Тема. Прикладное программное обеспечение информационных систем

Учебные вопросы темы

1. Архивирование данных
2. Технологии работы с документами

Литература к теме 4

Основная литература

1. Жданов С.А., Иванова Н.А., Маняхина В.Г., Костин А.Н., Матросов В.Л. Информатика. Серия: высшее профессиональное образование. Бакалавриат. – М.: Academia, 2012. – 336 с.
2. Алехина Г.В. и др., Основы информатики. – М.: Маркет ДС, 2009. – 472 с.

Дополнительная литература

3. Левин А.Ш. Word и Excel. Серия: Самоучитель Левина. – Спб: Питер, 2011. – 226 с.
4. Официальный русскоязычный сайт корпорации Microsoft http://www.microsoft.com/ru-ru/default.aspx

4.1 Архивирование данных

1. Уменьшение объема
2. Объединение файлов
3. Контроль обновления
4. Защита данных

Характеристики:

- По степени сжатия.
- По скорости сжатия.

На рынке

1. Коммерческие

ALZip • ArchiveUtility • MacBinary • PowerArchiver • Squeez • StuffIt • WinAce • WinRAR • WinZip

2. Открытые и свободные

7-Zip • Ark • File Roller • FreeArc Info-ZIP • KGB Archiver • PeaZip • The Unarchiver

4.2 Технологии работы с документами

Методы обработки текстовой информации

1. Форматирование текста
2. Редактирование текста
3. Создание списков, таблиц, колонок
4. Создание оглавлений, списков стилей
5. Добавление рисунков, комментариев
6. Автоматическая нумерация рисунков, таблиц
7. Совместное редактирование
8. Сохранение в разных форматах
9. Печать документа

Технологии обработки табличных данных

1. Создание и оформление таблиц
2. Создание и оформление диаграмм
3. Действия над ячейками
4. Использование стандартных функций
5. Сводные таблицы и диаграммы
6. Надстройки
7. Экспорт и импорт данных
8. Печать книги

1. Презентационные технологии

1. Применение шаблонов оформления
2. Создание слайда
3. Добавление рисунков, диаграмм, Smart-объектов
4. Анимация
5. Использование мультимедиа
6. Автоматический показ
7. Форматы сохранения
8. Создание заметок
9. Печать
10. Печать раздаточного материала

Тема 5. Задачи обеспечения информационной безопасности

Учебные вопросы темы

1. Понятие информационной безопасности
2. Программные способы защиты от злоумышленников

Литература к теме 5

Основная литература

1. Жданов С.А., Иванова Н.А., Маняхина В.Г., Костин А.Н., Матросов В.Л. Информатика. Серия: высшее профессиональное образование. Бакалавриат. – М.: Academia, 2012. – 336 с.
2. Алехина Г.В. и др., Основы информатики. – М.: Маркет ДС, 2009. – 472 с.

Литература к теме 5 (продолжение)

Дополнительная литература

3. Петров С.В., Кисляков П.А. Информационная Безопасность. – Цифровая книга. Ozon.ru, 2011. – 236 с.

4. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. – М.: Академия, 2012. – 336 с.

5. Сайт журнала «Хакер». http://www.xakep.ru/articles/magazine/

6. Сайт, посвященный информационной безопасности. http://www.itsec.ru/main.php

5.1 Понятие информационной безопасности

Информационная безопасность - -это

защищенность информации и вычислительной системы от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб владельцам и пользователям информации и вычислительной системы

ОСНОВНЫЕ УГРОЗЫ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УНИВЕРСИТЕТ СИНЕРГИЯ

ДОСТУПНОСТЬ	ЦЕЛОСТНОСТЬ	КОНФИДЕНЦИАЛЬНОСТЬ
• возможность за приемлемое время получить требуемую информационную услугу	• актуальность и непротиворечивость информации • защищенность от разрушения и несанкционированного изменения	• защита от несанкционированного доступа к информации

ОСНОВНЫЕ УГРОЗЫ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УНИВЕРСИТЕТ СИНЕРГИЯ

Угроза	Атака	Злоумышленник
• потенциальная возможность определенным образом нарушить информационную безопасность.	• попытка реализации угрозы	• тот, кто предпринимает попытку атаки

Угрозы доступности

1. Непреднамеренные ошибки
2. Отказ пользователей
3. Внутренний отказ информационной системы
4. Отказ поддерживающей инфраструктуры
5. Преднамеренные атаки
6. Вредоносное ПО

Угрозы целостности

1. Непреднамеренные ошибки
2. Ввод неверных данных
3. Изменение данных
4. Активное прослушивание

Угрозы конфиденциальности

1. Размещение конфиденциальных данных в незащищенной среде
2. Перехват данных
    1. Подслушивание
    2. Кража оборудования
3. Злоупотребление полномочиями

Вредоносная программа - это программа, наносящая какой-либо вред компьютеру, на котором она запускается, или другим компьютерам в сети.

Вирусы

Жизненный цикл любого компьютерного вируса:

1. Проникновение на чужой компьютер
2. Активация
3. *Поиск объектов* для заражения
4. Подготовка копий
5. Внедрение копий

Вирусы

Основная черта компьютерного вируса - это способность к саморазмножению.

Компьютерный вирус - это программа, способная создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

5.2 Программные методы защиты информации

Антивирусные программы

Антивирусные программы - это программы, основной задачей которых является защита именно от вирусов, или точнее, от вредоносных программ.

Методы и принципы защиты теоретически не имеют особого значения, главное чтобы они были направлены на борьбу с вредоносными программами. Но на практике дело обстоит несколько иначе: практически любая антивирусная *программа*объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню.

Антивирусные программы

Из всех методов антивирусной защиты можно выделить две основные группы:

Сигнатурные методы - точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов

Эвристические методы - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен

Брандмауэр

- Для обеспечения **компьютерной безопасности** нужно защитить от несанкционированного доступа все ресурсы, находящиеся внутри локальной сети:
  - аппаратные ресурсы (серверы, дисковые массивы, маршрутизаторы),
  - программные ресурсы (операционные системы, СУБД, почтовые службы и т. п.),
  - данные, хранящиеся в файлах и обрабатываемые в оперативной памяти.
- Наиболее часто используемым средством защиты этого типа является **брандмауэр,** устанавливаемый в местах всех соединений внутренней сети с Интернетом.