МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им В.Г.ШУХОВА»
(БГТУ им. В.Г.Шухова)

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

Расчётно-графическое задание
дисциплина: Информатика
тема: «Компьютерные вирусы, их свойства и классификация»

Выполнил: ст.группы ПВ-201
Машуров Дмитрий Русланович
Проверил: Бондаренко Т.В.

Белгород 2020

Содержание

ВВЕДЕНИЕ

Постановка темы

С приходом 21 века в нашу жизни постепенно проникали различные бытовые устройства, облегчающие жизнь человека: холодильник, микроволновая печь, стиральная машина, телефон... Но самым главным из этих изобретений был компьютер.

Согласно определению, **компьютер** — устройство или система, способная выполнять заданную, чётко определённую, изменяемую последовательность операций [1].

Появление компьютера в несколько раз облегчило жизнь человека. Он помогает нам в различных областях деятельности - от набора текста до моделирования математических и физических расчётов.

Но, к сожалению, вместе с появлением компьютеров пришли люди, которые начали пользоваться данным изобретением в корыстных целях. Они крадут деньги и конфиденциальную информацию, выводят из строя банковские системы. Делают они это с помощью вредоносных программ, нызываемых **вирусами**.

Актуальность темы

Актуальность данной темы объясняется тем, что с появлением компьютеров и телефонов люди стали хранить практически всю информацию на них. А это в свою очередь очень выгодно мошенниками, которые с помощью компьютерных вирусов проникают на устройства своих жертв и крадут важные данные: адреса, номера телефонов, пароли от аккаунтов, личную информацию.

Но что вообще такое компьютерный вирус? Как он попадает к нам на компьютер и самое главное - как от него защититься?

ОСНОВНАЯ ЧАСТЬ

Что такое компьютерный вирус

Согласно определению, **компьютерный вирус** - вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, и распространять свои копии по каналам связи.

Основная задача вируса - его ***распространение***.

Помимо кражи данных, компьютерные вирусы также могут нарушать работу компьютера путём:

- изменения названия или подмена расширения файлов (например, все файлы *.exe* меняются на *.jpg*)
- заполнения оперативной и встроенной памяти
- повреждения системно-важных частей
- аппаратного нарушение работы компьютера (увеличение температуры ЦП и ГП, снижение скорости вращения кулеров и т.д.)
- шифрования всей информации на компьютере

Классификация компьютерных вирусов

В настоящее время специалисты по компьютерной вирусологии ещё не выработали единую классификацию для вирусов. Но всё же можно выделить несколько пунктов по которым мы сможем систематизировать их [4].

Компьютерные вирусы различаются по:

- Операционной системе
- Среде обитания
- Способу заражения
- По «опасности» вируса
- Способу заражения файлов

Далее разберём каждый из вышеуказанных пунктов отдельно.

Операционная система

На данный момент существуют несколько операционных систем: Windows, macOS и Linux - для компьютеров, Android и iOS - для мобильных устройств. И поскольку архитектуры у этих систем совершенно разные, то и вирусы для этих ОС разные и работают по-разному.

Среда обитания

Под «средой обитания» понимается то, куда внедряется вирус. По среде обитания разделяют на:

- Файловые вирусы

  Попадая на устройство, внедряется в различные файлы операционной системы этого устройства [5].

- Загрузочные вирусы

  При попадании на устройство выделяют место на компьютере, недоступное для поиска, и при каждом запуске ОС, запускают себя [6].

- Макро-вирусы

Встроены в графические и текстовые системы обработки (например, MS Word) [7].

- Скрипт-вирусы

  Находясь в уязвимом месте программы, заставляют её совершать несвойственные ей действия [8].

Способ заражения

Под способом заражения понимается то, каким образом вирус заражает устройства. Различают:

- Резидентные вирусы

  При попадании на устройство оставляют свою резидентную часть в памяти и остаются активным от включения до выключения устройства.

- Нерезидентные

  Данный тип оставляет на устройстве нерезидентную часть, не способную к размножению.

«Опасность вируса»

Под «опасностью» имеется ввиду, какой вред может причинить вирус устройству. По данному пункту различают:

- Неопасные вирусы

  Данные вирусы зачастую направлены на заполнение памяти компьютера, поэтому их ущерб минимален.

- Безвредные вирусы

  Данные вирусы заполняют как встроенную, так и оперативную память, заставляя устройство работать чуть медленнее обычного, но никакого сильного влияния на работу устройства не оказывают.

- Вредные

  Данные вирусы уже могут причинять более существенный вред компьютеру помимо потребления ресурсов устройства.

- Опасные

  Данные вирусы являются самыми опасными, потому что их воздействие на устройство может привести к потере данных и программ.

Способ заражения файлов

Под способом заражения имеется ввиду, каким образом вирус внедряется в файлы на устройстве.

Перезаписывающие

Вирус полностью перезаписывает свой код вместо кода заражённого файла. Естественно, что файлы не подлежат восстановлению. Обнаруживаются из-за нарушения работы операционной и файловой систем из-за отсутствия необходимых компонентов, которые были перезаписаны.

Паразитические

Вирусы, распространяясь на устройстве, внедряются в файлы путём изменения содержимого файлов. Однако работоспособность файлов остаётся такой же или немного ухудшается. Основные типы таких вирусов:

- внедряющиеся в начало

  Вирус помещается в начало файла, тем самым запускаясь первее, чем код основной программы.

- внедряющиеся в середину

  Аналогично помещению в начало или конец кода. Некоторые вирусы при этом могут компрессировать переносимый блок файла без изменения длины.

- внедряющиеся в конец

  Вирус помещается в конец файла, тем запускаясь в последнюю очередь.

Разновидность вирусов

Вирусы различаются по своим целям и способам проникновения в компьютеры жертв. Одни заполняют память компьютера, заставляя его работать медленнее, а другие позволяют иным вирусам проникнуть на устройство незамеченными. Разберём некоторые из них:

Черви

Цель данного вируса - заполнение памяти компьютера различным «мусором» с целью замедлить его работу. Может размножаться, но при этом не является частью како-либо программы. [12].

Троян

Цель - проникновение на устройство для дальнейшей кражи данных. Попадает на устройство в виде программного обеспечения или его компонента. Начинает свою работу только при запуске самого программного обеспечения, поэтому до запуска нанести вред ***не может***. [13]

Бэкдор (программа-шпион)

Бэкдор *(от англ. backdoor - чёрный вход)* - алгоритм, дающий злоумышленникам удалённо управлять устройством жертвы. **Цель** - кража конфиденциальной информации, а также дальнейшее проникновение. На-

пример, дроппер на компьютере работника какой-либо фирмы позволяет получить доступ к системе этой фирмы. [9]

Эксплойт

Эксплойт *(от англ. exploit - эксплуатировать* - программы, использующие уязвимости программ для проникновения на устройство жертвы. **Цель** - получение доступа к устройству с последующей кражей конфиденциальных данных. [10]

Дроппер

Дроппер *(от англ. dropper - «бомбосбрасыватель»)* - программа (семейства троянов), предназначенная для скрытой установки других, более опасных вирусных программ. **Цель** - установка других вредоносных программ без возможности обнаружения. [11]

Обнаружение вирусов и методы защиты против них

Как понять, что ваш компьютер заражен вредоносной программой? Обнаружить это можно по следующим признакам:

- неправильное поведение ранее корректно работающих программ
- сильное замедление работы компьютера

- операционная система загружается с ошибками или не загружается вообще
- искажение файлов, изменение их размеров или увеличение их количества в памяти
- уменьшение количества свободной оперативной памяти
- сбои в работе компьютера
- аномальное повышение температуры компонентов компьютера

Итак, вы заметили, что несколько признаков из данного списка присутствуют на вашем компьютере. Теперь нужно понять как избавиться от «зловреда».

Ни в коем случае не нужно самостоятельно пытаться найти и удалить данную программу - это не поможет. В настоящее время от вирусов нельзя избавиться простым удалением. Нужна более глубокая чистка компьютера - от файловой системы до реестра. С этим могут справиться только **антивирусные программы**.

Они так же, как и вирусы, имеют несколько разновидностей [14]. Каждая предназначена для определённой задачи. Существуют:

- программы-детекторы
- программы-доктора
- программы-ревизоры

- программы-фильтры
- программы-вакцины

Разберём каждую из них отдельно.

Программы-детекторы

Осуществляют поиск вируса по его **сигнатуре**.

Согласно определению, **сигнатура вируса** - характерные признаки вируса, используемые для его обнаружения. Этими признаками может быть как строки кода, последовательность байтов вируса, так и его поведение на устройстве [3].

Программы-доктора

Находят и лечат заражённые файлы, возвращая их в первоначальное состояние. Сначала ищут вредоносное ПО в оперативной памяти, затем ищут в файлах, хранящихся в памяти устройства

Программы-ревизоры

Они запоминают первоначально-зафиксированные параметры файлов на устройстве и периодически сверяют текущее состояние с исходным с це-

лью обнаружить изменения, которые внёс вирус. Параметры, фиксирующиеся программой-детектором:

- длина
- вес
- *контрольная сумма*
- дата, время модификаций
- др. параметры

Согласно определению, **контрольная сумма** - некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении [2].

Программы-фильтры

Следят за действиями, которые происходят на устройстве, и фиксируют подозрительные операции. Если совершённая операция показалась программе странной и пользователь не знал о ней, то фильтр блокирует выполнение операции, а пользователь в свою очередь узнаёт о присутствии вируса.

Программы-вакцины

Полностью предотвращают распространение вируса и применяются в тех случаях, когда нет программ-докторов, способных избавится от вируса.

Защита от вирусов

Чтобы устройство снова не подверглось **вирусной атаке**, нужно соблюдать некоторые правила:

1. Установить на своё устройство антивирусную программу
2. Перед считыванием информации с флешки или диска всегда проверять их на наличие вирусов
3. При разархивации различных файлов, проверять архивы на наличие вирусов
4. Периодически проверять жёсткие диски на наличие зловреда
5. Проверяйте все скачиваемые с Интернета файлы, так как именно оттуда чаще всего можно получить вредоносную программу
6. Регулярно делать резервную копию важных данных

Соблюдение данных правил не даёт гарантию защиты от вредоносных программ, но значительно снижает шанс их проникновение на устройство.

ЗАКЛЮЧЕНИЕ

История приводит нам много случаев угрозы информационным ресурсам. Число вирусов, как и их опасность, растёт. Алгоритмы программ становятся сложнее, их труднее обнаружить и избавиться от них. И в связи с этим разработчикам антивирусных программ приходится подстраиваться под различные ситуации и совершенствовать антивирусные программы.

Список литературы

[1] Wikipedia // Компьютерный вирус // Ссылка на источник

[2] Wikipedia // Контрольная сумма // Ссылка на источник

[3] TCI (Технический центр Интернет) // Сигнатура вируса // Ссылка на источник

[4] TADVISER // Классификация вирусов // Ссылка на источник

[5] ДиалогНаука // Файловый вирус // Ссылка на источник

[6] ДиалогНаука // Загрузочный вирус // Ссылка на источник

[7] Wikipedia // Макровирус // Ссылка на источник

[8] VUZLIT // Скрипт-вирус // Ссылка на источник

[9] Wikipedia // Бэкдор // Ссылка на источник

[10] Wikipedia // Эксплойт // Ссылка на источник

[11] Wikipedia // Дроппер // Ссылка на источник

[12] Wikipedia // Червь // Ссылка на источник

[13] Wikipedia // Троян // Ссылка на источник

[14] Wikipedia // Антивирусы // Ссылка на источник