Практическая работа 14

Тема: Защита информации. Антивирусная защита

Цель работы. Изучение вредоносных программ и антивирусного программного обеспечения

План

1) Изучить теоретические основы
2) Выполнить тестирование съемных носителей и локальных дисков компьютера на наличие компьютерных вирусов
3) Ответить на контрольные вопросы

Краткие сведения

Вредоносная программа — компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ресурсов системы, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы. К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Независимо от типа, вредоносные программы способны наносить значительный ущерб, реализуя любые угрозы информации — угрозы нарушения целостности, конфиденциальности, доступности.

1. Сетевые черви. К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- ✓ проникновения на удаленные компьютеры;
- ✓ запуска своей копии на удаленном компьютере;
- ✓ дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Некоторые черви обладают свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы и/или компьютерного вируса.

2. Классические компьютерные вирусы. К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- ✓ последующего запуска своего кода при каких-либо действиях пользователя;
- ✓ дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- ✓ при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- ✓ вирус скопировал себя на съёмный носитель или заразил файлы на нем;
- ✓ пользователь отослал электронное письмо с зараженным вложением.

3. Троянские программы. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети).

4. Хакерские утилиты и прочие вредоносные программы. К данной категории относятся:

- ✓ утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- ✓ программные библиотеки, разработанные для создания вредоносного ПО;
- ✓ хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- ✓ «злые шутки», затрудняющие работу с компьютером;
- ✓ программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;

✓ прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Руткит (Rootkit) - программа или набор программ, использующих технологии сокрытия системных объектов (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр.) посредством обхода механизмов системы.

В системе Windows под термином руткит принято считать программу, которая внедряется в систему и перехватывает системные функции, или производит замену системных библиотек. Перехват и модификация низкоуровневых API функций в первую очередь позволяет такой программе достаточно качественно маскировать свое присутствие в системе, защищая ее от обнаружения пользователем и антивирусным ПО. Кроме того, многие руткиты могут маскировать присутствие в системе любых описанных в его конфигурации процессов, папок и файлов на диске, ключей в реестре. Многие руткиты устанавливают в систему свои драйверы и сервисы (они естественно также являются «невидимыми»).

В последнее время угроза руткитов становится все более актуальной, т.к. разработчики вирусов, троянских программ и шпионского программного обеспечения начинают встраивать руткит-технологии в свои вредоносные программы. Одним из классических примеров может служить троянская программа Trojan-Spy.Win32.Qukart, которая маскирует свое присутствие в системе при помощи руткит-технологии. Ее RootKit-механизм прекрасно работает в Windows 95, 98, ME, 2000 и XP.

Современные антивирусные программы обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер (Интернет, локальная сеть, электронная почта, съемные носители информации). Большинство антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

Межсетевой экран — это программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа к компьютеру. Другое распространенное название сетевого экрана — файервол от английского термина firewall. Иногда сетевой экран называют еще брандмауэром (нем. brandmauer) — это немецкий эквивалент слова firewall. Основная задача сетевого экрана — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации сетевого экрана. Межсетевой экран позволяет:

✓ Блокировать хакерские атаки;
✓ Не допускать проникновение сетевых червей;
✓ Препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.

Задание.1 В операционной системе Windows проверить выбранные объекты на наличие вредоносных объектов, выполнить лечение или удаление зараженных объектов

Порядок работы

1) Запустить на выполнение антивирусную программу.
2) Запустить обновление из контекстного меню.
3) Выполнить проверку съемного носителя.
4) Выполнить проверку локального диска.
5) Отчет о работе антивирусной содержит информацию о результатах проверки.

Задание №2. Ответьте на вопросы:

Вопрос	Ответ
Что такое компьютерный вирус?	
В чем состоит принцип работы вируса?	
Перечислите вредные действия вирусов.	

Задание №3. Запишите признаки заражения ПК вирусом.

№	Признак

Задание №4. Проанализируйте и запишите, какие типы файлов подвержены заражению?

Типы файлов, подверженные заражению	Типы файлов, не подверженные заражению

Задание №5. Проанализируйте и запишите основные способы заражения ПК.

№	Способ заражения ПК
1	
2	
3	
4	

Задание №6.Запишите меры профилактики заражения ПК вирусом:

№	Способ профилактики
1	
2	
3	
4	
5	
6	

Задание №7. Запишите классификацию вирусов в виде таблицы

№	Вид (название) вируса	Особенность вируса

Задание №8. Сравните виды антивирусных программ, дайте им краткую характеристику.

№	Вид	Характеристика	Достоинства	Недостатки
1	Антивирусы-сканеры			
2	Антивирусы-мониторы			

Задание 9. Сопоставьте названия программ и изображений.
Укажите соответствие для всех 6 вариантов ответа:

1) 
2) 
3) 
4) 
5) 
6) 

__ Antivir
__ DrWeb
__ Nod 32
__ Antivirus Kaspersky
__ Avast
__ AntivirusPanda

Контрольные вопросы

1. Дайте понятие компьютерного вируса.
2. Какие угрозы информации способны нанести вредоносные программы?
3. Для чего предназначены антивирусные программы?
4. Каковы функции брандмауэра?
5. В чем разница между антивирусными сканерами и мониторами?
6. Какие существуют признаки заражения компьютерным вирусом?
7. Что необходимо сделать в первую очередь в случае заражения компьютерным вирусом?