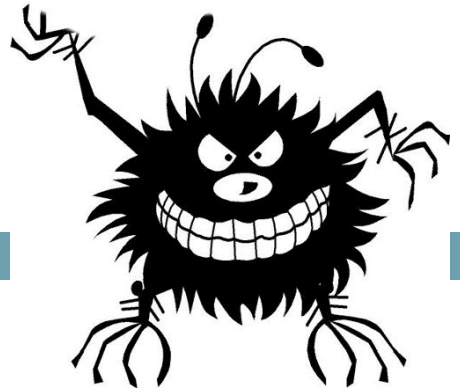
КОМПЬЮТЕРНЫЕ ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ.

Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/

Компьютерный вирус

- — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распростра свои копии по разнообразны каналам связи.

Цели вирусов:



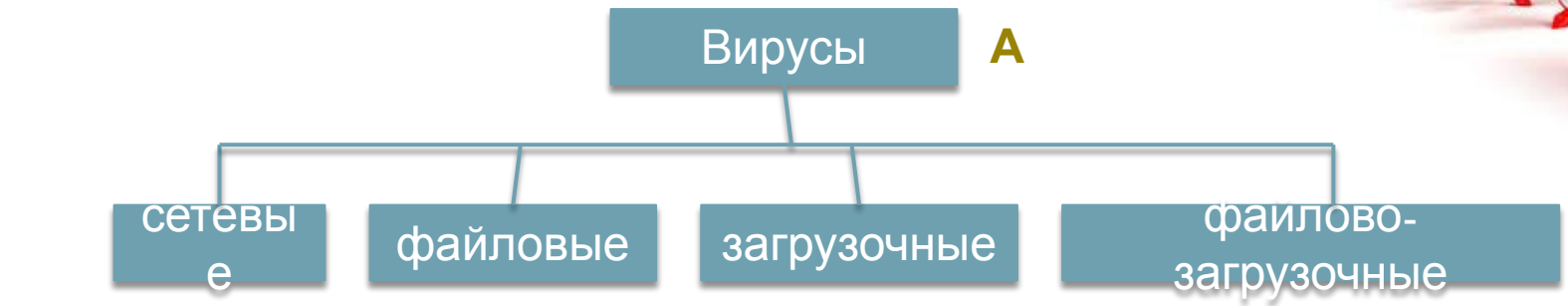
- удаление файлов;
- приведение в негодность структур размещения данных;
- блокирование работы пользователей ;
- приведение в негодность аппаратных комплексов компьютера;
- вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами;
- вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы.

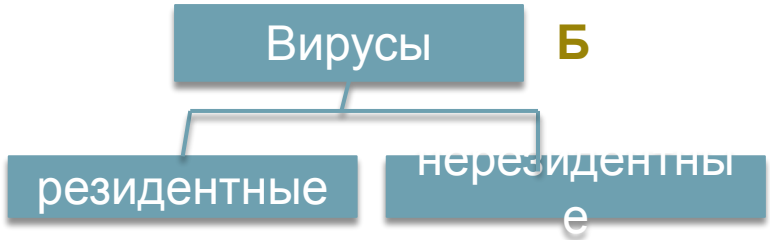
Признаки появления вирусов:

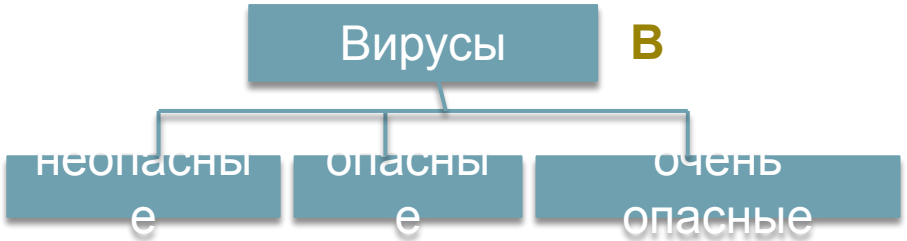
- Неправильная работа нормально работающих программ
- Частые зависания и сбои в работе ПК
- Медленная работа ПК
- Изменение размеров файлов
- Исчезновение файлов и каталогов
- Неожиданное увеличение количество файлов на диске
- Уменьшение размеров свободной оперативной памяти
- Вывод на экран неожиданных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

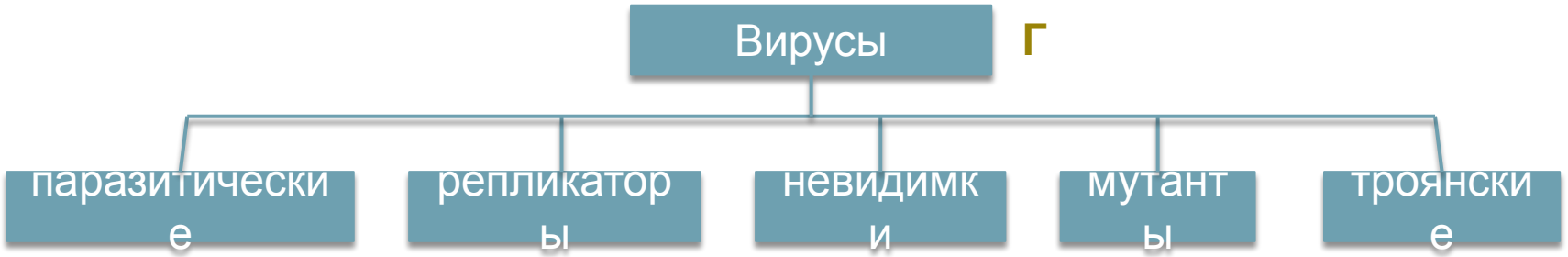
Классификация вирусов:

А – по среде обитания;
Б - по способу заражения;
В – по степени воздействия
Г - по особенностям алгоритм
алгоритмов









Классификация вирусов: по среде обитания

- **Сетевые вирусы** используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

- **Файловые вирусы** либо различными способами внедряются в выполняемые файлы (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы)

- **Загрузочные вирусы** записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.

Классификация вирусов: по способу заражения

- **Резидентные** (такой вирус при инфицировании ПК оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение ОС к объектам заражения и поражает их. Резидентные вирусы живут до первой перезагрузки ПК)
- **Нерезидентные** (не заражают оперативную память и могут быть активными ограниченное время)

Классификация вирусов: по степени воздействия

- **Неопасные** (как правило эти вирусы забивают память компьютера путем своего размножения и могут организовывать мелкие пакости – проигрывать заложенную в них мелодию или показывать картинку);

- **Опасные** (эти вирусы способны создать некоторые нарушения в функционировании ПК – сбои, перезагрузки, глюки, медленная работа компьютера и т.д.);

- **Очень опасные** (опасные вирусы могут уничтожить программы, стереть важные данные, убить загрузочные и системные области жесткого диска, который потом можно выбросить)

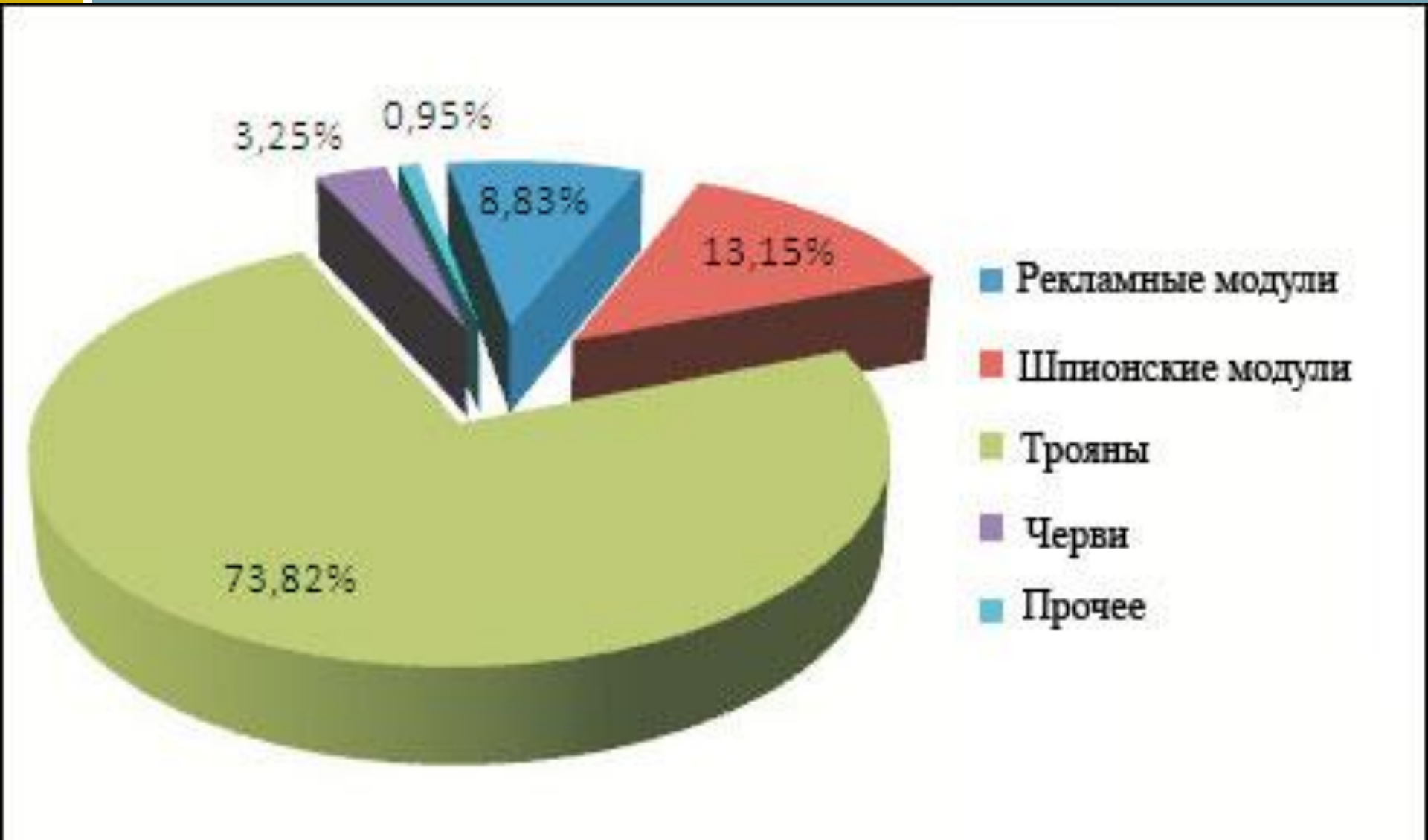
Классификация вирусов по особенностям алгоритмов

- **Паразитические** (изменяют содержимое файлов и секторов диска. Такие вирусы легко вычисляются и удаляются);
- **Мутанты** (их очень тяжело обнаружить из-за применения в них алгоритмов шифрования. Каждая следующая копия размножающегося вируса не будет похожа на предыдущую);
- **Репликаторы** (вирусы-репликаторы, они же сетевые черви, проникают через компьютерные сети, они находят адреса компьютеров в сети и заражают их);
- **Троянский конь** (один из самых опасных вирусов, так как трояны не размножаются, а воруют ценную (порой очень дорогую) информацию – пароли, банковские счета, электронные деньги и т.д.);
- **Невидимки** (это трудно обнаружимые вирусы, которые перехватывают обращения ОС к зараженным файлам и секторам дисков и подставляют вместо своего незараженные участки.

Пути проникновения вирусов

- Глобальная сеть Internet
- Электронная почта
- Локальная сеть
- Компьютеры «Общего назначения»
- Пиратское программное обеспечение
- Ремонтные службы
- Съемные накопители

Распространенные виды вирусов



Антивирусные программы

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

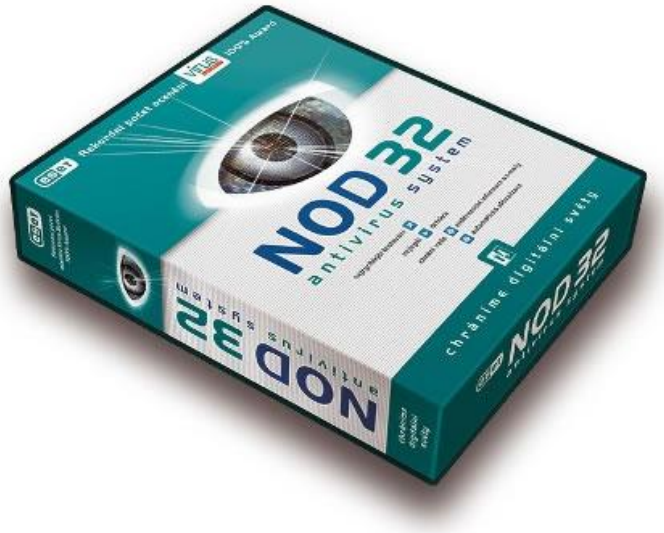
Параметры антивирусной программы

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

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

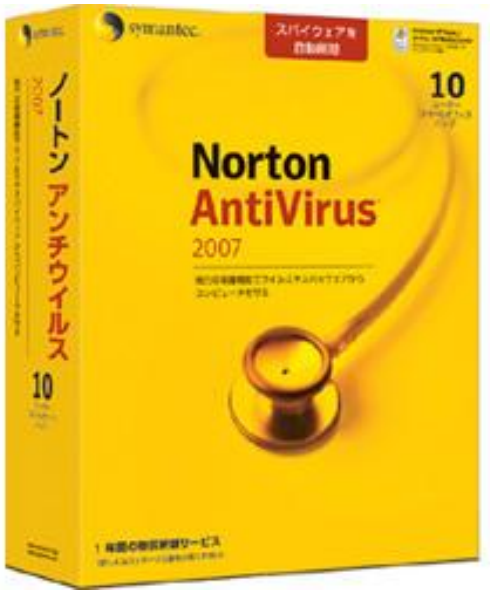
Виды антивирусных программ

- Антивирусные блокировщики
- Ревизоры
- Полифаги
- Полифаги-мониторь



Виды антивирусных программ
Антивирусные блокировщики

- Программы, которые перехватывают «вирусоопасные» ситуации и сообщают об этом пользователю.



Виды антивирусных програм

Ревизоры

- Принцип работы ревизоров основан на подсчете контрольных сумм для хранящихся на диске файлов. Эти суммы, а также некоторая другая информация (длины файлов, даты их последней модификации и др.) 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

Виды антивирусных программ

Полифаги

- Принцип работы полифагов основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных полифагу) вирусов.
- Для поиска известных вирусов используются маски вирусов (некоторая постоянная последовательность программного кода, специфичная для каждого конкретного вируса).

Виды антивирусных программ

Полифаги-мониторы

- Постоянно находятся в оперативной памяти компьютера и проверяют все файлы в реальном режиме времени.
- Полифаги-сканеры производят

  проверку системы по команде пользователя.

Антивирусные программы

Microsoft
Security Essentials

Kaspersky Antivirus

- Вирусов после проверки не оставляет, сетевые атаки надежно блокирует.
- Часто обновляется.
- Платный.
- Имеет репутацию лучшего антивируса в России.

Avast Home Ed

- Бесплатный.
- Очень быстро обновляется.
- Обладает встроенным сетевым экраном (Firewall).
- Проверяет почту.
- Русифицирован полностью.
- Память и ресурсы процессора использует очень умеренно.
- Обновляется раз в сутки.

DrWeb

- Рекомендовано обновлять каждый час при постоянном использовании Интернета.
- Периодические проблемы с обновлениями, даже лицензионных версий.
- Проблемы в работе при настройках по умолчанию.
- Очень высокая загрузка процессора, памяти, частое обращение к жёсткому диску.

Antivir

- Бесплатный.
- Крайне долго обновляется.
- Высокая затрата ресурсов компьютера.
- Интерфейс на английском.
- Вполне употребим для домашнего использования.