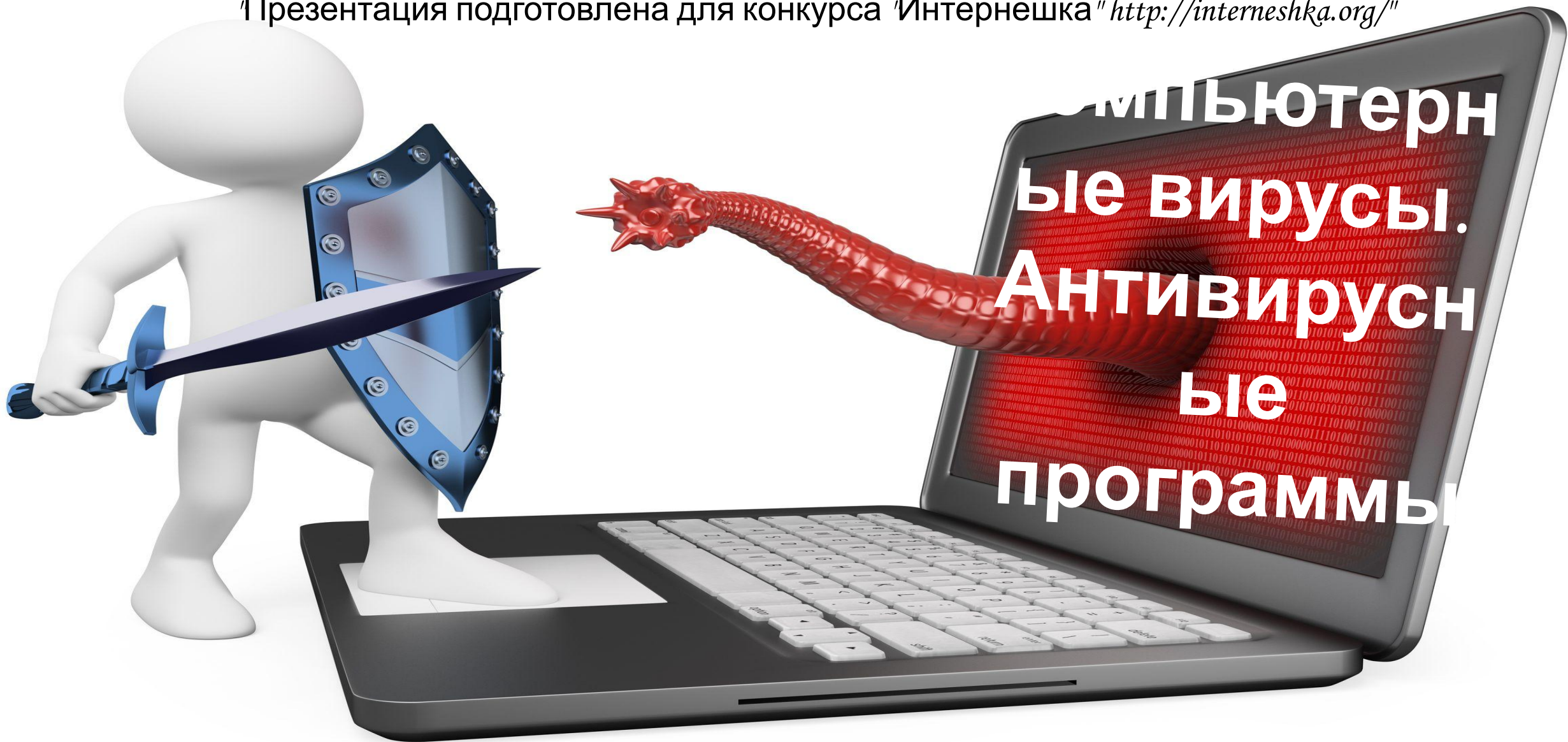


Презентация подготовлена для конкурса "Интернешка" <http://interneshka.org/>



Выполнил ученик 7А класса МБОУ «Школа № 161» г. Казани

Хохлов Алексей

Руководитель: Яблонская Анна Николаевна,

Что такое компьютерный вирус?

- **Компьютерный вирус** — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

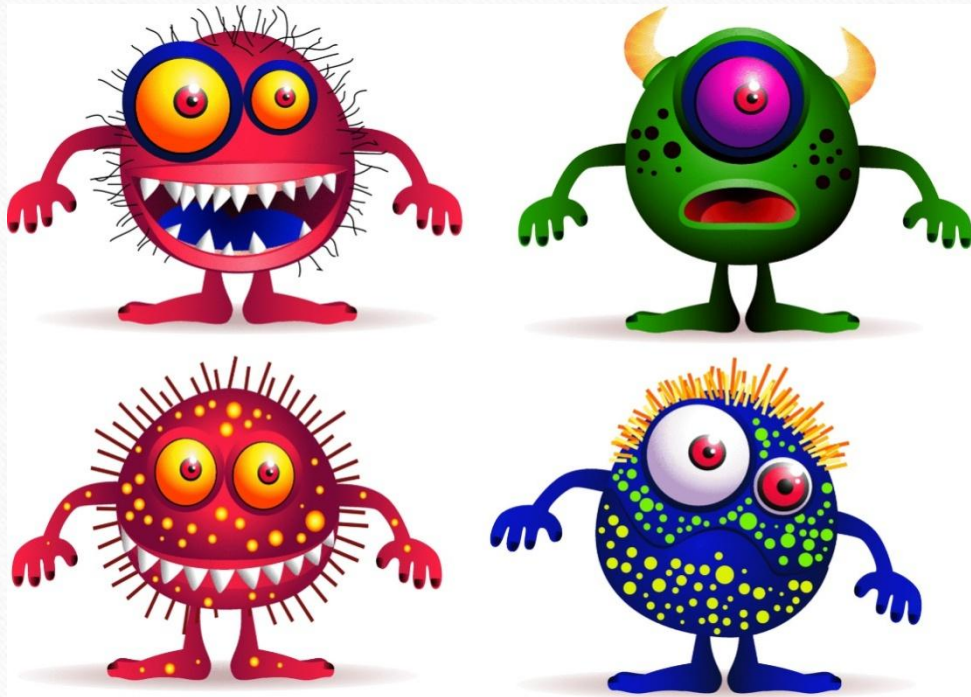


Цель вируса

- Как правило, целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера и т.п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с



Первые вирусы



- Первыми известными вирусами являются *Virus 1,2,3* и *Elk Cloner* для ПК *Apple II*, появившиеся в 1981 году. Зимой 1984 года появились первые антивирусные утилиты — *СНКАВОМВ* и *ВОМBSQAD* авторства Энди Хопкинса (англ. *Andy Hopkins*). В начале 1985 года Ги Вонг (англ. *Gee Wong*) написал программу *DPROTECT* — первый резидентный антивирус.

Классификация вирусов по масштабу вредных действий

| Тип вируса | Действия |
|---------------|---|
| Безвредные | Уменьшают свободную память на диске за счет своего «размножения» |
| Неопасные | Уменьшают свободную память на диске. Вызывают появление графических, звуковых и др. внешних эффектов. |
| Опасные | Могут привести к сбоям и зависаниям при работе компьютера. |
| Очень опасные | Потеря программ и данных (изменение, удаление файлов и каталогов), форматирование винчестера и т.п. |

Классификация вирусов по среде обитания

| Среда обитания | Действия вируса |
|----------------|---|
| Файловые | Внедряются в исполняемые файлы (программы) и активизируются при их запуске. Находятся в ОП до выключения компьютера |
| Загрузочные | Записывают себя в загрузочный сектор диска (в программу-загрузчик ОС). При загрузке ОС с зараженного диска внедряется в ОП и ведет себя как файловый вирус. |
| Макровирусы | Являются макрокомандами, которые заражают файлы документов <i>Word, Excel</i> . Находятся в ОП до закрытия приложения |
| Драйверные | Заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки. |
| Сетевые | Заражают компьютер после открытия вложенного файла (вируса) в почтовое сообщение. Похищают пароли |

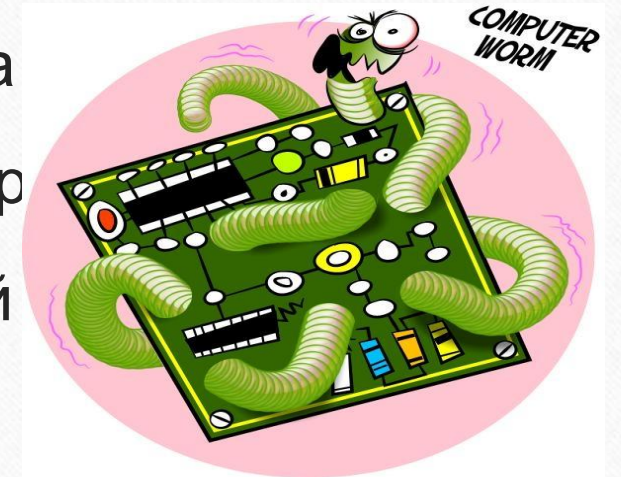
Пути проникновения вирусов

- Глобальная сеть *Internet*.
- Электронная почта
- Локальная сеть
- Компьютеры «Общего назначения»
- Пиратское программное обеспечение
- Съёмные накопители



Признаки проявления вирусов

- Неправильная работа программ
- Медленная работа компьютера
- Невозможность загрузки операционной системы
- Исчезновение файлов и каталогов
- Изменение размеров файлов
- Неожиданное увеличение количества файлов на
- Вывод на экран неожиданных сообщений и изобра
- Уменьшение размеров свободной операционной
- Подача непредусмотренных звуковых сигналов
- Частые «зависания» и сбои в работе компьютера



Профилактика вирусов

- Иметь специальный загрузочный диск
- Систематически проверять компьютер на наличие вирусов
- Иметь последние версии антивирусных средств
- Проверять все поступающие данные на наличие вирусов
- Не использовать нелегальные программные средства
- Выбирать запрет на загрузку макросов при открытии документов *Word* и *Excel*
- Выбрать высокий уровень безопасности в «Свойствах обозревателя»
- Делать архивные копии файлов
- Добавить в файл автозагрузки антивирусную программу сторож
- Не открывать вложения электронного письма, если отправитель



Вирус *NetTraveler*

- В июне 2013 года «Лаборатория Касперского» объявила о раскрытии новой кибершпионской сети, получившей название *NetTraveler* и затронувшей более 350 компьютерных систем в 40 странах мира. Атаке подверглись государственные и частные структуры, в том числе правительственные учреждения, посольства, научно-исследовательские центры, военные организации, компании нефтегазового сектора, а также политические активисты. Россия оказалась в числе наиболее пострадавших стран, заняв вторую строчку в рейтинге государств, испытавших на себе наиболее заметные последствия операции *NetTraveler*. Согласно результатам расследования, проведенного экспертами «Лаборатории Касперского», кампания шпионажа стартовала еще в 2004 году, однако пик ее пришелся на период с 2010 по 2013 гг. В последнее время в сферу интересов атакующих входили такие отрасли, как



Червь Морисса

- В 1988 году Робертом Моррисом-младшим был создан первый массовый сетевой червь. 60 000-байтная программа разрабатывалась с расчётом на поражение операционных систем *UNIX Berkeley 4.3*. Вирус изначально разрабатывался как безвредный и имел целью лишь скрытно проникнуть в вычислительные системы, связанные сетью *ARPANET*, и остаться там необнаруженным. Вирусная программа включала компоненты, позволяющие раскрывать пароли, имеющиеся в инфицированной системе, что, в свою очередь, позволяло программе маскироваться под задачу легальных пользователей системы, на самом деле занимаясь размножением и рассылкой копий. Вирус не остался скрытым и полностью безопасным, как задумывал автор, в силу незначительных ошибок, допущенных при разработке, которые привели к стремительному



Вирус *Flame*.

- *Flame* — компьютерный червь, поражающий компьютеры под управлением операционной системы *Microsoft Windows* версий *XP*, *7*, *Vista*.
- Его обнаружил Роэль Шувенберг, старший научный сотрудник по компьютерной безопасности Лаборатории Касперского во время исследования вируса *Wiper*, атаковавшего компьютеры в Иране, о чём было объявлено 28 мая 2012 года. Наиболее пострадавшими странами являются Иран, Израиль, Судан, Сирия, Ливан, Саудовская Аравия и Египет.
- Вирус способен собирать файлы данных, удалённо менять параметры компьютера, записывать звук, скриншоты и подключаться к чатам, действует, по меньшей мере, с марта 2010 года. Код *Flame* имеет объём 20 МБ и значительно превосходит в этом отношении вирус *Stuxnet*. *Flame* использует библиотеки *zlib*, *libbz2*, *ppmd* для сжатия, встроенную СУБД *sqlite3*, виртуальную машину *lua*



Антивирусные программы

- Какие существуют антивирусные программы:

- *Dr.Web*
- Антивирус Касперского
- *NOD32*
- *Norton 360*
- *AVG*
- *Avast!*





Полифаги



- Самыми популярными и эффективными антивирусными программами являются антивирусные программы полифаги (например, *Kaspersky Anti-Virus*, *Dr.Web*).

Для поиска известных вирусов используются так называемые *маски*.

Маской вируса является некоторая постоянная последовательность программного кода, специфичная для этого конкретного вируса.

Если антивирусная программа обнаруживает такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению.



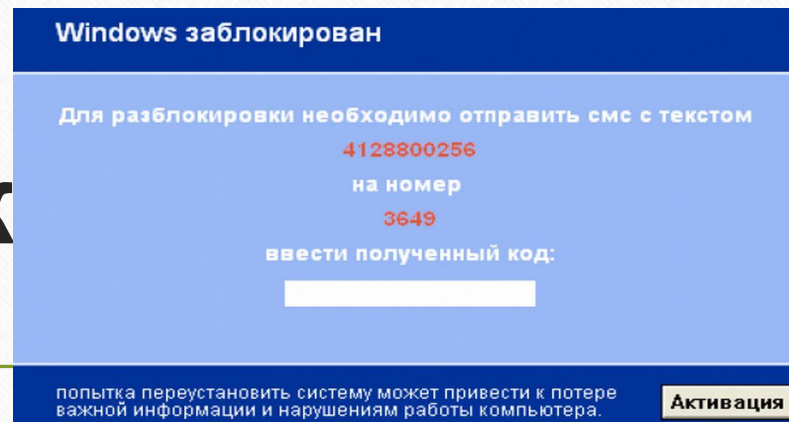
Ревизорь



- Принцип работы ревизоров (например, *ADinf*) основан на подсчете контрольных сумм для присутствующих на диске файлов. Эти контрольные суммы затем сохраняются в базе данных антивируса, как и некоторая другая информация: длины файлов, даты их последней модификации и пр.
- При последующем запуске ревизоры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то ревизоры сигнализируют о том, что файл был изменен или заражен вирусом.



ЛОКИРОВЩИК



- Антивирусные блокировщики - это программы, перехватывающие 'вирусоопасные' ситуации и сообщающие об этом пользователю. К таким ситуациям относится, например, запись в загрузочный сектор диска. Эта запись происходит при установке на компьютер новой операционной системы или при заражении загрузочным вирусом.
- Наибольшее распространение получили антивирусные блокировщики в *BIOS* компьютера.

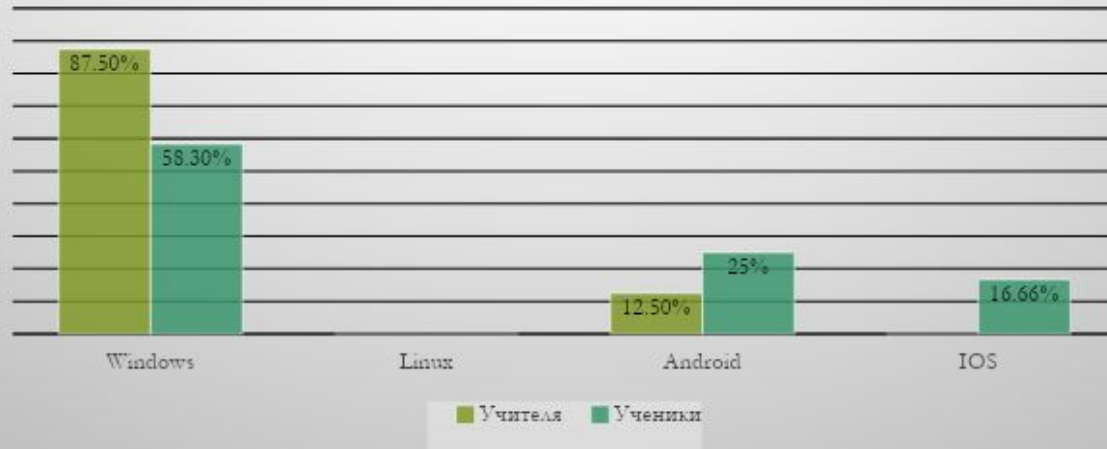


Исследования

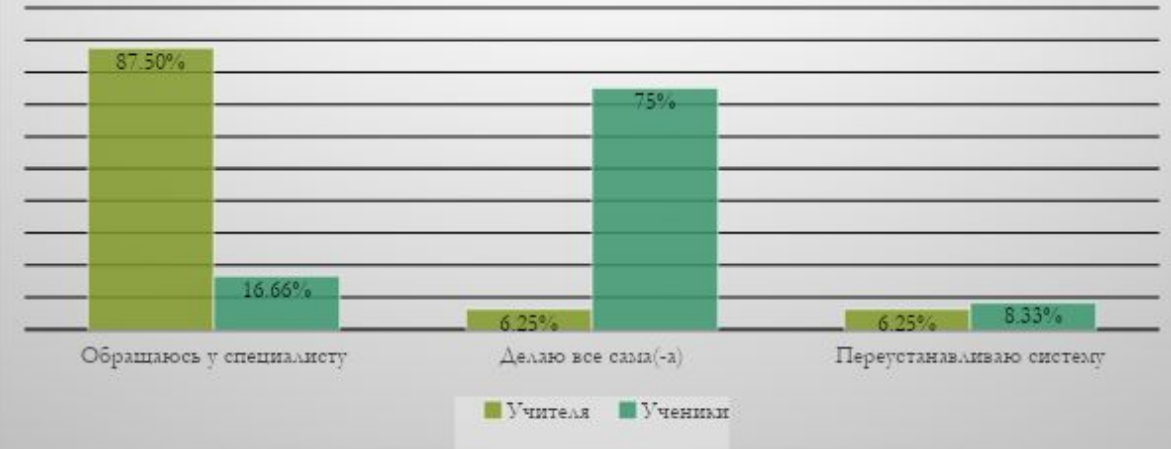
Анкетирование учителей и учеников.

Мне стало интересно, как учителя и ученики избавляются от вирусов и используют ли они антивирусные программы.

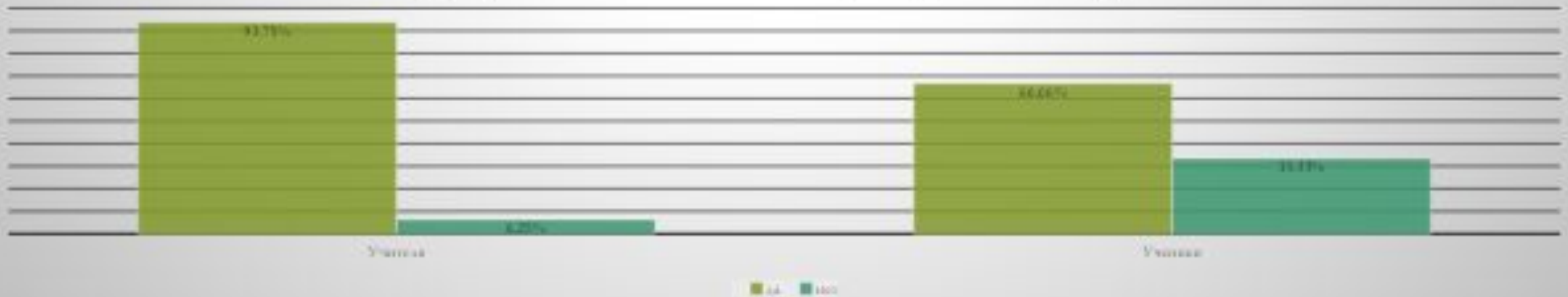
Ответы на вопрос:
"Какая у Вас операционная система?"



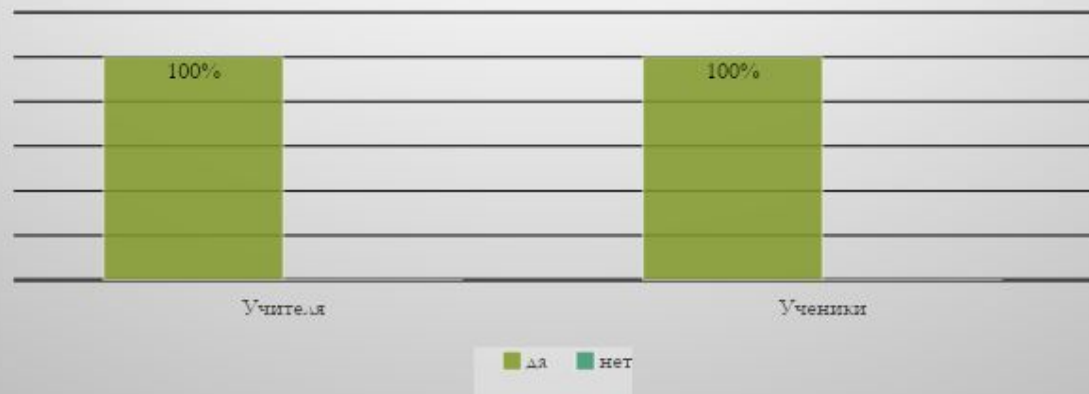
Ответы на вопрос:
"Как Вы боритесь с вирусом?"



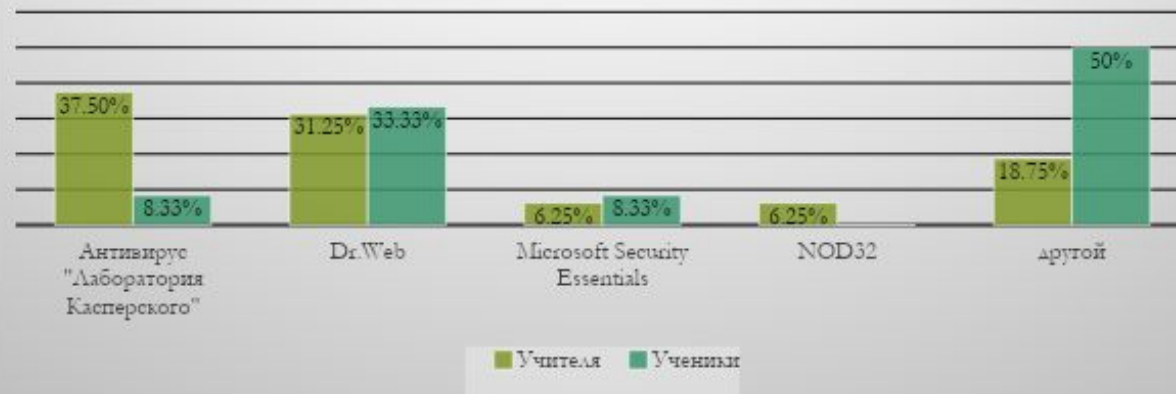
Ответы на вопрос:
"Подвергался ли Ваш компьютер воздействию вируса?"



Ответы на вопрос:
"Используете ли Вы антивирусную программу?"



Ответы на вопрос:
"Какую антивирусную программу вы используете?"

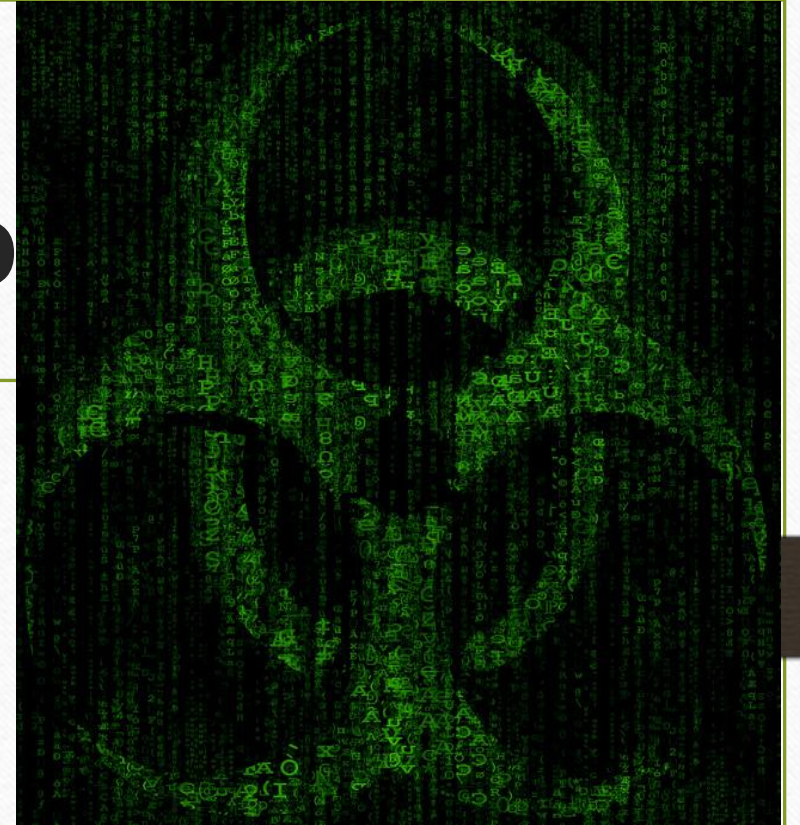


Ответы на вопрос:
"Какие последствия были после воздействия вируса?"



Правила защиты от вир

- Регулярно обновляйте антивирусные программы.
- Не используйте программы, поведение которых непонятно.
- Не оставляйте диски в дисковом диске.
- Делайте архивные копии ценной для Вас информации.
- Всегда защищайте свои диски от записи при работе на других компьютерах.
- Перед считыванием информации с диском проверяйте их на наличие вирусов.
- Регулярно тестируйте компьютер на наличие вирусов с помощью антивирусных программ.





ВЫВОДЪ



- Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность...
- Слишком уж бояться вирусов не стоит, особенно если компьютер приобретен совсем недавно, и много информации на жестком диске еще не накопилось. Вирус компьютер не взорвет. Ныне известен только один вирус (*Win95.CIH*), который способен испортить "железо" компьютера.

- Компьютерные вирусы распространяются по многим принципам. Для обнаружения замаскированных вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.
- Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на



- Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелонированная" оборона. Средствам разведки в "обороне" от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов. На переднем крае обороны находятся программы-фильтры. Эти программы могут первыми сообщить о работе вируса и предотвратить заражение программ и дисков. Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры. Самый глубокий эшелон обороны - это средства разграничения доступа. Они не позволяют



**Спасибо
за внимание**

