МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕВЕРО-КАВКАЗСКИЙ ФИЛИАЛ ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
СВЯЗИ И ИНФОРМАТИКИ»

С.А. ШВИДЧЕНКО

Методические указания для проведения лабораторных работ по дисциплине

Б1.В.05 «Разработка безопасного программного обеспечения»

Кафедра **«Информатика и вычислительная техника»**

Направление подготовки **10.03.01 Информационная безопасность**

Профиль **Безопасность компьютерных систем**

Разработала:
Доцент кафедры ИВТ Швидченко С.А.

Ростов-на-Дону
2022

Методические указания
для проведения лабораторных работ
по дисциплине
«Разработка безопасного программного обеспечения»

Составитель: Швидченко С.А., доц. каф. «ИВТ»

Рассмотрено и одобрено
на заседании кафедры «ИВТ»
Протокол от «30» августа 2022 г., № 1.

Лабораторная работа №1. МЕТОДЫ ПОИСКА И СБОРА ИНФОРМАЦИИ. МЕТОДИКА УСТРАНЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

Цель работы: Приобретение навыков поиска информации используя поисковые системы.

Интернет – это глобальная компьютерная сеть, объединяющая многие локальные, корпоративные, региональные сети и включающая десятки миллионов компьютеров.

В каждой такой локальной или корпоративной сети обычно имеется хотя бы один компьютер, который имеет постоянное подключение к Интернет с помощью лини связи с высокой пропускной способностью. В качестве таких магистральных линий связи обычно используют оптоволоконные или спутниковые линии с пропускной способностью от 1 до 100 Мбит/с.

Таким образом, основу, «каркас» Интернет составляют более 40-ка миллионов серверов, постоянно подключенных к сети. К ним, в свою очередь, могут подключаться с помощью локальных сетей или коммутированных телефонных линий сотни миллионов пользователей Интернет.

Для подключения компьютера к телефонной линии используется модем.Компьютер передает модему информацию в виде последовательности электрических импульсов, модем на передающей стороне преобразует цифровые сигналы компьютера (электрические импульсы) в аналоговый сигнал, т.е. он модулирует аналоговый сигнал цифровым.

Поиск информации в Интернете осуществляется с помощью специальных программ, обрабатывающих запросы — информационно-поисковых систем (ИПС). Существует несколько моделей, на которых основана работа поисковых систем, но исторически две модели приобрели наибольшую популярность — это поисковые каталоги и поисковые указатели.

Поисковые каталоги устроены по тому же принципу, что и тематические каталоги крупных библиотек. Они обычно представляют собой иерархические гипертекстовые меню с пунктами и подпунктами, определяющими тематику сайтов, адреса которых содержатся в данном каталоге, с постепенным, от уровня к уровню, уточнением темы. Поисковые каталоги создаются вручную.

Основной проблемой поисковых каталогов является чрезвычайно низкий коэффициент охвата ресурсов WWW. Чтобы многократно увеличить коэффициент охвата ресурсов Web, из процесса наполнения базы данных поисковой системы необходимо исключить человеческий фактор — работа должна быть автоматизирована.

Автоматическую каталогизацию Web-ресурсов и удовлетворение запросов клиентов выполняют поисковые указатели. Работу поискового указателя можно условно разделить на три этапа:

· сбор первичной базы данных. Для сканирования информационного пространства WWW используются специальные агентские программы — черви, задача которых состоит в поиске неизвестных ресурсов и регистрация их в ба-

зе данных

· индексация базы данных — первичная обработка с целью оптимизации поиска. На этапе индексации создаются специализированные документы — собственно поисковые указатели;

· рафинирование результирующего списка. На этом этапе создается список ссылок, который будет передан пользователю в качестве результирующего. Рафинирование результирующего списка заключается в фильтрации и ранжировании результатов поиска. Под фильтрацией понимается отсев ссылок, которые нецелесообразно выдавать пользователю (например, проверяется наличие дубликатов). Ранжирование заключается в создании специального порядка представления результирующего списка (по количеству ключевых слов, сопутствующих слов и др.).

В России наиболее крупными и популярными поисковыми указателями являются:

· «Яndex» (www.yandex.ru)
· «Рамблер» (www.rambler.ru)
· «Google» (www.google.ru)
· «Апорт2000» (www.aport.ru)

Ход работы

1. Освоить элементарные приемы поиска информации в сети Интернет.
2. Осуществить поиск образовательных сайтов.
3. Освоить приёмы поиска информации с помощью поисковой машины, используя группы слов для организации простого поиска.
4. Освоить приёмы поиска информации с помощью поисковой машины, изучить особенности поиска нормативного документа.
5. Сформировать документ по теме «Указать заданную тему», используя электронные документы, представленные глобальной сетью Internet.
6. Подготовить отчёт, и ответы на контрольные вопросы.

1. Для того чтобы освоить элементарные приёмы поиска информации в сети Интернет необходимо выполнить следующие действия:

· запустить обозреватель MS Internet Explorer;
· в адресной строке набрать адрес поискового WWW-сервера;
· открыть новое окно браузера, выполнив последовательность команд в главном меню Файл - Создать - Окноили использовав сочетание клавиш Ctrl+N;
· повторить п.п. 2, 3 не менее четырех раз. В разные окна браузера загрузите главные страницы поисковых машин;
· сравнить интерфейсы поисковых WWW-серверов;
· с помощью справочных систем познакомьтесь с основными средствами простого и расширенного поиска;
· организуйте поиск, заполните таблицу и прокомментируйте результаты поиска:

· организуйте поиск интересующей Вас информации (как называется самое большое пресноводное озеро в мире) и внесите результаты в таблицу;

2. Для поиска образовательных сайтов, выполните следующие действия:

- запустить обозреватель MS Internet Explorer;
- ввести адрес http://www.list.ru в адресную строку обозревателя;
- в списке категорий перейти последовательно по следующим ссылкам. Образование - Наука - Школы - Физико-математические школы.

В результате мы получили список 14 физико-математических школ. Каждая строка списка – гипертекстовая ссылка, перейдя по которой, можно просмотреть заинтересовавший вас школьный сайт.

3. Освоение приёмов поиска информации с помощью поисковой машины, формирование группы слов для организации простого поиска.

Найдите биографию министра образования Российской Федерации Фурсенко А.А. с помощью поисковой системы Google.Ru. Выполните следующие действия:

- запустить обозреватель MS Internet Explorer;
- в адресной строке набрать адрес поисковой системы http://www.google.ru и инициализировать процесс загрузки ресурса;
- в интерфейсе начальной страницы поисковой системы Google.Ru найти форму для поиска и строку ввода запроса. Щелчком левой клавишей мыши по строке установить в ней курсор и напечатать: биография Филиппов министр;
- инициализировать процесс поиска в поисковой системе, нажав на кнопку Поиск в Google;
- просмотреть результаты поиска и найти среди них наиболее подходящие (релевантные) вашему запросу.

4. Для того чтобы найти Приказ Министерства образования и науки Российской Федерации от 24 марта 2010 г. № 209 "О порядке аттестации педагогических работников государственных и муниципальных образовательных учреждений". Для проведения поиска документа воспользуемся, например, поисковой машиной Яndex.ru. В группу ключевых слов запроса необходимо включить значимые по смыслу слова и исключить стоп-слова (под значимыми понимают те слова, которые несут основную смысловую нагрузку документа; стоп-слова – слова не несущие смысловой нагрузки, например, предлоги, или слова, встречающиеся в каждом подобном документе). Словосочетания «Министерство образования РФ», «муниципальные и образовательные учреждения» можно отбросить, т. к. они встречаются в большинстве нормативных об-

разовательных документов. Наш запрос будет выглядеть так: положение о порядке аттестации педагогических и руководящих работников.

1. Запустите обозреватель MS Internet Explorer.

2. В адресной строке наберите адрес поисковой системы http://www.yandex.ru.

3. В строку поиска введите запрос: положение о порядке аттестации педагогических и руководящих работников.

4. Открыть найденный документ.

5. Сформируйте документ по теме «Указать заданную тему», используя электронные документы, представленные глобальной сетью Internet

Методика устранения компьютерной информации.

Цель работы: Приобретение навыков устранения и восстановления информации на различных носителях.

Определение

Уничтожение персональных данных (согл. ФЗ № 152 «О персональных данных») — действия, врезультате которых невозможно восстановить содержание персональных данных в информационнойсистеме персональных данных или в результате которых уничтожаются материальные носителиперсональных данных.

Как показывают результаты исследований[источник не указан 1138 дней], уничтожение персональных данных неотделяются от вопроса уничтожения информации в широком смысле. При этом имеют ряд особенностей,которые обусловлены в первую очередь федеральным законодательством РФ.

Способы уничтожения персональных данных

Способы уничтожения персональных данных принято делить на 2 категории:

1. Физическое уничтожение носителя
2. Уничтожение информации с носителя

Уничтожение материального носителя

• **Бумажный носитель**. Используются 2 вида уничтожения: уничтожение через шредирование (измельчение игидрообработка) и уничтожение через термическую обработку (сжигание). У шредеров есть различныестепени секретности (от 1 до 5). Законодательно степень секретности, при уничтожении, как и самипроцедуры не регламентируется.

• **Электронный носитель**. Уничтожение заключается в таком воздействии на рабочие слои дисков, врезультате, которого разрушается физическая, магнитная или химическая структура рабочего слоя.Примерами могут быть: механическое разрушение дисков (прессование, механическое эрозирование-

поверхности — пескоструй, ультразвуковое и электрохимическое эрозирование), химическое травление вагрессивных средах и обжиг или переплавка дисков. Съём данных с магнитных дисков, подвергшихся такимвоздействиям, становится невозможным.

Уничтожение информации с носителя

Существует большое количество как программной, так и программно-аппаратной реализации процессаобеспечения уничтожения информации, представленной на магнитных носителях.

Ряд алгоритмов уничтожения информации, в том числе и персональных данных, основывается намногократной перезаписи в секторах магнитного диска. С физической точки зрения, они основываются намногократном перемагничивании материала записывающей поверхности диска.

Алгоритмы национальных стандартов предусматривают запись в каждый байт каждого сектора жесткогодиска единиц, случайных чисел, а также чисел, дополнительных к записанным на предыдущем проходе.Предполагается несколько перезаписей для одного материального носителя.

Стандарты уничтожения данных

- ГОСТ Р50739-95;
- DoD 5220.22-M; NAVSO P-5239-26 (RLL);
- NAVSO P-5239-26 (MFM);
- VSITR.

Методы восстановления файлов

Прежде чем начать рассматривать различные методы восстановления файлов отметим одну важную особенность:

Если данные на диске перезаписаны, то их не удастся восстановить ни одной программой и ни одном из известных методов.

Поэтому крайне важно чтобы до восстановления данных на диск не записывалась какая-либо информация.

Есть два метода восстановления файлов которые не были перезаписаны. Во всех утилитах восстановления используется либо один из них, либо оба.

Метод 1: Восстановление файлов посредством анализа информации о файлах и папках

Это самый первый метод используемый в программах восстановления данных, так как при его успешном применении восстанавливаются файлы с оригинальными именами, путями, отметками даты/времени, и сами данные.

Работа утилиты восстановления файлов начинается с попытке чтения и обработки первой копии информации о файлах и папках. В некоторых случаях (например при случайном удалении файла) это единственное что требуется для восстановления файлов.

Если первая копия информации о файлах и папках сильно повреждена, то утилита сканирует диск и ищет вторую копию информации о файлах и папках. При этом также производится детальный поиск дополнительной инфорации о структуре папок и файлов, которая может находиться в области диска, где

хранятся данные. После этого вся найденная информация обрабатывается и воссоздается оригинальная структура папок и файлов.

Если файловая система диска серьезно не повреждена, то вполне вероятно удастся полностью восстановить структуру папок и файлов.

При сильном же повреждении файловой системы данный метод не позволит воссоздать полную структуру папок. В этом случае восстановленные файлы будут находиться в папках с присвоенными им виртуальными именами.

Метод 2: Восстановление файлов при помощи сканирования файлов известных типов (поиска файлов по сигнатурам).

Если при помощи первого метода на удастся добиться желаемого результата, то следует произвести поиск файлов по сигнатурам. Этот метод позволяет восстановить больше данных, однако при этом не удается получить оригинальные имена файлов, отметки даты/времени или полную структуру папок и файлов на диске.

Для оценки шансов восстановления файлов как всегда лучше попробовать наши программы бесплатно в демонстрационном режиме. В данном режиме доступно полное сканирование диска и дополнительный анализ возможностей восстановления данных, в результате чего вы сможете понять, удастся ли вам восстановить файлы или нет. Если вы удовлетворены содержанием найденных файлов, то можете купить лицензию, ввести полученный регистрационный ключ в регистрационное поле программы и сразу же сохранить восстановленные файлы на другой диск независимо от их размеров.

Recuva является самой «раскрученной» программой для восстановления данных. При этом, скачать ее можно бесплатно. Данное программное обеспечение позволяет начинающему пользователю достаточно легко восстановить удаленные файлы (с флешки, карты памяти или жесткого диска). Позволяет искать определенные типы файлов — например, если Вам нужны именно фотографии, которые были на карте памяти фотоаппарата.

Надо отметить, что несмотря на то, что программа очень проста в использовании (для восстановления данных предусмотрен удобный мастер), функциональность ее оставляет желать лучшего. Уверенно восстанавливаются лишь те файлы, которые были удалены и, при этом, флешка или жесткий диск после этого вообще не использовались. Если флешка была отформатирована, то восстановить данные с нее уже не получится. Также программа не справится и в случаях, когда компьютер сообщает «диск не отформатирован».

UndeletePlus

Еще одно достаточно простое программное обеспечение, которое, как это можно увидеть из названия, предназначено для восстановления именно удаленных файлов. Программа работает со все теми же носителями — флешками, жесткими дисками и картами памяти. Работа по восстановлению так же, как и в предыдущей программе, происходит с помощью мастера. На первом этапе которого Вам необходимо будет выбрать, что именно произошло: файлы были удалены, диск был отформатирован, были повреждены разделы диска или что-то еще (причем в последнем случае программа не справится). После этого следует указать какие файлы были утеряны — фотографии, документы и т.д.

Я бы рекомендовал использовать данную программу лишь для восстанов-

ления только что удаленных файлов (которые были удалены не в корзину).

Подробнее о программе UndeletePlus

R-studio — одна из лучших программ для восстановления данных

Да, действительно, одна из лучших, однако стоит отметить, что она является платной. Итак, вот немного о возможностях данной программы:

- Восстановление данных с жестких дисков, карт памяти, флешек, дискет, CD и DVD
- Восстановление RAID массивов (В том числе RAID 6)
- Восстановление поврежденных жестких дисков
- Восстановление переформатированных разделов
- Поддержка разделов Windows (FAT, NTFS), Linux и Mac OS

Таким образом, перед нами профессиональная программа, позволяющая восстановить данные, которые были потеряны по самым разным причинам — форматирование, повреждение, удаление файлов. И сообщения операционной системы о том, что диск не отформатирован ей не помеха, в отличие от ранее описанных программ. Имеется возможность запуска программы с загрузочной флешки или компакт-диска, в случае если операционная система не загружается.

Более подробно и скачать

Программы для восстановления данных на Android телефонах и планшетах

Если вам требуется восстановить удаленные файлы, фотографии, видео или контакты с Android устройства, то имеются программы, предназначенные специально для этих целей. На настоящий момент я могу рекомендовать две из них, о которых вы можете прочитать в статьях:

- Восстановление данных на Android в Wondershare Dr. Fone
- Использование 7-Data Android Recovery

Первое из двух приложений работает практически со всеми популярными марками устройств, позволяя восстанавливать не только файлы, но и другую информацию, такую как заметки или контакты. Вторая программа, 7-Data Android Recovery работает по тому же принципу, что и бесплатная Recuva и, по сути, делает то же самое.

Power Data Recovery — еще один профессионал восстановления

Аналогично предыдущему продукту, Power Data Recovery позволяет восстановить данные с поврежденных жестких дисков, с DVD и CD, карт памяти и многих других носителей. Также программа поможет в случае, если требуется восстановление поврежденного раздела на жестком диске. Программой поддерживаются интерфейсы IDE, SCSI, SATA и USB.

В программе для восстановления данных Power Data Recovery присутствуют возможности для поиска потерянных разделов жестких дисков, поиска нужных типов файлов, а также поддерживается создание образа жесткого диска с тем, чтобы производить все операции не на физическом носителе, тем самым делая процесс восстановления безопаснее.

Также примечателен удобный предварительный просмотр найденных файлов, при этом отображаются (при наличии такой возможности) оригинальные имена файлов.

Подробнее: программа для восстановления файлов Power Data Recovery

Stellar Phoenix — еще одно замечательное ПО

Программа Stellar Phoenix позволяет искать и восстанавливать 185 различных типов файлов с разнообразных носителей, будь то флешки, жесткие диски, карты памяти или оптические диски. (Возможности восстановления RAID не предусмотрено). Также программа позволяет создать образ восстанавливаемого жесткого диска для лучшей эффективности и безопасности восстановления данных. В программе предусмотрена удобная возможность предварительного просмотра найденных файлов, кроме этого все эти файлы сортируются в древовидном виде по типам, что также делает работу удобнее.

Восстановление данных в Stellar Phoenix по умолчанию происходит с помощью мастера, предлагающего три пункта — восстановление жесткого диска, компакт-дисков, потерянных фотографий. В дальнейшем мастер проведет через все восстановления, делая процесс простым и понятным даже для начинающих пользователей компьютера.

Data Rescu PC — восстановление данных на неработающем компьютере

Еще один мощный продукт, позволяющий работать без загрузки операционной системы при поврежденном жестком диске. Программа может быть запущена с LiveCD и позволяет сделать следующее:

- Восстановить любые типы файлов
- Работать с поврежденными дисками, дисками, которые не монтируются в системе
- Восстановить данные после удаления, форматирования
- Восстановление RAID (после установки отдельных компонентов программы)

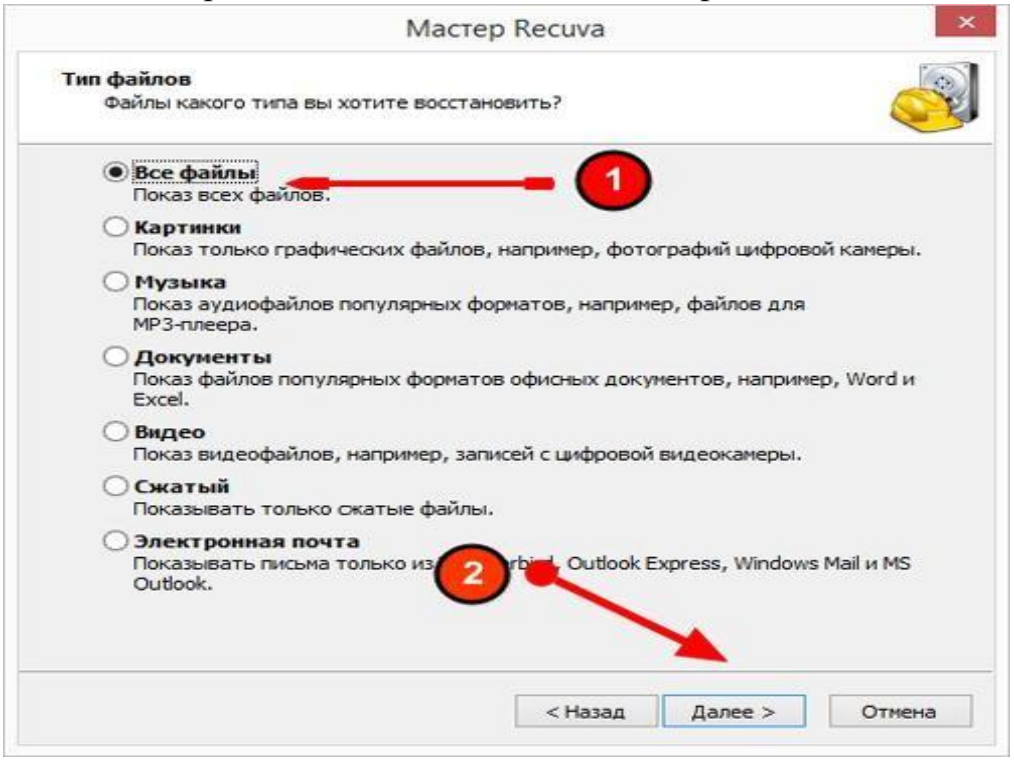
Несмотря на профессиональный набор функций, программа проста в использовании и имеет интуитивно понятный интерфейс. С помощью программы можно не только восстановить данные, но и извлечь из с поврежденного диска, который перестала видеть Windows.

Подробнее о возможностях программы можно прочесть здесь.

Seagate File Recovery for Windows — восстановление данных с жесткого диска.

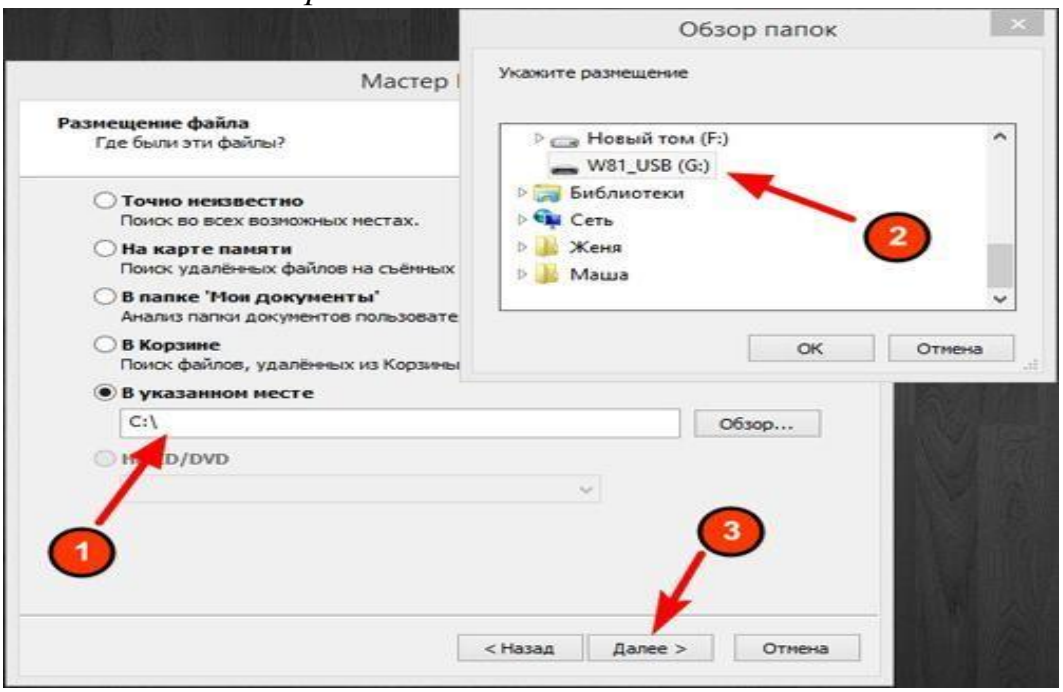
Recuva — бесплатная программа для восстановления удаленных файлов. Благодаря своим уникальным алгоритмам, recuva поможет вам восстановить потерянные данные с любых носителей — жесткого диска компьютера или ноутбука, флешки, смартфона, камеры, mp3-плеера и любых других. Т.к. у многих пользователей возникают вопросы как правильно пользоваться Recuva, мы написали для вас эту пошаговую инструкцию.

Шаг 1: Выбираем тип восстанавливаемых файлов



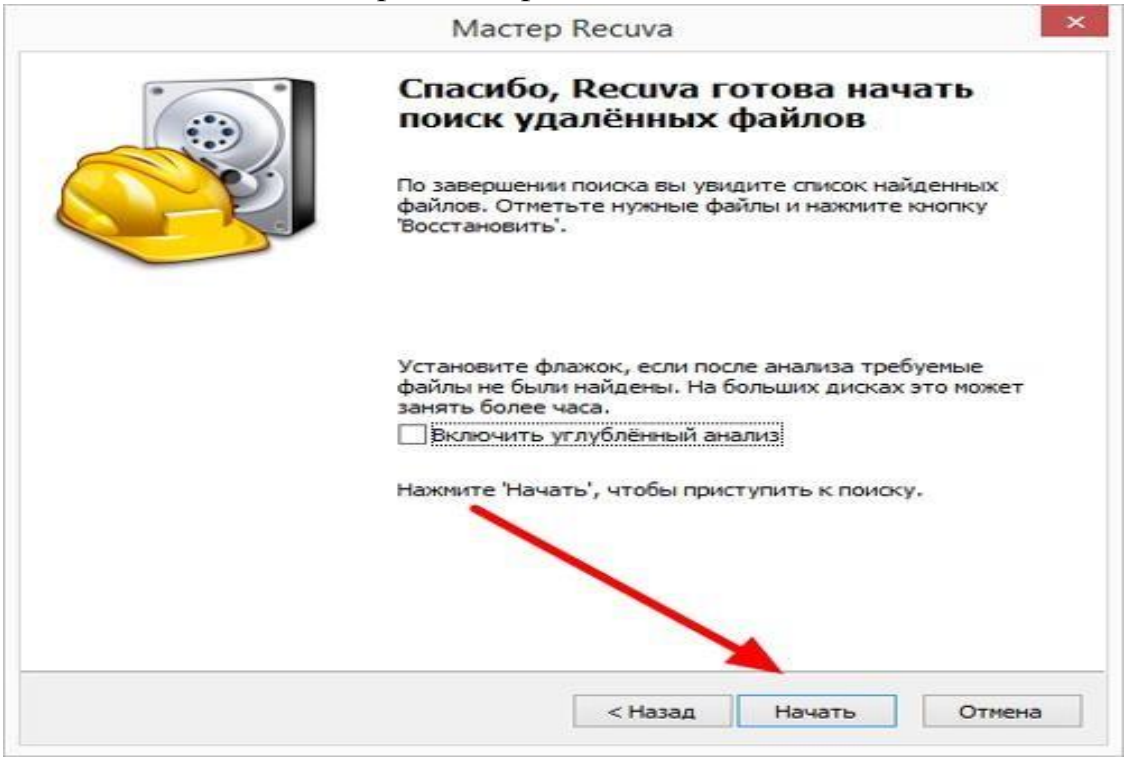
После установки и запуска программы выберете тип восстанавливаемых данных. Если вы, к примеру, хотите восстановить только музыку, удаленную с флешки, выбирайте третий пункт. Если же желаете увидеть все найденные к восстановлению данные, оставляйте флажок на первом пункте *«все файлы»,* и нажимайте *«далее».*

Шаг 2: Указываем расположение восстанавливаемых данных



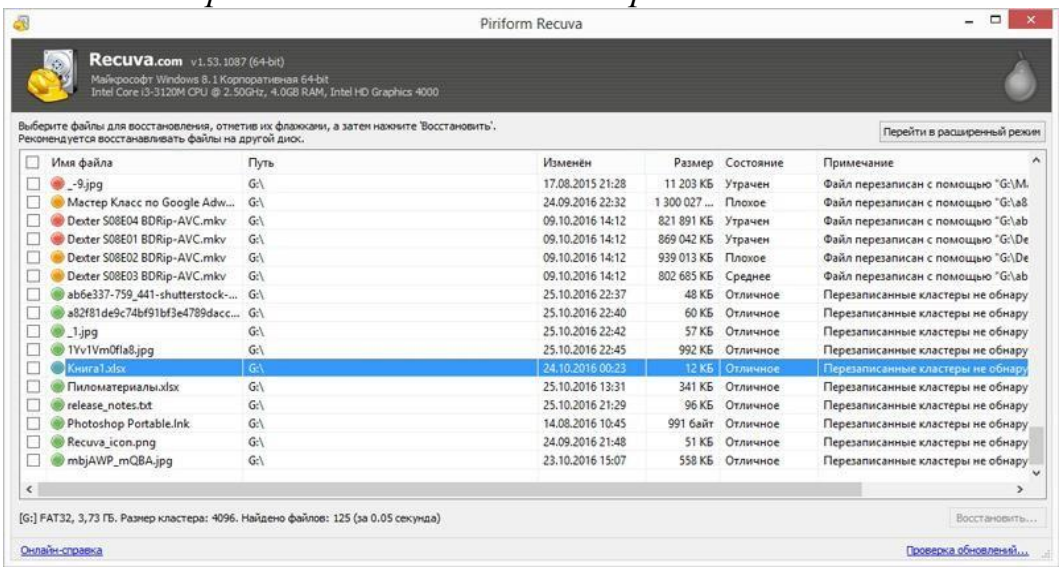
Если вы точно знаете месторасположение удаленных файлов (в нашем примере — это флешка), выбирайте пятый пункт *«В указанном месте»,* отмечайте двойным кликом в появившемся списке нужный диск/папку и нажимайте *«Далее».*

Шаг 3: Начинаем сканирование файлов

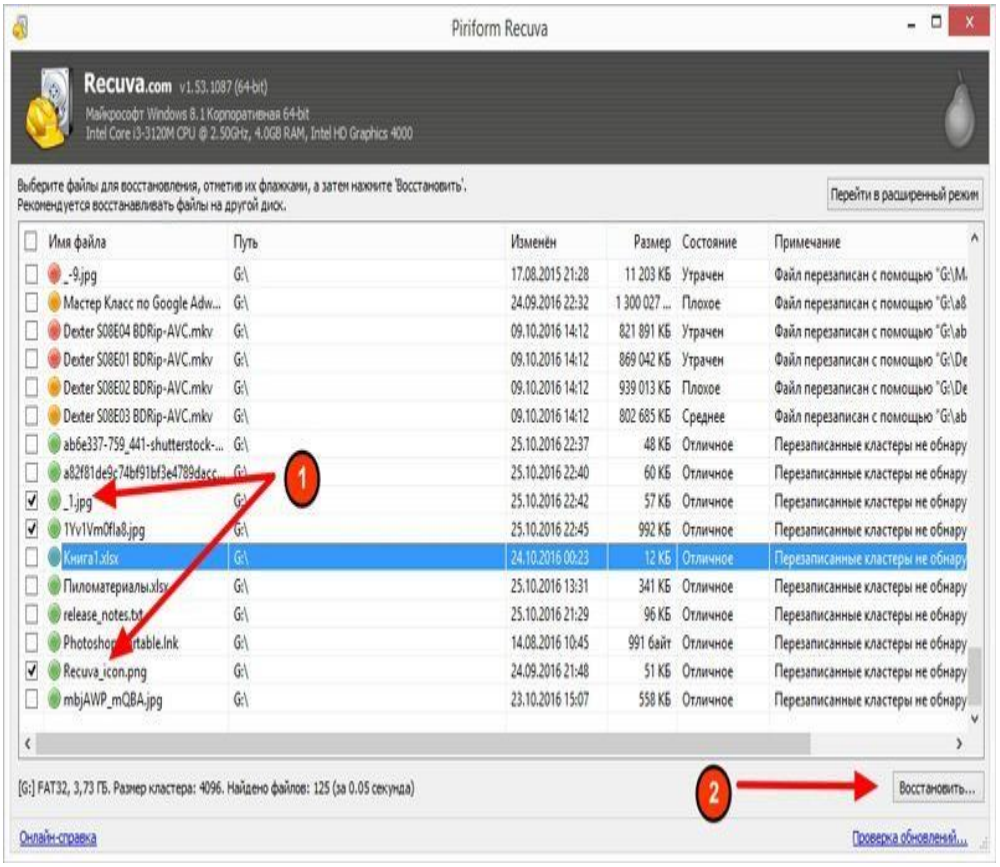


После того, как вы выбрали нужный диск/папку, перед вами появится окно завершения работы мастера Recuva, где он предложит вам включить углубленный анализ. При первичном проходе делать этого не рекомендуется, т.к. включение данной функции сильно увеличит время сканирования, при этом результаты не факт что будут отличаться. Так что оставляйте пока как есть и нажимайте *«Начать».*

Шаг 4: Выбираем восстанавливаемые фалы

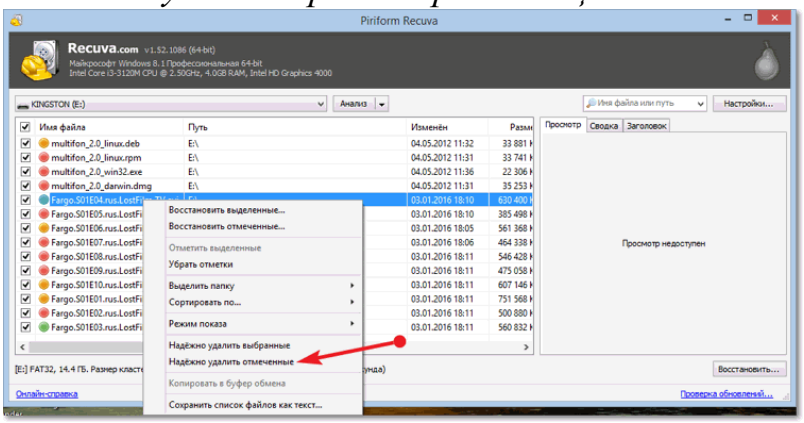


После того, как закончится сканирование, перед вами появится окно в найденными удаленными файлами. Как видите, есть три типа цветовой индикации найденных файлов — красные (восстановить не получится), желтые (возможно частичное восстановление) и зеленые (могут быть восстановлены полностью).



Отмечайте искомые файлы, нажимайте *«Восстановить…»* и выбирайте папку, куда будут помещены восстановленные файлы. Поздравляем — восстановление удаленных файлов завершено, но это ещё не всё. Recuva также умеет надежно удалять данные без возможности восстановления!

Надежно удаляем файлы при помощи Recuva



В том же окне выбора файлов отметьте те, которые хотите удалить навсегда, вызовите правой кнопкой мыши контекстное меню и выбирайте пункт «Надежно удалить отмеченные». Через некоторое время Recuva удалит эти файлы без возможности восстановления.

Контрольные вопросы ЛР1(ПК-3):

1. Что такое сбор первичной базы данных?
2. Что такое индексация базы данных?
3. Что такое рафинирование результирующего списка?
4. Какие поисковые указатели являются В России наиболее крупными и популярными?
5. Приведите примеры приёмов поиска информации с помощью поисковой машины.
6. Приведите примеры устранения и восстановления информации на различных носителях
7. Приведите примеры Методов восстановления файлов
8. Поясните предназначение термина Stellar Phoenix
9. Поясните предназначение термина UndeletePlus

Уязвимости Windows.

Цель работы: Приобретение навыков настройки **Windows** для уменьшения уязвимостей.

Уязвимости операционных систем при прочих равных представляют большую опасность, чем уязвимости отдельных программ, поскольку имеют больше распространение и чаще используются злоумышленниками для атак компьютеров. Уязвимости в операционных системах устраняются с помощью установки обновлений безопасности, которые исправляют ошибки в уязвимых компонентах системы. Установкой обновлений занимается специальная служба Центр обновления Windows. Она в автоматическом режиме проверяет наличие новых обновлений на серверах Windows и, в зависимости от настроек, устанавливает их, или запрашивает разрешение на установку у пользователя.

Центр обновления Windows вполне удовлетворительно справляется с задачей доставки обновлений безопасности на клиентские компьютеры. Но сценарий, при котором для обновлений используется только эта служба, имеет два недостатка. Во-первых, у администратора нет возможности проконтролировать установку критических обновлений — не известно на всех ли компьютерах она завершена, и не отключил ли загрузку обновлений пользователь. Во-вторых, загрузка обновлений выполняется каждым клиентским компьютером самостоятельно, что создает избыточный сетевой трафик. KasperskySecurityCenter позволяет устранить оба этих недостатка.

Обнаружение уязвимостей

Сбором информации об обновлениях операционной системы, которые уже установлены и которые нужно установить, занимается Агент администрирования. KasperskyEndpointSecurity в этом процессе не участвует. Агент получает информацию непосредственно от службы Центр обновления Windows, и передает ее на Сервер администрирования. Для того чтобы агент мог получить информацию об обновлениях безопасности должны выполняться два условия:

Служба Центр обновления Windows должна быть запущена

В настройках Центра обновления Windows должен быть установлен любой режим обновления, кроме Не проверять наличие обновлений

Информация об обновлениях отображается в Консоли администрирования в контейнере Обновления WindowsUpdate, узла Программы и уязвимости. Обновления отображаются единым списком, но у администратора есть возможность использовать фильтры по уровням важности обновлений и состоянию (установлено или нет на клиентских компьютерах, назначена или нет задача установки и т.п.).

В правом верхнем углу экрана отображается диаграмма с информацией о том, когда с клиентских компьютеров поступали последние данные об обновлениях. Компьютеры на диаграмме разделены на три категории, в зависимости

от давности полученных данных. Щелчком по ссылке с названием категории открывается список компьютеров удовлетворяющих условиям категории. Таким образом администратор может получить список проблемных компьютеров, информация с которых не передается на сервер. Эту же диаграмму можно добавить на страницу статистики Состояние защиты.

Описание уязвимости

В свойствах уязвимости на закладке Общие предоставляется следующая информация:

Уровень важности — уровень важности определяется Microsoft при выпуске обновления и характеризует опасность, которую уязвимость представляет для системы. Уровень может принимать значения:

Критический

Важный

Обычный или

Низкий

Ссылки на описание уязвимости в MicrosoftKnowledgeBase и MicrosoftSecurityBulletin

Статистическая информация о статусе уязвимости на клиентских компьютерах — к скольким компьютерам применима, на скольких установлена и т.п.

На закладке Компьютеры отображается список компьютеров, с операционными системами которые обладают данной уязвимостью.

Устранение уязвимостей

Создание задачи установки обновлений

KasperskySecurityCenter позволяет централизовано устанавливать обновления Windows на клиентские компьютеры. Для этого выделена специальная задача — Установка обновлений WindowsUpdate.

Запустить установку обновлений можно из контекстного меню списка уязвимостей в контейнере Обновления WindowsUpdate с помощью команды Установить обновление. Перед выполнением команды из списка можно выбрать сразу несколько обновлений, чтобы выполнить их установку в рамках одной задачи. Команда вызывает мастер создания задачи Установка обновлений WindowsUpdate, который создаст соответствующую задачу в группе Управляемые компьютеры.

Единственным нестандартным параметром задачи Установка обновлений WindowsUpdate является список устанавливаемых обновлений. Его можно редактировать и после того, как задача создана.

В рамках выполнения задачи KasperskySecurityCenter загрузит с серверов обновления Windows необходимые обновления, и установи их на компьютеры группы средствами Агента администрирования.

Главным недостатком указанно выше подхода является то, что задача ус-

тановки обновлений Windows запускается на всех исполняемых компьютерах, даже там где обновления не применимы. Этого можно избежать, если создавать задачу установка обновлений вручную, в контейнере Задачи для наборов компьютеров. Но в таком случае и устанавливаемые обновления, и компьютеры, на которых будет выполняться установка, администратору придется задавать вручную.

Результаты установки обновлений Windows можно посмотреть непосредственно в отчете задачи. Кроме того, успешность установки можно косвенно отследить по изменению статуса уязвимости в контейнере Обновления WindowsUpdate.

Известно, уязвимости в операционных системах очень опасны. Риск выше, если сравнивать с отдельными программными разработками. ОС отличаются широким распространением - это знает каждый! Соответственно, с большей периодичностью они фигурируют в планах злоумышленников, которые атакуют компьютеры. Ошибки в системе безопасности операционных систем можно устранить, используя обновления, которые выпускает производитель. Инсталляция обновлений происходит с помощью «Центра обновлений Windows». Данная служба автоматически сканирует ОС на новые «заплатки». Если они не определяются, с серверов Windows, в зависимости от выбранных опций, начинается инсталляция. Также может запрашиваться разрешение на выполнение этого действия.

«Центр обновления Windows» отлично выполняют задачу, как доставка обновлений безопасности на различные компьютеры пользователей. Однако сценарий, когда для установки обновлений используется только эта служба, имеет определенные недостатки. Для начала, администратор не может контролировать, как происходит инсталляция критических обновлений - непонятно, на каждом ли компьютере это действие было успешно завершено, и не отключена ли загрузка обновлений самим пользователем. Далее, процесс загрузки обновлений клиентские компьютеры выполняют самостоятельно. Таким образом, появляется избыточный сетевой трафик. С помощью KasperskySecurityCenter можно решить эти две проблемы.

Статистические даУязвимости операционных систем при прочих равных представляют большую опасность, чем уязвимости отдельных программ, поскольку имеют больше распространение и чаще используются злоумышленниками для атак компьютеров. Уязвимости в операционных системах устраняются с помощью установки обновлений безопасности, которые исправляют ошибки в уязвимых компонентах системы. Установкой обновлений занимается специальная служба Центр обновления Windows. Она в автоматическом режиме проверяет наличие новых обновлений на серверах Windows и, в зависимости от настроек, устанавливает их, или запрашивает разрешение на установку у пользователя.

Центр обновления Windows вполне удовлетворительно справляется с задачей доставки обновлений безопасности на клиентские компьютеры. Но сценарий, при котором для обновлений используется только эта служба, имеет два недостатка. Во-первых, у администратора нет возможности проконтролировать установку критических обновлений — не известно на всех ли компью-

терах она завершена, и не отключил ли загрузку обновлений пользователь. Во-вторых, загрузка обновлений выполняется каждым клиентским компьютером самостоятельно, что создает избыточный сетевой трафик. KasperskySecurityCenter позволяет устранить оба этих недостатка.

Обнаружение уязвимостей

Сбором информации об обновлениях операционной системы, которые уже установлены и которые нужно установить, занимается Агент администрирования. KasperskyEndpointSecurity в этом процессе не участвует. Агент получает информацию непосредственно от службы Центр обновления Windows, и передает ее на Сервер администрирования. Для того чтобы агент мог получить информацию об обновлениях безопасности должны выполняться два условия:

Служба Центр обновления Windows должна быть запущена

В настройках Центра обновления Windows должен быть установлен любой режим обновления, кроме Не проверять наличие обновлений

Информация об обновлениях отображается в Консоли администрирования в контейнере Обновления WindowsUpdate, узла Программы и уязвимости. Обновления отображаются единым списком, но у администратора есть возможность использовать фильтры по уровням важности обновлений и состоянию (установлено или нет на клиентских компьютерах, назначена или нет задача установки и т.п.).

В правом верхнем углу экрана отображается диаграмма с информацией о том, когда с клиентских компьютеров поступали последние данные об обновлениях. Компьютеры на диаграмме разделены на три категории, в зависимости от давности полученных данных. Щелчком по ссылке с названием категории открывается список компьютеров удовлетворяющих условиям категории. Таким образом администратор может получить список проблемных компьютеров, информация с которых не передается на сервер. Эту же диаграмму можно добавить на страницу статистики Состояние защиты.

Описание уязвимости

В свойствах уязвимости на закладке Общие предоставляется следующая информация:

Уровень важности — уровень важности определяется Microsoft при выпуске обновления и характеризует опасность, которую уязвимость представляет для системы. Уровень может принимать значения:

Критический

Важный

Обычный или

Низкий

Ссылки на описание уязвимости в MicrosoftKnowledgeBase и MicrosoftSecurityBulletin

Статистическая информация о статусе уязвимости на клиентских компь-

ютерах — к скольким компьютерам применима, на скольких установлена и т.п.

На закладке Компьютеры отображается список компьютеров, с операционными системами которые обладают данной уязвимостью.

Устранение уязвимостей

Создание задачи установки обновлений

KasperskySecurityCenter позволяет централизовано устанавливать обновления Windows на клиентские компьютеры. Для этого выделена специальная задача — Установка обновлений WindowsUpdate.

Запустить установку обновлений можно из контекстного меню списка уязвимостей в контейнере Обновления WindowsUpdate с помощью команды Установить обновление. Перед выполнением команды из списка можно выбрать сразу несколько обновлений, чтобы выполнить их установку в рамках одной задачи. Команда вызывает мастер создания задачи Установка обновлений WindowsUpdate, который создаст соответствующую задачу в группе Управляемые компьютеры.

Единственным нестандартным параметром задачи Установка обновлений WindowsUpdate является список устанавливаемых обновлений. Его можно редактировать и после того, как задача создана.

В рамках выполнения задачи KasperskySecurityCenter загрузит с серверов обновления Windows необходимые обновления, и установи их на компьютеры группы средствами Агента администрирования.

Главным недостатком указанно выше подхода является то, что задача установки обновлений Windows запускается на всех исполняемых компьютерах, даже там где обновления не применимы. Этого можно избежать, если создавать задачу установка обновлений вручную, в контейнере Задачи для наборов компьютеров. Но в таком случае и устанавливаемые обновления, и компьютеры, на которых будет выполняться установка, администратору придется задавать вручную.

Результаты установки обновлений Windows можно посмотреть непосредственно в отчете задачи. Кроме того, успешность установки можно косвенно отследить по изменению статуса уязвимости в контейнере Обновления WindowsUpdate.

Известно, уязвимости в операционных системах очень опасны. Риск выше, если сравнивать с отдельными программными разработками. ОС отличаются широким распространением - это знает каждый! Соответственно, с большей периодичностью они фигурируют в планах злоумышленников, которые атакуют компьютеры. Ошибки в системе безопасности операционных систем можно устранить, используя обновления, которые выпускает производитель. Инсталляция обновлений происходит с помощью «Центра обновлений Windows». Данная служба автоматически сканирует ОС на новые «заплатки». Если они не определяются, с серверов Windows, в зависимости от выбранных опций, начинается инсталляция. Также может запрашиваться разрешение на

выполнение этого действия.

«Центр обновления Windows» отлично выполняют задачу, как доставка обновлений безопасности на различные компьютеры пользователей. Однако сценарий, когда для установки обновлений используется только эта служба, имеет определенные недостатки. Для начала, администратор не может контролировать, как происходит инсталляция критических обновлений - непонятно, на каждом ли компьютере это действие было успешно завершено, и не отключена ли загрузка обновлений самим пользователем. Далее, процесс загрузки обновлений клиентские компьютеры выполняют самостоятельно. Таким образом, появляется избыточный сетевой трафик. С помощью KasperskySecurityCenter можно решить эти две проблемы.

Статистические данные показывают, что уязвимости ОС Windows для совершения взлома используются в меньше 10 процентах случаев. Конечно, показатель обнадеживает.

Какой уязвимостью пользуются злоумышленники для заражения компьютеров?

Исследование проводилось сотрудником «Лаборатории Касперского», ДиазомВисентом. Его целью был анализ пяти самых распространенных эксплойтов 2010 года (пользовались большим спросом у киберпреступников). Их хакеры применяли для атак на пользовательские компьютеры - Eleonore, SEOSploitPack, Phoenix, Neosploit, YESExploitKit.

Проанализировав ошибки, удалось выявить направление основной цели злоумышленников. Речь идет о популярных приложениях, которые используются практически на всех компьютерах. На это и делают ставки хакеры. Программа AdobeReader, по результатам исследования, была атакована в 28 процентах случаев. С показателем 27 процентов идет браузер InternetExplorer. Третье строчку с 19 процентами занимает Java. Четвертое место с 9 процентами за AdobeFlash. На пятом месте с 7 процентами оказался браузер MozillaFireFox. Остальные 10 процентов случаев остаются другим уязвимостям. То есть, имеются в виду дыры в операционной системе Microsoft.

Как происходит закрытие уязвимостей в Windows?

Операционная система проходит комплексное сканирование и ее самые значимые компоненты проверяются на наличие ошибок и замедление работы. В этом случае учитываются ошибки в реестре, временные и бесполезные файлы, проблемы диска, а также фрагментированные файлы.

Проверять Windows на ошибки нужно:

- при нестабильной или медленной работе, когда появились сбои ОС;
- если обнаружились дыры с помощью сторонних программных разработок или антивирусов;
- для профилактики.

Получив итоговые результаты тестирования, можно о многом судить:

- удалить ошибки из системного реестра;
- очистить диск от временных и ненужных объектов;
- удалить логические ошибки на винчестере;
- использовать дефрагментацию жесткого диска.

Как определить уязвимости в Windows?

Собирать информацию о различных обновлениях операционной системы, которые были инсталлированы и которые следует использовать, можно с помощью «Агента администрирования» от «Лаборатории Касперского». Инструмент KasperskyEndpointSecurity в данном случае не будет полезным. Системе «Агента» обменивается информацией напрямую с «Центром обновления Windows». После этого отправляет данные на сервер администрирования. Чтобы у «Агента» была возможность получить сведения об обновлениях безопасности, необходимо выполнить несколько условий. Об этом подробно можно прочитать в справке KasperskySecurityCenter.

нные показывают, что уязвимости ОС Windows для совершения взлома используются в меньше 10 процентах случаев. Конечно, показатель обнадеживает.

Какой уязвимостью пользуются злоумышленники для заражения компьютеров?

Исследование проводилось сотрудником «Лаборатории Касперского», ДиазомВисентом. Его целью был анализ пяти самых распространенных эксплойтов 2010 года (пользовались большим спросом у киберпреступников). Их хакеры применяли для атак на пользовательские компьютеры - Eleonore, SEOSploitPack, Phoenix, Neosploit, YESExploitKit.

Проанализировав ошибки, удалось выявить направление основной цели злоумышленников. Речь идет о популярных приложениях, которые используются практически на всех компьютерах. На это и делают ставки хакеры. Программа AdobeReader, по результатам исследования, была атакована в 28 процентах случаев. С показателем 27 процентов идет браузер InternetExplorer. Третье строчку с 19 процентами занимает Java. Четвертое место с 9 процентами за AdobeFlash. На пятом месте с 7 процентами оказался браузер MozillaFireFox. Остальные 10 процентов случаев остаются другим уязвимостям. То есть, имеются в виду дыры в операционной системе Microsoft.

Как происходит закрытие уязвимостей в Windows?

Операционная система проходит комплексное сканирование и ее самые значимые компоненты проверяются на наличие ошибок и замедление работы. В этом случае учитываются ошибки в реестре, временные и бесполезные файлы, проблемы диска, а также фрагментированные файлы.

Проверять Windows на ошибки нужно:

- при нестабильной или медленной работе, когда появились сбои ОС;
- если обнаружились дыры с помощью сторонних программных разработок или антивирусов;
- для профилактики.

Получив итоговые результаты тестирования, можно о многом судить:

- удалить ошибки из системного реестра;
- очистить диск от временных и ненужных объектов;

- удалить логические ошибки на винчестере;
- использовать дефрагментацию жесткого диска.

Как определить уязвимости в Windows?

Собирать информацию о различных обновлениях операционной системы, которые были инсталлированы и которые следует использовать, можно с помощью «Агента администрирования» от «Лаборатории Касперского». Инструмент KasperskyEndpointSecurity в данном случае не будет полезным. Системе «Агента» обменивается информацией напрямую с «Центром обновления Windows». После этого отправляет данные на сервер администрирования. Чтобы у «Агента» была возможность получить сведения об обновлениях безопасности, необходимо выполнить несколько условий. Об этом подробно можно прочитать в справке KasperskySecurityCenter.

Защита от копирования переносных носителей.

Цель работы: Приобретение навыков защиты от копирования переносных носителей.

Защита от копирования — система мер, направленных на противодействие несанкционированному копированию информации, как правило, представленной в электронном виде (данных или кода программного обеспечения).

При защите могут использоваться организационные, юридические и технические средства.

Преимуществом технических мер защиты является возможность предотвращения несанкционированного копирования.

В ряде случаев копирование разрешено законодательством (например, резервное). Однако определить его законность только техническими средствами невозможно (пример — WindowsGenuineAdvantage: было зафиксировано множество ложных срабатываний)[источник не указан 2270 дней]. Поэтому технические средства защиты авторских прав зачастую запрещают любое копирование, создавая неудобства пользователям, за что подвергаются критике со стороны правозащитников.

Защита аудио треков

Ряд производителей портативных плееров защищают от копирования музыку путём использования известных только им протоколов обмена между электронным музыкальным магазином и проигрывающим устройством. В результате купленная музыка может прослушиваться только с их указанного устройства и, наоборот, закачать музыку на плеер можно только с использованием их программного обеспечения и изихMusicStore. Это создает некоторые неудобства конечным пользователям.

Защита аудио компакт-дисков

Компакт-диски делают не полностью соответствующими спецификации RedBook, из-за чего (теоретически) диск должен читаться на плеерах и не чи-

таться на компьютерных приводах CD-ROM. На практике такие диски читаются на некоторых приводах и, наоборот, не читаются на некоторых плеерах. Фирма Philips, владеющая знаком «CompactDiscDigitalAudio», отказалась ставить эту марку на защищённых дисках. Из таких защит известныCactusDataShield и CopyControl.

В 2005 фирма Sony BMG использовала (англ.)русск. свой метод защиты компакт-дисков, известный как ExtendedCopyProtection (XCP). Диски с XCP имеют дополнительную дорожку с данными, и при первой установке в системах семейства MicrosoftWindows устанавливают скрытую программу, запрещающую копирование дисков. Поскольку эта программа ставится независимо от желания пользователя, маскируется и препятствует своему удалению, многие независимые исследователи охарактеризовали её как руткит, то есть вредоносную программу. В результате скандала Sony предложила программу-деинсталлятор и бесплатную замену дисков с XCP, но не все проблемы были решены. Системы с ОС, отличной от Windows, не подвержены этой опасности.

У аудиодисков, видео, книг и подобных носителей есть «аналоговая брешь»: если музыку можно воспроизвести, то её можно и записать. Если текст можно прочитать, то его можно и сфотографировать. В таком случае некоторые компании используют ТСЗАП, снижающие качество воспроизведения — то есть качество самого продукта.

Основные функции средств защиты от копирования

При защите программ от несанкционированного копирования применяются методы, которые позволяют привносить в защищаемую программу функции привязки процесса выполнения кода программы только на тех ЭВМ, на которые они были инсталлированы. Инсталлированная программа для защиты от копирования при каждом запуске должна выполнять следующие действия:

- анализ аппаратнопрограммной среды компьютера, на котором она запущена, формирование на основе этого анализа текущих характеристик своей среды выполнения;
- проверка подлинности среды выполнения путем сравнения ее текущих характеристик с эталонными, хранящимися на винчестере;
- блокирование дальнейшей работы программы при несовпадении текущих характеристик с эталонными.

Этап проверки подлинности среды является одним из самых уязвимых с точки зрения защиты. Можно детально не разбираться с логикой защиты, а немного "подправить" результат сравнения, и защита будет снята.

При выполнении процесса проверки подлинности среды возможны три варианта: с использованием множества операторов сравнения того, что есть, с тем, что должно быть, с использованием механизма генерации исполняемых команд в зависимости от результатов работы защитного механизма и с использованием арифметических операций. При использовании механизма генерации исполняемых команд в первом байте хранится исходная ключевая контрольная сумма BIOS, во второй байт записывается подсчитанная контрольная сумма в процессе выполнения задачи. Затем осуществляется вычитание из значения первого байта значение второго байта, а полученный результат до-

бавляется к каждой ячейки оперативной памяти в области операционной системы. Понятно, что если суммы не совпадут, то операционная система функционировать не будет. При использовании арифметических операций осуществляется преобразование над данными арифметического характера в зависимости от результатов работы защитного механизма.

Для снятия защиты от копирования применяют два основных метода: статический и динамический

Статические методы предусматривают анализ текстов защищенных программ в естественном или преобразованном виде. Динамические методы предусматривают слежение за выполнением программы с помощью специальных средств снятия защиты от копирования.

Основные методы защиты от копирования
Криптографические методы

Для защиты инсталлируемой программы от копирования при помощи криптографических методов инсталлятор программы должен выполнить следующие функции:

- анализ аппаратнопрограммной среды компьютера, на котором должна будет выполняться инсталлируемая программа, и формирование на основе этого анализа эталонных характеристик среды выполнения программы;
- запись криптографически преобразованных эталонных характеристик аппаратнопрограммной среды компьютер на винчестер.

Преобразованные эталонные характеристики аппаратнопрограммной среды могут быть занесены в следующие области жесткого диска:

- в любые места области данных (в созданный для этого отдельный файл, в отдельные кластеры, которые должны помечаться затем в FAT как зарезервированные под операционную систему или дефектные);
- в зарезервированные сектора системной области винчестера;
- непосредственно в файлы размещения защищаемой программной системы, например, в файл настройки ее параметров функционирования.

Можно выделить два основных метода защиты от копирования с использованием криптографических приемов:

- с использованием односторонней функции;
- с использованием шифрования.

Проблема несанкционированногокопированияявляется сплошь и рядом. Она обусловлена "самой сутью человеческой психологии и будет существовать до тех пор, пока программный продукт является товаром" Несанкционированное копирование осуществляется тогда, когда у пользователя существует потребность в эксплуатации какого-то программного продукта, а затраты на копирование существенно меньше затрат на приобретение легальной копии. Вряд ли в нашей стране найдётся хотя бы сотня разработчиков или людей, использующих ПК в своей деятельности, которые с абсолютной уверенностью могут признаться в том, что никогда в жизни не использовали "пиратские" программные продукты...

Сегодня сложилась парадоксальная ситуация, когда в большинстве отечественных ПК в основном используется «ворованное» программное обеспечение. В Росии 95% используемого софта «пиратское», оставшиеся 5% -

FreeWare.

Поэтому вопросы защиты ПО от несанкционированного копирования я вляется важнейшим направлением в обеспечении информационной безопасности.

Все методы защиты можно разделить на программные и аппаратные . К программным относятся методы, реализующиеся чисто софтверным путем, в них не затрагиваются физические характеристики материальных носителей информации, специальное оборудование, например, электронные ключи или смарт-карты. К аппаратным относятся методы, использующие специальное оборудование или физические особенности материальных носителей информации. Основными методами являются:

1) Криптографические методы:

шаг 1: выделение эталонных характеристик среды выполнения ПО;

шаг 2: запись криптографических преобразований эталонных характеристик на диск (с помощью различных алгоритмов шифрования и хеширования - RC5, RC4, MD5);

2) Методы привязки к идентификатору.

Идентификатор - это информация, формируемая инсталятором. Инсталятор формирует уникальный идентификатор, наличие которого потом проверяется инсталированной программой при каждом запуске. Приотсутствие или несовпадении идентификатора прога блокирует свое дальнейшее выполнение. Основное требованире к идентификатору заключается в том, что он не должен копироваться стандартным способом. Для этого целесообразно записывать идентификатор в следующей области жеского диска: в отдельные кластеры области данных, в зарезервированные сектора систем области винтчестера.

3) Методы, основанные на работе с переходами и стеком. Реализация этого метода предполагает включение в прогу переходов по динамически изменяемым адресам и прерываниям, а так же использование самогенерируемых команд (полученных с помощью сложения и вычитания). Кроме того вместо перехода jmp может использоваться возврат из подпрограммы ret. Предварительно в стек записывается адрес перехода, который в процессе работы ПО модифицируется непосредственно в стеке.

4) Манипуляция с кодом программы:

a) включение в ПО пустых модулей, на которые имитируется передача управления, но реально никогда не осуществляется. Эти модули содержат большое количество команд не имеющих отношения к логике работы программы;

b) Изменение защищаемой программы таким образом, чтобы стандартный дизассемблер не смог ее правильно дизассемблировать (программа Nota или CopyLock полностью модифицируют заголовок exe-файла).

Приведенные методы направлены на защиту ПОот статического способа снятия защиты от копирования (с использованием дизассемблера).

Методы противодействия динамическим способам снятия защиты ПО от копирования (с использованием отладчика) включают:

1) Периодический подсчет контрольной суммы, занимаемой образом задачи области оперативной памяти, в процессе выполнения;

2) Проверка количества свободной памяти и сравнение с тем объемом, к которому задача привыкла или приучена;

3) Проверка содержимого векторов прерывания (13h и 21h) на наличие тех значений, к которым задача привыкла;

4) Переустановка векторов прерывания. При этом слежение за известными векторами не дает желаемого результата;

При защите ПОот несанкционированного копирования необходимо учитывать следующее ограничение: не потеряет ли программа за время снятия ее защиты своей актуальности.

StarForce — торговая марка, под которой выходят программные продукты, разработанные российской компанией ProtectionTechnology. Направления деятельности компании: информационная безопасность, защита от несанкционированного копирования, анализа и модификации (декомпиляции).

Варианты защиты зависят от ответов на вопросы: что нужно защитить и от каких угроз. StarForce эффективен, если ответом на первый вопрос являются: программное обеспечение (в основном разработанное под Windows), документы, аудио-, видеофайлы и электронная почта. Среди угроз: анализ и модификация, копирование и нелегальное распространение, читы и боты. Для защиты от копирования также имеют значение способы привязки: к компьютеру, серверу, диску.

Электронный ключ (также аппаратный ключ, иногда донгл от англ. dongle) — аппаратное средство, предназначенное для защиты программного обеспечения (ПО) и данных от копирования, нелегального использования и несанкционированного распространения.

Современные электронные ключи

Основой данной технологии является специализированная микросхема, либо защищённый от считывания микроконтроллер, имеющие уникальные для каждого ключа алгоритмы работы. Донглы также имеют защищённую энергонезависимую память небольшого объёма, более сложные устройства могут иметь встроенныйкриптопроцессор (для аппаратной реализации шифрующих алгоритмов), часы реального времени. Аппаратные ключи могут иметь различные форм-факторы, но чаще всего они подключаются к компьютеру через USB. Также встречаются с LPT- или PCMCIA-интерфейсами.

Принцип действия электронных ключей. Ключ присоединяется к определённому интерфейсу компьютера. Далее защищённая программа через специальный драйвер отправляет ему информацию, которая обрабатывается в соответствии с заданным алгоритмом и возвращается обратно. Если ответ ключа правильный, то программа продолжает свою работу. В противном случае она может выполнять определенные разработчиками действия, например, переключаться в демонстрационный режим, блокируя доступ к определённым функциям.

Существуют специальные ключи, способные осуществлять лицензирования (ограничения числа работающих в сети копий программы) защищенного приложения по сети. В этом случае достаточно одного ключа на всю локальную сеть. Ключ устанавливается на любой рабочей станции или сервере сети. Защищенные приложения обращаются к ключу по локальной сети. Преиму-

щество в том, что для работы с приложением в пределах локальной сети им не нужно носить с собой электронный ключ.

Контрольные вопросы ЛР2 (ПК-3):

1. Какие известны Уязвимости Windows?
2. Каким образом происходит Обнаружение уязвимостей?
3. Приведите примеры Описания уязвимостей.
4. Каким образом происходит Устранение уязвимостей?
5. Как происходит закрытие уязвимостей в Windows?
6. Как определить уязвимости в Windows?
7. Какой уязвимостью пользуются злоумышленники для заражения компьютеров?
8. Как происходит Защита от копирования переносных носителей?
9. Приведите примеры: Основные функции средств защиты от копирования?
10. Поясните: Основные методы защиты от копирования и Криптографические методы
11. Поясните: Методы привязки к идентификатору
12. Поясните термин: Современные электронные ключи

Существует довольно много различных моделей распространения программного обеспечения. Рассмотрим характерные особенности некоторых их них.

Бесплатные программы (Freeware)

Эта модель распространения программного обеспечения подразумевает отсутствие оплаты за использование программ. Очень часто по такому принципу распространяются небольшие утилиты, которые, по мнению авторов, могут оказаться полезными широкому кругу пользователей, но не будут иметь спроса, если назначить плату за их использование. Разумеется, существуют программисты, создающие бесплатные приложения из любви к искусству или нелюбви к излишней коммерциализации современных информационных технологий. Часто несколько добровольцев организуют команду, разрабатывающую и поддерживающую достаточно сложную программную систему. Многие бесплатные программы распространяются в исходных текстах. Но надо отдавать себе отчет в том, что программы в исходных текстах и бесплатные программы — это совсем не одно и то же. Коммерческие продукты тоже могут поставляться в исходных текстах.

Довольно часто встречается ситуация, когда программа или библиотека бесплатна для личного использования, но требует лицензии (иногда весьма не дешевой) для коммерческого применения. Не редки случаи, когда бесплатное программное обеспечение разрабатывается крупными коммерческими компаниями для упрочнения положения на рынке. Так, например, документы в формате PDF вряд ли имели бы сегодня такую популярность, если бы никогда не существовала бесплатная программа для их просмотра — Adobe Acrobat Reader, дополняющая линейку платных продуктов для создания PDF-документов (Acrobat Exchange, Distiller, Business Tools, Approval и т. д.). Аналогично, для документов, созданных в коммерческой программе Microsoft Word, существовала бесплатная программа просмотра Microsoft Word Viewer, также разработанная корпорацией Microsoft. Иногда автор бесплатного проекта продает кому-нибудь все права на свое детище, а новый владелец начинает распространять ту же самую программу за деньги, иногда нанимая бывшего автора для продолжения разработки. Не удивительно, что такая судьба, в подавляющем большинстве случаев, постигает именно удачные и полезные бесплатные программы.

Почти бесплатные программы

Иногда авторы программ по каким-то соображениям не хотят распространять их как коммерческие продукты, но и не возражают против получения каконибудь отдачи, не считая морального удовлетворения. Чаще всего выбирается один из следующих методов распространения".

• Cardware — каждый пользователь программы, желающий зарегистрироваться, должен послать автору программы почтовую открытку с видом местности, где он проживает;

• Mailware — более современный вариант Cardware, подразумевающий отсылку автору электронного письма. Как правило, в ответ автор присылает регистрационный код, дающий возможность работать с программой;

• Donationware — это когда автор не требует никакой оплаты, но предлагает всем, кому понравилась программа, пожертвовать произвольную сумму, чтобы поддержать разработку;

• Gifrware — почти то же самое, что и Donationware, но автор готов принимать не только денежные пожертвования, но и другие подарки;

• Beerware — благодарность за программу принимается в виде пива;

• Vegeware — автор собирает с пользователей плату за программу в форме рецептов вегетарианских блюд;

• Memorialware — человек по имени Гари Крэмблитт (Gary Cramblitt) посвятил свою программу памяти отца и распространяет ее как Memorialware. Для пользователей программа бесплатна, но всем желающим предлагается помочь мемориальному фонду Крэмблитта-отца.

Программы, показывающие рекламу (Adware)

В последние годы XX века, когда бурный рост интернет-технологий еще не успел перейти в глубокий кризис, была популярна модель распространения программного обеспечения, демонстрирующего рекламу. "Ad" яачяется сокращением от английского слова Advertisement — реклама. Основная идея заключалась в том, что разработчик получал плату за использование программы не от конечного потребителя, которому программа доставалась бесплатно, а от рекламодателей. А пользователь был вынужден смотреть на доставляемые программой через Интернет рекламные картинки. Разумеется, этот подход годился преимущественно для программ, работа которых прямо связана с доступом в Интернет. Однако со временем эффективность рекламы такого рода значительно снизилась, и найти желающих платить за нее настоящими деньгами стало довольно трудно. Но продолжают существовать спонсируемые программные продукты (как правило, информационной направленности), разработка которых ведется на деньги рекламодателей в обмен на размещение их информации в программе.

Коммерческие программы (Commercial)

Коммерческое программное обеспечение, очевидно, создается с целью извлечения прибыли и распространяется за материальное вознаграждение. Наверное, коммерческие программы больше всего похожи на обычные товары, которые люди привыкли покупать в магазинах. Прежде всего, для программного обеспечения, распространяемого как чисто коммерческое, применяется принцип "деньги — вперед", т. е. пользователь получает программу только после полного внесения оплаты. Очень многие программы, распространяемые таким способом, являются "коробочными" — при покупке пользователь получает коробку, в которой уложены носители информации (например DVD или компакт-диски), документация, регистрационная карточка и еще все что угодно, на усмотрение продавца. Разумеется, автор (или правообладатель) кровно заинтересован в том, чтобы собрать плату с каждого пользователя программы. Для достижения этого необходимо применять технологические методы, огра-

ничивающие распространение нелегальных (нелицензированных) копий программы. К популярным технологическим методам относятся различные аппаратные защиты, системы регистрации и активации, проверка лицензии через Интернет при каждом запуске программы и т. д. Однако чисто коммерческое программное обеспечение обладает одной очень важной особенностью. Конечный потребитель сможет получить представление о том, что он покупает, только после совершения покупки, и, следовательно, достаточно высока вероятность того, что он будет разочарован и захочет избавиться от программы и вернуть назад заплаченные деньги. Для того чтобы не отпугнуть покупателей, продавцы часто вынуждены обещать возврат денег в течение, например, двух недель с момента покупки, если программа не понравится.

Почти работоспособные программы

Разработчики коммерческих программ в рекламных целях выпускают ограниченные ознакомительные версии своих продуктов. Такие версии обычно не позволяют плодотворно работать, но создают правдивое впечатление о функциональности программы. Можно выделить несколько основных типов ограниченных программных продуктов:

- Demoware — это когда в программе присутствуют функциональные ограничения. Например, можно обрабатывать файлы не более определенного размера, нельзя выполнять сохранение и т. д. Такие программы иногда называют Crippleware — "урезанное" программное обеспечение;
- Trialware — подразумевается наличие ограничений по времени использования. Ограничения могут выражаться в виде длительности периода време- ни, на протяжении которого можно пользоваться программой (например 30 дней с момента инсталляции) или в виде фиксированной даты истечения тес- тового периода. Может ограничиваться число запусков программы или число процессов обработки;
- Nagware — пользователь регулярно извещается о том, что данная версия программы не является полноценной коммерческой версией. Такое извещение может выглядеть как диалоговое окно, появляющееся при запуске программы и с некоторой периодичностью во время работы, дополнительные надписи, выводимые на принтер или экран, и т. д.

Разумеется, возможны различные комбинации описанных ограничений. И далеко не каждый коммерческий продукт имеет ознакомительную версию — такой подход скорее исключение.

Условно бесплатные продукты (Shareware)

Наличие возможности оценить программу до покупки ("try before you buy") является отличительной чертой условно бесплатных продуктов. Share переводится с английского языка как разделять, совместно использовать. Подразумевается, что незарегистрированную версию условно бесплатной программы можно свободно распространять в неизмененной форме. Условно бесплатное программное обеспечение так же, как и коммерческое, разрабатывается с целью извлечения прибыли. Но потенциальному пользователю до того, как он заплатит деньги, обязательно предоставляется возможность попробовать программный продукт в действии в течение некоторого периода времени. По истечении тестового периода потенциальный покупатель должен принять

решение о приобретении программы. Если решено отказаться от покупки, то надо прекратить использовать программу и удалить ее с компьютера. В противном случае, необходимо оплатить лицензию на программу, после чего продавец предоставит возможность получения полнофункциональной версии программы. Обычно условно бесплатные программы доставляются через Интернет и имеет небольшой размер (единицы мегабайтов). Также очень часто для превращения ограниченной версии в полнофункциональную не требуются никакие дополнительные файлы — достаточно ввести правильный регистрационный код, полученный от продавца.

На период бесплатного использования накладываются ограничения, схожие с ограничениями на оценочные версии коммерческих программных продуктов. Точные ограничения оценочного периода, как правило, оговариваются в лицензионном соглашении на использование каждого конкретного продукта. Условно бесплатные продукты очень популярны. Многие крупные разработчики берут на вооружение концепцию "try before you buy", чтобы заинтересовать покупателей. По сути, ограниченные ознакомительные версии коммерческих продуктов являются всего лишь одной из модификаций идеи Shareware. Даже корпорация Microsoft бесплатно распространяет 120-дневные версии Windows 2003 Server и Visual Studio .NET. Правда, небольшое отличие заключается в том, что для превращения 120-дневной версии в полноЦенную придется получить диск с новой версией и выполнить процедуру обновления, а для "классических" условно бесплатных программ переход к полной версии происходит сразу же после ввода правильного регистрационного кода.

Контрольные вопросы ЛР3 (ПК-3):

1. Что такое Бесплатные программы (Freeware)?
2. Что значит Почти бесплатные программы?
3. Что значит Программы, показывающие рекламу?
4. Что значит Коммерческие программы (Commercial)?
5. Что такое системное программное обеспечение?
6. Что такое прикладное программное обеспечение?
7. Что такое Почти работоспособные программы?
8. Что такое Условно бесплатные продукты

Лабораторная работа №4. АППАРАТНЫЕ КЛЮЧИ ЗАЩИТЫ. КОЛИЧЕСТВЕННАЯ ОЦЕНКА СТОЙКОСТИ ПАРОЛЬНОЙ ЗАЩИТЫ..

Аппаратные ключи защиты.

Электронный ключ (также аппаратный ключ, иногда донгл от англ. dongle) — аппаратное средство, предназначенное для защиты программного обеспечения (ПО) и данных от копирования, нелегального использования и несанкционированного распространения.

Современные электронные ключи

Основой данной технологии является специализированная микросхема, либо защищённый от считывания микроконтроллер, имеющие уникальные для каждого ключа алгоритмы работы. Донглы также имеют защищённую энергонезависимую память небольшого объёма, более сложные устройства могут иметь встроенныйкриптопроцессор (для аппаратной реализации шифрующих алгоритмов), часы реального времени. Аппаратные ключи могут иметь различные форм-факторы, но чаще всего они подключаются к компьютеру через USB. Также встречаются с LPT- или PCMCIA-интерфейсами.

Принцип действия электронных ключей. Ключ присоединяется к определённому интерфейсу компьютера. Далее защищённая программа через специальный драйвер отправляет ему информацию, которая обрабатывается в соответствии с заданным алгоритмом и возвращается обратно. Если ответ ключа правильный, то программа продолжает свою работу. В противном случае она может выполнять определенные разработчиками действия, например, переключаться в демонстрационный режим, блокируя доступ к определённым функциям.

Существуют специальные ключи, способные осуществлять лицензирования (ограничения числа работающих в сети копий программы) защищенного приложения по сети. В этом случае достаточно одного ключа на всю локальную сеть. Ключ устанавливается на любой рабочей станции или сервере сети. Защищенные приложения обращаются к ключу по локальной сети. Преимущество в том, что для работы с приложением в пределах локальной сети им не нужно носить с собой электронный ключ.

HASP

Одним из наиболее распространенных в России защитных устройств такого типа является устройство HASP (HardwareAgainstSoftwarePiracy) от компании Aladdin, по сути ставшее стандартом де-факто. AladdinSoftwareSecurity R.D. — это российская компания, представитель мирового лидера в области разработки и производства систем аутентификации, защиты информации при работе с Интернетом и защиты программного обеспечения от несанкционированного использования AladdinKnowledgeSystemsLtd (http://www.aladdin.ru/).

HASP — это аппаратно-программная инструментальная система, предна-

значенная для защиты программ и данных от нелегального использования, пиратского тиражирования и несанкционированного доступа к данным, а также для аутентификации пользователей при доступе к защищенным ресурсам. В первых версиях это небольшое устройство подключалось к параллельному порту компьютера. Затем появились USB-HASP-устройства. Иметь маленький USB-ключ значительно удобнее, чем большой 25-штырьковый сквозной разъем, да и часто возникающие проблемы с совместимостью ключей и устройств, работающих через параллельный порт, типа принтеров и ZIP-дисководов изрядно утомляли пользователей. А с USB-устройствами работает автоматическое подключение (plug-and-play), порты USB выносятся на переднюю панель, встраиваются в клавиатуру и монитор. А если даже такого удобного разъема под рукой нет, то в комплекте с этими ключами часто продают удлинители. Существуют несколько разновидностей ключей — с памятью, с часами и т.д.

Hardlock

Hardlock — это электронный ключ компании Aladdin, предназначенный для защиты приложений и связанных с ними файлов данных, позволяющий программировать ключи защиты и лицензировать авторское программное обеспечение. Механизм работы ключей Hardlock базируется на заказном ASIC-чипе со встроенной EEPROM-памятью.

Чип имеет сложную внутреннюю организацию и нетривиальные алгоритмы работы. Логику работы чипа практически невозможно реализовать с помощью стандартных наборов микросхем, его очень сложно воспроизвести, а содержащийся в его памяти микрокод — считать, расшифровать или эмулировать.

Такие ключи могут устойчиво работает во всех компьютерах (включая ноутбуки), на различных портах, в самых разных режимах, позволяя подключать через них практически любые устройства — принтеры, сканеры, модемы и т.п. А малый ток потребления позволяет каскадировать любое количество ключей.

Hardlock осуществляет защиту 16- и 32-разрядных приложений и связанных с ними файлов данных в прозрачном режиме. При чтении данные автоматически расшифровываются, при записи — зашифровываются с использованием заданного аппаратно-реализованного алгоритма. Эта возможность может использоваться также для хранения и безопасной передачи информации в сети Интернет.

eToken

Как уже говорилось, наилучшим решением сегодня в области защиты информации являются смарт-карты, но для их использования необходимы специальные устройства считывания (карт-ридеры). Эту проблему снимают устройства типа eToken — электронные смарт-ключи производства той же компании Aladdin, подключаемые напрямую к USB-порту.

eToken — это полнофункциональный аналог смарт-карты, выполненный в виде брелока. Он напрямую подключается к компьютеру через USB-порт и

не требует наличия дорогостоящих карт-ридеров и других дополнительных устройств. Основное назначение eToken — аутентификация пользователя при доступе к защищенным ресурсам сети и безопасное хранение цифровых сертификатов, ключей шифрования, а также любой другой секретной информации.

Каждому брелоку eToken можно присвоить уникальное имя, например имя его владельца. Чтобы узнать имя владельца eToken, достаточно подклю- чить брелок к USB-порту и открыть окно «Свойства». Однако получить дос- туп к защищенной памяти eToken и воспользоваться этим брелоком без знания специального PIN-кода нельзя.

Кроме того, eTokenвыполнен в прочном водонепроницаемом корпусе и защищен от воздействия окружающей среды. Он имеет защищенную энергонезависимую память (модели PRO и RIC снабжены микропроцессором). Небольшой размер позволяет носить его на связке с ключами.

Если нужно подключить к компьютеру несколько ключей одновременно, а USB-портов не хватает, то можно воспользоваться концентратором (USB-HUB). Для удобства применения eToken поставляется вместе с удлинителем для USB-порта.

Таким образом, eToken может стать универсальным ключом, легко интегрируемым в различные системы для обеспечения надежной аутентификации. С его помощью можно осуществлять безопасный доступ к защищенным Web-страницам, к сетям, отдельным приложениям и т.д. Универсальность применения, легкость в использовании, удобство для пользователей и администраторов, гарантированное качество делают его прекрасным средством при необходимости использовать цифровые сертификаты и защищенный доступ.

SecretDisk

В случае если объем конфиденциальной информации довольно значителен, можно воспользоваться устройством SecretDisk, выполненным с применением технологии eToken. SecretDisk — это разработка компании AladdinSoftwareSecurity R.D., предназначенная для защиты конфиденциальной информации на персональном компьютере с ОС Windows 2000/XP.

Принцип защиты данных при помощи системы SecretDisk заключается в создании на компьютере пользователя защищенного ресурса — секретных дисков, предназначенных для безопасного хранения конфиденциальной информации. Доступ к этой информации осуществляется посредством электронного ключа eToken, подсоединяемого к USB-порту компьютера. Доступ к информации, защищенной системой SecretDisk, получают только непосредственный владелец информации и авторизованные им доверенные лица, имеющие электронный ключ eToken и знающие его PIN-код. Для других пользователей защищенный ресурс будет невидим и недоступен. Более того, они даже не догадаются о его наличии.

Устанавливая на компьютере систему SecretDisk, пользователь может быть уверен в сохранности защищаемых данных. Конфиденциальная информация не может быть просмотрена, скопирована, уничтожена или повреждена другими пользователями. Она не может быть использована посторонними при

ремонте или краже компьютера, а также при утере съемного зашифрованного диска.

Для защиты корпоративных серверов используется специальная версия — SecretDiskServer. Особенностью системы SecretDiskServer также является отсутствие следов закрытого «контейнера с информацией» в файловой системе. Таким образом, если злоумышленники снимут диск с вашего сервера, то они не только не смогут расшифровать данные — они даже не увидят, где именно находится информация.

Заключение

Аппаратно-программные средства защиты выпускаются в достаточном количестве (помимо лидера — компании Aladdin и другими производителями, в том числе и российскими). Однако если говорить о программном обеспечении, то, пожалуй, единственным способом надежной защиты является перевод ее разработки из разряда ПО в разряд платформ. Иными словами, достаточно сложный программный комплекс требует при эксплуатации тесного сотрудничества с производителем. Купить продукт легко, гораздо труднее правильно настроить его и поддерживать. Естественно, такой подход легко реализуем для систем корпоративного назначения, но плохо применим к коробочным программам для широкого пользователя. Однако и в этом направлении работы уже давно ведутся (подписка на ПО, мультимедийные программы с онлайновым обращением и пр.), и производитель получает дополнительные возможности для улучшения защиты.

Что касается проблем аутентификации, то все чаще применяется технология PKI (PublicKeyInfrastructure), использующая системы сертификатов и специальных серверов для их проверки — центров сертификации CA (CertificationAuthorities). Одни из самых популярных систем сертификации — RSA Keon, Baltimore, Verisign и Entrust, работающие по протоколам HTTP и LDAP (сертификаты X.509). Центр сертификации уже входит в поставку Windows 2000 Server; в платформе .Net будет встроена поддержка цифровых сертификатов. Остается нерешенной только проблема защищенного хранения цифровых сертификатов.

Однако даже индивидуальным пользователям к таким хранилищам стоит относиться с опаской: если специальное устройство хранит все пароли пользователя (в том числе и его privatekey) и впускает его в систему по аппаратному ключу, то достаточно подобрать к этому устройству один пароль — и все секреты как на ладони…

Обход защиты

Задача злоумышленника — заставить защищённую программу работать в условиях отсутствия легального ключа, подсоединённого к компьютеру. Не вдаваясь очень глубоко в технические подробности, будем исходить из предположения, что у злоумышленника есть следующие возможности:

перехватывать все обращения к ключу;

протоколировать и анализировать эти обращения;

посылать запросы к ключу и получать на них ответы;

протоколировать и анализировать эти ответы;

посылать ответы от имени ключа и др.

Такие широкие возможности противника можно объяснить тем, что он имеет доступ ко всем открытым интерфейсам, документации, драйверам и может их анализировать на практике с привлечением любых средств.

Для того чтобы заставить программу работать так, как она работала бы с ключом, можно или внести исправления в программу (взломать её программный модуль), или эмулировать наличие ключа путём перехвата вызовов библиотеки API обмена с ключом.

Стоит отметить, что современные электронные ключи (к примеру, ключи Guardant поколения Sign и современные ключи HASP HL) обеспечивают стойкое шифрование протокола обмена электронный ключ -- библиотека API работы с ключом. В результате наиболее уязвимыми местами остаются точки вызовов функций этого API в приложении и логика обработки их результата.

Эмуляция ключа

При эмуляции никакого воздействия на код программы не происходит, и эмулятор, если его удается построить, просто повторяет все поведение реального ключа. Эмуляторы строятся на основе анализа перехваченных запросов приложения и ответов ключа на них. Они могут быть как табличными (содержать в себе все необходимые для работы программы ответы на запросы к электронному ключу), так и полными (полностью эмулируют работу ключа, так как взломщикам стал известен внутренний алгоритм работы).

Построить полный эмулятор современного электронного ключа — это достаточно трудоёмкий процесс, требующий большого количества времени и существенных инвестиций. Ранее злоумышленникам это удавалось: например, компания Aladdin признаёт, что в 1999 году злоумышленникам удалось разработать довольно корректно работающий эмулятор ключа HASP3 и HASP4. Это стало возможным благодаря тому, что ключ использовал проприетарный алгоритм кодирования, который был взломан. Сейчас большинство ключей используют публичные криптоалгоритмы, поэтому злоумышленники предпочитают атаковать какой-то конкретный защищённый продукт, а не защитный механизм в общем виде. Для современных систем защиты HASP и Guardant эмуляторов в свободном доступе нет, так как используется криптосистема с открытым ключом.

Информации о полной эмуляции современных ключей Guardant не встречалось. Существующие табличные эмуляторы реализованы только для конкретных приложений. Возможность их создания была обусловлена неиспользованием (или неграмотным использованием) основного функционала электронных ключей разработчиками защит.

Так же отсутствует какая-либо информация о полной или хотя бы частичной эмуляции ключей LOCK, либо о каких-либо других способах обхода этой защиты.

Взлом программного модуля

Злоумышленник исследует логику самой программы, с той целью, чтобы, проанализировав весь код приложения, выделить блок защиты и деактивировать его. Взлом программ осуществляется с помощью отладки (или пошагово-

го исполнения), декомпиляции и дампа оперативной памяти. Эти способы анализа исполняемого кода программы чаще всего используются злоумышленниками в комплексе.

Отладка осуществляется с помощью специальной программы — отладчика, который позволяет по шагам исполнять любое приложение, эмулируя для него операционную среду. Важной функцией отладчика является способность устанавливать точки (или условия) остановки исполнения кода. С помощью них злоумышленнику проще отслеживать места в коде, в которых реализованы обращения к ключу (например, остановка выполнения на сообщении типа «Ключ отсутствует!Проверьте наличие ключа в USB-интерфейсе»).

Дизассемблирование — способ преобразования кода исполняемых модулей в язык программирования, понятный человеку — Assembler. В этом случае злоумышленник получает распечатку (листинг) того, что делает приложение.

Декомпиляция - преобразование исполняемого модуля приложения в программный код на языке высокого уровня и получение представления приложения, близкого к исходному коду. Может быть проведена только для некоторых языков программирования (в частности, для .NET приложений, создаваемых на языке C# и распространяемых в байт-коде - интерпретируемом языке относительно высокого уровня).

Суть атаки с помощью дампа памяти заключается в считывании содержимого оперативной памяти в момент, когда приложение начало нормально исполняться. В результате злоумышленник получает рабочий код (или интересующую его часть) в "чистом виде" (если, к примеру, код приложения был зашифрован и расшифровывается только частично, в процессе исполнения того или иного участка). Главное для злоумышленника — верно выбрать момент.

Отметим, что существует немало способов противодействия отладке, и разработчики защиты используют их: нелинейность кода, (многопоточность), недетерминированную последовательность исполнения, «замусоривание» кода, (бесполезными функциями, выполняющими сложные операции, с целью запутать злоумышленника), использование несовершенства самих отладчиков и др.

Количественная оценка стойкости парольной защиты.

Цель работы: реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

Теоретические сведения

Подсистемы идентификации и аутентификации пользователя играют важную роль в системах защиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации являются одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации. В данном случае информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя, как правило, передний край обороны СЗИ. В связи с этим модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель последнего в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя наиболее просты и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю:

1) минимальная длина пароля должна быть не менее 6 символов;

2) пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.);

3) в качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

К подсистеме парольной аутентификации:

1) администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, пароль следует сменить;

2) в подсистеме парольной аутентификации необходимо установить ограничение числа попыток ввода пароля (как правило, не более трёх);

3) в подсистеме парольной аутентификации требуется установить временную задержку в случае ввода неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы – автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

Количественная оценка стойкости парольной защиты

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля: если пароль состоит только из малых английских букв, то $A = 26$), L – длина пароля, $S = A^L$ – число всевозможных паролей длины L, которые можно составить из символов алфавита A, V – скорость перебора паролей злоумышленником, T – максимальный срок действия пароля.

Тогда, вероятность P подбора пароля злоумышленником в течение срока

его действия V определяется по следующей формуле:

$P = (V \cdot T) / S = (V \cdot T) / A^L$.

Эту формулу можно использовать в обратную сторону для решения следующей задачи.

Задача. Определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

Данная задача имеет неоднозначное решение. При исходных данных V, T, P однозначно можно определить лишь нижнюю границу S^* числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле

$S^* = [V \cdot P / T]$,

(1)

где [] – целая часть числа, взятая с округлением вверх.

После определения нижней границы S^* необходимо выбрать такие A и L для формирования $S = A^L$, чтобы выполнялось следующее неравенство:

$S^* \le S = A^L$.

(2)

При выборе S, удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных V и T) будет меньше, чем заданная P.

Следует отметить, что при осуществлении вычислений по формулам (1) и (2), величины должны быть приведены к одним размерностям.

Пример. Исходные данные: $P = 10^{-6}$, T = 7 дней = 1 неделя, V = 10 (паролей / минуту) = 10 · 60·24·7 = 100800 паролей в неделю. Тогда, $S^* = [(10800 \cdot 1) / 10^{-6}] = = 108 \cdot 10^8$.

Условию $S^* \le A^L$ удовлетворяют, например, такие комбинации A и L, как A = 26, L = 8 (пароль состоит из восьми малых символов английского алфавита), A = 36, L = 6 (пароль состоит из шести символов, среди которых могут быть малые латинские буквы и произвольные цифры).

Задание на лабораторную работу

1. В табл. 3 найти для указанного варианта значения характеристик P, V, T.

2. Вычислить по формуле (1) нижнюю границу S^* для заданных P, V, T.

3. Выбрать некоторый алфавит с мощностью A и получить минимальную длину пароля L, при котором выполняется условие (2).

4. Реализовать программу для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины L, при этом должен использоваться алфавит из A символов.

5. Оформить отчет по лабораторной работе.

Коды символов:

1. Коды английских символов : «A» = 65, …, «Z» = 90, «a» = 97,…, «z» = 122.

2. Коды цифр : «0» = 48, «9» = 57.

3. «!» = 33, «“» = 34, «#» = 35, «$» = 36, «%» = 37, «&» = 38, «‘» = 39.

4. Коды русских символов : «А» – 128, … «Я» – 159, «а» – 160,…, «п» – 175, «р» – 224,…, «я» – 239.

Таблица 3. Варианты заданий

Вариант	*P*	*V*	*T*
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней
9	10^{-4}	3 паролей/мин	15 дней
10	10^{-5}	10 паролей/мин	1 неделя
11	10^{-6}	11 паролей/мин	2 недели
12	10^{-7}	100 паролей/день	10 дней
13	10^{-4}	10 паролей/день	5 дней
14	10^{-5}	20 паролей/мин	6 дней
15	10^{-6}	15 паролей/мин	12 дней
16	10^{-7}	3 паролей/мин	1 месяц
17	10^{-4}	10 паролей/мин	3 недели
18	10^{-5}	11 паролей/мин	20 дней
19	10^{-6}	100 паролей/день	15 дней
20	10^{-7}	10 паролей/день	1 неделя
21	10^{-4}	20 паролей/мин	2 недели
22	10^{-5}	15 паролей/мин	10 дней
23	10^{-6}	3 паролей/мин	5 дней
24	10^{-7}	10 паролей/мин	6 дней
25	10^{-4}	11 паролей/мин	12 дней
26	10^{-5}	100 паролей/день	1 месяц
27	10^{-6}	10 паролей/день	3 недели
28	10^{-7}	20 паролей/мин	20 дней
29	10^{-4}	15 паролей/мин	15 дней
30	10^{-5}	3 паролей/мин	1 неделя

Контрольные вопросы ЛР4 (ПК2):

1. Что такое Аппаратные ключи защиты?
2. Электронный ключ?
3. Поясните термин Современные электронные ключи
4. Что значит HASP?
5. Что значит eToken?

6. Что значит SecretDisk?
7. Что значит Аппаратно-программные средства защиты?
8. Поясните идею Обхода защиты
9. Что значит Дизассемблирование?
10. Что значит Декомпиляция?
11. Поясните идею Количественной оценки стойкости парольной защиты

Лабораторная работа №5. ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. БЕЗОПАСНАЯ РАБОТА В ИНТЕРНЕТ

Вредоносной программой называется любое программное обеспечение, предназначенное для получения несанкционированного доступа к информации, хранимой на компьютере, с целью причинения вреда владельцу информации, хранимой на компьютере, с целью причинения вреда владельцу информации или владельцу компьютера.

Компьютерный вирус — программа способная самопроизвольно внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере. Иликомпьютерный вирус – это целенаправленно созданная программа, автоматически приписывающая себя к другим программным продуктам, изменяющая или уничтожающая их.

Признаки заражения:

- Прекращение работы или неправильная работа ранее успешно функционировавших программ;
- Медленная работа компьютера;
- Невозможность загрузки операционной системы;
- Исчезновение файлов и каталогов или искажение их содержимого;
- Изменение даты и времени модификации файлов;
- Изменение размеров файлов;
- Неожиданное значительное увеличение количества файлов на диске;
- Существенное уменьшение размера свободной оперативной памяти;
- Вывод на экран непредусмотренных звуковых сигналов;
- Частые зависания и сбои в работе компьютера.

Схема работы компьютерных вирусов :

— Заражение.

Происходит при запуске инфицированной программы или при обращении к носителю, имеющему вредоносный код в системной области; обычно код вируса сначала поступает в оперативную память работающего компьютера, откуда он копируется на запоминающие устройства.

— Размножение.

Вирусный код может воспроизводить себя в теле других программ. Происходит как серия последовательных заражений; в первую очередь поражаются файлы самой операционной системы, чем чаще срабатывает механизм, тем больше файлов поражается.

— Атака.

Последняя фаза развития вируса; во время атаки вирус производит более или менее разрушительные действия. После создания достаточного числа копий программный вирус начинает осуществлять разрушение: нарушение рабо-

ты программ и ОС, удаление информации на жестком диске, самые разрушительные вирусы вызывают форматирование жесткого диска. Некоторые вирусы могут уничтожать данные, в этом случае требуется замена микросхемы (хотя считается, что никакой вирус не в состоянии вывести из строя аппаратное обеспечение ПК).

Существует класс программ, которые были изначально написаны с целью уничтожения данных на чужом компьютере, похищения чужой информации, несанкционированного использования чужих ресурсов и т. п., или же приобрели такие свойства вследствие каких-либо причин. Такие программы несут вредоносную нагрузку и соответственно называются вредоносными.

К вредоносным программам относятся вирусы и программные закладки.

В ГОСТ Р 51272-99 «Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положение» вводится следующее понятие вируса: Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

Программной закладкой называют программу, обладающую одной из разрушительных функций по отношению к информационной системе:

1. уничтожение или внесение изменений в функционирование программного обеспечения;

2. превышение полномочий пользователя с целью несанкционированного копирования конфиденциальной информации – "троянские программы";

3. подмена отдельных функций подсистемы защиты или создание в ней люков-уязвимостей;

4. перехват паролей пользователей (перехват всего клавиатурного ввода);

5. перехват потока информации, передаваемого в сети;

6. распространение в распределенных информационных системах, с целью реализации определенной угрозы – так называемые "черви" – самостоятельно действующие программы, не внедряющиеся в тела других файлов.

Компьютерные вирусы классифицируются по следующим признакам:

1. По способу распространения в информационной системе: файловые (заражающие файлы определенного типа), загрузочные (заражающие загрузочные сектора) и комбинированного типа;

2. По способу заражения: резидентные (часть кода которых постоянно находится в оперативной памяти) и нерезидентные (которые заражают только в момент непосредственного обращения к уже зараженным файлам);

3. По особенностям реализуемого алгоритма:

а. вирусы-спутники, создающие для заражаемых файлов одноименные файлы с кодом вируса и переименовывающие исходные файлы;

б. паразитические вирусы, которые обязательно изменяют содержимое заражаемых объектов;

в. "стелс"-вирусы, в которых путем перехвата обращений операционной системы к заражённым объектам и возврата вместо них оригинальных незараженных данных скрывается факт присутствия вируса;

г. вирусы-призраки (полиморфы), каждая следующая копия которых в заражённых объектах отличается от предыдущих.

Безопасная работа в Интернет.

Потенциально опасные веб-сайты: снижение риска при работе в Интернете можно совершенно случайно попасть на небезопасные сайты.

Созданием таких сайтов занимаются мошенники. Опасные сайты применяются для распространения вредоносного ПО, для сбора адресов электронной почты, номеров сотовых телефонов, информации об учетных записях. Определить сайт мошенников можно по нижеследующим характеристикам: Зайдя на такой сайт, можно заметить странное поведение браузера.• К примеру, пользователь нажал на какую-нибудь ссылку, после этого открылась страница сайта, и впоследствии этого, открылись новые страницы сайта в новом окне браузера. В такой ситуации, нужно незамедлительно закрыть подозрительные страницы. При переходе на сайт мошенников возможно предложение об установке или загрузке какого-либо приложения. К примеру, пользователь может увидеть сообщение, в котором говорится, что данный компьютер заражен опасным вирусом. В этом же сообщение будет сказано, что для излечения вируса надо установить новый антивирус. Также текст сообщения может говорить о том, что браузер пользователя устарел и необходимо скачать обновление. В таких случаях, пользователь не должен загружать или устанавливать приложения, если он не уверен в надёжности сайта, на котором эти приложения размещены.

Установка таких приложений может привести к существенным проблемам. Web-дизайн сайта, который знаком пользователю, может быть несколько изменён. Допустимо ухудшение качества изображений, изменение вида кнопок и полей ввода. Текст сайта может содержать ошибки. Также незначительно изменён адрес сайта, это сделано так, что невооружённым глазом изменения можно не заметить. Эти факторы указывают на то, что пользователь находится совсем не на том сайте, куда хотел зайти. К примеру, если пользователь ввёл в адресную строку адрес сайта с ошибкой в одном символе, то вместо желаемого сайта откроется сайт мошенников. Этот сайт может очень чётко копировать Web-дизайн и действия другого сайта. При своих сомнениях в достоверности сайта, пользователю нужно закрыть данный сайт и попробовать открыть нужный сайт заново. К тому же надо использовать тот способ, которым пользователь регулярно пользуется. К примеру, при открытии сайта использовать сохранённую закладку сайта, или, точно ввести адрес сайта, при этом внимательно проверив точное написание адреса. Возможно такое, что при повторном открытии сайта, его подлинность не подтверждается. Это значит, что компьютер пользователя заражён вирусом, который подменяет страницы. При открытии сайта высвечивается окно с просьбой ввести свои данные (ФИО, адрес электронной почты). Чаще всего это делается под весьма благовидным предлогом. При вводе своей электронной почты на подозрительном сайте, пользователь подвергает свой почтовый ящик опасности, например, рассылка нежелательной рекламы. При переходе на сайт мошенников пользо-

вателю может быть предъявлено требование об отправке SMS-сообщения на какой-либо номер для подтверждения учетной записи или для входа в учетную запись. Такой метод используют злоумышленники для кражи денежных средств пользователей. В таких случаях, сайты мошенников могут иметь внешний вид популярных веб-сайтов, – к примеру, страницы входа в учетные записи социальных сетей. При своих подозрениях, пользователь должен постараться закрыть вкладки браузера, на которых открыта его страница. Пользователь должен учесть, что при подозрениях о подлинности сайта, который требует ввод логина и пароля, не стоит вводить никакие данные. 19 Также при работе в Интернете можно увидеть рекламные изображения, которые настойчиво призывают кликнуть по ним. Такие объявления могут привести на мошеннические сайты. Безопасность при работе с электронной почтой и системами обмена сообщениями Электронная почта и системы обмена сообщениями (Skype, ICQ) часто являются каналами распространения вредоносных программ. Кроме того, ими пользуются мошенники для того, чтобы обманом получать какие-либо секретные сведения. В опасных сообщениях в основном находятся ссылки, и предлагается перейти по ним. Предлоги могут быть самые разные. Например, в сообщении может говориться о том, что по ссылке расположена какая-то интересная страница. Нередко в подобных сообщениях говорится о том, что учетная запись пользователя на каком-либо сайте взломана, и для того, чтобы восстановить доступ к ней, ему нужно перейти по ссылке и выполнить какие-либо действия. Потенциально опасное сообщение может быть замаскировано под сообщение от администрации некоего сайта, с которым пользователь работает. Переход по ссылке приведет либо на мошеннический сайт, либо на страницу, которая используется для распространения вредоносных программ. При этом сообщение может быть отправлено и с незнакомого адреса, и с адреса человека, с которым пользователь уже переписывался. Текст таких сообщений часто изобилует ошибками и выглядит неестественно. Это результат автоматического составления текста письма вредоносной программой. Даже если текст письма не содержит ошибок, его стиль может отличаться от стиля того человека, от имени которого написано письмо. Это признаки потенциально опасного письма. Надежнее всего – связаться с этим человеком альтернативным способом (например, позвонив по телефону) и 20 спросить у него, отправлял ли он письмо, которое показалось подозрительным. Иногда в потенциально опасных сообщениях можно увидеть поля для ввода логина и пароля на каком-либо сайте. В тексте может быть указано, что, введя здесь логин и пароль, пользователь может восстановить доступ к взломанной учетной записи. Основное правило при получении подобных сообщений заключается в том, что нельзя переходить по ссылкам, которые в них присутствуют. Если пользователь зарегистрировался на каком-либо сайте и получил письмо с просьбой щелкнуть по ссылке для подтверждения адреса почтового ящика, по этой ссылке можно щелкнуть, не опасаясь мошенничества. Если же письмо со ссылкой пришло неожиданно – не нужно переходить по ссылкам, которые в нем есть. Иногда потенциально опасные сообщения содержат, в виде вложений, различные файлы. В них может присутствовать предложение скачать эти файлы. Не нужно скачивать такие файлы и пытаться с ними работать. В них могут находиться замаскированные вредоносные про-

граммы. Если, работая с электронной почтой, используется веб-интерфейс почтовой системы, следует ознакомиться с настройками безопасности этой системы. Обычно к настройкам имеются пояснения. Нужно Изучить эти материалы и выполнить те настройки, которые позволят повысить безопасность работы. Периодически нужно менять пароль к электронному почтовому ящику. Если некто пытается подобрать пароль, это серьезно усложнит ему задачу. Эта рекомендация касается и паролей к другим учетным записям. Безопасная работа с банковскими картами и платежными системами Для расчетов в сети Интернет используются пластиковые банковские карты и системы электронных денег.

Злоумышленников интересуют следующие данные банковских карт:

- Номер карты.
- CVV2-код (у карт системы Visa).
- CVC2-код (у карт системы Master Card).
- Срок действия карты.
- Имя и фамилия владельца карты

Кража этих данных (или хотя бы номера карты и CVV2/CVC2-кодов), сравнима с кражей карты и кода для снятия денежных средств с нее в банкомате. Если появляется подозрение, что кто-то узнал конфиденциальные данные карты, ее нужно немедленно заблокировать. Банки при открытии карты сообщают клиентам номера телефонов, позвонив по которым можно заблокировать карту. Блокировка карты в подобной ситуации – самый быстрый и надежный способ обезопасить себя от кражи денежных средств с карты. Повысить безопасность расчетов по карте помогает система одноразовых паролей для подтверждения факта списания средств. Обычно такой па- роль приходит в виде SMS-сообщения на сотовый телефон владельца карты. Для того чтобы снизить вероятность серьезных потерь при краже данных карты, на карте, которая применяется для покупок в Интернете, не следует хранить крупные суммы денег. Еще значительнее повысить безопасность расчетов можно, используя так называемые виртуальные предоплаченные карты. Обычно выпуск таких карт производится в Интернет-службах банков, в которых открыты карты. Оплачивая покупки в Интернете с помощью виртуальной предоплаченной карты, пользователь рискует лишь суммой остатка на ней. Доступ к системам электронных денег напоминает доступ к обычному электронному почтовому ящику. Обычно в таких системах можно использовать дополнительные средства защиты. Среди них следующие: Использование платежного пароля для подтверждения операций по списанию средств. Использование одноразовых паролей, высылаемых по SMS на телефон владельца счета в системе. Повышенные требования к основному паролю для входа в систему. Использование дополнительных ключевых данных для доступа к электронному кошельку. Работая с некоей платежной системой, нужно выяснить, какие средства обеспечения безопасности в ней предусмотрены, и пользоваться ими. Если есть подозрение, что кто-то узнал пароль к электронному кошельку, – следует немедленно поменять его. Если сделать этого не удастся (то есть злоумышленник поменял пароль) – нужно связаться с администрацией системы и сообщить о проблеме. Данные для связи обычно указаны на веб- сайтах платежных систем.

Кража денежных средств в Интернете – это не только кража данных банковских карт или информации для доступа к платежным системам, это и непосредственная кража денежных средств, которые поступают недобросовестным продавцам от покупателей. Речь идет о мошеннических Интернет- магазинах. Оценивая надежность Интернет-магазина, нужно обратить внимание на наличие среди контактной информации адреса и телефона. Следует позвонить по указанному телефону, уточнить информацию о тех товарах, которые собираетесь заказать.

Мошенники обычно не любят приводить такие данные или размещают на страницах контактной информации поддельные адреса и телефоны. Для того чтобы убедиться в надежности некоего нового Интернет- магазина, нужно поискать отзывы о нем на независимых ресурсах. Следует учесть, что положительные отзывы могут быть оставлены создателями магазина, а отрицательные – его конкурентами. Если анализ отзывов показывает, что магазин создан не мошенниками, и очень нужно то, что в нем продается, можно использовать для первого заказа метод оплаты, который не предусматривает электронное совершение платежа. Это оплата при доставке товара курьером, оплата почтовым или банковским переводом, оплата наложенным платежом при получении на почте. Если, получив первый заказ, пользователь убедился в том, что магазин действительно существует, и довольны качеством товара – продолжать работу с ним можно, используя и электронные средства платежей. Списки надежных Интернет-магазинов обычно можно найти на веб- сайтах электронных платежных систем.

Контрольные вопросы ЛР5 (ПК-2):

1. Что называется Вредоносной программой?
2. Что такое Компьютерный вирус ? Признаки заражения
3. Схема работы компьютерных вирусов.
4. Что значит Безопасная работа в Интернет?
5. Какие данные банковских карт интересуют Злоумышленников?

Лабораторная работа №6. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЛОКАЛЬНОЙ СЕТИ. НАСТРОЙКА ПАРАМЕТРОВ БЕЗОПАСНОСТИ БРАУЗЕРА.

Цель: изучить возможности настройки безопасности локальной сети и браузера

Политику безопасности можно сравнить с пограничником, охраняющим границу страны. Рассмотрим два способа улучшения безопасности работы виртуальной сети за два приема.

Шаг 1. Меняем учетную запись администратора (Пользователь Администратор с пустым паролем — это уязвимость)

Часто при установке Windows пароль администратора пустой и этим может воспользоваться злоумышленник. Иначе говоря, при установке Windows в автоматическом режиме с настройками по умолчанию мы имеем пользователя **Администратор** с пустым паролем и любой **User** может войти в такой ПК с правами администратора. Чтобы решить проблему выполним команду **Мой компьютер-Панель управления-АдминистрированиеУправление компьютером-Локальные пользователи-Пользователи** (рис. 1).

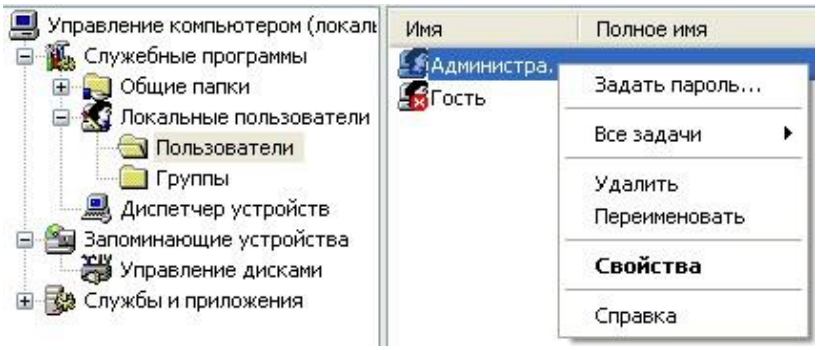


Рис. 1. Диалоговое окно Управление компьютером

Здесь по щелчку правой кнопкой мыши на **Администраторы** зададим администратору пароль, например, 12345. Это плохой пароль, но лучше, чем ничего. Теперь в окне **Администрирование** зайдем в **Локальную политику безопасности**. Далее идем по веткам дерева: **Локальные политикиПараметры безопасности-Учетные записи: Переименование учетной записи Администратор** (рис..2).

Рис. 2. Находим в системном реестре запись Переименование учетной записи Администратор

Здесь пользователя **Администратор** заменим на **Admin** (рис. 3).

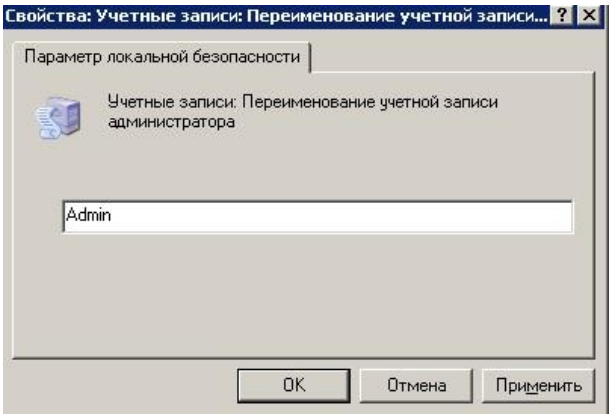


Рис. 3. Пользователю Администратор присваиваем новое имя

Перезагружаем ОС. После наших действий у нас получилась учетная запись Admin с паролем 12345 и правами администратора (рис. 4).

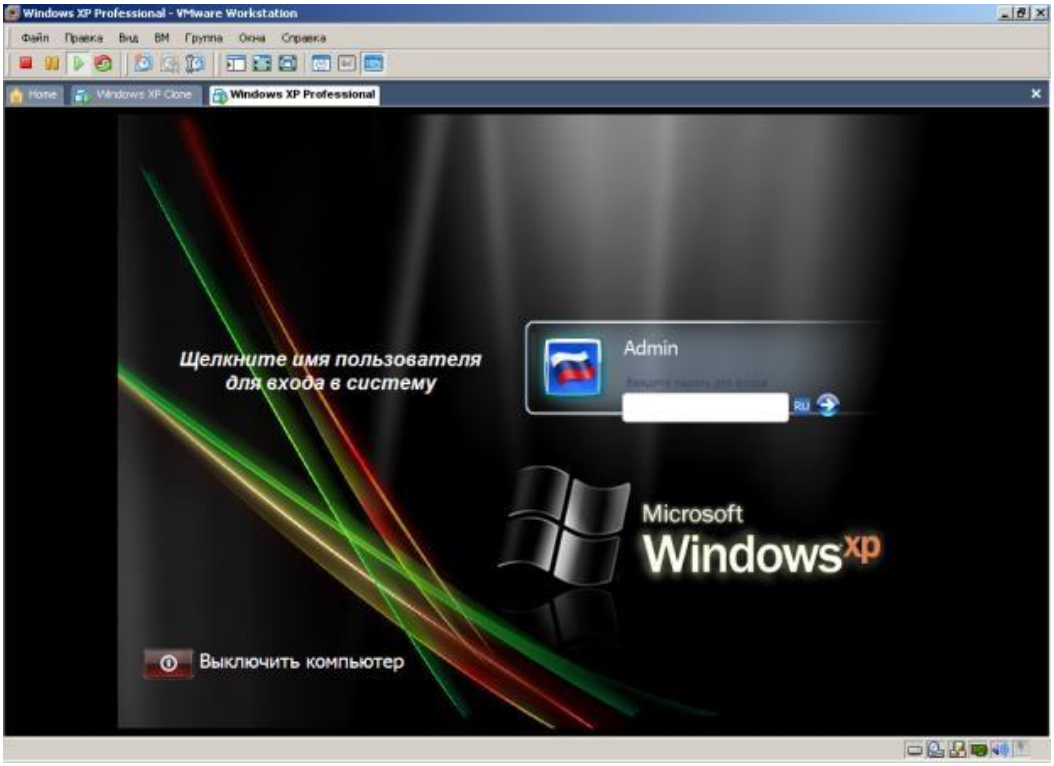


Рис. 4. Окно входа в ОС Windows XP

Теперь мы имеем пользователя **Администратор** с паролем, одна из уязвимостей системы устранена.

Примечание

Операцию по изменению имени пользователя и заданию пароля мы также могли бы выполнить без использования системного реестра, использовав окно **Учетные записи пользователей**, что гораздо проще (рис.
5).

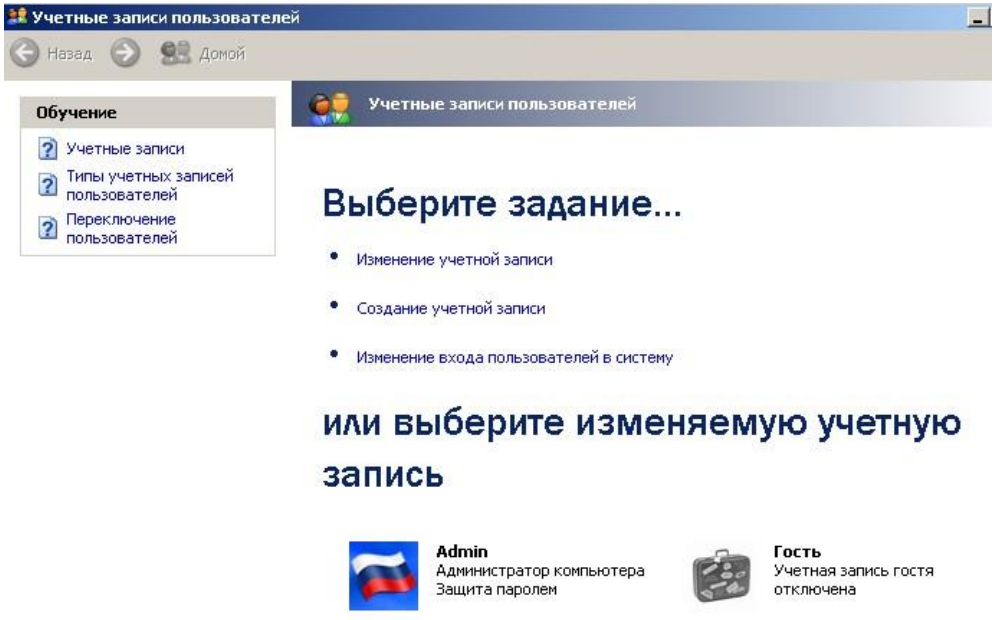


Рис. 5. Окно Учетные записи пользователей

Примечание

Учетная запись Гость позволяет входить в ПК и работать на нем (например, в Интернет) без использования специально созданной учетной записи. Запись Гость не требует ввода пароля и по умолчанию блокирована. Гость не может устанавливать или удалять программы. Эту учетную запись можно отключить, но нельзя удалить.

Шаг 2. Делаем окно приветствия пустым (убираем уязвимость 2)

У нас окно входа в систему содержит подсказку Admin, давайте ее уберем, сделав окно пустым. Для начала в окне **Учетные записи пользователей** жмем на кнопку **Изменение входа пользователей в систему** и уберем флажок **Использовать страницу приветствия** (рис.
6 и рис. 7).

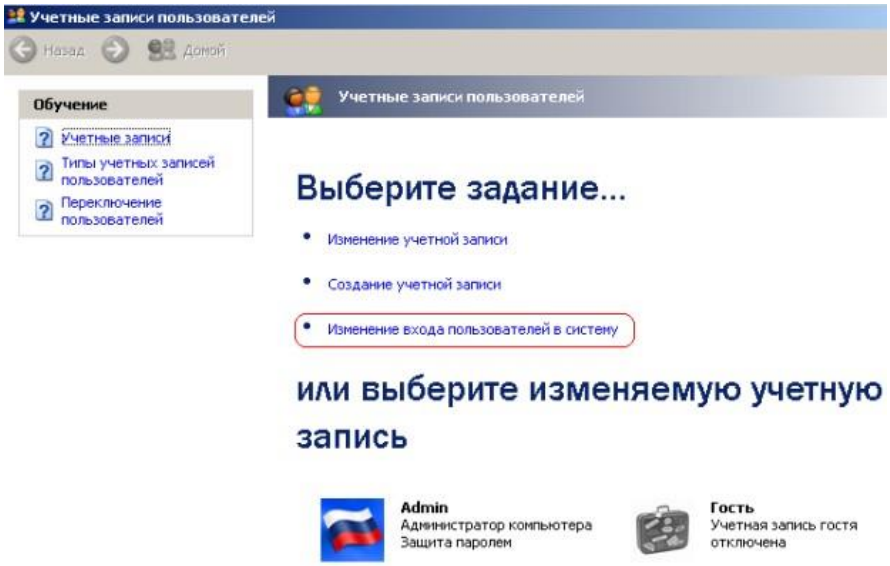


Рис. 6. Окно Учетные записи пользователей

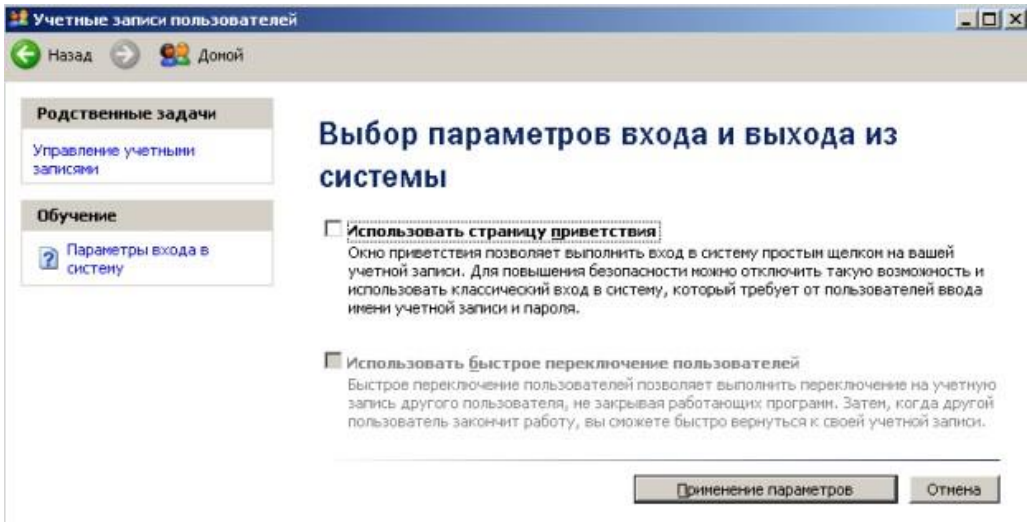


Рис. 7. Убираем флажок Использовать страницу приветствия

Теперь повысим безопасность сети еще на одну условную ступень, сделав оба поля окна приветствия пустыми (рис. 8).

Рис. 8. Обе строки данного окна сделаем пустыми

Выполним команду **Панель управления-Администрирование – Локальные политики безопасности- Локальные политики-Параметры безопасности—Интерактивный вход: не отображать последнего имени пользователя**. Эту запись необходимо включить (рис. 9).

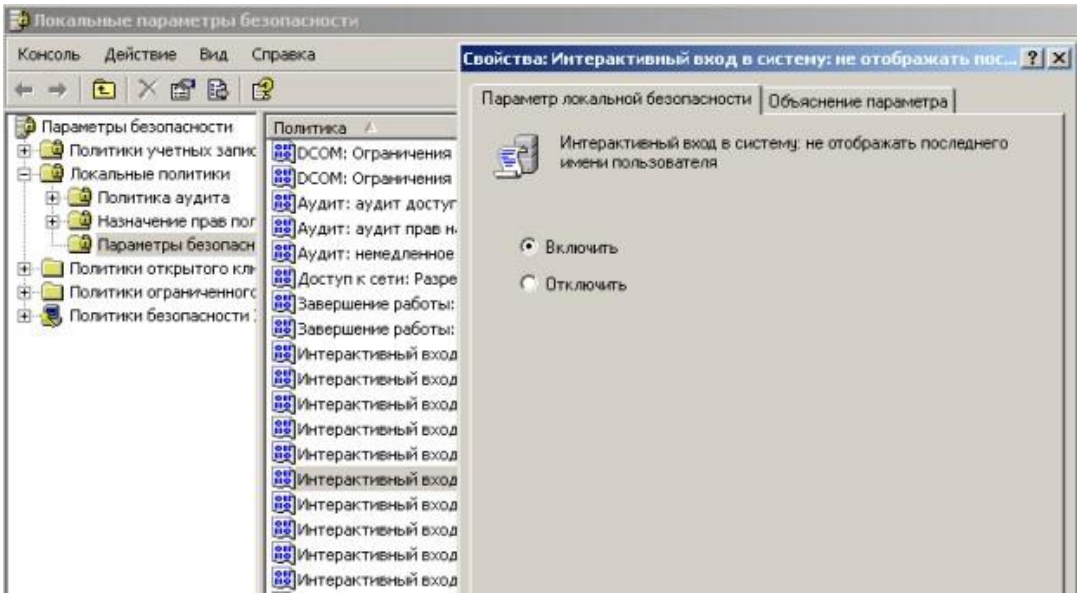


Рис. 9. Активируем переключатель Включить

Теперь после завершения сеанса пользователь должен угадать не только пароль, но и имя пользователя (рис. 10).

Рис. 10. Обе строки окна приветствия пусты

Выявление сетевых уязвимостей сканированием портов ПК

Злоумышленники используют сканирование портов ПК для того, чтобы воспользоваться ресурсами чужого ПК в Сети. При этом необходимо указать **IP** адрес ПК и открытый **port,** к примеру, **195.34.34.30:23**. После этого происходит соединение с удаленным ПК с некоторой вероятностью входа в этот ПК.

- TCP/IP port — это адрес определенного сервиса (программы), запущенного на данном компьютере в Internet. Каждый открытый порт — потенциальная лазейка для взломщиков сетей и ПК. Например, SMTP (отправка почты) — 25 порт, WWW — 80 порт, FTP —21 порт.
- Хакеры сканируют порты для того, чтобы найти дырку (баг) в операционной системе. Пример ошибки, если администратор или пользователь ПК открыл

полный доступ к сетевым ресурсам для всех или оставил пустой пароль на вход к компьютер.

Одна из функций администратора сети (сисадмина) — выявить недостатки в функционировании сети и устранить их. Для этого нужно просканировать сеть и закрыть (блокировать) все необязательные (открытые без необходимости) сетевые порты. Ниже, для примера, представлены службы TCP/IP, которые можно отключить:

- finger — получение информации о пользователях
- talk— возможность обмена данными по сети между пользователями
- bootp — предоставление клиентам информации о сети
- systat — получение информации о системе
- netstat — получение информации о сети, такой как текущие соединения
- rusersd — получение информации о пользователях, зарегистрированных в данный момент

Просмотр активных подключений утилитой Netstat

Команда **netstat** обладает набором ключей для отображения портов, находящихся в активном и/или пассивном состоянии. С ее помощью можно получить список серверных приложений, работающих на данном компьютере. Большинство серверов находится в режиме **LISTEN**— ожидание запроса на соединение. Состояние **CLOSE_WAIT** означает, что соединение разорвано. **TIME_WAIT** — соединение ожидает разрыва. Если соединение находится в состоянии **SYN_SENT**, то это означает наличие процесса, который пытается, установить соединение с сервером. **ESTABLISHED** — соединения установлены, т.е. сетевые службы работают (используются).

Итак, команда **netstat** показывает содержимое различных структур данных, связанных с сетью, в различных форматах в зависимости от указанных опций. Для сокетов (программных интерфейсов) TCP допустимы следующие значения состояния:

- CLOSED — Закрыт. Сокет не используется.
- LISTEN — Ожидает входящих соединений.
- SYN_SENT — Активно пытается установить соединение.
- SYN_RECEIVED — Идет начальная синхронизация соединения.
- ESTABLISHED — Соединение установлено.
- CLOSE_WAIT — Удаленная сторона отключилась; ожидание закрытия сокета.
- FIN_WAIT_1 — Сокет закрыт; отключение соединения.

- CLOSING — Сокет закрыт, затем удаленная сторона отключилась; ожидание подтверждения.
- LAST_ACK — Удаленная сторона отключилась, затем сокет закрыт; ожидание подтверждения.
- FIN_WAIT_2 — Сокет закрыт; ожидание отключения удаленной стороны.
- TIME_WAIT — Сокет закрыт, но ожидает пакеты, ещё находящиеся в сети для обработки

Примечание

Что такое «сокет» поясняет рис. 11. Пример сокета – 194.86.6..54:21

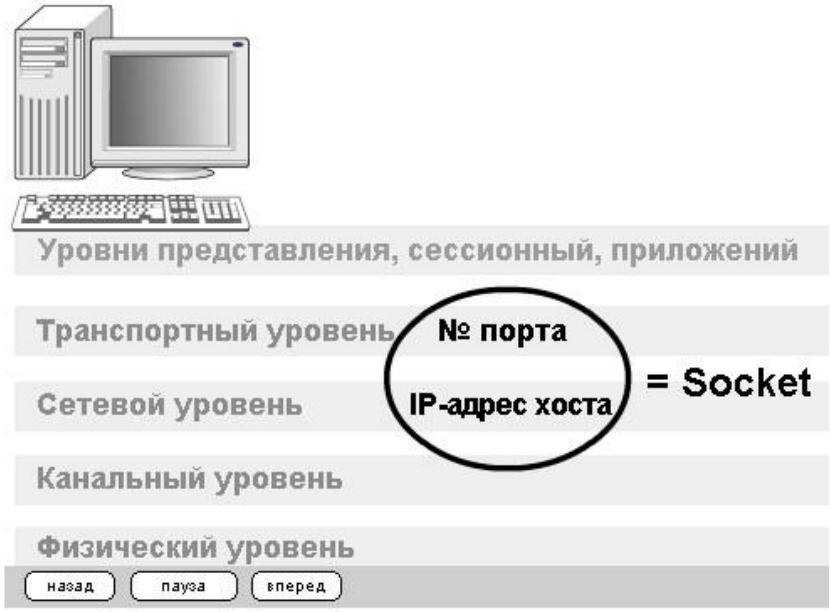


Рис. 11. Сокет это № порта + IP адрес хоста

Выполните практическое задание:

Задание 1. Обнаружение открытых на ПК портов утилитой Netstat

Для выполнения практического задания на компьютере необходимо выполнить команду **Пуск-Выполнить**. Откроется окно **Запуск программы**, в нем введите команду **cmd** (рис. 12).

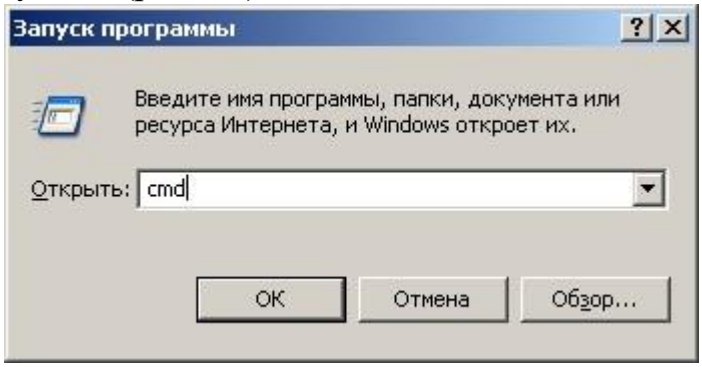


Рис. 12. Окно Запуск программы

Чтобы вывести все активные подключения TCP и прослушиваемые компьютером порты TCP/ UDP введите команду **netstat** (рис. 13). Мы видим Локального адреса (это ваш ПК) прослушиваются 6 портов. Они нужны для поддержки сети. На двух портах мы видим режим **ESTABLISHED** — соединения установлены, т.е. сетевые службы работают (используются). Четыре порта используются в режиме **TIME_WAIT** — соединение ожидает разрыва.

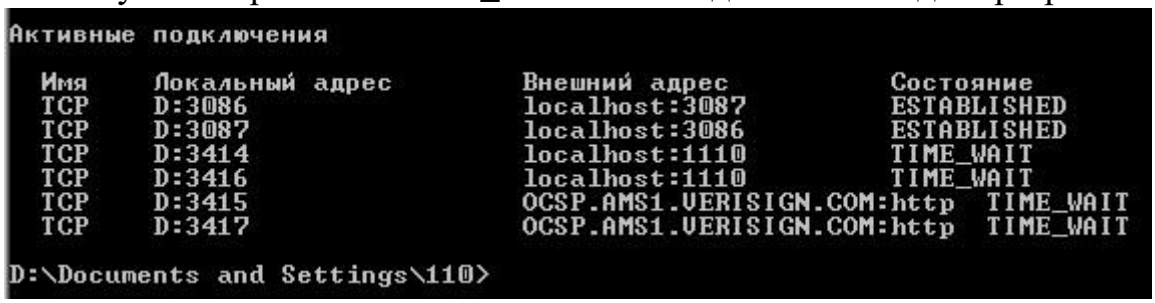


Рис. 13. Список активных подключений на тестируемом ПК

Запустите на вашем ПК Интернет и зайдите, например на **www.yandex.ru**. Снова выполните команду **netstat** (рис. 14). Как видим, добавилось несколько новых активных портов с их различными состояниями.

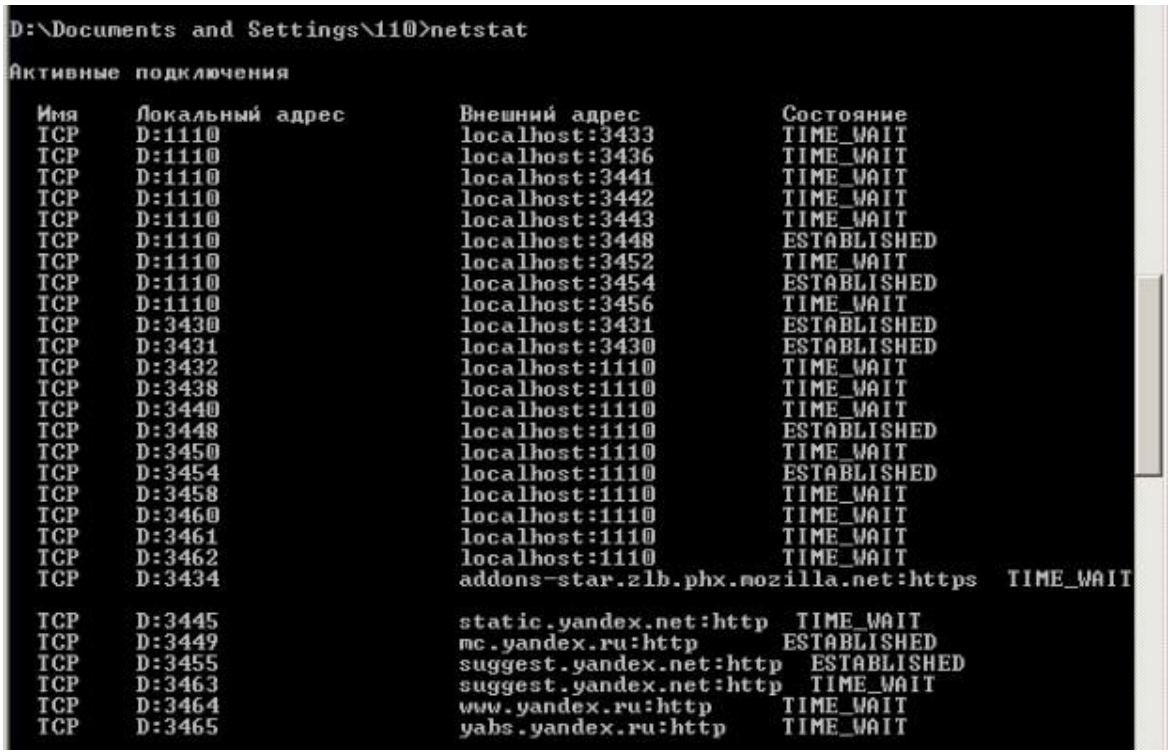


Рис. 14. Активные подключения при работе ПК в Интернет

Команда **netstat** имеет следующие опции – табл. 1.

Опция (ключ)	Назначение
-a	Показывать состояние всех сокетов; обычно сокеты, используемые серверными процессами, не показываются.
-A	Показывать адреса любых управляющих блоков протокола, связанных с сокетами; используется для отладки.
-i	Показывать состояние автоматически сконфигурированных (autoconfigured) интерфейсов. Интерфейсы, статически сконфигурированные в системе, но не найденные во время загрузки, не показываются.
-n	Показывать сетевые адреса как числа. netstat обычно показывает адреса как символы. Эту опцию можно использовать с любым форматом показа.
-r	Показать таблицы маршрутизации. При использовании с опцией -s, показывает статистику маршрутизации.
-s	Показать статистическую информацию по протоколам. При использовании с опцией -r, показывает статистику маршрутизации.
	Ограничить показ статистики или адресов управляющих блоков только указанным семейством_адресов, в качестве которого можно -f указывать:**inet** Для семейства адресов **AF_INET**,или **unix** Для семейство_адресов семейства адресов **AF_UNIX**.
	Выделить информацию об указанном интерфейсе в отдельный столбец; по умолчанию (для третьей формы команды) используется интерфейс с наибольшим объёмом переданной информации с момента последней перезагрузки системы. В качестве интерфейса можно указывать любой из интерфейсов, перечисленных в файле -I интерфейс конфигурации системы, например, emd1 или lo0.
-p	Отобразить идентификатор/название процесса создавшего сокет (-p, —programs display PID/Program name for sockets)

Таблица 1. Ключи для команды netstat

Программа NetStat Agent

Представьте ситуацию: ваше Интернет-соединение стало работать медленно, компьютер постоянно что-то качает из Сети. Вам поможет программа NetStat Agent. С ее помощью вы сможете найти причину проблемы и заблокировать ее. Иначе говоря, **NetStat Agent** — полезный набор инструментов для мониторинга Интернет соединений и диагностики сети. Программа позволяет отслеживать TCP и UDP соединения на ПК, закрывать нежелательные соединения, завершать процессы, обновлять и освобождать DHCP настройки адаптера, просматривать сетевую статистику для адаптеров и TCP/IP протоколов, а также строить графики для команд **Ping** и**TraceRoute** (рис. 15).

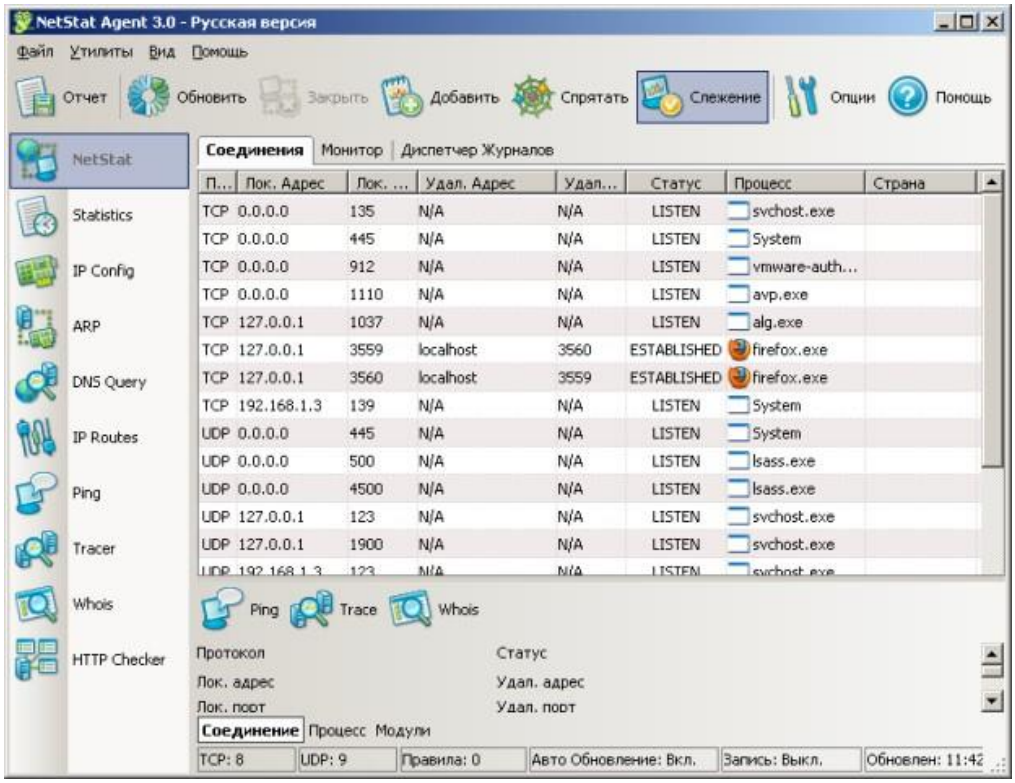


Рис. 15. Главное окно программы NetStat Agent

В состав программы NetStat Agent вошли следующие утилиты:

- **NetStat** — отслеживает TCP и UDP соединения ПК (при этом отображается географическое местоположение удаленного сервера и имя хоста).
- **IPConfig** — отображает свойства сетевых адаптеров и конфигурацию сети.
- **Ping** — позволяет проверить доступность хоста в сети.
- **TraceRoute** — определяет маршрут между вашим компьютером и конечным хостом, сообщая все IP-адреса маршрутизаторов.

- **DNS Query** — подключается к DNS серверу и находит всю информацию о домене (IP адрес сервера, MX-записи (Mail Exchange) и др.).
- **Route** — отображает и позволяет изменять IP маршруты на ПК.
- **ARP** — отслеживает ARP изменения в локальной таблице.
- **Whois** — позволяет получить всю доступную информацию об IPадресе или домене.
- **HTTP Checker** — помогает проверить, доступны ли Ваши веб-сайты.
- **Statistics** — показывает статистику сетевых интерфейсов и TCP/IP протоколов.

Сканер портов Nmap (Zenmap)

Nmap — популярный сканер портов, который обследует сеть и проводит аудит защиты. Использовался в фильме «Матрица: Перезагрузка» при взломе компьютера. Наша задача не взломать, а защитить ПК, поскольку одно и то же оружие можно использовать как для защиты, так и для нападения. Иначе говоря, сканером портов **nmap** можно определить открытые порты компьютера, а для безопасности сети пользователям рекомендуется закрыть доступ к этим портам с помощью брандмауэра (рис.
16).

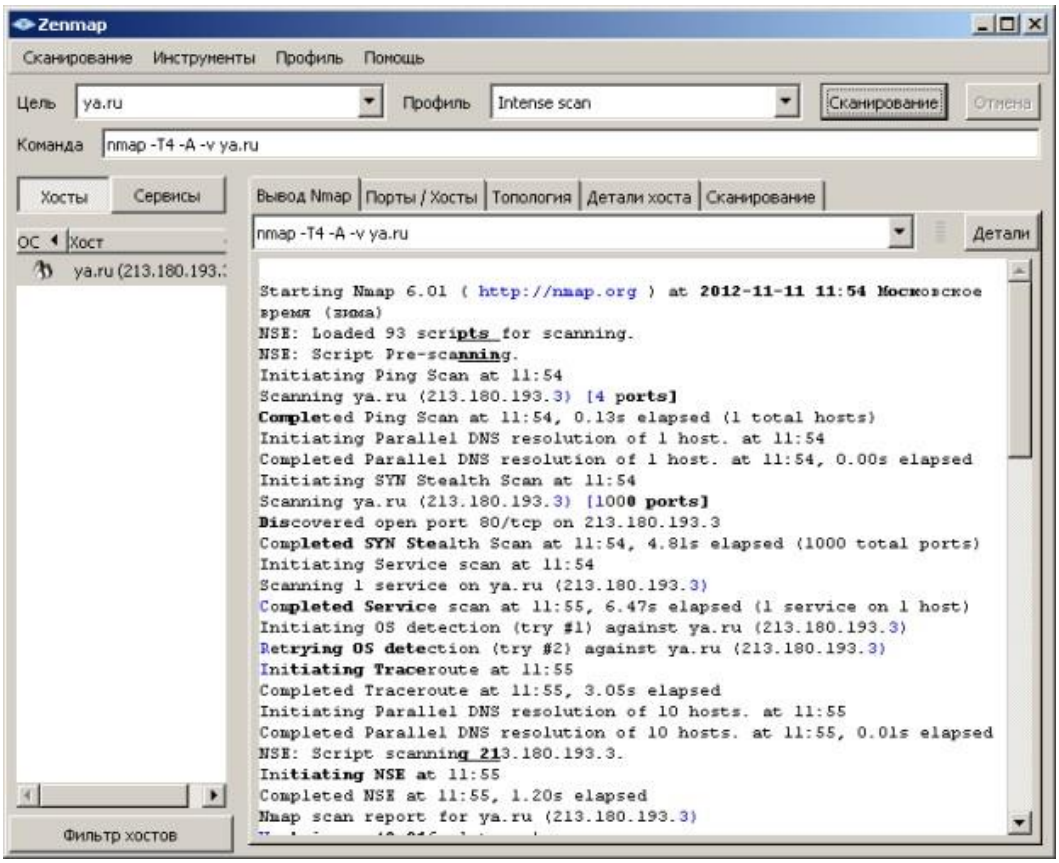


Рис. 16. Интерфейс программы Nmap

Обычно для того, чтобы просканировать все порты какого-либо компьютера в сети вводится команда **nmap –p1-65535 IP-адрес_**компьютера или **nmap –sV IP-адрес компьютера,** а для сканирования сайта — команда **nmap –sS –sV –O -P0 адрес сайта.**

Монитор портов TCPView

TCPView — показывает все процессы, использующие Интернетсоединения. Запустив **TCPView**, можно узнать, какой порт открыт и какое приложение его использует, а при необходимости и немедленно разорвать соединение – рис. 17.

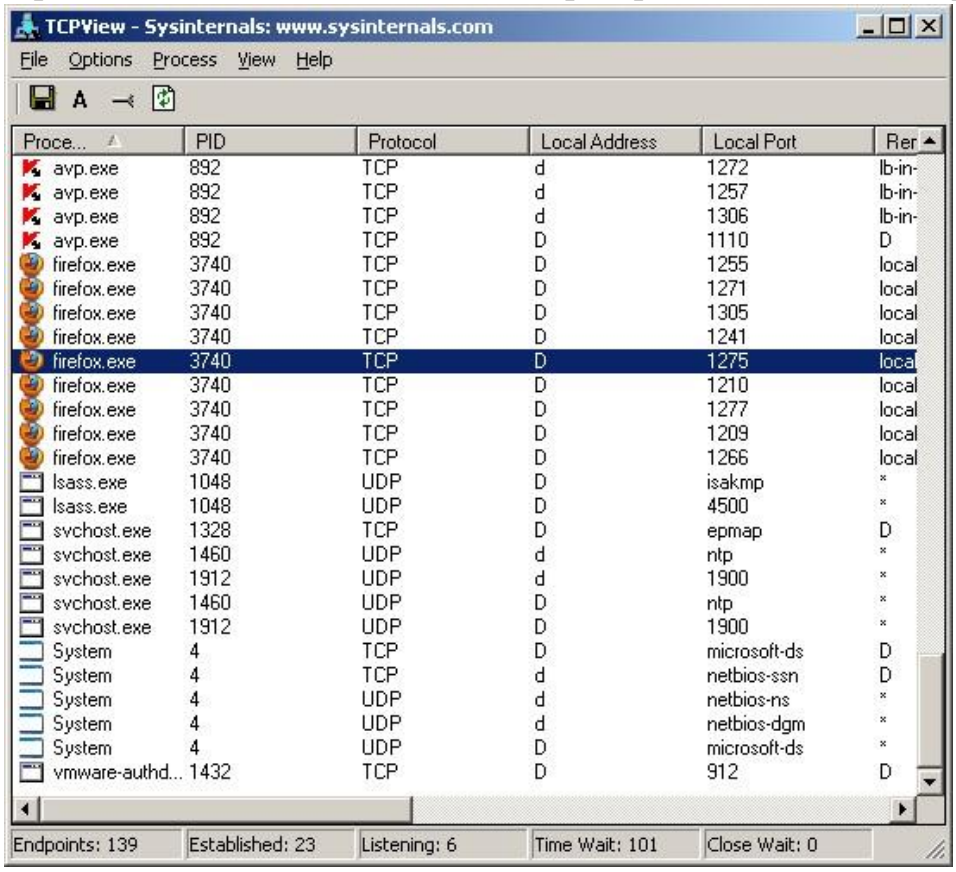


Рис. 17. Главное окно программы TCPView

Просмотрите активные сетевые подключения локального ПК с помощью монитора портов tpiview. Определите потенциально возможные угрозы (какие порты открыты, и какие приложения их используют). При необходимости можно закрыть установленное приложением TCP-соединение или процесс правой кнопкой мыши.

Оформить конспект работы в тетради

Контрольные вопросы ЛР6 (ПК-2):

1. Какие уязвимости ОС Windows были устранены в данной практической работе и какими путями?
2. Для чего используется утилита Netstat?
3. Перечислите, какие утилиты вошли в состав программы NetStat Agent? Для чего используется каждая из утилит?
4. Для чего используется программа Nmap? TCPView?