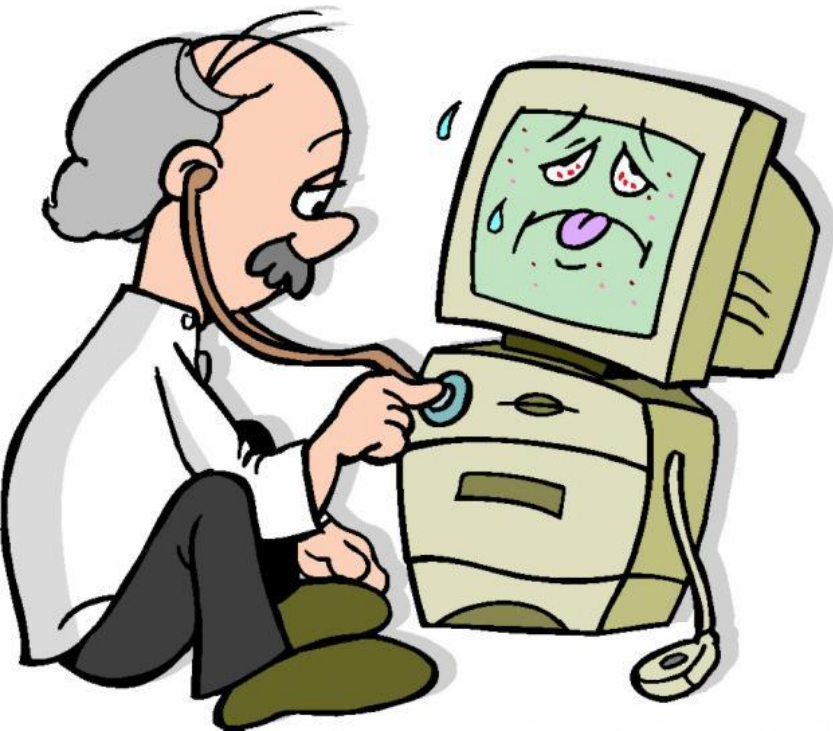


# Компьютерные вирусы и антивирусные программы

Автор:

преподаватель информатики  
МОУ «Центр образования» г.  
Урюпинска Волгоградской  
области

Меринова Елена Васильевна



# Компьютерные вирусы и антивирусные программы

Персональный компьютер играет в жизни современного человека важную роль, поскольку он помогает ему почти во всех областях его деятельности. Современное общество все больше вовлекается в виртуальный мир Интернета. Но с активным развитием глобальных сетей актуальным является вопрос информационной безопасности, так как проникающие их сети вирусы могут нарушить целостность и сохранность вашей информации.

**Защита компьютера от вирусов – это та задача, решать которую приходится всем пользователям, и особенно тем, кто активно пользуется Интернетом или работает в локальной сети.**



Разгадайте ребус. Дайте определение зашифрованного понятия.

„ „ „

~~Е~~



***Программа***

Разгадайте ребус. Дайте определение зашифрованного понятия.

„ „ „



Й

~~Е~~



*Драйвер*

Разгадайте ребус. Дайте определение  
зашифрованного понятия.

””

”



1

,



,



3

2

PHOTOBYOLEG.RU

**Утилиты**

# ИСТОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

**Первая «эпидемия»** компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг») «заражал» дискеты персональных компьютеров. В настоящее время известно несколько десятков тысяч вирусов, заражающих компьютеры и распространяющихся по компьютерным сетям.

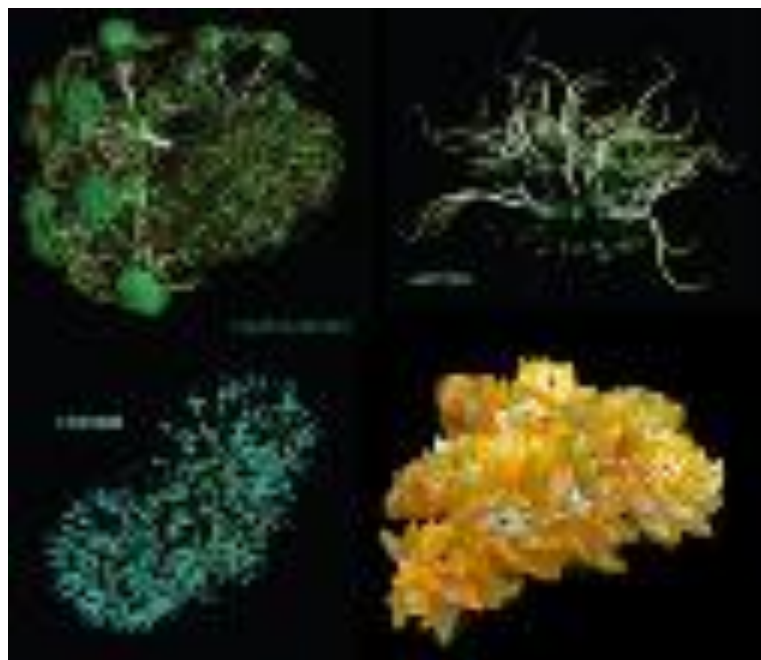


# Что же такое вирус? И чем биологический вирус отличается от компьютерного?

Обратимся к вирусной энциклопедии «Лаборатории Касперского», электронной энциклопедии Кирилла и Мефодия и к толковому словарю русского языка С.И. Ожегова и Н.Ю. Шведовой



**Вирус** – мельчайшая неклеточная частица, размножающаяся в живых клетках, возбудитель инфекционного заболевания.



*Толковый словарь русского языка  
С. И. Ожегова и Н. Ю. Шведовой*



# Компьютерный вирус –

специально созданная небольшая программа, способная к саморазмножению, засорению компьютера и выполнению других нежелательных действий.



*Энциклопедия вирусов*

*«Лаборатории Касперского»*

*<http://www.viruslist.com/ru/viruses/encyclopedia>*

# Что же общего между биологическим и компьютерным вирусами?

1. Способность к размножению.
2. Вред для здоровья человека и нежелательные действия для компьютера.
3. Скрытность, т.к. вирусы имеют инкубационный период.



# ИСТОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Первый прототип вируса появился еще в 1971г.. Программист Боб Томас, пытаясь решить задачу передачи информации с одного компьютера на другой, создал программу Creeper, самопроизвольно «перепрыгивавшую» с одной машины на другую в сети компьютерного центра.

Правда эта программа не саморазмножилась, не наносила ущерба.



# ИСТОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

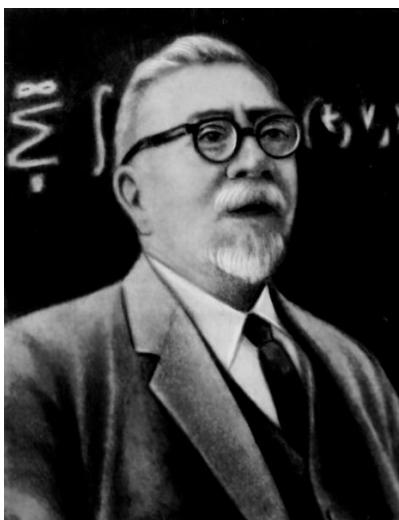
Первые исследования саморазмножающихся искусственных конструкций проводилась в середине прошлого столетия учеными фон Нейманом и Винером.





**Джон фон Нейман**

**(1903 - 1957)**



**Норберт Винер**

**(1894 - 1964)**

**Фред Коэн**

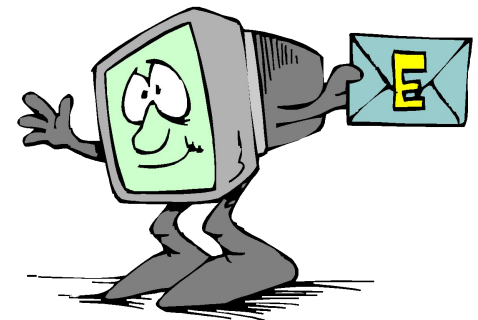
**1984**

# ЧЕМ ОПАСЕН КОМПЬЮТЕРНЫЙ ВИРУС?

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 определённой даты или дня недели*
- *запуском программы*
- *открытием документа...*



# Признаки заражения



- общее замедление работы компьютера и уменьшение размера свободной оперативной памяти;
- некоторые программы перестают работать или появляются различные ошибки в программах;
- на экран выводятся посторонние символы и сообщения, появляются различные звуковые и видеоэффекты;
- размер некоторых исполнимых файлов и время их создания изменяются;
- некоторые файлы и диски оказываются испорченными;
- компьютер перестает загружаться с жесткого диска.





# Классификация компьютерных вирусов



# ПРИЗНАКИ КЛАССИКАЦИИ

```
graph TD; A[ПРИЗНАКИ КЛАССИКАЦИИ] --- B[Среда обитания]; A --- C[Особенности алгоритма работы]; A --- D[Операционная система]; A --- E[Деструктивные возможности];
```

**Среда обитания**

**Особенности  
алгоритма работы**

**Операционная  
система**

**Деструктивные  
возможности**

# СРЕДА ОБИТАНИЯ

```
graph TD; A[СРЕДА ОБИТАНИЯ] --> B[файловые]; A --> C[загрузочные]; A --> D[макро]; A --> E[сетевые]
```

**файловые**

**загрузочные**

**макро**

**сетевые**

# ФАЙЛОВЫЕ ВИРУСЫ

Внедряются в программы и активизируются при их запуске. После запуска заражённой программой могут заражать другие файлы до момента выключения компьютера или перезагрузки операционной системы.



# Файловые вирусы

перезаписывающие

е

файловые черви

паразитические

компаньоны

вирусы-звенья

поражающие код программ



# По способу заражения файловые вирусы разделяются на:

1. **Перезаписывающие вирусы.** Записывают свое тело вместо кода программы, не изменяя название исполняемого файла, вследствие чего программа перестает запускаться.
2. **Вирусы-компаньоны.** Создают свою копию на месте заражаемой программы, но не уничтожают оригинальный файл, а переименовывают его или перемещают. При запуске программы вначале выполняется код вируса, а затем управление передается оригинальной программе.
3. **Файловые черви** создают собственные копии с привлекательными для пользователя названиями в надежде, что он их запустит.
4. **Вирусы-звенья** не изменяют код программы, а заставляют ОС выполнить свой код, изменяя адрес местоположения на диске зараженной программы, на собственный адрес.

# По способу заражения файловые вирусы разделяются на:

5. **Паразитические вирусы** изменяют содержимое файла, добавляя в него свой код. При этом зараженная программа сохраняет полную или частичную работоспособность. Код может внедряться в начало, середину или конец программы.
6. **Вирусы, поражающие исходный код программы.** Вирусы данного типа поражают исходный код программы или ее компоненты (.OBJ, .LIB, .DCU). После компиляции программы оказываются встроенными в неё.



# МАКРОВИРУСЫ

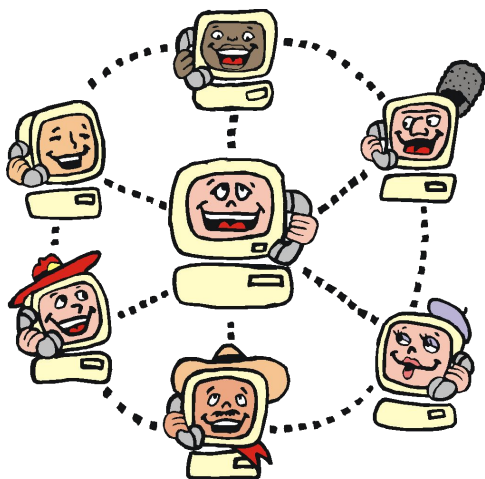
Заражают файлы документов, например текстовых. После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы. Угроза заражения прекращается только после закрытия текстового редактора.





# СЕТЕВЫЕ ВИРУСЫ

Могут передавать по компьютерным сетям свой программный код и запускать его на компьютерах, подключённых к этой сети. Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной паутине.

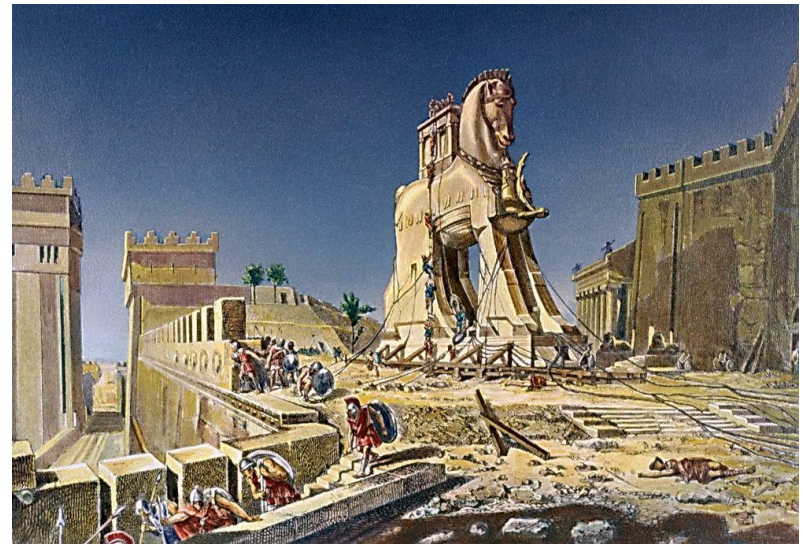


# Сетевые вирусы

сетевые черви

троянские программы

хакерские утилиты



# Сетевые вирусы

**Сетевые черви** – программы, распространяющие свои копии по локальным или глобальным сетям с целью:

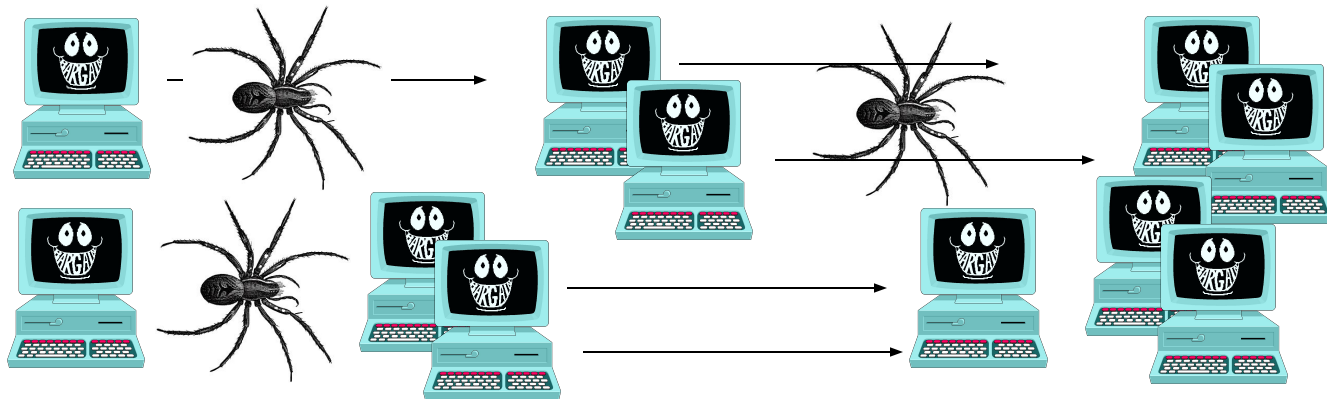
- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие



# Сетевые вирусы

**Троянские программы.** «Троянский конь» употребляется в значении: тайный, коварный замысел. Эти программы осуществляют различные несанкционированные пользователем действия:

- сбор информации и ее передача злоумышленникам;
- разрушение информации или злонамеренная модификация;
- нарушение работоспособности компьютера;
- использование ресурсов компьютера в неблагоприятных целях.



# Сетевые вирусы

## Хакерские утилиты и прочие вредоносные программы.

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ;
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки;
- 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 удаленным компьютерам.



# ОСОБЕННОСТИ АЛГОРИТМА РАБОТЫ

```
graph TD; A[ОСОБЕННОСТИ АЛГОРИТМА РАБОТЫ] --> B[резидентность]; A --> C[стелс-алгоритмы]; A --> D[самошифрование полиморфичность]; A --> E[нестандартные приемы];
```

**резидентность**

**стелс-  
алгоритмы**

**самошифрование  
полиморфичность**

**нестандартные  
приемы**

# Особенности алгоритма работы

**Резидентный вирус** при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них.

Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. Резидентными можно считать макро-вирусы, поскольку они постоянно присутствуют в памяти компьютера на все время работы зараженного редактора.

Использование **стелс-алгоритмов** позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации.

# Особенности алгоритма работы

## **Самошифрование и полиморфичность**

используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик-вирусы - это достаточно труднообнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные **нестандартные приемы** часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре ОС, защитить от обнаружения свою резидентную копию, затруднить лечение от вируса и т.д.



# ДЕСТРУКТИВНЫЕ ВОЗМОЖНОСТИ

```
graph TD; A[ДЕСТРУКТИВНЫЕ ВОЗМОЖНОСТИ] --> B[безвредные]; A --> C[опасные]; A --> D[неопасные]; A --> E[очень опасные];
```

**безвредные**

**опасные**

**неопасные**

**очень опасные**

# По деструктивным особенностям вирусы можно разделить на:

- **безвредные**, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- **неопасные**, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
- **опасные вирусы**, которые могут привести к серьезным сбоям в работе компьютера;
- **очень опасные**, в алгоритмах работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить в резонанс и разрушать головки некоторых типов винчестеров.



# Физкультминутка



## Упражнение первое:

резко зажмурить глаза на 2-3 секунды: и широко открыть на 2-3 секунды, повторить упражнение 10 раз.

## Упражнение второе:

часто-часто моргать глазами, повторить 10 раз.

## Упражнение третье:

поднять глаза вверх, при этом голова остается в одном положении, задержать взгляд на 2-3 секунды, затем опустить глаза вниз и задержать взгляд на 2-3 секунды

 повторить упражнение 10 раз .



# Пути проникновения вирусов

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

# Пути проникновения вирусов

## Глобальная сеть Интернет

Основным источником вирусов на сегодняшний день является глобальная сеть Internet. Возможно заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта, а ничего не подозревающие пользователи зайдя на такой сайт рискуют заразить свой компьютер.



# Пути проникновения вирусов

## Электронная почта

Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.

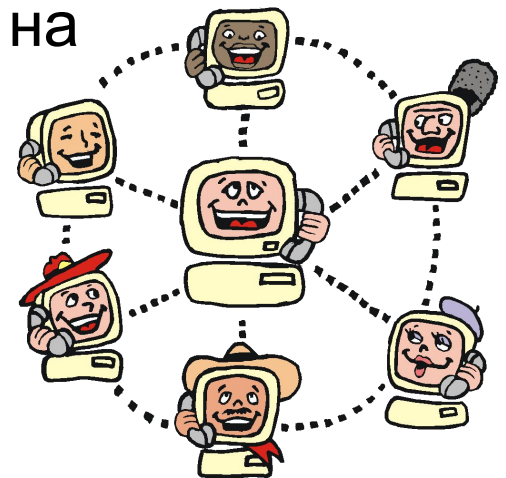


# Пути проникновения вирусов

## Локальные сети

Третий путь «быстрого заражения» — локальные сети. Если не принимать необходимых мер защиты, то зараженная рабочая станция при входе в сеть заражает один или несколько служебных файлов на сервере

На следующий день пользователи при входе в сеть запускают зараженные файлы с сервера, и вирус, таким образом, получает доступ на компьютеры пользователей.





# Пути проникновения вирусов

## **Персональные компьютеры «общего пользования»**

Опасность представляют также компьютеры, установленные в учебных заведениях. Если один из учащихся принес на своих носителях вирус и заразил какой-либо учебный компьютер, то очередную «заразу» получат и носители всех остальных учащихся, работающих на этом компьютере.

То же относится и к домашним компьютерам, если на них работает более одного человека.

## **Пиратское программное обеспечение**

Нелегальные копии программного обеспечения, как это было всегда, являются одной из основных «зон риска». Часто пиратские копии на дисках содержат файлы, зараженные самыми разнообразными типами вирусов.



# Пути проникновения вирусов

## Ремонтные службы

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре. Ремонтники — тоже люди, и некоторым из них свойственно наплевательское отношение к элементарным правилам компьютерной безопасности.

## Съемные накопители

В настоящее время большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны.



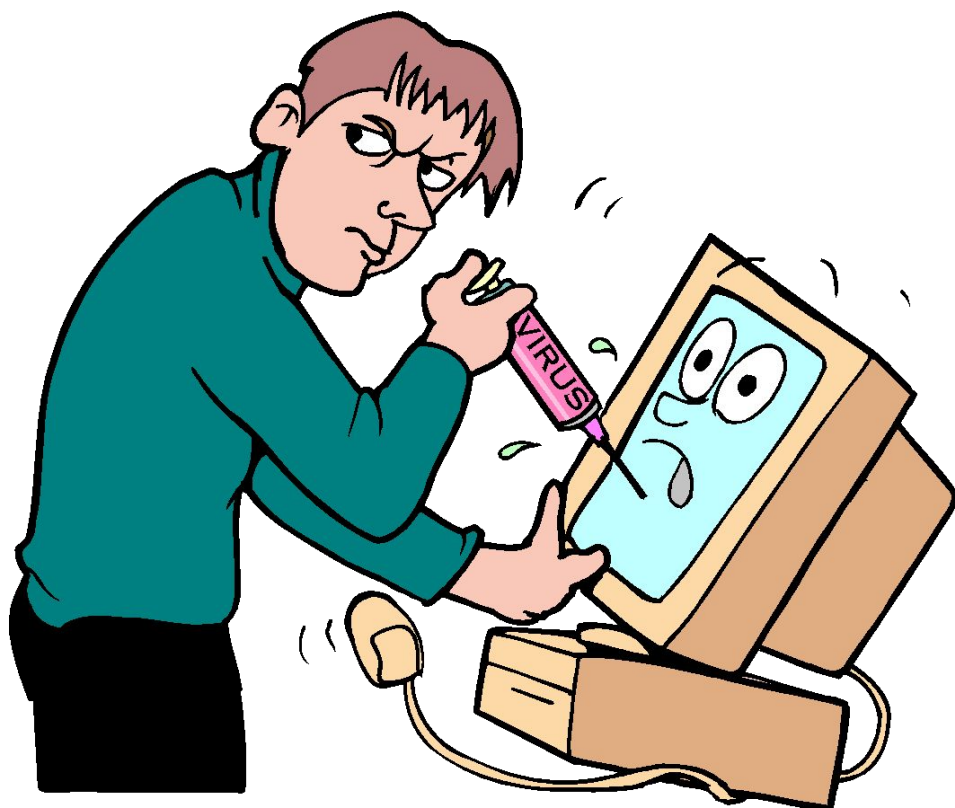
A photograph of a computer monitor and keyboard. The monitor is the central focus, displaying a solid light blue screen. It is heavily secured with thick, dark metal chains that crisscross over its surface. A large metal padlock is attached to the chains, locking them together. The keyboard is visible at the bottom of the frame, also partially covered by the chains. The background is a dark, textured blue, suggesting a night sky or a digital environment. The overall image conveys a sense of robust security and protection.

# Методы защиты

- Защита локальных сетей
- Использование дистрибутивного ПО
- Резервное копирование информации
- Использование антивирусных программ
- Не запускать непроверенные файлы



# Антивирусные программы

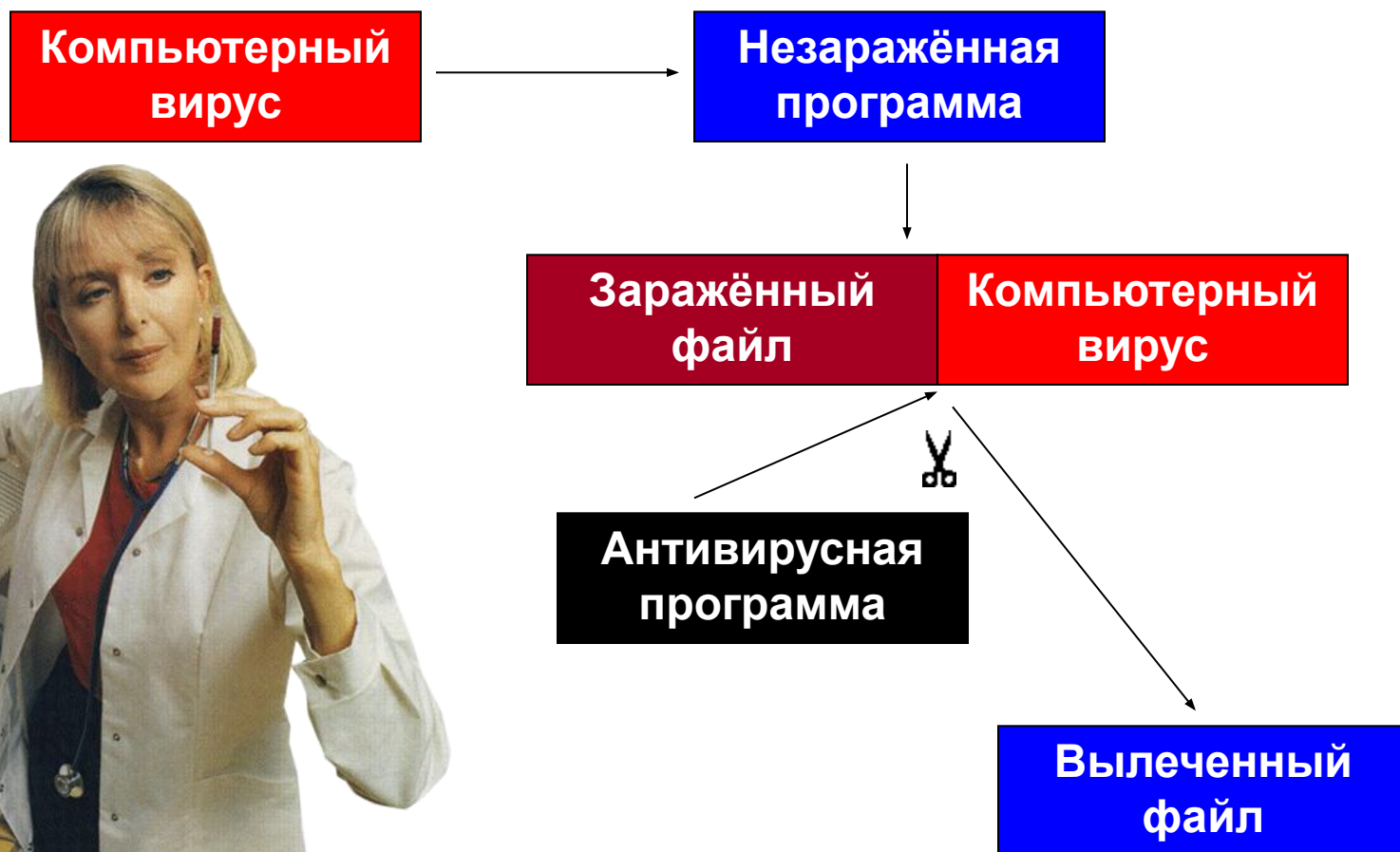


# Критерии выбора антивирусных программ

- Надежность и удобство в работе
- Качество обнаружения вирусов
- Существование версий под все популярные платформы
- Скорость работы
- Наличие дополнительных функций и возможностей



# ПРОЦЕСС ЗАРАЖЕНИЯ ВИРУСОМ И ЛЕЧЕНИЯ ФАЙЛА



# АНТИВИРУСНЫЕ ПРОГРАММЫ

```
graph TD; A[АНТИВИРУСНЫЕ ПРОГРАММЫ] --> B[СКАНЕРЫ (фаги, полифаги)]; A --> C[СРС-СКАНЕРЫ (ревизоры)]; A --> D[Иммунизаторы]; B --> E[Универсальные]; B --> F[Специализированные]; B --> G[Резидентные]; B --> H[Нерезидентные]; C --> I[Блокировщики]; C --> D;
```

**СКАНЕРЫ**  
(фаги, полифаги)

**СРС-СКАНЕРЫ**  
(ревизоры)

**Блокировщики**

**Иммунизаторы**

Универсальные

Специализированные

Резидентные

Нерезидентные



# Программы-детекторы



Принцип работы  
антивирусных  
сканеров основан на  
проверке файлов,  
секторов и  
системной памяти и  
поиске в них  
вирусов

# Программы-доктора



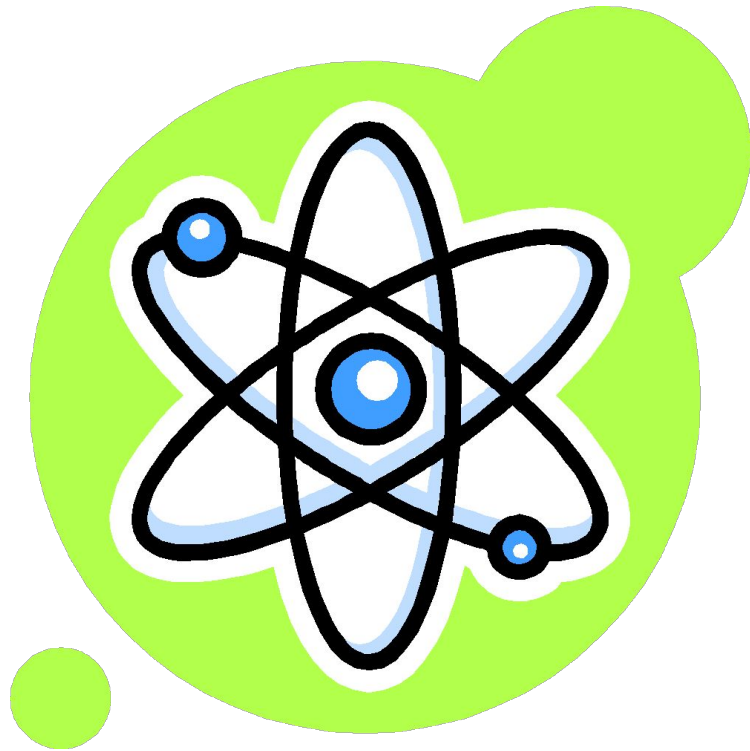
Принцип работы  
антивирусных  
сканеров основан на  
проверке файлов,  
секторов и  
системной памяти и  
поиске в них  
вирусов

# Программы-ревизоры



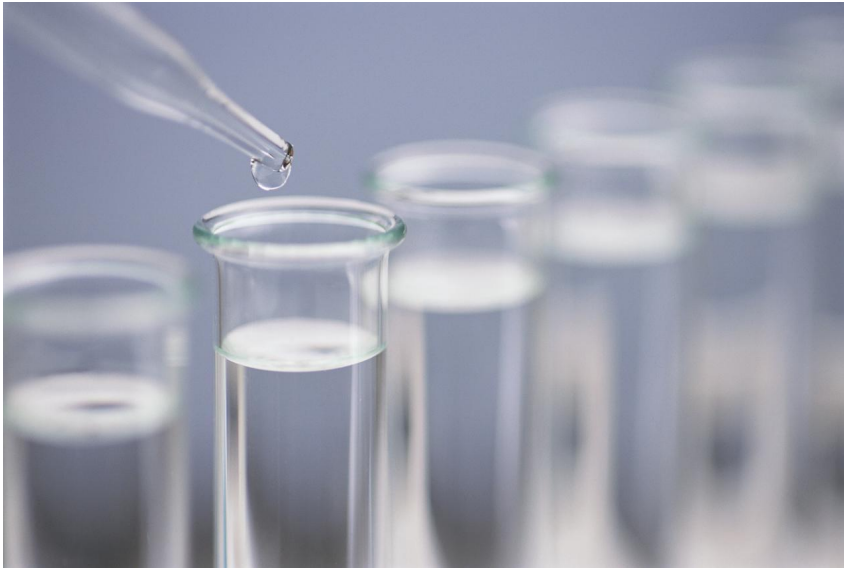
Принцип их работы состоит в подсчете контрольных сумм для присутствующих на диске файлов/системных секторов. Эти суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

# Программы-фильтры



Антивирусные блокировщики — это резидентные программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю. К «вирусоопасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или винчестера, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты из размножения.

# Программы-вакцины



**Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.**

ADinf32 v3.02/Pro ( Настройки по умолчанию )



# Advanced DiskinfoScope™



- Рабочий стол
- Мой компьютер
  - Дискета 3,5" A:
  - Диск C: 20 янв 2005 г.
  - Диск D: 20 янв 2005 г.

Режимы

Без CRC

Не обнов.

<http://www.adinf.com>

Диски: 0  
Готово 0 из 0

Настройки

Старт

Выход

Нажмите "Старт" для начала работы или F1 для помощи

# ESET Smart Security 4

Business Edition



Состояние защиты



Сканирование ПК



Обновление



Настройка



Справка и поддержка



## Максимальная степень защиты

- ✓ Защита от вирусов и шпионских программ
- ✓ Персональный фаервол
- ✓ Модуль защиты от спама

Количество обнаруженных атак: 0  
Версия вирусной базы данных сигнатур: 4798 (20100122)

**АНТИВИРУС**



**КАСПЕРСКОГО**



# Возможности программы

## Антивирус Касперского

- защита от вирусов, троянских программ и червей;
- защита от шпионских, рекламных и других потенциально опасных программ;
- проверка файлов, почты и интернет-трафика в реальном времени;
- проактивная защита от новых и неизвестных угроз;
- антивирусная проверка данных на любых типах съемных носителей;
- проверка и лечение архивированных файлов;
- контроль выполнения опасных макрокоманд в документах Microsoft Office;
- средства создания диска аварийного восстановления системы.

Kaspersky  
**Anti-Virus**



Настройка



Справка



Защита

Активация защиты

Анти-Спам



Плигк вирусов



Сервис

Обновление

Файлы данных

Аварийный диск

Поддержка

Сервис

Информация о программе

|                        |                     |
|------------------------|---------------------|
| Версия:                | 6.0.3.837           |
| Срочное обновление:    | b.c.d.e             |
| Дата выпуска сигнатур: | 17.12.2008 12:59:56 |
| Количество сигнатур:   | 1468877             |

Информация о системе

|                              |  |
|------------------------------|--|
| <u>Операционная система:</u> | <u>Microsoft Windows XP Professional Service Pack 3 (build 2600)</u> |
|------------------------------|--|

Информация о лицензии

|                 |  |   |
|-----------------|--|---|
| Владелец:       | ОУсредняя ОШ 3 "Образовательный центр" | ▲ |
|                 | Мартынова Ольга Владимировна           | ■ |
|                 | Россия                                 | ■ |
|                 | пр-т Гагарина                          | ▼ |
| Номер:          | 0B2C-0003F4-03CA22F7                   |   |
| Тип:            | Коммерческая на 89 компьютеров         |   |
| Дата окончания: | 03.01.2011 2:59:59                     |   |



**Законодательство  
Российской Федерации о  
вредоносных программах**

# **Глава 28**

***«Преступления в сфере  
компьютерной информации»***

**Уголовного кодекса  
Российской Федерации**

## **Статья 273**

# Статья 273 гласит:

*«Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ, или машинных носителей с такими программами, – наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда, в размере заработной платы, или иного дохода осужденного за период от двух до пяти месяцев.*

*То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок от трех до семи лет».*

Используя выписку из главы 28 «Преступления в сфере компьютерной информации» Уголовного Кодекса Российской Федерации ответьте на следующий вопрос: «Можно ли квалифицировать действия лица (группы лиц) в описанной ситуации как противоправные?» Ответ необходимо обосновать, указав соответствующий нормативный документ, его статью пункт статьи.

### Задача 1.

П. П. Андреев, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтоживший исполняемые файлы (файлы с расширением .exe). В результате внедрения этого вируса было уничтожено 40% банковских программных приложений, что принесло банку материальный ущерб в размере 750 000 рублей.

Используя выписку из главы 28 «Преступления в сфере компьютерной информации» Уголовного Кодекса Российской Федерации ответьте на следующий вопрос: «Можно ли квалифицировать действия лица (группы лиц) в описанной ситуации как противоправные?» Ответ необходимо обосновать, указав соответствующий нормативный документ, его статью пункт статьи.

## **Задача 2.**

Будет ли удовлетворен иск компании «Интермедиа» о привлечении к уголовной ответственности гражданина Р. И. Сизова и выплате им фирме денежной компенсации, если он внедрил в компьютерную сеть компании программу, действие которой заключается в уничтожении исполняемых файлов в какой-либо компьютерной сети? Функционирование данной программы принесло убытки разным организациям на общую сумму 670 000 рублей.

# СРЕДСТВА ЗАЩИТЫ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ

*антивирусные программы*

*брандмауэры или файрволы*

*антишпионы*



# Функции файрвола

- информирует пользователя о попытках извне получить несанкционированный доступ к ресурсам данного компьютера, а также блокирует эти попытки;
- предотвращает попытки несанкционированно передать в сеть информацию с вашего компьютера (хищение паролей и конфиденциальной информации);
- отслеживает любые изменения в размерах выполняемых файлов, которые могут быть свидетельством заражения вирусом;
- блокирует рекламные окна на интернетовских сайтах;

# Функции файрвола

- предупреждает, когда одна программа пытается запустить другую программу (это тоже может быть следствием работы вируса);
- закрывает от возможного доступа определенные сетевые порты компьютера;
- предупреждает о так называемом сканировании портов вашего компьютера, так как это может быть предвестником хакерской атаки;
- блокирует выполнение различных шпионских программ;
- предотвращает деструктивные действия троянских программ.

# Пути проникновения рекламных шпионов

- скачивание бесплатного программного обеспечения;
- вирусы и трояны;
- сайты сомнительного содержания.

Из предложенного списка уберите термины, не относящиеся к антивирусным программам:

- **детекторы**
- **доктора (фаги)**
- **ревизоры**
- **интерпретаторы**
- **ревизоры**
- **фильтры**
- **драйверы**
- **вакцины (иммунизаторы)**

# ПАМЯТКА

## безопасности для пользователя домашнего компьютера

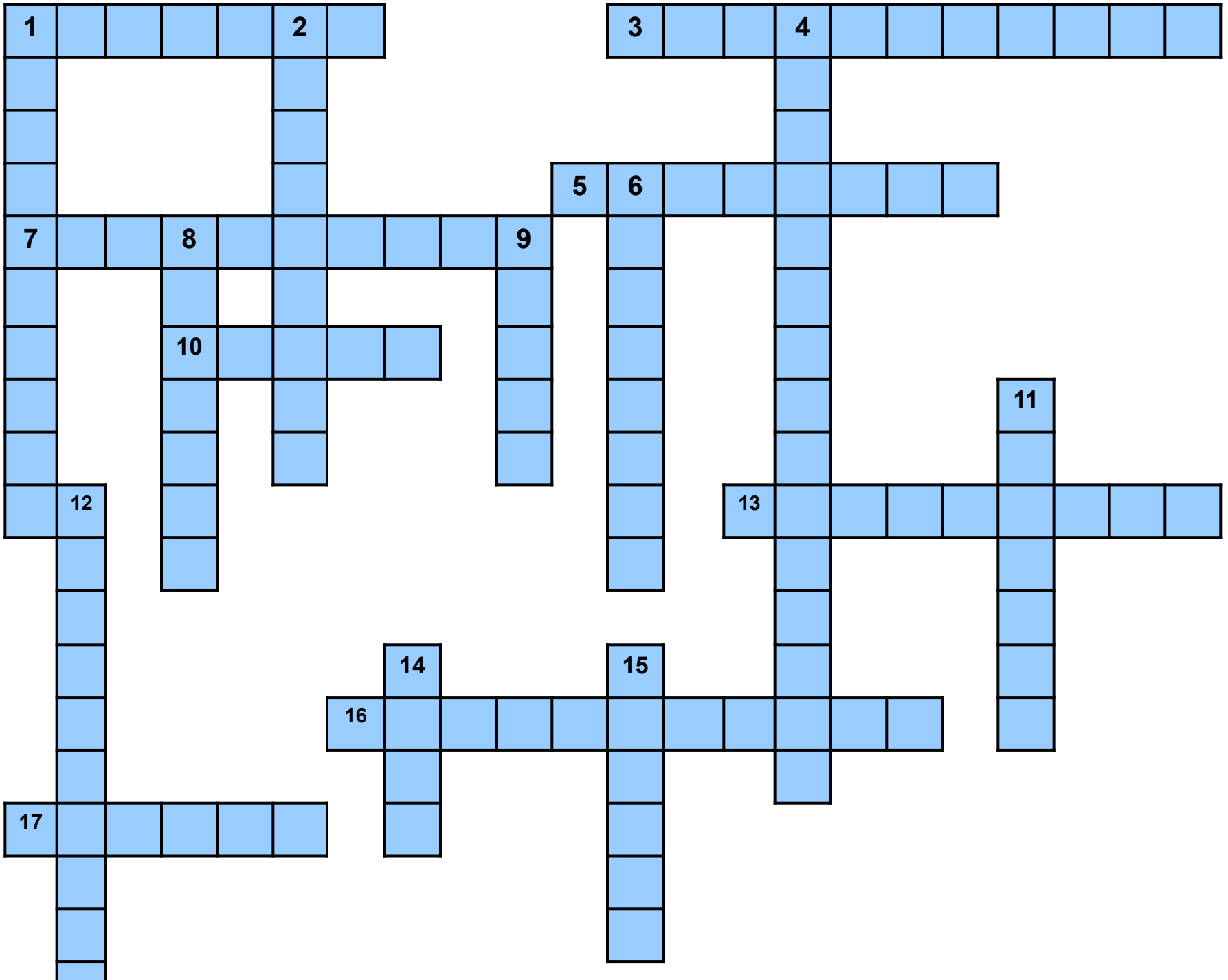
- Ограничить физический доступ к компьютеру, установить пароль на вход в систему и отключать доступ в Интернет, когда он не нужен;
- подписаться на информационные бюллетени Microsoft и регулярно обновлять операционную систему;
- отключить все неиспользуемые службы и закрыть порты, через которые могут осуществляться атаки;
- тщательно настроить все программы, работающие с Интернет, начиная с браузера — например, запретить использование Java и ActiveX;
- установить и обновлять антивирусную программу;

# ПАМЯТКА

## безопасности для пользователя домашнего компьютера

- использовать брандмауэр, хотя бы встроенный в систему, и внимательно анализировать его сообщения и логи;
- крайне аккуратно работать с почтой, а также программами для обмена сообщениями и работы с файлообменными сетями, например, следует отключить использование HTML в принимаемых письмах;
- никогда не запускать программы сомнительного происхождения, даже полученные из заслуживающих доверия источников, например, из присланного другом письма;
- ни при каких условиях не передавать по телефону или по почте свои персональные данные, особенно пароли;
- регулярно создавать резервные копии критических данных.

*Владимир Каталов,  
исполнительный директор компании «Элкомсофт»*



# Вопросы по горизонтали:

1. Антивирусная программа, принцип работы которой основан на проверке файлов, загрузочных секторов дисков и оперативной памяти в поиске в них известных и новых вирусов.
3. Утилита для создания новых компьютерных вирусов.
5. Наука, от которой пришло название "вирус".
7. Вирусы, поражающие документы MS Office, основанные на использовании макрокоманд.
10. Программа, способная к саморазмножению.
13. Вирусы, не изменяющие файлы, но создающие для .EXE файлов .COM файлы с тем же именем.
16. Мутация вирусов.
17. Антивирусная программа, то же что и полифаг.



# Вопросы по вертикали:

1. Вирус, предпринимающие специальные меры для затруднения их поиска и анализа, не содержат ни одного постоянного участка кода.
2. Программа против вирусов.
4. Одно из главных свойств вирусов, способность к созданию себе подобных.
6. ...-черви. Вирусы, распространяющиеся в сети во вложенных файлах в почтовое сообщение.
8. Антивирус, чей принцип работы основан на подсчете контрольных сумм для присутствующих на диске файлов.
9. Вирус-"невидимка".
11. Резидентно находящаяся в оперативной памяти утилита, которая позволяет выявлять «подозрительные» действия пользовательских программ, а при обнаружении «подозрительной» функции либо выдает на экран сообщение, либо блокирует выполнение перехваченной функции, либо совершает другие специальные действия.
12. Видоизменение вируса.
14. Троянский-...
15. "Лечащий" антивирус.

ПОЛИФАГ

КОНСТРУКТОР

О  
Л  
И  
И

Н  
Т  
И

А  
М

БИОЛОГИЯ

МАКРОВИРУС

Н

Р

О  
Р

Е  
И  
В  
И  
Р  
У  
С

Т

Т

А

Ф  
И

И  
З  
О  
Р

Е  
Л  
С

Е  
Р  
Н  
Е  
Т

З  
М  
Н

М

К  
М  
О  
Д  
И  
Ф  
И

О  
Р

Т

КОМПАНИЯ

О

С  
К  
А  
Н  
Е  
Р

Р

ПОЛИМОРФИЗМ

К

Д

Ж

И

А  
Ц  
И

Р

Н  
Т  
О  
Р

Е

Т  
О  
Р

С

А

Н  
Ь

Ь

К

Е

Р

С

А

Н  
Ь

Т

Н

Р

С

А

Н  
Ь

Р

Е

Р

С

А

Н  
Ь

Р

Е

Р

С

А

Н  
Ь

Р

Е

Р

С

А

Н  
Ь

Р

Е

Р

С

А

Н  
Ь

Р

Е

Р

С

А

Н  
Ь

Р

Е

Р

С

А

Н  
Ь

Р

Е

Р

С

А

Н  
Ь

Р

Е

Р

С

А

Н  
Ь

Р

Е

Р



# Физкультминутка



## Упражнение 1.

Выполняется сидя. Быстро моргать в течение 30 сек.

## Упражнение 2.

Выполняется стоя. Смотреть вдаль прямо перед собой 2-3 с, поставить палец руки по средней линии лица на расстоянии 25-30 см от глаз, перевести взгляд на конец пальца и смотреть на него 3-5 с, опустить руку. Повторить 5 раз.

## Упражнение 3.

Растереть наружные и внутренние поверхности ладоней до ощущения тепла.

## Упражнение 4.

Кисти постепенно сжимать в кулаки, все крепче и крепче на счет 1-6. Встряхнуть кистями, расслабиться на счет 7-9.



*СПАСИБО*

*за внимание*

Автор презентации является  
участником конкурса компьютерных  
презентаций проводимого на сайте  
[«Информатика в школе»](http://www.inf777.narod.ru)  
[www.inf777.narod.ru](http://www.inf777.narod.ru)  
при спонсорстве издательского дома  
«Питер»