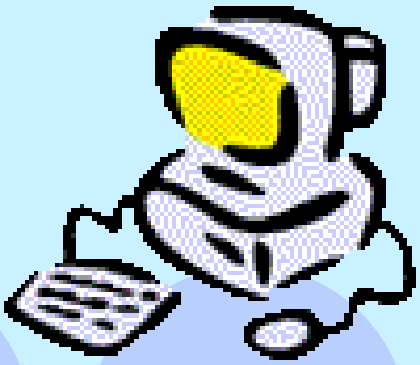


Компьютерные вирусы и антивирусные программы

Введение

В настоящее время очень многие области деятельности человека связаны с применением компьютеров. Они выполняют рутинную расчетную и оформительскую работу, освобождая наш мозг для более необходимых и ответственных задач. В результате утомляемость резко снижается, и мы начинаем работать гораздо производительнее, нежели без применения компьютера.

Но кто бы мог подумать, что этому электронному чуду техники свойственны болезни похожие на человеческие. Он, так же как и человек может подвергнуться атаке "вируса" но компьютерного. И если не принять мер, компьютер скоро "заболеет" т.е. начнет выполнять неправильные действия или вообще "умрет", т.е. повреждения нанесенные "вирусом" окажутся очень серьезными.

Что такое вирус?

- Первая «эпидемия» компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг») «заражал» дискеты персональных компьютеров.
- В настоящее время известно более 50 тысяч вирусов, заражающих компьютеры и распространяющихся по компьютерным сетям.
- **Компьютерные вирусы – *это программы, которые могут «размножаться» (самокопироваться) и незаметно для пользователя внедрять свой программный код в файлы, документы, Web-страницы Всемирной паутины и сообщения электронной почты.***

Двадцатка наиболее распространенных вредоносных программ

1. I-Worm.Klez
2. I-Worm.Sobig
3. I-Worm.Lentin
4. I-Worm.Avron
5. Macro.Word97.Thus
6. I-Worm.Tanatos
7. Macro.Word97.Marker
8. Worm.Win32.Opasoft
9. Worm.Hybris
10. Win95.CIH

11. Worm.Win32.Randon
12. VBS.Redlof
13. Backdoor.Death
14. Win95.Spaces
15. I-Worm.Roron
16. Trojan.PSW.Gip
17. Backdoor.NetDevil
18. Win32.HLLP.Hantaner
19. TrojanDropper.Win32.Delf
20. TrojanDropper.Win32.Yabinder

Типы вредоносных программ

Виды вирусов

- После заражения компьютера вирус может активизироваться и начать выполнять вредные действия по уничтожению программ и данных.
- Активизация вируса может быть связана с различными событиями: наступлением определенной даты или дня недели, запуском программы, открытием документа и некоторыми другими.
- По «среде обитания» вирусы можно разделись на **файловые вирусы, макровирусы и сетевые вирусы**.

Файловые вирусы

Внедряются в программы и активи-зируются при их запуске.

После запуска зараженной программы вирусы находятся в оперативной памяти компьютера и могут заражать другие файлы до момента выключения компьютера или перезагрузки операци-онной системы.

Макровирусы

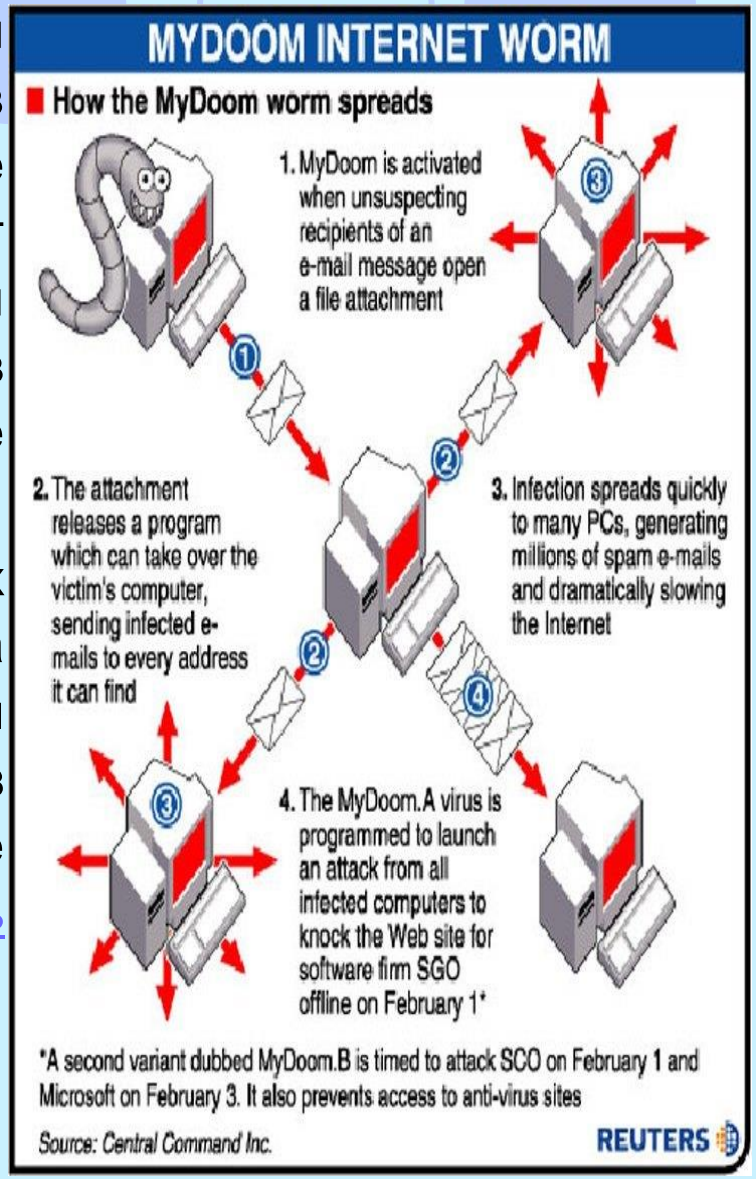
- **Заражают файлы документов**, (например текстовых документов).
- После загрузки зараженного документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы.
- Угроза заражения прекращается только после закрытия текстового редактора.

Сетевые вирусы

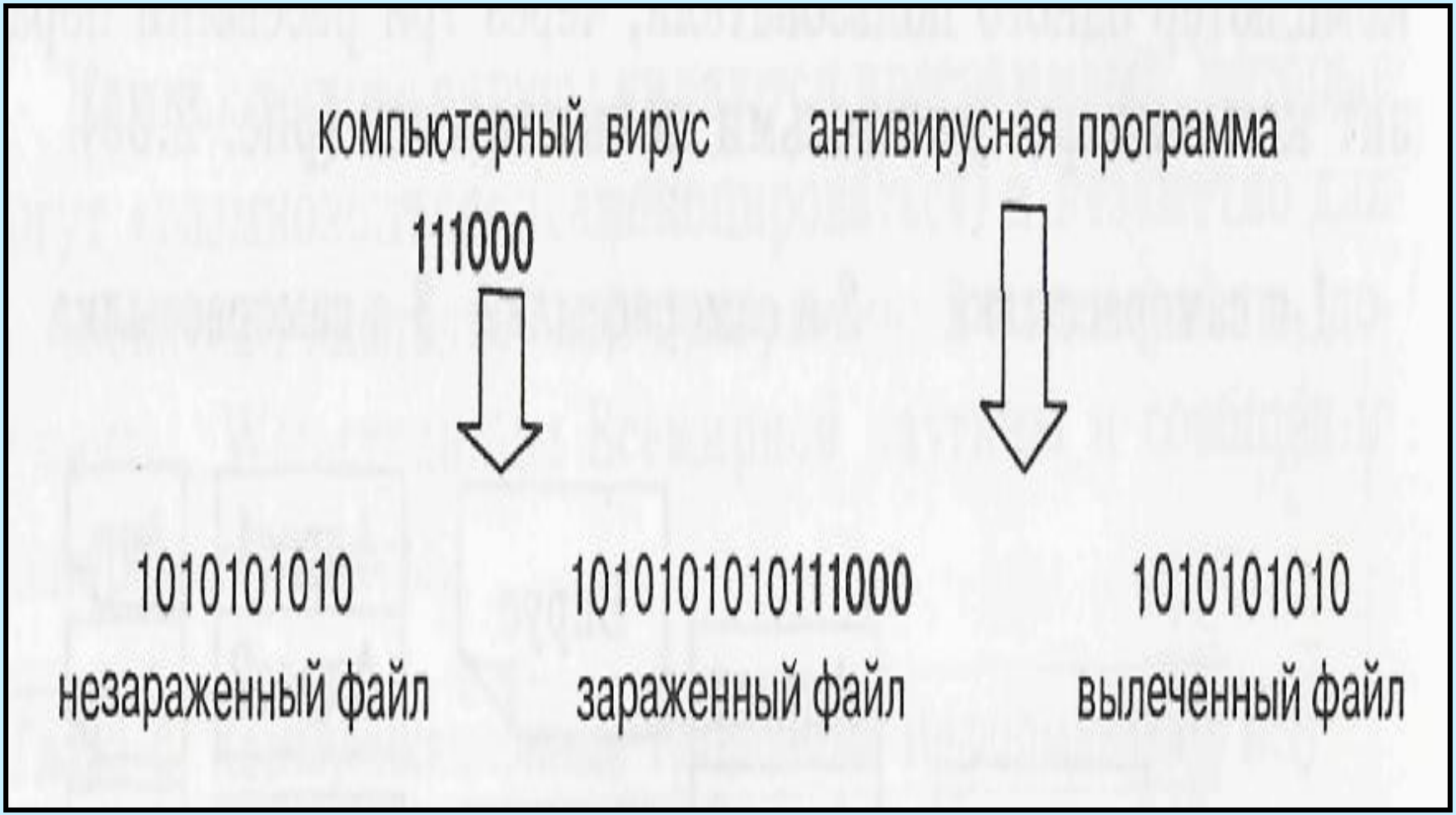
- *Передают по компьютерным сетям свой программный код и запускают его на компьютерах, подключенных к этой сети.*
- **Заражение** сетевым вирусом может произойти при **работе с электронной почтой** или при **«путешествиях» по Всемирной паутине.**
- Наибольшую опасность создают почтовые сетевые вирусы, которые распространяются по компьютерным сетям во вложенных в почтовое сообщение файлах.
- Активизация почтового вируса и заражение компьютера может произойти при просмотре сообщения электронной почты.

Лавинообразная цепная реакция распространения почтовых вирусов базируется на том, что вирус после заражения компьютера начинает рассылать себя по всем адресам электронной почты, которые имеются в электронной адресной книге пользователя.

Например, даже если в адресных книгах пользователей имеются только по два адреса, почтовый вирус, заразивший компьютер одного пользователя, через три рассылки поразит компьютеры уже восьми пользователей (смотреть рисунок).



Заражение файла компьютерным вирусом и его лечение с использованием антивирусной программы



Основные источники вирусов.

- Дискета, CD, Flash.
- Жесткий диск

- Компьютерная сеть
- Локальная или глобальная сеть

Основные ранние 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

Существует очень много разных вирусов.

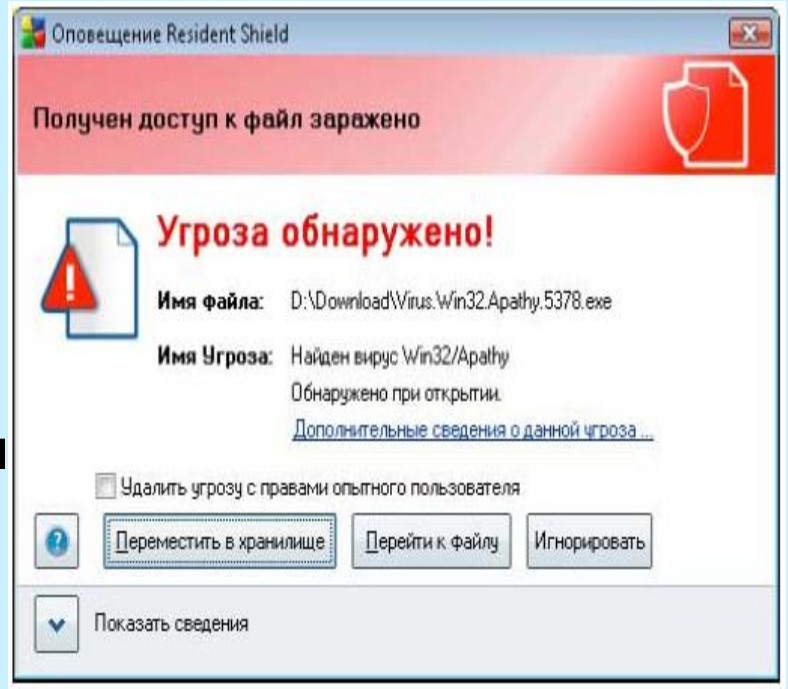
Условно их можно классифицировать следующим образом:

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

2) **файловые вирусы** заражают файлы.

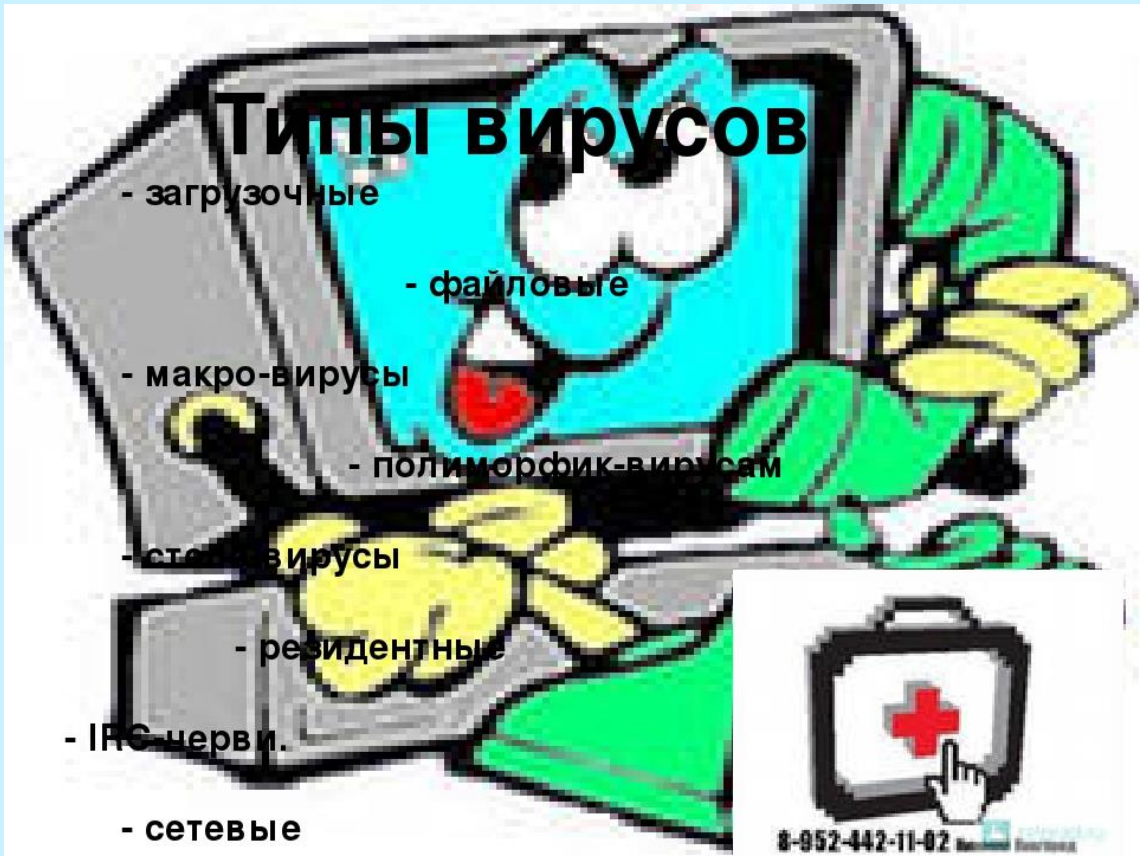
Делятся на:

- **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;



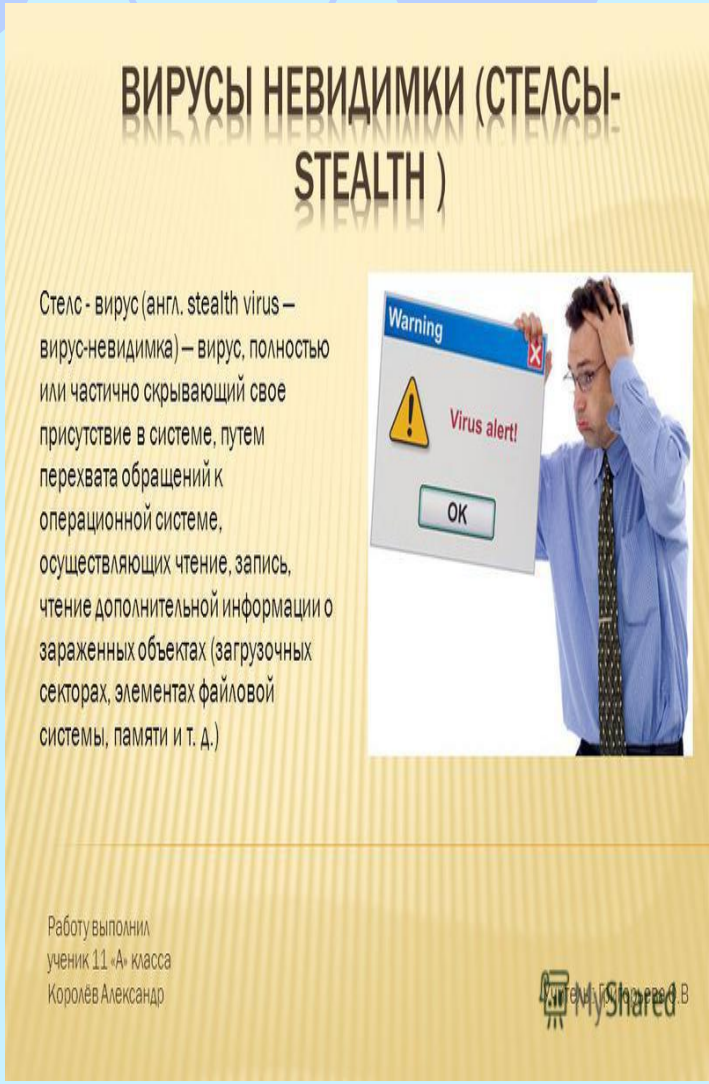
3) **загрузочно-файловые вирусы**

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



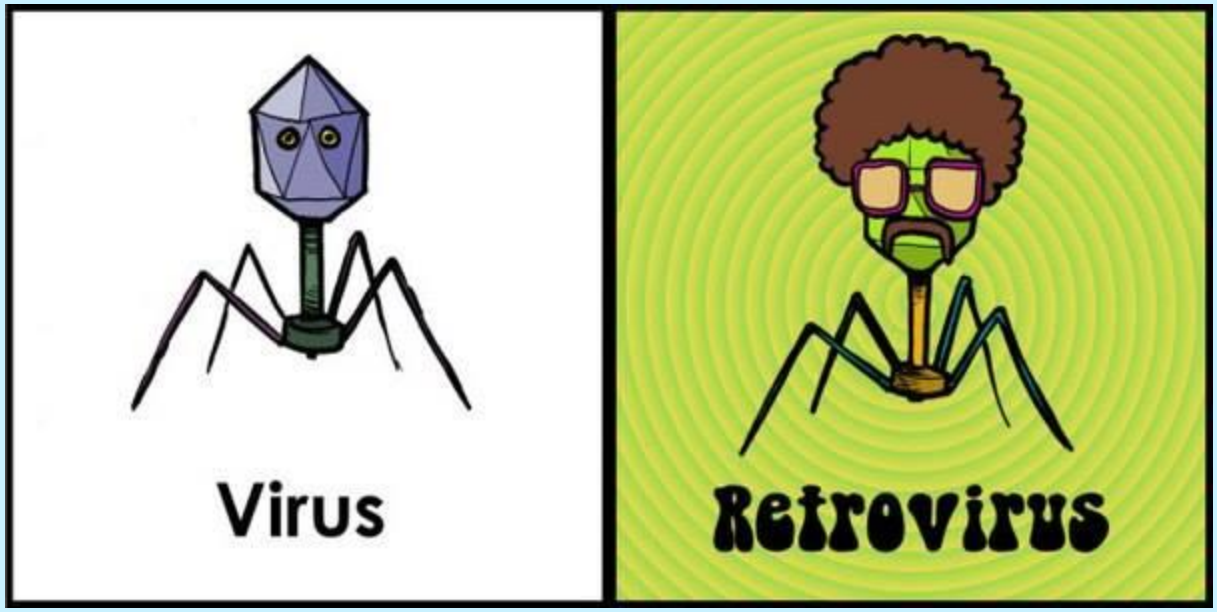
4) **вирусы-невидимки** или STEALTH-вирусы

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



5) **ретровирусы**

заражают антивирусные программы, стараясь уничтожить их или сделать нетрудоспособными;



6) **вирусы-черви**

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

Безвредные вирусы проявляются только в том, что уменьшают объем памяти на диске в результате своего распространения.
Неопасные вирусы, кроме отмеченного проявления, порождают графические, звуковые и другие эффекты.

К программным средствам защиты относят разные антивирусные программы (антивирусы).

- Антивирус - это программа, выявляющая и обезвреживающая компьютерные вирусы.
- Следует заметить, что вирусы в своем развитии опережают антивирусные программы, поэтому даже в случае регулярного пользования антивирусов, нет 100% гарантии безопасности.
- Антивирусные программы могут выявлять и уничтожать лишь известные вирусы, при появлении нового компьютерного вируса защиты от него не существует до тех пор, пока для него не будет разработан свой антивирус.
- Однако, много современных антивирусных пакетов имеют в своем составе специальный программный модуль, называемый эвристическим анализатором, который способен исследовать содержимое файлов на наличие кода, характерного для компьютерных вирусов. Это дает возможность своевременно выявлять и предупреждать об опасности заражения новым вирусом.

Вспомогательными средствами защиты информации

являются средства аппаратной защиты.

Так, например, простое отключение перемычки на материнской плате не позволит осуществить стирание перепрограммируемой микросхемы ПЗУ (флэш-BIOS), независимо от того, кто будет пытаться это сделать: компьютерный вирус, злоумышленник или неаккуратный пользователь.

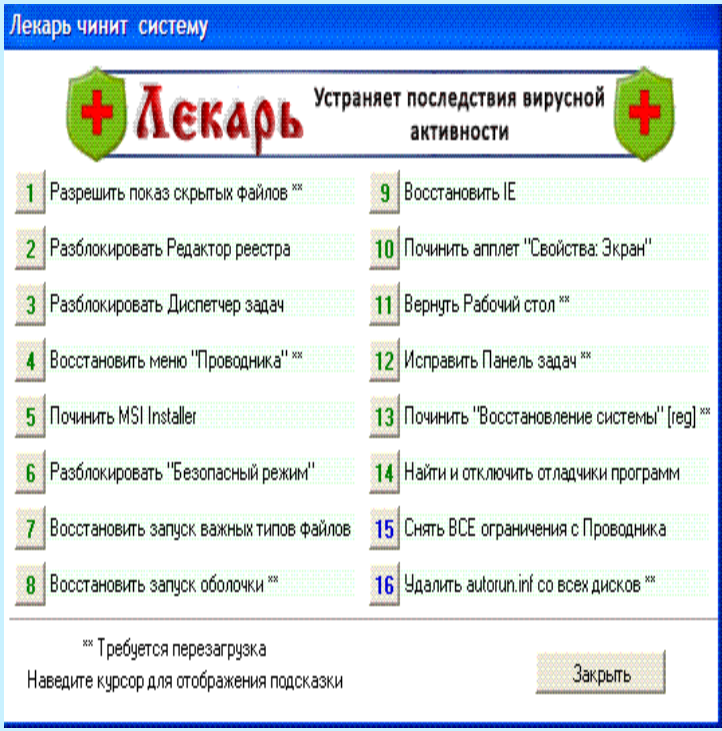
Различают такие типы антивирусных программ:

1) **программы-детекторы**:

предназначены для нахождения зараженных файлов одним из известных вирусов. Некоторые программы-детекторы могут также лечить файлы от вирусов или уничтожать зараженные файлы. Существуют специализированные, то есть предназначенные для борьбы с одним вирусом детекторы и полифаги, которые могут бороться с многими вирусами;

2) **программы-лекари**:

предназначены для лечения зараженных дисков и программ. Лечение программы состоит в изъятии из зараженной программы тела вируса. Также могут быть как полифагами, так и специализированными;



3) **программы-ревизоры**:

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

4) **лекари-ревизоры**:

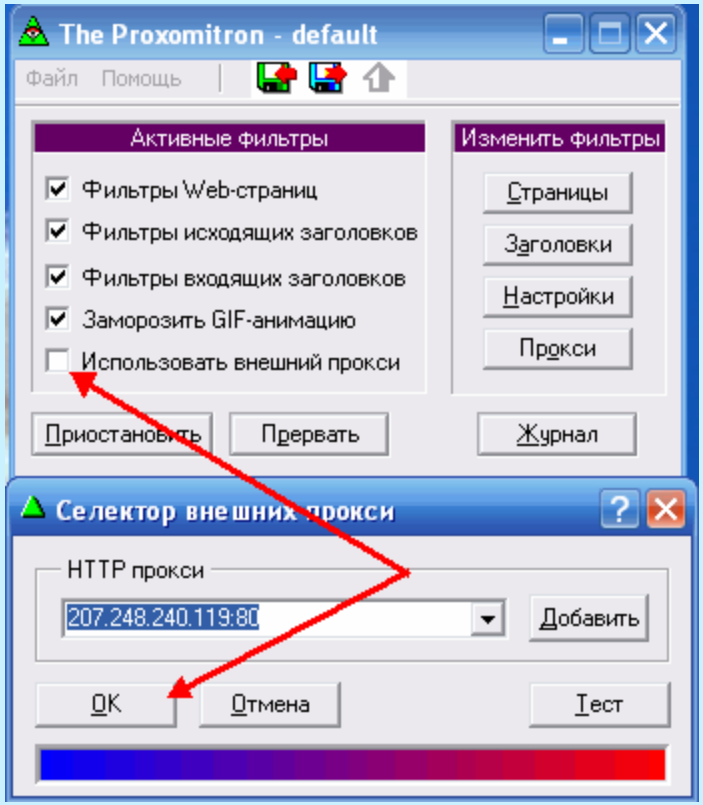
предназначены для выявления изменений в файлах и системных областях дисков и, в случае изменений, возвращают их в начальное состояние

5) **программы-фильтры**:

предназначены для перехвата обращений к операционной системе, которые используются вирусами для размножения и сообщают об этом пользователя.

Пользователь может разрешить или запретить выполнение соответствующей операции.

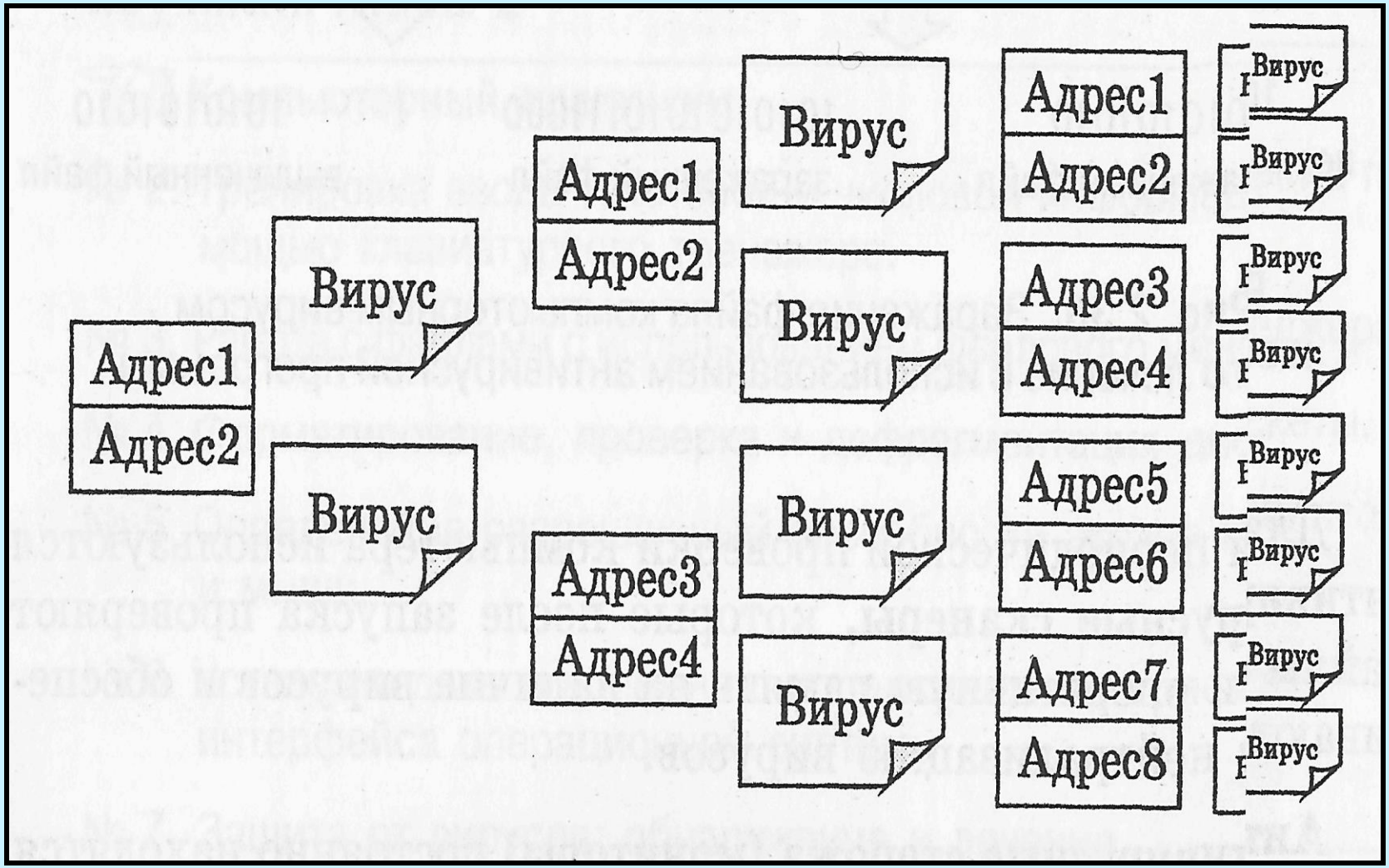
Такие программы являются резидентными, то есть они находятся в оперативной памяти компьютера.



6) **программы-вакцины**:

используются для обработки файлов и boot-секторов с целью предупреждения заражения известными вирусами (в последнее время этот метод используется все чаще).

Лавинообразное заражение ПК почтовым вирусом



Из истории

Всемирная эпидемия заражения почтовым вирусом началась **5 мая 2000 года**, когда десятки миллионов компьютеров, подключенных к глобальной компьютерной сети Интернет, получили почтовое сообщение с привлекательным названием ILOVEYOU (англ. «Я люблю тебя»).

Сообщение содержало вложенный файл, являющийся вирусом.

После прочтения этого сообщения получателем вирус заражал компьютер и начинал разрушать файловую систему.

Кто создаёт вирусы?

Вирусы пишутся опытными программистами или студентами просто из любопытства или для отместки кому-либо или предприятию, которое обошлось с ними недостойным образом или в коммерческих целях или в целях направленного вредительства.

Какие бы цели не преследовал автор, вирус может оказаться на вашем компьютере и постарается произвести те же вредные действия, что и у того, для кого он был создан.

Антивирусные программы

В целях профилактической защиты от компьютерных вирусов не рекомендуется запускать программы, открывать документы и сообщения электронной почты, полученные из сомнительных источников и предварительно не проверенные **антивирусными программами.**

- Наиболее эффективны в борьбе с компьютерными вирусами **антивирусные программы**.
- Антивирусные программы используют постоянно обновляемые списки известных вирусов, которые включают название вирусов и их программные коды.
- **Если антивирусная программа обнаружит компьютерный код вируса в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению,**
- **т.е. из него удаляется программный код вируса.**
- Если лечение невозможно, то зараженный файл удаляется целиком (смотреть рисунок).

- Для периодической проверки компьютера используются **антивирусные сканеры,** которые после запуска проверяют файлы и оперативную память на наличие вирусов и обеспечивают нейтрализацию вирусов.
- **Антивирусные сторожа (мониторы)** постоянно находятся в оперативной памяти компьютера и обеспечивают проверку файлов в процессе их загрузки в оперативную память.

Примеры наиболее распространенных антивирусных программ

- Doctor Web. Dr.Web
- Aidstest,
- Doctor Web,
- MicroSoft AntiVirus
- Антивирус Касперского
- …

Заключение

- В заключение хотелось бы предостеречь от слишком рьяной борьбы с компьютерными вирусами. Ежедневный запуск полного сканирования жесткого диска на наличие вирусов так же не блестящий шаг в профилактике заражений. Единственный цивилизованный способ защиты от вирусов в соблюдении профилактических мер предосторожности при работе на компьютере.
- Нередко главной бедой Интернета являются не вирусы и хакеры, а такое распространенное явление, как компьютерная безграмотность.
- Пользуясь аналогией Касперского, незнание правил дорожного движения. Люди, недавно научившиеся принимать и отправлять почту, демонизируют компьютерные вирусы, чуть ли не представляя их себе в виде невидимых черных червячков, ползающих по проводам.

- **Вот несколько простых правил, соблюдая которые можно постараться избежать заражение вирусами.**
- **Первое: не боятся компьютерных вирусов, все они лечатся.**
- **Второе: перевести Microsoft Outlook в режим функционирования в зоне ограниченных узлов, что запретит ей автоматическое выполнение некоторых программ – основной принцип размножения компьютерных вирусов.**
- **Третье: не открывайте письма от подозрительных адресатов.**
- **Четвертое: использовать свежий антивирус.**

Тест: Задание 1.

1. Что такое "компьютерный вирус"?

А) это программы, активизация которых вызывает уничтожение программ и файлов;

Б) это совокупность программ, находящиеся на устройствах долговременной памяти;

В) это программы, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы;

Г) это программы, передающиеся по Всемирной паутине в процессе загрузки Web-страниц.

2. Какие файлы заражают макро-вирусы?

А) исполнительные;

Б) графические и звуковые;

В) файлы документов Word и элект. таблиц Excel;

Г) html документы.

3. Неопасные компьютерные вирусы могут привести

А) к сбоям и зависаниям при работе компьютера;

Б) к потере программ и данных;

В) к форматированию винчестера;

Г) к уменьшению свободной памяти компьютера.

4. Какой вид компьютерных вирусов внедряются и поражают исполнительный файлы с расширением *.exe, *.com?

А) файловые вирусы;

Б) загрузочные вирусы;

В) макро-вирусы;

Г) сетевые вирусы.

5. Основные типы компьютерных вирусов:

1)Аппаратные, программные, загрузочные

2)Программные, загрузочные, макровирусы.

3)Файловые, сетевые, макровирусы, загрузочные.

6. На чем основано действие антивирусной программы?

1)На ожидании начала вирусной атаки.

2)На сравнении программных кодов с известными вирусами.

3)На удалении зараженных файлов.

7. Какие программы относятся к антивирусным

1)AVP, DrWeb, Norton AntiVirus.

2)MS-DOS, MS Word, AVP.

3)MS Word, MS Excel, Norton Commander.

8. Какие существуют вспомогательные средства защиты?

1)Аппаратные средства.

2)Программные средства.

3)Аппаратные средства и антивирусные программы.

9. Вставь пропущенное слово, определив тип антивирусной программы

Антивирусные ... - это программы, перехватывающие «вирусноопасные» ситуации и сообщающие об этом пользователю.

10.Основные меры по защите информации от повреждения вирусами:

1)проверка дисков на вирус

2)создавать архивные копии ценной информации

3)не пользоваться "пиратскими" сборниками программного обеспечения

4)передавать файлы только по сети

Домашнее задание

Заполнить таблицу

Тип вируса	**Источник заражения**	**Объект заражения**	**Последствия заражения**
Загрузочные			
Файловые			
Макро-вирусы			
Сетевые			