Защита информации. Компьютерные вирусы и антивирусные программы

Программное обеспечение ПК

- Информацию, пригодную для обработки персональным компьютером называют .
- Алгоритм, предназначенный для исполнения персональным компьютером, называют
- Принцип программного управления предполагает,
- Совокупность программ, установленных на данном компьютере, называют
- Программное обеспечение персонального компьютера классифицируют на

1	Разновидность носителя информации	1	Отдельный процесс (акт) лечения, закаливания, ухода за телом
2	Действие, воспроизводимое над данными	2	Возбудитель инфекционной болезни
3	Подпрограмма, в которой решается некоторая частная задача, оформленная особым образом и снабженная именем	3	Организм человека в его внешней материальной форме
4	Часть оператора цикла, в которой указываются действия, повторяемые при выполнении оператора	4	Хрящевая прокладка между позвонками
5	Программа, обладающая способностью к самовоспроизведению	5	Непосредственное механическое (хирургическое) воздействие на орган человека с лечебной целью

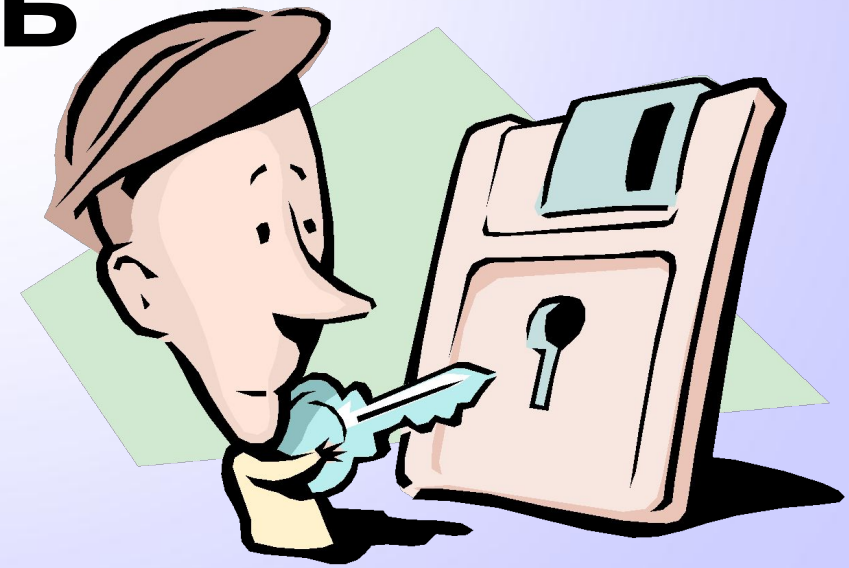
Разновидность носителя информации		Хрящевая прокладка между позвонками
Действие, воспроизводимое над данными		Непосредственное механическое (хирургическое) воздействие на орган человека с лечебной целью
Подпрограмма, в которой решается некоторая частная задача, оформленная особым образом и снабженная именем		Отдельный процесс (акт) лечения, закаливания, ухода за телом
Часть оператора цикла, в которой указываются действия, повторяемые при выполнении оператора		Организм человека в его внешней материальной форме
Программа, обладающая способностью к самовоспроизведению		Возбудитель инфекционной болезни

Защита организма человека

- **Иммунитет** – способ защиты организма от генетически чужеродных веществ живой и неживой природы с целью сохранения структурной и функциональной целостности организма и его биологической индивидуальности (гомеостаза).

Понятие информационной безопасности

- **Конфиденциальность**
- **Целостность**
- **Доступность**



Защита организма от антигенов

- *механические барьеры*
- *физико-химические барьеры*
- *иммунобиологические барьеры*
- *специфическая защита*

Средства физической защиты информации

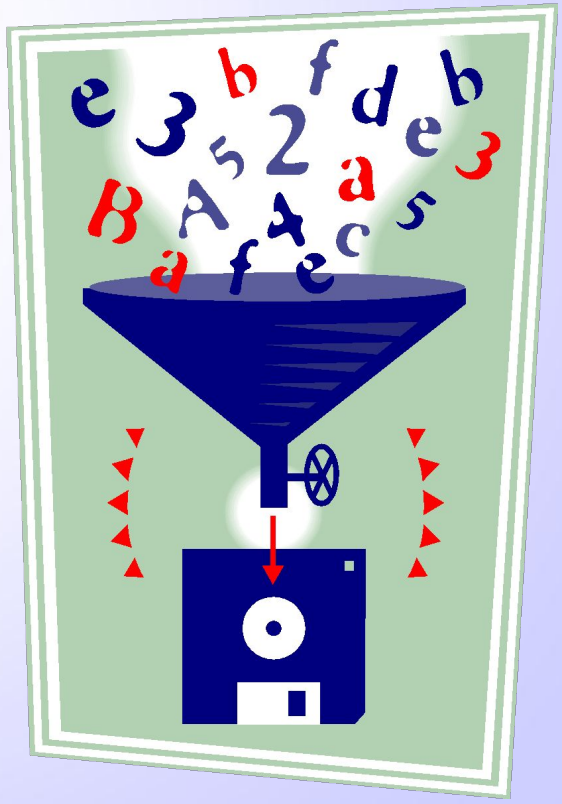
- *средства защиты кабельной системы, систем электропитания*
- *средства архивации*
- *дисковые массивы*

Административные средства защиты информации

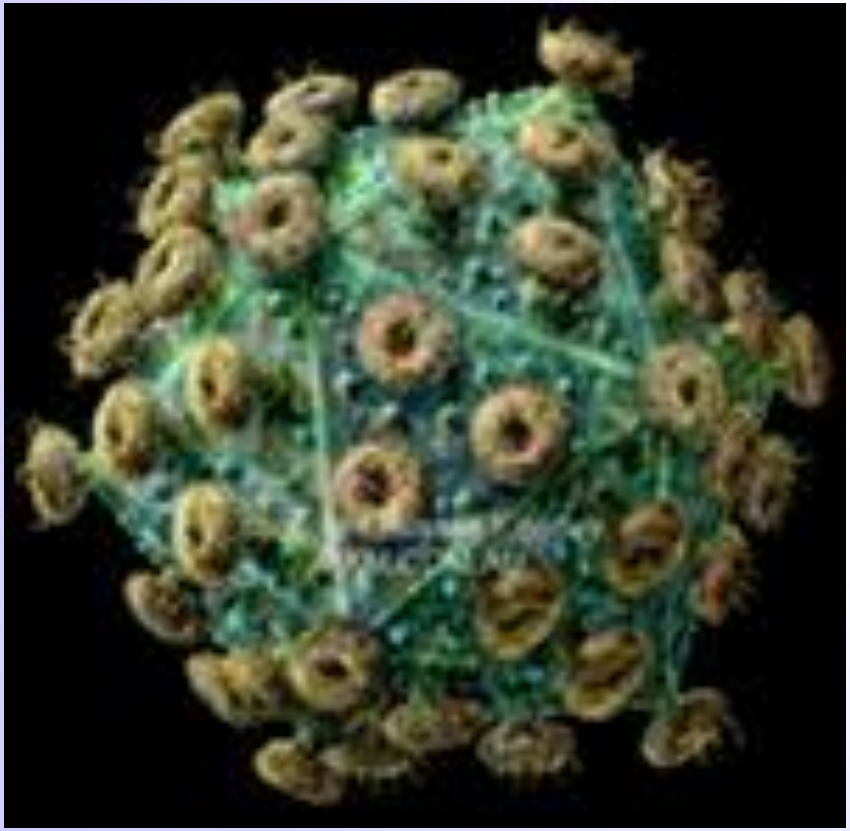
- *контроль доступа в помещения*
- *разработка стратегии безопасности*
- *планы действий в чрезвычайных ситуациях*

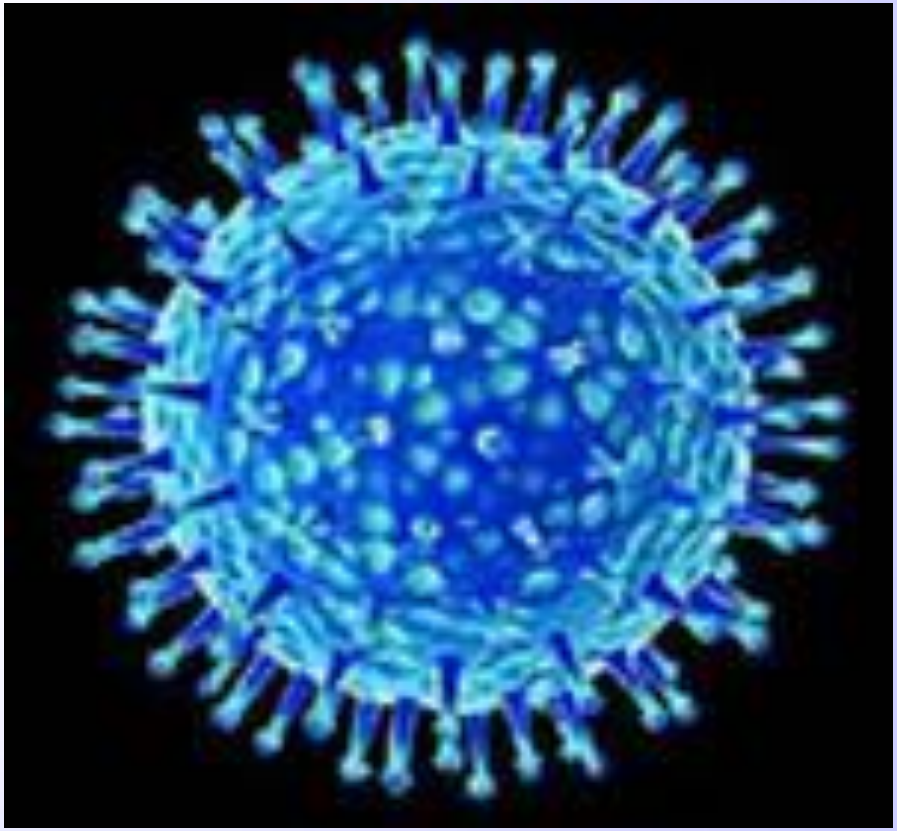
Программные средства защиты информации

- *антивирусные программы*
- *системы разграничения полномочий*
- *программные средства контроля доступа*



Вирусы – облигатные внутриклеточные паразиты, не имеющие клеточного строения, белоксинтезирующей системы и содержащие только один тип нуклеиновой кислоты (ДНК или РНК)





Обязательным (необходимым) свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и скрытно внедрять их в вычислительные сети или файлы, системные области компьютера и прочие выполняемые объекты.

- Компьютерный вирус – это целенаправленно созданная программа, автоматически приписывающая себя к другим программным продуктам, изменяющая или уничтожающая их.
- Компьютерным вирусом называется программа, способная выполнить на компьютере несанкционированные действия.
- Компьютерный вирус – это программный код, встроенный в другую программу, или в документ, или в определенные области носителя данных и предназначенный для несанкционированных действий на компьютере.
- Компьютерный вирус – это программа, способная создавать свои копии, внедрять их в различные объекты или ресурсы компьютерных систем и сетей и производить определенные действия без ведома пользователя.

Таким образом, вирус

1. специально созданная программа
2. самопроизвольно присоединяется к другим программам
3. создает свои копии
4. приводит к порче и потере информации

Компьютерный вирус – специально созданная компьютерная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии, внедрять их в файлы с целью нарушения работы других программ, порчи файлов и каталогов.

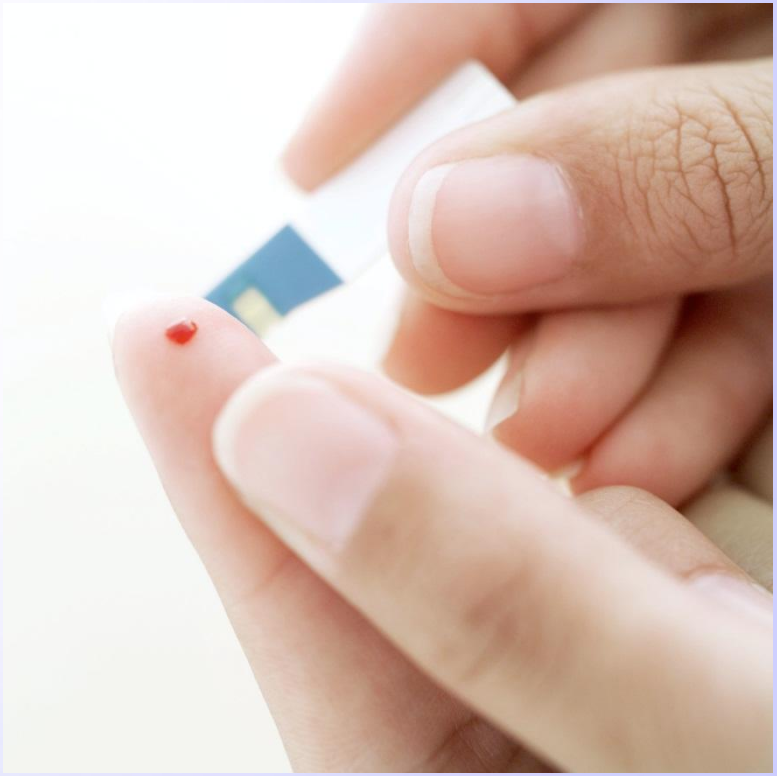
Пути и источники заражения

Источниками заражения биологическими вирусами служат больные и носители.

Заражение происходит:

– *фекально-оральным путем*
– *воздушно-капельным путем*
– *парентеральным путем*
– *при укусе инфицированными*
– *клещами, комарами, другими*

кровососущими членистоногими
или при прямом контакте
с инфицированными животными



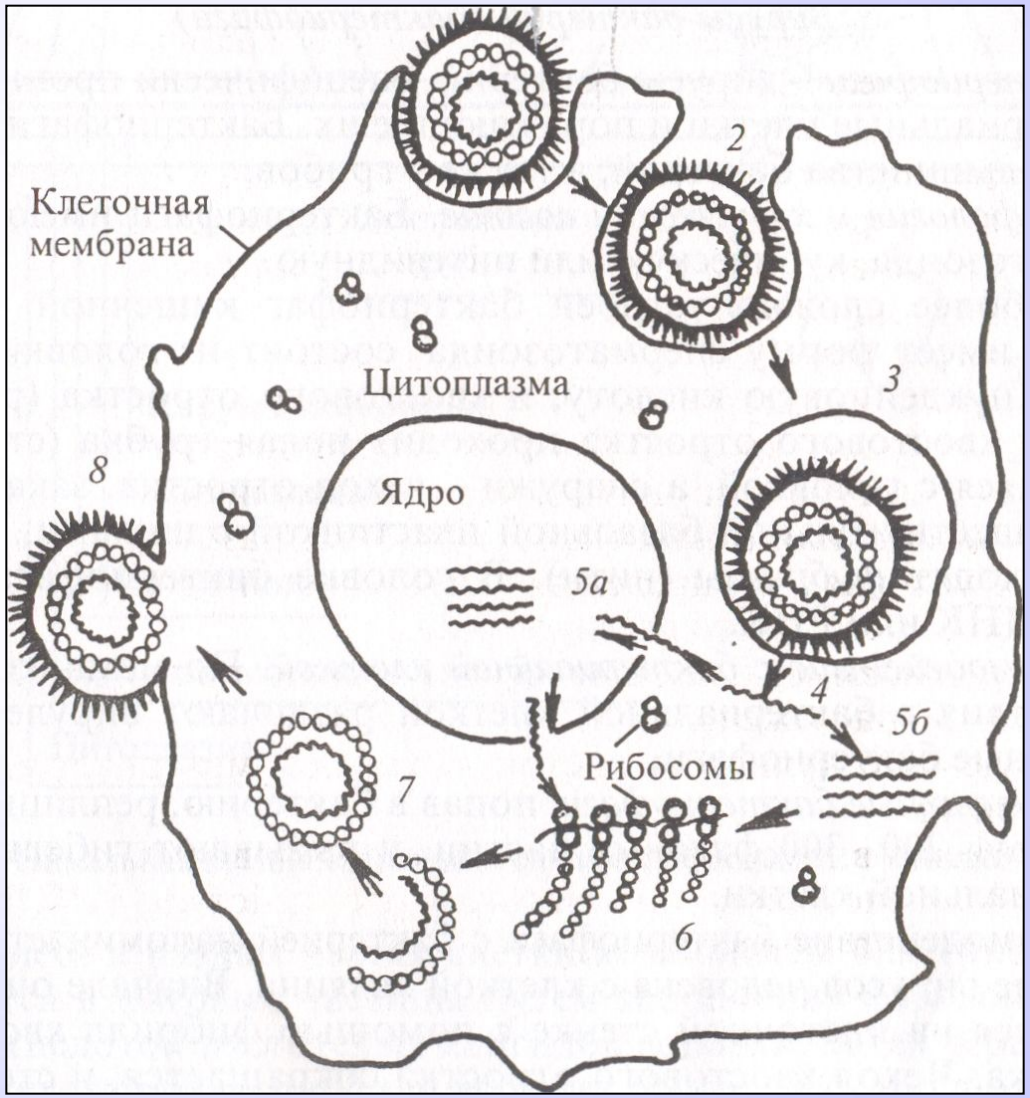
Компьютерные вирусы могут распространяться через

- *исполняемые файлы*
- *документы Word, Excel*
- *Web-страницы*
- *файлы из Интернета*
- *письма e-mail*
- *компакт-диски*

и flash-носители

Механизм воздействия вируса

- В клетке **биологический вирус** может воспроизводиться в виде многочисленных вирионов. Различают три типа взаимодействия вируса с клеткой:
- ***продуктивный***
- ***абортивный***
- ***интегративный тип***



Механизм воздействия вируса

- **При запуске инфицированной программы** или **при обращении к носителю**, имеющему **вредоносный вирусный код** в системной области, происходит **заражение**.
- При каждой загрузке инфицированной программы в оперативную память происходит **размножение**.
- Последняя фаза развития вируса – **активизация** или **вирусная атака**.

Признаки заражения. Вас должны насторожить:

- неправильная работа программ
- медленная работа компьютера
- невозможность загрузки операционной системы
- исчезновение файлов и каталогов
- изменение даты, времени создания файла или его размера
- неожиданное увеличение количества файлов на диске
- уменьшение размеров свободной оперативной памяти
- вывод на экран неожиданных сообщений и изображений
- подача непредусмотренных звуковых сигналов
- частые «зависания» и сбои в работе компьютера

***Биологический вирус* не** может существовать вне клетки.

***Компьютерный вирус* не** может содержаться в ASCII-текстах, графических или звуковых файлах, так как он является программой и требует исполнение своего кода.

Основание классификации – *степень вредных воздействий*

группа вирусов	*характеристика вирусов*
Безвредные	Уменьшают свободную память на диске за счет своего «размножения»
Неопасные	Уменьшают свободную память на диске. Вызывают появление графических, звуковых и др. внешних эффектов
Опасные	Могут привести к сбоям и зависаниям при работе компьютера
Очень опасные	Потеря программ и данных (изменение, удаление файлов и каталогов), форматирование винчестера и т.п.

Основание классификации – *среда обитания*

группа вирусов	*характеристика вирусов*
Файловые	Внедряются в исполняемые файлы (программы) и активизируются при их запуске. Находятся в ОЗУ до выключения компьютера.
Загрузочные	Записывают себя в загрузочный сектор диска (в программу – загрузчик ОС). При загрузке ОС с зараженного диска внедряются в ОЗУ и ведут себя как файловые вирусы.
Макровирусы	Являются макрокомандами, которые заражают файлы документов Word, Excel. Находятся в ОЗУ до закрытия приложения.
Драйверные	Заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки.
Сетевые	Заражают компьютер после открытия вложенного файла (вируса) в почтовое сообщение. Похищают пароли пользователей. Рассылают себя по электронным адресам.

Основание классификации – ***особенности алгоритма***

группа вирусов	*характеристика вирусов*
компаньоны (спутники)	не изменяют файлы, а создают для исполняемых программ (.exe) одноименные командные программы (.com), которые при выполнении исходной программы запускаются первыми, а затем передают управление исходной программе
репликаторы (черви)	распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии, не изменяют файлы или сектора на дисках
паразиты	изменяют содержимое файлов и секторов диска, легко обнаруживаются и уничтожаются
троянские (квазивирусы)	маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков, передают конфиденциальную информацию, модифицируют программы систем защиты
невидимки (стелс)	перехватывают обращения операционной системы к пораженным файлам и подставляют вместо своего тела незараженные участки
мутанты (призраки)	не содержат одинаковых фрагментов, хранят свое тело в закодированном виде, постоянно меняя параметры этой кодировки

Основание классификации – способ заражения

группа вирусов	*характеристика вирусов*
резидентные	записывают в оперативную память свою часть, которая потом перехватывает обращения ОС к любым объектам, активны до выключения или перезагрузки компьютера
нерезидентные	не заражают память компьютера, активны ограниченное время, активизируются в определенные моменты

Основание классификации – целостность

группа вирусов	*характеристика вирусов*
монолитные	внедряются в программы нераздельно
распределенные	части вредоносного кода внедряются в различные места кода программ


классификация компьютерных вирусов
целостность
монолитные
распределенные
степень вредных воздействий
безвредные
неопасные
опасные
очень опасные
способ заражения
резидентные
нерезидентные
среда обитания
файловые
загрузочные
макровирусы
драйверные
сетевые
особенности алгоритма
«спутники»
«черви»
«паразиты»
квазивирусы
стелс-вирусы
«мутанты»

Предотвращение поступления вирусов

- иметь антивирусную программу-сторож (блокировщик)
- не вскрывать писем от неизвестных адресатов
- не запускать программы неизвестного происхождения и непонятного поведения
- перед считыванием информации с внешних носителей проверять их на наличие вирусов с помощью антивирусных программ

Предотвращение вирусной атаки, если вирус поступил на ПК

- иметь антивирусную программу-ревизора или полифага
- регулярно тестировать компьютер на наличие вирусов с помощью антивирусной программы
- регулярно обновлять базу данных антивирусной программы

Предотвращение разрушительных последствий, если атака произошла

- осуществлять резервное копирование особо ценной информации
- хранить дистрибутивные диски всех программ, установленных на компьютере
- не сохранять на персональном компьютере регистрационные и парольные данные для доступа в Интернет и адреса
- обязательно создать системный загрузочный диск компьютера, заранее проверить его работоспособность и хранить в надежном месте

Иммунная система

- центральные органы (*костный мозг и вилочковая железа)*
- периферические органы *(лимфатические узлы, скопления лимфоидной ткани (пейеровы бляшки, миндалины), селезенка, кровь и лимфа)*

Вакцинация

- *живые вакцины*
- *убитые вакцины*
- *адъюванты*
- *рекомбинантные вакцины*
- *ассоциированные вакцины*
- *бактериофаги*

Антивирусные программы

Наименование	Описание	Плюсы	Минусы
Полифаги	В файлах, загрузочных секторах дисков и ОП поиск известных масок вирусов (постоянной последовательности программного кода, специфичного для этого вируса) и поиск «подозрительной» последовательности команд. Могут проверять файлы в процессе их загрузки в ОП (мониторы)	Универсальность	Большие размеры используемых баз данных, невысокая скорость работы
Ревизоры	Подсчет контрольных сумм для присутствующих на диске файлов и сохранения их, длины файлов, даты последней модификации в базе данных антивируса. При запуске сверяются данные ревизора с реальными значениями	Оперативность	Не может определить вирус в новых файлах (при разархивировании, почтовых)
Блокировщики (сторожа)	Программы, перехватывающие вирусоопасные ситуации и сообщающие об этом поль зователю (например, запись в загрузочный сектор диска).	Остановка вируса на ранней стадии	Нет универсальности

Примеры антивирусных программ

- *программы-полифаги*
  - **Norton AntiVirus**
  - **DoctorWeb**
  - **Aidstest**
  - **AntiViral Toolkit Pro**
  - **Symantec**
  - **Not32**
- *программы-блокировщики (сторожа)*
  - **AntiViral Toolkit Pro Monitor**
  - **Avast**

Параметры сравнения	**Вирусы биологические**	**Вирусы компьютерные**
краткая характеристика и строение		
механизм воздействия		
классификация по различным основаниям		
пути и источники заражения		
признаки заражения		
антивирусные средства		
примеры антивирусных средств		
профилактика		