**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ \
ЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
«Юго-Западный государственный университет»

Кафедра «Информационная безопасность»

«ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ И СИСТЕМАХ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

для студентов бакалавров по направлениям
5523500 – «Информационная безопасность»

Курск 2007

В методических указаниях описывается: современное состояние проблемы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации в организациях и на предприятиях различных направлений деятельности.

Методические указания содержат 5 лабораторных работ, в которых содержится необходимые сведения об алгоритмах криптографической защиты информации: симметричном и ассиметричном шифровании, практические сведения о работе с программами резервирования данных и аутентификации пользователей. Каждая лабораторная работа сопровождается заданиями и вопросами для самопроверки, что способствует закреплению материала.

Лабораторная работа №1

Тема: Программирование арифметических алгоритмов

Введение

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, которая определяется степенью защищенности и устойчивости как компьютерных систем в целом, так и отдельных программ.

1. Цель работы

Исследование и разработка основных методов симметричных криптосистем.

2. Краткие сведения из теории

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифрованием, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптосистемы разделяются на ***симметричные*** и *с* ***открытым ключом***.

В ***симметричных криптосистемах*** и для шифрования, и для дешифрования используется ***один и тот же ключ***.

В ***системах с открытым ключом*** используются два ключа - ***открытый*** и ***закрытый***, которые математически связаны друг с

другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений. Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования - расшифрования. В соответствии со стандартом ГОСТ 28147-89 под **шифром** понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа, как при шифровании, так и при расшифровании сообщений. В **асимметричных** криптосистемах для зашифрования данных используется один (общедоступный) ключ, а для расшифрования – другой (секретный) ключ.

Симметричные криптосистемы.

Шифры перестановки. В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Сегодня новый день” записывается в таблицу из 4 строк и 4 столбцов по столбцам.

С	Д	О	Д
Е	Н	В	Е
Г	Я	Ы	Н
О	Н	Й	Ь

Для получения шифрованного сообщения текст считывается по строкам и группируется по 4 букв: СДОД_ЕНВЕ _ГЯЫН_ОНЙЬ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово Ваза, получим следующую таблицу

В	А	З	А					А	А	В	З
З	1	4	2					1	2	3	4
С	Д	О	Д					Д	Д	С	О
Е	Н	В	Е					Н	Е	Е	В
Г	Я	Ы	Н					Я	Н	Г	Ы
О	Н	Й	Ь					Н	Ь	О	Й

До перестановки. После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились

бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка: ДДСО_НЕЕВ_ЯНГЫ_НЬОЙ.

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок будет обратный. Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

Пример данного метода шифрования показан в следующих таблицах. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы :

	2	4	1	3			1	2	3	4			1	2	3	4
4	С	Е	Г	О		4	Г	С	О	Е		1	Я	Д	Н	Н
1	Д	Н	Я	Н		1	Я	Д	Н	Н		2	Ы	О	Й	В
2	О	В	Ы	Й		2	Ы	О	Й	В		3	Н	Д	Ь	Е
3	Д	Е	Н	Ь		3	Н	Д	Ь	Е		4	Г	С	О	Е

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка: ЯДННЫОЙВНДЬЕГСОЕ. В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы,

которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			_	Ж	А	С
4	15	14	1			Е	Г	О	П

П Р И Е З Ж А Ю _ Ш Е С Т О Г О

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 - 880; а для таблицы 5*5-250000.

3. Порядок выполнения работы

На языке DELPHI, VBA C++ или C# написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем.

Содержание отчета

1. Название работы.
2. Цель работы.
3. Блок-схему алгоритма шифрования.
4. Тексты программ.

4. Вопросы для самопроверки

1. Цель и задачи криптографии.

2. Шифры одиночной перестановки и перестановки по ключевому слову.
3. Шифры двойной перестановки. Шифрование с помощью магического квадрата.

Рекомендуемая литература

1. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1997. – 336с.
2. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001 г.
5. Масленников А. Практическая криптография BHV – СПб 2003 г.
6. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002 г.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002 г.

Дополнительно

8. ftp://ftp.kiae.su/msdos/crypto/pgp
9. http://drago.centerline.com:8080/franl/pgp/…
10. Yahoo - Computers, Security-and-Encryption

Лабораторная работа №2

Тема: Программирование алгебраических алгоритмов

Введение

Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации.

1. Цель работы

Исследование и разработка классических методов симметричных криптосистем

2. Краткие сведения из теории

Шифры простой замены. Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на K букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены. Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не

третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение СОВЕРШЕННО СЕКРЕТНО

Ключ 3143143143143143

Шифровка ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

Гаммирование

Процесс зашифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $Т(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i$=$Г(ш)_i$+$Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i$=$Г(ш)_i$+$Т(ш)_i$.

3. Порядок выполнения работы

Основные шаги шифрования текстового файла методом гаммирования.

1. Получить от пользователя ключ, имя входного и выходного файла.
2. Инициализировать генератор случайных чисел с помощью ключа. Открыть указанные файлы.
3. Прочитать строку из файла.
4. Получить случайное число.
5. Получить ASCII-код очередного символа строки и увеличить его на случайное число, полученное на шаге 4.
6. Проверить правильность (допустимый диапазон) нового ASCII-кода.
7. В выходную строку записать очередной символ, соответствующий ASCII-коду, полученному на шаге 6.

8. Если не достигли конца входной строки, то перейти к шагу 4.
9. Записать полученную строку в выходной файл.
10. Если не достигнут конец файла, то перейти к шагу 3.
11. Закрыть файлы.

Алгоритм дешифрации аналогичен алгоритму шифрации за исключением того, что из ASCII –кода вычитаем 256 и проверяем больше ноля или нет.

Open Filename For Input As # FileNumber –открытие файла для чтения.

Out Put –для вывода.

В ASCII –коде символы 10 и 13 (возврат каретки).

Надо открывать файлы как двоичные, ключевое слово Binary.

Line Input # FileNumber, A$ -переменная строковая.

Print –для записи.

Для чтения и записи двоичного файла объявляем переменную типа Variant.

Put # NF,, VA

Get # NF,, VA

Close –закрытие файла.

На языке VBA, C++ или C# написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем.

Содержание отчета

1. Название работы.
2. Цель работы.
3. Блок-схему алгоритма шифрования.
4. Тексты программ.

4. Вопросы для самопроверки

1. Шифр Гронсфельда.
2. Шифры двойной перестановки. Шифрование с помощью магического квадрата.

3. Шифр многоалфавитной замены и алгоритм его реализации.

Рекомендуемая литература

1. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1997. – 336с.
2. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001 г.
5. Масленников А. Практическая криптография BHV – СПб 2003 г.
6. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002 г.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002 г.

Лабораторная работа №3

Тема: Защита от закладок при разработке программ

1. Цель работы

Исследование и анализ служебных программ Windows XP для повышения эффективности работы компьютера.

2. Краткие сведения из теории

Брандмауэр - это система безопасности, действующая как защитный барьер между сетью и внешним миром. Брандмауэр подключения к Интернету (Internet Connection Firewall, ICF) - это программное средство, используемое для настройки ограничений,

регулирующих обмен данными между Интернетом и домашней или небольшой офисной сетью. Для настройки параметров сетевого подключения можно использовать мастер настройки сети. Открывая общий доступ к ресурсам компьютера, никогда не открывайте для доступа весь диск «С:» так как в каталоге Windows хранятся ваши пароли.

3. Порядок выполнения работы

Задание 1. Установите проверку подлинности доступа к ресурсам компьютера из локальной сети. Запретите доступ к ресурсам вашего компьютера из Интернета.

1. Для проверки подлинности доступа к ресурсам компьютера из локальной сети выполните следующие действия.

Откройте Панель управления, выбрав в Главном меню Windows команду **Пуск-Настройка-Панель управления.** Откройте двойным щелчком значок **Сетевые подключения** и в окне *Свойства сетевых подключений* выберите закладку **Проверка подлинности.** Включите флажки **Управлять сетевым доступом с помощью IEEE 802.1X, Проверять подлинность как у компьютера при доступности сведений о компьютере и Проверять подлинность как у гостя при отсутствии сведений о компьютере или пользователе.**

2. Чтобы включить брандмауэр подключения к Интернету, установите флажок, откройте закладку **Дополнительно** и включите флажок **«Защитить мое подключение к Интернету».** Щелкнув на кнопке «ОК», завершите настройку свойств сетевых подключений.

Задание 2. Разрешить удаленный доступ к ресурсам вашего компьютера.

1. Щелкнув правой кнопкой мыши на значке Мой компьютер, откройте окно *Свойства системы* па вкладке Удаленное использование. Включите флажок Разрешить

удаленный доступ к этому компьютеру и щелкните на кнопке «ОК», чтобы закрыть окно *Свойства системы.*

2. Для разрешения общего доступа к принтеру, установленному на данном компьютере из сети, выбрав в главном меню Windows команду **Настройка - Принтеры и факсы**, откройте окно *Принтеры и факсы.* Выберите в окне нужный принтер и откройте окно свойств принтера. На вкладке Доступ щелкните ссылку «Если риск безопасности известен, но требуется разрешить общий доступ к принтеру без запуска мастера, щелкните здесь». В окне *Разрешение общего доступа к принтеру* включите вариант «Разрешить общий доступ» и щелкните на кнопке «ОК». После этого в окне свойств принтера на вкладке Доступ включите флажок Общий доступ к данному принтеру, в поле *Сетевое имя* задайте имя принтера. Щелкнув на кнопке «Применить», примените внесенные в свойства принтера изменения, и закройте окно свойств принтера, щелкнув на кнопке «ОК». В окне *Принтеры и факсы* под значком принтера появится изображение ладони, указывающее на общий доступ к данному принтеру. Закройте окно *Принтеры и факсы.*

3. Для просмотра параметров доступа и безопасности диска или определенной папки укажите объект (диск или отдельную папку) и в контекстном меню выберите команду Общий доступ и безопасность. В окне *Свойства* откройте вкладку Доступ и включите флажок Открыть общий доступ к этой папке. Задайте имя, под которым данный ресурс будет виден пользователям сети. Если вы разрешаете пользователям сети изменять файлы в данной папке, включите флажок. Разрешить изменение файлов по сети.

Щелкнув на кнопке «Применить», примените внесенные в свойства папки изменения, и закройте окно свойств, щелкнув на кнопке «ОК».

Задание 3. Использование удаленного доступа к сетевым ресурсам.

1. Для подключения к сетевому диску или папке откройте окно проводника Windows и выберите в меню Сервис команду **Подключить сетевой диск.** В окне *Подключение сетевого диска* укажите букву диска и сетевую папку, к которой необходимо подключиться. Если вам не известно точное имя папки, щелкнув на кнопке «Обзор», выберите ее в окне *Обзор папок* и щелкните на кнопке «ОК». Если подключение к данной сетевой папке нужно всякий раз восстанавливать при входе в систему, включите флажок **«Восстанавливать при входе в систему».** Щелкнув на кнопке «Готово», завершите подключение к сетевому ресурсу.

2. Для подключения к сетевому принтеру выберите в Главном меню Windows команду **Настройка - Принтеры и факсы.** В окне *Принтеры и факсы* выберите в меню **Файл** команду **Установить принтер.** В окне *Мастер установки* принтеров выберите тип устанавливаемого принтера, включив флажок на варианте Сетевой принтер, подключенный к другому компьютеру. Щелкнув на кнопке «Далее», выберите вариант «Подключиться к принтеру», в поле *Имя* задайте имя принтера.

Щелкнув на кнопке «Готово», завершите подключение к сетевому принтеру.

Закройте окно *«Принтеры и факсы».*

Задание 4. Защита и восстановление данных на компьютере

1. Используя служебную программу **Архивация данных,** архивируйте данные из папки C:\Program Files\Microsoft Office\ Templates в архив с именем Templates на диске D:.

Для запуска приложения Архивация данных выберите в меню **Пуск** команды **Программы-Стандартные-Служебные-Архивация данных.** Если программа архивации запускается в режиме мастера, то для переключения в расширенный режим нажмите кнопку «Расширенный» в окне мастера архивации.

Для архивации выбранных файлов и папок на жестком диске перейдите на вкладку **Архивация** и установите флажок в списке Установите флажки для папки C:\Program Files\Microsoft Office\ Templates, данные из которой вы хотите заархивировать.

Задайте в качестве носителя диск D: и имя файла для архива Templates, нажмите на кнопку «Архивировать», а затем в окне *Сведения о задании архивации* выберите вариант **Затереть данные носителя этим архивом.**

Щелчком на кнопке «Архивировать» запустите процедуру архивации. После этого в окне *Ход архивации* пронаблюдайте за процессом архивации, по окончании которого будет выведено окно сообщения о завершении архивации с краткими сведениями. Для просмотра подробного текста отчета щелкните на кнопке «Отчет».

2. Используя служебную программу **Архивация данных,** создайте архив системных файлов и дискету аварийного восстановления, которые могут быть использованы в целях восстановления системы в случае ее отказа.

Приготовьте чистую дискету емкостью 1,44 Мбайта для сохранения параметров системы, затем запустите приложение Архивация в режиме **Расширенный. В** меню **Сервис** выберите команду **Мастер** аварийного восстановления системы. Следуйте инструкциям, появляющимся на экране. Для перехода к следующему шагу мастера щелкайте на кнопке «Далее». Выбрав тип носителя для системного архива и имя носителя для хранения архивных данных, например, D:\Arxiv\Backup.bkf, щелкните на кнопке «Далее» для создания архива. После этого будет выполнена архивация системных файлов, необходимых для загрузки системы, и создание дискеты аварийного восстановления.

По окончании процесса архивации в ответ на предложение вставить дискету вставьте чистую дискету, после этого будет создана дискета аварийного восстановления. Для

просмотра подробного отчета щелкните на кнопке «Отчет». Закройте окно программы **Архивация данных.**

4. Задание к работе

1 . Используя программу Сведения о системе, определите следующие параметры компьютерной системы: сведения об имеющихся на компьютере[x]портах, звуковом устройстве, о системных драйверах и автоматически загружаемых программах.

2.Используя стандартную программу Windows **Проверка диска,** проверьте диск А: на наличие поврежденных секторов и ошибок файловой системы. При этом если будут обнаружены ошибки, то задайте режим восстановления поврежденных секторов диска автоматического исправления системных ошибок.

3.Используя стандартную программу **Очистка диска, выполните очистку диск D:.**

4.Используя стандартную программу **Дефрагментация диска,** выполните оценку фрагментированности файлов на диске D: и, если требуется, то выполните дефрагментацию этого диска.

5.Используя служебную программу **Архивация данных,** архивируйте данные из папки C:\Program Files\Microsoft OfficeVTemplates в архив с именем Templates на диске D:.

6.Используя служебную программу **Архивация данных,** создайте архив системных файлов и дискету аварийного восстановления, которые могут быть использованы в целях восстановления системы в случае ее отказа.

5. Вопросы для самопроверки

1 . Почему при эксплуатации компьютерной системы важно знать ее параметры?

2.Какие стандартные средства Windows XP обеспечивают пользователю возможность определения параметров компьютерной системы?

3.Почему обеспечение бесперебойной работы дисковой системы компьютера является одной из основных мер

обеспечения информационной безопасности?

4.Опишите причины нарушений в работе магнитных дисков.

5.Почему необходима процедура очистки диска?

6.Что такое фрагментация файла? Почему она возникает и как влияет на скорость операций чтения информации с диска?

7.В каких случаях рекомендуется выполнить дефрагментацию диска?

8.С какой целью выполняется архивация данных компьютера?

9.Что такое дискета аварийного восстановления? Какой программой она создается?

10. Какие вы знаете программы восстановления информации на магнитных дисках?

Рекомендуемая литература

1. Гук М. Аппаратные средства IBM PC. Энциклопедия. - СПб.: Питер, 2002, - 928 с.

На страницах этой книги приведено систематизированное описание «железной» части семейства самых распространенных персональных компьютеров. Книга дает глубокие знания как по отдельным электронным подсистемам (память, процессоры, диски и т.п.), так и по их соединению в единое целое. Аппаратные средства рассматриваются во взаимодействии с программным обеспечением, что дает целостную картину функционирования компьютера.

2. Мииаси М. Модернизация и обслуживание персонального компьютера. Базовый курс. - М.; Век, 2000. - 592 с.

Лабораторная работа №4
Тема: Программирование алгоритмов криптосистем с открытом ключом

Введение

Как бы ни были сложны и надежны криптографические системы - их слабое мест при практической реализации - проблема *распределения ключей*. Для того, чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. Т.е. в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены *системы с открытым ключом.*

Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется *открытым*, а другой *закрытым*. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст в принципе не может быть расшифрован тем же открытым ключом. Дешифрование сообщение возможно только с использованием закрытого ключа, который известен только самому адресату.

1. Цель работы

Исследование и анализ основных методов ассимметричных криптосистем

2. Краткие сведения из теории

В самом определении необратимости присутствует неопределенность. Под *необратимостью* понимается не теоретическая необратимость, а практическая невозможность

вычислить обратное значение используя современные вычислительные средства за обозримый интервал времени.

Поэтому чтобы гарантировать надежную защиту информации, к системам с открытым ключом (СОК) предъявляются два важных и очевидных требования:

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.
2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

Схема шифрования Эль Гамаля. Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает два больших числа P и G, причем $P > G$.
2. Получатель выбирает секретный ключ - случайное целое число $X < P$.
3. Вычисляется открытый ключ $Y = G^x \bmod P$.
4. Получатель выбирает целое число K, $1 < K < P-1$.
5. Шифрование сообщения (M): $a = G^K \bmod P$, $b = Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA. Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Они воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Доказано (теорема [Dhatch]абина), что раскрытие шифра RSA эквивалентно такому разложению. Поэтому

для любой длины ключа можно дать нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин популярности этой СОК на фоне десятков других схем. Поэтому алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

В настоящее время алгоритм RSA используется во многих стандартах, среди которых SSL, S-HHT*P*, S-MIME, S/WAN, STT и *P*СТ.

Последовательность действий пользователя:

6. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $N=pq$; $M=(p-1)(q-1)$.
7. Получатель выбирает целое случайное число d, которое является взаимопростым со значением M, и вычисляет значение e из условия $ed=1(\text{mod } M)$.
8. d и N публикуются как открытый ключ, e и M являются закрытым ключом.
9. Если S –сообщение и его длина: $1<\text{Len}(S)<N$, то зашифровать этот текст можно как $S'=S^d(\text{mod } N)$, то есть шифруется открытым ключом.
10. Получатель расшифровывает с помощью закрытого ключа: $S=S'^e(\text{mod } N)$.

Пример Зашифруем сообщение "CAB". Для простоты будем использовать маленькие числа (на практике применяются гораздо большие).

1. Выберем $p=3$ и $q=11$.
2. Определим $n=3*11=33$.
3. Найдем $(p-1)(q-1)=20$. Следовательно, в качестве d, взаимно простое с 20, например, $d=3$.

4. Выберем число e. В качестве такого числа может быть взято любое число, для которого удовлетворяется соотношение (e*3) (mod 20) = 1, например 7.

5. Представим шифруемое сообщение как последовательность целых чисел с помощью отображения: A1, B2, C3. Тогда сообщение принимает вид (3,1,2). Зашифруем сообщение с помощью ключа {7,33}.

ШТ1 = (3^7) (mod 33) = 2187 (mod 33) = 9,

ШТ2 = (1^7) (mod 33) = 1 (mod 33) = 1,

ШТ3 = (2^7) (mod 33) = 128 (mod 33) = 29.

6. [Dhatch]асшифруем полученное зашифрованное сообщение (9,1,29) на основе закрытого ключа {3,33}:

ИТ1 = (9^3) (mod 33) = 729 (mod 33) = 3,

ИТ2= (1^3) (mod 33) = 1 (mod 33) = 1,

ИТ3 = (29^3) (mod 33) = 24389 (mod 33) = 2.

Итак, в реальных системах алгоритм RSA реализуется следующим образом: каждый пользователь выбирает два больших простых числа, и в соответствии с описанным выше алгоритмом выбирает два простых числа e и d. Как результат умножения первых двух чисел (p и q) устанавливается n.

$\{e,n\}$ образует открытый ключ, а $\{d,n\}$ - закрытый (хотя можно взять и наоборот).

Открытый ключ публикуется и доступен каждому, кто желает послать владельцу ключа сообщение, которое зашифровывается указанным алгоритмом. После шифрования, сообщение невозможно раскрыть с помощью открытого ключа. Владелец же закрытого ключа без труда может расшифровать принятое сообщение.

3. Порядок выполнения работы

Основные шаги шифрования текстового файла методом гаммирования.

1. Получить от пользователя ключ, имя входного и выходного файла.

2. Инициализировать генератор случайных чисел с помощью ключа. Открыть указанные файлы.
3. Прочитать строку из файла.
4. Получить случайное число.
5. Получить ASCII-код очередного символа строки и увеличить его на случайное число, полученное на шаге 4.
6. Проверить правильность (допустимый диапазон) нового ASCII-кода.
7. В выходную строку записать очередной символ, соответствующий ASCII-коду, полученному на шаге 6.
8. Если не достигли конца входной строки, то перейти к шагу 4.
9. Записать полученную строку в выходной файл.
10. Если не достигнут конец файла, то перейти к шагу 3.
11. Закрыть файлы.

4. Задание к работе

На языке VBA, C++ или C# написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем.

Содержание отчета

1. Название работы.
2. Цель работы.
3. Блок-схему алгоритма шифрования.
4. Тексты программ.

5. Вопросы для самопроверки

1. Алгоритм шифрации двойным квадратом. Шифр Enigma.
2. Алгоритм шифрования DES.
3. Алгоритм шифрования ГОСТ 28147-89.
4. Алгоритм шифрования RSA.
5. Алгоритм шифрования Эль Гамаля.
6. Задачи и алгоритмы электронной подписи.

7. Задачи распределения ключей.

Рекомендуемая литература

1. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1997. – 336с.
2. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001 г.
5. Масленников А. Практическая криптография BHV – СПб 2003 г.
6. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002 г.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002 г.

Дополнительно

8. ftp://ftp.kiae.su/msdos/crypto/pgp
9. http://drago.centerline.com:8080/franl/pgp/…
10. Yahoo - Computers, Security-and-Encryption

Лабораторная работа №5

Тема: Профилактика заражения вирусами компьютерных систем

1. Цель работы

Анализ и исследование антивирусных программ.

2. Краткие сведения из теории

Антивирус Касперского 7.0 это принципиальный новый подход к защите информации. Антивирус Касперского 7.0- это новое поколение решений по защите информации.

Основное отличие Антивируса Касперского 7.0 от существующих продуктов, в том числе и от продуктов компании ЗАО «Лаборатория Касперского», - это комплексный подход к защите информации на компьютере пользователя.

Антивирус Касперского 7.0 - это принципиально новый подход к защите информации. Главное в приложении - это объединение и заметное улучшение текущих функциональных возможностей всех продуктов компании в одно комплексное решение защиты. Приложение обеспечивает не только антивирусную защиту, но и защиту от неизвестных угроз.

Больше не нужно устанавливать несколько продуктов на компьютер, чтобы обеспечить себе полноценную защиту. Достаточно просто установить Антивирус Касперского 7.0.

Комплексная защита обеспечивается на всех каналах поступления и передачи информации. Гибкая настройка любого компонента приложения позволяет максимально гибко адаптировать Антивирус Касперского под нужды конкретного пользователя. Предусмотрена также единая настройка всех компонентов защиты.

Вы можете работать с Антивирусом Касперского посредством командной строки. При этом предусмотрена возможность выполнения следующих операций:

- запуск, остановка, приостановка и возобновление работы компонентов приложения;

- запуск, остановка, приостановка и возобновления выполнения задач проверки на вирусы;
- получение информации о текущем статусе компонентов и задач и их статистики;
- проверка выбранных объектов;
- обновление баз и модулей приложения;
- вызов справки по синтаксису командной строки;
- вызов справки по синтаксису команды.

Синтаксис командной строки:

avp.com <команда> [параметры]

В качестве <команд> используются:

ACTIVATE	активация приложения через интернет с помощью кода активации
ADDKEY	активация приложения с помощью файла ключа (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
START	запуск компонента или задачи
PAUSE	приостановка работы компонента или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
RESUME	возобновление работы компонента или задачи
STOP	остановка работы компонента или задачи (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
STATUS	вывод на экран текущего статуса компонента или задачи
STATISTICS	вывод на экран статистики по работе компонента или задачи
HELP	помощь по синтаксису команды, вывод списка команд
SCAN	проверка объектов на присутствие вирусов
UPDATE	запуск обновления приложения
ROLLBACK	откат последнего произведенного обновления приложения (выполнение команды возможно только с

	вводом пароля, заданного через интерфейс приложения)
EXIT	завершение работы с приложением (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
IMPORT	импорт параметров защиты Антивируса Касперского (выполнение команды возможно только с вводом пароля, заданного через интерфейс приложения)
EXPORT	экспорт параметров защиты Антивируса Касперского

Защита Антивируса Касперского строится исходя из источников угроз, то есть на каждый источник предусмотрен отдельный компонент программы, обеспечивающий его контроль и необходимые мероприятия по предотвращению вредоносного воздействия этого источника на данные пользователя. Такое построение системы защиты позволяет гибко настраивать приложение под нужны конкретного пользователя или предприятия в целом.

Антивирус Касперского включает:

- Компоненты постоянной защиты, обеспечивающие защиту вашего компьютера на всех каналах поступления и передачи информации.
- Задачи поиска вирусов, посредством которых выполняется поиск вирусов в отдельных файлах, каталогах, дисках или областях, либо полная проверка компьютера.
- Обновление, обеспечивающее актуальность внутренних модулей приложения, а также баз, использующихся для поиска вредоносных программ.
- Сервисные функции, обеспечивающие информационную поддержку в работе с приложением и позволяющие расширить его функциональность.

В состав Антивируса Касперского включен специальный компонент, обеспечивающий защиту файловой системы вашего компьютера от заражения, - Файловый Антивирус. Он запускается

при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы.

Индикатором работы компонента является значок Антивируса Касперского в области уведомлений панели задач Microsoft Windows, который принимает вид каждый раз при проверке файла.

По умолчанию Файловый Антивирус проверяет только новые или измененные файлы, то есть файлы, которые добавились или изменились со времени последнего обращения к ним. Процесс проверки файла выполняется по следующему алгоритму:

1. Обращение пользователя или некоторой программы к каждому файлу перехватывается компонентом.
2. Файловый Антивирус проверяет наличие информации о перехваченном файле в базе iChecker™ и iSwift™. На основании полученной информации принимается решение о необходимости проверки файла.

Процесс проверки включает следующие этапы:

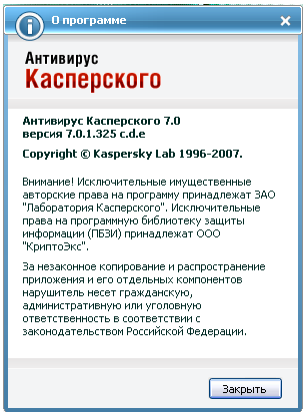
1. Файл анализируется на присутствие вирусов. Распознавание вредоносных объектов происходит на основании баз приложения. Базы содержат описание всех известных на настоящий момент вредоносных программ, угроз, сетевых атак и способов их обезвреживания.
2. В результате анализа возможны следующие варианты поведения приложения:
   a. Если в файле обнаружен вредоносный код, Файловый Антивирус блокирует файл и пытается его лечить. В результате успешного лечения файл становится доступным для работы, если же лечение произвести не удалось, файл удаляется. При выполнении лечения файла или его удалении копия файла помещается в резервное хранилище.
   b. Если в файле обнаружен код, похожий на вредоносный, но стопроцентной гарантии этого нет, файл помещается в

специальное хранилище- карантин. Позже можно попытаться вылечить его с обновленными базами.

с. Если в файле не обнаружено вредоносного кода, он сразу же становится доступным для работы.

3. Порядок выполнения работы

Задание1.1. Ознакомьтесь с энциклопедией компьютерных вирусов на сайте лаборатории Касперского в Интернете по адресу **http:// www.viruslist.com/viruslist.asp,** для чего, загрузив web-обозреватель и указав адрес энциклопедии, изучите разделы; Что такое компьютерный вирус, классификация компьютерных вирусов. Просмотрите описание одного из самых популярных вирусов недели на сайте лаборатории Касперского. В разделе «Методы обнаружения и удаления компьютерных вирусов» изучите тему Методика использования антивирусных программ.



2. Запустите Антивирус Касперского 7.0 изучите главное окно программы.

Рис. 5.1. Главное окно Антивирус Касперского 7.0

3.Одной из важных составляющих обеспечения антивирусной защиты компьютера является поиск вирусов в указанных пользователем областях. Антивирус Касперского 7.0 позволяет проверять на присутствие вирусов как отдельные объекты (файлы, папки, диски, сменные устройства), так и весь компьютер в целом. Проверка на вирусы позволяет исключить возможность распространения вредоносного кода, не обнаруженного компонентами постоянной защиты по тем или иным причинам.

В состав Антивируса Касперского 7.0 по умолчанию включены следующие задачи поиска вирусов:

Критические области

Проверка на присутствие вирусов всех критических областей компьютера. К ним относятся: системная память, объекты, исполняемые при старте системы, загрузочные сектора дисков, системные каталоги Windows и system32. Цель задачи - быстрое обнаружение в системе активных вирусов, без запуска полной проверки компьютера.

Мой Компьютер

Поиск вирусов на вашем компьютере с тщательной проверкой всех подключенных дисков, памяти, файлов.

Объекты автозапуска

Проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.

Поиск руткитов (rootkit)

Поиск на компьютере руткитов, обеспечивающих сокрытие вредоносных программ в операционной системе. Данные утилиты внедряются в систему, маскируя свое присутствие, а также наличие в системе процессов, каталогов, ключей реестра любых вредоносных программ, описанных в конфигурации руткита.

По умолчанию данные задачи выполняются с рекомендуемыми параметрами. Вы можете изменять эти параметры, а также устанавливать расписание запуска задач.

Также предусмотрена возможность создавать собственные задачи поиска вирусов и формировать расписание их запуска. Например, можно создать задачу проверки почтовых ящиков раз в неделю или задачу поиска вирусов в каталоге Мои документы.

Кроме того, вы можете проверить на вирусы любой объект (например, один из жестких дисков, на котором находятся программы и игры, почтовые базы, принесенные с работы, пришедший по почте архив и т.п.), не создавая для этого специальной задачи проверки. Выбрать объект для проверки можно из интерфейса Антивируса Касперского 7.0 или стандартными средствами операционной системы Microsoft Windows (например, в окне программы Проводник или на Рабочем столе и т.д.).

Полный список задач поиска вирусов, сформированных для вашего компьютера, можно просмотреть в разделе Поиск вирусов в левой части главного окна приложения.

Вы можете создать диск аварийного восстановления, который предназначен для восстановления системы после вирусной атаки, в результате которой повреждены системные файлы операционной системы и невозможна ее первоначальная загрузка. Для этого воспользуйтесь ссылкой Создать диск аварийного восстановления.

4.Для проверки работоспособности Файлового Антивируса;

1. Разрешите запись в отчет всех событий, для того чтобы в файле отчета сохранялись данные о поврежденных объектах или объектах, не проверенных в результате сбоя. Для этого установите флажок «Записывать» некритические события в разделе «Отчеты» и файлы данных окна настройки приложения.

2. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации, а также созданные вами модификации тестового «вируса».

Файловый Антивирус перехватит обращение к файлу, проверит его и уведомит вас об обнаружении опасного объекта:

Выбирая различные варианты действий над обнаруженным объектом, вы сможете проверить реакцию Файлового Антивируса при обнаружении объектов различных типов.

Полный результат работы Файлового Антивируса можно посмотреть в отчете по работе компонента.

5.Для проверки задачи Поиска вирусов;

1. Создайте папку на диске, скопируйте в нее тестовый «вирус», загруженный с официального сайта организации, а также созданные вами модификации тестового «вируса».

2. Создайте новую задачу поиска вирусов и в качестве объекта проверки выберите папку, содержащую набор тестовых «вирусов».

3. Разрешите запись в отчет всех событий, для того чтобы в файле отчета сохранялись данные о поврежденных объектах или объектах, не проверенных в результате сбоя. Для этого установите флажок «Записывать» некритические события в разделе «Отчеты» и файлы данных окна настройки приложения.

4. Запустите задачу поиска вирусов на выполнение.

При проверке, по мере обнаружения подозрительных или зараженных объектов, на экран будут выведены уведомления с

информацией об объекте и запросом дальнейшего действия у пользователя:

Таким образом, выбирая различные варианты действий, вы сможете проверить реакцию Антивируса Касперского при обнаружении объектов различных типов.

Полный результат выполнения задачи поиска вирусов можно посмотреть в отчете по работе компонента.

7.Для ознакомления с возможностями программы и управлением ею выберите в меню **Справка** команду **Содержание.** В окне *Справочная система: Kaspersky Anti-Virus Scanner* изучите раздел **Работа с антивирусным сканером,** темы **Интерфейс программы, Настройка параметров сканирования, Поиск и удаление вирусов, Запуск программы обновления антивирусных баз.** После изучения справочной информации закройте окно справки.

8.Для просмотра сведений о вирусах в Интерактивной вирусной энциклопедии щелкните на задаче View Online Virus Encyclopedia. После этого откроется web-страница онлайн-энциклопедии вирусов на сайте компания Symantec (http://securityresponse.Symantec.com/avcenter/virfodb.html?prodid = nav2007). На этой странице можно просмотреть, чем заражен тот или иной файл и как удалить этот вирус.

9.Для просмотра протокола работы программы щелкните на задаче View Activity log. После этого откроется протокол работы программы по трем параметрам - обнаруженные вирусные угрозы, сканирование и ошибки.

Задание 2. Изучить дополнительные возможности программы Norton AntiVirus по защите данных (восстановление ошибочно удаленных файлов и гарантированного удаления файлов и папок).

Для защиты данных Norton AntiVirus имеет UnEraze Wizard (мастер восстановления ошибочно уничтоженных файлов) и Wipe

Info (инструмент для гарантированного удаления файлов). Вызвав мастера UnEraze Wizard, достаточно указать имя (или часть) файла, его расширение и место расположения на дисках компьютера. После поиска UnEraze Wizard покажет все найденные по предложенным критериям файлы и предложит выбрать, какой из них подлежит восстановлению.

Если вам часто приходится удалять файлы, и хочется иметь гарантию невозможности их восстановления, то поможет инструмент Wipe Info. Но рекомендуется в настройках Wipe Info установить защиту от удаления системных файлов, чтобы после необдуманного действия не столкнуться с отказом операционной системы от загрузки.

1. Для восстановления ошибочно уничтоженных файлов щелкните в главном окне на «кнопке Advanced Tools». Затем в окне *Advanced Tools* выберите вариант UnErase Wizard и щелкните на кнопке «Start Tool». На следующем шаге мастера восстановления выберите вариант поиска удаленных файлов, включите флаг **Find Norton Protected Users files** (Поиск всех защищенных файлов) и щелкните на кнопке «Далее». После этого будет выполнен поиск выбранной вами категории файлов. На следующем шаге мастера восстановления, указав восстанавливаемые файлы, щелкните на кнопке «Recover» (Восстановить). Щелчком на кнопке «Далее» перейти к сообщению о результатах восстановления. Просмотрев сообщение и щелкнув на кнопке «Готово», завершите работу мастера восстановления.

2. Для гарантированного удаления файлов выберите в окне *Advanced Tools* вариант Wipe Info и щелкните на кнопке «Start Tool». На следующем шаге мастера удаления перетащите в окно *Wipe Info* файлы и папки, которые требуется гарантированно удалить. После этого щелкните на кнопке «Wipe All» (Удалить все).

4. Задание к работе

1. Используя пакет программ, демонстрирующих действие

вирусов, изучите действие вирусов различного типа. Поочередно запуская программы из пакета демонстрационных программ, изучите проявление вирусного заражения. По окончании наблюдения перезагрузить компьютер.

2.Запустите программу DrWeb и выполните проверку оперативной памяти компьютера на наличие вирусов. Выполните тестирование дисков A; и C: на наличие вирусов. Если на дисках будут обнаружены вирусы, выполните лечение зараженных файлов.

3.Загрузите из Интернета и установите на компьютере ознакомительную версию ADinf32. Задайте расписание работы ADinf, чтобы ее активизация осуществлялась еженедельно по субботам с 18.00.

4.Загрузите из Интернета и установите на компьютере ознакомительную версию антивируса Kaspersky Anti-Virus. Создайте новую задачу сканирования дисков компьютера на вирусы.

5.Загрузите из Интернета и установите на компьютере ознакомительную версию антивируса Norton AntiVirus. Выполните обновление антивирусной базы и проверьте компьютер на наличие вирусов.

6.Посетите web-страницу http://www.sarc.eom//avcenter/vinfodb. html онлайн-экспедиции вирусов на сайте компания Symantec. На этой странице можно просмотреть, чем заражен тот или иной файл и как удалить этот вирус.

5. Вопросы для самопроверки

1.Что такое компьютерный вирус? Какими свойствами обладают компьютерные вирусы?

2.По каким признакам классифицируют компьютерные вирусы? Перечислите типы вирусов.

3.Какие вирусы называются резидентными и в чем особенность таких вирусов?

4.Каковы отличия вирусов-репликаторов, стелс - вирусов, мутантов и «троянских» программ?

5.Опишите схему функционирования загрузочного вируса.

6.Опишите схему функционирования файлового вируса.

7.Опишите схему функционирования загрузочно-файловых вирусов.

8.Что такое полиморфный вирус? Почему этот тип вирусов считается наиболее опасным?

9.Каковы причины появления компьютерных вирусов. Приведите примеры широко известных вирусов.

10.Существует ли в мире и в РФ уголовная ответственность за создание и распространение компьютерных вирусов?

1 1 . Каковы пути проникновения вирусов в компьютер и признаки заражения компьютера вирусом?

12.Каковы способы обнаружения вирусов и антивирусной профилактики?

13.Перечислите основные меры по защите от компьютерных вирусов.

14.Опишите назначение антивирусных программ различных типов.

15. Назовите примеры современных антивирусных программ и опишите их особенности.

Рекомендуемая литература

1. Козлов Д.А., Парандовский А.А., Парандовский А.К. Энциклопедия компьютерных вирусов. - М.:СОЛОН-Р, 2001. - 461 с.

В энциклопедии собрана исчерпывающая информация по проблеме компьютерных вирусов, от создания до обнаружения и уничтожения. Приведены примеры написания и уничтожения COM-,EXE-,Boot-, Internet- и макровирусов, как нерезидентных, так резидентных и полиморфных. Основное преимущество данной книги в ее практическом применении.

2.http://www.avp.ru - сервер антивирусной лаборатории Евгения Касперског 6.0, на котором имеется возможность

бесплатно и быстро проверить файлы на наличие вирусного кода. В разделе «Триальные версии» вы можете познакомиться с антивирусными продуктами Лаборатории Касперского перед приобретением.

3.http://www.viruslist.com/virusHst.asp - раздел сервера антивирусной лаборатории Евгения Касперского, содержащий огромное число описаний вирусов и демонстраций вызываемых вирусами эффектов, классификацию вирусов, общие методы обнаружения и удаления компьютерных вирусов.

4.http://www.dials.ru - сервер антивирусной лаборатории «Лаборатория Данилова» и «ДиалогНаука». На данном сервере вы можете:найти информацию о программах сканер Doctor Web; резидентный сторож SpIDer Guard; ревизор дисков ADinf и универсальный лекарь ADinf Cure Module, выполнить через Интернет бесплатно удаленную проверку ваших файлов на наличие вирусов с помощью последней версии антивирусного сканера Doctor Web, а также получить некоммерческие версии антивирусных продуктов, дополнения для программы Doctor Web и документацию.

5.http://www.adinf.ru - WEB-сайт разработчиков антивируса ADinf.

***6*.http://www.symantec.ru** - Российское Интернет-представительство компании Symantec, производящей антивирусный пакет Norton Anti Virus.

ОГЛАВЛЕНИЕ

Составители: Профессор Каримов М.М.
Ассистент Иргашева Д.Я.

Формат 60x84 1/16
Гарнитура «Times New Roman», объём – 1, 125
Тираж___ Заказ №___

Подготовлено к изданию и отпечатано в издательско-полиграфическом центре «ALOQAChI» при Ташкентском университете информационных технологий, 700084, г. Ташкент, ул. Амира Темура, 108