Обязательные условия вредоносности

- Отсутствие предварительного уведомления собственника информации (добросовестного пользователя) о действиях программы и их последствиях
- (или) действие без явного согласия (санкции) собственника информации (добросовестного пользователя)

Операционная система является самой опасной программой, поскольку ее возможности позволяют делать с компьютерной системой и информацией все, что угодно

Деструктивные возможности стандартных команд

- **Форматирование жесткого магнитного диска**
- **Логическая разметка жесткого диска**
- **Удаление дерева каталогов (файловой системы)**
- **Удаление файлов и каталогов с использованием «джокеров» и др.**

Разновидности программ

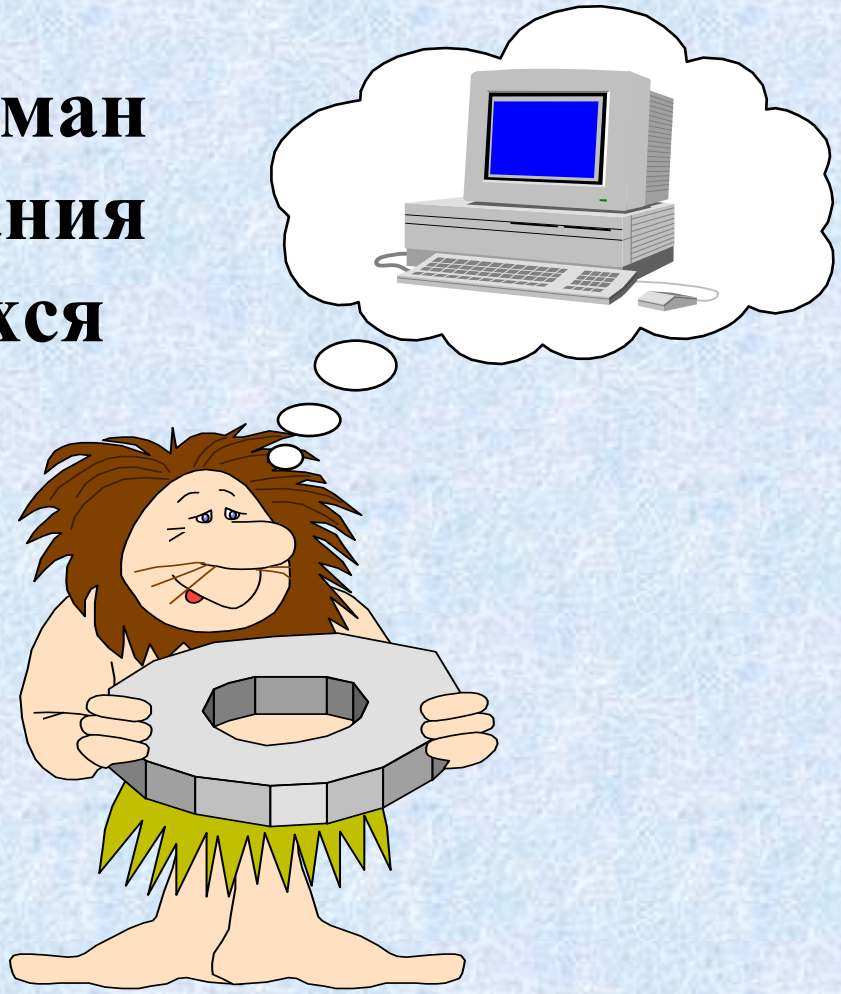
- **Исполняемый файл - основная программа в двоичном коде, которая содержит инструкции на языке центрального процессора.**
- **Макрос - укрупненная последовательность команд, автоматизирующая выполнение каких-либо повторяющихся операций**
- **Скрипт или сценарий - последовательность команд на языке символов, подлежащая анализу и выполнению с помощью командного интерпретатора.**
- **Библиотека - набор программных инструкций для выполнения стандартных операций**

Разновидности вредоносных программ

- Обычные файловые вирусы
- Загрузочные вирусы
- Flash-вирусы
- Макровирусы
- Генераторы вирусов
- Сетевые «черви»
- Программы «удаленного администрирования»
- Программные закладки
- «Троянские» оболочки
- «Логические бомбы»
- «Жадные» программы
- Программы - «глюки»

Происхождение вирусов

- **В 1951 году фон Нейман описал метод создания самовоспроизводящихся механизмов**



Классическое определение вирусов (Ф.Коэн)

- «Компьютерный вирус - программа, которая может заражать другие программы, модифицируя их посредством добавления своей, возможно измененной, копии»
- «Копии» вируса могут структурно и функционально отличаться между собой

Отличительные свойства компьютерных вирусов

- **Паразитическое существование - размещение внутри программного файла или программного фрагмента**
- **Способность к саморазмножению через внедрение в другие программы**
- **Выраженные деструктивные действия**
- **Наличие латентного (скрытого) периода**
- **Признаки авторства**

Характеристика «традиционных» вирусов

- Вирусы — программный код, обладающий следующими свойствами:

① **связан тем или иным способом с какой-нибудь программой и исполняется при запуске этой программы-носителя на выполнение;**

② **саморазмножается путем привязки самого себя, своей копии или подобного себе кода к другим программам**

Сущность вирусного заражения

- **Процесс - копирование двоичного или текстового кода в другой файл. Если этот файл уже существует - он модифицируется. Если не существует - он создается.**
- **Созданный или модифицированный файл должен иметь возможность автоматического или ручного запуска.**
- **При запуске инфицированного файла он вновь копирует свой код в другие файлы.**
- **Перед модификацией возможна проверка на наличие вирусного кода (чужой вирус уничтожается)**

Сущность вирусного заражения

- **Вирусное заражение отличается от обычного копирования. При копировании создается еще один файл (с другим именем или в другом каталоге). При вирусном заражении копируется код (бинарный или текстовый), причем созданный или модифицированный файл также должен уметь «размножаться» и иметь шансы на запуск**

Макровирусы

Макровирус - это событийно управляемый интерпретируемый код, содержащийся в программных сегментах (блоках) документов и шаблонов приложений офисного пакета фирмы Microsoft, обладающий свойством копирования в другие документы и шаблоны в ходе сеансов работы, и способный к выполнению различного рода деструктивных и (или) шпионских функций, наносящих ущерб конфиденциальности, целостности и доступности компьютерной информации

Особенности макрокода

- **Использование в качестве операционной системы приложений офисного пакета**
- **Размещение в документах, шаблонах и надстройках**
- **Текстовый формат интерпретируемого кода**
- **Использование возможностей автозапуска и событийного управления**
- **Хорошая «переносимость» на иную аппаратно-программную платформу**

Причины распространения макровирусов

- **Microsoft Office - базовая среда для разработки и редактирования документов**
- **Интегрированная среда разработки документов обеспечивает изоляцию от защитных механизмов операционной системы**
- **Широкие возможности встроенной в Office интегрированной среды программирования наряду с легкостью освоения VB и VBA начинающими пользователями.**

«Мифические» вирусы

- **Программы, способные вызвать неисправность жесткого диска за счет его повышенного износа**
- **Программы, способные «прожечь» экран монитора**
- **Программы, способные вызвать заболевания или смерть человека-оператора за счет мелькания экрана, изображений и др.**

Программные закладки - это особая категория вредоносных программ, запрограммированных на скрытое добывание информации о компьютерной системе

Отличительные свойства программных закладок

- Скрытность работы на всех этапах жизненного цикла
- Отсутствие механизма саморазмножения
- Явно выраженные «шпионские» функции
- Отсутствие демонстративных и выраженных вредоносных действий
- Анонимность разработки и пользования

Функции, реализуемые программными закладками

- Различные виды перехвата информации
- Выявление защитных функций ОС и приложений, их нейтрализация
- Повышение полномочий злоумышленника
- Избирательное уничтожение информации

Деструктивные воздействия программных закладок

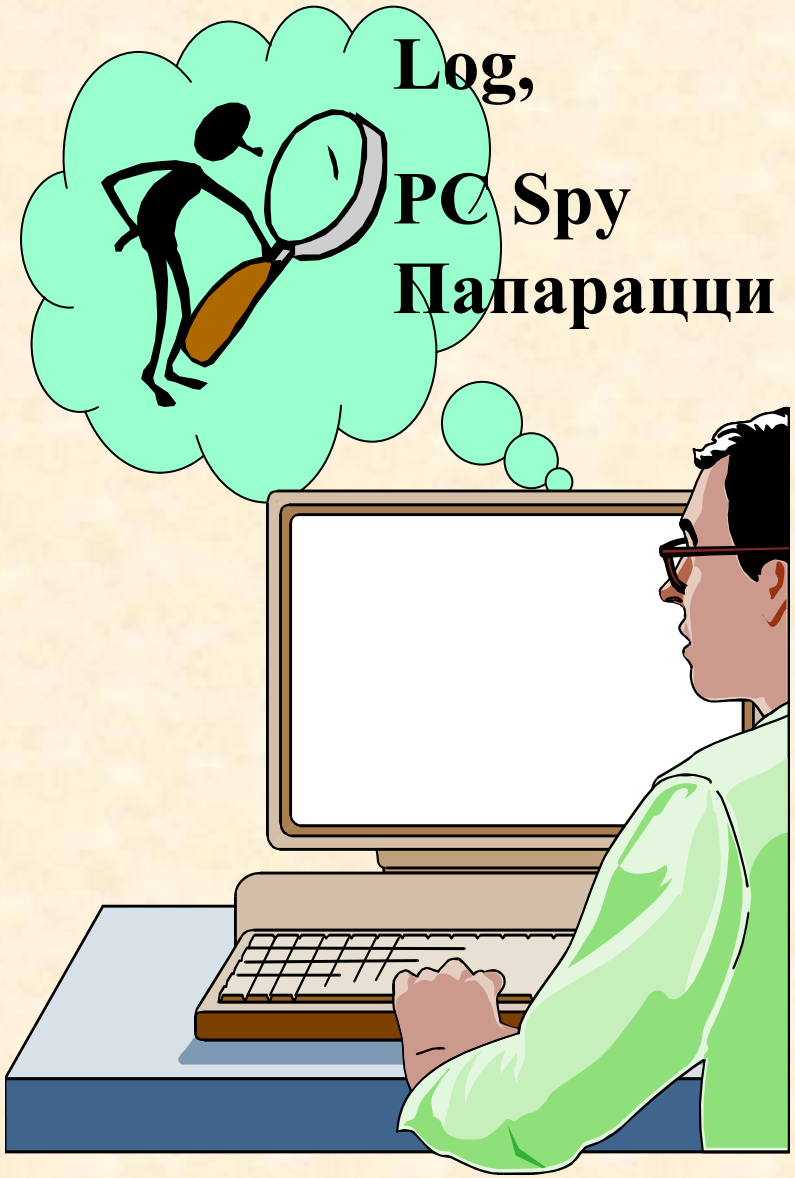
- **Копирование конфиденциальной информации (паролей, ключей, электронных документов)**
- **Изменение алгоритмов функционирования системных и прикладных программ (например, с целью отключения защиты)**
- **Навязывание определенных режимов работы (блокирование записи на диск при удалении файлов и др.)**

Информация, перехватываемая программными закладками

- Перехват клавиатурного и манипуляторного ввода
- Перехват аутентифицирующей информации
- Перехват информации, выводимой на печать
- Перехват документов, выводимых для редактирования
- Перехват удаляемой информации

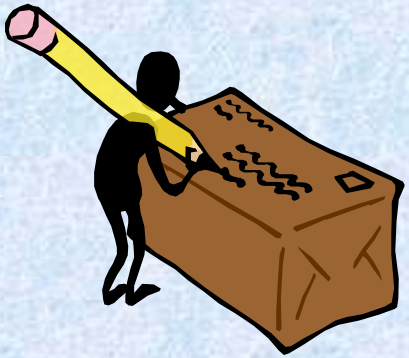
Предполагается, что хранимая информация для закладки недоступна (шифрование и др.)

Слежение за пользователем



- Хронометраж работы
- Кто работал (клавиатурный почерк)
- Характер деятельности (расчеты, работа с документами, программирование, игры)
- Запускаемые программы
- Исполняемые документы
- Снимки экрана

Клавиатурные перехватчики



- **Фиксация клавиатурного набора**
- **Фиксация «щелчков» мышью**
- **Шифрование и скрытие перехваченной информации**
- **Вывод на дискету или e-mail**

KeyLogger, HookDump, PC Activity Monitor Pro (PAMP и другие

Жизненный цикл «вредоносной» программы

ВИРУСЫ

- Проникновение
- Запуск на исполнение
- Заражение
- *********
- Заражение
- Деструктивные действия

ЗАКЛАДКИ

- Скрытое проникновение
- Легализация
- Отбор информации
- Упаковка и вывод отобранной информации
- Самоликвидация

«Логические бомбы»

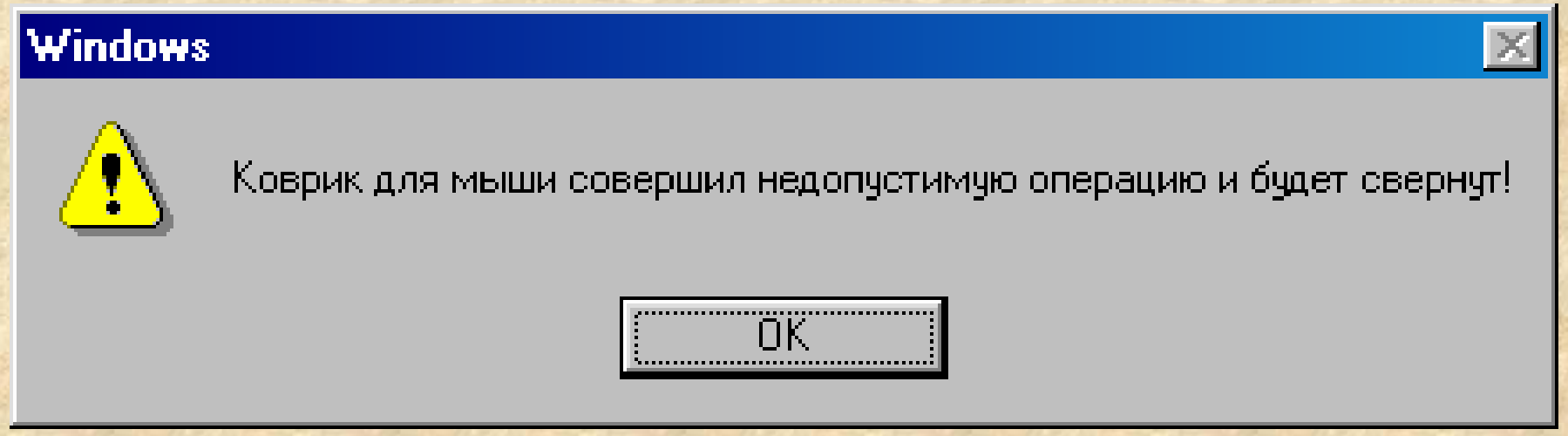
- **«Логической бомбой» называется фрагмент (модуль, процедура, функция) общей программы, который запускается по определенному событию и совершает определенные вредоносные действия**
- **Создатель «логической бомбы» - как правило программист-разработчик программы**

«Логическая бомба» может составлять часть иной вредоносной программы

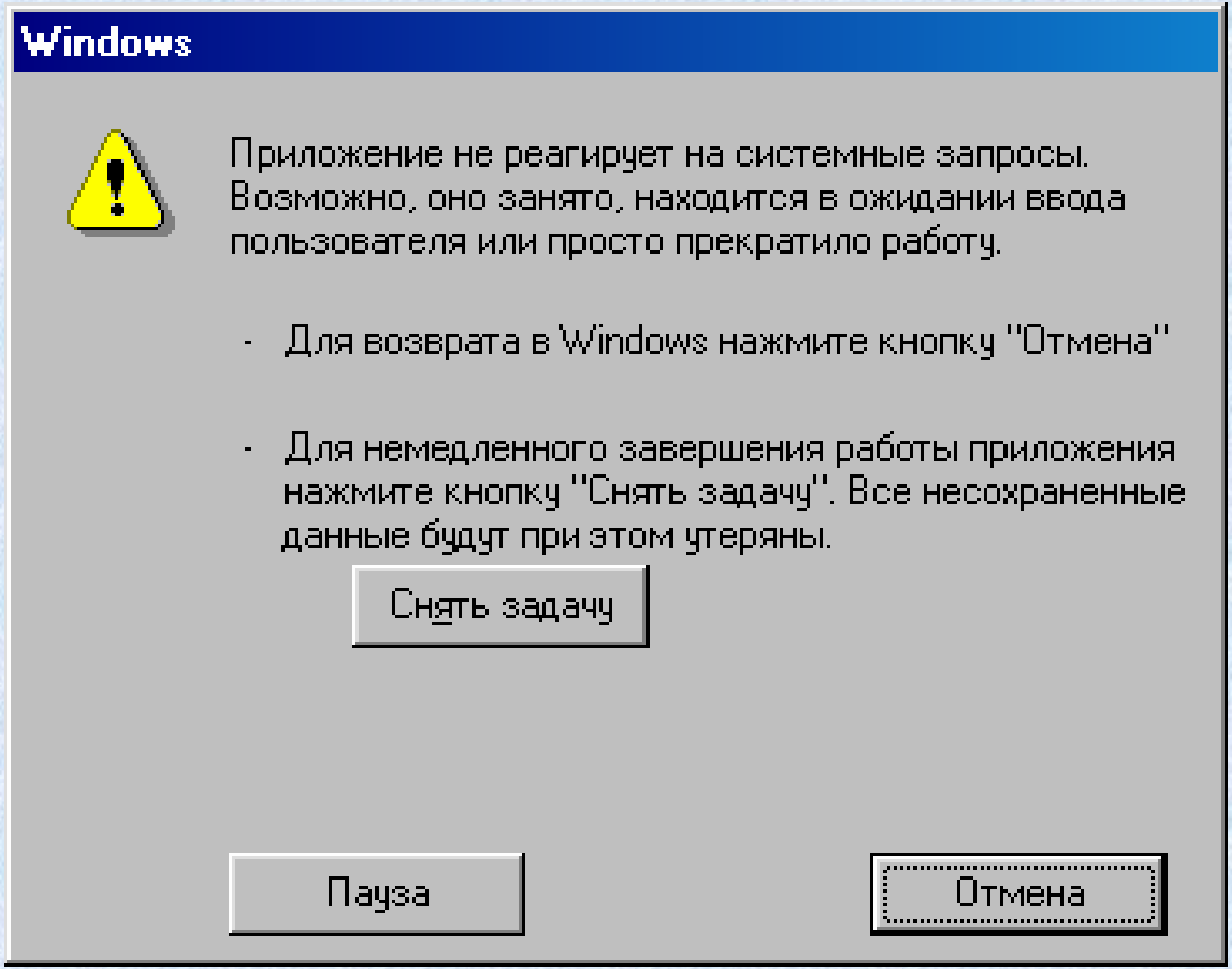
Примеры «логических бомб»

- **Программа на распечатку бухгалтерской ведомости начисления зарплаты, которая разрушает базу данных, если в ее списке не окажется фамилии программиста-разработчика**
- **Шифрование базы данных с требованием выкупа за предоставление ключа**

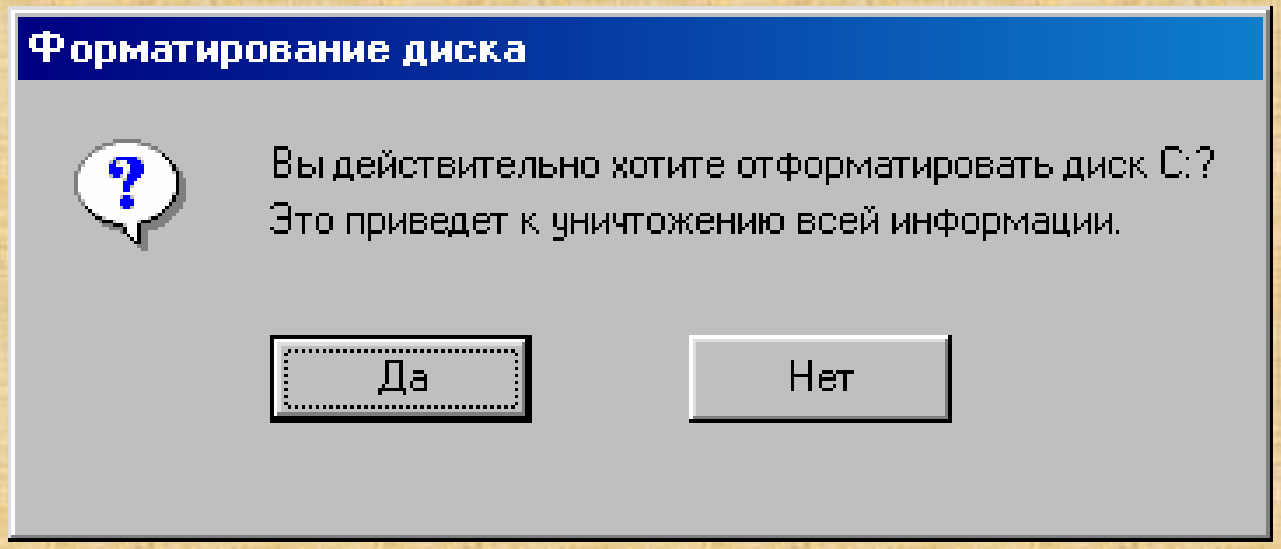
Программы - «глюки»

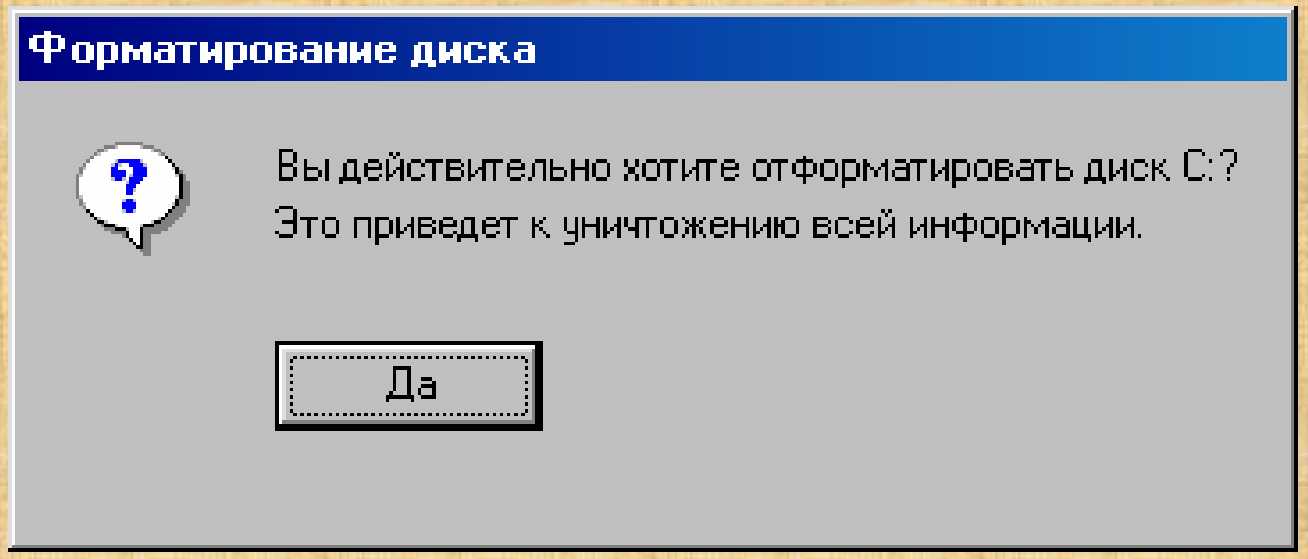


Примеры программ - «глюков»



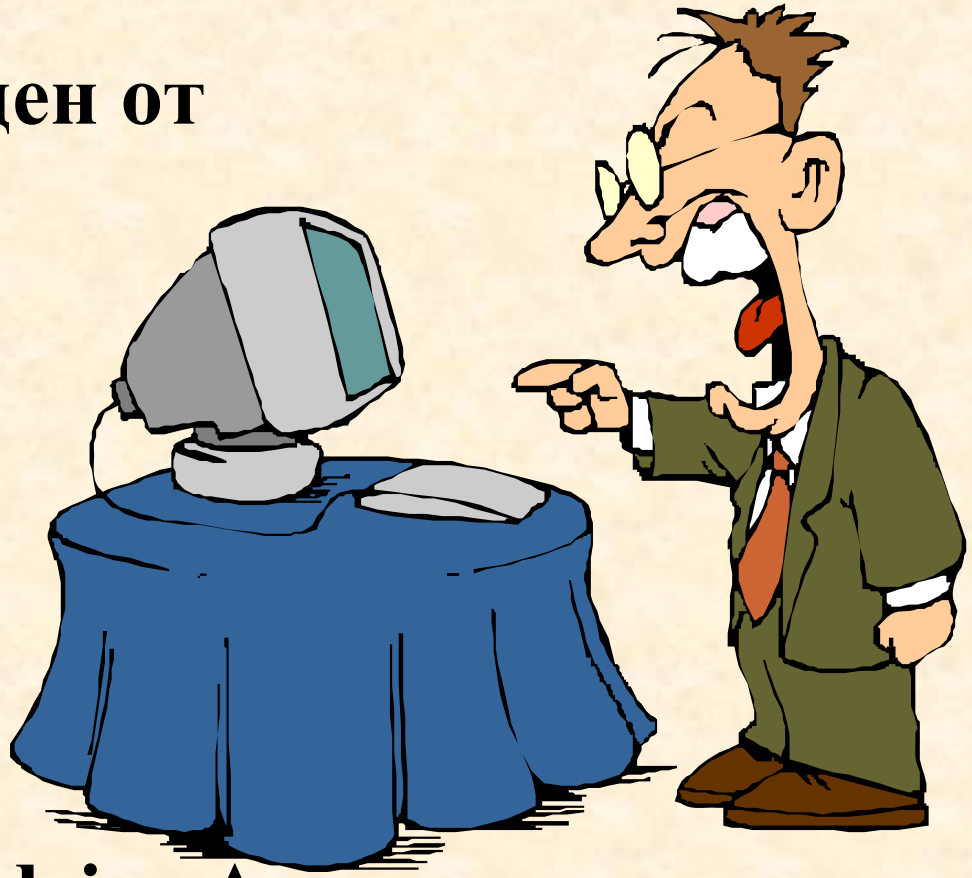
Примеры программ - «глюков»





Шутливые сообщения

- **Вентилятор защищен от записи!**
- **Дырка в диске C:**
- **В дисководе A: две дискеты!**
- **Invalid user at the computer!**
- **Insert 10$ in floppy drive A:**



Классификация вредоносных программ по деструктивным функциям

- Безвредные: создание звуковых и/или визуальных эффектов (проигрывание мелодий, движущиеся изображения, осыпающиеся буквы текста и др.)
- Опасные: сброс CMOS-памяти, логическое стирание файлов и каталогов, изменение системных параметров и др.
- Особо опасные: форматирование фиксированных дисков, разрушение файловой системы, реестра, стирание BIOS и др.

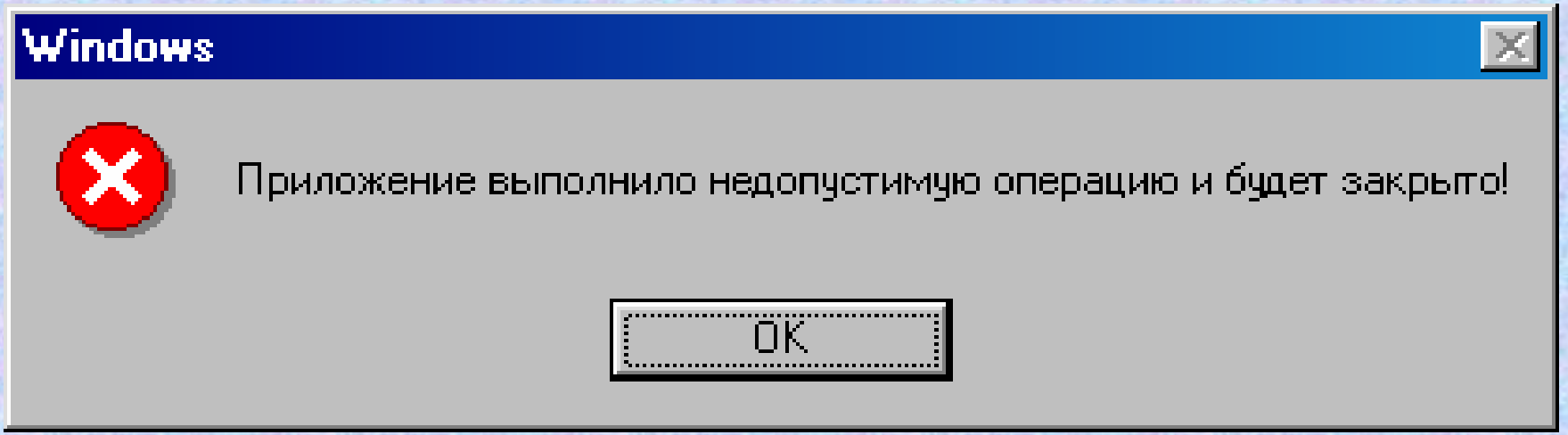
Характер деструктивных действий

- Генерация звуковых и визуальных эффектов
- Шутки с пользовательским интерфейсом
- Имитация программных сбоев и неисправностей аппаратуры
- Модификация, перемещение, удаление файлов и каталогов, манипуляции с их атрибутами
- Удаление файловой системы или ее части
- Форматирование фиксированных МНИ
- Перезапись (стирание) энергонезависимой памяти Flash-типа

Имитация правдоподобных отказов аппаратуры

- «Торможение» или неверное позиционирование курсора манипулятора
- «Отказ» одной или нескольких клавиш на клавиатуре
- Периодическое выключение монитора, изменение цветопередачи, частоты разверток
- Выдача сообщений о том, что дискета защищена от записи
- Шум во встроенном динамике при наборе текста
- Выдача информации о большом числе плохих секторов на винчестере (при тестировании и др.)

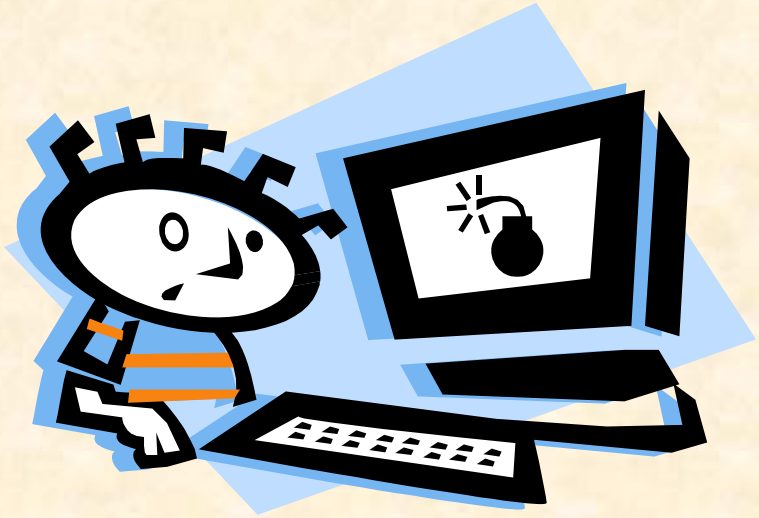
Имитация сбоев системного программного обеспечения



Внедрение вредоносных программ

- **Внедрением постороннего программного кода является помещение в оперативную или долговременную память компьютера кода и/или данных с целью последующего запуска на исполнение.**
- **Внедрение кода может сопровождаться его немедленным, либо отсроченным запуском, либо подготовкой к последующему запуску**

Условия, способствующие внедрению и запуску постороннего программного кода



- Огромное пространство угроз
- Значительная сложность компьютерных систем, которые пользователь не в силах контролировать
- Многочисленные настройки безопасности
- Режимы и настройки «по умолчанию», установленные разработчиками ПО