Частное учреждение образовательная организация высшего образования

"Омская гуманитарная академия"

КОНТРОЛЬНАЯ РАБОТА

на тему:

Компьютерные вирусы. Основные понятия и классификация

по учебной дисциплине: Информатика

Выполнил(а):

Направление подготовки:

Форма обучения: заочная

Оценка:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Подпись Фамилия. И.О.

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_г.

Омск, 2018

Оглавление

[1 Компьютерные вирусы. Основные понятия 3](#_Toc531209710)

[1.1 Понятие «компьютерный вирус», виды и признаки вредоносного воздействия компьютерных вирусов 3](#_Toc531209711)

[1.2 Классификация компьютерных вирусов 5](#_Toc531209712)

[2 Методы защиты от компьютерных вирусов 9](#_Toc531209713)

[2.1 Классификация методов защиты 9](#_Toc531209714)

[2.2 Программные меры защиты от компьютерных вирусов 9](#_Toc531209715)

[2.3 Методы обнаружения компьютерных вирусов 12](#_Toc531209716)

[Заключение 14](#_Toc531209717)

[Список использованных источников 15](#_Toc531209718)

1 Компьютерные вирусы. Основные понятия

1.1 Понятие «компьютерный вирус», виды и признаки вредоносного воздействия компьютерных вирусов

Компьютерный вирус – программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии, внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе на компьютере.

Таким образом, компьютерные вирусы – это вредоносные программы, внедряемые в другие программы с целью выполнения вредоносных действий.

Компьютерные вирусы во многом сходны с биологическими вирусами: способны размножаться, имеют высокую скорость распространения, обладают избирательность поражаемых систем, достаточно высокой сложностью борьбы с ними.

Компьютерные вирусы проходят следующие этапы в своем жизненном цикле:

* внедрение;
* инкубационный период (необходим для скрытия источника проникновения);
* размножение (вирусный код воспроизводит себя в теле других программ);
* выполнение деструктивных функций.

Некоторые вирусы инфицируют файлы загрузки системы, другие специализируются на различных программных файлах. Всякий раз, когда пользователь копирует файлы на машинный носитель информации или посылает инфицированные файлы по сети, переданная копия вируса пытается скопировать себя на новый диск.

Некоторые вирусы разрабатываются так, чтобы они появлялись, когда происходит некоторое событие вызова: например, пятница 13-е, 26 апреля, другая дата, определенное число перезагрузок зараженного или какого-то конкретного приложения, процент заполнения винчестера и т. д.

Компьютерные вирусы способны выполнять различные деструктивные действия, например, демонстрировать визуальные и звуковые эффекты, осуществлять воздействие на файлы, изменять содержимое секторов диска, выполнять воздействие на базы данных, на аппаратное обеспечение компьютера, на систему в целом,  получать несанкционированный доступ и похищение информации, компрометировать и провоцировать пользователя.

После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и ее работа некоторое время не отличается от работы незараженной.

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователь часто не замечает, что его компьютер заражен и не успевает принять соответствующих адекватных мер.

Существуют очевидные признаки, свидетельствующие о заражении компьютера вирусами:

* на экран выводятся непредусмотренные системой сообщения или изображения;
* подаются непредусмотренные системой звуковые сигналы;
* неожиданно открывается и закрывается лоток CD-ROM-устройства;
* произвольно, без участия пользователя, на компьютере запускаются программы;
* на экран выводится предупреждение о попытке какой-либо из программ компьютера соединится с Интернетом, хотя пользователь никак не инициировал такое ее поведение (при наличии установленной на вашем компьютере соответствующей антивирусной программы).

Существуют и косвенные признаки заражения вашего компьютера:

* частые зависания и происхождение сбоев в работе компьютера;
* замедленная работа компьютера при запуске программ;
* невозможность загрузки операционной системы;
* исчезновение файлов и каталогов или искажение их содержимого;
* частое обращение к жесткому диску, когда часто мигает лампочка на системном блоке.

1.2 Классификация компьютерных вирусов

Компьютерные вирусы можно классифицировать по признакам: среда обитания; способ заражения; степень воздействия; особенности алгоритма работы.

Рассмотрим подробнее каждую из представленных групп вирусов.

1. По среде их обитания компьютерные вирусы делятся на файловые или программные, загрузочные, макровирусы и сетевые вирусы (рисунок 1).

Сетевые вирусы попадают в компьютер по локальным и глобальным сетям.

Файловые вирусы внедряются в исполняемые модули программ, то есть в файлы с расширениями СОМ и ЕХЕ.

Загрузочные вирусы внедряются в загрузочные сектора диска или сектора, содержащие с программой загрузки системного диска.

Файлово–загрузочными вирусами заражаются файлы и загрузочные сектора дисков.

 Рисунок 1 – Классификация компьютерных вирусов по среде их обитания

2. По способу заражения компьютерные вирусы делятся на:

* резидентные, попадающие в оперативную память компьютера и, находясь в памяти, проявляющие активность вплоть до выключения или перезагрузки компьютера;
* нерезидентные, не внедряющиеся в память и активные только на время выполнения компьютером определенных задач.

3. По степени воздействия компьютерные вирусы делятся на безвредные, неопасные, опасные и очень опасные (рисунок 2).

Неопасные вирусы не мешают стабильной работе компьютера. Опасные  вирусы приводят к различного рода нарушениям в работоспособности компьютера. Очень опасные  вирусы приводят к потере программ, уничтожению конфиденциальных данных и все информации на компьютере, стиранию информации в системных разделах диска.

Рисунок 2 – Классификация компьютерных вирусов по степени воздействия

4. По особенностям алгоритма работы выделяют следующие вирусы, (рисунок 3):



Рисунок 3 – Классификация компьютерных вирусов по особенностям алгоритма работы

* компаньон – вирусы, суть работы которых заключается в том, что ими создаются файлы-спутники для ЕХЕ – файлов, обладающие тем же самым именем, но имеющие расширение СОМ. При запуске файла такого рода DOS первым обнаруживает и выполняет файл с расширением СОМ, то есть вирусный файл, который затем запускает и файл с расширением ЕХЕ;
* вирусы – «черви» – разновидность компаньон – вирусов. Вирусами – че6рвями не связываются их копии с какими-то файлами. Ими создаются собственные копии на дисках и в подкаталогах дисков, причем другие файлы никак не изменяются и не используется СОМ – ЕХЕ прием, используемый компаньон – вирусом;
* «паразитические», к которым относятся все вирусы, обязательно изменяющие при распространении своих копий содержимое дисковых разделов или файлов (все вирусы, кроме «червей» и «компаньон – вирусов»;
* «стелс» – вирусы (невидимые вирусы), представляющие собой программы, перехватывающие обращения DOS к пораженным файлам или секторам дисков и подставляющие вместо себя незараженные участки информации. Вирусы – невидимки при обращении к файлам используют оригинальные алгоритмы, позволяющие обходить антивирусные программы;
* полиморфные– вирусы (вирусы-призраки или самошифрующиеся вирусы), являющиеся трудно обнаруживаемыми, не обладающие ни одним постоянным участком кода. Два экземпляра одного и того же полиморфного вируса не будут иметь совпадений. Это достигается за счет шифрования основного тела вируса и модификации программы-расшифровщика;
* Макро – вирусы, использующие возможности макроязыков (например, Basic), встроенных в системы обработки данных (текстовые редакторы, электронные таблицы, СУБД и т.д.). На сегодняшний день широкое распространение получили макро – вирусы, заражающие документы текстового редактора Microsoft Word и электронных таблиц Microsoft Excel;
* сетевые вирусы или сетевые черви, распространяющиеся в компьютерных сетях и, точно так же, как компаньон – вирусы, не изменяющие файлы или сектора дисков. Такие вирусы проникают через компьютерные сети, вычисляя сетевые адреса других компьютеров и рассылая по ним свои копии. Такими вирусами иногда создаются рабочие файлы на дисках системы, но они могут вообще не обращаться к ресурсам компьютера (исключение составляет оперативная память).

2 Методы защиты от компьютерных вирусов

2.1 Классификация методов защиты

Компьютерные вирусы были и остаются одним из распространенных причин потери информации. Особенную опасность компьютерные вирусы представляют при работе с локальными и глобальными сетями.

Защита от компьютерных вирусов является комплексной задачей и включает в себя:

* юридические меры защиты от компьютерных вирусов. Для успешной борьбы с распространением вирусов и других типов вредоносных программ в нашей стране необходимо совершенствовать отечественное законодательство в этой области. Создание и распространение вредоносных программ преследуется в России согласно Уголовному Кодексу РФ (глава 28, статья 273);
* административные и организационные меры защиты от компьютерных вирусов на современном этапе являются более действенными. Они заключаются в составлении четких планов профилактических мероприятий и планов действия на случай возникновения заражений;
* программно-аппаратные меры защиты основаны на использовании программных антивирусных средств и специальных аппаратных средств (специальных плат), с помощью которых производится контроль зараженности вычислительной системы, контроль доступа, шифрование данных и регистрация попыток обращения к данным.

2.2 Программные меры защиты от компьютерных вирусов

Самым эффективным способом борьбы с вирусами является применение специальных программ, способных распознавать и обезвреживать вирусы в файлах и других объектах. Программы такого рода называются антивирусными.

Ранние версии антивирусных программ по выполняемым ими функциям подразделялись на:

1. Программы – детекторы, осуществляющие поиск характерной для конкретного вируса сигнатуры в оперативной памяти и файлах и при обнаружении выдающие соответствующее сообщение. Недостатком программ – детекторов является то, что ими находятся только те вирусы, которые известны разработчикам антивирусных программ.

2. Программы – доктора или флаги, которыми не только находятся зараженные файлы, но и возвращаются файлы в исходное состояние. В начале своей работы программы – доктора ведут поиск вирусов в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов.

3. Программы – ревизоры, которыми запоминается исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивающие текущее состояние с исходным.

4. Программы – фильтры или сторожа, представляющие собой небольшие резидентные программы, которые предназначены для обнаружения подозрительных характерных для вирусов воздействий при работе компьютера:

* попытки изменения файлов с расширениями СОМ и ЕХЕ;
* попытки изменения атрибутов файла;
* прямая запись на диск через абсолютный адрес;
* запись в загрузочный сектор диска;
* загрузка резидентной программы.

При попытке вирусной атаки программой - фильтром посылается сообщение и предлагается запрет или разрешение соответствующего действия.

5. Программы – вакцины или иммунизаторы, представляющие собой резидентные программы и предотвращающие заражение файлов.

В настоящее время большинство современных антивирусных программ осуществляют комплексную защиту от компьютерных вирусов и выполняют все перечисленные функции.

Примерами антивирусных программ служат:

* Антивирус Касперского, предоставляющий надежную защиту данных, обладающий высоким уровнем защиты и максимальной производительностью.
* Doctor Web, обеспечивающий многоуровневую защиту системной памяти, жесткого диска и сменных носителей от заражения вирусами, троянскими программами, шпионским и рекламным ПО, хакерских утилит, а так же различного рода вредоносных объектов.
* Nod32, обеспечивающий высокую производительность, практически не влияющий на работу системы. Интерфейс данной программы позволяет быстро и эффективно управлять защитой компьютера. Антивирусная программа Nod32 создана таким образом, чтобы минимизировать его влияние на ресурсы системы.
* Panda, не нуждающаяся в каждодневных обновлениях, предоставляющая максимальную производительность, предоставляющая отчёт о проделанной работе и нахождении скрытых угроз в системе.
* Avast, очень хорошо обнаруживающий вирусы и подозрительные процессы с большой скоростью, практически не замедляющий работу компьютера, обеспечивающий безопасную работу в интернете.

 Процесс защиты делят на три рубежа:

* предотвращение попадания вирусов;
* предотвращение атаки вирусов, если вирус уже проник в компьютер;
* предотвращение разрушительных последствий, в случае уже наступления вирусной атаки.

2.3 Методы обнаружения компьютерных вирусов

В современных антивирусных программах используется два подхода к обнаружению вирусов: сигнатурный и эвристический.

Сигнатурный метод основан на сравнении файла с известными образцами вирусов. Данная технология предполагает непрерывное отслеживание новых экземпляров вредоносных программ, их описание и включение в базу сигнатур. Задачей выявления сигнатур занимаются эксперты в области вирусологии.

Главным критерием эффективности сигнатурного метода является скорость реакции на новые появившиеся угрозы, частота обновления и максимальное количество обнаруженных угроз.

Главным недостатком сигнатурного метода является задержка при реакции на новые угрозы. Для создания сигнатуры экспертам необходимо иметь образец вируса. Только после попадания вируса в руки экспертов можно создать сигнатуру. Именно поэтому сигнатуры появляются лишь спустя некоторое время после появления нового вируса. По этой причине сигнатурный метод не пригоден для оперативной защиты от новых вирусов.

Эвристический метод основан на предположении, что новые вирусы часто оказываются похожими на уже известные. Этот метод часто называют поиском вирусов, похожих на известные или статистическим анализом.

Эвристический анализатор представляет собой программу, которая анализируя программный код проверяемого объекта, ищет подозрительные команды, свойственные для вредоносного программного обеспечения.

Достоинством эвристического метода является высокая скорость работы, простота реализации, возможность обнаружения новых еще никому не известных вирусов до того, как для них будут созданы сигнатуры.

Недостатком эвристического метода является то, что уровень обнаружения вирусных кодов программ остается низким, а вероятность ложных срабатываний – высокой.

Заключение

Таким образом, в реферате работы были представлены основные сведения, связанные с компьютерными вирусами: дано определение данному виду вредоносных программ, рассмотрены их жизненный цикл, перечислены признаки заражения компьютера вирусами. Особое внимание уделено рассмотрению многообразия существующих компьютерных вирусов.

Было определено, что защита от компьютерных вирусов является комплексной задачей и включает в себя юридические, административные и организационные, а так же программно-аппаратные меры защиты. Нами подробно рассмотрены вопросы, связанные с применение специальных программ - антивирусов, способных распознавать и обезвреживать вирусы.

Список использованных источников

1. Асокин В.В. Основы информационной безопасности / В.В. Асокин. – М.: КУБГУ, 2012. – 297 с.
2. Баранова Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – М.: ЕАОИ, 2012. – 311 с.
3. Информационные технологии: / А. Денисов, И. Коноплева, О. Хохлова. –[Электрон. текстовые данные]. – Режим доступа: https://www.intuit.ru/studies/courses/3609/851/lecture/31660?page=7
4. Климентьев К. Компьютерные вирусы и антивирусы. Взгляд программиста. / К. Климентьев. – ДМК Пресс, 2013.– 656 с.
5. Прокушев Я.Е. Программно-аппаратные средства защиты информации: учебное пособие/ Я.Е. Прокушев. – СПб.: Интермедия, 2017. – 160 c.