Итоговый индивидуальный проект

Направление: Физико-математическое

Тема: «Способы защиты от компьютерных вирусов»

Выполнил: _____

Руководитель проекта: _____

_____ год

Содержание

Введение

В настоящее время компьютер имеет широкие сферы применения. Его можно использовать для вычислений, развлечения, учёбы, работы. Компьютеры используются в стратегической обороне стран, в различных отраслях науки и т.д.

Актуальность: каждый год миллионы компьютеров подвергаются заражению компьютерными вирусами. Следовательно, необходимо знать, как защитить свой компьютер.

Цель: рассмотреть способы защиты системы от вредоносного ПО на примере виртуальных машин с установленной на них ОС Windows 10.

Для достижения цели были решены следующие задачи:

- изучение структуры компьютерных вирусов;
- изучение принципа работы компьютерных вирусов;
- классификация компьютерных вирусов по разным критериям;
- выработка способов защиты от компьютерных вирусов.

В результате работы над проектом «Способы защиты от компьютерных вирусов» были сделаны виртуальные машины, призванные продемонстрировать последствия заражения вирусом и некоторые способы защиты от них.

Глава 1

Компьютерные вирусы

1.1 Что такое «компьютерные вирусы»

Компьютерный вирус — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи. Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов, удаление операционной системы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

В настоящее время не существует единой системы классификации и именования вирусов, однако вирусы принято разделять:

- по поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);
- файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
- по поражаемым операционным системам и платформам (DOS, Windows, Unix, Linux, Android);
- по используемым технологиям (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты, шифровальщики и др.).

В обиходе «вирусами» называют всё вредоносное ПО, хотя на самом деле это лишь один его вид.

1.2 Структура вирусов, способы заражения

Вирус чаще всего состоит из двух частей: голова и хвост. Такие вирусы называют сегментированными. В случае, если вирус состоит только из одной части (головы) его называют несегментированным.

Способов заражения также довольно много, основные из них:

1. Через электронные письма (при открытии письма или вложения будет установлено вредоносное ПО, например, вирус ILOVEYOU).
2. Через Microsoft Office (а именно через макросы, в которых содержится вредоносный код).
3. Заражённые съёмные носители информации (USB устройства, SD карты, CD/DVD диски, дискеты) (при подключении вредоносный файл «перепрыгивает» на компьютер).
4. Через исполнительные файлы (.exe) с другими программами (при открытии файла активируется вредонос).
5. Взломанные веб-страницы (при заходе на страницу устанавливается вредонос).
6. Дистанционный взлом через уязвимости ОС (например, EternalBlue, позволявшая дистанционно и, что самое страшное, незаметно, заражать компьютер, и из-за которой произошла эпидемия WannaCry) .

1.3 Способы защиты от вирусов

Способов защиты от вирусов тоже существует немало:

1. Не открывать электронные письма от незнакомых отправителей и незнакомые вложения (даже если в заражённом письме нет вложений, оно всё равно способно заразить ваш компьютер)
2. Использование антивирусного ПО (особенно актуально для Linux и всех Windows до 10-той (т.к. в десятке появился Windows Defender))
3. Не используйте учётную запись с правами администратора на постоянной основе (изменение системных файлов требует прав администратора)
4. Если вы знаете, какие файлы перезаписывает вирус, эпидемия которого сейчас идёт поставьте на них атрибут «только чтение», это не даст вредоносу перезаписать ключевой для его работы файл, в результате чего он не будет работать)
5. Не открывайте файлы из неизвестных источников, или проверяйте их антивирусом или на сайте virustotal.com
6. Можно установить ОС на другой системный диск (например не C а F). Поможет от самых серьёзных вирусов, так как в них вручную прописан путь к файлу (Например, у вируса BadRabbit прописан путь C:\Windows\System32\rundll32.exe)

К сожалению, люди часто пренебрегают простыми правилами, в результате чего

Глава 2

Ход Работы

Изучив всю предоставленную мне информацию, я принялся за работу. Сначала следовало выбрать программу, в которой будут созданы виртуальные машины. Выбор пал на VMware Workstation Pro 7. Почему? Она наиболее удобна в использовании, к тому же, мне уже приходилось работать в ней, и я имел некоторое представление, что несколько облегчило задачу.

Далее нужно было определиться, какую операционную систему я буду использовать в своих виртуальных машинах. Выбор был нетрудным – Windows 10. Почему? «Десятка» - самая ходовая ОС на данный момент, к тому же в ней есть встроенный антивирус.

Всего в проекте задействовано три виртуальные машины. Одна – не защищённая, для демонстрации последствий заражения. Две другие – для показа способов защиты от вирусов: одна специально настроенная, другая с антивирусом.

Вывод

В ходе работы над проектом, были созданы виртуальные машины. Их можно использовать для наглядной демонстрации последствий заражения вирусами и способов защиты от них для любой аудитории (например, для школьников на уроках информатики).

После анализа антивирусных программ, можно определить три лучших **бесплатных** антивируса на 2023 год это:

1. Bitdefender (актуальная база данных и малая нагрузка на устройство)
2. Avira (чуть менее богатая база данных, но более богатый инструментарий)
3. Panda Free Antivirus for Windows (неплохая защита, но хуже чем у представленных выше вариантов)

Стоит напомнить, что человек должен внимательно проверять файлы и письма, прежде чем открыть их. Если же он бездумно открывает неизвестные файлы, скачанные из подозрительных источников, то ему не поможет никакой антивирус.

Использованная литература

1. Интернет-безопасность: что это и как сохранить безопасность в сети?/ [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-internet-security?ysclid=lfy8lxpllv788623051

2. Угрозы в сети Интернет [Электронный ресурс] – Режим доступа: https://safe-surf.ru/users-of/article/212/?ysclid=lfy8o2ixfm127401182 (дата обращения: 26.11.2022).

3. Босова Л.Л. Информатика. Базовый уровень 9 класс : учебник / Л.Л. Босова, А.Ю. Босова - : БИНОМ. Лаборатория знаний, 2019