Министерство образования Российской Федерации
Томский политехнический университет

Кафедра компьютерных измерительных систем и метрологии
(КИСМ)

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Учебное пособие по изучению дисциплины "Информационные технологии стандартизации и сертификации" для студентов специальности 072000 "Стандартизация и сертификация"

Разработчик

Канд. техн. наук, доцент
О.В. Стукач

УДК 658.8:681.3

О.В. Стукач. Информационные технологии. Учебное пособие по изучению дисциплины "Информационные технологии стандартизации и сертификации" для студентов специальности 072000 "Стандартизация и сертификация".

Учебное пособие рекомендуется студентам специальности 072000 "Стандартизация и сертификация (в приборостроении)" в качестве основного методического материала по курсу "Информационные технологии стандартизации и сертификации". В пособии приводится программа, описание лабораторных работ и экзаменационные вопросы. Даются комментарии к изучению дисциплины и выбору литературы.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

Новые информационные технологии (ИТ) быстро изменяют наш мир, непосредственно влияют на производственные процессы, методы организации и развития общества. В силу единства реального мира, новые технологии организации бизнеса проникают в социальные, политические, культурные и другие сферы жизни общества, изменяют способы общения, ведения дел и образования. Эта технологическая революция сильно повлияла не только на бизнес, но также на частную и профессиональную жизнь. Внутренняя сложность и предельная простота применения современных ИТ поражает воображение каждого, кто ежедневно сталкивается с применением ИТ в своей профессиональной деятельности.

ИТ являются лучшим примером стандартизации бизнес-процессов, освобождая время для продуктивной творческой деятельности человека. Главное преимущество ИТ в современных условиях проявляется в децентрализации и повышении прозрачности управленческой деятельности, что приводит к ликвидации монополии на управленческое знание.

Курс "Информационные технологии стандартизации и сертификации" рассматривает ИТ с точки зрения применения их в стандартизации и сертификации в триединстве обзора современных сетевых технологий передачи и обработки информации, технологии защищенного документооборота и проектирования реляционных баз данных. Особое внимание уделяется управлению качеством как главному потребителю и движущей силе ИТ.

2. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ УКАЗАНИЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ "ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ СТАНДАРТИЗАЦИИ И СЕРТИФИКАЦИИ"

2.1. Цели и задачи изучения дисциплины

Целью преподавания дисциплины является усвоение студентом вопросов теории и практики использования информационных технологий при исследовании, разработке, конструировании, технологии производства продукции или услуги, сбыте и обслуживании потребителя и формировании у студентов мотивации к проектированию компьютерных систем стандартизации и сертификации.

Задачами изложения и изучения дисциплины являются:

- разработка содержания разделов дисциплины, позволяющих реализовать общую схему решения научно-технических задач профессиональной деятельности (анализ информационных технологий в области стандартизации и сертификации; проектирование компьютерных систем в области качества; разработка методов измерения, обработки и представления информации о качестве объекта);
- организация учебного процесса с элементами научно-практической деятельности;
- реализация текущего, промежуточного и итогового контроля с использованием вопросов и задач, позволяющих студентам применить на практике необходимые знания и умения.

2.2. Знания, умения и навыки, которые должен приобрести студент в результате изучения дисциплины

В результате изучения данной дисциплины студент должен **понимать:**

- необходимость использования новых информационных технологий в жизнедеятельности человека;
- общие принципы информационной безопасности;
- сущность реляционной модели баз данных;

знать:

- общие вопросы теории и практики проектирования компьютерных систем в области контроля, управления, обеспечения и планирования качества объектов различной природы;
- методы проектирования, модернизации и автоматизации оборудования для обеспечения гарантии качества и испытаний;
- развитие современных информационных технологий и их использование в стандартизации и управлении качеством;
- общие принципы построения программного обеспечения для компьютерных систем стандартизации и сертификации;

- проблемы и тенденции развития техники и технологии в сфере производства продукции и оказания услуг в приборостроении;
- организационные и технические основы создания и совершенствования систем контроля и управления системами обеспечения качества;

уметь:

- применять современные информационные технологии в системах стандартизации и сертификации;
- применять технические и программные средства для контроля, управления и обеспечения качества;
- профессионально работать с программными средствами обеспечения защищенного документооборота и базами данных.

3. ПРОГРАММА ДИСЦИПЛИНЫ "ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ СТАНДАРТИЗАЦИИ И СЕРТИФИКАЦИИ".

3.1. *Общие сведения об информационных технологиях*

Обработка информации. Что такое ИТ. Этапы развития новых информационных технологий. Компоненты ИТ. ИТ как глобальное явление. Цели использования информационных технологий для стандартизации и сертификации.

3.2. Интернет

Интернет как информационная система. Преимущества Интернета. Интернет-протоколы. Услуги, предоставляемые сетью. Программное обеспечение Интернета.

3.3. CALS-технологии

Что такое CALS. Краткое описание CALS-технологий. Текущее состояние новых информационных технологий.

3.4. Основы безопасности информационных технологий и систем

Основные проблемы информационной безопасности. Степень важности информации. Безопасность субъектов информационных отношений. Угрозы безопасности системам обработки информации. Определение требований к защищенности информации. Основные меры противодействия угрозам безопасности. Пять главных категорий информационной безопасности. Контроль за информационной безопасностью. Основные принципы построения систем защиты. Меры безопасности информационных систем.

3.5. Методы криптологии в информационных технологиях

Основные определения криптологии. Шифрование с секретным ключом. Стандарты шифрования данных. Системы с открытым ключом. Электронная цифровая подпись. Хеш-функция (дайджест сообщения). Стандарты цифровой подписи. Электронный конверт. Юридический статус документов, подписываемых цифровыми подписями. Магнитные и смарт-карты. Основные понятия и принципы использования магнитных карт. Смарт-карты. Пластиковая карта как платёжный инструмент. Платёжная система. POS-терминалы и банкоматы. Аутентификация данных на картах.

3.6. Системы управления базами данных

Основные определения: данные, база данных, системы управления базами данных (СУБД). Основная идея реляционной модели. Структура реляционных баз данных. Null-значения. Трёхзначная логика. Первичный ключ. Целостность сущностей. Внешние ключи. Язык SQL. Реляционная алгебра. Транзакции и целостность баз данных. Ограничения целостности. Транзакции и восстановление данных. Виды восстановления данных.

3.7. Системы баз знаний

Знание против информации. Определение и систематика знания. Знание как процесс. Общие сведения о системах баз знаний. Машинное решение задач. Природа человеческих знаний. Экспертные системы.

3.8. Системы поддержки принятия решений

Развитие систем поддержки принятия решений. Архитектура систем поддержки принятия решений. Процесс принятия решений и его функции. Подсистемы поддержки принятия решений. Подсистемы поддержки принятия решений, основанные на организационных перспективах. Будущее СППР.

3.9. Компьютерные средства коллективной работы в сети

Компьютерные системы поддержки коллективной. работы и программное обеспечение коллективного пользования. Программные средства совместной работы. Программное обеспечение коллективной работы для поддержки хранения и поиска информации. Программное обеспечение коллективной работы для поддержки принятия решений.

3.10. Информационные технологии управления

Классификация управленческой информации. Источники управленческой информации. Управленческие информационные системы. ИТ и корпоративная стратегия. Информационные технологии в управленческих функциях. Телекоммуникации. Интеллектуальные системы. Системы знаний и мудрости. Повышение качества управления. Системы виртуальной реальности. Менеджмент и управление проектами.

3.11. Реинжиниринг

Что такое реинжиниринг. Семь принципов реинжиниринга. Процессное мышление. Реинжиниринг как реинтеграция. Правило "10-90". Реинжиниринг и стратегия. Применение новых технологий для обеспечения качества технологических процессов

3.12. Системы планирования ресурсов предприятия

Системы планирования ресурсов предприятия (ERP). Перспективы систем ERP. Системы ERP и конкурентные преимущества. Архитектура типовой системы ERP. Реализация ERP-систем.

3.13. Информационные технологии управления качеством

Принципы и философия управления качеством. Стратегия управления качеством и области его применения. ИТ как конкурентное преимущество в управлении качеством.

3.14. Использование информационных технологий для метрологического обеспечения качества

Принципы использования новых технологий для стандартизации и сертификации обеспечения качества. Стратегия автоматизированного контроля для обеспечения качества. Примеры интеллектуальных систем стандартизации и сертификации. Системы проектирования информационных технологий.

4. ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ И ОФОРМЛЕНИЮ ОТЧЕТА

Лабораторные работы не могут быть выполнены вне аудитории на посторонних компьютерах. Совершенно недопустимо использовать программы не в учебных целях.

При выполнении лабораторных работ следует строго руководствоваться требованиями задания к работе. Пункты задания, как правило, взаимосвязаны, поэтому нарушение последовательности их выполнения не рекомендуется.

5. ТЕМАТИКА ЛАБОРАТОРНЫХ ЗАНЯТИЙ

5.1. Лабораторная работа № 1. Недокументированные возможности Windows приложений

5.1.1. Цель работы

На персональных компьютерах существует возможность ведения протокола работы и слежения за операциями или процессами. Это возможность записи того, что вы печатаете на чужом компьютере, владельцем этого компьютера, или, если смотреть на это с другой стороны, ваше право посмотреть, что творилось на вашем компьютере, пока вас не было в офисе.

И то, и другое делается одним методом: все, что набирается на клавиатуре, заносится в файл специальной программой. Технически такая операция выполняется классом программ, называемых keyboard loggers. Они существуют для разных операционных систем, могут иметь много настроек, позволяющих определять нужную конфигурацию, могут автоматически загружаться при включении компьютера, при этом никак не проявляя своего присутствия. Набранный на клавиатуре текст, названия программ, в которых набирался текст, и даже скрытые пароли записываются в скрытый лог-файл. Существуют также программы, которые периодически делают копии экрана, записывая их в каком-либо графическом формате. В работе изучаются некоторые из широко распространенных программ.

5.1.2. Лабораторное задание

1. Убедиться, что содержание файлов MTT-1.DOC и MTT-2.DOC одинаково. Исследовать внутреннюю структуру файлов, например, с помощью Far Manager или HIEW.EXE. Сравнить размер файлов. Объяснить причину разницы в размере файлов.

2. Запустить несколько выбранных вами программ-шпионов, а затем поработать на компьютере, запуская различные программы, создавая и удаляя файлы и каталоги. Работать в режиме полной невидимости не рекомендуется для избежания частых перезагрузок компьютера. Найти файлы протоколов и убедиться, что все действия на компьютере не остались незамеченными. Включить избранные места из этих файлов и характерные скриншоты в отчет.

5.2. Лабораторная работа № 2. Сжатие данных и архиваторы

5.2.1. Цель работы

Цель работы – ознакомиться с программами сжатия данных (архиваторами), изучить методы вскрытия паролей и сравнить методы сжатия информации по степени избыточности.

5.2.2. Краткие теоретические сведения

Для затруднения криптоанализа стараются исключить избыточность из открытого текста. Методология исключения избыточности имеет самостоятельное значение – для проектирования программ архивирования данных. Алгоритмы архивирования исключают избыточность данных в файлах, за счет чего уменьшается объем хранимой в архиве информации.

Мерой избыточности может служить величина:

$$U = 1 - H / \log_2 n ,$$

где $H = -\sum_{i=1}^{n} p_i \log_2 n$ – средняя энтропия на один символ, n – число символов, используемых в файле, p – частота появления символа в файле.

Большинство программ-архиваторов допускают использование паролей, что позволяет защитить данные от несанкционированного использования. Существуют вырожденные пароли, которые нельзя использовать при архивировании, так как обратная операция возможна при любом значении пароля.

5.2.3. Назначение используемых файлов и программ

FILE-1.TXT – текстовый файл для экспериментов;
ARJ.EXE – архиватор ARJ;
BRKARJ.EXE – программа вскрытия пароля ARJ архива;
SOLVEPWD.COM – программа вскрытия пароля ARJ архива при известном архиве без пароля;
ISXTXT.ARJ – архив, содержащий исходный текст;

RAR.EXE – архиватор RAR;
ANYPASS.RAR – архив с вырожденным паролем;
PLENTY.EXE – программа расчета избыточности файлов;

5.2.4. Лабораторное задание

1. Архиватором ARJ архивировать файл FILE-1.TXT. Параметры командной строки для консольного архиватора:

arj a ИМЯ_АРХИВА FILE-1.TXT

2. Архиватором RAR архивировать файл FILE-1.TXT. Параметры командной строки для консольного архиватора:

rar a ИМЯ_АРХИВА FILE-1.TXT

3. С помощью программы PLENTY.EXE провести анализ избыточности полученных архивов и открытого текста. Используйте следующие параметры командной строки:

PLENTY.EXE входн.файл выходн.файл

и установленные по умолчанию в меню параметры.

4. Сравнить избыточность полученных архивов и открытого текста. Какой архиватор лучше сжимает текст? Как изменился размер файла? Исследовать внутреннюю структуру архивных файлов, например, с помощью Far Manager. Из чего состоит заголовок архива?

5. Архивировать еще раз какой-нибудь архивный файл и провести анализ избыточности. Повысилась ли степень сжатия информации в архиве? Почему? Как изменился размер файла?

6. Распаковать архив ISXTXT.ARJ. Параметры командной строки для консольного архиватора:

arj x ISXTXT.ARJ

С помощью программы PLENTY.EXE провести анализ избыточности полученного открытого текста и архива. Исследовать внутреннюю структуру архива ISXTXT.ARJ с помощью Far Manager. Сравнить содержимое архива ISXTXT.ARJ с открытым текстом. В чем состоит причина наблюдаемых явлений?

7. Архиватором ARJ архивировать файл FILE-1.TXT С ПАРОЛЕМ. Рекомендуется использовать четырехсимвольный пароль из строчных букв. Параметры командной строки:

arj a -gПАРОЛЬ ИМЯ_АРХИВА FILE-1.TXT

Попробовать распаковать архив, указав неверный пароль.

8. С помощью программы BRKARJ.EXE вскрыть пароль ARJ архива. Оценить скорость вскрытия пароля.

9. С помощью программы SOLVEPWD.COM вскрыть пароль ARJ архива при известном открытом тексте. Оценить скорость вскрытия пароля.

10. Файл ANYPASS.RAR представляет собой архив с вырожденным паролем. Распаковать архив и убедиться в том, что он распаковывается при любом значении пароля. Сравнить с результатами п. 4.7. Сделать выводы о необходимости проверки паролей на вырожденность.

5.3. Лабораторная работа № 3. Информационная безопасность

5.3.1. Цель работы

Для защиты конфиденциальной информации часто используется программное шифрование. В настоящее время на предприятиях и организациях различных форм собственности используется большое количество программ шифрования. Однако лишь небольшая часть из них прошла проверку на криптостойкость алгоритма и его программной реализации. Пользователи, работающие с непроверенными программами, подвергают себя и защищаемые данные неоправданно большому риску.

Известно много методов шифрования, отличающихся по криптостойкости. Для оценки криптостойкости часто используют вскрытие шифра. Одним из криптоаналитических нападений является частотный способ – подсчет редко и часто встречающихся символов в шифртексте.

Целью работы является ознакомление со стандартными методами и программами шифрования, оценка стойкости шифрования к нападению частотным способом, изучение простейших методов проверки стойкости программного шифрования.

5.3.2. Краткие теоретические сведения

Частотный анализ криптограммы позволяет определить частоту встречаемости символов шифралфавита. Сильная неравномерность таблицы, характерная для теоретически известной (см. табл. 1) позволяет вскрыть шифр путем эквивалентной замены символов. Это вовсе не свидетельствует, что не будут попадаться сообщения, в которых другая буква будет встречаться чаще, чем "О" и реже, чем "Ф". Но для достаточно большого числа сообщений могут быть установлены определенные характерные частоты, что дает путь к раскрытию шифра.

Таблица 1.

Частоты встречаемости букв русского алфавита

Буква	Частота	Буква	Частота	Буква	Частота
пробел	0,145	к	0,029	ч	0,013
о	0,095	м	0,026	й	0,010
е	0,074	д	0,026	х	0,009
а	0,064	п	0,024	ж	0,008
и	0,064	у	0,021	ю	0,007
т	0,056	я	0,019	ш	0,006
н	0,056	ы	0,016	ц	0,004
с	0,047	з	0,015	щ	0,003
р	0,041	ъь	0,015	э	0,003

в	0,039	б	0,015	ф	0,002
л	0,036	г	0,014		

Для определения того, находятся ли криптоаналитики на правильном пути, они часто используют индекс соответствия:

$$ИС = 1/[N(N-1)]\sum_{i=1}^{k} f_i(f_i-1)$$

где k – число символов в алфавите; f – общее число встречаемости i буквы в зашифрованном тексте; N – общее число букв в шифртексте. Теоретически ожидаемое значение ИС для английского языка определяется выражением:

ИС = (N–m)/[m(N–1)]*0,066+0,038*(m–1)*N/[m(N–1)],

где N – длина сообщения, m – число алфавитов (табл. 2).

Таблица 2

Теоретически ожидаемое значение ИС для английского языка

m	ожидаемый ИС при больших N
1	0,066
2	0,052
3	0,047
4	0,045
5	0,044
10	0,041
очень много	0,038=1/26

Если значение ИС больше 0,066, то, вероятно, использовалась моноалфавитная подстановка, если значение ИС находится между 0,052 и 0,047, то, вероятно, был использован двухалфавитный шифр подстановки и т.д. Это дает криптоаналитику превосходный инструмент для вскрытия шифра. Ситуация осложняется, если полученный ИС меньше 0,038.

5.3.3. Назначение используемых файлов и программ

FILE-1.TXT – текстовый файл для экспериментов;

FREQ-AN.EXE – программа частотного анализа файлов;

VIGINER.EXE – программа шифрования методом Вижинера;

EIW.EXE – программы шифрования по криптоалгоритму стандарта DES и расчета статистики (EID.EXE - для DOS);

DES.EXE – программа шифрования по криптоалгоритму стандарта DES с интерфейсом в виде командной строки.

MGOST.EXE – программа шифрования файла по криптоалгоритму стандарта ГОСТ 28147-89;

IDEA.COM – программа шифрования файла по криптоалгоритму стандарта IDEA;

HIEW.EXE – текстовый редактор.

5.3.4. Описание используемых программ

С помощью программы EIW можно шифровать файлы и проводить их частотный анализ. Программа частотного анализа файлов FREQ-AN.EXE проводит подсчет частоты встречаемости символов в исследуемом файле, сортирует частоты встречаемости по убыванию и строит графики полученного распределения и распределения частот встречаемости букв в русскоязычных текстах (табл. 1).

Для удобства сравнения распределений графики нормируются к максимальной частоте встречаемости символов (ось ординат) и по количеству символов (ось абсцисс). В отличие от FREQ-AN.EXE, программа EIW не сравнивает частотные распределения.

5.3.5. Лабораторное задание

1. Зашифровать файл FILE-1.TXT с помощью программ: MGOST.EXE, IDEA.COM, EIW.EXE, VIGINER.EXE односимвольным, двухсимвольным и четырехсимвольным ключами. Поскольку в процессе работы будет создано достаточно большое количество файлов, записывайте или запоминайте их имена. Записывайте или запоминайте ключи и пароли.

2. С помощью программ частотного анализа файлов FREQ-AN.EXE и EIW.EXE (EID.EXE) провести частотный анализ всех полученных криптограмм и открытого текста FILE-1.TXT.

3. Сравнить полученные результаты с теоретически известными. Проанализировав таблицы и графики частотного распределения символов открытого текста и криптограммы, сделать выводы об изменении таблицы частотного распределения, о стойкости криптограмм к частотному криптоанализу для КАЖДОГО метода и изменении размера файлов при шифровании. Для метода Вижинера сделать выводы о влиянии длины ключа на стойкость к криптоанализу.

4. Сравнить ИС для всех полученных криптограмм и открытого текста. Для метода Вижинера определить, совпадает ли ИС с теоретически известным и можно ли определить количество алфавитов.

5. Изменить хотя бы один байт во всех криптограммах, например, с помощью HIEW.EXE. Параметры командной строки: HIEW имя_файла.

6. Расшифровать все криптограммы. Сравнивая расшифрованные криптограммы с исходным текстом, сделать выводы об имитостойкости всех стандартов шифрования.

5.4. Лабораторная работа № 4. Электронная цифровая подпись

5.4.1. Цель работы

В настоящее время широкое распространение на практике получили двухключевые системы шифрования, или системы с открытым ключом. Их основная особенность состоит в том, что для шифрования и дешифрования используются разные ключи.

Цель работы – изучить криптографические системы с открытым ключом на примере системы RSA, используемой в алгоритме программы PGP, встроенной в почтовый клиент The Bat! В работе также исследуется проблема защиты банковских карт.

5.4.2. Содержание работы

1. С помощью программы CRC.EXE рассчитать CRC для файла FILE-1.TXT. Изменить хотя бы один символ файла с помощью программы HIEW.EXE и проверить CRC. Можно ли использовать CRC в качестве цифровой подписи?

2. С помощью программы CRYPTO.EXE исследовать криптосистему RSA. Выбрать два простых числа P, Q и возможный открытый ключ. Сгенерировать секретный ключ. Доказать ручным расчетом правильность найденного секретного ключа. Написать текст, зашифровать его открытым ключом и расшифровать текст с помощью секретного ключа.

3. С помощью почтовой программы The Bat! исследовать все возможности криптосистем с открытым ключом:

- создать открытые и закрытые ключи отправителя и получателя (Tools/OpenPGP/Open PGP Key Manager, далее следовать инструкциям);
- создать письмо (кнопка Create a new message) и подписать его открытым ключом получателя (включить Privacy/Sign when Completed; выключить Privacy/Enable S/MIME);
- "отправить" письмо (кнопка Put the letter in Outbox), переместив его в папку "отправленные (Outbox)";
- "получить" письмо, скопировав в папку "полученные (Inbox)" (Message/Copy to Folder...);
- проверить подпись и аутентичность сообщения (Tools/OpenPGP/Check OpenPGP Signature или просто Shift+Ctrl+C);
- изменить хотя бы один символ письма или подписи, проверить подпись и аутентичность сообщения. Тексты подписанных электронной подписью писем включить в отчет.

Для внесения изменений в письмо или подпись необходимо воспользоваться Far Manager или программой HIEW.EXE. Почтовая программа The Bat! хранит все письма в файлах message.tbb, поэтому необходимо найти этот файл в соответствующий папке, например, C:\Program Files\The Bat!\имя_ящика\Inbox\message.tbb и внести исправления. Нельзя изменять размер файла message.tbb и служебную информацию для содержащихся там писем.

4. С помощью какой-либо программы для работы с номерами банковских карт CRDTWIZ.EXE, CCMAKER.EXE (Windows), CMASTER4.EXE,

VALICARD.EXE, CCARDS.EXE (DOS) сгенерировать несколько номеров и проверить их правильность. Вы можете проверить ваши банковские карты.

5. Изменить последнюю цифру валидного номера карты на единицу и проверить номер.

6. Исследовать все режимы работы программ (генерация и проверка номеров карт, экстраполяция новых номеров, формирование электронной цифровой подписи).

5.5. Лабораторная работа № 5. Системы управления базами данных

5.5.1. Цель работы

Системы хранения, ведения и анализа данных имеют первостепенное значение в любых сферах деятельности. В работе рассматривается реляционная модели данных и принципы функционирования реляционных баз данных. Изучается целостность реляционных данных, целостность сущностей и целостность ключей.

Цель работы – овладеть различными методами непосредственного анализа данных, хранящихся в СУБД.

5.5.2. Используемые программы и файлы

DBF_STR.TXT – описание структуры файла баз данных типа .DBF;
DBFNAVI.EXE – редактор DBF формата (Windows);
SC.EXE – редактор DBF формата (DOS);
СУБД (исполняемый файл – SP.EXE);
HIEW.EXE – текстовый редактор юного хакера;
SYSTEM.DBF – пример DBF файла.

5.5.3. Содержание работы

1. Кратко ознакомиться со структурой формата баз данных DBF (файл DBF_STR.TXT).

2. С помощью программы DBFNAVI ознакомиться с работой СУБД sp. Исследовать структуру базы, найти первичный ключ. Определить, какие свойства отношений выполняются в данной СУБД, а какие нет. Сколько отношений содержит база? Можно ли было сократить их количество при проектировании базы? Найти дочерние и родительские отношения.

3. Нарушить ссылочную целостность СУБД. Что произошло с СУБД? Как изменилась ее работа? К чему приводит вставка и удаление кортежей отношений? *Примечание:* для быстрого восстановления работоспособности базы предварительно копируйте файлы, которые будете редактировать.

6. ПЕРЕЧЕНЬ ЭКЗАМЕНАЦИОННЫХ ВОПРОСОВ

1. Задачи обработки информации, решаемые информационными технологиями (ИТ).
2. Что такое ИТ.
3. Этапы развития новых информационных технологий.
4. Компоненты ИТ (Hardware, Software, Brainware).
5. ИТ как глобальное явление. Всемирные ИТ-проекты.
6. Функции Интернета.
7. Преимущества Интернета.
8. Система доменных имен и IP-адреса.
9. Услуги, предоставляемые Интернетом.
10. Гиперссылки и гипертекст.
11. Универсальный локатор ресурса (URL). Функция браузера.
12. Что такое CALS-технологии.
13. Области применения CALS-технологий.
14. Цели защиты информации.
15. Степени важности информации.
16. Определение требований к защищенности информации.
17. Главные категории информационной безопасности.
18. Универсальные механизмы защиты информации (идентификация, аутентификация, авторизация, контроль доступа).
19. Цели сертификации продукции ИТ.
20. Основные принципы построения систем защиты.
21. Меры безопасности информационных систем.
22. Стандарты шифрования данных (DES, ГОСТ 28147-89).
23. Системы с открытым ключом.
24. Алгоритм RSA.
25. Хеш-функция (дайджест сообщения), ее свойства.
26. Электронный конверт.
27. Электронная цифровая подпись.
28. Юридический статус документов, подписываемых цифровыми подписями.
29. Структура систем защищенного документооборота.
30. Общая проблема аутентификации с использованием магнитных карт.
31. Модели баз данных.
32. Сущность реляционной модели данных.
33. Структура реляционных баз данных.
34. Свойства отношений в СУБД.
35. В чем заключается проблема Null-значений?
36. Первичный ключ и его свойства.
37. Правило целостности сущностей и способы его обеспечения в СУБД.
38. Теоретико-множественные операторы реляционной алгебры.
39. Специальные реляционные операторы реляционной алгебры.
40. Свойства транзакции.
41. Что такое ограничения целостности и для чего они используются в СУБД.

42. Виды восстановления данных в СУБД.
43. Как выполняется индивидуальный откат транзакции?
44. Цели использования ИТ для стандартизации и сертификации.

Экзаменационный билет состоит из трех задач, составленных по вышеуказанным вопросам.

7. СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

7.1. Основная литература

Базы данных: модели, разработка, реализация / Т.С. Карпова. – СПб.: Питер, 2001. – 304 с.
Баричев С. В. Криптография без секретов. – М.: Наука, 1998. – 120 с.
Бойко В.В., Савинков В.М. Проектирование баз данных информационных систем. – М.: Финансы и статистика, 1989. – 351 с.
Базы знаний интеллектуальных систем / Т. А. Гаврилова, В. Ф. Хорошевский – СПб: Питер, 2000. – 384 с.
Дейт К. Введение в системы баз данных. – Киев: Диалектика, 1998. – 784 с.
Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1996. – 336 с.
Змитрович А.И. Базы данных. – Минск.: Университетское, 1991. – 271 с.
Информационные технологии в бизнесе / Под ред. М. Желены. – СПб: Питер, 2002. – 1120 с. (серия "Бизнес-класс").
Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 1999. – 672 с.
Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – Серия "Учебники для вузов" – СПб.: Лань, 2000. – 224 с.
Мейер М. Теория реляционных баз данных. – М.: Мир, 1987. – 608 с.
Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электронинформ, 1997. – 368 с.
Петренко С. А., Петренко А. А. Аудит безопасности Intranet. – М.: ДМК Пресс, 2002. – 416 с. (Информационные технологии для инженеров).
Столлингс В. Криптография и защита сетей: принципы и практика. Пер. с англ. – М.: Изд. дом "Вильямс", 2001. – 672 с.
Ульман Д. Основы систем баз данных. – М.: Финансы и статистика, 1983. – 334 с.
Хофманн Д. Измерительно-вычислительные системы обеспечения качества / Пер. с нем. – М.: Энергоатомиздат, 1991. – 272 с.
Шишкин И.Ф. Метрология, стандартизация и управление качеством: Учеб. для вузов / Под. ред. Н.С. Соломенко. – М.: Изд-во стандартов, 1990. – 342 с.

Шураков В.В. Обеспечение сохранности информации в системах обработки данных. Учебн. пособ. для вузов. – М.: Финансы и статистика, 1985. – 224 с.

7.2. Дополнительная литература

Бородаев В.А., Кустов В.Н. Банки и базы данных. – Л.: ВИКИ им. А.ф.Можайского, 1989. – 224 с.
Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат. 1994. – 400 с.
Голубев В.В., Дубров П.А., Павлов Г.А. Механизмы защиты операционных систем и систем управления базами данных // Зарубежная радиоэлектроника, 1989. – N12. – С. 36-47.
Джинчарадзе А. К., Ефимов А. К., Судов Е. В. Автоматизированная информационная поддержка жизненного цикла продукции (объектов управления) на основе CALS-технологий // Качество: теория и практика, 1999, N 4. – С. 4-22.
Джинчарадзе А. К., Подлепа С. А. Открытые системы и функциональные стандарты // Стандарты и качество, 1998, № 4.
Диго С.М. Проектирование и использование баз данных. – М.: Финансы и статистика, 1995. – 208 с.
Мартин Д. Планирование развития автоматизированных систем. – М.: Финансы и статистика, 1984. – 196 с.
Нагао М., Катаяма Т., Уэмура С. Структуры и базы данных. – М.: Мир, 1986. – 197 с.
Тиори Т., Фрай Д. Проектирование структур баз данных. В 2 кн., – М.: Мир, 1985. Кн. 1. – 287 с.: Кн. 2. – 320 с.
Ухлинов Л.М. Принципы построения системы управления безопасностью данных // Автоматика и вычислительная техника, 1990. – N 4, 5. – С. 11-17.
Хоффман П. Internet – К.: Диалектика, 1995.
Caloyannides M.A. Encryption wars: early battles. In IEEE Spectrum, 2000, no. 4, pp. 37-43.
Caloyannides M.A. Encryption wars: shifting tactics. In IEEE Spectrum, 2000, no. 5, pp. 46-51.
M.E. Hellman, "An Overwiew of Public Key Cryptography". In IEEE Communications Magazine. 50th Anniversary Commemorative Issue. May 2002, no. 5, pp. 42-49.