста по строкам может производиться в таком порядке: 48127653,а считывание криптограммы может происходить по столбцам в следующем порядке: 81357642.

При усложнении перестановки по таблицам для повышения стойкости шифра в таблицу перестановки вводятся неиспользуемые клетки таблицы. Количество и расположение неиспользуемых элементов является дополнительным ключом шифрования.

При шифровании текста в неиспользуемые элементы не заносятся символы текста и в зашифрованный текст из них не записываются никакие символы - они просто пропускаются. При дешифровании символы зашифрованного текста также не заносятся в неиспользуемые элементы.

Для дальнейшего увеличения криптостойкости шифра можно в процессе шифрования менять ключи, размеры таблицы перестановки, количество и расположение неиспользуемых элементов по некоторому алгоритму, причем этот алгоритм становится дополнительным ключом шифра.

Высокую стойкость шифрования можно обеспечить усложнением перестановок по маршрутам типа гамильтоновских. При этом для записи символов шифруемого текста

используются вершины некоторого гиперкуба, а знаки зашифрованного текста считываются по маршрутам Гамильтона, причем используются несколько различных маршрутов. Для примера рассмотрим шифрование по маршрутам Гамильтона при n=3.
Номера вершин куба определяют последовательность его заполнения символами шифруемого текста при формировании блока. В общем случае n-мерный гиперкуб имеет 2№ вершин.

Последовательность перестановок символов в шифруемом блоке для первой схемы 5-6-2-1-3-4-8-7, а для второй 5-1-3-4-2-6-8-7. Аналогично можно получить последовательность перестановок для других маршрутов: 5-7-3-1-2-6-8-4, 5-6-8-7-3-1-2-4, 5-1-2-4-3-7-8-6 и т.д.

Размерность гиперкуба, количество вид выбираемых маршрутов Гамильтона составляют секретный ключ метода.

Стойкость простой перестановки однозначно определяется размерами используемой матрицы перестановки. Например, при использовании матрицы 16*16 число возможных перестановок достигает 1.4E26. Такое число вариантов невозможно перебрать даже с использованием ЭВМ. Стойкость усложненных перестановок еще выше. Однако следует иметь ввиду, что при шифровании перестановкой полностью сохраняются вероятностные характеристики исходного текста, что облегчает криптоанализ.

Шифрование методом гаммирования

Суть метода состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, называемой гаммой. Иногда такой метод представляют как наложение гаммы на исходный текст, поэтому он получил название "гаммирование".

Наложение гаммы можно осуществить несколькими способами, например по формуле $t_ш = t_0$ XOR $t_г$, где $t_ш, t_0, t_г$ - ASCII коды соответственно зашифрованного символа, исходного символа и гаммы. XOR - побитовая операция "исключающее или". Расшифровка текста проводится по той же формуле: $t_0 = t_ш$XOR $t_г$

Последовательность гаммы удобно формировать с помощью датчика псевдослучайных чисел (ПСЧ).

Стойкость гаммирования однозначно определяется длиной периода гаммы. При использовании современных ПСЧ реальным становится использование бесконечной гаммы, что приводит к бесконечной теоретической стойкости зашифрованного текста.

Шифрование с помощью аналитических преобразований

Достаточно надежное закрытие информации может обеспечить использование при шифровании некоторых аналитических преобразований. Например, можно использовать методы алгебры матриц - в частности умножение матрицы на вектор.

В качестве ключа задается квадратная матрица ||a|| размера n*n, исходный текст разбивается на блоки длиной n символов; каждый блок рассматривается как n-мерный вектор, а процесс шифрования блока заключается в получении нового n-мерного вектора (зашифрованного блока) как результат умножения матрицы ||a|| на исходный вектор.

Расшифровка текста происходит с помощью такого же преобразования, только с помощью матрицы, обратной ||a||. Очевидно, что ключевая матрица ||a|| должна быть невырожденной.

Комбинированные методы шифрования

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов шифрования, т.е. последовательное шифрование исходного текста с помощью двух или более методов.

Стойкость комбинированного шифрования S не ниже произведения стойкостей используемых способов $S >= S_1*S_2*...*S_k$

Если какой-либо способ шифрования при независимом применении может обеспечить стойкость не ниже S, то комбинировать его с другими способами целесообразно лишь при

выполнении условия $R>R_1+R_2+ ... +R_k$, где R_i - трудоемкость i-го способа, используемого при комбинированном шифровании, R - трудоемкость того способа, который обеспечивает стойкость не ниже S.

На практике наибольшее распространение получили следующие комбинации: Подстановка + гаммирование ; перестановка + гаммирование; гаммирование + гаммирование; подстановка + перестановка

Алгоритм ГОСТ-28147-89.

ГОСТ является 64-битовым алгоритмом с 256-битовым ключом. ГОСТ также использует дополнительный ключ, который рассматривается ниже. В процессе работы алгоритма на 32 этапах последовательно выполняется простой алгоритм шифрования.

Для шифрования текст сначала разбивается на левую половину *L* и правую половину *R*. На этапе *i* используется подключ K_I . На этапе *i* алгоритма ГОСТ выполняется следующее:

$$L_i = R_{i-1},$$
$$R_i = L_{i-1} + F(R_{i-1}, k_i).$$

Этап ГОСТ показан(рис-1) Функция f проста. Сначала правая половина и i-ый подключ складываются по модулю 2^{32}. Результат разбивается на восемь 4-битовых кусочков, каждый из которых поступает на вход своего S-блока. ГОСТ использует восемь различных S-блоков, первые 4 бита попадают в первый S-блок, вторые 4 бита - во второй S-блок, и т.д. Каждый S-блок представляет собой перестановку чисел от 0 до 15. Например, S-блок может выглядеть как: 7, 10, 2, 4, 15, 9, 0, 3, 6, 12, 5, 13, 1, 8, 11

В этом случае, если на входе S-блока 0, то на выходе 7. Если на входе 1, на выходе 10, и т.д. Все восемь S-блоков различны, они фактически являются дополнительным ключевым материалом. S-блоки должны храниться в секрете.

Выходы всех восьми S-блоков объединяются в 32-битовое слово, затем все слово циклически сдвигается влево на 11 битов. Наконец результат объединяется с помощью XOR с левой половиной, и получается новая правая половина, а правая половина становится новой левой половиной. Выполните это 32 раза, и все в порядке.

Генерация подключей проста. 256-битовый ключ разбивается на восемь 32-битовых блоков: *k1, k2, . . .k8.* На каждом этапе используется свой подключ, как показано в таблице - 1. Дешифрирование выполняется также, как и шифрование, но инвертируется порядок подключей κ_i.

Стандарт ГОСТ не определяет способ генерации S-блоков, говорится только, что блоки должны быть предоставлены каким-то образом. Это породило домыслы о том, что советский производитель может поставлять хорошие S-блоки "хорошим" организациям и плохие S-блоки тем организациям, которых производитель собирается надуть. Это вполне может быть так, но неофициальные переговоры с российским производителем микросхем ГОСТ выявили другую альтернативу. Производитель создает перестановки S-блока самостоятельно с помощью генератора случайных чисел.

Таблица-1. Использование подключей на различных этапах ГОСТ

Этап	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Подключ	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Этап	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Подключ	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8

Совсем недавно стал известным набор S-блоков, используемых в приложениях Центрального Банка РФ. Эти S-блоки также используются в однонаправленной хэш-функции ГОСТ. Они перечислены в таблице -2.

Таблица-2. S – блоки ГОСТ

00	01	02:	03	04	05	06	07	08	09	10	11	12	13	14	15

S-блок 1:

4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3

S-блок 2:

14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9

S-блок 3:

5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11

S-блок 4:

7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3

S-блок 5:

6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2

S-блок 6:

4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14

S-блок 7:

13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12

S-блок 8:

1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

Алгоритм предусматривает четыре режима работы: простая замена, гаммирование, гаммирование с обратной связью, выработка имитовставки[15].

В любом случае для шифрования данных используется 256-битовый ключ K, который представляется в виде восьми 32-битовых подключей K_i:

$$K = K_7K_6K_5K_4K_3K_2K_1K_0.$$

Расшифрование выполняется по тому же ключу, что и шифрование, но этот процесс является инверсией процесса шифрования данных.

Контрольные вопросы

1 Что представляет собой криптографический алгоритм?
2 Объясните метод шифрования заменой?
3 Объясните метод шифрования одноконтурной обыкновенной подстановки?
4 Объясните метод шифрования простой перестановки?
5 Объясните шифрование методом гаммирования?
6 Какова стойкость комбинированные методы шифрования?

2.7. Асимметричные криптографические системы

Цель: Дать понятие и необходимости криптографии, а также шифрования.

План:

Основы асимметричных систем. Криптосистема RSA. Криптосистема Эль-Гамаля. Функции хэширования. Системы электронной цифровой подписи. Криптографические протоколы

Теоретический материал:

Симметричные криптосистемы, рассмотренные нами в предыдущих главах, несмотря на множество преимуществ, обладают одним серьезным недостатком, о котором Вы, наверное, еще не задумывались. Связан он с ситуацией, когда общение между собой производят не три-четыре человека, а сотни и тысячи людей. В этом случае для каждой пары, переписывающейся между собой, необходимо создавать свой секретный симметричный ключ. Это в итоге приводит к существованию в системе из N пользователей $N^2/2$ ключей. А это уже очень "приличное" число. Кроме того, при нарушении конфиденциальности какой-

либо рабочей станции злоумышленник получает доступ ко всем ключам этого пользователя и может отправлять, якобы от его имени, сообщения всем абонентам, с которыми "жертва" вела переписку.

Своеобразным решением этой проблемы явилось появление асимметричной криптографии. Эта область криптографии очень молода по сравнению с другими представителями. Первая схема, имевшая прикладную значимость, была предложена всего около 20 лет назад. Но за это время асимметричная криптография превратилась в одно из основных направлений криптологии, и используется в современном мире также часто, как и симметричные схемы.

Асимметричная криптография изначально задумана как средство передачи сообщений от одного объекта к другому (а не для конфиденциального хранения информации, которое обеспечивают только симметричные алгоритмы). Поэтому дальнейшее объяснение мы будем вести в терминах "отправитель" – лицо, шифрующее, а затем отправляющее информацию по незащищенному каналу и "получатель" – лицо, принимающее и восстанавливающее информацию в ее исходном виде. *Основная идея асимметричных криптоалгоритмов состоит в том, что для шифрования сообщения используется один ключ, а при дешифровании – другой.*

Кроме того, процедура шифрования выбрана так, что она необратима даже по известному ключу шифрования – это второе необходимое условие асимметричной криптографии. То есть, зная ключ шифрования и зашифрованный текст, невозможно восстановить исходное сообщение – прочесть его можно только с помощью второго ключа – ключа дешифрования. А раз так, то ключ шифрования для отправки писем какому-либо лицу можно вообще не скрывать – зная его все равно невозможно прочесть зашифрованное сообщение. *Поэтому, ключ шифрования называют в асимметричных системах "открытым ключом", а вот ключ дешифрования получателю сообщений необходимо держать в секрете – он называется "закрытым ключом".* Напрашивается вопрос : "Почему, зная открытый ключ, нельзя вычислить закрытый ключ ?" – это третье необходимое условие асимметричной криптографии – алгоритмы шифрования и дешифрования создаются так, чтобы зная открытый ключ, невозможно вычислить закрытый ключ.

В целом система переписки при использовании асимметричного шифрования выглядит следующим образом. Для каждого из N абонентов, ведущих переписку, выбрана своя пара ключей : "открытый" E_j и "закрытый" D_j, где j – номер абонента. Все открытые ключи известны всем пользователям сети, каждый закрытый ключ, наоборот, хранится только у того абонента, которому он принадлежит. Если абонент, скажем под номером 7, собирается передать информацию абоненту под номером 9, он шифрует данные ключом шифрования E_9 и отправляет ее абоненту 9. Несмотря на то, что все пользователи сети знают ключ E_9 и, возможно, имеют доступ к каналу, по которому идет зашифрованное послание, они не могут прочесть исходный текст, так как процедура шифрования необратима по открытому ключу. И только абонент №9, получив послание, производит над ним преобразование с помощью известного только ему ключа D_9 и восстанавливает текст послания. Заметьте, что если сообщение нужно отправить в противоположном направлении (от абонента 9 к абоненту 7), то нужно будет использовать уже другую пару ключей (для шифрования ключ E_7, а для дешифрования – ключ D_7).

Как мы видим, во-первых, в асимметричных системах количество существующих ключей связано с количеством абонентов линейно (в системе из N пользователей используются 2*N ключей), а не квадратично, как в симметричных системах. Во-вторых, при нарушении конфиденциальности k-ой рабочей станции злоумышленник узнает только ключ D_k : это позволяет ему читать все сообщения, приходящие абоненту k, но не позволяет выдавать себя за него при отправке писем.

Концепция криптографии с открытым ключом основана на т.н. однонаправленных (односторонних) функциях- функция $F : x \to y$, обладающая следующими свойствами:

1) существует полиномиальный алгоритм вычисления F(x)

2) не существует полиномиального алгоритма инвертирования функции F, т.е. нахождения x по известному y и виду F(x)В н.вр. не удалось построить или найти ни одной односторонней функцией, поэтому пока к классу односторонних функций относят те, для которых инвертирование представляет неразрешимую вычислительную преграду

Примеры односторонних функций:

•произведение двух очень больших простых чисел N=P*Q.

Обратная задача - разложение на множители большого целого числа практически неразрешима (по совр. оц. теории чисел при $N=2^{664}$ и P=Q треб-ся около 10^{23} оп.)

•модульная экспонента с фиксированным основанием A и модулем N - $f_{A,N}(x)=A^x(\mathrm{mod}\ N)$, где A, N и x - целые числа, 1£x £(N-1).

Алгоритм решения обратной задачи - по известным целым A, N и y найти такое целое число x, что $A^x(\mathrm{mod}\ N)=y$, на сегодняшний день не известен (подбором потребуется около 10^{26} оп.) На практике в асимметричных криптосистемах нашли применение однонаправленные функции с секретом К (с "потайным ходом")- функция $F_K : x \rightarrow y$, зависящая от параметра К и обладающая следующими свойствами:

1) при любом известном К существует полиномиальный алгоритм вычисления $F_K(x)$

2) при неизвестном К не существует полиномиального алгоритма инвертирования функции F, т.е. нахождения x по известному y и виду F(x)

3) при известном К существует полиномиальный алгоритм инвертирования $F_K(x)$

Асимметричная криптосистема шифрования данных RSA Р.Райвест (Rivest), А.Шамир (Shamir) и А.Адлеман (Adleman), 1978г.

Выбираются два очень больших простых числа P и Q примерно равной величины (не менее 200 цифр, чтобы $P*Q>2^{512}$)

Вычисляется N=P*Q Выбирается очень большое случайное число d, которое д.б. взаимно простым с числом (P-1)*(Q-1). Определяется (на основе расширенного алгоритма Евклида) такое число e, что (e*d) mod(P-1)(Q-1)=1 Открытым ключом $К_В$ объявляются числа e и N, которые направляются по открытому каналу пользователю A

Пользователь A разбивает текст сообщения на блоки из N последовательных цифр M_i, шифрует их по формуле $C_i=M_i^e(\mathrm{mod}\ N)$ и направляет B Секретным ключом k_B являются d (потайн.ход мод.exp) и пара чисел P и Q Пользователь B расшифровывает принятую криптограмму по формуле $M_i=C_i^d(\mathrm{mod}\ N)$

Цифровая подпись

Попытка использовать подпись в компьютерных файлах сопряжена с еще большими трудностями. Во-первых, любой файл может быть скопирован вместе с имеющейся в нем подписью. Во-вторых, после подписания в файл можно внести любые изменения, которые в принципе не поддаются обнаружению.

Криптографы придумали множество алгоритмов цифровой подписи. Все они основаны на криптосистемах с открытым ключом. При этом секретная информация используется для того, чтобы поставить подпись под документом, а общедоступная — чтобы проверить подлинность этой подписи. Поэтому часто процесс подписания документа называют шифрованием на тайном ключе, а процесс проверки подлинности подписи — расшифрованием на открытом ключе. Однако это справедливо только для одного алгоритма шифрования с открытым ключом — RSA, а подавляющее большинство остальных алгоритмов цифровой подписи совершенно непригодны для шифрования сообщений.

По этой причине в ходе дальнейшего изложения о процессах подписания документа и проверки подлинности подписи будет говориться без упоминания конкретных алгоритмов,

которые используются для этих целей. Подписание документа P при помощи тайного ключа K будет обозначаться $S_K(P)$, а проверка подлинности подписи с использованием соответствующего открытого ключа — $V_K(P)$.

Битовая строка, которая присоединяется к документу при его подписании (например, хэш-значение файла, зашифрованное на тайном ключе) будет именоваться цифровой подписью. И наконец, протокол, при помощи которого получатель сообщения убеждается в подлинности и целостности этого сообщения, будет называться аутентифнкационным протоколом.

Несколько подписей под одним документом. Каким образом Антон и Борис могут поставить свои цифровые подписи под одним и тем же документом? Если не задействовать однонаправленные хэш-функции, существуют 2 способа сделать это.

Первый заключается в создании двух идентичных копий документа, одну из которых подписывает Антон, а другую — Борис. Однако тогда придется хранить документ, длина которого в 2 раза превышает размер исходного документа, предназначенного для совместного подписания Антоном и Борисом.

Второй способ состоит в том, чтобы сначала документ подписал Антон, а затем подпись Антона заверил своей подписью Борис. Но в этом случае будет невозможно убедиться в подлинности подписи Антона, не проверив подпись Бориса.

Если использовать однонаправленную хэш-функцию, от перечисленных недостатков можно легко избавиться:

1. Антон подписывает хэш-значение документа.
2. Борис подписывает хэш-значение того же самого документа.
3. Борис отсылает свою подпись Антону.
4. Антон шлет документ вместе со своей подписью и подписью Бориса Владимиру.
5. Владимир проверяет подлинность подписей Антона и Бориса.

Неоспоримость. Вполне возможна ситуация, при которой Антон, подписав некоторый документ, впоследствии попытается ее оспорить — заявит о том, что подпись под документом поставил не он. Причиной может послужить, например. потеря Антоном своего тайного ключа в людном месте или намеренная его публикация Антоном в разделе частных объявлений популярной газеты. Эта ситуация называется отказ от обязательств.

Уменьшить ущерб отказа от обязательств помогает введение в подпись даты и времени, когда она была поставлена под документом. Конечно, ничего нельзя поделать в случае, если Антон заранее предпринял определенные действия для создания условий, при которых его подпись под документом должна быть признана недействительной. Но можно, по крайней мере, сделать так, чтобы эти действия не позволили Антону объявить поддельными все остальные его подписи, которые он ранее поставил под другими документами:

1. Антон подписывает документ.
2. Антон генерирует заголовок, в который помещает свои личные данные. присоединяет этот заголовок к подписанному им документу, еще раз подписывает итоговый документ и посылает его Дмитрию.
3. Дмитрий проверяет вторую подпись Антона, добавляет к его сообщению отметку о дате и времени получения этого сообщения, подписывает его. а затем отправляет Антону и Борису.
4. Борис проверяет подпись Дмитрия, персональные данные Антона и его подпись.
5. Антон знакомится с содержанием сообщения, присланного Дмитрием Если Антон обнаруживает в этом сообщении что-то подозрительное, он должен немедленно заявить об этом во всеуслышание.

Цифровая подпись и шифрование. Аналогии из повседневной жизни помогают лучше понять, как должны быть устроены криптографические протоколы, чтобы обеспечивать максимальную защиту от мошенников и злоумышленников. Возьмем, к примеру. обыкновенное письмо, приготовленное Антоном для отправки Борис) по почте. Антон всегда

подписывает свои письма Борису, прежде чем вкладывает их в конверты. А почему бы Антону не подписывать сами конверты? Да потому, что получив конверт с подписью Антона и обнаружив в нем неподписанное письмо, Борис не сможет убедиться в том, что подлинное письмо Антона не было подменено на пути следования от отправителя к адресату.

Антон может использовать разные ключи для зашифрования документа и для того, чтобы поставить под ним подпись. Это позволит ему при необходимости передать ключ шифрования правоохранительным органам, не компрометируя собственную подпись, а также по своему выбору отдать один из двух ключей на хранение доверенным третьим лицам, сохранив второй и тайне от посторонних.

Однако совместное использование шифрования и цифровой подписи таит в себе особую опасность, если для зашифрования и генерации цифровой подписи используется один и тот же криптографический алгоритм.

Цифровая подпись от Эль-Гамаля

1. Абоненты A и B знают C и случайное число $d = W^{-1} C \bmod M$ из интервала $r_1, r_2, \ldots, r_n$. A генерирует случайные числа $r_i \in \{0,1\}$ и $d = r_1 b_1 + r_2 b_2 + \ldots + r_n b_n$ из того же интервала. $m_i = r_{\pi(i)}$ нужно хранить в секрете, а $i = \overline{1, n}$, являющееся открытым ключом, должно быть взаимно простым с $\pi = \begin{pmatrix} 1 2 3 4 5 6 \\ 3 6 1 2 5 4 \end{pmatrix}$.

2. A вычисляет π и $C = m_1 a_1 + m_2 a_2 + \ldots + m_n a_n = 319 + 250 + 477 + 559 = 1605$, решает относительно S уравнение $d = W^{-1} C \bmod M = 136$ и передает B документ с подписью $136 = 12 r_1 + 17 r_2 + 33 r_3 + 74 r_4 + 157 r_5 + 316 r_6$.

3. Получатель проверяет подпись, контролируя тождество $r_1 = 1, r_2 = 1, r_3 = 1, r_4 = 1, r_5 = 0, r_6 = 0$.

Или другой вариант шифра — цифровая подпись.

1. Оба абонента знают:

$m_1 = r_3 = 1, m_2 = r_6 = 0, m_3 = r_1 = 1, m_4 = r_2 = 1, m_5 = r_5 = 0, m_6 = r_4 = 1$ — общедоступное большое простое число; g — примитивный элемент.

2. A имеет закрытый ключ X и открытый ключ $m = g^X \bmod P$. Чтобы подписаться, A вычисляет $Z = m^X \bmod P$

3. B выбирает случайное a и b из $(1, P)$, вычисляет $C = m^a g^b \bmod P$ и посылает его A.

4. A выбирает q из $(1, P)$ и отправляет к B $S_1 = C g^q \bmod P$ и a.

5. B посылает A a и b

6. A посылает B q, чтобы он мог воспользоваться m^X и восстановить S_1 и S_2. Если $S_1 \in C g^q \bmod P$ и $S_2 \in \left(g^X\right)^{b+q} \left(Z^a\right) \bmod P$, то подпись правильна.

Основное назначение шифра «цифровая подпись» — не столько шифрование/расшифровка данных, сколько подписание любого электронного документа или идентификация удаленных пользователей.

Развитие современных средств безбумажного документооборота, средств электронных платежей немыслимо без развития средств доказательства подлинности и целостности документа. Таким средством является электронно-цифровая подпись (ЭЦП), которая сохранила основные свойства обычной подписи.

На сегодняшний день придумано и реализовано не так много алгоритмов цифровой подписи:

- алгоритм подписи Ривеста-Шамира-Адельмана (RSA);
- алгоритм DSA, являющийся федеральным стандартом на цифровую подпись в США;
- алгоритм Эль-Гамаля, на котором построен "старый" российский стандарт на цифровую подпись ГОСТ Р 34.10-94.

Почему криптосистемы ненадежны. В настоящее время криптография успешно используется почти во всех информационных системах — от Internet до баз данных. Без нее обеспечить требуемую степень конфиденциальности в современном, до предела компьютеризированном мире уже не представляется возможным. Кроме того, с помощью криптографии предотвращаются попытки мошенничества в системах электронной коммерции и обеспечивается законность финансовых сделок. Со временем значение криптографии, по всей вероятности, возрастет. Для этого предположения имеются веские основания.

Однако с огорчением приходится признать, что подавляющее большинство криптографических систем не обеспечивает того высокого уровня зашиты, о котором с восторгом обычно говорится в их рекламе. Многие из них до сих пор не были взломаны по той простой причине, что пока не нашли широкого распространения. Как только эти системы начнут повсеместно применяться на практике, они, словно магнит, станут привлекать пристальное внимание злоумышленников, которых сегодня развелось великое множество. При этом удача и везение будут явно на стороне последних. Ведь для достижения своих целей им достаточно найти в защитных механизмах всего лишь одну брешь, а обороняющимся придется укреплять все без исключения уязвимые места.

Потайные ходы. Причины появления потайных ходов в криптографических системах довольно очевидны: их разработчики хотят иметь контроль над шифруемой в этих системах информацией и оставляют для себя возможность расшифровывать ее, не зная ключа пользователя. Средство, с помощью которых данная возможность реализуется на практике, и принято именовать потайным ходом. Иногда потайные ходы применяются для целей отладки, а после ее завершения разработчики в спешке просто забывают убрать их из конечного продукта.

Криптографические методы являются наиболее эффективными средствами защиты информации в АС, при передаче же по протяженным линиям связи они являются единственным реальным средством предотвращения несанкционированного доступа к ней. Метод шифрования характеризуется показателями надежности и трудоемкости.

Важнейшим показателем надежности криптографического закрытия информации является его стойкость - тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст. Таким образом стойкость шифра определяет допустимый объем информации, зашифровываемый при использовании одного ключа.

Трудоемкость метода шифрования определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста. Основные требования к криптографическому закрытию информации в АС:

- Сложность и стойкость криптогр. закрытия данных должны выбираться в зависимости от объема и степени секретности данных.
- Надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику становится известен метод шифрования.
- Метод закрытия, набор используемых ключей и механизм их распределения не должны быть слишком сложными.
- Выполнение процедур прямого и обратного преобразований должно быть формальным. Эти процедуры не должны зависеть от длины сообщений.
- Ошибки, возникающие в процессе преобразования не должны распространяться по системе. Вносимая процедурами защиты избыточность должна быть минимальной.

Контрольные вопросы

1 Что представляет собой криптографический алгоритм?
2 Какова стойкость комбинированные методы шифрования?
3 Почему криптосистемы ненадежны?
4 Объясните принцип шифра Ривеста — Шамира — Алдемана?
5 Для чего используется цифровая подпись?

2.8. Примеры практической реализации систем защиты и безопасности

Цель: Изучить вопросы, связанные с идентификацией и аутентификацией пользователей.

План:

Построение парольных систем. Особенности - применения криптографических методов. Способы реализации криптографической подсистемы. Особенности реализации систем с симметричными и несимметричными ключами. Способы реализации стеганографических систем

Теоретический материал:

Основой защиты от злонамеренных атак в компьютерной сети является система парольной защиты, которая имеется во всех современных операционных системах. В соответствии с установившейся практикой перед началом сеанса работы с операционной системой пользователь обязан зарегистрироваться, сообщив ей свое имя и пароль. Имя требуется операционной системе для идентификации пользователя, а пароль служит подтверждением правильности произведенной идентификации. Информация, введенная пользователем в диалоговом режиме, сравнивается с той, которая имеется в распоряжении операционной системы. Если проверка дает положительный результат, то пользователю становятся доступны все ресурсы операционной системы, связанные с его именем.

В настоящее время ни один злоумышленник не станет пытаться подобрать имя и пароль для входа в операционную систему, по очереди перебирая и вводя с клавиатуры все возможные варианты. Скорость такого подбора пароля будет чрезвычайно низкой, тем более что в операционных системах с хорошо продуманной парольной защитой количество подряд идущих повторных вводов конкретного пользовательского имени и соответствующего ему пароля всегда можно ограничить двумя-тремя. При этом если это число будет превышено, то вход в систему с использованием данного имени будет заблокирован в течение фиксированного периода времени или до вмешательства системного администратора(Как работает парольный взломщик. См. тема -3).

Метод парольной защиты и его модификации

Законность запроса пользователя определяется по паролю, представляющему собой, как правило, строку знаков. Метод паролей считается достаточно слабым, так как пароль

может стать объектом хищения, перехвата, перебора, угадывания. Однако простота метода стимулирует поиск путей его усиления.

Для повышения эффективности парольной защиты рекомендуется:

- выбирать пароль длиной более 6 символов, избегая распространенных, легко угадываемых слов, имен, дат и т.п.;
- использовать специальные символы;
- пароли, хранящиеся на сервере, шифровать при помощи односторонней функции;
- файл паролей размещать в особо защищаемой области ЗУ ЭВМ, закрытой для чтения пользователями;
- границы между смежными паролями маскируются;
- комментарии файла паролей следует хранить отдельно от файла;
- периодически менять пароли;
- предусмотреть возможность насильственной смены паролей со стороны системы через определенный промежуток времени;
- использовать несколько пользовательских паролей: например, собственно пароль, персональный идентификатор, пароль для блокировки/разблокировки аппаратуры при кратковременном отсутствии и т.п.

В качестве более сложных парольных методов используется случайная выборка символов пароля и одноразовое использование паролей. В первом случае пользователю (устройству) выделяется достаточно длинный пароль, причем каждый раз для опознавания используется часть пароля, выбираемая случайно. При одноразовом использовании пароля пользователю выделяется не один, а большое количество паролей, каждый из которых используется по списку или по случайной выборке один раз.

Расширением парольного метода является опознавание пользователя по сугубо индивидуальным характеристикам. Эти методы, как правило, требуют специального и достаточно сложного оборудования. Известны такие методы:

а) персональные: отпечатки пальцев; строение лица;

б) квазистатические: геометрия руки; особенность глаз; отпечатки ладоней; рисунок кровеносных сосудов;

в) квазидинамические: пульс; баллистокардиография; энцефалография;

г) динамические: голос; почерк; стилю печатания.

Широкое распространение получили средства опознавания атрибутного типа, изготовляемые в виде карточек. Карточка является носителем идентификационной информации, нанесенной механическим, оптическим или магнитным способом.

На смену магнитным карточкам приходят более устойчивые к подделке “интеллектуальные карточки” (ИК) (smartcard), содержащие электронные компоненты (микропроцессор, энергонезависимая память). Существует международный стандарт на ИК -ISO 7816. Устройство ИК позволяет многократную запись/чтение содержимого памяти. Карточку можно использовать для хранения:

- идентификационной информации;
- ключей шифрования и использования в качестве криптопроцессора;
- любой конфиденциальной информации.

Подсистема управления ключами

Подсистема управления СЗИ предназначена для управления ключами подсистемы криптографической защиты, а также контроля и диагностирования программно-аппаратных средств и обеспечения взаимодействия всех подсистем СЗИ.

Под управлением криптографическими ключами понимаются все действия, связанные с генерацией, распределением, вводом в действие, сменой, хранением, учетом и уничтожением ключей.

К функциям подсистемы управления ключами шифрования относятся:
-генерация, тестирование, учет и распределение ключей;
-контроль за хранением и уничтожением ключей;
- контроль за вводом в действие и сменой ключей;
-ведение базы данных открытых ключей (БД ОК) на центре распределения ключей (ЦРК);
- рассылка БД ОК пользователям;
- контроль за вводом в действие и сменой ключей цифровой подписи;
- контроль и диагностирование программно-аппаратных средств защиты.

Подсистема состоит из центра распределения ключей и программно-аппаратных средств, интегрированных в рабочие станции пользователей.
В СЗИ ИС управление ключами возлагается на центр распределения ключей. ЦРК осуществляет:
-централизованную генерацию симметричных шифрключей, их распределение и контроль за дальнейшим использованием;
-ведение и рассылку базы данных открытых ключей;
- контроль за использованием несимметричных ключей;
- ведение архивов открытых ключей цифровой подписи;
- участие в предварительной проверке спорных ситуаций, возникающих при использовании цифровой подписи;
- разработку мероприятий на случай компрометации ключей;
- гарантированное стирание ключевых данных на носителях по истечении срока действия ключей.

В качестве ключевой схемы целесообразно выбрать двухуровневую (главный ключ, формируемый на ЦРК, плюс сеансовый ключ, формируемый пользователем).

Ключи цифровой подписи рекомендуется формировать самим пользователям, чтобы не создавать проблему доверия к ЦРК. ЦРК осуществляет управление открытыми ключами цифровой подписи. При этом формируется база данных открытых ключей, которая рассылается всем пользователям ИС, применяющим цифровые подписи. ЦРК следит за обновлением базы, контролирует ввод в действие и срок действия ключей цифровой подписи, разрабатывает мероприятия на случай компрометации ключей.

Любая криптографическая система основана на использовании криптографических ключей. В симметричной криптосистеме отправитель и получатель сообщения используют один и тот же секретный ключ. Этот ключ должен быть неизвестен всем остальным и должен периодически обновляться одновременно у отправителя и получателя. Процесс распределения (рассылки) секретных ключей между участниками информационного обмена в симметричных криптосистемах имеет весьма сложный характер.

Асимметричная криптосистема предполагает использование двух ключей открытого и личного (секретного). Открытый ключ можно разглашать, а личный надо хранить в тайне. При обмене сообщениями необходимо пересылать только открытый ключ. Важным требованием является обеспечение подлинности отправителя сообщения. Это достигается путем взаимной аутентификации участников информационного обмена.

Протокол Kerberos

Протокол Kerberos обеспечивает распределение ключей симметричного шифрования и проверку подлинности пользователей, работающих в незащищенной сети. Реализация Kerberos – это программная система, построенная по архитектуре «клиент-сервер». Клиентская часть устанавливается на все компьютеры защищаемой сети, кроме тех, на которые устанавливаются компоненты сервера Kerberos. В роли клиентов Kerberos могут, в частности, выступать и сетевые серверы (файловые серверы, серверы печати и т.д.).

Серверная часть Kerberos называется центром распределения ключей (англ. Key

Distribution Center, сокр. KDC) и состоит из двух компонент:

- сервер аутентификации (англ. Authentication Server, сокр. AS);
- сервер выдачи разрешений (англ. Ticket Granting Server, сокр. TGS).

Каждому субъекту сети сервер Kerberos назначает разделяемый с ним ключ симметричного шифрования и поддерживает базу данных субъектов и их секретных ключей. Kerberos основывается на симметричной криптографии (реализован алгоритм DES, хотя возможно применение и других симметричных криптоалгоритмов). Kerberos разделяет отдельный секретный ключ с каждым субъектом сети. Знание такого секретного ключа равносильно доказательству подлинности субъекта сети.

Основной протокол Kerberos является, вариантом протокола аутентификации и распределения ключей Нидхема-Шредера. В основном протоколе Kerberos (версия 5) участвуют две взаимодействующие стороны A и B и доверенный сервер KS (Kerberos Server). Стороны A и B, каждая по отдельности, разделяют свой секретный ключ с сервером KS. Доверенный сервер KS выполняет роль центра распределения ключей ЦРК.

Область действия системы Kerberos распространяется на тот участок сети, все пользователи которого зарегистрированы под своими именами и паролями в базе данных Kerberos-сервера.

Что касается реализации протокола Kerberos в Windows, то надо отметить следующее.

1). Ключ пользователя генерируется на базе его пароля. Таким образом, при использовании слабых паролей эффект от надежной защиты процесса аутентификации будет сведен к нулю.

2). В роли Kerberos-серверов выступают контроллеры домена, на каждом из которых должна работать служба Kerberos Key Distribution Center (KDC). Роль хранилища информации о пользователях и паролях берет на себя служба каталога Active Directory. Ключ, который разделяют между собой сервер аутентификации и сервер выдачи разрешений формируется на основе пароля служебной учетной записи *krbtgt* – эта запись автоматически создается при организации домена и всегда заблокирована.

3). Microsoft в своих ОС использует расширение Kerberos для применения криптографии с открытым ключом. Это позволяет осуществлять регистрацию в домене и с помощью смарт-карт, хранящих ключевую информацию и цифровой сертификат пользователя.

4). Использование Kerberos требует синхронизации внутренних часов компьютеров, входящих в домен Windows.

Инфраструктура открытых ключей.

Как было рассмотрено в предыдущем разделе, использование протокола Kerberos позволяет провести аутентификацию и распределить ключи симметричного шифрования. Использование методов асимметричной криптографии сделало возможным безопасный обмен криптографическими ключами между отправителем и получателем без использования центров распределения ключей.

Но возникает другая проблема – как убедиться в том, что имеющийся у Вас открытый ключ другого абонента на самом деле принадлежит ему. Иными словами, возникает проблема аутентификации ключа. Без этого, на криптографический протокол может быть осуществлена атака типа «человек посередине» (man in the middle).

Идею данной атаки поясняет следующий пример. Абонент A (Алиса) хочет послать абоненту B (Боб) зашифрованное сообщение и берет его отрытый ключ из общедоступного справочника. Но, на самом деле, ранее нарушитель E (Ева) подменил в справочнике открытый ключ Боба своим открытым ключом. Теперь Ева может расшифровать те сообщения, которые Алиса формирует для Боба, ознакомиться с их содержимым, возможно, зашифровать их на настоящем ключе Боба и переслать ему (рисунок 3.

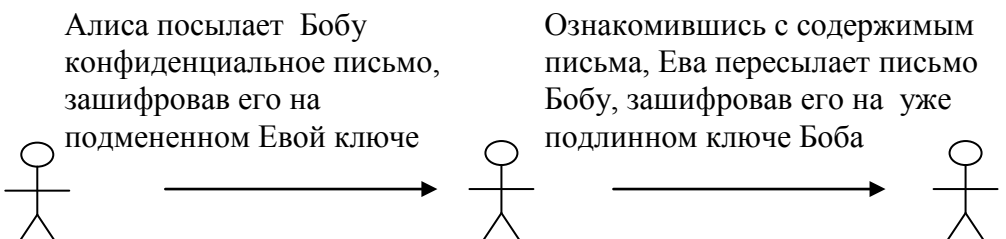


Рисунок 3 - Атака типа man-in-the-middle.

Избежать подобной атаки можно, подтвердив подлинность используемого ключа. Но Алиса и Боб лично никогда не встречались, и передать, например, дискету с ключом из рук в руки не могут. Поэтому, решение задачи подтверждения подлинности берет на себя третья доверенная сторона – некий арбитр, которому доверяют оба абонента. Заверяется ключ с помощью цифрового сертификата.

На самом деле, подобный способ применяется и вне компьютерных систем. Когда для подтверждения подлинности человека используется паспорт, то в роли третьей доверенной стороны выступает государство (от имени которого действовали в выдавшем паспорт отделе милиции).

Но вернемся к цифровым сертификатам. Для подтверждения подлинности открытых ключей создается инфраструктура открытых ключей (англ. Public Key Infrastructure, сокр. PKI). PKI представляет собой набор средств, мер и правил, предназначенных для управления ключами, политикой безопасности и обменом защищенными сообщениями.

Для простоты последующего изложения, будем представлять сеть в виде совокупности удостоверяющих центров (другое название – центр сертификации, от англ. Certification Authority, сокр. – CA) и пользователей. Центр сертификации – абонент, которому доверено право удостоверять своей подписью сертификаты, связывающие открытые ключи абонентов с их идентификационной информацией. Сами центры сертификации тоже получают сертификаты своих ключей у центров более высокого уровня.

Таким образом, центры сертификации и пользователи формируют древовидную иерархическую структуру (рисунок 4). В вершине этого дерева находится корневой центр сертификации, на рисунке – CA_1. Его особенность заключается в том, что он использует самоподписанный сертификат, т.е. сам заверяет свой ключ.

В приведенном примере, CA_1 заверяет электронной подписью сертификаты подчиненных центров сертификации CA_2 и CA_3, а те, в свою очередь, подписывают сертификаты пользователей и центров более низкого уровня.

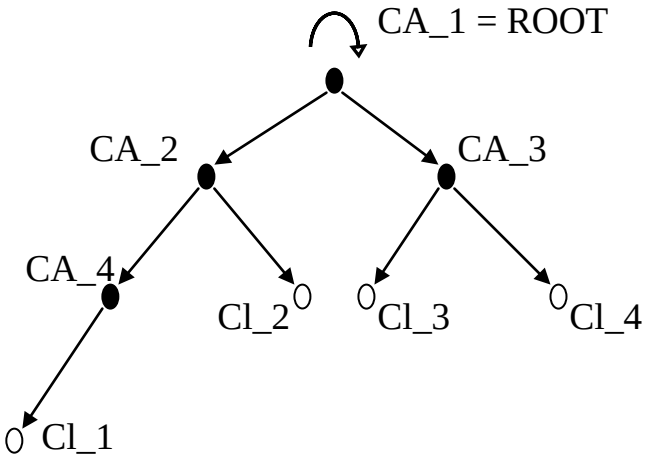


Рисунок -4. Иерархия центров сертификации и клиентов.

Наибольшее распространение получили цифровые сертификаты, формат которых определен стандартом X.509. Формат сертификата изображен на рисунок -5.

Номер версии содержит числовое значение, соответствующее номеру версии (для сертификата версии 1 равен 0 и т.д.). В первой версии X.509 не было уникальных номеров («ID Изготовителя», «ID Субъекта») и полей расширения. Во второй версии добавились указанные идентификаторы, в третьей – расширения.

Серийный номер – уникальный номер, присваиваемый каждому сертификату.

Алгоритм подписи – идентификатор алгоритма, используемого при подписании сертификата. Должен совпадать с полем *Алгоритм ЭЦП*.

Изготовитель – имя центра сертификации, выдавшего сертификат. Записывается в формате Relative Distinguished Name - RDN (варианты перевода названия – «относительное отдельное имя», «относительное характерное имя»). Данный формат используется в службах каталога, в частности, в протоколе LDAP.

При записи Relative Distinguished Name используются специальные ключевые слова:

CN (Common Name) – общее имя;

OU (Organization Unit) – организационная единица;

DC (Domain Component) – составная часть доменного имени.

Например, в сертификате Microsoft Windows Hardware Compatibility, который находится в хранилище сертификатов Windows'XP значение данного поля следующее:

CN = Microsoft Root Authority

OU = Microsoft Corporation

OU = Copyright (c) 1997 Microsoft Corp.

Как видно, указывается имя центра сертификации, компания, которой он принадлежит и т.д.

Субъект – имя владельца сертификата, представленное в том же формате RDN. Для указанного в предыдущем примере сертификата значения данного поля:

CN = Microsoft Windows Hardware Compatibility

OU = Microsoft Corporation

OU = Microsoft Windows Hardware Compatibility Intermediate CA

OU = Copyright (c) 1997 Microsoft Corp.

Период действия – описывает временной интервал, в течение которого центр сертификации гарантирует отслеживание статуса сертификата (сообщит абонентам сети о факте досрочного отзыва сертификата и т.д.). Период задается датами начала и окончания действия.

Открытый ключ – составное поле, содержащее идентификатор алгоритма, для которого предназначается данный открытый ключ, и собственно сам открытый ключ в виде набора битов.

ID Изготовителя и *ID Субъекта* содержат уникальные идентификаторы центра сертификации и пользователя (на случай совпадения имен различных CA или пользователей).

Расширения – дополнительный атрибут, связанный с субъектом, изготовителем или открытым ключом, и предназначенный для управления процессами сертификации. Более подробно он описан ниже.

Алгоритм электронной цифровой подписи (ЭЦП) – идентификатор алгоритма, используемый для подписи сертификата. Должен совпадать со значением поля *Алгоритм подписи*.

ЭЦП – само значение электронно-цифровой подписи для данного сертификата.

Расширения могут определять следующие дополнительные параметры:

- идентификатор пары открытый/секретный ключ центра сертификации (изготовителя), если центр имеет несколько различных ключей для подписи сертификатов;
- идентификатор конкретного ключа пользователя (субъекта), если пользователь имеет несколько сертификатов;
- назначение ключа, например, ключ для шифрования данных, проверки ЭЦП данных, для проверки ЭЦП сертификатов и т.д.;

- уточнение периода использования – можно сократить время действия сертификата, указанное в поле Период действия (т.е. период, в течение которого статус сертификата отслеживается, станет больше, чем разрешенное время использования сертификата);
- политики использования сертификата;
- выбор соответствия политик использования сертификата для центра сертификации и пользователя, если имеются различные варианты;
- альтернативное имя пользователя и центра сертификации;
- указания, является ли пользователь сам центром сертификации и насколько глубоко разрешается разворачивать сертификационный путь.

Предположим, что ключевые пары сгенерированы, открытые ключи заверены сертификатами и размещены в каталоге, реализованном с помощью web-сервера, ftp-сервера, службы каталога или другой технологии. Теперь, если абонент *A* желает проверить подпись абонента *B* под полученным сообщением (или зашифровать для B сообщение с помощью его открытого ключа и т.д.), он выполняет следующие действия:

1) запрашивает в сетевом справочнике сертификат C_B открытого ключа подписи (шифрования, …) абонента *B*;
2) проверяет достоверность сертификата C_B (см. ниже);
3) в случае успеха проверяет подпись под сообщением (зашифровывает сообщение, …) с помощью открытого ключа, извлеченного из C_B.

Процедура проверки достоверности сертификата C_B состоит в следующем:

1) проверяется срок действия сертификата C_B, если он закончился, сертификат считается недостоверным;
2) из C_B извлекается имя ЦС, подписавшего этот сертификат, обозначим его D;
3) если $D=B$, то сертификат самоподписанный, он считается достоверным только, если $D=ROOT$ (хотя, возможно, в некоторых сетях право выдавать самоподписанные сертификаты имеет не один ROOT, это – политика сети);
4) если же $D\neq B$, то из справочника запрашивается сертификат C_D открытого ключа подписи абонента *D*, проверяется на достоверность сертификат C_D;
5) в случае отрицательного ответа принимается решение о недостоверности сертификата C_B, иначе из C_D извлекается открытый ключ K_D;
6) с помощью K_D проверяется подпись под сертификатом C_B, по результатам проверки этой подписи судят о достоверности C_B.

Надо отметить, что сфера применения цифровых сертификатов сейчас достаточно широка. В частности, они используются для распределения открытых ключей в протоколах защиты электронной почты S/MIME или PGP, с помощью цифровых сертификатов проверяется подлинность участников соединения по протоколу SSL и т.д.

Начиная с Windows 2000 Server с состав серверных ОС Microsoft входит программное обеспечение для создания центров сертификации. Создание корпоративного ЦС может понадобиться, если принято решение использовать защиту электронной почты с помощью S/MIME, шифрование данных при хранении средствами EFS (EFS - Encrypted File System - реализует шифрование данных на дисках с файловой системой NTFS), шифрование сетевого трафика с помощью протокола IPSec.

Контрольные вопросы:

1 Какие основные функции включает управление ключами?
2 Перечислите носители ключевой информации.
3 Понятие концепции иерархии ключей.
4. Какие протоколы аутентификации и распределения ключей для симметричных криптосистем вы можете назвать?

2.9. Основные характеристики защищенной информационной системы

Цель: Изучить основные характеристики защищенности информационной системы

План:

Концепция защищенного ядра. Методы верификации. Защищенные домены. Применение иерархического метода для построения защищенной операционной системы.

Теоретический материал:

Очевидно, однако, что абсолютно надежных и безопасных систем не существует, это абстракция. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

В "Оранжевой книге" доверенная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Обратим внимание, что в рассматриваемых Критериях и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности (статической). Степень доверия оценивается по двум основным критериям.

1. Политика безопасности - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности - это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.
2. Уровень гарантированности - мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

Важным средством обеспечения безопасности является механизм подотчетности (протоколирования). Доверенная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть анализом регистрационной информации.

Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности. Доверенная вычислительная база - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор.

Вообще говоря, компоненты вне вычислительной базы могут не быть доверенными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки доверия безопасности ИС достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.

Основное назначение доверенной вычислительной базы - выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к

программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

1. Изолированность. Необходимо предупредить возможность отслеживания работы монитора.
2. Полнота. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.
3. Верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности. Ядро безопасности - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют периметром безопасности. Как уже указывалось, компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, - нет.

В основе построения СРД лежит концепция разработки защищенной универсальной ОС на базе ядра безопасности. Под **ядром безопасности** понимают локализованную, минимизированную, четко ограниченную и надежно изолированную совокупность программно-аппаратных механизмов, доказательно правильно реализующих функции диспетчера доступа.

Правильность функционирования ядра безопасности доказывается путем полной формальной верификации его программ и пошаговым доказательством их соответствия выбранной математической модели защиты.

Применение ядра безопасности требует провести изменения ОС и архитектуры ЭВМ. Ограничение размеров и сложности ядра необходимо для обеспечения его верифицируемости.

Для аппаратной поддержки защиты и изоляции ядра в архитектуре ЭВМ должны быть предусмотрены:

• многоуровневый режим выполнения команд;
• использование ключей защиты и сегментирование памяти;
• реализация механизма виртуальной памяти с разделением адресных пространств;
• аппаратная реализация части функций ОС;
• хранение программ ядра в постоянном запоминающем устройстве (ПЗУ);
• использование новых архитектур ЭВМ, отличных от фоннеймановской архитектуры (архитектуры с реализацией абстрактных типов данных, теговые архитектуры с привилегиями и др.).

Обеспечение многоуровневого режима выполнения команд является главным условием создания ядра безопасности. Таких уровней должно быть не менее двух. Часть машинных команд ЭВМ должна выполняться только в режиме работы ОС. Основной проблемой создания высокоэффективной защиты от НСД является предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние. Для современных сложных ОС практически нет доказательств отсутствия возможности несанкционированного получения пользовательскими программами статуса программ ОС.

Использование ключей защиты, сегментирование памяти и применение механизма виртуальной памяти предусматривает аппаратную поддержку концепции изоляции областей памяти при работе ЭВМ в мультипрограммных режимах. Эти механизмы служат основой для организации работы ЭВМ в режиме виртуальных машин. Режим виртуальных машин позволяет создать наибольшую изолированность пользователей, допуская использование даже различных ОС пользователями в режиме разделения времени.

Аппаратная реализация наиболее ответственных функций ОС и хранение программ ядра в ПЗУ существенно повышают изолированность ядра, его устойчивость к попыткам модификации. Аппаратно должны быть реализованы прежде всего функции идентификации и аутентификации субъектов доступа, хранения атрибутов системы защиты, поддержки криптографического закрытия информации, обработки сбоев и отказов и некоторые другие.

Под *механизмами защиты* ОС будем понимать все средства и механизмы защиты данных, функционирующие в составе ОС. Операционные системы, в составе которых функционируют средства и механизмы защиты данных, часто называют защищенными системами.

Под *безопасностью* ОС будем понимать такое состояние ОС, при котором невозможно случайное или преднамеренное нарушение функционирования ОС, а также нарушение безопасности находящихся под управлением ОС ресурсов системы. Укажем следующие особенности ОС, которые позволяют выделить вопросы обеспечения безопасности ОС в особую категорию:

− управление всеми ресурсами системы;

− наличие встроенных механизмов, которые прямо или косвенно влияют на безопасность программ и данных, работающих в среде ОС;

− обеспечение интерфейса пользователя с ресурсами системы;

− размеры и сложность ОС.

Большинство ОС обладают дефектами с точки зрения обеспечения безопасности данных в системе, что обусловлено выполнением задачи обеспечения максимальной доступности системы для пользователя.

Рассмотрим *типовые функциональные дефекты* ОС, которые могут привести к созданию каналов утечки данных.

1. *Идентификация*. Каждому ресурсу в системе должно быть присвоено уникальное имя – идентификатор. Во многих системах пользователи не имеют возможности удостовериться в том, что используемые ими ресурсы действительно принадлежат системе.

2. *Пароли*. Большинство пользователей выбирают простейшие пароли, которые легко подобрать или угадать.

3. *Список паролей*. Хранение списка паролей в незашифрованном виде дает возможность его компрометации с последующим НСД к данным.

4. *Пороговые значения*. Для предотвращения попыток несанкционированного входа в систему с помощью подбора пароля необходимо ограничить число таких попыток, что в некоторых ОС не предусмотрено.

5. *Подразумеваемое доверие*. Во многих случаях программы ОС считают, что другие программы работают правильно.

6. *Общая память*. При использовании общей памяти не всегда после выполнения программ очищаются участки оперативной памяти (ОП).

7. *Разрыв связи*. В случае разрыва связи ОС должна немедленно закончить сеанс работы с пользователем или повторно установить подлинность субъекта.

8. *Передача параметров по ссылке, а не по значению* (при передаче параметров по ссылке возможно сохранение параметров в ОП после проверки их корректности, нарушитель может изменить эти данные до их использования).

9. *Система может содержать много элементов* (например, программ), имеющих различные привилегии.

Средства профилактического контроля необходимы для отстранения пользователя от непосредственного выполнения критичных с точки зрения безопасности данных операций и передачи этих операций под контроль ОС. Для обеспечения безопасности данных работа с ресурсами системы осуществляется с помощью специальных программ ОС, доступ к которым ограничен.

Применение иерархического метода для построения защищенной операционной системы.

Самые важные проблемы при построении защищенных информационных систем: распределение задач администрирования средствами защиты информации между субъектами управления системой; использование встроенных механизмов защиты на всех уровнях иерархии системы.

Уровни сложной системы:

1) уровень платформы (операционная система),
2) общесистемный уровень (СУБД и другие системные средства),
3) уровень приложений.

Каждый уровень требует своего администрирования.

Для разрешения важных проблем возможны следующие альтернативные подходы:

- Все задачи администрирования информационной безопасностью системы возложить на администратора безопасности. Но тогда задача администрирования будет слишком сложной и потребует для решения очень высокой квалификации администратора безопасности, и для использования данного решения нужно разграничивать функции администрирования на всех уровнях иерархии системы, что возможно только с реализацией защиты на всех уровнях добавочными средствами.
- Задачи администрирования информационной безопасностью системы распределить между администраторами на всех уровнях иерархии. Тогда будут не ясны задачи и функции администратора безопасности как основного звена управления информационной безопасностью сложной защищенной системы.

Контрольные вопросы:

1 Что понимают под ядром безопасности?
2 Что является основной проблемой создания высокоэффективной защиты от НСД?
3 Сформулируйте список функциональных дефектов с точки зрения защиты в используемой ОС.
4 Какие элементы безопасности содержит ОС Windows NT?

2.10. Методология корректности информационной защиты

Цель: Изучить методологию обследования и проектирования защитных механизмов информационных систем

План:

Исследование корректности систем защиты. Методология обследования и проектирования защитных механизмов. Модель политики контроля целостности.

Теоретический материал:

В публикациях по современным стандартам, средствам и методам защиты информации достаточно полно обоснованы объективные частные задачи по гарантированному обеспечению надежной защиты информации в СОИ и представлены рациональные пути их решения. Однако отсутствует единая для всех видов СОИ концепция защиты информации. В тоже время, такие современные работы как по своей сути являются обобщением существующих формальных моделей, нормативных документов и зарубежных стандартов в области защиты информации.

При разработке и построении комплексной системы защиты информации в компьютерных системах необходимо придерживаться определенных методологических принципов проведения исследований, проектирования, производства, эксплуатации и развития таких систем. Системы защиты информации относятся к классу сложных систем, и для их построения могут использоваться основные принципы построения сложных систем с учетом специфики решаемых задач:

• параллельная разработка КС и СЗИ;
• системный подход к построению защищенных КС;
• многоуровневая структура СЗИ;
• иерархическая система управления СЗИ;
• блочная архитектура защищенных КС;
• возможность развития СЗИ;
• дружественный интерфейс защищенных КС с пользователями и обслуживающим персоналом.

Первый из приведенных принципов построения СЗИ требует проведения одновременной параллельной разработки КС и механизмов защиты. Только в этом случае можно эффективно обеспечить реализацию всех остальных принципов. Причем в процессе разработки защищенных КС должен соблюдаться разумный компромисс между созданием встроенных неразделимых механизмов защиты и блочных унифицированных средств и процедур защиты. Только на этапе разработки КС можно полностью учесть взаимное влияние блоков и устройств собственно КС и механизмов защиты, добиться системности защиты оптимальным образом.

Принцип системности является одним из основных концептуальных и методологических принципов построения защищенных КС. Он предполагает:

• анализ всех возможных угроз безопасности информации;
• обеспечение защиты на всех жизненных циклах КС;
• защиту информации во всех звеньях КС;
• комплексное использование механизмов защиты.

Потенциальные угрозы выявляются в процессе создания и исследования модели угроз. В результате исследований должны быть получены данные о возможных угрозах безопасности информации, о степени их опасности и вероятности реализации. При построении СЗИ учитываются потенциальные угрозы, реализация которых может привести к существенному ущербу, и вероятность таких событий не близка к нулю.

Защита ресурсов КС должна осуществляться на этапах разработки, производства, эксплуатации и модернизации, а также по всей технологической цепочке ввода, обработки, передачи, хранения и выдачи информации. Реализация этих принципов позволяет обеспечить создание СЗИ, в которой отсутствуют слабые звенья как на различных жизненных циклах КС, так и в любых элементах и режимах работы КС.

Механизмы защиты, которые используются при построении защищенных систем, должны быть взаимоувязаны по месту, времени и характеру действия. Комплексность предполагает также использование в оптимальном сочетании различных методов и средств защиты информации: технических, программных, криптографических, организационных и правовых. Любая, даже простая СЗИ, является комплексной.

Система защиты информации должна иметь несколько уровней, перекрывающих друг друга, т.е. такие системы целесообразно строить по принципу построения матрешек. Чтобы добраться до закрытой информации, злоумышленнику необходимо «взломать» все уровни защиты.

Например, для отдельного объекта КС можно выделить 6 уровней (рубежей) защиты:

- охрана по периметру территории объекта;
- охрана по периметру здания;
- охрана помещения;
- защита аппаратных средств;

- защита программных средств;
- защита информации.

Комплексные системы защиты информации всегда должны иметь централизованное управление. В распределенных КС управление защитой может осуществляться по иерархическому принципу. Централизация управления защитой информации объясняется необходимостью проведения единой политики в области безопасности информационных ресурсов в рамках предприятия, организации, корпорации, министерства. Для осуществления централизованного управления в СЗИ должны быть предусмотрены специальные средства дистанционного контроля, распределения ключей, разграничения доступа, изготовления атрибутов идентификации и другие.

Одним из важных принципов построения защищенных КС является использование блочной архитектуры. Применение данного принципа позволяет получить целый ряд преимуществ:

• упрощается разработка, отладка, контроль и верификация устройств (программ, алгоритмов);
• допускается параллельность разработки блоков;
• упрощается модернизация систем;
• используются унифицированные стандартные блоки;
• удобство и простота эксплуатации.

Основываясь на принципе блочной архитектуры защищенной КС, можно представить структуру идеальной защищенной системы. В такой системе имеется минимальное ядро защиты, отвечающее нижней границе защищенности систем определенного класса, например ПЭВМ. Если в системе необходимо обеспечить более высокий уровень защиты, то это достигается за счет согласованного подключения аппаратных блоков или инсталляции дополнительных программных.

В случае необходимости могут быть использованы более совершенные блоки КС, чтобы не допустить снижения эффективности применения системы по прямому назначению. Это объясняется потреблением части ресурсов КС вводимыми блоками защиты.

Стандартные входные и выходные интерфейсы блоков позволяют упростить процесс модернизации СЗИ, альтернативно использовать аппаратные или программные блоки. Здесь просматривается аналогия с семиуровневой моделью ЭМВОС.

При разработке сложной КС, например, вычислительной сети, необходимо предусматривать возможность ее развития в двух направлениях: увеличения числа пользователей и наращивания возможностей сети по мере совершенствования информационных технологий. С этой целью при разработке КС предусматривается определенный запас ресурсов по сравнению с потребностями на момент разработки. Наибольший запас производительности необходимо предусмотреть для наиболее консервативной части сложных систем – каналов связи. Часть резерва ресурсов КС может быть востребована при развитии СЗИ. На практике резерв ресурсов, предусмотренный на этапе разработки, исчерпывается уже на момент полного ввода в эксплуатацию сложных систем. Поэтому при разработке КС предусматривается возможность модернизации системы. В этом смысле сложные системы должны быть развивающимися или открытыми. Термин открытости в этой трактовке относится и к защищенным КС. Причем механизмы защиты, постоянно совершенствуясь, вызывают необходимость наращивания ресурсов КС. Новые возможности, режимы КС, а также появление новых угроз в свою очередь стимулируют развитие новых механизмов защиты. Важное место в процессе создания открытых систем играют международные стандарты в области взаимодействия устройств, подсистем. Они позволяют использовать подсистемы различных типов, имеющих стандартные интерфейсы взаимодействия.

Комплексная система защиты информации должна быть дружественной по отношению к пользователям и обслуживающему персоналу. Она должна быть максимально

автоматизирована и не должна требовать от пользователя выполнять значительный объем действий, связанных с СЗИ.

Комплексная СЗИ не должна создавать ограничений в выполнении пользователем своих функциональных обязанностей. В СЗИ необходимо предусмотреть меры снятия защиты с отказавших устройств для восстановления их работоспособности.

Контрольные вопросы:

1 Классификация информационных систем и объектов
2 Расскажите о фрагментарном подходе построения системы защиты информации?
3 Что подразумевается под комплексным подходом построения системы защиты информации?
4 Принципы системы защиты.

2.11. Мера защиты информации

Цель: Изучить методы оценки меры защиты информации.

План:

Определение необходимой меры защиты информационных ресурсов. Методы оценки меры защиты информации. Основные показатели оценки уровня защиты информации. Характеристики мер защиты. Оптимальное управление процессами защиты.

Теоретический материал:

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышает зависимости общества от степени безопасности используемых им информационных технологий.

Чем сложнее задача автоматизации и чем ответственнее область, в которой используются компьютерные системы обработки информации, тем все более и более критичными становятся такие свойства как надежность и безопасность информационных ресурсов, задействованных в процессе сбора, накопления, обработки, передачи и хранения компьютерных данных.

Под защитой информации в СОИ понимается регулярное использование в них средств и методов, принятие мер и осуществление мероприятий с целью системного обеспечения требуемой безопасности информации, хранимой и обрабатываемой с использованием средств СОИ.

Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних дестабилизирующих факторов. Под защищенностью информации будем понимать интегральный показатель, характеризующий качество информации с точки зрения: целостности, конфиденциальности, доступности.

Из определения защищенности информации вытекают задачи обеспечения безопасности информации в СОИ:

- предупреждение нарушения целостности хранимой и обрабатываемой в СОИ информации;
- обеспечение конфиденциальности сохраняемых в СОИ данных;
- обеспечение доступности систем, данных и служб СОИ, для субъектов, имеющих право доступа.

Вследствие совокупности действия всех перечисленных факторов перед разработчиками современных КСОИ, стоят следующие задачи: разработка защищенных систем обработки информации, требующего эффективного обеспечение безопасности информационных ресурсов. Поскольку компьютерные системы теперь напрямую интегрированы в информационные структуры современного общества, средства защиты должны учитывать

современные формы представления информации(гипертекст, мультимедиа и др.). Это означает, что система защиты должны обеспечивать безопасность на уровне информационных ресурсов, а не отдельных документов, файлов или сообщений.

Понятие многоуровневой защиты или эшелонированной обороны, а в английской версии - Defence (амер. Defense) in depth, пришло в информационные технологии из военных руководств.

С точки зрения информационной безопасности, модель многоуровневой защиты определяет набор уровней защиты информационной системы. Модель часто используется корпорацией Майкрософт в руководствах по безопасности. Корректная организация защиты на каждом из выделенных уровней, позволяет уберечь систему от реализации угроз информационной безопасности.

Как уже отмечалось выше, 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.

Контрольные вопросы:

1 Перечислите уровни информационной безопасности.
2 Охарактеризуйте целевую направленность Общих Критериев.
3 Требования и концепции Общих Критериев.
4.Дайте общую характеристику стандартам и рекомендациям в области информационной безопасности.
5 Основные этапы разработки КСЗИ
6 Охарактеризуйте основные модели управление
7 Общие требования для управления процессами безопасности информации

2.12.Оценка системы защиты

Цель: Изучить основные методы и принципы оценки надежности защитных механизмов.

План:

Комплексная оценка системы защиты информации. Тестирование программного обеспечения. Проблема тестирования программных продуктов, автоматическое тестирование, принципы написания самотестирующихся программных продуктов.

Теоретический материал:

Решение любой задачи ИС (информационной системы) осуществляется при взаимодействии аппаратных средств и программного обеспечения (ПО), поэтому надежность работы ИС зависит не только от надежности оборудования, но также и от надежности ПО в равной степени.

*Надежность ПО определяется его безотказностью и восстанавливаемостью***.** Безотказность характеризуется способностью выполнить все функции в процессе обработки информации. Восстанавливаемость характеризуется способностью восстановления работоспособности после отказов.

Основными показателями безотказности ПО является среднее время между отказами, вызванными ошибками в программе, а также интенсивность отказов. Причинами отказов ПО могут быть ошибки в программе, ошибки в вычислении, логические ошибки, ошибки ввода/вывода (I/O), ошибки пользователей и т.д.

Ошибки в программе**.** При создании сложных структурированных продуктов далеко не всегда удается обнаружить и устранить все ошибки на стадии отладки. Поэтому в эксплуатации могут послужить программы со скрещенными дефектами. Они проявляются при сочетании входных данных или режимов, непредусмотренных при отладке, т.к. все возможные комбинации практически невозможно предусмотреть. Именно скрытые ошибки в программе являются причиной отказа ПО.

Ошибки вычислений. К ним относятся неправильные кодировки форм, ошибки в знаках (арифметических), непрерывное преобразование и т.д. В результате ошибок вычислений появляется отказ в форме исправительного результата.

Логические ошибки**.** Неправильная передача управления, ошибки при формировании условия поиска и т.д. Логические ошибки приводят к искажению алгоритма обработки данных.

Ошибки I/O**.** Недопустимые форматы данных, неправильное указание размещения на экране или бумаге, неверное задание числа разрядов и др.

Ошибки пользователей**.** Неправильное понимание выводимых указаний, ввод недопустимых данных и т.д.

Основной характеристикой восстанавливаемости ПО является среднее время устранения ошибки. Оно состоит из времени поиска ошибки и времени ее устранения. Время восстановления работоспособности ПО зависит от многих факторов: сложности и объема программы, наличие ее объема комментариев, языка программирования, опыта и квалификации программиста.

Важной особенностью ПО по сравнению с аппаратурой является то, что с течением времени его надежность возрастает: в процессе функционирования программ ошибки устраняются.

Основным средством защиты от злоумышленных действий является ограничение доступа к аппаратуре и ПО. Для пользователей и обслуживающих специалистов устанавливается иерархическая схема доступа на приоритетной основе. Уровнями защиты могут быть: доступ к аппаратным средствам, доступ к отдельным полям, записям БД, доступ к файлам БД, доступ к ОС, доступ к сетевым средствам. необходимо также иметь возможность запоминать лиц, имеющих полномочия, к какой информации они были допущены, а также использованное машинное время. Доступ к программным средствам осуществляется на основе репутации пользователей, вход в систему осуществляется при помощи системы паролей. В зависимости от приоритета и полномочий пользователей он получает доступ от отдельных полей БД до ОС и выше.

Повышение эффективности функционирования предприятий невозможно без внедрения современных методов управления, базирующихся на информационных системах (ИС) управления предприятиями. Одними из самых серьезных проблем программного обеспечения (ПО) ИС является его дороговизна и низкая надежность. Многие специалисты считают первый из этих недостатков продолжением второго. Поскольку программное обеспечение по самой своей природе ненадежно, его тестирование и сопровождение требует постоянных существенных расходов. Дадим определение основных понятий надежности ПО в соответствии с классической работой Г. Майерса:

- в программном обеспечении имеется ошибка, если оно не выполняет того, что пользователю разумно от него ожидать.
- отказ программного обеспечения - это появление в нем ошибки.
- надежность программного обеспечения - есть вероятность его работы без отказов в течении определенного периода времени, рассчитанного с учетом стоимости для пользователя каждого отказа.

Из данных определений можно сделать важные выводы:

- надежность программного обеспечения является не только внутренним свойством программы.
- надежность программного обеспечения - это функция как самого ПО, так и ожиданий (действий) его пользователей.

Основными причинами ошибок программного обеспечения являются:

- большая сложность ПО, например, по сравнению с аппаратной конфигурацией ПЭВМ.
- неправильный перевод информации из одного представления в другое на макро- и микроуровнях. На макроуровне, уровне проекта, осуществляется передача и преобразование

различных видов информации между организациями, подразделениями и конкретными исполнителями на всех этапах жизненного цикла ПО. На микроуровне, уровне исполнителя, производится преобразование информации по схеме: получить информацию - запомнить - выбрать из памяти (вспомнить) - воспроизвести информацию (передать).

Источниками ошибок (угрозами надежности) программного обеспечения являются:

- внутренние: ошибки проектирования, ошибки алгоритмизации, ошибки программирования, недостаточное качество средств защиты, ошибки в документации.
- внешние: ошибки пользователей, сбои и отказы аппаратуры ЭВМ, искажение информации в каналах связи, изменения конфигурации системы.

Методы проектирования надежного программного обеспечения можно разбить на следующие группы:

- предупреждение ошибок, методы позволяющие минимизировать или исключить появление ошибки.
- обнаружение ошибок, методы направленные на разработку дополнительных функций программного обеспечения, помогающих выявить ошибки.
- устойчивость к ошибкам, дополнительные функции программного обеспечения, предназначенные для исправления ошибок и их последствий и обеспечивающие функционирование системы при наличии ошибок.

Методы предупреждения ошибок концентрируются на отдельных этапах процесса проектирования программного обеспечения и включают в себя:

- методы, позволяющие справиться со сложностью системы.
- методы достижения большей точности при переводе информации.
- методы улучшения обмена информацией.
- методы немедленного обнаружения и устранения ошибок на каждом шаге (этапе) проектирования, не откладывая их на этап тестирования программы.

Сложность системы является одной из главных причин низкой надежности программного обеспечения. В общем случае, сложность объекта является функцией взаимодействия (количества связей) между его компонентами. В борьбе со сложностью ПО используются две концепции:

1) Иерархическая структура. Иерархия позволяет разбить систему по уровням понимания (абстракции, управления). Концепция уровней позволяет анализировать систему, скрывая несущественные для данного уровня детали реализации других уровней. Иерархия позволяет понимать, проектировать и описывать сложные системы.

2) Независимость. В соответствии с этой концепцией, для минимизации сложности, необходимо максимально усилить независимость элементов системы.

Это означает такую декомпозицию системы, чтобы её высокочастотная динамика была заключена в отдельных компонентах, а межкомпонентные взаимодействия (связи) описывали только низкочастотную динамику системы. Методы обнаружения ошибок базируются на введении в программное обеспечение системы различных видов избыточности:

1) временная избыточность. Использование части производительности ЭВМ для контроля исполнения и восстановления работоспособности ПО после сбоя;
2) информационная избыточность. Дублирование части данных информационной системы для обеспечения надёжности и контроля достоверности данных;
3) программная избыточность включает в себя: взаимное недоверие - компоненты системы проектируются, исходя из предположения, что другие компоненты и исходные данные содержат ошибки, и должны пытаться их обнаружить; немедленное обнаружение и регистрацию ошибок; выполнение одинаковых функций разными модулями системы и сопоставление результатов обработки; контроль и восстановление данных с использованием других видов избыточности.

Методы обеспечения устойчивости к ошибкам направлены на минимизацию ущерба, вызванного появлением ошибок, и включают в себя:

- обработку сбоев аппаратуры;
- повторное выполнение операций;
- динамическое изменение конфигурации;
- сокращенное обслуживание в случае отказа отдельных функций системы;
- копирование и восстановление данных;
- изоляцию ошибок.

Важным этапом жизненного цикла программного обеспечения, определяющим качество и надёжность системы, является тестирование. Тестирование - процесс выполнения программ с намерением найти ошибки. Этапы тестирования:

- автономное тестирование, контроль отдельного программного модуля отдельно от других модулей системы.
- тестирование сопряжений, контроль сопряжений (связей) между частями системы (модулями, компонентами, подсистемами).
- тестирование функций, контроль выполнения системой автоматизируемых функций.
- комплексное тестирование, проверка соответствия системы требованиям пользователей.
- тестирование полноты и корректности документации, выполнение программы в строгом соответствии с инструкциями.
- тестирование конфигураций, проверка каждого конкретного варианта поставки (установки) системы.

Существуют две стратегии при проектировании тестов: тестирование по отношению к спецификациям (документации), не заботясь о тексте программы, и тестирование по отношению к тексту программы, не заботясь о спецификациях. Разумный компромисс лежит где-то посередине, смещаясь в ту или иную сторону в зависимости от функций, выполняемых конкретным модулем, комплексом или подсистемой.

Качество подготовки исходных данных для проведения тестирования серьёзно влияет на эффективность процесса в целом и включает в себя:

- техническое задание;
- описание системы;
- руководство пользователя;
- исходный текст;
- правила построения (стандарты) программ и интерфейсов;
- критерии качества тестирования;
- эталонные значения исходных и результирующих данных;
- выделенные ресурсы, определяемые доступными финансовыми средствами.

Однако, исчерпывающее тестирование всех веток алгоритма любой серьёзной программы для всех вариантов входных данных практически неосуществимо. Следовательно, продолжительность этапа тестирования является вопросом чисто экономическим. Учитывая, что реальные ресурсы любого проекта ограничены бюджетом и графиком, можно утверждать, что искусство тестирования заключается в отборе тестов с максимальной отдачей.

Ошибки в программах и данных могут проявиться на любой стадии тестирования, а также в период эксплуатации системы. Зарегистрированные и обработанные сведения должны использоваться для выявления отклонений от требований заказчика или технического задания. Для решения этой задачи используется система конфигурационного управления версиями программных компонент, база документирования тестов, результатов тестирования и выполненных корректировок программ. Средства накопления сообщений об отказах, ошибках, предложениях на изменения, выполненных корректировках и характеристиках версий являются основной для управления развитием и сопровождением комплекса ПО и состоят из журналов :

- предлагаемых изменений;
- найденных дефектов;

- утвержденных корректировок;
- реализованных изменений;
- пользовательских версий.

Рассмотрим применение описанных выше методов повышения надёжности программного обеспечения при разработке информационной системы управления предприятием.

Предупреждение ошибок - лучший путь повышения надёжности программного обеспечения. Для его реализации была разработана методика проектирования систем управления предприятиями, соответствующая спиральной модели жизненного цикла ПО. Методика предусматривает последовательное понижение сложности на всех этапах анализа объекта. При декомпозиции ИС были выделены уровни управления системы, затем подсистемы, комплексы задач и так далее, вплоть до отдельных автоматизируемых функций и процедур. Методика базируется на методах структурно-функционального анализа (SADT), диаграммах потоков данных (DFD), диаграммах "сущность-связь" (ERD), методах объектно-ориентированного анализа (OOA) и проектирования (OOD), которые мы студенты изучили в курсе «Проектирование ИС».

На основании методов обнаружения ошибок были разработаны следующие средства повышения надёжности ПО.

Средства использующие временную избыточность**:** авторизация доступа пользователей к системе, анализ доступных пользователю ресурсов, выделение ресурсов согласно ролям и уровням подготовки пользователей, разграничение прав доступа пользователей к отдельным задачам, функциям управления, записям и полям баз данных.

Средства обеспечения надёжности, использующие информационную избыточность: ссылочная целостность баз данных обеспечивается за счёт системы внутренних уникальных ключей для всех информационных записей системы, открытая система кодирования, позволяющая пользователю в любой момент изменять коды любых объектов классификации, обеспечивает стыковку системы классификации ИСУ, например 1С: Предприятие (Казахстанская настройка Класс версия 1.7), с ПО других разработчиков, механизмы проверки значений контрольных сумм записей системы, обеспечивают выявление всех несанкционированных модификаций (ошибок, сбоев) информации, средства регистрации обеспечивают хранение информации о пользователе и времени последней модификации (ввода, редактирования, удаления) и утверждения каждой записи информационной системы, введение в структуры баз данных системы времени начала и окончания участия записи в расчётах позволяет ограничить объём обрабатываемой информации на любом заданном периоде, а также обеспечить механизмы блокировки информации для закрытых рабочих переводов, ведение служебных полей номеров версий баз данных и операционных признаков записей позволяет контролировать и предупреждать пользователей о конфликтах в случае несоответствия номеров версий модулей и структур баз, либо о нарушении технологических этапов обработки информации, средства автоматического резервного копирования и восстановления данных (в начале, конце сеанса работы или по запросу пользователей) обеспечивают создание на рабочей станции клиента актуальной копии сетевой базы данных, которая может быть использована в случае аварийного сбоя аппаратуры локальной и вычислительной сети и перехода на локальный режим работы и обратно.

Средства обеспечения надёжности, использующие программную избыточность: распределение реализации одноименных функций по разным модулям ИС с использованием разных алгоритмов и системы накладываемых ограничений и возможностью сравнения полученных результатов; специальные алгоритмы пересчётов обеспечивают в ручном и автоматическом режимах переформирование групп документов, цепочек порождаемых документов и бухгалтерских проводок, что повышает эффективность и надёжность обработки информации; средства обнаружения и регистрации ошибок в сетевом и локальных протоколах; в программные модули системы встроены средства протоколирования

процессов сложных расчётов с выдачей подробной диагностики ошибок; средства отладки и трассировки алгоритмов пользовательских бизнес-функций.

Средства обеспечивающие устойчивость системы к ошибкам: процедура обработки сбоев обеспечивает в автоматическом режиме несколько попыток повторного выполнения операций прежде, чем выдать пользователю сообщение об ошибке (например, для операций раздельного доступа к ресурсам, операций блокировки информации или обращения к внешним устройствам); средства динамического изменения конфигурации осуществляют контроль доступа к сетевым ресурсам, а в случае их недоступности или конфликта обеспечивают автоматический запуск системы по альтернативным путям доступа; средства контроля и обслуживания данных обеспечивают восстановление заголовков баз данных, восстановление индексных файлов, конвертацию модифицированных структур баз данных; средства слияния, копирования, архивирования и восстановления данных.

Для обеспечения качества программного обеспечения ИС на этапе развития и сопровождения системы разработан комплекс программных средств обеспечивающий:

- управление версиями ПО;
- регистрацию поставок;
- сопровождение заявок клиентов.

Использование рассмотренных методов и средств обеспечения надёжности при проектировании и сопровождении информационной системы предприятия обеспечивает высокий уровень надёжности системы, необходимый для одновременной работы десятков пользователей производственной системы управления в реальном масштабе времени.

Контрольные вопросы:

1. Приведите классификацию систем защиты программного обеспечения.
2. Сравните основные технические методы и средства защиты программного обеспечения.
3. Назовите отличия систем защиты от несанкционированного доступа от систем защиты от несанкционированного копирования.
4. Дайте характеристику показателей эффективности систем защиты.
5. Приведите примеры взаимодействия участников процесса создание и распространения ПО.

2.13. Безопасность компьютерных систем

Цель: Изучить основные методы защиты информации в локальных сетях.

План:

Защита в локальных сетях. Программные средства индивидуальной защиты информации. Использование экспертных систем для распознавания попыток несанкционированного доступа.

Теоретический материал:

Обеспечение надежной защиты корпоративной сети — очень сложный процесс, который представляет собой непрерывную и постоянную последовательность действий по реализации комплекса мер информационной безопасности.

Что могут сделать компании для защиты корпоративной сети? Большинство экспертов по безопасности рекомендуют начать с тщательного отбора (в том числе по этическим и моральным критериям) сотрудников, в задачи которых будет входить администрирование сети и, в частности, создание и эксплуатация подсистемы информационной безопасности корпоративной сети. И хотя многие руководители полагают, что самыми широкими правами доступа к важным для компании данным обладают только они вместе с адвокатами и

бухгалтерами, но это не так. Доступом ко всем конфиденциальным материалам обладают администраторы корпоративной сети. А поскольку они, как правило, не имеют долевого участия в прибылях компании, то представляют собой одну из самых серьезных потенциальных угроз для безопасности компании. Поэтому вполне очевидно, что люди, претендующие на эту работу, должны быть тщательно проверены.

Одним из основных компонентов системы защиты корпоративной сети являются межсетевые экраны, которые обеспечивают организацию защитного периметра, защищающего информационные ресурсы организации от доступа извне и контролирующего процедуры взаимодействия пользователей корпоративной сети с внешними сетями, в основном с Интернетом. Межсетевой экран обеспечивает решение таких задач, как защита локальной сети от несанкционированного доступа из внешних сетей, безопасный доступ в Интернет корпоративных пользователей, удаленное подключение пользователей к ресурсам корпоративной информационной системы. На критически важные узлы корпоративной сети возможна установка отдельного межсетевого экрана.

Антивирусные продукты обеспечивают надежную защиту серверов, рабочих станций, почтовых систем и Интернет-трафика от поражения компьютерными вирусами.

Система организации защищенного удаленного доступа пользователей к ресурсам корпоративной сети предоставляет возможность создания защищенных Интернет-каналов, реализованных на базе технологии построения виртуальных частных сетей, что обеспечивает высокий уровень безопасности корпоративного трафика при небольших финансовых затратах.

Системы обнаружения вторжений и системы анализа защищенности ресурсов корпоративной сети, работающие в едином комплексе, обеспечивают предотвращение хакерских атак, позволяют предупреждать внешние и внутренние хакерские атаки, контролируют проходящий трафик и процессы на ключевых серверах сети, дают возможность в автоматическом режиме блокировать атаки, обнаруживать и устранять уязвимости в системе защиты корпоративной сети.

Средства управления политикой безопасности и защиты от несанкционированного доступа реализуют комплексные решения для организации доступа пользователей и администраторов к ресурсам корпоративной сети, предусматривают использование электронных ключей с уникальными персональными идентификаторами пользователей, электронных замков и других средств защиты серверов, рабочих станций и телекоммуникационного оборудования от несанкционированного доступа.

Многие пользователи считают, что для обеспечения надежной защиты вполне достаточно антивирусного программного обеспечения, другие полагают, что лучшее решение — полная шифрация данных. Однако использование антивирусного ПО при его правильной настройке и эксплуатации означает всего лишь то, что вирусы из общеизвестных списков с большой долей вероятности не попадут в защищаемый информационный ресурс. Кроме того, существует большое количество программ, типа троянцев и т.п., которые не обнаруживаются антивирусным программным обеспечением и могут функционировать на зараженном компьютере годами. Полное шифрование данных само по себе тоже не является панацеей, так как шифруемая стойкими алгоритмами важная информация может быть легко передана злоумышленнику так называемыми клавиатурными шпионами. В то же время следует учитывать, что система шифрования является одним из ключевых (хотя и не единственным!) элементов единой комплексной подсистемы информационной безопасности корпоративной сети компании.

Администратору подсистемы безопасности следует иметь в виду то, что конфиденциальная информация компании может быть послана сотрудником компании по электронной почте. Для обнаружения подобных фактов подсистема безопасности должна включать средства контроля содержимого почтовых сообщений.

Система управления политикой безопасности и защиты от несанкционированного доступа

Прежде всего следует отметить, что данная система не выполняет функций защиты от таких злонамеренных действий, как использование побочных электромагнитных излучений и наводок, подслушивание, подглядывание и т.п., — для противодействия подобного рода нарушениям должен быть реализован комплекс организационно-технических мероприятий по физическому контролю (размещение, охрана и т.п.) контролируемых узлов корпоративной сети. Основной же задачей системы управления политикой безопасности и защиты от несанкционированного доступа является обнаружение фактов несанкционированных действий пользователей корпоративной сети на основе сбора и анализа информации о событиях, регистрируемых на информационных ресурсах корпоративной сети.

Данная система обеспечивает мониторинг, контроль и сбор информации о действиях легальных пользователей корпоративной сети. Если по результатам анализа собранных данных выявляется факт несанкционированных действий, система блокирует дальнейшие действия нарушителя и оповещает администратора безопасности о действиях пользователя. Кроме того, система контролирует работу приложений, запущенных на рабочих станциях пользователей. Информация о случае нарушении политики безопасности записывается в базу данных системы и может использоваться для дальнейшего анализа.

В задачу этой системы входит сбор информации о следующих событиях:

- изменение файловой системы контролируемого узла корпоративной сети;
- использование внешних устройств ввода-вывода (дисководов, USB-устройств и т.п.);
- запуск и остановка процессов на контролируемом узле;
- локальная либо удаленная регистрация начала сеанса работы пользователя, а также завершение работы пользователей;
- использование принтеров и других периферийных устройств;
- ведение статистики использования сетевых сервисов;
- изменение аппаратной и программной конфигурации контролируемого узла.

Система управления политикой безопасности и защиты от несанкционированного доступа имеет распределенную архитектуру и включает такие компоненты, как программные сенсоры, сервер управления сенсорами и консоль администратора. Программные сенсоры устанавливаются на контролируемые узлы корпоративной сети и обеспечивают сбор, фильтрацию и передачу параметров собранных событий серверу управления сенсорами. Сервер управления сенсорами осуществляет хранение и анализ информации о событиях, поступающих от сенсоров системы. Консоль администратора служит для централизованного управления сервером управления сенсорами и сенсорами системы, отображения результатов работы системы и формирования отчетов.

Использование таких средств защиты, как межсетевые экраны, системы контроля доступа пользователей и т.п., не дает полной гарантии устойчивости корпоративной сети к атакам. Любое программное или аппаратное обеспечение не является совершенным, и в нем имеются уязвимости, позволяющие совершить какие-либо действия в нарушение установленного порядка использования информационных ресурсов. Кроме того, реагировать на несанкционированную активность или попытки взлома сети в режиме реального времени практически невозможно, если эти функции выполняются вручную. Своевременное обнаружение попыток взлома информационных ресурсов и оперативная реакция на эти действия позволяют значительно повысить уровень защищенности сети [2].

Система обнаружения и предотвращения вторжений

Данная система позволяет обнаруживать атаки и злоупотребления в отношении узлов корпоративной сети компании. Система может обеспечивать как защиту конкретного узла, так и целого сетевого сегмента. Основной принцип работы системы обнаружения и предотвращения вторжений заключается в выявлении и блокировании сетевых атак в

корпоративной сети на основе анализа пакетов данных, циркулирующих в этой сети, и в последующем выявлении аномалий сетевого трафика сети. Система позволяет с равной степенью эффективности выявлять и блокировать атаки со стороны как внешних, так и внутренних нарушителей.

Для обнаружения вторжений система использует метод, основанный на выявлении сигнатур известных атак, а также метод, базирующийся на анализе поведения сети. Метод, основанный на выявлении сигнатур, обеспечивает обнаружение атак посредством специальных шаблонов. В качестве сигнатуры атаки могут выступать строка символов, семантическое выражение на специальном языке, формальная математическая модель и др., причем каждая сигнатура может быть соотнесена с соответствующей атакой нарушителя. При получении исходных данных о сетевом трафике корпоративной сети система проводит их анализ на соответствие определенным шаблонам или сигнатурам атак, хранимым в постоянно обновляющейся базе данных системы. В случае обнаружения сигнатуры в исходных данных система фиксирует факт обнаружения сетевой атаки и блокирует ее дальнейшие действия. Преимуществом сигнатурного метода является его высокая точность.

Для выявления новых типов атак в системе обнаружения вторжений реализован метод, который основан на анализе поведения корпоративной сети и использует информацию о штатном процессе функционирования корпоративной сети. Принцип работы этого метода заключается в обнаружении несоответствия между текущим режимом функционирования корпоративной сети и моделью штатного режима работы, заложенной в параметрах работы метода. Любое несоответствие рассматривается как информационная атака. В случае осуществления атаки, которая может привести к выведению из строя узлов корпоративной сети, возможны автоматическое завершение соединения с атакующим узлом, блокировка учетной записи нарушителя (если он является сотрудником компании) или реконфигурация межсетевых экранов и маршрутизаторов таким образом, чтобы в дальнейшем соединения с атакующим узлом были запрещены.

В состав системы обнаружения и предотвращения вторжений входят следующие компоненты: сетевые сенсоры, серверные сенсоры, датчики, сервер управления сенсорами, а также консоль администратора. Сетевые сенсоры, предназначенные для защиты объектов сетевых сегментов корпоративной сети, обеспечивают перехват и анализ всего сетевого трафика, передаваемого в рамках того сегмента, где они установлены. Серверные сенсоры устанавливаются на серверы корпоративной сети и обеспечивают защиту определенных сетевых сервисов сети. В числе таких сенсоров могут быть серверные сенсоры для почтовых, файловых и Web-серверов, а также для серверов баз данных. На одном сервере корпоративной сети может быть одновременно установлено несколько типов сенсоров. Датчики выполняют функции управления серверными и сетевыми сенсорами, а также функции обеспечения передачи информации между сенсорами и сервером управления сенсорами. Сервер управления сенсорами обеспечивает централизованный сбор, хранение и анализ информации, поступающей от серверных и сетевых сенсоров, и дает возможность выявления распределенных сетевых атак на основе анализа полученной информации. Консоль администратора предназначена для централизованного управления компонентами системы и отображения результатов работы системы.

Сообщение об обнаруженной атаке, как правило, формируется в соответствии со стандартом IDMEF (Intrusion Detection Message Exchange Format) и содержит следующую информацию:

- дата и время обнаружения атаки;
- общее описание атаки, включая возможные ссылки на дополнительные источники информации о выявленной атаке;
- символьный идентификатор атаки по классификатору CVE (Common Vulnerabilities Exposures, http://cve.mitre.org) или CERT (Computer Emergency Response Team, http://www.cert.org/);
- уровень приоритета обнаруженной атаки (низкий, средний или высокий);
- информация об источнике атаки (IP-адрес, номер порта, доменное имя и др.);

- информация об объекте атаки (IP-адрес, номер порта, доменное имя и др.);
- рекомендации по устранению уязвимости, в результате которой был зафиксирован факт реализации атаки.

База данных сигнатур атак системы обнаружения и предотвращения вторжений должна регулярно обновляться.

Система анализа защищенности корпоративной сети

Система анализа защищенности предназначена для проведения регулярных, всесторонних или выборочных тестов с целью выявления и устранения уязвимостей программно-аппаратного обеспечения корпоративной сети: сетевых сервисов, операционных систем, прикладного программного обеспечения, систем управления базами данных, маршрутизаторов, межсетевых экранов, а также для проверки наличия последних модулей обновления и т.п. При выявлении уязвимостей система предоставляет администратору отчеты, содержащие подробное описание каждой обнаруженной уязвимости, данные об их расположении в узлах корпоративной сети и рекомендации по их коррекции или устранению.

В состав системы анализа защищенности входят сканеры безопасности, предназначенные для проведения заданного множества проверок в соответствии с параметрами, определенными администратором безопасности; сервер хранения результатов работы системы; консоль администратора для централизованного управления системой.

Сканер безопасности представляет собой программное средство для удаленной или локальной диагностики различных элементов сети на предмет выявления в них уязвимостей, использование которых может привести к компьютерным нарушениям. Основными пользователями таких сканеров являются системные администраторы и специалисты по безопасности. Сканеры безопасности сокращают время, необходимое для поиска уязвимостей, за счет автоматизации операций по оценке защищенности систем. Принципы работы такого сканера заключается в том, что основной модуль программы подсоединяется по сети к удаленному компьютеру. В зависимости от активных сервисов формируются проверки и тесты. Найденная при сканировании каждого порта служебная информация сравнивается с таблицей правил определения сетевых устройств, операционных систем и возможных уязвимостей. На основе проведенного сравнения делается вывод о наличии или отсутствии потенциальной уязвимости.

Система анализа защищенности требует постоянного внимания и контроля. Любое изменение конфигурации корпоративной сети компании, а также сетевого программного обеспечения должно быть исследовано системой анализа защищенности. Несоответствие в конфигурации может привести к увеличению количества ложных срабатываний, а также к появлению дыр в безопасности. Работа системы основана на анализе сетевого трафика с использованием метода сигнатур, поэтому система анализа защищенности требует постоянного обновления базы уязвимостей. Эксплуатация данной системы имеет смысл только при условии, что она развивается вместе с сетью, которую она защищает. Разумеется, что подразумевается регулярное проведение тестов.

В настоящее время многие компании, занимающиеся вопросами информационной безопасности (например, Internet Security Systems и др.), предлагают стратегию применения описанных выше систем в составе единых комплексов, позволяющих осуществлять централизованное управление информационной безопасностью корпоративной сети. С помощью единого управления всеми компонентами подсистемы информационной безопасности корпоративной сети, а также на основе сбора и анализа информации от различных компонентов в режиме реального времени можно значительно повысить эффективность работы администраторов безопасности, сократить число сотрудников соответствующих служб и уменьшить затраты на их обучение.

Подобные системы позволяют вести единую базу данных шаблонов, вариантов реагирования и обновлений для всех компонентов подсистемы безопасности, автоматизировать рутинные

задачи администраторов безопасности (обновление сигнатур атак, сканирование удаленных узлов и т.д.), а также проводить всесторонний анализ различных событий путем корреляции данных от разнообразных средств защиты.

Контрольные вопросы:

1 Что могут сделать компании для защиты корпоративной сети?
2 Чем обусловлена сложность создания системы защиты информации?
3 Что входит в компоненты сетевой системы защиты?
4 Что выполняют межсетевые экраны?
5 Поясните цели политики безопасности в ИВС.

3.МУЛЬТИМЕДИЙНЫЕ ТЕХНОЛОГИИ

Слово *мультимедиа* в буквальном переводе означает много средств для представления информации пользователю. Компьютер без средств мультимедиа сегодня уже не считается полноценным. Многие относятся к этим средствам чуть ли не как к возможности превратить свою жизнь в сказку. Это, пожалуй, преувеличение, хотя иногда и оправданное.

Термин *мультимедиа* используют для характеристики компьютерных систем, графической, звуковой, видео-и иной информации. Существенно, что этот синтез и обработку информации сегодня удаётся выполнять практически в реальном времени, то есть без ощутимой пользователем задержки во времени. Расцвет мультимедиа в середине 90-х годов связывают с быстродействием и памятью, достигнутыми в системах Pentium, и в частности, с возможностями записи и воспроизведения больших объёмов информации с помощью компакт-дисков CD-ROM. До этого времени по техническим причинам использование компьютерных средств для нужд образования, науки, искусства выглядело довольно блекло по сравнению с традиционными средствами. Однако сегодня средства мультимедиа имитируют реальность для многих целей вполне удовлетворительно.

Существенно, что имитация реальности с помощью мультимедийных средств происходит в диалоговом режиме. Пользователь имеет возможность постоянного взаимодействия с программой. В любой момент можно запросить необходимую информацию, представить её в разнообразном удобном для себя виде, а также получить оценку от программы правильности действий пользователя. Развитие диалоговых систем мультимедиа привело к появлению учебников, энциклопедий, атласов, журналов, художественной литературы с «живыми» картинками и звуком.

Компьютер – в отличие от более раздражительного живого педагога – может сколь угодно долго и терпеливо исправлять ошибки ученика. И не важно, идёт ли речь о корректировке акцента при изучении иностранного языка, устранении погрешностей при проектировании нестыковок при создании физической модели природного явления.

Многие считают наиболее интересным использование средств мультимедиа для формального участия дилетанта в эффектной модернизации произведений искусства. Уже сегодня с помощью компьютера новичок может подправить в своём стиле картину классика эпохи Возрождения или музыку знаменитого автора, а также изменить сюжет в видеофильме известного режиссёра. Уже сегодня компьютер может спеть современную песенку голосом и в манере давно умершего певца. Естественно, что всё это называет немало споров среди специалистов, обывателей и медиаманов.

Весьма модное направление развития мультимедийных технологий – виртуальная реальность. Виртуальная реальность – это получение почти реальных ощущений человеком от нереального мира. Моделирование такого нереального мира неплохо выполняется с помощью современного компьютера. Компьютерные средства создают настолько полные зрительные, звуковые и иные ощущения, что пользователь забывает о реальном окружающем мире и с увлечением погружается в вымышленный мир. Особый эффект присутствия достигается возможностями свободного перемещения в виртуальной реальности, а также возможностями воздействия на эту реальность.

Простейший и наименее утомительный вход в виртуальную реальность осуществляется через экран компьютера, на котором эту реальность и можно наблюдать. При этом

перемещения и воздействие на виртуальный мир осуществляется обычно с помощью мышки, джойстика и клавиатуры.

Более полное (и более навязчивое) погружение в придуманный мир осуществляется с помощью специального и довольно дорогого шлема-дисплея, надеваемого на голову человека. Для достижения объёмности изображения два небольших экрана, расположенные внутри шлема, создают раздельные изображения для каждого глаза. При этом при показе изображения пользователю положение картинки меняется в соответствии с поворотом головы. К тому же шлем довольно хорошо изолирует человека от воздействия реального мира.

В качестве недорогого варианта погружения в мультимедиа можно использовать очки с разными стёклами, обеспечивающими объёмное восприятие изображения. Например, объёмное монохроматичное изображение можно наблюдать с помощью очков, одно из стёкол которых красное, а другое - синее. Если при этом на экран выводятся две проекции изображения, одна красная, другая синяя, - то создаётся иллюзия объёмности. Однако такой способ не позволяет передать гамму цветов.

Дополнительные ощущения погружения в виртуальную реальность достигаются при использовании специальной информационной перчатки, которая позволяет «трогать» предметы виртуального мира. При этом для управления компьютером вместо обычной клавиатуры удобно пользоваться специальным пультом, рассчитанным на одну руку. Такая аппаратура позволяет, например, испытать забавные ощущения от того, что трогаешь рукой человека, который в реальном мире находится на большом удалении.

Сегодня ведущие компьютерные фирмы тратят значительные усилия на создание компьютера с человеческим интерфейсом. Это подразумевает, что компьютер должен обладать всеми органами чувств человека, а также способностью воздействовать на все эти человеческие органы. Современные компьютерные системы во многих случаях неплохо анализируют и синтезируют изображения и звуки, так что со слухом и зрением у них всё в относительном порядке. Компьютерная мышь и другие устройства вполне можно считать имитацией осязания. Предполагается, что в ближайшие годы персональный компьютер научится работать с запахами и близкими к запахам по механизму восприятия вкусами.

По техническим причинам буквально воссоздать человеческие органы обоняния с помощью искусственных средств сегодня невозможно. Поэтому работа органов обоняния моделируется чаще на основе оптической, а не электрохимической модели. При этом важную роль играет протекание оптических процессов в исследуемых газовых средах и соотношение спектральных интенсивностей различных оптических линий. Особого внимания заслуживают методы инициации специфичных оптических процессов, позволяющие проявить особенности отдельных категорий запахов. Извлекаемая сложная оптическая информация классифицируется по оптическим моделям наборов запахов с помощью трудоёмкой компьютерной обработки.

Мультимедиа технологии - возможность представления информации пользователю

во взаимодействии различных форм (текст, графика, анимация, звук, видео) в интерактивном режиме.

Технологию мультимедиа составляют специальные аппаратные и программные средства.

Мультимедиа-продукты можно разделить на несколько категорий в зависимости от того, на какие группы потребителей они ориентированны.

С начала 90-х годов средства мультимедиа развивались и совершенствовались, став к началу XXI века основой новых продуктов и услуг, таких как электронные книги и газеты, новые технологии обучения, видеоконференции, средства графического дизайна, голосовой и видеопочты. Применение средств мультимедиа в компьютерных приложениях стало возможным благодаря прогрессу в разработке и производстве новых микропроцессоров и систем хранения данных.

Нажатием кнопки пользователь компьютера может заполнить экран текстом; нажав другую, он вызовет связанную с текстовыми данными видеоинформацию; при нажатии следующей кнопки прозвучит музыкальный фрагмент. Например, Bell Canada, предоставляющая услуги общественной, личной и коммерческой связи для всей Канады, использует средства мультимедиа для выявления и устранения неполадок в телефонной сети. Специальные программы содержат тысячи отсканированных руководств по ремонту техники, которые предоставлены в пользование сотрудникам отделов технического обеспечения и аналитикам. Каждая мультимедийная рабочая станция может отобразить любой участок схемы сети. При обнаружении неисправности подается звуковой сигнал и показывается место, где произошла авария. Также система может отослать по электронной почте или факсу всю необходимую информацию бригаде ремонтников, выезжающей на объект. Система голосового сопровождения позволяет прослушивать информацию и комментарии, необходимые для диагностики и анализа в случае возникновения аварийной ситуации.

Несомненным достоинством и особенностью технологии являются следующие возможности мультимедиа, которые активно используются в представлении информации:

- возможность хранения большого объема самой разной информации на одном носителе (до 20 томов авторского текста, около 2000 и более высококачественных изображений, 30-45 минут видеозаписи, до 7 часов звука);
- возможность увеличения (детализации) на экране изображения или его наиболее интересных фрагментов, иногда в двадцатикратном увеличении (режим "лупа") при сохранении качества изображения. Это особенно важно для презентации произведений искусства и уникальных исторических документов;
- возможность сравнения изображения и обработки его разнообразными программными средствами с научно- исследовательскими или познавательными целями;
- возможность выделения в сопровождающем изображение текстовом или другом визуальном материале "горячих слов (областей)", по которым осуществляется немедленное получение справочной или любой другой пояснительной (в том числе визуальной) информации (технологии гипертекста и гипермедиа);
- возможность осуществления непрерывного музыкального или любого другого аудиосопровождения, соответствующего статичному или динамичному визуальному ряду;

- возможность использования видеофрагментов из фильмов, видеозаписей и т.д., функции "стоп-кадра", покадрового "пролистывания" видеозаписи;
- возможность включения в содержание диска баз данных, методик обработки образов, анимации (к примеру, сопровождение рассказа о композиции картины графической анимационной демонстрацией геометрических построений ее композиции) и т.д.;
- возможность подключения к глобальной сети Internet;
- возможность работы с различными приложениями (текстовыми, графическими и звуковыми редакторами, картографической информацией);
- возможность создания собственных "галерей" (выборок) из представляемой в продукте информации (режим "карман" или "мои пометки");
- возможность "запоминания пройденного пути" и создания "закладок" на заинтересовавшей экранной "странице";
- возможность автоматического просмотра всего содержания продукта ("слайд-шоу") или создания анимированного и озвученного "путеводителя-гида" по продукту ("говорящей и показывающей инструкции пользователя"); включение в состав продукта игровых компонентов с информационными составляющими;
- возможность "свободной" навигации по информации и выхода в основное меню (укрупненное содержание), на полное оглавление или вовсе из программы в любой точке продукта.

Появление систем мультимедиа, безусловно, производит революционные изменения в таких областях, как образование, компьютерный тренинг, во многих сферах профессиональной деятельности, науки, искусства, в компьютерных играх и т.д.

Возможности технологии мультимедиа безграничны. В бизнес-приложениях мультимедиа в основном применяются для обучения и проведения презентаций. Благодаря наличию обратной связи и живой среде общения, системы обучения на базе мультимедиа обладают потрясающей эффективностью и существенно повышают мотивацию обучения. Уже давно появились программы, обучающие пользователя иностранным языкам, которые в интерактивной форме предлагают пользователю пройти несколько уроков, от изучения фонетики и алфавита до пополнения словарного запаса и написания диктанта. Благодаря встроенной системе распознавания речи, осуществляется контроль произношения обучаемого. Пожалуй, самая главная особенность таких обучающих программ – их ненавязчивость, ведь пользователь сам определяет место, время и продолжительность занятия.

3.1.Аппаратные средства создания проектов

Для построения мультимедиа системы необходима дополнительная аппаратная поддержка: аналогоцифровые и цифроаналоговые преобразователи для перевода аналоговых аудио и видео сигналов в цифровой эквивалент и обратно, видеопроцессоры для преобразования обычных телевизионных сигналов к виду, воспроизводимому электронно лучевой трубкой дисплея, декодеры для взаимного преобразования телевизионных стандартов, специальные интегральные схемы для сжатия данных в файлы допустимых размеров и так далее. Все оборудование отвечающее за звук объединяются в так называемые звуковые карты, а за видео в видео карты. Дальше рассматривается подробно и в отдельности об устройстве и характеристиках звуковых карт, видео карт и CD-ROM приводах.

Аппаратные средства мультимедиа:

- Средства звукозаписи;
- Звуковоспроизведении;

- Манипуляторы;
- Средства «виртуальной реальности»;
- Носители информации (CD-ROM);
- Средства передачи;
- Средства записи;
- Обработки изображения;

Звуковые карты

С течением времени перечень задач выполняемых на ПК вышел за рамки просто использования электронных таблиц или текстовых редакторов. Компакт- диски со звуковыми файлами, подготовка мультимедиа призентаций, проведение видео конференций и телефонные средства, а также игры и прослушивание аудио CD для всего этого необходимо чтобы звук стал неотъемлемой частью ПК. Для этого необходима звуковая карта. Любители игр будут удовлетворены новыми возможностями объемного звучания.

Для звуковых карт IBM совместимых компьтеров прослеживаются следующие тенденции:

Во-первых, для воспроизведения звука вместо частотной модуляции (FM) теперь все больше используют табличный (wavetable) или WT синтез, сигнал полученный таким образом, более похож на звук реальных инструментов, чем при FM синтезе. Используя соответствующие алгоритмы, даже только по одному тону музыкального инструмента можно воспроизводить все остальное, то есть восстановить его полное звучание. Выборки таких сигналов хранятся либо в постоянно запоминающем устройстве (ROM) устройства, либо программно загружается в оперативную память (RAM) звуковой карты.

В более дешевых платах чаще реализован частотно модулированный синтез с использованием синусоидальным колебаний что в результате при водит к несовсем точному звучанию инструментов, отражение звука и рева, характерных для последнего поколения игр в игровых залах. Расположенная на плате микросхема для волнового синтеза хранит записанные заранее оцифрованные образцы (Samples) звучания музыкальных инструментов и звуковых эффектов. Достигаемые результаты очевидны музыкальные записи получаются более убедительны, а азартные игроки более впечатлительны.

Пионером в реализации WT синтеза стала в 1984 году фирма Ensoning. Вскоре WT синтезаторы стали производить такие известные фирмы, как Emu, Korg, Roland и Yamaha.

Фирмы производители звуковых карт добавляют WT синтез двумя способами либо встраивают на звуковую карту в виде микросхем, либо реализуя в виде дочерней платы. Во втором случае звуковая карта дешевле, но суммарная стоимость основной и дочерней платы выше.

Во-вторых, это совместимость звуковых карт. За сравнительно не долгую историю развития средств мультимедиа появилось уже несколько основных стандартов де-факто на звуковые карты. Так почти все звуковые карты, предназначенные для игр и развлечений, поддерживают совместимость с Adlib и Sound Blaster. Все звуковые карты, ориентированные на бизнес- приложения, совместимы обычно с MS Windows Sound Sistem фирмы Microsoft.

В третьих, одним из компонентов современных звуковых карт стал сигнальный процессор DSP(Digital Signal Processor) к возможности функциональным обязанностям этого устройства можно отнести: распознание речи, трехмерное звучание, WT синтез, сжатие и

декомпресия аудиосигналов. Количество звуковых карт, оснащенных DSP, не так велико. Причина этого то что такое достаточно мощное устройство помогает только при решении строго определенных задач.
Как правило DSP устройство достаточно дорогое, поэтому сразу устанавливается только на профессиональных музыкальных картах. Одним из мощных DSP производителей сейчас является фирма Texas Instruments.

В-четвертых, появилась устойчивая тенденция интегрирования функций звуковых карт на системной плате. Несмотря на то что ряд производителей материнских плат уже включают в свои изделия микросхемы для воспроизводства звука, обеспокоиности в рядах поставщиков звуковых карт незаметно.

Потенциальная проблема при использовании встроенных средств обработки звука состоит в ограниченности системных ресурсов IBM PC совместимых компьютеров, а именно в возможности конфликтов по каналам прямого доступа к памяти (DMA). Пример такой платы это системная плата OPTi495 SLC, в которой используется 16-разрядный звуковой стереокодек AD 1848 фирмы ANALOG DEVICES.

В пятых, стремление к более естественному воспроизведению звука заставляет фирмы производителей использовать технологии объемного или трехмерного (3D) звучания. Самое модное направление в области воспроизведения звука в наши дни предоставляет так называемые объемность звучания. Применение этих эффектов объемного звучания позволяет расширить стереопространство что в свою очередь придает большую глубизну ограниченного поля воспроизведения присущем не большим близко расположенным друг к другу колонок.

В шестых, это подключение приводов CD-ROM. Практически все звуковые карты имеют встроенные интерфейсы для подключения приводов CD-ROM одной или сразу всех трех фирм Sony, Panasonic/Matsushita и Mitsumi.Тем не менее большинство звуковых карт рассчитано на подключение приводов Sony.

Появились карты и приводы поддерживающие стандартный интерфейс ATA(IDE), используемый для компьютеров с винчестером.

В седьмых, на картах используется режим DualDMA то есть двойной прямой доступ к памяти. С помощью двух каналов DMA можно реализовать одновременно запись и воспроизведение.

И последние это устойчивое внедрение звуковых технологий в телекомуникации. Звуковые карты приобретаются в 90% случаев для игр, из оставшихся 10% для речевого сопроваждения мультимедиа программ. В таком случае потребительские качества зависят только от ЦАП (цифро-аналогового преоброзователя) и от усилителя звуковой частоты. Еще более важным является совместимость со стандартом Sound Blaster, так как далеко не все программы будут поддерживать менее распространенные стандарты.

В набор Звуковых карт входят драйвера, утилиты, программмы записи и воспроизведения звука, средства для подготовления и произведения презентаций, энциклопедий, игр.

Воспроизведение звука

Современноые средства мультимедиа дают качество стереозвука, удовлетворяющее самым придирчивым требованиям HiFi (сокращенно это означает высокую верность

воспроизведения). Современные платы синтеза звука способны синтезировать звучание одновременно 20 и более музыкальных инструментов, создавая при этом множество специальных звуковых эффектов - плавное изменение громкости каждого инструмента, вибрацию звуков, их модуляцию по частоте и т.д. Появилась возможность записи звуковых сигналов на магнитные носители ПК в виде файлов и их сложной математической обработки - например наложения сигналов, фильтрации шумов и т.д.

Сейчас HiFi-звучание неразрывно связано с лазерными аудиодисками (или компакт-дисками CD), использующими цифровые методы кодирования звуковых сигналов. Диск представляет из себя пластмассовый кружок, на поверхности которого имеются микроскопические углубления, созданные записывающим устройством (точнее говоря, технологическим процессом тиражирования дисков с некоторого оригинала). Они покрыты "толстым" слоем прозрачного лака, предохраняющим поверхность диска от повреждений. Рабочей является только одна поверхность, вторая используется для красочной маркировки.

Для проигрывания диска используется полупроводниковый лазерный диод с фокусирующей оптической системой. Область диска под лаком с микроуглублениями находится в фокусе, и отраженный от нее сигнал воспринимается фотодиодом, расположенным рядом с лазерным излучателем. Диск вращается с переменной скоростью, что дает постоянную линейную скорость считывания данных. Наружняя поверхность диска находится не в фокусе. Поэтому ее загрязнения и даже царапины практически не влияют на воспроизведение. Тем более что специальная электронная система коррекции ошибок устраняет их проникновение в данные. Тряска, вибрация и магнитные поля - бичь граммофонных проигрывателей и магнитофонов - на работу дисковых проигрывателей практически не влияют.

Сигнал фотодиода имеет форму импульсов. Для работы прогрывателя важно лишь наличие или отсутствие импульса - т.е. логический 0 или 1. Ну прямо как в компьтере, скажете вы и будете правы. Оптический диск как бы идеально подходит для создания ПЗУ (ROM) компьютера с огромной емкостью. Но история распорядилась по иному - такой диск был вначале задуман как средство цифровой записи звука для обычных целей HiFi-звуковоспроизведения. И лишь в начале 90-х годов он стал использоваться для записи компьютерных данных и программ в связи с практической реализацией идей мультимедиа.

В основе цифровой записи лежит представление мгновенного значения звукового сигнала его численным значением. Оно дискретное, т.е. выражается целым числом. Звуковой сигнал обычно имеет аналоговое (непрерывное) представление. И чтобы представить его в числовой форме, надо провести дискретизацию сигнала, представив его конечным числом уровней. Для HiFi-звуковоспроизведения в первом приближении хватает 65536 ступенек цифрового представления мгновенного значения цифрового сигнала. Это означает, что достаточно иметь 16 разрядов аналого-цифрового преобразования звукового сигнала. Первые платы звука ПК имели разрядность преобразования 8 и квантовали звуковой сигнал 128 ступеньками уровня. Это, конечно, было явно недостаточно для HiFi- звуковоспроизведения.

Итак, важный параметр звуковых плат мультимедиа (аудиоадаптеров) - разрядность их аналого-цифрового преобразователя (АЦП). Другой не менее важный параметр - частота квантования. Сколько дискретных значений сигнала надо получить за период сигнала? На этот вопрос можно ответить точно, если сигнал является периодическим - например всем знакомой синусоидой.

Чтобы можно было принципиально судить о величине (амплитуде) синусоидального сигнала, мы должны взять минимум две его выборки в моменты времени, соответствующие максимуму и минимуму синусоиды. По этим двум значениям с помощью фильтра можно восстановить синусоиду. Естественно, что синусоида с большим периодом представляется уже множеством выборок, что дает лучшее приближение. Восстановление аналогового представления сигнала по его цифровому выполняется с помощью цифро-аналоговых преобразователей (ЦАП) и фильтров, подавляющих шумы квантования, расположенные в области высоких частот.

Манипуляторы

Простым, удобным и популярным средством для управления компьютером является мышь. Это устройство с проводом по внешнему виду и характеру перемещений действительно похоже на мелкое животное, в честь которого оно названо. Однако в отличие от вредного грызуна компьютерная мышь – весьма полезное устройство ввода информации в компьютер, позволяющее во многих случаях практически полностью заменить громоздкую клавиатуру. И это при том, что мышь имеет всего две-три клавиши, а используют из них обычно одну.

Разнообразные применения мышки основаны на преобразовании направления и скорости перемещения кисти руки в управляющие сигналы. Водит пользователь мышкой по коврику взад-вперёд и вправо-влево, изредка нажимая при этом пальцем на клавишу – а компьютер выполняет задаваемые этими действиями операции. Конечно же, мышь по своей сути – вследствие простоты управления компьютером, чем клавиатура, хотя они и не всегда взаимозаменяемы. Особенно удобно работать мышью с графическими программами и с таблицами. Мышь может иметь две или три кнопки. Чувствительность мыши характеризующей разрешающей способностью. В некоторых ситуациях оказывается удобным работать ножной мышью. Такая мышь представляет собой две педали для ног, одна из которых управляет перемещением курсора, а другая заменяет кнопки. Конечно же, не каждый сможет столь же ловко управляться с ножной мышью, как с ручной. Однако неоспоримым достоинством ножной мыши является то, что она позволяет высвободить руки для более важных занятий. И совсем незаменимой она становится тогда, когда руками невозможно воспользоваться из-за болезни или по другим обстоятельствам.

Существуют не только механические мышки, но и оптические, в которых направление и скорость движения определяется по отражению света от специального коврика. Бывают беспроводные мышки и даже миниатюрные беспроводные мышки, которые при работе одевают на палец как перстень.

Шаровой манипулятор выполняет ту же работу, что и мышь. Да и внешне он выглядит как механическая компьютерная мышь, перевёрнутая на спину. Шарик, по которому ездит мышь и который находится у неё внизу, у манипулятора расположен на виду – сверху. Он вмонтирован обычно в корпус компьютера или в клавиатуру. Для управления компьютером этот шарик вращают в разных направлениях пальцами. Рядом с шариком размещены клавиши манипулятора.

Одни люди предпочитают работать мышью, другие – шаровым манипулятором. Манипулятор более точен, чем мышь, поскольку шарик в нём крупнее, да и вращают его более чувствительными пальцами, а не грубой кистью.

Если компьютер используется для игровых и тренажёрных задач, а также в некоторых случаях, то для управления перемещением объекта по экрану удобно пользоваться специальной ручкой, имеющей название джойстик – в буквальном переводе палочка радости. Эта ручка похожа на одну из ручек пилота в кабине самолёта. Впрочем, джойстиком называют не только ручку, но и другие конструктивные варианты устройства со сходными функциями. Придумали даже джойстик, с которым можно работать на весу, похаживая по комнате. Джойстик применяется во многих играх с примитивным сюжетом. Простейший джойстик по принципам действия похож на клавиши. И возможности его близки к возможностям клавиатуры. В такой ситуации опытный пользователь может предпочесть клавиатуру, а новичку более привычным может показаться джойстик. Более интересные возможности открывает джойстик с пропорциональным управлением, при котором скорость перемещения рукоятки джойстика пропорциональна скорости перемещения.

Современные джойстики делят на пять конструктивных вариантов. Они могут быть выполнены в виде самолётной ручки управления или штурвала, а также бывают кнопочными, настольными и комбинированными.

Виртуальная реальность

- Очки виртуальной реальности.

Самые ранние - это красно-синие очки. В игровой индустрии применяются они не часто, т.к. игру с самого начала надо делать под них. И, что отрадно, игра не требует мощных систем: отлично идёт на P133&16 Мб RAM. Существуют и более сложные очки. Принцип их действия заключается в следующем. На экран выводится изображение для одного глаза в тот момент, когда очки затемняют другой. И, поочередно показывая для каждого глаза свое изображение, очки создают иллюзию трехмерности изображения на экране. Такой тип очков наиболее распространен и прилагается к некоторым видеокартам.

Более современными являются EyeScream от Wicked3D и Crystal Eyes от Stereographics. Первые более распространены, вторые более профессиональны. Ниже вы видите рисунки CrystalEyes (High- end) и CrystalEyes Wired (базовый уровень).

Есть множествьо других фирм по производству очков ВР, в этом реферате приведены лишь некоторые из них.

При использовании "метода затемнения одного глаза" нужно помнить, что для создания такого изображения необходима вдвое большая частота обновления экрана, т.к. система для каждого глаза обрабатывает отдельную камеру, и для каждого глаза выводится свое, невидимое для другого изображение. Так что, если частота регенерации изображения 80 Гц, то для каждого глаза в отдельности она будет лишь 40 Гц. Для наиболее комфортного использования таких очков надо вастaвлять частоту около 160-170 Гц.

- Виртуальные бинокли.

Эти приспособления уже не просто затемняют поочередно глаза, а сами выводят изображения для каждого глаза. Основа биноклей - активные LCD-матрицы с углом обзора 30-60 градусов. Появились они на рынке сравнительно недавно и не успели завоевать доверие у широких масс. Сегодня можно купить такие бинокли как V6 и V8 от Virtual Research Systems, Virtual Binoculars (VB) от n- Vision, а также и у нескольких других фирм. Как видите выгледят ВР-бинокли все на одно лицо (VB, V8).

Изображение в V8 обеспечивается 1.3" ЖК матрицами, разрешение ((640x3)x480), но частота регенерации изображения низкая - 60 Гц, т.е. по 30 на каждый глаз. К сожалению, техника еще не достигла нужного уровня для безопасной работы.

- VR-шлем (Head-Mounted-Display, HMD).

Этот тип устройств наиболее распространен и известен. Принцип действая такой же, как иу биноклей: фиксирование изображения для каждого глаза. Производство ВР шлемов началось давно, первыми моделями были Vfx1 и CyberFX. Первый, наиболее известный, обладает разрешением 789x230 (181,470) пикселей, отслеживанием поворотов головы на 45 градусов по вертикали и 360 по горизонтали. Сегодня он стоит $600 (с карточкой + $150), а CyberFX $100.

Естественно, они были несовершенны с точки зрения гигиены и качества. Позднее появился несколько улучшеный Vfx3D. Он снабжен 0.7" активно-матричными ЖК дисплеями, обеспечивающими частоту регенерации 75 Гц в разрешении 640x480, 70 Гц для разрешения 800x600 и 62.5 Гц при разрешении 1024x768. Система отслеживания положения головы (position tracker) имеет чувствительность 0.5° при допустимом 70-градусном отклонении вверх/вниз и 0.1-градусную чувствительность во всей горизонтальной плоскости

(360°). Фокус расположен на расстоянии 3.35 метра, что препятствует быстрому утомлению глаз. Интерфейс шлема предусмаотрен для платформ Silicon Graphics, Macintosh и PC (USB-порт).
Производством HMD занимаются многие зарубежные фирмы. n-Vision, сотрудничащая с SGI, предлагает шлема VR со специфическим дизайном. Но, несмотря на это, они отличаются высокими технологическими характеристиками. Вот, например, Datdvisor 80-легкий VR-шлем из пластика, отличающийся 120-градусной свободой вертикального вращения.

- 3D панели.

Эти устройства можно сравнить с VR-очками, но с тем отличием, что они одеваются на монитор. При использованием 3D панелей изображение на обычном мониторе обретает глубину, правда есть одно ограничение: диагональ дисплея должна быть 17 или 21 дюйм.

- 3D звук.

Существует несколько технологий создания 3D-звука. У Creative это EAX, у Aureal - A3D, у Microsoft это DirectSound3D, реализованный в библиотеках DirectX. Все они позволяют воспроизводить настолько реалистичный звук, что его трудно отличить от настоящего. Поэтому для более глубокого погружения в виртуальные миры все HMD снабжены наушниками. Сейчас ими стали снабжать и некоторые стереоочки.

Трехмерный звук заставляет воспринимать игру по-другому. Ощущения становятся настолько реалистичными... эти голоса и выстрелы в тонелях и трубах меняются при выходе на открытые пространства, переливаются на ветру... в общем лучше один раз услышать, чем сто раз прочитать.

- Vr - перчатки.

Пока что перчатки для виртуальной реальности не заняли таких прочных позиций, как некоторые очки. Их технологии еще слишком дороги для развлечений, хотя и могут быт доступны в некоторых виртуальных залах от Electronic Visualization Lab. Хотя чаще всего они используются не для игр.

Отслеживать движения пальцев им помогает сложная система эластичных световодов и пара десятков датчиков. Как только палец начинает сгибаться, световод сужает просвет, а датчики улавливливают падение интенсивности света на каком-либо участке. Адекватно этим изменениям ведет себя кисть в виртуальном пространстве. Естественно, эта технология разработана больше для научных исследований, нежели для игр. Посудите сами: зачем в 3DAction'e (тем более в RTS) отслеживать движения пальцев?

Есть и технология с механическими датчиками, но она тяжела и несовершенна.

- Датчики кисти.

Помимо перчаток существуют и другие устройства слежения за перемещениями кисти. В самые простые встроен только position tracker, отслеживающий перемещения небольшого кубика, который нужно держать в одной из рук. По сравнению с остальной продукцией это устройство стоит дешево-от 20 до 40 долларов.

Производством таких датчиков занимается фирма Ascension Technology Corporation.

- VR-костюм.

Самым полным набором оборудования для виртуальной реальности является виртуальный костюм. Он состоит из обтягивающего комбинезона со множеством магнитных сенсоров, которые отслеживают движения всех частей тела. К нему добавляется HMD, датчик(и) кисти (реже перчатка) и провода для присоединения всего этого к компьютеру. Тогда уж точно будет полный комплект ощущений. Единственное, чего не хватает, так это ForceFeedback VR-костюмов. Хотя кто знает, может, работы по созданию таких кстройств уже ведутся?

- Перспективные устройства.

В лекции не рассмотрены устройства имитации обоняния и вкуса. Насчет последнего не знаю, а вот примитивное устройство имитации обоняния уже известно. Оно состоит из системы химических аэрозолей, смешивающихся при необходимости. У подопытных сперва было ощущение восторга, а потом совсем небыло ощущений. Дело в том, что химический состав балончиков не безвреден - он притупляет чувствительность нашего носа. Поэтому первое время люди, испытавшие на себе это чудо техники, совсем не различали запахи. А создатели даже и предположить не могли о таком побочном эффекте. Мне кажется эти устройства уже лишние: кому интересно испытать полноту ощущений в канализации или на свалке?

Технологии виртуальной реальности сегодня очень быстро развиваются. Сама ВР применяется во многих сферах жизни. Роботы, которыми управляет человек из виртуальной реальности, выполняют опасную или тонкую работу. Для создания игр широко применяется технология Motion Capture, позволяющая "снять" движения с человека и присвоить их трехмерной модели. К примеру, этот метод применялся в некоторых играх благодаря чему мы можем видеть и крадущегося вора, и танцующих скелетов. Та же технология исползуется и при оживлении рисованных персонажей в голивудских фильмах. Ну и наконец виртуальная реальность может использоваться для развлечений, ведь она помогает представить себя в другой роли и в другом обличии. Кто бы отказался поплавать рыбкой в коралловых рифах? Или воспарить птицей над небесами?

Все это заставляет стремительно развиваться VR-технологии. Многие из них стоят больших денег, но кто знает, может быть описаные в статье устройства завтра станут обыденностью, а затем и вовсе вытеснятся новыми.

Лазерные диски, CD-ROM

В связи с ростом объемов и сложности прграмного обеспечения, широким внедрением мультимедиа приложений, сочетающих движущиеся изображения, текст и звук, огромную популярность в последнее время приобрели устройства для чтения компакт- дисков CD-ROM. Эти устройства и сами диски, относительно недорогие, очень надежны и могут хранить весьма большие объемы информации (до 650 Мбайт), поэтому они очень удобны для поставки программ и данных большего объема, например каталогов, энциклопедий, а также обучающихся, демонстрационных и игровых программ. И многие программы полностью или частично поставляются на CD-ROM.

История развития. Компакт- диски изначально разработанные для любителей высоко качественного звучания, прочно вошли на рынок компьютерных устройств. Оптические компакт- диски перешли на смену виниловым в 1982 году. Было решено что стандарт рассчитан на 74 минуты звучания "Red Book". Когда 74 минуты пересчитали в байты получилось 640 Мбайт.

Первые приводы имели единичную скорость (Single speed) равную 150 Кбайт/с. Модели накопителей с удвоенной скоростью появились в 1992 году. Приводы с утроенной и с учетверенной скоростью в начале 1994 году. Сегодня речь уже идет о скорости увеличенной в шесть и даже восемь раз. Коэффициент увеличения скорости не обязательно целый.

Принцип действия. Как и в компакт-дисках, применяемых в бытовых CD-плейерах, информация на компьютерных компакт-дисках кодируется посредством чередования отражающих и не отражающих свет участков на подложке диска. При промышленном производстве комакт-дисков эта подложка выполняется из алюминия, а не отражающие свет участки делаются с помощью продавливания углублений в подложке специальной пресформой. При единичном производстве компакт-дисков (так называемых CD-R дисков, см. ниже) подложка выполняется из золота, а нанесение информации на нее осуществляетя лучом лазера. В любом случае сверху от подложки на компакт-диске находится прозрачное покрытие, защищающее занесенную на компакт-диск информацию от повреждений.

Хотя по внешнему виду и размеру используемые в компьютерах компакт-диски не отличаются от дисков, применяемых в бытовых CD плейерах, однако компьютерные устройства для чтения компакт-дисков стоят существенно дороже. Это не удивительно, ведь чтение программ и компьютерных данных должно выполняться с гораздо высокой надежностью, чем та, которая достаточна при воспроизведении музыки. Поэтому чтение используемых в компьютере компакт-дисков осуществляется с помощью луча лазера небольшой мощности. Использование такой технологии позволяет записывать на компакт-диски очень большой объем информации (650 Мбайт), и обеспечивает высокую надежность информации.

Однако скорость чтения данных с компакт-дисков значительно ниже, чем с жестких дисков. Одна из причин этого состоит в том, что компакт-диски при чтении вращаются не с постоянной угловой скоростью, а так, чтобы обеспечить неизменную линейную скорость отхождения информации под читающей головкой. Стандартная скорость чтения данных с компакт-дисков всего 150-200 Кбайт/с, а время доступа 0,4 с. Впрочем, в последнее время выпускаются в основном устройства с двойной, тройной и даже четвертой скоростью вращения, они обеспечивают соответственно более высокие скоростные показатели: время доступа 0,2-0,3 с, скорость считывания 500 Кбайт/с. Заметим, однако, что устройства с тройной скоростью в реальных задачах увеличивают скорость работы с компакт-диском не в полтора и не в два раза по сравнению с устройством с двойной скоростью, а всего на 30 - 60%.

Видеокарты

При смешении сигналов основные проблемы возникают с видео–изображением. Различные ТВ–стандарты, существующие в мире (NTSC, PAL, SECAM), применение разных мониторов и видеоконтроллеров диктует разнообразие подходов в разрешении возникающих проблем. Однако в любом случае требуется синхронизация двух изображений, для чего служит устройство *генлок (genlock).* С его помощью на экране монитора могут быть совмещены изображение, сгенерированное компьютером (анимированная или неподвижная графика, текст, титры), и “живое” видео. Если добавить еще одно устройство — *кодер (encoder),* компьютерное изображение может быть преобразовано в форму ТВ–сигнала и записано на видеопленку. "Настольные видео–студии”, являющиеся одним из примеров применения систем мультимедиа, позволяют готовить совмещенные видео–компьютерные клипы, титры для видеофильмов, помогают при монтаже кинофильмов.

Системы такого рода не позволяют как-то обрабатывать или редактировать само аналоговое изображение. Для того, чтобы это стало возможным, его необходимо оцифровать

и ввести в память компьютера. Для этого служат так называемые *платы захвата (capture board, frame grabbers).* Оцифровка аналоговых сигналов порождает огромные массивы данных. Так, кадр стандарта NTSC (525 строк), преобразованный платой типа Truevision, превращается в компьютерное изображение с разрешением 512x482 пиксель. Если каждая точка представлена 8 битами, то для хранения всей картинки требуется около 250 Кбайт памяти, причем падает качество изображения, так как обеспечивается только 256 различных цветов. Считается, что для адекватной передачи исходного изображения требуется 16 млн. оттенков, поэтому используется 24-битовый формат хранения цветной картинки, а необходимый размер памяти возрастает. Оцифрованный кадр может затем быть изменен, отредактирован обычным графическим редактором, могут быть убраны или добавлены детали, изменены цвета, масштабы, добавлены спецэффекты, типа мозаики, инверсии и т.д. Естественно, интерактивная экранная обработка возможна лишь в пределах разрешения, обеспечиваемого данным конкретным видеоадаптером. Обработанные кадры могут быть записаны на диск в каком–либо графическом формате и затем использоваться в качестве реалистического неподвижного фона для компьютерной анимации. Возможна также покадровая обработка исходного изображения и вывод обратно на видеопленку для создания псевдореалистического мультфильма.

Запись последовательности кадров в цифровом виде требует от компьютера больших объемов внешней памяти: частота кадров в американском ТВ–стандарте NTSC — 30 кадров/с (PAL, SECAM — 25 кадров/с), так что для запоминания одной секунды полноцветного полноэкранного видео требуется 20–30 Мбайт, а оптический диск емкостью 600 Мбайт вместит менее полминуты изображения. Но последовательность кадров недостаточно только запомнить, ее надо еще вывести на экран в соответствующем темпе. Подобной скоростью передачи информации — около 30 Мбайт / с — не обладает ни одно из существующих внешних запоминающих устройств. Чтобы выводить на экран компьютера оцифрованное видео, приходится идти на уменьшение объема передаваемых данных, (вывод уменьшенного изображения в небольшом окне, снижение частоты кадровой развертки до 10–15 кадров / с, уменьшение числа бит / пиксель), что, в свою очередь приводит к ухудшению качества изображения.

Более радикально обе проблемы — памяти и пропускной способности — решаются с помощью методов сжатия / развертки данных, которые позволяют сжимать информацию перед записью на внешнее устройство, а затем считывать и разворачивать в реальном режиме времени при выводе на экран. Так, для движущихся видео–изображений существующие адаптивные разностные алгоритмы могут сжимать данные с коэффициентом порядка 100:1— 160:1, что позволяет разместить на CD–ROM около часа полноценного озвученного видео. Работа этих алгоритмов основана на том, что обычно последующий кадр отличается от предыдущего лишь некоторыми деталями, поэтому, взяв какой–то кадр за базовый, для следующих можно хранить только относительные изменения. При значительных изменениях кадра, например, при монтажной склейке, наезде или панорамировании камеры,

автоматически выбирается новый базовый кадр. Для статических изображений коэффициент сжатия, естественно, ниже — порядка 20–30:1. Для аудиоданных применяют свои методы компрессии.

При использовании специальных видео–адаптеров (видеобластеров) мультимедиа–ПК становятся центром бытовой видео–системы, конкурирующей с самым совершенным телевизором.

Новейшие видеоадаптеры имеют средства связи с источниками телевизионных сигналов и встроенные системы захвата кадра (компрессии / декомпрессии видеосигналов) в реальном масштабе времени, т.е. практически мгновенно. Видеоадаптеры имеют быструю видеопамять до 512 Мбайт и специальные графические 3D-ускорители процессоры. Это позволяет получать до 100 кадров в секунду и обеспечить вывод подвижных полноэкранных изображений.

Имеется большое количество устройств, предназначенных для работ с видеосигналами на IBM PC совместимых компьютеров. Условно можно разбить на несколько групп: устройства для ввода и захвата видеопоследовательностей (Cupture play), фреймграбберы (Framegrabber), TV-тюнеры, преобразователи сигналов VGA-TV и др..

TVтюнеры

Эти устройства выполняются обычно в виде карт или бокса (небольшой коробочки). Они преобразуют аналоговый видеосигнал поступающий по сети кабельного телевидения или от антенны, от видеомагнитофона или камкодера (camcorder). TV-тюнеры могут входить в состав других устройств таких как MPEG-плейеры или фреймграбберы.

Некоторые из них имеют встроенные микросхемы для преобразования звука. Ряд тюнеров имеют возможность для вывода телетекста.

Фрейм грабберы

Появились примерно 8 лет назад . Как правило они объединяют графические, аналогово-цифровые и микросхемы для обработки видеосигналов, которые позволяют дискретизировать видеосигнал, сохранять отдельные кадры изображения в буфере с последующей записью на диск либо выводить их непосредственно в окно на мониторе компьютера. Содержимое буфера обновляется каждые 40 мс. то есть с частотой смены кадров. Вывод видеосигналов происходит в режиме наложения (overby). Для реализации окна на экране монитора с "живым" видео карта фреймграббера соединена с графическим адаптером через 26 контактный Feature коннектор. С ним обычно поставляется пакет Video for Windows вывод картинки размером 240*160 пикселов при воспроизведении 256 цветов и больше. Первые устройства Video Blaster, Video Spigot.

Преобразователи VGA-TV

Данные устройства транслируют сигнал в цифровом образе VGA изображения в аналоговый сигнал пригодный для ввода на телевизионный приемник. Производители обычно предлагают подобные устройства выполненные либо как внутренние ISA карта либо как внешний блок.
Ряд преобразователей позволяют накладывать видеосигнал например для создания титров. При этом осуществляется полная синхронизация преобразованного компьютерного сигнала по внешнему(gtnlok). При наложении формируется специальный ключевой (key) сигнал трех видов lumakey, chromakey или alpha chenol.

1. В первом случае наложение производится там где яркость Y превышает заданного уровня.
2. Накладывание изображения прозрачно только там где его цвет совпадает с заданным.
3. Альфа канал используется в профессиональном оборудовании основанном на формировании специального сигнала с простым распределением, который определяет степень смещения видеоизображения в различных точках.

MPEG-плейеры

Данные устройства позволяют воспроизводить последовательности видеоизображения (фильмы) записываемых на компакт- дисках, качеством VNS Скорость потока сжатой информации не превышает обычно 150 Кбайт/с.

Основная сложность задачи решаемой MPEG кодером, состоит в определении для каждого конкретного видеопотока оптимального соотнашения между тремя видами изображения: (I)ntra, (P)redicted и (B)idirectional. Первым MPEG -плейерам была плата Reel Magic компании Sigina Desing в 1993 году.

3.2.Программные средства создания проектов

Существует большое множество программных средств для разработки мультимедийных приложений. К сожалению, перечисление всех невозможно, остановимся только на наиболее распространенных программ. Их можно разделить на несколько категории:

- Средства создания и обработки изображения;
- Средства создания и обработки анимации, 2D, 3D – графики;
- Средства создания и обработки видеоизображения (видеомонтаж, 3D-титры);
- Средства создания и обработки звука;
- Средства создания презентации;

Графика и фотоизображения

Один из способов представления изображения в компьютере — растровая графика (bitmap). В этом случае изображение делится на элементы (pixels), которые определяют размер картинки — X пикселов по ширине и Y пикселов по высоте. Важной характеристикой является цветовое разрешение растровой графики, определяемое числом битов, используемых для кодирования цвета каждого пиксела (его называют также числом битовых плоскостей). Понятно, что чем больше битовых плоскостей в файле, тем больше места требуется на диске для его сохранения.

Существуют следующие варианты представления цвета в графических файлах:

- 256-цветный файл использует 8 бит на каждый пиксел и имеет соответствующую таблицу цветов, называемую палитрой.
- 16-битный цветной файл не использует палитру, а для сохранения красных, зеленых и синих цветовых компонентов каждого пиксела отводится 16 бит. Имеется два варианта: RGB555 (32768 цветов), RGB565 (65536 цветов).
- 24-битный цветной файл отводит по 8 бит для цветовых компонентов каждого пиксела. Использует 16,7 млн. возможных цветовых сочетаний, и поэтому самые маленькие отличия между ними могут быть едва замечены глазом.
- 32-битный цветной файл отводит по 8 бит для цветовых компонентов и 8 бит для альфа-канала каждого пиксела. Альфа-канал определяет уровень прозрачности каждого пиксела в изображении. Он используется программным обеспечением для применения масок, чтобы отображать видеоданные или изображения одно за другим.

Черно-белые полутоновые изображения могут быть записаны в 8-битный файл с 256 оттенками серого цвета (градации от белого до черного).

Другой способ представления — векторные изображения, которые сохраняются в виде геометрического описания объектов, составляющих рисунок. Эти изображения могут также

включать в себя данные в формате растровой графики. В векторных форматах число битовых плоскостей заранее не определено.

Графические редакторы ориентированы на манипулирование существующими изображениями (в основном сканированными) и обладают набором инструментов, позволяющих корректировать любой аспект изображения.

- Adobe Photoshop

Профессиональный пакет обработки фотографий. Поддерживает работу со слоями и экспорт объектов из программ векторной графики. Обладает полным набором инструментов для коррекции цвета, ретуширования, регулировки контрастности и насыщенности цветов, маскирования, создания различных цветовых эффектов. Более 40 фильтров позволяют создавать разнообразные специальные эффекты. Различными производителями создано множество подключаемых модулей.

- Corel PhotoPaint

Графический редактор, имеющий все необходимое для создания и редактирования изображений, однако уступает Adobe Photoshop в быстродействии при работе с файлами. Позволяет публиковать эти изображения в Интернете. Содержит инструменты для работы с анимированными изображениями и слайд-шоу в формате QuickTime.

- PhotoDraw

PhotoDraw входит в состав Office 2000 и объединяет возможности пакетов векторной и растровой графики. Он содержит большой набор рисованных фигур и множество типов линий для их оформления, включая разнообразные художественные мазки кистью либо фотоизображения. При использовании шаблонов специальный мастер проведет вас через все шаги создания иллюстрации необходимого типа. PhotoDraw поддерживает сохранение иллюстраций в формате большинства других приложений. Он включает большое количество различных эффектов, которые могут быть применены к изображениям и отдельным объектам, в частности можно выбирать эффекты добавления тени, задания прозрачности, смазывания или усиления границ объектов, придания им трехмерности, перспективных искажений, а также специальных эффектов, придающих изображению вид рисунка пером, наброска, живописного произведения и многих других. Предусмотрено применение plug-in фильтров, предназначенных для Photoshop.

- PhotoImpact

Графический пакет, разработанный фирмой Ulead Systems, предназначен не только для создания и редактирования изображений. Он предлагает также средства для создания и управления базами данных фотографий, просмотра файлов изображений, создания мультимедийных слайд-шоу, захвата изображения с экрана, преобразования файлов. Технология pick-and-apply позволяет применять расширения из наборов стилей, эффектов, градиентов и текстур, собранных в позиции меню Easy Palette, и сразу видеть результаты преобразований. Поддерживает работу со слоями, предварительный просмотр в реальном времени, расширенные специальные эффекты, размещение текста на заданной кривой, инструменты ретуширования изображения.

- Paint Shop Pro

Графический редактор, предоставляющий широкий выбор кистей для рисования и ретуширования изображения, более 25 стандартных фильтров для его обработки, базовый набор стандартных эффектов и подключаемые фильтры для пакета Photoshop. Поддерживает работу со слоями изображения и многоуровневую отмену действий. В его состав также включен Animation Shop — утилита для создания анимационных GIF-файлов, которые можно использовать в Интернете или в собственных мультимедиа-приложениях.

- Picture Man

Графический пакет, разработанный российской фирмой STOIK Software. Он позволяет создавать и редактировать графические файлы, монтировать и обрабатывать цифровое видео и даже имеет встроенный модуль морфинга. Пакет содержит более 70 высококачественных фильтров для работы с изображениями, инструменты цветокоррекции, фильтрации и ретуширования. Все фильтры пакета можно применить не только к одному изображению, но и к их последовательности.

- Painter

Программа редактирования растровой живописи фирмы Metacreations. Painter обладает достаточно широким спектром средств рисования и работы с цветом. В частности, он моделирует различные кисти (карандаш, ручка, уголь, аэрограф и др.), позволяет имитировать рисунки акварелью и маслом, а также добиться эффекта натуральной среды.

Существуют также рисовальные программы, которые моделируют традиционные инструменты и средства художников. Поддержка графических планшетов для ввода рисунков — главная особенность этих программ. Обычно они используются профессиональными художниками или пользователями, имеющими развитые художественные способности. Painter Classic считается одной из лучших программ для рисования кистями. Похожими свойствами обладает также Fauve Matisse.

2D-графика и анимация

В программах векторной графики объекты и изображения, которые сохраняются в виде геометрического описания, существуют независимо друг от друга, что позволяет в любой момент изменять слой, расположение и любые другие атрибуты объекта, создавая произвольную композицию. Современные программы векторной графики содержат также инструменты для работы с растровыми изображениями. Двухмерная анимация использует традиционный метод по кадровой анимации. В некоторых случаях используется твининг (tweening) — автоматическое генерирование промежуточных кадров. Применяется также морфинг, деформирование изображений, разнообразные оптические эффекты и циклическое изменение света.

- CorelDRAW

Графический редактор, обладающий широкими возможностями и огромной библиотекой готовых изображений, ставший уже классической программой векторного рисования. Пакет предназначен не только для рисования, но и для подготовки графиков и редактирования растровых изображений. Он имеет отличные средства управления файлами и возможность показа слайд-фильмов на дисплее компьютера, позволяет рисовать от руки и работать со слоями изображений, поддерживает спецэффекты, в том числе трехмерные, и имеет гибкие возможности для работы с текстами.

- CorelXARA

Позволяет создавать векторные изображения. Обладает прекрасно реализованным эффектом прозрачности с градиентными свойствами. Программа выполняет основные операции с растровыми изображениями: изменение глубины цвета, яркости, контраста, резкости, применения фильтра размытого изображения и других специальных эффектов. Огромное внутреннее разрешение (72 тыс. точек на дюйм) позволяет увеличивать объекты до 2500 раз. Позволяет просматривать файлы формата JPG, GIF и анимированные GIF. Совместима с plug-in для Adobe Photoshop.

- Macromedia FreeHand

Профессиональный графический редактор, позволяющий помимо создания графических объектов, также использовать и обрабатывать тексты, используя таблицы стилей, проверку правописания и способы размещения текста на странице. Позволяет использовать подключаемые модули. Содержит библиотеку спецэффектов и набор инструментов для работы с цветом, в том числе средства многоцветной градиентной заливки.

- Adobe Illustrator

Векторный пакет Illustrator фирмы Adobe предназначен для создания иллюстраций и разработки общего дизайна страниц и ориентирован на вывод готовых изображений с высоким разрешением. Пакет позволяет создавать фигуры и символы произвольной формы, а затем масштабировать, вращать и деформировать их. Кроме того, Illustrator содержит широкий спектр инструментов для работы с текстом и многостраничными документами.

- Deneba’s Canvas

Кроме создания векторной графики имеет модули для работы с растровыми изображениями и дизайна. Позволяет создавать фотомонтажи, оригинал-макеты изданий и Web-страницы, содержащие анимированные GIF-изображения и кнопки. Использует запатентованную Deneba’s технологию SpriteLayers и SpriteEffects.

- Photo Graphics

Использует объектно-ориентированный подход. Каждый объект представлен парой — регион и эффект, последний действует только в пределах региона. Объекты, расположенные в разных слоях, взаимодействуют, то есть эффект объекта верхнего слоя в пределах своего региона накладывается на объект нижнего слоя. При перемещении объекта эффект перемещается вместе с ним. Достоинством программы является малый размер файлов, в которых хранятся правила его построения изображений, а не информация о точках. Поэтому вывод может осуществляться с любым разрешением независимо от размера рисунка.

- GIF Animator

Программа анимации фирмы Ulead использует преимущества GIF-файлов для хранения нескольких изображений. В отличие от видео, при анимации для каждого изображения отдельно задается момент, место и длительность появления изображения на экране. Так как изображения могут иметь произвольные размеры, то можно создавать сложные композиции, собирая их из отдельных частей.

- Animation Shop

Анимационная программа фирмы Jasc Software. К одному или нескольким статическим изображениям можно применить различные эффекты и переходы для создания анимации. Animation Shop поддерживает различные графические форматы изображений. Встроенные мастера позволяют быстро создать анимацию, подобрать цвета и сохранить файл. Анимация сохраняется в файле (.gif) или собственном формате Animation files (.mng).

- paint* v2

Программа предназначена для создания, редактирования и анимации двухмерных изображений. Она содержит большое количество визуальных эффектов и комбинацию мощных инструментов анимации и различных эффектов перехода. Разрешение для каждого объекта независимо, поэтому результат можно сохранять в любой форме: видео, CD-ROM или Web.

- Macromedia Director

Программа Director позволяет создавать анимацию двумерных изображений, подготовить и отредактировать видео- и звуковой ряд, объединить все компоненты в одном видеоролике. Файл DIR, полученный в программе, может быть сжат с помощью функции Autobuffer и записан в формате DCR, который используется в Интернете. Такие файлы проигрываются с помощью специально подключаемого модуля.

- Animation Works Interactive

Пакет 2D-анимации Animation Works Interactive фирмы Gold Disk использует нетрадиционные и смешанные техники. Он позволяет импортировать растровые изображения, имеет хороший набор инструментов для работы с траекториями, а полученную анимацию может комбинировать со звуком и цифровым видео, применяя профессиональные эффекты.

- Animo

Пакет Animo фирмы Cambridge Animation Systems воспроизводит технику традиционной анимации “один к одному” и поэтому очень популярен среди профессиональных “некомпьютерных” мультипликаторов, в том числе российских.

- Tic Tac Toon

Еще одна из профессиональных программ двумерной анимации. Программа Tic Tac Toon фирмы ToonBoom для SGI имеет потенциал близкий к Animo.

- Elastic

Хорошим дополнением к анимационным программам является сплайновый пакет Elastic Reality фирмы ADSG, предназначенный для двумерных деформаций и превращений (морфинга) кино и видеоматериала. Пакет работает с замкнутыми и незамкнутыми кривыми, позволяет управлять степенью прозрачности объектов, сглаживать их контуры и применять спецэффекты.

3D-графика и анимация

Трехмерная анимация по технологии напоминает кукольную: необходимо создать каркасы объектов, определить материалы, их обтягивающие, скомпоновать все в единую сцену, установить освещение и камеру, а затем задать количество кадров в фильме и движение предметов. Движение объектов в трехмерном пространстве задается по траекториям, ключевым кадрам и с помощью формул, связывающих движение частей сложных конструкций. После задания нужного движения, освещения и материалов запускается процесс визуализации. В течение некоторого времени компьютер просчитывает все необходимые кадры и выдает готовый фильм. Недостатком является чрезмерная гладкость форм и поверхностей и некоторая механистичность движения объектов.

Для создания реалистичных трехмерных изображений используются различные приемы. Для создания “неровных” объектов, например, волос или дыма, используется технология формирования объекта из множества частиц. Вводится инверсная кинематика и другие техники оживления, возникают новые методы совмещения видеозаписи и анимационных эффектов, что позволяет сделать сцены и движения более реалистичными.

Кроме того, технология открытых систем позволяет работать сразу с несколькими пакетами. Можно создать модель в одном пакете, разрисовать ее в другом, оживить в третьем, дополнить видеозаписью в четвертом. И, наконец, функции многих профессиональных пакетов можно сегодня расширить с помощью дополнительных приложений, написанных специально для базового пакета.

- 3D Studio MAX

Один из самых известных пакетов 3D-анимации производства фирмы Kinetix. Программа обеспечивает весь процесс создания трехмерного фильма: моделирование объектов и формирование сцены, анимацию и визуализацию, работу с видео. Программа претендует на роль конкурента мощным пакетам для рабочих станций SGI. Интерфейс программы един для всех модулей и обладает высокой степенью интерактивности. 3D Studio MAX реализует расширенные возможности управления анимацией, хранит историю жизни каждого объекта и позволяет создавать разнообразные световые эффекты, поддерживает 3D-акселераторы и имеет открытую архитектуру, то есть позволяет третьим фирмам включать в систему дополнительные приложения.

- TrueSpace

Пакет TrueSpace фирмы Caligari предназначен для трехмерной анимации и отличается легкостью в использовании, гибкостью в управлении формами, поддержкой сплайнов и булевых операций над объектами. Это пакет 3D-моделирования, анимации и рендеринга. Новаторский интерфейс показывает линейки инструментов прямо в 3D-пространстве и выравнивает их по объекту, кроме того, они контекстно-зависимы. TrueSpace имеет встроенный язык сценариев (Python). Расширения (Plugin) и открытость архитектуры позволяют увеличить возможности пакета.

- LightWave3D

Пакет LightWave 3D, созданный фирмой NewTek имеет дружественный интерфейс, сильные средства моделирования, анимации и визуализации, хорошую библиотеку объектов и текстур, а также разрешает создавать VRML-файлы, что позволяет работать с ним в сети. По своим функциональным возможностям близок к 3D Studio MAX.

- ElectricImage

Пакет Electric Image фирмы Animation System, включает большой комплекс анимационных средств, спецэффекты, инструментарий для работы со звуком и генератор шрифтов с настраиваемыми параметрами. Хотя у этой программы нет средств моделирования, но зато есть возможность импорта свыше тридцати различных форматов моделей. Пакет также поддерживает работу с иерархическими объектами и средствами инверсной кинематики.

- SoftImage3D

Программа фирмы Softimage работает на платформах SGI и Windows NT. Она поддерживает моделирование на базе полигонов и сплайнов, создание спецэффектов, работу с частицами и технологию переноса движения с живых актеров на компьютерных персонажей. Высокопрофессиональный пакет 3D-анимации. Доступны такие инструменты, как моделлинг, анимация и рендеринг, позволяющие применять их в создании спецэффектов в фильмах, телепередачах, играх.

- Ray Dream Studio

Программа обеспечивает набор профессиональных инструментов для 3D-дизайна и анимации. Пользователи могут создавать различные модели с использованием булевых операций и деформаций. К этим моделям можно применять различные текстуры или видеоизображения, а также рисовать прямо на их поверхности. Полнофункциональная анимация использует нерезкость движений для придания им реалистичности. Параметры визуализации позволяют не только задавать направления лучей, но и придавать изображению вид рисованного мультфильма.

Maya

Пакет трехмерной анимации фирмы Alias|Wavefront. Его средства моделирования, поддерживающие работу со сложными иерархическими объектами и поверхностями, представляют собой один из наиболее мощных и удобных комплексов инструментов создания объектов на основе полигонов и, главное, сплайнов. Пакет позволяет создавать реалистичные образы, в частности, благодаря отличным возможностям освещения — направленного и рассеянного, с использованием бликов и других эффектов. Пакет поддерживает богатые средства затенения и техники придания реалистичности поверхностям, которые позволяют оживить гладкие и жесткие конструкции, неизбежно выдающие свое компьютерное происхождение. Maya содержит богатые инструменты анимации объектов, источников света и камер, отличный инструментарий для работы с частицами и автоматизации анимации. Анимация в пакете создается на основе ключевых кадров, инверсной кинематики и с помощью технологии переноса движения с живых актеров на компьютерных персонажей, что позволяет получить очень естественные движения объектов.

- Painter3D

Это полнофункциональный пакет 3D-моделирования. Painter 3D дает возможность применять к объектам текстуры, удары, свет, отражение и свечение, а также позволяет автоматически обновлять текстуры. Кроме всего прочего, этот пакет поддерживает расширения (Plugin), что дает возможность, использовать множество стандартных и дополнительных спецэффектов. В пакет входят дополнения для Ray Dream Studio и 3D Studio MAX. Возможен также импорт (экспорт) объектов из форматов OBJ, DXF или 3DMF.

- SoftF/X Pro

Это пакет для 3D-моделирования, рендеринга и анимации. Поддерживает написание скриптов, в частности Script Renderer. Позволяет создавать видео из обычного фотографического материала, путем применения дополнительных спецэффектов. Новая версия включает такие возможности, как: трассировка лучей, анимация скелетов с учетом законом кинематики, совмещение отображаемых образов и теней, специальные эффекты переходов. А также 40 видеоэффектов, в том числе затуманивание, монохромность, негатив, тонирование, картинка в картинке, увеличение, уменьшение, направление по сторонам, поворот, шум и другие.

Видео

В настоящее время существует два типа видео: аналоговое и цифровое.

Аналоговый видеосигнал в телевидении содержит 625 строк в кадре при соотношении размера кадра 4 x 3, что соответствует телевизионному стандарту. Этот сигнал является композитным и получается сложением яркостного сигнала Y, сигнала цветности (два модулированных цветоразностных сигнала U и V) и синхроимпульсов. Так как глаз человека менее чувствителен к изменениям оттенков цвета, чем к изменениям яркости, то цветовая информация может передаваться с меньшей четкостью. Поэтому в телевизионном сигнале, где каждый цвет описывается тремя составляющими: красной (R), зеленой (G) и синей (B), на их базе формируются сигнал яркости Y и цветоразностные сигналы U и V, причем последние передаются с разрешением, в два раза меньшим, чем Y. В телевизионном приемнике эти сигналы декодируются, и восстанавливается исходный RGB-сигнал.

В бытовых видеомагнитофонах для простоты декодирования сигналов объем информации в них ограничивается, что ведет к уменьшению четкости изображения и снижению числа строк до 240. Такое решение используется в форматах VHS и Video-8.

Более качественный результат получается при передаче двух композитных сигналов: яркости вместе с синхроимпульсами (Y) и модулированных цветовых сигналов (C). При этом обеспечивается разрешение в 400 линий. Такому решению соответствуют форматы записи S-VHS и Hi-8.

Только при переходе к компонентному сигналу, в котором все три составляющих — Y, U и V — передаются отдельно, можно достичь наиболее высокого качества. Такой сигнал используется в профессиональной аппаратуре формата Betacam, что позволяет получить разрешение до 650 линий.

Цифровое видео первоначально представляло собой преобразованный в цифровой формат аналоговый сигнал, в котором данные о серии изображений сохранялись на каком-либо запоминающем устройстве. Появление цифровых видеокамер позволило получать сигнал сразу в цифровой форме. Для них был разработан новый цифровой формат записи на магнитную ленту — DVC (*Digital Video Cassette*) или DV (*Digital Video*). Это компонентный формат представления сигнала, который обеспечивает разрешение по горизонтали 500 линий. Оцифровка осуществляется с разрешением 720 x 576 согласно схеме 4:2:0 (каждый кадр содержит 720 x 576 значений яркости Y и по 360 x 288 значений цветоразностных сигналов U и V). Благодаря раздельной записи видео и звука формат DV позволяет добавлять звуковое сопровождение после завершения записи или редактирования видео, а также перезаписывать звук.

Для телевидения также разработан новый цифровой стандарт HDTV (*High Definition Television*), который обеспечивает 1200 строк разрешения при соотношении размера кадра 16x9 по горизонтали и вертикали.

Для уменьшения объема цифровых видеофайлов используют методы сжатия данных, которые базируются на математических алгоритмах устранения, группировки и усреднения схожих данных, присутствующих в видеосигнале. Существует большое количество разнообразных алгоритмов сжатия, включая Compact Video, Indeo, Motion-JPEG, MPEG, Cinepak, Sorenson Video. Все они могут быть разделены на следующие категории.

Обычное сжатие (в режиме реального времени). Система оцифровки видеосигнала с одновременным сжатием. Для качественного выполнения этих операций требуются высокопроизводительные специальные процессоры. Большинство плат ввода/вывода видео на PC пропускают кадры, что нарушает плавность изображения и его синхронизацию со звуком.

Симметричное сжатие. Оцифровка и запись производится при параметрах последующего воспроизведения (например, разрешение 640 x 480 при скорости 30 кадров в секунду).

Асимметричное сжатие. Обработка выполняется при существенных затратах времени. Так, отношение асимметричности 150:1 указывает, что 1 минута сжатого видео соответствует затратам на сжатие в 150 минут реального времени.

Сжатие с потерей или без потери качества. Все методы сжатия приводят к некоторой потере качества. Существует только один алгоритм (разновидность Motion-JPEG для формата Kodak Photo CD), который выполняет сжатие без потерь, однако он оптимизирован только для фотоизображений и работает с коэффициентом 2:1.

Коэффициент сжатия — это цифровое выражение соотношения между объемом исходного и сжатого материала. Качество видео зависит от используемого алгоритма сжатия, параметров видеоплаты оцифровщика, конфигурации компьютера и даже от программного обеспечения. Для MPEG сейчас стандартом считается соотношение 200:1. Различные варианты Motion-JPEG работают с коэффициентами от 5:1 до 100:1, хотя уже при уровне 20:1 трудно добиться нормального качества изображения.

Для редактирования видео существует большое количество программных продуктов. В дополнение к пакетам трехмерной анимации существуют узкоспециализированные программы, например, для создания объемных шрифтов. Они также используют разнообразные эффекты анимации, выполняют визуализацию изображения и позволяют создать видео файлы. Некоторые из них будут представлены далее.

- Quick Editor

Это условно-бесплатный редактор, осуществляющий основные операции с видеоизображением в формате MOV и AVI быстро и просто. Он представляет собой хорошее и доступное средство для работы с небольшими видеопоследовательностями. Для работы с этим редактором на вашем компьютере должна быть установлена программа просмотра QuickTime версии 3 и выше. Конечно, данный редактор не заменит средств для профессионалов, но для многих небольших проектов будет крайне полезен.

- Adobe Premiere

Наиболее распространенная программа редактирования цифрового видео. Обладает удобным интуитивно понятным интерфейсом. Поддерживает несколько видео- и звуковых каналов, содержит набор переходов между кадрами, позволяет синхронизировать звук и изображение. Поддерживает файлы форматов MOV и AVI. Подключение дополнительных модулей (plug-ins) от независимых производителей расширяет возможности программы.

- Speed Razor SE

Программа фирмы in-sync, имеющая удобный пользовательский интерфейс. Благодаря более развитым инструментам работы с видео- и звуковыми каналами Speed Razor удобнее использовать в проектах со сложной композицией и наложениями. Содержит набор часто используемых спецэффектов, монтаж встык (прямые склейки) выполняется в режиме реального времени и не требует рендеринга. Поддерживает работу с картами видеозахвата miroVIDEO DC30, обеспечивая все их возможности и обратную связь с VGA монитором. Мультимедиа-проекты, созданные с помощью этой программы, могут быть записаны на видео, CD-ROM или помещены на Web-сайт.

- Ulead VideoStudio

Программа Ulead VideoStudio предназначена для начинающих пользователей. В ней доступна полная поддержка форматов DV и MPEG-2 для цифрового видео. А для музыкального сопровождения фильма можно использовать музыкальные файлы в формате MP3 или звуковые дорожки с аудиодиска. Работа с программой достаточно проста благодаря продуманному и дружественному к пользователю интерфейсу. Оцифровка легко выполняется с помощью специального модуля Video Wizard. Он помогает пройти по всем стадиям этого процесса и дает необходимую информацию для начала редактирования. С помощью технологии SmartRender работа с оцифрованным видео происходит достаточно быстро. Это связано с тем, что при получении результата идет просчет не по всей видеоинформации, а лишь только той ее части, которая подверглась изменениям. В видеофильм можно вставить титры, воспользоваться плавными переходами между отдельными фрагментами и добавить голос или фоновую музыку к получившемуся клипу.

- Video Trope

Простая программа для редактирования и добавления эффектов к видео и компьютерной анимации. Позволяет добавить звуковую дорожку к видеоматериалу и синхронизировать ее. С ее помощью можно также построить цифровую видеопоследовательность или анимацию, собрав ее из отдельных, подготовленных ранее статических кадров или из захваченных отдельных фрагментов созданных ранее оцифрованных фильмов. Video Trope также позволит добавить звуковую дорожку к видеоматериалу, синхронизировав звук с изображением. Сохраняет видео в формате AVI.

- AVIedit

Небольшая, но мощная программа для работы с видео в формате AVI. По своим функциональным возможностям во многом совпадает с Video Trope. Позволяет захватывать отдельные кадры и живое видео в файлы формата AVI и выполнять их редактирование. Возможно создание клипа путем импорта серий изображений из файлов BMP и анимированных GIF и, наоборот, экспорт выбранных кадров или всего клипа в последовательность отдельных файлов BMP, TARGA или в другой клип. Можно также

создать клип с текстовыми титрами, указывая размер шрифта и цвет. От аналогичных программ отличается большей гибкостью настроек и удобством работы. В программе приняты меры для преодоления ограничения в 2 Гбайта на размер файлов AVI.

- VideoMan

Программа, разработанная российской фирмой STOIK Software. VideoMan — редактор видео с многодорожечной временной шкалой. Имеет дорожку для создания переходов между видеофрагментами, три звуковых дорожки и три видеодорожки (включая одну оверлейную дорожку для клипов с прозрачностью). Содержит библиотеку переходов и динамических специальных эффектов и звуковой редактор. В работе можно использовать интерактивный предварительный просмотр, утилиту для захвата видео и режим автовставки, который позволяет захватывать клипы с TV- или VCR-входа и создавать собственные фильмы с титрами, звуком и специальными эффектами.

- Digital Movie Studio

Программа для редактирования видео фирмы Hitachi. Она позволяет создавать MPEG-файл (*.mpg) на основе видеоклипов и статичных изображений, добавлять звуковую дорожку или заменять ее, добавлять титры, дату и время, использовать эффекты перехода между кадрами, изменять скорость изображения.

- PowerVCR

Программа фирмы CyberLink, работающая как интерактивная видеокамера, записывает файлы непосредственно в формате MPEG-1 с разрешением CIF (352 x 288) или SIF (352 x 240), что позволяет пользователю экономить как время, так и место на жестком диске. PowerVCR также обеспечивает возможность редактирования и создания титров, и преобразование файлов формата AVI в MPEG-1. Имеет интуитивно понятный пользовательский интерфейс. Позволяет получать сигнал от видеомагнитофона или видеокамеры, а также с TV-тюнера.

- Producer

Программа фирмы Emulive позволяет записывать видео и звук, полученные от различных источников. Она обеспечивает преобразование изображения в реальном масштабе времени и включает возможности добавления титров, статичных изображений, размывания изображения или увеличения резкости, подсвечивания изображения, его вращения и др. Для последующей передачи можно сохранить запись в формате JFX, разработанном фирмой Emulive. Также возможно преобразование файла в форматы AVI и WAV. Технология Screenscrape позволяет использовать в качестве источника изображения экран компьютера, задавая размер изображения от полного экрана до 320 x 240, 240 x 180, 160 x 120 либо 80 x 60 точек. Режим “pointer-follow-me” дает возможность отслеживать перемещения указателя мыши.

- COOL 3D

Программа создания 3D-заголовков фирмы Ulead для презентаций, видео, мультимедиа и Web-страниц. Программа включает в себя более 100 автоматических мастеров, множество эффектов, которые в значительной степени упрощают моделирование и рендеринг конечной сцены. Также содержит огромную библиотеку 3D-объектов и материалов плюс фотореалистичные шаблоны и текстуры.

- 3Dplus

Программа 3DPlus фирмы Serif автоматизирует создание трехмерных сцен с помощью большого набора мастеров. Она специально приспособлена для совместной работы с PagePlus — приложением, предназначенным для создания публикаций на бумаге или Web-страниц.

Цифровой звук

Хотя в воспринимаемом человеком потоке информации зрительный канал играет главенствующую роль, но не менее важен и канал звуковой. Звук является наиболее выразительным элементом мультимедиа. Рассмотрим, какие существуют способы получения звука на компьютере.

В звуковых платах реализуются два основных метода синтеза: таблично-волновой и на основе частотной модуляции. Первый основан на воспроизведении сэмплов — образцов звучания реальных инструментов. Сложные синтезаторы для воспроизведения каждой ноты применяют параллельное проигрывание нескольких сэмплов и дополнительную обработку звука (модуляцию, фильтрацию, спецэффекты и др.) в результате чего достигается реалистичность звучания. Синтезаторы с частотной модуляцией используют несколько генераторов сигнала с взаимной модуляцией. При этом достигается большое разнообразие звучаний, но трудно имитировать звучание реальных инструментов и обеспечить благозвучный тембр.

Программы для работы со звуком можно условно разделить на две большие группы: программы-секвенсоры и программы, ориентированные на цифровые технологии записи звука, так называемые звуковые редакторы.

MIDI-секвенсоры предназначены для создания музыки. С помощью секвенсоров выполняется кодировка музыкальных пьес. Они используются для аранжировки, позволяя “прописывать” отдельные партии, назначать тембры инструментов, выстраивать уровни и балансы каналов (треков), вводить музыкальные штрихи (акценты громкости, временное смещение, отклонения от настройки, модуляция и проч.). В отличие от обычного сочинения музыки эффективное использование секвенсора требует от композитора-аранжировщика специальных инженерных знаний. Программы звуковых редакторов позволяют записывать звук в режиме реального времени на жесткий диск компьютера и преобразовывать его, используя возможности цифровой обработки и объединения различных каналов.

- Cakewalk Pro Audio

Профессиональный многодорожечный секвенсор компании Twelve Tone Systems пользуется заслуженной популярностью у профессионалов. Поддерживает до 64 аудиодорожек и 256 — MIDI, 64 канала звуковых эффектов. Cakewalk был одним из первых программных продуктов, в котором появилась поддержка дополнительных подключаемых модулей (plug-in) разнообразных аудиоэффектов, созданных для интерфейса DirectX. Характерная особенность DirectX-эффектов заключается в том, что все они работают в реальном времени — достаточно щелкнуть по кнопке *Preview*, и можно настраивать все параметры выбранного эффекта прямо в процессе воспроизведения звукового фрагмента.

- Cubase VST

Это универсальный и сложный профессиональный секвенсор фирмы Steinberg. Он имеет большее количество способов просмотра и манипулирования музыкой, чем какая-либо другая программа. В отличие от других, эта программа использует много непривычных терминов, поэтому для работы с ней требуется подготовка. Программа поддерживает как подключаемые модули с интерфейсом DirectX, так и с интерфейсом VST. VST специально разработан фирмой Steinberg как альтернативная платформа для поддержки эффектов реального времени.

- Logic Audio Platinum

HiEnd профессиональный секвенсор фирмы Emagic имеет 128 аудиодорожек и неограниченное количество MIDI. Обеспечивает поддержку DirectX, обработку в реальном времени, качество 16/24 бит, может работать с несколькими звуковыми картами. Он также позволяет записывать звук и выполнять цифровую его обработку. Удобный оконный интерфейс отображает пьесу в виде, соответствующем решаемой задаче. Команды меню можно представить на разных языках.

- Band in Box

Профессиональный авто аранжировщик фирмы PGmusic. Позволяет создавать импровизации в различных стилях от блюза до техно. Обеспечивает также поддержку аудиозаписи, что дает возможность добавить вокал или инструментальное сопровождение. Мастер стиля показывает, какие стили имеют такой же темп, жанр и чувство. Поддерживает дополнительные подключаемые модули, различные стили, соло, эффекты (MegaPack). Позволяет сохранять файлы в форматах как MIDI, так и WAV, а также использовать установленные в Windows кодеки для сжатия файла.

- MusiNum

Программа позволяет создать музыку и не требует знания нот, так как алгоритм ее работы основан на теории чисел. Первоначально задается, какие инструменты будут в оркестре, который проиграет сочиняемую мелодию. Всего в оркестре может быть до 16 участников. Настройки каждого голоса вызываются щелчком мыши по кнопке с номером вверху окна. Четыре числовых параметра в первой строке обозначают коэффициенты математической формулы, по которой работает программа. Подробную информацию об этом можно прочесть в файле помощи. Эти коэффициенты определяют мелодию для выбранного инструмента. Следующая строка описывает характер звучания мелодии, а строка под ней — инструмент. Самая нижняя строка описывает положение инструмента в стереофонической панораме и ритм музыки. Параметры мелодии можно сохранить в собственном формате программы MusiNum (MIN). Также возможно создание MIDI-файла, для чего нужно задать начальный и конечный номера нот для участка генерируемой последовательности.

- Sound Forge

Программа Sound Forge является одним из лидеров среди звуковых редакторов. Она обладает мощными функциями редактирования, позволяет встраивать любые подключаемые модули, поддерживающие технологию DirectX, имеет удобный современный интерфейс. Включает две дополнительных компонента: Batch Converter, позволяющий объединить группу файлов в один общий файл, и Spectrum Analysis, представляющий данные в двух видах (спектр и фонограмма), используя быстрое преобразование Фурье. Поддерживает современные звуковые форматы, в том числе RealAudio.

- CoolEdit Pro

Профессиональная студия звукозаписи фирмы Syntrillium Software. Она позволяет записывать звук через звуковую карту от микрофона, CD-проигрывателя или другого источника, считывать и записывать файлы в популярном формате MP3, редактировать полученные звуковые файлы и добавлять в них разнообразные фантастические эффекты. Позволяет использовать эффекты: ревербератор, chorus, эхо, эквалайзер, компрессор, шумоподавление, изменение высоты тона и темпа, CD-премастеринг, анализ спектров и АЧХ. Обеспечивает работу с мультимедиа-сайтами, подготовку звука для MP3, RealAudio, DVD при качестве до 24 бит/96 кГц. Позволяет объединять до 64 каналов, создавая файлы объемом до 2 Гбайт и сохраняя их в одном из 25 различных форматов.

- WaveLab

Стереоредактор фирмы Steinberg входит в группу лидеров среди звуковых редакторов. Это самый быстрый пакет для премастеринга и редактирования звука. Он обладает множеством эффектов, обеспечивает запись CDR, анализ спектров, имеет возможность работы со встроенными подключаемыми модулями DirectX и VST, поддерживает многие форматы звуковых файлов, в том числе и MP3. Программа открывает звуковой файл в двх окнах: первое — для общего обзора, а второе — для конкретного редактирования. Существует возможность открывать несколько файлов одновременно. Они могут быть сведены в группу и сохранены как проект (project). Большой массив звуковых файлов можно объединить в базу данных (database).

- PowerTracks Pro

Мощный многодорожечный аудио-миди-редактор фирмы PGmusic, совместимый с Band-in-Box. Позволяет записывать воспроизводить и контролировать до 16 каналов аудио, MIDI или их комбинаций одновременно. Каждый канал может быть сохранен в отдельном файле для экспорта в другой проект. При загрузке новой мелодии каналы, не имеющие названия, автоматически получают имена из списка General MIDI для файлов MID или из пользовательского списка для файлов SEQ. Список этих имен отображается в специальном окне на панели инструментов.

- Akoff Music Composer

Программа распознает мелодию, поступающую на микрофон или записанную в WAV-файле и переводит ее в формат MIDI. Помимо этого, присутствует MIDI-проигрыватель с расширенными возможностями. Для своей работы требует наличия высококачественного микрофона. Хотя от пользователя не требуется никаких знаний нотной грамоты, нужно потренироваться напевать мелодию так, чтобы ее могла распознать программа.

Презентации и др. мультимедиа-продукты

После создания всех мультимедиа-компонентов необходимо объединить их в единое мультимедиа-приложение. При этом возникает задача выбора программного средства для его разработки. Существующие средства объединения различных мультимедиа-компонентов в единый продукт условно можно разделить на три группы:

- алгоритмические языки для непосредственной разработки управляющей программы;
- специализированные программы для создания презентаций и публикации их в Интернет (быстрая подготовка мультимедиа-приложений);

- авторские инструментальные средства мультимедиа.

Деление это достаточно условно, потому что многие средства обладают возможностью создавать программные модули на языке сценариев. Как правило, выбор средства основывается на требованиях к эффективности работы мультимедиа-приложения и скорости его разработки. Также существенным требованием является степень взаимодействия с пользователем. Специализированные презентационные программы ориентированы в первую очередь на передачу информации от компьютера к пользователю. Авторские инструментальные средства позволяют осуществить высокую степень взаимодействия и создать действительно интерактивное приложение.

Разработка мультимедиа-приложения на каком-либо алгоритмическом языке требует знания программирования, хотя современные среды визуального программирования дополнены различными мастерами для создания отдельных элементов интерфейса, позволяющих автоматизированно получать код программы. Затраты времени на разработку будут в этом случае значительны, но получившееся приложение — оптимальным по использованию ресурсов компьютера и скорости функционирования.

Авторские инструментальные средства позволяют существенно сократить процесс разработки, но дают проигрыш в эффективности работы создаваемого приложения. Кроме того, для разработки необходимо хорошее знание возможностей данного средства и эффективных методов работы с ним.

Наиболее простым и быстрым является использование программ создания презентаций, возможностей которых в некоторых случаях оказывается достаточно для создания несложного мультимедиа-приложения. Авторские системы предназначены для создания программных продуктов с высокой степенью взаимодействия с пользователем. Часто для разработки пользовательского интерфейса авторские системы предлагают специальный язык сценариев. Они позволяют создать конечный продукт, объединяющий все мультимедиа-компоненты единой управляющей программой. Его отличительной чертой является наличие общего интерфейса, позволяющего выбрать любой из мультимедиа-компонентов, запустить его на выполнение (прослушать звуковой файл или просмотреть видео), организовать поиск требуемого объекта и т.п.

Программы создания презентации первоначально предназначенные для создания электронных слайдов, помогающих иллюстрировать сообщение докладчика, теперь все более ориентируются на применение мультимедиа. Существует большое количество таких программ, различающихся набором изобразительных и анимационных эффектов.

- PowerPoint

Презентационная программа, входящая в пакет Microsoft Office. По количеству изобразительных и анимационных эффектов не уступает многим авторским инструментальным средствам мультимедиа. Содержит средства для создания гибкого сценария презентации и записи звукового сопровождения каждого слайда. Наличие русскоязычной версии позволяет успешно работать с текстами на русском языке. Встроенная поддержка Интернета позволяет сохранять презентации в формате HTML, однако анимированные компоненты требуют установки специального дополнения PowerPoint Animation Player. Позволяет создавать сложные программные надстройки на языке программирования Visual Basic for Application, что существенно расширяет возможности программы. Специальная надстройка Custom Soundtracks Add-In дополняет презентацию фоновым музыкальным сопровождением с широким выбором мелодий.

- Freelance Graphics

Программа фирмы Lotus для создания слайд-шоу. Обеспечивает широкий набор возможностей форматирования текста, рисунков, графиков и таблиц на слайдах. Демонстрация презентации может проводиться на компьютерах, где сама программа Freelance Graphics отсутствует. Поддерживает изображения в формате GIF, в том числе с прозрачным фоном. Преобразование презентации в формат HTML с помощью специального мастера позволяет публиковать ее на Web-сервере, обеспечивая при этом оптимальную скорость загрузки страницы. Демонстрация слайд-шоу в Интернете требует дополнительных компонентов Plug-In для броузера или Freelance Graphics' ActiveX.

- Formula Graphics

Авторская система Formula Graphics фирмы Formula Software применяется для разработки интерактивных приложений мультимедиа. Она имеет простой и удобный в использовании графический интерфейс и не накладывает никаких ограничений на изображения, звуки и анимации, которые могут быть объединены с ее помощью. Formula Graphics имеет мощный объектно-ориентированный язык, однако приложения можно разрабатывать и без применения программирования. Управляющие элементы на экране отображаются в виде гипертекста и графических гиперссылок. Formula Graphics имеет программируемую двух- и трехмерную графику и используется также для разработки приложений с анимацией и игровых программ. Разработанные мультимедиа-приложения могут быть проиграны с гибкого диска, CD-ROM, непосредственно через Интернет или внедрены в Web-страницу.

- HyperMethod

Российская авторская система HyperMethod работает под Windows 95/98/NT. Она позволяет создавать самые разнообразные мультимедиа-приложения и по своим функциональным возможностям приближается к программе Macromedia Director. Поддерживает распространенные форматы звуковых и видеофайлов, а также возможность контролируемой покадровой анимации. Обеспечивает быстрое создание гипертекстовых приложений, а совместимость с HTML позволяет создавать приложения для Интернета. Имеет собственный язык сценариев. Новые возможности, добавленные в последней версии, делают ее привлекательной как для новичков, так и для профессионалов.

3.3.Этапы разработки проекта

1 этап - выбор темы и описание проблемы;

2 этап - анализ объекта;

3 этап - разработка сценария и синтез модели;

4 этап - форма представления информации и выбор программных продуктов;

5 этап - синтез компьютерной модели объекта

Процесс создания мультимедийного продукта

Процесс создания мультимедиа-информационных систем может рассматриваться как состоящий из двух основных фаз:

- **фазы проектирования**
- **фазы реализации**

Фаза проектирования

1. Проектирование концептуальной модели сценария для мультимедиа-информационной системы.
2. Проектирование медиа-зависимых представлений информации.
3. Проектирование информационных структур.
4. Проектирование медиа-комбинаций и синхронизаций (звук - видео)
5. Проектирование структур узел-связь (ссылки)
6. Проектирование информационных топологий (общая среда)
7. Проектирование интерфейса пользователя
8. Проектирование пользовательского интерфейса
9. **Проектирование методов навигации**

Фаза реализации

Реализация должна сопровождаться инструментами и методами создания.

1. Первичная интеграция
    a) Создание фрагментов
    b) Создание структуры
2. Полная интеграция мультимедиа-продукта монтаж, т.е. соединение всех элементов в единый продукт, в соответствии с определенной структурой и заданными средствами навигации.
3. Производство мультимедиа-продукта (определяется носителем)
4. Распространение мультимедиа-продукта

3.4.Мультимедийный компьютер

«Мультимедийный компьютер» – это такой компьютер, на котором мультимедийные приложения могут в полной мере реализовать все свои возможности. Мультимедийный компьютер должен уметь многое: отображать на экране монитора графическую и видео-информацию, анимацию, воспроизводить с высоким качеством различное звуковое сопровождение, музыку, в ом числе и с музыкальных компакт-дисков, и многое другое…

Аппаратный состав мультимедийного компьютера

Обычно под набором комплектующих, объединенных понятием «мультимедийный компьютер», понимают следующий их состав:

- Корпус с блоком питания
- Системная (материнская) плата
- Центральный процессор
- Оперативная память
- Видеоадаптер
- Монитор

- Накопитель на жестких дисках
- Клавиатура
- Мышь
- Дисковод CD-ROM
- Дисковод гибких дисков
- Звуковая карта
- Дисковод DVD
- Модем
- Телевизионный и УКВ тюнер

Не так давно корпорация Intel и Microsoft при участии других грандов компьютерной индустрии подготовили спецификацию компьютера PC 99. Этот стандарт определяет типы систем персональных компьютеров, предназначенных для выполнения определенных функций (см. Приложение). Рассмотрим класс «Entertainment PC» (развлекательный или мультимедийный компьютер).

С точки зрения этапов развития аппаратной части компьютера наибольший интерес вызывают следующие требования:

- Полный отказ от интерфейса шины ISA
- Все компоненты системной (материнской) платы должны соответствовать спецификации Plug-and-Play
- Порты COM и LPT рекомендуется использовать только для подключения принтеров
- Интерфейсы IDE/ATA и ATAPI для внешних накопителей подлежат замене на IEEE1394
- Для модемов рекомендуется интерфейс USB
- Для сканеров и других устройств ввода изображений рекомендуется использовать интерфейсы SCSI или IEEE1394
- Для звуковых карт возможны интерфейсы USB или PCI
- Графические адаптеры допустимы только с интерфейсом AGP или PCI
- Подключать мышь и клавиатуру рекомендуется через интерфейс USB или PS/2

Впервые в спецификации отражены требования к разрешению и другим параметрам мониторов.

Требования, приводимые в PC 2001, направлены на создание компьютеров под управлением Windows Me, Windows 2000 Professional, Window XP предназначенных для работы с типичными Windows-приложениями. Естественно, речь идет не о базовых аппаратных требованиях, предъявляемых операционными системами, а об оптимальных. Впервые PC 2002 не содержит классических рекомендаций — указываются только минимальные требования! Все то, что было из лучших побуждений рекомендовано в PC 99, либо стало требованием в PC 2001, либо безжалостно удалено.

Основная идея PC 2001 — сделать стандартом де-юре требования инициативы Intel Easy PC, направленной на превращение компьютера в несложный, надежный и стабильно работающий бытовой прибор. «Лейтмотив» Easy PC — отказ от шины ISA, быстрая загрузка и интеллектуальное управление питанием. Безусловно, это далеко не полный список идей Easy PC, однако он дает довольно четкое представление.

Особенность PC 2001 — отсутствие жесткого разделения ПК на классы. В частности из текста исключены упоминания об Office PC, Consumer PC и Entertainment PC, которые были четко специфицированы в PC 99. Теперь все, что не является Workstation (рабочей станцией) и Mobile (ноутбуком), попадает под категорию PC System.

В PC 2001 происходит полный отказ от шины ISA, а также признаются устаревшими ее производные – PS/2, COM, LPT, FDD. Последний пункт означает, сто 3,5-дюймовые дисководы флоппи-дисков либо исчезнут как класс, либо перейдут на новый интерфейс, вероятнее всего на USB. Причем сам USB должен эволюционировать до уровня спецификации 2.0, где скорость передачи данных достигает 480 Мбит/с.

Программный состав мультимедийного компьютера

Даже самый современный компьютер не будет работать без программного обеспечения. Как уже говорилось, мультимедийное программное обеспечение можно условно разделить на прикладную часть (мультимедиа-энциклопедии, компьютерные инры, аудио и видеоплееры и т.п.) и специализированную, к которой можно отнести программы, предназначенные для создания прикладных программ (профессиональные графические редакторы, редакторы 3D-графики, звуковые редакторы и т.д.)

Рассмотрим основные части программного обеспечения мультимедиа-компьютера:

- Операционная система
- Прикладные мультимедийные приложения

Операционная система

За последние несколько лет мультимедийные приложения стали одним из наиболее быстро растущих сегментов рынка программного обеспечения. Большинство современных компьютеров продаются с установленными приводами CD-ROM, звуковыми картами и мощными графическими адаптерами. Чтобы иметь возможность воспользоваться всеми этими аппаратными средствами поддержки мультимедиа на компьютере должна быть установлена операционная система, поддерживающая все эти устройства. Наиболее ярким примером является ОС Microsoft Windows 98 или Windows Millenium. Архитектурные решения в мультимедийном расширении Windows 9x позволяют воспроизводить оцифрованное видео, аудио, MIDI.

Windows 9x – это 32-разрядная операционная система с поддержкой приоритетной многозадачности и многопоточности. Благодаря этому достигается более качественное воспроизведение информации от различных источников, а большое число встроенных драйверов мультимедийных устройств в значительной степени облегчают работу на современных компьютерах различной конфигурации.

Прикладные мультимедийные приложения

К прикладным можно отнести мультимедийные приложения, с которыми непосредственно работает обычный пользователь мультимедийного компьютера. В первую очередь это компьютерные игры. Также сюда можно отнести мультимедиа-энциклопедии, видео и аудиоплееры, программы для создания и просмотра презентаций и многие другие.

Основными целями применения продуктов, созданных в мультимедиа технологиях (CD-ROM с записанной на них информацией), являются:

- Популяризаторская и развлекательная (CD используются в качестве домашних библиотек по искусству или литературе).
- Научно-просветительская или образовательная (используются в качестве методических пособий).
- Научно-исследовательская - в музеях и архивах и т.д. (используются в качестве одного из наиболее совершенных носителей и "хранилищ" информации).

Популяризаторская цель

Широчайшее использование мультимедиа продуктов с этой целью не подвергается сомнению, тем более, что популяризаторство стало ныне некоторым эквивалентом рекламы. К сожалению, многие разработчики подчас не понимают, что простое использование широко

известного носителя (CD-ROMa) и программного обеспечения еще не обеспечивают действительно мультимедийный характер продукта. Тем не менее, приходится признать, что "разноцветье" представленных работ является отражением существующего общественного сознания в гуманитарных областях.

Научно-просветительская или образовательная цель

- Отбор путем чрезвычайно строгого анализа из уже имеющихся рыночных продуктов тех, которые могут быть использованы в рамках соответствующих курсов. Как показывает практика, задача отбора чрезвычайно сложна, поскольку лишь немногие готовые продукты могут соответствовать тематике преподаваемых курсов и тем высоким требованиям к достоверности, репрезентативности и полноте материала, которые, как правило, предъявляются преподавателями. Это связано с тем, что в создании продуктов не принимают участие специалисты-"предметники", обладающие необходимыми знаниями в представляемой области. А те немногие авторы, которые пытаются работать совместно с техническим персоналом над созданием подобных мультимедийных продуктов, плохо знают специфику этого компьютерного жанра и психологию восприятия информации, представленной на экране компьютера.
- Разработка мультимедийного продукта преподавателями в соответствии с целями и задачами учебных курсов и дисциплин.

Научно-исследовательские цели

Применяемое и в продуктах, созданных на основе мультимедиа технологии. Наиболее очевидная и почти автоматически вспоминаемая область применения мультимедиа продуктов в научно-исследовательской области - это электронные архивы и библиотеки - для документирования коллекций источников и экспонатов, их каталогизации и научного описания, для создания "страховых копий", автоматизации поиска и хранения, для хранения данных о местонахождении источников, для хранения справочной информации, для обеспечения доступа к внемузейным базам данных, для организации работы ученых не с самими документами, а с их электронными копиями и т.д.). Деятельность по разработке и осуществлению этих направлений архивно-музейной научной работы координируется Международным комитетом по документации (CIDOC) при Международном совете музеев, Музейной компьютерной сетью при Комитете по компьютерному обмену музейной информации (CIMI), а также Международной программой Гетти в области истории искусства (AHIP). Кроме этого, названные организации занимаются разработкой единых международных стандартов документирования и каталогизации музейных и архивных ценностей, осуществлением возможностей обмена информационными компонентами исследовательских систем.

4.ИНТЕРНЕТ ТЕХНОЛОГИЯ

Сегодня много говорят о том, что Интернет возник на средства Управления перспективных разработок Министерства обороны США *(DARPA — Defense Advanced Research Project Agency).* Была, якобы, у Министерства Обороны потребность связать между собой научно-исследовательские центры и крупнейшие университеты, чтобы ученые, занимающиеся важными проблемами, могли оперативно обмениваться документацией и информацией. Называется и дата, когда это замечательное событие произошло — примерно осенью 1969 года. Так что совсем недавно мир мог справлять тридцатилетие Интернета. Однако ни в Пентагоне (якобы создателе Интернета), ни в других ответственных организациях по этому поводу никаких торжеств отмечено не было. Интересно, к чему бы это?

А дело в том, что никаких “интернетов” Министерство обороны США не создавало и не финансировало, а роль его агентства *DARPA* была совсем не той, которую ему ныне приписывают. Мы можем только поражаться, как быстро рождаются легенды и мифы. Прошло всего три десятилетия, а создание Интернета уже овеяно легендами. Интересно отметить, что всего

лишь десять лет назад, когда Интернет еще не был у всех “на слуху”, никаких мифов относительно его рождения не существовало. Тогда все было просто и понятно. В те годы фальсификаторы истории еще не приложили к этому делу руку.

Давайте разберемся, что к чему, и выясним, как же на самом деле появился Интернет, и чем на самом деле занималось агентство *DARPA.* А заодно мы выясним, кем, когда и зачем была придумана “сладкая сказка” о мудрой прозорливости Министерства обороны США для наивных американских обывателей.

Заняться исследованиями рождения Интернета нас побудила естественная недоверчивость. Те, кто знают, как развивалась наука в XX веке, никогда поверят, что Министерство обороны США (или какое-либо иное Министерство обороны) может вложить миллиарды долларов, чтобы ученым стало удобно работать. В жизни так не бывает.

области ядерного оружия, ракетной техники, средств спецсвязи и во многих других специальных областях. Никогда ни одно правительство мира не допустит, чтобы участники стратегических проектов свободно разгуливали где хотят и контактировали с кем попало. Тем более никто не будет тратить деньги на то, чтобы сделать эти контакты более удобными. Так зачем же Министерству обороны США пришло в голову вкладывать деньги в создание удобных условий для коллективной работы ученых, разбросанных по университетам США?

Ответ на этот вопрос прост. Ничего Управление перспективных разработок не внедряло и ничего не финансировало. Оно занималось не внедрением, а *контролем за внедрением* компьютерных сетей в гражданской сфере, которое к концу 60-х годов стало уже неотвратимым. Ничего Пентагон не финансировал кроме контроля. Более того, в 1969 г. уже ничего и не надо было внедрять, поскольку все уже было давно внедрено там, где это действительно было нужно — в тех самых “закрытых” центрах. Речь шла только о контроле над тем, чтобы “очкарики” не внедрили чего-нибудь лишнего и наоборот, чтобы вовремя перехватить у них идеи, на которые тем доведется наткнуться. Вот на это на самом деле и шли деньги Министерства обороны США.

Изгибы истории

Подлинную хронологию Интернета можно отсчитывать с конца 50-х годов. Можно точно назвать дату, когда было принято правительственное решение, в результате которого и появилась первая глобальная сеть. Это произошло в 1958 году. Правда, понятия Интернет тогда, разумеется, не существовало. И никто вовсе не собирался обустраивать работу ученых с помощью компьютерной сети. Это был, так сказать, “побочный эффект”, который сегодня задним числом выдают за цель и достижение. Истинная же цель была гораздо важнее — настолько важнее, что для ее достижения действительно было не жаль миллиардов долларов.

Вот как обстояло дело.

В 1949 г. в СССР успешно испытали первую атомную бомбу. В 1952 г. не менее успешно была испытана водородная бомба. В 1956 г. военное руководство в США впервые заговорило о необходимости разработки системы защиты от ядерного оружия, но первые запросы остались без внимания.

В 1957 г. в СССР был выведен на орбиту первый искусственный спутник Земли. Для кого-то это великое научное достижение, а для кого-то — нечто совсем иное. Американцы поняли все правильно: отныне в СССР есть, чем доставить бомбу им на голову. В результате в 1958 г. было, наконец, принято правительственное решение о создании глобальной системы раннего оповещения о пусках ракет. Сегодня такие системы строят на базе спутниковых комплексов, вращающихся на полярных орбитах, а тогда оставалось только развернуть сеть наземных станций на вероятных маршрутах приближения ракет.

А вот еще факт. Согласно закону всемирного тяготения плоскость траектории баллистических ракет расположена так, что проходит через точку старта, точку цели и (обязательно!) через центр земного шара. Мысленно разрежьте глобус такой плоскостью, и вы увидите, что Америка ожидает основную массу ракет со стороны Северного Ледовитого океана. Вот на этих безжизненных просторах и пришлось создавать систему раннего оповещения. Так в конце 50-х годов началась разработка системы *NORAD* (North American Aerospace Defence Command). Предотвратить атаку она, конечно, не могла, но могла дать минут пятнадцать на то, чтобы зарыться в землю.

Система *NORAD* получилась очень большой. Ее станции протянулась от Аляски до Гренландии через весь север Канады. Сразу возникла новая проблема: как обрабатывать результаты наблюдения воздушных объектов (а летают на Севере не только ракеты), как согласовать действия многочисленных постов, как выделить из множества сигналов те, которые представляют угрозу и как привести в действие систему оповещения. Все это могут делать люди, но людям на принятие и согласование решений нужны часы, а здесь счет шел на секунды. Эту огромную систему нужно было компьютеризировать, а компьютеры объединить в единую разветвленную сеть.

Стоимость системы *NORAD* измерялась десятками миллиардов долларов. В рамках такого бюджета действительно нашлись те несколько миллиардов, которые были использованы для создания глобальной компьютерной сети, обрабатывающей информацию со станций наблюдения.

Ответ СССР на развертывание системы *NORAD* был недорогим и эффективным. Эта система легко обходится, если разместить стратегические ракеты где-нибудь в Карибском море, например на Кубе — тогда их траектория будет совсем иной. Соответствующие решения были приняты в начале 60-х. А в США, соответственно, началось “закапывание под землю”. Были созданы сложнейшие подземные убежища в Вашингтоне, а в Колорадо Спрингс, что в Скалистых горах, началось закапывание под землю командного центра *NORAD.* Так к 1964 году в недрах горы Шайенн возник целый город с трехэтажными сооружениями. Со всей страны к нему потянулись компьютерные и другие линии связи, соединившие центр управления *NORAD со* станциями наблюдения, рабочими постами и правительственными органами.

Сеть системы *NORAD* не долго оставалась внутриведомственной. Сразу после запуска началось подключение к ней служб управления авиаполетами — это логично, ведь все равно система контролировала воздушное пространство на огромных просторах. Сначала подключались военные авиаслужбы, но уже в середине 60-х годов активно шло подключение гражданских авиационных служб. Сеть неуклонно расширялась и развивалась, она вбирала в себя метеорологические службы, службы контроля состояния взлетных полос аэродромов и другие системы, как военные, так и гражданские.

Вот так и получилось, что задолго до создания проекта *ARPANET, в* США уже действовала глобальная компьютерная сеть Министерства обороны.

4.1.Проблема устойчивости глобальной сети

Первая очередь системы *NORAD* была завершена в мае 1964 года, но к тому времени уже стало известно о существовании в России ядерных зарядов мощностью 50 мегатонн. Несмотря на то, что гора, в которой разместился центр управления, отбиралась очень тщательно (она представляет из себя единый скальный массив), стало ясно, что и у нее нет шансов. А выход из строя центра управления однозначно вызывал (в те годы) выход из строя всей глобальной системы. В итоге многомиллиардная затея с разработкой и строительством подземного центра управления оказалась бесполезной. Поэтому во второй половине 60-х годов перед Пентагоном встала проблема разработки такой архитектуры глобальной Сети, которая не выходила бы из строя даже в случае поражения одного или нескольких узлов.

Экспериментировать с системой, на которой базируется национальная безопасность,— дело невозможное. Бумаги на любое испытание будут согласовываться годами. Вот если бы у Министерства обороны была другая глобальная сеть, содержащая

несколько узлов, да к тому же работающих в неустойчивой среде, она стала бы прекрасным полигоном. А теперь спросите себя, что может быть лучше для этой цели, чем университетские компьютеры и вычислительные центры научных организаций? Это же идеальный полигон, который даже не надо создавать — он уже есть! Его надо только подтолкнуть, а потом немножко порулить.

Вот она истинная причина участия Министерства обороны США в том проекте, который ныне стал Интернетом! Вот как родилась сеть *ARPANETl* Как видите, не была она Первой глобальной. И не было у Министерства обороны ни малейшего желания обеспечить научные круги удобным средством для обмена научной и технической документацией. В то время шла дорогая и бесславная война во Вьетнаме. Мог ли Пентагон в эти годы финансировать то, что нужно научной общественности? Не мог! Вместо этого было желание получить за гроши удобный полигон для испытаний, который можно держа под постоянным контролем и использовать для себя найденные оригинальные решения. Вот этим делом и занялось агентство *DARPA.*

Дальнейшая история подтверждает наши выводы. Как только проблема устойчивости и выживания сети при выходе из строя ее узлов была решена, работа *DARPA* немедленно прекратилась. Это событие произошло в 1983 г. после внедрения протокола *TCP/IP.* Свою задачу Пентагон выполнил и тихо удалился. В том же 1983 г. сеть *ARPANET* передали местной Академии наук (в США ее функции выполняет Национальный научный фонд, *NSF).* С тех пор сеть стала называться *NSFNET,* и к ней началось подключение зарубежных узлов.

Второе рождение Интернета

Ранние глобальные сети представляли собой группы компьютеров, связанные между собой прямыми соединениями. Основной проблемой того времени была проблема надежности и устойчивости сети. Нужна была

такая сеть, которую нельзя вывести из строя даже атомной бомбардировкой. Конечно "атомная бомбардировка" — понятие условное. Сеть, состоящую из прямых соединений, могут вывести из строя мыши, перегрызшие провода, похитители, стащившие жесткий диск из узлового компьютера, *хакеры,* не вовремя заправившие вирус, куда не следует. Существуют тысячи причин, по которым обычное разгильдяйство может вызвать последствия не хуже атомной бомбардировки. С точки зрения военных эксплуатация сети в научном и университетском окружении должна была стать для неё самым суровым испытанием, какое только можно придумать. В борьбе со множеством непредсказуемых случайностей университетские круги рано или поздно должны были найти простое и эффективное решение. Так оно и произошло. Решением проблемы стало внедрение в 1983 г. протокола *TCP/IP. С* этого времени отсчитывают второй этап развития Интернета.

Строго говоря, *TCP/IP* — это не один протокол, а пара протоколов, один из которых *(TCP — Transport Control Protocol)* отвечает за то, *как* представляются данные в Сети, а второй *(IP — Internet Protocol)* определяет методику адресации, то есть отвечает за то, *куда* они отправляются и *как* доставляются. Эта пара протоколов принадлежит разным уровням и называется *стеком протоколов TCP/IP.* Собственно говоря, только с появлением IP-протокола и появилось понятие Интернет.

Третье рождение Интернета

Долгое время Интернет оставался уделом специалистов. Обмен технической документацией и сообщениями электронной почты — это все-таки не совеем то, что нужно рядовому потребителю. Революционное развитие Интернета началось только после 1993 г. с увеличением в геометрической прогрессии числа узлов и пользователей. Поводом для революции стало появление службы World Wide Web (WWW), основанной на пользовательском протоколе передачи данных *HTTP* и на особом формате представления

данных — *HTML.* Документы, выполненные в этом формате, получили название Web-страниц.

Одновременно с введением концепции WWW была представлена программа Mosaic, обеспечивающая отправку запросов и прием сообщений в формате *HTML.* Эта программа стала первым в мире *Web-броузером,* то есть программой для просмотра Web-страниц. После этого работа в Интернете перестала быть уделом профессионалов. Интернет превратился в распределенную по миллионам серверов единую базу данных, навигация в которой не сложнее, чем просмотр обычной мультимедийной энциклопедии.

Как выглядит Интернет сегодня

Сегодня Интернет — это крупный комплекс, включающий в себя локальные сети и автономные компьютеры, соединенные между собой любыми средствами связи, а также программное обеспечение, которое обеспечивает взаимодействие всех этих средств на основе единого транспортного протокола *TCP* и адресного протокола *IP.*

Опорная сеть Интернета

Опорную сеть Интернета представляют узловые компьютеры и каналы связи, объединяющие их между собой. Узловые компьютеры также называют *серверами.*

Маршрутизаторы

На каждом из узлов работают так называемые *маршрутизаторы,* способные по IP-адресу принятого TCP-пакета автоматически определить, на какой из соседних узлов пакет надо переправить. Маршрутизатором может быть программа, но может быть и отдельный специально выделенный для этой цели компьютер. Маршрутизатор непрерывно сканирует пространство соседних серверов, общается с их маршрутизаторами, и потому знает состояние своего окружения. Он знает, когда какой-то из соседей “закрыт” на техническое обслуживание или просто перегружен. Принимая решение о переправке проходящего TCP - пакета, маршрутизатор учитывает состояние своих соседей и динамически перераспределяет потоки так, чтобы пакет ушел в том направлении, которое в данный момент наиболее оптимально.

Шлюзы

Локальные сети, работающие на основе своих протоколов (не *TCP/IP,* а других) подключаются к узловым компьютерам Интернета с помощью так называемых *шлюзов.* Опять-таки, шлюзом может быть специальный компьютер, но это может быть и специальная программа. Шлюзы выполняют преобразование данных из форматов, принятых в локальной сети, в формат, принятый в Интернете, и наоборот.

Многоликость Интернета

Интернет столь многолик и многообразен, что если спросить несколько разных людей о том, что в нем главное, то они, скорее всего, дадут разные ответы.

Один может сказать, что Интернет — это всемирное объединение разнообразных информационных сетей, основанных на *любых* физических принципах и использующих *любые* каналы связи от телефонных до спутниковых и волоконно-оптических.

Другой скажет, что каналы связи — это не главное, поскольку они существовали давным-давно, когда никакого Интернета и в помине не было. А то, что множество сетей можно объединить в одну, так это уже сто лет как делается в телефонии, энергетике и на транспорте. Поэтому главная особенность Интернета в том, что это не просто сеть, а всемирная информационно-справочная служба. Его можно рассматривать как хитросплетенную паутину, состоящую из сотен миллионов взаимосвязанных документов. Начав читать один документ, можно из него перейти в другой, потом — в третий, и так далее — до любого.

Третий скажет, что оба подхода *узколобы и однобоки.* За ними не видно человека и его потребностей. Один действительно любит копаться в документах, а другому подавай новейшие компьютерные игры. Третьему же не надо ни того, ни другого — он хочет общаться с людьми по всему свету и не платить при этом сумасшедшие деньги за телефонные звонки. Так что главное в Интернете — совокупность сервисов, которые с его помощью можно получить-(эти сервисы называются *службами).*

Для потребителя Интернет представляется как множество служб, больших и малых. Их даже нет смысла перечислять, поскольку каждый день создаются новые и отмирают старые.

Четвертый человек может сказать, что все это ерунда. От всех других видов сетей Интернет отличается автоматизацией. Деятельность всех служб обеспечивается компьютерами и программами — они и составляют суть Интернета. Для тех, кто поставляет информацию — одни программы, а для тех, кто ее получает — другие. Можно вообще забыть и о каналах связи, и о службах, и об Интернете, а думать только о своем компьютере. Сколько на нем жестких дисков? Один? Два? Забудьте об этом. Представьте себе, что Интернет — это миллион жестких дисков, подключаемых к вашему компьютеру. Какая вам разница, что к своим жестким дискам компьютер обращается с помощью внутренних шлейфов, а к чужим — с помощью внешних линий связи? Главное в Интернете — те программы, с помощью которых это можно сделать. Никто не возьмет от Интернета больше, чем позволят его программы. Не будь у клиента специальных программ — не было бы и Интернета, хоть трижды соедини все компьютеры планеты между собой.

Пятый человек может сказать, что все эти рассуждения неконкретны, а Интернет на самом деле — это совокупность протоколов, которым все подчиняется. Ну как бы работали в едином комплексе самые разные модели компьютеров, разнообразные каналы и линии связи, десятки тысяч программ и сотни служб? С его точки зрения Интернет — это именно совокупность единых стандартных протоколов. Они и составляют его лицо.

Скажем прямо: все приведенные выше высказывания об Интернете - правильные, но ни одно из них не характеризует Интернет полностью. Его надо рассматривать шире и глубже.

4.2. Уровни сетевой модели Интернета

Пользовательский уровень. Представим себе, что мы сидим за компьютером и работаем во Всемирной сети. На самом деле мы работаем с программами, установленными на нашем компьютере. Назовем их *клиентскими программами.* Совокупность этих программ и представляет для нас наш *пользовательский уровень.* Наши возможности в Интернете зависят от состава этих программ и от их настройки. То есть, *на пользовательском уровне наши возможности работы в Интернете определяются составом клиентских программ.*

На таком уровне Интернет представляется огромной совокупностью файлов с документами, программами и другими ресурсами, для работы с которыми и служат наши клиентские программы. Чем шире возможности этих программ, тем шире и наши возможности. Есть программа для прослушивания радиотрансляций — можем слушать радио; есть программа для просмотра видео — можем смотреть кино, а если есть *почтовый клиент* — можем получать и отправлять сообщения электронной почты.

Уровень представления. А что дает нам возможность устанавливать на компьютере программы и работать с ними? Конечно же, это его операционная система. Она выступает посредником между человеком, компьютером и программами.

На втором уровне и происходит “разборка” с моделью компьютера и его операционной системой. Выше этого уровня они важны и играют роль. Ниже — уже безразличны. Все, что происходит на нижележащих уровнях, одинаково относится ко всем типам компьютеров.

Если взглянуть на Интернет с этого уровня, то это уже не просто набор файлов — это огромный набор “дисков”.

Сеансовый уровень. Давайте представим себе компьютер с тремя жесткими дисками. У компьютера есть три владельца. Каждый настроил операционную систему так, чтобы полностью использовать “свой” диск, а для других пользователей сделал его скрытым. Свою работу они начинают с регистрации — вводят имя и пароль при включении компьютера.

Если спросить одного из них, сколько в ее компьютере жестких дисков, то он ответит, что только один, и будет прав — в своем *персональном сеансе работы с* компьютером он никогда не видел никаких иных дисков. Того же мнения будут придерживаться и двое других. Такой же взгляд на Интернет открывается с высоты *сеансного уровня.*

Подключение к Интернету и наличие необходимых клиентских программ еще не означает, что нас в Интернете ждут. То есть, связаться с приятелем, конечно, можно, но со штаб-квартирой ЦРУ нас не соединят. Надо либо иметь соответствующие права, либо знать заветное слово. А если нет ни того, ни другого, то и некоторых секторов Интернета в наших сеансах не будет.

Транспортный уровень. Предположим, что заветное слово у нас имеется, и мы можем отправить запрос на получение файла с игрой (картинкой, статьей, музыкой). А как этот запрос должен кодироваться? Это зависит от сети. Внутри университетской сети действуют одни правила, вне ее — другие. Эти правила называют *протоколами.* Интернет — он потому и считается всемирной сетью, что на всем ее пространстве действует один единый транспортный протокол —*TCP.* На тех компьютерах, через которые к Интернету подключены малые *локальные сети,* работают *шлюзы.* Шлюзовые программы преобразуют потоки данных из формата, принятого в локальных сетях или на автономных компьютерах, в единый формат, принятый в Интернете.

Таким образом, если взглянуть на Интернет на этом уровне, то можно сказать, что это глобальная компьютерная сеть, в которой происходит передача данных с помощью протокола *TCP.*

Сетевой уровень. А что, если соединить между собой пару компьютеров и пересылать между ними данные, нарезанные на пакеты по протоколу *TCP?* Это тоже будет Интернет?

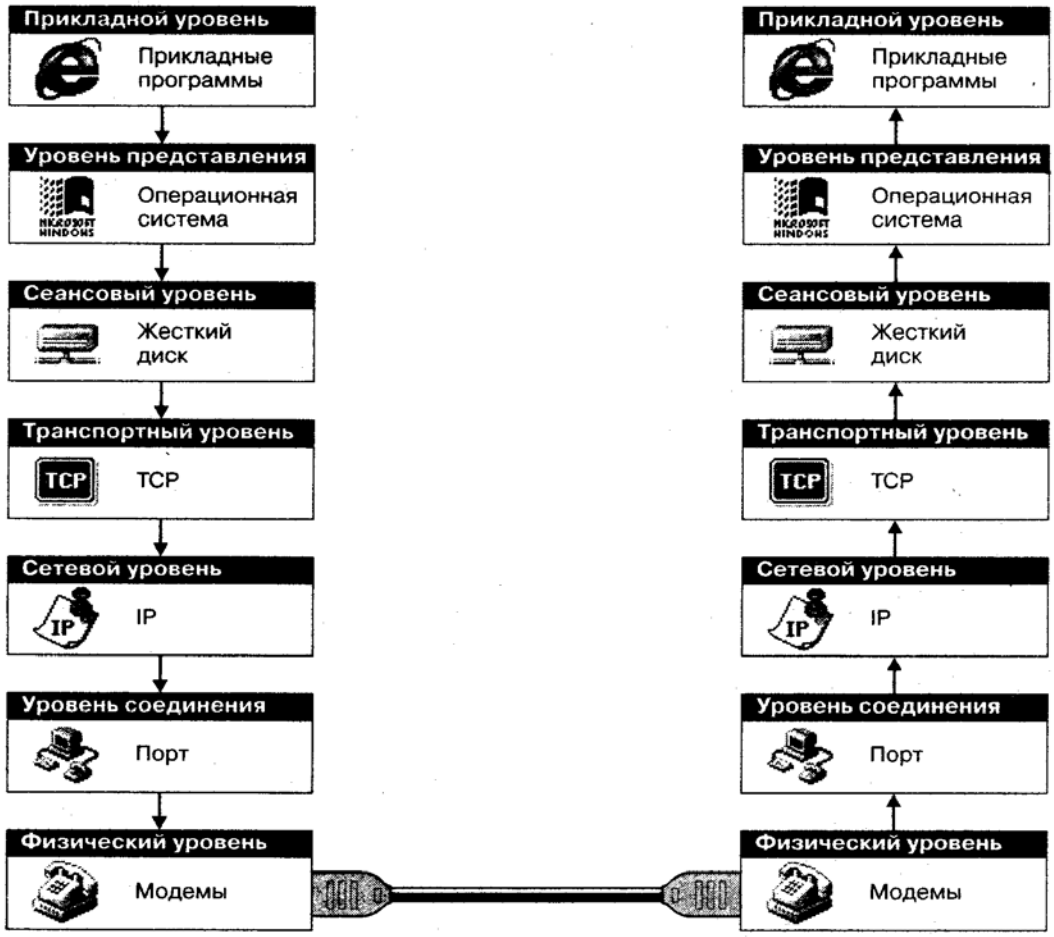
Нет, это будет не Интернет, а *интранет* — разновидность локальной сети. Такие сети существуют — их называют *корпоративными.* Они популярны тем, что все пользовательские программы, разработанные для Интернета, можно использовать и в интранете. Не правда ли, удобно работать с компьютером, установленным в соседней комнате, теми же средствами, которыми мы работаем с компьютерами, находящимися в Америке?

Интернет отличается от локальных сетей не только единым транспортным протоколом, но и единой системой адресации. Подведем итог. Если взглянуть на Интернет с пятого уровня, то можно сказать, что Интернет — это всемирное объединение множества компьютеров, каждый из которых имеет уникальный IP-адрес.

Уровень соединения. Дело подходит к тому, чтобы физически передать сигналы с одного компьютера на другой, например с помощью модема. На этом уровне цифровые данные из пакетов, созданных ранее, накладываются на физические сигналы, генерируемые модемом, и изменяют их (принято говорить *модулируют).* Как и все операции в компьютере, эта операция происходит под управлением программ. В данном случае работают программы, установленные вместе с драйвером модема. При взгляде с шестого уровня Интернет — это совокупность компьютерных сетей или автономных компьютеров, объединенных всевозможными (любыми) средствами связи.

Физический уровень. При взгляде с самого “низкого” уровня Интернет представляется как всемирная паутина проводов и прочих каналов связи. Сигнал от одного модема (или иного аналогичного устройства) отправляется в путь по каналу связи к другому устройству. Физически этот сигнал может быть пучком света, потоком радиоволн, пакетом звуковых импульсов и т. п. На физическом уровне можно забыть о данных, которыми этот сигнал промодулирован. Люди, которые занимаются Интернетом на этом уровне, могут ничего не понимать в компьютерах.

4.3.Назначение WWW - сервера. Общая схема работы.СЕРВЕР NCSA.



Семиуровневая модель архитектуры Интернета

Широкие возможности WWW - технологии по представлению пользователям Internet информации, включая текст, картинки, графики, видео и звуковые дорожки, обусловили процесс бурного роста сети WWW - серверов и Internet в целом. Целью данного пособия является освещение технологии работы и процессов установки и администрирования WWW - сервера, т.е. той части сети, которая отвечает за предоставление гипертекстовой информации по запросам пользователей сети.

Назначение WWW - сервера. Общая схема работы.

WWW сервер - это такая часть глобальной или внутрикорпоративной сети, которая дает возможность пользователям сети получать доступ к гипертекстовым документам, расположенным на данном сервере. Для взаимодействия с WWW сервером пользователь

сети должен использовать специализированное программное обеспечение - броузер (от англ. browser), другое название - программа просмотра.

Схема работы

Рассмотрим более подробно, чем в предыдущих главах, схему работы WWW-сервера. В общем виде она выглядит так:

1. Пользователь сети запускает пакет программного обеспечения, называемый ***броузером,*** в функции которого входит
   - Установление связи с сервером
   - Получение требуемого документа
   - Отображение полученного документа
   - Реагирование на действия пользователя - доступ к новому документу
   - После запуска броузер по команде пользователя или автоматически устанавливает связь с заданным WWW - сервером и передает ему запрос на получение заданного документа (см рис.).

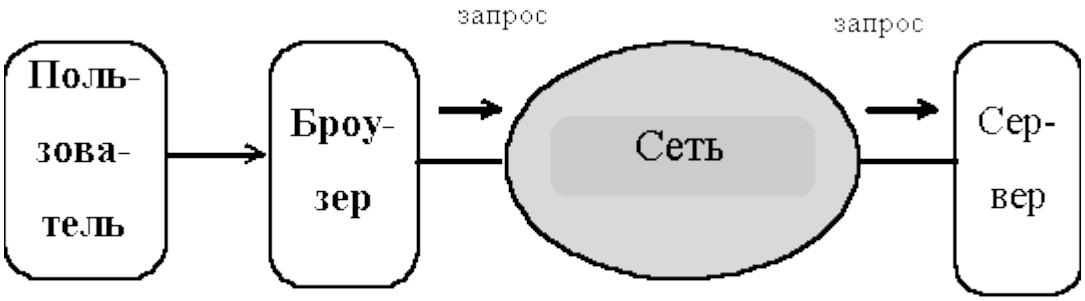


Рис. 3-1

2. WWW сервер ищет запрашиваемый документ и возвращает результаты броузеру (см. рис. 3-2).

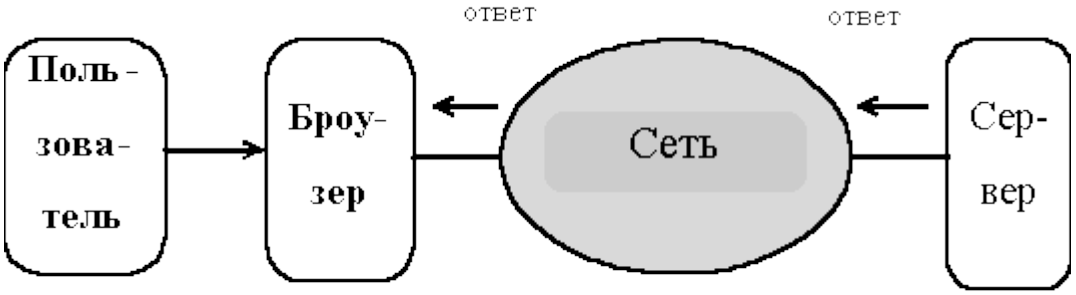


Рис 3-2

3. Броузер, получив документ, отображает его пользователю и ожидает его реакции. Возможные варианты:

   - Ввод адреса нового документа
   - Печать, поиск, другие операции над текущим документом
   - Активизация (нажатие) специальных зон полученного документа, называемых ***связями*** (link) и ассоциированными с адресом нового документа.

В первом и третьем случае происходит обращение за новым документом.

Адрес

Адрес документа указывается в виде специальной строки, называемой **URL**. Для протокола HTTP, используемого при взаимодействии WWW клиента и WWW сервера, URL состоит из следующих компонент:

1. Наименование протокола, по которому работает сервер (http).
2. Имя машины - сервера в Internet или ее IP - номер.
3. Порт TCP, обращение к которому обрабатывает сервер.
4. Место (путь) документа на машине - сервере.

Например:
http://www.cnit.nsu.ru:80/welcome.html

Здесь ***http*** означает протокол работы с WWW - сервером

- '***:***' - разделитель
- "***www.cnit.nsu.ru***" - имя машины - сервера в Internet
- "***80***" - номер tcp - порта
- ***/welcome.html*** - путь до документа на машине - сервере

Из общей схемы работы видно, что функции WWW сервера заключаются в следующем:

1. Установление соединения с клиентским ПО по протоколу tcp.
2. Принятие запроса на документ по протоколу http.
3. Поиск документа в локальных ресурсах.
4. Возврат результатов поиска по протоколу http.

В общем случае, **WWW - сервером** будем называть программно - аппаратный комплекс, предназначенный для выполнения вышеперечисленных действий.

Среда работы сервера

В настоящее время все известные WWW - серверы представляют собой компьютер общего назначения с многозадачной операционной системой. Один или несколько процессов такой системы отвечают за поддержку специфических для WWW - сервера функций. Другие процессы ОС отвечают за обеспечение других функций, не обязательно связанных с поддержкой технологии WWW (см. рис. 3-3).

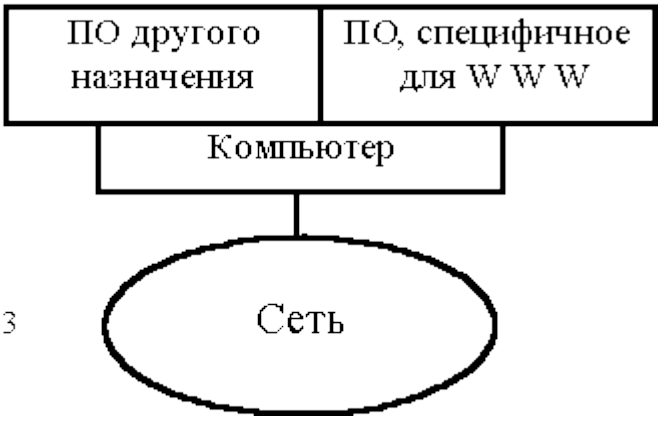


Рис. 3-3

Такая структура приводит к тому, что под WWW сервером начинают подразумевать только часть программного обеспечения, единственными функциями которой являются функции WWW сервера, а остальную часть - компьютер, операционную систему, другие процессы, сетевую структуру называют средой работы WWW сервера или платформой. Ниже приведена таблица 3-1, содержащая список наиболее распространенных платформ для WWW - сервера.

Таблица 3-1

Компьютер	Операционная Система
IBM PC	• Unix (UnixWare, Open Server, Solaris, BSD, Linux и т.д. • Microsoft Windows NT • IBM OS/2 • Novell NetWare
Sun SparcStation и SparcServer	• SunOS • Solaris
Silicon Graphics серверы и рабочие станции	IRIS

Непосредственные функции сервера. Базовые определения

В простейшем случае гипертекстовый документ представляет собой совокупность файлов. Представление этих файлов как единого документа производится броузером. По каждому файлу документа броузер делает запрос к WWW - серверу. Таким образом, сервер не имеет представления о структуре и составе документов, он отвечает только за выдачу локальных файлов по запросам.

На различных платформах, в различных операционных системах пути файлов выглядят по разному.

Например:
D:\DOCUMENTS\HTML\INDEX.HTM - в Windows,
/u/data/www/html/index.html - в Unix - системах,
USR:WWW/HTML - в NetWare и т.д.

Путь файла, указываемый в URL, имеет стандартный вид:

/<имя_каталога>/ ... /<имя_каталога>/<имя_файла>

Таким образом, в функции WWW - сервера входит преобразование адреса из внешнего единого формата в платформенно ориентированный внутренний формат. Появляется ряд понятий, специфичных для такого преобразования, необходимых для него.

Исходный каталог документов

Это каталог реальной файловой системы сервера, от которого идет вычисление пути, указанного в URL.

Например, если исходным каталогом документов является ***D:\Documents\HTML***, то на запрос к этому серверу документа по URL

http://<имя_сервера>/index.htm

будет возвращен файл

D:\Documents\HTML\index.htm

Синонимы

В случае, когда необходимо осуществить обращение к конкретному каталогу или файлу, находящемуся вне иерархии *Исходного каталога документов,* используется механизм синонимов. Синоним позволяет явно определить соответствие между путем, указанным в URL, и путем локальной файловой системы.

Например:
Синонимом для ***/Harvest*** объявляется ***/projects/www/harvest*** или

синонимом для ***/test/myfile.html*** объявляется ***C:\MYDIR\FILE.HTM***

В первом случае все обращения к файлам каталога ***/Harvest*** будут обрабатываться в каталоге ***/projects/www/harvest***. Второй пример показывает работу синонима с конкретным файлом файловой системы.

Индексный файл

Для каждого сервера определено имя так называемого индексного файла. Обычно этот файл содержит ссылки на другие файлы данного каталога. Содержимое индексного файла выдается сервером в случае, если в URL указан каталог без конкретного файла.

Пользовательский раздел

Для многопользовательских операционных систем (таких как Unix) ПО WWW - сервера позволяет каждому пользователю предоставлять доступ к своему собственному набору гипертекстовых документов вне основной иерархии (*Исходного каталога документов, Синонимов* и т.д.). Этот набор документов должен находиться в собственном (т.н. "домашнем") каталоге пользователя. Для доступа к таким документам в URL перед путем ставится знак тильда и имя пользователя: ~<имя_пользователя>.

Например:
На сервере ***Indy.cnit.nsu.ru*** создан пользователь с именем fancy и "домашним" каталогом ***/home/fancy***. Собственные гипертекстовые документы он хранит в каталоге ***/home/fancy/public_html***. При обращении по URL ***http://Indy.cnit.nsu.ru/~fancy/start.html,*** WWW - сервер будет искать документ ***start.html*** в каталоге ***/home/fancy/public_html.***

Протокол MIME

Протокол MIME - многоцелевое расширение электронной почты, был создан как способ передачи нетекстовой информации: изображений, звука, видео в письмах электронной почты. Механизм оказался удачным, и его перенесли и в on-line сервисы, в том числе WWW. Здесь MIME используется для передачи документов от сервера к клиенту.

В общем виде MIME основывается на передаче вместе с основными данными дополнительной информации, описывающей что это и в каком виде передается. Эта дополнительная информация называется **заголовок MIME**. Базовой частью заголовка является строка, описывающая тип передаваемого сообщения. Формат строки:

Content-Type: <тип_MIME>

Перечень типов MIME (т.е. видов передаваемых данных) постоянно пополняется и может быть дополнен даже пользователем для описания своего собственного вида данных. Формат типа MIME:

<Тип> **/** *<Подтип>* [**;** *<параметры>*]

Где <Тип> - определяет общий тип данных:
Audio - для звуковых данных
Application - данные, являющиеся входными для какого-либо приложения (программы)
Image - для графических образов
Message - для сообщения, которое само по себе является MIME - документом
Multipart - для сообщения, состоящего из нескольких MIME - документов
Text - для текстовых данных в различном виде
Video - для видеоданных.
<Подтип> - указывает на специфический формат данных типа <Тип>

Например:
text/html - текстовые данные в формате HTML
image/giff - графические данные в формате gifF
<Параметры> - список параметров, необходимых для интерпретации данных.

Для ведения специфичной обработки файлов различных типов и форматов на клиентской и серверной частях поддерживаются списки соответствий типов MIME и расширений файлов. Формат записи такого списка:

<Тип>/<Подтип> <расширение1> ... <расширениеN>

Эти списки сопоставляют всем файлам, имеющим определенные расширения, определенные типы MIME.

Например:
image/giff gif giff
text/html html htm

В первой строке всем файлам с расширением gif и giff приписывается тип содержимого image/giff. Если для типа содержимого image/giff определены специальные правила обработки (например, отображение на экране в определенной области), то так будут обрабатываться все файлы с расширениями gif и giff.

Протокол HTTP

Протокол HTTP определяет язык запросов от WWW - клиента к WWW - серверу. Сам запрос состоит из следующих компонент:

<Заголовок>
<Метод> <Источник / Данные>

где
Заголовок - определяет версию протокола HTTP и другие служебные параметры;
Метод - одно из ключевых слов:
GET - для передачи запросов на выдачу документов
PUT, **POST** - для передачи данных от клиента к серверу (например, из форм)

Пример запроса:
HTTP/1.1
GET /index.html

Описывает запрос на получение файла index.html из корневого каталога документов сервера.

Интерфейс CGI

Помимо доступа к статическим документам сервера существует возможность получения документов как результата выполнения прикладной программы. Такая возможность реализуется на сервере WWW благодаря использованию интерфейса CGI (Common Gateway Interface). Спецификация CGI описывает формат и правила обмена данными между ПО WWW сервера и запускаемой программой.

Для инициирования CGI необходимо, чтобы в запрашиваемом URL был указан путь до запускаемой программы. ПО WWW сервера исполняет эту программу, передает ей входные параметры и возвращает результаты ее работы, как результат обработки запроса, клиенту. CGI - программой может являться любая программа локальной операционной системы сервера - в двоичном виде или в виде программы для интерпретатора (Basic, SH, Perl и т.д.).

С целью облегчения администрирования CGI - программ, а также для удовлетворения требованиям безопасности CGI - программы группируются в одном или нескольких явно указанных серверу каталогах. По умолчанию это каталог ***cgi-bin*** в иерархии серверных каталогов, однако, его имя и положение могут отличаться.

Например:
клиент, обращающийся к CGI - программе test-query, будет использовать URL ***http://<имя_сервера>/cgi-bin/test-query***

Интерфейс CGI позволяет расширить границы применения WWW - технологии. CGI - программа может обрабатывать сигналы с датчиков установок, взаимодействовать с мощным сервером баз данных, переводить и т.п. Полное описание интерфейса и требований к приложениям, использующих его, приведены в главе 4 настоящего отчета.

СЕРВЕР NCSA

Национальный Центр по Суперкомпьютерным Приложениям (NCSA) Иллинойского университета стал второй организацией после ЦЕРН, интенсивно взявшейся за развитие WWW - технологии. Семейство ПО WWW - серверов NCSA прошло длинный путь развития. Последние версии поддерживают все современные возможности, включая виртуальные узлы, управление доступом, параллельную обработку запросов и т.п.

Требования к ресурсам

Программное обеспечение сервера NCSA представляет собой прикладное программное обеспечение, предназначенное для работы под ОС Unix. В зависимости от аппаратной платформы требуемый размер оперативной памяти и дискового пространства существенно изменяются. Для семейства "Unix для PC" (Solaris, SCO, UnixWare, Linux, BSD, BSDI), необходимо ориентироваться на 2 Mb оперативной памяти. Дисковое пространство, требуемое при установке, составляет около 2Mb, однако при планировании установки нужно учитывать, что при интенсивном доступе к серверу статистика доступа будет составлять до нескольких сот килобайт в день и нескольких десятков мегабайт в месяц.

Состав дистрибутива сервера NCSA. Варианты дистрибуции

Сервер NCSA поставляется как в виде исходных текстов, так и в виде исполняемых модулей для различных операционных систем. Распакованный дистрибутив размещается в каталоге ***httpd_<номер версии>-<модификация>*** где <номер версии> - версия программного обеспечения WWW сервера, <модификация> - модификация текущей версии.

Например:
httpd_1.5.1-export

В этом каталоге содержатся следующие файлы и подкаталоги:

README - текстовый файл для первоначального ознакомления. Содержит список всех значимых файлов и каталогов с объяснением их назначения.

COPYRIGHT - текстовый файл с описанием лицензионного соглашения на использование ПО WWW - сервера NCSA.

CHANGES - текстовый файл со списком изменений между различными версиями ПО сервера.

Makefile - файл верхнего уровня для утилиты make. Содержит список команд, которые необходимо выполнить для сборки и установки ПО WWW - сервера.

src - каталог с исходными текстами ПО сервера.

conf - каталог, содержащий примеры конфигурационных файлов ПО сервера.

icons - каталог, содержащий иконки, необходимые для работы сервера.

cgi-bin - каталог, содержащий примеры CGI - программ.

cgi-src - каталог, содержащий исходные тексты примеров CGI - программ.

support - каталог с программным обеспечением, не являющимся часью ПО сервера, но полезным при работе с ним.

Процедура установки сервера NCSA

Для запуска процедуры сборки и установки сервера необходимо в корневом каталоге сервера, описанном в предыдущем параграфе, запустить утилиту ***make***. Для сборки сервера необходимо указать команде make аббревиатуру операционной системы:

aix3, aix4, sunos, sgi4, sgi5, hp-cc, hp-gcc, solaris, netbsd, svr4, linux, next, ultrix, osf1, aux, bsdi. Полный список поддерживаемых систем можно получить, выполнив команду make без параметров. Каждая аббревиатура ассоциирована с конкретной операционной системой. Появление дополнительных параметров после дефиса указывает на специфику конкретной конфигурации в одной и той же ОС. Например, ***hp-cc*** и ***hp-gcc*** указывают на общий тип ОС - HP-UX, однако ориентированы на использование разных компиляторов - базового C - компилятора (cc) или GNU C (gcc). Для сборки сервера под ОС UnixWare необходимо использовать команду ***make svr4***.

Ряд основных параметров сервера - пути файлов, режимы работы задаются по умолчанию на этапе сборки. В случае, если нужна их корректировка под конкретные условия, необходимо отредактировать файл ***src/config.h***.

После сборки сервера необходимо разместить его компоненты в файловой системе. Исполняемый модуль сервера ***httpd*** размещается в каталоге серверных программ - ***/usr/local/sbin*** или ***/usr/sbin***. Файлы конфигурации, журналы и стандартные cgi-программы размещаются в подкаталогах каталога, определяемого параметром ServerRoot. Обычно это ***/usr/local/etc/httpd***, однако его можно изменить либо изменив параметр HTTPD_ROOT файла ***src/config.h***, либо указав ключ ***-d*** при запуске сервера.

Например:
/usr/local/sbin/httpd -d /var/httpd

В каталоге, определяемом параметром ServerRoot, размещаются три подкаталога:

- ***conf/*** - содержащий файлы конфигурации сервера
- ***logs/*** - содержащий журналы работы сервера
- ***cgi-bin/*** - содержащий стандартные cgi-программы, поставляемые с сервером.

4.4.Web-страницы

Все Web-страницы Интернета имеют одну общую черту – они созданы с помощью средств языка HTML. HTML – не обычный язык программирования, хотя процесс создания Web-страницы очень близок к процессу программирования. HTML – это язык разметки гипертекста. Он определяет правила, согласно которым обычный текст представляется в виде Web-страниц

World Wide Web и HTML

Современный этап развития Интернета начался в начале 90-х годов с появлением нового *протокола* обмена информацией. Этот протокол называется *HTTP (HyperText Transfer Protocol – протокол передачи гипертекста).* Вместе с этим протоколом появилась и служба *World Wide Web* (часто также называемая *WWW* или просто *Web),* которая представляет собой обширную сеть серверов HTTP, передающих файлы через Интернет.

Основную часть этих файлов представляют собой *Web-страницы* – специальные файлы, написанные на языке *HTML (HyperText Markup Language – язык разметки гипертекста).* Web-страницы *публикуются,* в Интернете путем размещения таких файлов на *серверах HTTP (Web-узлах).* Содержание Web-страниц может быть разным и посвященным совершенно произвольным темам, но все они используют одну и ту же основу – язык HTML. Документы HTML обычно имеют расширение .HTM или .HTML

Язык HTML появился одновременно со службой World Wide Web и развивался вместе с ней, постепенно вбирая в себя новые черты, которые позволяли создавать все более и более впечатляющие Web-страницы. Он является основой World Wide Web и одновременно

причиной ее широчайшей популярности. Смысл и назначение языка HTML можно понять, исходя из его названия.

Гипертекст – это текст, в который встроены специальные коды, управляющие дополнительными элементами, такими как форматирование, иллюстрации, мультимедийные вставки и гиперссылки на другие документы. Под *разметкой* понимается вставка в текст этих кодов, определяющих то, как итоговый гипертекстовый документ должен отображаться специальной *программой-броузером.* Разметка может быть простой или сложной, но в любом случае исходный текст сохраняется в документе в неизменном виде. Но самое важное слово в этом описании – *язык.* HTML представляет собой компьютерный язык, в некотором смысле родственный языкам программирования. Он включает достаточно строгие правила, которые необходимо соблюдать, чтобы получить правильные результаты.

Назначение языка HTML

Несмотря на то, что Web-страницы появляются на экране компьютера в отформатированном виде, язык HTML не предназначен для форматирования документов, поскольку жесткое задание оформления и точное позиционирование элементов текста на странице приводит к ограничениям, недопустимым в Интернете.

Так, например, когда мы форматируем текст с помощью текстового процессора Word, мы *однозначно* определяем, как должен выглядеть этот текст при печати на *совершенно определенном принтере* и на бумаге *заданного формата.* Когда документ размещен в Интернете, невозможно предсказать, какой компьютер будет использован для его просмотра, да и будет ли вообще у этого компьютера монитор.

Может быть, текст появится на экране компьютера, работающего в системе Windows в окне одного из современных броузеров. Может быть, это будет текстовый броузер (неспособный отображать графику), работающий в системе MS-DOS. Возможно, текст документа вообще не будет отображаться на экране, а будет воспроизводиться вслух с помощью синтезатора речи. Для слепого пользователя документ может выводиться на специальное устройство шрифтом Брайля.

В связи с необходимостью подготавливать документы для столь разнообразных устройств язык HTML не предназначен для описания формата документа. Он служит для *функциональной разметки документа,* то есть позволяет определить *назначение* фрагментов текста.

Например, если в тексте встречается заголовок, то код HTML просто указывает, что соответствующий фрагмент является заголовком. Получив такой код, программа просмотра (броузер) сама «решает», что ей делать с заголовком. Возможно, она отобразит его более крупным шрифтом, а может быть выравняет по центру экрана. Возможно, что синтезатор речи, воспроизводящий текст документа, использует код заголовка для того, чтобы повысить громкость и сделать необходимую интонационную паузу.

Язык HTML все-таки имеет некоторые команды форматирования, но общий курс на разделение содержания и оформления документа выдерживается четко. В последней версии HTML 4.0 использовать команды форматирования, как правило, не рекомендуется.

Теги HTML

Коды языка HTML, с помощью которых выполняется разметка исходного текста, называются *тегами.* Тег – это набор символов. Все теги начинаются с символа «меньше» (<) и заканчиваются символом «больше» (>). Пару этих символов иногда называют *угловыми скобками.* После открывающей угловой скобки идет *ключевое слово,* определяющее тег.

Каждый тег в языке HTML имеет специальное назначение. Регистр букв в названиях тегов не имеет значения – можно использовать как строчные, так и прописные буквы, хотя общепринято использовать прописные буквы, чтобы теги отличались от обычного текста документа.

Как правило, один тег HTML воздействует только на часть документа, например на абзац. В таких случаях используют парные теги: *открывающий* и *закрывающий.*

Открывающий тег создает эффект, а закрывающий – прекращает его действие. Закрывающие теги начинаются с символа косой черты (/).

Некоторые теги дают разовый эффект в месте своего появления. В этом случае необходимости в закрывающем теге нет, и он не употребляется.

Если по ошибке в теге указано ключевое слово, отсутствующее в языке HTML, то тег игнорируется целиком.

При отображении документа в броузере сами теги не отображаются, но влияют на способ отображения документа.

Атрибуты тегов

Открывающие теги часто могут содержать *атрибуты,* влияющие на эффект, создаваемый тегом. Атрибуты – это дополнительные ключевые слова, отделенные от ключевого слова тега и друг от друга пробелами.

Многие атрибуты требуют указания *значения атрибута.* Это значение отделяется от ключевого слова знаком равенства (=). Значение атрибута должно заключаться в кавычки, но во многих случаях эти кавычки могут опускаться без какого-либо вреда. Закрывающие теги никогда не содержат атрибутов.

Комментарии

В языках программирования общепринята возможность использования комментариев – текстовых строк, не являющихся частью программы, а служащих для пояснения. Язык HTML тоже имеет такую возможность.

Комментарии в языке HTML начинаются со специального тега <!-- . Следует обратить внимание на отсутствие закрывающей угловой скобки. Любой текст, идущий за этим тегом, рассматривается как комментарий и не отображается при отображении документа.
Заканчивают комментарий символами -->. Комментарий может содержать любые символы, кроме символа «больше» (>), и, таким образом, не может включать в себя теги.

Структура документа HTML

Примеры тегов HTML:

<title> <Body> <TABLE> </A> <img> </Center>

Примеры парных тегов HTML:

<HTML>	</HTML>
<B>	</B>
<HEAD>	</HEAD>
<H3>	</H3>
<ADDRESS>	</ADDRESS>
<LI>	</LI>

Примеры одиночных тегов HTML

 <HR> <META> <BASEFONT> <FRAME>

Примеры тегов HTML с атрибутами:

<BODY BGCOLOR="#00EEFF" TEXT="#FFFFFF" BACKGROUND="RAIN.GIF">

<FRAME SRC="file.html" NORESIZE>

Документ HTML состоит из основного текста документа и тегов разметки, которые, как мы уже знаем, являются наборами обычных символов. Таким образом, документ HTML – это, по существу, обычный текстовый файл. Для его создания можно использовать любой

текстовый редактор, хотя бы и тот простейший редактор Блокнот, который входит в состав Windows 9x.

1. Все документы HTML имеют строго заданную структуру. Документ должен начинаться с тега <HTML> и заканчиваться соответствующим закрывающим тегом </HTM1>. Эта пара тегов сообщает броузеру, что перед ним действительно документ HTML.

2. Документ HTML состоит т раздела заголовков и тела документа, идущих именно в таком порядке. Раздел заголовков заключен между тегами <HEAD> и </HEAD> и содержит информацию о документе в целом. В частности, этот раздел должен содержать внутри себя теги <TITLE> и </TITLE >, между которыми размещают «официальный» заголовок документа. Большинство броузеров, работающих в системе Windows, используют этот заголовок, чтобы заполнить строку заголовка окна броузера.

3. Сам текст документа располагается в теле документа. Тело документа располагается между тегами <BODY> и </BODY>.

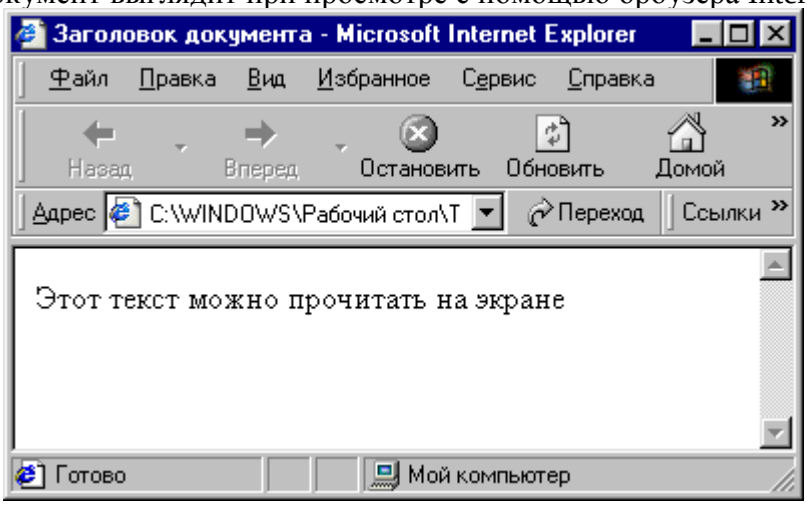
Четыре перечисленных парных тега определяют основную структуру документа HTML. Они встречаются [или их наличие подразумевается) во всех документах HTML.

На практике определить местоположение этих основных структурных тегов можно и при их отсутствии. Поэтому, если теги <HTML>, <HEAD> и <BODY>, а также соответствующие им закрывающие теги опущены, то программа-броузер может сама определить то место, где они должны были находиться. Тег <TITLE>, определяющий заголовок документа, считается обязательным, но и его пропуск не вызовет катастрофических последствий в современных броузерах. Но все-таки при создании Web-страниц опускать все эти теги не рекомендуется, ведь заранее неизвестно, как поведет себя конкретный броузер, установленный на компьютере читателя.

Простейший правильный документ HTML

```
<HTML>
  <HEAD>
    <TITLE> Заголовок документа </TITLE>
  </HEAD>
  <BODY> Этот текст можно прочитать на экране
  </BODY>
</HTML>
```

Вот как этот документ выглядит при просмотре с помощью броузера Internet Explorer:



4.5.Основные теги HTML

Цель работы научить студентов:

- созданию первичного HTML-документа,
- использованию основных тегов,
- построению простейших HTML-документов.

1. HTML-документ – это просто текстовый файл с расширением ИМЯ.htm. Набрать следующий самый простой HTML-документ в блокноте:

```
<html>
   <head> Моя первая страница
      <title>
         Пример 1
      </title>
   </head>
   <body>
      <H1>
         Привет!
      </H1>
      <P>
         Это простейший пример HTML-документа.
      </P>
      <P>
         Этот *.htm-файл может быть одновременно открыт
         и в Notepad, и в Netscape. Сохранив изменения в Notepad,
         просто нажмите кнопку Перезагрузить в Netscape,
         чтобы увидеть эти изменения реализованными в HTML-документе.
      </P>
   </body>
</html>
```

Теперь нужно этот текст сохранить на *Рабочем столе* под именем PROBA.HTM, далее его нужно закрыть. Для просмотра этого текста как в Интернете нужно загрузить с рабочего стола снова файл PROBA. Загрузится этот текст в броузере Internet Explorer**.** Результат этого фрагмента HTML-программы на экране:

Моя первая страница

Привет!

Это простейший пример HTML-документа.
Этот *.htm-файл может быть одновременно открыт и в Notepad, и в Netscape. Сохранив изменения в Notepad, просто нажмите кнопку Перезагрузить в Netscape, чтобы увидеть эти изменения реализованными в HTML-документе.

Для изменения исходного текста программы в виде HTML выполните команду *Вид – В виде HTML* и после каждого изменения нужно выполнить команду *Файл – Сохранить***.**

Для просмотра эти изменения в броузере нужно перейти в Internet Explorer и выполнить команду *Обновить***.**

2. Для удобства чтения введены дополнительные отступы, однако в HTML это совсем не обязательно. Более того, броузеры просто игнорируют символы конца строки и множественные пробелы в HTML-файлах. Поэтому наша программа вполне мог бы выглядеть и вот так:

```
<html>  <head>  <title> Пример 1</title> </head>  <body>  <H1>Привет!</H1>
   <P>     Это простейший пример HTML-документа.</P>
```

```
  <P>    Этот *.htm-файл может быть одновременно открыт и в Notepad, и в
         Internet Explorer. Сохранив изменения в Блокнот, просто сохраните как
         ИМЯ.HTM . Далее закройте и загрузите документ ИМЯ.HTM ,
         чтобы увидеть      эти изменения реализованными в HTML-документе.</P>
</body> </html>
```

Результат работы на экране:

Привет!

Это простейший пример HTML-документа.

Этот *.htm-файл может быть одновременно открыт и в Notepad, и в Internet Explorer. Сохранив изменения в Блокнот, просто сохраните как ИМЯ.HTM . Далее закройте и загрузите документ ИМЯ.HTM, чтобы увидеть эти изменения реализованными в HTML-документе.

3. В нашем простейшем документе

<html> ... </html>

Метка <html> должна открывать HTML-документ. Аналогично, метка </html> должна завершать HTML-документ.

<head> ... </head>

Эта пара меток указывает на начало и конец заголовка документа. Помимо наименования документа (см. описание метки <title> ниже), в этот раздел может включаться некоторые служебные информации.

<title> ... </title>

Все, что находится между метками <title> и </title>, толкуется браузером как название документа. *Internet Explorer*, например, показывает название текущего документа в заголовке окна и печатает его в левом верхнем углу каждой страницы при выводе на принтер. Рекомендуется название не длиннее 64 символов.

<body> ... </body>

Эта пара меток указывает на начало и конец тела HTML-документа, каковое тело, собственно, и определяет содержание документа.

<H1> ... </H1> – <H6> ... </H6>

Метки вида <Hi> (где i - цифра от 1 до 6) описывают заголовки шести различных уровней. Заголовок первого уровня – самый крупный, шестого уровня, естественно – самый мелкий.

<P> ... </P>

Такая пара меток описывает абзац. Все, что заключено между <P> и </P>, воспринимается как один абзац. Метки <Hi> и <P> могут содержать дополнительный атрибут ALIGN (читается "элайн", от английского "выравнивать"), например:
<H1 ALIGN=CENTER>Выравнивание заголовка по центру</H1>
или
<P ALIGN=RIGHT>Образец абзаца с выравниванием по правому краю</P>
4. Подытожим все, что мы знаем, и поработаем с помощью примера 2:

```
<html>
  <head>
   <title>Пример 2</title>
  </head>
  <body>
    <H1 ALIGN=CENTER>Привет!</H1>
    <H2>Это чуть более сложный пример HTML-документа</H2>
    <P>Теперь мы знаем, что абзац можно выравнивать не только влево, </P>
    <P ALIGN=CENTER>но и по центру</P> <P ALIGN=RIGHT>или по
        правому краю.</P>
  </body>
</html>
```

Результат на экране:

Привет!

Это чуть более сложный пример HTML-документа

Теперь мы знаем, что абзац можно выравнивать не только влево,

но и по центру

или по правому краю

С этого момента Вы знаете достаточно, чтобы создавать простые HTML-документы самостоятельно от начала до конца.

5. Теперь рассмотрим, как можно улучшить наш простой HTML-документ. Для отделения абзацев друг от друга иногда используется следующий тег.

**
**

Эта метка используется, если необходимо перейти на новую строку, не прерывая абзаца. Очень удобно при публикации стихов. Следующий пример демонстрирует использование этого тега.

```
<html>  <head>  <title> Пример 3 </title>  </head>
  <body>
    <H2> Стихотверения Абая </H2>
    <P> А того, кто жил не любя, <BR> Человеком назвать нельзя. <BR>
          Пусть ты наг и нищ – утебя <BR> Все же есть семья и друзья. <BR>
    <P>Ясный свет юных лет, <BR>  Вера в жизнь и мечту, <BR>
          С чем сравнить внешний цвет, <BR> Юных лет красоту!  <BR>
  </body>
</html>
```

Результат работы этого фрагмента на экране:

Стихотверения Абая

А того, кто жил не любя,
Человеком назвать нельзя.
Пусть ты наг и нищ – утебя
Все же есть семья и друзья.

Ясный свет юных лет,
Вера в жизнь и мечту,
С чем сравнить внешний цвет,
Юных лет красоту!

<HR>

Метка <HR> без атрибутов описывает вот такую горизонтальную линию:

Метка может дополнительно включать атрибуты SIZE (определяет толщину линии в пикселах) и/или WIDTH (определяет размах линии в процентах от ширины экрана). В примере 4 приведена небольшая коллекция горизонтальных линий.

```
<html>
  <head>
   <title>Пример 4</title>
  </head>
  <body>
            <H1>Коллекция горизонтальных линий</H1>
            <HR SIZE=2 WIDTH=100%> <BR>
            <HR SIZE=4 WIDTH=50%> <BR>
            <HR SIZE=8 WIDTH=25%> <BR>
            <HR SIZE=16 WIDTH=12%> <BR>
  </body>
</html>
```

Результат работы этого фрагмента программы на экране:

Коллекция горизонтальных линий

6. Для задания размера, цвета и начертания шрифта служит тег <FONT>. Этот парный тег влияет на весь текст, заключенный между открывающим и закрывающим тегами. Тег <FONT> должен иметь хотя бы один из трех возможных атрибутов: **SIZE= … COLOR= … FACE= ...**

Атрибут SIZE= … задает размер шрифта. Предполагается, что возможны семь заранее заданных размеров шрифта (от 1 до 7). Эти значения не соответствуют каким-либо единицам измерения, но чем больше значение, тем крупнее шрифт. По умолчанию используется значение 3.

Атрибут COLOR=… задает цвет шрифта, который может быть задан либо ключевым словом (например, RED – красный), либо шестнадцатиричным значением в системе *RGB* (например, #FF0000 – это тоже красный).

Атрибут FACE= … задает вид шрифта. Значением этого атрибута должно быть название одного из шрифтов, установленных на компьютере. Но для документа, размещенного в Интернете, нельзя предсказать, какие шрифты доступны на компьютере пользователя, поэтому этот атрибут лучше не использовать.

Чтобы задать значения этих параметров для всего документа в целом, используют одиночный тег <BASEFONT>. Он содержит аналогичные атрибуты и задает значение вида, цвета и размера шрифта, используемое по умолчанию.

Попробуйте использовать различные цвета и типы шрифтов для различных фрагментов текста, как указано в следующем примере.

```
<HTML>
    <HEAD>   <TITLE>Управление стилем шрифта  </TITLE>
    </HEAD>
     <BODY>
          <BASEFONT   SIZE=5  FACE="Arial"> <HR>
   Этот текст использует пятый размер шрифта Arial,  заданного  по умолчанию.  <HR>
   <P>  <FONT  SIZE= 2   FACE="Times New Roman"   COLOR="GREEN">
   Этот текст мельче и использует шрифт Times New Roman и другой – зеленый цвет.
</FONT>  <HR>
  </BODY>
 </HTML>
```

Результат этого фрагмента на экране:

Управление стилем шрифта

Этот текст использует пятый размер шрифта Arial, заданного по умолчанию.

Этот текст мельче и использует шрифт Times New Roman и другой – зеленый цвет.

Задания

Используя вышеприведенные примеры выполните следующее:

1. Создайте объявление в виде HTML-документа о предстоящем заседании студсовета. Посмотрев текст объявления с помощью программы Internet Explorer измените и оформите его по вашему усмотрению. Окончательный вариант работы сохраните на диске.
2. Составьте список студентов вашей группы, оформите его, используя возможности тегов, описанных выше. Сохраните на диске полученный HTML-документ.
3. Подготовьте приветственное послание Вашим друзьям с праздником Наурыз. Оформите текст поздравления, используя рисунки из папки *Учебный процесс* (можно использовать герб и знамя Республики).

4.6.Форматирование HTML-документа

Цель работы научить студентов:

- форматированию фрагментов HTML-документа,
- работе с гиперссылками и с изображениями в HTML-документах,
- использованию шрифтового оформления.

Форматирование шрифта

HTML допускает два подхода к шрифтовому выделению фрагментов текста. С одной стороны, можно прямо указать, что шрифт на некотором участке текста должен быть **жирным**, *наклонным* или подчеркнутым, то есть изменить **физический стиль** текста. С другой стороны, можно пометить некоторый фрагмент текста как имеющий некоторый отличный от нормального **логический стиль**, оставив интерпретацию этого стиля браузеру. Поясним это на примерах.

Физические стили

Под физическом стилем принято понимать прямое указание браузеру на модификацию текущего шрифта.

Например, все, что находится между метками <**B**> и </**B**>, будет написано **жирным шрифтом**.

Текст между метками <**I**> и </**I**> будет написан *наклонным шрифтом*.

Текст между метками <**U**> и </**U**> будет написан с подчеркиванием.

Несколько особняком стоит пара меток <**TT**> и </**TT**>. Текст, размещенный между этими метками, будет написан шрифтом, имитирующим пишущую машинку, то есть имеющим фиксированную ширину символа.

Логические стили

При использовании логических стилей автор документа не может знать заранее, что увидит на экране читатель. Разные браузеры толкуют одни и те же метки логических стилей по-разному. Некоторые браузеры игнорируют некоторые метки вообще и показывают нормальный текст вместо выделенного логическим стилем. Вот самые распространенные логические стили.

<EM> ... </EM>

От английского *emphasis – акцент, т.е. курсив* .

<STRONG> ... </STRONG>

От английского **strong emphasis – сильный акцент, т.е. полужирный**.

<CODE> ... </CODE>

Рекомендуется использовать для фрагментов исходных текстов.

<SAMP> ... </SAMP>

От английского *sample – образец.* Рекомендуется использовать для демонстрации образцов сообщений, выводимых на экран программами.

<KBD> ... </KBD>

От английского *keyboard – клавиатура.* Рекомендуется использовать для указания того, что нужно ввести с клавиатуры.

<VAR> ... </VAR>

От английского *variable – переменная.* Рекомендуется использовать для написания имен переменных, этот шрифт также напоминает курсив.

Подытожим наши знания о логических и физических стилях с помощью примера 3.1. Заодно Вы сможете увидеть, как Ваш браузер показывает те или иные логические стили. Пример 3-1:

```
<HTML>  <HEAD>  <TITLE>Пример 3.1 </TITLE>  </HEAD>
```

```
<BODY> <CENTER> <H1>Шрифтовое выделение фрагментов текста</H1> <HR>
<P>Теперь мы знаем, что фрагменты текста можно выделять
<BR> <B>жирным</B> или <BR> <I>наклонным</I> шрифтом или
<BR> <U> с подчеркиванием </U> шрифтом.
<BR> Кроме того, можно включать в текст фрагменты
с фиксированной шириной символа
<TT>(имитация пишущей машинки)</TT> <HR>
<P>Кроме того, существует ряд логических стилей:
<P><EM>EM - от английского emphasis - акцент,
то же самое, что курсив </EM><BR>
<STRONG>STRONG - от английского strong emphasis - сильный акцент,
то же самое,  что полужирный </STRONG><BR>
<CODE>CODE - для фрагментов исходных текстов</CODE><BR>
<SAMP>SAMP - от английского sample - образец </SAMP><BR>
<KBD>KBD - от английского keyboard - клавиатура</KBD><BR>
<VAR>VAR - от английского variable - переменная </VAR> <HR>
</CENTER></BODY>
</HTML>
```

Результат этой программы:

Шрифтовое выделение фрагментов текста

Теперь мы знаем, что фрагменты текста можно выделять

жирным шрифтом или

наклонным шрифтом или

подчеркнутым шрифтом.

Кроме того, можно включать в текст фрагменты с фиксированной шириной символа

(имитация пишущей машинки)

Кроме того, существует ряд логических стилей:

EM - от английского emphasis - акцент

STRONG - от английского strong emphasis - сильный акцент

CODE - для фрагментов исходных текстов

SAMP - от английского sample - образец

KBD - от английского keyboard - клавиатура

VAR - от английского variable - переменная

Тело документа

Теги (метки) <**BODY**> и </**BODY**> содержат основное тело документа. Тело документа может содержать параметры в виде атрибутов. Основные атрибуты метки <BODY>:

bgcolor Определяет цвет фона документа. Синтаксис цвета см. ниже.

text Определяет цвет текста.

link Определяет цвет ключевых слов для гипертекстовых ссылок.

vlink Определяет цвет использованных гипертекстовых ссылок.

alink Определяет цвет гипертекстовой ссылки в момент нажатия на нее.

background Определяет изображение, служащее фоном, т.е. рисунок обоя.

Цвета в HTML указываются с помощью шестнадцатеричной системы кодирования. Эта система основана на трех компонентах – красном (Red), зеленом (Green) и синем (Blue), отсюда и ее название – RGB, по первым буквам названий этих цветов. Каждый из компонентов соответствует шестнадцатеричному числу от 00 до FF (0 и 255 в десятичной системе счисления). Эти три значения затем объединяются в одно значение, которому предшествует знак #, например #800080, что соответствует фиолетовому цвету. Поскольку немногие могут определить цвет по его шестнадцатеричному коду, в HTML можно использовать английские стандартные названия цветов, которые перечислены вместе с их шестнадцатеричными значениями в нижней табл.

Названия цветов и **значения #RGB**

Названия	коды	Названия	коды
Black (черный)	"#000000"	Green (зеленый)	"#008000"
Silver (серебристый)	"#C0C0C0"	Lime (лимонный)	"#00FF00"
Gray (серый)	"#808080"	Olive (олифковый)	"#808000"
White (белый)	"#FFFFFF"	Yellow (желтый)	"#FFFF00"
Maroon (темнобордовый)	"#800000"	Navy (темносиний)	"#000080"
Red (красный)	"#FF0000"	Blue (синий)	"#0000FF"
Purple (фиолетовый)	"#800080"	Teal (Зеленоголубой)	"#008080"
Fuchsia (розовый, фуксия)	"#FF00FF"	Aqua (светлосиний)	"#00FFFF"

Пример: <body bgcolor = white text = black link = red vlink = maroon alink = fuschia background = "face.jpg">

При определении цветов для документа HTML вы можете использовать либо названия цветов, либо их коды. Например, следующие строки идентичны:

<BODY BGCOLOR=”#FFFFFF”>
<BODY BGCOLOR=”WHITE”>

HR - ***горизонтальные линии***

Горизонтальные линии можно использовать, чтобы указать на изменение темы. Закрывающие метки в элементах **HR** запрещены. Допустимые атрибуты: **ALIGN, NOSHADE, SIZE** и **WIDTH**.

Атрибут	*Назначение*
ALIGN	С помощью этого атрибута можно задать выравнивание линии по левому краю (align=LEFT), по правому краю (align=RIGHT) или по центру (align=CENTER). По умолчанию, линия выравнивается по центру.
WIDTH	Длину линии можно указать в пикселях (например, width=100) или в процентном отношении (например, width="50%") к ширине окна броузера. Если используются проценты, добавьте знак процента к числу. По умолчанию установлено 100%.
SIZE	Высота линии в пикселях, этот атрибут может принять значения в виде целых чисел, например, 4, или 8, или 16 и т.д..
NOSHADE	Если имеется этот атрибут, то броузер не использует эффект трехмерности. Он показывает, что линия должна выводиться в виде полосы одного цвета, а не в виде традиционной двухцветной "канавки".
COLOR	Для указания цвета разделительной линии можно использовать шестнадцатеричное значение RGB или стандартное название цвета

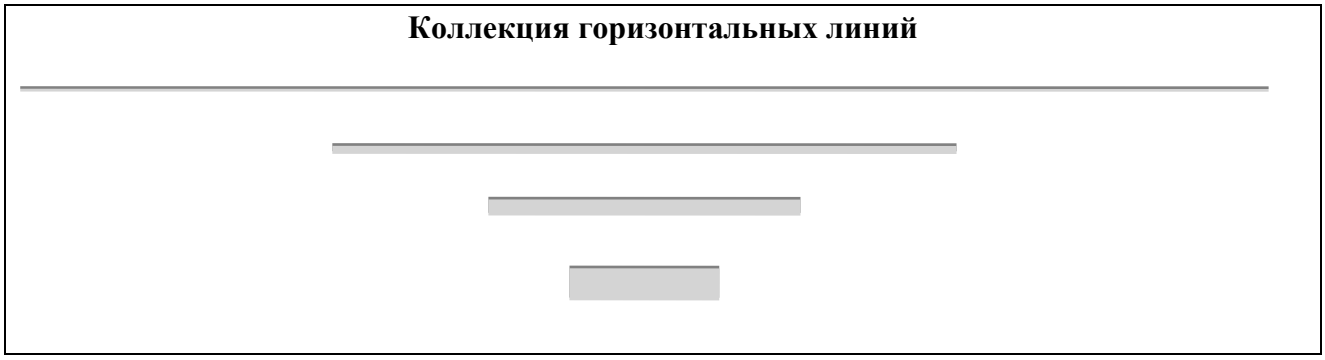
Горизонтальные линии следует использовать в тех случаях, когда требуется жесткое разделение текста. Основные принципы использования линий заключаются в том, что они никогда не должны располагаться между заголовком и последующим текстом. Их также не следует использовать для создания пустот в документе. Пустые места, не заполненные текстом, играют важную роль в оформлении страниц. Конечно, излишек пустых мест на страницах портит общий вид документа; однако если свободного места совсем нет, то страницы выглядят переполненными.

<HR ALIGN=CENTER WIDTH=50% SIZE=5 COLOR=NAVY>

В нижнем примере приведена небольшая коллекция горизонтальных линий.

```
<html> <head> <title>Пример 4</title> </head>
   <body> <H1 ALIGN=CENTER>Коллекция горизонтальных линий</H1>
          <HR SIZE=2 WIDTH=100%><BR>
          <HR SIZE=4 WIDTH=50%><BR>
          <HR SIZE=8 WIDTH=25%><BR>
          <HR SIZE=16 WIDTH=12%><BR>
  </body>
</html>
```

Результат данного фрагмента программы приведен ниже:



Переход по гиперссылке – тег <A> (анкер)

В HTML переход от одного фрагмента текста к другому задается с помощью тега вида:

<A HREF="[адрес перехода]">выделенный фрагмент текста</A>

В качестве параметра *[адрес перехода]* может использоваться несколько типов аргументов. Самое простое – это задать имя другого HTML-документа, к которому нужно перейти. Например:

<A HREF="pr2.htm">Перейти к оглавлению</A>

Такой фрагмент HTML-текста приведет к появлению в документе выделенного фрагмента Перейти к оглавлению, при нажатии на который в следующее окно будет загружен документ *pr.htm.*

Обратите внимание: если в адресе перехода не указан каталог, переход будет выполнен внутри текущего каталога. После просмотра загруженного файла обратно можно вернуться нажатием кнопки НАЗАД в панели инструментов броузера.

Таким образом, если Вы подготовили к публикации некоторую группу HTML-документов, которые ссылаются друг на друга только по имени файла и находятся в одном каталоге на Вашем компьютере, вся эта группа документов будет работать точно так же,

если ее поместить в любой другой каталог на любом другом компьютере, на локальной сети или... на Интернет! Теперь у Вас появляется возможность разрабатывать целые коллекции документов без подключения к Интернет, и только после окончательной готовности, подтвержденной испытаниями, помещать коллекции документов на Интернет целиком.

При необходимости можно задать переход не просто к некоторому документу, но и к определенному месту внутри этого документа. Для этого необходимо создать в документе, к которому будет задан переход, некоторую опорную точку, или **анкер**. Разберем это на примере.

Допустим, что необходимо осуществить переход из файла **pr1.htm** к словам "Переход закончен" в файле pr2.htm (файлы находятся в одном каталоге). Прежде всего, необходимо создать вот такой анкер в файле pr2.htm:

<A NAME="AAA">Переход закончен</A>

Слова "Переход закончен" при этом никак не будут выделены в тексте документа.

Затем в файле 1.htm (или в любом другом) можно определить переход на этот анкер:

<A HREF="2.htm#AAA">Переход к анкеру AAA</A>

Кстати говоря, переход к этому анкеру можно определить и внутри самого документа pr2.htm – достаточно только включить в него вот такой фрагмент:

<A HREF="#AAA">Переход к анкеру AAA</A>

На практике это очень удобно при создании больших документов. В начале документа можно поместить оглавление, состоящее из ссылок на анкеры, расположенные в заголовках разделов документа.

Во избежание недоразумений рекомендуется задавать имена анкеров латинскими буквами. Следите за написанием имен анкеров: большинство браузеров отличают большие буквы от маленьких. Если имя анкера определено как AAA, ссылка на анкер aaa или AaA не выведет Вас на анкер AAA, хотя документ, скорее всего, будет загружен корректно.

Пока что мы обсуждали только ссылки на HTML-документы. Однако возможны ссылки и на другие виды ресурсов:

<A HREF="ftp://server/directory/file.ext">Выгрузить файл</A>

Такая ссылка, если ей воспользоваться, запустит протокол передачи файлов и начнет выгрузку файла file.ext, находящегося в каталоге directory на сервере server, на локальный диск пользователя.

<A HREF="mailto:user@mail.box">Послать письмо</A>

Если пользователь совершит переход по такой ссылке, у него на экране откроется окно ввода исходящего сообщения его почтовой программы. В строке To: ("Куда") окна почтовой программы будет указано user@mail.box.

Разберем все, что мы знаем о связывании, с помощью примера .

```
<HTML>
<HEAD>
<TITLE>Пример 7</TITLE>
</HEAD>
<BODY>
<H1>Связывание </H1>
<P>С помощью ссылок можно переходить к другим файлам
(например, к <A HREF="pr.htm">оглавлению этого
руководства</A>).</P>
<P>Можно выгружать файлы (например,
<A HREF="ftp://yi.com/home/ChuvakhinNikolai/html-pr.doc">это
руководство в формате Microsoft Word 2.0</A>) по FTP.</P>
<P>Можно дать пользователю возможность послать почту (например,
<A HREF="mailto:nc@iname.com">автору этого руководства</A>).</P>
</BODY>
</HTML>
```

Анкеры не могут находиться один внутри другого. Открывающая и закрываюшая метки обязательны. Анкеры используются для определения гипертекстовых ссылок, например,

Путь к счастье.

а также конкретных точек внутри документа, на которые могут указывать гипертекстовые ссылки, например,

<h2> Тек-Сквер 545 – рай для хакера</h2>

name Строка, определяющая имя анкера. Имена анкеров в одном документе не должны повторяться.

href Указывает адрес ресурса, на который будет производиться переход по гипертекстовой ссылке. Это может быть другой HTML-документ, PDF-файл, изображение и т.п.

title Указывает наименование ресурса, на который сделана ссылка.

Добавление изображений в документ HTML

Поместить изображение в документ HTML очень просто. Введите этот тег в то место документа HTML, где вы хотите поместить изображение. Затем замените имя *файла* на URL рисунка.

<IMG SRC=”имя файла”>

Здесь SRC обязательный атрибут. Указывает путь к изображению - файлу формата GIF, JPEG или PNG.

По умолчанию, броузер отобразит это изображение в указанном месте, справа от текста или другого объекта, который непосредственно предшествует изображению.

Посмотрите на пример, приведенный ниже. Он показывает одно и то же изображение три раза. Каждый раз изображение отображается в строке, поэтому броузер располагает его справа от предшествующего текста.

<HTML> <HEAD>
<TITLE>Использование тега IMG</TITLE> </HEAD> <BODY> <P>
<IMG SRC=”dog.gif”>
Этот текст идет сразу же после рисунка.

<P> Этот текст разорван <IMG SRC=”dog.gif”> рисунком.

<P> В этом случае рисунок появляется после текста.
<IMG SRC=” dog.gif”>
</BODY> </HTML>

Выравнивание текста с изображениями в строке осуществляется атрибутом ALIGN. По умолчанию при помещении изображения в строке текст выравнивается по нижней части изображения. Возможно, вы захотите изменить такое выравнивание, поскольку при этом остается слишком много пустого места на странице. Эту настройку можно изменить с помощью атрибута ALIGN в дескрипторе <IMG>. В табл. перечислены значения, которые можно присвоить этому атрибуту.

Значение	*Описание*
align=TOP	Выравнивает текст по верхнему краю изображения
align=MIDDLE	Выравнивает текст по средней части изображения
align=BOTTOM	Выравнивает текст по нижнему краю изображения

align=left	Выравнивает изображение по левому полю. Текст, следующий за изображением, "обтекает" изображение справа.
align=right	Выравнивает изображение по правому полю. Текст, следующий за изображением, "обтекает" изображение слева.

В примере ниже приведен код документа HTML, включающего три изображения, для каждого из которых используется одна из опций выравнивания, перечисленных выше.

```
<HTML> <HEAD>
<TITLE>Использование атрибута ALIGN в дескрипторе IMG</TITLE> </HEAD>
<BODY> <P>
<IMG SRC=”dog.gif” ALIGN=TOP>
Этот текст выравнивается по верхнему краю изображения. </P> <P>
<IMG SRC=”dog.gif” ALIGN=MIDDLE>
Этот текст выравнивается по средней части изображения. </P> <P>
<IMG SRC=”dog.gif” ALIGN=BOTTOM>
Этот текст выравнивается по нижнему краю изображения. </P> </BODY> </HTML>.
Следующий пример показывает варианты обтекания рисунка текстом.
<HTML> <HEAD>
<TITLE>Использование атрибута ALIGN в теге IMG&</TITLE> </HEAD> <BODY>
<P>
<IMG SRC=”dog.gif” ALIGN=LEFT>
Этот текст располагается справа от изображения и ниже.
</P> <P>
<IMG SRC=”dog.gif” ALIGN=RIGHT>
Этот текст располагается слева от изображения и ниже.
</P>
</BODY>
</HTML>
```

Тег FONT

Для управления внешним видом текста в HTML служит элемент FONT. Элемент FONT является контейнером, который открывается тегом <FONT> и закрывается тегом </FONT>. Если в открывающем теге не указаны атрибуты, то элемент FONT не будет оказывать никакого воздействия.

Элемент FONT можно использовать внутри любого текста. С помощью атрибутов FACE (гарнитура), SIZE (размер) и COLOR (цвет) можно радикально изменить внешний вида текста в документах.

FACE позволяет выбрать шрифт, который вы хотите использовать при отображении вашего документа. Параметр атрибута FACE – название шрифта. Название, указанное в атрибуте, должно точно совпадать с названием шрифта на компьютере пользователя – в противном случае броузер игнорирует этот атрибут и использует шрифт, заданный читателем по умолчанию. Прописные и строчные буквы в названии шрифта игнорируются, а пробелы являются обязательными. Ниже показано, как задать определенный шрифт.

```
<HTML>
<HEAD>
<TITLE>Выбор типа шрифта</TITLE>
```

</HEAD>
<BODY>
<FONT FACE=”Arial”>Здесь выбран другой тип шрифта</FONT>
</BODY>
</HTML>

Если вы не знаете, какие шрифты могут быть на компьютере читателя, то в атрибуте FACE можно указать несколько названий шрифтов через запятую. Броузер просматривает список шрифтов слева направо и использует первый подходящий шрифт. Ниже используется несколько типа шрифтов.

<HTML>
<HEAD>
<TITLE>Пример выбора шрифта</TITLE>
</HEAD>
<BODY>
<FONT FACE=”Verdana”, “Arial”, “Helvetica”>
Это пример выбора шрифта. </FONT>
</BODY>
</HTML>

В этом примере указалн в качестве основного варианта шрифт Verdana, но кроме того перечислены также допустимые шрифты Arial и Helvetica.

SIZE Этот элемент позволяет указать высоту знаков текста. Размер шрифта указывается в условных единицах от 1 до 7, причем эта шкала основана на шрифте обычного стиля, которому соответствует значение 3. Атрибут size можно использовать двумя различными способами: указать абсолютный размер шрифта, например SIZE=5, или относительный размер, например SIZE=+2. Второй способ чаще применяется в том случае, если был указан основной шрифт basefont.

Приведенный ниже пример показывет эффект установки абсолютного размера шрифта:

 size=1
 size=2
 size=3
 size=4
 size=5
 size=6
 size=7

Результат работы этой программы:
size=1 size=2 size=3 size=4 size=5 size=6 size=7
Следующий пример показвыает эффект относительного размера шрифта при базовом размере шрифта, равном 3:
size=-4 size=-3 size=-2 size=-1 size=+1 size=+2 size=+3 size=+4
То же самое при базовом размере шрифта, равном 6:
size=-4 size=-3 size=-2 size=-1 size=+1 size=+2 size=+3 size=+4
Пример изменения размера шрифтов.

<HTML>
<HEAD>
<TITLE>Пример выбора размера шрифта</TITLE>
</HEAD>
<BODY>
<FONT SIZE=l>Размер 1</FONT>
<FONT SIZE=-l>Размер 2</FONT>

<FONT SIZE=3>Размер 3</FONT>
<FONT SIZE=4>Размер 4</FONT>
<FONT SIZE=+2>Размер 5</FONT>
<FONT SIZE=6>Размер 6</FONT>
<FONT SIZE=+4>Размер 7</FONT>
</BODY>
</HTML>

COLOR Цвет текста можно указать таким же образом, как и название шрифта или его размер. Атрибут COLOR воспринимает либо шестнадцатеричное значение RGB, либо стандартные названия цветов. Ниже показан пример определения цветов в документе. Определение цвета аналогично применяемому в атрибуте BGCOLOR элемента BODY**.**

```
<HTML>
<HEAD>
<TITLE>Пример выбора цвета</TITLE>
</HEAD>
<BODY>
<FONT COLOR=”#FF0000”> Этот текст имеет красный цвет</FONT><BR>
<FONT COLOR= “GREEN”>Этот текст имеет зеленый цвет</ FONT><BR >
</BODY> </HTML>
```

Задания

1.Открыть файл **lab2.htm** (C:\Мои документы\st) и выполнить сл. изменения:

а) Слова **Главный заголовок** и **Подзаголовок** отцентрировать;

б) Текст первого абзаца до линии сделать красным, текст второго абзаца до линии – синим, текст третьего абзаца до линии – зеленым;

в) Три черные горизонтальные линии после абзацев перекрасить в др. цвета, их толщины и длины также изменить по своему усмотрению;

г) Общий фон для текста сделать серым;

2.Открыть файл **lab2.htm** (C:\Мои документы\st) на рабочем столе и выполнить сл. изменения:

а) Создать гиперссылки на –документ pr4.htm, pr5.htm, pr6.htm, pr7.htm, и на картинки

Orantang.jpg

Popugay.jpg

Monky.jpg

Eagle.jpg

Kenya5.jpg

```
<A HREF="#Третий">Переход к анкеру Третий</A>
<A name="Третий">
```

4.7.Организация бегущих строк и списков средствами HTML

Цель работы научить студентов:

- организовать бегущие строки в HTML-документах,
- работе с различными типами списков.

1. Бегущие строки

Теги <MARQUEE> и **</MARQUEE>** образуют «бегущую строку» в окне броузера и используются со следующими параметрами:

<MARQUEE [ALIGN="align"] [BEHAVIOR="behavior"] [BGCOLOR="#rrggbb"] [DIRECTION="direction"] [HEIGHT="integer"] [HSPACE="integer"] [LOOP="integer"] [SCROLLAMOUNT="integer"] [SCROLLDELAY="integer"] [VSPACE="integer"] [WIDTH="integer"]> </MARQUEE>

ALIGN задает выравнивание «бегущей строки» и может принимать одно из следующих значений: TOP, MIDDLE, BOTTOM.

BEHAVIOR определяет характер текстовой анимации и принимает значения SCROLL, SLIDE, ALTERNATE.

BGCOLOR определяет фоновый цвет (в шестнадцатеричном формате RGB или как одно из английских названий цвета) «бегущей строки».

DIRECTION задает направление движения текста. Возможны значения LEFT и RIGHT, но по умолчанию установлено LEFT.

HEIGHT – целое число, определяющее высоту «бегущей строки» в пикселях. Может также определяться в процентах (%).

HSPACE – целое число, указывающее размеры левого и правого полей в пикселях между внешним краем области прокрутки и окном броузера.

LOOP – целое число, определяющее количество повторений «бегущей

строки». Может принимать значение INFINITE (бесконечно).

SCROLLAMOUNT – целое число, определяющее расстояние в пикселях, на которое текст перемещается за один шаг.

SCROLLDELAY – целое число, указывающее интервал между шагами в миллисекундах.

VSPACE – целое число, задающее размеры верхнего и нижнего полей в пикселях между внешним краем «бегущей строки» и окном броузера.

WIDTH – целое число, задающее ширину «бегущей строки» в пикселях. Может определяться в процентах (%).

Следующий пример 3.1 иллюстрирует использование тегов <MARQUEE> </MARQUEE> и их атрибутов:

```
<HTML> <HEAD> <TITLE>Пример 3-1 </TITLE> </HEAD>
<BODY text=red>
<CENTER>
<H2>Бегущие строки </H2> <HR>
<H3> <MARQUEE BGCOLOR="Yellow" BEHAVIOR="SCROLL"
   DIRECTION="RIGHT" SCROLLAMOUNT="10" SCROLLDELAY="200"
   WIDTH="90%"> Это бегущая строка </MARQUEE>
<P> <MARQUEE BGCOLOR="Green" BEHAVIOR="SCROLL" DIRECTION="LEFT"
HEIGHT=30 SCROLLAMOUNT="10" SCROLLDELAY="100" VSPACE="40"
WIDTH="90%">
Это другая бегущая строка </MARQUEE> </H3>
<HR></CENTER></BODY>
</HTML>
```

Организация текста внутри документа

HTML позволяет определять внешний вид целых абзацев текста. Абзацы можно организовывать в списки, выводить их на экран в отформатированном виде, или увеличивать левое поле. Разберем все по порядку.

Ненумерованные списки: <UL> ... </UL>

Текст, расположенный между метками <UL> и </UL>, воспринимается как ненумерованный список. Каждый новый элемент списка следует начинать с метки <LI>. Например, чтобы создать вот такой список:

- ручки;
- карандаши;
- краски

необходим вот такой HTML-текст (пример 3-2):

```
<HTML> <HEAD> <TITLE>Пример 3-2 </TITLE>  </HEAD>
<BODY text=green>
<H2 FLIGN=CENTER>Маркированный список </H2> <HR>
<UL>
<LI> ручки;
<LI> карандаши;
<LI> краски
</UL>
<HR></BODY>
</HTML>
```

Обратите внимание: у метки <**LI**> нет парной закрывающей метки.

Нумерованные списки: <OL> ... </OL>

Нумерованные списки устроены точно так же, как ненумерованные, только вместо символов, выделяющих новый элемент, используются цифры. Если слегка модифицировать наш предыдущий пример (3-3):

```
<HTML> <HEAD> <TITLE>Пример 3-3 </TITLE> </HEAD>
<BODY text=green>
<H2 FLIGN=CENTER>Нумерованный список </H2> <HR>
<OL>
<LI> ручки;
<LI> карандаши;
<LI> краски
</OL>
<HR></BODY>
</HTML>
```

получится вот такой список:

1. ручки;
2. карандаши;
3. краски

Списки определений: <DL> ... </DL>

Список определений несколько отличается от других видов списков. Вместо меток <LI> в списках определений используются метки <DT> (от английского definition term – определяемый термин) и <DD> (от английского definition definition – определение определения). Разберем это на примере (3-4, первая часть):

```
<H3 FLIGN=CENTER>Длинные определения </H3>
<DL>
<DT>HTML
```

<DD>Термин HTML (HyperText Markup Language) означает 'язык маркировки гипертекстов'. Первую версию HTML разработал сотрудник Европейской лаборатории физики элементарных частиц Тим Бернерс-Ли.
<DT>HTML-документ
<DD>Текстовый файл с расширением *.htm (Unix-системы могут содержать файлы с расширением *.html).
</DL>

Этот фрагмент будет выведен на экран следующим образом:

HTML
Термин HTML (HyperText Markup Language) означает 'язык маркировки гипертекстов'. Первую версию HTML разработал сотрудник Европейской лаборатории физики элементарных частиц Тим Бернерс-Ли.

HTML-документ
*Текстовый файл с расширением *.htm (Unix-системы могут содержать файлы с расширением *.html).*

Обратите внимание: точно так же, как метки <LI>, метки <DT> и <DD> не имеют парных закрывающих меток.

Если определяемые термины достаточно коротки, можно использовать модифицированную открывающую метку <DL COMPACT>. Например, вот такой фрагмент HTML-текста (пример 3-4, вторая часть):

<HR> <H3 FLIGN=CENTER>Короткие определения </H3>
<DL COMPACT>
<DT>А
<DD>Первая буква алфавита
<DT>Б
<DD>Вторая буква алфавита
<DT>В
<DD>Третья буква алфавита
</DL>

будет выведен на экран примерно так:

А Первая буква алфавита
Б Вторая буква алфавита
В Третья буква алфавита

Вложенные списки

Элемент любого списка может содержать в себе целый список любого вида. Число уровней вложенности в принципе не ограничено, однако злоупотреблять вложенными списками все же не следует.

Вложенные списки очень удобны при подготовке разного рода планов и оглавлений. Наши знания о списках можно вкратце свести в пример 3-5:

<html> <head> <title>Пример 3-5</title> </head>
<body>
<H1>HTML поддерживает несколько видов списков </H1>
<DL>
<DT>Ненумерованные списки
<DD>Элементы ненумерованного списка выделяются специальным символом и отступом слева:
<UL>

<LI>Элемент 1
<LI>Элемент 2
<LI>Элемент 3
</UL>
<DT>Нумерованные списки
<DD>Элементы нумерованного списка выделяются отступом слева, а
также нумерацией:
<OL>
<LI>Элемент 1
<LI>Элемент 2
<LI>Элемент 3
</OL>
<DT>Списки определений
<DD>Этот вид списков чуть сложнее, чем два предыдущих, но и выглядит более эффектно.
<P>Помните, что списки можно встраивать один в другой, но не следует закладывать слишком много уровней вложенности. </P>
<P>Обратите внимание, что внутри элемента списка может находиться несколько абзацев. Все абзацы при этом будут иметь одинаковое левое поле. </P>
</DL>
</body> </html>

Результат этого фрагмента программы:

HTML поддерживает несколько видов списков

Ненумерованные списки

Элементы ненумерованного списка выделяются специальным символом и отступом слева:

- Элемент 1
- Элемент 2
- Элемент 3

Нумерованные списки

Элементы нумерованного списка выделяются отступом слева, а также нумерацией:

1. Элемент 1
2. Элемент 2
3. Элемент 3

Списки определений

Этот вид списков чуть сложнее, чем два предыдущих, но и выглядит более эффектно.

Помните, что списки можно встраивать один в другой, но не следует закладывать слишком много уровней вложенности.

Обратите внимание, что внутри элемента списка может находиться несколько абзацев. Все абзацы при этом будут иметь одинаковое левое поле.

Задания

1.Набрать пример 3-1 на стр. 1, посмотреть результат и далее выполнить сл. изменения:

а) Поменять высоту бегущей строки;

б) Фон текста первой бегущей строки красным, второго текста – синим;

в) Горизонтальные линии после абзацев перекрасить в др. цвета, их толщины и длины также изменить по своему усмотрению;

2. Набрать пример 3-2 на стр. 2, посмотреть результат и далее в каждой строке перечислить имена студентов группы;

3. Набрать пример 3-3 на стр. 2, посмотреть результат и далее в каждой строке перечислить фамилии студентов группы, провести толстые и разноцветные разделительные горизонтальные линии;

4. Набрать пример 3-4 на стр. 2, посмотреть результат и далее в каждой строке длинных определений дать пояснения профессиям экономиста, бухгалтера и финансиста;

5. Набрать пример 3-4 на стр. 3, посмотреть результат и далее в каждой строке коротких определений записать имена студентов группы и дать краткую характеристику типа “отличник учебы”, “галантный парень”, “симпатичная девушка” и т.д.;

6. Набрать пример 3-5 на стр. 3 с вашими измененными фрагментами текста, посмотреть результат и далее в каждой строке изменять строки и их оформления по вашему усмотрению.

4.8.Построение таблиц

Цель работы научить студентов:

- использованию основных тегов по созданию таблиц,
- создавать таблицы в HTML-документах,

Таблица определяется тегами <TABLE> и </TABLE>, строки – <TR> и </TR>, а отдельные столбцы в строке – <TD> и </TD> или <TH> и </TH>. Теги заголовков таблицы, находящихся в объединенных столбцах <TH> и </TH> выполняют те же функции, что и теги ячеек <TD></TD>, но <TH></TH> предписывают броузеру назначить заключенному между ними тексту полужирное начертание.

Теги заглавия <CAPTION> </CAPTION> задают заголовок таблицы. Определение таблицы имеет следующий синтаксис:

<TABLE ALIGN="align" BGCOLOR="#rrggbb" BORDER="integer"
BORDERCOLOR="#rrggbb" CELLPADDING="integer"
CELLSPACING="integer" WIDTH="integer">
</TABLE>

ALIGN определяет выравнивание таблицы (по умолчанию – по левому краю). ALIGN может принимать одно из следующих значений: LEFT, CENTER, RIGHT.

BGCOLOR задает цвет фона (в шестнадцатеричном формате RGB или как одно из предопределенных названий цвета).

BORDER – целое число, задающее толщину рамки таблицы в пикселях. Если BORDER не определен, рамка не отображается.

BORDERCOLOR определяет цвет рамки (в шестнадцатеричном формате RGB или как одно из предопределенных названий); должен использоваться совместно с атрибутом BORDER.

CELLPADDING – целое число, задающее горизонтальное и вертикальное расстояние между данными в ячейке и рамкой ячейки. Задается в пикселях.

CELLSPACING – целое число, которое определяет горизонтальное и вертикальное расстояние между ячейками. Задается в пикселях.

WIDTH - целое число, определяющее ширину таблицы. Его значение может быть задано в пикселях или в процентах (%).

Заголовок определяется тегом <CAPTION> в соответствии со следующим синтаксисом:

<CAPTION ALIGN="align" VALIGN="valign"> </CAPTION>
Тэг <CAPTION> имеет следующие атрибуты.

ALIGN определяет выравнивание заголовка и принимает одно из следующих значений: LEFT, CENTER (по умолчанию) или RIGHT.

VALIGN определяет вертикальное выравнивание заголовка и может принимать одно из следующих значений: TOP, MIDDLE, BOTTOM (по умолчанию), BASELINE.

Строка таблицы определяется тегом <TR></TR>, который имеет свои атрибуты:

<TR ALIGN="align" BGCOLOR="#rrggbb" BORDERCOLOR="#rrggbb"> Строка… </TR>

Атрибуты тега <TR>

ALIGN – выравнивание строки. Возможны следующие значения: LEFT (по умолчанию), CENTER, RIGHT.

BGCOLOR определяет цвет фона (в шестнадцатеричном формате RGB или как одно из предопределенных названий).

BORDERCOLOR – цвет рамки строки (в шестнадцатеричном формате RGB или как одно из предопределенных названий). Этот атрибут будет использоваться только в том случае, если для атрибута BORDER тега <TABLE> определено значение, отличное от нуля.

Ячейки (столбцы) таблицы определяются тегами <TD></TD> и <TH></TH> в соответствии со следующим синтаксисом:

<TD или TH ALIGN="align" BACKGROUND="url"] BGCOLOR="#rrggbb" BORDERCOLOR="#rrggbb"] > Столбец… </TD или /TH>

Теги <TD> и <TH> имеют следующие атрибуты:

ALIGN – горизонтальное выравнивание текста. ALIGN может принимать одно из следующих значений: LEFT, CENTER (по умолчанию), RIGHT.

BGCOLOR – цвет фона (в шестнадцатеричном формате RGB или как одно из предопределенных названий).

BORDERCOLOR – цвет рамки ячейки (в шестнадцатеричном формате RGB или как одно из предопределенных названий цвета). Этот атрибут будет использоваться только в том случае, если для атрибута BORDER тега <TABLE> определено значение, отличное от нуля.

COLSPAN – целое число, определяющее количество столбцов, попадающих в данную ячейку, предназначенную для заголовка столбцов.

Теперь рассмотрим задания.

Задания

1.Набрать сл. пример, посмотреть результат и далее выполнить некоторые изменения:

```
<TABLE  ALIGN=CENTER  BORDER=3  CELLSPACING=2
    CELLPADDING=2  WIDTH="80%"
    BGCOLOR=YELLOW  BORDERCOLOR=BLUE>
    <CAPTION> <H2> Заголовок  таблицы </H2>  </CAPTION>
    <TR>  <TD> первая клетка таблицы </TD>
          <TD> вторая клетка таблицы </TD> </TR>
     <TR> <TD> первая клетка таблицы </TD>
          <TD> вторая клетка таблицы </TD></TR>
</TABLE>
```

а) изменить цвет фона 1-строки (<TR BGCOLOR=SILVER>) серебристый, серый цвета.
б) изменить толщину рамок (бордюра), текст в клетках и т.д.

2) Набрать сл. пример, посмотреть результат и далее выполнить некоторые изменения:

```
<TABLE ALIGN="RIGHT" BORDER="3" BORDERCOLOR="Blue"  WIDTH="80%">
<CAPTION  ALIGN="RIGHT"  >  Заголовок появится справа и сверху от таблицы
</CAPTION>
```

```
<TR>  <TH COLSPAN="3"> Заголовок Столбца </TH> </TR>
  <TR ALIGN="RIGHT" BGCOLOR="yellow">
  <TH> Столбец 1 </TH> <TH> Столбец 2 </TH> <TH> Столбец 3 </TH>
</TR>
<TR> <TD> Данные для Столбца 1 </TD>
        <TD> Данные для Столбца 2 </TD>
        <TD> Данные для Столбца 3 </TD>
</TR>
</TABLE>
```

а) Добавить ещё один столбец к обеим строкам;

б) Добавить ещё две строки;

в) Изменить слова текстов в клетках, цвет фона строк и отдельных клеток;

г) Изменить цвет заголовка и т.д.

д) Провести перед таблицы, после заголовка таблицы и в конце горизонтальные линии разного цвета.

Контрольные вопросы

1. Почему для разработки Web-страниц используется специальный язык разметки гипертекста? Мы знаем, что с помощью текстового процессора Word вполне можно получать представительные документы. Почему нельзя использовать этот удобный и мощный текстовый процессор для разработки Web-документов?
2. Как вы понимаете, что такое тег HTML?
3. С помощью каких известных вам программ можно создавать Web-документы в коде HTML?
4. С помощью каких известных вам программ можно просматривать Web-документы?
5. В языке HTML нет тега, с помощью которого можно было бы создать абзац текста фиксированной ширины, например 800 пикселов. Почему нет таких тегов?
6. Несмотря на отсутствие тегов для создания текста фиксированной ширины, управлять шириной текста все-таки можно. С помощью какого средства можно создать текст, расположенный в трех (например) колонках заданной ширины?
7. Что такое альтернативный текст? Зачем он нужен и когда используется?
8. Чем отличаются текстовые и графические гиперссылки?
9. Предположим, что на Web-странице опубликован очень длинный документ (повесть). Для удобства пользователя автор ввел в начало документа содержание, состоящее из 20 пунктов, соответствующих главам повести. Что он должен предусмотреть, чтобы читатель мог перейти к любой главе щелчком на соответствующем пункте в содержании?
10. Какие виды списков вы знаете? Какими средствами создают списки на Web-страницах? Что такое вложенные списки?

5.ДИСТАНЦИОННЫЕ ТЕХНОЛОГИИ

Основные характеристики современного мира – информатизация и глобализация.

Дистанционное обучение - универсальная форма обучения, базирующаяся на использовании широкого спектра традиционных, новых информационных и телекоммуникационных технологий, и технических средств, которые создают условия для обучаемого свободного выбора образовательных дисциплин, соответствующих стандартам, диалогового обмена с преподавателем, при этом процесс обучения не зависит от расположения обучаемого в пространстве и во времени.

Информационно-образовательная среда ДО представляет собой системно-организованную совокупность средств передачи данных, информационных ресурсов, протоколов взаимодействия, аппаратно-программного и организационно-методического обеспечения, и ориентируется на удовлетворение образовательных потребностей пользователей.

5.1. Характерные черты дистанционного обучения

Дистанционное обучение от традиционных форм обучения отличают следующие характерные черты:

Гибкость. Возможность заниматься в удобное для себя время, в удобном месте и темпе. Нерегламентированный отрезок времени для освоения дисциплины.

Модульность. Возможность из набора независимых учебных курсов - модулей формировать учебный план, отвечающий индивидуальным или групповым потребностям.

Параллельность. Параллельное с профессиональной деятельностью или учебой в других учебных заведениях, обучение.

Охват. Одновременное обращение ко многим источникам учебной информации (электронным библиотекам, банкам данных, базам знаний и т.д.) большого количества обучающихся. Общение через сети связи друг с другом и с преподавателями.

Экономичность. Эффективное использование учебных площадей, технических средств, концентрированное и унифицированное представление учебной информации и мультидоступ к ней снижает затраты на организацию учебного процесса.

Технологичность. Использование в образовательном процессе новейших достижений информационных и телекоммуникационных технологий, способствующих продвижению человека в мировое постиндустриальное информационное пространство.

Социальное равноправие. Равные возможности получения образования независимо от места проживания, состояния здоровья, элитарности и материальной обеспеченности обучаемого.

Интернациональность. Экспорт и импорт мировых достижений на рынке образовательных услуг.

Новая роль преподавателя. ДО расширяет и обновляет роль преподавателя, который должен координировать познавательный процесс, постоянно усовершенствовать преподаваемые им курсы, повышать творческую активность и квалификацию в соответствии с нововведениями и инновациями.

Качество ДО не уступает качеству очной формы получения образования, а улучшается за счет привлечения выдающегося кадрового преподавательского состава и использования в учебном процессе наилучших учебно-методических изданий и контролирующих тестов по тем или иным дисциплинам.

5.2.Методы дистанционного обучения.

Дистанционная форма включает пять общедидактических методов обучения:

- информационно-рецептивный,
- репродуктивный,
- проблемное изложение,
- эвристический,
- исследовательский.

Они охватывают всю совокупность педагогических актов взаимодействия преподавателя и обучающихся.

В образовательном процессе ДО используются как традиционные, так и инновационные средства обучения, основанные на применении компьютерной техники и телекоммуникаций, а также последних достижений в области образовательных технологий.

Комплекс материальных и технических средств, необходимых для обучения в соответствии с учебными программами включает в себя учебные и учебно-вспомогательные помещения; лабораторное оборудование, технические средства обучения, учебники, учебные пособия и другие учебно-методические материалы. Большая часть учебно-научной

материальной базы образует виртуальную информационно-образовательную среду по причине удаленности ее слушателей.

Новые информационные технологии воздействуют на все компоненты системы обучения: цели, содержание, методы и организационные формы обучения, средства обучения, что позволяет решать сложные и актуальные задачи педагогики, а именно: развитие интеллектуального, творческого потенциала, аналитического мышления и самостоятельности человека.

При получении дистанционного образования средства обучения значительно шире и, кроме традиционных, включают такие, как:

- учебные электронные издания;
- компьютерные обучающие системы;
- аудио- видео учебные материалы и мн. др.

Электронные издания учебного назначения, обладая всеми особенностями бумажных изданий, имеют ряд положительных отличий и преимуществ. В частности: компактность хранения в памяти компьютера или на дискете, гипертекстовые возможности, мобильность, тиражируемость, возможность оперативного внесения изменений и дополнений, удобство пересылки по электронной почте. Это - автоматизированная обучающая система, которая включает в себя дидактические, методические и информационно-справочные материалы по учебной дисциплине, а также программное обеспечение, которое позволяет комплексно использовать их для самостоятельного получения и контроля знаний.

Аудио и видео учебные материалы - записываются на магнитные носители, аудио - и видеокассеты, и могут быть представлены обучаемому с помощью магнитофона, видеомагнитофона или лазерных компакт-дисков CD-ROM.

Компьютерные сети - средство обучения, включающее в себя различного рода информацию и совокупность компьютеров, соединенных каналами связи. Глобальная сеть INTERNET, является интегральным средством, широко используемым в ДО.

Таким образом, дистанционное образование может составить серьезную конкуренцию традиционным классно- урочным формам, особенно для детей- инвалидов и учеников сельской местности.

СОЦИАЛЬНОЕ СЛЕДСТВИЕ ИНФОРМАТИЗАЦИИ – ИНФОРМАЦИОННОЕ НЕРАВЕНСТВО

Снизить остроту этого неравенства возможно за счет **e-learning**

СОЦИАЛЬНОЕ СЛЕДСТВИЕ ГЛОБАЛИЗАЦИИ

- Появление новых форм образования, которые начинают приобретать черты широкомасштабных систем с размытыми границами.
- Дистанционное образование (e-learning) относится к этим системам

ХАРАКТЕРИСТИКИ СОВРЕМЕННОГО МИРА

- Общество находится в критическом состоянии (переломном) во многих сферах
- Ключевая роль для выхода из кризиса принадлежит новой стратегии развития человечества и *новым формам образования*

ВОЗМОЖНОСТИ ЭЛЕКТРОННОГО ОБУЧЕНИЯ

- Материалы – доступны 24/7, можно добавить свои собственные (wiki)!
- Знания – можно проверить, углубить и отточить практикой сразу же!
- Картотека, список литературы – все формы связей, все виды поиска
- Контакты – доступны здесь же, общение с «сокурсниками» и преподавателями

ОСНОВНЫЕ СВОЙСТВА СОВРЕМЕННОГО ОБРАЗОВАНИЯ

- Доступность образования для многих
- Глобальный характер образовательной среды
- Превращение образования в мощную отрасль экономики
- Превращение образования в глобальное культурное явление

ЖИЗНЬ ЛЮДЕЙ В СОВРЕМЕННОМ ОБЩЕСТВЕ ВЫДВИГАЕТ НОВЫЕ ТРЕБОВАНИЯ К ЗНАНИЯМ

Современный специалист должен уметь:

- создавать контент;
- извлекать знания из данных и информации;
- создавать и коммерциолизировать свои и привлеченные знания;
- ставить и решать проблемы;
- эффективно работать и общаться в сетях;

Такими же знаниями должен обладать преподаватель.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

ПРОГНОЗ ЮНЕСКО НА 21 ВЕК:

- Очное обучение будет занимать 30 – 40 % времени
- 40% будет отведено на дистанционное обучение

- Остальное время на самообразование при поддержке e-learning.

ИНТЕРЕСНЫЕ ЦИФРЫ

- В Турецком Дистанционном Университете обучается более половины зарегистрированных студентов страны
- 81% всех высших заведений США предлагают как минимум один курс дистанционного обучения.
- 67% учебных заведений США считают дистанционное обучение стратегически важным направлением своего развития

ОТ ЧЕГО ЗАВИСИТ КАЧЕСТВО ЭЛЕКТРОННОГО ОБУЧЕНИЯ

- Качества сетевого курса
- качество учебно-методического комплекса (УМК), размещенного на сервере
- качество контрольных ресурсов, размещенных на сервере
- частота обновления и актуализации содержания курса
- обратная связь «преподаватель-студент»
- Качества получившего студентом образования

ПРИЛОЖЕНИЕ

Толковый словарь по HTML

HTML-документ (страничка) - документ, написанный на языке разметки гипертекста (HTML). Заключается между тегами **<HTML>** и **</HTML>.**

Web-сайт, Web-сервер - цепочка логически связанных документов, написанных на языке HTML.

Значения тегов разметки документа

Теги разметки - специальные команды для расположения на экране текста, графики, видео и аудио фрагментов, а также команды, служащие для связи с другими HTML-документами и ресурсами Интернет.

Основные теги разметки

<HEAD> и **</HEAD>.** Между этими тегами располагается информация о документе. **<TITLE>** и **</TITLE>.** В этих тегах заключается название странички, которое будет выведено в рамке окна программы просмотра.

<BODY> и **</BODY>.** "Тело" документа (текст, графика и т.д.) располагается между этими двумя тегами.

Параметры тега **<BQDY>:**

BGCOLOR - цвет фона (<BODY BGCOLOR ="#FFFFFF">)

BACKGROUND - "обои" или бэкграунд

TEAT-цвет текста

LINK - цвет гипертекстовой связи (ссылки)

VLINK - цвет ссылки, уже посещенной в прошлом

ALINK - цвет активной ссылки Теги, служащие для форматирования текста <P> и </P> Теги, служащие для выделения абзацев. Новый абзац всегда отделяется от предыдущего пустой строкой.

**
** Тег, служащий для переноса текста на другую строку. Может также служить для отделения графики от текста на интервал.

<HR> Тег, служащий для логического разделения текста горизонтальной линией.

<PRE> и **</PRE>** Между этими тегами располагается предварительно отформатированный текст. На экран он выводится шрифтом типа "курьер".

Параметры выравнивания

Используются в <P> и <H*> *ALIGN=LEFT* - выравнивание по левому полю *ALIGN=RIGHT* - выравнивание по правому полю *ALIGN=CENTER* - выравнивание по центру

Теги выравнивания

<LEFT> и **</LEFT>** - выравнивание по левому полю

<RIGHT> и **</RIGHT>** - выравнивание по правому полю

<CENTER> и **</CENTER>** - выравнивание по центру.

Заголовки, служащие для выделения логических частей текста

<H1> и **</H1>** Заголовок первого уровня. **<H2>** и **</H2>** Заголовок второго уровня. **<H3>** и **</H3>** Заголовок третьего уровня. **<H4>** и **</H4>** Заголовок четвертого уровня. **<H5>** и **</H5>** Заголовок пятого уровня. **<H6>** и **</H6>** Заголовок шестого уровня.

Теги для выделения текста и **шрифта**

<B> и </B> Теги для выделения текста (слов, букв) жирным шрифтом.

<1> и </I> Теги для выделения текста (слов, букв) курсивным шрифтом, типа Italic.

<U> и </U> Текст, расположенный между двумя этими тегами, будет подчеркнут.

<BLINK> и **</BLINK>** Текст, расположенный между двумя этими тегами, будет мигать.

<FONT SIZE=+n> и **</FONT>**

<FONT SIZE=-n> и **</FONT>** Теги для изменения размера шрифта.

<FONT COLOR="#OOOOFF> и **</FONT>** Теги для изменения цвета шрифта.

Теги для формирования списков

<OL> и **</OL>** Теги, показывающие начало и конец нумерованного списка **<UL>** и </UL> Теги, показывающие начало и конец маркированного списка. **<LI>** Элемент списка

<DL> и **</DL>** Теги, показывающие начало и конец глоссария.

<DT> Термин глоссария, располагается без отступа от левого поля страницы.

<**DD**> рписание термина, располагается с отступом от левого поля страницы.

Теги-команды для вставки в текст объектов нетекстовой информации

<IMG SRC ="file.gif '> или <IMG SRC =" file.jpg"> - команда для вставки графического изображения.

<IMG SRC =" file.wav"> - команда для вставки звукового фрагмента

<IMG SRC =" file.avi"> - команда для вставки видео фрагмента

Параметры графического изображения

WIDHT- ширина картинки в пикселях

HEIGHT- высота картинки в пикселях

ALIGN - выравнивание (ALIGN=LEFT - выравнивание по левому полю, ALIGN=RIGHT – по правому полю, ALIGN=TOP - по верхней границе, ALIGN=BOTTOM - по нижней границе, ALIGN=MIDDLE или CENTER - по центру).

HSPACE - горизонтальный отступ от графического изображения

VSPACE - вертикальный отступ

ALT- альтернативный текст, служит для обозначения изображения

Команды, служащие для гиперсвязи с другими HTML-документами и **рессурсами Интернет**

<A HREF="fail.htm"> и **</A>** или **<A HREF="http://www.ru">** и </A> - гиперсвязи **<ADDRESS><A HREF=mailto: person@firm.ru> person@firm.ru</ADDRESS>** - гиперсвязь с адресом электронной почты

Таблицы

Таблица - сетка для показа данных в строках и столбцах, а также средство для форматирования текста

<TABLE> и **</TABLE>** Теги для вставки таблицы в HTML документ Параметры тега **<TABLE>**

BGCOLOR - цвет фона

BORDER - ширина бордюра

WIDHT' - ширина таблицы

Теги разметки таблицы

<CAPTION> и **</CAPTION>** - название таблицы, имеет параметр ALIGN=TOP - выравнивание над таблицей и ALIGN=BOTTOM - под таблицей.
<TR> и **</TR>** Строчка таблицы. Может иметь параметры BGCOLOR - цвет фона внутри строки; ALIGN=LEFT, RIGHT, CENTER - выравнивание внутри строки; VALIGN=TOP, BOTTOM, MIDDLE - вертикальное выравнивание внутри строки таблицы.
<TD> и **</TD>** Столбец таблицы. Может иметь параметры BGCOLOR - цвет фона под столбцом; ALIGN=LEFT, RIGHT, CENTER - выравнивание внутри столбца; VALIGN=TOP, BOTTOM, MIDDLE - вертикальное выравнивание; COLSPAN растягивание клетки на несколько столбцов, ROWSPAN - растягивание клетки на несколько строк.
<TH> и **</TH>** Заголовок столбца. Может иметь параметры BGCOLOR - цвет фона под названием; ALIGN=LEFT, RIGHT, CENTER - выравнивание; VALIGN=TOP, BOTTOM, MIDDLE - вертикальное выравнивание; COLSPAN, ROWSPAN - растягивание клетки на несколько столбцов или строк; WIDHT - ширина названия.

Рамки-фреймы

Рамки-фреймы - средство для разделения экрана на несколько областей, в каждой из которых отображается содержимое отдельной Web-странички или даже целого Web-сайта.

<FRAMESET> и **</FRAMESET>** Теги для создания рамки

Параметры тега <FRAMESET>

COLS–подразделяют экран на определенное количество колонок (вертикальных)

ROWS – подразделяют экран на опредленное количество колонок (горизонтальных)

BORDCOLOR - цвет рамки

BORDER -ширина бордюра

FRAMEBORDER- граница рамки (FRAMEBORDER=YES - есть граница,

FRAMEBORDER=NO-нет границы,

FRAMESPACING=n - ширина границы)
<FRAME> Тег для описания рамки (<FRAME SRC-'file.htm">).
Параметры тега <FRAME>
SCROLING - параметр для регулировки полосы прокрутки:

SCROLING=YES - полоса прокрутки будет всегда

SCROLING=NO - полосы прокрутки не будет

SCROLING=AUTO - полоса прокрутки появляется только в случае необходимости

MARGINWIDHT и *MARGINHEIGHT* - параметры, которые управляют отступом внутри рамок, служат для выравнивания графического изображения внутри рамки

NORESIZE - параметр, указывающий на то, что размер рамки-фрейма никогда не будет меняться.

A link to <A HREF="file.htm" TARGET="frame2"> file.htm</A> - Связь между фреймами *TARGET*- атрибут связи между фреймами. Имеет несколько значений:

_BLANK загружает содержимое страницы, заданной ссылкой, в новое пустое окно.

_SELF содержимое страницы, заданной ссылкой, в окно, которое содержит ссылку.

_PARENT загружает содержимое страницы, заданной ссылкой, в окно, являющееся непосредственным владельцем набора фреймов.

_TOP содержимое страницы, заданной ссылкой, в окно, игнорируя используемые фреймы.

Обработка браузеров, не поддерживающих фреймы:
<FRAMESET>
Здесь располагаются фреймы
</FRAMESE1>
<NOFRAMES>
<BODY>
Здесь располагается текст без фреймов
<BODY>
</NOFRAMES>
В секции, предназначенной для тех пользователей, которые "не видят" рамки, можно расположить какой-нибудь пояснительный текст.

Бегущая строка
<**MARQUEE>**ТЕКСТ<**/MARQUEE**> - Тег, создающий бегущую строку

<MARQUEE DIRECTION=left>TEKCT</MARQUEE> - Если бегущую строку нужно направить справа налево

<MARQUEE DIRECTION=right>TEKCT</MARQUEE> - движение слева направо.

scroll - стандартное движение от правого края к левому

slide - надпись один раз пробегает от правого края к левому, где и остается.

alternate- движение от правого края страницы к левому и обратно. Бесконечный цикл.
<MARQUEE LOOP=n BEHAVIOR=scroll>TEKCT</MARQUEE> - Ограничение числа циклов.
Значение n оператора LOOP указывает число повторений цикла.
<MARQUEE WIDHT=n>TEKCT</MARQUEE>- указать ширину участка, занимаемого бегущей строкой, где n - ширина той части страницы, на которой расположена бегущая строка. Значение n указывается как в пикселях, так и в процентах от общей ширины видимой части страницы.

<MARQUEE scrollamount=n>TEKCT</MARQUEE> - Регулировка движения надписи по экрану. Здесь n - число пикселей,

<MARQUEE scrolldelay=t>TEKCT</MARQUEE> В данном случае переменная величина - время t - измеряется в миллисекундах. Метод задания скорости состоит в указании времени, спустя которое текст будет перерисован на экране заново.

<FONTSIZE=n><MARQUEE> TEKCT</MARQUEE></FONT> - возможность указывать величину шрифта текста в строке.

<MARQUEE BGCOLOR=n> TEKCT </MARQUEE> - окрасить поверхность бегущей строки в какой-либо цвет, где n, как это бывало и раньше, можно указать в вид шестнадцатеричного числа либо написав его название

<MARQUEE HEIGHT=n>TEKCT</MARQUEE> - указать высоту бегущей строки, задавая величину *n* в пикселях.

ПРИЛОЖЕНИЕ

Толковый словарь по HTML

HTML-документ (страничка) – документ, написанный на языке разметки гипертекста (HTML). Заключается между тегами **<HTML>** и **</HTML>.**

Web-сайт, Web-сервер – цепочка логически связанных документов, написанных на языке HTML.

Теги разметки – специальные команды для расположения на экране текста, графики, видео и аудио фрагментов, а также команды, служащие для связи с другими HTML-документами и ресурсами Интернет.

Основные теги разметки

<HEAD> и **</HEAD>.** Между этими тегами располагается информация о документе.

<TITLE> и **</TITLE>.** В этих тегах заключается название странички, которое будет выведено в рамке окна программы просмотра.

<BODY> и **</BODY>.** "Тело" документа (текст, графика и т.д.) располагается между этими двумя тегами.

Параметры тега **<BODY>:**

BGCOLOR – цвет фона (<BODY BGCOLOR ="#FFFFFF">)

BACKGROUND – "обои" или бэкграунд

TEXT – цвет текста

LINK – цвет гипертекстовой связи (ссылки)

VLINK – цвет ссылки, уже посещенной в прошлом

ALINK – цвет активной ссылки

Теги, служащие для форматирования текста

<P> и **</P>** Теги, служащие для выделения абзацев. Новый абзац всегда отделяется от предыдущего пустой строкой.

**
** Тег, служащий для переноса текста на другую строку. Может также служить для отделения графики от текста на интервал.

<HR> Тег, служащий для логического разделения текста горизонтальной линией.

<PRE> и **</PRE>** Между этими тегами располагается предварительно отформатированный текст. На экран он выводится шрифтом типа "курьер".

Параметры выравнивания, использующиеся в тегах <P> и <H*> :

ALIGN=LEFT – выравнивание по левому полю

ALIGN=RIGHT – выравнивание по правому полю

ALIGN=CENTER – выравнивание по центру

Теги выравнивания

<LEFT> и **</LEFT> –** выравнивание по левому полю

<RIGHT> и **</RIGHT> –** выравнивание по правому полю

<CENTER> и **</CENTER> –** выравнивание по центру.

Заголовки, служащие для выделения логических частей текста

<H1> и **</H1>** Заголовок первого уровня.

<H2> и **</H2>** Заголовок второго уровня.

<H3> и **</H3>** Заголовок третьего уровня.

<H4> и **</H4>** Заголовок четвертого уровня.

<H5> и **</H5>** Заголовок пятого уровня.

<H6> и **</H6>** Заголовок шестого уровня.

Теги для выделения текста и шрифта

<B> и **</B>** Теги для выделения текста (слов, букв) жирным шрифтом.

<I> и **</I>** Теги для выделения текста (слов, букв) курсивным шрифтом, типа Italic.

<U> и **</U>** Текст, расположенный между двумя этими тегами, будет подчеркнут.

<BLINK> и **</BLINK>** Текст, расположенный между двумя этими тегами, будет мигать.

<FONT SIZE=+n> и **</FONT>**

<FONT SIZE=-n> и **</FONT>** Теги для изменения размера шрифта.

<FONT COLOR="#OOOOFF> и **</FONT>** Теги для изменения цвета шрифта.

Теги для формирования списков

<OL> и **</OL>** Теги, показывающие начало и конец нумерованного списка

<UL> и </UL> Теги, показывающие начало и конец маркированного списка.

<LI> Элемент списка

<DL> и **</DL>** Теги, показывающие начало и конец глоссария.

<DT> Термин глоссария, располагается без отступа от левого поля страницы.

<**DD**> описание термина, располагается с отступом от левого поля страницы.

Теги-команды для вставки в текст объектов нетекстовой информации

<IMG SRC ="file.gif '> или **<IMG SRC =" file.jpg">** – команда для вставки графического изображения.

<IMG SRC =" file.wav"> – команда для вставки звукового фрагмента

<IMG SRC =" file.avi"> – команда для вставки видео фрагмента

Параметры графического изображения

WIDHT- ширина картинки в пикселях

HEIGHT- высота картинки в пикселях

ALIGN – выравнивание (ALIGN=LEFT – выравнивание по левому полю, ALIGN=RIGHT – по правому полю, ALIGN=TOP – по верхней границе, ALIGN=BOTTOM – по нижней границе, ALIGN=MIDDLE или CENTER – по центру).

HSPACE – горизонтальный отступ от графического изображения

VSPACE – вертикальный отступ

ALT- альтернативный текст, служит для обозначения изображения

Команды, служащие для гиперсвязи с другими HTML-документами и рессурсами Интернет

<A HREF="fail.htm"> и **</A>** или **<A HREF="http://www.ru">** и </A> – гиперсвязи

<ADDRESS><A HREF=mailto: person@firm.ru> person@firm.ru **</ADDRESS> –** гиперсвязь с адресом электронной почты

Таблицы

Таблица – сетка для показа данных в строках и столбцах, а также средство для форматирования текста

<TABLE> и **</TABLE>** Теги для вставки таблицы в HTML документ Параметры тега **<TABLE>**

BGCOLOR – цвет фона

BORDER – ширина бордюра

WIDHT – ширина таблицы

Теги разметки таблицы

<CAPTION> и **</CAPTION> –** название таблицы, имеет параметр ALIGN=TOP – выравнивание над таблицей и ALIGN=BOTTOM – под таблицей.
<TR> и **</TR>** Строчка таблицы. Может иметь параметры BGCOLOR – цвет фона внутри строки; ALIGN=LEFT, RIGHT, CENTER – выравнивание внутри строки; VALIGN=TOP, BOTTOM, MIDDLE – вертикальное выравнивание внутри строки таблицы.
<TD> и **</TD>** Столбец таблицы. Может иметь параметры BGCOLOR – цвет фона под столбцом; ALIGN=LEFT, RIGHT, CENTER – выравнивание внутри столбца; VALIGN=TOP, BOTTOM, MIDDLE – вертикальное выравнивание; COLSPAN растягивание клетки на несколько столбцов, ROWSPAN – растягивание клетки на несколько строк.
<TH> и **</TH>** Заголовок столбца. Может иметь параметры BGCOLOR – цвет фона под названием; ALIGN=LEFT, RIGHT, CENTER – выравнивание; VALIGN=TOP, BOTTOM, MIDDLE – вертикальное выравнивание; COLSPAN, ROWSPAN – растягивание клетки на несколько столбцов или строк; WIDHT – ширина названия.

Рамки-фреймы

Рамки-фреймы – средство для разделения экрана на несколько областей, в каждой из которых отображается содержимое отдельной Web-странички или даже целого Web-сайта.

<FRAMESET> и **</FRAMESET>** Теги для создания рамки

Параметры тега <FRAMESET>

COLS–подразделяют экран на определенное количество колонок (вертикальных)

ROWS – подразделяют экран на опредленное количество колонок (горизонтальных)

BORDCOLOR – цвет рамки

BORDER -ширина бордюра

FRAMEBORDER- граница рамки (FRAMEBORDER=YES – есть граница,

FRAMEBORDER=NO-нет границы,

FRAMESPACING=n – ширина границы)
<FRAME> Тег для описания рамки (<FRAME SRC= "file.htm">).
Параметры тега <FRAME>
SCROLING – параметр для регулировки полосы прокрутки:

SCROLING=YES – полоса прокрутки будет всегда

SCROLING=NO – полосы прокрутки не будет

SCROLING=AUTO – полоса прокрутки появляется только в случае необходимости

MARGINWIDHT и *MARGINHEIGHT* – параметры, которые управляют отступом внутри рамок, служат для выравнивания графического изображения внутри рамки

NORESIZE – параметр, указывающий на то, что размер рамки-фрейма никогда не будет меняться.

A link to <A HREF="file.htm" TARGET="frame2"> file.htm</A> – Связь между фреймами *TARGET*- атрибут связи между фреймами. Имеет несколько значений:

_BLANK загружает содержимое страницы, заданной ссылкой, в новое пустое окно.

_SELF содержимое страницы, заданной ссылкой, в окно, которое содержит ссылку.

_PARENT загружает содержимое страницы, заданной ссылкой, в окно, являющееся непосредственным владельцем набора фреймов.

_TOP содержимое страницы, заданной ссылкой, в окно, игнорируя используемые фреймы.

Обработка браузеров, не поддерживающих фреймы:
<FRAMESET>
Здесь располагаются фреймы
</FRAMESE1>
<NOFRAMES>
<BODY>
Здесь располагается текст без фреймов
<BODY>
</NOFRAMES>
В секции, предназначенной для тех пользователей, которые "не видят" рамки, можно расположить какой-нибудь пояснительный текст.

Бегущая строка
<**MARQUEE>** ТЕКСТ … </**MARQUEE**> – Тег, создающий бегущую строку

<MARQUEE DIRECTION=left>TEKCT</MARQUEE> – Если бегущую строку нужно направить справа налево

<MARQUEE DIRECTION=right>TEKCT</MARQUEE> – движение слева направо.

scroll – стандартное движение от правого края к левому

slide – надпись один раз пробегает от правого края к левому, где и остается.

alternate- движение от правого края страницы к левому и обратно. Бесконечный цикл.
<MARQUEE LOOP=n BEHAVIOR=scroll>TEKCT</MARQUEE> – Ограничение числа циклов.
Значение n оператора LOOP указывает число повторений цикла.
<MARQUEE WIDHT=n>TEKCT</MARQUEE>- указать ширину участка, занимаемого бегущей строкой, где n – ширина той части страницы, на которой расположена бегущая строка. Значение n указывается как в пикселях, так и в процентах от общей ширины видимой части страницы.

<MARQUEE scrollamount=n>TEKCT</MARQUEE> – Регулировка движения надписи по экрану. Здесь n – число пикселей,

<MARQUEE scrolldelay=t>TEKCT</MARQUEE> В данном случае переменная величина – время t – измеряется в миллисекундах. Метод задания скорости состоит в указании времени, спустя которое текст будет перерисован на экране заново.

<FONTSIZE=n><MARQUEE> TEKCT</MARQUEE></FONT> – возможность указывать величину шрифта текста в строке.

<MARQUEE BGCOLOR=n> TEKCT </MARQUEE> – окрасить поверхность бегущей строки в какой-либо цвет, где n, как это бывало и раньше, можно указать в вид шестнадцатеричного числа либо написав его название

<MARQUEE HEIGHT=n>TEKCT</MARQUEE> – указать высоту бегущей строки, задавая величину n в пикселях.

(Симонович С., Евсеев Г., Алексеев А. Специальная информатика: Учебное пособие. –М.: АСТ-ПРЕСС: Инфорком-Пресс, 1998. –480 с.)

Словарь терминов

Атрибуты файла -содержит характеристики файла: системный файл, скрытый файл, файл только для чтения (read-only) и т.д.

Аудиоадаптер (***Sound Blaster*** или ***звуковая плата***) - специальная электронная плата, которая позволяет записывать звук, воспроизводить его и создавать программными средствами с помощью микрофона, наушников, динамиков, встроенного синтезатора и другого оборудования.

Архивация – это процесс сжатия (плотной упаковки) информации с целью уменьшения занимаемого информацией объёма памяти. Для этой цели служат специальные архивирующие программы (программы - архиваторы), например PKZIP, ARJ, ARC, PAK и т.д. В каждой из них используется свой метод сжатия данных. В результате архивации содержимое нескольких файлов или даже подкаталогов в сжатом виде помещается в один файл называемый – архивом, архивным файлом.

Архитектура – концепция взаимосвязи элементов сложной структуры.

База – основные, опорные данные или элементы.

База данных – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными.

Буфер обмена - область памяти, предоставляемая операционной системой для временного хранения данных, которые необходимо передать. Можно вырезать или скопировать данные из одной прикладной программы в буфер обмена, а затем передать их из буфера обмена в другие прикладные программы.

Backup - резервные копии программного обеспечения, баз данных, рабочих файлов и т.д. Создаются для восстановления информации в случае ее потери, например при сбое компьютера, или при заражении вирусом.

BIOS (Basic Input-Output System) - базовая система ввода-вывода. Часть программного обеспечения, входящего в состав компьютера. Отвечает за тестирование и начальную загрузку системы. Также поддерживает стандартный интерфейс с внешними устройствами (экраном, дисками, принтером и т.д.). Хранится в ПЗУ.

Винчестер (Winchester disk) – малогабаритный пакет жестких магнитных дисков, герметизированных вместе с головками записи-чтения. Является внешней памятью персонального компьютера.

Boot-сектор (загрузочный сектор) - первый сектор логического диска (на флоппи-дисках совпадает с первым физическим сектором). Содержит программу-загрузчик, отвечающую за запуск операционной системы.

MBR (Master Boot Record) - первый физический сектор диска. Обычно содержит небольшую программу-загрузчик и таблицу разбиения диска (Disk Partition Table). Программа-загрузчик анализирует Disk Partition Table, выделяет в ней активный логический диск, загружает в память Boot-сектор этого диска и передает на него управление.

MCB (Memory Control Block) - единица (блок) системной памяти. Выделяется, изменяется и освобождается DOS при запуске программ или при соответствующих запросах. В памяти блоки памяти организованы в виде списка, состоящего из M-блоков и заканчивающегося Z-блоком.

PSP (Program Segment Prefix) - префикс программного сегмента. Расположен в начале участка памяти, выделяемого DOS под запускаемую программу. Создается операционной системой и содержит информацию о некоторых векторах прерываний, адресах системных полей и т.д.

DOS (Disk Operating System) – дисковая операционная система.

Драйвер (Driver) **–** программа вычислительной машины, предназначенная для непосредственного управления устройством на физическом уровне и поддержки работы периферийных устройств.

Заголовок EXE-файла **-** часть EXE-файла, содержащая управляющую информацию. Располагается в начале EXE-файла и содержит информацию для системного загрузчика: длину загружаемого модуля, значения регистров, таблицу настройки адресов и др.

Интерфейс (***interface***) - совокупность средств сопряжения и связи устройств компьютера, обеспечивающая их эффективное взаимодействие.

Кэш-память (cache) - сверхоперативная память - очень быстрое запоминающее устройство небольшого объёма, которое используется при обмене данными между микропроцессором и оперативной памятью для компенсации разницы в скорости обработки информации процессором и несколько менее быстродействующей оперативной памятью.

Кластер - единица разбиения логического диска. Состоит из одного или нескольких подряд расположенных логических секторов диска. Длина кластера на флоппи-дисках обычно равна 1 или 2 секторам, на винчестере - до 64 секторов.

Компьютер (англ. ***computer — вычислитель***) - программируемое электронное устройство, способное обрабатывать данные и производить вычисления, а также выполнять другие задачи манипулирования символами.

Корреляция (correlatio - соотношение) **–** термин, применяемый в различных областях науки и техники для обозначения взаимозависимости.

Корреляция (в математической статистике) **–** статистическая или вероятностная зависимость, не имеющая строго функционального характера. В отличии от функциональной, корреляционная зависимость возникает тогда, когда один из признаков зависит не только от данного второго, но и от ряда других меняющихся условий или же оба зависят от условии, среди которых имеются общие для них обоих.

Логический диск - единица разбиения диска. Состоит из подряд расположенных физических секторов. Логический диск делится на Boot-сектор, секторы FAT, корневого каталога и области данных. Секторы, входящие в область данных, группируются в кластеры. В пределах логического диска возможна логическая адресация к секторам.

Манипуляторы (мышь, джойстик и др.) —специальные устройства, которые используются для управления курсором.

Микропроцессор **-** центральный блок персонального компьютера, предназначенный для управления работой всех блоков машины и для выполнения арифметических и логических операций над информацией.

Модем — устройство для передачи компьютерных данных на большие расстояния по телефонным линиям связи.

Монитор — устройство визуального отображения информации (в виде текста, таблиц, рисунков, чертежей и др.).

Монитор - программа-монитор, блокировщик **-** резидентно находящаяся в оперативной памяти утилита, которая позволяет выявлять "подозрительные" действия пользовательских программ: изменение и переименование выполняемых программ (COM- и EXE-файлов), запись на диск по абсолютному адресу, форматирование диска и т.д. При обнаружении "подозрительной" функции программа-монитор либо выдает на экран сообщение, либо блокирует выполнение перехваченной функции, либо совершает другие специальные действия.

Основная память **-** предназначена для хранения и оперативного обмена информацией с прочими блоками машины, содержит два вида запоминающих устройств: постоянное запоминающее устройство (ПЗУ) и оперативное запоминающее устройство (ОЗУ).

Оперативная память (ОЗУ, англ. RAM, Random Access Memory — память с произвольным доступом) — предназначена для оперативной записи, хранения и считывания информации, непосредственно участвующей в информационно - вычислительном процессе, выполняемом ПК в текущий период времени.

Операционная система - комплекс управляющих и обрабатывающих программ, который, с одной стороны, выступает как интерфейс между аппаратурой компьютера и пользователем с его задачами, а с другой – предназначен для наиболее эффективного использования ресурсов вычислительной системы. Под управлением ОС выполняются команды по хранению, обработке и передаче информационных данных.

Постоянная память (ПЗУ, англ. ROM, Read Only Memory — память только для чтения) — энергонезависимая память, используется для хранения данных, которые никогда не потребуют изменения. Содержание памяти специальным образом “зашивается” в устройстве при его изготовлении для постоянного хранения. Из ПЗУ можно только читать.

Прерывание - сигнал, по которому процессор прерывает выполнение текущей последовательности команд и передает управление на программу - обработчик прерывания. Адрес программы-обработчика вычисляется по таблице векторов прерываний. Прерывание может быть инициировано либо программами пользователя при работе с дисками, экраном, принтером и т.д. (программные прерывания) либо внешними устройствами: клавиатурой, таймером (аппаратные прерывания).

Принтеры (печатающие устройства) - устройства вывода данных из ЭВМ, преобразующие информационные ASCII-коды в соответствующие им графические символы (буквы, цифры, знаки и т.п.) и фиксирующие эти символы на бумаге.

Псевдосбойный кластер - каждый кластер логического диска помечается в FAT как свободный, занятый или сбойный. Сбойным (плохим) считается кластер, который содержит один или несколько дефектных секторов. Такой кластер не используется DOS и невидим для нее. Псевдосбойным называется нормальный кластер (т.е. не имеющий дефектных секторов), но помеченный в FAT как сбойный. Выделить псевдосбойный кластер из, на самом деле, сбойных секторов можно несколько раз прочитав содержимое секторов кластера. Если при этом не произошло ошибки, то кластер псевдосбойный. Нормальные кластеры (т.е. не имеющие дефектных секторов) помечаются как сбойные некоторыми вирусами, которые могут затем использовать пространство таких кластеров в своих целях.

Регрессия (regressus – обратное движение) - в математической статистике регрессия обобщает понятие функциональной зависимости $y=f(x)$. Если в случае функциональной зависимости каждому значению независимого переменного x соответствует одно вполне определённое значение величины y, то в случае *Регрессии* одному и тому же значению $x=x_i$ в различных случаях соответствуют различные значения y.

Резидентная программа (TSR - Terminate and Stay Resident) - запускаемые на выполнение программы делятся на резидентные и нерезидентные программы. *Резидентная программа* по окончании оставляет свой код или часть кода в оперативной памяти, при этом DOS резервирует необходимый для ее работы участок памяти. Затем резидентная программа работает параллельно другим программам, некоторые из резидентных программ могут быть выгружены из памяти. *Нерезидентная программа* при завершении не оставляет в памяти своего кода, а занимаемая программой память освобождается.

Сектор - минимальная единица разбиения диска (т.е. минимальная адресуемая часть диска). Разбиение диска на секторы происходит при его форматировании. Различают физические (абсолютные) и логические секторы диска. Один и тот же сектор может рассматриваться как физический при обращении к нему функциями BIOS и как логический при обращении к нему при помощи прерываний DOS. Длина сектора обычно равна 512 байтам.

Системная шина - основная интерфейсная система компьютера, обеспечивающая сопряжение и связь всех его устройств между собой.

Сканер - устройство ввода в ЭВМ информации (тексты, схемы, рисунки, графики, фотографии и др.) непосредственно с бумажного документа.

Стелс (Stealth) - "Стелс"-вирусы (вирусы-невидимки) представляют собой программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков и "подставляют" вместо себя незараженные участки информации. Кроме этого такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие

"обманывать" резидентные антивирусные мониторы. К "стелс"-вирусам относятся вирусы "V-4096", "Fish#6", "Brain" и некоторые другие.

Системная или ***материнская плата*** - основная плата компьютера, где размещаются основные электронные компоненты, определяющие архитектуру процессора.

Центральный процессор (***Central Processing Unit***) —основной рабочий компонент компьютера, который выполняет арифметические и логические операции, заданные программой, управляет вычислительным процессом и координирует работу всех устройств компьютера.

Файл - единица организации логического диска. Файлы содержат информацию, содержащую какой-либо конкретный объект: программу, часть базы данных, тексты, прочие данные. К характеристикам файла относятся его длина (объем содержащейся в файле информации), атрибуты, время и дата последней модификации.

FAT (File Allocation Table)

Таблица распределения файлов. Состоит из последовательных секторов логического диска и содержит таблицу расположения файлов на этом диске. Размещается в секторах, следующих за Boot-сектором. Дополнительно информирует о свободных и сбойных секторах логического диска.

Файл (***File***) - именуемая единица информации, поддерживаемая операционной системой. Доступ к данным реализуется либо в рамках ОС, либо пользовательскими программами, либо в рамках СУБД, либо комбинированно.

Файл ASCII (***ASCII - file***) - файл, содержащий символьную информацию, представленную только ASCII - кодами «левой части» (первые 128 символов кодовой таблицы) и символьную разметку.

Файл базы данных - физически файл ОС, используемый для размещения базы данных. Управление данными в таком файле производится совместно ОС, СУБД.

Файл бинарный (***Binary file***) - файл, содержащий произвольную двоичную информацию (текст с бинарной разметкой, программа, графика, архивный файл).

Файл графически (***Image file***)- бинарный файл, содержащий данные, обычно полученные с помощью растрового сканера и соответствующие двумерному изображению объекта.

Файл текстовый (***Text file***) - файл, содержащий символьную информацию в одном из соответствующих кодов и коды, управляющие режимом отображения символов на печать и экранные устройства.

Фонд данных - общая совокупность хранящихся в банке данных, состоящая из БД и архивов. Основанием для этого разбиения является режим использования данных, находящаяся под оперативным управлением СУБД и размещенная, как правило, на магнитных дисках. Все остальные данные-архивы, обычно располагаются на магнитных лентах. Одни и те же данные в разные моменты времени могут входить как в БД, так и в архивы.

Форматы файлов - представление информации на уровне взаимодействия операционной системы с прикладными программами.

COM-файл - двоичный выполняемый файл, располагаемый при старте в одном сегменте и работающий в пределах этого сегмента. Программы, содержащиеся в COM-файлах (COM-программы) могут использовать и другие сегменты, но эти действия требуют специальных вычислений внутри самих программ. Поэтому все ссылки в COM-программах внутрисегментные и не требуют привязки к сегментному адресу.

EXE-файл - двоичный выполняемый файл, который может занимать в оперативной памяти один или несколько сегментов. При обращении к какому-либо сегменту EXE-программе требуется знать сегментный адрес этого сегмента. Для этого при загрузке в память DOS привязывает (настраивает) EXE-файл к адресам памяти, т.е. помещает в необходимые ячейки соответствующие сегментные адреса. Настройка EXE-файла происходит по таблице настройки адресов. Таблица настройки адресов расположена в заголовке EXE-файла и содержит адреса, по которым происходит привязка EXE-программы к сегментным адресам памяти.

OVL-файл **-** файл, содержащий выполняемые двоичные коды, используемые основной программой по мере необходимости.

SYS-файл **-** файл, содержащий системный драйвер. Загружается в память при инициализации DOS после загрузки системы. Для запуска SYS-файла необходимо поместить соответствующую команду в файл CONFIG.SYS и перезагрузить компьютер.

Список литературы

1. Основы кредитной системы обучения в Казахстане. / С.Б.Абдыгаппарова, Г.К.Ахметова, С.Р.Ибатуллин, А.А.Кусаинов, Б.А.Мырзалиев, С.М.Омирбаев; Под общей редакцией Ж.А.Кулекеева, Г.Н.Гамарника, Б.С.Абдрасилова. – Алматы, 2004. – 198 с.
2. Указ Президента Республики Казахстан от 17 мая 2003 года № 1096 О Стратегии индустриально-инновационного развития Республики Казахстан на 2003-2015 годы.
3. Ляхович В.Ф., Крамаров С.О. Основы информатики. Учебное пособие. – Ростов-на-Дону: Изд-во «Феникс», 2003. – 704 с.
4. Ершов А.П. Концепция использования средств ВТ в сфере образования. – Новосибирск: ВЦСО АН СССР, №888, 1990. – 58 с.
5. Бабанский Ю.К. Интенсификация процесса обучения. – М., 1997. – 80 с.
6. Коменский Я.А. Избранные педагогические сочинения: В 2 т. М., 1982. - Т.1. – 656 с., Т. 2. – 576 с.
7. Подласый И.П. Педагогика. Кн. 1: Общие основы. Процесс обучения. - Москва, 2003. – 576 с.
8. Методика преподавания и использования интерактивных методов обу-чения // Материалы семинара: «Создание электронных курсов на примере СДО MOODLE». – Алматы, 2004. – С. 5-21.
9. Государственный общеобязательный стандарт образования Республики Казахстан. Образование высшее профессиональное. Бакалавриат. Основные положения. ГОСО РК 5.03.001 – 2004. Утвержден приказом Министерства образования и науки Республики Казахстан от 30 апреля 2004 г., №380.
10. Назарбаев Н.А. Казахстан на пути ускоренной экономической, социальной и политической модернизации: Послание Президента РК народу Казахстана от 18 февраля 2005 года. // Казахстанская правда, №39(24649), 19.02.2005.
11. Материалы семинара «Создание электронных курсов на примере CDO MOODLE». – Алматы: Академия Образовательной Сети Казахстан, 2004. – 42 с.
12. В.П.Беспалько. Педагогика и прогрессивные технологии обучения. М.:Педагогика, 1995.- 836 с.
13. Макарова Н.В.Информатика: Учебник / под р.проф.Макаровой Н.В. - М.:Финансы и статистика, 1997.
14. Девис У. Операционные системы,- М.: Мир, 1980г.
15. Хакимова Т.Руководство к тестированию по курсу "Основы информатики":Учебное пособие..-Алматы: Қазақ университеті,2003.-51с.
16. Хакимова Т.Специальные программы для работы на персональном компьютере.:Учебное пособие..-Алматы: Қазақ университеті,2004.-31с.
17. Хакимова Т.Практикум самостоятельных работ по обучению автоматизации обработки данных.:Учебное пособие..-Алматы: Қазақ университеті,2005.-71с.
18. Хакимова Т. Компьютерлік өңдеудің мүмкіндігін жоғарылату.:Оқу құралы.- Алматы: Қазақ университеті,2006æ.,-65 áåò.
19. ХакимоваТ.Практикум по курсу "Основы информатики":Учебное пособие.- Алматы,Научно-издательский центр : Ғылым,2001.-117с.
20. Хакимова Т. Компьютерлік өңдеудің әдістемелері.:Оқу құралы.-Алматы:Ғылым,2002-160б.

21. Хакимова Т.Х. Информатика курсында MICROSOFT ACCESS бағдарламасын оқытудың кейбір әдістері.Журнал«ПОИСК»Серия естественных технических наук.Научное приложение международного журнала «Высшая школа Казахстана» МОиН РК №1(2).2004г.185-190стр. г.Алматы
22. Жангисина Г.Д.,Хакимова Т.Х, ТЕОРИЯ И МЕТОДИКА КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ ДЛЯ ЗАДАЧ БАЗЫ ДАННЫХ И ГЛОБАЛЬНОЙ СЕТИ(учебное пособие).-Алматы: МО и наукиРК.г.Алматы:НАУЧНО-ИЗДАТЕЛЬСКИЙ ЦЕНТР"ГЫЛЫМ",Алматы ,2007 г.,94стр.
23. Информатика. Базовый курс. 2-е издание. /Под редакцией С.В. Симоновича. - СПб: Питер, 2003. – 640 с.:ил.
24. Хакимова Т. Графикалықік компьютерлік моделдеу. :Оқу құралы.-Алматы:Заң әдебиеті,2008.-130б.
25. «Мультимедиа-Сервис» Лекционный курс. Государственный Университет Молдовы (http://www.iatp.md/virtualka).
26. «Компьютер для работы и дома» 1998г В.А.Никеров.
27. «Мультимедиа для всех» статьи И.Р.Куцнецова (http://inftech.webservis.ru/it/multimedia)
28. .«Мультимедийные технологии» лекционный курс. Якушин А.В http://www.tula.net/tgpu/resouces/yakushin/html_doc/doc08/doc08index.htm
29. «Тенденции развития аппаратного обеспечения компьютеров» Статья «Мультимедия» (http://cdo.bseu.by/dl/hardware)
30. Информационный сайт http://informika.ru
31. Сайт рефератов http://www.bankreferatov.ru
32. Угринович Н. Д. Информатика и информационные технологии: Учебник для 10—11 классов. М.: Лаборатория Базовых Знаний, 2002.
33. Угринович Н. Д., Босова Л. Л., Михайлова Н. И. Практикум по информатике и информационным технологиям: Учебное пособие для общеобразовательных учреждений. М.: Лаборатория Базовых Знаний, 2002.
34. Бобцов А. А., Лямин А. В., Чежин М. С. Программное обеспечение для работы в Internet.
М.: Федерация Интернет Образования, 2003.
35. Microsoft FrontPage 2000: Учебный курс. СПб.: Питер, 2000.
36. Столингс, Вильям. Криптография и защита сетей: принципы и практика,2-е изд.: Издательский дом “Вильямс”2001.-672 с.
37. Месси Дж. Л. Введение в современную криптологию. // ТИИЭР.- т. 76.-№ 5.-1988.-с. 24.
38. Симонович С., Евсеев Г., Алексеев А. Специальная информатика: Учебное пособие. М.: АСТ-ПРЕСС: Инфорком-Пресс, 1998. –480
39. Хакимова Т.Х.Ақпаратты қорғаудың алгоритмін математикалық моделдеудің кейбір түрі Международная научная конференция «Независимый Казахстан: 20 лет развития космических исследований» 4-5октября .Алматы,2011
40. Хакимова Т.Х.Особенности гипертекстовой технологии в кредитной системе обучения студентов университета(статья) Материалы V международной научно-методической конференции «Математическое моделирование и информационные технологии в образовании и науке» ММ ИТОН V»,1-2 октября 2010г.III-том,243-248стр.Алматы,2010
41. Закон РК «Об образовании».
42. Государственная программа развития образования Республики Казахстан на 2011-2020 годы. Проект. http://www.edu.gov.kz/index.php?id=838&L=1
43. ГОСО РК. Организация обучения по дистанционным образовательным технологиям. Основные положения (от 4.06.2009 №266).

44. Правила организации учебного процесса по дистанционным образовательным технологиям от 13 апреля 2010 года № 169.
45. Правила организации учебного процесса по дистанционным образовательным технологиям от 20 мая.2010 года № 6242.
46. Джандигулов А.Р. Методические рекомендации по организации и проведению индивидуального компьютерного тренинга по технологии дистанционного обучения. - Астана: Издательство КРУ, 2005. – 19 с.