УДК 004.056 **Информационные технологии**

Копылова Яна Антоновна, *студентка бакалавриата 2 курс,*
МИРЭА-Российский технологический университет (РТУ МИРЭА), г. Москва,
Институт информационных технологий, Россия, г. Москва
Свищёв Андрей Владимирович, *старший преподаватель кафедры*
практической и прикладной информатики
МИРЭА-Российский технологический университет (РТУ МИРЭА), г. Москва
Институт информационных технологий, Россия, г. Москва

ИССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ВИРУСОВ И ИХ ВЛИЯНИЕ НА БЕЗОПАСНОСТЬ ДАННЫХ В ОРГАНИЗАЦИИ

Аннотация: В наше время сильно развиты информационные технологии. В связи с этим, все больше появляется компьютерных вирусов. В данной статье рассмотрим виды вирусов, их взаимодействие с файлами, а также все возможные способы защиты и как предотвратить заражение системы.

Ключевые слова: Компьютер, вирус, антивирус, вредоносный код, устройство.

Abstract: The information technology is highly developed nowadays. In this regard, more and more computer viruses appear. In this article, we will consider the types of viruses, their interaction with files, as well as all possible methods of protection and how to prevent infection of the system.

Key words: Computer, virus, antivirus, malicious code, device.

Персональные компьютеры пользователей все чаще становятся жертвами вредоносных программ. В результате заражения появляется риск утечки различных персональных данных: от логинов и паролей социальных сетей, до данных банковских карт. Для борьбы с угрозами необходимо иметь максимально

полное и актуальное представление о разнообразии вирусов, а также об их способах воздействия на атакуемую систему.

Компьютерный вирус - программа, способная самопроизвольно подсоединяться к другим программам компьютера и вызывать сбои в их работе [3]. Многие вирусы визуально незаметны пользователю, однако большинство из них задействуют ресурсы зараженного компьютера или даже получают контроль над устройством. Вирус может распространяться между компьютерами и сетями путем самовоспроизведения - так же, как биологический вирус переходит с одного носителя на другого.

Многообразие вирусов можно разделить на несколько категорий:

1. **По среде обитания** различают вирусы сетевые, файловые и загрузочные.

Сетевые вирусы опасны. Они проникают в компьютер благодаря уязвимостям в протоколах локальных и глобальных сетей. Также нередко вирусы распространяются, используя недочеты программного обеспечения, например, операционных систем или браузера. Основная опасность такого типа вируса заключается в том, что его представители распространяются без сторонней помощи. Данные вирусы могут самостоятельно запустить свой программный код, заражая систему пользователя.

Файловые вирусы представляют не меньшую опасность устройствам пользователей. Такие вирусы размножаются, использую файловую систему компьютера. Существует несколько способов заражения данными вирусами, при заражении методом Overwriting, вредоносная программа внедряет свой программный код в другие файлы, полностью уничтожая содержащуюся в них информацию. Если файл заражается методом Parasitic, то содержимое полностью изменяется, однако работоспособность сохраняется.

Третий тип вирусов – **загрузочный**. Они записываются в сектор диска, который работает при запуске системы. Данный тип вируса вмешивается в процесс загрузки операционной системы, перехватывая управление. Первичная

цель этого вируса – заражение всех дисков устройства и получить полный контроль над компьютером.

2. **По способу заражения** выделяют резидентные и нерезидентные вирусы.

Резидентными называют такие вирусы, как те, что сохраняют свою постоянную (резидентную) часть во временной памяти компьютера, то есть в оперативной памяти устройства. Таким образом, файлы вируса удаляются при перезапуске системы, но зараженные файлы остаются поврежденными.

Нерезидентные, в свою очередь, работают определенное количество времени, не сохраняясь в памяти компьютера. Затем же вирус удаляется, оставляя пользователя на один с нанесенным ущербом.

3. **По степени воздействия;**

Вирусы бывают неопасные. Такими являются вирусы, не имеющие цели нанести вред файлам системы, они просто лишают нас комфортной работе за устройством. Ярким примером таких вирусов являются рекламные. Их задача – показывать различную рекламу пользователю при выполнении определенных действий, например, при выходе в интернет.

Опасные вирусы приводят к нарушениям работе каких-либо программ в системе компьютера.

Очень опасные вирусы, как правило, полностью и безвозвратно удаляют данные, программы.

4. **По особенностям алгоритмов** вирусы делят на паразитические, репликаторы, невидимки, мутанты, троянские.

Репликаторы могут проникнуть в компьютер, используя сеть. Вирус создает свою копию и рассылает ее по найденным адресам. Репликаторы довольно быстро заполняют основную память системы, что усложняет уничтожение данного вируса.

Паразитические вирусы, распространяя свои копии, изменяют содержимое файла, добавляя в него свой код. Есть несколько способов добавления вредоносной части, например, размещение кода может быть в начале

файла – вирус переносит начало файла в конец, а сам в то время записывается в свободное место. Если вирус так запишется, то при запуске файла управление получает код. Также вирус может записаться в середину, в таком случае он разделяет содержимое файла и размещает свой код «между двух частей». Самым распространенным способом является запись в конец файла. Однако при такой записи вирус изменяет начало файла так, что первым запускается вредоносный код.

Вирусы, которые антивирусы не могут распознать, называются **невидимками**. Данный тип невозможно обнаружить средствами операционной системы. Работает это так, что при сканировании программой, вирус изменяет свой вредоносный код на полезный. Также при открытии файла он удаляет свое тело, при закрытии снова его заражает. Данный вирус хранится в памяти резидентно, то есть постоянно находится в операционной памяти компьютера.

Вирусы **мутанты** являются самыми сложными для обнаружения, так как они распространяются по сетям, меняя свой вид так, чтобы копии не совпадали.

Трояны — это программное обеспечение, способное маскировать свои задачи. Дело в том, что оно выглядит как какая-либо знакомая нам программа, а порой и выполняет некоторый функционал тех файлов, под которые маскируется. Данными вирусами можно заразиться, как и злоумышленниками, так и самим, случайно запустив на компьютере. Троянские программы размещают на открытые ресурсы, поэтому попасть на наш компьютер им не составит труда. Это вредоносное программное обеспечение может иметь несколько расширений (см. таблицу 1).

Таблица 1 - Виды расширений

Вид расширений	Описание
.com, .exe	• Файлы **расширения. com** очень легко заражаются вредоносными программами. COM являются небольшими приложениями, системными утилитами. Обычно файлы данного расширения не превышают 65280 байт. • **EXE расширение** применяется в операционных системах DOS, Windows

Вид расширений	Описание
.js, .vbs, .bat, .cmd	• **JS файлы** – это текстовый документ, в котором хранятся строчки кода JavaScript • **Расширения .vbs** – это скрипт, написанный на языке Visual Base, который используется для выполнения команд в среде Windows • **BAT и CMD файлы** – обычные текстовые документы, в которых содержаться наборы команд
.html, .htm, .shtml	• **Html файлы** используются в как страницы веб-сайтов. Такие документы могут скачивать вирусы из интернета. • .htm выполняют ту же цель, что и html.
.pif	Это ярлык, который может выполнять вредоносные действия

Для лучшей защиты своих устройств стоит разобраться какие же объекты могут быть заражены вирусами:

1. Загружаемые при выполнении других программ, помимо них, файлы с расширениями .com, .exe. Если вирус находится в исполняемых файлах, то его работа начинается после запуска файла.

2. Загрузчик операционной системы и главная загрузочная запись жесткого диска. Вирусы способные поразить данные объекты, как было сказано ранее, называются загрузочными. Они постоянно находятся в памяти компьютера, начинают свою работу сразу после запуска компьютера.

3. Файлы документов, также файлы баз данных и так далее.

Заметить, что ваш компьютер заразился вирусом, порой бывает легко, для этого стоит знать некоторые признаки:

1. Производительность вашего компьютера стала меньше. Это довольно явный признак заражения вирусом. Происходит из-за того, что вирусы нагружают операционную память устройства, вследствие чего, компьютер начинает работать значительно медленно.

2. Приложения перестают работать, то есть при использовании какой-либо программы могут часто появляться сообщения об ошибках.

3. Часто всплывает различная реклама. Обычно такие вирусы просто мешают работе за компьютером, по порой могут быть предназначены для кражи вашей информации.

4. Отсутствие подключения к Интернету. Вирус, поражающий компьютер, могут подключиться к интернету тем самым снизить его пропускную способность.

5. При подключении к Интернету открываются окна, которые Вы не открывали. Это происходит из-за того, что вирусы могут перенаправлять трафик на определённые сайты против вашей воли.

6. Пропали файлы. Если вы заметили, что не хватает каких-либо файлов, то это тоже может быть признак заражения компьютера, ведь существует различное количество вирусов, которые удаляют или шифруют файлы.

7. Происходит отправка сообщений без вашего ведома.

Главное помнить, что вирусы можно обнаружить на раннем этапе их развития, когда еще не все файлы были повреждены. Чтобы раньше обнаружить и избавиться от них, необходимо регулярно выполнять проверку антивирусными программами. Пренебрежение проверок может привести к плачевным ситуациям, что не только ваш компьютер будет заражен, но и другие. Поэтому стоит разобраться какие типы антивирусов существуют:

1. **Антивирусы детекторы**. Их принцип работы – это сообщать пользователю, что вирус обнаружен. Примером такой программы может служить **антивирус Касперского;**

2. **Антивирусы ревизоры** запоминают начальное состояние программ, файлов, чтобы в дальнейшей своей работе сравнивать с текущим. Таким образом данные программы контролируют все изменения и в нужный момент сообщают об этом пользователю. Явным представителем таких антивирусов является **AVP (Anti-Virus Protection);**

3. **Фильтры** выявляют подозрительные процедуры, были ли какие-то изменения программ, файлов, дисков. Данные антивирусы следят, например,

изменялся ли размер файлов. При обнаружении каких-то подозрительных действий фильтры запрашивают пользователя о правомерности их выполнения**.** **Ативирус Avast** является таким типом;

4. **Доктора** самый распространённый тип. Такие антивирусы помимо обнаружения вирусов, могут и от них избавиться, другими словами, они «лечат» программы. **Dr. Web –** представитель таких антивирусов;

5. **Антивирусы Вакцины**. Они изменяют программы, файлы таким образом, что для вирусов они уже выглядят зараженными.

Сейчас существует множество написанных антивирусных программ, поэтому для определения лучшей, рассмотрим самые известные среди них (см. таблицу 2).

Таблица 2 - Популярные антивирусы

Название	**Описание**	**Достоинства**	**Недостатки**
Антивирус Касперского	Разработчики данного антивируса обещают защиту в реальном времени, быструю работу системы, быстрая проверка на вирусы, откат изменений.	Постоянно обновляются базы данных, что способствует быстрому обнаружению вредоносных программ. большинство вирусов заносятся в реестр Касперского на неделю раньше, в отличие от конкурирующих программ.	Антивирус сильно заполняет оперативную память компьютера, что ухудшает производительность компьютера. Касперский часто блокирует программы, считая их вредоносными
Антивирус Dr.Web	Антивирус Dr.Web очень популярная антивирусная программа. Защита блокирует любые автоматические модификации критических объектов системы, позволяя пользователям контролировать доступ к тем или иным объектам Windows,	Постоянно обновляемые и наиболее полные реестры вредоносных и пиратских программ, занимает достаточно мало оперативной памяти компьютера;	Бывают случаи, когда останавливал всю работу компьютера, проверяя программу

Название	Описание	Достоинства	Недостатки
	различным приложениям, обеспечивая защиту от вредоносных программ		
Avast Pro Antivirus	Современная защита от всех типов вредоносного ПО в сочетании с дополнительными компонентами защиты и гибкими настройками для более качественной защиты вашего ПК.	Существует бесплатная версия. Программа обновляется автоматически. Наличие версий для различных платформ: Windows и Android. Высокая скорость полной проверки	Ограниченный функционал бесплатной версии. Практически полностью не совместимо с антивирусным обеспечением других компаний

На мой взгляд, антивирус Avast является самым оптимальным среди всех, ведь им можно пользоваться совершенно бесплатно, да с какими-то ограничениями, но остальной функциональности достаточно для обеспечения безопасности системы.

Необходимо всегда помнить, что антивирусы не способны обнаружить любой вирус. Ведь это программа способна найти и избавиться только от известных вредоносных файлов. Для конкретного вируса пишется антивирус только, если программист будет иметь хотя бы один экземпляр вредоносного кода. Если не делать ничего для защиты, то последствия заражения могут быть очень серьезными. Поэтому также надо уделить свое внимание другим мерам защиты от вирусов, помимо антивирусных программ:

- Перед тем как начнете считывать информацию с других устройств, стоит проверять их на наличие вирусов;
- Проверяйте на наличие вирусов диски компьютера;
- Также необходимо не забывать проверять информационные носители, например, флешку;
- Чаще обновлять операционные системы и программы, ведь в обновлении исправляют ошибки и улучшают безопасность. Особенно стоит уделить внимание актуальной версии антивируса, так как с каждым обновлением в нем увеличивается база известных вирусов, что способствует сильной защите;

- Осторожно обращаться с сообщениями, которые приходят, например, на почту, не стоит открывать какие-либо неизвестные вам ссылки;
- Необходимо следить за сайтами, которые вы посещаете в интернете;
- Какую-либо программу качайте только с официального сайта.

Подводя итог, во времена активного развития технологий, когда почти вся наша жизнь находится в наших устройствах, появилось и множество мошенников, которые написали различные компьютерные вирусы, однако для безопасности было создано большое количество антивирусных программ, каждая из которых имеет свои достоинства и недостатки. Но как уже выяснили, многое зависит не только от антивирусов, но и от пользователя компьютера.

Хотела бы добавить, что написание компьютерного вируса наказуемо, например, в 1989 г. вирусом, который написал американский студент Моррисом, были заражены около тысячи компьютеров, в том числе принадлежащих министерству обороны США. Студента приговорили к трем месяцам тюрьмы и штрафу в 270 тыс. дол.

Библиографический список:

1. Зенкин Д. В., Касперский Е. В. Компьютерные вирусы: происхождение, реальная угроза и методы защиты, режим доступа: свободный / [Электронный ресурс] URL: https://www.nkj.ru/archive/articles/7889/ (Дата обращения: 05.10.2021).

2. Каптерев А.И. Электронный учебник по информатике [Электронный ресурс] URL: http://www.mediagnosis.ru/Autorun/Page6/11_1_.htm (Дата обращения: 01.10.2021).

3. Кузнецов С.А. Большой толковый словарь русского языка [Электронный ресурс] URL: http://www.gramota.ru/slovari/dic/?bts=x&word=%D0%B2%D0%B8%D1%80%D1%83%D1%81 (Дата обращения: 20.09.2021).

4. Kaspersky.ru: сайт [Электронный ресурс] URL: https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs (Дата обращения: 02.10.2021).

5. Shkolo.ru: сайт [Электронный ресурс] URL: http://shkolo.ru/antivirusyi/ (Дата обращения: 10.10.2021).