
Защита от вирусов
семинар

Самые известные вирусы и вирусные атаки

Двадцатка наиболее распространенных вредоносных программ

1. I-Worm.Klez 37,60%
2. I-Worm.Sobig 10,75%
3. I-Worm.Lentin 9,03%
4. I-Worm.Avron 3,30%
5. Macro.Word97.Thus 2,62%
6. I-Worm.Tanatos 1,38%
7. Macro. Word97.Marker 1,21%
8. Worm.Win32.Opasoft 1,13%
9. I-Worm.Hybris 1,04%
10. Win95.CIH 0,69%
11. Worm.Win32.Randon 0,58%
12. VBS.Redlof 0,57%
13. Backdoor.Death 0,51%
14. Win95.Spaces 0,51%
15. I-Worm.Roron 0,49%
16.Trojan.PSW.Gip 0,49%
17. Backdoor.NetDevil 0,48%
18. Win32.HLLP.Hantaner 0,45%
19. TrojanDropper.Win32.Delf 0,42%
20. TrojanDropper.Win32.Yabinder 0,41%

Самые известные вирусы и вирусные атаки

(доклады учащихся)

Brain

Первая эпидемия 1987 года была вызвана вирусом Brain (также известен как Пакистанский вирус), который был разработан братьями Амджатом и Базитом Алви (Amdjat и Basit Faroog Alvi) в 1986 и был обнаружен летом 1987. По данным McAfee, вирус заразил только в США более 18 тысяч компьютеров. Программа должна была наказать местных пиратов, ворующих программное обеспечение у их фирмы. В программке значились имена, адрес и телефоны братьев. Однако неожиданно для всех The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру. Вирус Brain являлся также и первым стелс-вирусом — при попытке чтения заражённого сектора он «подставлял» его незаражённый оригинал.

Чернобыль

Вирус "Чернобыль", например, полностью стирает BIOS (стартовую программу, расположенную в микросхеме ПЗУ, обеспечивающую работу компьютера). После такого компьютер вообще ничего не сможет выдать на экран. Но его работа легко блокируется, если внутри компьютера установлен переключатель, запрещающий писать в область ПЗУ. По этому это был первый, но и, как я думаю, последний представитель аппаратных вирусов.

Вирус Ball

На экране компьютера появлялся небольшой шарик. Он перемещался по экрану, отражаясь от его границ и некоторых символов.

Для борьбы с вирусом использовали специальную антивирусную программу SCAN фирмы McAfee. Она легко находила вирус на дискетах и жестких дисках компьютеров, а затем удаляла его. После такой процедуры вирус некоторое время не появлялся.

Впоследствии выяснилось, что вирус Ping Pong, он же вирус Ball, распространялся через загрузочные секторы дискет и дисков.

Вируса CloneWar

Имеет множество разновидностей.

Самая большая версия вируса, имеющая длину 923 байта, проверяет значение системного таймера и в некоторых случаях исполняет через динамик компьютера небольшую мелодию. Затем код вируса зацикливается, вызывая зависание компьютера.

Черная пятница

Вирус Jerusalem или Черная пятница удаляет файлы всех программ, запускаемых в пятницу тринадцатого числа.

Вирус Gloomy

Заражает выполнимые файлы в формате COM и EXE, резидентный. При каждом шестнадцатом запуске программы портит случайный сектор. Удаляет с диска файлы с именами "*.MS" и "*.?AS". Заменяет главную загрузочную запись на программу, которая после 511 загрузок компьютера форматирует диск. Содержит тексты "Gloomy Nutcracker(AB5) from the city of Brest(BY) with best wishes!" и "Only the Hope dies last!".

AIDS

В 1989 году появился первый «троянский конь» AIDS.[17] Вирус делал недоступными всю информацию на жёстком диске и высвечивал на экране лишь одну надпись: «Пришлите чек на $189 на такой-то адрес». Автор программы был арестован в момент обналичивания чека и осуждён за вымогательство.

Методики обнаружения и защиты от вирусов

Сканирование

Эвристический анализ

Обнаружение изменений

Резидентные мониторы

Вакцинирование программ

Аппаратная защита от вирусов

Сканирование

Антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов. Под сигнатурой понимается уникальная последовательность байт, принадлежащая вирусу, и не встречающаяся в других программах.

Эвристический анализ

Антивирусные программы, реализующие метод эвристического анализа, проверяют программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов.

Обнаружение изменений

Антивирусные программы могут предварительно запомнить характеристики всех областей диска, которые подвергаются нападению вируса, а затем периодически проверять их (отсюда происходит их название программы-ревизоры). Если будет обнаружено изменение, тогда возможно что на компьютер напал вирус.

Резидентные мониторы

Резидентный монитор сообщит пользователю, если какая-либо программа попытается изменить загрузочный сектор жесткого диска или дискеты, выполнимый файл.

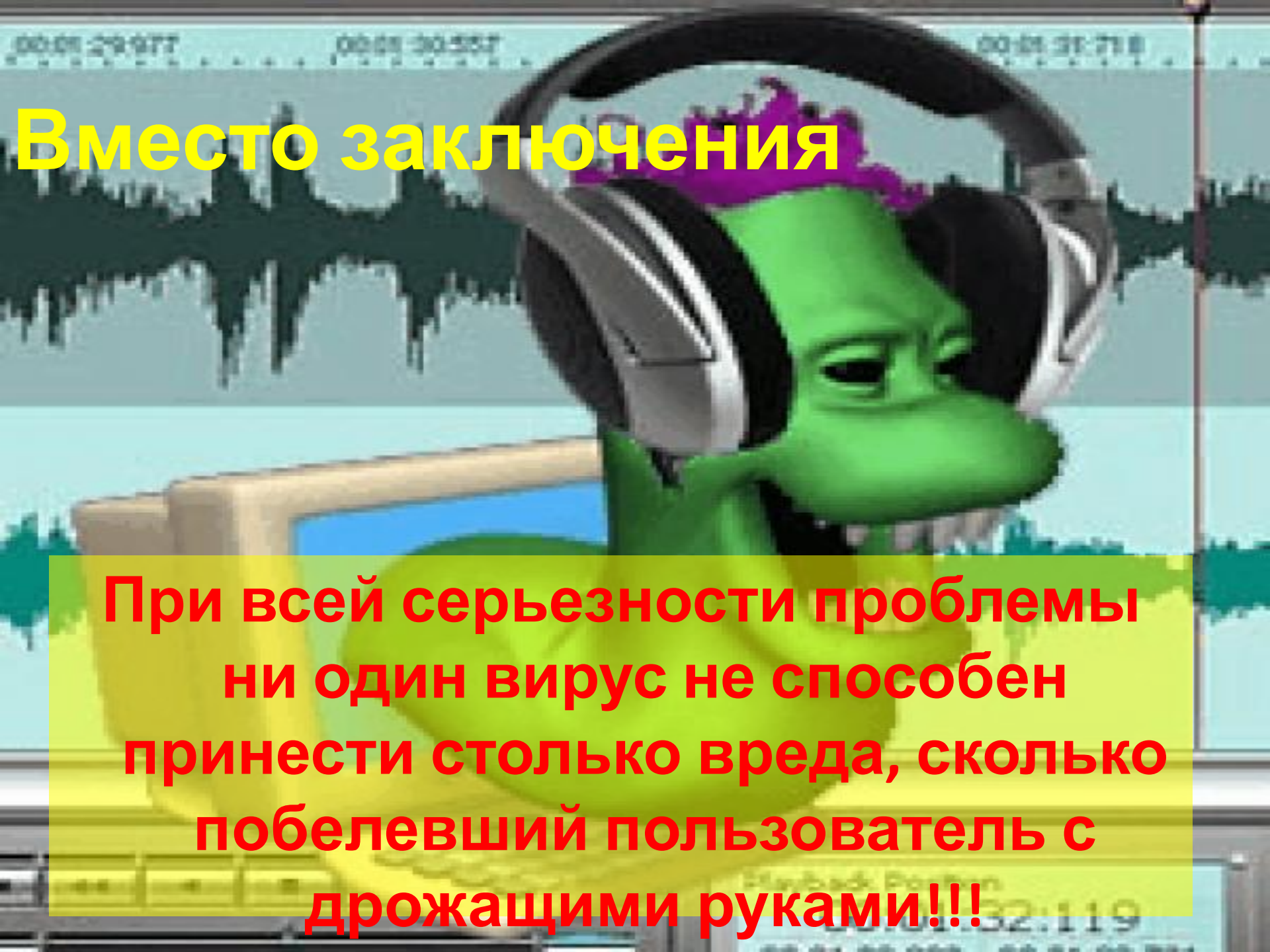
Вакцинирование программ

Для того, чтобы человек смог избежать некоторых заболеваний, ему делают прививку. Существует способ защиты программ от вирусов, при котором к защищаемой программе присоединяется специальный модуль контроля, следящий за ее целостностью. При этом может проверяться контрольная сумма программы или какие-либо другие характеристики. Когда вирус заражает вакцинированный файл, модуль контроля обнаруживает изменение контрольной суммы файла и сообщает об этом пользователю.

Аппаратная защита от вирусов

На сегодняшний день одним из самых надежных способов защиты компьютеров от нападений вирусов являются аппаратно-программные средства. Обычно они представляют собой специальный контроллер, вставляемый в один из разъемов расширения компьютера и программное обеспечение, управляющее работой этого контроллера

Вместо заключения



При всей серьезности проблемы ни один вирус не способен принести столько вреда, сколько побелевший пользователь с дрожащими руками!!!

Домашняя работа

§ 1.5 - 1.7, подготовиться к контрольной работе