Гафарова Елена Аркадьевна

Программно-аппаратные средства обеспечения информационной безопасности. Практикум.

Учебное пособие

Челябинск, 2021

УДК: 004.056

ББК: 32.97

Г24

Гафарова, Е.А. Программно-аппаратные средства обеспечения информационной безопасности. Практикум. [Текст]: Учебное пособие / Е.А. Гафарова – 180 с.

ISBN 978-5-93162-539-3

Учебное пособие предназначено для организации практических занятий, лабораторных работ и самостоятельной работы магистров направления 44.04.04 «Профессиональное обучение (по отраслям)», профильной направленности «Управление информационной безопасностью в профессиональном образовании» по дисциплине «Программно-аппаратное обеспечение информационной безопасности». Учебное пособие содержит необходимые сведения для получения практических навыков по применению программно-аппаратных средств обеспечения информационной безопасности и состоит из 9 лабораторных работ 8 самостоятельных работ.

Задания, представленные в практикуме, позволяют ознакомиться с методами и средствами защиты информационных систем, подсистем безопасности, а также получить навыки использования программно-аппаратных средств обеспечения безопасности информационных систем.

Рецензент:

Диденко Галина Александровна, кандидат педагогических наук, доцент ФГБОУ ВО «ЮУГМУ Минздрава России»

ISBN 978-5-93162-539-3

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Анализ существующих программ магистерской подготовки в области информационной безопасности показывает, что возможны различные варианты формирования профессиональных компетенций образовательной области «Информационная безопасность».

Приказом Министерства образования и науки РФ от 1 декабря 2016 г. № 1513 «Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры)» определены требования государства в этой области, в связи с чем, содержание существующих магистерских программ требует своевременного осмысления, актуализированного наполнения при условии оптимальной преемственности между ступенями высшего образования – бакалавриата и магистратуры.

Дисциплина «Программно-аппаратное обеспечение информационной безопасности» является одной из базовой дисциплин в профессиональной подготовке магистров направления «Управление информационной безопасности в профессиональном обучении».

При изучении дисциплины магистранты формируют компетенции, необходимые для выполнения следующих видов деятельности:

- организация работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации (ФСБ РФ), Федеральной службы но техническому и экспортному контролю Российской Федерации (ФСТЭК РФ);
- организация и выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;
- аттестация объектов информатизации по требованиям безопасности информации.

Изучение дисциплины «Программно-аппаратное обеспечение информационной безопасности» основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин предметной подготовки: «Информатика», «Информационные технологии», «Технические средства информатизации», «Основы информационной безопасности» и других.

Дисциплина «Программно-аппаратное обеспечение информационной безопасности» формирует знания, умения и компетенции, необходимые для освоения следующих дисциплин: «Проектирование и модернизация учебных мастерских, лабораторий и классов», «Проектирование и мониторинг образовательных результатов», «Технологии свободно распространяемого программного обеспечения», «Цифровизация и квалиметрическая оценка учебных достижений в образовательной организации», «ЭИОС организаций профессионального образования» и других.

Цель изучения дисциплины: формирование у студентов системы теоретических знаний и практических навыков, необходимых для совершенствования управления информационной безопасностью в аспекте применения программно-аппаратных средств

Задачи дисциплины:

1) дать студентам знания сущность информационной безопасности, правовые нормы, регламентирующие ее реализацию; понятие и современное состояние средств информационной защиты; понятие семиуровневой системы обеспечения информационной безопасности; компоненты программно-аппаратных средств обеспечения информационной защиты; системы оценки информационной защищенности

2) научить студентов давать оценку защищенности информационной системе; применять на практике программно-аппаратные средства обеспечения информационной безопасности;

3) научить будущих специалистов по управлению информационной безопасностью выстраивать комплексную систему защиты информации по принципу разумной достаточности.

Значимость дисциплины обусловлена применением полученных знаний в дальнейшей исследовательской работе, при подготовке и защите магистерской диссертации, в будущей профессиональной деятельности.

Для формирования профессиональных компетенций магистранту необходимо предложить различные виды практических работ.

Практические занятия проводятся с целью закрепления и углубления теоретических знаний, полученных обучающимися на лекциях и в ходе самостоятельной работы.

Настоящее учебное пособие предназначено для проведения практических лабораторных работ магистрантов направления «Управление информационной безопасности в профессиональном обучении», а также для организации самостоятельной работы студентов по дисциплине.

Отдельные учебные материалы могут быть использованы для организации занятий у студентов – бакалавров направления «Профессиональное обучение (по отраслям)» профильной направленности «Информатика и вычислительная техника» и «Правоведение и правоохранительная деятельность».

Раздел 1. Основные средства и методы программно-аппаратной защиты информации.

Лабораторная работа №1: Установление пароля на текстовый документ, архивирование документов и установление пароля на архив, установление пароля на папку.

Цель: научиться ставить пароли на документы в разных форматов.

Теоретические сведения.

В документах MS Office предусмотрено несколько уровней защиты, позволяющих управлять доступом к данным и их изменением.

Просмотр документов MS Word, книг MS Excel и баз данных MS Access может быть ограничен с помощью парольной защиты (пароль для открытия файла). При установке пароля на открытие документа содержимое файла шифруется (алгоритм шифрования AES).

Для документов MS Word и MS Excel также имеется возможность установки парольной защиты на сохранение внесенных изменений (пароль разрешения записи). Если пользователю не известен пароль разрешения записи, он может открыть документ в режиме «только для чтения». В этом случае возможно внесение изменений в текст документа, однако нельзя сохранить измененный файл документа под старым именем. Для сохранения изменений требуется ввести новое имя файла.

Пароль на открытие, пароль разрешения записи устанав-лива-ются на файл, то есть относятся к документу/книге в целом.

Кроме паролей на файл в целом, имеются возможности защиты отдельных элементов документов MS Office:

Парольная защита от просмотра элементов книги Excel (строк, столбцов, листов). Невозможно защитить от просмотра часть документа MS Word, отдельные ячейки книги MS Excel;

Парольная защита от изменения частей (разделов) документа Word, содержимого отдельных ячеек и их диапазонов в Excel, структуры листа (вставка, удаление и форматирование строк и столбцов),структуры книги (добавление и удаление листов, отображение, скрытые листов), изменение размеров, положения или видимости окна, настроенного для отображения книги Excel.

Разграничение доступа (возможность изменения) к диапазонам ячеек Excel для локальных и сетевых пользователей ОС Windows;

Разграничение доступа аутентифицированных пользователей к фрагментам текста MS Word, задание ограничений на несанкционированное распространение документа (пересылка по электронной почте, изменение, копирование) требует установки дополнительного программного обеспечения (сервера аутентификации, WRM – клиента управления правами Windows).

Следует учитывать, что функциональные возможности парольной защиты на отдельные элементы MS Excel (скрытие данных и защита листов и книг) и MS Word (защита разделов) не предназначены для защиты данных или важных сведений в документах MS Office.

Они используются для более понятного представления сведений, скрывая сведения или формулы, которые могут сбить с толку некоторых пользователей. Эти средства служат также для предотвращения случайного изменения данных пользователями. Скрытые или защищенные паролем данные внутри документов MS Office не шифруются. При определенных усилиях и наличии времени пользователи смогут просмотреть и изменить все сведения внутри документа MS Office, если они имеют доступ к самому документу (пароль на открытие документа не установлен или известен). Чтобы предотвратить изменение данных и обеспечить безопасность важных сведений, следует ограничить доступ к файлам (пароль на открытие файла), содержащим подобные сведения, сохранив их в расположениях, доступных только пользователям, прошедшим аутентификацию (разграничение доступа к файлам и папкам средствами ОС).

В документах MS Office имеется возможность заверять цифровой подписью как документ в целом, так и внедренный в документ код макросов на языке VBA. Наличие действительной цифровой подписи гарантирует целостность (неизменность) содержимого, а также аутентичность и неотрекаемость (подлинность авторства и невозможность отказа от авторства).

Полноценная проверка подлинности цифровых подписей возможна в том случае, если они выданы сетевым сервером аутентификации (в домене локальной сети), либо доверенным центром сертификации в Интернете. Если же используется локальный сертификат, создаваемый самим пользователем с помощью утилиты selfcert.exe (Digital Certificate for VBA Projects, Цифровой сертификат для проектов VBA), то проверить на другом компьютере подлинность подписи, созданной с его помощью, будет невозможно.

Один из самых простых, но в то же время надежных способов защиты своих документов – это установить пароль на документ Microsoft Word, причем можно установить пароль как и на открытие документа MS Word, так и на изменение содержимого документа.

Ход работы

Для того чтобы установить пароль для своего документа Microsoft Word, нужно выполнить следующее действие Сервис/Параметры… (см. рисунок 1).

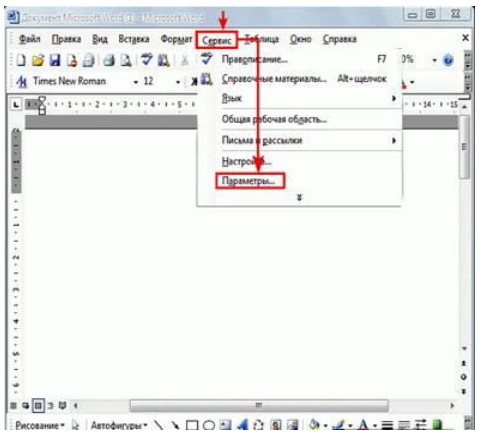


Рисунок 1 – Меню Сервис MS Word

После выполнения всех действий появится окно Microsoft Word – Параметры. В этом окне Microsoft Word - Параметры нужно перейти на закладку Безопасность (см. рисунок 2); далее в строке «пароль для открытия файла» ввести пароль. После ввода пароля нажмите кнопку ОК.

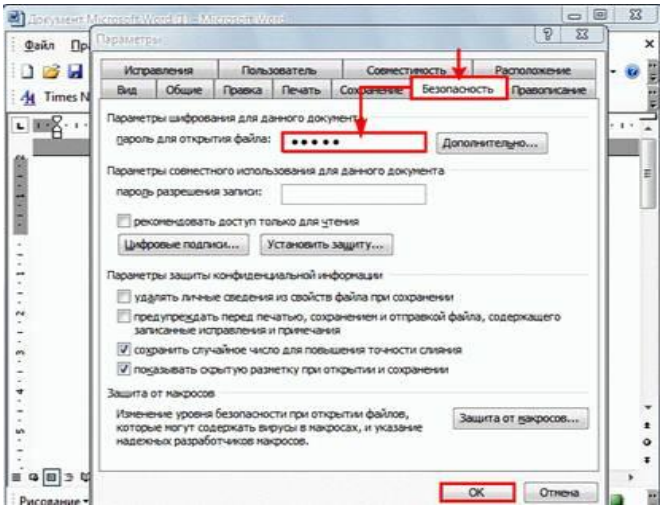


Рисунок 2 – Меню Безопасность MS Word

Для безопасности документа Microsoft Excel можно установить свой пароль на открытие документа. После того как вы установили пароль на открытие документа Microsoft Excel, Excel будет требовать пароль на открытие вашего документа.

Для того чтобы установить пароль для своего документа Microsoft Excel, нужно выполнить следующее действие Сервис/Параметры… (см. рисунок 3).

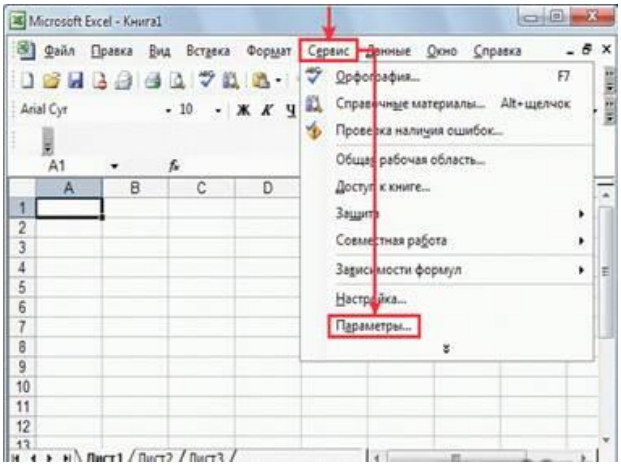


Рисунок 3 – Меню Сервис MS Excel

В этом окне Microsoft Excel – Параметры нужно перейти на закладку Безопасность(см. рисунок 4) далее в строке «пароль для открытия» ввести пароль. После ввода пароля нажмите кнопку ОК.

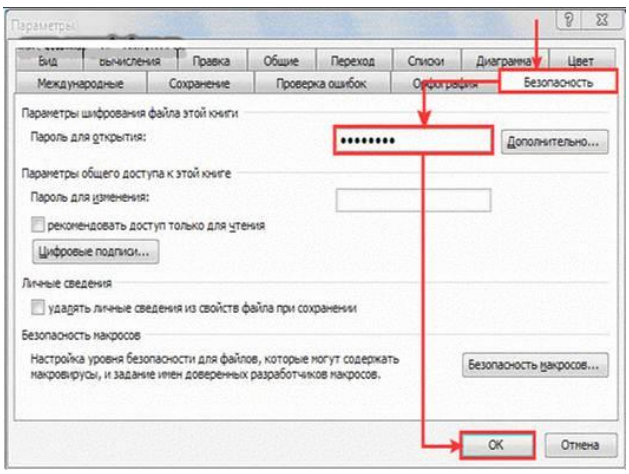


Рисунок 4 – Меню Безопасность MS Excel

После нажатия кнопки ОК появится окошко Microsoft Excel – «Подтверждения пароля», здесь вам нужно будет еще раз ввести пароль, который вы вводили, и нажать кнопку ОК (см. рисунок 5).

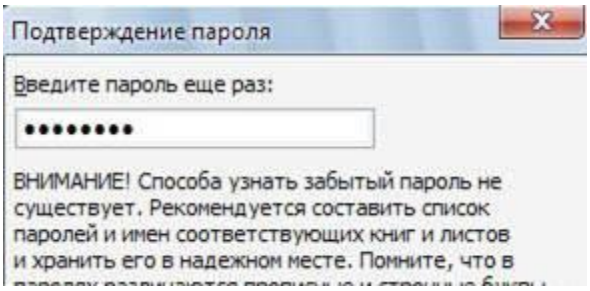


Рисунок 5 – Меню Подтверждение пароля MS Excel

При установке пароля стоит помнить об очень важных моментах. Пароль можно «сломать». Для этого есть немало программ. Особенно легко «взламывать» короткие пароли. Поэтому желательно чтобы пароль был сложный. Лучше всего, чтобы пароль состоял как из латиницы, так и из кириллицы. Для надежности можно добавить еще несколько цифр. Желательно использовать пароль минимум из семи символов. Чем сложнее пароль, тем меньше шансов, что он будет «взломан». Но также не нужно слишком усердствовать, так как можно этот пароль забыть и самому. А еще лучше пароль записать и хранить в надежном месте, на случай если вы его

забудете. Также для дополнительной защиты можно заархивировать документ и установить пароль к архиву. Тогда вероятность того, что кому-либо удастся сломать защиту, становится крайне низкой.

Чтобы установить пароль для защиты базы данных MS Access:

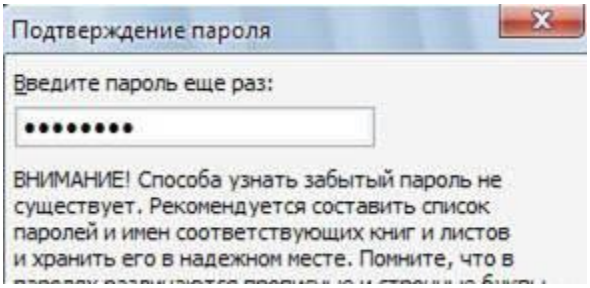


Рисунок 6 – Меню Задание пароля базы данных MS Access

- в появившемся диалоговом окне введите в поле Пароль пароль для защиты базы данных с учетом регистра символов;

- введите пароль еще раз в поле Подтверждение;

- нажмите кнопку ОК.

Теперь база данных защищена паролем, и всякий раз, когда пользователь будет открывать базу данных, будет отображаться диалоговое окно с требованием ввести пароль. Запомните или сохраните пароль в надежном месте. Если вы забудете пароль, базу данных будет невозможно открыть**.**

Содержание отчета: тема, цель, скриншоты основных этапов работы, защищенные объекты.

Контрольные вопросы:

1. Чем различается действие защиты от изменения текста документа, установленной с помощью защиты форм (команда Защитить документ) и защиты в режиме «только для чтения» (установка на файл пароля разрешения записи)?

2. Чем различается действие защиты от изменения в случае задания пароля разрешения записи и в случае рекомендации открытия документа в режиме «только для чтения»?

Задание для самостоятельного выполнения – самостоятельная работа №1.

В приложении MS Word создайте короткий опросник (анкету) с защищенным от изменения текстом вопросов для получения от пользователей различных данных. Сформулировать вопросы так, чтобы требовались:

- ответы в произвольной форме, подразумевающие ввод текста, (например, ФИО, какие-либо комментарии или пожелания, номер учебной группы, дата заполнения),
- выбор даты (дата дня рождения, начала сессии, рекомендуемая дата мероприятия или посещения и т.п.),
- выбор единственного варианта ответа из списка и с помощью переключателей (например, пол, возрастная группа, форма обучения, специальность),
- выбор нескольких вариантов с помощью флажков (например, знания, предпочтения, сферы интересов, участие в мероприятиях и т.п.)

Для вставки в документ флажков и переключателей используйте инструменты из предыдущих версий Word – кнопка на вкладке Разработчик.

Содержание отчета: выполненное задание для самостоятельной работы и ответы на контрольные вопросы необходимо представить для проверки преподавателю.

Лабораторная работа №2: Изучение настроек Ethernet и способов анализа трафика на сетевых интерфейсах в ОС Windows.

Цели работы: ознакомиться с настройками сетевой платы и встроенными инструментальными средствами ОС MS Windows анализа трафика на сетевых интерфейсах.

Теоретические сведения

Правильная настройка сетевой платы позволяет не только обеспечить соединение с сеть, но улучшить производительность сетевого подключения и получить необходимое качество сервиса предоставляемой локальной сетью.

Для просмотра состояния взаимодействия компьютера с локальной сетью различные разработчики операционных систем представляют средства диагностик.

Средства диагностики могут быть графическими или использовать командную строку (так называемый CLI - Command lininterface). Диагностика с помощью CLI позволяет создавать скрипты или программы для включения их в приложения занимающиеся мониторингом или анализом сети в целом.

В данной работе необходимы следующие понятия:

- **Скрипт (script)** - небольшая программа для выполнения средствами операционной системы и для расширения ее возможностей
- **Loopback** (обратная, возвратная петля) Тип диагностического интерфейса, при котором сигнал возвращается передающему устройству, пройдя по коммуникационному каналу в обоих направлениях.
- **GUI** - (Graphical User Interface) графический пользовательский интерфейс
- **CLI** - (Command Line Interface) Интерфейс командной строки, в котором инструкции компьютеру даются только путём ввода с клавиатуры текстовых строк (команд). Также известен под названием консоль.
- **MMC** (Microsoft Management Console) -средство для создания, сохранения и открытия средств администрирования (называемых консолями

MMC), которые управляют оборудованием, программными и сетевыми компонентами операционной системы Windows.

Ход работы

Для выполнения лабораторной работы достаточно одного компьютера без подключения к какой-либо сети.

1. Описать свойства сетевой платы

Выполнить в следующей последовательности доступ к настройкам сетевой платы: Пуск - панель управления - подключение к локальной сети (сетевые подключения) – вызов контекстного меню- свойства- настроить.

Сохранить в отчет все свойства сетевой интерфейса виде таблицы 1.

Таблица 1 Свойства сетевой платы

Свойство	Установленное значение	Возможные значение
Скорость и дуплекс	Автосогласование	От 10Мбит/с дуплекс…до 100Мбит/с полудуплекс
Wake Up Capabilities Magic packet	None,	Wake Up Frame, Both,

2. Изучить возможность консоли управления MMC по встроенной справке (Консоль - действия – справка). Кратко отразить полученные сведения в отчете.

3. Настройка консоли ОС MS Windows для анализа трафика сетевого интерфейса.

Панель управления – Администрирование – Производительность - контекстное меню – добавить счетчики - объект - сетевой интерфейс - добавить счетчики: «отправлено байт/сек», «получено байт/сек». В свойствах графика указать диапазон вертикальной шкалы =5. Вывести заголовок над динамическим графиком- «Сетевой трафик».

4. В окне командного процессора выполнить команду:

ping -l 10000 127.0.0.1 -t (Выход – ctrl+c)

В течении ~1 минуты снять статистику, проанализировать, сделать вывод. В отчет вставить формат отклика.

5. В окне командного процессора выполнить команду: ping -l 65500 127.0.0.1 -t

В течении ~1 минуты снять статистику, проанализировать сделать вывод. В отчет вставить формат отклика.

Данные процедуры позволяют рассмотреть скорее качественное состояние статистики интерфейса, чем количественное. Это связано с тем, что ping отправляет 1 пакет/сек, а статистика собирается за секунду, таким образом, статистика отображает среднюю за секунду величину, а не текущую.

6. Определение размера ICMP-пакетов.

Подобрать значение длины пакетов, чтобы не было сообщений ошибках пакетов. Для этого в текстовом редакторе создать командный файл proba.bat следующего содержания:

```
@echo off
for /L %%i in (1000#,100#,100000#) do (
for /F "usebackq delims=< tokens=2" %%a IN (
`ping -l %%i 127.0.0.1 -n 1`) DO @echo Размер буфера
отправки=%%i.....Время отклика=%%a)
```

В отчете дать объяснения остановки команды ping и указать величину параметров остановки.

Подобрать значение длины пакетов, чтобы не было сообщений ошибках при фрагментации пакетов.

В текстовом редакторе создать командный файл proba_2.bat следующего содержания:

```
@echo off
for /L %%i in (1000#,1#,10000#) do (
for /F "skip=2 usebackq delims=< tokens=2" %%a IN (
`ping -f -l %%i 127.0.0.1 -n 1`) DO @echo Размер буфера
```

отправки=%%i.....Время отклика=%%a).

В отчете дать объяснения остановки команды ping и указать величину параметров остановки.

7. Просмотр статистики Ethernet интерфейса и протоколов IP стека.

Работа и оформление отчета по данному пункту в виде таблицы 2.

Таблица 2 Просмотр статистики

Описание действий	Команды	Статистика
Просмотреть MAC-адреса Ethernet	getmac	
С помощью утилит собрать статистику Ethernet интерфейса и протоколов стека IP	netstat	
Ознакомление с командами	netstat –s –p ICMP l	
	netstat –s –p UDP l	
	netstat –s –p TCP l	

Содержание отчета: характеристики сетевой платы – таблица 1; возможности консоли управления MMC – анализ и выводы; формат отклика по п. 3.4, 3.5, 3.6; статистика Ethernet интерфейса - таблица 2.

Контрольные вопросы

1. Перечислите характеристики сетевой платы.

2. Расскажите о способах диагностики сетевых подключений в ОС MS Windows.

Самостоятельная работа №2 – сделать аналитический обзор, эссе, либо дайджест по предложенным темам.

Темы для самостоятельной работы № 2:

1. Создание шифрованных пользовательских виртуальных дисков.
2. Анализ программных средств криптографической защиты информации.

3. Анализ программно-аппаратных средств усиленной аутентификации

4. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям

5. Защита программ от изучения

6. Настройка политики безопасности операционной системы.

7. Анализ защищенности изолированной программной среды.

8. Исследование систем идентификации на основе устройств Bluetooth.

9. Обзор средств построения виртуальных частных сетей.

10.Изучение средств межсетевого экранирования

11.Исследование технологий доверенной загрузки операционной системы

12.Технологии защищенной загрузки терминальных клиентов.

13.Методы сокрытия программных закладок.

14.Методы сокращения влияния человеческого фактора на защищенность системы

15.Средства обеспечения защиты информации в СУБД

16.Средства идентификации и аутентификации объектов баз данных, управление доступом

17.Средства контроля целостности информации, организация аудита

18.Типы контроля безопасности: потоковый, контроль вывода, контроль доступа.

19.Использование транзакции для изолирования действий пользователей

20.Блокировки.

21. Ссылочная целостность.

Образец выполнения самостоятельной работы: Обзор программно-аппаратных средств.

Классификации современных программно-аппаратных комплексов.

Бурное развитие средств вычислительной техники, автоматизированных информационных систем, появление новых

информационных технологий в нашей стране сопровождается появлением таких малоприятных явлений, как промышленный шпионаж, компьютерная преступность и прежде всего несанкционированный доступ к конфиденциальной информации. Этим обуславливается актуальность и значимость проблемы защиты информации. Острая необходимость в защите информации нашла выражение в создании Государственной системы защиты информации (ГСЗИ). Развивается так же и правовая база информационной безопасности, а именно, приняты и введены в действие законы «О государственной тайне», «Об информации, информатизации и защите информации», «О правовой охране программ для электронных вычислительных машин и баз данных» и др. Целями защиты информации являются:

1. предотвращение ущерба, возникновение которого возможно в результате утери (хищения, утраты, искажения, подделки) информации в любом ее проявлении;

2. реализация адекватных угрозам безопасности информации мер защиты в соответствии с действующими законами и нормативными документами по безопасности информации

3. создание определенных программно-аппаратных средств защиты, соответствующих потребностям владельцев (пользователей) информации.

Любое современное предприятие (учреждение, фирма и т.д.), независимо от вида деятельности и форм собственности, не может сегодня успешно развиваться и вести хозяйственную и иную деятельность без создания надежной системы защиты своей информации, включающей не только организационно-нормативные меры, но и технические средства контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах, прежде всего, программно-аппаратные.

Большинство функций современных КС реализованы в виде программ, поддержание целостности которых при запуске системы и особенно в процессе функционирования является трудной задачей. Значительное число

пользователей в той или иной степени обладают познаниями в программировании, осведомлены об ошибках в построении операционных систем. Поэтому существует достаточно высокая вероятность применения ими имеющихся знаний для атак на программное обеспечение. Проверка целостности одних программ при помощи других не является надежной. Необходимо четко представлять, каким образом обеспечивается целостность собственно программы проверки целостности. Если обе программы находятся на одних и тех же носителях, доверять результатам такой проверки нельзя. В связи с этим к программным системам защиты от несанкционированного доступа следует относиться с особой осторожностью.

Использование аппаратных средств снимает проблему обеспечения целостности системы. В большинстве современных систем защиты от НСД применяется зашивка программного обеспечения в ПЗУ или в аналогичную микросхему. Таким образом, для внесения изменений в ПО необходимо получить доступ к соответствующей плате и заменить микросхему. В случае использования универсального процессора реализация подобных действий потребует применения специального оборудования, что еще более затруднит проведение атаки. Использование специализированного процессора с реализацией алгоритма работы в виде интегральной микросхемы полностью снимает проблему нарушения целостности этого алгоритма.

Для того, чтобы защитить информацию от НСД, существует ряд специально проводимых мер:

- Применение аппаратных средств:
  - ✓ установка фильтров, межсетевых экранов;
  - ✓ блокировка клавиатуры;
  - ✓ устройства аутентификации;
  - ✓ использование электронных замков на микросхемах.
- Применение программных средств:
  - ✓ использование пароля для доступа к компьютеру;

- ✓ использование средств парольной защиты BIOS — как на сам BIOS, так и на ПК в целом.
- Применение аппаратно-программных средств:
  - ✓ использование аппаратно-программных средств доверенной загрузки
- Применение шифрования.
- Проведение организационных мероприятий:
  - ✓ осуществление пропускного режима;
  - ✓ хранение носителей информации в закрытом доступе;
  - ✓ ограничение лиц, имеющих доступ к компьютеру.

Рассмотрим несколько программно-аппаратных комплексов защиты информации.

1) Программно-аппаратный комплекс «Аккорд – 1.95».

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа (ПАК СЗИ НСД) «Аккорд – 1.95», далее комплекс «Аккорд», предназначен для применения на ПЭВМ типа IBM PC в целях защиты ПЭВМ и информационных ресурсов от НСД и обеспечения конфиденциальности информации, обрабатываемой и хранимой в ПЭВМ при многопользовательском режиме ее эксплуатации. Комплекс разработан ОКБ САПР при участии фирмы «Инфокрипт» на основании лицензии Государственной технической комиссии при Президенте РФ (Гостехкомиссии России) от 02.06.95 N 56. Комплекс «Аккорд» состоит из программно-аппаратных средств «Аккорд АМДЗ» и ПО разграничения доступа «Аккорд 1.95-00». В настоящее время комплекс «Аккорд-1.95» выпускается в трех основных версиях в зависимости от модификации аппаратных средств (контроллеров):

- версия 2.0 – контроллер «Аккорд – 4++»;
- версия 3.0 – контроллер «Аккорд – 5»;
- версия 4.0 – контроллер «Аккорд – 4.5»; «Аккорд – СБ/2».

Все модификации могут использоваться на ПЭВМ с процессором 80386 и выше, объемом RAM 640 Кбайт и более. Для установки необходим свободный слот:

- ISA – для контроллеров «Аккорд – 4++»,«Аккорд – 4.5»;
- PCI – для контроллера «Аккорд – 5»;
- «Аккорд – СБ/2».

Используют для идентификации персональные ТМ-идентификаторы DS 199X с объемом памяти до 64 Кбит. Используют для аутентификации пароль до 12 символов. Блокируют загрузку с FDD, CD ROM, ZIP Drive. Предусматривают регистрацию от 16 до 32 пользователей. 147 Имеют аппаратный датчик случайных чисел (ДСЧ). Имеют возможность применения съемника, использующего внутреннее подключение к контроллеру (внутренний съемник). Обеспечивают контроль целостности программ, данных и системных областей жестких дисков. Имеют внутреннюю энергонезависимую память для хранения данных о зарегистрированных пользователях и журнала регистрации событий. Допускают изменение встроенного ПО (технологический режим) без замены платы контроллера. Обеспечивают режим доверенной загрузки ОС (выполнение процедур идентификации/аутентификации пользователя, контроль целостности аппаратной части ПЭВМ, системных файлов, программ и данных до загрузки ОС на аппаратном уровне).

2) Программно-аппаратный комплекс Secret Net NT 4.0.

Автономный вариант системы защиты информации Secret Net NT 4.0 предназначен для защиты ресурсов рабочей станции локальной сети или неподключенного к сети компьютера и разработан научно-инженерным предприятием «ИНФОРМЗАЩИТА».

Система Secret Net NT 4.0 дополняет стандартные защитные механизмы ОС Windows NT функциями, обеспечивающими:

- идентификацию пользователей при помощи специальных аппаратных средств (Touch Memory, Smart Card, Smarty);

- дополнительно к избирательному (дискреционному) управлению доступом, реализованному в ОС Windows NT, полномочное (мандатное) управление доступом пользователей к конфиденциальной информации на локальных и подключенных сетевых дисках;
- оперативный контроль работы пользователей компьютера путем регистрации событий, связанных с безопасностью ИС, удобные средства просмотра и представления зарегистрированной информации;
- контроль целостности программ, используемых пользователями и операционной системой;
- возможность создания для любого пользователя замкнутой программной среды (списка разрешенных для запуска программ);
- простоту управления объектами благодаря использованию механизма шаблонов настроек.

3) Комплекс КРИПТОН-ЗАМОК для ограничения доступа к компьютеру

Комплекс КРИПТОН-ЗАМОК предназначен для построения аппаратно- программных средств ограничения доступа к компьютеру с использованием УКЗД серии КРИПТОН. Комплекс позволяет организовать на базе персонального компьютера рабочее место с ограничением круга лиц, имеющих доступ к содержащейся в нем информации. Для работы комплекса КРИПТОН-ЗАМОК необходим персональный компьютер IBM PC с процессором не ниже i386 и операционной системой-MS DOS, Windows 95/98/NT, UNIX и другими, для которых имеется соответствующий драйвер, позволяющий под управлением MS DOS понимать формат установленной на компьютере файловой системы. Комплекс служит для защиты компьютеров с жесткими дисками, с файловыми системами в форматах FAT 12, FAT 16, FAT 32, NTFS, UNIX и т.д. Работа с дисками с файловыми системами FAT 12, FAT 16 и FAT 32 обеспечивается средствами комплекса без дополнительных драйверов. Работа с 121 дисками с нестандартными файловыми системами NTFS, HTFS, UNIX и т.д., не поддерживаемыми

операционной системой MS-DOS, может производиться только при наличии на компьютере соответствующих DOS-драйверов.

4) Система защиты конфиденциальной информации Secret Disk.

Система защиты конфиденциальной информации Secret Disk разработана компанией Aladdin при участии фирмы АНКАД и предназначена для широкого круга пользователей компьютеров: руководителей, менеджеров, бухгалтеров, 125 аудиторов, адвокатов, т. е. всех тех, кто должен заботиться о защите личной или профессиональной информации.

При установке системы Secret Disk на компьютере создаются новые логические диски, при записи на которые информация автоматически шифруется, а при чтении-расшифровывается. Работа с секретными дисками совершенно незаметна и равносильна встраиванию шифрования во все запускаемые приложения (например, бухгалтерскую программу, Word, Excel).

В системе Secret Disk используется смешанная программно-аппаратная схема защиты с возможностью выбора, соответствующего российским нормативным требованиям криптографического алгоритма ГОСТ 28147-89 с длиной ключа 256 бит (программный эмулятор платы КРИПТОН или криптоплата КРИПТОН фирмы АНКАД).

Важная особенность системы Secret Disk заключается в том, что для доступа к защищенной информации необходим не только вводимый пользователем пароль, но и электронный идентификатор. В качестве такого идентификатора может использоваться обычный электронный ключ для параллельного порта, карточка PCMCIA для ноутбуков или смарт-карта (в этом случае необходимо установить в компьютер специальный считыватель смарт- карт).

5) Система защиты данных Crypton Sigma

Система Crypton Sigma - это программный комплекс, предназначенный для защиты данных на персональном компьютере. По своим возможностям он во многом аналогичен системе Secret Disk. Будучи установленной на

компьютере, система Crypton Sigma хранит конфиденциальные данные в зашифрованном виде, не допуская несанкционированный доступ и утечку данных. Для шифрования данных в системе Crypton Sigma используется алгоритм шифрования ГОСТ 28147-89.

Система защиты конфиденциальных данных Crypton Sigma ориентирована на широкий круг пользователей компьютеров-бизнесменов, менеджеров, бухгалтеров, адвокатов и др., т.е. всех тех, кто нуждается в защите профессиональной и личной информации.

Система Crypton Sigma легко устанавливается, проста и надежна в использовании, а также полностью "прозрачна" для всех программ и системных утилит операционной системы. При установке системы Crypton Sigma на компьютере создаются новые логические диски. При записи на эти диски информация автоматически шифруется, а при считывании-расшифровывается. Этот метод прозрачного шифрования позволяет полностью снять с пользователя заботу о защите данных. Работа с защищенными дисками незаметна для пользователя и равносильна встраиванию процедур шифрования/расшифрования в запускаемые приложения. Защищенные 127 системой диски на вид ничем не отличаются от обычных и могут использоваться в локальной или глобальной сети.

Список литературы:

1) Зайцев А.П., Голубятников И.В., Мещеряков Р.В., Шелупанов А.А. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие. Издание 2-е испр. и доп.– М.:Машиностроение-1, 2006. − 260 с.

2) С.К. Варлатая, М.В. Шаханова. Программно-аппаратная защита информации: учеб. Пособие.- Владивосток: Изд-во ДВГТУ, 2007.

3) Саяркин Л. А., Зайцева А. А., Лапин С. П., Домбровский Я. А. Программно-аппаратные средства защиты автоматизированных систем от несанкционированного доступа // Молодой ученый. — 2017. — №1

Раздел 2. Идентификация, аутентификация. Управление доступом.

Лабораторная работа №3: Назначение прав пользователей при произвольном управлении доступом в ОС Windows.

Цель: научиться создавать учетные записи пользователей, локальных групп, блокировать учетные записи пользователей и.т.д.

Теоретические сведения

После выполнения аутентификации идентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы. Обычно полномочия субъектов представляются списком ресурсов, доступным пользователю и правами по доступу к каждому ресурсу из списка.

При разграничении доступа по спискам задаются соответствия: каждому пользователю – список ресурсов и прав доступа к ним или каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Ход работы

Задание: Создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе и блокировать учетную запись.

А. Создание учетной записи.

1. Откройте оснастку Настройка – Панель управления – Администрирование (рис. 7) – Управление компьютером (рис. 8).

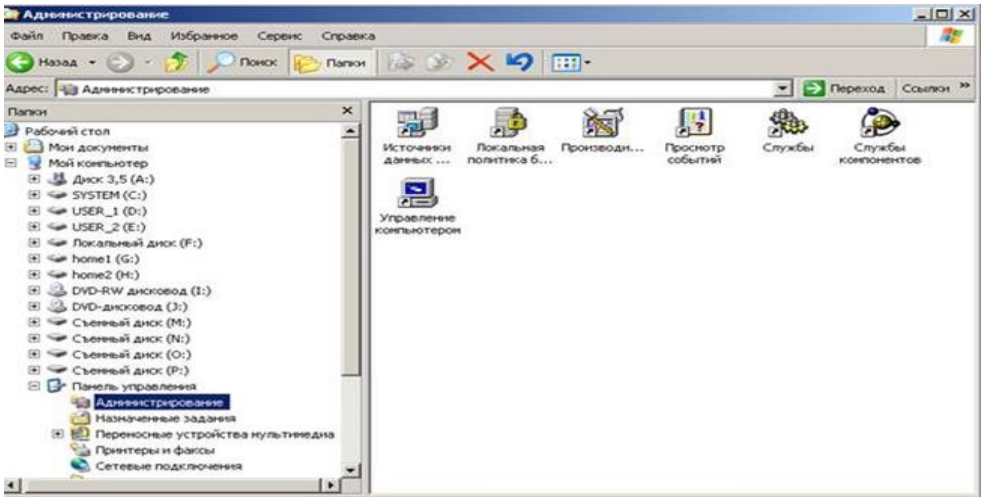


Рисунок 7 - Вид панели администрирования

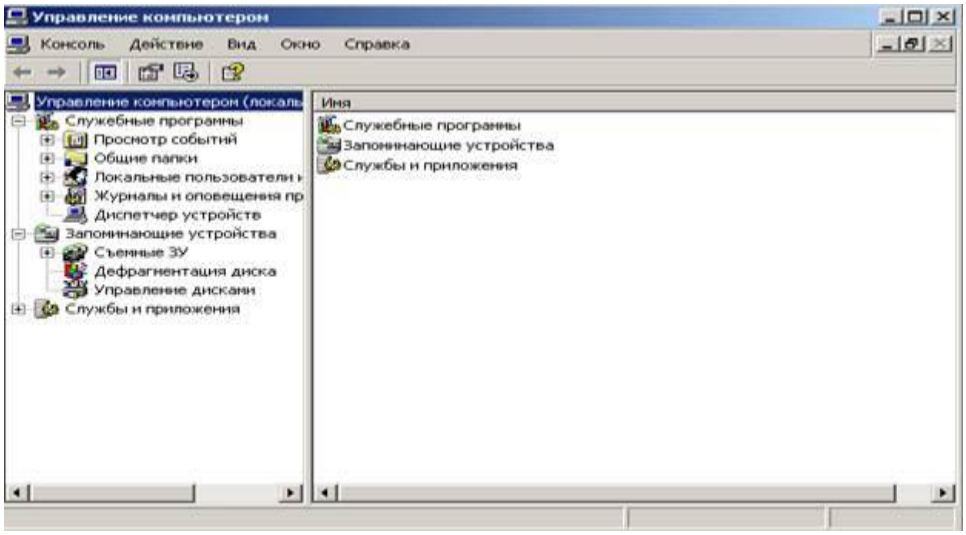


Рисунок 8 – Вид управление компьютером

2. В оснастке Локальные пользователи и группы установите указатель мыши на папку Пользователи и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду Новый пользователь (рис. 9), после чего появится окно диалога Новый пользователь (рис. 10).

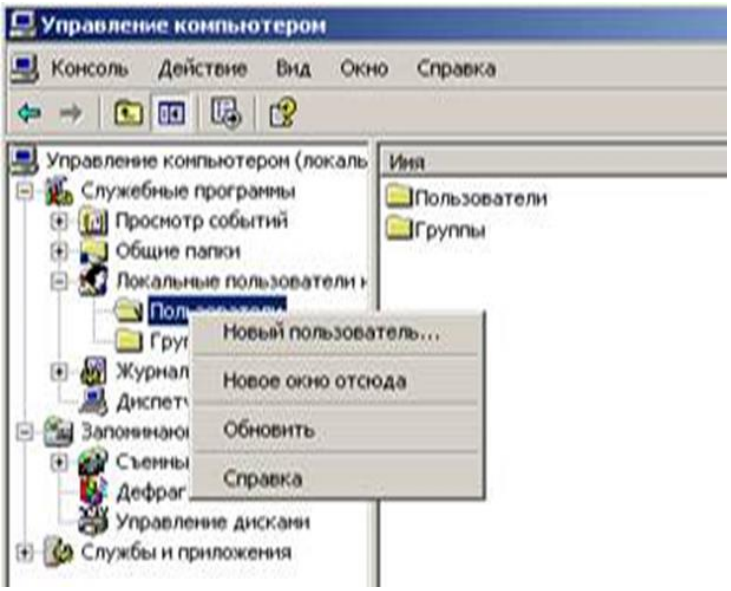


Рис. 9 - Команда Новый пользователь

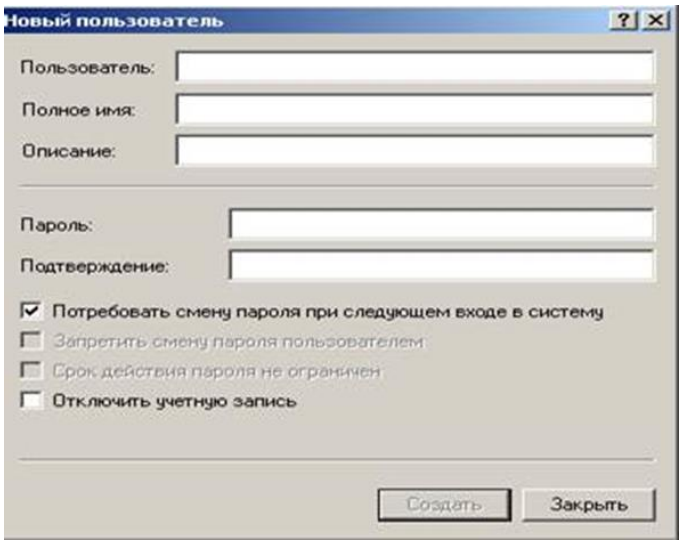


Рис. 10 – Диалоговое окно Новый пользователь

4. В поле Пользователь введите имя создаваемого пользователя, например, свою фамилию.

Примечание: Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра, недопустимые символы:*[];:=.,<>? Имя пользователя не может состоять целиком из точек и пробелов.

5. В поле Полное имя введите полное имя создаваемого пользователя.

6. В поле Описание введите описание создаваемого пользователя или учетной записи, например, «студент ……».

7. В поле Пароль введите пароль пользователя и в поле Подтверждение подтвердите его правильность вторичным вводом.

Примечание: Длина пароля не может превышать 14 символов.

8. Установите или снимите флажки:

Потребовать смену пароля при следующем входе в систему

Запретить смену пароля пользователем

Срок действия пароля не ограничен

Отключить учетную запись

9. Чтобы создать ещё одного пользователя, нажмите кнопку Создать и повторите шаги с 1 по 8. Для завершения работы нажмите кнопку Создать и затем Закрыть.

В. Создание локальной группы.

1. В окне оснастки Локальные пользователи и группы установите указатель мыши на папке Группы и нажмите правую кнопку.

2. В появившемся контекстном меню выберите команду Новая группа.

3. В поле Имя группы (рис. 11) введите имя новой группы, например, Студенты.

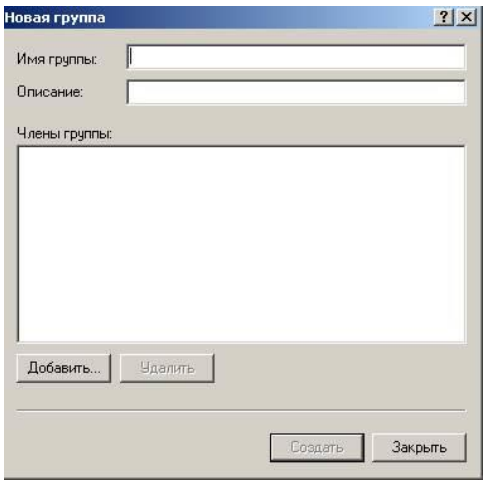


Рисунок 11 – Окно Новая группа

Примечание: Имя локальной группы должно быть уникальным. Оно сможет содержать до 256 символов в верхнем и нижнем регистрах.

4. В поле Описание введите описание новой группы.

5. В поле Члены группы можно сразу добавить пользователей и группы, которые войдут в новую группу: для этого нужно нажать кнопку Добавить и выбрать их в списке. Для завершения нажмите кнопку Создать и затем Закрыть.

С. Изменение членства в локальной группе.

1. В окне оснастки Локальные пользователи и группы щелкните на папке Группы.

2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.

3. В появившемся контекстном меню выберите команду Добавить в группу или Свойства.

4. Для того чтобы добавить новые учетные записи в группу, нажмите кнопку Добавить (рис. 12)

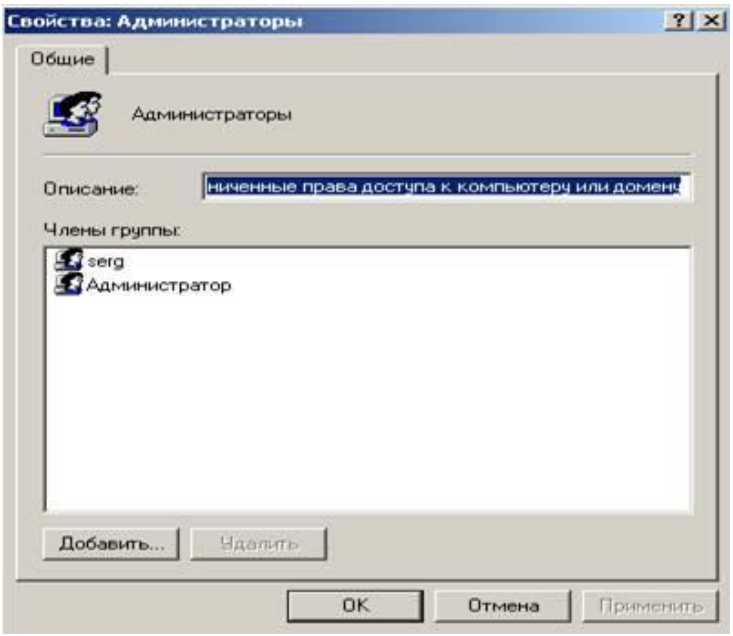


Рисунок 12 – Окно свойства Администраторы

5. Далее следуйте указателям окна диалога Выбор: Пользователи или группы.

6. Для того, чтобы удалить из группы некоторых пользователей, в поле Члены группы (рис. 12) окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку Удалить.

Примечание: В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и локальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в неё пользователей.

D. Временная блокировка учетной записи.

1. Откройте оснастку Управление компьютером.

2. Для этого либо выберите на Рабочем столе ярлык Мой компьютер и нажмите правую кнопку мыши, после этого выберите пункт контекстного меню Управление, либо воспользуйтесь разделом Администрирование в Панели управления.

3. В открывшейся оснастке выберите пункты Служебные программы/Локальные пользователи и группы (рис. 13).

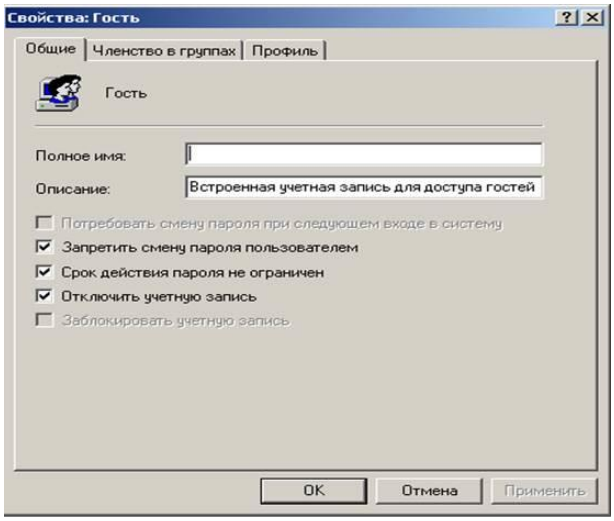


Рисунок 13 – Окно локальные пользователи и группы

4. Откройте папку пользователи и выберите учетную запись Гость.

5. Нажмите правую кнопку мыши и выберите пункт свойства.

6. В открывшемся окне снимите отметку пункта Отключить учетную запись

7. Нажмите кнопку ОК и сделайте вывод о состоянии учетной записи.

8. Выполните пункт 5 и отметьте пункт Отключить учетную запись.

Задание для самостоятельной работы*.

1. Создайте учетную запись с именем ПЗ-3, используя команду Print Screen клавиатуры, сохраните копию экрана со списком пользователей Вашего компьютера (для чего после нажатия клавиши Print Screen вставьте скопированное изображение в новый документ Word) для представления в качестве отчета.

2. Создайте группу Информационная безопасность и, как в первом задании, сохраните окно со списком групп Вашего компьютера для отчета.

3. Заблокируйте учетную запись ПЗ-3 и после этого удалите ее.

Контрольные вопросы:

1. Какие методы управления доступом Вам известны?

2. Чем отличается мандатное управление доступом от дискретного?

3. Допустимо ли имя пользователя П38/44? Почему?

Содержание отчета: тема, цель, скриншоты основных этапов хода работы.

Самостоятельная работа №3: Реализация модели политики безопасности посредством управления доступом. Матрица доступа.

Цель: ознакомиться с моделью политики безопасности, реализованной через матрицу доступа и ролевой доступ.

Теоретические сведения

Под политикой безопасности понимают набор норм, правил и практических приемов, регулирующих управление, защиту и распределение ценной информации.

Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные доступы.

Политика безопасности реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.

Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.

Политика безопасности определяется способом управления доступом, который задаёт порядок доступа к объектам системы.

В ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах Гостехкомиссии РФ определены два вида (принципа) разграничения доступа:

- Дискретное (дискреционное, избирательное) управление доступом;
- Мандатное (полномочное) управление доступом.

Избирательное (или дискреционное) управление доступом характеризуется заданным администратором множеством разрешенных отношений доступа (например, в виде троек объект – субъект – тип доступа). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.

Матрица доступа представляет собой матрицу, в которой столбец соответствует объекту системы, а строка – субъекту.

На пересечении столбца и строки матрицы указывается тип разрешенного доступа субъекта к объекту.

Обычно выделяют такие типы доступа субъекта к объекту, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и т.п.

Матрица доступа является самым простым подходом к моделированию систем управления доступом. Однако она служит основой для сложных моделей, более адекватно описывающих реальные автоматизированные системы обработки информации.

Недопущение утечек информации является одной из важнейших задач службы информационной безопасности любого учреждения

.Если есть конфиденциальная информация (государственная, коммерческая тайна, персональные данные), то существует задача ее защиты.

С ростом организации, увеличивается опасность хищения информации, в том числе сотрудниками, возрастают финансовые и репутационные риски, это приводит к ужесточению политик и систем контроля.

Любые избыточные права доступа сотрудников ведут к увеличению риска утечки информации. Риск потери конфиденциальной информации очень велик и последствия могут быть различными - начиная от потери репутации компании и заканчивая уголовным преследованием, поэтому большинство компаний с ростом численности сотрудников усиливают меры по контролю за правами их доступа. Происходит ужесточение политики ИБ, так как увеличиваются риски утечки информации.

Избирательная политика безопасности широко применяется в автоматизированных системах коммерческого сектора, так как её реализация соответствует требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость.

Полномочная политика безопасности основана на полномочном (мандатном) способе управления доступом. Полномочное (или мандатное) управление доступом характеризуется совокупностью правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя. Полномочное управление доступом подразумевает, что:

1) все субъекты и объекты системы однозначно идентифицированы;

2) каждому объекту системы присвоена метка конфиденциальности информации, определяющая ценность содержащейся в нем информации;

3) каждому субъекту системы присвоен определенный уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.

Чем важнее объект, тем выше его метка конфиденциальности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.

Основное назначение полномочной политики безопасности – регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.

При выборе и реализации политики безопасности в автоматизированной системе, как правило, работают в следующем порядке.

В информационную структуру вносится структура ценностей (определяется ценность информации) и проводится анализ угроз и рисков для информации и информационного обмена.

Определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей.

Одним из первых этапов по упорядочиванию процесса выдачи прав к информационным системам – ввод системы согласования заявок.

Далее обычно принимаются меры по уменьшению полномочий сотрудников, такие как запрет создания ресурсов и изменения прав доступа к тем ресурсам, где пользователь владелец, блокировка прав локального администратора и так далее.

Следующим этапом, как правило, вводится периодическая инвентаризация и ресертификация существующих прав доступа, то есть пересмотр прав пользователей к информационным ресурсам компании.

Пример простейшей матрицы доступа представлен в таблице 3.

Таблица 3 Пример матрицы доступа

Объект / Субъект	Файл_1	Файл_2	CD-RW	Дисковод
1. Администратор	Полные права	Полные права	Полные права	Полные права
2. Гость	Запрет	Чтение	Чтение	Запрет
3. Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Запрет

Ролевое управление доступом.

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить. Таким решением является **ролевое управление доступом.**

Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права (рис.14).

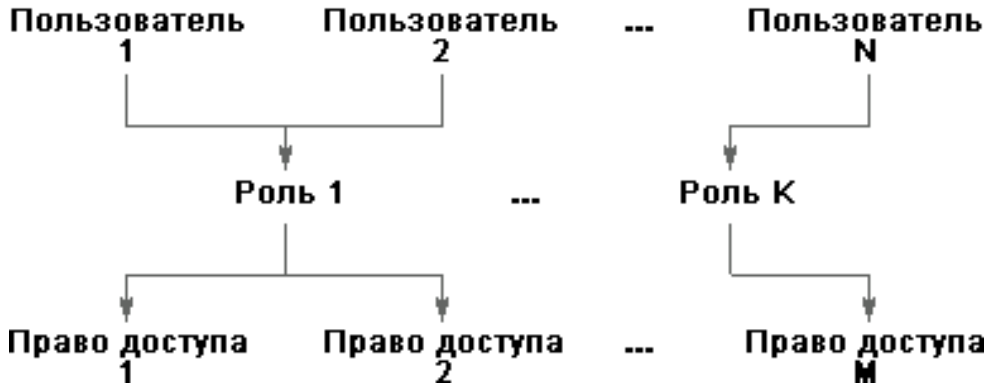


Рисунок 14 – Схема ролевого управления доступом.

Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах.

Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится

пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно.

Ролевое управление доступом оперирует следующими основными понятиями:

- **пользователь** (человек, интеллектуальный автономный агент и т.п.);
- **сеанс работы пользователя**;
- **роль** (обычно определяется в соответствии с организационной структурой);
- **объект** (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);
- **операция** (зависит от объекта; для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными);
- **право доступа** (разрешение выполнять определенные операции над определенными объектами).

Ролям приписываются пользователи и права доступа; можно считать, что они (роли) именуют отношения "многие ко многим" между пользователями и правами.

Роли могут быть приписаны многим пользователям; один пользователь может быть приписан нескольким ролям.

Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов.

Между ролями может быть определено отношение частичного порядка, называемое наследованием. Если роль r2 является наследницей r1, то все права r1 приписываются r2, а все пользователи r2 приписываются r1. Очевидно, что **наследование ролей** соответствует наследованию классов в объектно-ориентированном программировании, только правам доступа

соответствуют методы классов, а пользователям – объекты (экземпляры) классов.

Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц (и, естественно, несколько наследниц, которых мы будем называть также преемницами).

Можно представить формирование **иерархии ролей**, начиная с минимума прав (и максимума пользователей), приписываемых роли "сотрудник", с постепенным уточнением состава пользователей и добавлением прав (роли "системный администратор", "бухгалтер" и т.п.), вплоть до роли "руководитель" (что, впрочем, не значит, что руководителю предоставляются неограниченные права; как и другим ролям, в соответствии с принципом **минимизации привилегий**, этой роли целесообразно разрешить только то, что необходимо для выполнения служебных обязанностей).

Задание для практического выполнения.

1. составить матрицу доступа для сотрудников образовательного учреждения, используя сайт учреждения и другие открытые информационные источники.
2. Разработать возможное ролевое управление доступом для учреждения с описанием ролей и перечнем ролей для сотрудников.

Контрольные вопросы:

1. Что понимается под политикой безопасности в автоматизированной системе?
2. Каково соотношение политики безопасности учреждения и автоматизированной системы данного учреждения?
3. В чем заключается модель дискреционной политики безопасности ?
4. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?

5. Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту системы?
6. Как соотносятся матрица доступа и ролевой доступ?
7. В каких случаях целесообразно использовать ролевой доступ?

Содержание отчета: Тема, цель, матрица доступа, схема ролевого доступа, ответы на контрольные вопросы.

Самостоятельная работа №4- написать реферат по заданной теме.

Темы для рефератов:

1. Штрихкодовая идентификация.
2. Радиочастотная идентификация.
3. Биометрическая идентификация.
4. Технологии идентификации на основе карт с магнитной полосой.
5. Аутентификация по многоразовым паролям.
6. Технология Kerberos.
7. Протоколы аутентификации для удаленного доступа.
8. Аутентификация на основе одноразовых паролей.
9. Аутентификация на основе токенов.
10. Аутентификация по предъявлению цифрового сертификата.
11. Использование смарт-карт и USB-ключей.
12. Эволюция методов аутентификации в ОС Windows.
13. Средства аутентификации в компьютерных системах Apple Macintosh.
14. Способы усиления парольной аутентификации.
15. Эволюция методов и средств биометрической аутентификации.
16. Атаки на системы биометрической аутентификации.
17. Способы защиты от подбора паролей.
18. Обзор средств «запоминания» паролей в сетевых службах.
19. Особенности биометрической аутентификации.
20. Обзор функций хеширования паролей в ОС и СУБД.

21. Обзор средств генерации паролей.
22. Обзор средств выявления «слабых» паролей.
23. Обзор средств фильтрации паролей.
24. Использование биометрии в идентификационных картах и паспортах.
25. Практическое применение биометрии в России.

Методические рекомендации по написанию рефератов.

Реферат — письменная работа, выполняемая обучающимся в течение длительного срока (от одной недели до месяца).

Реферат (от лат. referrer — докладывать, сообщать) — краткое точное изложение сущности какого-либо вопроса, темы на основе одной или нескольких книг, монографий или других первоисточников. Реферат должен содержать основные фактические сведения и выводы по рассматриваемому вопросу.

Реферат отвечает на вопрос — что содержится в данной публикации (публикациях).

Однако реферат — не механический пересказ работы, а изложение ее существа.

В настоящее время, помимо реферирования прочитанной литературы, от обучающегося требуется аргументированное изложение собственных мыслей по рассматриваемому вопросу. Тему реферата может предложить преподаватель или сам обучающийся, в последнем случае она должна быть согласованна с преподавателем.

В реферате нужны развернутые аргументы, рассуждения, сравнения. Материал подается не столько в развитии, сколько в форме констатации или описания.

Содержание реферируемого произведения излагается объективно от имени автора. Если в первичном документе главная мысль сформулирована недостаточно четко, в реферате она должна быть конкретизирована и выделена.

Структура реферата:

1. Титульный лист.

2. После титульного листа на отдельной странице следует оглавление (план, содержание), в котором указаны названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.

3. После оглавления следует введение. Объем введения составляет 1,5-2 страницы.

4. Основная часть реферата может иметь одну или несколько глав, состоящих из 2-3 параграфов (подпунктов, разделов) и предполагает осмысленное и логичное изложение главных положений и идей, содержащихся в изученной литературе. В тексте обязательны ссылки на первоисточники. В том случае если цитируется или используется чья-либо неординарная мысль, идея, вывод, приводится какой-либо цифрой материал, таблицу - обязательно сделайте ссылку на того автора у кого вы взяли данный материал.

5. Заключение содержит главные выводы, и итоги из текста основной части, в нем отмечается, как выполнены задачи и достигнуты ли цели, сформулированные во введении.

6. Приложение может включать графики, таблицы, расчеты.

7. Библиография (список литературы) здесь указывается реально использованная для написания реферата литература. Список составляется согласно правилам библиографического описания.

Этапы работы над рефератом.

Работу над рефератом можно условно подразделить на три этапа:

1. Подготовительный этап, включающий изучение предмета исследования;

2. Изложение результатов изучения в виде связного текста;

3. Устное сообщение по теме реферата.

1. Подготовительный этап работы.

Формулировка темы. Подготовительная работа над рефератом начинается с формулировки темы. Тема в концентрированном виде выражает содержание будущего текста, фиксируя как предмет исследования, так и его ожидаемый результат. Для того чтобы работа над рефератом была успешной, необходимо, чтобы тема заключала в себе проблему, скрытый вопрос (даже если наука уже давно дала ответ на этот вопрос, студент, только знакомящийся с соответствующей областью знаний, будет вынужден искать ответ заново, что даст толчок к развитию проблемного, исследовательского мышления).

Поиск источников. Грамотно сформулированная тема зафиксировала предмет изучения; задача обучающегося — найти информацию, относящуюся к данному предмету и разрешить поставленную проблему. Выполнение этой задачи начинается с поиска источников. На этом этапе необходимо вспомнить, как работать с энциклопедиями и энциклопедическими словарями (обращать особое внимание на список литературы, приведенный в конце тематической статьи); как работать с систематическими и алфавитными каталогами библиотек; как оформлять список литературы (выписывая выходные данные книги и отмечая библиотечный шифр).

Работа с источниками. Работу с источниками надо начинать с ознакомительного чтения, т. е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения. В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной

проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет. Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции — это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Создание конспектов для написания реферата.

Подготовительный этап работы завершается созданием конспектов, фиксирующих основные тезисы и аргументы. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы).

По завершении предварительного этапа можно переходить непосредственно к созданию текста реферата.

2. Создание текста.

Общие требования к тексту.

Текст реферата должен подчиняться определенным требованиям: он должен раскрывать тему, обладать связностью и цельностью.

Раскрытие темы предполагает, что в тексте реферата излагается относящийся к теме материал и предлагаются пути решения содержащейся в теме проблемы; связность текста предполагает смысловую

соотносительность отдельных компонентов, а цельность - смысловую законченность текста.

С точки зрения связности все тексты делятся на тексты-констатации и тексты-рассуждения. Тексты-констатации содержат результаты ознакомления с предметом и фиксируют устойчивые и несомненные суждения. В текстах-рассуждениях одни мысли извлекаются из других, некоторые ставятся под сомнение, дается им оценка, выдвигаются различные предположения.

План реферата.

Универсальный план реферата – введение, основной текст и заключение.

Требования к введению.

Во введении аргументируется актуальность исследования, -

т. е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками; перечисляются положения, которые должны быть обоснованы. Введение может также содержать обзор источников или экспериментальных данных, уточнение исходных понятий и терминов, сведения о методах исследования. Во введении обязательно формулируются цель и задачи реферата.

Объем введения - в среднем около 10% от общего объема реферата.

Основная часть реферата.

Основная часть реферата раскрывает содержание темы. Она наиболее значительна по объему, наиболее значима и ответственна. В ней обосновываются основные тезисы реферата, приводятся развернутые аргументы, предполагаются гипотезы, касающиеся существа обсуждаемого вопроса. Важно проследить, чтобы основная часть не имела форму монолога. Аргументируя собственную позицию, можно и должно анализировать и оценивать позиции различных исследователей, с чем-то соглашаться, чему-то возражать, кого-то опровергать. Текст основной части делится на главы,

параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала: классификации (эмпирические исследования), типологии (теоретические исследования), периодизации (исторические исследования).

Заключение — последняя часть научного текста. В ней краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования. Здесь же могут намечаться и дальнейшие перспективы развития темы. Небольшое по объему сообщение также не может обойтись без заключительной части - пусть это будут две-три фразы. Но в них должен подводиться итог проделанной работы.

Список использованной литературы.

Реферат любого уровня сложности обязательно сопровождается списком используемой литературы. Названия книг в списке располагают по алфавиту с указанием выходных данных использованных книг.

Требования, предъявляемые к оформлению реферата

Объемы рефератов колеблются от 10-18 машинописных страниц. Работа выполняется на одной стороне листа стандартного формата. По обеим сторонам листа оставляются поля размером 35 мм. слева и 15 мм. справа, рекомендуется шрифт 12-14, интервал - 1,5. Все листы реферата должны быть пронумерованы. Каждый вопрос в тексте должен иметь заголовок в точном соответствии с наименованием в плане-оглавлении. При написании и оформлении реферата следует избегать типичных ошибок, например, таких:

– поверхностное изложение основных теоретических вопросов выбранной темы, когда автор не понимает, какие проблемы в тексте являются главными, а какие второстепенными,

– в некоторых случаях проблемы, рассматриваемые в разделах, не раскрывают основных аспектов выбранной для реферата темы,

– дословное переписывание книг, статей, заимствования рефератов из интернет и т. д.

При проверке реферата преподавателем оцениваются:

1. Знания и умения на уровне требований стандарта конкретной дисциплины: знание фактического материала, усвоение общих представлений, понятий, идей.

2. Характеристика реализации цели и задач исследования (новизна и актуальность поставленных в реферате проблем, правильность формулирования цели, определения задач исследования, правильность выбора методов решения задач и реализации цели; соответствие выводов решаемым задачам, поставленной цели, убедительность выводов).

3. Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, логичность и последовательность изложения материала, корректность аргументации и системы доказательств, характер и достоверность примеров, иллюстративного материала, широта кругозора автора, наличие знаний интегрированного характера, способность к обобщению).

4. Качество и ценность полученных результатов (степень завершенности реферативного исследования, спорность или однозначность выводов).

5. Использование литературных источников.

6. Культура письменного изложения материала.

7. Культура оформления материалов работы.

Раздел 3. Протоколирование и аудит. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств.

Лабораторная работа№4: Протоколирование и аудит: изучение сетевых средств операционной системы MS Windows. Диагностики сети средствами операционной системы.

Цель: ознакомиться с встроенными инструментальными средствами ОС MS Windows для отладки связности и диагностики сети; собрать информацию о сетевом оборудовании, программном обеспечении и сетевых подключениях персонального компьютера, работающего под управлением ОС MS Windows.

Теоретические сведения

Диагностика сети собирает информацию о компьютере для решения сетевых проблем. Чаще всего, диагностика сети выполняется администратором сети или под руководством специалиста службы технической поддержки по телефону или через Интернет.

Диагностика сети позволяет выполнить различные тесты и собрать информацию о сети. В зависимости от выбранных параметров, диагностика сети тестирует сетевое взаимодействие и проверяет доступность некоторых сетевых служб и программ. Также, производится сбор основной информации о компьютере. Это средство предоставляет возможность поиска причин, вызвавших проблемы с сетью.

Диспетчер состояния - еще один ключевой компонент справочной системы Windows XP. Его назначение - собирать данные, позволяющие выявить существующие или возможные неполадки, такие как некорректная загрузка или нехватка свободного пространства на диске. Система обрабатывает эту информацию и отображает ее в консоли центра справки и поддержки.

Работу диспетчера состояния обеспечивает служба Help and Support (Справка и поддержка). Она запускает исполняемый файл SVCHOST.EXE, который в свою очередь взаимодействует с файлом WMIPRVSE.EXE, собирающим информацию о системе. Еще несколько исполняемых файлов передают в центр справки и поддержки и отображают информацию, собранную службой-поставщиком Windows Management Instruments - WMI (Инструментарий управления Windows), сокращенно WMIPRVSE. Исполняемый файл HELPCTR.EXE поддерживает основной интерфейс центра справки и поддержки и использует файлы HELPHOST.EXE и HELPSVC.EXE для обеспечения работы слушателя хоста и служб поддержки соответственно.

Не всегда проблемы связности очевидны, и выявить их инструментальными средствами не всегда сразу удается. Часто наблюдаются только симптомы, которые необходимо интерпретировать. Необходимо поэтапно в логической последовательности использовать ряд инструментальных средств, при этом пользователь должен быть осведомлен относительно принципов организации сетей и возможностей каждого сетевого инструментального средства.

Возможные проблемы связности сети:

1. Оконечные нагрузки ЛВС должным образом не подключены.
2. ЛВС-интерфейс не работоспособен.
3. ЛВС-интерфейс имеет не правильный IP-адрес.
4. Маска подсети имеет не верное значение.
5. Тот же IP-адрес используется другой системой.
6. Конфигурация таблицы маршрутизации настроена неправильно.
7. Маршрутизатор выключен.
8. Кабель ЛВС поврежден.
9. Длина сегмента ЛВС слишком велика.
10. Неправильно указан DNS-сервер.

Ход работы

1. С помощью "Центра справки и поддержки" MS Windows собрать информацию о системе.

Вызовите "Центр справки и поддержки" MS Windows с помощью клавиши [F1].

Выберите меню "Использование служебных программ для просмотра информации о компьютере и диагностики неполадок", далее "Расширенные сведения о системе". После выполнения "Настроить параметры сбора информации" выберите следующую возможность диагностики MS Windows: "Диагностика сети". Диагностика сети собирает информацию об оборудовании, программном обеспечении и сетевых подключениях.

Проанализируйте информацию и представьте описание свойств системы: "Службы Интернета", "Информация о компьютере", "Модемы и сетевые адаптеры".

2. С помощью программы MS Windows "Сведения о системе" и systeminfo соберите информацию о системе, для чего выполните следующую последовательность действий:

1.Запустить командный процессор: "Пуск"//"Выполнить"//"cmd

2.Выполнить команду: cd C:\Program Files\Common Files\Microsoft Shared\MSInfo\

3.Выполнить команду: msinfo32

4.Выполнить команду: systeminfo

5.Проанализировать информацию, дополнить недостающие данные, полученные в **п. 1.3.1.**

3.3. Проанализировать связность сети, к которой подключен компьютер. С помощью команд MS Windows просмотреть и описать подсоединение к локальной сети. С командной строки выполните команды, указанные в таблице 3.

Таблица 3 Команды для просмотра сетевых характеристик

Команды	Содержание команды
C:\>netstat.exe –rn	Просмотреть записи в локальной таблице IP-маршрутизации
netstat.exe -s	Просмотреть статистические данные протоколов
netstat.exe -a	Просмотреть все подключения и ожидающие порты
net /help	Просмотреть команды сетевых служб
tracert	Проверить TCP/IP-соединения с помощью команд
ipconfig.exe / all	Вывод IP-адреса, маски подсети и основного шлюза для каждого сетевого адаптера
nslookup	Диагностировать инфраструктуру DNS (выйти из nslookup , >exit или Ctrl-C)
ping	Проверить TCP/IP-соединения с помощью команд
arp -a	Просмотр записей кэш, использующихся для хранения IP-адресов и соответствующих им физических адресов

4. Содержание отчета: тема, цель, теоретические сведения - «Возможные проблемы связности сети», описание полученных результатов: "Информация о компьютере", "Модемы и сетевые адаптеры", информация о сетевых настройках, о подключениях компьютера, таблица 3 с фиксацией основных результатов исполнения команд.

5. Контрольные вопросы

1. Что определяет связность сети?

2. Какие утилиты используются в ОС Windows для анализа сетевых подключений компьютера?

Лабораторная работа №5: Анализ защищенности. Защита от потери и отказов программно-аппаратных средств. - Изучение встроенных средств диагностики - WMIC.

Цель работы: изучить возможности встроенных средств управления рабочей станцией с использованием системы Windows Management Instrumentation .

Ход работы

1. При выполнении заданий лабораторной работы рекомендуется ознакомиться с материалами: встроенная помощь ОС MS Windows "Центр справки и поддержки": поиск по ключу " wmic " , "makecab", "expand"; встроенная помощь к программам OS MS Windows, (при помощи команды: wmic /?)

2. Ознакомиться с теоретическими сведениями, сохранить основные в отчет.

Программа WMIC (WMI Command-line) предоставляет простой интерфейс командной строки для работы с подсистемой.

WMI (Windows Management Instrumentation - Инструментарий управления Windows). Это позволяет воспользоваться преимуществами WMI для управления компьютерами с операционными системами Microsoft Windows. WMIC взаимодействует с существующими оболочками и служебными программами, а также может быть легко расширена с помощью сценариев или других административным приложений.

WMIC позволяет выполнять следующие задачи:

- просматривать схемы WMI и запрашивать их классы и экземпляры (обычно с использованием <псевдонимов>,

упрощающих работу с WMI);

- работать с локальным компьютером, удаленными компьютерами или выполнять команды сразу для нескольких компьютеров;

- настраивать псевдонимы и форматы вывода в соответствии с имеющимися потребностями;

- создавать и выполнять сценарии на основе WMIC.

Поставщики WMI позволяют управлять различными аппаратными компонентами, подсистемами операционной системы и прикладными системами. WMIC можно использовать со всеми схемами, внедряемыми поставщиками WMI. WMIC можно использовать с любого компьютера, на котором включена WMIC, для удаленного управления любым компьютером с WMI. При этом наличие WMIC на удаленном управляемом компьютере необязательно. В следующих типичных сценариях WMIC позволяет упростить выполнение задач:

1. Локальное управление компьютером - оператор находится на компьютере и использует WMIC для управления им.
2. Удаленное управление компьютером - оператор находится на одном компьютере и использует WMIC для управления другим компьютером.
3. Удаленное управление несколькими компьютерами - оператор находится на одном компьютере и использует WMIC для управления несколькими компьютерами общей командой.
4. Удаленное управление компьютером (с использованием удаленного сеанса) - оператор использует технологию сеансов удаленного доступа (такую как Telnet или службы терминалов) для подключения к удаленному компьютеру и управления им при помощи WMIC.

Автоматизированное управление с использованием сценариев администрирования - оператор использует WMIC для написания простого сценария, автоматизирующего управление компьютером (локальным, удаленным или несколькими компьютерами - поочередно или одновременно).

3. Просмотреть параметры компьютера, используя командную строку и программу wmic:

wmic /? - Ознакомиться с командами WMIC

wmic BASEBOARD get /value | more - Управление системной платой.

wmic BIOS get /value | more - Управление базовой системой ввода-вывода (BIOS).

wmic BOOTCONFIG get /value | more - Управление конфигурацией загрузки.

wmic COMPUTERSYSTEM get /value |more - Управление компьютером.

wmic CPU get /value |more - Управление ЦП

Сохранить непустые данные в отчет

4. Просмотреть параметры сетевого подключения компьютера в html-формате :

wmic /RECORD:nic.htm nic get /value /format:mof & Start nic.htm

wmic /RECORD:nicconfig.htm nicconfig get /value /format:mof & Start nicconfig.htm

wmic /RECORD:Protocol.htm netprotocol get /value /format:mof & Start Protocol.htm

wmic /RECORD:netuse.htm netuse get /value /format:mof & Start netuse.htm

wmic /RECORD:Protocol.htm netprotocol get Description, ConnectionlessService /format:mof & Start Protocol.htm

wmic /RECORD:address.htm nicconfig get Description,IPAddress,DefaultIPGateway, MACAddress /format:mof & Start address.htm

wmic /RECORD:nic.htm nic get Description, AdapterType,Manufacturer, NetConnectionID, SystemName /format:mof & Start nic.htm

5. Посмотреть параметры сетевой платы

wmic PATH "Win32_Environment.Name='PROCESSOR_IDENTIFIER'" GET VariableValue > Ethernet.htm

wmic nic where (NetConnectionID ="Подключение по локальной сети") get /format:mof >> Ethernet.htm.

6. Определить индекс сетевой платы:

wmic nic where (AdapterType ="Ethernet 802.3") get Index,NetConnectionID

в следующей строке заменить XX на реальное значение и выполнить следующую команду:

wmic nicconfig where (Index= XX) get /format:mof >> Ethernet.htm & start Ethernet.htm

7. В интернете найти форумы или статьи о возможностях использования WMIC, вставить их в отчет.

Содержание отчета: тема, цель, теоретические сведения по " wmic " , "makecab", "expand", скриншоты работы с командной строкой по п.3,4,5,6; фрагмент форума или статья по п.7

Самостоятельная работа №5: Способы резервирования информации - составление пошаговой детализированной схемы.

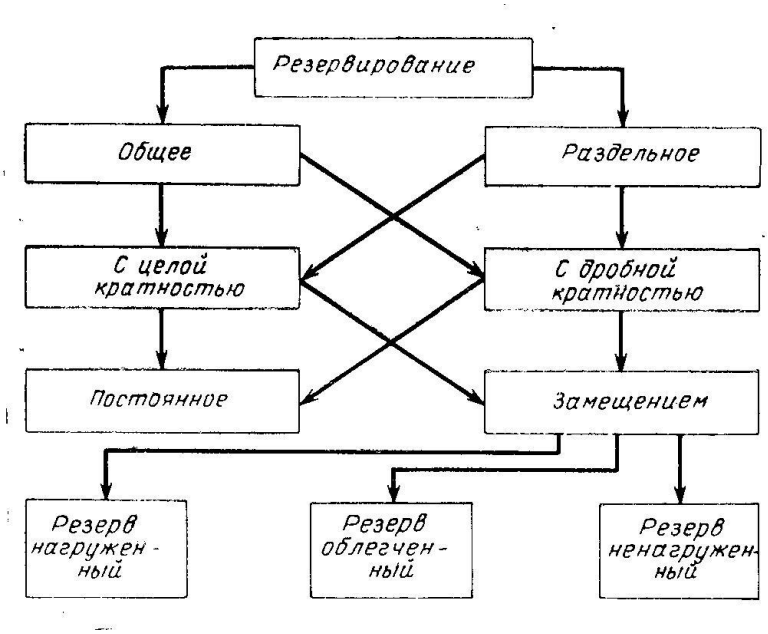


Рисунок 15 Пример детализированной схемы.

Метод пошаговой детализации

С использованием метода пошаговой детализации разработку алгоритмов выполняют поэтапно. На первом этапе описывают решение поставленной задачи «по крупному», выделяя подзадачи, которые необходимо решить. На следующем – аналогично описывают решение подзадач, формулируя уже подзадачи следующего уровня. Процесс продолжают, пока не доходят до подзадач, алгоритмы решения которых очевидны. При этом, описывая решение каждой задачи, желательно использовать не более одной-двух конструкций, таких как цикл или ветвление, чтобы четче представить себе структуру программы.

Индивидуальное задание по теме магистерской диссертации: составить пошаговую детализацию решения проблемы исследования.

Раздел 4. Шифрование. Криптография.

Лабораторная работа № 6: Шифрование, дешифрование в MS Excell

Цель: изучение простейших методов криптографической зашиты информации и закрепление навыков работы в программной среде Microsoft Excel.

Порядок работы:

1. Изучить теоретического материала.
2. Зашифровать своих фамилии и имени, используя метод Цезаря и среду Microsoft Excel.
3. Расшифровывать фразы с карточки – индивидуального варианта, используя метод Цезаря и среду Microsoft Excel.
4. Ответить устно на вопросы.
5. Оформить отчет и предъявить работу преподавателю.

Теоретические сведения

Система шифрования Цезаря – частный случай шифра простой замены. Метод основан на замене каждого символа сообщения (открытого текста) на другой символ того же алфавита, путем смещения от исходного на *k* позиций (получаем закрытый текст). Величина *k* называется ключом шифра (ключ – это информация, необходимая для беспрепятственного дешифрования информации). Ключ в методе Цезаря – целое число. Если поставить в соответствие каждому символу используемого алфавита число, то процесс шифрования будет проходить по формуле:

$$y_i = (x_i + k) \mod n,$$

где x_i – номер i-того символа в открытом тексте, y_i – номер i-того символа в закрытом тексте, k – ключ, n – число символов в алфавите. Операция mod – это взятие остатка от деления одного числа на другое (например: 5 mod 2 = 1, 10 mod 5 = 0, 20 mod 7 = 6).

Дешифрование (расшифровывание) будет проходить по формуле:

$$x_i = (y_i + (n-k)) \mod n.$$

Пример: зашифруем методом Цезаря с ключом k=7 слово «*шифр*».

Будем использовать русский алфавит без буквы ё, где букве А соответствует число 0, а следовательно букве Я – 31. Т.е. n=32.

Поставим в исходном слове в соответствие каждой букве число:

ш $\rightarrow$ 24 $= x_1$

и $\rightarrow$ 8 $= x_2$

ф $\rightarrow$ 20 $= x_3$

р $\rightarrow$ 16 $= x_4$

Тогда $y_1 = (x_1 + k) \mod 32 = (24 + 7) \mod 32 = 31 \mod 32 = 31 \rightarrow$ я

$y_2 = (x_2 + k) \mod 32 = (8 + 7) \mod 32 = 15 \mod 32 = 15 \rightarrow$ п

$y_3 = (x_3 + k) \mod 32 = (20 + 7) \mod 32 = 27 \mod 32 = 27 \rightarrow$ ы

$y_4 = (x_4 + k) \mod 32 = (16 + 7) \mod 32 = 23 \mod 32 = 23 \rightarrow$ ч

Таким образом, получили слово «*япыч*».

Для дешифрования необходимо каждому символу слова «*япыч*» поставить в соответствие число:

я $\rightarrow$ 31 $= y_1$

п $\rightarrow$ 15 $= y_2$

ы $\rightarrow$ 27 $= y_3$

ч $\rightarrow$ 23 $= y_4$

Тогда $x_1 = (y_1 + (32 - k)) \mod 32 = (31 + (32 - 7)) \mod 32 = 56 \mod 32 = 24 \rightarrow$ ш

$x_2 = (y_2 + (32 - k)) \mod 32 = (15 + 25) \mod 32 = 40 \mod 32 = 8 \rightarrow$ и

$x_3 = (y_3 + (32 - k)) \mod 32 = (27 + 25) \mod 32 = 52 \mod 32 = 20 \rightarrow$ ф

$x_4 = (y_4 + (32 - k)) \mod 32 = (23 + 25) \mod 32 = 48 \mod 32 = 16 \rightarrow$ р

Получили слово «шифр», следовательно шифрование было выполнено правильно.

Шифр перестановки с ключом – является одним из многочисленных видов шифров перестановки (символы исходного сообщения переставляются по определенным законам).

Для перестановки с ключом выбирается ключ – любое слово. Символы ключа нумеруется в порядке следования их в алфавите. Строится таблица, в которой количество столбцов равно количеству букв в ключе. Исходный текст вместе с пробелами и знаками препинания записывается в эту таблицу. Если последняя срока заполнена не полностью, до до конца строки записываются любые символы («пустышки»). Затем текст переписывается по столбцам, учитывая их нумерацию согласно ключу.

Пример. Выберем в качестве ключа слово «*информация*». Пронумеруем ключ (первая, из имеющихся в ключе, в алфавите буква А, следовательно ей присваивается номер 1; следующая по алфавиту буква И, следовательно первая буква И будет иметь номер 2, а вторая – 3; далее идет буква М, ей присваиваем номер 4 и т.д.):

и	н	ф	о	р	м	а	ц	и	я
2	5	8	6	7	4	1	9	3	10

Зашифруем пословицу: «От умного научишься, от глупого разучишься»

Запишем ее в таблицу под ключом. Оставшиеся ячейки до конца строки заполняют «пустышками».

и	н	ф	о	р	м	а	ц	и	я
2	5	8	6	7	4	1	9	3	10
о	т		у	м	н	о	г	о	
н	а	у	ч	и	ш	ь	с	я	,
	о	т		г	л	у	п	о	г
о		р	а	з	у	ч	и	ш	ь
с	я	а	б	в	г	д	е	ж	з

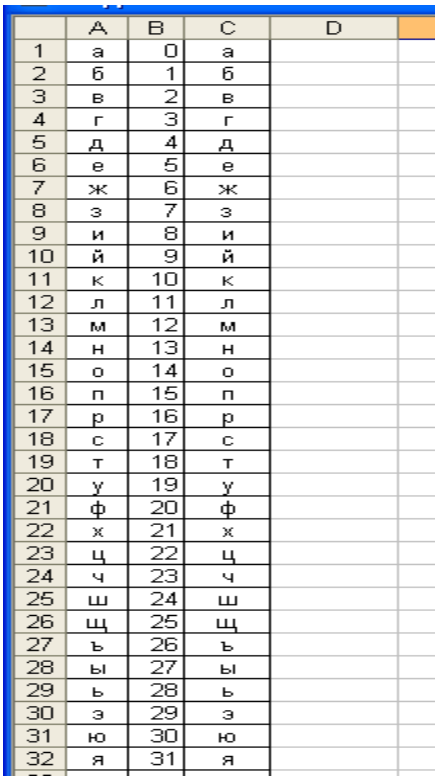
Переписываем столбцы, учитывая их номер:

Оьучдон осояошжншлугтао яуч абмигзв утрагспие ,гьз

Для дешифрования зашифрованный текст записывается в таблицу по столбцам, учитывая их номер.

Ход работы

1. Ознакомьтесь с теоретической частью практической работы.
2. Загрузите программу Microsoft Excel.
3. На первом листе электронной книги запишите в столбец А буквы русского алфавита. В столбце В – номер букв, в столбце С – опять буквы (такая запись будет необходима для использования функции ВПР).



	A	B	C	D
1	а	0	а	
2	б	1	б	
3	в	2	в	
4	г	3	г	
5	д	4	д	
6	е	5	е	
7	ж	6	ж	
8	з	7	з	
9	и	8	и	
10	й	9	й	
11	к	10	к	
12	л	11	л	
13	м	12	м	
14	н	13	н	
15	о	14	о	
16	п	15	п	
17	р	16	р	
18	с	17	с	
19	т	18	т	
20	у	19	у	
21	ф	20	ф	
22	х	21	х	
23	ц	22	ц	
24	ч	23	ч	
25	ш	24	ш	
26	щ	25	щ	
27	ъ	26	ъ	
28	ы	27	ы	
29	ь	28	ь	
30	э	29	э	
31	ю	30	ю	
32	я	31	я	

Рисунок 16 - фрагмент таблицы с алфавитом

4. Переименуйте лист1 в Алфавит.
5. На втором листе электронной книги запишите название работы, ключ и название столбцов таблицы (S – исходные символы, X – числа исходных символов, Y – пересчитанные по формуле значения, S1 – символы закрытого текста). Значение ключа можно взять любым и обязательно его значение записать в отдельную ячейку (B5). В столбец S, начиная с 8 строки, впишите фамилию и имя, каждую букву в отдельной ячейке.

	A	B	C	D	E	F	G
1					Шифр Цезаря		
2							
3	1. Зашифровывание						
4							
5	k=	5					
6							
7	S	X	Y	S1			
8	и						
9	в						
10	а						
11	н						
12	о						
13	в						
14	а						
15	н						
16	д						
17	р						
18	е						
19	й						
20							

Рисунок 17 – фрагмент таблицы для вписывания фамилии и имени.

6. В столбце X должны быть числовые значения символов из столбца S. Эти значения хранятся на листе Алфавит. Чтобы получить их, можно воспользоваться функцией **ВПР** (категория – ссылки и массивы). Встаем в ячейку B8 и вызываем функцию ВПР. Заполняем ее окно следующим образом:

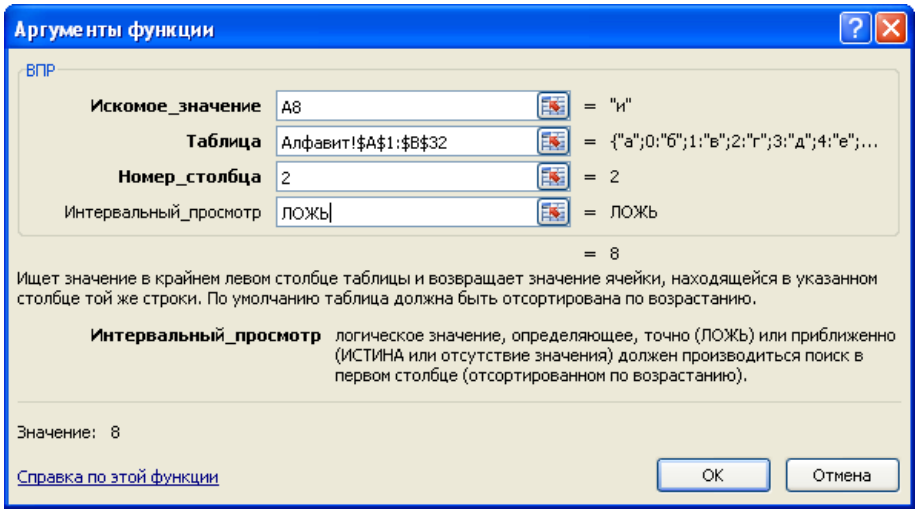


Рисунок 18 – диалоговое окно функции ВПР

7. Растянуть формулу вниз до конца таблицы.
8. В ячейку C8 (столбец Y) записывается формула для шифрования. Исходная формула метода Цезаря имеет вид: $y_i = (x_i + k) \mod n$

.Операции mod в Excel соответствует функция **ОСТАТ(число; делитель)**. В нашем случае **число** – это $(x_i + k)$, а **делитель** – 32. Т.е. функция **ОСТАТ** будет иметь вид **=ОСТАТ((B8+B5);32)**.

9. Эту формулу необходимо растянуть вниз до конца таблицы.
10. В ячейку D8 (столбец S1) опять записываем функцию **ВПР**, которая по числу Y найдет букву. Эта функция будет выглядеть следующим образом:

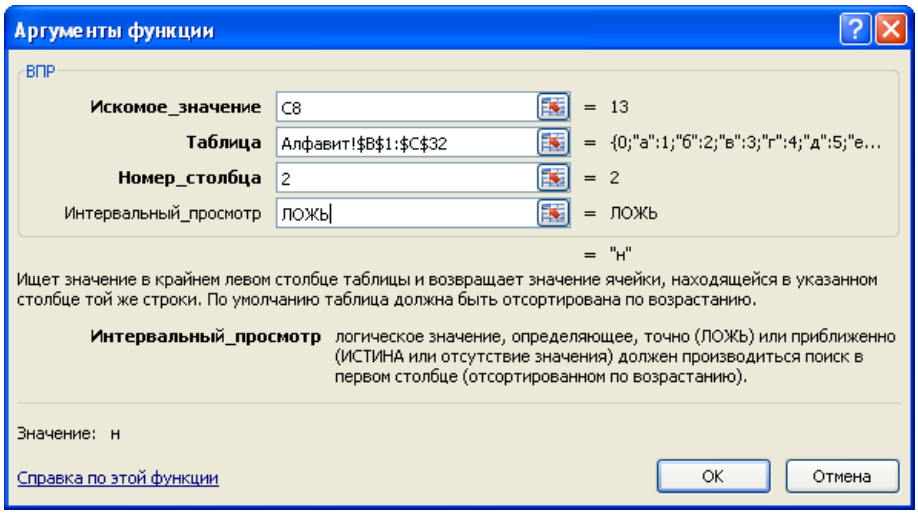
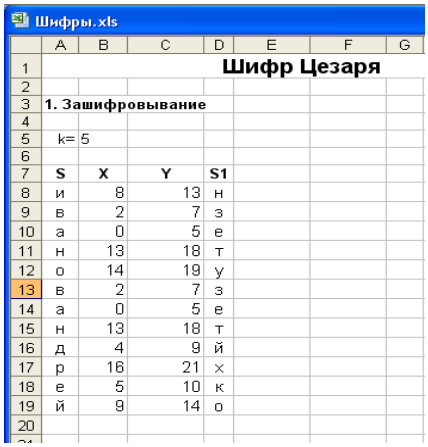


Рисунок 19 – диалоговое окно функции ВПР

11. Окончательно таблица должна выглядеть следующим образом:

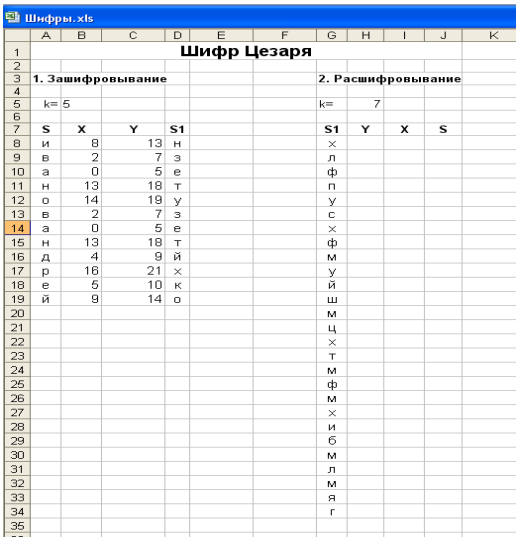


	A	B	C	D	E	F	G
1				Шифр Цезаря			
2							
3	1. Зашифровывание						
4							
5	k=	5					
6							
7	S	X	Y	S1			
8	и	8	13	н			
9	в	2	7	з			
10	а	0	5	е			
11	н	13	18	т			
12	о	14	19	у			
13	в	2	7	з			
14	а	0	5	е			
15	н	13	18	т			
16	д	4	9	й			
17	р	16	21	х			
18	е	5	10	к			
19	й	9	14	о			
20							

Рисунок 20 – фрагмент таблицы для зашифрования

Запишите полученный закрытый текст (столбец S1) в тетрадь.

12.Рядом приготовьте место для дешифрования информации. Получите у преподавателя карточку с закрытым текстом и впишите его в столбец S1 новой таблицы.



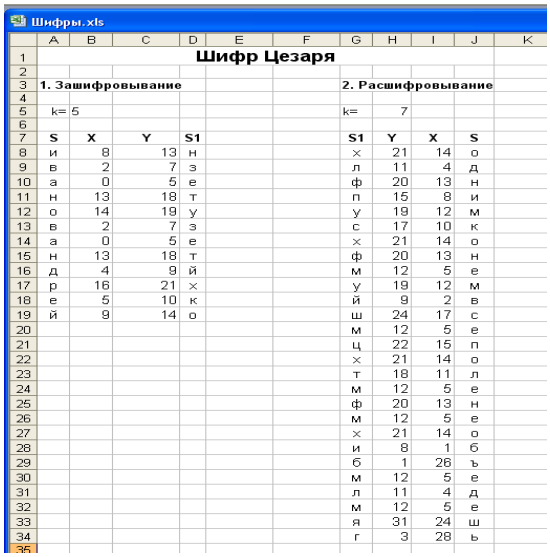
Шифры.xls

	A	B	C	D	E	F	G	H	I	J	K
1				Шифр Цезаря							
2											
3	1. Зашифровывание						2. Расшифровывание				
4											
5	k=	5					k=	7			
6											
7	S	X	Y	S1			S1	Y	X	S	
8	и	8	13	н			х				
9	в	2	7	з			л				
10	а	0	5	е			ф				
11	н	13	18	т			п				
12	о	14	19	у			у				
13	в	2	7	з			с				
14	а	0	5	е			х				
15	н	13	18	т			ф				
16	д	4	9	й			м				
17	р	16	21	х			у				
18	е	5	10	к			й				
19	й	9	14	о			ш				
20							м				
21							ц				
22							х				
23							т				
24							м				
25							ф				
26							м				
27							х				
28							и				
29							б				
30							м				
31							л				
32							м				
33							я				
34							г				
35											

Рисунок 21 – фрагмент таблицы для расшифрования

13.Проведите дешифрования текста по аналогии с зашифровыванием. Для расшифровывания (столбца X) используйте формулу

$$x_i = (y_i + (32 - k)) \mod 32.$$



Шифры.xls

	A	B	C	D	E	F	G	H	I	J	K
1				Шифр Цезаря							
2											
3	1. Зашифровывание						2. Расшифровывание				
4											
5	k=	5					k=	7			
6											
7	S	X	Y	S1			S1	Y	X	S	
8	и	8	13	н			х	21	14	о	
9	в	2	7	з			л	11	4	д	
10	а	0	5	е			ф	20	13	н	
11	н	13	18	т			п	15	8	и	
12	о	14	19	у			у	19	12	м	
13	в	2	7	з			с	17	10	к	
14	а	0	5	е			х	21	14	о	
15	н	13	18	т			ф	20	13	н	
16	д	4	9	й			м	12	5	е	
17	р	16	21	х			у	19	12	м	
18	е	5	10	к			й	9	2	в	
19	й	9	14	о			ш	24	17	с	
20							м	12	5	е	
21							ц	22	15	п	
22							х	21	14	о	
23							т	18	11	л	
24							м	12	5	е	
25							ф	20	13	н	
26							м	12	5	е	
27							х	21	14	о	
28							и	8	1	б	
29							б	1	26	ъ	
30							м	12	5	е	
31							л	11	4	д	
32							м	12	5	е	
33							я	31	24	ш	
34							г	3	28	ь	
35											

Рисунок 21- фрагмент таблицы для расшифрования.

14. Запишите полученную фразу
15. Зашифруйте в тетради расшифрованную фразу методом перестановки с ключом. В качестве ключа используйте свою фамилию.
16. Оформите отчет и предъявите работу преподавателю.

Контрольные вопросы.

1. Какой текст называется открытым?
2. Какой текст называется закрытым?
3. Что такое ключ?
4. Как осуществляется процесс шифрования в методе Цезаря?
5. Что такое «шифрование методом перестановки»?
6. Как работает функция ОСТАТ?
7. Что делает функция ВПР?

Содержание отчета: описание выполненной работы со скриншотами, ответы на контрольные вопросы

Варианты заданий

№1 Используя ключ 8 проведите дешифрование информации, зашифрованной методом Цезаря: фищтршцкти - еъц эръшцщъд р щхцшцкти	№2 Используя ключ 6 проведите дешифрование информации, зашифрованной методом Цезаря: ршф ыфэлш туфйф нужшв, шфтщ ужкф тжсф чхжшв
№3 Используя ключ 4 проведите дешифрование информации, зашифрованной методом Цезаря: уфйичуфйимца жтжфйрг - ийпт ифчлйн	№4 Используя ключ 6 проведите дешифрование информации, зашифрованной методом Цезаря: ифнвтлшче ужцфк - фнлцф хлцлсвлш
№5 Используя ключ 7 проведите дешифрование информации, зашифрованной методом Цезаря: хлфпу схфму йшм цхтм фм хибмлмяг	№6 Используя ключ 9 проведите дешифрование информации, зашифрованной методом Цезаря: мно ъфчлй щонус, ыйх чцс лоъ схозы
№7 Используя ключ 10 проведите дешифрование информации, зашифрованной методом Цезаря: цкх йсеф, ок мыпц ьпхшц мхкоппь	№8 Используя ключ 7 проведите дешифрование информации, зашифрованной методом Цезаря: юму ихтгям фзъсп, щму ъуфмм чъсп

№9 Используя ключ 9 проведите дешифрование информации, зашифрованной методом Цезаря: хйфч нсшфчх схоые, цйнч нофч щйрьхоые	№10 Используя ключ 4 проведите дешифрование информации, зашифрованной методом Цезаря: рчифтхца - сдмрйсаьдг цгкйпдг стьд ж учцм
№11 Используя ключ 10 проведите дешифрование информации, зашифрованной методом Цезаря: щъшнэхжчеп очт мшъшмыьмэ ыъшочт	№12 Используя ключ 5 проведите дешифрование информации, зашифрованной методом Цезаря: уч ирем чурпш серу, кцрн шс цркф
№13 Используя ключ 6 проведите дешифрование информации, зашифрованной методом Цезаря: рфтщ цжзфшж и шейфчшв, шфтщ ул илкфтж	№14 Используя ключ 7 проведите дешифрование информации, зашифрованной методом Цезаря: ьхчхямм йхшцпщзфпм - тъюямм фзштмлшщйх
№15 Используя ключ 8 проведите дешифрование информации, зашифрованной методом Цезаря: чцфиэинад тцщцс - йымнъ щуимцт чцтцс	№16 Используя ключ 9 проведите дешифрование информации, зашифрованной методом Цезаря: уыч хцчмч цйасцйоы, ычы хйфч учцайоы

Самостоятельная работа №6 «Кодирование и шифрование информации».

Вариант 1

1. Дана кодовая таблица азбуки Морзе

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

—— ——— • — • • ——— — • • — • — • — • ——

2. Закодируйте с помощью азбуки Морзе слова

СТЕНОГРАФИЯ, ШИФРОВАНИЕ, КОДИРОВАНИЕ.

Таблица ASCII-кодов

SP	!	"	#	S	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	*B*	C	D	E	*F*	*G*	*M*	I	J	*K*	L	*M*	*N*	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	*Q*	*R*	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	*a*	*в*	c	d	e	*f*	g	h	i	*j*	*k*	l	*m*	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	*v*	*w*	*x*	*y*	*z*	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

3. Дана таблица ASCII-кодов

Расшифровать слово : 48 41 54 52 48 58 (Шестнадцатеричная СС)

4. Зашифрованная пословица.

Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).

Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .

Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.

Самый колючий зверь в лесу – это 12, 13. А теперь прочитайте пословицу: 1, 2, 3, 4, 5, 1, 6 7, 8, 9, 10, 11 9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ КОДИРОВАТЬ ИНФОРМАЦИЮ”. Зашифрованный текст должен быть записан без пропусков.

1.	А	8.	Ж	15.	Н	22.	Ф	29.	Ы
2.	Б	9.	З	16.	О	23.	Х	30.	Ь
3.	В	10.	И	17.	П	24.	Ц	31.	Э
4.	Г	11.	Й	18.	Р	25.	Ч	32.	Ю
5.	Д	12.	К	19.	С	26.	Ш	33.	Я
6.	Е	13.	Л	20.	Т	27.	Щ		
7.	Ё	14.	М	21.	У	28.	Ъ		

,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ РАБОТАТЬ С ИНФОРМАЦИЕЙ!

Используя эту же кодировочную таблицу, расшифруйте текст: 252015383503040538351115030400 38

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения могут быть закодированы с помощью этой таблицы? Привести примеры.

8. При помощи таблицы Вижинера зашифровать текст «Полиалфавитная замена». Ключ «Шифр».

9. Закодировать методом Гамильтона «Аутентификация», «Детектор движения».

10. Аналитические методы шифрования

Зашифровать слово **ТОМ** Ключ – матрица

A=

1		
		2

Выполнить проверку (расшифровать слово)

Вариант 2

1. Дана кодовая таблица азбуки Морзе

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

—— ——— • — • • ——— — • • — • — • — • ——

2. Закодируйте с помощью азбуки Морзе слова **КРИПТОАНАЛИЗ,**

Таблица ASCII-кодов

SP	!	"	#	S	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	*B*	C	D	E	*F*	*G*	*M*	I	J	*K*	L	*M*	*N*	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	*Q*	*R*	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	*a*	*в*	c	d	e	*f*	g	h	i	*j*	*k*	l	*m*	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	*v*	*w*	*x*	*y*	*z*	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

КЛЮЧ, ШИФР

3. Дана таблица ASCII-кодов

Расшифровать слово при помощи таблицы ASCII гкодов:

32 2A 78 2B 79 3D 30.

4. Зашифрованная пословица.

Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).

Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .

Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.

Самый колючий зверь в лесу – это 12, 13.

А теперь прочитайте пословицу:

1, 2, 3, 4, 5, 1, 6

7, 8, 9, 10, 11

9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ”. Зашифрованный текст должен быть записан без пропусков.

1.	А	8.	Ж	15.	Н	22.	Ф	29.	Ы
2.	Б	9.	З	16.	О	23.	Х	30.	Ь
3.	В	10.	И	17.	П	24.	Ц	31.	Э
4.	Г	11.	Й	18.	Р	25.	Ч	32.	Ю
5.	Д	12.	К	19.	С	26.	Ш	33.	Я
6.	Е	13.	Л	20.	Т	27.	Щ		
7.	Ё	14.	М	21.	У	28.	Ъ		

,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ!

Используя эту же кодировочную таблицу, расшифруйте текст:

252015383503040538351115030400 38

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения могут быть закодированы с помощью этой таблицы? Привести примеры.

8. При помощи таблицы Вижинера зашифровать текст «Криптографическая защита». Ключ «Шифр».
9. Закодировать методом Гамильтона (создать свой маршрут(ы)).

Криптоанализ

а) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Криптостойкость

10. Аналитические методы шифрования: зашифровать слово **БАР**

Ключ-матрица

A=

0	1	2
2	2	1
3	1	-1

Выполнить проверку (расшифровать слово)

Вариант 3

1. Дана кодовая таблица азбуки Морзе

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

—— ——— •—•• ——— —•• —•—• —•——

2. Закодируйте с помощью азбуки Морзе слова **КРИПТОГРАФИЯ, ВИРУС, ДЕКОДИРОВАНИЕ**

Таблица ASCII-кодов

SP	!	"	#	S	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	*B*	C	D	E	*F*	*G*	*M*	I	J	*K*	L	*M*	*N*	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	*Q*	*R*	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	*a*	*в*	c	d	e	*f*	g	h	i	*j*	*k*	l	*m*	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	*v*	*w*	*x*	*y*	*z*	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

3. Дана таблица ASCII-кодов

Закодировать при помощи таблицы ASCII кодов следующий текст **Password.** Результат представить в шестнадцатеричной СС

4. Зашифрованная пословица.

Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).

Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .

Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.

Самый колючий зверь в лесу – это 12, 13.

А теперь прочитайте пословицу:

1, 2, 3, 4, 5, 1, 6

7, 8, 9, 10, 11

9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ”. Зашифрованный текст должен быть записан без пропусков.

1.	А	8.	Ж	15.	Н	22.	Ф	29.	Ы
2.	Б	9.	З	16.	О	23.	Х	30.	Ь
3.	В	10.	И	17.	П	24.	Ц	31.	Э
4.	Г	11.	Й	18.	Р	25.	Ч	32.	Ю
5.	Д	12.	К	19.	С	26.	Ш	33.	Я
6.	Е	13.	Л	20.	Т	27.	Щ		
7.	Ё	14.	М	21.	У	28.	Ъ		

,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ ШИФРОВАТЬ ДАННЫЕ! Используя эту же кодировочную таблицу, расшифруйте текст: 252015383503040538351115030400 38

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения могут быть закодированы с помощью этой таблицы? Привести примеры.

8. При помощи таблицы Вижинера зашифровать текст «Методы шифрования». Ключ «Шифр»
9. Шифры перестановки.

b) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Кодирование

c) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Декодирование

10. Аналитические методы шифрования

Зашифровать слово **ГАМ**

Ключ – матрица

A=

-1	0	4
0	2	2
3	1	-2

Выполнить проверку (расшифровать слово)

Вариант 4

1. Дана кодовая таблица азбуки Морзе

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

—— ——— •—•• ——— —•• —•—• —•——

2. Закодируйте с помощью азбуки Морзе слова **ШИФРОВАНИЕ, ШИФР, МАСКИРОВКА**

Таблица ASCII-кодов

SP	!	"	#	S	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	*B*	C	D	E	*F*	*G*	*M*	I	J	*K*	L	*M*	*N*	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	*Q*	*R*	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	*a*	*в*	c	d	e	*f*	g	h	i	*j*	*k*	l	*m*	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	*v*	*w*	*x*	*y*	*z*	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

3. Дана таблица ASCII-кодов

Закодировать при помощи таблицы ASCII кодов следующий текст **Windows.** Результат представить в шестнадцатеричной СС

4. Зашифрованная пословица.

Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).

Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .

Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.

Самый колючий зверь в лесу – это 12, 13.

А теперь прочитайте пословицу:

1, 2, 3, 4, 5, 1, 6

7, 8, 9, 10, 11

9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ КОДИРОВАТЬ ДАННЫЕ ДАННЫЕ”. Зашифрованный текст должен быть записан без пропусков.

1.	А	8.	Ж	15.	Н	22.	Ф	29.	Ы
2.	Б	9.	З	16.	О	23.	Х	30.	Ь
3.	В	10.	И	17.	П	24.	Ц	31.	Э
4.	Г	11.	Й	18.	Р	25.	Ч	32.	Ю
5.	Д	12.	К	19.	С	26.	Ш	33.	Я
6.	Е	13.	Л	20.	Т	27.	Щ		
7.	Ё	14.	М	21.	У	28.	Ъ		

,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ КОДИРОВАТЬ ДАННЫЕ!

Используя эту же кодировочную таблицу, расшифруйте текст:

252015383503040538351115030400 38

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения могут быть закодированы с помощью этой таблицы? Привести примеры.

8. При помощи таблицы Вижинера зашифровать текст «Криптографическая защита». Ключ «Шифр»
9. Шифры перестановки

d) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Маскировка

e) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Шифрование

10. Аналитические методы шифрования

Зашифровать слово **МИР**

Ключ – матрица

A=

1	0	4
0	2	2
5	-1	4

Выполнить проверку (расшифровать слово)

Вариант 5

1. Дана кодовая таблица азбуки Морзе

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

—— ——— •—•• ——— —•• —•—• —•——

2. Закодируйте с помощью азбуки Морзе слова **ПАРОЛЬ, ЭКРАНИРОВАНИЕ, КОДИРОВАНИЕ.**

Таблица ASCII-кодов

SP	!	"	#	S	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	*B*	C	D	E	*F*	*G*	*M*	I	J	*K*	L	*M*	*N*	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	*Q*	*R*	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	*a*	*в*	c	d	e	*f*	g	h	i	*j*	*k*	l	*m*	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	*v*	*w*	*x*	*y*	*z*	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

3. Дана таблица ASCII-кодов

Расшифровать слово при помощи таблицы ASCII rкодов:

49 20 6C 6F 76 65 20 79 6F 75

4. Зашифрованная пословица.

Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).

Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .

Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.

Самый колючий зверь в лесу – это 12, 13.

А теперь прочитайте пословицу:

1, 2, 3, 4, 5, 1, 6

7, 8, 9, 10, 11

9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ ДЕКОДИРОВАТЬ ДАННЫЕ”. Зашифрованный текст должен быть записан без пропусков.

1.	А	8.	Ж	15.	Н	22.	Ф	29.	Ы
2.	Б	9.	З	16.	О	23.	Х	30.	Ь
3.	В	10.	И	17.	П	24.	Ц	31.	Э
4.	Г	11.	Й	18.	Р	25.	Ч	32.	Ю
5.	Д	12.	К	19.	С	26.	Ш	33.	Я
6.	Е	13.	Л	20.	Т	27.	Щ		
7.	Ё	14.	М	21.	У	28.	Ъ		

,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ ДЕКОДИРОВАТЬ ДАННЫЕ!

Используя эту же кодировочную таблицу, расшифруйте текст: 252015383503040538351115030400 38

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения могут быть закодированы с помощью этой таблицы? Привести примеры.

8. При помощи таблицы Вижинера зашифровать текст «Криптографическая защита». Ключ «Шифр»
9. Шифры перестановки

f) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Туннелирование

g) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Криптоанализ

10. Аналитические методы шифрования

Зашифровать слово **ЛУГ**

Ключ – матрица

A=

1	0	1
0	2	2
5	-2	4

Выполнить проверку (расшифровать слово)

Вариант 6

1. Дана кодовая таблица азбуки Морзе

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

—— ——— •—•• ——— —•• —•—• —•——

2. Закодируйте с помощью азбуки Морзе слова **ХАКЕР, АНТИВИРУС, ШИФРОВАНИЕ**

Таблица ASCII-кодов															
SP	!	"	#	S	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	*B*	C	D	E	*F*	*G*	*M*	I	J	*K*	L	*M*	*N*	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	*Q*	*R*	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	*a*	*в*	c	d	e	*f*	g	h	i	*j*	*k*	l	*m*	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	*v*	*w*	*x*	*y*	*z*	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

3. Дана таблица ASCII-кодов

Расшифровать слово при помощи таблицы ASCII rкодов:

49 20 6C 6F 76 65 20 79 6F 75

4. Зашифрованная пословица.

Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).

Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .

Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.

Самый колючий зверь в лесу – это 12, 13.

А теперь прочитайте пословицу:

1, 2, 3, 4, 5, 1, 6

7, 8, 9, 10, 11

9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я УМЕЮ ДЕКОДИРОВАТЬ ДАННЫЕ ”. Зашифрованный текст должен быть записан без пропусков.

1.	А	8.	Ж	15.	Н	22.	Ф	29.	Ы
2.	Б	9.	З	16.	О	23.	Х	30.	Ь
3.	В	10.	И	17.	П	24.	Ц	31.	Э
4.	Г	11.	Й	18.	Р	25.	Ч	32.	Ю
5.	Д	12.	К	19.	С	26.	Ш	33.	Я
6.	Е	13.	Л	20.	Т	27.	Щ		
7.	Ё	14.	М	21.	У	28.	Ъ		

,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы зашифруйте фразу: Я УМЕЮ ДЕКОДИРОВАТЬ ДАННЫЕ!

Используя эту же кодировочную таблицу, расшифруйте текст:

252015383503040538351115030400 38

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения могут быть закодированы с помощью этой таблицы? Привести примеры.

8. При помощи таблицы Вижинера зашифровать текст «Криптографическая защита». Ключ «Шифр»
9. Шифры перестановки

h) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Антивирус

i) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Вирусное заражение

10. Аналитические методы шифрования

Зашифровать слово **ЖУК**

Ключ – матрица

A=

-1	1	1
3	2	4
5	-2	4

Выполнить проверку (расшифровать слово)

Вариант 7

1. Дана кодовая таблица азбуки Морзе

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

—— ——— •—•• ——— —•• —•—• —•——

2. Закодируйте с помощью азбуки Морзе слова **ПАРОЛЬ, ЭКРАНИРОВАНИЕ, КОДИРОВАНИЕ**

Таблица ASCII-кодов

SP	!	"	#	S	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	*B*	C	D	E	*F*	*G*	*M*	I	J	*K*	L	*M*	*N*	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	*Q*	*R*	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	*a*	*в*	c	d	e	*f*	g	h	i	*j*	*k*	l	*m*	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	*v*	*w*	*x*	*y*	*z*	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

3. Дана таблица ASCII-кодов

Расшифровать слово при помощи таблицы ASCII rкодов:

49 20 6C 6F 76 65 20 79 6F 75

4. Зашифрованная пословица.

Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).

Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .

Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.

Самый колючий зверь в лесу – это 12, 13.

А теперь прочитайте пословицу:

1, 2, 3, 4, 5, 1, 6

7, 8, 9, 10, 11

9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я ЗНАЮ МЕТОДЫ ШИФРОВАНИЯ ”. Зашифрованный текст должен быть записан без пропусков.

1.	А	8.	Ж	15.	Н	22.	Ф	29.	Ы
2.	Б	9.	З	16.	О	23.	Х	30.	Ь
3.	В	10.	И	17.	П	24.	Ц	31.	Э
4.	Г	11.	Й	18.	Р	25.	Ч	32.	Ю
5.	Д	12.	К	19.	С	26.	Ш	33.	Я
6.	Е	13.	Л	20.	Т	27.	Щ		
7.	Ё	14.	М	21.	У	28.	Ъ		

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы зашифруйте фразу: Я ЗНАЮ МЕТОДЫ ШИФРОВАНИЯ

Используя эту же кодировочную таблицу, расшифруйте текст:

252015383503040538351115030400 38

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения могут быть закодированы с помощью этой таблицы? Привести примеры.

8. При помощи таблицы Вижинера зашифровать текст «Профилактика заражения вирусами». Ключ «ВИРУС»
9. Шифры перестановки

j) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Скремблирование

k) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Туннелирование

10. Аналитические методы шифрования

Зашифровать слово **МАК**

Ключ – матрица

A=

3	0	1
1	2	-2
5	-2	4

Выполнить проверку (расшифровать слово)

Вариант 8

1. Дана кодовая таблица азбуки Морзе

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

—— ——— • — • • ——— — • • — • — • — • ——

2. Закодируйте с помощью азбуки Морзе слова **АУТЕНТИФИКАЦИЯ, ПАРОЛЬ, КОДИРОВАНИЕ**

Таблица ASCII-кодов

SP	!	"	#	S	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	*B*	C	D	E	*F*	*G*	*M*	I	J	*K*	L	*M*	*N*	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	*Q*	*R*	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	*a*	*в*	c	d	e	*f*	g	h	i	*j*	*k*	l	*m*	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	*v*	*w*	*x*	*y*	*z*	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

3. Дана таблица ASCII-кодов

Закодировать при помощи таблицы ASCII кодов следующий текст **PASCAL.** Результат представить в шестнадцатеричной СС

4. Зашифрованная пословица.

Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).

Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .

Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.

Самый колючий зверь в лесу – это 12, 13.

А теперь прочитайте пословицу:

1, 2, 3, 4, 5, 1, 6

7, 8, 9, 10, 11

9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я ЗНАЮ МЕТОДЫ КОДИРОВАНИЯ ”. Зашифрованный текст должен быть записан без пропусков.

1.	А	8.	Ж	15.	Н	22.	Ф	29.	Ы
2.	Б	9.	З	16.	О	23.	Х	30.	Ь
3.	В	10.	И	17.	П	24.	Ц	31.	Э
4.	Г	11.	Й	18.	Р	25.	Ч	32.	Ю
5.	Д	12.	К	19.	С	26.	Ш	33.	Я
6.	Е	13.	Л	20.	Т	27.	Щ		
7.	Ё	14.	М	21.	У	28.	Ъ		

,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы зашифруйте фразу: Я ЗНАЮ МЕТОДЫ КОДИРОВАНИЯ

Используя эту же кодировочную таблицу, расшифруйте текст: 252015383503040538351115030400 38.

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения могут быть закодированы с помощью этой таблицы? Привести примеры.

8. При помощи таблицы Вижинера зашифровать текст «Профилактика заражения вирусами». Ключ «ВИРУС».
9. Шифры перестановки

l) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Генератор паролей

m) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Вирусное заражение.

10. Аналитические методы шифрования

Зашифровать слово **СОК**

Ключ – матрица

A=

2	0	-1
1	2	-2
4	-2	3

Выполнить проверку (расшифровать слово)

Вариант 9

1. Дана кодовая таблица азбуки Морзе

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

—— ——— •—•• ——— —•• —•—• —•——

2. Закодируйте с помощью азбуки Морзе слова **ДАКТЕЛОСКОПИЯ, ПАРОЛЬ,СТЕНОГРАФИЯ**

Таблица ASCII-кодов

SP	!	"	#	S	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	*B*	C	D	E	*F*	*G*	*M*	I	J	*K*	L	*M*	*N*	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	*Q*	*R*	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	*a*	*в*	c	d	e	*f*	g	h	i	*j*	*k*	l	*m*	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	*v*	*w*	*x*	*y*	*z*	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

3. Дана таблица ASCII-кодов

Расшифровать слово при помощи таблицы ASCII rкодов:

32 2A 78 2B 79 3D 30

4. Зашифрованная пословица.

Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).

Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .

Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.

Самый колючий зверь в лесу – это 12, 13.

А теперь прочитайте пословицу:

1, 2, 3, 4, 5, 1, 6

7, 8, 9, 10, 11

9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я ЗНАЮ МЕТОДЫ КОДИРОВАНИЯ ”. Зашифрованный текст должен быть записан без пропусков.

1.	А	8.	Ж	15.	Н	22.	Ф	29.	Ы
2.	Б	9.	З	16.	О	23.	Х	30.	Ь
3.	В	10.	И	17.	П	24.	Ц	31.	Э
4.	Г	11.	Й	18.	Р	25.	Ч	32.	Ю
5.	Д	12.	К	19.	С	26.	Ш	33.	Я
6.	Е	13.	Л	20.	Т	27.	Щ		
7.	Ё	14.	М	21.	У	28.	Ъ		

,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы зашифруйте фразу: Я ЗНАЮ МЕТОДЫ КОДИРОВАНИЯ

Используя эту же кодировочную таблицу, расшифруйте текст:

252015383503040538351115030400 38

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения могут быть закодированы с помощью этой таблицы? Привести примеры.

8. При помощи таблицы Вижинера зашифровать текст «Биометрические характеристики». Ключ «ВИРУС»
9. Шифры перестановки
   n) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Атака на шифр

   o) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Защита информации

10. Аналитические методы шифрования

Зашифровать слово **ПАР**

Ключ – матрица

A=

2	0	-2
3	2	-2
4	2	0

Выполнить проверку (расшифровать слово)

Вариант 10

1. Дана кодовая таблица азбуки Морзе

А • —	Л • — • •	Ц — • — •
Б — • • •	М — —	Ч — — — •
В • — —	Н — •	Ш — — — —
Г — — •	О — — —	Щ — — • —
Д — • •	П • — — •	Ъ • — — • — •
Е •	Р • — •	Ы — • — —
Ж • • • —	С • • •	Ь — • • —
З — — • •	Т —	Э • • — • •
И • •	У • • —	Ю • • — —
Й • — — —	Ф • • — •	Я • — • —
К — • —	Х • • • •	

Расшифруйте (декодируйте), что здесь написано (буквы отделены друг от друга пробелами)?

—— ——— • — • • ——— — • • — • — • — • ——

2. Закодируйте с помощью азбуки Морзе слова **АНТИВИРУС, МАСКИРОВКА, ЗАРАЖЕНИЕ**

Таблица ASCII-кодов

SP	!	"	#	S	%	&	`	(	)	*	+	,	-	.	/
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
@	A	*B*	C	D	E	*F*	*G*	*M*	I	J	*K*	L	*M*	*N*	O
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
P	*Q*	*R*	S	T	U	V	W	X	Y	Z	[	\	]	^	_
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
`	*a*	*в*	c	d	e	*f*	g	h	i	*j*	*k*	l	*m*	n	0
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
p	q	r	s	t	u	*v*	*w*	*x*	*y*	*z*	{	|	}	~	
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127

3. Дана таблица ASCII-кодов

Закодировать при помощи таблицы ASCII кодов следующий текст **NORTON COMMANDER.** Результат представить в шестнадцатеричной СС

4. Зашифрованная пословица.

Разгадайте слова в предложениях (каждой букве соответствует определенная цифра).

Чтобы рубить дрова, нужен 14, 2, 3, 2, 7 , а чтобы полить огород – 10, 4, 5, 1, 6 .

Рыбаки сделали во льду 3, 7, 2, 7, 8, 9, 11 и стали ловить рыбу.

Самый колючий зверь в лесу – это 12, 13.

А теперь прочитайте пословицу:

1, 2, 3, 4, 5, 1, 6

7, 8, 9, 10, 11

9, 4, 7, 4, 13, 12, 14.

5. Заменяя каждую букву ее порядковым номером в алфавите, зашифруйте фразу: “Я ЗНАЮ МЕТОДЫ КОДИРОВАНИЯ ”. Зашифрованный текст должен быть записан без пропусков.

1.	А	8.	Ж	15.	Н	22.	Ф	29.	Ы
2.	Б	9.	З	16.	О	23.	Х	30.	Ь
3.	В	10.	И	17.	П	24.	Ц	31.	Э
4.	Г	11.	Й	18.	Р	25.	Ч	32.	Ю
5.	Д	12.	К	19.	С	26.	Ш	33.	Я
6.	Е	13.	Л	20.	Т	27.	Щ		
7.	Ё	14.	М	21.	У	28.	Ъ		

,

6. Дана кодировочная таблица (первая цифра кода – номер строки, вторая – номер столбца).

	0	1	2	3	4	5	6	7	8
0	А	Б	В	Г	Д	Е	Ё	Ж	З
1	И	К	Л	М	Н	О	П	Р	С
2	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
3	Ы	Ь	Э	Ю	Я	_	.	,	?
4	:	;	-	!	»				

С помощью этой кодировочной таблицы зашифруйте фразу: Я ЗНАЮ МЕТОДЫ КОДИРОВАНИЯ

Используя эту же кодировочную таблицу, расшифруйте текст:

252015383503040538351115030400 38

7. Каждая буква алфавита может быть заменена любым числом из соответствующего столбика кодировочной таблицы.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
20	13	59	25	75	43	19	29	06	65	74	48	36	28	16
52	39	07	49	33	85	58	80	50	34	17	56	78	64	41
89	67	93	76	18	51	87	66	81	92	42	79	86	05	57

Какие сообщения могут быть закодированы с помощью этой таблицы? Привести примеры.

8. При помощи таблицы Вижинера зашифровать текст «Технологии аутентификации». Ключ «ВИРУС»
9. Шифры перестановки

p) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Криптографическая защита

q) Закодировать методом Гамильтона (создать свой маршрут(ы)).

Кодирование информации

10. Аналитические методы шифрования

Зашифровать слово **ТИР**

Ключ – матрица

A=

2	0	-2
3	2	-2
1	-2	0

Выполнить проверку (расшифровать слово)

Раздел 5. Экранирование. Классификация межсетевых экранов.

Самостоятельная работа №7: Использование межсетевых экранов (брандмауэров) для защиты информации в сетях

Цель работы: изучить классификацию сетевых экранов, овладеть навыками работы с сетевой программой ATGuard.

Теоретические сведения

Требования к установке :Операционная система: Windows 95, Windows 98, Windows NT 4.0 + Service Pack 3, Windows 2000 и выше. Не поддерживаются: Windows NT 3.51, Windows 3.1x, Windows ME, Mac, Linux/UNIX.

Компьютер: на Intel 80386DX или выше (для Windows 95), или на 486/25 или выше (для Windows NT 4.0).

Около 3 MB свободного дискового пространства.

Установленный протокол TCP/IP.

Общие сведения о межсетевых экранах.

Межсетевой экран(firewall или брандмауэр) является программно-аппаратным средством осуществления сетевой политики безопасности в выделенном сегменте IP-сети.

В сфере компьютерных сетей межсетевой экран представляет собой барьер, защищающий от вторжения злоумышленников во внутреннюю локальную сеть для того, чтобы скопировать, изменить или стереть информацию либо воспользоваться памятью или вычислительной мощностью работающих в этой сети компьютеров. Межсетевой экран призван обеспечить безопасный доступ к внешней сети и ограничить доступ внешних пользователей к внутренней сети (см. рис 1.)

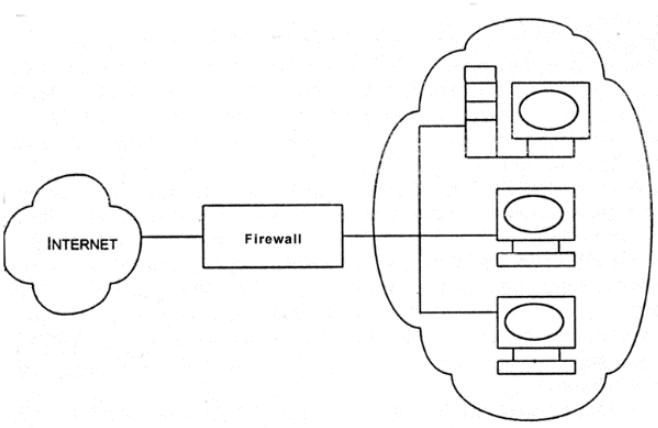


Рисунок 22. Схема установления firewall.

Название «брандмауэр», может относиться к одному устройству или одной программе. Термин «межсетевой экран» был принят для обозначения совокупности компонентов, которые находятся между вашей сетью и внешним миром и образуют защитный барьер.

Брандмауэр не может защитить от:

✓ ***вирусов.*** Хотя некоторые брандмауэры и способны распознавать вирусы в проходящем через них трафике, существует множество способов спрятать вирусы в программе. Если даже в описании вашего брандмауэра заявлена функция антивирусной проверки, не выключайте проверку вирусов на отдельных компьютерах в сети;

✓ ***«троянских коней»***. Как и в случае с вирусами, блокировать проникновение в сеть «троянских коней» (Trojan horses) достаточно сложно. Пользователь нередко поддается искушению загрузить программу из Internet или открыть прикрепленный к сообщению электронной почты файл, проложив тем самым путь в систему вредоносной программе;

✓ ***«социальной инженерии»***. Термин «social engineering» возник недавно и применяется для описания методов получения хакерами информации от доверчивых пользователей. Часто люди готовы сообщить свой пароль любому, кто позвонил по телефону и отрекомендовался представителем службы безопасности, что-нибудь «проверяющим».

Межсетевой экран не в состоянии остановить невоздержного на язык сотрудника

✓ ***некомпетентности***. Плохо подготовленные сотрудники или небрежное руководство приводят к ошибкам в настройках локальной сети и межсетевого экрана. Если сотрудники не понимают, как работает брандмауэр и как правильно его настраивать, не исключено, что это будет способствовать возникновению проблем;

✓ ***атаки изнутри***. Межсетевой экран не может предотвратить злонамеренные действия внутри вашей сети. Это одна из причин, по которой безопасность компьютеров в сети остается важной проблемой и после установки брандмауэра.

Интерфейс AtGuard.

После инсталляции программы и перезагрузки компьютера Вы обнаружите в системном трее (system tray) иконку запущенного AtGuard'а , а вверху экрана его же панель (dashboard)

Рисунок 23. Внешний вид dashboard

Это означает, что инсталляция и первый запуск прошли успешно. Двойной щелчок на иконке открывает окно настроек.

Установка флажка Enable web filters включает блокирование, опции секретности и активные установки фильтров, определенные в диалоговом окне Web (HTTP) Filters. Уберите этот флажок, если Вы хотите выключить все web-фильтры.

Enable web filters действует как главный переключатель, который позволяет вам отменять индивидуальные установки фильтра в диалоговом окне Web (HTTP) Filters и отключать всю фильтрацию веб-трафика. Когда Вы отключаете web-фильтры, программное обеспечение прекратит фильтровать любые HTTP данные, входящие или исходящие от рабочей

станции. Если Вы устанавливаете или снимаете флажок Enable web filters, то эти изменения начинают действовать сразу.

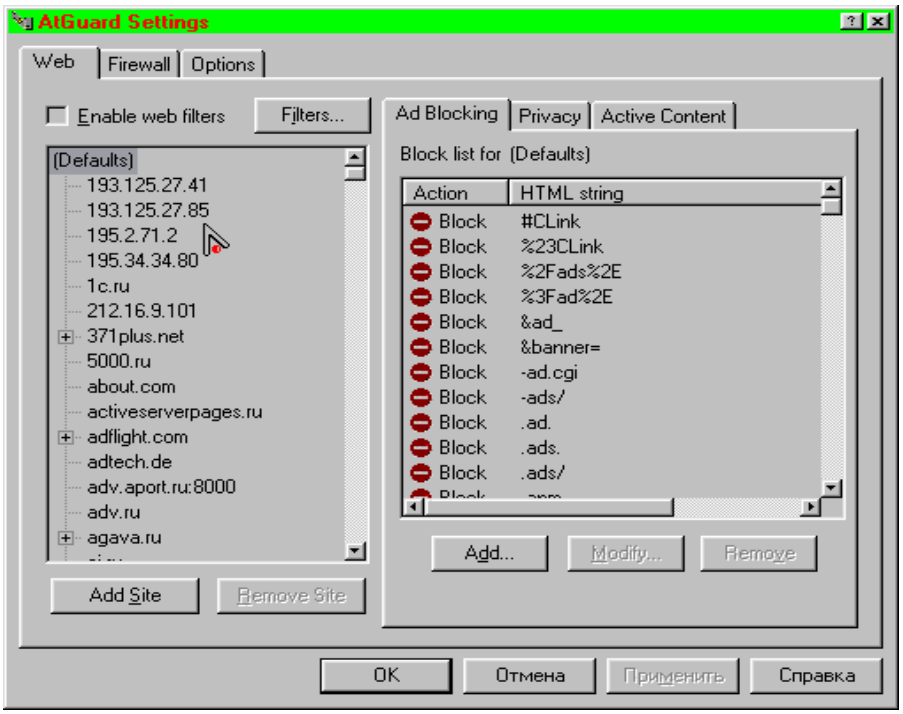


Рисунок 24 Окно настроек Web

Опции в этом диалоговом окне позволяют Вам включать или выключать индивидуальные web-фильтры, cookie и Java/ActiveX мониторы. Вы можете также модифицировать список портов, которые AtGuard контролирует для HTTP связи, когда web-фильтры включены. Установите флажки Ad Blocking, Privacy, Active Content и Cookie Assistant в этом диалоговом окне - этого будет достаточно. Флажок Java/ActiveX Assistant можете не устанавливать, иначе AtGuard будет каждый раз задавать ненужные вопросы, что очень утомляет.

HTTP Port List - сетевые сервисы (типа HTTP или FTP) используют специфические порты на вашем компьютере. Например, HTTP-связь обычно проводится через порт 80. Web-фильтры AtGuard'а контролируют весь HTTP-трафик, посланный и полученный через порты, которые указаны в Port List, применяя блокирование, секретность и другие опции, которые Вы определили. Ваша рабочая станция может соединяться с Интернетом посредством proxy-сервера, при этом весь HTTP-трафик проходит через порт,

используемый этим proxy-сервером. Или Вы можете использовать приложение, которое инициирует HTTP-связь через нестандартный порт. Если HTTP-трафик идет через нестандартный порт, вы должны добавить номер этого порта в Port List. Изменения в настройках фильтров вступают в действие сразу после нажатия кнопки "Применить".

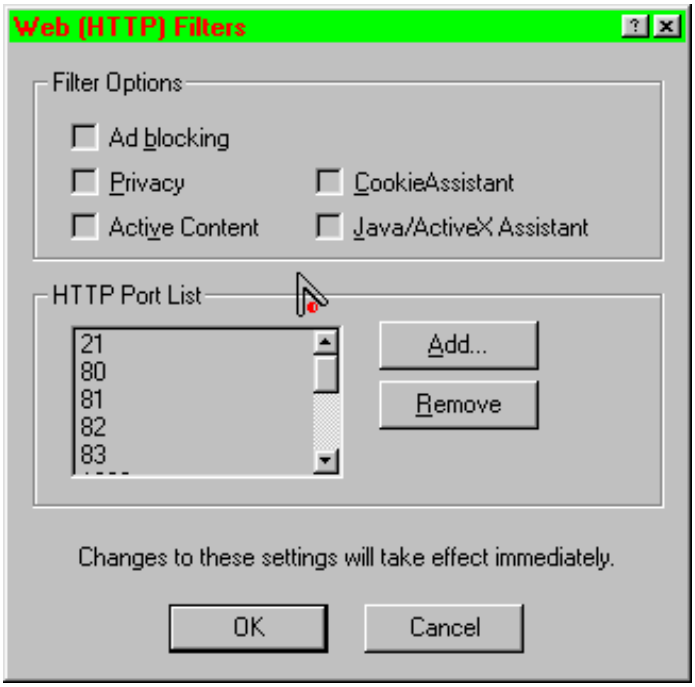


Рисунок 25 - Окно настроек Web Filters

Add Site - нажмите эту кнопку, чтобы открыть диалоговое окно New Site/Domain, которое используется для добавления нового сайта или домена к иерархическому списку сайтов в левом окне. Напечатайте имя web-сайта или имя домена и нажмите OK. После добавления сайта Вы можете выбрать его в списке. Используйте установки Ad Blocking, Privacy, Active Content, чтобы определить правила и набор блокировок, которые AtGuard использует только когда Вы посещаете конкретный web-сайт.

Ad Blocking - эти установки позволяют поддерживать блокирующий список по умолчанию и специфические для конкретных сайтов блокирующие списки, которые используются, чтобы указать, чего не нужно отображать на веб-страницах. Когда блокирующий фильтр включен, все HTML-страницы просматриваются на предмет наличия HTML-строк, специфичных для

конкретного сайта, указанного в списке для блокирования, плюс значения по умолчанию, определенные для всех сайтов. Любой HTML-код, который содержит разрешенную к блокированию строку, будет удален из web-страницы AtGuard'ом прежде, чем эта страница будет интерпретирована и показана браузером.

Privacy - установки секретности позволяют определять правила, управляющие тем, как Ваш браузер обрабатывает запросы о различных типах информации, сделанных сайтами, которые Вы посещаете.

Cookies - это информация, которую web-серверы сохраняют на вашем компьютере для более позднего использования. Web-серверы могут читать cookies, чтобы следить, сколько раз вы их посетили, когда и какую информацию вы просматривали. Они могут даже использовать cookies, чтобы передать эту информацию другим web-серверам, типа серверов рекламы. Положительная сторона cookies в том, что они могут использоваться, чтобы сохранить вашу собственную конфигурацию web-сайта, запоминать, что вы поместили в вашу "покупательскую корзину" в интерактивном магазине или сохранять имя пользователя и пароль для сайтов подписки. Чтобы обеспечить максимальную секретность, разрешите использование cookies только проверенным сайтам, которым вы доверяете.

Referer - позволяет вам определить, узнают ли третьи сайты о том, из какого места поступил запрос данных с этих серверов.

Refer field - эти поля используются, чтобы обеспечить "третьи" сайты информацией относительно сайта, с которого поступил запрос данных из их сервера. Refer поля позволяют веб-серверам знать, где вы только что были. Вполне возможно, что вы не захотите, чтобы эта информация становилась известной. Иногда это опасно. Например, некоторые онлайновые почтовые службы подставляют пароль просто в сетевой путь, который отображается в браузере. Если вам пришло письмо, содержащее ссылку на какой-нибудь сайт, и вы последовали по ссылке прямо из web-mail, то в статистике сайта на, который вы пришли, будет зафиксирован адрес страницы, содержавшей

ссылку на него - refferer. А этот самый refferer может содержать ваш логин и пароль к вашему почтовому ящику. Некоторые сайты не позволяют заходить на них с включенным Block refer fields.

Browser (User-agent) - позволяет определить, обеспечиваются ли сайты информацией, какой браузер вы используете.

E-mail (From) - позволяет определить, получат ли сайты адрес электронной почты, который использует ваш браузер, чтобы идентифицировать вас как отправителя почты.

Active Content - эти установки позволяют Вам предотвращать выполнение следующих типов программ: JavaScript, Java applets, ActiveX controls. Кроме того, можно установить, чтобы анимационные изображения проигрывались только один раз. Когда блокирование активного содержимого включено, все HTML страницы просматриваются, и любой HTML-код, который активизирует нежелательное содержание, будет удален из страницы AtGuard'ом прежде, чем страница интерпретируется и отобразится веб-браузером.

Совет: включите все флажки. При этом перестанут появляться всплывающие окна на некоторых сайтах. С одной стороны в большинстве случаев JavaScript - это средство украшения. С другой стороны, расположенный на странице java-апплет вполне может, например, отправить куда-нибудь письмо с важной информацией, т.к. апплет не ограничен в праве соединения с smtp-портом сервера, с которого он был загружен.

AtGuard settings / Firewall

Установки файрвола определяют, должен ли AtGuard запретить или разрешить приложениям на вашем компьютере посылать или получать информацию по TCP/IP. Для этого имеется список правил, которые описывают, какие типы сетевой активности разрешаются, и через какие

сервисы приложения могут связываться. Вы можете добавлять, изменять, или удалять правила.

Включите опции Enable firewall, Enable RuleAssistant (interactive learning mode)

Для временного отключения какого-либо правила уберите флажок напротив соответствующей строки в списке правил.

Совет: правила обрабатываются в порядке, в котором они перечислены.

Если правило "Блокировать" (Block) или "Разрешить" (Permit) указано, все оставшиеся правила игнорируются. Другими словами если вы, например, закрыли порт номер N, а ниже прописано правило, разрешающее использование этого порта, то оно будет проигнорирована и соединение по этому порту будет закрыто.

Если правило "Игнорировать" (Ignore) указано, тип связи, которая была предпринята, регистрируется в лог-файле firewall'a и затем обработка продолжается, пока не произойдет какого-либо другого соответствия. Если не найдется никакого правила, связь или блокируется (по умолчанию) или вызывается RuleAssistant. Чтобы перемещать правило по списку, выделите соответствующую строку и затем используйте кнопки "стрелка вверх" или "стрелка вниз" для помещения правила в соответствующую позицию.

Любое TCP/IP соединение, для которого нет firewall правила, блокируется по умолчанию. Если Вы хотите выборочно блокировать или разрешать соединение, для которого нет правила, установите флажок Enable RuleAssistant (интерактивный режим изучения).

Если флажок RuleAssistant включен, вам будет автоматически задан вопрос запретить (Block) или разрешить (Permit) соединение всякий раз, когда приложение на вашей рабочей станции или какое-то приложение извне делает попытку установить связь, для которой не описано никаких правил в firewall. В результате вашего решения AtGuard разрешает или блокирует

сетевую связь и может создавать правило firewall, которое применяется в дальнейшем для данного типа сетевого соединения.

Add Firewall Rule

Name. Это просто краткое описание вашего правила. Имя правила также появится в Firewall лог-файле, если вы выберете регистрацию события для этого правила.

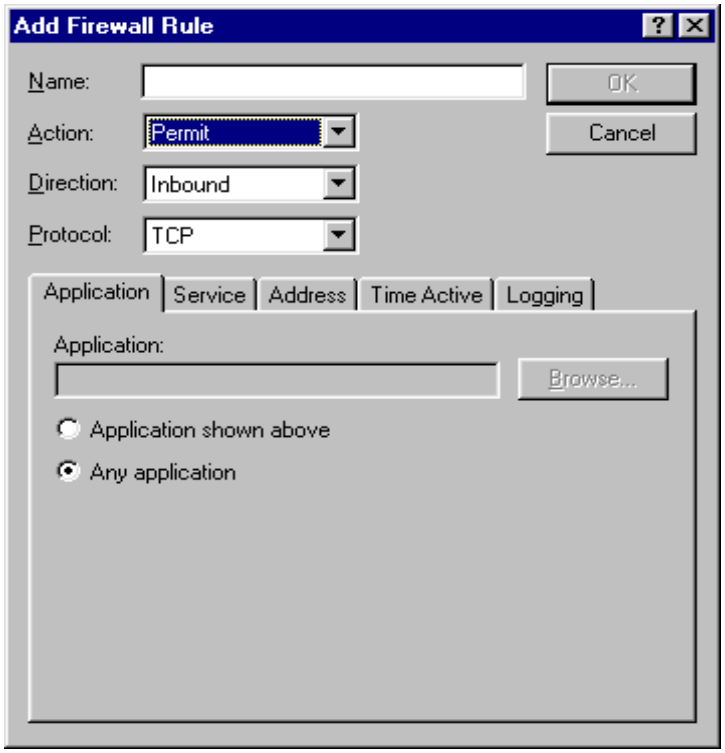


Рисунок 26 - Окно Add firewall rule

Action. Permit (разрешить), Block (запретить), Ignore (игнорировать). Регистрирует событие в лог-файле. Затем обработка события продолжается, пока не будет найдено соответствующее правило. Если никакое правило не будет найдено связь или блокируется (по умолчанию) или вызывается RuleAssistant.

Как использовать правило Ignore? Когда задано правило Ignore, происходит регистрация события и затем обработка продолжается пока не будет найдено правило разрешающее или запрещающее данный тип связи. Обратите внимание: для того чтобы правило Ignore сработало, оно должно появиться в списке правил firewall'a выше любого правила описывающего

данный тип связи. Лучше поместить все правила Ignore в верхнюю часть списка firewall.

Действие Ignore предназначено, чтобы позволить Вам регистрировать события до предписания "Разрешить" или "Блокировать", которое применяется к этому типу связи. Например, есть разрешающее правило firewall, которое позволяет вашему FTP серверу связываться с любым сетевым адресом. Можно отследить, как часто пользователи с определенного сетевого адреса соединялись с вашим FTP сервером, задав игнорирующее правило для регистрации соединений. Правило Ignore должно предшествовать правилу Permit.

Direction. Inbound связь включает пакеты, посланные вашему компьютеру. Outbound связь включает пакеты, посланные вашим компьютером. Either - связь в любом направлении.

Protocol. Определяет, к какому протоколу связи применяется правило: TCP, UDP, или TCP и UDP, ICMP...

TCP - стандартный протокол Интернета транспортного уровня, обеспечивает надежную полнодуплексную связь. Программное обеспечение, реализующее протокол TCP, обычно постоянно находится в операционной системе и использует IP протокол, чтобы передать информацию. Примеры TCP приложений и сервисов - FTP, web-браузер, email и IRC.

UDP - транспортный уровень в TCP/IP сетях. UDP - низкоуровневый протокол, который использует IP, чтобы доставить пакеты. Примеры сервисов и приложений, которые используют UDP - DNS, NetBIOS.

ICMP - протокол межсетевых управляющих сообщений.

Application. Эта опция позволяет определять, применяется ли правило к конкретному приложению или к любому приложению, которое делает попытку сетевой связи, определенной правилом.

Service. Позволяет определять, применяется ли правило к локальным или удаленным сервисам и применяется ли это к одиночному определенному

сервису или к любому сервису, который делает попытку сетевой связи, определенной правилом.

Сервисы - протоколы, которые используются, чтобы позволить одному компьютеру обращаться к специфическому виду данных, сохраненных в другом компьютере. Например, HTTP серверы используют протокол передачи гипертекста, чтобы обеспечить по всему миру сервис web, FTP серверы предлагают сервисы протокола передачи файла, SMTP серверы используют простой протокол транспорта почты, чтобы посылать почту, и POP серверы используют POP протокол, чтобы передать электронную почту.

Time Active. Используйте эти установки, чтобы определить время когда, правило будет действовать.

Logging. Определяет, что событие регистрируется в лог-файле, когда устанавливается описанное правилом соединение.

AtGuard settings / Options

Show taskbar icon - при запущенном AtGuard показывать его иконку в панели задач.

Show dashboard window - при запущенном AtGuard показывать dashboard.

Enable password protection - если выбрано, то как только вы попытаетесь открыть диалоговое окно AtGuard Settings, окно Dashboard Properties, Event Log, или окно статистики, вы будете должны ввести пароль.

StartUp Options / Run at network startup. Когда эта опция выбрана, AtGuard запускается автоматически, если вы открываете сетевое соединение, и останавливается также автоматически, когда вы закрываете ваше сетевое соединение.

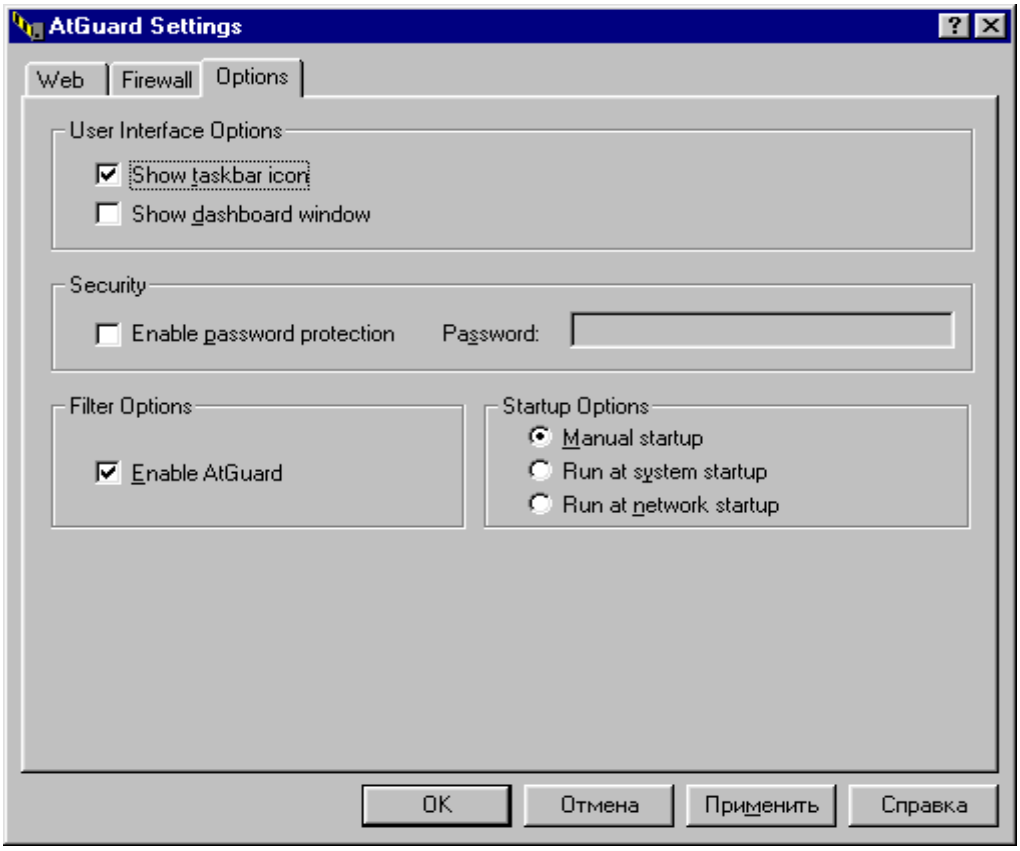


Рисунок 27 - Окно Options

AtGuard settings / Dashboard

Рисунок 28 - Панель AtGuard

Во-первых, установите все флажки. Во-вторых, чтобы понять назначение элементов управления и отображения данных на этой панели, просто задержите указатель мыши на интересующем объекте – всплывет подсказка.

Справа видна мусорная корзина. Мусорная корзина нужна, чтобы можно было избавиться от ненужных вам изображений (рекламные баннеры) и даже определенных частей HTML-кода.

Для помещения, например, баннера в корзину, щелкните правой кнопкой мыши на баннере. Выберите пункт Copy link location. Затем

щелкните мышкой на изображение мусорной корзины и выберите пункт Paste Into Trashcan, далее ответьте Yes. Аналогичным способом можно избавиться и от счетчиков.

AtGuard / Event Log

Мощное средство для анализа находится в меню Event Log.

Ad Blocking. Отображает содержание файла событий (лог-файла) Ad Blocking. Здесь показано, что и когда было блокировано AtGuard'ом. Указывается HTML-код, который был удален, чтобы заблокировать нежелательные изображения, web-страница из которой было удалено и URL, который вызвал блокировку.

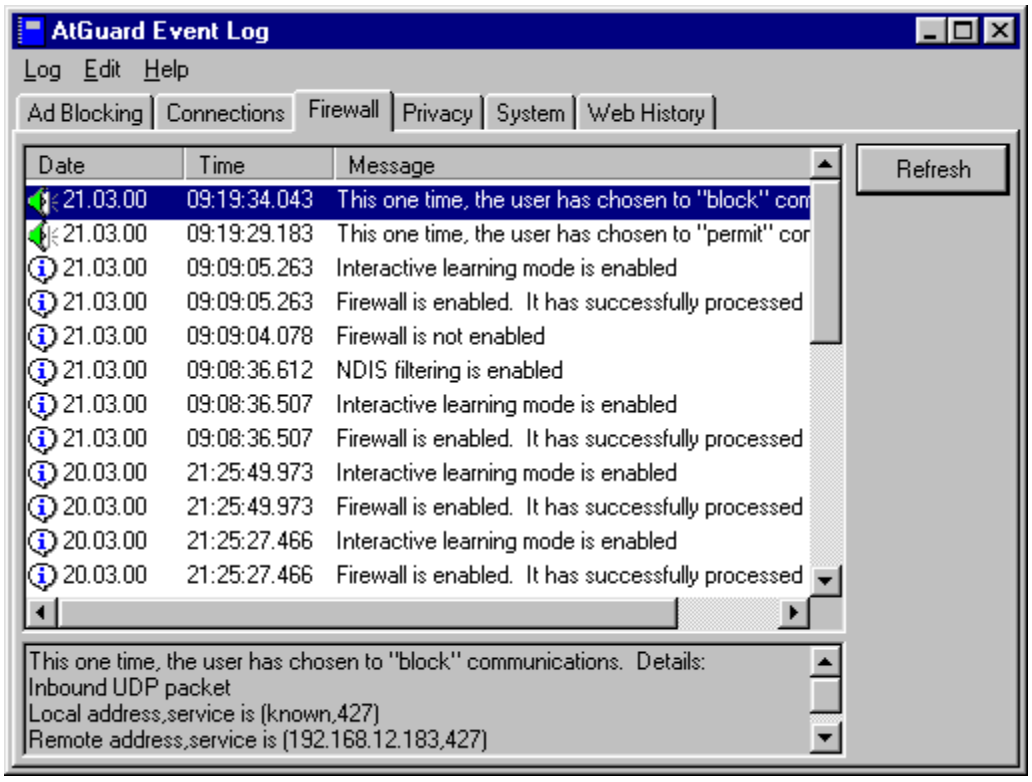


Рис 8. Окно Event Log

Connections. Показывает содержание лог-файла ваших соединений. Показывается хронология всех TCP/IP соединений, сделанных вашей рабочей станцией. Кнопка Refesh обновляет хронологию соединений.

Firewall. Лог-файл событий firewall.

Privacy. Информация о блокированных cookies, referers и т.п.

System. Информация о действиях AtGuard, таких как запуск AtGuard как сервиса Windows и действия по IP фильтрации. Запись inbound и outbound попыток соединения и действия пользователя в ответ на эти попытки.

Web History. Перечисляются посещенные вами URL'ы, показывая хронологию активности в web.

Несколько простых практических приемов

Сразу после инсталляции, зайдите в настройки Firewall. Снимите флажки Default Inbound ICMP, Default Inbound DNS, Default Inbound Bootp, Default Inbound NetBIOS

Для дальнейшей настройки Inbound DNS необходимо узнать DNS адрес вашего провайдера. Затем Settings -> Firewall -> Add. В поле "Name" впишите DNS, поля "Action" и "Directon" изменять не нужно. Поле "Protocol" установите "TCP or UDP 3". Здесь же нажмите закладку "Service" и установите "Remote service" в "Single service", в появившееся поле впишите 53 (номер порта домена). Теперь выберите закладку "Address" и поставьте "Remote address" = "Host address" и в появившееся поле впишите адрес DNS вашего провайдера, нажмите OK. Теперь повторите эту же операцию только измените "Directon" на "Inbound". Повторите то же самое и для остальных адресов DNS, если они есть. Все, настройка DNS закончена.

Как можно защититься от рекламных баннеров. Правой кнопкой мыши нажимаем по баннеру. В всплывающем меню выбираем "Копировать ярлык". Вызываем AtGuard Settings -> Web. Выбираем в списке (Defaults), Ad Blocking -> Add. В появившемся окошке нажимаем правой кнопкой мыши, выбираем «вставить». Например, для linkexchange будет такая строка http://www.linkexchange.ru/users/091164/goto.map Ее нужно отредактировать, чтобы получилось linkexchange.ru/users/ ибо удаленная часть может изменяться от сайта к сайту. Всё. Еще пример. http://www.reklama.ru/cgi-bin/href/myclub?3353573 После правки: reklama.ru/cgi-bin/ .

Есть еще один более простой способ. Если у вас запущен Dashboard, то в правом углу будет Trashcan ("Мусорная корзина") AtGuard'a. Чтобы переместить рекламу в мусорку при использовании MSIE 4.0, выберите рисунок и мышкой перетащите его в Trashcan. При использовании Netscape или MSIE 3.0, щелкните правой кнопкой мыши на баннере. Чтобы заблокировать все подобные ссылки, выберите пункт Copy link location (если картинка грузится с того же сервера, что и страница). Если баннер грузится с сервера рекламодателя (например, это могут быть баннеры сетей reklama.ru, linkexchange), то выберите пункт Copy image location. Затем щелкните правой кнопкой мыши на иконке Trashcan и выберите пункт Paste (Вставка) из всплывающем меню.

Как говорилось выше, нашу задачу сильно облегчает то, что вся реклама объединяется или уже объединена в рекламные (баннерные) сети. Поэтому закрыв для себя AtGuard'ом один рекламный сайт, вы избавитесь от сотен и сотен рекламных баннеров. Это сохранит вам деньги, нервы и высокую скорость соединения**.**

Для захода на такие сайты с познавательной целью, вам нужно будет на время отключить web filters.

Обязательно установите все флажки в окне AtGuard Settings -> Web -> Active Content.

В окне AtGuard Settings -> Firewall включите Enable Rule-Assistant для интерактивного обучения вашего стража. Если в процессе вам встретится непонятное на первый взгляд сообщение о каком-либо соединении, запретите его, потом всегда можно посмотреть в лог-файлах.

Защита от атак WinNuke.

Чтобы защититься от атаки WinNuke, нужно поставить соответствующий фильтр. Атака WinNuke заключается в посылке OOB-данных на 139 порт. Таким образом, достаточно будет заблокировать TCP-соединения с 139 портом. Однако 139 порт используется для NetBIOS и

потому при работе в локальной сети его перекрывать не следует. Но если вы заходите в Сеть с домашнего компьютера, то блокируйте смело.

В настройке Firewall добавляем новое правило – “Add”. Назовем “WinNuke”, действие – “Block”, направление только входящие – “Inbound”, протокол “TCP”. Далее на закладках: Any Application. Service: remote - "Any", local – single service 139 порт. Остальные настройки можно оставить по умолчанию. Включите протоколирование, чтобы можно было видеть, что вы подверглись атаке. По аналогии можно настроить и другие фильтры.

Лабораторное задание

Задание 1. Изучите функции программы, пользуясь данным описанием.

Задание 2. Установить с диска, указанного преподавателем, 2 виртуальные машины. Настроить локальную сеть между двумя виртуальными машинами, если требуется.

Задание 3. Установить с диска, указанного преподавателем, на обе виртуальные машины AtGuard.

Задание 4. Попробуйте обменяться пакетами запрещенного типа при включенном и при выключенном AtGuard с другим компьютером сети.

Задание 5. Создать правило запрещающее получение доступа к компьютеру с удаленного компьютера (с конкретного IP-адреса или с определенного имени компьютера), попытаться обратиться с запрещенного компьютера и отследить реакцию AtGuard.

Задание 6. Подготовить компьютер к безопасной работе в Интернете (блокирование cookies, active-content, java-script).

Задание 7. Ответить на контрольные вопросы. Сдать работу преподавателю

Контрольные вопросы

1. Что такое ATGuard и для чего применяется?
2. От чего защищает и от чего не защищает ATGuard?
3. Как ATGuard вырезает баннеры и активное содержимое?
4. Зачем скрывать информацию о cookies файлах?

5. Как можно избирательно устанавливать настройки для определенных сайтов?
6. Как посмотреть статистику и лог-файлы?
7. Как работает ATGuard с прокси-серверами?

Содержание отчета: выполненное задание для самостоятельной работы и ответы на контрольные вопросы необходимо выслать для проверки преподавателю.

Самостоятельная работа №8 Типы межсетевых экранов. Конспектирование.

Конспект - универсальная форма записи. Он объединяет все или две любые из этих форм. Главное требование к конспекту - запись должна быть систематической, логически связной.

Конспекты можно условно подразделить па четыре типа: плановые, текстуальные, свободные и тематические.

Плановый конспект составляется с помощью предварительного плана литературного источника. Каждому вопросу плана в такой записи соответствует определенная часть конспекта. Если какой-то пункт плана не требует дополнений и разъяснений, его не следует сопровождать текстом. Это одна из особенностей короткого плана-конспекта, помогающего лучше усвоить материал уже в процессе его изучения.

Составление такого конспекта приучает последовательно и четко излагать свои мысли, работать над источником, обобщая его содержание в формулировках плана. Краткий, простой, ясный по своей форме план-конспект - незаменимое подспорье при необходимости быстро подготовить доклад, выступление па семинаре, конференции.

Когда конспект создается на основе плана, то надо иметь в виду, что характерную для плана определенную схематичность, неполноту предстоит исправить в новой записи. Именно это - одна из основных задач написания

такого конспекта. Здесь есть возможность внести в запись недоступные для плана подробности, обстоятельно раскрыть его пункты.

Самый простой плановый конспект составляется в виде ответов на пункты плана, сформулированные в вопросительной форме. В процессе подготовки, а иногда и при последующей переделке плановый конспект может отразить логическую структуру и взаимосвязь отдельных положений.

Текстуальный конспект составляется в основном из цитат. Они связываются друг с другом логическими переходами. Конспект может быть снабжен планом и включать отдельные тезисы в изложении составителя или автора.

Текстуальный конспект - хороший источник дословных высказываний автора. Он помогает выявить спорные моменты. Особенно целесообразно использовать этот вид конспектирования при изучении материалов для сравнительного анализа положений, высказанных рядом авторов.

Существенный недостаток текстуального конспекта заключается в том, что он мало активизирует внимание и память. Это особенно проявляется в случаях, когда конспект составлен без глубокой проработки материала, без его усвоения. Отсюда - необходимость постоянной работы над этими видами записи.

Текстуальный конспект при последующей его разработке или даже в процессе составления может превратиться в свободный конспект - сочетание цитат, тезисов, собственных суждений составителя. Такой конспект требует умения самостоятельно четко и кратко формулировать основные положения. Для этого необходимо глубокое осмысление материала, большой и активный запас слов. Само составление такого конспекта успешно развивает эти качества. Свободный конспект, по всей видимости, наиболее полноценный, но он довольно трудоемок, требует определенного опыта и эрудиции.

Тематический конспект дает в большей или меньшей мере ответ на поставленный вопрос-тему. Специфика этого типа конспекта заключается в

том, что, разрабатывая определенную тему по ряду источников, он не отображает всего содержания используемых произведений.

Составление тематического конспекта помогает всесторонне осмыслить тему, проанализировать различные точки зрения на один и тот же вопрос, мобилизовать свой интеллектуальный «багаж».

Разновидностью тематического конспекта является обзорный тематический конспект. Это тематический обзор на определенную тему с использованием нескольких источников.

К обзорному тематическому конспекту можно отнести и хронологический конспект. Как видно из названия, основное, чему подчинена запись в данном случае, это хронологическая последовательность событий на фоне отражения самих событий. В отличие от обзорного конспекта на ту же тему хронологический конспект более краткий и конкретный.

Раздел 6. Компьютерные вирусы как особый класс разрушающих программных воздействий и защита от них.

Лабораторная работа №8: Изучение основных признаков присутствия на компьютере вредоносных программ

Цель работы: получение практических навыков по выявлению *вредоносных программ* на локальном компьютере под управлением Microsoft *Windows* XP.

Задание 1. Изучение настроек браузера

Действия *вредоносных программ* бывают явными, косвенными и скрытыми. Если первые можно заметить сразу, то косвенные и тем более скрытые требуют от пользователя определенной квалификации - необходимо знать что, где и как нужно искать.

Не все вредоносные программы стремятся спрятаться – многие из них ведут себя весьма активно, то есть явно проявляют себя. Это характерно для троянских и, так называемых, рекламных программ. Явные проявления наиболее часто выражаются в неожиданно появляющихся рекламных баннерах, в изменении *домашней страницы* в браузере или появляющихся на рабочем столе окнах, как показано на рис. 19.1.

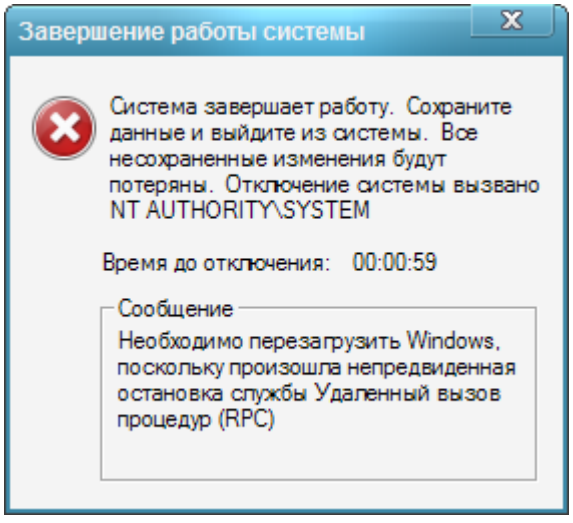


Рисунок 28 – Пример системного вызова.

Некоторые рекламные вредоносные программы являются по сути безвредными, так как их основная цель – привлечь внимание к определенному товару или услуге.

Вредоносными программами с косвенными признаками называются программы, которые пытаются отключить или полностью удалить *антивирус*, блокировать обновление антивирусных баз. Соответственно, если *антивирус* вдруг ни с того, ни с сего перестал запускаться, либо перестали открываться сайты антивирусных компаний при том, что в целом доступ в Интернет работает нормально, это могут быть проявления вирусов. Вредоносные программы, которые никак не выдают себя, называются скрытыми. Обнаружить их можно только по подозрительным процессам в памяти компьютера, в нестандартной сетевой активности, в изменениях системного реестра.

В этом задании предлагается исследовать явные проявления вирусной активности на примере несанкционированного изменения настроек браузера. Этот механизм используется для того, чтобы вынудить пользователей зайти на определенный сайт. Для этого меняется адрес *домашней страницы*, то есть адрес сайта, который автоматически загружается при каждом открытии браузера.

1. Откройте браузер **Internet Explorer**, воспользовавшись одноименным ярлыком на рабочем столе или в системном меню **Пуск / Программы**

2. Если у Вас открыт и настроен доступ в Интернет и после установки операционной системы стартовая страница изменена не была, должна открыться страница по умолчанию.

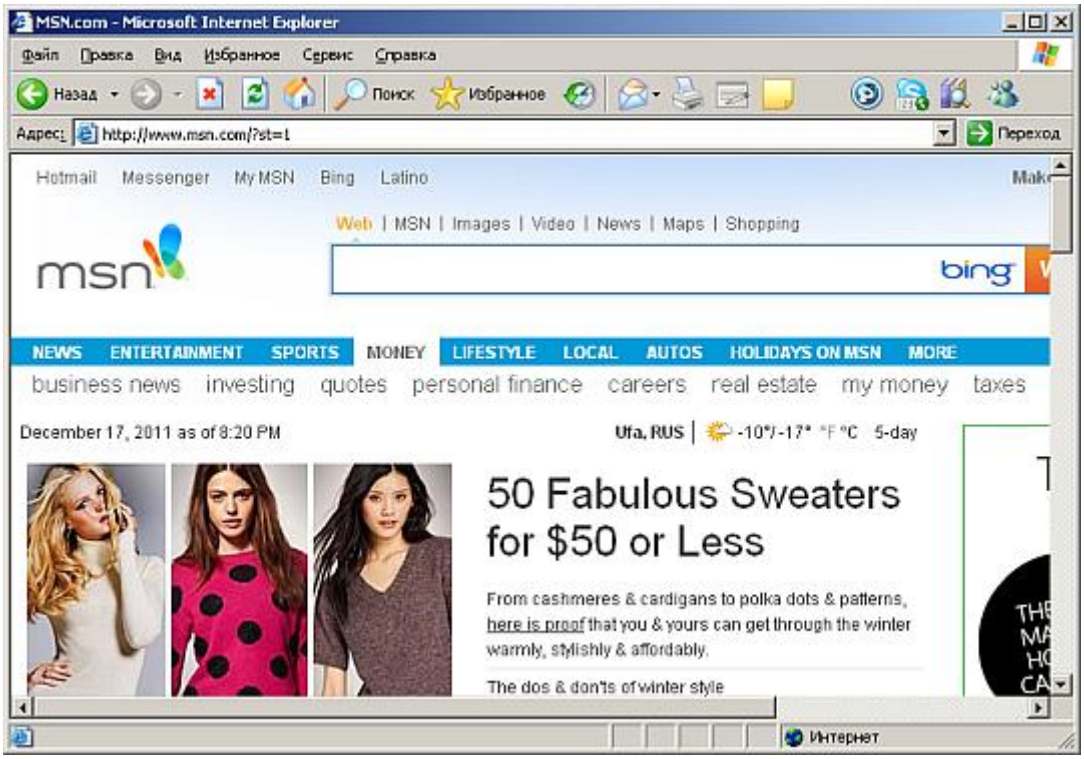


Рисунок 29 – Домашняя страница

3.Для того чтобы проверить настройку стартовой страницы воспользуйтесь в меню **Сервис** пунктом **Свойства обозревателя**.

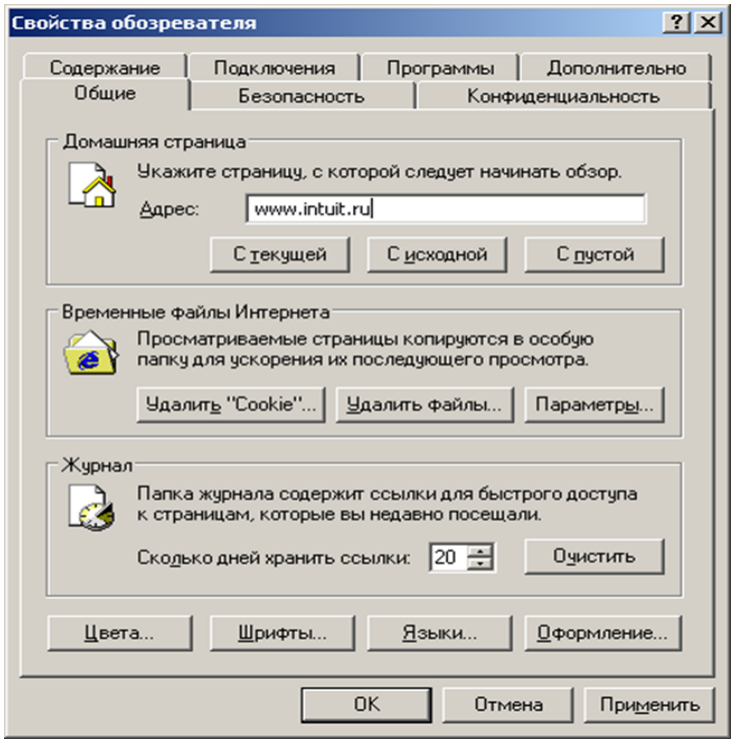


Рисунок 30 – Окно свойства обозревателя

4. В открывшемся окне **Свойства обозревателя** на закладке **Общие** в поле **Адрес** указан адрес стартовой страницы. Измените поле, введя любой другой адрес, например,19.http://www.intuit.ru, и нажмите ОК. Закройте и снова откройте Internet Explorer.

5. Убедитесь, что теперь первым делом была загружена страница 19.http://www.intuit.ru

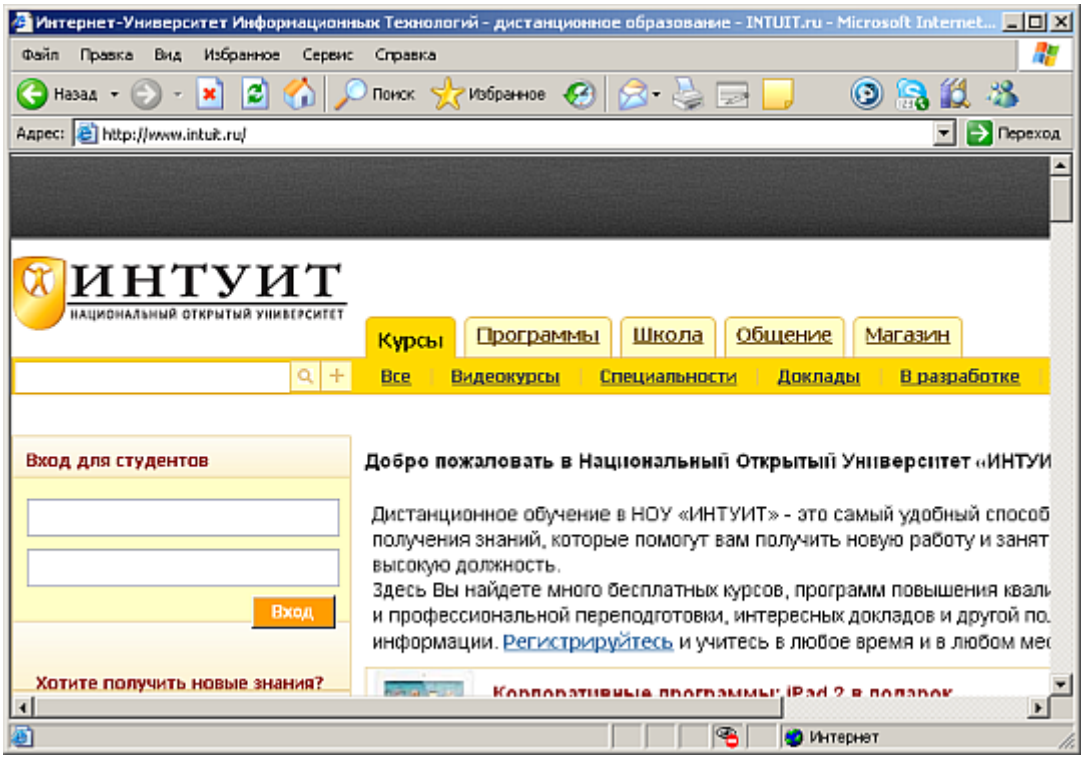


Рисунок 31 – страница Intuit

Если Ваш браузер самостоятельно стал при запуске загружать посторонний сайт, проверьте его настройки: какой адрес выставлен в качестве *домашней страницы*. Некоторые вредоносные программы ограничиваются изменением настройки стартовой страницы, и для устранения последствий их действия необходимо только изменить страницу на желаемую. Однако следует иметь ввиду, что это может быть только частью вредоносной нагрузки. Поэтому при выявлении

несанкционированной смены адреса *домашней страницы* проверьте свой компьютер с помощью антивирусной программы.

Задание 2. Подозрительные процессы/

Основным проявлением *вредоносной программы* является наличие подозрительного процесса в списке запущенных процессов(программ). Имея достаточную квалификацию можно проанализировать список вручную и выявить вредоносную программу вручную. Этот способ является одним из наиболее эффективных для выявления *вредоносных программ*, имеющих только косвенные или скрытые признаки.

Естественно необходимо четко понимать и уметь отличать легальные процессы (например, системные или запущенные программы) от подозрительных. Для того чтобы посмотреть список запущенных на данный момент программ необходимо воспользоваться **Диспетчером задач Windows**.

Диспетчер задач Windows - это стандартная утилита, входящая в любую версию Microsoft Windows. С ее помощью можно в режиме реального времени отслеживать выполняющиеся приложения и запущенные процессы, оценивать загруженность *системных ресурсов* компьютера и использование сети.

1. Для того, чтобы открыть **Диспетчер задач Windows** нажмите одновременно клавиши **Ctrl+Alt+Delete.**

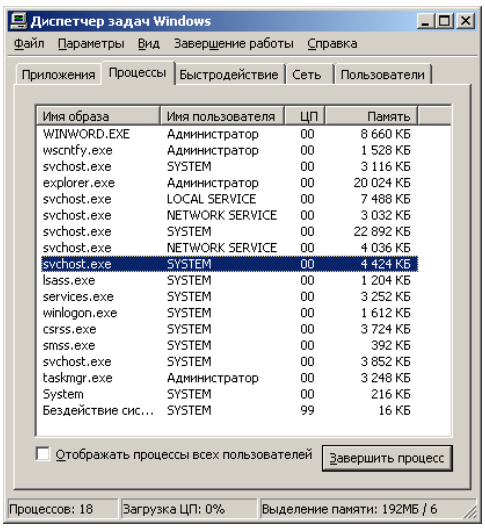


Рисунок 32 – Диспетчер задач

Открывшееся окно содержит пять закладок, отвечающих пяти видам активности, которые отслеживает Диспетчер: приложения, процессы, быстродействие (использование *системных ресурсов*),Сеть и Пользователи. По умолчанию открывается вторая закладка Процессы.

Если на компьютере не запущены никакие пользовательские программы, список текущих процессов должен содержать только служебные процессы операционной системы.

Внимание! Эти процессы необходимы системе для стабильной работы.

Таблица №4 Процессы в диспетчере задач

Название процесса	Описание	Возможность завершения
CSRSS.EXE	Сокращение от "Client/Server Run – Time *Subsystem*".Процесс отвечает за окна консоли, за создание и удаление потоков, а также частично за работу 16-битной среды MS-DOS. Он относится к подсистеме *Win32* пользовательского режима (*WIN32*.SYS же относится к ядру Kernel) и должен всегда выполняться.	-
EXPLORER.EXE	Пользовательская среда, содержащая такие компоненты, как Панель задач, Рабочий стол и тому подобное. Его практически всегда можно закрывать и снова открывать без каких-либо последствий.	+
INTERNAT.EXE	Загружает различные выбранные *пользователем языки* ввода, показывает на панели задач значок "RL", который позволяет переключать языки ввода. С помощью панели управления возможно без использования данного процесса безо всяких проблем переключать раскладку клавиатуры.	+
LSASS.EXE	Этот локальный сервер авторизации отвечает за IP-директивы безопасности (Интернет- протоколы) и загружает драйвер безопасности. Он запускает процесс, отвечающий за авторизацию пользователей. При успешной авторизации пользователя приложение создает и присваивает ему специальный протокол. Все запущенные	-

	далее процессы используют этот протокол.	
MSTASK.EXE	Отвечает за службу планирования Schedule, которая предназначена для запуска различных приложений в определенное пользователем время.	-
SMSS.EXE	Диспетчер сеансов запускает высокоуровневые подсистемы и сервисы. Процесс отвечает за различные действия, например запуск Winlogon- и *Win32*-процессов, а также за операции с системными переменными. Когда Smss определяем, что Winlogon или Csrss закрыты, он автоматически выключает систему.	-
SPOOLSV.EXE	Обеспечивает создание очереди на печать, временно сохраняя документы и факсы в памяти.	-
SVCHOST.EXE	Этот всеобъемлющий процесс служит хостом для других процессов, запускаемых с помощью DLL. Поэтому иногда работают одновременно несколько Svchost. С помощью команды "tlist - s" можно вывести на экран все процессы, использующие Svchost.	-
SERVICES.EXE	Процесс управления *системными службами*. Запуск, окончание, а также все остальные действия со службами происходят через него.	-
SYSTEM	Этот процесс выполняет все потоки ядра Kernel.	-
SYSTEM *IDLE* PROCESS	Этот процесс выполняется на любом компьютере. Нужен он, правда, всего лишь для мониторинга процессорных ресурсов, не используемых другими программами.	-
TASKMGR.EXE	Процесс диспетчера задач, закрывать который крайне не рекомендуется.	+
WINLOGON.EXE	Отвечает за управление процессами авторизации пользователей. Он активен, только когда пользователь нажимает "Ctrl+Alt+Del".	-
WINMGTM.EXE	Основной компонент клиентской службы Windows. Процесс запускается одновременно с первыми клиентскими приложениями и выполняется при любом запросе служб. В XP он запускается как клиент процесса Svchost.	-

Представленные в таблице процессы необходимы для работы Windows XP. В *Windows Vista* их значительно больше.

2. Для каждого процесса выводятся его параметры: имя образа, имя пользователя, от чьего имени был запущен процесс, загрузка этим процессом процессора и объем занимаемой им оперативной памяти.

3. Поскольку в данный момент не должна быть запущена ни одна пользовательская программа, процессор должен быть свободен. Следовательно, "Бездействие системы" должно оказаться внизу списка с достаточно большим процентом "использования" процессора.

4. Если Вы обнаружили подозрительный процесс, не относящийся к системным, завершите его вручную с помощью кнопки "Завершить процесс". Естественно, это не избавляет от наличия вируса на компьютере, а только останавливает его работу в данное время. Далее следует провести проверку с помощью антивируса.

5. Выпишите все запущенные процессы на лист бумаги или в текстовый файл и перейдите к закладке **Приложения**. В данном окне отобразятся все запущенные в настоящий момент приложения. Если в настоящий момент запущенных приложений нет, появится пустое окно, показанное на рис. 33

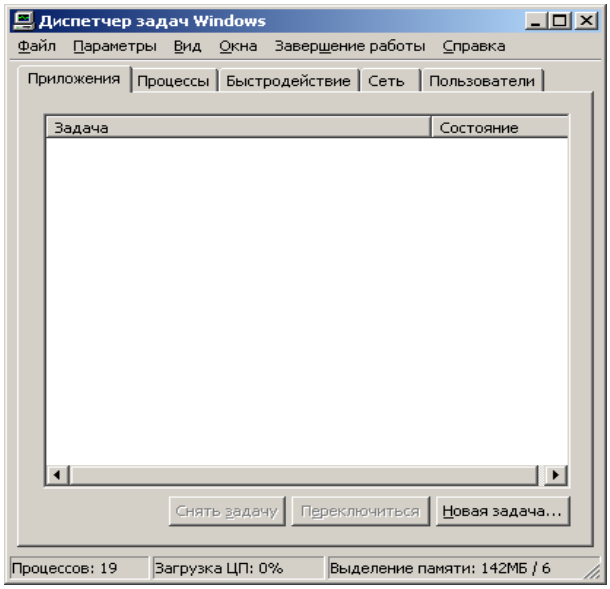


Рисунок 33 – пустое окно

6.Не закрывая окна **Диспетчера задач Windows**, откройте программу **Paint**. Для этого воспользуйтесь системным меню **Пуск / Программы / Стандартные / Paint**. Дождитесь запуска **Paint**.

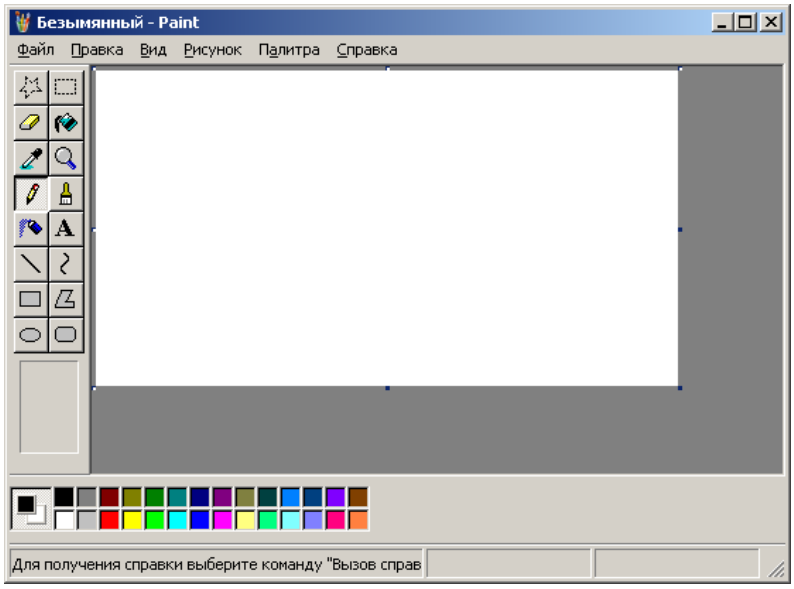


Рисунок 34 – окно Paint

Не закрывая приложение **Paint**, вернитесь к окну **Диспетчера задач Windows** и проследите за изменениями на закладке **Приложения**. В списке запущенных приложений появился **Paint**.

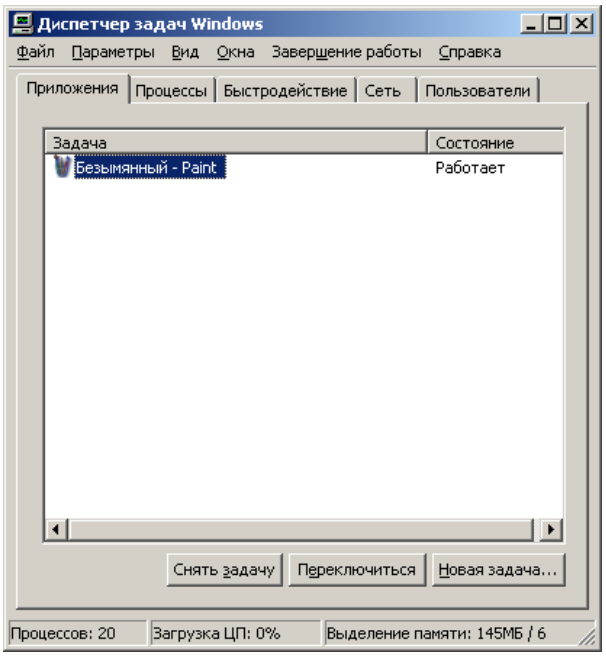


Рисунок 35 – диспетчер задач с Paint

Иногда случается так, что программа вызывает ошибку - тогда в ее состоянии будет написано "Не отвечает". Если некое ранее бесперебойно

работающее приложение начало часто без видимых причин переходить в состояние "Не отвечает", это может быть косвенным признаком заражения.

7.Перейдите к закладке **Процессы** и сравните список в тем, который видели ранее. Найдите процесс, соответствующий **Paint**, - **mspaint.exe**.

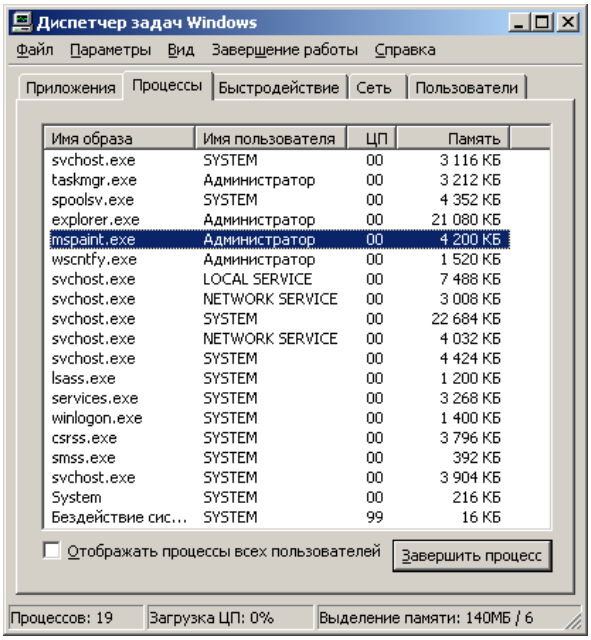


Рисунок 36 – диспетчер задач с приложением Paint

8.Перейдите к закладке **Быстродействие**. Внимательно изучите расположенные тут графики. Всплески на графиках соответствуют по времени определенным действиям, например, запуску программы, требовательной к ресурсам. Если Вы не запускали ничего, а всплески есть, это может быть причиной для более детального исследования компьютера.

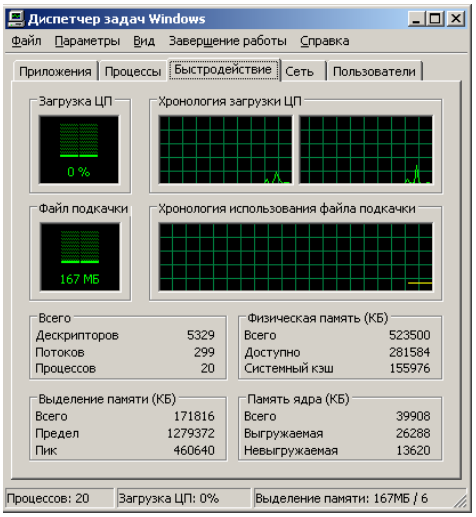


Рисунок 37 – Окно быстродействие

Задание 3. Элементы автозапуска

Вредоносная программа, так же как любая другая программа, для работы нуждается в запуске. При этом возможно два варианта – сделать так, чтобы пользователь сам запустил вредоносную программу, либо внедриться в конфигурационные файлы и запускаться одновременно с легитимными программами. Оптимальным вариантом для *вредоносной программы* является "прописывание" себя в автозагрузку при запуске операционной системы.

1. Самый простой способ добавить какую-либо программу в автозагрузку - это поместить ее ярлык в раздел **Автозагрузка** системного меню **Пуск / Программы**. По умолчанию, сразу после установки операционной системы этот раздел пуст.

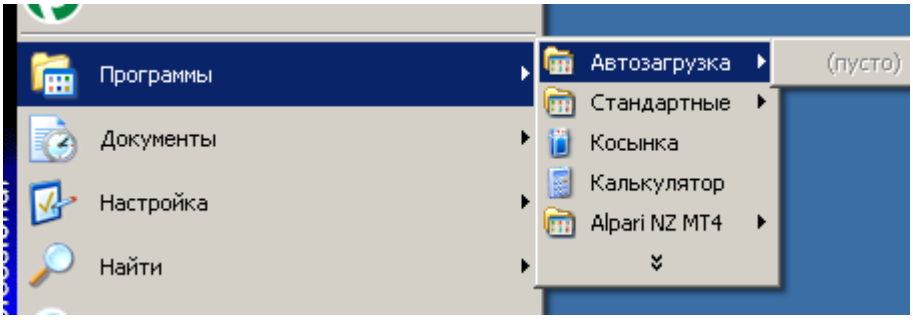


Рисунок 38 – фрагмент панели Пуск

2. Добавьте в список автозагрузки свою программу (создайте ярлык на любую программу, например Калькулятор или Блокнот и поместите

его в группу Автозагрузка). Для этого дважды щелкните левой клавишей мыши по названию группы **Автозагрузка**. Откроется папка автозагрузки в стандартном окне – рис. 39. По умолчанию путь к папке следующий: **C:\Documents and Settings\Администратор\Главное меню\Программы\Автозагрузка**

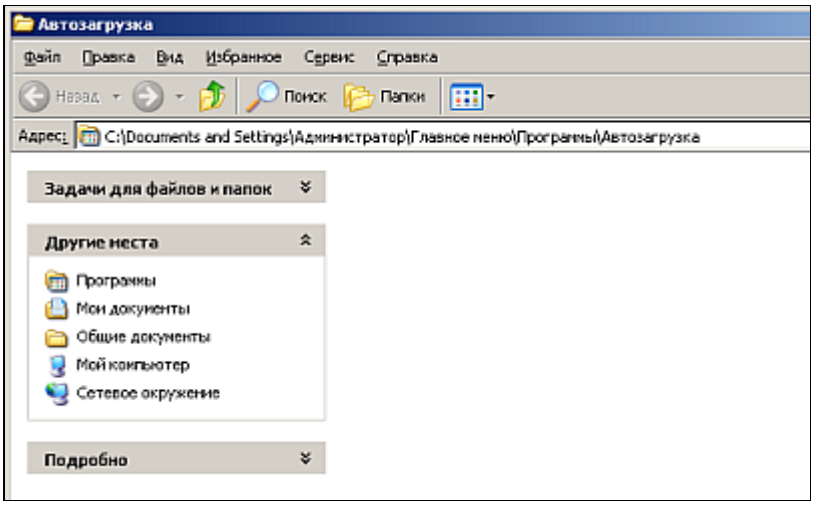


Рисунок 39 – окно автозагрузка

Всё, что нужно сделать, для того, чтобы программа запускалась автоматически при запуске операционной системы – поместить в данную папку ее ярлык.

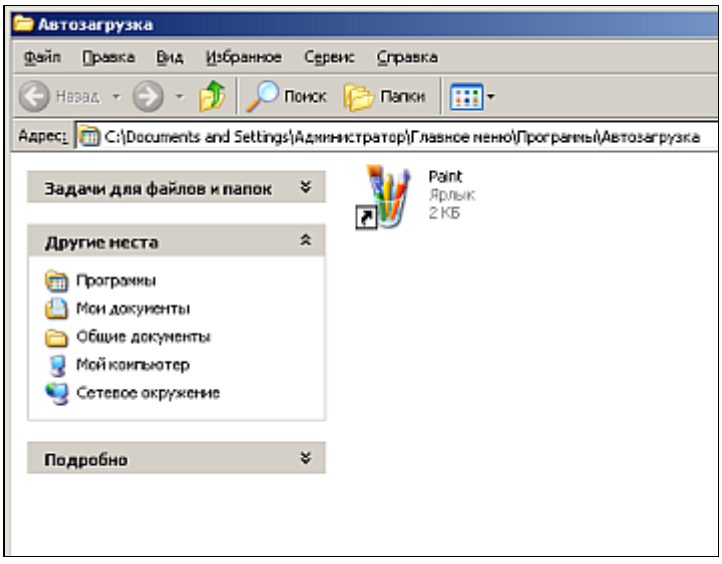


Рисунок 40 – окно автозагрузки с ярлыком.

3.Закройте окно и убедитесь, что теперь раздел **Автозагрузка** в меню **Пуск / Программы** содержит **Paint**.

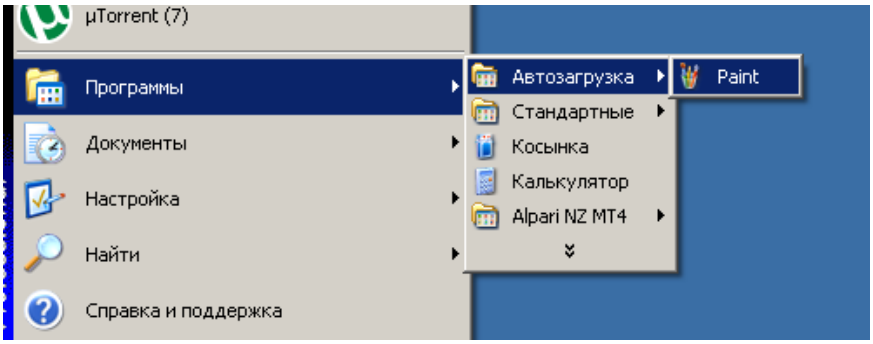


Рисунок 41 – пуск – программы.

4.Перезагрузите компьютер. Убедитесь, что в процессе загрузки операционной системы автоматически запустился **Paint**.

5.Отсутствие подозрительных ярлыков в разделе **Автозагрузка** системного меню **Пуск / Программы**, к сожалению, не гарантирует, что ни одна вредоносная программа не запускается автоматически. Технически для автозапуска нужно добавить соответствующую запись в системный реестр операционной системы.

Несмотря на то, что реестр Windows очень большой, существует оболочка, позволяющая с ним работать напрямую - **regedit**. Но делать это рекомендуется только в крайнем случае. Для большинства ситуаций, связанных с автозапуском, достаточно использовать *системную утилиту* **Настройка системы** .

Запустите ее. Для этого откройте системное меню **Пуск** и перейдите к пункту **Выполнить** и в открывшемся окне **Запуск программы** наберите **msconfig** и нажмите OK.

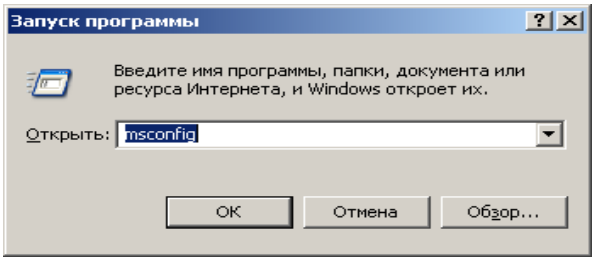


Рисунок 42 – окно запуска программы

6.Ознакомьтесь с внешним видом окна утилиты **Настройка системы**. На первой закладке **Общие**, можно выбрать вариант запуска операционной системы. По умолчанию отмечен Обычный запуск. Он обеспечивает максимальную функциональность системы. Остальные два варианта запуска предназначены для диагностики.

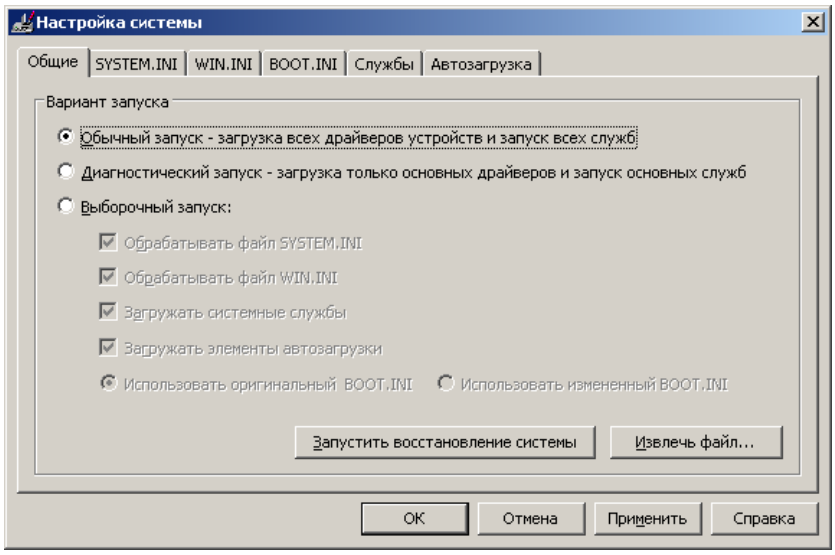


Рисунок 43 – Окно настройка системы

Диагностический запуск рекомендуется использовать также при подтвердившемся наличии *вредоносной программы* - если компьютер уже заражен, сразу установить *антивирус* в ряде случаев нельзя, например, если вирус сознательно блокирует запуск ряда антивирусных программ. Тогда, если нет возможности удалить или хотя бы временно обезвредить вирус вручную, рекомендует запустить операционную систему в безопасном режиме, инсталлировать *антивирус* и сразу же проверить весь жесткий диск на наличие вирусов.

7.Ознакомьтесь со списком запускаемых драйверов и других параметров операционной системы, перейдя к закладке SYSTEM.INI . Тут отображаются все ссылки, указанные в одноименном системном файле.

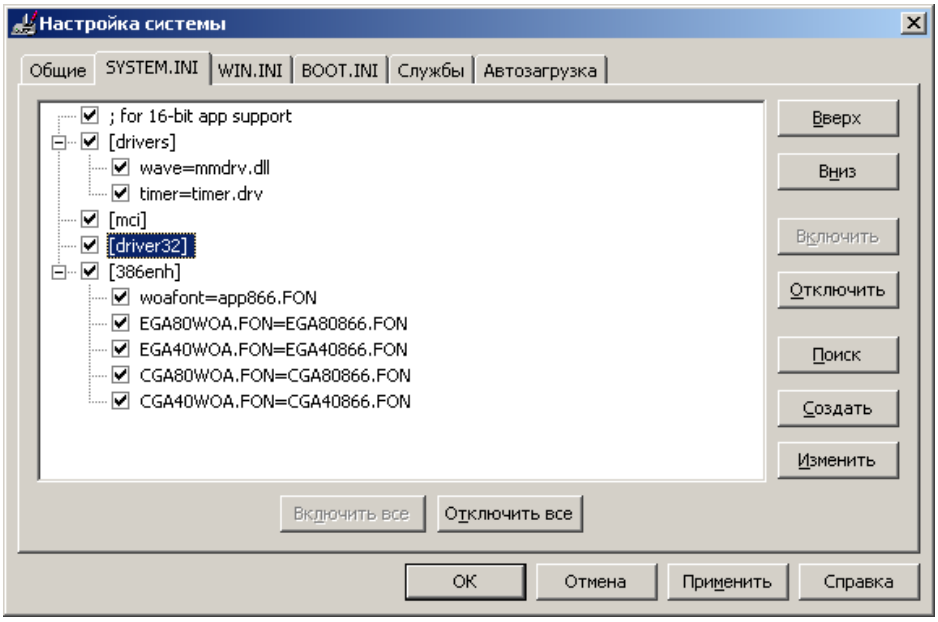


Рисунок 44 – Окно настройки системы

8.Перейдите к аналогичной закладке **WIN.INI** и ознакомьтесь с ее содержимым.

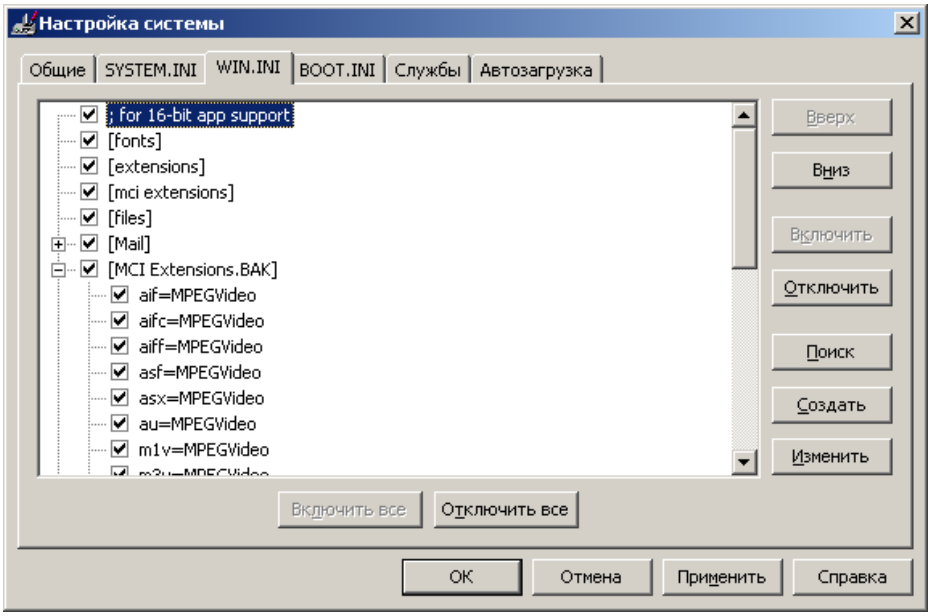


Рисунок 45 – Окно настройки системы

9.Следующая закладка **BOOT.INI** также отображает данные из одноименного файла. Как и предыдущие две, она также содержит системную информацию. Изменять ее можно только обладая соответствующими знаниями!

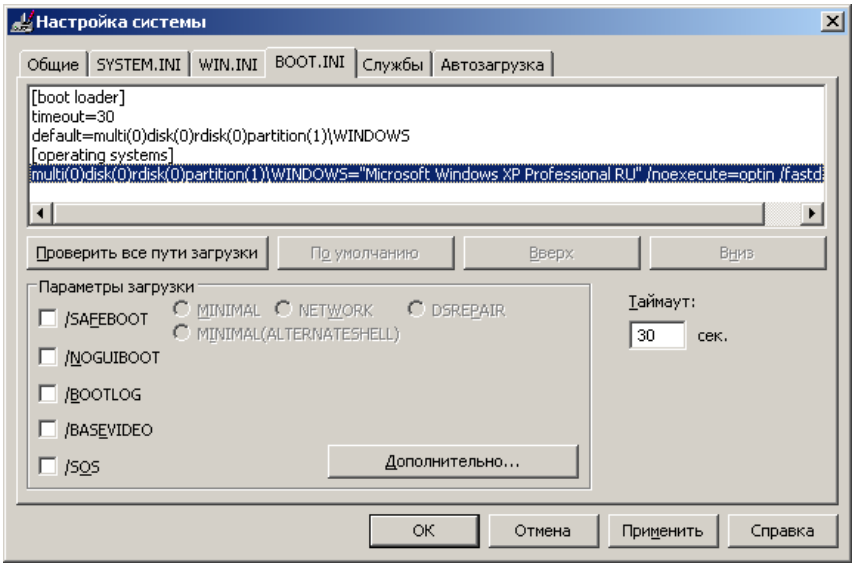


Рисунок 47 – Окно настройки системы

10. Перейдите на закладку **Службы**. Здесь представлен список всех служб, установленных в системе. Каждая служба представляет собой некое приложение, работающее в фоновом режиме. Например, антивирусный комплекс, обеспечивающий постоянную защиту, также встраивает свою службу, следовательно, она должна присутствовать в этом перечне. Так же и вирус может установить свою службу в системе.

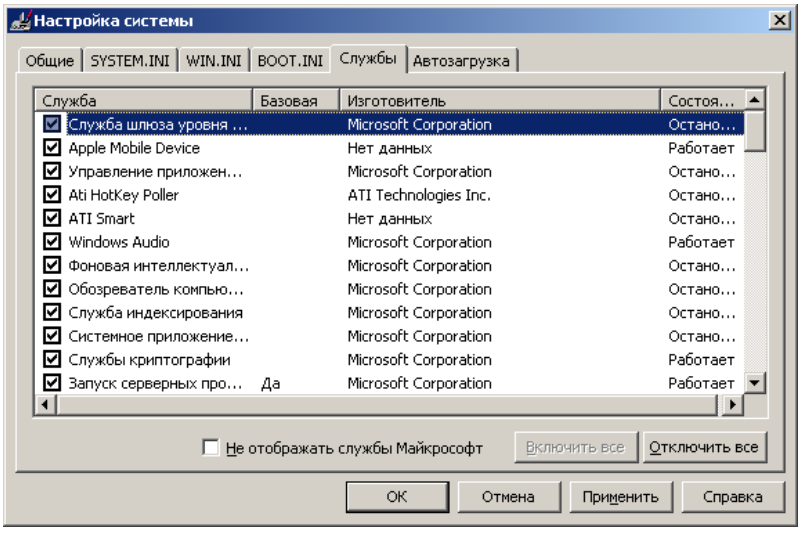


Рисунок 48 – Окно настройки системы

11. Перейдите к последней закладке **Автозагрузка** и убедитесь, что в списке приложений, автоматически запускаемых при загрузке системы, есть **Paint**.

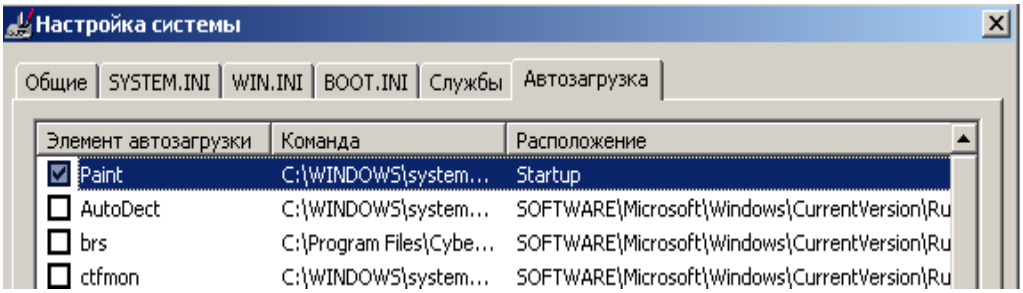


Рисунок 49 – Окно настройки системы

12. Отключите автоматическую загрузку **Paint**, убрав галочку напротив него в столбце **Элемент автозагрузки** и нажмите ОК. В открывшемся окне согласитесь на перезагрузку.

13. После того, как компьютер перезагрузится, система выведет предупреждение в виде окна, представленного на рис. 19.23.

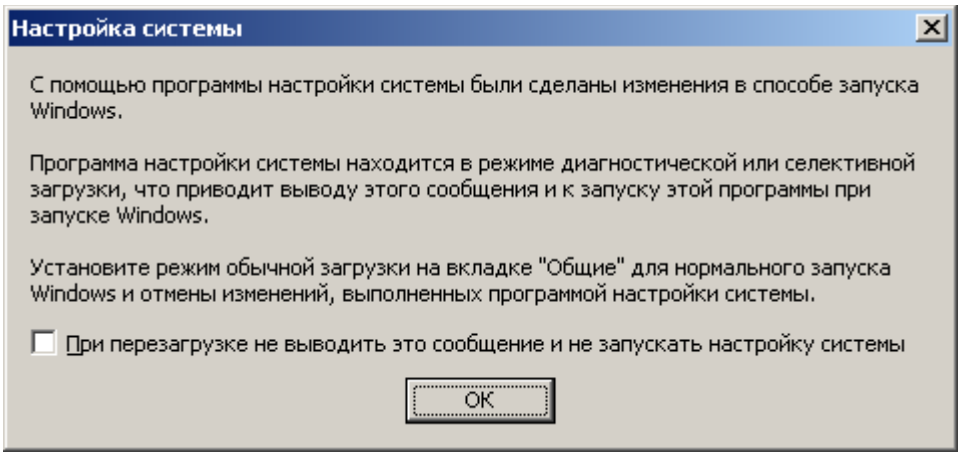


Рисунок 50 – Окно настройки системы

14. Откройте окно **Настройка системы**. Обратите внимание, что теперь используется не обычный запуск, а выборочный. При этом полностью обрабатываются все элементы файлов SYSTEM.INI, WIN.INI и BOOT.INI, загружаются все службы, но флаг **Загружать элементы автозагрузки затенен**. Это означает неполную загрузку .

15. Перейдите к закладке **Автозагрузка** и убедитесь, что ее вид не изменился - **Paint** все так же присутствует в списке, но отключен.

16. Не закрывая окна **Настройка системы** проверьте, что Paint автоматически не запустился и раздел **Пуск / Программы / Автозагрузка** теперь снова пуст.

17. Необходимо учесть, что если выбрать после изменений **Обычную загрузку** – все файлы, находящиеся на вкладке **Автозагрузка** будут запускаться снова, в том числе и **Paint**.

Содержание отчета: тема, цель, скриншоты этапов выполнения работы, вывод: основными признаками присутствия вредоносных программ являются…..

Лабораторная работа № 9: Работа с Антивирусом Касперского 2011.

Цель работы: изучить интерфейс и модули антивируса Касперского 2011.

Теоретические сведения

Антивирус Касперского 2011 обеспечит комплексную защиту компьютера от известных и новых угроз, сетевых и мошеннических атак, нежелательной информации.

В состав продукта добавлен компонент Мониторинг активности, который отслеживает активность программ в системе и предоставляет расширенную информацию другим компонентам защиты. Кроме того, благодаря сохраняемой истории активности программ, компонент может выполнять откат действий вредоносной программы при обнаружении вредоносной активности различными компонентами защиты.

Режим проверки во время простоя компьютера позволит регулярно выполнять проверку и в то же время не снижать быстродействие компьютера тогда, когда он нужен.

Для быстрого доступа к основным функциям программы: индикации состояния защиты компьютера, проверке объектов на вирусы, просмотру отчётов о работе программы, – предназначен гаджет Kaspersky Gadget (доступен для пользователей операционной системы Windows Vista и Windows 7).

После установки Антивируса Касперского 2011, возможно временно переключиться на работу с Kaspersky Internet Security 2011, чтобы оценить его возможности и при желании приобрести лицензию для работы с ним. При этом устанавливать Kaspersky Internet Security 2011 отдельно не потребуется.

Задание 1.1 Изучение системны требований.

При создании любого приложения программисты дают гарантию, что их продукт будет работать на технике с определёнными характеристиками. Это требования к программному обеспечению. Бывают, требования к аппаратному обеспечению – в этом случае постулируется необходимость

наличия на компьютере некоторого минимального объёма оперативной памяти (если её меньше 375 Мб, то программа будет очень медленно работать или же не запустится вовсе), свободного пространства на диске (для размещения всех необходимых в работе приложения файлов), тактовой частоты процессора, от которой зависит производительность компьютера и другое.

В случае антивирусных программ часто выдвигается дополнительное требование отсутствия на компьютере другого антивирусного средства, совместная работа с которым может вызвать конфликты (при установке любой антивирусной программы, установщик выводит предупреждение: если на компьютере установлено другое антивирусное программное обеспечение, могут возникнуть конфликтные ситуации).

Системные требования обычно приводятся в сопровождающем дистрибутив текстовом файле и/или в документации к продукту. Также с системными требованиями можно ознакомиться на сайте компании–производителя.

В соответствии с заданием на лабораторную работу, изложенным после цели, нужно сравнить системные требования Антивируса Касперского 2011 с конфигурацией компьютера пользователя и убедиться, что установка этого приложения возможна.

1. Необходимо узнать версию операционной системы, в которой работает пользователь. Для этого нужно найти иконку Мой компьютер, вывести её контекстное меню (щелкнув на ней правой кнопкой мыши) и выбрать пункт Свойства.

2. Открывшееся окно Свойства системы содержит основные сведения о компьютере и установленной на нём операционной системе. На первой закладке, Общие, представлена сводная информация, в том числе название и версия операционной системы. На рисунке это Microsoft Windows XP Professional с установленным Service Pack 3.

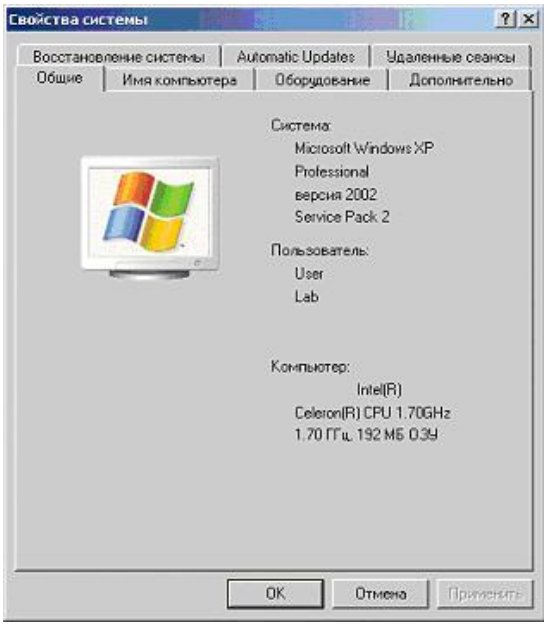


Рисунок 51 – Свойства системы

3. Для нормального функционирования Kaspersky Internet Security 2011должен удовлетворять следующим минимальным требованиям:

Общие требования:

– 480 МБ свободного места на жёстком диске;

– CD/DVD-ROM (для установки продукта с дистрибутивного CD-диска);

– Подключение к сети Интернет (для активации продукта);

– Microsoft Internet Explorer 6.0 или выше (для обновления антивирусных баз и модулей приложения через интернет);

– Microsoft Windows Installer 2.0 или выше.

Операционные системы:

– Microsoft Windows XP Home Edition (Service Pack 2 и выше);

– Microsoft Windows XP Professional (Service Pack 2 и выше);

– Microsoft Windows XP Professional x64 Edition (Service Pack 2 и выше);

– Процессор Intel Pentium 800 МГц 32-бит (x86)/64-бит (x64) или выше (или совместимый аналог);

– 512 МБ свободной оперативной памяти:

– Microsoft Windows Vista Home Basic (32/64 бит);

– Microsoft Windows Vista Home Premium (32/64 бит);

– Microsoft Windows Vista Business (32/64 бит);

– Microsoft Windows Vista Enterprise (32/64 бит);

– Microsoft Windows Vista Ultimate (32/64 бит);

– Microsoft Windows Vista Home Basic SP1 (32/64 бит);

– Microsoft Windows Vista Home Premium SP1 (32/64 бит);

– Microsoft Windows Vista Business SP1 (32/64 бит);

– Microsoft Windows Vista Enterprise SP1 (32/64 бит);

– Microsoft Windows Vista Ultimate SP1 (32/64 бит);

– Процессор Intel Pentium 1 ГГц 32-бит (x86)/64-бит (x64) или выше (или совместимый аналог);

– 1 Гб свободной оперативной памяти (32-бит);

– 2 Гб свободной оперативной памяти (64-бит).

ОС Windows 7 поддерживается продуктами Лаборатории Касперского версии 11.0.1.400 (в русской версии) и выше:

– Microsoft Windows 7 Начальная (Starter) (32/64 бит);

– Microsoft Windows 7 Домашняя базовая (Home Basic) (32/64 бит);

– Microsoft Windows 7 Домашняя расширенная (Home Premium) (32/64 бит);

– Microsoft Windows 7 Профессиональная (Professional) (32/64 бит);

– Microsoft Windows 7 Максимальная (Ultimate) (32/64 бит);

– Процессор Intel Pentium 1 ГГц 32-бит (x86)/64-бит (x64) или выше (или совместимый аналог);

– 1 Gb свободной оперативной памяти (32-бит);

– 2 Gb свободной оперативной памяти (64-бит).

Для оптимального отображения интерфейса продукта рекомендуется использовать стандартные режимы от 800x600 и выше.

Требования для нетбуков:

– Процессор Intel Atom 1.3 МГц (Z520) (или совместимый аналог);

– Видеокарта Intel GMA950 с видеопамятью объёмом не менее 64 Мб (или совместимый аналог);

– Диагональ экрана не менее 10,1 дюйма;

– Операционная система Microsoft Windows XP Home Edition или выше.

Для проверки свойств системы пользователю нужно вернуться к окну Свойства системы и убедиться, что установленная операционная система соответствует требованиям Антивируса Касперского 2011.

4. Следует проверить наличие свободного места на диске. Для этого откройте папку Мой компьютер и задержите на пару секунд курсор мыши над иконкой системного диска. В появившемся сообщении будет указан объём свободного пространства на нём и общий объём диска.

5. Далее необходимо ознакомиться со списком установленных на компьютер программ и убедиться, что среди них нет других антивирусов. Для этого вызовите Панель управления (Пуск/Настройка/Панель управления). В Панели управления найдите элемент Установка и удаление программ и откройте его.

6. Ознакомьтесь со списком установленных на компьютере программ и убедитесь, что среди них нет других антивирусов.

7. Обратите внимание на системную дату, установленную на компьютере пользователя. Для этого задержите на пару секунд курсор мышки над системным временем в правом нижнем углу экрана. Системная дата должна соответствовать реальной дате, это будет необходимо для корректной активации продукта.

На этом подготовительный этап окончен и можно переходить непосредственно к установке.

Задание 1.2. Установка программного обеспечения

Большинство современных приложений перед запуском необходимо установить.

Стандартная процедура установки включает в себя копирование необходимых в работе программы файлов на диск (в нужное место) и регистрацию в реестр операционной системы. Иногда для завершения установки требуется перезагрузка компьютера.

Для успешной установки Антивируса Касперского 2011 требуется дистрибутив и код активации. Эти файлы как правило записываются на CD и передаются пользователю при покупке. В случае приобретения в Интернет–магазине, дистрибутив можно либо загрузить с сайта Лаборатории Касперского, либо заказать отправку почтой или курьером на CD, лицензионный ключ высылается по e–mail.

Если имеется код активации, то Антивирус Касперского можно активировать с помощью него, после установки.

Начиная с версии 2009, продукты Лаборатории Касперского можно активировать только кодом активации при наличии соединения с сетью Интернет. Для активации продукта при отсутствии подключения к сети Интернет обратитесь в Службу технической поддержки, написав запрос через Личный кабинет с любого компьютера, имеющего доступ в глобальную сеть.

В запросе обязательно укажите следующую информацию:

– код активации продукта Лаборатории Касперского;
– подробное описание проблемы.

Для установки будет использоваться пробная версия Kaspersky Internet Security 2011.

1. Откройте папку с дистрибутивом Антивируса Касперского 2011. Её расположение можно узнать у преподавателя.

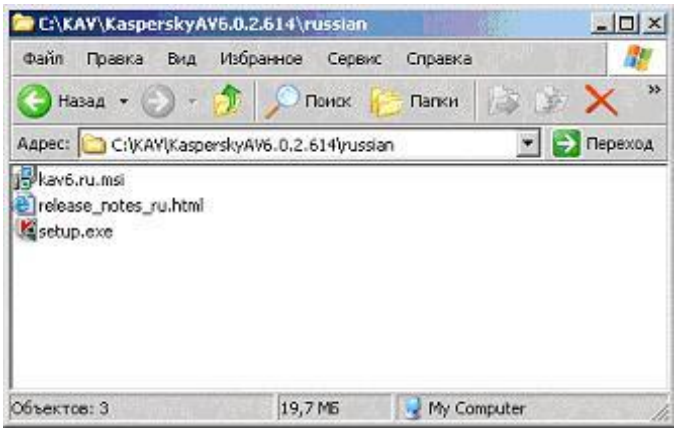


Рисунок 52– Папка с дистрибутивом

Перед началом установки рекомендуется выполнить следующие действия:

– Закрыть все работающие программы.

– Проверить, установлены ли на компьютере другие продукты Лаборатории Касперского или несовместимое антивирусное ПО стороннего производителя. Список несовместимых с Антивирусом Касперского 2011 программ можно найти в статье KB3988.

2. Запустите Мастер установки Антивируса Касперского 2011.

Установка с возможностью изменения параметров – в данном случае (флажок Изменить параметры установки установлен) пользователю будет предложено указать папку, куда будет установлена программа и при необходимости выключить защиту процесса установки.

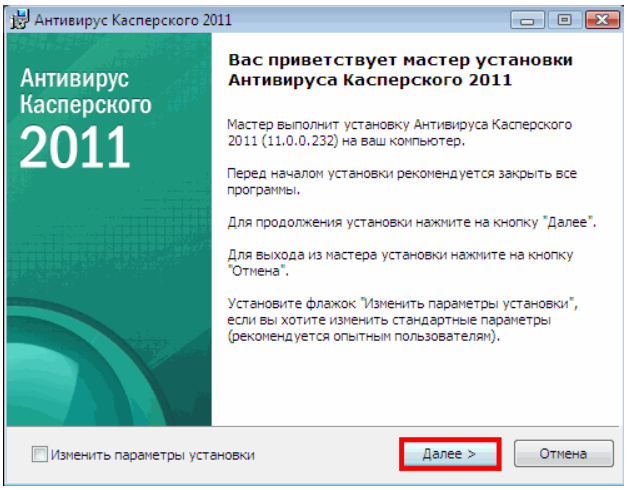


Рисунок 53 – Мастер установки Антивируса Касперского 2011

Чтобы сделать это, выполните одно из действий, описанных ниже.

Если Антивирус Касперского 2011 куплен на компакт-диске, то установка продукта начинается автоматически после того как компакт диск вставлен в CD-ROM привод. Если по какой-то причине автоматический запуск установки не произошел, запустите файл инсталляции вручную. Для этого достаточно выбрать диск и папку, в которой находится установочный файл и дважды щелкнуть левой кнопкой мыши по исполняемому файлу (с расширением .exe).

Если Антивирус Касперского 2011 приобретён в онлайн-магазине, покупатель получаете ссылку на исполняемый файл инсталлятора, который необходимо запустить вручную.

В результате запустится Мастер установки Антивируса Касперского 2011.

Чтобы запустить стандартную установку Антивируса Касперского 2011, нажмите кнопку Далее.

3. Ознакомьтесь с Лицензионным соглашением Лаборатории Касперского. Внимательно прочтите соглашение и, если согласны со всеми его пунктами, нажмите на кнопку Я согласен. Установка программы на компьютер пользователя будет продолжена. Для отказа от установки нажмите на кнопку Отмена.

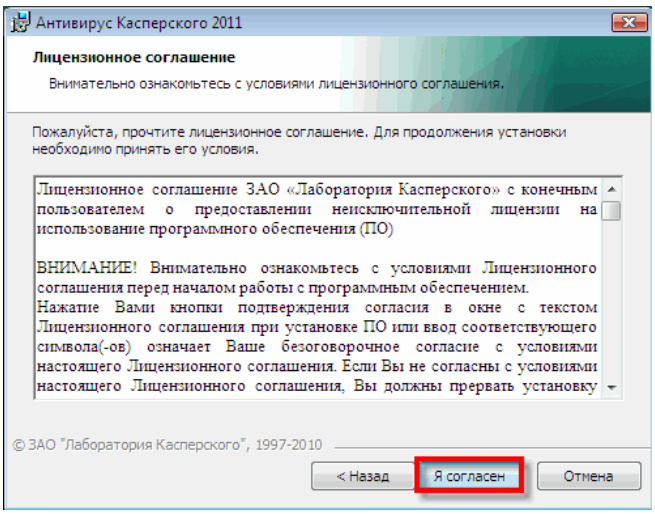


Рисунок 54 – Лицензионное соглашение Лаборатории Касперского

4. Ознакомьтесь с текстом положения об использовании Kaspersky Security Network.

Участие в программе Kaspersky Security Network предусматривает отправку в Лабораторию Касперского информации о новых угрозах, обнаруженных на компьютере пользователя, отправку уникального идентификатора, присвоенного компьютеру Антивирусом Касперского, и информации о системе. При этом гарантируется, что персональные данные отправляться не будут.

Если пользователь согласен со всеми его пунктами, тогда он должен установить флажок Я принимаю условия участия в Kaspersky Security Network. Нажмите на кнопку Установить. Установка будет продолжена.

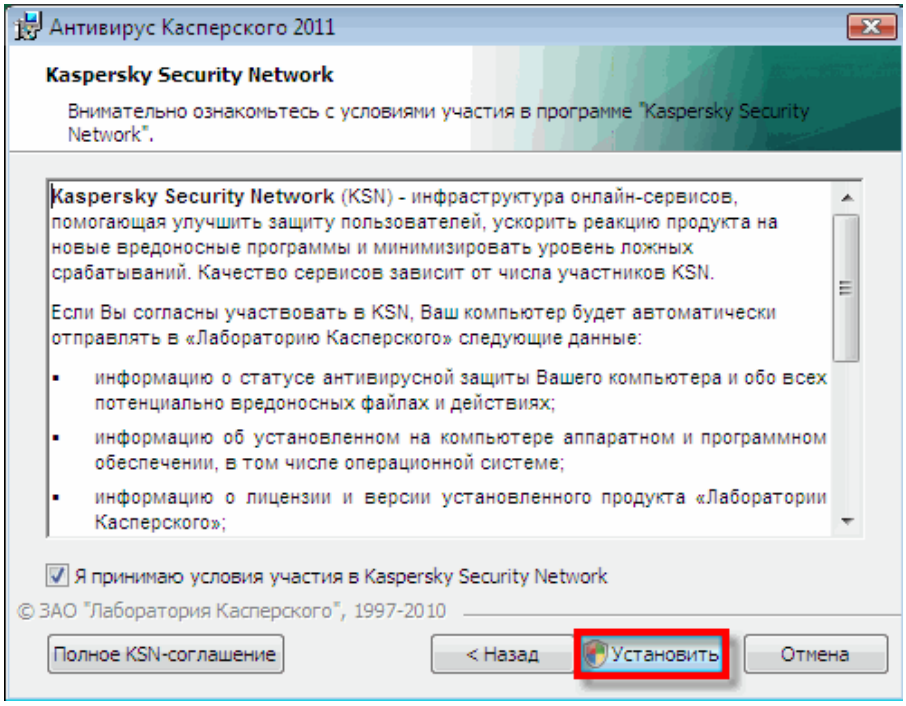


Рисунок 55 – Положение об использовании Kaspersky Security Network

Если программа устанавливается на ОС Windows Vista/7, возможно появление сообщения от службы Контроля учётных записей пользователей (UAC). Для продолжения процесса установки в окне Контроль учётных записей пользователей введите пароль администратора и нажмите на кнопку Да.

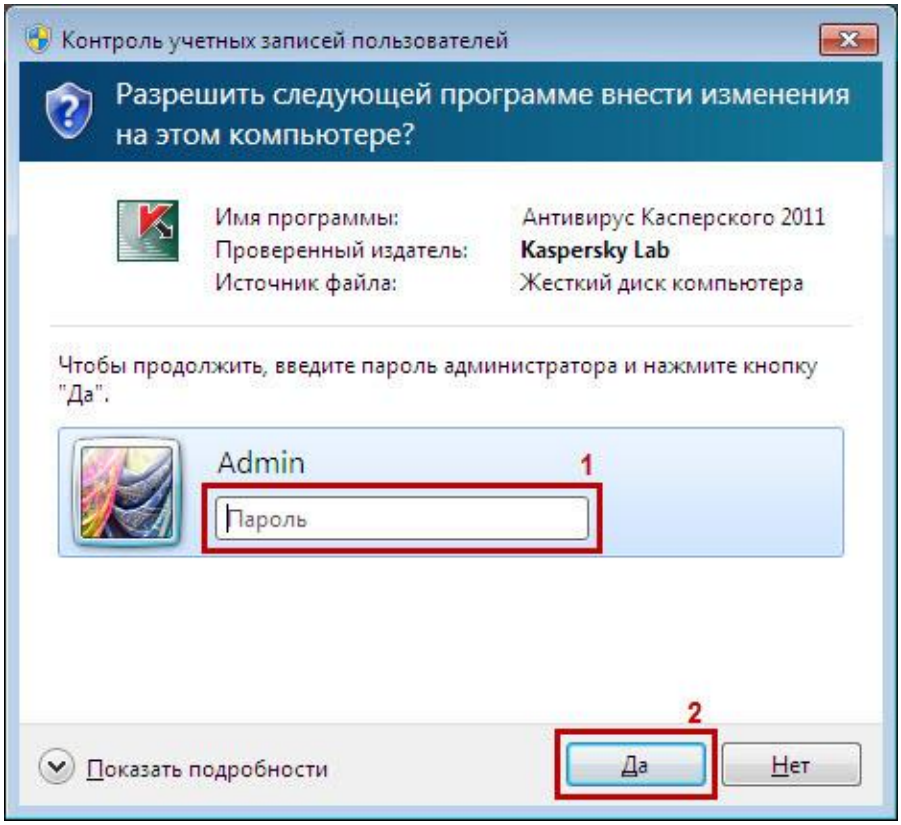


Рисунок 56 – Контроль учётных записей пользователей

5. Активируйте Антивирус Касперского 2011.

1) Код активации

Код активации – это уникальный набор из 20 символов, с помощью которого может быть активирован продукт Лаборатории Касперского версии 2011. Код состоит из 4 блоков, в каждом блоке по 5 символов, и имеет вид XXXXX-XXXXX-XXXXX-XXXXX.

Код активации необходим для активации коммерческой версии продукта Лаборатории Касперского версии 2011.

Если продукт Лаборатории Касперского установлен, то для полноценной работы программы необходимо активировать программу, купив для неё лицензию. Приобрести лицензию можно в интернет-магазине.

Коды активации выписываются отдельно для каждого продукта Лаборатории Касперского.

2) Коробочная версия продукта.

Если приобретена коробочная версия продукта Лаборатории Касперского, то код активации можно найти на первой странице краткого руководства пользователя.

Рисунок 57 – Код активации коробочной версия продукта Лаборатории Касперского

3) Электронная версия.

Если продукт Лаборатории Касперского приобретён в интернет-магазине, то код активации будет выслан на указанный вами при заказе адрес электронной почты

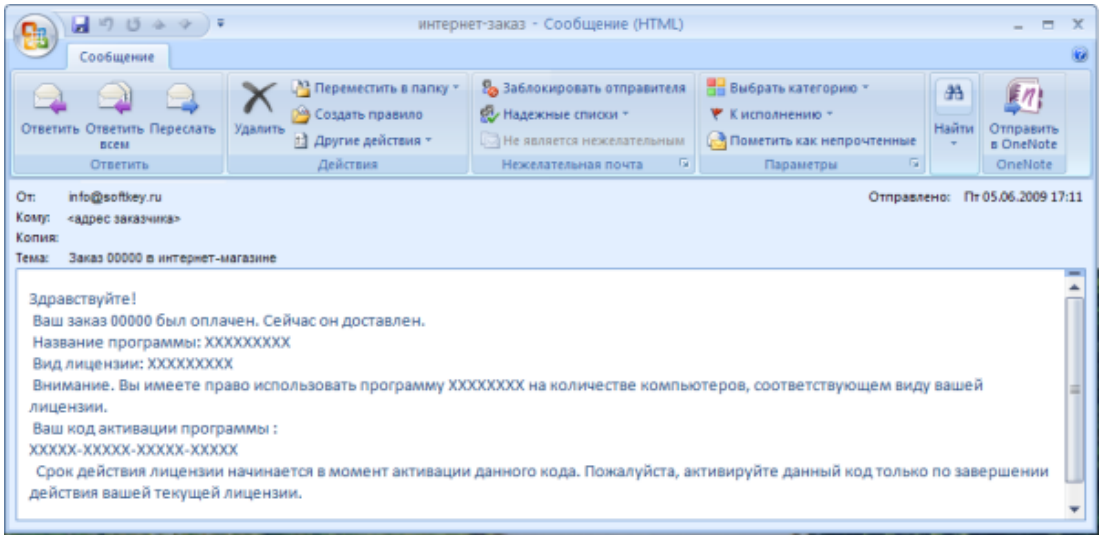


Рисунок 58 – Код активации электронной версии

4) *Срок годности кода активации.*

Срок годности у кода активации, который не был активирован ни разу, отсутствует. Если приобретена коробочная и/или электронная версия продукта, то код активации будет действителен сколько угодно времени до тех пор, пока не будет произведена первая активация. Отсчет срока лицензии продукта начинается с момента первой активации.

Данная информация не относится к пробным (триальным) кодам активации и кодам, которые поставляются на компакт-дисках с различными печатными изданиями. Срок годности таких кодов активации ограничен.

5) *Активационный код был потерян или удален.*

Если активационный код был потерян или удален по ошибке, то для его восстановления необходимо отправить запрос в Службу технической поддержки Лаборатории Касперского через сервис Личный кабинет. В запросе сообщите информацию о месте и дате приобретения продукта, а также ОБЯЗАТЕЛЬНО номер лицензии (вида 0XXX-000XXX-000XXXXX).

Информацию о том, как узнать номер лицензии, можно найти в следующих статьях Базы знаний Лаборатории Касперского.

Если продукт Лаборатории Касперского приобретён в интернет-магазине, нужно обратиться в отдел продаж Лаборатории Касперского по

адресу sales@kaspersky.com. В письме описать проблему и указать следующие данные:

– место и дату покупки;

– информацию о владельце: ФИО, адрес электронной почты;

– номер интернет-заказа, присланного в письме-подтверждении, которое было отправлено после покупки программы.

Нажмите кнопку Далее для продолжения.

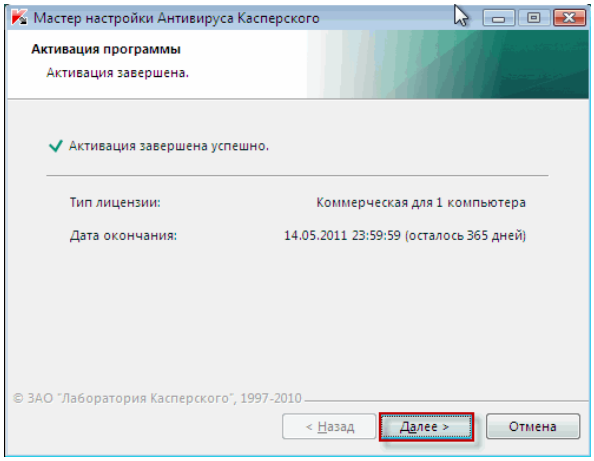


Рисунок59 – Активация программы

6) Дождитесь завершения работы Мастера установки и нажмите кнопку Завершить.

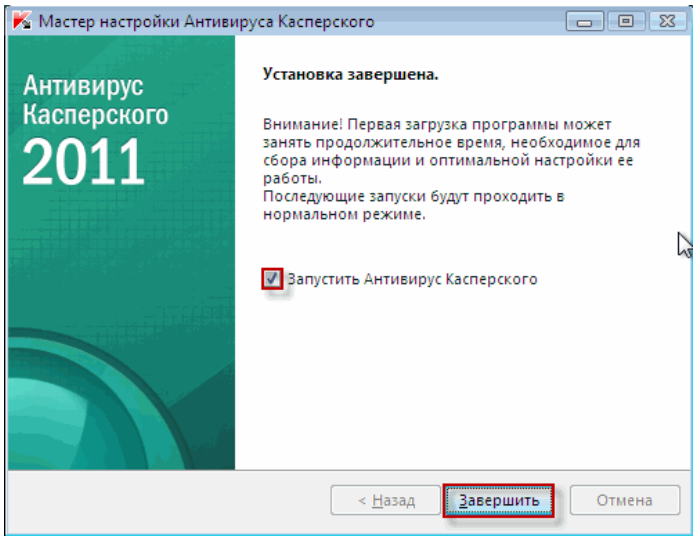


Рисунок 60 – Завершение установки

Мастер установки анализирует информацию о системе и создает правила для доверенных приложений, которые входят в состав операционной системы Windows. Дождитесь окончания процесса анализа информации. Нажмите кнопку Завершить для завершения установки Антивируса Касперского 2011.

Задание 1.3 Установка Антивируса Касперского из командной строки

Чтобы провести установку Антивируса Касперского/Kaspersky Internet Security 2011 из командной строки, выполните следующие действия:

– на компьютере, где необходимо провести установку продукта Лаборатории Касперского версии 2011, запустите командную строку;

– в левой нижней части экрана нажмите на кнопку Пуск;

– выберите пункты меню (Все) Программы – Стандартные – Командная строка.

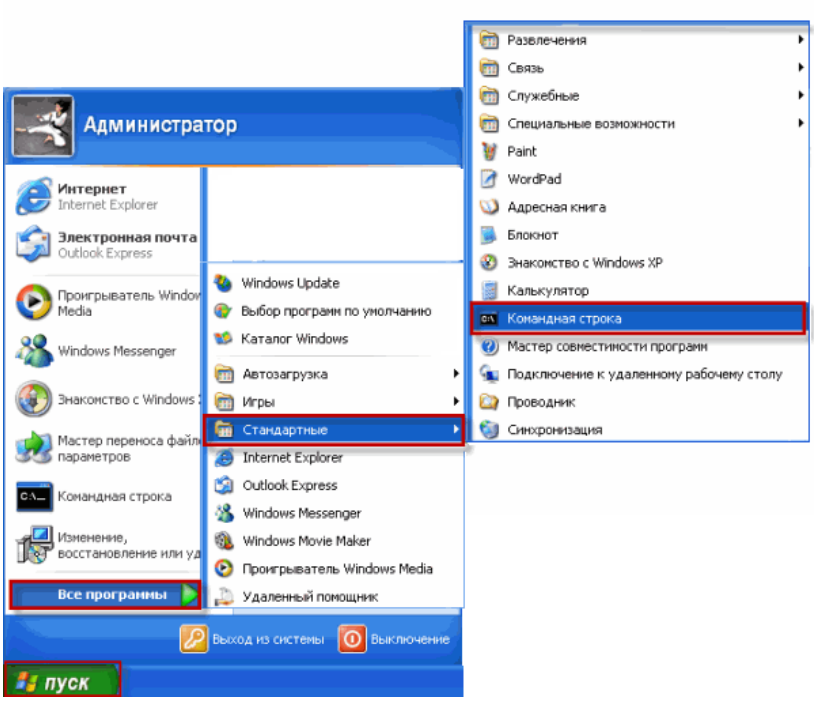


Рисунок 61 – Запуск командной строки

В окне командной строки нужно ввести команду для запуска исполняемого файла setup.exe с различными параметрами и свойствами установки. Запуск файла сопровождается следующими ключами:

Основные параметры:

/s – неинтерактивный (silent) режим (без вывода диалоговых окон в процессе установки) (пример ввода команды в командной строке: setup.exe /s);

/p <свойство>=<значение> – задание свойства для установки (пример ввода команды в командной строке: setup.exe /p «ALLOWREBOOT=1 SKIPPRODUCTCHECK=1»);

/h – справка;

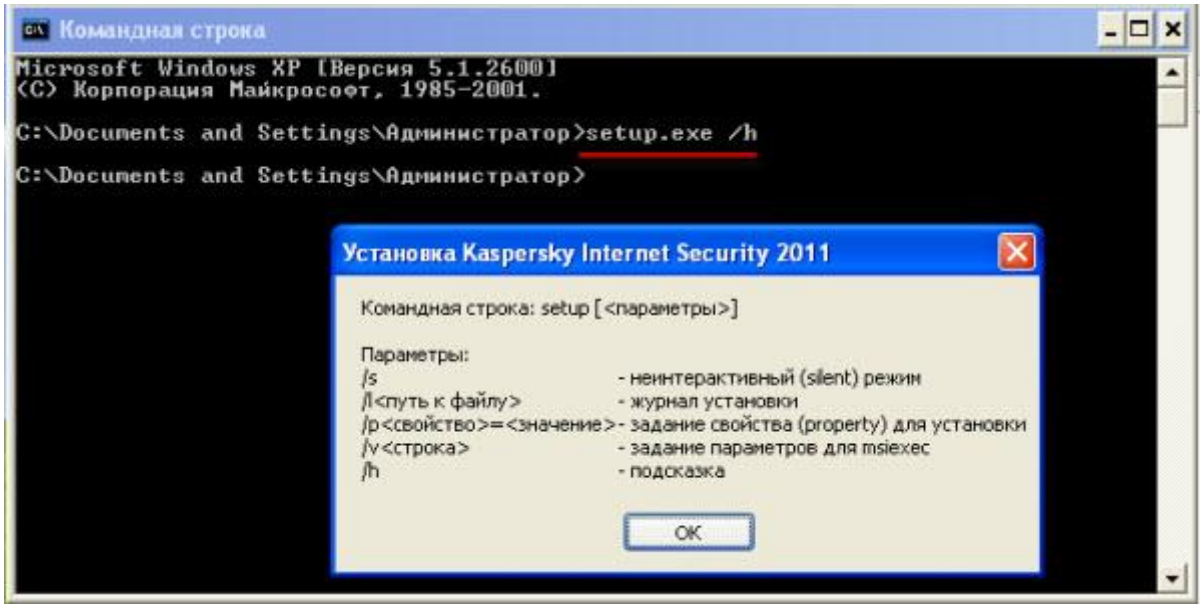


Рисунок 62 – Установка Kaspersky Internet Security 2011 через командную строку

Дополнительные параметры:

/a – административная установка (копирование файлов, необходимых для установки, в указанную сетевую папку) (пример ввода команды в командной строке: setup.exe /a «Z:\Kaspersky Lab»);

/x – удаление продукта (пример ввода команды в командной строке: setup.exe /x).

Наиболее значимые свойства установки:

ACTIVATIONCODE=<значение> – код активации продукта;

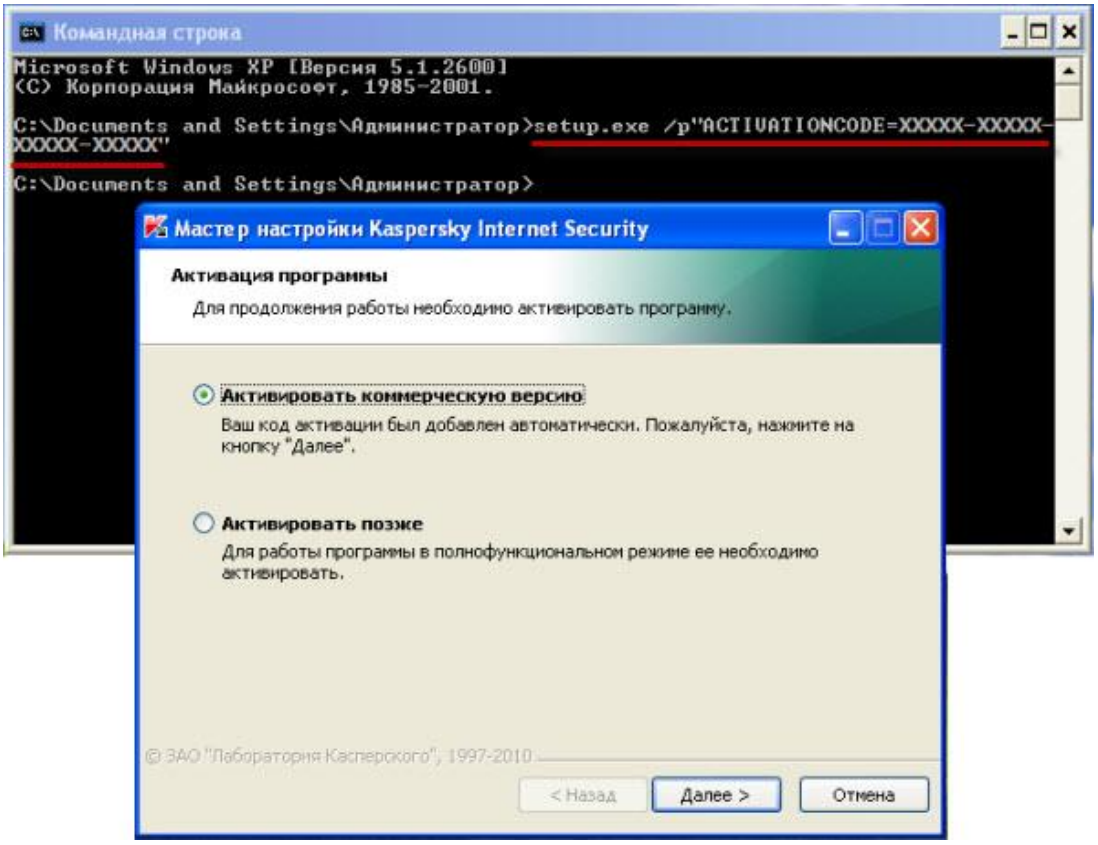


Рисунок 63 – Активация коммерческой версии

ALLOWREBOOT=1 – разрешить перезагрузку, если необходимо (пример ввода команды в командной строке: setup.exe /p «ALLOWREBOOT=1»);

INSTALLDIR=<значение> – место установки (пример ввода команды в командной строке: setup.exe /p «INSTALLDIR=C:\Documents and Settings\Администратор\kis2011»);

KLPASSWD=<значение> – установка пароля на различные функции продукт (пример ввода команды в командной строке: setup.exe /p «KLPASSWD=12345678»). Если при этом не задано значение параметра KLPASSWDAREA, то используется область действия пароля по умолчанию:

– изменение настроек продукта;

– завершение работы продукта.

KLPASSWDAREA=[SET|EXIT|PARCTL|UNINST] – область действия пароля, заданного параметром KLPASSWD:

SET – изменение настроек продукта;

EXIT – завершение работы продукта;

PARCTL – изменение настроек Родительского контроля (применение параметра возможно только для Kaspersky Internet Security 2011);

UNINST – удаление продукта.

SELFPROTECTION=1 – включить самозащиту продукта в процессе установки (пример ввода команды в командной строке: setup.exe /p «SELFPROTECTION=1»);

SKIPPRODUCTCHECK=1 – не выполнять поиск продуктов, несовместимых с продуктами Лаборатории Касперского версии 2011 (пример ввода команды в командной строке: setup.exe /p «SKIPPRODUCTCHECK=1»).

Например, при вводе и выполнении команды: setup.exe /p «ALLOWREBOOT=1 SKIPPRODUCTCHECK=1» во время установки продукта Лаборатории Касперского версии 2011 разрешена перезагрузка компьютера и не будет выполняться поиск несовместимых продуктов.

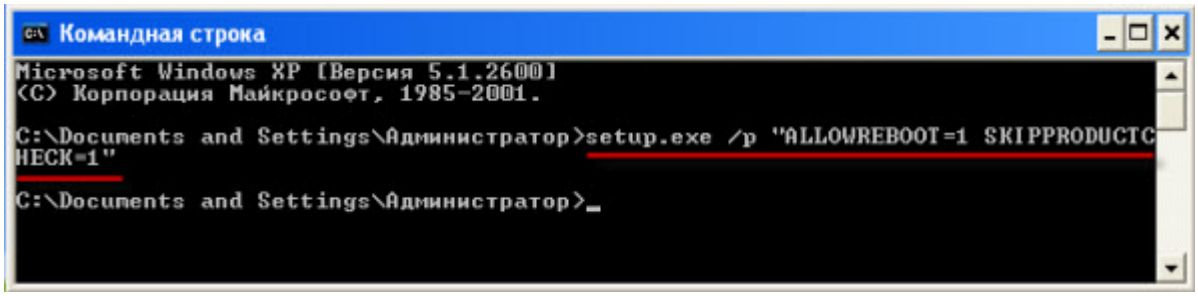


Рисунок 64 – Выполнение перезагрузки компьютера без поиска несовместимых продуктов

После ввода команды в окне командной строки нажмите клавишу Enter на клавиатуре. Будет запущена установка Антивируса Касперского/Kaspersky Internet Security 2011.

Следуя инструкциям Мастера установки завершите установку Антивируса Касперского/Kaspersky Internet Security 2011.

Задание 4: Проверка подлинности дистрибутива.

Все дистрибутивы (установочные файлы) Лаборатории Касперского подписаны цифровой подписью, что гарантирует неизменность файла при загрузке его с сайта Лаборатории Касперского на ваш компьютер.

Цифровая подпись необходимое и достаточное условие проверки подлинности дистрибутива.

Чтобы посмотреть наличие цифровой подписи, необходимо выполнить следующие шаги:

1. щелкнуть правой кнопкой мыши по загруженному файлу (дистрибутиву);
2. в появившемся контекстном меню выберать пункт Свойства;
3. в открывшемся окне выберать вкладку Цифровые подписи;
4. выделить в списке подпись Kaspersky Lab и нажать на кнопку Сведения;

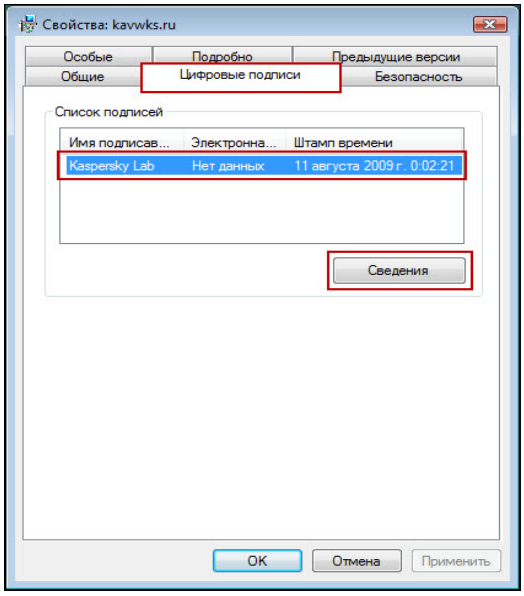


Рисунок 65 – Свойства дистрибутива

В окне Состав цифровой подписи на вкладке Общие можно посмотреть, действительна ли цифровая подпись.

На вкладке Общие отображается штамп времени – указание, в какое именно время была наложена подпись.

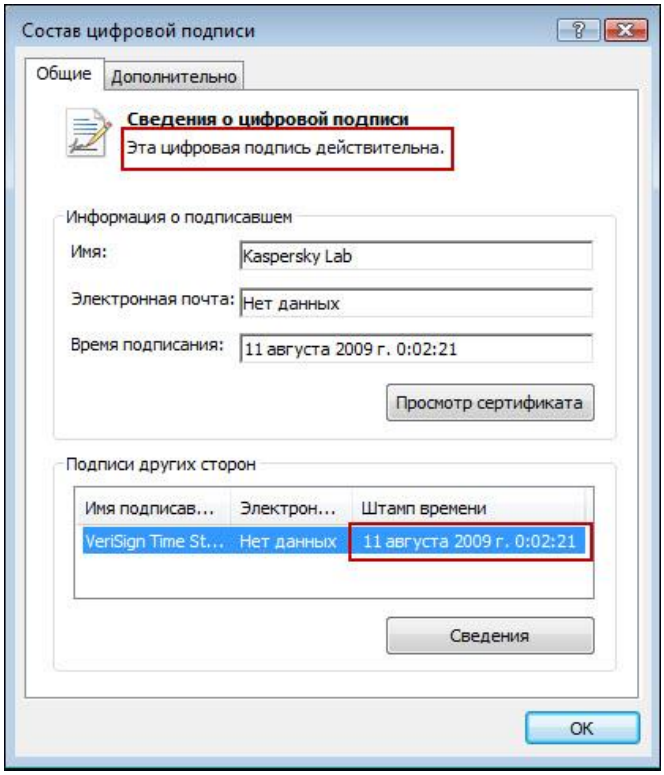


Рисунок 66 – Состав цифровой подписи

Если подпись недействительна, значит дистрибутив был изменён и использовать его не следует.

Если цифровая подпись нарушена, то вкладка Цифровые подписи пропадает из окна свойств файла. Следует проверять наличие этой вкладки, чтобы быть уверенным в том, что файл является подлинным.

Сертификат, которым Лаборатория Касперского подписывает свои файлы и драйверы, действует около года.

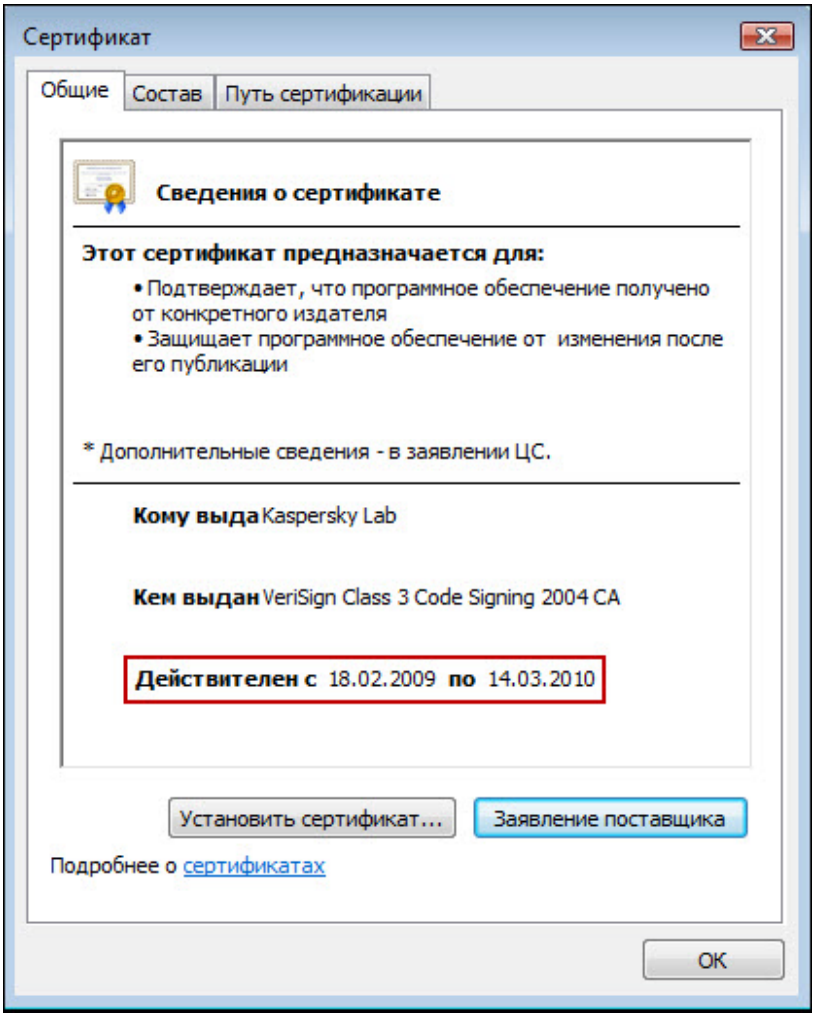


Рисунок 67 – Сведения о сертификате

Срок действия сертификата может истечь, но подпись будет считаться действительной, если она была наложена в то время, когда сертификат действовал.

Задание 5: Изучение интерфейса программы

Kaspersky Internet Security обладает простым и удобным интерфейсом. В данном разделе подробно рассмотрены его основные элементы.

Kaspersky Internet Security имеет компоненты расширения (плагины), встраиваемые в Microsoft Office Outlook, Microsoft Outlook Express, The Bat!, Thunderbird, Mozilla Firefox, Microsoft Internet Explorer и Microsoft Windows Explorer. Плагины расширяют возможности перечисленных программ, позволяя из их интерфейса настраивать параметры компонентов программы.

Сразу после установки Kaspersky Internet Security его значок появляется в области уведомлений панели задач Microsoft Windows.

В операционной системе Microsoft Windows 7 значок программы по умолчанию скрыт, для работы с программой вы можете его отобразить.

Значок выполняет следующие основные функции:

– служит индикатором работы программы;

– обеспечивает доступ к контекстному меню, главному окну программы и окну просмотра новостей.

Индикация работы программы

Значок служит индикатором работы программы. Он отражает состояние защиты, а также показывает ряд основных действий, выполняемых программой на текущий момент:

 – проверяется почтовое сообщение;

 – проверяется веб-трафик;

 – обновляются базы и модули программы;

 – требуется перезагрузка компьютера для применения обновлений;

 – произошел сбой в работе какого-либо компонента программы.

По умолчанию включена анимация значка: например, при проверке почтового сообщения на фоне значка программы пульсирует миниатюрный значок письма, а при обновлении баз программы – вращается значок глобуса. Есть возможность выключить анимацию.

При выключенной анимации значок может принимать следующий вид:

 (цветной значок) – все или некоторые компоненты защиты работают;

 (черно-белый значок) – все компоненты защиты выключены.

С помощью значка можно открыть контекстное меню и главное окно программы.

Чтобы открыть контекстное меню, наведите курсор на значок и нажмите на правую клавишу мыши.

Чтобы открыть главное окно программы, наведите курсор на значок и нажмите на левую клавишу мыши.

При появлении новостей от «Лаборатории Касперского» в области уведомлений панели задач Microsoft Windows появляется значок  . Двойным щелчком мыши на этом значке можно открыть окно Новостного агента.

С помощью новостного агента «Лаборатория Касперского» информирует обо всех важных событиях, касающихся Kaspersky Internet Security и защиты от компьютерных угроз в целом.

Программа будет уведомлять о появлении новостей с помощью всплывающего сообщения в области уведомлений панели задач. Значок программы в этом случае видоизменяется (см. ниже). Информация о количестве непрочитанных новостей также отображается в главном окне программы. В контекстном меню значка программы появляется пункт Новости, а в интерфейсе гаджета Kaspersky Internet Security появляется значок новости.

Контекстное меню позволяет перейти к выполнению основных задач защиты.

Меню Kaspersky Internet Security содержит следующие пункты:

– Обновление – запускает процесс обновления баз и модулей программы.

– Инструменты – открывает вложенное меню, содержащее следующие пункты.

– Контроль программ – открывает окно Активность программ;

– Мониторинг сети – открывает окно Мониторинг сети;

– Виртуальная клавиатура – выводит на экран виртуальную клавиатуру.

– Безопасный запуск программ – запускает безопасный рабочий стол для работы с программами, которые, могут быть небезопасны. Если безопасный рабочий стол уже запущен, то выполняется переключение на него.

– Kaspersky Internet Security – открывает главное окно программы.

– Приостановка защиты / Возобновление защиты – временно выключает / включает работу компонентов постоянной защиты. Данный пункт меню не влияет на обновление программы и на выполнение задач поиска вирусов.

– Включить Родительский контроль / Выключить Родительский контроль – включает / выключает Родительский контроль для текущей учётной записи.

– Настройка – открывает окно настройки параметров работы программы.

– О программе – открывает информационное окно со сведениями о программе.

– Новости – открывает окно новостного агента. Этот пункт меню отображается при наличии непрочитанных новостей.

– Выход – завершает работу Kaspersky Internet Security (при выборе данного пункта меню программа будет выгружена из оперативной памяти компьютера).

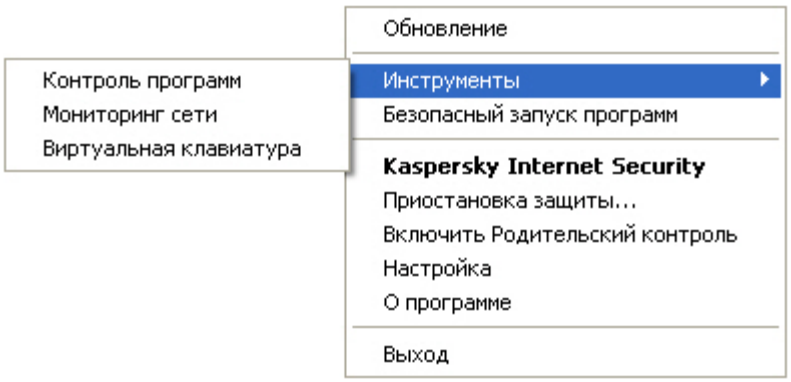


Рисунок 68 – Контекстное меню

Если в момент открытия контекстного меню запущена какая-либо задача проверки на вирусы или задача обновления программы, её название будет отражено в контекстном меню с указанием результата выполнения в процентах. Выбрав пункт меню с названием задачи, можно перейти к главному окну с отчётом о текущих результатах её выполнения.

Чтобы открыть контекстное меню, наведите курсор мыши на значок программы в области уведомлений панели задач и нажмите на правую клавишу мыши.

В операционной системе Microsoft Windows 7 значок программы по умолчанию скрыт, для работы с программой можно его отобразить.

В главном окне программы сосредоточены элементы интерфейса, предоставляющие доступ ко всем основным функциям программы.

Главное окно можно условно разделить на три части:

1. В верхней части окна расположен индикатор состояния защиты, который сигнализирует о текущем состоянии защиты вашего компьютера.

Рисунок 69 – Индикатор состояния защиты

Существует три возможных состояния защиты, каждое из которых обозначено цветом. Зелёный цвет означает, что защита компьютера осуществляется на должном уровне; жёлтый и красный предупреждают о наличии разного рода угроз безопасности. К угрозам относятся не только вредоносные программы, но и устаревшие базы программы, некоторые выключенные компоненты защиты.По мере возникновения угроз безопасности их необходимо устранять.

2. Левая часть окна позволяет быстро перейти к работе с основными функциями программы: включению и отключению компонентов защиты, выполнению задач проверки на вирусы, обновлению баз и модулей программы и т. д.

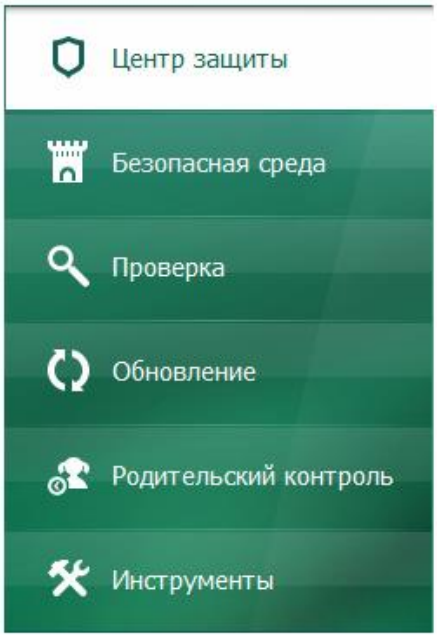


Рисунок 70 – Основные функции программы

3. Правая часть окна содержит информацию о функции программы, выбранной в левой части окна, а также позволяет настроить её параметры, предоставляет инструменты для выполнения задач проверки на вирусы, получения обновлений и т. д.

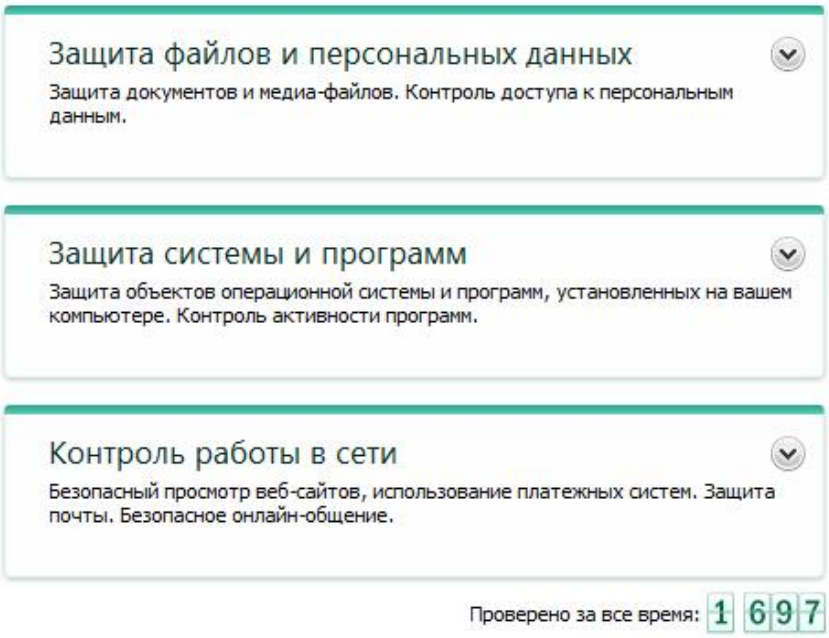


Рисунок 71 – Информация о функциях программы

Можно воспользоваться следующими кнопками и ссылками:

– Настройка – переход к окну настройки параметров программы.

– Карантин – переход к работе с объектами, помещёнными на карантин.

– Отчёты – переход к отчёту о работе программы, выполненному в виде диаграмм.

– Новости – переход к просмотру новостей в окне новостного агента. Ссылка отображается после получения программой новости.

– Справка – переход к справочной системе Kaspersky Internet Security.

– Личный кабинет – переход в Личный кабинет пользователя на веб-сайте Службы технической поддержки.

– Поддержка – открытие окна с информацией о системе и ссылками на информационные ресурсы «Лаборатории Касперского» (сайт Службы технической поддержки, форум).

– Лицензия – переход к активации Kaspersky Internet Security, продлению срока действия лицензии.

Можно изменять внешний вид Kaspersky Internet Security, используя альтернативные графические оболочки.

Чтобы открыть главное окно программы, выполните одно из следующих действий:

– Наведите курсор на значок программы в области уведомлений панели задач и нажмите на левую клавишу мыши. (В операционной системе Microsoft Windows 7 значок программы по умолчанию скрыт, для работы с программой вы можете его отобразить).

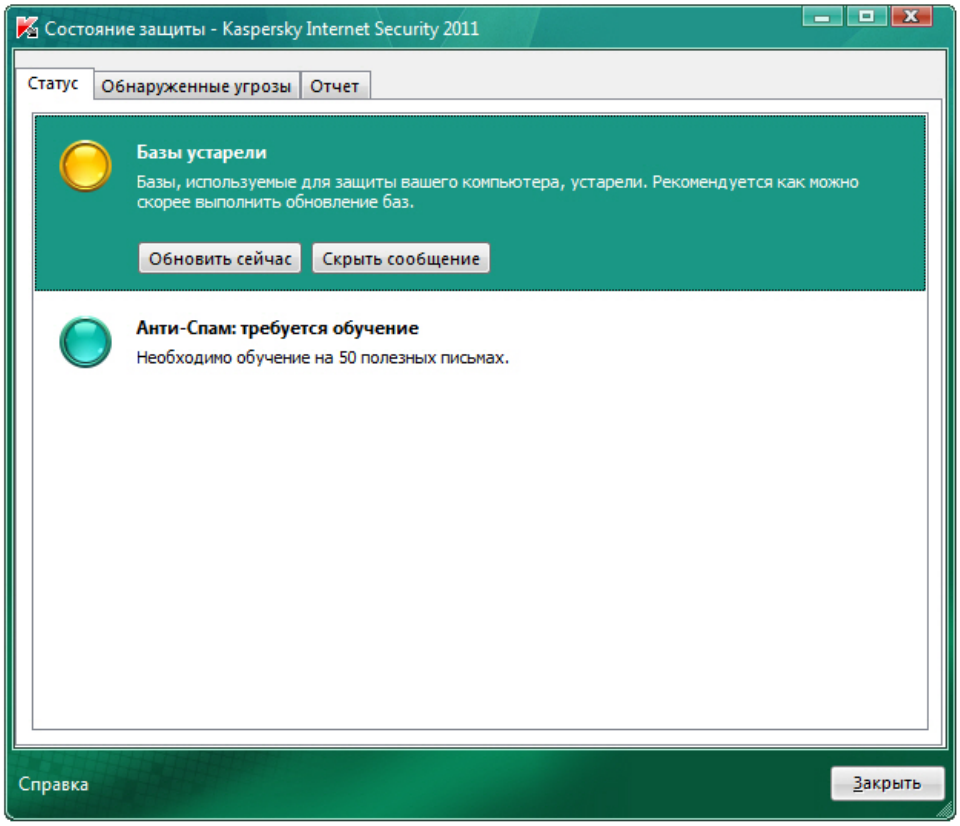
– Выберите пункт Kaspersky Internet Security в контекстном меню.

– Нажмите на значок Kaspersky Internet Security, расположенный в центральной части Kaspersky Gadget (только для операционных систем Microsoft Windows Vista и Microsoft Windows 7).

О появлении проблем в защите компьютера сигнализирует индикатор состояния защиты, расположенный в верхней части главного окна программы. Индикатор меняет цвет в зависимости от состояния защиты

компьютера: зелёный цвет означает, что компьютер защищён, жёлтый цвет свидетельствует о наличии проблем в защите, красный – о серьёзной угрозе безопасности компьютера. Проблемы и угрозы безопасности рекомендуется немедленно устранять.

Нажав на значок индикатора в главном окне программы, можно открыть окно Состояние защиты, в котором приведена подробная информация о состоянии защиты компьютера и предложены варианты действий для устранения проблем и угроз.



Решение проблем безопасности

Рисунок 72 – Состояние защиты

На закладке Статус окна Состояние защиты приведён список проблем в защите, в том числе обусловленных отклонениями от оптимальной работы программы (например, устареванием баз). Для устранения угроз предлагаются следующие варианты действий:

– Немедленно устранить. Нажатие на соответствующие кнопки позволит перейти к непосредственному устранению проблемы. Это действие является рекомендуемым.

– Отложить устранение. Если по какой-либо причине немедленное устранение проблемы невозможно, можно отложить данное действие и вернуться к нему позже. Для этого нажмите на кнопку Скрыть сообщение.

Обратите внимание, что для серьёзных проблем возможность отложить устранение не предусмотрена. К числу таких проблем относятся, например, наличие невылеченных вредоносных объектов, сбой в работе одного или нескольких компонентов, повреждение файлов программы.

Чтобы ранее скрытые сообщения были вновь отображены в общем списке, установите флажок Показать скрытые сообщения, который отображается в нижней части закладки при наличии скрытых сообщений.

На закладке Обнаруженные угрозы можно просмотреть список найденных вредоносных и возможно вредоносных объектов и выбрать действие над этими объектами (например, поместить на карантин). Для выбора действия используйте элементы управления, расположенные над списком, а также контекстное меню записей в списке.

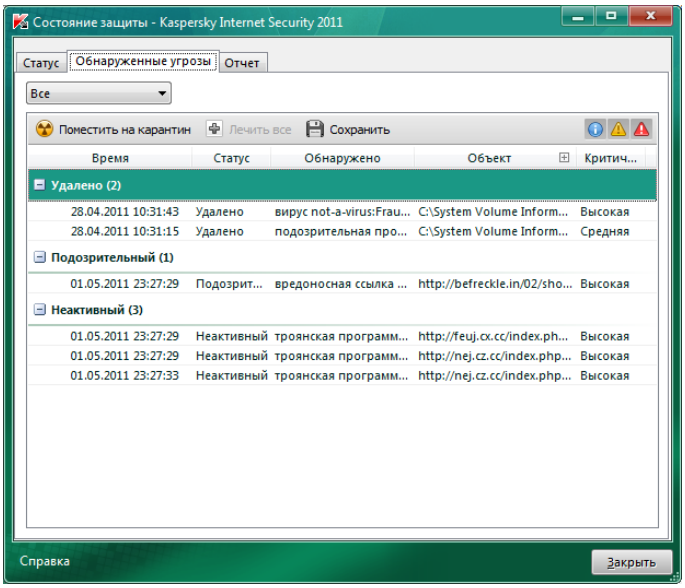


Рисунок 73 – Вкладка Обнаруженные угрозы

Список Обнаруженные угрозы содержит перечень найденных опасных объектов и выполняемых над ними действий. Объекты сгруппированы согласно принятой классификации угроз компьютерной безопасности. Можно отфильтровать список найденных объектов по следующим критериям:

– Все. В списке отображаются все найденные опасные объекты.

– Активные. В списке отображаются опасные объекты, обнаруженные программой, в отношении которых не было предпринято никаких действий. Такие объекты представляют угрозу безопасности для компьютера пользователя. Рекомендуется предпринять действия для устранения угроз.

– Карантин. В списке отображаются объекты, помещённые пользователем на карантин с целью их дальнейшего лечения. Чтобы поместить зараженный объект на карантин, воспользуйтесь ссылкой Поместить на карантин.

– Нейтрализованные. В списке отображаются объекты, которые были успешно вылечены Kaspersky Internet Security.

Поместить на карантин. Кнопка позволяет открыть стандартное окно для помещения выбранного файла на карантин.

Лечить все. Кнопка позволяет отправить на лечение все объекты из списка обнаруженных угроз.

Сохранить. Кнопка позволяет открыть стандартное окно для сохранения списка обнаруженных угроз в файл формата txt или csv.

Фильтрация:

- **Информационное событие**

  Нажатие на кнопку позволяет отфильтровать список по информационным событиям.
- **Важное событие**

  Нажатие на кнопку позволяет отфильтровать список по важным событиям.
- **Критическое событие**

  Нажатие на кнопку позволяет отфильтровать список по критическим событиям.

Время. Графа, в которой отображается время обнаружения опасного объекта. Вы можете использовать меню фильтра для этой графы.

Статус. Графа, в которой отображается статус обнаруженного объекта, присвоенный программой при его проверке / обработке. Можно использовать меню фильтра для этой графы.

Обнаружено. Графа, в которой отображается тип угрозы, обнаруженной в объекте, например, Сетевая атака. Можно использовать меню фильтра для этой графы.

Объект. Графа, в которой отображается тип объекта, в котором обнаружена угроза, например, Файл. Можно использовать меню фильтра для этой графы.

Знак «+» позволяет просмотреть подробную информацию об обнаруженном объекте: тип, признак наличия безопасного запуска, полный путь, имя.

Критичность. Графа, в которой отображается степень опасности объекта.

Возможные значения:

– средняя;

– высокая;

– низкая.

На закладке Отчёт можно ознакомиться с отчётами о работе программы.

Отчёт содержит статистику опасных и подозрительных объектов, обнаруженных программой за указанный период. Объекты сгруппированы согласно принятой классификации угроз компьютерной безопасности.

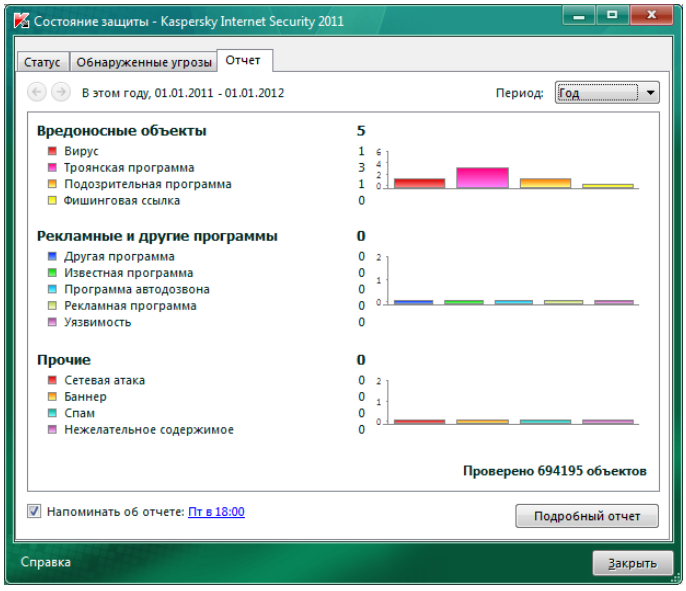


Рисунок 74 – Вкладка Отчёт

Нажатие на кнопки позволяет просмотреть отчёт за предыдущий и следующий период.

Период. Период, за который формируется отчёт.

Возможные значения:

- День.
- Неделя.
- Месяц.
- Год.
- Весь период.

Напоминать об отчёте. Флажок включает / выключает отправку уведомлений о готовности отчёта.

Если флажок установлен, Kaspersky Internet Security уведомляет пользователя о готовности отчёта. Кроме того, можно настроить расписание отправки уведомлений, перейдя по ссылке с заданной периодичностью в окно Отчёт: расписание.

Если флажок не установлен, Kaspersky Internet Security не отправляет уведомлений о готовности отчёта.

По умолчанию флажок установлен, и отправка уведомлений предлагается каждую пятницу в 18.00.

Подробный отчёт. Нажатие на кнопку открывает окно Подробный отчёт, в котором можно просмотреть детальные отчёты о работе компонентов и задач Kaspersky Internet Security.

Окна уведомлений и всплывающие сообщения. Kaspersky Internet Security уведомляет о значимых событиях, происходящих в процессе его работы, с помощью *окон уведомлений* и *всплывающих сообщений*, которые появляются над значком программы в области уведомлений панели задач.

Окна уведомлений Kaspersky Internet Security выводит на экран в тех случаях, когда возможны различные варианты действий в связи с событием: например, при обнаружении вредоносного объекта можно заблокировать

доступ к нему, удалить его или попытаться вылечить. Программа предложит пользователю выбрать действие из числа возможных. Окно уведомления исчезает с экрана только после того, как вы выберете одно из предложенных действий.

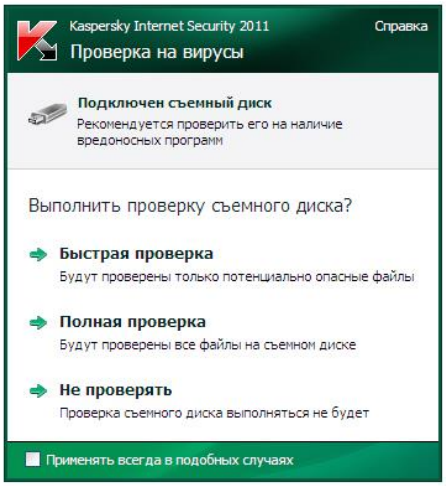


Рисунок 75 – Окно уведомления о проверке съёмного диска

Содержание отчета: тема, цель, описание основных этапов работы, скриншоты.

Самостоятельная работа №8: Компьютерные вирусы и борьба с ними.

Задание 1. Составьте инструкцию пользователю по применению антивирусной программы, указанной в индивидуальном задании, укажите: назначение программы, выполняемые функции, технология работы, рекомендации пользователю.

Индивидуальные задания: AidsTest, ADinf, Norton AntiVirus, ADinf Cure Module, AVZ, Scan, Symantec Endpoint Protection, Антивирус Касперского, Panda Antivirus, Avast, McAfee, Nod32, USB Disk Security, Zillya!, Microsoft Security Essentials, NANO Антивирус, TrustPort Antivirus,

ВирусБлокАда (VBA32), ActiveVirusShield, Ashampoo AntiVirus, Outpost Antivirus, Winpooch, Comodo AntiVirus, ClamWin, eScan Antivirus

Номер варианта должен соответствовать порядковому номеру студента в учебном журнале.

Образец выполнения: Антивирусная программа Doctor Web. *Назначение программы*: Эта программа-полифаг предназначена, прежде всего, для борьбы с полиморфными вирусами, которые сравнительно недавно появились в компьютерном мире. Использование Dr. Web для проверки дисков и удаления обнаруженных вирусов в целом подобно программе Aidstest. При этом дублирования проверки практически не происходит, так как Aidstest и Dr. Web работают на разных наборах вирусов. Программа Dr. Web может эффективно бороться со сложными вирусами-мутантами, которые оказываются не под силу программе Aidstest. В отличие от Aidstest программа Dr. Web способна обнаруживать изменения в собственном программном коде, эффективно определять файлы, зараженные новыми, неизвестными вирусами, проникая в зашифрованные и упакованные файлы, а также преодолевая "вакцинное прикрытие". Это достигается благодаря наличию достаточно мощного эвристического анализатора.

Выполняемые функции: В режиме эвристического анализа программа Dr. Web исследует файлы и системные области дисков, пытаясь обнаружить новые или неизвестные ей вирусы по характерным для вирусов кодовым последовательностям. Если таковые будут найдены, то выводится предупреждение о том, что объект, возможно, инфицирован неизвестным вирусом. Предусмотрены три уровня эвристического анализа.

В режиме эвристического анализа возможны ложные срабатывания, т.е. детектирование файлов, не являющихся зараженными. Уровень "эвристики" подразумевает собой уровень анализа кода без наличия ложных срабатываний. Чем выше уровень "эвристики", тем выше процент наличия ошибок или ложных срабатываний.

Рекомендуются первые два уровня работы эвристического анализатора.

Третий уровень эвристического анализа предусматривает дополнительную проверку файлов на "подозрительное" время их создания. Некоторые вирусы при заражении файлов устанавливают некорректное время создания, как признак зараженности данных файлов. Например, для зараженных файлов секунды могут иметь значение 62, а год создания может быть увеличен на 100 лет.

В комплект поставки антивирусной программы Dr.Web могут входить также файлы-дополнения к основной вирусной базе программы, расширяющие ее возможности. Работать с программой Dr.Web можно в двух режимах: в режиме полноэкранного интерфейса с использованием меню и диалоговых окон; в режиме управления через командную строку. Для разового нерегулярного применения более удобен первый режим, но для регулярного применения с целью систематического входного контроля дискет лучше применять второй режим. При использовании второго режима соответствующая команда запуска Dr.Web должна быть включена либо в меню пользователя операционной оболочки Norton Commander, либо в специальный командный файл.

Командная строка для запуска Dr. Web выглядит следующим образом: ^ *DrWeb (диск:[путь]][ключи]* где диск:

X:− логическое устройство жесткого диска или физическое устройство гибкого диска, например F: или A:,
*−все логические устройства на жестком диске,
путь—это путь или маска требуемых файлов.
Наиболее важные ключи: /AL− диагностика всех файлов на заданном устройстве; /CU[P]− "лечение" дисков и файлов, удаление найденных вирусов; /P удаление вирусов с подтверждением пользователя; /DL− удаление файлов, корректное лечение которых невозможно; /HA[уровень]− эвристический анализ файлов и поиск в них неизвестных вирусов, где уровень может принимать значения 0, 1,2; /RP[имя файла] − запись протокола работы в файл (по умолчанию в файл REPORT.WEB); /CL− запуск

программы в режиме командной строки, при тестировании файлов и системных областей не используется полноэкранный интерфейс; /QU− выход в DOS сразу после тестирования;/?− вывод на экран краткой справки.

Если в командной строке Dr.Web не указано ни одного ключа, то вся информация для текущего запуска будет считываться из файла конфигурации DRWEB.INI, расположенного в том же каталоге, что и файл DRWEB.EXE. Файл конфигурации создается в процессе работы с программой Dr. Web с помощью команды сохранения параметров, необходимых д тестирования.

Технология работы с программой Dr. Web в режиме полноэкранного интерфейса: Для запуска в режиме полноэкранного интерфейса достаточно ввести в командную crpoi только имя программы. Сразу после загрузки программы начнется тестирование операти ной памяти компьютера, если оно не отключено предыдущей установкой параметров. Хс тестирования отображается в окне тестирования. После завершения тестирования памш произойдет остановка. Работу программы можно продолжить, если воспользоваться ochoi ным меню, расположенным в верхней строке экрана. Для активизации меню следует нажать клавишу: Основное меню содержит следующие режимы: *Dr.Web Тест Настройки Дополнения* При выборе любого режима открывается соответствующее подменю. Подменю Dr. Web позволяет временно выйти в DOS, получить краткую информацию о программе Dr.Web и о ее авторе или покинуть программу. Подменю *Тест* дает возможность выполнить основные операции тестирования и "лечения" файлов и дисков, а также просмотреть отчеты о произведенных действиях. Подменю *Настройки* служит для установки с помощью диалоговых окон параметров настройки программы, установки путей и масок поиска и сохранения параметров в файл конфигурации DRWEB.INI. Для подключения файлов-дополнений к основной вирусной базе программы, расширяющих ее возможности, используется режим *Дополнения.*

Рекомендации пользователю: Для того чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила: оснастите свой компьютер современными антивирусными программами и постоянно обновляйте их версии; перед считыванием с дискет информации, записанной на других компьютерах, всегда проверяйте эти дискеты на наличие вирусов, запуская антивирусные программы своего компьютера; при переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами; периодически проверяйте на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив операционную систему также с защищенной от записи системной дискеты; всегда защищайте свои дискеты от записи при работе на других компьютерах, если на них не будет производиться запись информации обязательно делайте архивные копии на дискетах ценной для вас информации; не оставляйте в кармане дисковода дискеты при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами используйте антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей.

4. Контрольные вопросы

1. Что такое программный вирус и какова его природа?
2. В чем состоят вредные проявления компьютерных вирусов?
3. Какие основные виды компьютерных вирусов вам известны?
4. Какие существуют виды программ для обнаружения и защиты от вирусов?
5. В чем состоят достоинства программ-ревизоров и программ-фильтров?
6. Назовите основные меры по защите от компьютерных вирусов.

7. Опишите технологию периодической проверки жесткого диска на наличие вирусов.

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ К ЭКЗАМЕНУ

1. Понятие защищенной операционной системы.
2. Подходы к организации защиты операционной системы.
3. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа.
4. Применение типовых моделей управления доступом в операционных системах.
5. Управление доступом в UNIX.
6. Управление доступом в Windows.
7. Назначение атрибутов защиты вновь создаваемым объектам Windows, наследование дескрипторов защиты.
8. Средства минимизации полномочий пользователей в Windows.
9. Управление средствами аутентификации в Linux и Windows.
10. Управление средствами аудита в Linux и Windows.
11. Управление доменами Windows.
12. Групповая политика в доменах Windows.
13. Сетевые атаки.
14. Адаптивная безопасность в вычислительных сетях.
15. Пакетные фильтры и межсетевые экраны, их классификация и особенности применения.
16. Виртуальные частные сети.
17. Угрозы безопасности баз данных: общие и специфичные.
18. Модели безопасности СУБД.
19. Средства и методы обеспечения целостности данных СУБД.
20. Ролевое разграничение доступа к данным в современных СУБД.
21. Понятие программной закладки.
22. Модели взаимодействия программной закладки с атакуемой компьютерной системой.

23. Предпосылки к внедрению программных закладок.

24. Метод внедрения программных закладок.

25. Основные принципы построения политики безопасности, повышающей защищенность от программных закладок.

26. Сигнатурное и эвристическое сканирование как метод выявления программных закладок.

27. Контроль целостности как метод выявления программных закладок.

28. Антивирусный мониторинг как метод выявления программных закладок.

29. Изолированная программная среда как метод выявления программных закладок.

30. Файловые вирусы: жизненный цикл, особенности функционирования, особенности противодействия файловым вирусам.

31. Сетевые вирусы: жизненный цикл, особенности функционирования, особенности противодействия сетевым вирусам.

32. Скриптовые вирусы: жизненный цикл, особенности функционирования, особенности противодействия Скриптовым вирусам.

33. Стелс-технологии: назначение, методы противодействия.

34. Основные компоненты подсистемы защиты Unix

35. Файловая система – как основа подсистемы защиты.

36. Права доступа к элементам файловой системы.

37. Управление процессами. Создание и удаление бюджетов пользователей

38. Основные компоненты подсистемы защиты ОС Windows

39. Основы взаимодействия элементов гетерогенных сетей

40. Методы и средства ограничения доступа к компонентам ЭВМ.

ПОНЯТИЙНЫЙ МИНИМУМ

Аутентификация Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности (ГОСТ Р ИСО 7498-2-99, ОСТ 45.127-99).

База данных Объективная форма представления и организации совокупности данных (статей, расчетов и так далее), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронной

вычислительной машины (Закон Российской Федерации № 5351-1 от 09 июля 1993 г. с изменениями от 19 июля 1995 г.).

Безопасность информации Состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации и т.п. (Положение о государственном лицензировании деятельности в области защиты информации: Утверждено Решением Государственной Технической Комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации № 10 от 27 апреля 1994 г. и № 60 от 24 июня 1997 г.).

Безопасность информации (данных) Состояние защищенности информации (данных), обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз (ОСТ 45.127-99).

Данные Информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека (ГОСТ Р 15971-90, ОСТ 45.127-99).

Дестабилизирующий фактор (ДФ) Явление или событие, следствием наступления которого может быть нарушение конфиденциальности, целостности и/или доступности информационных ресурсов, нарушению работоспособности сети или ее элементов. Информационная угроза, угроза информационной безопасности (см. далее) могут быть отнесены к ДФ.

Достоверность Идентичность объекта защиты заявленному.

Доступ несанкционированный к информации Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами (ОСТ 45.127-99).

Доступность Свойство субъекта и/или объекта доступа быть доступным и используемым по запросу со стороны уполномоченного логического объекта (ГОСТ Р ИСО 7498-2-99).

Живучесть сети Свойство сети сохранять способность выполнять требуемые функции в условиях, создаваемых воздействиями внешних ДФ.

Защита информации Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию (ГОСТ Р 50922-96, ОСТ 45.127-99) воплощенная в совокупности технических и организационных мер, обеспечивающих информационную безопасность.

Защита информации от несанкционированного доступа Деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. (ГОСТ Р 50922-96).

Защищаемая информация Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (ГОСТ Р 50922-96).

Злоумышленник Лицо, осуществляющее осознанные действия по нарушению информационной безопасности объекта защиты.

Идентификация Присвоение субъектам и/или объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов (Защита от несанкционированного доступа к информации. Термины и определения: Руководящий документ).

Информационная безопасность Состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства (Федеральный Закон № 85 от 4 июля 1996 г. "Об участии в международном информационном обмене").

Информационная безопасность (ЕСЭ РФ) Состояние (степень) защищенности информационной сферы Единой сети электросвязи (быв. Взаимоувязанной сети связи) Российской Федерации от заданного Руководящими или нормативными документами множества угроз информационной безопасности Взаимоувязанной сети связи Российской Федерации (ОСТ 45.127-99).

Информационная безопасность инфокоммуникационной системы Это состояние информации, информационных ресурсов и инфокоммуникационной системы, при котором с требуемой надежностью обеспечивается защищенность от угроз системе формирования, распространения и использования информационных ресурсов.

Информационная система Организационно упорядоченная совокупность документов (массивов документов) и информационных технологий , в том числе с использованием средств вычислительной техники и связи (Федеральный Закон № 24 от 20 февраля 1995 г. "Об информации, информатизации и защите информации").

Информационная сфера (ЕСЭ РФ) Совокупность информационных ресурсов и информационной структуры Единой сети электросвязи (быв. Взаимоувязанной сети связи Российской Федерации (ОСТ 45.127-99)).

Информационная угроза Фактор или совокупность факторов, создающих опасность нарушения свойств информации.

Информационные потоки Совокупность передаваемой информации между двумя и более взаимодействующими объектами

Информационные ресурсы Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах) (Федеральный Закон № 24 от 20 февраля 1995 г. "Об информации, информатизации и защите информации").

Информация Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления (Федеральный Закон № 24 от 20 февраля 1995 г. "Об информации, информатизации и защите информации").

Канал Маршрут передачи информации (ГОСТ Р ИСО 7498-2-99).

Конфиденциальность информации Состояние информации и её носителей, при котором обеспечивается защищённость информации от раскрытия.

Криптографическая защита Защита данных при помощи криптографического преобразования данных (ГОСТ 28147-89).

Критическая (конфиденциальная, защищаемая) информация Это информация с соответствующими грифами секретности, информация для служебного пользования, информация, являющаяся собственностью организации.

Легальные пользователи Пользователи, имеющие законные основания для доступа к заданным ресурсам и сервисам.

Мероприятие по защите информации Совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации (ГОСТ Р 50922-96).

Меры обеспечения информационной безопасности (ЕСЭ РФ) Правовые, организационные, программные и аппаратные способы, правила и процедуры использования механизмов защиты Единой сети электросвязи (быв. Взаимоувязанной сети связи) Российской Федерации (ОСТ 45.127-99).

Механизм обеспечения информационной безопасности (ЕСЭ РФ) Аппаратно-программные и организационные средства системы обеспечения информационной безопасности ЕСЭ РФ, реализующие в соответствии с заданной политикой информационной безопасности ЕСЭ РФ один или несколько аспектов защиты информационной сферы ЕСЭ РФ в соответствии с одним из трех перекрывающих друг друга классов защиты: предотвращение воздействий нарушителя информационной безопасности, обнаружение воздействия нарушителя информационной безопасности, восстановление (ликвидация) последствия воздействия нарушителя информационной безопасности (ОСТ 45.127-99).

Надежность сети Свойство сети сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях использования и технического обслуживания.

Нарушитель (в автоматизированной системе) Субъект, имеющий доступ к работе со штатными средствами автоматизированной системы и средствами вычислительной техники как части автоматизированной системы (Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: Руководящий документ).

Нарушитель информационной безопасности (ЕСЭ РФ) Физическое или юридическое лицо, общественное объединение, ведомство, процесс, событие, способное произвести несанкционированные или непреднамеренные действия (операции) над информационной сферой ЕСЭ РФ, приводящие к нежелательным для пользователя или оператора связи ЕСЭ РФ последствиям (ОСТ 45.127-99).

Несанкционированный доступ Нарушение регламентированного доступа к объекту защиты (Защита информации. Специальные защитные знаки. Классификация и общие требования: Руководящий документ).

Несанкционированный доступ к информационной сфере (ЕСЭ РФ) Последствие воздействия нарушителя информационной безопасности на ЕСЭ РФ, характеризующееся доступом к информационной сфере ЕСЭ РФ с нарушением установленных прав и правил разграничения доступа, дающим возможность нарушителю совершать последующие действия (операции) по реализации той или иной угрозы информационной безопасности ЕСЭ (ОСТ 45.127-99).

Несанкционированный доступ к услугам электросвязи (ЕСЭ РФ) Последствие воздействия нарушителя информационной безопасности на Единую сеть электросвязи (быв. Взаимоувязанную сеть связи) Российской Федерации, характеризующееся доступом к слугам связи с нарушением установленных прав и правил разграничения доступа (ОСТ 45.127-99).

Обслуживающий персонал Сотрудники, не имеющие доступа к технологическому оборудованию СС, выполняющие функции по обслуживанию заданий, сооружений, технических систем и имеющих возможность физического доступа к оборудованию связи.

Объект защиты информации Информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации (ГОСТ Р 50922-96).

Оперативность (работы, функционирования) сети Свойство сети, отражающее возможность передачи информации в заданные сроки или в темпе работы пользователя.

Подконтрольность Это обеспечение того, что действия субъекта по отношению к объекту атаки могут быть прослежены уникально по отношению к субъекту.

Работоспособность сети Свойство сети выполнять заданные функции в соответствии с требованиями.

Рентабельность сети Способность сети оправдывать расходы, связанные с обеспечением ее функционирования и развития; способность сети быть целесообразной с хозяйственной точки зрения.

Сеть связи Совокупность пространственно разнесенных технических и программных средств, сооружений и организационно.

Сеть связи общего пользования Составная часть Единой сети электросвязи (быв. Взаимоувязанной сети связи) Российской Федерации, открытая для пользования физическим и юридическим лицам, в услугах которой эти лицам не может быть отказано (Федеральный Закон № 15 от 16 февраля 1995 г. "О связи", ОСТ 45.127-99).

Система обеспечения информационной безопасности Совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Средство защиты информации Техническое, программное средство, вещество и /или материал, предназначенные или используемые для защиты информации (ГОСТ Р 50922-96).

Технические каналы утечки информации Это физическая среда распространения опасных сигналов, несущих конфиденциальную информацию, выходящая за пределы охраняемой территории.

Угроза безопасности информации Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее (ГОСТ Р 51624-00).

Угроза информационной безопасности (ЕСЭ РФ) Последствия воздействия нарушителя информационной безопасности ЕСЭ РФ, не предотвращение, либо не обнаружение и не ликвидация которого средствами ЕСЭ РФ может привести к ухудшению заданного Руководящими и нормативными документами уровня качества службы или к ухудшению заданных качественных характеристик функционирования ЕСЭ РФ и, как следствие, нанесению ущерба пользователю или оператору связи ЕСЭ РФ.

Угроза информационной безопасности инфокоммуникационной системы Действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.

Управление Процесс целенаправленного воздействия на объект, осуществляемого для организации его функционирования в соответствии с заданными требованиями.

Услуги связи Продукт деятельности по приему, обработке, передаче и доставке почтовых отправлений или сообщений электросвязи (ОСТ 45.127-99).

Устойчивость Способность сети сохранять работоспособное состояние во времени и в условиях, создаваемых воздействиями внешних и внутренних ДФ. Устойчивость характеризуется свойствами надежности и живучести.

Уязвимость Некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации (ГОСТ Р ИСО 7498-2-99).

Целостность информации Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения) (ОСТ 45.127-99).

Эффективность защиты: степень соизмерения результатов с затратами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК.

ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования .

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические ___ . Госстандарт России. - М., 1995.

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. - М., 2006.

ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие требования. Госстандарт России. - М., 2006.

ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем». – М.: Стандартинформ, 2015.

1. [Электронный ресурс] // URL: http://fstec.ru/- (Дата обращения: 13.10.2021)

2. [Электронный ресурс] // URL: http://www.e-nigm.ru/rticles/- (Дата обращения: 12.10.2021)

3. [Электронный ресурс] // URL:http://www.iso27000.ru/zkonodtelstvo/normtivnye-dokumenty-fstek-rossii- (Дата обращения: 12.10.2021)

4. APPROBATION OF A MATHEMATICAL MODEL OF THE INFLUENCE OF THREE-LEVEL SEMANTIC REPRESENTATION OF A EDUCATIONAL MESSAGE ON THE DYNAMICS OF STUDENTS′ CREATIVITY. Gafarova Ye., Belevitin V., Korchemkina Yu., Smirnov Ye., Khasanova M. // International Journal of Engineering and Technology. 2018. Т. 7. № 4. С. 171.

5. DEVELOPMENT OF A MATERIAL SELECTION MODEL FOR ROLLS ROLLING MILLS USING NEURAL NETWORKS Gafarov M.F., Pavlova K.P., Gafarova E.A. в сборнике: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020. 2020. С. 9271519.

6. MACHINE LEARNING METHODS AND QUALIMETRIC APPROACH TO DETERMINE THE CONDITIONS FOR TRAIN STUDENTS IN THE FIELD OF ENVIRONMENTAL AND ECONOMIC ACTIVITIES. Salamatov A.A., Gafarova E.A., Belevitin V.A., Gafarov M.F., Gordeeva D.S.//International Journal of Emerging Technologies in Learning. 2021. Т. 16. № 3. С. 72-85.

7. MODELING OF MATERIAL AND HEAT BALANCE OF FERROMANGANESE BLAST FURNACE SMELTING USING COMPUTER ENVIRONMENT LAZARUS. Gafarov M.F., Senin A.V., Gafarova E.A.//Materials Science Forum. 2019. Т. 946 MSF. С. 411-416.

8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

9. Буслов Д.И., Холкин И.Н. Как, используя диверсионный анализ ТРИЗ, найти критическую уязвимость, грозящую безопасности SP Hn // Математика и информационные технологии в нефтегазовом комплексе. 2015. №2. URL: http://cyberlenink.ru/rticle/n/kk-ispolzuy-diversionnyy-nliz-triz-nyti-kriticheskuyu-uyzvimost-grozyschuyu-bezopsnosti-sp-hn (дата обращения: 11.10.2021).

10. Галатенко В.А. Идентификация и аутентификация, управление доступом [Электронный ресурс]: http://citforum.ru/security/articles/galatenko/- (дата обращения -17.10.2021)

11. Гафарова Е.А. Развитие креативности путем расширения разнообразия модального опыта обучаемого /Гафарова Е.А. Дискуссия. 2016. № 6 (69). с. 121-129.

12. Гафарова Е.А. Формирование творческих умений у старшеклассников при изучении информационно-коммуникационных технологий / Гафарова Е.А. диссертация на соискание ученой степени кандидата педагогических наук / Челябинск, 2007

13. Гафарова Е.А., Синицын Ф.В. К вопросу проектирования онтологий предметной области при подготовке магистров по направлению информационная безопасность.// Инновационные технологии в подготовке современных профессиональных кадров: Опыт, проблемы. Сборник научных трудов. 2016, Челябинский филиал РАНХиГС, 56-59 с.

14. Диденко Е.В., Гафарова Е.А., Диденко Г.А. ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ ФОРМИРОВАНИЯ ГОТОВНОСТИ ОБУЧАЮЩИХСЯ КОЛЛЕДЖА К ПРОТИВОДЕЙСТВИЮ ВОВЛЕЧЕНИЮ В КИБЕРЭКСТРЕМИСТСКУЮ ДЕЯТЕЛЬНОСТЬ // Современные наукоемкие технологии. – 2019. – № 3-2. – С. 280-283

15. Диденко Е.В., Гафарова Е.А., Степанова О.А., Диденко Г.А., Шамаева Т.Н. АНАЛИЗ РЕЗУЛЬТАТОВ ЭКСПЕРИМЕНТАЛЬНОЙ РАБОТЫ ПО ФОРМИРОВАНИЮ ГОТОВНОСТИ ОБУЧАЮЩИХСЯ КОЛЛЕДЖА К ПРОТИВОДЕЙСТВИЮ ВОВЛЕЧЕНИЯ В КИБЕРЭКСТРЕМИСТСКУЮ ДЕЯТЕЛЬНОСТЬ // Современные наукоемкие технологии. – 2019. – № 8. – С. 112-116, URL: https://top-technologies.ru/ru/article/view?id=37640 (дата обращения: 17.10.2021).

16. Коноваленко С. А., Королев И. Д. Выявление уязвимостей информационных систем. // Инновации в науке: сб. ст. по матер. LXI междунар. науч.-практ. конф. № 9(58). – Новосибирск: СибАК, 2016. – С. 12-20.

17. Мезенов А.С., Гафарова Е.А. О реализации конституционного права граждан на доступ к информации в условиях интенсификации сетевого взаимодействия.//Сборник научных трудов конференции «Инновационные технологии в подготовке современных профессиональных кадров: опыт, проблемы», 2016, Издательство: Челябинский филиал РАНХиГС, с.94-99

18. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России.

19. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. ФСТЭК России.

20. Организационно-правовое обеспечение информационной безопасности [Текст] / Гафарова Е.А. Учебное пособие, Южно-Уральский государственный гуманитарно-педагогический университет, ЗАО "Библиотека А. Миллера" г. Челябинск, 2019, 153 с.

21. Приказ Министерства образования и науки РФ от 1 декабря 2016 г. № 1513 “Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры)”

22. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

23. ПРИМЕНЕНИЕ ПЕДАГОГИЧЕСКИХ ПРОГРАММНЫХ СРЕДСТВ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ ВУЗА И ИХ РОЛЬ В ПОСТРОЕНИИ ИНДИВИДУАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ТРАЕКТОРИИ ОБУЧАЮЩИХСЯ. Корчемкина Ю.В., Гафарова Е.А., Хасанова М.Л., Аксенова Л.Н.//Ученые записки университета им. П.Ф. Лесгафта. 2018. № 8 (162). С. 95-100.

24. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция)

25. Фомичева Т.Г. Лабораторный практикум по курсу «Компьютерные технологи и в правовой практике» Южно-Российский государственный технический университет, Новочеркасск 2008, 112 с.

Учебное издание

Гафарова Елена Аркадьевна

Программно-аппаратные средства обеспечения информационной безопасности. Практикум.

Издательство ЗАО «Библиотека А.Миллера»
454091, г. Челябинск. Ул. Свободы, 159

Подписано в печать 20.10.2021 Формат 60х90/16
Объем 10, 46 усл.-печ. л. Тираж 100 экз.

Заказ 572
Отпечатано с готового оригинал-макета
в типографии ЮУРГГПУ
454080, г. Челябинск, пр. Ленина, 69