

Компьютерные вирусы -

**что это такое и как
защититься от них!**

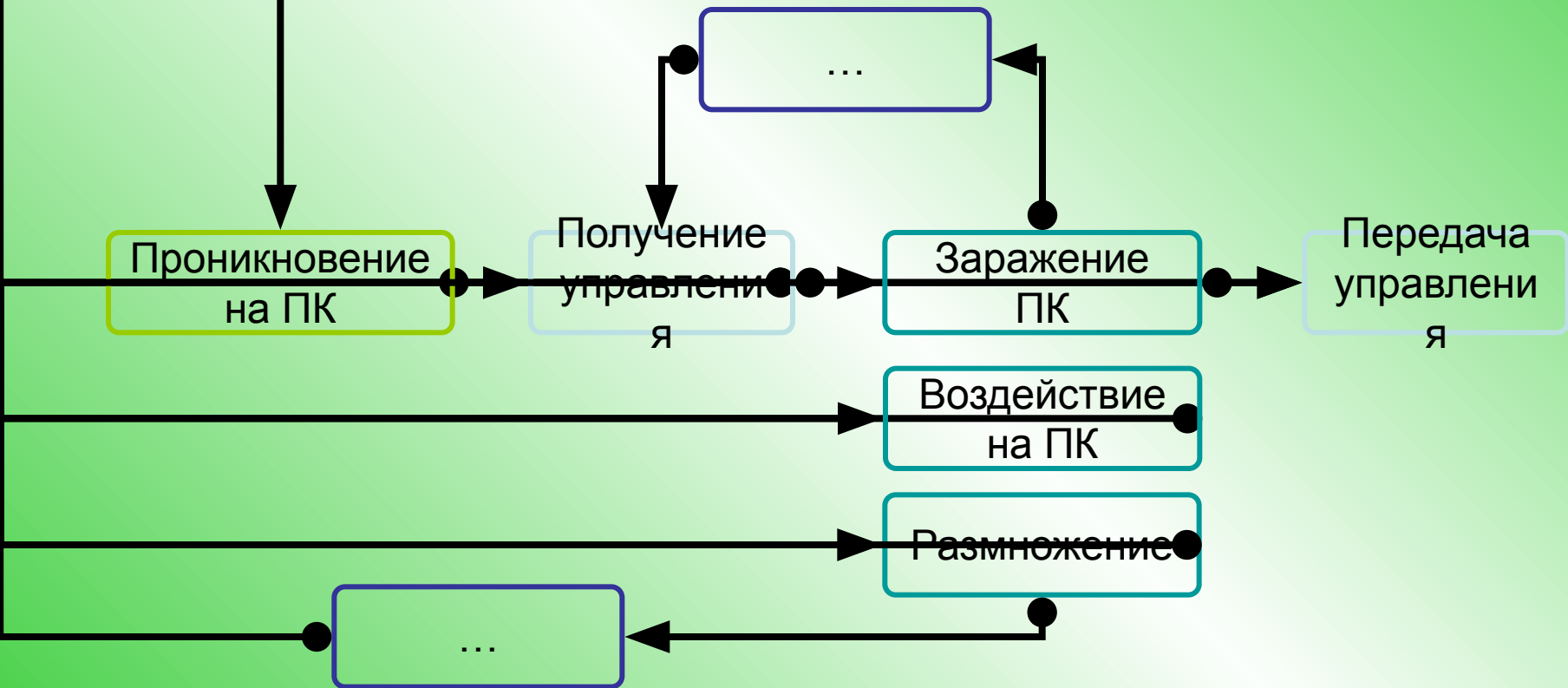


Определение

- **Компьютерный вирус** — это специально написанная программа, выполняющая нежелательные действия на ПК.



Алгоритм работы компьютерного вируса

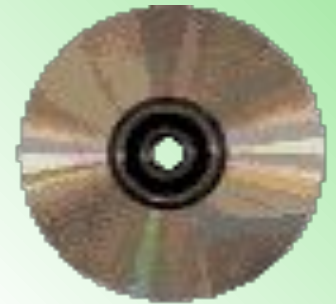


Классификация по среде обитания



Загрузочные вирусы

- **Заражаемые объекты:** boot-сектор логического диска или MBR винчестера
- **Способ заражения:** встраивание своего кода в загрузчик
- Получают управление при загрузке с зараженного диска



Файловые вирусы



- **Заражаемые объекты:** файловая система ПК, ее структуры и объекты (*.EXE, *.COM, *.BAT файлы)
- **Способы заражения:** добавление своего кода к программе
- Получают управление при запуске зараженного объекта

Макро-вирусы

- **Заражаемые объекты:** объекты некоторых системы обработки данных (MS Office и др.)
- **Способ заражения:** встраивание своего кода в макросы документа
- Получают управление при выполнении зараженного макроса



Сетевые вирусы



- **Заражаемые объекты:** оперативная память ПК
- **Способ заражения:** проникновение из сети с использованием сетевых протоколов
- В чистом виде сетевые вирусы не получили широкого распространения.

Источники заражения компьютерными вирусами

Источники заражения

Носители информации

Компьютерные сети

Пиратское ПО

Электронная почта (E-mail)

ПК «общего пользования»

Серверы обмена файлами (ftp, BBS)

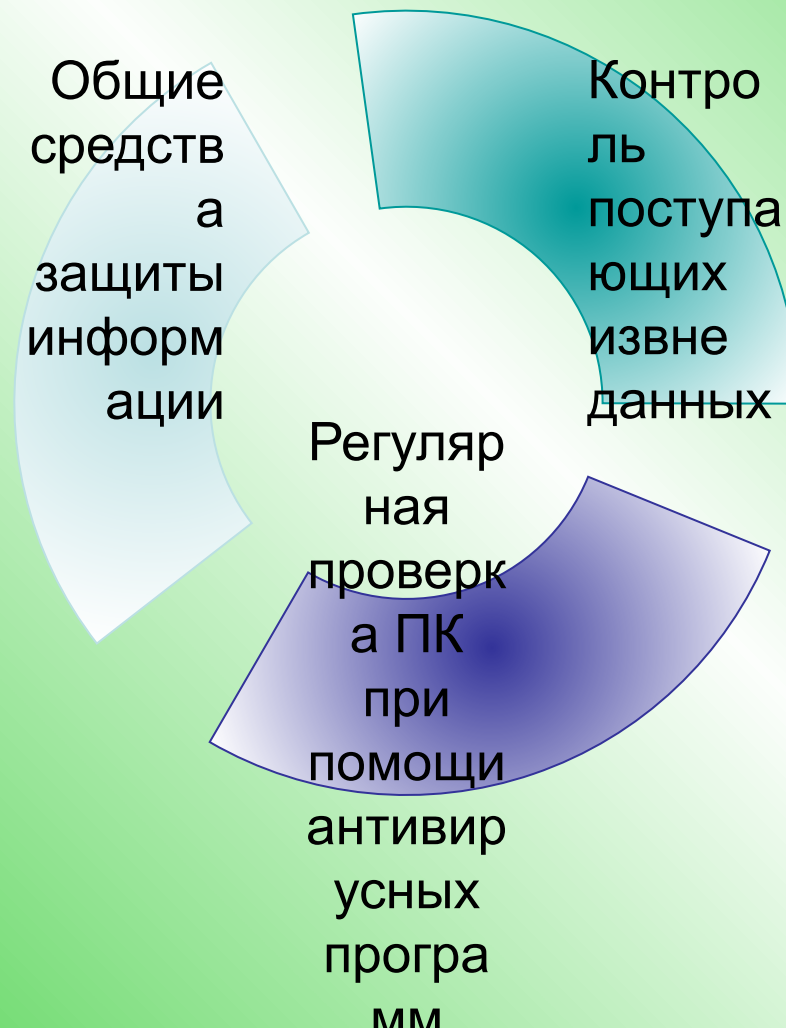
Сервисные службы

«Дыры» в защите ПО

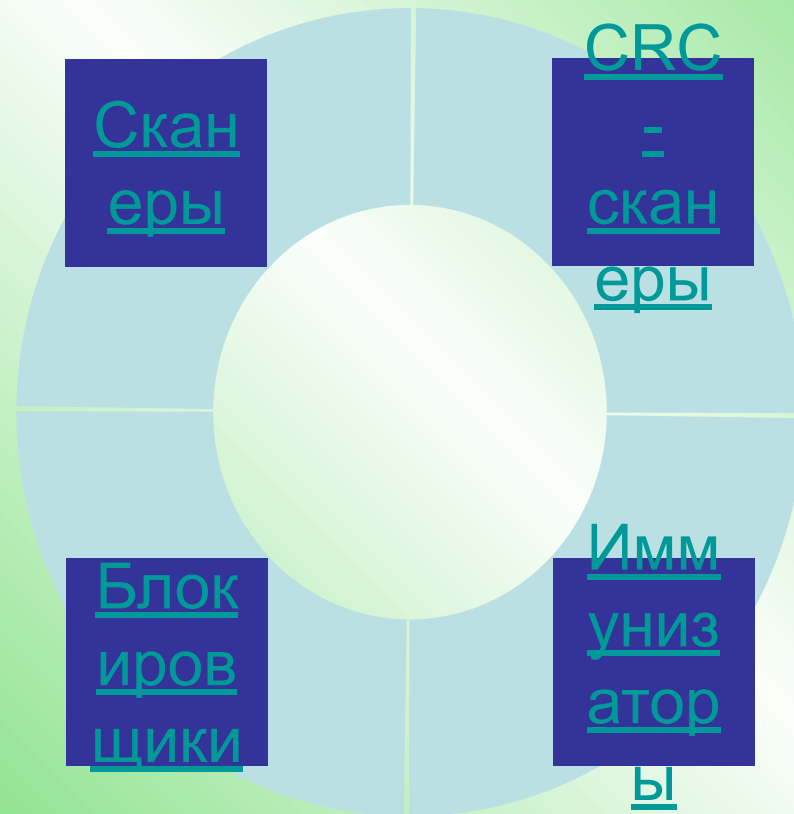
Обмен информацией

Web-страницы, документы

Профилактика заражения компьютерными вирусами



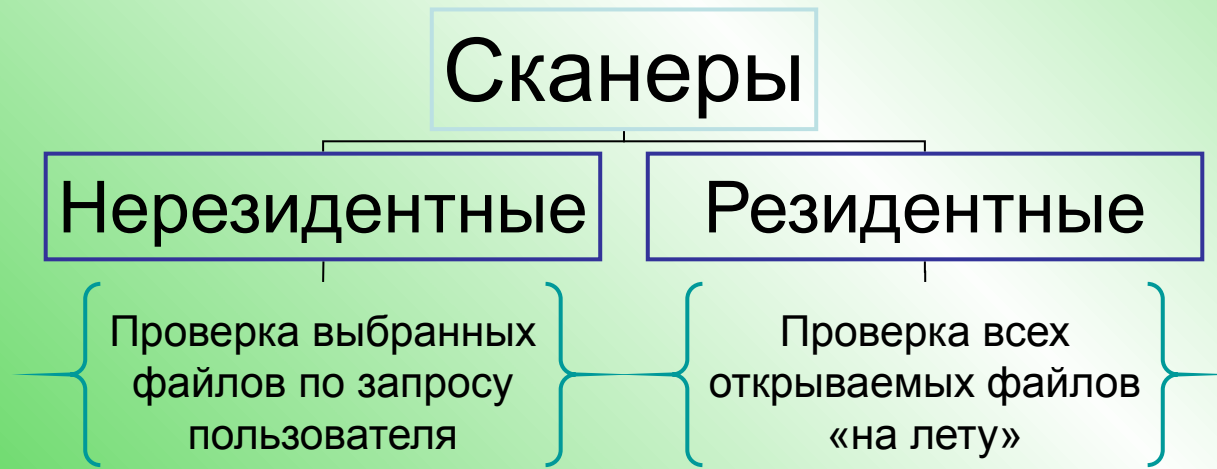
Классификация антивирусных программ



Антивирусные сканеры

Другие названия: детекторы, фаги, полифаги

- **Метод работы:** поиск по маске и эвристический анализ
- **Достоинства:** универсальность, сбалансированность
- **Недостатки:** Большое время проверки, большие размеры вирусных баз, необходимость постоянного обновления баз



CRC-сканеры

Другое название: ревизоры

- **Метод работы:** Создание базы данных контрольных сумм файлов и последующее сравнение реальных значений с записанными ранее
- **Достоинства:** высокая эффективность и скорость проверки
- **Недостатки:** Невозможность обнаружения вирусов в момент их появления

Блокировщики

Другое название: фильтры

- **Метод работы:** Перехват потенциально опасных действий программ и выдача сообщения об этом пользователю.
- **Достоинства:** обнаружение и остановка вируса на ранней стадии его размножения
- **Недостатки:** возможность обхода защиты блокировщиков и большое количество ложных срабатываний

Иммунизаторы

Другое название: вакцины

- **Метод работы:** Модификация программ таким образом, что конкретный вирус считает их уже зараженными
- **Достоинства:** эффективны против конкретного вируса
- **Недостатки:** взаимоисключение вакцин от разных вирусов, невозможность вакцинации от неизвестных вирусов

В настоящее время практически не используются

Современные антивирусы



Антивирус
Касперского



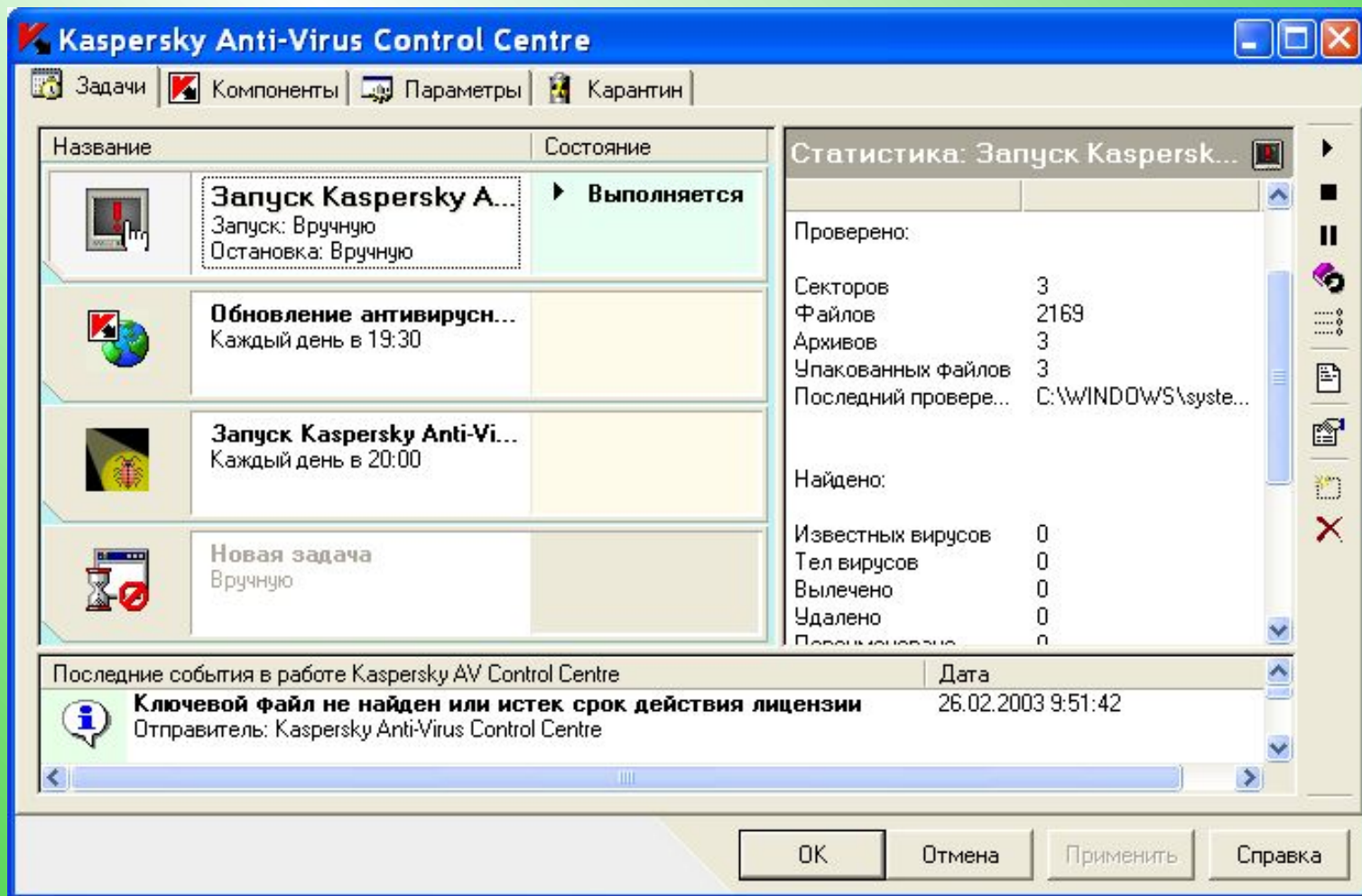
Dr. Web для Windows

Антивирусные программы:

Антивирус Касперского

- **Разработчик:** «Лаборатория Касперского»
- **ОС:** MS Windows, MS DOS, OS/2, Linux, Novell NetWare, Unix, Solaris
- **Возможности:**
 - Нерезидентный и резидентный сканеры
 - Проверка почты
 - Проверка макросов
 - Система автоматического обновления
 - CRC-сканер
 - Планировщик
 - Специальная система защиты MS Office
- **Интерфейс:**
 - Модульный интерфейс
 - Центр управления компонентами

Антивирусные программы: Антивирус Касперского



Kaspersky Anti-Virus Control Centre. Главное окно программы (версия 4)

Антивирусные программы: Dr. Web для Windows

- **Разработчик:** «Лаборатория Данилова» и «ДиалогНаука»
- **ОС:** MS Windows, Novell NetWare, Linux, FreeBSD, Solaris
- **Возможности:**
 - Нерезидентный сканер
 - Резидентный сканер SpIDer
 - Система автоматического обновления через Internet
 - Планировщик
- **Интерфейс**
 - Простой, удобный интерфейс.
 - Наглядные и гибкие средства выбора объектов тестирования путем просмотра дерева подкаталогов вплоть до уровня отдельных файлов.

Антивирусные программы: Dr. Web для Windows



Dr. Web for Windows Главное окно программы (версия 4.29)

Антивирусные программы

Сообщение о вирусе



Сообщение об обнаружении вируса. Kaspersky Anti-Virus Monitor (версия 4)

Признаки заражения КОМПЬЮТЕРНЫМ ВИРУСОМ

- прекращение работы или неправильная работа ранее успешно функционировавших программ
- медленная работа компьютера
- невозможность загрузки операционной системы
- исчезновение файлов и каталогов или искажение их содержимого
- изменение даты и времени модификации файлов
- изменение размеров файлов
- неожиданное значительное увеличение количества файлов на диске
- существенное уменьшение размера свободной оперативной памяти
- вывод на экран непредусмотренных сообщений или изображений
- подача непредусмотренных звуковых сигналов
- частые зависания и сбои в работе компьютера

Действия при заражении компьютерным вирусом

- Не паниковать
- Выключить ПК
- Проверить ПК на вирусы при помощи заранее подготовленной загрузочной дискеты с антивирусом
- По возможности восстановить всю информацию с незараженных резервных копий
- Если невозможно самостоятельно решить проблему, обратиться к специалистам

Заключение

- При обнаружении вируса, неизвестного используемой вами антивирусной программе соберите образцы зараженных программ и отправьте их производителю вашего антивирусного ПО.
- Главное средство борьбы с компьютерными вирусами – просвещение. Знание – СИЛА!

Вопрос:

Компьютерный вирус –
это программа?

1. да

2. нет



Правильный ответ:

Компьютерный вирус — это специально написанная, размножающаяся программа, выполняющая нежелательные действия на ПК.



И помните, что лучшая
защита информации это
антивирусная
профилактика!

