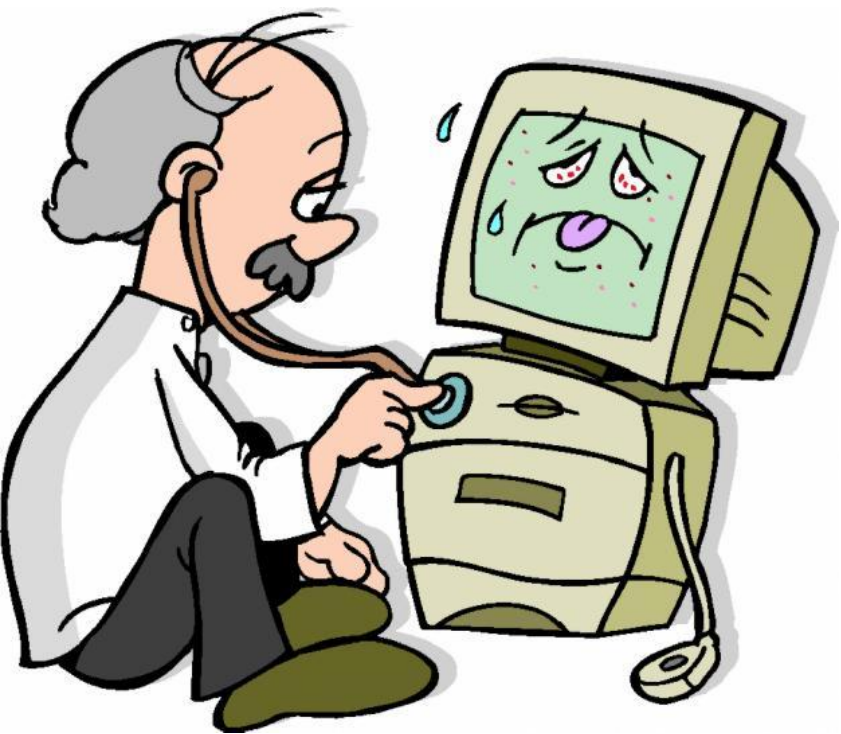


«История компьютерных вирусов и систем противодействия им»



Решетняк Роман

ученик 8 класса

Руководитель:

Ульданова Р.Р.

Компьютерный вирус –
специально созданная небольшая
программа, способная к
саморазмножению, засорению
компьютера и выполнению других
нежелательных действий.



*Энциклопедия вирусов
«Лаборатории Касперского
<http://www.viruslist.com/ru/viruses/encyclopedia>*

ИСТОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ



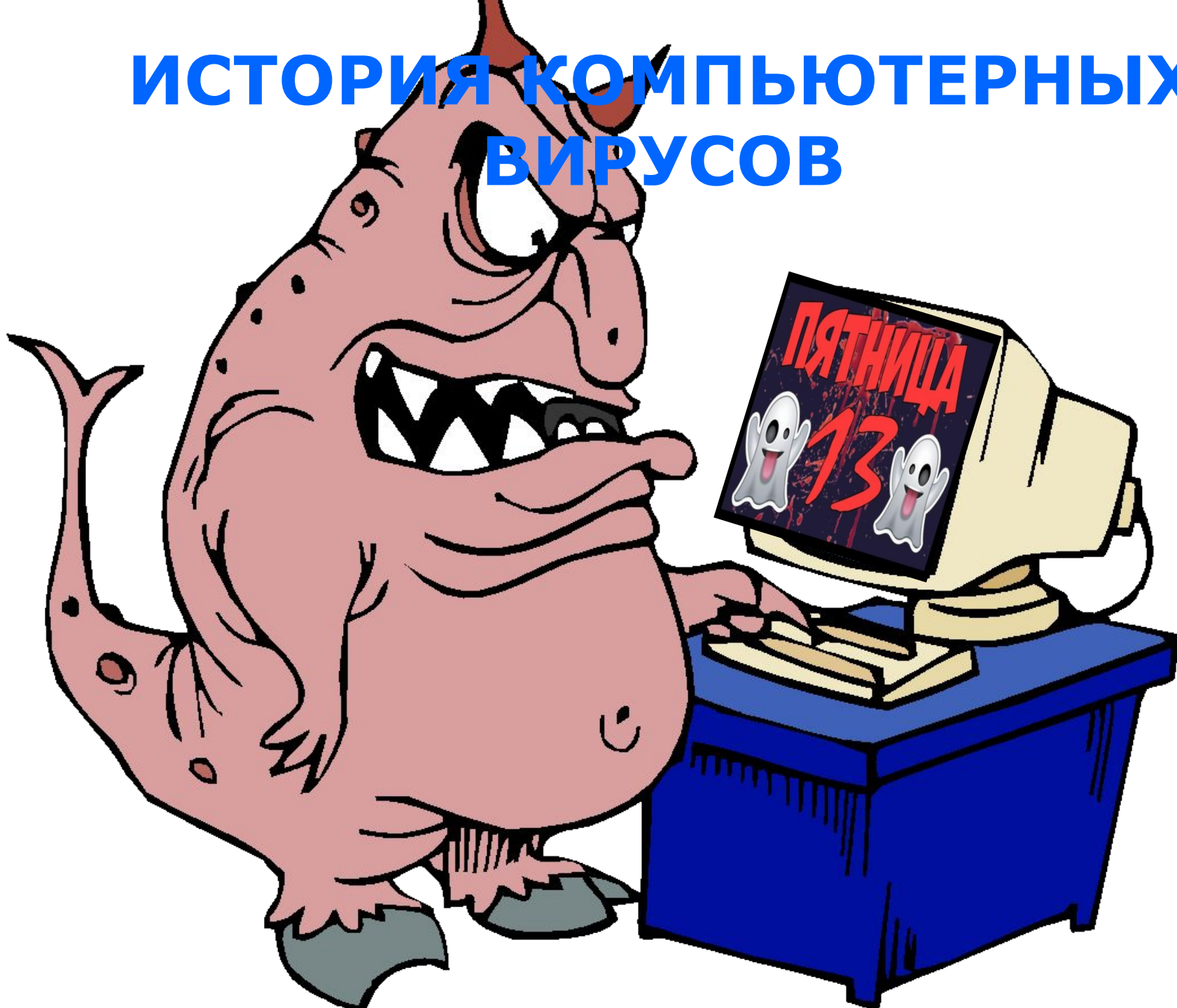
Джон фон Нейман
(1903 - 1957)



ИСТОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ



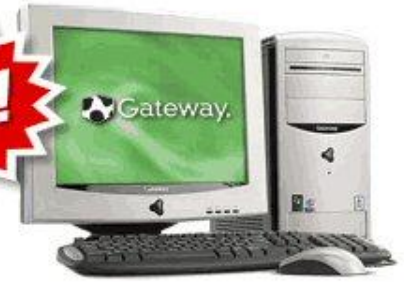
ИСТОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ



CONGRATULATIONS!

You've been chosen to receive a **FREE* Gateway Desktop Computer!**

- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (18-inch viewable)



[Click Here to Claim Your FREE* Desktop Computer!](#)

by ExclusiveRewards

*with participation in our program

WELCOME TO CASINO DEL RIO - Mic

File Edit View Favorites Tools Help

Back Forward Stop Home

Address <http://www.casinodelrio.com/>

SideFind X

sideFind powered by IST

casino Find

www.888.com X

CASINO ON NET Click

SideFind X

sideFind powered by IST

casino Find

www.888.com X

CASINO ON NET Click

Casino On Net - Up to 200\$
Welcome Bonus
Since 1996, over 8,000,000 people have experienced Casino On...

www.casinoonnet.com

50 Best Online Casinos-
Ranked by Quality
Top 50 online casinos ranked by quality and payout rate...

www.30TopCasinos.com

Done

Microsoft Internet Explorer

Click OK to download our free software while browsing the site

OK Cancel



Download Getting Started Features Contact Us Help In

> Current Events

Finale
\$5,000




Blackjack
Roulette
Slot Machine

Click Here!

Вирьмейкер –
человек, который
пишет» вирусы





**Законодательство
Российской Федерации о
вредоносных программах**

Глава 28

***«Преступления в сфере
компьютерной информации»***

**Уголовного кодекса
Российской Федерации**

Статья 273

Статья 273 гласит:

«Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ, или машинных носителей с такими программами, – наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда, в размере заработной платы, или иного дохода осужденного за период от двух до пяти месяцев.

То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок от трех до семи лет».

Классификация вирусов



• по среде обитания

• по способу заражения
среды обитания

• по степени
воздействия

• по свойствам
алгоритма

СРЕДА ОБИТАНИЯ

```
graph TD; A[СРЕДА ОБИТАНИЯ] --> B[файловые]; A --> C[загрузочные]; A --> D[макро]; A --> E[сетевые]
```

файловые

загрузочные

макро

сетевые

ДЕСТРУКТИВНЫЕ ВОЗМОЖНОСТИ

```
graph TD; A[ДЕСТРУКТИВНЫЕ ВОЗМОЖНОСТИ] --> B[безвредные]; A --> C[опасные]; A --> D[неопасные]; A --> E[очень опасные]
```

безвредные

опасные

неопасные

очень опасные

МАКРОВИРУСЫ

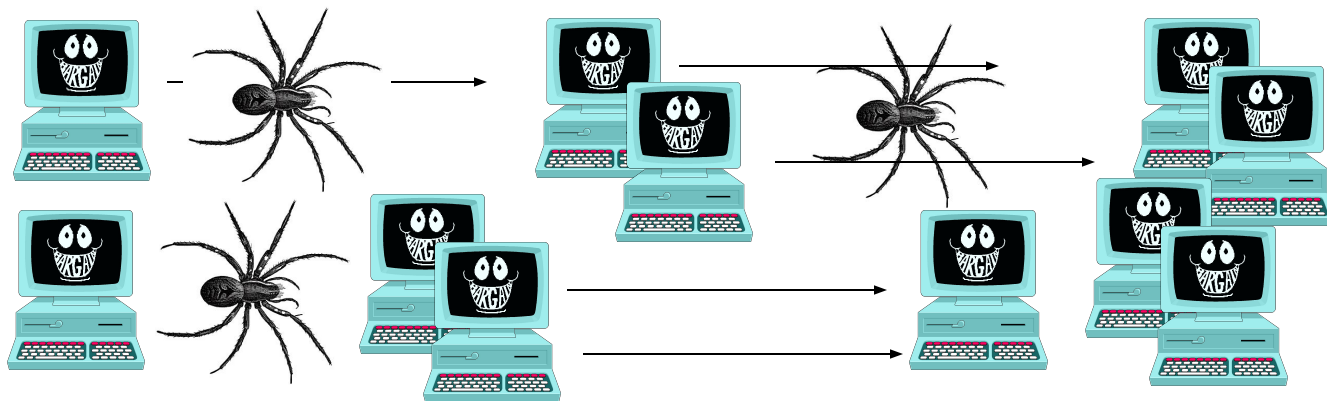
Заражают файлы документов, например текстовых. После загрузки заражённого документа в текстовый редактор макровирус постоянно присутствует в оперативной памяти компьютера и может заражать другие документы. Угроза заражения прекращается только после закрытия текстового редактора.



Троянские программы. «Троянский конь»

употребляется в значении: тайный, коварный замысел. Эти программы осуществляют различные несанкционированные пользователем действия:

- сбор информации и ее передача злоумышленникам;
- разрушение информации или злонамеренная модификация;
- нарушение работоспособности компьютера;
- использование ресурсов компьютера в неблагоприятных целях.



Сетевые черви – программы, распространяющие свои копии по локальным или глобальным сетям с целью:

- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие



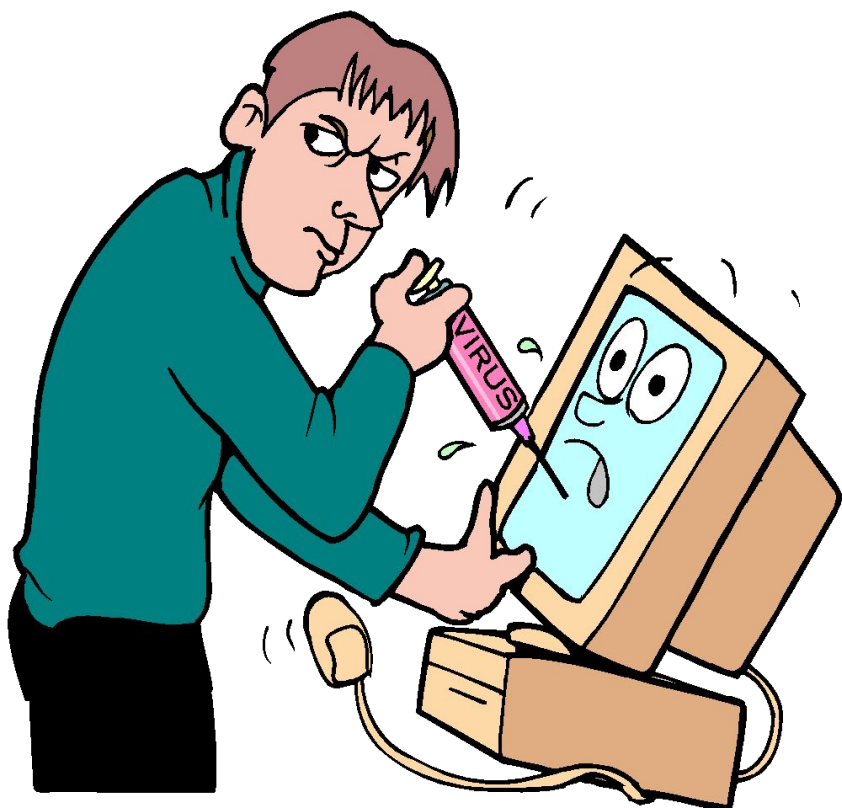
A photograph of a computer monitor and keyboard. The monitor is the central focus, displaying a solid blue screen. It is heavily secured with thick, dark metal chains that crisscross over its surface. A large metal padlock is attached to the chains, locking them together. The keyboard is visible at the bottom of the frame, also partially covered by the chains. The background is a dark, textured blue. The overall image conveys a sense of robust security and protection.

Методы защиты

- Защита локальных сетей
- Использование дистрибутивного ПО
- Резервное копирование информации
- Использование антивирусных программ
- Не запускать непроверенные файлы



Антивирусные программы



Антивирусная программа (антивирус) - программа, позволяющая выявлять вирусы, лечить зараженные файлы и диски, обнаруживать и предотвращать подозрительные действия.

ПАМЯТКА

безопасности для пользователя домашнего компьютера

- Ограничить физический доступ к компьютеру, установить пароль на вход в систему и отключать доступ в Интернет, когда он не нужен;
- подписаться на информационные бюллетени Microsoft и регулярно обновлять операционную систему;
- отключить все неиспользуемые службы и закрыть порты, через которые могут осуществляться атаки;
- тщательно настроить все программы, работающие с Интернет, начиная с браузера — например, запретить использование Java и ActiveX;
- установить и обновлять антивирусную программу;

ПАМЯТКА

безопасности для пользователя домашнего компьютера

- использовать брандмауэр, хотя бы встроенный в систему, и внимательно анализировать его сообщения и логи;
- крайне аккуратно работать с почтой, а также программами для обмена сообщениями и работы с файлообменными сетями, например, следует отключить использование HTML в принимаемых письмах;
- никогда не запускать программы сомнительного происхождения, даже полученные из заслуживающих доверия источников, например, из присланного другом письма;
- ни при каких условиях не передавать по телефону или по почте свои персональные данные, особенно пароли;
- регулярно создавать резервные копии критических данных.

*Владимир Каталов,
исполнительный директор компании «Элкомсофт»*

СПАСИБО ЗА ВНИМАНИЕ