Практическая работа № 2

УСТАНОВКА, НАСТРОЙКА И ОБНОВЛЕНИЕ АНТИВИРУСНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

2 часа

1. Цель работы

1.1. Усвоить основные методы и приемы обеспечения информационной безопасности в контексте антивирусной защиты;

1.2. Усвоить приемы работы с антивирусной программой.

2. Обеспечивающие средства

2.1. Персональный компьютер;

2.2. MS Word, антивирус Касперского;

2.3. Методические указания по выполнению практической работы.

3. Задание

3.1. Изучить теоретический материал о вирусах и антивирусной защите;

3.2. Заполнить в Word таблицу классификации компьютерных вирусов;

3.3. Выполнить практические действия и ответить на вопросы, используя меню, режимы работы и справку Антивируса Касперского.

4. Общие теоретические сведения

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.

Признаки заражения:

- прекращение работы или неправильная работа ранее функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение размеров файлов и их времени модификации;
- уменьшение размера оперативной памяти;
- непредусмотренные сообщения, изображения и звуковые сигналы;
- частые сбои и зависания компьютера и др.

<u>Классификация компьютерных вирусов</u>

По среде обитания:

- сетевые – распространяются по различным компьютерным сетям;
- файловые – внедряются в исполняемые модули (COM, EXE);
- загрузочные – внедряются в загрузочные секторы диска или секторы, содержащие программу загрузки диска;
- файлово-загрузочные – внедряются в загрузочные секторы и в исполняемые модули.

По способу заражения:

- резидентные – при заражении оставляют в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения;

- нерезидентные – не заражают оперативную память и активны ограниченное время.

По воздействию:

- неопасные – не мешают работе компьютера, но уменьшают объём свободной оперативной памяти и памяти на дисках;
- опасные - приводят к различным нарушениям в работе компьютера;
- очень опасные – могут приводить к потере программ, данных, стиранию информации в системных областях дисков.

По особенностям алгоритма:

- обычные вирусы – программы, способные размножаться и внедрять свои копии в другие файлы. Вирусы заражают исполняемые файлы обычных программ и активируются при их запуске, при этом зараженный файл, перенесенный с одного компьютера на другой может его инфицировать;
- паразиты – изменяют содержимое файлов и секторов, легко обнаруживаются;
- сетевые «черви» – вредоносные программы, распространяющиеся без участия пользователя. Черви пользуются уязвимыми местами операционной системы и запущенных программ, вычисляют адреса сетевых компьютеров и отправляют по ним свои копии;
- стелсы – перехватывают обращение ОС к поражённым файлам и секторам и подставляют вместо них чистые области;
- мутанты – содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую;
- трояны – исполняемые файлы, обычно маскирующиеся под новую версию какой-нибудь популярной программы, не способны к самораспространению, но маскируясь под полезную информацию, разрушают загрузочный сектор и файловую систему;
- руткиты – программы, которые после внедрения на компьютер захватывают над ним контроль и маскируются. Компьютер, зараженный такой программой, может подолгу оставаться инфицированным, так как наличие руткита может никак не мешать работе пользователя. Такой компьютер используется злоумышленниками для рассылки спама или атаки на другие компьютеры и Интернет-сайты.

<u>Основные меры по защите от вирусов</u>

- оснастите свой компьютер одной из современных антивирусных программ: Doctor Web, Norton Antivirus, Антивирус Касперского, Nod 32 Antivirus, Microsoft Security Essentials и др.;
- постоянно обновляйте антивирусные базы;
- делайте архивные копии ценной для Вас информации на внешние носители.

Классификация антивирусного программного обеспечения

Выделяют пять групп антивирусных программ в зависимости от принципа работы:

- детекторы;
- доктора (фаги);
- ревизоры (инспекторы);
- фильтры (сторожа);
- вакцинаторы (иммунизаторы).

Антивирусы-фильтры – это резидентные программы, которые оповещают пользователя обо всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его, а также о других подозрительных действиях (например, о попытках изменить установки CMOS). При этом выводится запрос о разрешении или запрещении данного действия. К преимуществу программ этого класса по сравнению с программами-детекторами можно отнести универсальность по отношению как к известным, так и неизвестным вирусам, тогда как детекторы пишутся под конкретные, известные на данный момент программисту виды. Это особенно актуально сейчас, когда появилось множество вирусов-мутантов, не имеющих постоянного кода. Однако, программы-фильтры не могут отслеживать вирусы, обращающиеся непосредственно к BIOS, а также и BOOT-вирусы, активизирующиеся еще до запуска антивируса, в начальной стадии загрузки DOS. К недостаткам также можно отнести частую выдачу запросов на осуществление какой-либо операции: ответы на вопросы отнимают у пользователя много времени и действуют ему на нервы.

Наибольшее распространение в нашей стране получили программы-детекторы, а вернее программы, объединяющие в себе детектор и доктор. Наиболее известные представители этого класса – Aidstest, Doctor Web, Microsoft AntiVirus.

Антивирусы-детекторы рассчитаны на конкретные вирусы и основаны на сравнении последовательности кодов содержащихся в теле вируса с кодами проверяемых программ. Многие программы-детекторы позволяют также “лечить” заражённых файлы или диски, удаляя из них вирусы (разумеется, лечение поддерживается только для вирусов, известных программе-детектору). Такие программы нужно регулярно обновлять, так как они быстро устаревают и не могут обнаруживать новые виды вирусов.

Ревизоры – это программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохранённой ранее в одном из файлов данных ревизора. При этом проверяется состояние BOOT-сектора, таблицы FAT, а также длина файлов, их время создания, атрибуты, контрольная сумма. Анализируя сообщения программы-ревизора, пользователь может решить, чем вызваны изменения: вирусом или нет. При выдаче такого рода сообщений не следует предаваться панике, так как причиной изменений, например, длины программы может быть вовсе и не вирус.

К последней группе относятся самые неэффективные антивирусы – вакцинаторы. Они записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает её уже заражённой.

Сигнатура вируса – это повторяющийся участок кода.

Детекторы - выполняют поиск известных вирусов по их сигнатуре.

Доктора - поиск и лечение зараженный файлов.

Фильтры - оповещение о записи на диск.

5. Технология работы

5.1. Изучить теоретический материал о вирусах и антивирусной защите; заполнить в Word таблицу классификации компьютерных вирусов:

Признак классификации	***Виды компьютерных вирусов***
1. По среде обитания	1. 2. …

5.2. Откройте антивирусную программу, изучите интерфейс программы, ответы на вопросы представить в текстовом файле, созданном ранее:

5.2.1. Просмотрите информацию о текущих базах, выбрав раздел *ОБНОВЛЕНИЕ*. Ответьте на вопросы:

a) Дата последнего обновления.
b) Срок действия лицензии
c) Статус баз
d) Режим запуска

5.2.2. Выберите раздел *ЗАЩИТА* и ответьте, какие компоненты входят в комплексную защиту компьютер?

5.2.3. Выберите раздел слева *ПРОВЕРКА* и просмотрите:

a) Какие объекты проверяет Антивирус Касперского?
b) Может ли пользователь задавать, какие объекты следует проверять, а какие нет? Как это сделать?

5.2.4. Откройте окно *НАСТРОЙКА*, нажав на кнопку ***Настройка***, и подготовьте ответы на следующие вопросы:

a) Проверяются ли на наличие вирусов файлы, находящиеся в архивах? Где это задано?
b) Какие действия может выполнять Антивирус Касперского с инфицированными и подозрительными объектами?

5.2.5. Используйте *СПРАВКУ*, найдите информацию о защите сетевых атак и скопируйте найденную информацию в текстовый документ.

5.2.6. Выполните проверку своей папки, флешки на наличие вирусов.

5.2.7. Импортируйте отчет в текстовый файл под именем ***Отчет*** в свою папку, нажав на кнопку ***Сохранить как***.

5.2.8. Используя раздел ***Справки***, ответьте на следующие вопросы:

a) Отличие *полной проверки* от *быстрой проверки*
b) Понятие *вирусной атаки*
c) Назначение *доверенного процесса*
d) Понятие *карантина*
e) С какой целью объекты помещаются на карантин?
f) Понятие *подозрительного объекта*

6. Контрольные вопросы

1. Что такое вирус?
2. Дайте классификацию вирусов.
3. Для чего нужны антивирусные программы?
4. Дайте их классификацию.
5. Что такое сигнатура вируса?
6. Перечислите признаки заражения компьютерным вирусом.
7. Укажите последовательность действий при проверке своей рабочей папки, флешки на наличие вирусов.