

АНТИВИРУСНЫЕ

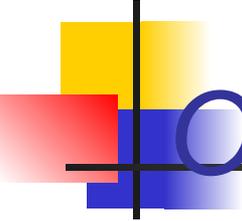
программы

*Виды компьютерных  
вирусов.*

*и Антивирусных  
программ.*

*Преподаватель ГБПОУ КК «КИТТ»*

*Якунина А.Т.*



# Оглавление:

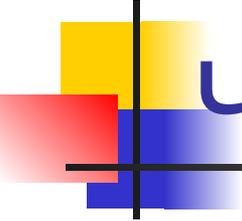
---

- ❖ Вирус

- ❖ Что такое вирус?
- ❖ Классификация вирусов

- ❖ Антивирусные программы

- ❖ Что такое антивирусная программа?
- ❖ Некоторые её параметры
- ❖ Виды антивирусных программ



# Что такое вирус?

---

- *Прежде всего, вирус – это программа, которая может «размножаться» и скрытно внедрять свои копии в файлы, загрузочные сектора дисков и в документы.*
- *Активизация компьютерного вируса может вызвать уничтожение программ системы, самой системы и данных.*

**200 - 5000 байт**

**более 50 тыс. вирусов**

**НАЗАД**



# **Признаки появления вирусов:**

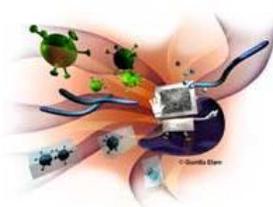
---

- **Неправильная работа нормально работающих программ**
- **Частые зависания и сбои в работе ПК**
- **Медленная работа ПК**
- **Изменение размеров файлов**
- **Исчезновение файлов и каталогов**
- **Неожиданное увеличение количество файлов на диске**
- **Уменьшение размеров свободной оперативной памяти**
- **Вывод на экран неожиданных сообщений и изображений**
- **Подача непредусмотренных звуковых сигналов**
- **Невозможность загрузки Операционной Системы**



# КЛАССИФИКАЦИЯ ВИРУСОВ

- Резидентные и нерезидентные
- Загрузочные вирусы
- Файловые вирусы
- Макро- вирусы
- Сетевые вирусы



**НАЗАД**

# Вирусы делятся также на резидентные и нерезидентные

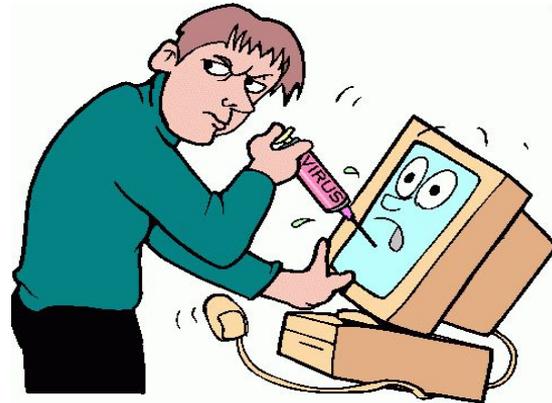
*Первые, в отличие от нерезидентных, при получении управления загружаются в память и могут действовать не только во время работы зараженного файла.*



**НАЗАД**

# Загрузочные вирусы

При заражении дисков, загрузочный вирус «заставляет» систему, при ее перезапуске, считать в память и отдать управление не программному коду загрузчика операционной системы, а коду вируса.

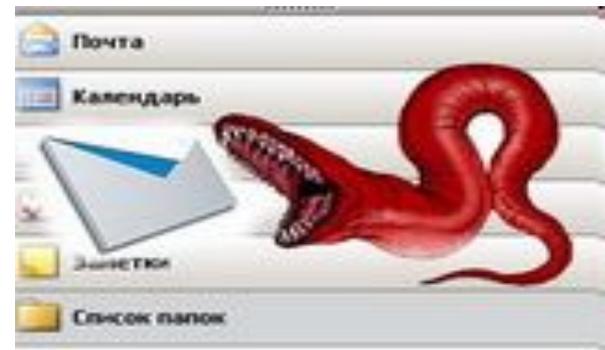


**НАЗАД**

# Файловые вирусы

При своем размножении тем или иным способом используют файловую систему операционной системы.

Файловые вирусы могут поражать исполняемые файлы различных типов.

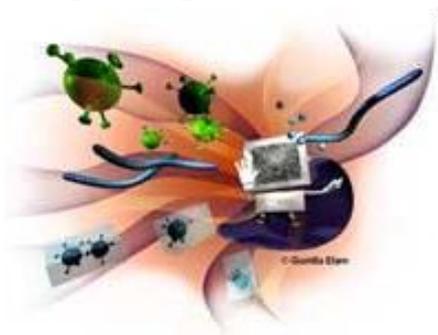


**Назад**

# Макро-вирусы

Являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).

Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

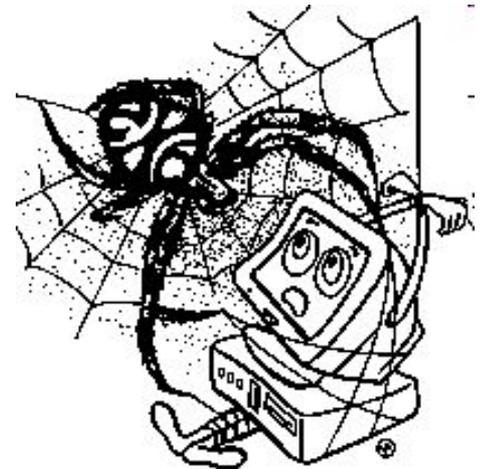


**Назад**

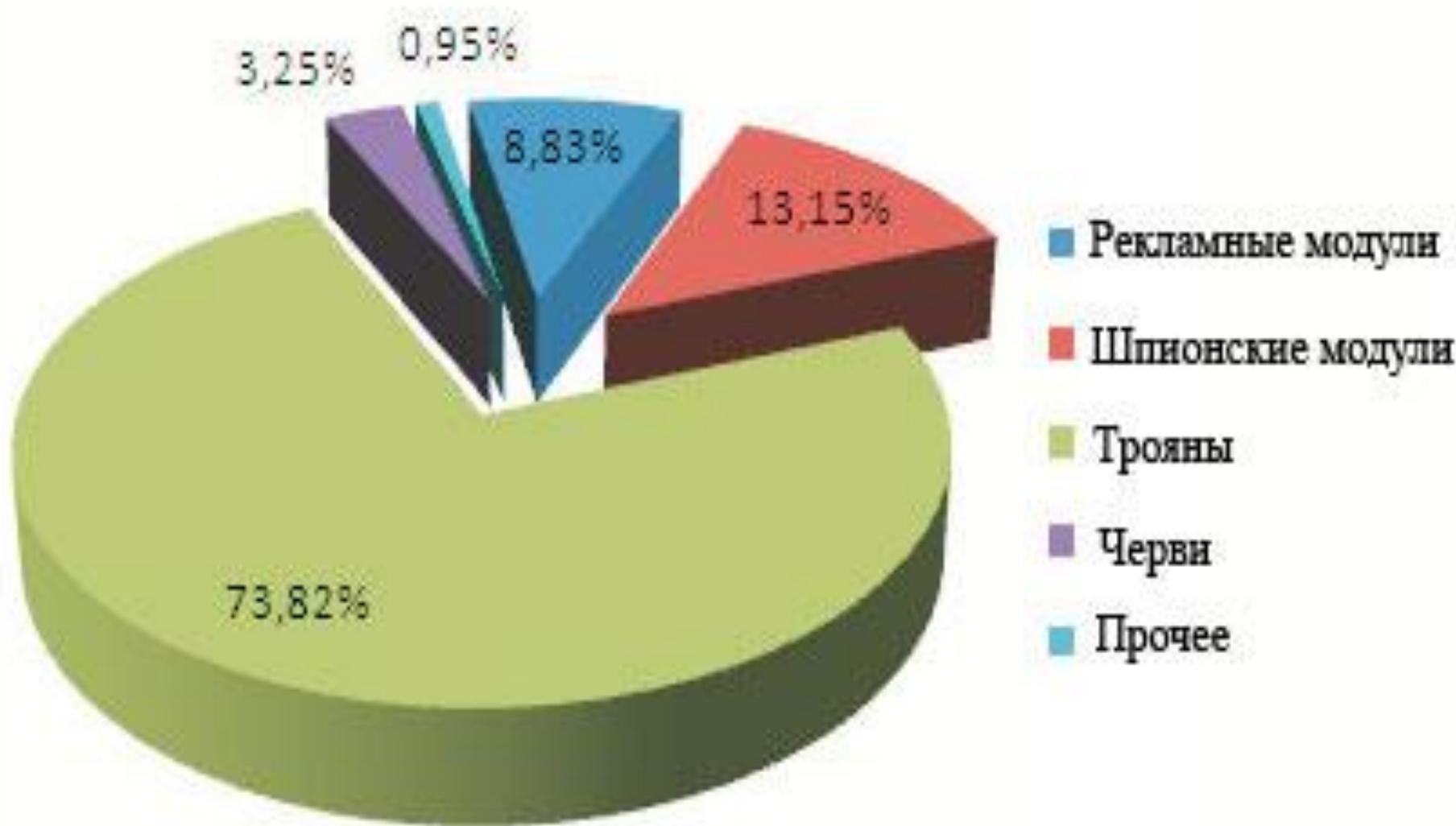
# Сетевые вирусы

Для своего распространения используют протоколы и возможности локальных и глобальных компьютерных сетей.

Основным принципом работы сетевых вирусов является возможность передать и запустить свой код на удаленном компьютере.



**Назад**



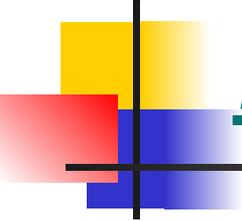
***Распространенные виды вирусов***

# Хакерские утилиты и прочие вредоносные программы



К данной категории относятся:

- автоматизации создания вирусов, червей и троянских программ (конструкторы);
- скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;



# Хакерские утилиты и прочие вредоносные программы

---

- программные библиотеки, разработанные для создания вредоносного ПО;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

# Каналы распространения



- **Флеш-накопители (флешки)**

В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители. Флешки — основной источник заражения для компьютеров.

- **Системы обмена мгновенными сообщениями**

Так же распространена рассылка ссылок на якобы фото, музыку либо программы, по ICQ и через другие программы мгновенного обмена сообщениями, в действительности являющиеся вирусами.

- **Веб-страницы**

Возможно также заражение через страницы Интернет.



# Антивирусные програ



*Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные программы, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.*

**НАЗАД**

## Их параметры...

---



Для быстрой и эффективной работы антивирусная программа должна отвечать некоторым параметрам:

- ✓ *Стабильность и надежность работы*
- ✓ *Размеры вирусной базы программы*
- ✓ *Многоплатформенность*

# АНТИВИРУСНЫЕ ПРОГРАММЫ

- Антивирусные блокировщики



- Ревизоры



- Полифаги



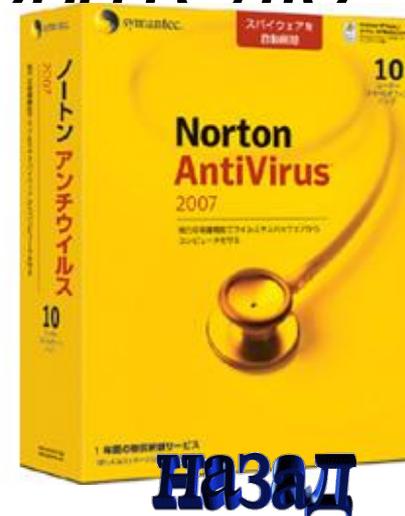
- Полифаги-мониторы



**НАЗАД**

# Антивирусные блокировщики

Резидентные программы, которые перехватывают «вирусоопасные» ситуации и сообщают об этом пользователю



Назад

# Ревизоры



*Принцип работы ревизоров основан на подсчете контрольных сумм для хранящихся на диске файлов. Эти суммы, сохраняются в базе данных антивируса. При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.*

**НАЗАД**



## *Полифаги*

---

*Принцип работы полифагов основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов.*

*Для поиска известных вирусов используются маски вирусов.*

**Назад**

# Полифаги-мониторы

*Постоянно находятся в оперативной памяти компьютера и проверяют все файлы в реальном режиме времени.*

*Полифаги-сканеры производят проверку системы по команде пользователя.*



**НАЗАД**

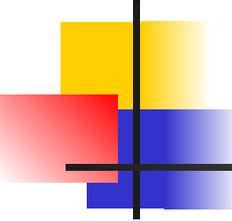
# Краткий обзор антивирусных программ

При выборе антивирусной программы необходимо учитывать не только процент обнаружения вирусов, но и способность обнаруживать новые вирусы, количество вирусов в антивирусной базе, частоту ее обновления, наличие дополнительных функций.



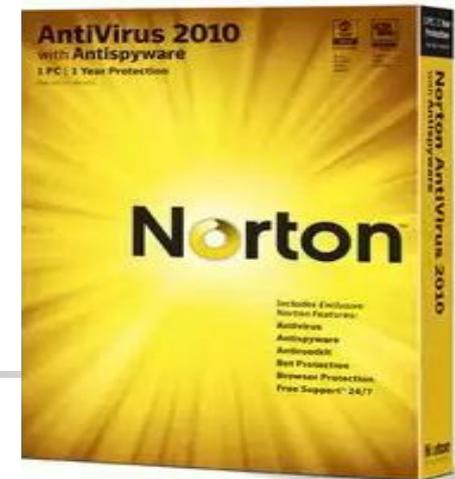
# Наиболее известные из антивирусных программ

ТОП	Антивирус	1 фактор	2 и 3 фактор	ИТОГИ
1	<b>Kaspersky</b>	2	2	4
2	<b>NOD32</b>	1	3	4
3	<b>Dr.Web</b>	3	1	4
4	Avast	4	4	8
5	Avira	6	6	12
6	ВирусБлокАда (VBA)	5	9	14
7	Norton	7	7	14
8	MSE	10	5	15
9	McAfee	8	10	18
10	Panda	12	8	20
11	другой антивирус	9	12	21
12	не использую	11	12	23



# *Norton AntiVirus*

---



*Один из известных и популярных антивирусов. Процент распознавания вирусов очень высокий (близок к 100%). В программе используется механизм, который позволяет распознавать новые неизвестные вирусы.*

[Параметры](#)[Быстродействие](#) ↻[Отзывы](#)[Учетная запись](#)[Поддержка](#) ▶

## Защита компьютера

[Начать сканирование](#) ▼ [Журнал](#) [Карантин](#)[Рейтинг приложений](#)[Запустить LiveUpdate](#) [29 минут назад](#) ▶Insight Protection [Сведения](#) Антивирусная защита Защита от программ-шпионов Защита SONAR [Справка](#)

## Сканирование компьютера

Выполняйте сканирование областей, наиболее подверженных заражению, всего компьютера или отдельных дисков, папок и накопителей.

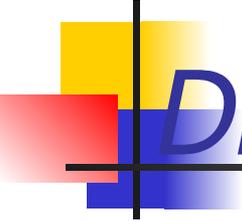
[Быстрое сканирование](#)

Последнее выполнение: 11.09.2010

[Сканирование всей системы](#)

Последнее выполнение: 11.09.2010

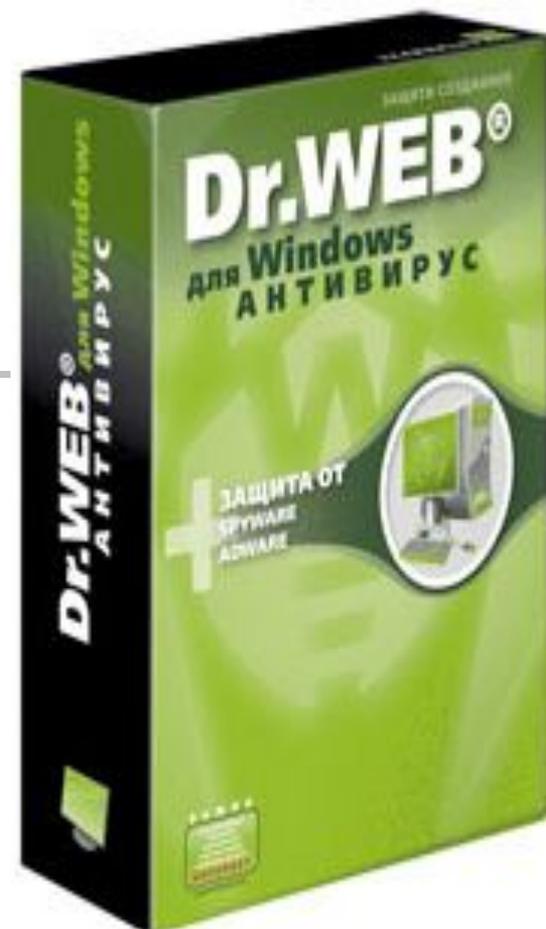
[Выборочное сканирование](#)[Сканирование с учетом репутации](#) ▶



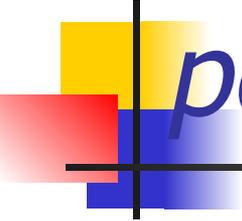
# DrWeb

---

*Популярный  
отечественный антивирус.  
Хорошо распознает вирусы,  
но в его базе их меньше чем  
у других антивирусных  
программ*



# *Нетребовательность к ресурсам*



---

- *Антивирус Dr.Web нетребователен к ресурсам, работает, не перегружая систему, что позволяет ему уверенно защищать даже самые маломощные компьютеры прежних поколений.*

Проверка **Статистика**

- Быстрая проверка
- Полная проверка
- Выборочно

В этом режиме проверяются:

- \* Загрузочные секторы всех дисков
- \* Все сменные носители
- \* Все локальные диски



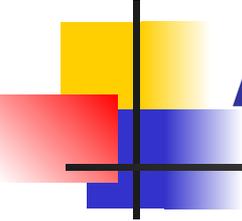
Объект	Путь	Статус	Действие
<b>comss.ru</b>			

Выделить все      Вылечить      Переименовать      Переместить      Удалить

# Антивирус Касперского



- Максимально эффективно сочетает антивирусные технологии, сосредоточенные на серверах Лаборатории Касперского.
- Это позволяет практически мгновенно реагировать на новые и неизвестные вредоносные угрозы: вирусы, троянские программы, интернет-черви, шпионское ПО.



# Основные компоненты Антивируса Касперского

---

- Файловый антивирус
- Почтовый антивирус
- Веб-антивирус
- Мониторинг активности
- Проактивная защита
- Инструменты безопасности



## Компьютер защищен

- ✓ **Угрозы:** отсутствуют
- ✓ **Компоненты защиты:** включены
- ✓ **Базы:** давно не обновлялись
- ✓ **Лицензия:** осталось 52 дня



Проверка



Обновление



Инструменты



Виртуальная клавиатура



Спасибо  
за внимание!