



Компьютерные вирусы и антивирусные программы Исследовательская работа по информатике



Цель исследования: Выяснить пути проникновения и влияние вирусов на работу компьютера и найти методы защиты от них.

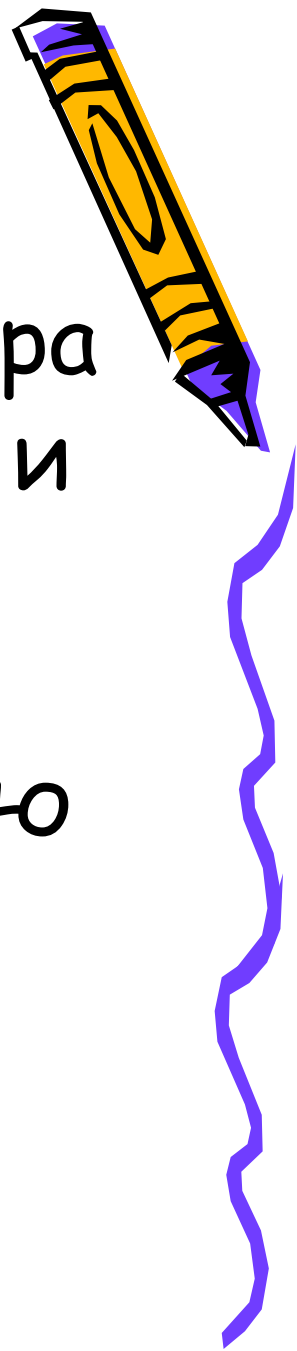
Исходя из темы, можно сформулировать следующие **задачи**:

1. Определить пути проникновения вирусов в компьютер;
2. Определить влияние компьютерных вирусов;
3. Ознакомиться с существующими методами защиты.
4. Провести исследование по теме антивирусные программы;
5. Разработать памятки «Правила безопасности при работе с электронной почтой» и «Компьютерные вирусы и антивирусные программы».

Объект исследования: Компьютерные вирусы и антивирусные программы.

Предмет исследования: Методы защиты от компьютерных вирусов.





Гипотеза: Проверка компьютера
антивирусными программами и
систематическое обновление
вирусных баз будет
препятствовать проникновению
и распространению
компьютерных вирусов.





Компьютерные вирусы



Компьютерные вирусы - это маленькие вредоносные программки, следующие в своей жизни только трём заповедям - Плодиться, Прятаться и Портить.



Массовое использование компьютеров в автономном режиме и в сети породило проблему заражения их компьютерными вирусами. Первая массовая эпидемия компьютерного вируса произошла в 1986 году. В настоящее время известно несколько миллионов вирусов, заражающих компьютеры.

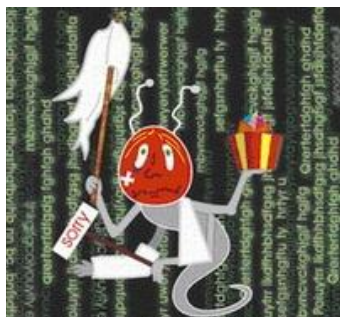


Классификация компьютерных вирусов

Файловые вирусы



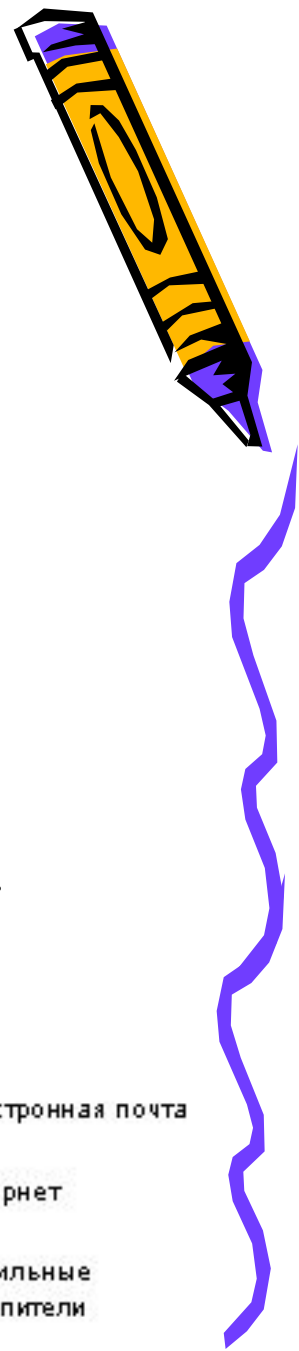
Сетевые вирусы



Макровирусы

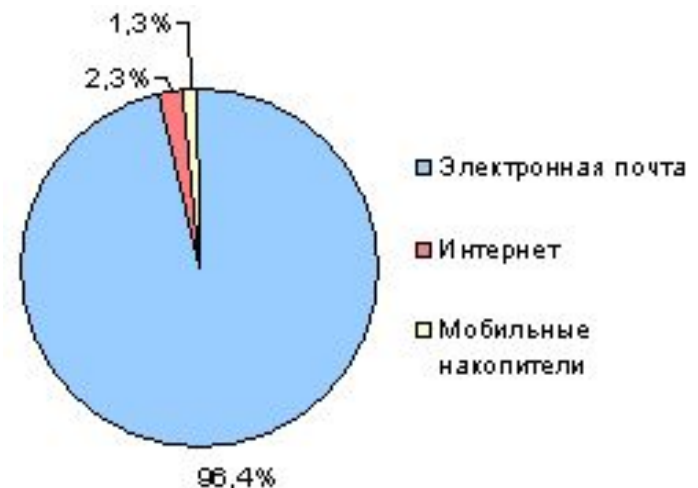


Основные пути распространения вирусов



Согласно статистике службы технической поддержки около 96,4% всех зарегистрированных случаев заражения были вызваны проникновением вирусов через электронную почту.

Следом за ней находятся Интернет - 2,3%, и мобильные накопители информации (дискеты, CD-ROM, флеш-карты)- 1,3%.



ПРИЗНАКИ ЗАРАЖЕНИЯ КОМПЬЮТЕРА



Вывод на экран непредусмотренных сообщений или изображений

Подача непредусмотренных звуковых сигналов

Неожиданное открытие и закрытие лотка CD/DVD дисковода

Произвольный запуск на компьютере каких-либо программ

Частые «зависания» и сбои в работе компьютера

Медленная работа компьютера при запуске программ

Исчезновение или изменение файлов и папок

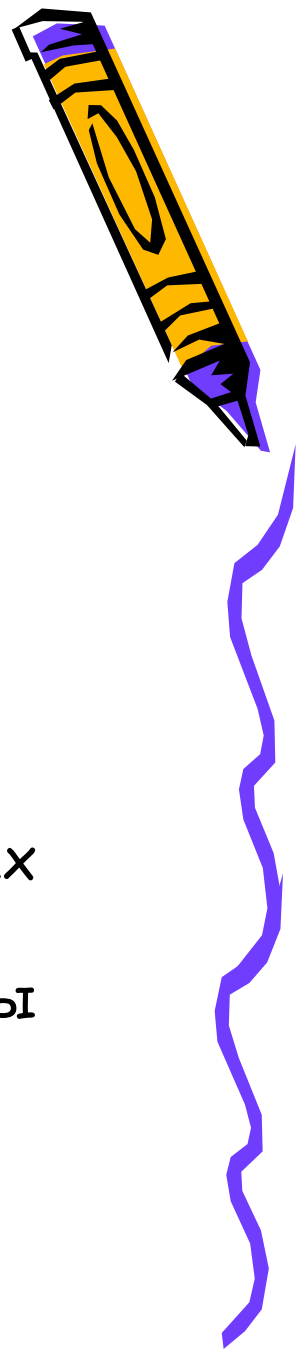
Частое обращение к жесткому диску

«Зависание» или неожиданное поведение браузера



Защита от КОМПЬЮТЕРНЫХ вирусов

- Регулярно тестируйте компьютер на наличие вирусов с помощью антивирусных программ
- Перед считыванием информации со съемных носителей проверяйте их на наличие вирусов
- Делайте архивные копии ценной для вас информации
- Не оставляйте дискету в дисковом диске
- Не используйте программы, поведение которых непонятно
- Регулярно обновляйте антивирусные программы



Антивирус — программа для обнаружения и лечения программ, заражённых компьютерным вирусом.



Принцип работы **антивирусных программы** основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вирусов.

Для поиска известных вирусов используются сигнатуры, т.е. некоторые постоянные последовательности двоичного кода, специфичные для конкретного вируса.

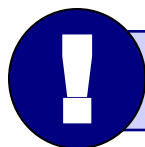
Для поиска **новых** вирусов используются алгоритмы **эвристического сканирования**, т.е. анализ последовательности команд в проверяемом объекте.

Большинство антивирусных программ сочетает в себе функции постоянной защиты (**антивирусный монитор**) и функции защиты по требованию пользователя (**антивирусный сканер**).

Антивирусные программы

Коммерческие

- ☐ AVP = Antiviral Toolkit Pro (www.avp.ru) – Е. Касперский
- ☐ DrWeb (www.drweb.com) – И. Данилов
- ☐ Norton Antivirus (www.symantec.com)
- ☐ McAfee (www.mcafee.ru)
- ☐ NOD32 (www.eset.com)



Есть бесплатные пробные версии!

Бесплатные

- ☐ Avast Home (www.avast.com)
- ☐ Antivir Personal (free-av.com)
- ☐ AVG Free (free.grisoft.com)



avast! antivirus

ДЕЙСТВИЯ ПРИ НАЛИЧИИ ПРИЗНАКОВ ЗАРАЖЕНИЯ КОМПЬЮТЕРА



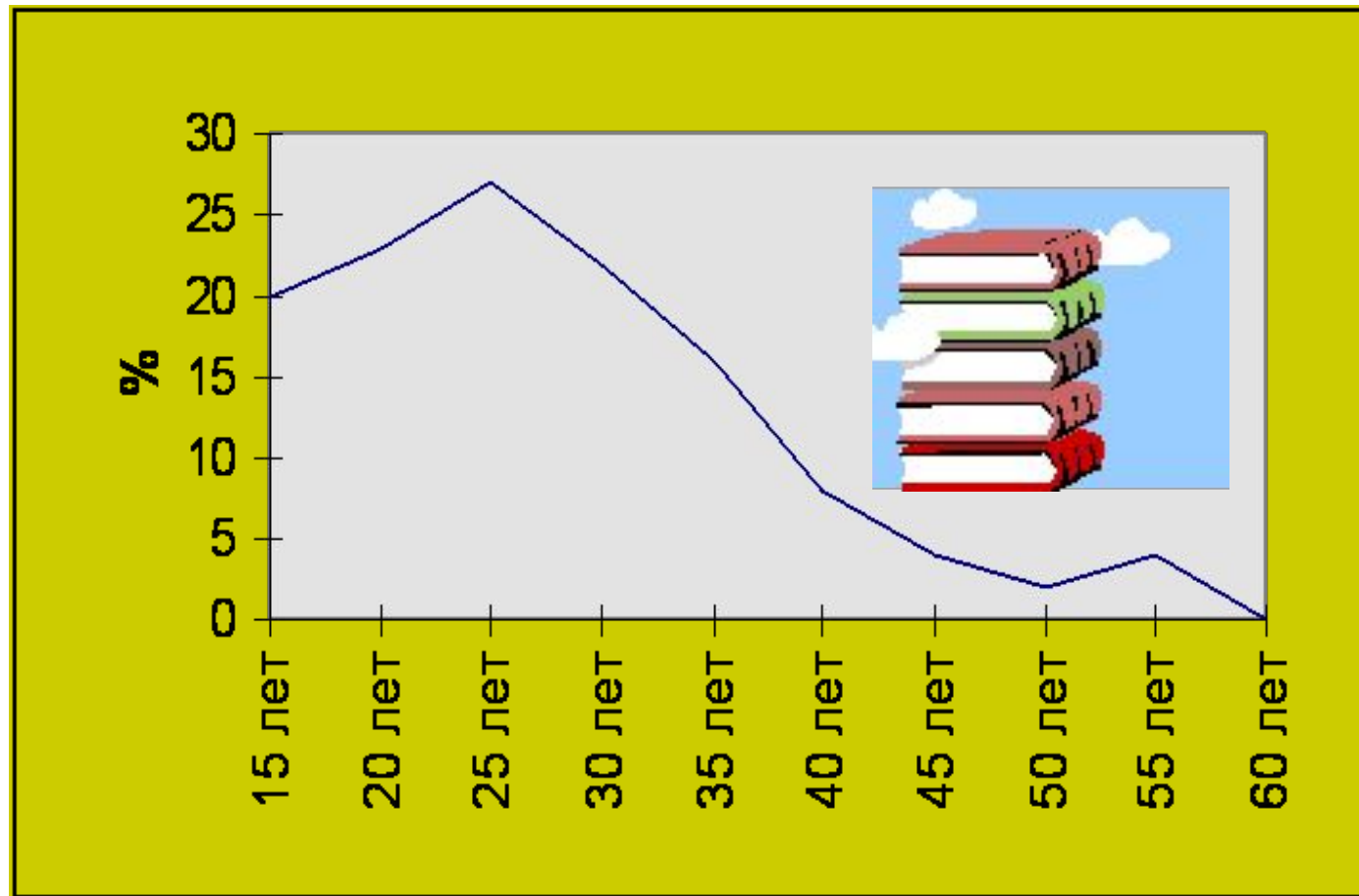
1. Сохраните результаты работы на внешнем носителе

2. Отключите компьютер от локальной сети и Интернета, если он к ним был подключен

3. Загрузите в режиме защиты от сбоев или с диска аварийной загрузки Windows (если компьютер выдает ошибку, когда вы его включаете)

4. Запустите антивирусную программу

КТО ПИШЕТ КОМПЬЮТЕРНЫЕ ВИРУСЫ?



Вывод: Большинству из авторов вирусов от 17 до 25 лет, и они учатся в Высших учебных заведениях, чаще всего эти молодые люди знакомы с компьютером с раннего детства. Данные, основанные на информации National Center for Computer Crime Data.

Исследования проведены специалистами по компьютерной безопасности из США доктором Дэвидом Стэнгом и Сильвией Мун.



Вы видите перед собой диаграмму, которая показывает появление вирусов по месяцам их авторства, независимо от года создания.

Вывод: больше всего вирусов появляется во время летних и зимних каникул у студентов Высших и средних учебных заведений.

КАКОВА ГЕОГРАФИЯ ВИРУСОВ? (2008 год)

Малайзия

Испания

Швеция

Герм

США

Стран

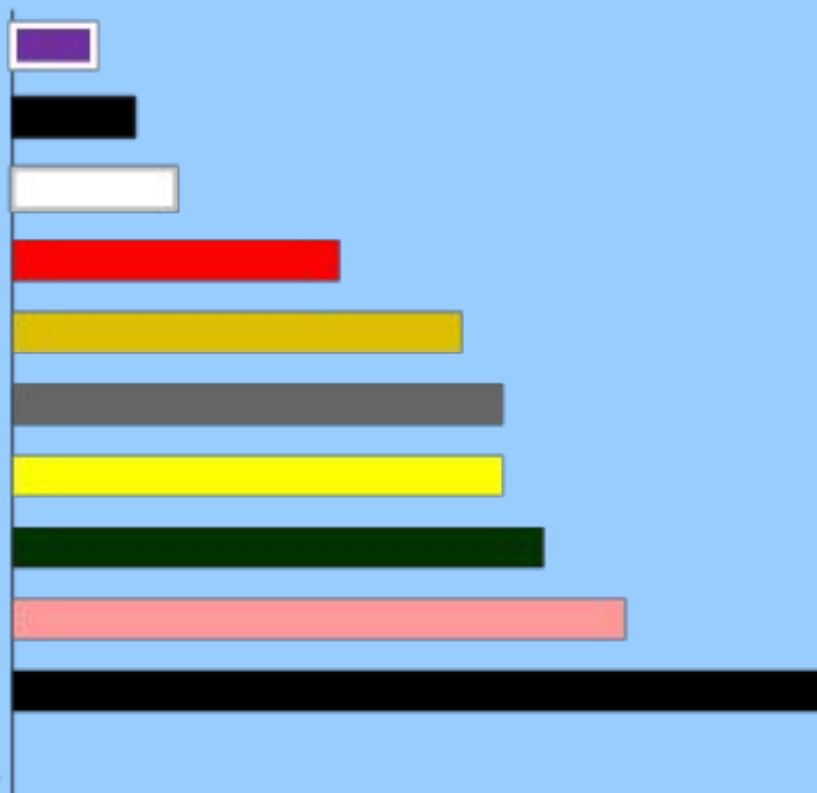
Росси

Турц

Бразилия

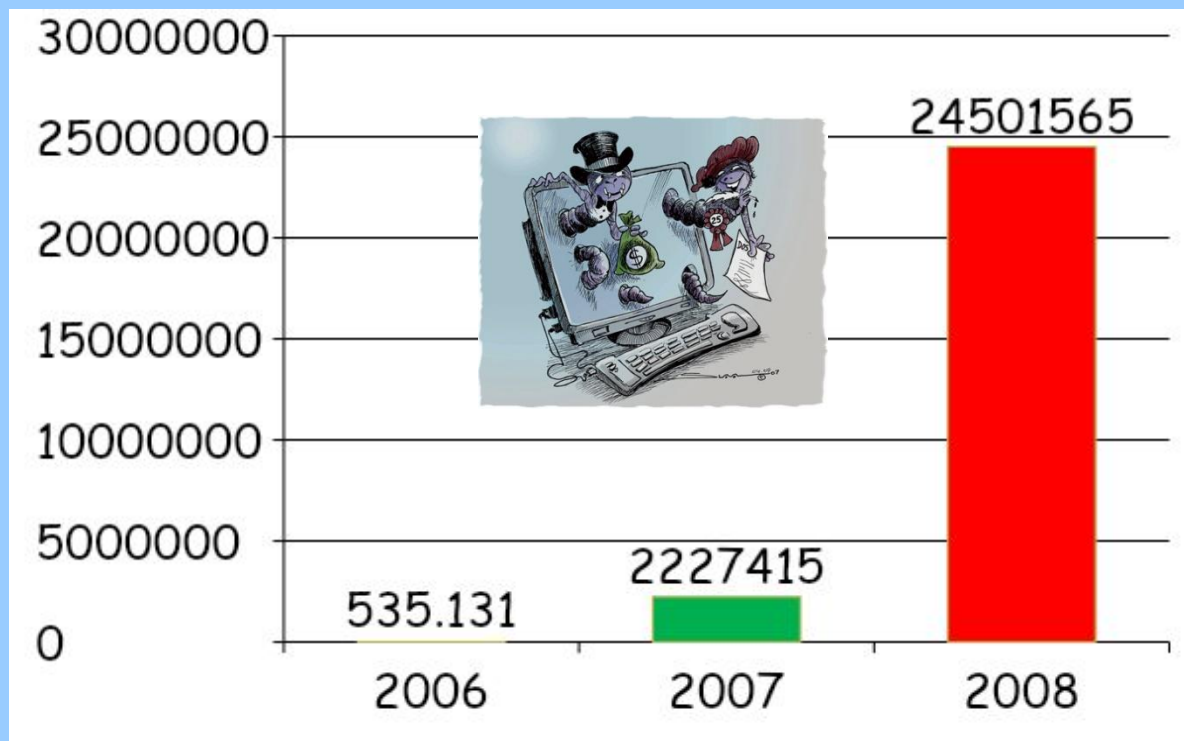
Китай

Страны производящий вирусы



Вывод: Согласно наблюдениям аналитика "Лаборатории Касперского" Александра Гостева, в настоящее время пальма первенства в этом соревновании принадлежит Китаю, за которым следует Бразилия. Весьма значительный процент современных вирусов создается в Турции. Страны бывшего СССР можно сравнить с Турцией по числу создаваемых вирусов. По его словам, в десятку лидеров по распространению компьютерных вирусов вошли США, Германия, Швеция, Испания и Малайзия.

КОЛИЧЕСТВО ВИРУСОВ



*Количество новых вредоносных программ, обнаруженных
аналитиками «Лаборатории Касперского»*

ВЫВОД: В прошедшем году количество вредоносных компьютерных программ превысило 20 миллионов. Растет не только количество, но и качество вирусов.

Отчет вирусной активности за 2008 год, подготовленный «Лабораторией Касперского».

ОСНОВНЫЕ ИСТОЧНИКИ РАСПРОСТРАНЕНИЯ ВИРУСОВ



ВЫВОД: Абсолютное лидерство среди главных источников вирусной угрозы остается электронная почта - 96,4% от всех зарегистрированных инцидентов (по зарубежным данным), около 85% согласно статистике службы технической поддержки "Лаборатории Касперского".

Следом за ней находятся Интернет (web-сайты, FTP-сайты, P2P-сети, IRC-каналы и пр.) - 2,3%, и мобильные накопители информации (дискеты, CD-ROM, флеш-карты)- 1,3%.



**За создание, использование и
распространение вредоносных программ
в России и большинстве стран
предусмотрена уголовная
ответственность!**

**ПОКАЗАТЕЛИ НАДЕЖНОСТИ
АНТИВИРУСОВ В УСЛОВИЯХ
ИНФОРМАЦИОННОЙ СРЕДЫ
ЛАБОРАТОРИИ FOMSOFT.**

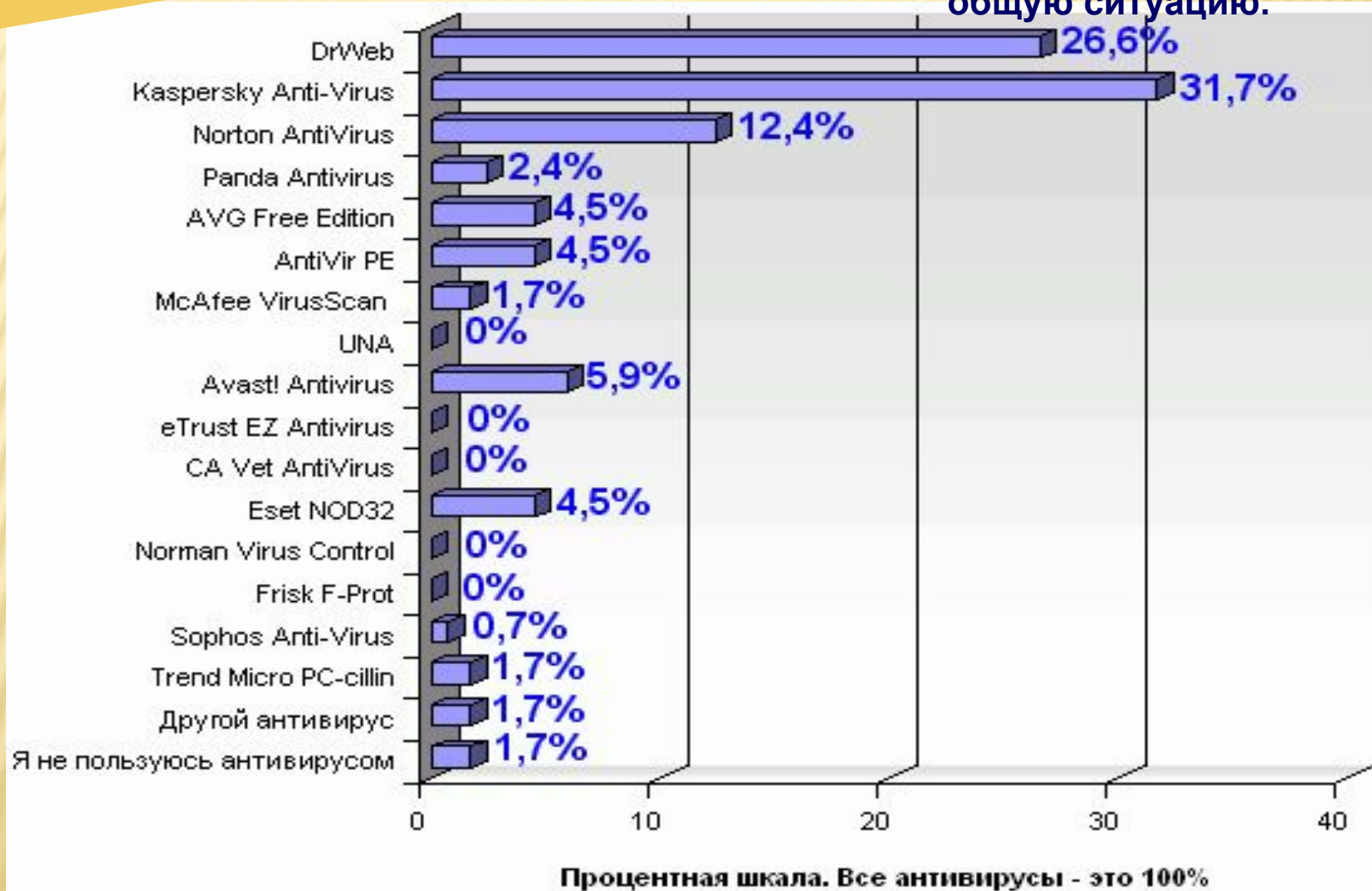
**Для ответа на вопрос - какой
антивирус лучше, достаточно
посмотреть последнюю колонку.
Чем ближе показатель надежности
антивируса к единице, тем он
лучше.**

Пропущено вирусов за период наблюдений с 01.2008 по 12.2008 г.

Наименование антивируса	<u>Январь</u> из 67	<u>Февраль</u> из 72	<u>Март</u> из 23	<u>Апрель</u> из 2	<u>Май</u> из 19	<u>Июль</u> из 23	<u>Август</u> из 55	<u>Сентябрь</u> из 60	<u>Октябрь</u> из 31	<u>Ноябрь</u> из 20	<u>Декабрь</u> из 15	всего из 387	Надежность защиты
AhnLab-V3	47	34	13	0	17	14	23	28	23	10	8	217	0.440
AntiVir	10	2	2	1	5	3	4	8	5	5	1	46	0.882
Authentium	50	46	12	1	6	15	23	7	16	5	5	186	0.520
Avast	26	23	5	0	4	2	7	8	10	2	2	89	0.770
AVG	22	11	8	0	5	5	7	9	12	6	5	90	0.768
BitDefender	17	16	5	0	6	10	8	13	11	2	1	89	0.770
CAT-QuickHeal	26	25	11	0	4	7	11	19	13	11	6	133	0.657
ClamAV	45	34	15	1	10	12	27	27	18	8	0	197	0.491
DrWeb	6	5	0	0	3	6	5	1	0	1	0	27	0.931
eSafe	31	33	13	1	8	16	20	41	11	9	6	189	0.512
F-Secure	14	7	1	0	0	2	6	4	7	3	0	44	0.887
Fortinet	21	24	8	0	7	9	15	20	12	8	4	128	0.670
Kaspersky	7	6	1	0	0	2	4	4	7	3	0	34	0.913
NOD32	25	21	6	0	4	14	22	30	8	3	2	135	0.652
Norman	15	20	6	1	7	11	19	29	15	9	5	137	0.646
Panda	16	21	7	0	7	9	21	40	16	9	5	151	0.610
Symantec	25	17	5	0	3	12	19	31	15	9	8	144	0.628

**ИССЛЕДОВАНИЕ ЛАБОРАТОРИИ
КАСПЕРСКОГО. ТЕМА ОПРОСА: "КАКОЙ
АНТИВИРУС ВЫ ИСПОЛЬЗУЕТЕ?"**

Была опрошена группа респондентов (3000 чел.), но можно практически со 100% уверенностью сказать, что данный график имеет небольшие погрешности и отражает в целом общую ситуацию.



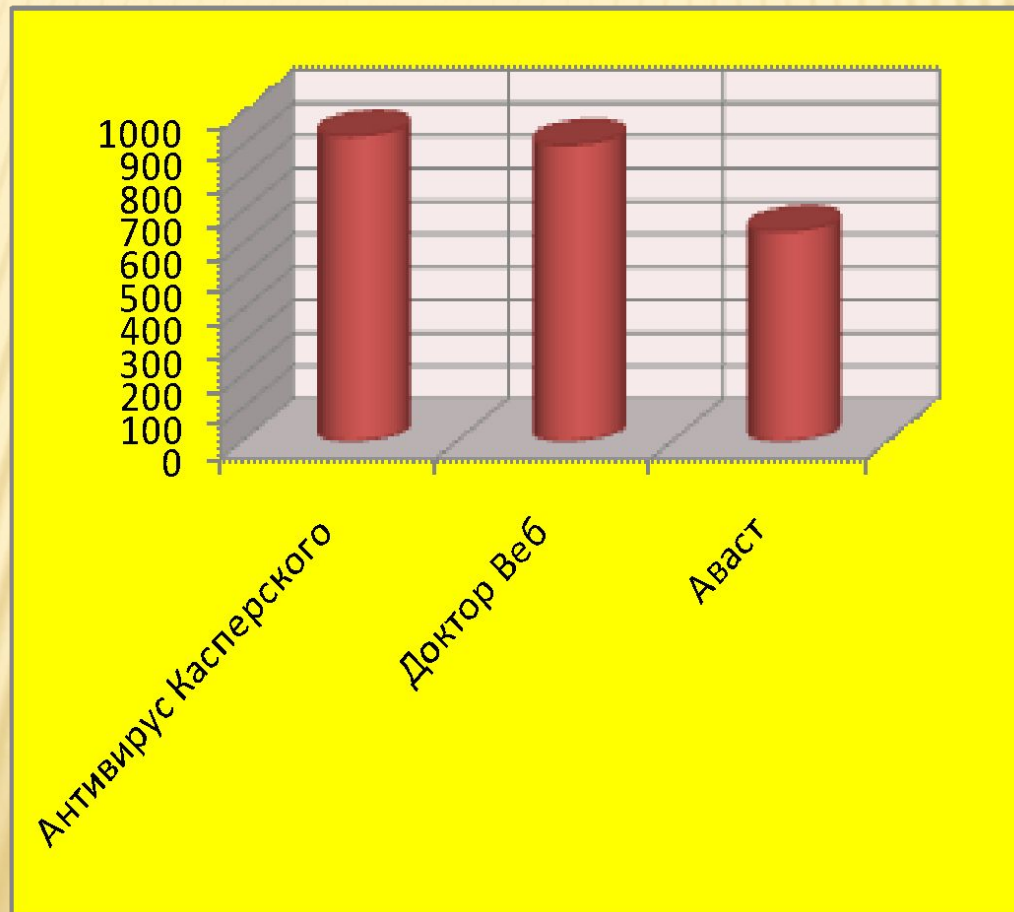
**ТЕСТ ПОЛЬЗОВАТЕЛЕЙ ПОИСКОВОЙ
СИСТЕМЫ ЯНДЕКС
КАКОЙ АНТИВИРУС ЛУЧШЕ?**



Kaspersky	253 (33.82%)
NOD 32	223 (29.81%)
Dr.Web	78 (10.43%)
Norton	20 (2.67%)
McAfee	6 (0.80%)
Panda	15 (2.01%)
Avast	128 (17.11%)
AVG	7 (0.94%)
AVZ	6 (0.80%)
от Agnitum'a	7 (0.94%)
Barricade	1 (0.13%)

**РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ
ПРОВЕДЕННЫХ В 2007-2008 ГОДУ
СТУДЕНТАМИ НОВОСИБИРСКИХ ВУЗОВ:**

- I место - Антивирус Касперского, 930 баллов**
- II место - Доктор Веб, 903 балла**
- III место - Аваст, 640 баллов**



ВЫВОД

Лидерами по
результатам

исследования стали:



- ❑ **AVP = Antiviral Toolkit Pro**
(www.avp.ru) – Е. Касперский



- ❑ **DrWeb** (www.drweb.com) – И.
Данилов



- ❑ **Avast Home**
(www.avast.com)



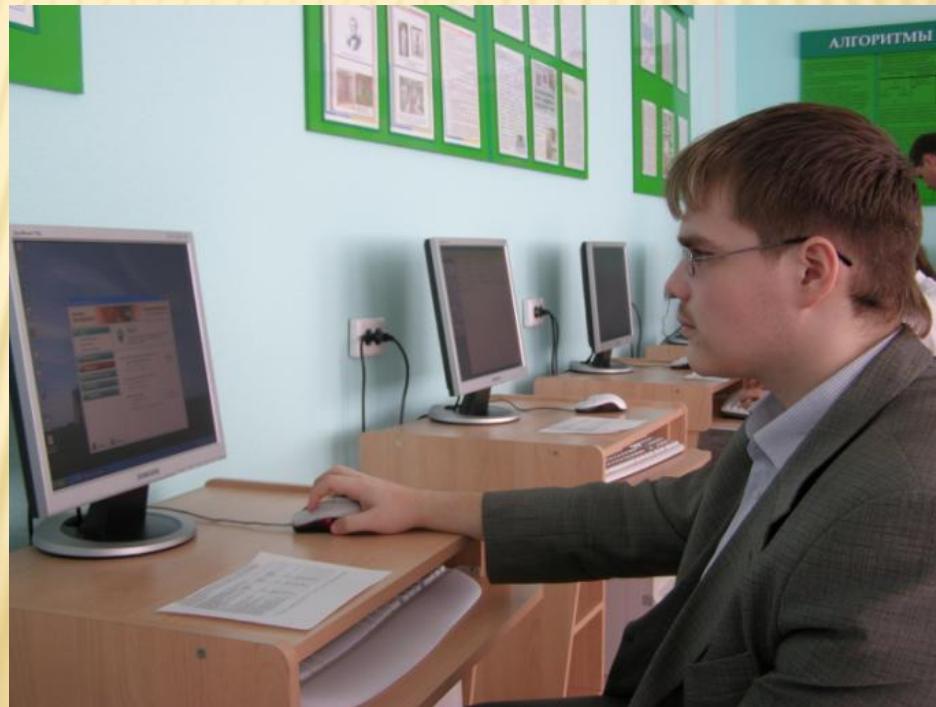
- ❑ **NOD32**
(www.eset.com)



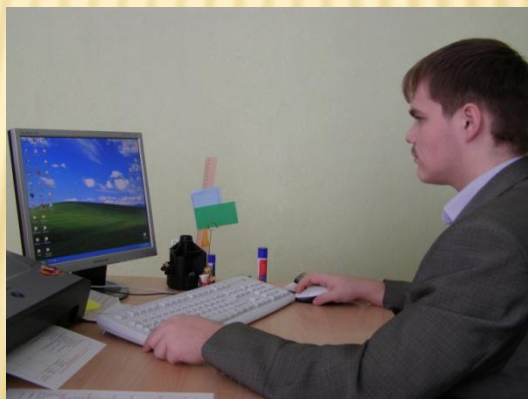
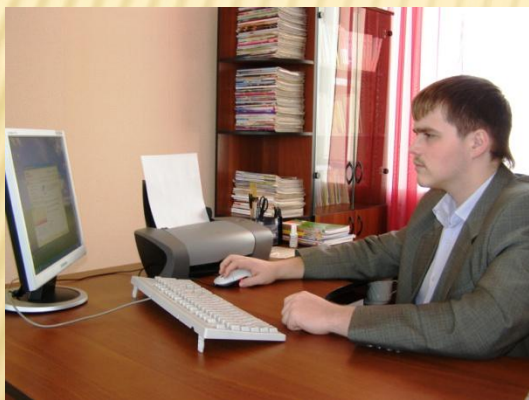
- ❑ **Norton Antivirus**
(www.symantec.com)



- Я провел тестирование антивирусной программой Доктор Веб компьютеров на наличие вирусов в следующих кабинетах нашей школы.
- В Кабинете информатики на компьютере учителя установлена программа: Антивирус Касперского. Обновляются вирусные базы. Вирусов не обнаружено.
 - В Кабинете Завучей на компьютере заместителя директора по учебно-воспитательной работе установлена программа: Антивирус Касперского. Обновляются вирусные базы. Вирусов не обнаружено.
 - В Кабинете информатики на компьютере ученик 4 установлена программа: Антивирус Аваст. **Обнаружено 2 вируса.**
Причина: Не обновлялись вирусные базы.

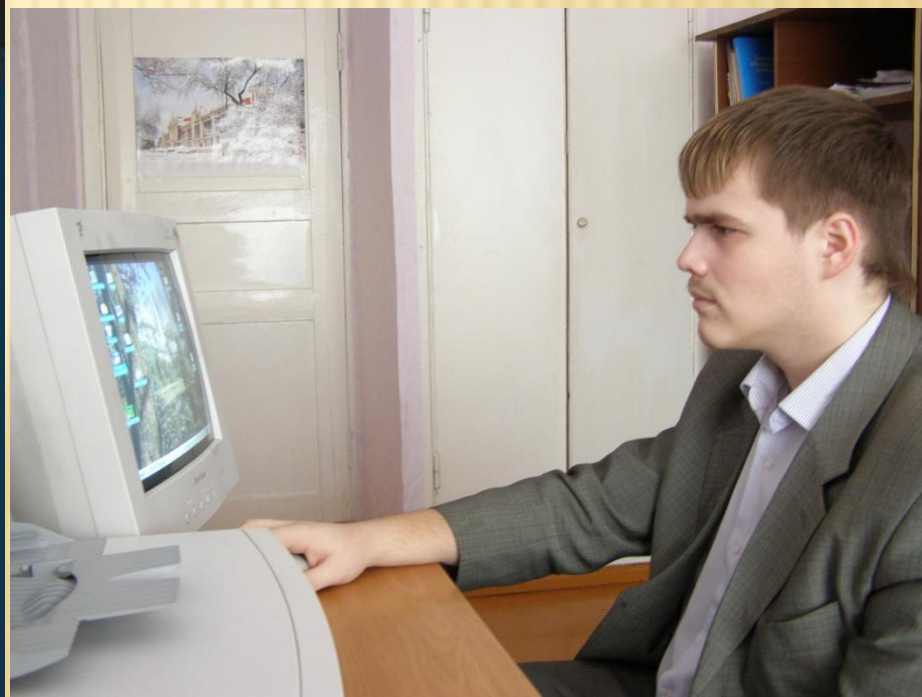


- В кабинете психолога на компьютере установлена программа: Антивирус Аваст. **Обнаружен 1 вирус.**
Причина: Не обновлялись вирусные базы
- В кабинете Социального педагога на компьютере установлена программа: Антивирус Касперского. Обнаружен 1 вирус:
Причина: Не обновлялись вирусные базы.
- В кабинете детской организации «Радуга» на компьютере установлена программа: Антивирус Аваст. Обнаружено 2 вируса:
Причина: Не обновлялись вирусные базы.
- В кабинете информатики компьютер ученик 11 на одну неделю был оставлен без антивирусной защиты. При тестировании в нем было обнаружено 12 вирусов.
Причина: Не установлена антивирусная программа.



Вывод

Анализируя результаты исследования на базе школы-интерната № 18, можно сделать вывод, что гипотеза подтвердилась. Проверка антивирусными программами и систематическое обновление вирусных баз препятствует проникновению и распространению компьютерных вирусов.



Заключение

Подводя итог своей работы, хочу напомнить, что компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации и сбоев операционной системы. Чтобы избежать этого, нужно обязательно использовать антивирус. Я рекомендую вам использовать антивирусную программу, которая входит в пятерку лучших:

AVP = Antiviral Toolkit Pro (www.avp.ru) – Е. Касперский

DrWeb (www.drweb.com) – И. Данилов

Avast Home (www.avast.com)

NOD32 (www.eset.com)

Norton Antivirus (www.symantec.com)

Хочу напомнить, что среди этих программ только одна является бесплатной это **Avast Home**. Стоимость остальных составляет примерно около 1,5 тысяч рублей на один год.

Не забывайте периодически обновлять антивирусную программу. Антивирусные сканеры способны защищать только от тех компьютерных вирусов, данные о которых содержатся в антивирусной базе.