Автономная образовательная некоммерческая организация высшего образования

«Институт менеджмента, маркетинга и финансов»

Учебное издание

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ ЗАДАНИЙ И САМОСТОЯТЕЛЬНОЙ РАБОТЕ

по дисциплине Информационная безопасность

Практические занятия (лабораторный практикум)

В авторской редакции

Шифр и наименование направления подготовки:	09.03.03 Прикладная информатика
Профиль:	Прикладная информатика в экономике
Квалификация (степень) выпускника:	бакалавр
Форма обучения:	Очная, заочная

Составитель: Степанов Л.В.

Кафедра прикладной информатики и математики

Методические указания рассмотрены и одобрены на заседании кафедры прикладной информатики и математики (протокол № 3 от 22.10.2015 г.)

2015

ББК 32.973
С 79

С 79

Степанов Л.В. Информационная безопасность. Методические указания по выполнению практических заданий и самостоятельной работы для обучающихся направления подготовки 09.03.03 Прикладная информатика профиль Прикладная информатика в экономике. Квалификация (степень) выпускника бакалавр / Л.В. Степанов. - Воронеж: АОНО ВО «Институт менеджмента, маркетинга и финансов», 2016. - 86 с.

Методические указания предназначены для подготовки и выполнения практических заданий и самостоятельной работы по дисциплине Информационная безопасность обучающимися по направлению подготовки 09.03.03 Прикладная информатика профиль Прикладная информатика в экономике. Методические указания содержат практические задания и самостоятельной работы, а также описание их выполнения.

Сведения о составителе:

Степанов Леонид Викторович - д.т.н., профессор кафедры прикладной информатики и математики АОНО ВО «Институт менеджмента, маркетинга и финансов».

ББК 32.973

Содержание

Введение

Цель: изучить основные проблемы защиты информации, ознакомиться с ее базовыми понятиями.

Тема, касающаяся защиты, включает все аспекты управления доступом к компьютерам, сетям и информации, которая хранится, обрабатывается и передается в компьютерных системах. К основным средствам защиты относятся:

Внешний контроль – классификация защиты. Классификация может основываться только на внутренних механизмах, поддерживающих три домена защиты, такие как ядро, система и пользователь, или подразделять информацию на категории “сов.секретно”, “секретно”, “для служебного пользования” и т.д. Для пользователя компьютерной системы назначаются категории информации, которую ему разрешено читать, записывать и передавать.

Шифрование. Идея шифрования заключается в преобразовании информации таким образом, чтобы ее не смогли понять неавторизованные пользователи, но можно было восстановить путем дешифрования. Метод шифрования часто используется для передачи данных по сети. Данные могут храниться в зашифрованном виде. Пароли обычно хранятся зашифрованными, а не в виде обычного текста.

Аутентификация. Процедура регистрации в системе, позволяющая идентифицировать пользователя-человека или программу как зарегистрированного пользователя, владеющего такими элементами как зашифрованные ключи для преобразования данных между зашифрованным и открытым представлениями, и проверки пароля.

Авторизация, защита или контроль доступа. Политика авторизации, определяющая кому разрешен доступ к объекту и какие операции с объектом можно выполнять.

Проверка импортированного программного обеспечения. Политика контроля доступа могут не обеспечить необходимой защиты в случае неосторожного использования непроверенного программного обеспечения. Запущенная пользователем программа получает его права доступа и может читать, переписывать и удалять его файлы. Поэтому источники программного обеспечения должны быть проверенными.

Сохранение информации. Включает вопросы резервного копирования, архивации, восстановления данных**.**

Лабораторная работа № 1 Защита от компьютерных вирусов. Антивирусная защита, антивирусной программа

Краткая теория вирусов

Вирусом называется специально созданная программа, которая способна самостоятельно распространяться в компьютерной среде. Это означает, что если вирус попал к вам в компьютер вместе с одной из программ или с документом, то через некоторое время ваши программы или документы будут "заражены" вирусом. Если к тому же компьютер подключен к локальной или глобальной сети, вирус может распространиться и на другие компьютеры.

Цель создания вирусной программы может быть самой различной, но никогда не бывает благородной. В результате распространения вирусы изменяют программы и документы, хранящиеся на дисках компьютера, что часто приводит к их утрате. Хуже всего то, что вирусы способны уничтожить вообще всю информацию, которая есть в компьютере.

Компьютерные вирусы не только распространяются, заражая новые компьютеры. Большинство из них, попав в компьютер, начинают всячески вредить пользователю. Внешние проявления вирусов могут быть разнообразными. Они ограничиваются исключительно фантазией автора вируса и возможностями компьютера.

Многие вирусы относительно безопасны для данных, хранящихся в компьютере, и по большей части действуют только на нервы пользователя. Они могут, например, осыпать символы, отображаемые на экране в текстовом режиме, выводить на экран посторонние надписи, воспроизводить посторонние звуки с помощью встроенного в компьютер динамика.

Вирус может не только уничтожить, но и немного изменить информацию, записанную на диске компьютера или изменить ее. Этот случай наиболее опасен. Если пользователь вовремя не обнаружит вирус, и вирус незаметно изменит документы или файлы баз данных, ошибка может выявится уже слишком позже в виде неправильного счета или искаженного баланса.

На сегодня автору не известны вирусы, способные безвозвратно вывести из строя аппаратуру компьютера, но в некоторых случаях они могут нанести значительный ущерб. Так, существуют вирусы, изменяющие пароль, необходимый для запуска компьютера. Этот пароль хранится в энергонезависимой памяти компьютера, питающейся от маленькой батарейки или аккумулятора. Как правило, можно временно отключить питание энергонезависимой памяти, чтобы сбросить ее содержимое. Но если такая возможность отсутствует (что иногда бывает), остается только приступить к подбору пароля или обратиться в фирму изготовитель.

В описании вирусов автор обнаружил вирус, выполняющий компрессию заражаемых файлов. Этот своего рода навязчивый аналог утилиты Diet, не спрашивая разрешения, сжимает файлы всех заражаемых приложений. Таким образом вирус увеличивает объем дисковой памяти компьютера. Не стоит обольщаться по поводу полезных вирусов и строить далеко идущие планы. Даже такие безобидные на первый взгляд вирусы таят в себе многие потенциальные опасности. Среди них возможные ошибки в коде самого вируса и несовместимость с другими программами.

В мире не существует единой классификации вирусов, однако можно выделить три группы вирусов:

- файловые вирусы;
- загрузочные вирусы;
- комбинированные файлово-загрузочные вирусы.

Кроме того, вирусы бывают макрокомандные, резидентные и нерезидентные, полиморфные и маскирующиеся (стелс-вирусы).

Файловые вирусы

Как нетрудно догадаться из названия, областью обитания файловых вирусов являются файлы. Вирусы записывают свой код в тело программного файла таким образом, что при запуске программы вирус первым получает управление. Сделав свое черное дело, вирус передает управление зараженной программе, так что пользователь ничего не замечает. При запуске вирус сканирует локальные диски компьютера и сетевые каталоги в поисках очередной жертвы. После того как подходящий программный файл будет найден, вирус записывает в него свой код.

Механизм распространения файловых вирусов достаточно прост.

Создатель вируса намеренно заражает какой-либо программный файл и записывает его на электронную доску объявлений BBS, FTP-сервер, посылает в телеконференцию или отдает приятелю. Как правило, для заражения выбирается что-нибудь интересное: новая игра, самораскрывающийся архив с привлекательным названием или новая версия популярной программы.

Получив новую игру от хорошего знакомого, даже бывалые системные администраторы и опытные программисты не всегда могут удержаться от того, чтобы сразу же ее запустить. Результат может оказаться плачевным. Следовало бы вначале проверить программу антивирусами, но такая проверка тоже не дает полной гарантии - каждый день появляются все новые и новые вирусы.

Самый простой способ гарантированно удалить вирусы с компьютера заключается в том, чтобы после форматирования диска компьютера на низком уровне установить операционную систему и прикладные программы с лицензионных дистрибутивов, и в дальнейшем избегать использования нелицензионных, бесплатных (Freeware) и условно-бесплатных (Shareware) программ.

Однако в жизни так бывает очень редко. Даже из числа тех, кто пользуется только лицензионными программами, найдется немало людей, у кого есть условно-бесплатные архиваторы, демонстрационные версии игр, бесплатные средства доступа к Internet или аналогичные средства. Свободный обмен этими программами может привести к вирусному заражению.

Но и в том случае, если вы не пользуетесь программами сомнительного происхождения, вы можете получить относительно новую разновидность файлового вируса - макрокомандный вирус, распространяющийся с документами офисных приложений, таких как Microsoft Word for Windows или Microsoft Excel for Windows.

Документы офисных приложений содержат в себе не только текст и графические изображения, но и макрокоманды, которые представляют собой ничто иное как программы. Эти программы составляются на языке, напоминающим Бейсик. Вирус может

изменять существующие макрокоманды и добавлять новые, внедряя свое тело в файл документа.

Механизм распространения макрокомандных вирусов основан на том, что существуют макрокоманды, которые запускаются при открывании документа для редактирования или при выполнении других операций. Разработчик макрокомандного вируса берет безобидный файл с именем, например, readme.doc, и записывает в него одну или несколько вирусных макрокоманд, например, вирусную макрокоманду с именем AutoExec. Когда вы открываете такой файл при помощи текстового процессора Microsoft Word for Windows, эта макрокоманда будет автоматически запущена на выполнение. При этом вирус получит управление и может заразить другие документы, хранящиеся на ваших дисках. Если вирусная макрокоманда имеет имя FileSaveAs, то распространение вируса будет происходить при сохранении документа.

Для предотвращения заражения макрокомандными вирусами вы должны перед просмотром или редактированием проверять новые файлы документов с помощью антивирусных программ, способных искать такие вирусы.

Загрузочные вирусы

Вторая большая группа вирусов - это так называемые загрузочные вирусы. Распространение и активизация этих вирусов происходит в момент загрузки операционной системы, еще до того, как пользователь успел запустить какую-либо антивирусную программу.

Для того чтобы вам был понятнее механизм распространения загрузочных вирусов, напомним, как протекает процесс начальной инициализации компьютера и загрузки операционной системы.

Сразу после включения электропитания компьютера начинает работать программа инициализации, записанная в ПЗУ базовой системы ввода/вывода BIOS. Эта программа проверяет оперативную память и другие устройства компьютера, а затем передает управление программе начальной загрузки, которая также находится в BIOS.

Программа начальной загрузки пытается прочитать в оперативную память содержимое самого первого сектора нулевой дорожки жесткого диска, в котором находится главная загрузочная запись Master Boot Record (MBR), либо содержимое самого первого сектора нулевой дорожки дискеты, вставленной в устройство A:. Этот сектор содержит загрузочную запись Boot Record (BR).

Выбор способов начальной загрузки зависит от многих факторов. Если компьютер не оборудован жестким диском, то программа начальной загрузки попытается прочитать загрузочную запись с дискеты. Но такая попытка будет предпринята только в том случае, если в таблице конфигурации компьютера указано, что накопитель на флоппи-диске присутствует. Напомним, что таблица конфигурации компьютера хранится в энергонезависимой памяти и может изменяться при помощи программы BIOS Setup.

Если в компьютере имеется жесткий диск и он правильно описан в таблице конфигурации компьютера, последовательность загрузки зависит от выбора, сделанного при помощи все той же программы BIOS Setup. Пользователь может указать, что компьютер должен загружаться либо только с жесткого диска, либо с дискеты, вставленной в устройство A:, а если такой дискеты нет, то с жесткого диска. Возможны и другие случаи, здесь все зависит от конкретной реализации BIOS.

Итак, существуют две возможности загрузить операционную систему - с жесткого диска или с дискеты. Рассмотрим вначале первую возможность.

При загрузке с жесткого диска в память по фиксированному адресу читается содержимое главной загрузочной записи. Эта запись представляет собой программу, задачей которой является загрузка операционной системы с логического диска. Как эта загрузка выполняется?

Загрузчик, расположенный в главной загрузочной записи MBR просматривает таблицу разделов диска Partition Table, которая находится в том же секторе диска, что и сама запись MBR. После того как в этой таблице будет найден раздел, отмеченный как активный, выполняется чтение самого первого сектора этого раздела в оперативную память, - сектора загрузочной записи BR. В этом секторе находится еще один (!) загрузчик, на этот раз последний.

Задачей загрузчика BR является считывание в оперативную память стартовых модулей операционной системы и передача им управления. Способ загрузки, очевидно, зависит от операционной системы, поэтому каждая операционная система имеет свой собственный загрузчик BR.

Теперь о загрузке с дискеты.

Этот процесс намного проще, так как формат дискеты в точности соответствует формату логического диска. Самый первый сектор нулевой дорожки дискеты содержит загрузочную запись BR, которая читается в память. После чтения ей передается управление.

Заметим, что дискеты могут быть системными и несистемными.

Известно, что системную дискету MS-DOS можно подготовить при помощи команды format, указав ей параметр /s, либо при помощи команды sys. И в том, и в другом случае в первый сектор нулевой дорожки дискеты записывается программа начальной загрузки MS-DOS.

Если же дискета была отформатирована командой format без параметра /s, она будет несистемной. Тем не менее, в первый сектор нулевой дорожки дискеты все равно записывается программа, единственным назначением которой является вывод сообщения о необходимости вставить в НГМД системную дискету.

Данное обстоятельство - присутствие загрузочной записи на несистемной дискете - играет важную роль при распространении загрузочных вирусов, поэтому мы советуем обратить на него внимание.

Из сказанного выше следует, что загрузка операционной системы является многоступенчатым процессом, ход которого зависит от разных обстоятельств. Для нас сейчас важно то, что в этом процессе задействовано три программы, которые служат объектом нападения загрузочных вирусов:

- главная загрузочная запись;
- загрузочная запись на логическом диске;
- загрузочная запись на дискете

Вирусы могут заменять некоторые или все перечисленные выше объекты, встраивая в них свое тело и сохраняя содержимое оригинального загрузочного сектора в каком-либо более или менее подходящем для этого месте на диске компьютера. В результате при включении компьютера программа загрузки, расположенная в BIOS, загружает в память вирусный код и передает ему управление. Дальнейшая загрузка операционной системы происходит под контролем вируса, что затрудняет, а в некоторых случаях и исключает его обнаружение антивирусными программами.

Как распространяются загрузочные вирусы? Главным образом, с помощью забывчивых пользователей.

Разработчик вируса создает дискету с зараженным загрузочным сектором или заражает главную загрузочную запись на жестком диске компьютера, к которому имеет доступ много пользователей. После загрузки операционной системы вирус контролирует все обращения к дискетам. Как только пользователь вставит дискету, не защищенную от записи, вирус запишет свое тело в загрузочный сектор дискеты. Через некоторое время все дискеты, которые когда-либо вставлялись в компьютер, окажутся зараженными.

Вставив зараженную дискету в устройство A: ранее незараженного компьютера и поработав с ней, многие пользователи забывают извлечь ее оттуда. Пользователь выключает компьютер и уходит домой спать, а вирус ждет своего часа. Включив утром компьютер, пользователь выполняет загрузку с забытой дискеты, в результате чего вирус проникает в главную загрузочную запись. Все, цель достигнута - вирус завоевал еще один компьютер.

Вы можете полностью перекрыть доступ к вашему компьютеру для загрузочных вирусов, отключив при помощи программы BIOS Setup возможность загрузки с устройства A:. Хотя иногда (например, при переустановке операционной системы) вам все же придется загружать компьютер с дискет.

Разумеется, не следует снимать с дискет защиту от записи без крайней на то необходимости. Особенно это относится к дистрибутивным дискетам, с которых выполняется установка программного обеспечения.

И конечно, все дискеты, полученные вами, следует проверять антивирусными программами. Это относится даже к новым форматированным дискетам в запечатанной коробке, так как вирус может находится в области загрузочной записи. Известен случай, когда в продажу поступили зараженные форматированные дискеты.

Комбинированные файлово-загрузочные вирусы

Наиболее совершенные и наиболее опасные вирусы используют методы распространения, характерные и для файловых, и для загрузочных вирусов. Такие вирусы записывают свое тело в файлы и в загрузочные записи дискет и дисков. Вы можете получить такой вирус, загрузив компьютер с зараженной дискеты, либо запустив зараженный файл. Результат будет одинаковый - вирус поселится в вашем компьютере и начнет свою "работу".

Простые и полиморфные вирусы

Обычные компьютерные вирусы обнаружить достаточно легко, так как в процессе заражения они записывают в заражаемый файл или системную область диска свой собственный код. Автору антивирусной программы достаточно выделить из этого кода

уникальную последовательность команд или байт, характерную именно для данного вируса. Такая последовательность носит название сигнатуры.

Затем антивирусная программа уже в автоматическом режиме просматривает все файлы и системные области дисков в поиске сигнатур известных вирусов. Естественно, что проблем с обнаружением таких вирусов нет.

Очень скоро авторы вирусов догадались использовать в своих вирусах алгоритмы шифрования, затрудняющие их обнаружение и выделение сигнатуры. Такие вирусы, получившие название шифрующихся, при заражении новых файлов и системных областей диска шифруют собственный код, пользуясь для этого случайными паролями (ключами). Когда вирус получает управление, он первым делом расшифровывает собственный код.

Сложность обнаружения таких вирусов состоит в том, что код вируса случайным образом изменяется при каждом новом заражении и, соответственно, автору антивируса сложнее выделить сигнатуру такого вируса. Однако, так как шифрующийся вирус все же должен содержать неизменную процедуру расшифровки, то сигнатуру получить можно. Даже простые антивирусные программы способны успешно обнаруживать и удалять вирусы, применяющие алгоритм шифровки.

Вслед за шифрующимися вирусами появилась еще более сложная разновидность вирусов, получившая страшное название вирусов-мутантов. Более научное название вирусов-мутантов - полиморфные вирусы. От шифрующихся вирусов они отличаются тем, что даже процедура расшифровки меняется у разных особей одного вируса. Каждый раз когда вирус заражает новый файл или системную область диска, он полностью изменяется, поэтому из полиморфных вирусов невозможно выделить сигнатуру.

Многие антивирусные программы не в состоянии обнаружить полиморфные вирусы. Например, самая известная антивирусная программа Aidstest, которая уже много лет защищает компьютеры, обнаруживает только самые примитивные экземпляры полиморфных вирусов. Автор видел много пользователей, постоянно проверяющих свои компьютеры программой Aidstest даже не смотря на предупреждение о необходимости дополнительно использовать антивирус Doctor Web. Полиморфные вирусы остаются в этом случае незамеченными и спокойно делают свое черное дело.

Извечная борьба щита и меча, брони и снаряда нашла свое отражение и в мире компьютеров. Для охоты за полиморфными вирусами были разработаны антивирусные программы нового поколения, далеко ушедшие от своих предшественников.

В качестве примеров программ, способных обнаруживать и удалять полиморфные вирусы, можно привести антивирус Doctor Web Игоря Данилова и Antiviral Toolkit Pro Евгения Касперского. Эвристический анализатор Doctor Web "выполняет" под своим управлением проверяемые программы и обнаруживает действия, характерные для вирусов. Благодаря этому он находит полиморфные вирусы также легко как и обычные вирусы, не использующие механизма маскировки.

Эвристический анализатор может обнаружить не только вирусы, ранее изученные автором антивирусной программы. Он может отыскать даже те вирусы, которые ранее не были известны. Надо сказать, что это не должно вызывать энтузиазм у авторов вирусов. Многие из них, еще не родившись, уже имеют все шансы быть обнаруженными.

Стелс-вирусы

В ходе проверки компьютера антивирусные программы считывают данные - файлы и системные области с жестких дисков и дискет, пользуясь средствами операционной системы и базовой системы ввода/вывода BIOS. Ряд вирусов, после запуска оставляют в оперативной памяти компьютера специальные модули, перехватывающие обращение программ к дисковой подсистеме компьютера. Если такой модуль обнаруживает, что программа пытается прочитать зараженный файл или системную область диска, он на ходу подменяет читаемые данные, как будто вируса на диске нет.

Стелс-вирусы обманывают антивирусные программы и в результате остаются незамеченными. Тем не менее, существует простой способ отключить механизм маскировки стелс-вирусов. Достаточно загрузить компьютер с не зараженной системной дискеты и сразу, не запуская других программ с диска компьютера (которые также могут оказаться зараженными), проверить компьютер антивирусной программой.

При загрузке с системной дискеты вирус не может получить управление и установить в оперативной памяти резидентный модуль, реализующий стелс-механизм. Антивирусная программа сможет прочитать информацию, действительно записанную на диске и легко обнаружит вирус.

Большинство антивирусных программ противодействуют попыткам стелс-вирусов остаться незамеченными, но чтобы не оставить им ни единого шанса, следует перед проверкой компьютера программами Antiviral Toolkit Pro, Aidstest и Doctor Web загружать компьютер с дискеты.

Системная дискета для антивирусного контроля должна быть подготовлена заранее. Кроме системных файлов, на нее следует записать антивирусные программы.

Многие антивирусные программы настолько успешно противостоят стелс-вирусам, что обнаруживают их при попытке замаскироваться. Такие программы считывают проверяемые программы с диска, пользуясь для этого различными методами. Например, с помощью операционной системы и базовой системы ввода/вывода. Если в полученных данных обнаруживается несоответствие, вероятнее всего в оперативной памяти находится стелс- вирус.

Антивирусные программы

В настоящее время существует огромное количество разнообразных антивирусных средств защиты. Их значительно больше, чем сортов зубной пасты, рекламируемой по телевизору. Такое разнообразие остро ставит вопрос выбора. Что лучше: пакет Antiviral Toolkit Pro доктора Касперского или комплект АО "ДиалогНаука"? А может лучше приобрести Norton Antivirus или что либо другое? Вряд ли кто-нибудь сможет дать вам однозначный ответ на этот вопрос.

Очень хороший результат могло бы дать одновременное использование нескольких антивирусных средств, но в этом случае резко возрастут затраты времени на проверку компьютера. Поэтому так или иначе, но выбор должен быть сделан. Чтобы выбор антивирусного средства не стал попыткой вытянуть счастливый билет на экзамене у строгого экзаменатора, лучше заранее узнать о методах, используемых антивирусными программами.

Отечественное антивирусное программное обеспечение успешно конкурирует с программным обеспечением, предлагаемым зарубежными фирмами. Хорошая поддержка пользователей отечественных антивирусных программ со стороны фирм - разработчиков антивирусов позволяет своевременно получать новые версии антивирусов, а также консультации по их использованию.

Существует несколько основополагающих методов поиска вирусов, которые применяются антивирусными программами:

- Сканирование
- Эвристический анализ
- Обнаружение изменений
- Резидентные мониторы

Антивирусные программы могут реализовывать все перечисленные выше методики, либо только некоторые из них.

Сканирование

Сканирование является наиболее традиционным методом поиска вирусов. Оно заключается в поиске сигнатур, выделенных из ранее обнаруженных вирусов. Антивирусные программы-сканеры, способные удалить обнаруженные вирусы, обычно называются полифагами.

Недостатком простых сканеров является их неспособность обнаружить полиморфные вирусы, полностью меняющие свой код. Для этого необходимо использовать более сложные алгоритмы поиска, включающие эвристический анализ проверяемых программ.

Кроме того, сканеры могут обнаружить только уже известные и предварительно изученные вирусы, для которых была определена сигнатура. Поэтому программы-сканеры не защитят ваш компьютер от проникновения новых вирусов, которых, кстати, появляется по несколько штук в день. Как результат, сканеры устаревают уже в момент выхода новой версии.

Эвристический анализ

Эвристический анализ зачастую используется совместно со сканированием для поиска шифрующихся и полиморфных вирусов. В большинстве случаев эвристический анализ позволяет также обнаруживать и ранее неизвестные вирусы. В этом случае скорее всего их лечение будет невозможно.

Если эвристический анализатор сообщает, что файл или загрузочный сектор возможно заражен вирусом, вы должны отнестись к этому с большим вниманием. Необходимо дополнительно проверить такие файлы с помощью самых последних версий антивирусных программ сканеров или передать их для исследования авторам антивирусных программ.

Обнаружение изменений

Заражая компьютер, вирус делает изменения на жестком диске: дописывает свой код в заражаемый файл, изменяет системные области диска и т. д. На обнаружении таких изменений основываются работа антивирусных программ-ревизоров.

Антивирусные программы-ревизоры запоминают характеристики всех областей диска, которые могут подвергнутся нападению вируса, а затем периодически проверяют их. В случае обнаружения изменений, выдается сообщение о том, что возможно на компьютер напал вирус.

Следует учитывать, что не все изменения вызваны вторжением вирусов. Так, загрузочная запись может изменится при обновлении версии операционной системы, а некоторые программы записывают внутри своего выполнимого файла данные.

Резидентные мониторы

Антивирусные программы, постоянно находящиеся в оперативной памяти компьютера и отслеживающие все подозрительные действия, выполняемые другими программами, носят название резидентных мониторов или сторожей. К сожалению, резидентные мониторы имеют очень много недостатков, которые делают этот класс программ малопригодными для использования. Они раздражают пользователей большим количеством сообщений, по большей части не имеющим отношения к вирусному заражению, в результате чего их отключают.

Лучшая защита - это нападение

Чем раньше вы начнете готовиться к нападению вирусов, тем лучше. Автор встречал немало пользователей, до поры до времени беспечно относящихся к этой проблеме. Многие из них даже не воспринимали компьютерные вирусы в качестве серьезной угрозы.

Только когда вирус уже уничтожит изрядное количество информации, они готовы отдать любые деньги, лишь бы удалить заразу и вернуть бесценную информацию.

Вы сохраните себе нервы и, возможно, деньги, если заранее проведете ряд мероприятий антивирусной защиты. Они зависят от антивирусных средств, которые вы применяете для защиты компьютера. Но, тем не менее, некоторые действия практически не зависят от вашего выбора и будут полезны в любом случае.

Одним из первых шагов, которые вы должны предпринять, является подготовка системной дискеты. Особенно подчеркнем, что системную дискету надо готовить заранее, до того как вирус появится в вашем компьютере.

На системную дискету надо записать последние версии антивирусных программ-полифагов, таких как Aidstest, Doctor Web или Antiviral Toolkit Pro. Кроме антивирусных программ, на дискету полезно записать драйверы внешних устройств компьютера, например драйвер устройства чтения компакт-дисков, программы для форматирования дисков - format и переноса операционной системы - sys, программу для ремонта файловой системы Norton Disk Doctor или ScanDisk.

Системная дискета будет полезна не только в случае нападения вирусов. Вы можете ей воспользоваться для загрузки компьютера в случае повреждения файлов операционной системы.

Периодически проверяйте компьютер на заражение вирусами. Лучше всего встроить вызов антивирусной программы в файл конфигурации autoexec.bat, чтобы проверка осуществлялась при каждом включении компьютера. Выполняйте проверку не только выполнимых файлов, имеющих расширение COM, EXE, но также пакетных файлов BAT и системных областей дисков.

Если в компьютере записано много файлов, их проверка антивирусами-полифагами скорее всего будет отнимать достаточно много времени. Поэтому во многих случаях предпочтительней для повседневной проверки использовать программы-ревизоры, а новые и изменившиеся файлы подвергать проверке полифагами.

Практически все ревизоры в случае изменения системных областей диска (главной загрузочной записи и загрузочной записи) позволяют восстановить их, даже в том случае если не известно, какой именно вирус их заразил. Лечащий модуль ADinf Cure Module даже позволяет удалять неизвестные файловые вирусы.

Не спешите воспользоваться этой возможностью. Во-первых, изменение файла и системных областей может быть вызвано не внедрением в них вируса, а гораздо более прозаическими причинами. А во-вторых, некоторые вирусы, например тот же OneHalf, так внедряются в компьютер, что простое их удаление может вызвать безвозвратную потерю информации. В любом случае перед удалением вируса с помощью ревизора следует попробовать удалить вирус программами-полифагами. Более подробные рекомендации вы можете получить только из документации на используемые вами антивирусные средства защиты. Еще лучше посоветуйтесь со специалистом по компьютерной технике или обратитесь в фирму, которая занимается антивирусным обслуживанием.

Практически все современные антивирусы могут правильно работать даже на зараженном компьютере, когда в его оперативной памяти находится активный вирус. Однако перед удалением вируса все же рекомендуется предварительно загрузить компьютер с системной дискеты, чтобы вирус не смог препятствовать лечению.

Когда вы загружаете компьютер с системной дискеты, следует обратить внимание на два важных момента.

Во-первых, для перезагрузки компьютера надо использовать кнопку Reset, расположенную на корпусе системного блока, или даже временно выключить его питание. Не используйте для перезагрузки комбинацию из трех известных клавиш. Некоторые вирусы могут остаться в памяти даже после этой процедуры.

Во-вторых, перед перезагрузкой компьютера с дискеты проверьте конфигурацию дисковой подсистемы компьютера и особенно параметры дисководов и порядок загрузки операционной системы (должна быть установлена приоритетная загрузка с дискеты), записанную в энергонезависимой памяти. Существуют вирусы, ловко меняющие параметры, записанные в энергонезависимой памяти компьютера, в результате чего компьютер загружается с зараженного вирусом жесткого диска в то время как вы думаете, что загрузка происходит с чистой системной дискеты.

Обязательно проверяйте с помощью антивирусных программ все дискеты и все программы, поступающие к вам от ваших знакомых или через модем. Если компьютер подключен к локальной сети, проверяйте файлы, полученные через сеть от других пользователей.

С появлением вирусов, распространяющихся через макрокоманды текстового процессора Microsoft Word и электронной таблицы Microsoft Excel, вы должны быть особенно внимательны и проверять не только выполнимые файлы программ и системные области дисков, но также и файлы документов. Убедитесь, что ваше антивирусное обеспечение способно обнаруживать такие вирусы.

Следите за выходом новых версий применяемых вами антивирусных средств и своевременно выполняйте их обновления на системной дискете и своем компьютере. Используйте для восстановления зараженных файлов и системных областей диска только самые последние версии антивирусов.

Лабораторные задания:

1. Изучить настройки антивирусной программы

2. Провести тестирование системных областей жесткого диска и нескольких подкаталогов

3. Проверить дискету на наличие вирусов

Лабораторная работа №2 Профилактика заражения вирусами компьютерных систем

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.

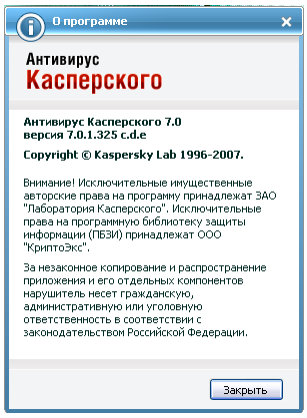
b. Если в файле обнаружен код, похожий на вредоносный, но стопроцентной гарантии этого нет, файл помещается в специальное хранилище- карантин. Позже можно попытаться вылечить его с обновленными базами.

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

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.

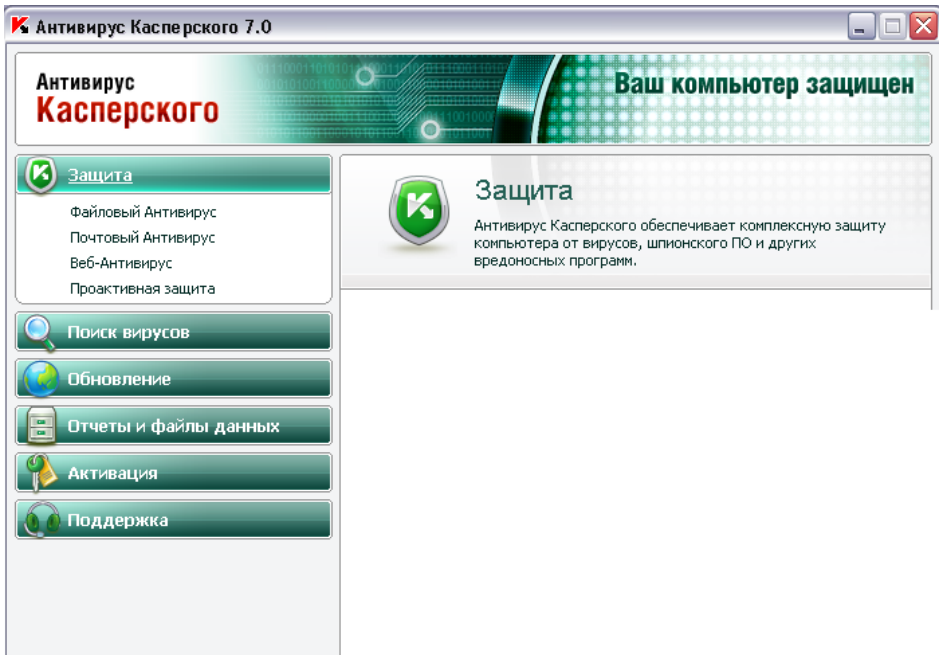


Рис. 5.1. Главное окно Антивирус Касперского 7.0

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).

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.

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?

11. 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.

Лабораторная работа № 3 Защита документа в Microsoft Word

При работе в Microsoft Word существует несколько возможностей ограничения изменений в документе:

назначение пароля[1] для открытия документа;

назначение пароля разрешения записи;

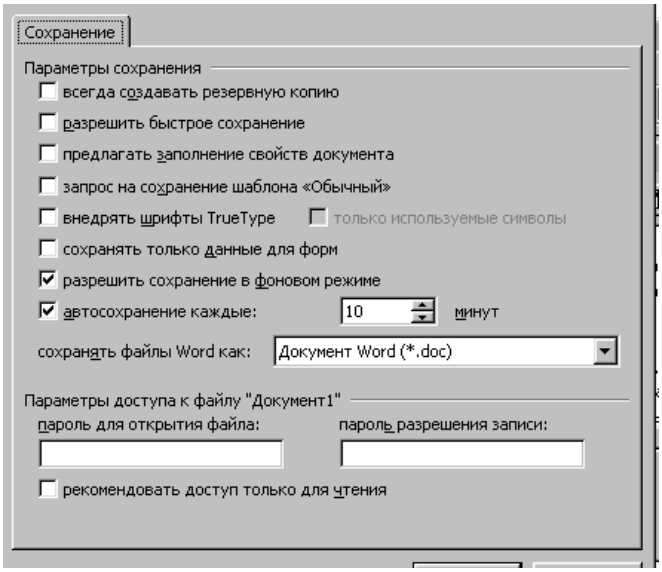
рекомендация доступа только для чтения;

подготовка документа к проверке;

защита полей электронной формы от изменения;

назначение пароля разрешения записи;

назначить документу пароль, предотвращающий открытие документа пользователем, не имеющим соответствующих полномочий.



Если открыть документ как файл, предназначенный только для чтения, и внести в него изменения, сохранить этот файл можно только под другим именем.

Если после присвоения пароля он будет забыт, невозможно будет ни открыть документ, ни снять с него защиту, ни восстановить данные из него. Поэтому следует составить список паролей и соответствующих им документов и хранить его в надежном месте.

Назначение пароля для открытия документа

1 Откройте документ.

2 Выберите команду **Сохранить как** в меню **Файл**.

[1] Предотвращает несанкционированный доступ к защищенному элементу или документу. Пароль может состоять из любого сочетания букв, цифр, пробелов и символов. Длина пароля не должна превышать 15 символов. При вводе пароля вместо вводимых символов отображаются звездочки (*). Пароль водится с учетом регистра.

3 Нажмите кнопку **Параметры**.

4 В поле **Пароль для открытия файла** введите пароль, а затем нажмите кнопку **OK**.

5 Затем введите тот же пароль еще раз и нажмите кнопку **OK**.

6 Нажмите кнопку **Сохранить**

Назначение пароля разрешения записи

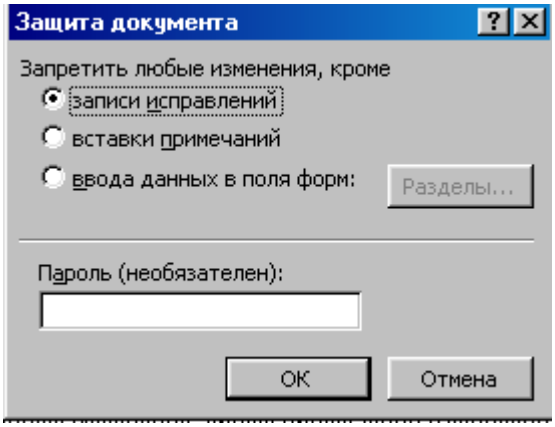
1 Откройте документ.

2 Выберите команду **Сохранить как** в меню **Файл**.

3 Нажмите кнопку **Параметры**.

4 В поле **Пароль разрешения записи** введите пароль, а затем нажмите кнопку **OK**.

5 Затем введите тот же пароль еще раз и нажмите кнопку **OK**.



6 Нажмите кнопку **Сохранить**.

Рекомендация доступа только для чтения

1 Откройте документ.

2 Выберите команду **Сохранить как** в меню **Файл**.

3 Нажмите кнопку **Параметры**.

4 Установите флажок **Рекомендовать доступ только для чтения** и нажмите кнопку **OK**.

5 Нажмите кнопку **Сохранить**

При рассылке документа для проверки можно запретить другим пользователям вносить любые изменения, кроме примечаний и записанных исправлений. Выберите команду **Установить защиту** в меню **Сервис**, а затем — параметр Записи исправлений. Чтобы разрешить только вставку примечаний, выберите параметр Вставки примечаний.

Как убедиться, что документ не содержит скрытых данных?

Порой требуется скрыть часть данных, содержащихся в документе, например, записанные исправления, примечания и скрытый текст. Перед тем как предоставить другим лицам копию документа, целесообразно просмотреть скрытые данные и решить, что из них следует оставить их в документе. Например, может потребоваться временно скрыть часть данных при печати документа или удалить все скрытые данные из документа перед его распространением средствами электронной почты.

Чтобы просмотреть записанные исправления, выберите команду **Исправления** в меню **Сервис**, выберите команду **Выделить исправления**, а затем установите флажок **Отображать исправления на экране**. Для получения сведений о принятии или отмене записанных исправлений в документе перед его распространением достаточно выполнить удаление примечания, для этого:

1 Выберите примечание, которое требуется удалить.

2 Нажмите кнопку **Удалить примечание** на панели инструментов **Рецензирование**.

Оставшиеся примечания будут автоматически перенумерованы.

·Для получения сведений о просмотре примечаний Word выводит примечание и имя рецензента, который его внес, в виде всплывающей подсказки над текстом. Если примечания не появляются, выберите команду **Параметры** в меню **Сервис**, а затем установите флажок **Всплывающие подсказки** на вкладке **Вид**.

Чтобы напечатать в документе только примечания Выберите команду **Печать** в меню **Файл**, а затем выберите **Примечания** из списка **Напечатать**.

. Чтобы напечатать документы без примечаний, выберите команду **Параметры** в меню **Сервис**, а затем снимите флажок **Примечания** в группе Печатать на вкладке **Печать**.

·Чтобы увидеть скрытый текст, выберите команду **Параметры** в меню **Сервис**, а затем установите флажок **Скрытый текст** в группе Непечатаемые символы на вкладке **Вид**. Чтобы не печатать скрытый текст при печати документа, выберите команду **Параметры** в меню **Серви**с, а затем снимите флажок **Скрытый текст** в группе **Печатать** на вкладке **Печать**. Перед распространением документа удалите скрытый текст так же, как и любой другой текст.

Если удаленные данные все еще содержатся

Если открыть документ, сохраненный в режиме быстрого сохранения, как текстовый файл, в нем можно найти ранее удаленные данные. Это происходит потому, что при быстром сохранении вносимые изменения (в том числе удаление данных) дописываются в конец документа, не отражаясь в самом документе.

Для окончательного удаления удаленных данных закройте текстовый файл и откройте документ как обычный документ Word. Выберите команду **Сохранить** как в меню **Файл**, а

затем нажмите кнопку **Сохранить**. Чтобы вообще отключить быстрое сохранение, выберите команду **Параметры** в меню **Сервис**, а затем снимите флажок **Разрешить быстрое сохранение** на вкладке **Сохранение**.

Для того, чтобы предотвратить просмотр версий распространяемого документа достаточно выполнить следующее:

Если нужно сохранить предыдущие версии, сохраните текущую версию как отдельный документ.

Если не требуется сохранение предыдущих версий, удалите ненужные версии, а затем сохраните оставшийся документ.

Сохранение данных и восстановление утерянных документов

Защитить себя от возможной потери результатов труда из-за сбоя в программе или отключения электричества можно с помощью автосохранения. Оно обеспечивает периодическое сохранение копий документа в процессе работы над ним или сохранение резервной копии документа при каждом сохранении конечного варианта. Чтобы иметь возможность восстановить введенные данные после падения напряжения или сбоя в программе, необходимо заранее установить флажки Автосохранение каждые ... минут и/или Всегда сохранять резервную копию на вкладке **Сохранение** диалогового окна **Параметры** (меню **Сервис**). Если необходимо, можно установить интервал для автоматического сохранения, меньший 10 минут.

Чтобы иметь возможность восстановить данные после случайного удаления или повреждения документа, необходимо заранее установить флажок **Всегда сохранять резервную копию**.

Кроме того, это позволит открыть и восстановить текст случайно поврежденного документа.

Изменение интервала автоматического сохранения документов

1 В меню **Серви**с выберите команду **Параметры**, а затем — вкладку **Сохранение**.

2 Установите флажок **Автосохранение** каждые ... минут.

3 В поле минут укажите интервал сохранения документа Word. Чем чаще производится сохранение документа, тем большую часть его удастся восстановить в случае, если при работе в Word произойдет сбой в программе или падение напряжения в сети.

4 После завершения работы с документом нажмите кнопку **Сохранить**.

Примечание. Если установлен флажок Автосохранение каждые ... минут, внесенные в документ изменения сохраняются во временный файл. Использование автосохранения

не избавляет от необходимости сохранять открытый документ обычным способом; временные файлы удаляются при закрытии или сохранении документа. В случае падения напряжения или после перезагрузки компьютера, если файл не был закрыт или сохранен, временные файлы сохраняются. При повторном запуске Word автоматически открываются все временные файлы, и их можно сохранить. Если временный файл не сохранить, он удаляется.

Восстановление документа, сохраненного автоматически

1 Запустите Word.

Все документы, открытые в момент падения напряжения или другой аварии, откроются автоматически. Будут утеряны только изменения, внесенные после последнего автосохранения документов.

2 Чтобы проверить наличие необходимого текста во временном файле до того, как заменить им имеющийся документ, откройте документ и просмотрите его.

3 В меню **Файл** выберите команду **Сохранить**.

4 В поле **Имя файла** введите новое имя или выберите имя имеющегося документа.

5 Нажмите кнопку **Сохранить**.

6 Если появится предложение подтвердить замену существующего документа новым (включающим последние изменения, внесенные в документ), нажмите кнопку **Да**.

7 Повторите шаги 2 — 6 для каждого восстановленного документа.

Все восстановленные документы, которые не были сохранены, будут удалены при закрытии Word.

Примечание. Если восстановленный документ не удается сохранить, его можно будет открыть. Для получения дополнительных сведений нажмите кнопку.

Сохранение резервной копии документа

1 Выберите команду **Сохранить как** в меню **Файл**.

2 Нажмите кнопку **Параметры**.

3 Установите флажок **Всегда создавать резервную копию**.

4 Нажмите кнопку **OK**.

5 Нажмите кнопку **Сохранить**.

Примечание. Для получения сведений об открытии резервной копии документа нажмите кнопку .

Открытие резервной копии документа

Чтобы иметь возможность восстановить предыдущую версию документа после внезапного падения напряжения или другой аналогичной аварии, необходимо заранее установить флажок **Всегда создавать резервную копию** на вкладке **Сохранение** в диалоговом окне **Параметры** (меню **Сервис**). Кроме того, перед этим документ должен быть сохранен хотя бы один раз.

1 Нажмите кнопку **Открыть** .

2 В поле **Тип файла** выберите параметр **Все файлы**.

3 Открывайте двойным щелчком папки из списка папок, пока в одной из них не обнаружится нужная резервная копия.

4 Нажмите кнопку **Таблица**.

В столбце Имя резервная копия будет обозначена как «Копия Имя документа»; в столбце Тип будет указан тип резервной копии: «Копия документа Microsoft Word».

5 Выделите и щелкните дважды резервную копию.

Восстановление текста поврежденного документа

Если при попытке открыть документ компьютер перестает отвечать на запросы пользователя, документ может быть поврежден. При следующем запуске Word автоматически запустится специальная программа преобразования файлов, восстанавливающая текст поврежденного документа. Эту программу преобразования в любой момент можно запустить вручную, как описано ниже.

1 В меню **Сервис** выберите команду **Параметры**, а затем — вкладку **Общие**.

2 Убедитесь, что флажок **Подтверждать преобразование при открытии** установлен, и нажмите кнопку **OK**.

3 Нажмите кнопку **Открыть**.

4 В поле **Тип файла** выберите параметр **Файл автосохранения**.

5 Откройте документ обычным способом.

Примечание. Если параметр **Файл автосохранения** отсутствует в списке **Тип файла**, необходимо установить программу преобразования.

Лабораторные задания:

Сформировать пароль в документе , руководствуясь правилами, описанными в работе.

Лабораторная работа № 4 Защита в Microsoft Excel

Microsoft Excel обладает следующими возможностями защиты:

Ограничение доступа к отдельным листам.

Ограничение возможности изменений для всей книги.

Ограничение совместного доступа к книге и ограничение доступа к списку изменений.

Ограничение доступа к книге с помощью пароля, запрашиваемого при открытии или сохранении книги, либо установка при открытии книги посторонними режима только для чтения.

Возможность проверки макросов на наличие вирусов при открытии книги

Управление доступом к книгам и листам

Имеется возможность защитить данные в книге с помощью пароля, необходимого для открытия или сохранения книги. Можно также разрешить другим пользователям открытие книги только для чтения.

· Чтобы скрыть от пользователя всю книгу, но оставить доступ к ее содержанию, выберите команду **Скрыть** в меню **Окно**, а затем сохраните изменения в скрытую книгу.

Возможен запрет изменения части или всего листа, просмотра скрытых строк и столбцов, просмотра формул, изменения графических объектов или сохраненных сценариев. Чтобы получить список всех элементов листа, которые могут быть защищены,

· Возможен запрет добавления и удаления страниц в книге, просмотра скрытых страниц. Можно также запретить изменение размера или положения окна книги, удаление общей книги из совместного доступа или отключение ведения журнала изменений. Чтобы получить список всех элементов книги, которые могут быть защищены.

·**Защищаемые элементы листа**

При защите листа с помощью команды **Защитить лист** (меню **Сервис**, подменю **Защита**) ограничивается доступ к этому листу. Для снятия этих ограничений необходимо снять защиту листа с помощью команды **Снять защиту листа** (меню **Сервис**, подменю **Защита**). Если для защищенного элемента был установлен пароль[2] для снятия защиты необходимо знать этот пароль.

Если в макросе содержатся инструкции, которые не могут быть выполнены в защищенном листе, выдается соответствующее сообщение и выполнение макроса останавливается.

Если в диалоговом окне **Защитить лис**т установлен флажок **Содержимое**, запрещается:

· Изменение ячеек, если только они не были разблокированы перед установкой защиты листа. Например, если лист используется в качестве формы, следует оставить заблокированными ячейки, содержащие метки и инструкции, и разблокировать поля

[2] слово или строка символов, которую необходимо ввести для доступа к защищенной ячейке, графическому объекту, листу, книге, папке или файлу. Паролем может являться любая комбинация чисел и пробелов. При вводе пароля Microsoft Excel вместо вводимых символов отображает звездочку (*). В паролях обычно учитывается регистр символов, так что при вводе символов следует правильно вводить строчные и прописные буквы.

ввода. Для перемещения по разблокированным полям в защищенном листе служит клавиша TAB.

· Просмотр скрытых перед защитой листа строк и столбцов.

· Просмотр скрытых перед защитой листа формул.

· Изменение элементов на листах диаграмм, таких как последовательностей данных, осей и описаний. Диаграммы продолжают отображать изменения, внесенные в их исходные данные.

Если в диалоговом окне **Защитить лист** установлен флажок **Объекты**, запрещается:

· Изменение графических объектов, включая созданные с помощью Microsoft Excel карты, внедренные диаграммы, формы и поля, если только они не были разблокированы перед защитой листа. Например, если лист содержит кнопку, запускающую макрос, возможно нажатие этой кнопки, но не возможно ее удаление.

· Изменение внедренных диаграмм. Однако при защите внедренных диаграмм их обновление продолжается при изменении исходных данных.

· Обновление карты, если она защищена.

· Добавление или изменение примечаний.

· Изменение на листах диаграмм графических объектов, таких как полей, если только они не были разблокированы перед защитой листа диаграмм.

Если в диалоговом окне **Защитить лист** установлен флажок **Сценарии**, запрещается:

· Просмотр скрытых сценариев.

· Изменение и удаление защищенных сценариев. При этом допускается изменение значений незащищенных ячеек и добавление новых сценариев.

Примечание. В редакторе *Visual Basic* для защиты ячеек предусмотрено свойство *Visual Basic* **EnableSelection** (защита выделенной области). Более подробные сведения содержатся в справочной системе редактора Visual Basic.

Защищаемые элементы книги

При защите книги с помощью команды **Защитить книгу** (меню **Сервис**, подменю **Защита**) ограничивается доступ к ней. Для снятия этих ограничений необходимо снять защиту книги с помощью команды **Снять защиту книги** (меню **Сервис**, подменю **Защита**). Если для защищенного элемента был установлен пароль, чтобы снять защиту, необходимо знать этот пароль.

Если в диалоговом окне **Защита книги** установлен флажок **Структуру**, запрещается:

· Просмотр скрытых листов.

· Перемещение, удаление, скрытие или переименование листов.

· Вставка новых листов или листов с диаграммами. Допускается добавление внедренных диаграмм с помощью мастера диаграмм.

· Перемещение или копирование листов в другую книгу.

· Отображение для ячейки в области данных в сводных таблицах исходных данных, а также отображение страниц полей страниц на отдельных листах.

· Создание для сценариев краткого отчета с помощью диспетчера сценариев.

· Использование инструментов анализа надстройки «Пакет анализа» для помещения результатов на новый лист.

· Запись новых макросов. Если в макросе содержатся инструкции, которые не могут быть выполнены в защищенной книге, выдается соответствующее сообщение и выполнение макроса останавливается.

Если в диалоговом окне **Защита книги** установлен флажок **Окна**, запрещается:

· Изменение размеров и положения окон открытой книги.

· Перемещение, изменение размеров и закрытие окон. Разрешается однако скрывать и отображать окна.

Примечание. В редакторе Visual Basic предусмотрена возможность защиты макросов от просмотра и изменения. Для этого следует воспользоваться вкладкой **Защита** диалогового окна **Свойства** проекта в редакторе Visual Basic (команда **Свойства** проекта из меню **Сервис**). Более подробные сведения содержатся в справочной системе редактора Visual Basic.

Ограничение прав доступа к общей книге

1 Если книга, которую вы хотите защитить является общей, и требуется установить пароль, чтобы ограничить доступ к ней самой или к ее страницам или к свойствам, удалите книгу из общего пользования.

Удаление книги из общего пользования

Чтобы другие пользователи больше не вносили изменений в общую книгу, откройте и работайте с ней как единственный пользователь. При удалении книги из общего пользования завершается связь остальных пользователей, выключается ведение журнала изменений, и удаляется сохраненный журнал изменений, таким образом, просмотр журнала и объединений данной копии с другими копиями общей книги становится невозможным.

Предупреждение. Для исключения потери не сохраненных данных остальными пользователями предупредите их, чтобы они сохранили книгу и закрыли ее, до того как книга будет удалена из общего пользования.

- В меню **Сервис** выберите **Доступ к книге**, а затем ярлык **Правка.**

- Убедитесь, что вы единственный пользователь в списке **Файл открыт следующими пользователями**. В противном случае, остальные пользователи потеряют не сохраненные данные.

- Снимите флажок **Разрешить совместный доступ** и нажмите кнопку **OK**.

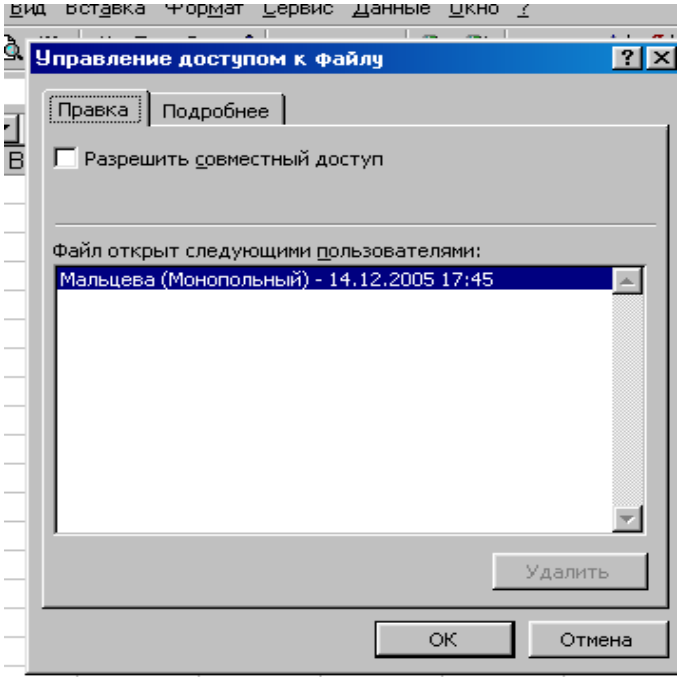
- Если появится сообщение о воздействии на других пользователей, выберите **Да**.

2 Чтобы обязать пользователя вводить пароль при открытии книги, установите его.

3 Чтобы обязать пользователя вводить пароль для изменения и сохранения общей книги, установите его.

4 Чтобы другие скрыть определенные строки или столбцы в документе от пользователей, выделите их. Затем в меню **Формат** выберите **по строкам** или **по столбцам** и нажмите кнопку **Скрыть**.

Чтобы позволить другим пользователям изменять только определенные места в общей книге, разблокируйте их, а затем защитите книгу. (Это также ограничит просмотр другими



пользователями скрытых строк и колонок.)

5 Для того чтобы скрыть определенные страницы общей книги, в меню **Формат** выберите **Лист** и затем выберите команду **Скрыть**. Повторите это для всех листов, которые надо скрыть.

После того, как все листы были скрыты, необходимо защитить книгу, чтобы другие пользователи не могли просматривать скрытые страницы, предварительно сняв ограничение на просмотр. В меню **Сервис** выберите команду **Защита** и затем **Защитить книгу**. Установите флажок структуру и нажмите кнопку **OK**.

6 Для изменения числа дней, в течение которых Microsoft Excel будет хранить журнал изменений для общей книги (по умолчанию 30 дней), в меню **Сервис** выберите **Доступ к книге** и затем выберите вкладку **Правка**. Установите флажок Разрешить совместный доступ, а затем выберите вкладку **Подробнее**. В группе **Регистрация изменений** убедитесь, что выбран параметр **хранить журнал изменений в течение** и затем в поле **Дни** введите число дней, в течение которых будет храниться журнал изменений.

Выберите ярлык **Правка**, снимите флажок **Разрешить совместный доступ** и щелкните **ОК**.

7 В меню **Сервис** выберите **Защита**, а затем **Защита общей книги** или **Защитить книгу** и **дать общий доступ**.

8 Установите флажок **Общий доступ с исправлениями**.

9 Чтобы обязать других пользователей вводить пароль для прекращения ведения журнала изменений или удаления книги из общего пользования, введите пароль в поле **Пароль**, а затем повторите его, когда будет предложено.

10 Когда будет предложено, сохраните книгу, чтобы сделать ее общей и включить ведение журнала изменений.

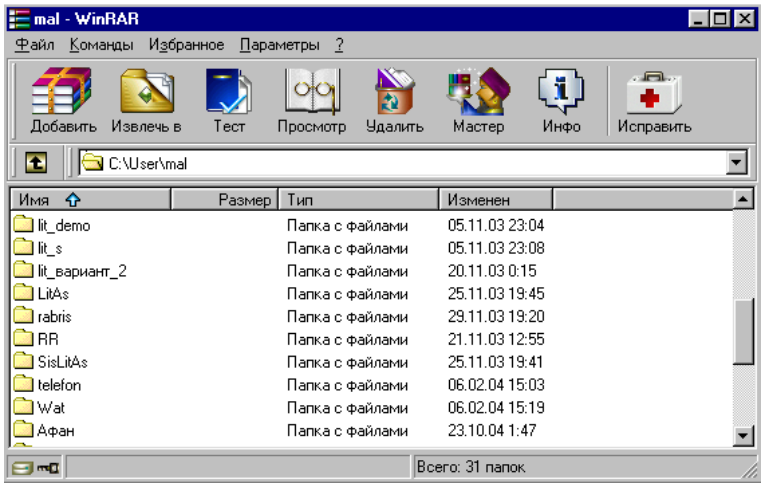
Примечания

Если защищены параметры доступа, то пользователь не может удалить книгу из общего пользования или выключить ведение журнала изменений.

Если книга уже является общедоступной, то можно установить права доступа и изменить журнал изменений, но нельзя установить пароль на эти права. Чтобы установить пароль, необходимо удалить книгу из общего пользования.

Лабораторная работа № 5 Защита информации путем создания архивов с паролем

Программы архивации файлов WinRaR



WinRAR можно использовать двумя способами: в режиме графической оболочки со стандартным интерфейсом Windows и в командной строке.

Чтобы использовать WinRAR в режиме оболочки, дважды щелкните мышью на значке WinRAR — после этого для архивации и извлечения файлов вы сможете пользоваться кнопками и меню

При открытии архива в окне WinRAR выводится его содержимое. Выделите те файлы и папки, которые вы хотите извлечь. Это можно сделать клавишами управления курсором или левой кнопкой мыши при нажатой клавише <Shift> (как в Проводнике и других программах Windows). Выделять файлы в WinRAR можно также клавишами <Пробел> или <Insert>. Клавиши <+> и <–> на цифровой клавиатуре позволяют выделять и снимать выделение с группы файлов с помощью шаблонов (т.е. задавая маски файлов символами '*' и '?').

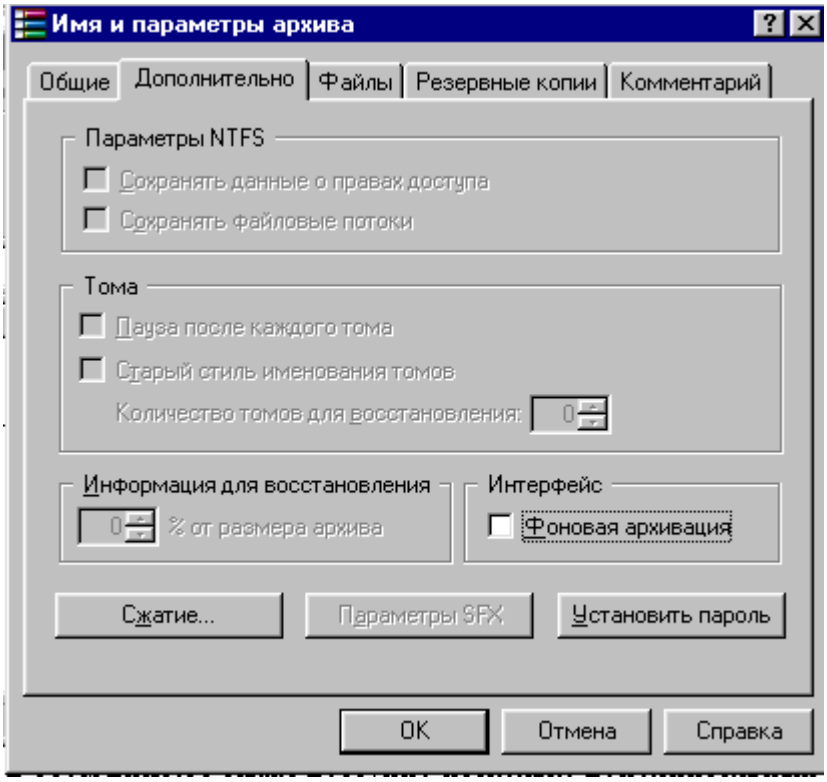
Выделив один или несколько файлов, нажмите кнопку **Извлечь в** вверху окна WinRAR, или же нажмите <Alt+E>, введите в появившемся диалоге нужный путь, а после этого нажмите кнопку **OK**. Здесь же можно поменять несколько дополнительных параметров

Этот диалог позволяет выбрать папку назначения и параметры для извлечения файлов. По умолчанию папка получает то же имя, что и архив (без расширения) и размещается в текущей папке. Для того, чтобы поместить в другой папке нужно в диалоге **Параметры архивации** В поле **Путь для извлечения** следует ввести нужный путь (если его еще не существует, то он будет создан) или выбрать папку в панели дерева папок.

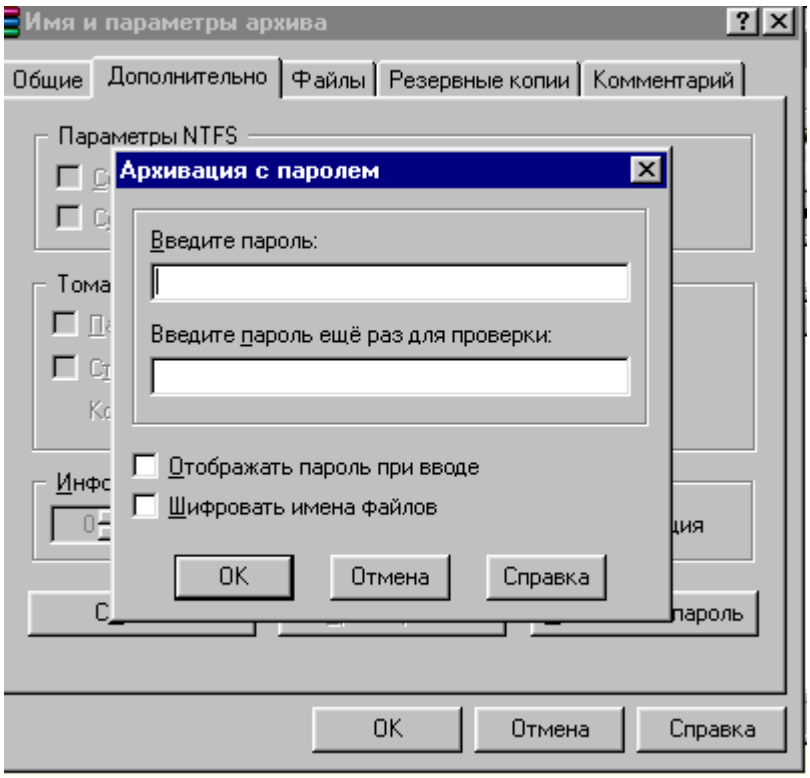
Оба формата — RAR и ZIP — поддерживают шифрование. Чтобы зашифровать файлы, нужно до начала архивации указать пароль — в командной строке, в меню или непосредственно на вкладке **Дополнительно** диалога **Имя и параметры архива**.

Если вы ввели пароль непосредственно в диалоге **Имя и параметры архива**, то вам не нужно отменять его самостоятельно — пароль будет действовать только в течение одной операции архивирования, по окончании которой сбросится автоматически.

При извлечении зашифрованных файлов можно ввести пароль заранее, хотя это и необязательно. Если пароль не был введен перед началом извлечения, и WinRAR обнаружил зашифрованный файл, он спросит пароль у пользователя. Для обеспечения достаточного уровня безопасности используйте пароли длиной не менее 8 символов. Не следует использовать в качестве пароля слова какого-либо языка, лучшим выбором является случайная комбинация букв и цифр. Обратите внимание, что в паролях учитывается регистр букв. Если вы потеряете свой пароль, восстановить из архива зашифрованные файлы не удастся — в этом вам не поможет даже сам автор WinRAR. Если включена опция **Шифровать имена файлов**, WinRAR будет зашифровывать не только находящиеся в файлах данные, но и другие важные области архива как-то: имена файлов, размеры, атрибуты, комментарии и другие блоки, благодаря чему достигается более высокая степень защиты от несанкционированного доступа. Если архив зашифрован с этой опцией, то без указания пароля не удастся даже просмотреть список содержащихся в нём файлов.



В этом диалоге также доступно несколько дополнительных параметров:



В командной строке пароль задается с помощью ключа -p<pwd>

Пример:

WinRAR a –pZaBaToAd –r secret games*.*

Эта команда добавит содержимое папки games в архив secret, используя пароль ZaBaToAd.

Ряд программ обслуживания архивов файлов позволяет использовать криптографическую технику. Наиболее широко используются из них программы ZIP и ARJ. Среди традиционных средств поддержки архивов как добавление, удаление, обновление, распечатка и извлечение файлов, в них входят операции «взбивания» файлов с паролем при их помещении в архив и извлечении. Задание пароля осуществляется ключами -sпароль (S - от английского слова scramble, что означает смешивать, взбивать, соединять. В программе ARJ используется ключ G - garble - подтасовывать, искажать). Так, например, создание архива всех файлов из каталога может быть выполнено утилитой PKZIP при помощи Trivia так:

>PKZIP -sTrivia archive.zip *.*

К особенностям работы с программами архивации нужно отнести неудовлетворительное задание пароля, который отображается на экране и может быть подсмотрен как визуально, так и техническими средствами перехвата излучения мониторов компьютеров. Кроме того, шифрование захватывает область данных архива, которая легко реконструируется, как длина исходного файла, его название и ряд резервных нулевых байт. Из-за этого, несмотря на вообще-то серьезное взбивание текста с паролем, возникают обоснованные опасения в возможности криптографической атаки на ключ. Поэтому данные способы засекречивания сообщений устойчивы лишь от любопытных, но не от профессиональных взломщиков и тем более от государственных криптографических служб. Известно множество «ломалок» для шифрованных архивов,

которые подбирают ключ, контролируя контрольную сумму. Эффективность их очень невелика, так как по контрольной сумме файл вскрывается весьма неоднозначно, а примененный способ тотального опробования ключей годится только для сверхбыстродействующих ЭВМ. Однако периодически приходится взламывать архивы, ключи к которым пользователи забыли или ввели с ошибкой. Обычно они смутно помнят ключ, который они вроде бы вводили. Простенькая программа модификация этого ключа, учитывающая ошибки при наборе позволяет примерно в половине случаев подобрать ключ за пару часов работы даже слабой персональной ЭВМ.

Использование архиватора RAR.

Данный архиватор пользуется не меньшей популярностью у нас в стране потому, что имеет вполне удобный для работы интерфейс, отчасти напоминающий всем известный NORTON COMMANDER, поддерживает некоторые файловые операции (например, удаление файлов, каталогов) и избавляет пользователя от проблем с указанием всех необходимых ключей в командной строке вызова архиватора (конечно, куда проще нажать F2 и ввести имя архива, чем набирать «arj a myarch.arj .....» и т.д. С другой стороны, архивация ZIP и ARJ является уже сформировавшемся стандартом, так что RAR является не более чем просто удобной программой-оболочкой для архивирования. К тому же, работа с ZIP и ARJ у данного архиватора происходит через вызовы всё тех же программ PKZIP и ARJ.

Архивация с паролем с помощью архиватора RAR происходит следующем образом. При нажатии ALT+P архиватор запросит пароль на архивную сессию, т.е. данный пароль будет действовать на всё время, пока пользователь не выйдет из среды архиватора. После ввода пароля RAR предложит пользователю подтвердить ввод путем повторного введения пароля. При несовпадении пароль запомнен не будет. Далее можно работать с файлами обычным путем, но все пакуемые файлы будут архивироваться с паролем. При открытии архива файлы, защищенные паролем будут иметь значок * перед своим именем, а при попытке разархивирования, если не был введен пароль на архивную сессию, RAR запросит пароль для первого встретившегося файла с паролем и затем спросит, следует ли использовать введенную последовательность для всех остальных архивных файлов.

Лабораторные задания:

1. Создайте архив, используя программу PKZIP, включив в него файлов 5-6. Теперь добавьте к архиву 4 файла, защищенных паролем.

2. Попытайтесь разархивировать созданный архив, введя неправильный пароль и проконтролируйте содержимое файлов, архивированных с паролем.

3. Повторите вышеприведенные задания, используя архиватор ARJ.

4. В программе RAR создайте архив, используя несколько различных паролей.

5. Используя программу RAR попытайтесь осуществить разархивирование созданных выше архивов, созданных программами PKZIP и ARJ. Все ли файлы разархивировались ?

6. Проверьте, влияет ли регистр вводимых в пароле символов при архивировании на правильность последующего ввода при разархивировании ?

7. Используя BAT-файл и архив с паролем из одной цифры, попробуйте осуществить подбор пароля.

Лабораторная работа № 6 Принципы уничтожения и восстановления файлов

Удаленные файлы

Доступ к дисковой памяти является, без сомнения, самой медленной операцией, выполняемой вашим компьютером. Для повышения эффективности при использовании DOS-овской команды DEL файлы в действительности не удаляются. Вместо этого записи удаляемых файлов в FAT (File Allocation Table - таблице размещения файлов) просто обозначаются как уничтоженные (и в их имени, если просматривать FAT вместо первой буквы появляется знак «x»). Эта метка говорит операционной системе, что область, занимаемая раньше удаленным файлом, теперь доступна для иного использования. До тех пор, пока в эту область не будет записан другой файл, старый файл фактически не изменяется, но его сохранность не гарантируется. Для оптимизации записи новых файлов используются первые *пустые* сектора, наиболее близкие к головкам дисковода, так что весь старый файл или его часть некоторое время может оставаться на диске, пока эти сектора не будут использованы повторно.

При удалении файлов в Windows 95 они по умолчанию перемещаются в Корзину (Recycle Bin) на случай, если вы вдруг решите вернуть их обратно. При очистке Корзины данные остаются на диске до тех пор, пока не будет создан другой файл, записанный поверх секторов удаленного файла.

Вот старый прием DOS: удалить файлы (чтобы скрыть их), а когда опасность миновала - использовать программу восстановления. Этот метод не слишком хорош. Во-первых, он обеспечивает плохую защиту, а во-вторых, обладает целым рядом недостатков. Если в тот отрезок времени, когда ценные файлы временно удалены, что-нибудь будет записано на диск, то они могут быть испорчены и исправить их станет просто невозможно. Кроме того, восстанавливающие утилиты теперь не редкость...

Уничтожение файлов

Потенциальные проблемы безопасности связаны с тем, что при выполнении команды удаления файлы фактически не уничтожаются. Эта проблема неоднократно обсуждалась в компьютерной литературе, но средний пользователь компьютера часто о ней забывает. Предприниматели давно поняли важность устройств для уничтожения бумажных документов, но еще недостаточно осознали, что уничтожать документы необходимо и на компьютере.

При уничтожении файлов важно помнить о двух важных проблемах. Первая состоит в том, что файлы станут действительно невосстановимыми только после того, как будут физически уничтожены. Никакая утилита восстановления уже не сможет вернуть их обратно. Это палка о двух концах - удаленные файлы станут недоступными для желающего порыться в ваших данных, но они не подлежат ремонту, если по ошибке вы удалите нужную информацию. При уничтожении файлов нужно быть очень внимательным.

Вторая проблема заключается в создании рабочих файлов, используемыми многими приложениями для временного хранения. Ваш текстовый процессор может иметь возможность автоматического сохранения через каждые 10 минут, или при редактировании перед записью в *действительный* файл он может использовать рабочую версию. После того, как система удалит копии рабочих файлов, злоумышленник сможет их восстановить. Поэтому нелишне вручную чистить диск, записывая нужную информацию в области, ранее занятые рабочими файлами, и тем самым их уничтожая.

Концепция, которая используется в программах типа Nuke, Terminator, WipeInfo и других уничтожителях файлов, состоит в перезаписи как элементов списка в FAT, так и дисковых секторов, занимаемых уничтожаемым файлом.

Программа UnErase

UnErase может вычислить большинство удаленных имен файлов и знает, где файл начинался и насколько большим он был. Из этого следует, что зачастую он может немедленно восстановить файл. В некоторых случаях, нет достаточной информации для продолжения, поэтому UnErase имеет «ручной» метод, который позволяет искать части файла и складывать их обратно вместе, фрагмент за фрагментом.

В главном окне UnErase можно выбрать файл или файлы путем перемещения полосы подсветки вверх и вниз. Затем следует нажать кнопку [UnErase] для восстановления файла.

Если вы не видите файл, который следует восстановить:

- Используйте в меню [Файл] команду [Смена каталога] для поиска в другом каталоге.

- Используйте в меню [Файл] команду [Просмотр всех каталогов] для вывода списка всех удаленных файлов на данном диске

- Используйте команды меню [Поиск] такие, как [Поиск потерянных имен] для поиска файлов, удаленных из каталогов, которые также были удалены.

Выберите кнопку [Инфо] для просмотра подробностей о выделенном файле и возможности его восстановления. Выберите кнопку [Просмотр] для изучения содержимого файла. Можно также отметить несколько файлов для восстановления.

Колонка **Имя** выдает имя и расширение файла. Существует четыре формата:

имя файла указывает файл, который был сохранен Norton SmartCan. Всегда можно восстановить этот файл со 100%-й гарантией.

?мя файла указывает незащищенный файл, который был удален. DOS перезаписала первый символ имени, когда удалила файл, поэтому будет запрос символа, заменяющего ? при восстановлении.

ИМЯКАТ (в заглавных буквах) указывает каталог, который не удален. Можно нажать клавишу Enter на этой строке для входа в этот каталог перед тем, как восстанавливать в нем удаленные файлы.

?МЯКАТ указывает на удаленный каталог. Восстановите этот каталог перед тем, как восстанавливать в нем удаленные файлы.

Размер, Дата и Время помогают идентифицировать файл. Дата и время показывают время создания и модификации файла, но не показывают, когда файл был удален.

Колонка **Прогноз** показывает предположение о вероятности восстановления файла. Файлы, защищенные Norton SmartCan, всегда показаны, как превосходные. Другие файлы имеют прогнозы от отличного до плохого, в зависимости от некоторых факторов (для подробностей выберите [Информация]). Эта же колонка сообщает ВОССТАНОВЛЕН для

уже восстановленных файлов и показывает НЕУДАЛЕННЫЙ для некоторых файлов, включенных в список командой Alt+F,Y.

Лабораторные задания:

1. Напишите командный файл, при запуске которого произойдет затирание файлов с расширением BAK на жестком диске C. Использовать программу WipeInfo.

2. Удалить на жестком диске несколько файлов, а затем попытаться с помощью программы UnErase восстановить их. Проэкспериментировать для случая, когда файлы удаляются вместе с подкаталогами, содержащими их.

3. Проверить жесткий диск и дискету на наличие сбоев с помощью программы Norton Disk Doctor. Создать ситуацию, когда на дискете могут появиться потерянные кластеры и исправить их.

Лабораторная работа № 7 Защита программ от дизассемблеров и отладчиков

Цель работы*:* изучить основные принципы защиты программных продуктов от дизассемблирования и противодействия трассировки исполняемого кода с помощью отладчика; программно реализовать один из указанных способов защиты.

Наличие механизмов защиты от дизассемблеров и отладчиков в исполняемом модуле исследуемой программы становится первым и, пожалуй, наиболее сложным препятствием для хакера. Задача таких механизмов защиты - недопущение или максимально возможное затруднение анализа исполняемого кода программы. Средства защиты от стандартных дизассемблеров и отладчиков должны быть неотъемлемой частью любого профессионального пакета защиты программ от возможных несанкционированных вмешательств.

Защита от дизассемблирования.

Приведем несколько методов противодействия дизассемблированию исполняемого кода программы:

- шифрование;
- архивация (как разновидность шифрования);
- использование самогенерируемых кодов.
- «обман» дизассемблера;

Шифрование исполняемого кода программы с целью защиты от дизассемблера - наиболее простое средство в отношении как реализации, так и снятия. Поэтому шифрование может рассматриваться лишь как часть механизма защиты и не обязательно должно быть сложным. Достаточно, например, к каждому байту исполняемого модуля прибавить некоторую константу, чтобы дизассемблер не смог работать.

Предварительная архивация кода программы также не представляет особых трудностей для хакера. Однако архивация более эффективна по сравнению с шифрованием, так как решает сразу две задачи; уменьшение размера защищаемого модуля и скрытие кода программы от дизассемблера. Методов сжатия исполняемых файлов на сегодняшний день известно множество. Мы не будем останавливаться на их описании, заметим только, что файлы должны быть самораспаковывающимися.

Для усиления защитного действия шифрованного кода его дешифрацию желательно выполнять поэтапно - на разных участках и в разные моменты работы программы.

Самогенерируемые коды - крайне сложное в реализации, но, пожалуй, наиболее эффективное средство борьбы с дизассемблерами. Кратко поясним их суть.

Самогенерируемые коды - это исполняемые коды программы, полученные в результате выполнения некоторого набора арифметических и/или логических операций над определенным, заранее рассчитанным массивом данных. Самогенерируемые коды вырабатываются непосредственно защищаемой программой, которая по ходу выполнения как бы сама себя «достраивает». Текст программы выглядит красивым и оригинальным, если массив исходных данных самогенерируемых кодов подобран таким

образом, что сам является исполняемым кодом (причем желательно, реально получающим управление).

«Обманом» дизассемблера будем называть такой стиль программирования, который позволяет «запутать» стандартный дизассемблер применением нестандартных приемов выполнения некоторых команд и нарушением общепринятых соглашений. Наиболее широкое распространение получили следующие способы:

- использование нестандартной структуры программы;
- скрытые переходы, скрытые вызовы и возвраты из подпрограмм и прерываний;
- переходы и вызовы подпрограмм по динамически изменяемым адресам;
- модификация исполняемых кодов.

Первый способ основывается на предположении, что программа, не имеющая стандартной сегментации (например, у которой отсутствует стековый сегмент), может быть неправильно воспринята «интеллектуальным» дизассемблером. В связи с этим защитные механизмы программ чаще всего располагаются в одном сегменте.

Для направления дизассемблера по ложному следу очень часто используются скрытые переходы, вызовы и возвраты, использующие нестандартные реализации команд JMP, CALL, INT, RET и IRET. Приведем несколько примеров.

Скрытый JMP

```
...                 ...
jmp m               mov ax,offset m     ; Занести в стек
                    push ax                     ; адрес метки
                    ret                 ; Перейти на метку
m:                  m:
...                         ...
```

Скрытый CALL

```
...                 ...
call subr           mov ax,offset m     ; Занести в стек
                            push ax             ; адрес возврата
                    jmp subr    ; Перейти на подпрограмму
              m:
                    ...
subr:               subr:
```

```
...                     ...
```

Скрытый INT

```
...                     ...
int 13h                         pushf           ; Занести в стек флаги
                        push cs                 ; Занести в стек CS
                        mov si,offset m         ; Занести в стек
                        push si                 ; адрес возврата
                        xor si,si
                        mov es,si
                        jmp dword ptr es:[13h*4]
        m:
...                     ...
```

Скрытый IRET

```
...                     ...
iret                    mov bp,sp     ; Переход на точку возврата
...                     jmp dword ptr [bp]; из прерывания
                        ...
                        add sp,4                ; Точка возврата
                        popf
...                     ...
```

Скрытый RET

```
...                     ...
ret                     pop bx          ; Взять из стека адрес возврата
                        jmp bx          ; и перейти на него
...                     ...
```

Переходы и вызовы подпрограмм по динамически изменяемым адресам подразумевают модификацию байтов адреса перехода или вызова подпрограммы, находящихся за первым байтом команды (байтом кода операции). Приведем несколько примеров.

Модификация адреса перехода

```
        ...
        mov word ptr cs:m[1],1234h      ; Подстановка нового адреса
        ...
m:      jmp place
        ...
```

Модификация адреса вызываемой подпрограммы

```
        ...
        mov word ptr cs:m[1],es
        mov word ptr cs:m[3],5678h
        ...
m:      call far subr
        ...
```

Модифицировать адрес гораздо проще, если использовать косвенные переходы и вызовы. Например

```
jmp dword ptr cs:[bx]
call word ptr es:[si]
```

Здесь возможности модификации адресов значительно шире.

Описанный прием можно также использовать для модификации любых исполняемых кодов. Например однобайтная команда PUSH AX имеет кодировку 50H (01010000). Изменив каким-либо способом один из битов команды (допустим 4-й), мы получим совершенно другую команду INC AX. Осуществить это практически можно, например, так:

```
...
and byte ptr cs:m,0Efh      ; Обнулить 4-й бит по адресу m
...
        m:      push ax
                ...
```

Все вышеописанные методы «обмана» дизассемблера рассчитаны на то, что «интеллектуальная» программа (например, Sourcer), отслеживая моменты передачи управления, не найдет некоторые участки программы и соответственно не

дизассемблирует их. Особенно успешно эта цель может быть достигнута при использовании самогенерируемых кодов и скрытых команд JMP и CALL.

Защита от трассировки.

Данный метод защиты заключается в том, что программа распознает факт пошаговой трассировки и пытается тем или иным способом противодействовать этому процессу. Чаще всего для этих целей используется прием, основанный на особенностях архитектуры микропроцессоров семейства Intel 80x86. Для повышения производительности этих кристаллов в них применяется конвейерный способ обработки команд, в соответствии с которым очередная инструкция загружается во внутреннюю очередь команд процессора до завершения обработки текущей инструкции. Если текущая инструкция изменяет следующую за ней команду, то при реальной работе программы это изменение не сказывается на алгоритме, так как к этому моменту содержимое изменяемой ячейки памяти уже загружено в очередь команд. Если же программа работает под управлением отладчика, внутренняя очередь оказывается заполненной командами отладчика и модификация ячейки приводит к изменению алгоритма работы.

```
start:      jmp         frwd

del:        pushf

            cld

            mov         ax,cs

            mov         es,ax

            rep         stosw

            popf

            ret

frwd:       push        cs

            pop         ds

            mov         cx,12

            mov         dl, offset start

            call        del

            mov         dx, offset msg

            mov         ah,9

            int         21h

            . . . . . .

msg         db          ‘Hello !’,0ah,0dh,’$’
```

В следующем примере команда POP SS заставляет отладчик пропустить следующую за ней команду PUSHF из-за потери трассировочного прерывания и тем самым позволяет программе выявить факт работы под отладчиком

```
        push   cs
        push   cs
        pop    ds
        pop    ss
        pushf
        pop    ax
        test   ah,1
        jz     norm_ex
        mov    dx,offset trace
        jmp    exit
norm_ex:
        mov    dx,offset norm
exit:
        mov    ah,9
        int    21h
. . . . . .
trace   db     'Trace',0ah,0dh,'$'
norm    db     'Normal',0ah,0h,'$'
```

Суть подхода к обнаружению факта работы под отладчиком в следующем примере: в PSP задачи по смещению 2Eh находится 4 байтная область, в которую DOS помещает указатель стека при обращении к системным функциям, т.к. во время выполнения ряда системных вызовов используется внутренний стек DOS. При пошаговом выполнении обработку прерывания 21h первым производит отладчик, чей указатель и будет сохранен в активном PSP.

```
        .DATA
Greeting        db      'Hello$'
Debugdb         ', debugger!',0ah,0dh,'$'
```

```
        .CODE
mov     ax,@data
        mov     ds,ax
        mov     ah,09h
        mov     dx,offset Greeting
        int     21h
        mov     ax,ss
        cmp     ax,es:[30h]
        je      Exit
        mov     ah,09h
        mov     dx,offset Debug
        int     21h
Exit: . . . .
```

Лабораторная работа № 8 Программирование арифметических алгоритмов

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.

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
3	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.

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.

Лабораторная работа № 9 Программирование алгебраических алгоритмов

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.

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 $Т(0)_i=Г(ш)_i+Т(ш)_i$.

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.

Лабораторная работа №10 Защита от закладок при разработке программ

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

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.

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.**

Задание к работе

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

2. Используя стандартную программу Windows **Проверка диска,** проверьте диск A: 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.

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?

Лабораторная работа №11 Программирование алгоритмов криптосистем с открытом ключом

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.

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*CT.

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 $ed=1 \pmod M$.

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 $S'=S^d \pmod N$, то есть шифруется открытым ключом.

10. Получатель расшифровывает с помощью закрытого ключа: $S=S'^e \pmod N$.

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.

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.

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.

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.

Лабораторная работа № 12 Шифрация информационных массивов методами подстановки и замены

Три основных типа шифров.

Среди традиционных методов кодирования имеются два базовых типа - перестановка (transposition) и замена (substitution). Шифры, использующие перестановку, «перемешивают» символы сообщения по определенному правилу. Шифр замены замещает одни символы другими, но сохраняет порядок их следования в сообщении. Оба метода могут быть доведены до любой степени сложности. Кроме того, на их основе можно создать комплексный метод, сочетающий черты каждого из них. Появление компьютеров добавило к существующим двум методам еще один, называемый битовой манипуляцией (bit manipulation). Этот метод изменяет компьютерное представление данных по определенному алгоритму.

Все три метода при желании могут использовать ключ (key). Как правило, ключ представляет собой строку символов, необходимую для того, чтобы декодировать сообщение. Однако, не стоит путать ключ с методом шифрования, поскольку наличие ключа является необходимым, но недостаточным условием успешной расшифровки сообщения. Кроме знания ключа, необходимо знать и алгоритм шифрации. Назначение ключа состоит в «персонализации» сообщения, с тем чтобы прочитать его могли только те, кому оно предназначено, даже несмотря на то, что применяемый для шифрования алгоритм широко известен.

Необходимо научиться различать два базовых понятия - открытый текст (plain text) и шифрованный текст (cipher text). Информация, переданная открытым текстом, представляет собой читаемое сообщение, шифрованный текст представляет собой закодированную версию сообщения.

Шифры замены

Шифр замены представляет собой метод шифрования сообщения путем замены одних символов другими на регулярной основе. Одной из простейших форм такого шифра является циклический сдвиг алфавита на определенное количество символов. Например, если латинский алфавит сдвинуть на три символа, то вместо

abcdefghijklmnopqrstuvwxyz

получим

defghijklmnopqrstuvwxyzabc

Таким образом, a превращается в b, b - в e, и т.д. Обратите внимание, что буквы «abc», находившиеся в начале алфавита, переместились в конец. Для того, чтобы закодировать сообщение, пользуясь этим методом, нужно просто заменить нормальный алфавит на его смещенную версию.

Вышеприведенный алгоритм, основанный на постоянном сдвиге алфавита сможет обмануть разве что совсем неопытного взломщика, поскольку взламывается исключительно просто. В конце концов, если есть всего 26 возможных вариантов сдвига, и все их можно перебрать за сравнительно короткое время вручную. Лучшим вариантом

по сравнению с вышеприведенным является использование неупорядоченного алфавита, а не просто сдвига. Еще одним недостатком метода простого постоянного сдвига является то, что сохраняются на своих местах пробелы между словами. Это еще более упрощает задачу взломщика, поэтому пробелы также следует кодировать (еще лучше будет кодировать и знаки препинания). Например, можно задать следующее соответствие строк, одна из которых содержит упорядоченный алфавит, а вторая, задающая преобразование, - его рандомизированную версию:

abcdefghijklmnopqrstuvwxyz<пробел>

qazwsxedcrfvtgbyhnujm ikolp

Дает ли эта рандомизированная версия существенное улучшение по сравнению с предыдущей версией, использовавшей простой постоянный сдвиг ? Ответ будет утвердительным, так как теперь имеется 26! (огромное число $\approx 4 \times 10^{26}$) способов упорядочивания алфавита, а с учетом пробела это число возрастет до 27! ($\approx 1 \times 10^{28}$).

Следует отметить, что даже этот улучшенный алгоритм шифрования с заменой может быть с легкостью взломан при использовании частотных таблиц английского языка, в которых содержится частотная информация по каждой букве алфавита. Далее, чем больше объем кодированного сообщения, тем проще расшифровать его с помощью частотных таблиц. Для того, чтобы замедлить процесс расшифровки сообщения взломщиком, применяющим частотные таблицы, можно воспользоваться шифром со множественными заменами (multiple substitution cipher). В этом случае одна и та же буква открытого текста не обязательно будет преобразовываться в одну и ту же букву зашифрованного сообщения. Этого можно добиться, включив второй рандомизированный алфавит и переключаясь между ними по заранее предопределенному методу (например, при встречающемуся в тексте пробелу).

Этот подход реализует нижеприведенная программа. В качестве второго рандомизированного алфавита используем poi uytrewqasdfghjklmnbvcxz:

```
// Шифр со множественными заменами

#include <iostream.h>

#include <fstream.h>

#include <ctype.h>

#include <<stdlib.h>


const int SIZE = 28;


void encode (char *input, char *output);

void decode (char *input, char *output);
```

```
int find(char *s, char ch);
char sub[SIZE] = "qazwsxedcrfvtgbyhnujm iklop";
char sub2[SIZE] = "poi uytrewqasdfghjklmnbvcxz";
char alphabet[SIZE] = "abcdefghijklmnopqrstuvwxyz";

main(int argc, char *argv[])
{
 if(argc != 4){
 cout << "Usage: input output encode/decode \n";
 exit(1);
 }
 if(toupper(*argv[3]) == 'E')
 encode(argv[1], argv[2]);
 else
 decode(argv[1], argv[2]);
 return 0;
}

// Encode
void encode(char *input, char *output)
{
 int ch, change;
 ifstream in(input, ios :: out | ios :: binary);
 ofstream out(output, ios :: out | ios :: binary);

 if (!in) {
 cout << "Cannot open input file.\n";
 exit(1);
```

```
 }

 if (!out) {
 cout << "Cannot open output file.\n";
 exit(1);
 }
 change = 1;
 do {
 ch = in.get();
 ch = tolower(ch);
 if(isalpha(ch))
 if(change)
 ch = sub[find(alphabet, ch)];
 else
 ch = sub2[find(alphabet, ch)];
 if(!in.eof()) out.put((char) ch);
 if(ch == ' ') change = !change;
 } while(!in.eof());
 in.close();
 out.close();
}
// Decode
void decode(char *input, char *output)
{
 int ch, change;
 ifstream in(input, ios :: out | ios :: binary);
 ofstream out(output, ios :: out | ios :: binary);
```

```
 if (!in) {
 cout << "Cannot open input file.\n";
 exit(1);
 }

 if (!out) {
 cout << "Cannot open output file.\n";
 exit(1);
 }
 change = 1;
 do {
 ch = in.get();
 ch = tolower(ch);
 if(isalpha(ch))
 if(change)
 ch = alphabet[find(sub, ch)];
 else
 ch = alphabet[find(sub2, ch)];
 if(!in.eof()) out.put((char) ch);
 if(ch == ' ') change = !change;
 } while(!in.eof());
 in.close();
 out.close();
}
// Find index
find (char *s, char ch)
{
 register int t;
```

```
 for(t=0;t<SIZE;t++) if(ch==s[t]) return t;

 return -1;

}
```

При использовании шифрования со множественными заменами взломать шифр с помощью частотных таблиц становится намного сложнее. С помощью нескольких рандомизированных алфавитов и совершенного механизма переключения между ними можно добиться построения такого алгоритма, в результате применения которого все алфавитные символы будут появляться с одинаковой частотой. При взломе такого алгоритма частотные таблицы языка будут практически бесполезны.

Лабораторные задания:

1. На одном из языков высокого уровня реализовать шифр замены

2. Реализовать предыдущее задание, используя многоалфавитную замену

3. На одном из языком высокого уровня реализовать шифр перестановки

Лабораторная работа № 13 Шифрация информационных массивов методами битовых манипуляций

Шифры битовых манипуляций.

Методы шифрования, приводимые в предыдущей работе представляют собой компьютеризированные версии шифрования, ранее выполнявшегося вручную. Однако, компьютерные технологии дали начало новому методу кодирования сообщений путем манипуляций с битами, составляющими фактические символы нешифрованного сообщения. Как правило, современные компьютеризированные шифры попадают в класс, называемый шифрами бытовых манипуляций (bit manipulating ciphers). Хотя ревнители чистоты теории могут спорить о том, что такие шифры представляют собой просто вариацию шифров методом замены, большинство специалистов соглашается с тем, что концепции и методы, лежащие в основе шифров битовых манипуляций отличаются от всего, что было известно ранее, настолько значительно, что заслуживают выделения в особый класс.

Шифры битовых манипуляций популярны по двум причинам. Во-первых, они идеально подходят для использования в компьютерной криптографии, так как используют операции, которые легко выполняются системой. Вторая причина заключается в том, что полученный на выходе зашифрованный текст выглядит абсолютно нечитаемым - фактически полной бессмыслицей. Это положительно сказывается на безопасности и защищенности, так как важные данные маскируются под поврежденные файлы, доступ к которым просто никому не нужен.

Как правило шифры битовых манипуляций применимы только к компьютерным файлам и не могут использоваться для бумажных копий зашифрованных сообщений. Причина этого заключается в том, что манипуляции с битами имеют тенденцию генерировать непечатаемые символы. Поэтому мы всегда будем полагать, что текст, зашифрованный с помощью битовых манипуляций, всегда будет оставаться в виде электронного документа.

Шифры битовых манипуляций переводят открытый текст в шифрованный с помощью преобразования набора бит каждого символа по определенному алгоритму, используя одну из следующих логических операций или их комбинацию:

AND OR NOT XOR

Простейший (и наименее защищенный) шифр, манипулирующий с битами, использует только оператор первого дополнения. Этот оператор инвертирует все биты, входящие в состав байта. Таким образом, все нули становятся единицами и наоборот. Поэтому байт, над которым дважды проведена такая операция, принимает исходное значение.

В действительности с этой простой схемой кодирования связаны две основные проблемы. Во-первых, программа шифрования для расшифровки текста не использует ключа. Поэтому любой, кто знает, что используется данный алгоритм и в состоянии написать программу, сможет прочитать файл. Во-вторых (и это самое главное), этот метод отнюдь не тайна для опытных программистов.

Улучшенный метод шифрования методом побитовой манипуляции использует оператор XOR. Результаты выполнения этого оператора приведены в следующей таблице:

XOR	1	0
1	0	1
0	1	0

Иными словами, результат выполнения оператора XOR получает значение ИСТИНА тогда и только тогда, когда один из операндов имеет значение ИСТИНА, а другой - ЛОЖЬ. Именно это и является уникальным свойством оператора XOR - если вы выполните эту операцию на одним байтом, используя другой байт в качестве «ключа», а затем возьмете результат и выполните над ним ту же самую операцию с помощью того же самого ключа, вы снова получите исходный байт. Например:

Исходный байт		11011001
Ключ	XOR	01010011 (ключ)
Зашифрованный байт		10001010

Зашифрованный байт		10001010
Ключ	XOR	01010011 (ключ)
Расшифрованный байт		11011001

Расшифрованный байт равен исходному.

Этот процесс может использоваться для кодирования файлов, так как он решает две основные проблемы с простейшей версией на базе первого дополнения. Во-первых, благодаря использованию ключа, расшифровать файл, имея только программу декодирования нельзя. Во-вторых, используемые манипуляции с битами не настолько просты, чтобы их можно было сразу распознать.

Ключ не обязательно должен иметь длину 1 байт. Фактически, можно использовать ключ, состоящий из нескольких символов, и чередовать эти символы на протяжении всего файла.

Стандарт ГОСТ.

Официально ГОСТ называется «Алгоритм криптографического преобразования данных ГОСТ 28147-89» - это несколько шире, чем просто зашифровывание или расшифровка данных. Все режимы криптопреобразований данных, согласно ГОСТ, базируются на трех циклах алгоритма.

* цикл зашифровывания (32 - З)

* цикл расшифровки (32 - Р)

* цикл выработки имитоприставки (16 - З)

Прежде чем перейти к изучению основных вопросов, рассмотрим дополнительную информацию, используемую ГОСТом, - именно ее секретность обеспечивает секретность шифрованного сообщения. Эта информация представляет собой 2 массива данных - ключ и таблицу замен. Приведем их характеристики.

1. *Ключ* - это массив из 8-ми 32-битовых элементов, обозначаемых в дальнейшем X_i, где i изменяется от 0 до 7. Таким образом, размер ключа составляет 32×8=256 битов или 32 байта.

2. *Таблица замен* - двумерная таблица - набор из 8-ми одномерных массивов (узлов замен), каждый из которых содержит 16 различных 4-битовых чисел (от 0 до 15) в произвольном порядке. Обозначим $K_m(y)$ значение первого элемента в m-ом узле замен. При этом m изменяется в пределах 0...7, а y - в пределах 0...15. Таким образом, общий объем таблицы замен равен 8 узлов×16 элементов×4 бита/элемент = 512 битов = 64 байта.

Рассмотрим основной шаг криптопреобразования. На входе шага заданы два 32-битовых элемента данных - N_1, N_2, с этими элементами выполняются следующие манипуляции:

1) добавление к N_1 элемента ключа - сложение по модулю 2^{32};

2) поблочная замена результата по 4 бита по таблице замен;

3) циклический сдвиг результата на 11 битов влево;

4) побитовое сложение результата по модулю 2 с элементом N_2;

5) перестановка элементов N_2 <- старое, N_1 <- результат;

После этого новые элементы N_1 и N_2 выдаются в качестве результата шага. Так как в основном шаге используется только один элемент ключа, еще одним параметром шага является номер этого элемента.

Рассмотрим базовые циклы криптоалгоритма ГОСТа. Они отличаются друг от друга только числом повторений основного шага и порядком просмотра элементов ключа. В обозначении цикла nn-X первый элемент (nn) - это число повторений основного шага, а второй кодирует порядок просмотра элементов ключа (буква З - порядок зашифровывания, Р - расшифровки). Кроме того, в конце циклов шифрования предусмотрена дополнительная перестановка элементов. Приведем порядок использования элементов ключа для трех базовых циклов:

* цикл зашифровывания (32 - З) - 3 раза вперед, 1 раз назад:

0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,7,6,5,4,3,2,1,0

* цикл расшифровки (32 - Р) - 1 раз вперед, 3 раза назад:

0,1,2,3,4,5,6,7,7,6,5,4,3,2,1,0,7,6,5,4,3,2,1,0,7,6,5,4,3,2,1,0

* цикл выработки имитоприставки (16 - 3) - 2 раза вперед:

0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7

Каждый из циклов получает на входе 2 32-битовых слова и после серии основных шагов выдает в качестве результата также 2 32-битовых слова.

Основные режимы шифрования.

ГОСТ 28147-89 предусматривает три режима шифрования данных:

1) простая замена;

2) гаммирование;

3) гаммирование с обратной связью;

и дополнительный режим

4) выработка имитоприставки.

В любом из этих режимов данные обрабатываются блоками по 64 бита - именно поэтому ГОСТ относится к блочным шифрам. Кратко опишем основные режимы шифрования.

Простая замена.

Зашифровывание заключается в применении цикла 32-З к бокам открытого текста, расшифровка - в применении цикла 32-Р к блокам шифротекста. Это наиболее простой режим шифрования, и он имеет следующие недостатки:

* с точки зрения стойкости шифра, одинаковые блоки исходных данных дают одинаковые блоки шифротекста; криптологи говорят, что это очень плохо;

* с точки зрения удобства применения, если длина массива информации не кратна 8 байтам, то возникают 2 проблемы:

* чем и как дополнять последний блок до полных 8 байтов.

* после зашифровывания неполного блока в нем все 8 байт станут значащими, то есть вместе с шифротекстом надо хранить количество байтов в последнем блоке исходного текста.

ГОСТ ограничивает возможные случаи применения простой замены шифрованием ключевой информации (ключи и таблицы замен);

Гаммирование.

Этот режим заключается в наложении на открытые данные гаммы с помощью побитовой функции XOR. Зашифровывание и расшифровка в этом режиме не отличаются друг от друга. Блоки гаммы получаются зашифровыванием в режиме простой замены некоторой последовательности 64-битовых блоков, вырабатываемых датчиком псевдослучайных чисел. От этого датчика не требуется обеспечения никаких статистических характеристик

выходной последовательности, а нужен лишь максимально возможный период повторения данных.

Гаммирование с обратной связью.

Данный режим похож на режим гаммирования и отличается от него только тем, что для выработки блока гаммы для шифрования следующего блока данных используется блок шифротекста, полученный на предыдущем шаге. Этим достигается зацепление блоков - каждый блок при шифровании зависит от всех предыдущих.

Выработка имитоприставки к массиву данных.

Имитоприставка - это контрольная комбинация, зависящая от открытых данных и секретной ключевой информации. Цель использования имитоприставки - обнаружение всех изменений в массиве информации. Для потенциального взломщика две следующие задачи, если он не владеет секретным ключом, практически неразрешимы:

* вычисление имитоприставки для заданного открытого массива информации;

* подбор открытых данных под заданную имитоприставку.

Метод замены.

$Y_i = (X_i + C) \bmod N,$

где X_i – номер i – го символа шифруемого текста в исходном алфавите; C – некоторая константа; N – количество символов в исходном алфавите; Y_i – номер i – го символа зашифрованного текста в исходном алфавите.

Метод перестановки.

$Y_i = (X_i)$,

где X_i – номер i – го символа шифруемого текста в исходном алфавите; Y_i – номер i – го символа зашифрованного текста в “случайном” алфавите.

Полиалфавитный метод замены.

Отличается от предыдущего наличием нескольких “случайных” алфавитов. Переключение между ними происходит по нахождению в исходном тексте определенного (заранее заданного) символа или нескольких символов.

Метод Виженера.

$Y_i = (X_i + K_i) \bmod N,$

где X_i – номер i – го символа шифруемого текста в исходном алфавите; K_i – номер i – го символа ключа в исходном алфавите; N – количество символов в исходном алфавите; Y_i – номер i – го символа зашифрованного текста в исходном алфавите.

Метод XOR.

$Y_i = X_i \text{ xor } K_i$,

где X_i – номер i – го символа шифруемого текста в исходном алфавите; K_i – номер i – го символа ключа в исходном алфавите; Y_i – номер i – го символа зашифрованного текста в исходном алфавите.

Лабораторное задание:

На одном из языков высокого уровня реализовать один из шифров битовых манипуляций.

Методические указания по подготовке и защите отчета

По каждому выполненному заданию необходимо подготовить отчет о выполненной работе, содержащий: титульный лист (с указанием названия работы); постановку задачи, цель работы, требования к результатам и т.п.; ход выполнения работы; полученные результаты в работе; выводы обучающегося о проделанной работе.

Подготовка отчета по выполненному заданию

При оформлении работы необходимо руководствоваться следующим:

1. отчет оформляется на ПК с использованием текстового редактора MS Word; при отсутствии ПК (в порядке исключения) по согласованию с преподавателем работа может быть принята в рукописном виде;
2. объем отчет не должен превышать 10 страниц машинописного текста (не включая приложений):
   - Формат страницы А4 (210*297 мм).
   - Поля: слева 30 мм, сверху и снизу 20 мм, справа 10 мм.
   - Шрифт: Times New Roman, размер — 14 пунктов.
   - Межстрочный интервал — 1,5
3. страницы должны быть пронумерованы;
4. каждую структурную часть работы следует начинать с нового листа; точку в конце заголовка структурной части работы не ставят;
5. необходимо стремиться к ясности, краткости и самостоятельности изложения материала;
6. каждая цитата, заимствованные цифры и факты должны сопровождаться ссылкой на источник, описание которого приводится в списке использованной литературы (в ссылке указывается номер источника по списку, например, [2]);
7. в тексте отчета не должно быть сокращений слов, за исключением общепринятых;
8. при представлении табличного материала над правым верхним углом таблицы помещают надпись «Таблица» с указанием ее порядкового номера (например, «Таблица 5»), снабжают тематическим заголовком, который располагают посередине страницы и пишут с прописной буквы без точки в конце;
9. приводимые в отчете иллюстрации (диаграмма, график, технический рисунок, фотография, скриншот) должны быть выполнены четко, аккуратно, разборчиво и иметь номер и подрисуночную подпись (например, Рисунок 4 - Окно надстройки «Поиск решения»);
10. табличному и графическому материалу по тексту необходимо давать пояснения и делать к таблицам и иллюстрациям ссылки, содержащие порядковые номера, под которыми они помещены в отчете;
11. отчет представляется в сброшюрованном виде и с титульным листом (листы должны быть скреплены по левому краю).

Контроль знаний и навыков и уровня освоения компетенций

Защита отчета позволяет выявить уровень знаний обучающегося по выбранной теме, степень его самостоятельности в выполнении работы. Защита проводится в компьютерном классе с демонстрацией фрагментов работы на ПК.

Заключительный этап

Результаты защиты отчета оцениваются на «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Критериями оценивания результатов работы обучающихся являются:
- уровень освоения учебного материала;
- уровень умения использовать теоретические знания при выполнении практических задач;
- уровень сформированности умений;
- уровень умения активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения материала;
- оформление материала в соответствии с требованиями стандарта предприятия;
- уровень умения ориентироваться в потоке информации, выделять главное;
- уровень умения четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- уровень умения определить, проанализировать альтернативные возможности, варианты действий;
- уровень умения сформулировать собственную позицию, оценку и аргументировать ее.

Отчет и демонстрация оцениваются по системе:
- Оценка «отлично» выставляется за отчет и демонстрацию, которые носят исследовательский характер, содержит грамотно изложенный материал, с соответствующими обоснованными выводами.
- Оценка «хорошо» выставляется за грамотно выполненный во всех отношениях отчет и демонстрацию при наличии небольших недочетов в их содержании или оформлении.
- Оценка «удовлетворительно» выставляется за отчет, который удовлетворяет всем предъявляемым требованиям, но отличается поверхностью, в нем просматривается непоследовательность изложения материала, представлены необоснованные выводы.
- Оценка «неудовлетворительно» выставляется за отчет, который не носит исследовательского характера, не содержит анализа источников и подходов по выбранной теме, выводы носят декларативный характер.

Самостоятельная работа. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская работа обучающихся, выполняемая вне занятий по заданию и при управлении преподавателем, но без его непосредственного участия.

Самостоятельная работа проводится с целью:
- систематизации и закрепления полученных теоретических знаний и практических умений обучающихся;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации;
- формирования общих и профессиональных компетенций
- развитию исследовательских умений.

Структура и содержание самостоятельной работы

№ п/п	Наименование раздела / темы дисциплины	Темы самостоятельной работы	Содержание самостоятельной работы	Форма контроля
1	Информационная безопасность и уровни ее обеспечения.	Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности. Информационные, программно-математические, физические и организационные угрозы. Методы и средства противодействия им	Основные аспекты информационной безопасности. Основные концептуальные положения системы защиты информации. Концептуальная модель информационной безопасности. Угрозы конфиденциальной информации. Действия, приводящие к неправомерному овладению конфиденциальной информацией Постановка задачи программно-технического обеспечения информационной безопасности. Направления обеспечения безопасности: правовая защита, организационная защита, инженерно-техническая защита. Инженерно-техническая защита: физические средства защиты, аппаратные средства защиты, программные средства защиты. Основные направления использования программной защиты информации	Реферат
2	Компьютерные вирусы и защита от них.	Криптографическая защита. Проблема вирусного заражения программ	Шифрование. Требования к системам криптографической защиты. Способы шифрования. Проверка подлинности. Проверка целостности сообщений. Шифры замены и перестановки.	Реферат
3	Информационная безопасность вычислительных сетей.	Безопасность в компьютерных сетях	Сетевые соединения. Постоянные соединения. Соединения удаленного доступа. Защита от	Реферат

№ п/п	Наименование раздела / темы дисциплины	Темы самостоятельной работы	Содержание самостоятельной работы	Форма контроля
			вредоносного кода. Аутентификация. Отслеживание. Аудит. Обнаружение вторжений. Шифрование. Обновление систем. Резервное копирование и восстановление. Физическая безопасность. Физический доступ. Климатические условия. Защита от пожара. Электроэнергия. Рекомендации по обеспечению сетевой безопасности. Определение типов межсетевых экранов. Определение виртуальных частных сетей.	
4	Механизмы обеспечения "информационной безопасности".	Защита от несанкционированного доступа, модели и основные принципы защиты информации.	Задача управления доступом. Защита от копирования. Защита информации от разрушения. Программная защита информации. Криптографические средства защиты. Способы защиты информации. Характеристика защитных действий.	Реферат
5	Информационная безопасность при использовании Internet.	Программно-аппаратные средства защиты информации	Программно-технические меры обеспечения ИБ. Особенности современных ИС. Обеспечение информационной безопасности. Подсистемы системы информационной безопасности. Наборы подсистем защиты. Функциональные подсистемы защиты. Идентификация и аутентификация. Парольная аутентификация. Аутентификация Kerberos. Использование биометрических данных. Управление доступом. Ролевое управление. Протоколирование и аудит. Экранирование. Программные закладки.	Реферат

№ п/п	Наименование раздела / темы дисциплины	Темы самостоятельной работы	Содержание самостоятельной работы	Форма контроля
			Компьютерные вирусы. Защита от вируса. Профилактика заражения компьютерными вирусами. Обзор антивирусных средств	
6	Безопасность операционных систем.	Безопасность операционных систем	Безопасность UNIX. Вопросы безопасности Windows 2000/ Windows 2003 Server	Реферат

Выбранная тема обязательно согласуется с преподавателем.

Методические рекомендации по выполнению реферата, презентации и устного сообщения

Самостоятельная работа в форме реферата является индивидуальной самостоятельно выполненной работой обучающегося.

Реферат, как правило, должен содержать следующие структурные элементы:
1. титульный лист;
2. содержание;
3. введение (1-2 стр.);
4. основная часть (10-20 стр.);
5. заключение (1-2 стр.);
6. список использованных источников (не менее 5 наименований);
7. приложения (при необходимости).

В содержании приводятся наименования структурных частей реферата, глав и параграфов его основной части с указанием номера страницы, с которой начинается соответствующая часть, глава, параграф.

Во введении дается общая характеристика реферата: обосновывается актуальность выбранной темы; определяется цель работы и задачи, подлежащие решению для её достижения; описываются объект и предмет исследования, информационная база исследования, а также кратко характеризуется структура реферата по главам.

Основная часть должна содержать материал, необходимый для достижения поставленной цели и задач, решаемых в процессе выполнения реферата. Она включает 2-3 главы, каждая из которых, в свою очередь, делится на 2-3 параграфа. Содержание основной части должно точно соответствовать теме проекта и полностью её раскрывать. Главы и параграфы реферата должны раскрывать описание решения поставленных во введении задач. Поэтому заголовки глав и параграфов, как правило, должны соответствовать по своей сути формулировкам задач реферата.

Главы основной части реферата могут носить теоретический, методологический и аналитический характер.

Обязательным для реферата является логическая связь между главами и последовательное развитие основной темы на протяжении всей работы, самостоятельное изложение материала, аргументированность выводов. Также обязательным является наличие в основной части реферата ссылок на использованные источники.

Изложение необходимо вести от третьего лица («Автор полагает...») либо использовать безличные конструкции и неопределенно-личные предложения («На втором этапе исследуются следующие подходы…», «Проведенное исследование позволило доказать...» и т.п.).

В заключении логически последовательно излагаются выводы, к которым пришел обучающийся в результате выполнения реферата. Заключение должно кратко характеризовать решение всех поставленных во введении задач и достижение цели реферата.

Список использованных источников является составной частью работы и отражает степень изученности рассматриваемой проблемы. Количество источников в списке определяется обучающимся самостоятельно, для реферата их рекомендуемое количество от 5 до 10. При этом в списке обязательно должны присутствовать источники, изданные в последние 5 лет, а также ныне действующие нормативно-правовые акты, регулирующие отношения, рассматриваемые в реферате.

В приложения следует относить вспомогательный материал, который при включении в основную часть работы загромождает текст (таблицы вспомогательных данных, инструкции, методики, формы документов и т.п.).

Реферат оформляется в печатном виде на листах формата А4. Рекомендуется использовать шрифт Times New Roman, размер шрифта - 14, межстрочный интервал - 1,5. Текст следует располагать на одной стороне листа, с полями шириной 2,5 см слева, 1 см справа, 2 см сверху и снизу. Листы должны быть последовательно пронумерованы, каждый параграф в тексте должен иметь заголовок в соответствии с содержанием.

В тексте не следует использовать сокращения, все условные обозначения и термины должны быть предварительно пояснены.

Оформление является важной и оцениваемой частью контрольной работы. Контрольная работа, оформленная неаккуратно, либо с отступлениями от перечисленных требований, возвращается на доработку.

Список использованных источников должен формироваться в алфавитном порядке по фамилии авторов. Литература обычно группируется в списке в такой последовательности:

1. законодательные и нормативно-методические документы и материалы;
2. специальная научная отечественная и зарубежная литература (монографии, учебники, научные статьи и т.п.);
3. статистические, инструктивные и отчетные материалы предприятий, организаций и учреждений.

Включенная в список литература нумеруется сплошным порядком от первого до последнего названия.

По каждому литературному источнику указывается: автор (или группа авторов), полное название книги или статьи, место и наименование издательства (для книг и брошюр), год издания; для журнальных статей указывается наименование журнала, год выпуска и номер. По сборникам трудов (статей) указывается автор статьи, ее название и далее название книги (сборника) и ее выходные данные.

Приложения следует оформлять как продолжение реферата на его последующих страницах. Каждое приложение должно начинаться с новой страницы. Вверху страницы справа указывается слово «Приложение» и его номер. Приложение должно иметь заголовок, который располагается по центру листа отдельной строкой и печатается прописными буквами. Приложения следует нумеровать порядковой нумерацией арабскими цифрами. На все приложения в тексте работы должны быть ссылки. Располагать приложения следует в порядке появления ссылок на них в тексте.

Регламент устного публичного выступления – не более 10 минут.

Любое устное выступление должно удовлетворять *трем основным критериям*, которые в конечном итоге и приводят к успеху: это критерий правильности, т.е. соответствия языковым нормам, критерий смысловой адекватности, т.е. соответствия содержания выступления реальности, и критерий эффективности, т.е. соответствия достигнутых результатов поставленной цели.

Работу по подготовке устного выступления можно разделить на два основных этапа: докоммуникативный этап (подготовка выступления) и коммуникативный этап (взаимодействие с аудиторией).

Работа по подготовке устного выступления начинается с формулировки темы. Лучше всего тему сформулировать таким образом, чтобы ее первое слово обозначало наименование полученного в ходе выполнения проекта научного результата (например, «Технология изготовления…», «Модель развития…», «Система управления…», «Методика выявления…» и пр.). Тема выступления не должна быть перегруженной, нельзя «объять необъятное», охват большого количества вопросов приведет к их беглому перечислению, к декларативности вместо глубокого анализа. Неудачные формулировки - слишком длинные или слишком краткие и общие, очень банальные и скучные, не содержащие проблемы, оторванные от дальнейшего текста и т.д.

Само выступление должно состоять из трех частей – вступления (10-15% общего времени), основной части (60-70%) и заключения (20-25%).

При подготовке к выступлению необходимо выбрать способ выступления: устное изложение с опорой на конспект (опорой могут также служить заранее подготовленные слайды) или чтение подготовленного текста. Отметим, однако, что чтение заранее написанного текста значительно уменьшает влияние выступления на аудиторию. Запоминание написанного текста заметно сковывает выступающего и привязывает к заранее составленному плану, не давая возможности откликаться на реакцию аудитории.
Во время выступления важно постоянно контролировать реакцию слушателей. Внимательность и наблюдательность в сочетании с опытом позволяют оратору уловить настроение публики. Возможно, рассмотрение некоторых вопросов придется сократить или вовсе отказаться от них. Часто удачная шутка может разрядить атмосферу.

После выступления нужно быть готовым к ответам на возникшие у аудитории вопросы.
Компьютерную презентацию, сопровождающую выступление докладчика, удобнее всего

подготовить в программе MS PowerPoint. Презентация как документ представляет собой последовательность сменяющих друг друга слайдов - то есть электронных страничек, занимающих весь экран монитора (без присутствия панелей программы). Чаще всего демонстрация презентации проецируется на большом экране, реже – раздается собравшимся как печатный материал. Количество слайдов адекватно содержанию и продолжительности выступления (например, для 5-минутного выступления рекомендуется использовать не более 10 слайдов).

На первом слайде обязательно представляется тема выступления и сведения об авторах.

На слайды помещается фактический материал (таблицы, графики, фотографии и пр.), который является уместным и достаточным средством наглядности, помогает в раскрытии стержневой идеи выступления. В этом случае к слайдам предъявляются следующие требования:

- выбранные средства визуализации информации (таблицы, схемы, графики и т. д.) соответствуют содержанию;
- использованы иллюстрации хорошего качества (высокого разрешения), с четким изображением (как правило, никто из присутствующих не заинтересован вчитываться в текст на ваших слайдах и всматриваться в мелкие иллюстрации).

Максимальное количество графической информации на одном слайде – 2 рисунка (фотографии, схемы и т.д.) с текстовыми комментариями (не более 2 строк к каждому). Наиболее важная информация должна располагаться в центре экрана.

Критерии оценивания результатов самостоятельной работы

Критериями оценивания результатов самостоятельной работы обучающихся являются:
- уровень освоения учебного материала;
- уровень умения использовать теоретические знания при выполнении практических задач;
- уровень сформированности умений;
- уровень умения активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения материала;
- оформление материала в соответствии с требованиями стандарта предприятия;
- уровень умения ориентироваться в потоке информации, выделять главное;
- уровень умения четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- уровень умения определить, проанализировать альтернативные возможности, варианты действий;
- уровень умения сформулировать собственную позицию, оценку и аргументировать ее.

Реферат, презентация и доклад оцениваются по системе:
- Оценка «отлично» выставляется за реферат, презентацию и выступление, которые носят исследовательский характер, содержит грамотно изложенный материал, с соответствующими обоснованными выводами.
- Оценка «хорошо» выставляется за грамотно выполненный во всех отношениях реферат, презентацию и выступление при наличии небольших недочетов в их содержании или оформлении.
- Оценка «удовлетворительно» выставляется за реферат, который удовлетворяет всем

предъявляемым требованиям, но отличается поверхностью, в нем просматривается непоследовательность изложения материала, представлены необоснованные выводы.
- Оценка «неудовлетворительно» выставляется за реферат, который не носит исследовательского характера, не содержит анализа источников и подходов по выбранной теме, выводы носят декларативный характер.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

1. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. - М. : ДМК Пресс, 2010. - 544 с. : ил. - http://www.book.ru
2. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft/ СА. Нестеров - М.: Национальный Открытый Университет "ИНТУИТ", 2009, 375 с. - http://www.knigafund.ru/books/173009
3. Гончарук С.В. Администрирование ОС Linux/ С.В. Гончарук - М.: Национальный Открытый Университет "ИНТУИТ", 2011, 170 с. - http://www.knigafund.ru/books/173018
4. Перетолчин А.С. Защита Windows от сбоев [Текст] / А. С. Перетолчин. — Новосибирск: Сиб. унив. изд-во, 2008. — 108 с. - http://www.knigafund.ru/books/17225
5. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. - http://znanium.com/bookread2.php?book=495249

Дополнительная литература

	Автор	Название	Издательство
1	Гладких Т.В., Воронова Е.В.	Разработка функциональных информационных подсистем организации: учебное пособие	ВГУИТ, 2014, 68 с.
2	Александров Д.В.	Инструментальные средства информационного менеджмента. CASE-технологии и распределенные информационные системы	Финансы и статистика, 2011
3	Бабаш А.В.	Информационная безопасность. Практикум. Учебное пособие для бакалавров	КноРус, 2013
4	Дейтел П.Дж.	Операционные системы. Распределенные системы, сети, безопасность	Бином, 2013
5	Джоханссон Дж. М.	Обеспечение безопасности. Ресурсы Windows Server 2008	БХВ-Петербург, 2012
6	Дукин А.Н.	Самоучитель Visual Basic 2010	БХВ-Петербург, 2010
7	Дунаев В. В.	Базы данных. Язык SQL	СПб.:БВХ-Петербург, 2006
8	Дунаев В.В.	Web-программирование для всех	БХВ-Петербург, 2012
9	Голенищев Э. П.	Информационное обеспечение систем управления	Ростов н/Д:Феникс, 2010
10	Зиборов В.	Visual Basic 2012 на примерах	БХВ-Петербург, 2013
11	Ивасенко А. Г.	Информационные технологии в	М.:КНОРУС, 2010

	Автор	Название	Издательство
		экономике и управлении	
12	Корячко В.П.	Корпоративные сети: технологии, протоколы, алгоритмы	Горячая линия - Телеком, 2011
13	Майо Дж.	Microsoft Visual Studio 2010	БХВ-Петербург, 2011
14	Олейник П.П.	Корпоративные информационные системы	Питер, 2012
15	Чипига А.Ф.	Информационная безопасность автоматизированных систем. Учебное пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности	Гелиос АРВ, 2010

Ресурсы информационно-телекоммуникационной сети «Интернет»

№ п/п	Источник
1	http://www.microsoft.com
2	http://msdn.microsoft.com
3	http://www.knigafund.ru
4	http://znanium.com

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине

Реализация программы предполагает наличие следующего программного обеспечения:

- Операционной системы Windows;
- Пакета прикладных программ Microsoft Office;
- Инструментальной среды разработки Visual Studio.

Учебное издание

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ ЗАДАНИЙ И САМОСТОЯТЕЛЬНОЙ РАБОТЕ

по дисциплине Информационная безопасность

для обучающихся по направлению 09.03.03 «Прикладная информатика»
профиль «Прикладная информатика в экономике»

Составитель:
Степанов Леонид Викторович

В авторской редакции

Подписано в печать 11.01.2016. Формат 60×84/16
АОНО ВО «Институт менеджмента, маркетинга и финансов»
394030, Воронеж, ул. Карала Маркса, 67
www.immf.ru