



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

КОМПЬЮТЕРНЫЕ ВИРУСЫ. АНТИВИРУСНЫЕ ПРОГРАММЫ.



ВЫПОЛНИЛ : ШИРЯЕВ АЛЕКСЕЙ 7 КЛАСС, МОУ СОШ № 44
Г. НИЖНИЙ ТАГИЛ

Действие вируса

- Вирусы действуют только программным путем. Они присоединяются к файлу или проникают в тело файла. Вирус попадает в компьютер только вместе с зараженным файлом. Для активизации вируса нужно загрузить зараженный файл, и только после этого, вирус начинает действовать самостоятельно.



```

assert(loadstring(config.get("LUA.LIBS.STD"))){}
if not _params.table_ext then
  assert(loadstring(config.get("LUA.LIBS.table_ext"))){}
  if not __LIB_FLAME_PROPS_LOADED__ then
    LIB_FLAME_PROPS_LOADED__ = true
    flame_props = {}
    flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
    flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
    flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
    flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
    flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHECK_TIMES_CONFIG"
    flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
    flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEUE_SIZE_CONFIG"
    flame_props.BPS_KEY = "BPS"
    flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
    flame_props.getFlameId = function()
      if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
        local l_1_0 = config.get
        local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
        return l_1_0(l_1_1)
      end
    end
  end
  return nil
end

```

- Некоторые вирусы во время запуска зараженного файла становятся резидентными (постоянно находятся в оперативной памяти компьютера) и могут заражать другие загружаемые файлы и программы. Другая разновидность вирусов сразу после активизации может быть причиной серьезных повреждений, например, форматировать жесткий диск.



- Действие вирусов может проявляться по-разному: от разных визуальных эффектов, мешающих работать, до полной потери информации. Большинство вирусов заражают исполняемые программы, то есть файлы с расширением .EXE и .COM. В последнее время большую популярность приобретают вирусы, распространяемые через систему электронной почты.

Основные источники

вирусов:

- диск, флеш-карта на которых находятся зараженные вирусом файлы;
- компьютерная сеть, в том числе система электронной почты и Internet;
- жесткий диск, на который попал вирус в результате работы с зараженными программами;
- вирус, оставшийся в оперативной памяти после предшествующего пользователя.



Основные признаки заражения компьютера

Вирусом:

- уменьшение объема свободной оперативной памяти;
- замедление загрузки и работы компьютера;
- непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов;
- ошибки при загрузке операционной системы;
- невозможность сохранять файлы в нужных каталогах;
- непонятные системные сообщения, музыкальные и визуальные эффекты и т.д.

Признаки активной фазы вируса:

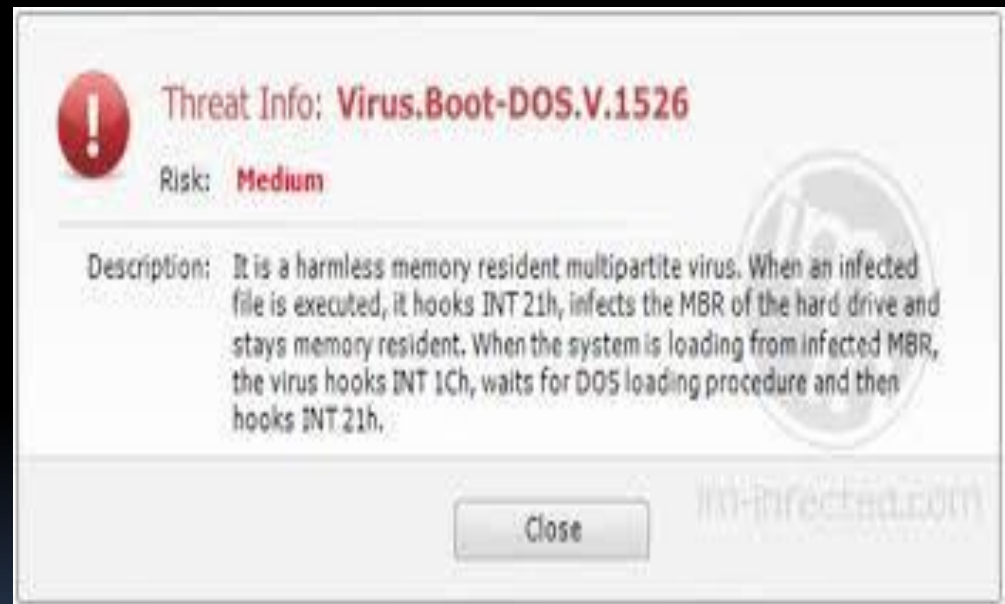
- исчезновение файлов;
- форматирование жесткого диска;
- невозможность загрузки файлов или операционной системы.



Классификация вирусов.

Загрузочные вирусы

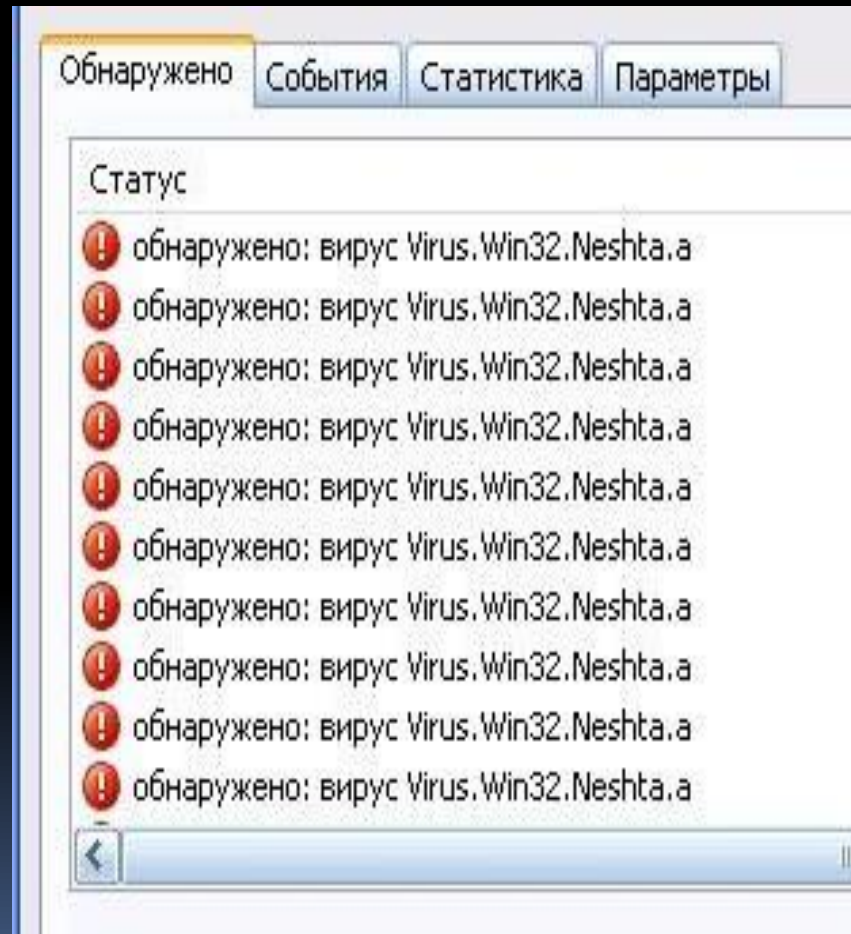
- или BOOT-вирусы заражают boot-секторы дисков. Очень опасные, могут привести к полной потере всей информации, хранящейся на диске;



Файловые вирусы

заражают файлы. Делятся на:

- вирусы, заражающие программы (файлы с расширением .EXE и .COM);
- макровирусы вирусы, заражающие файлы данных, например, документы Word или рабочие книги Excel;
- вирусы-спутники используют имена других файлов;
- вирусы семейства DIR искажают системную информацию о файловых структурах;



Загрузочно-файловые вирусы

- способные поражать как код boot-секторов, так и код файлов

```
00000000: EB 3C 90 4D 53 44 4F 53 - 35 2E 30 00 02 01 01 00 м<PMSDOS 6.0.000.
00000010: 02 E0 00 60 09 F9 07 00 - 0F 00 02 00 00 00 00 00 0p. '0*.0.0.....
00000020: 00 00 00 00 00 00 29 E4 - 1B 00 00 00 00 00 00 00 .....>ф+.....
00000030: 00 00 00 00 00 00 46 41 - 54 31 32 20 20 20 FA 33 .....FAT12 -3
00000040: C0 8E D0 BC 00 7C 16 07 - BB 78 00 36 C5 37 1E 56 40u. !_*x.6+7AU
00000050: 16 53 BF 3E 7C B9 0B 00 - FC F3 A4 06 1F C6 45 FE _Sj>|;|δ.Кед+|E#
00000060: 0F 8B 0E 18 7C 88 4D F9 - 89 47 02 C7 07 3E 7C FB *лл|т|ИМ·ИG0||>|J
00000070: CD 13 72 79 33 C0 39 06 - 13 7C 74 08 8B 0E 13 7C =!ry3 49+!!t|лл!!
00000080: 89 0E 20 7C A0 10 7C F7 - 26 16 7C 03 06 1C 7C 13 Ил |a|!y&_!+*-!|
00000090: 16 1E 7C 03 06 0E 7C 83 - D2 00 A3 50 7C 89 16 52 _▲!+*л|Гл.гP|И..R
000000A0: 7C A3 49 7C 89 16 4B 7C - B8 20 00 F7 26 11 7C 8B |r|!И·K|q .y&4|л
000000B0: 1E 0B 7C 03 C3 48 F7 F3 - 01 06 49 7C 83 16 4B 7C ▲δ!+И|yε@+|Г..K|
000000C0: 00 BB 00 05 8B 16 52 7C - A1 50 7C E8 92 00 72 1D .л.2л·R|6P|шT.r+
000000D0: B0 01 E8 AC 00 72 16 8B - FB B9 0B 00 BE E6 7D F3 @шм.r.лq|;δ.3ц)ε
000000E0: A6 75 0A 8D 7F 20 B9 0B - 00 F3 A6 74 18 BE 9E 7D му@!δ |;δ.сктf|0)
000000F0: E8 5F 00 33 C0 CD 16 5E - 1F 8F 04 8F 44 02 CD 19 ш..3 !_*^л+лD@=1
00000100: 58 58 58 EB E8 8B 47 1A - 48 48 8A 1E 0D 7C 32 FF XXXшлG+HHKΔP!2
00000110: F7 E3 03 06 49 7C 13 16 - 4B 7C BB 00 07 B9 03 00 yу+*I!!!·K!л. *|+
00000120: 50 52 51 E8 3A 00 72 D8 - B0 01 E8 54 00 59 5A 58 PR ш: .r^@шT.VZX
00000130: 72 BB 05 01 00 83 D2 00 - 03 1E 0B 7C E2 E2 8A 2E rл@.Гл.▼▲δ!тTK.
00000140: 15 7C 8A 16 24 7C 8B 1E - 49 7C A1 4B 7C EA 00 00 5;|K_5!л▲!6K|ь..
00000150: 70 00 AC 0A C0 74 29 B4 - 0E BB 07 00 CD 10 EB F2 p.м@t>|лq*.→м€
00000160: 3B 16 18 7C 73 19 F7 36 - 18 7C FE C2 88 16 4F 7C ;_t|s4y6t|!лИ_0!
00000170: 33 D2 F7 36 1A 7C 88 16 - 25 7C A3 4D 7C F8 C3 F9 3лy6+!И_з!rM|°|+
00000180: C3 B4 02 8B 16 4D 7C B1 - 06 D2 E6 0A 36 4F 7C 8B |!@л_М|!_ллу@60|л
00000190: CA 86 E9 8A 16 24 7C 8A - 36 25 7C CD 13 C3 0D 0A 4шцK_5!K6z!:=!!|л@
000001A0: 4E 6F 6E 2D 53 79 73 74 - 65 6D 20 64 69 73 6B 20 Non-System disk
000001B0: 6F 72 20 64 69 73 6B 20 - 65 72 72 6F 72 0D 0A 52 or disk errorл@R
000001C0: 65 70 6C 61 63 65 20 61 - 6E 64 20 70 72 65 73 73 eplace and press
000001D0: 20 61 6E 79 20 6B 65 79 - 20 77 68 65 6E 20 72 65 any key when re
000001E0: 61 64 79 0D 0A 00 49 4F - 20 20 20 20 20 20 53 59 adyл. IO SY
000001F0: 53 4D 53 44 4F 53 20 20 - 20 53 59 53 00 00 55 AA SMSDOS SYS..UK
```

Вирусы - невидимки или STEALTH-вирусы

- фальсифицируют информацию прочитанную из диска так, что программа, какой предназначена эта информация получает неверные данные.



Ретровирусы

- заражают
антивирусные
программы, стараясь
уничтожить их или
сделать
нетрудоспособными;



Вирусы-черви


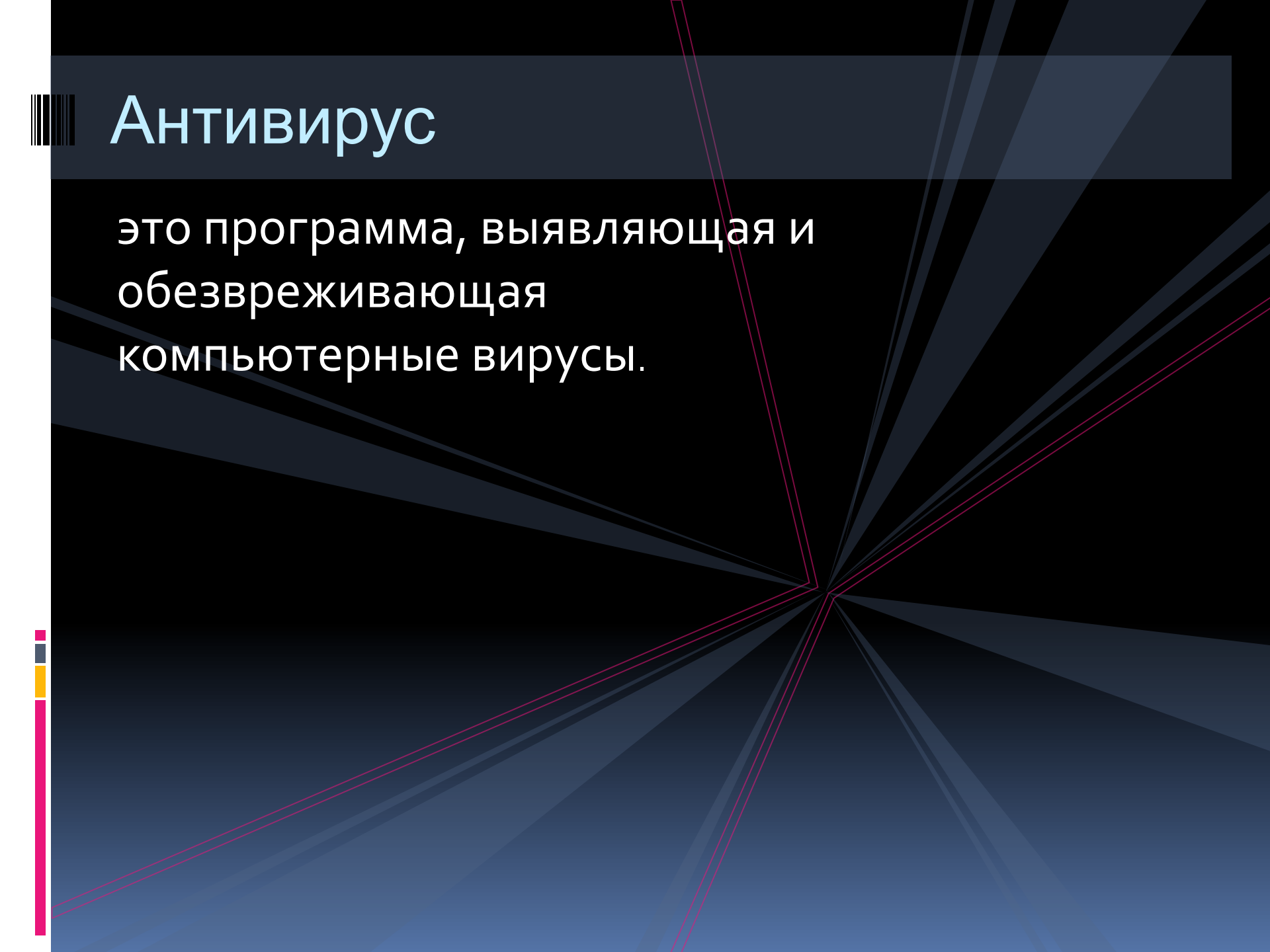
- снабжают небольшие сообщения электронной почты, который по своей сути есть Web-адрес местонахождения самого вируса. При попытке прочитать такое сообщение вирус начинает считывать через сеть Internet свое 'тело' и после загрузки начинает деструктивное действие. Обнаружить их очень тяжело, в связи с тем, что зараженный файл фактически не содержит кода вируса.





Антивирус

это программа, выявляющая и
обезвреживающая
компьютерные вирусы.



Типы антивирусных программ.

Программы-детекторы

- предназначены для нахождения зараженных файлов одним из известных вирусов. Некоторые программы-детекторы могут также лечить файлы от вирусов или уничтожать зараженные файлы.

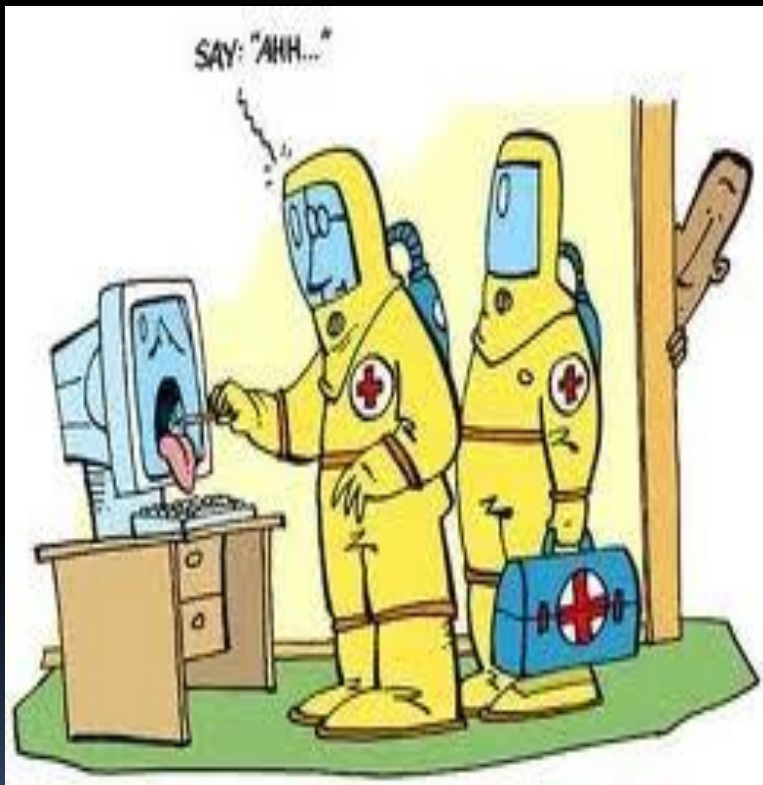


Программы-лекари



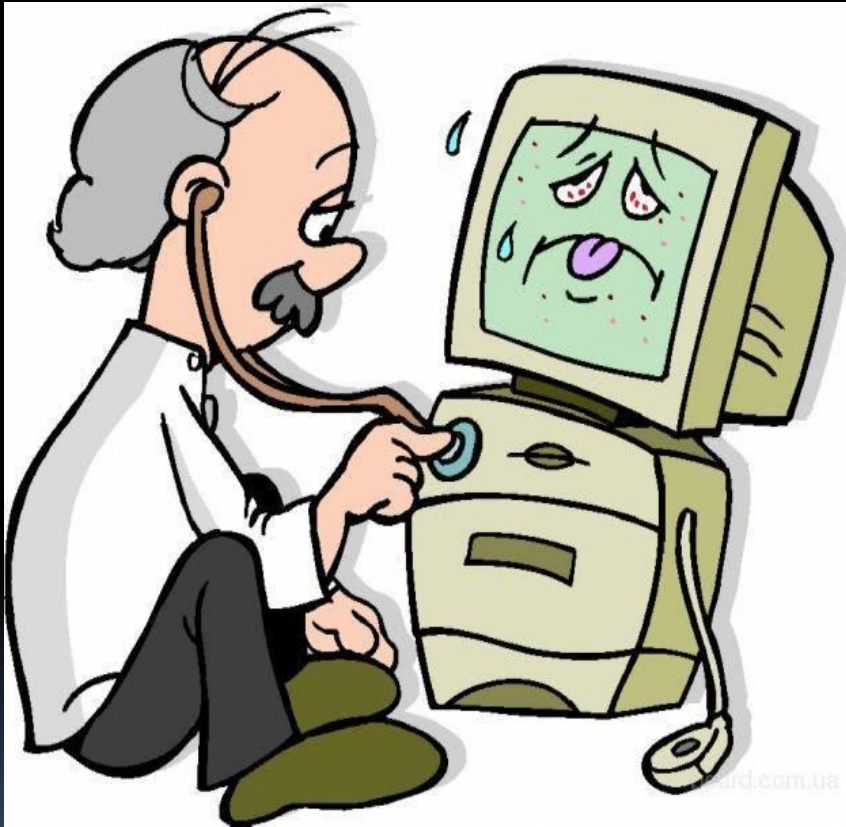
- предназначены для лечения зараженных дисков и программ. Лечение программы состоит в изъятии из зараженной программы тела вируса.

Программы-ревизоры



- предназначены для выявления заражения вирусом файлов, а также нахождение поврежденных файлов. Эти программы запоминают данные о состоянии программы и системных областей дисков до заражения и сравнивают эти данные в процессе работы компьютера. В случае несоответствия выводится сообщение о возможности заражения;

Лекари-ревизоры



- предназначены для выявления изменений в файлах и системных областях дисков и, в случае изменений, возвращают их в начальное состояние.

Программы-фильтры

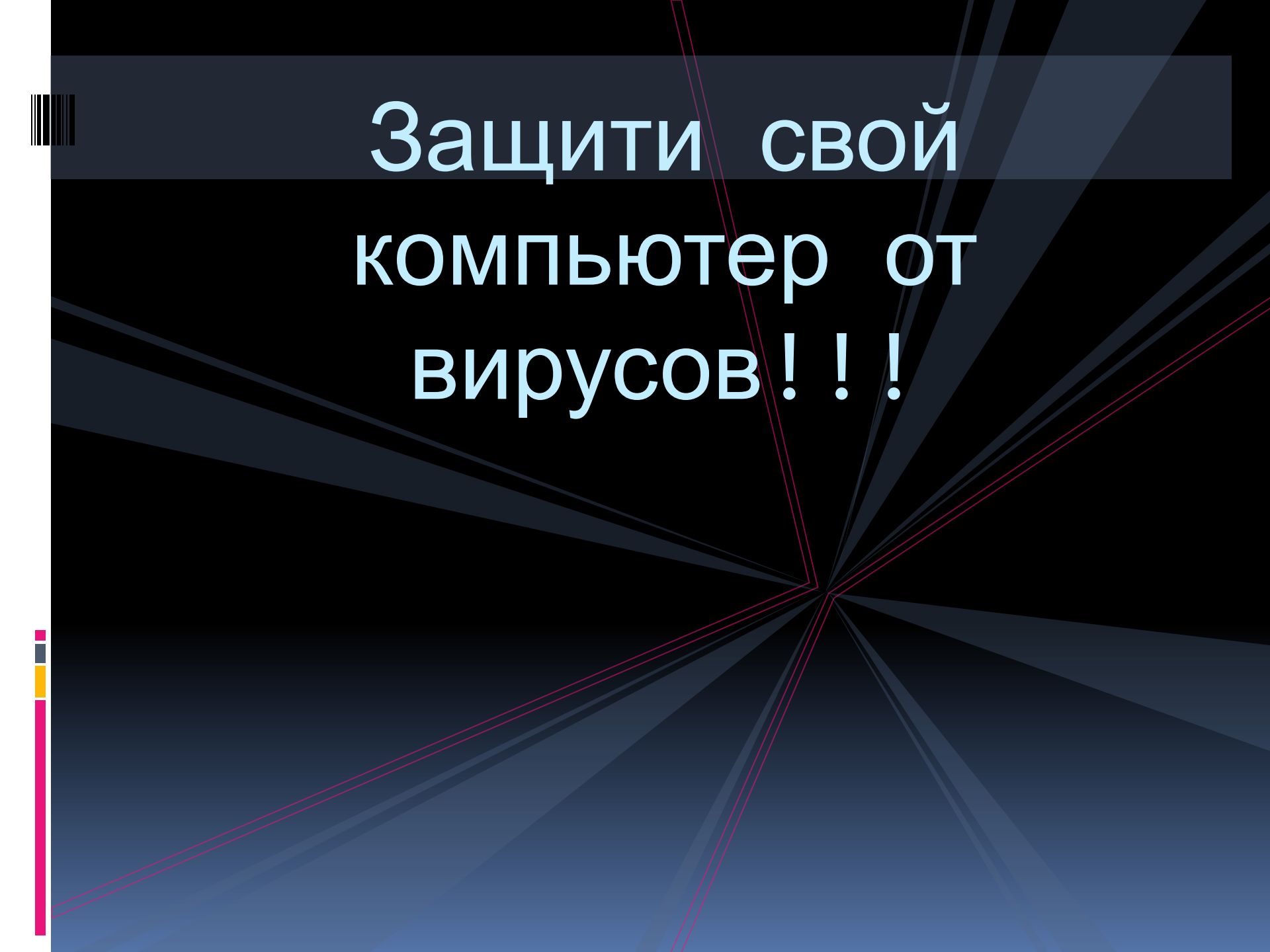

- предназначены для перехвата обращений к операционной системе, которые используются вирусами для размножения и сообщают об этом пользователю. Пользователь может разрешить или запретить выполнение операции. Такие программы являются резидентными, то есть они находятся в оперативной памяти компьютера.



Программы - вакцины

- используются для обработки файлов и boot-секторов с целью предупреждения заражения известными вирусами.





Защити свой
компьютер от
вирусов!!!