Лабораторная работа №3

Тема: Основные методы применения антивирусных средств защиты информации.

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

ОСНОВНЫЕ ИСТОЧНИКИ ВИРУСОВ:

- внешние накопители, на которой находятся зараженные вирусом файлы;
- компьютерная сеть, электронная почта и Internet;

ИНТЕРНЕТ УГРОЗЫ

Перехват

Любая открытая Wi-Fi сеть - в кафе, метро, аэропорту и т.д. - позволяет «подсмотреть» данные (например, пароли от соцсетей, почтовых сервисов, интернет-банков), которые получают или отправляют люди, подключенные к той же сети.

Спам

Анонимная массовая рассылка сообщений по электронной почте, засоряющей обычные почтовые ящики. Спам чаще всего используется для рекламы товаров и услуг. Злоумышленники используют спам для проведения фишинговых атак и распространения вредоносных программ.

Фишинг

Преступники создают поддельную страницу популярного сайта или сервиса. Все логины и пароли введенные на такой фишинговой странице, отправляются злоумышленнику. Пример: обычно адреса фишинговых страниц выглядят так: www.rg.ru.id4789538765.mo. То есть начало полностью повторяет адрес знакомого сайта, в нашем примере - "Российской газеты", но после домена RU (а также .com .net или любого другого) стоит не знак "/", а "." и после нее - любое продолжение.

Зараженные страницы

Многие сайты привлекают к себе пользователей только для того, чтобы подсадить в их компьютер или гаджет вредоносный код.

Вирусы

Самая распространённая интернет-угроза — это атака вирусов. Заразиться можно, например, скачав песенку или видеоролик. В дополнение придет небольшая программа, содержащая вирус.

Компьютерный Вирус – это небольшая вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в программы (исполняемые файлы), документы, загрузочные сектора носителей данных.

Вирусный код может воспроизводить себя в теле других программ – этот процесс называется ***размножением***.

Создав достаточное количество копий, вирус может перейти к разрушительным действиям. Этот процесс называется ***вирусной атакой***.

ОСНОВНЫЕ ПРИЗНАКИ ЗАРАЖЕНИЯ КОМПЬЮТЕРА ВИРУСОМ:

- уменьшение объема свободной ОП;
- замедление загрузки и работы компьютера,
- непонятные изменения в файлах, изменения размеров и даты последней модификации файлов;
- ошибки при загрузке операционной системы;
- невозможность сохранять файлы в нужных каталогах;
- непонятные системные сообщения, музыкальные и визуальные эффекты и т.д.

В зависимости от СРЕДЫ ОБИТАНИЯ вирусы делятся на:	
Файловые (программные)	внедрены внутрь исполняемых файлов (поражают файлы с расширением .COM и .EXE).
Загрузочные	поражают не файлы, а загрузочный сектор (Boot сектора) дисков.
Макровирусы	поражают документы Word и Excel, т.к. в них есть средства для исполнения макрокоманд. Если открыть зараженный документ, не откючив исполнение макрокоманд, вирус проникает на компьютер.
Сетевые	распространяются по компьютерной сети.
Flash вирусы	поражают микросхемы Flash памяти BIOS.

По СПОСОБУ ЗАРАЖЕНИЯ среды обитания вирусы разделяются на:	
Резидентные вирусы	способны оставлять свои копии в ОП, перехватывать обработку событий (например, обращение к файлам или дискам) и вызывать при этом процедуры заражения объектов (файлов или секторов). Эти вирусы активны в памяти не только в момент работы зараженной программы, но и после. Резидентные копии таких вирусов жизнеспособны до перезагрузки ОС, даже если на диске уничтожены все зараженные файлы.
Нерезидентные вирусы	не заражают ОП компьютера и проявляют активность ограниченное время.

По СТЕПЕНИ ВОЗДЕЙСТВИЯ вирусы бывают: безвредные, опасные, очень опасные.

По ОСОБЕННОСТЯМ АЛГОРИТМА РАБОТЫ вируса:

- **Черви (сетевые) -** проникают из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии.
- **Стелс-вирусы (невидимки) -** позволяют вирусам полностью или частично скрыть свое присутствие. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат эти объекты, либо подставляют вместо себя незараженные участки информации.
- **Троянские программы -** маскируясь под полезную программу.
- **Ботнеты** (или так называемые зомби-сети) **-** создаются троянцами или другими специальными вредоносными программами и централизованно управляются хозяином, который получает доступ к ресурсам всех зараженных компьютеров и использует их в своих интересах.
- **Полиморфные вирусы** - содержащие алгоритмы шифрования основного тела вируса, их копии практически не содержат полностью совпадающих участков кода.
- **и др.**

Антивирус - это программа, выявляющая и обезвреживающая компьютерные вирусы.

ТИПЫ АНТИВИРУСОВ:

- **Сторожа (фильтры)**, которые постоянно находятся в ОП. Они проверяют попытки изменения атрибутов файлов, изменения исполняемых *.COM,* .EXE файлов, записи в

загрузочные секторы диска. Сторожа не способны лечить файлы или диски (AVP, Norton Antivirus for Windows, Thunder Byte Professional, McAfee Virus Scan).

- **Ревизоры** - они запоминают исходное состояние, а потом периодически сравнивают его с текущим. При обнаружении несоответствий (по длине файла, дате модификации тд.) выдают сообщение (Adinf).
- **Доктора - Полифаги** предназначены для обнаружения и лечения вирусов. **Фаги** – это программы, с помощью которых отыскиваются вирусы определенного вида. (MS Antivirus, Aidstest, Doctor Web).
- **Детекторы** способны обнаруживать зараженные файлы и выдавать сообщение.

Задание

Задание 1. Написать конспект по теоретической части.

Задание 2. Знакомство с Антивирусным обеспечением и утилитой согласно варианту, их письменное описание и ссылки для скачивания.

Антивирусные программы

- 1 Kaspersky Internet Security
- 2 Kaspersky Internet Security
- 3 Kaspersky CRYSTAL
- 4 Касперский Яндекс-версия
- 5 ESET NOD32 Антивирус
- 6 ESET NOD32 Smart Security
- 7 ESET NOD32 Titan
- 8 Web Security Space
- 9 Антивирус Dr.Web для Windows
- 10 avast Free Antivirus
- 11 avast Internet Security
- 12 Panda Cloud Antivirus Free
- 13 Norton AntiVirus 2013
- 14 Avira Free Antivirus
- 15 Microsoft Security Essentials
- 16 Comodo Antivirus 2013
- 17 AVG AntiVirus FREE 2014
- 18 Ad-Aware Free Antivirus+

Утилиты

- 1 Kaspersky Rescue Disk 10
- 2 Kaspersky Virus Removal Tool
- 3 Kaspersky Security Scan
- 4 ESET SysInspector 32bit
- 5 Web CureIt
- 6 Web® LiveUSB
- 7 Web LiveCD
- 8 Panda QuickRemover
- 9 avast BackUp
- 10 avast EasyPass
- 11 avast! Virus Cleaner
- 12 Avira Antivir Rescue System
- 13 Kaspersky WindowsUnlocker
- 14 Kaspersky USB Rescue Disk Maker
- 15 Trojan Remover
- 16 Trojan Killer
- 17 ESET NOD32 LiveCD
- 18 Kaspersky KidoKiller

Содержание отчета

Отчет должен содержать:

1. Название работы.
2. Цель работы.
3. Задание и его решение.

Контрольные вопросы

1. Что такое компьютерный вирус?
2. Точки проникновения вирусов в сеть.
3. На какие функции подразделяют антивирусные программы по выполняемым