Лабораторная работа № 13

Тема: Вирусы. Антивирусные программы

Цель работы**:** ознакомление с видами программ – вирусов, выявление способов защиты от вирусов, приобретение навыков работы с антивирусными программами.

Предварительная подготовка: спец. дисциплины «Операционные системы».

Количество часов: 2 часа

Оборудование: Персональный компьютер.

Краткие теоретические сведения

Что такое вирус?

Вирус (вирусная программа) — это, как правило, небольшая по объему последовательность программных кодов, обладающая следующими свойствами:

1. Возможность создавать свои копии и внедрять их в другие программные объекты.
2. Обеспечение скрытое (латентность) до определенного момента ее существования и распространения.
3. Несанкционированность (со стороны пользователя) производимых ею действий.
4. Наличие отрицательных последствий от ее функционирования.

Приведенные признаки, строго говоря, не являются характеристическими, так как не все программы, обычно называемые вирусами, обладают всеми из перечисленных свойств. С другой стороны, другие программы, которые обладают одним или несколькими свойствами из этого списка, также могут не являться вирусами.

Реально существует целый комплекс причин существования и развития «индустрии» вирусов. Среди основных из них следует выделить:

– причины технического характера (пробелы в защите ранних версий операционных систем, предназначенных для персональных компьютеров с ограниченными возможностями);

– причины экономического характера (допустим, борьба с конкурентами);

– причины социального и психологического характера (наличие «специалистов», обладающих профессиональной квалификацией для написания вирусов и по той или иной причине не находящих путей для конструктивной реализации своих способностей).

Классификация вирусов

Существует несколько подходов к классификации компьютерных вирусов по их характерным особенностям:

1. По среде обитания вируса
2. По способу заражения
3. По деструктивным возможностям
4. По особенностям алгоритма работ

Рассмотрим каждый подход в отдельности.

По среде обитания вирусы подразделяются на:

Файловые вирусы - вирусы поражающие исполняемые файлы, написанные в различных форматах. Соответственно в зависимости от формата, в котором написана программа это будут EXE или COM вирусы.

Загрузочные вирусы - вирусы поражающие загрузочные сектора (Boot сектора) дисков или сектор содержащий системный загрузчик (Master Boot Record) винчестера.

Сетевые вирусы - вирусы, распространяющиеся в различных компьютерных сетях и системах.

Макро вирусы - вирусы поражающие файлы Microsoft Office

Flash - вирусы - вирусы поражающие микросхемы FLASH памяти BIOS.

По способу заражения вирусы делятся на:

Резидентные вирусы - вирусы, которые при инфицировании компьютера оставляют свою резидентную часть в памяти. Они могут перехватывать прерывания операционной системы, а также обращения к инфицированным файлам со стороны программ и операционной системы. Эти вирусы могут оставаться активными в плоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы - вирусы не оставляющие своих резидентных частей в оперативной памяти компьютера. Некоторые вирусы оставляют в памяти некоторые свои фрагменты не способные к дальнейшему размножению такие вирусы считаются не резидентными.

По деструктивным возможностям вирусы подразделяются на:

Безвредные вирусы - это вирусы ни как не влияющие на работу компьютера за исключение, быть может, уменьшения свободного места на диске и объема оперативной памяти.

Неопасные вирусы - вирусы, которые проявляют себя в выводе различных графических, звуковых эффектов и прочих безвредных действий.

Опасные вирусы - это вирусы, которые могут привести к различным сбоям в работе компьютеров, а также их систем и сетей.

Очень опасные вирусы - это вирусы, приводящие к потере, уничтожению информации, потере работоспособности программ и системы в целом.

По особенностям алгоритма работы вирусы можно подразделить на:

Вирусы спутники(companion) - эти вирусы поражают EXE-файлы путем создания COM-файла двойника, и по этому при запуске программы запустится сначала COM-файл с вирусом, после выполнения своей работы вирус запустит EXE-файл. При таком способе заражения "инфицированная" программа не изменяется.

Вирусы "черви" (Worms) - вирусы, которые распостраняются в компьютерных сетях. Они проникают в память компьютера из компьютерной сети, вычисляют адреса других компьютеров и пересылают на эти адреса свои копии. Иногда они оставляют временные файлы на компьютере но некоторые могут и не затрагивать ресурсы компьютера за исключением оперативной памяти и разумеется процессора.

"Паразитические" - все вирусы, которые модифицируют содержимое файлов или секторов на диске. К этой категории относятся все вирусы не являются вирусами-спутниками и вирусами червями.

"Стелс-вирусы" (вирусы-невидимки, stealth) - представляющие собой весьма совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам дисков и ?подставляют? вместо себя незараженные участки информации. Кроме этого, такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяющие "обманывать" резидентные антивирусные мониторы.

"Полиморфные" (самошифрующиеся или вирусы-призраки, polymorphic) - вирусы достаточно трудно обнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

"Макро-вирусы" - вирусы этого семейства используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). В настоящее время наиболее распространены макро-вирусы, заражающие текстовые документы редактора Microsoft Word.

Приведенная выше классификация не может считаться полной, так как прогресс не стоит на месте, появляются всё новые и новые интеллектуальные устройства и соответственно вирусы работающие на них, например уже появились вирусы поражающие мобильные телефоны.

Аппаратные устройства — источники вирусов

Заражение компьютера происходит через устройства, позволяющие вводить информацию в компьютер:

- модем.

Интернет — основной источник распространения вирусов. Заражение происходит через копирование зараженных файлов с серверов глобальной сети, при обмене через электронную почту письмами, в которых содержатся документы формата Word, которые могут быть заражены макровирусами.

- сетевая карта.

При регистрации в локальной сети зараженной рабочей станции происходит заражение системных файлов сервера. Инфицирование незараженной рабочей станции происходит при регистрации на зараженном сервере.

- устройства хранения информации со сменными носителями.

При использовании дискет на зараженном компьютере происходит заражение дискет, с которых можно заразить любой компьютер. Встречаются зараженные диски CD-ROM, которые, как правило, содержат пиратское программное обеспечение.

Исключение составляют устройства «ручного» ввода: клавиатура, мышь и т. д.

Способы защиты от вирусов

Защитить свой компьютер от вирусных атак, сохранить конфиденциальные данные, пароли в различных сервисах, обезопасить электронные деньги помогают антивирусные программы. Сложно представить пользователя, игнорирующего правила безопасности и работающего в интернете без установленного антивируса на своем компьютере. Еще совсем недавно цели, преследуемые авторами вредоносных программ, были не настолько опасными: они вносили изменения в работу каких-то определенных программ, вызывали «подвисание» операционной системы. Сейчас же самыми частыми последствиями заражения компьютера является установка смс-баннеров, которые требуют отправить платное смс, чтобы их удалить, и кража – как платежных данных и номеров пластиковых карт, так и электронных валют. Поэтому принципы сетевой безопасности предполагают обязательную установку антивирусной программы.

Чтобы правильно выбрать антивирус, нужно определиться с тем, какие его свойства вам наиболее важны. Все антивирусные программы делятся на три вида: проактивные, сигнатурные и комбинированные. Проактивные предотвращают проникновение вредоносных программ извне, проверяя

своими алгоритмами все файлы, попадающие на компьютер. Сигнатурные проверяют текущее состояние системы, сканируют и при необходимости лечат операционную систему. Ну а комбинированные соединяют в себе обе функции и наиболее рекомендованы для максимальной защиты вашего ПК, несмотря на то, что требуют больше ресурсов. Антивирусные программы бывают платные и бесплатные. Вопрос, обязательно ли платить деньги за безопасность своих личных данных, каждый решает сам в зависимости от степени важности информации, находящейся на его компьютере, и к каким последствиям может привести проникновение на него вирусов. Платные антивирусы более надежны, к тому же обычно «в комплекте» идут консультации специалистов и помощь в подборе нужной программы и ее настроек. Продаются они в любом компьютерном магазине и на специализированных сайтах, как в комплекте программа+ключ, так и одним электронным ключом, который нужно ввести в скачанную ранее на софт-портале программу. Бесплатные лежат в свободном доступе на многих сайтах.

Важно перед установкой антивируса проверить версию операционной системы, используемой на вашем компьютере и такой параметр, как ее «битность». «Битностью» называют разрядность чисел, которая определяет возможности процессора, в современных компьютерах она равна 32 или 64. Большинство антивирусных программ созданы в двух вариантах, для 32- или 64-битных систем. Проследите за тем, чтобы версия соответствовала вашей системе, иначе возможны перебои в дальнейшей работе компьютера и самого антивируса.

Антивирус, скачанный из интернета, обычно является программой с расширением .exe. Устанавливаются такие файлы автоматически после двойного щелчка левой кнопки мыши по нему. Купленные в магазинах программы чаще всего записаны на диске и запускаются автоматически после вставки его в CD-привод. Какой бы вариант вы ни выбрали, обязательно обновите сразу после установки базу данных программы, это позволит обеспечить более качественную защиту. При выборе антивирусного обеспечения следует принимать во внимание перечень и качество предоставляемых услуг:

– возможность сканирования «на лету», когда любой объект, к которому осуществляется доступ, проверяется на наличие вируса;

– возможность сканирования по запросу, когда время и область действия антивируса определяются пользователем;

– возможность настройки антивируса в соответствии с потребностями пользователя.

Качество работы антивируса определяется его надежностью (отсутствие ошибок, зависаний и т. п.) и эффективностью (обезвреживание всех вирусов, особенно полиморфик-вирусов, отсутствие ложных срабатываний).

Антивирусные программы

Антивирусные программы условно делятся на антивирусы-фильтры, антивирусы-ревизоры, антивирусы-вакцинаторы.

Антивирусы-фильтры или сторожа

Антивирус-фильтр есть практически на каждом компьютере - это брандмауэр.

Кроме этого существуют программы, которые уведомляют пользователя обо всех действиях на его ПК. Если троянская программа или вирус захотят проникнуть в вашу систему, или выкрасть пароль и отправить его злоумышленнику, сторож мгновенно выдаст на экран запрос: «Разрешить или запретить выполнение операции?».

К сожалению, работа с данным типом защиты требует определённых навыков, ведь не каждый пользователь знает, что обозначает тот или иной процесс. Вдруг это Windows вздумала обновиться, а сторож её фильтрует?

Антивирусы-детекторы

В странах СНГ получили наибольшее распространение: антивирус Касперского, AVAST, Doctor Web, AVIRA, Eset Smart Security (NOD32), AVIRA, COMODO – это неполный список популярных программ-детекторов.

Данный тип антивирусов нужно регулярно обновлять, потому что вредоносные программы быстро мутируют и размножаются. Какой антивирус-детектор лучше – не знает никто, хотя в интернете можно найти многочисленные тесты и сравнительные обзоры антивирусов. И дело не в стоимости, стране-производителе или размере баз для обновления. Немецкий у вас антивирус, чешский или российский – просто почаще обновляйте его и не забывайте продлевать лицензию! Хотя многие антивирусы можно скачать на свой комп и бесплатно.

Вакцинаторы

Уже заражённые компьютеры сложно вылечить с помощью обычного детектора и уж тем более фильтра. В очень тяжёлых случаях на помощь приходят программы-вакцинаторы: антитрояны, антишпионы и прочее. Вакцина в данном случае бывает двух типов: пассивная и активная. Даже если у вас стоит дорогой лицензионный антивирус, он не всегда может справиться с червём или троянской программой. К числу наиболее популярных вакцинаторов относятся – Anti Trojan Elite, Trojan Remover или

Dr.Web CureIt. Последний, кстати, лечит практически любую инфицированную систему, но для регулярной защиты ПК его недостаточно.

Какой антивирус выбрать?

Рассмотрим выбор антивируса на примере трех производителей таких популярных антивирусных средств как: Kaspersky Internet Security, Dr. Web Security Space, ESET Smart Security.

Наиболее простой способ состоит в определении ключевых различий между рассматриваемыми антивирусами. Например, если требуется функция “родительский контроль”, то рассматривать стоит только Kaspersky Internet Security и Dr. Web Security Space Pro. Но широкий функционал означает увеличенную нагрузку на систему, поэтому при не востребованности дополнительных опций можно остановиться на ESET. Ниже приводятся удобные таблицы сравнения антивирусов, а также таблицу с кратким описанием основных модулей таких программ, ведь для человека, далёкого от информационных технологий, названия компонентов вирусной защиты могут ничего не сказать.

Антишпион	Блокирует кражу персональных данных, различные перехватчики паролей, номеров кредитных карт.
E-mail сканер	Проверяет электронные письма в специализированных почтовых программах (Outlook, The Bat, Thunderbird и т.д.)
Антиспам	Останавливает письма, содержащие нежелательную рекламу.
Антируткит	Обнаруживает и удаляет замаскированные вредоносные программы.
Брандмауэр	Блокирует нежелательные сетевые соединения.
Родительский контроль	Позволяет ограничить ребёнку доступ к нежелательным ресурсам в сети Интернет. Дополнительно можно управлять временем работы детей за компьютером, с конкретными программами.
Веб-антивирус	Проверка интернет-страниц на вирусы и вредоносные скрипты.
Защита от фишинга	Программа блокирует фальшивые зловредные сайты, копирующие внешний вид популярных страничек в сети Интернет.
Игровой профиль	Особый режим работы, при котором антивирус минимизирует своё влияние на быстродействие игр, а также не мешает различными всплывающими уведомлениями.
Гаджет рабочего	Монитор активности, устанавливаемый на боковую панель

стола	в операционных системах Windows Vista и Windows 7.
Эвристический анализ	Способность находить новые вирусы, еще не попавшие в базы обновлений.

Для компьютеров, подключённых к сети:

Функции	Kaspersky Internet Security 2011	Dr. Web Security Space Pro	ESET Smart Security 4
Антишпион	+	+	+
E-mail сканер	+	+	+
Антиспам	+	+	+
Антируткит	+	+	+
Брандмауэр	+	+	+
Родительский контроль	+	+	—
Веб-антивирус	+	+	+
Защита от фишинга	+	+	+
Игровой профиль	+	—	—
Гаджет рабочего стола	+	—	—
Эвристический анализ	+	+	+

Для компьютеров, не подключённых к сети:

Функции	Антивирус Касперского 2011	Антивирус Dr. Web Pro	ESET NOD32 Antivirus 4
Антишпион	+	+	+
E-mail сканер	+	+	+
Антиспам	—	—	—
Антируткит	+	+	+
Брандмауэр	—	+	—
Родительский контроль	—	—	—
Веб-антивирус	+	—	+
Защита от фишинга	—	—	+
Игровой профиль	+	—	—
Гаджет рабочего стола	+	—	—
Эвристический анализ	+	+	+

Задание

Самостоятельно изучить материал, законспектировать и ответить на вопросы теста (см. Приложение 3).

Отчет должен содержать:

1. Название, цель, задание лабораторной работы;
2. Ответы на контрольные вопросы

Контрольные вопросы

1. Что такое «вирус», «антивирус»?
2. Каковы причины развития индустрии вирусов?
3. Как классифицируются вирусы?
4. Какие существуют разновидности антивирусных средств?
5. Как выбрать антивирусное средство?
6. Как избежать заражения вирусом?
7. Каковы способы проникновения вирусов в ПК?