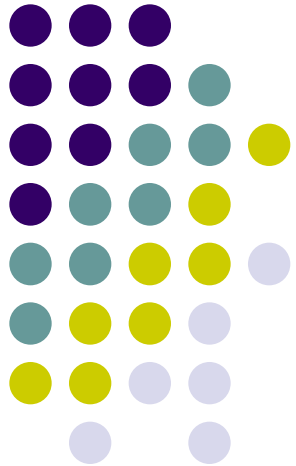
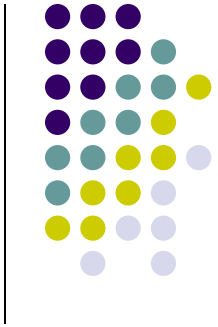
«Компьютерные вирусы».



Что такое «вирус»?



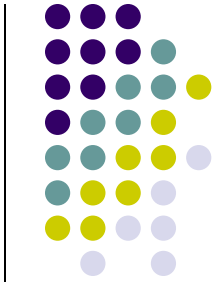
- Из словаря С.И. Ожегова:

Вирус – мельчайшая неклеточная частица, размножающаяся в живых
Клетках, возбудитель инфекционных заболеваний.

- Из энциклопедии «Лаборатории Касперского»:

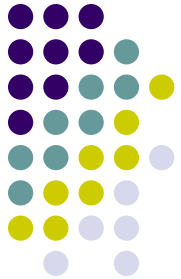
Компьютерный вирус – «специально созданная небольшая программа, способная к саморазмножению, «засорению» компьютера и выпол-нению других нежелательных действий.

Признаки заражения:



- Некоторые программы перестают работать или работают с ошибками;
- Размер некоторых исполнимых файлов и время их создания изменяются;
- На экран выводятся посторонние символы и сообщения, появляются странные видео – и звуковые эффекты;
- Работа компьютера замедляется и уменьшается размер свободной оперативной памяти;
- Некоторые файлы и диски оказываются испорченными (иногда необратимо, если вирус отформатирует диск);
- Компьютер перестаёт загружаться с жёсткого диска;

Пути проникновения вирусов в компьютер.



На столе лежит дискета,
У неё запорчен бут.
Через дырочку в конверте
Её вирусы грызут.

Как вы считаете, насколько реально то, что описано в стихотворении? Как вирусы могут проникнуть в компьютер?

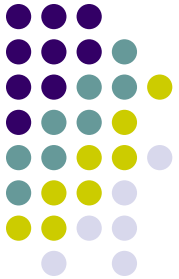
Пути проникновения:

- 1. Через дискету и другие внешние носители:

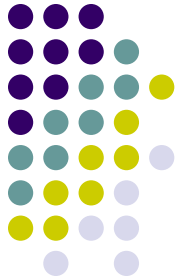
- 2. Через компьютерную сеть:

Вирусы можно разделить на классы по следующим основным признакам:

- По среде обитания;
- Вирусы операционной системы;
- По особенностям алгоритма работы;
- По деструктивным возможностям;

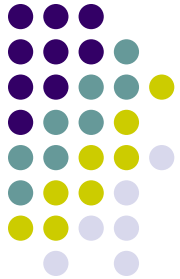


По среде обитания:



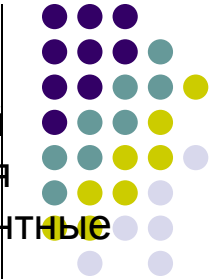
- Файловые вирусы – либо различными способами внедряются в выполняемые файлы, либо создают фильмы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (Link-вирусы).
- Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), или меняют указатель на активный boot-сектор;
- Макро-вирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов;
- Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты;

Вирусы операционной системы:



Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких операционных систем – DOS, WINDOWS и т.д. Макровирусы заражают файлы форматов Word, Excel и т.д. Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

По особенностям работы алгоритма:



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.

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

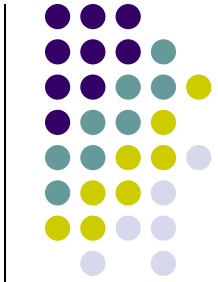
Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик-вирусы – это достаточно труднообнаруживаемые вирусы. Сложность их обнаружения достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

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

По деструктивным возможностям:

- 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 прочими эффектами;
- Опасные, которые могут привести к серьёзным сбоям в работе компьютера;
- Очень опасные, в алгоритм 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.

Методы защиты



Профилактические меры

Антивирусные программы.

Профилактические меры:

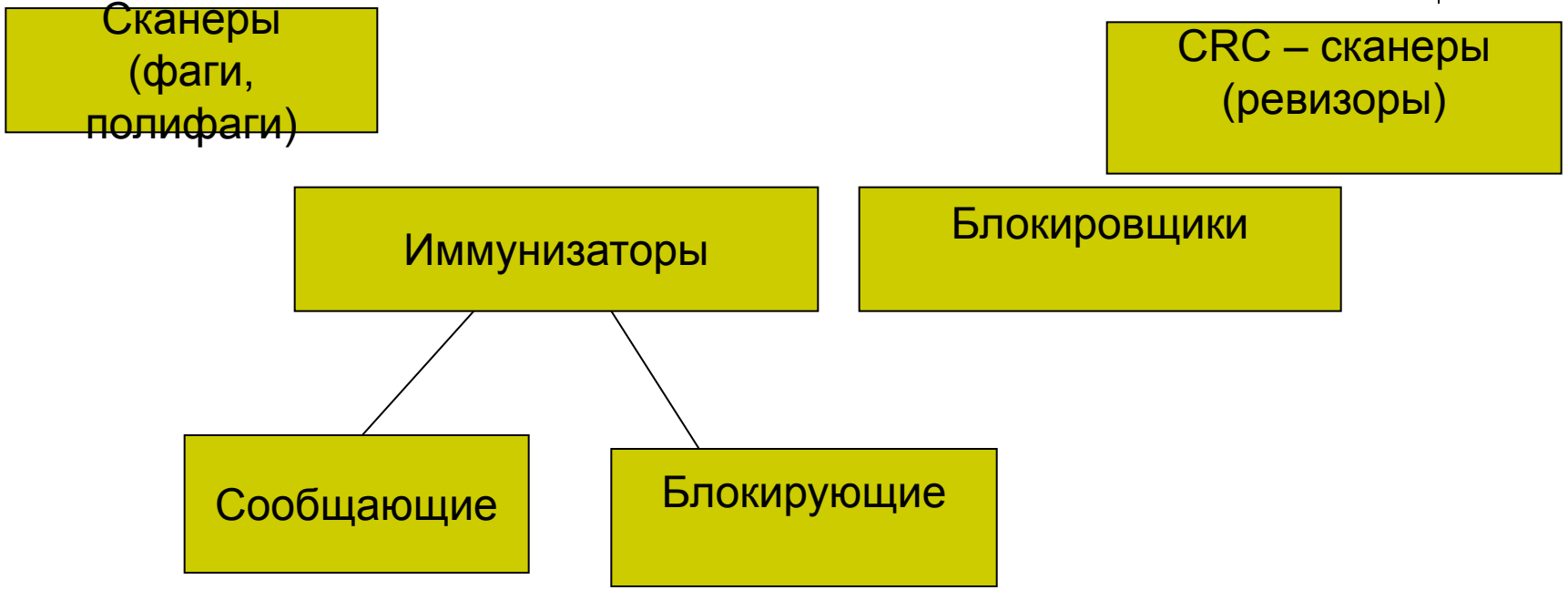
- Копирование информации.

(создание копий файлов и системных областей дисков).

- Разграничение доступа.

(предотвращение несанкционированного использования информации, в частности защита от изменения программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей).

Антивирусные программы:



Универсальные

Сканеры

Универсальные

Специализированные

Нерезидентные
(по запросу)

Резидентные
(на лету)

Составьте конспект в тетради в приведённой ниже форме:

Тема:

Определение вируса: (выделите одно общее свойство из обоих определений).

Признаки заражения:

Пути проникновения:

Типы вирусов:

Методы защиты: