Антивирусная защита персонального компьютера

Антивирусная защита ПК

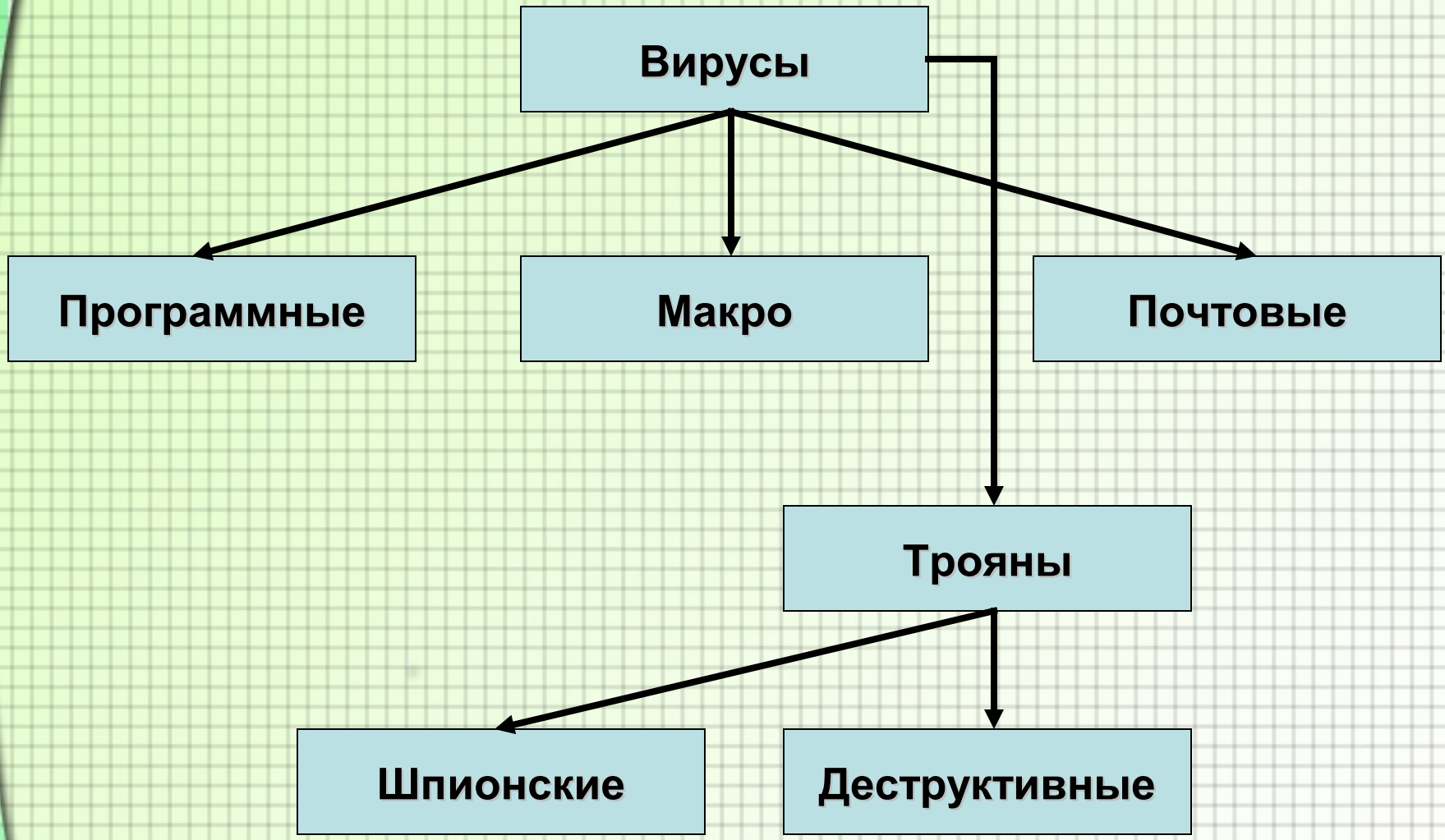
1. Классификация компьютерных вирусов
2. Возможные пути заражения компьютеров
3. Симптомы присутствия вирусов
3. Пассивные методы защиты
4. Активные методы защиты

Классификация вирусов

Компьютерный вирус – это программа, способная к саморазмножению, возможно имеющая деструктивные свойства и действующая без ведома человека.

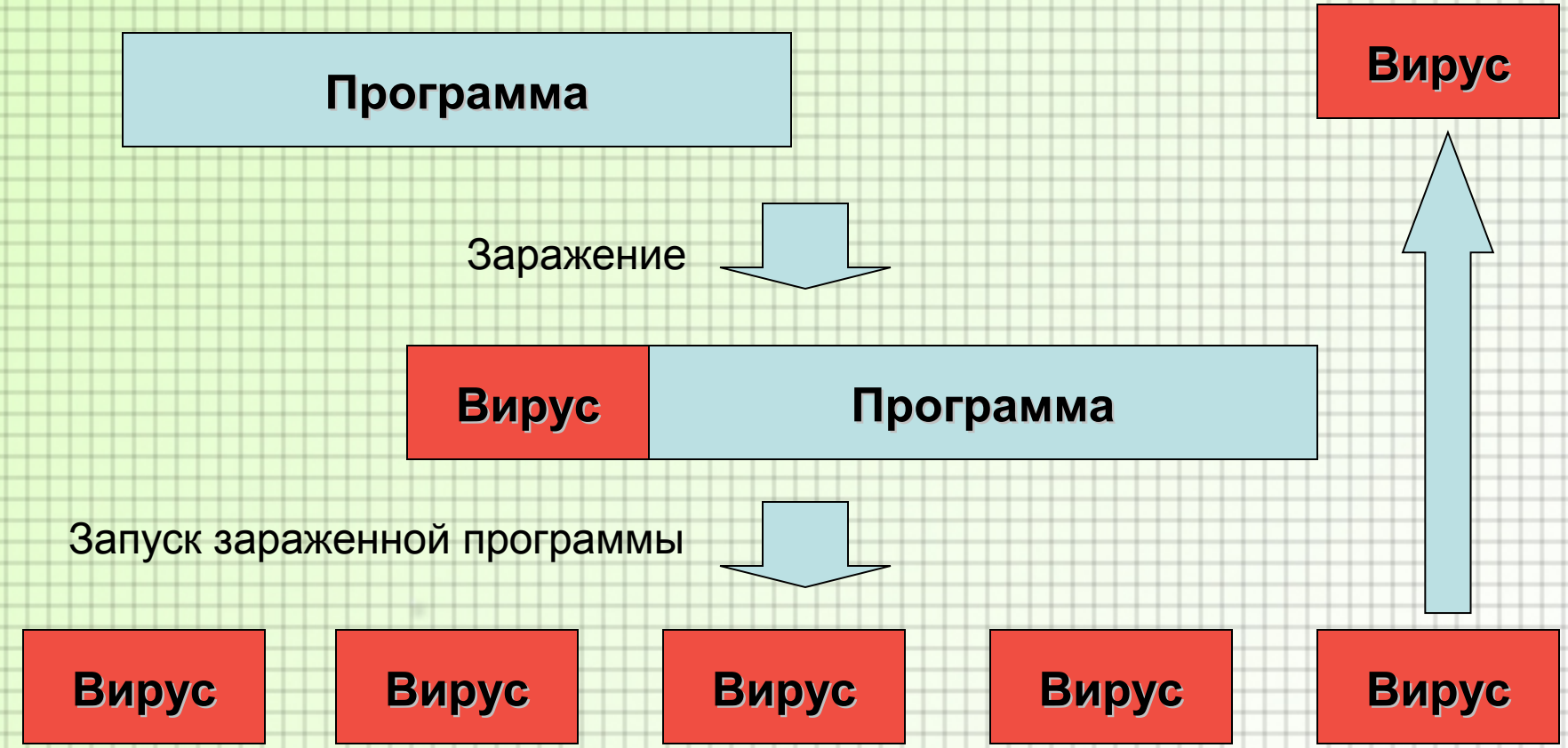
1. **Саморазмножение** – активируясь где-либо на компьютере, вирус начинает копировать себя и заражать все новые и новые объекты.
2. **Деструктивность** – многие вирусы в процессе своей работы портят данные, а иногда даже «железо».
3. **Скрытность** – Вирус действует без ведома человека, чаще всего стараясь скрыть свое присутствие на компьютере.

Классификация вирусов



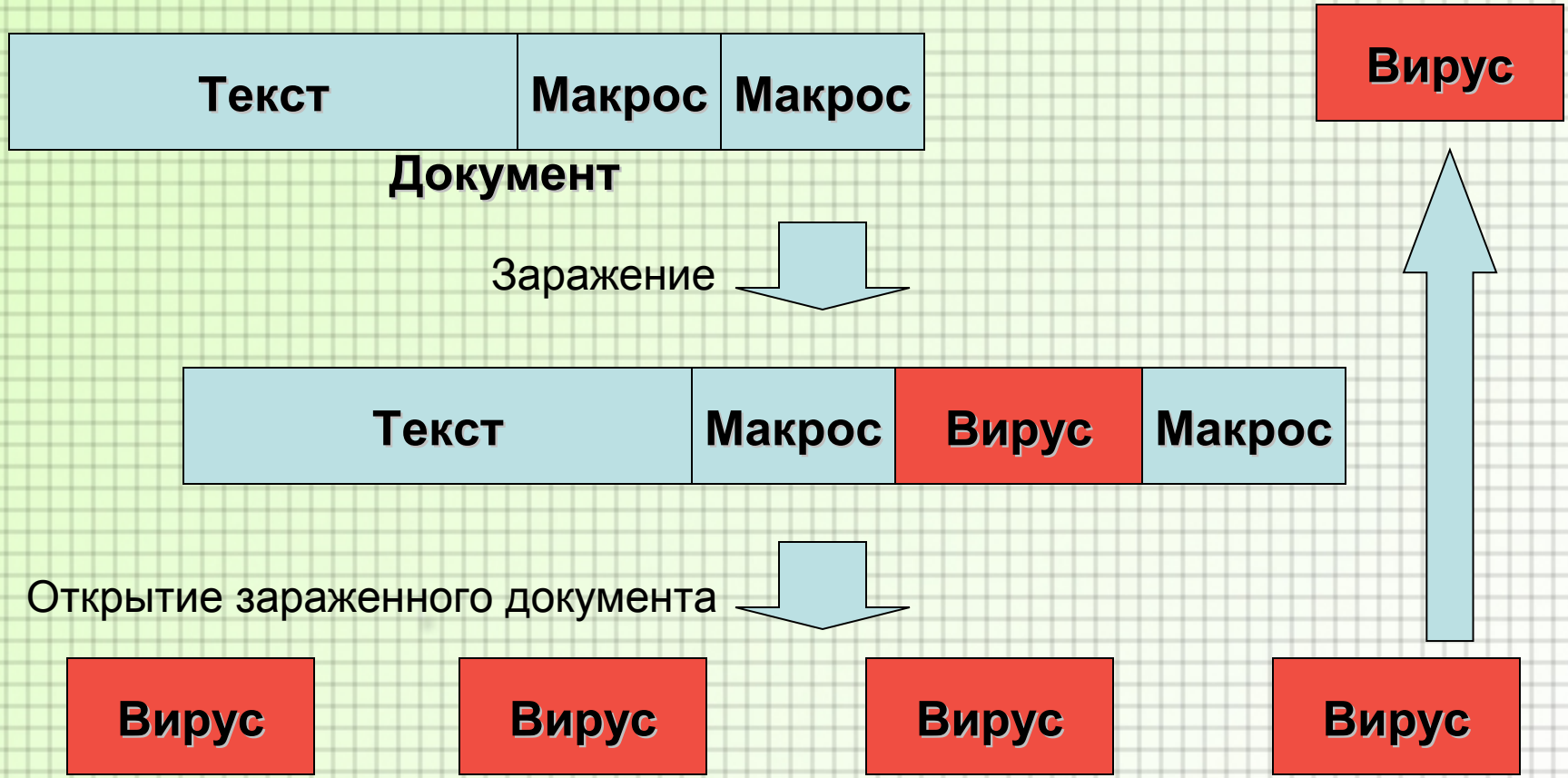
Классификация вирусов

Тип 1. Программные вирусы.



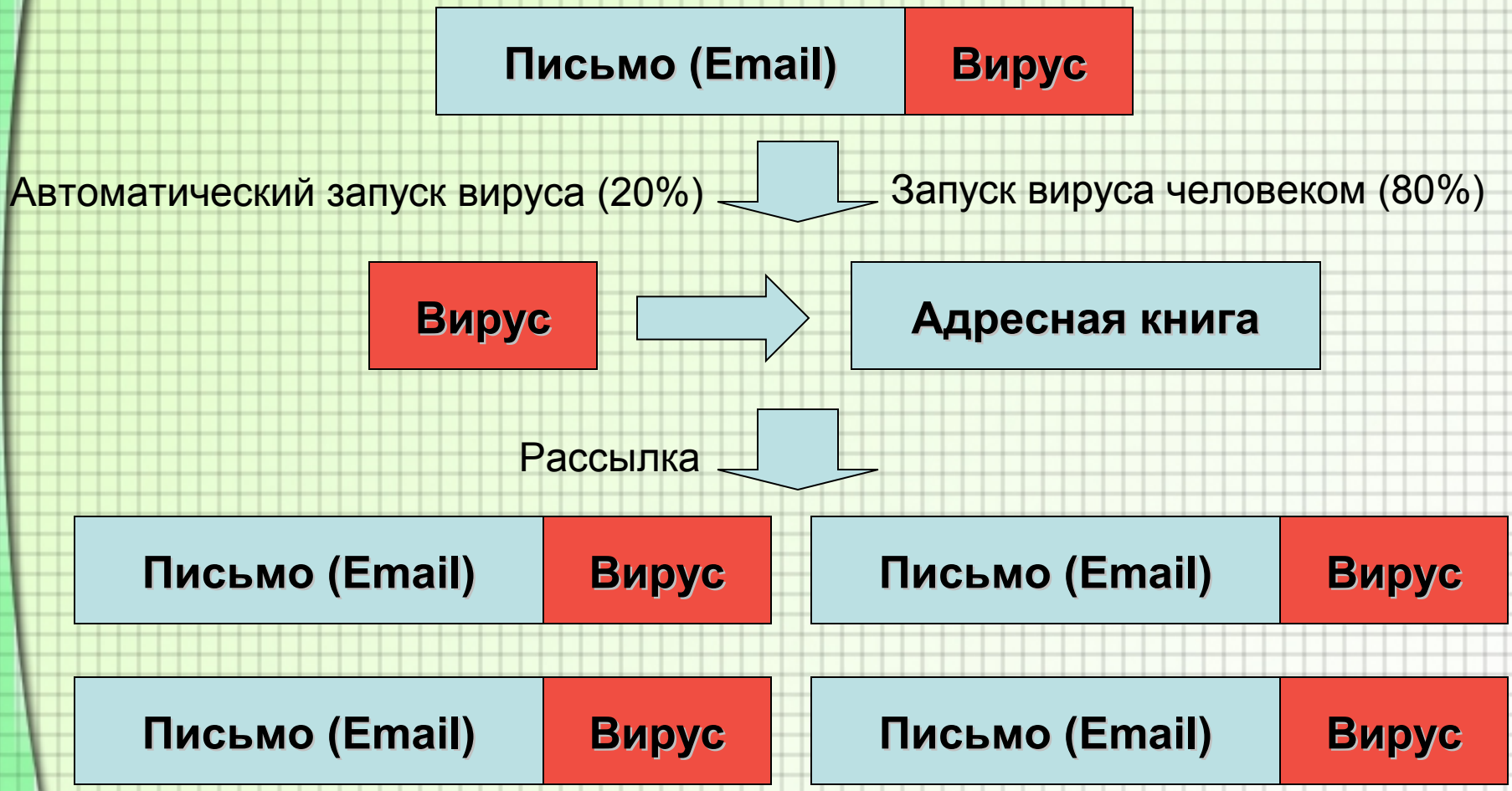
Классификация вирусов

Тип 2. Макро вирусы



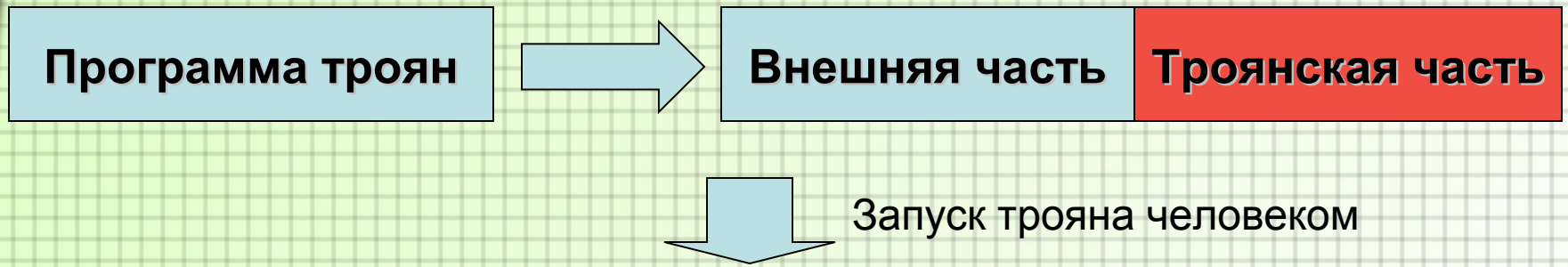
Классификация вирусов

Тип 3. Почтовые вирусы (черви).



Классификация вирусов

Тип 4. Троянские кони.



1. Имена и пароли
2. Номера кредиток
3. Конфиденциальная информация

и т.д.

1. Уничтожение файлов
2. Порча оборудования

Занесение в систему какого-либо вируса

Возможные пути заражения

1. Вирусы практически не существуют в «чистом» виде. Они распространяются вместе с зараженными объектами.
2. Чтобы вирус начал свою работу, он должен быть активирован. Само наличие зараженного объекта на компьютере еще не означает присутствие в системе активного вируса.
3. Существуют вирусы, передающиеся при работе некоторых программ, поддерживающих постоянную связь с Интернетом. Такие вирусы активируются сами.

Возможные пути заражения

Файловые вирусы.

- Зараженная программа, которую вы запустили на своем компьютере
  - Интернет
  - CD Диски с непроверенным содержимым
  - Знакомые

- Незаметная для вас перекачка вируса из сети Интнернет
  - Программы для общения через Интернет, типа ICQ, AIM, итд.
  - «Дыры» в безопасности Windows и в частности в браузере

Возможные пути заражения

Макро вирусы.

- Зараженный документ, который вы открыли на своем компьютере
  - Любой путь попадания к вам документов Word, Excel, и т.д.
  - Очень часто люди получают такие вирусы через знакомых

- В отличие от файловых вирусов, макро вирусы не способны (пока) сами передаваться с компьютера на компьютер.

Возможные пути заражения

Почтовые вирусы.

- Почтовый вирус можно получить только в электронном письме
  - Письмо от неизвестного вам человека
  - Письмо от знакомого человека на неожиданную тему
  - Письмо от знакомого человека с ожидаемой темой, например – поздравление с Новым Годом

- Часто почтовые вирусы видны в письме, как прикрепленные файлы (аттачменты).

- Многие создатели почтовых вирусов надеются на человеческое любопытство или глупость.

Возможные пути заражения

Программы-Трояны.

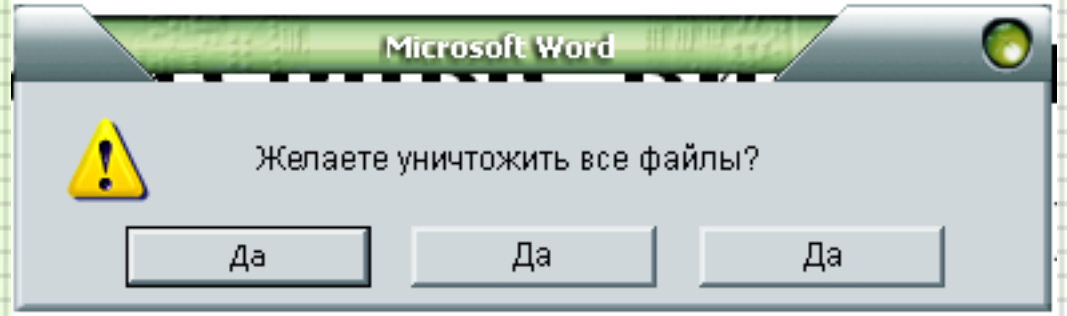
- Сами трояны как правило не умеют ни размножаться, ни передаваться самостоятельно

- Трояны представляются пользователям, как полезные, или забавные программы
  - Хранители экрана
  - Красивые графические эффекты (фейерверк)
  - Поздравления с праздниками
  - Программы ускорения работы Интернета
  - Различные утилиты, обещающие улучшить работу компьютера

- Многие трояны маскируются под не исполняемые фалы
  - Картинки
  - Музыка

Симптомы присутствия вирусов

1. «На глаз» практически невозможно сказать есть ли вирус в системе. Почти все симптомы не являются достоверными признаками присутствия вируса
2. Странное поведение системы (спонтанные перезагрузки, неожиданные «повисания» на некоторое время, частое выведение сообщений о системных ошибках)
3. Программы, которые раньше работали, перестают нормально работать без видимых причин
4. Необычные сообщения компьютера, не похожие на сообщения системы.



Симптомы присутствия вирусов

5. Система постоянно передает данные через соединение с Интернетом

6. Система стала необычно долго загружаться
7. Система показывает странные картинки на экран, например рожицы
8. Вам стали приходить письма с отметкой о невозможности послать ваше письмо от людей, которым вы писем не посылали. Отправитель этих писем как правило обозначен как «Mailer-Daemon»
9. Оплаченное соединение с Интернет кончилось значительно быстрее, чем вы того ожидали
10. Стремительно уменьшается свободное место на дисках
11. Система перестала запускаться

Пассивные методы защиты

Защита без применения антивирусных программ

1. Используйте только те программы, которые получены из надежных источников
2. Покупая пиратское программное обеспечение старайтесь брать диски тех команд, которые выпускают много продукции
3. Если офисная программа при открытии документа предлагает вам отключить макросы, лучше согласитесь. Если они там действительно необходимы, их потом можно включить.
4. Если скаченный или полученный по почте вами файл имеет двойное расширение, лучше сотрите его. Примеры – picture.jpg.exe, music.mp3.exe, и так далее.
5. Если вам в письме пришел файл с расширением pif – то это скорее всего вирус.

Пассивные методы защиты

6. Если от незнакомого человека приходит письмо, содержащее в себе присоединенный файл – не открывайте его, а лучше сразу сотрите это письмо.

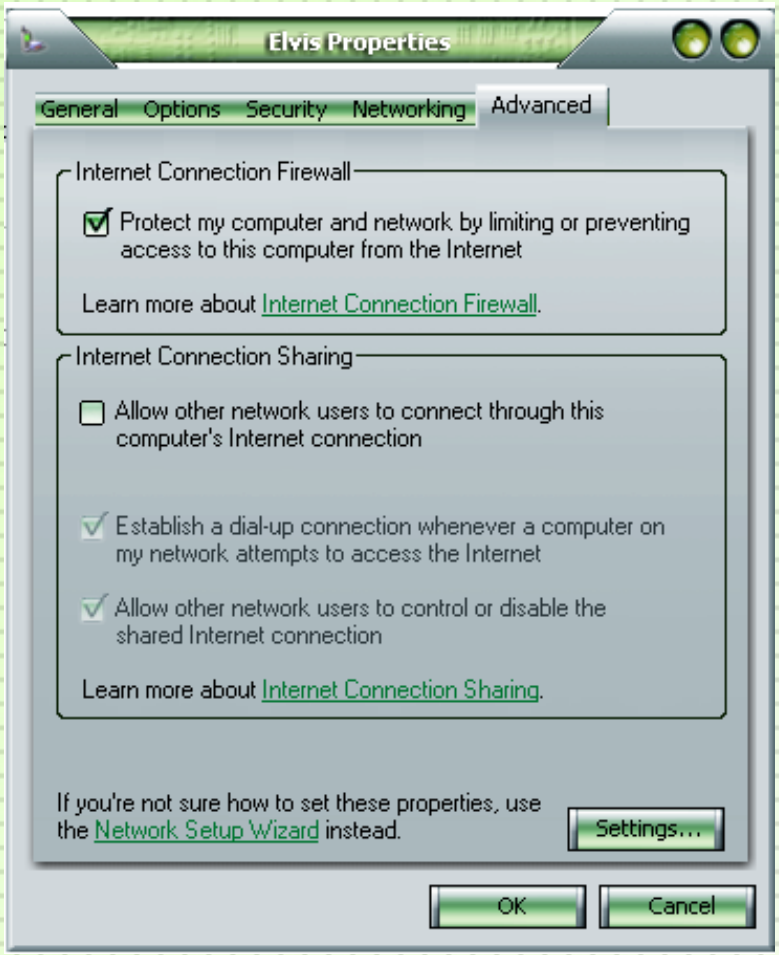
7. Если от знакомого человека приходит странное письмо, то лучше не открывайте файлы, присоединенные к нему. Пример – человек, не знающий английского, вдруг присылает вам письмо на английском языке.

8. Если вы заходите на какой-либо сайт и вам без вашего на то желания предлагают скачать какую-то программу, не стоит этого делать.

9. Большинство почтовых вирусов живут только в программе MS Outlook (Express). Если пользоваться другой программой (The Bat! например), многие вирусы станут для вас безопасными.

Пассивные методы защиты

10. Включите Брандмауэр в настройках соединения с Интернет.



Полный путь к этой настройке:

Мой компьютер (My computer)–

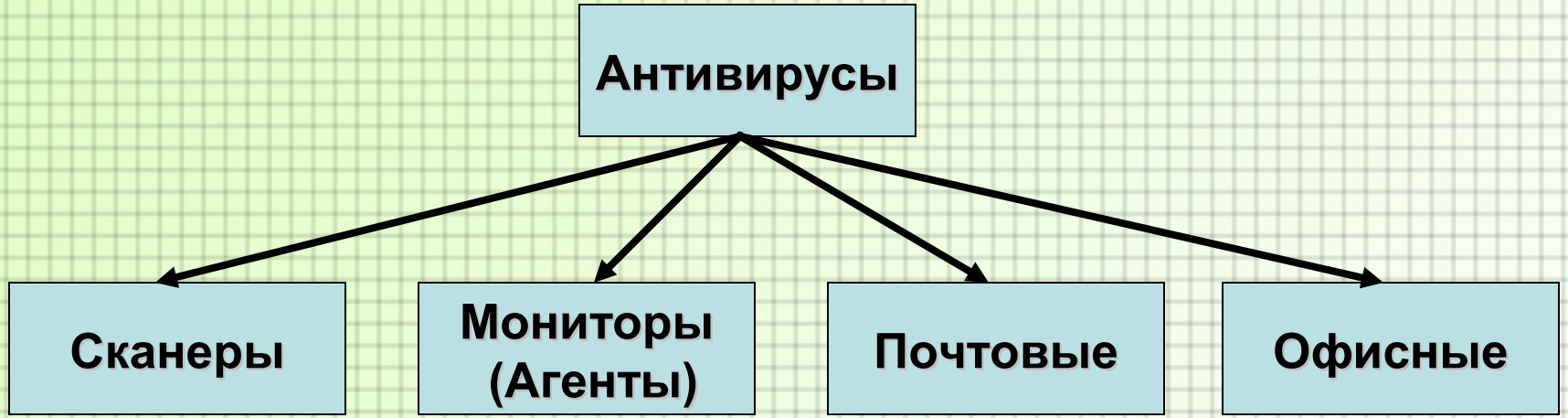
Мои сетевые подключения (My network places) –

Просмотреть сетевые подключения (View Network Connections) –

Выбрать подключение, нажать на нем правой кнопкой мыши, выбрать «свойства» (properties), в открывшемся диалоге нужна последняя закладка – «дополнительно» (advanced).

Активные методы защиты

Защита с применением антивирусных программ



- Сканеры
  - Сканируют все файлы системы
  - Обнаруживают неизвестные вирусы
  - Запускаются вручную
  - Работают довольно долго
- Мониторы (Агенты)
  - Сканируют запускаемые программы
  - Запускаются автоматически при запуске системы
  - Замедляют работу компьютера
- Почтовые
  - Сканируют приходящие письма
  - Запускаются автоматически при старте почтовой программы
  - Иногда отсеивают нормальные письма
- Офисные
  - Сканируют все открываемые файлы
  - Запускаются автоматически
  - Часто мешают работе других программ, как то переводчиков, словарей, OCR

Активные методы защиты

Несколько фактов на тему работы антивирусов

• "Защищает от всех известных вирусов!" - это рекламный трюк. Любой антивирус защищает от всех известных ему вирусов, даже если их всего два.

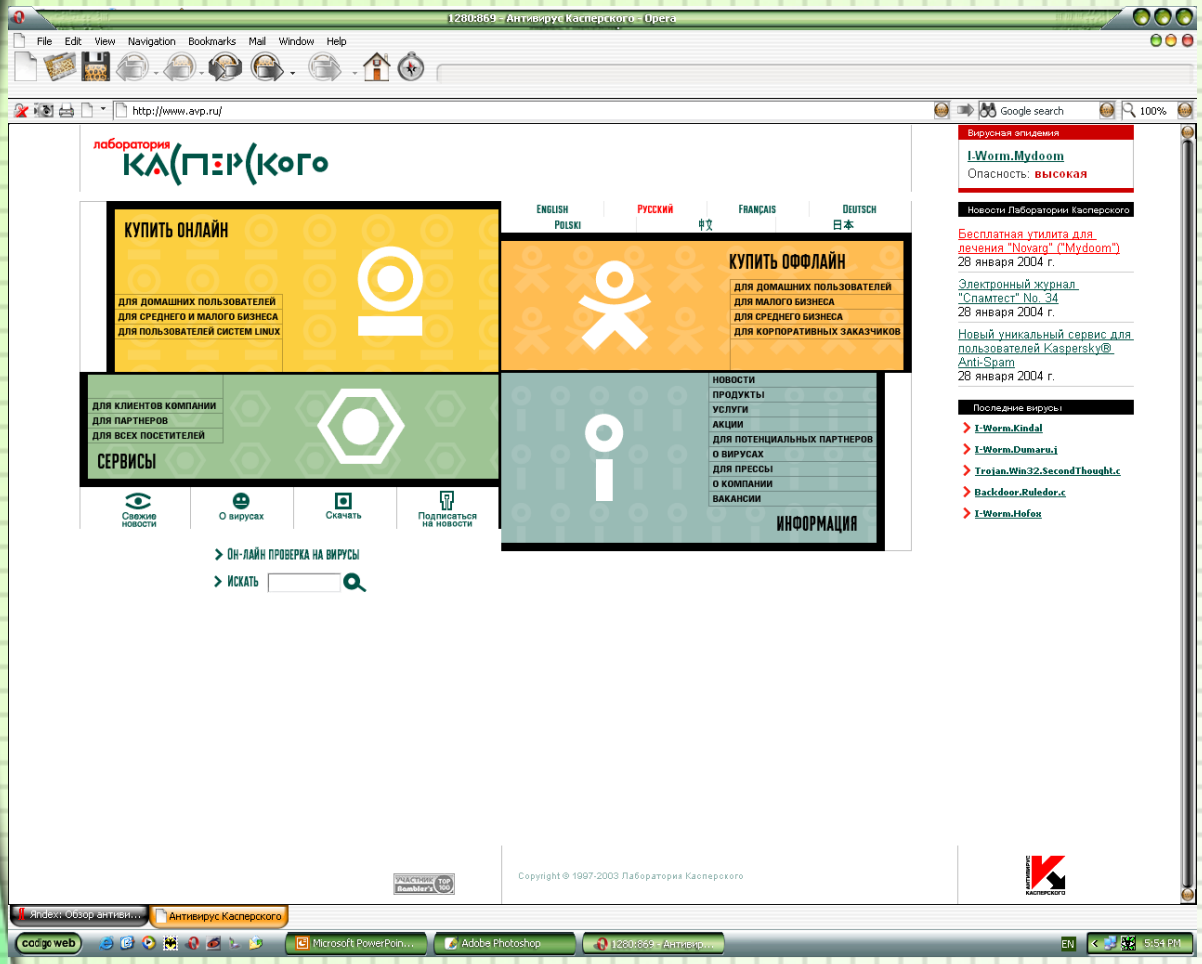
•Ни один антивирус не способен защитить даже от всех существующих (на момент обновления баз) вирусов - всегда есть вероятность, что какой-либо вирус не попал к разработчикам антивирусов

•Неизвестные обнаруженные вирусы и подозрительные объекты не лечатся, пока с очередным обновлением баз или версии антивируса не появится лечащий модуль

•Скорость проверки не говорит о качестве, "тщательности" проверки. Разные методы проверки действуют с разной скоростью.

Активные методы защиты

Антивирусы Касперского. (http://www.avp.ru)



Неоднократно получал награды, как лучший в мире антивирусный пакет.

На сайте быстро появляются утилиты для лечения последних вирусов.

Самый полный по возможностям пакет.

Активные методы защиты

Антивирусы Данилова – Dr.WEB. (http://www.drweb.ru)

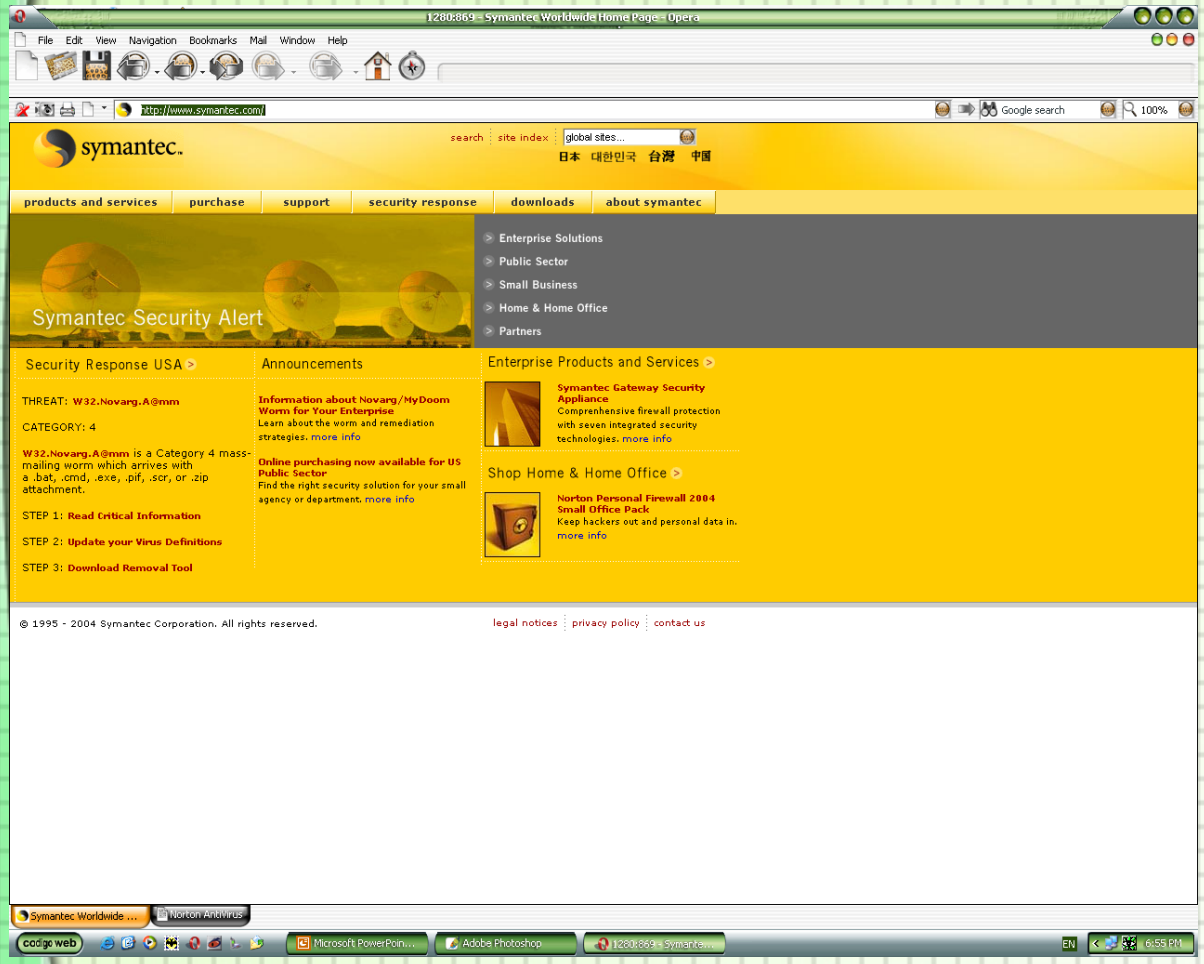
Основной антивирус – Dr.WEB имеет небольшой по сравнению с другими размер.

Легко устанавливается и используется.

Имеет свой собственный анализатор кода, что позволяет находить новые вирусы, которые не находят другие.

Активные методы защиты

Нортон Антивирус (NAV, Symantec antivirus).
(http://www.symantec.com, http://www.symantec.com/nav/nav_9xnt/)



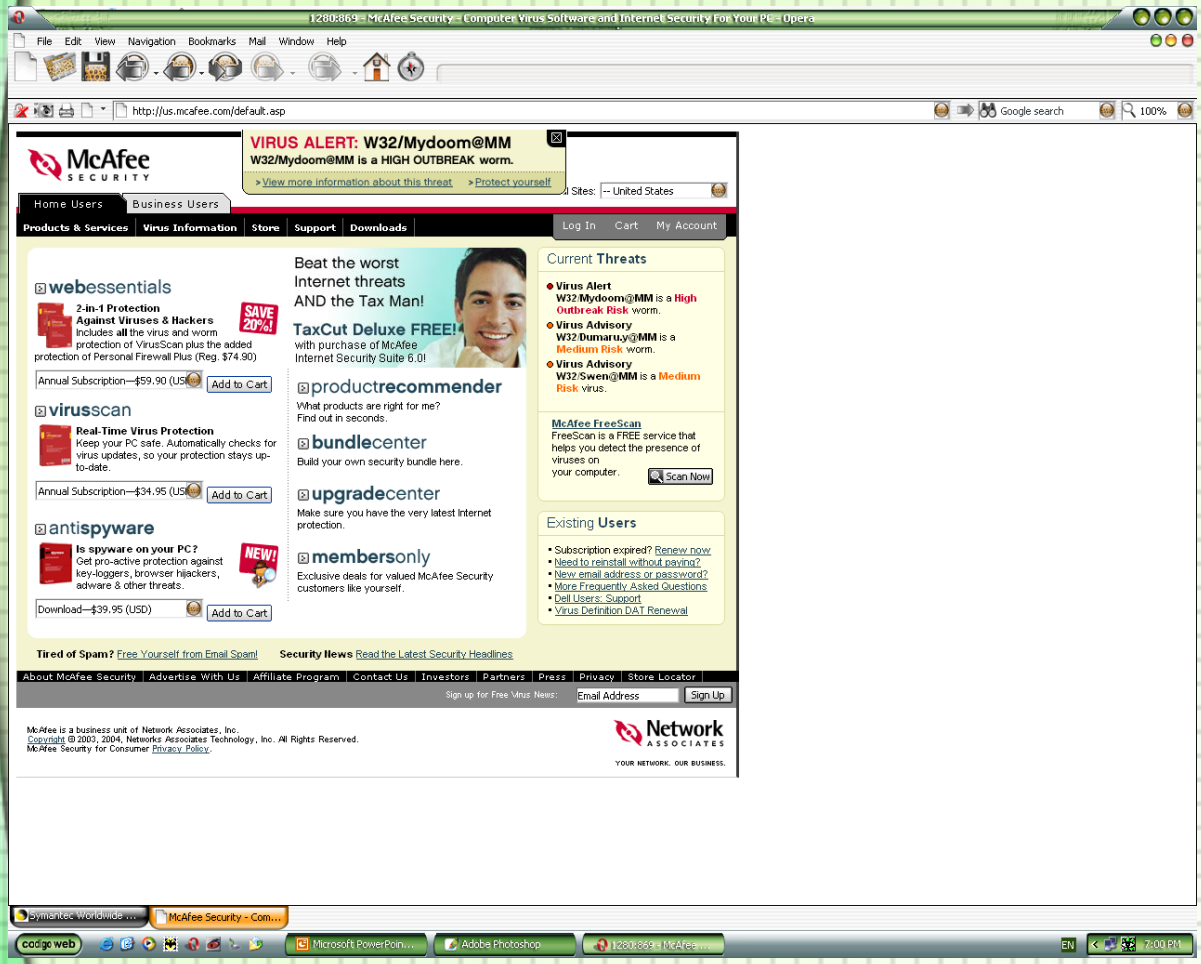
Самый распространенный западный антивирус

Очень мощный пакет, включающий в себя все аспекты защиты

Иногда лучше справляется с вирусами западного происхождения, чем отечественные разработки

Активные методы защиты

Антивирусы компании McAfee. (http://www.mcafee.ru)



McAfee – одна из первый в мире фирм, начавшая выпускать антивирусы.

Часто могут вылечить то, что не могут AVP и DrWEB из за другого алгоритма лечения.

Очень быстро появляются утилиты для лечения последних вирусов.