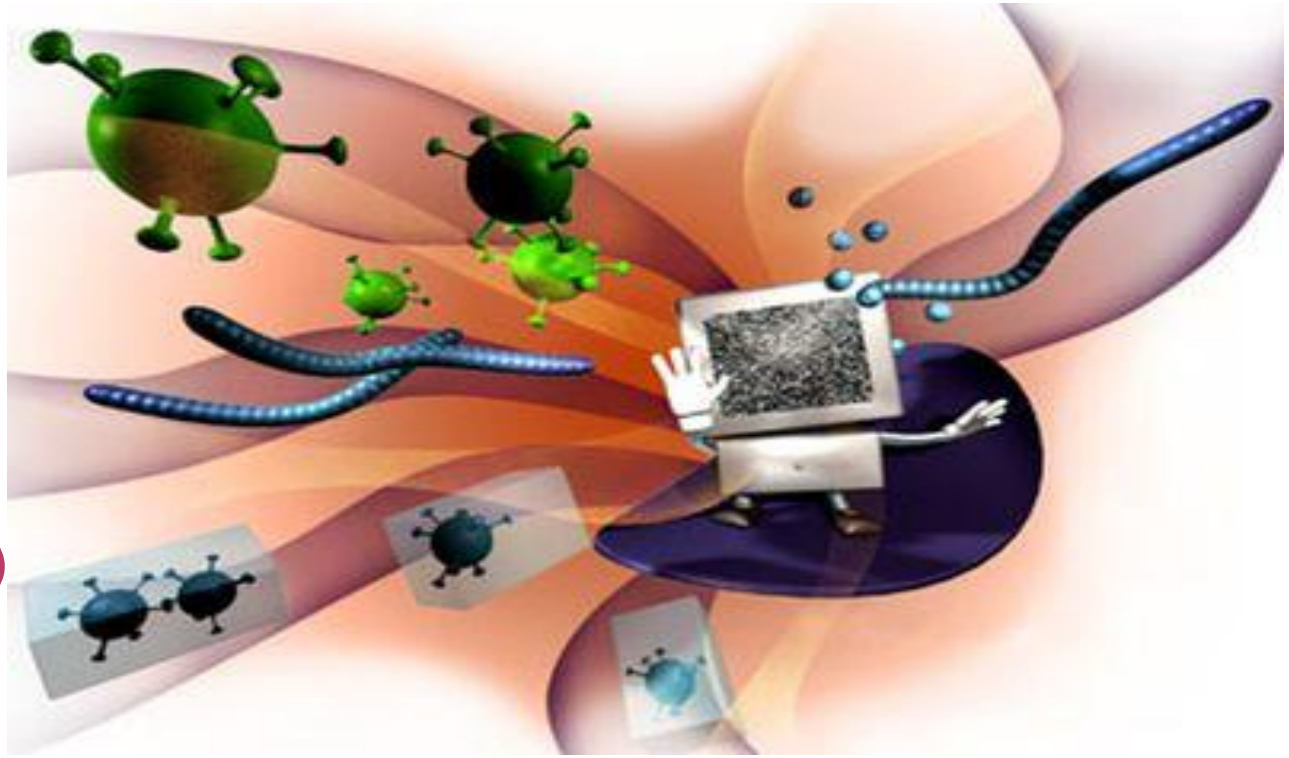
# Вирусы и антивирусные программы



**Выполнила:** Тесленко Н. В.

# СОДЕРЖАНИЕ





# 1. Что такое вирусы?

- **Вирусы** - ***программы или элементы программ, несанкционированно проникшие в компьютер с целью нанесения вреда, отличительной особенностью которых является способность самотиражирования. Наибольшая опасность таких вирусов заключается в том, что прежде чем нанести вред компьютеру и самообнаружиться, они копируются в другие программные файлы.***

# 2. Классификация вирусов

| *По среде обитания* | *По способу заражения* | *По степени воздействия* | *По особенностям алгоритма* |
|---|---|---|---|
| **Сетевые вирусы** распространяются по различным компьютерным сетям. **Файловые вирусы** внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE. **Загрузочные вирусы** внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord). **Файлово-загрузочные вирусы** заражают как файлы, так и загрузочные сектора дисков. | **Резидентные вирусы** -при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. **Нерезидентные вирусы -** не заражают память компьютера и являются активными ограниченное время. | **Неопасные вирусы**, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах. **Опасные вирусы,** которые могут привести к различным нарушениям в работе компьютера очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска. | **Простейшие вирусы,** изменяют содержимое файлов и секторов диска, легко обнаружить и уничтожить. **Вирусные черви** распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. **Вирусы-невидимки,** трудно обнаружить и обезвредить, перехватывают обращения опер. системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. **Вирусы-мутанты** содержат алгоритмы шифровки-расшифровки, копии одного вируса не имеют повторяющихся цепочек байтов, трудно обнаружить. **«Троянские» программы**, не способны к самораспространению, опасны, разрушают загрузочный сектор и файловую систему дисков. |

# 3. Виды вирусных программ

| *Троянский конь (Trojans)* | *Зомби (Zombie)* | *Червь (Worm)* |
|---|---|---|
| это программа, которая находится внутри другой, как правило, абсолютно безобидной программы, при запуске которой в систему инсталлируются программа, написанная с целью нанести ущерб целевому компьютеру путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях. | это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые рассылается огромное количество нежелательных сообщений электронной почты, а также распространяются вирусы и другие вредоносные программы. | это программа, которая тиражируется на жестком диске, в памяти компьютера и распространяется по сети. Особенностью червей является то, что они не несут в себе никакой вредоносной нагрузки, кроме саморазмножения, целью которого является замусоривание памяти, и как следствие, затормаживание работы операционной системы. |

# 3. Виды вирусных программ

| *Руткиты* | *Шпионская программа (Spyware)* | *Фишинг (Phishing)* |
|---|---|---|
| программы, установленные и работающие на компьютере без ведома пользователя и прячущие используемые злоумышленниками инструменты от антивирусного ПО. Они представляют значительный риск безопасности для домашних и корпоративных машин и сетей, так как их очень сложно обнаружить. Сами руткиты обычно устанавливаются с помощью вирусов или других вредоносных объектов, поэтому настоятельно рекомендуется постоянно обновлять антивирусную защиту и защиту от шпионов. | программный продукт, установленный или проникший на компьютер без согласия его владельца, с целью получения практически полного доступа к компьютеру, сбора и отслеживания личной или конфиденциальной информации. Эти программы, как правило, проникают на компьютер при помощи сетевых червей, троянских программ или под видом рекламы (adware). | почтовая рассылка имеющая своей целью получение конфиденциальной финансовой информации. Такое письмо, как правило, содержит ссылку на сайт, являющейся точной копией Интернет-банка или другого финансового учреждения. Пользователь, обычно, не догадывается, что находится на фальшивом сайте и спокойно выдает злоумышленникам информацию о своих счетах, кредитных карточках, паролях и т. д. |


# ЧТО ТАКОЕ АНТИВИРУСНАЯ ПРОГ

- **Антивирусная программа** – *это специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.*


# 5. Виды антивирусных программ

| *Антивирусы-фильтры* | *Антивирусы-детекторы* | *Антивирусы-вакцинаторы* |
|---|---|---|
| Программы, которые уведомляют пользователя обо всех действиях на его компьютере. Если вирус попытается проникнуть на ваш ПК или, наоборот, украсть пароль и отправить его злоумышленнику, сторож спросит: «Разрешить или запретить выполнение операции?». К сожалению, работа с данным типом защиты требует определённых навыков, ведь далеко не каждый знает, что обозначает тот или иной процесс. | Нужно регулярно обновлять, ведь 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. Главное почаще обновлять его и не забывать продлевать лицензию. | Уже заражённые компьютеры сложно вылечить с помощью детектора или фильтра. В очень тяжёлых случаях на помощь приходят программы-вакцинаторы. Даже дорогой лицензионный антивирус 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. |

# 6. Примеры антивирусных программ

| *Антивирус Касперского* | *Антивирус NOD32* | *Dr.Web* | *Avast* |
|---|---|---|---|
| антивирусное программное обеспечение, предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS. | Антивирус ESET NOD32 разработан на основе передовой технологии ThreatSense®. Ядро программы обеспечивает проактивное обнаружение всех типов угроз и лечение зараженных файлов (в том числе, в архивах) благодаря широкому применению интеллектуальных технологий, сочетанию эвристических методов и традиционного сигнатурного детектирования. | Предназначен для защиты от почтовых и сетевых червей, руткитов, файловых вирусов, троянских программ, стелс-вирусов, полиморфных вирусов, бестелесных вирусов, макровирусов, вирусов, поражающих документы MS Office, скрипт-вирусов, шпионского ПО (spyware), программ-похитителей паролей, клавиатурных шпионов, программ платного дозвона, рекламного ПО (adware), потенциально опасного ПО, хакерских утилит, программ-люков, программ-шуток, вредоносных скриптов и других вредоносных объектов. | Инновационное антивирусное и антишпионское ядро сканирования<br>Эффективная защита от руткитов – вредоносных программ, невидимых для антивирусов<br>Сканирование при загрузке – один из самых эффективных антивирусных инструментов Avast, позволяющий провести проверку ДО загрузки Windows<br>Система avast! WebRep, позволяющая получить информацию о надёжности веб-сайтов на основе отзывов пользователей. |



# СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ


- http://ppt4web.ru/informatika/virusy-i-antivirusnye-programmy.html
- https://ru.wikipedia.org/wiki/
- http://pctoall.ru/zashhita-i-bezopasnost/zashhita-ot-virusov/vidy-kompyuternyx-virusov.html

# СПАСИБО ЗА ВНИМАНИЕ!!!