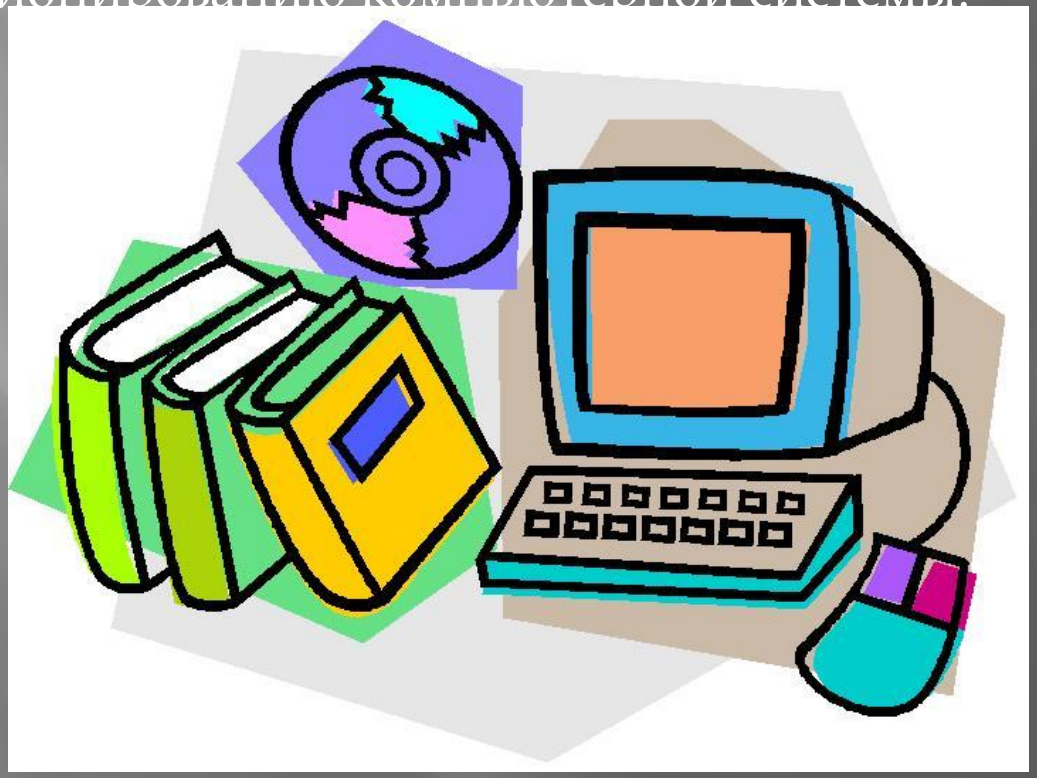
ВРЕДОНОСНЫЕ И АНТИВИРУСНЫЕ ПРОГРАММЫ

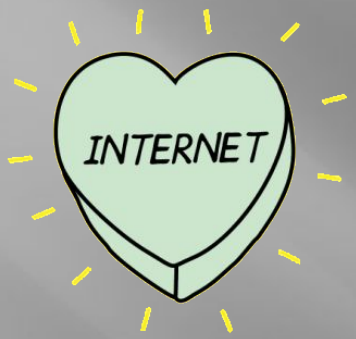
Выполнила: Шигина Яна

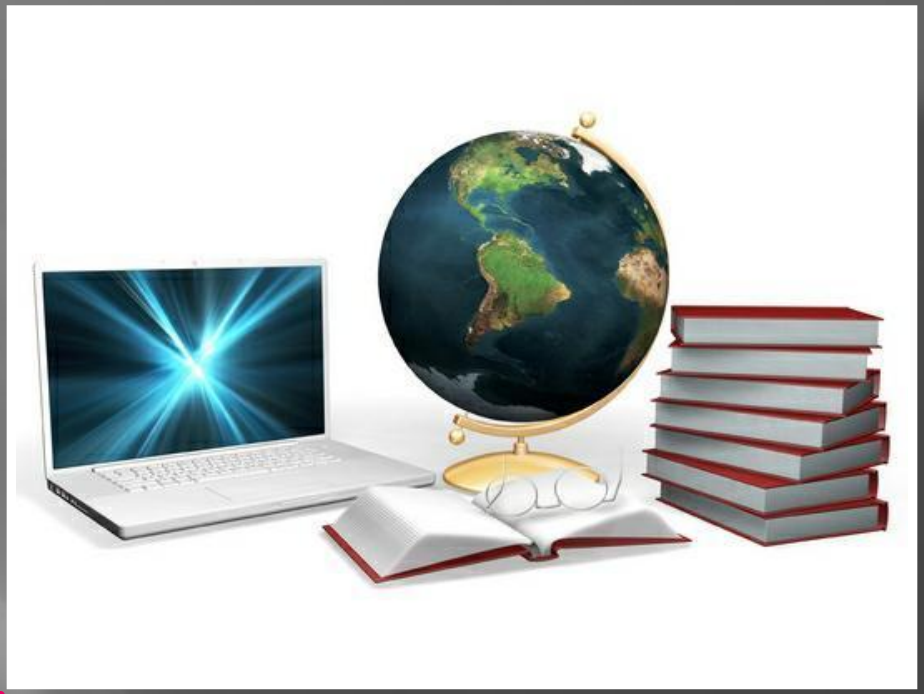
Содержание

Вредоносные программы

Вредоносная программа - компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ресурсов системы, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы.







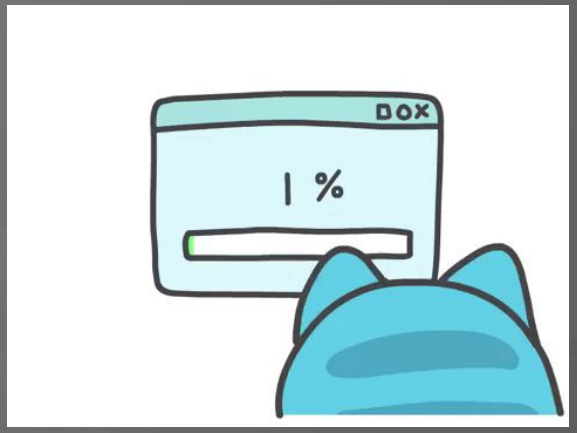
К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

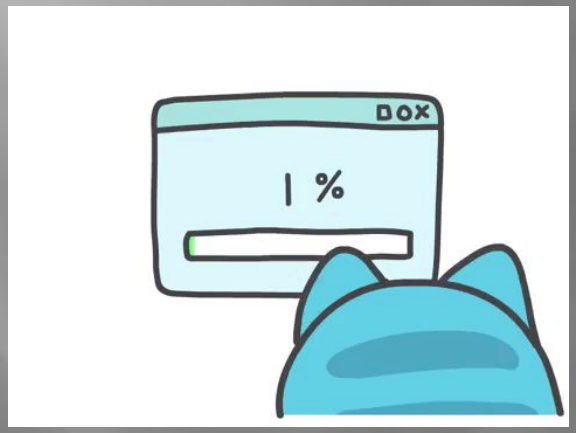
назад

Компьютерный *вирус*

Компьютерный вирус - разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (саморепликация). В дополнение к этому вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом.

После заражения компьютера вирус может начать выполнение вредоносных действий и распространение своих копий, а также заставлять компьютер выполнять какие-либо действия.





Активация компьютерного вируса может вызывать уничтожение программ и данных и может быть связана с различными событиями (наступлением определенной даты или дня недели, запуском программ, открытием документа и т.д.).

назад

Первые вредоносные и антивирусные программы

Первый вирус, появившийся в июле 1982 г., был написан 15-летним школьником Ричем Скрента (Rich Skrenta) для платформы Apple II и относился к категории загрузочных. Он распространялся, заражая код загрузочных секторов дискет для операционной системы Apple II. При загрузке компьютера вирус оставался в памяти и заражал все дискеты, которые вставлялись в дисковод. Жертвами вируса стали компьютеры друзей и знакомых автора, а также его учитель математики.

Первый антивирус всего лишь на два года младше своего врага. В 1984 г. программист Анди Хопкинс (Andy Hopkins) написал утилиты, позволяющие перехватывать некоторые операции, выполняемые через BIOS, а также анализировать загрузочный модуль, что давало возможность бороться с некоторыми типами вирусов того времени.

Как многие старые вирусы, Elk Cloner отличался визуальными проявлениями: при каждой 50-й загрузке он показывал короткое стихотворение («Elk Cloner - это уникальная программа. Она проникнет на все ваши диски, профильтрует ваши чипы. О да, это Cloner. Она приклеится к Вам, как клей. Программа способна изменить и RAM. Пустите к себе Cloner»).

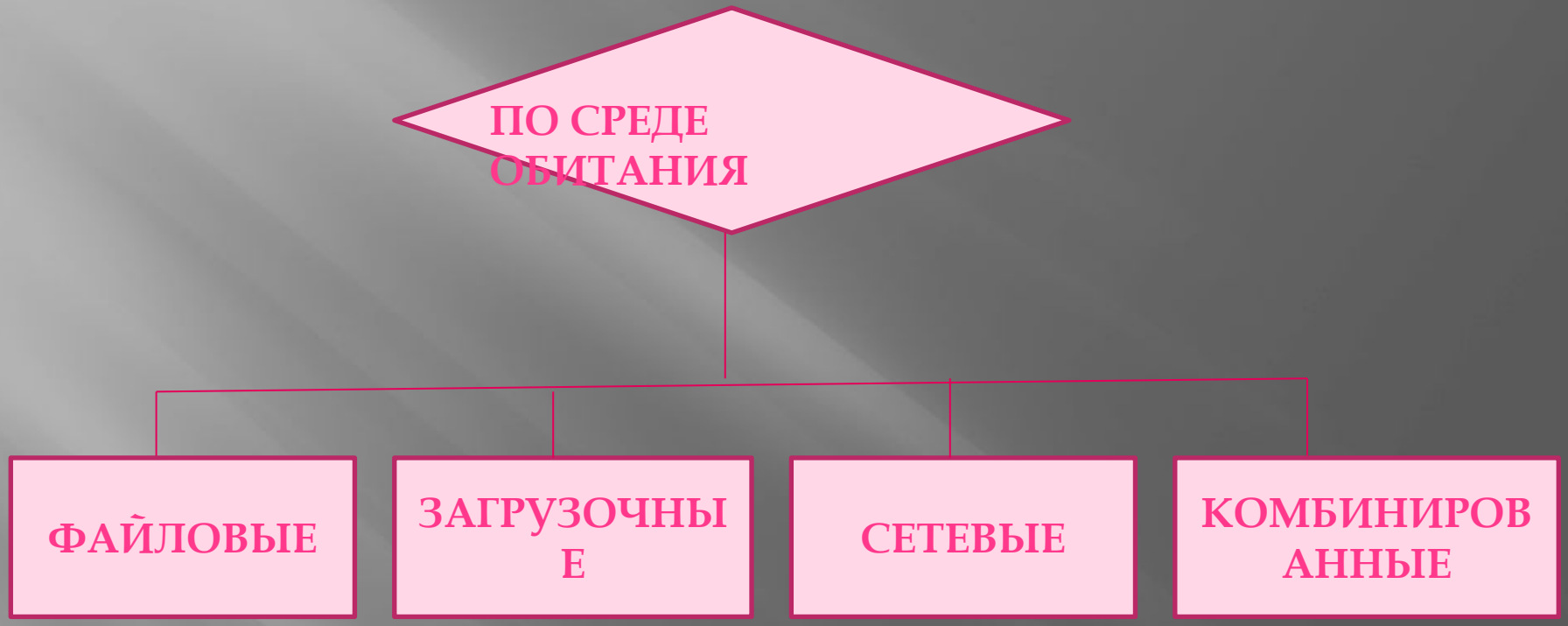
назад

Вирусы можно разделить на классы по следующим основным признакам:

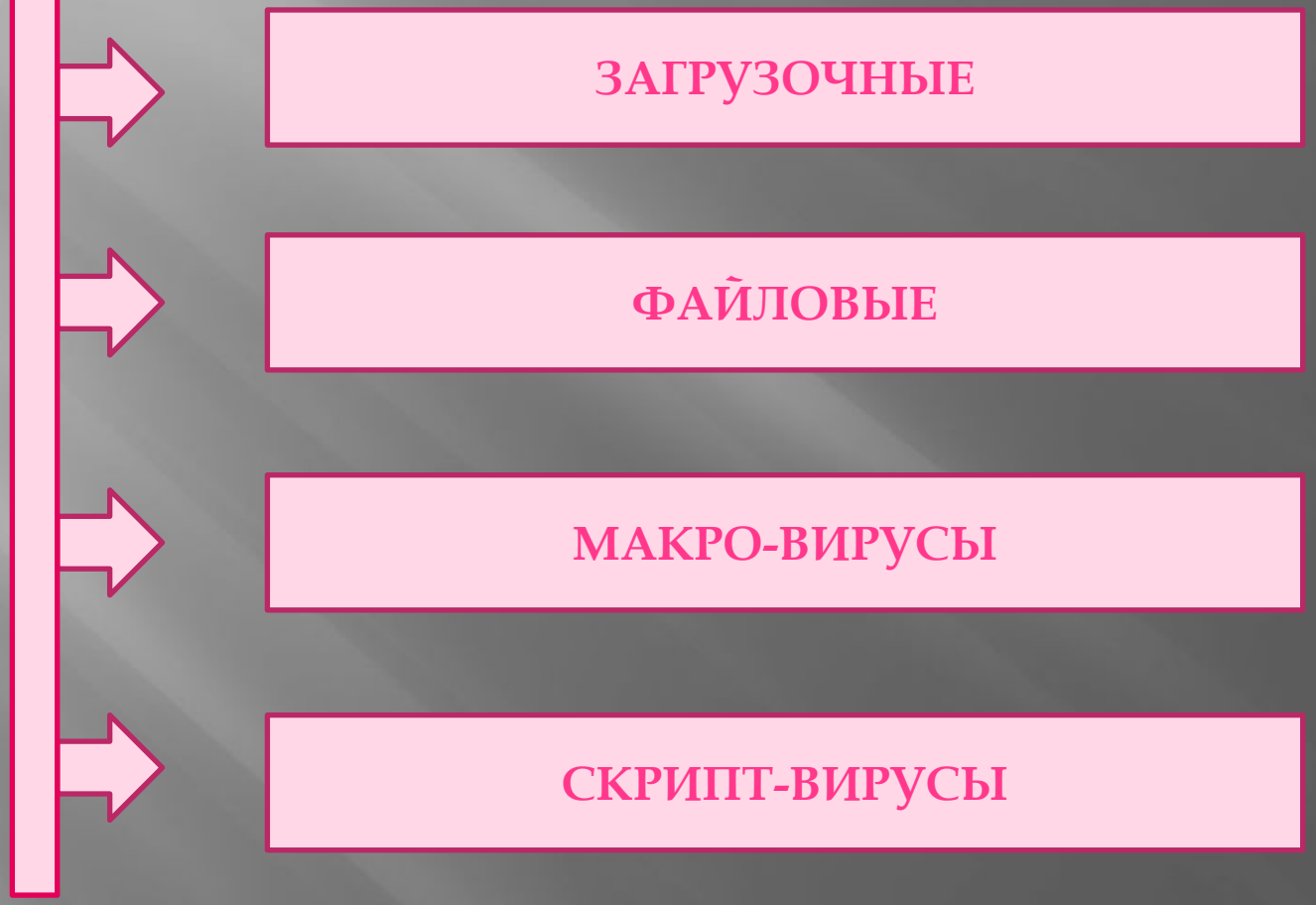
- среда обитания;
- операционная система (ОС);
- особенности алгоритма работы (способ работы);
- деструктивные возможности (вредоносные воздействия).

назад

Классификация компьютерных вирусов



ПО СПОСОБУ СОХРАНЕНИЯ И ИСПОЛНЕНИЯ СВОЕГО КОДА:



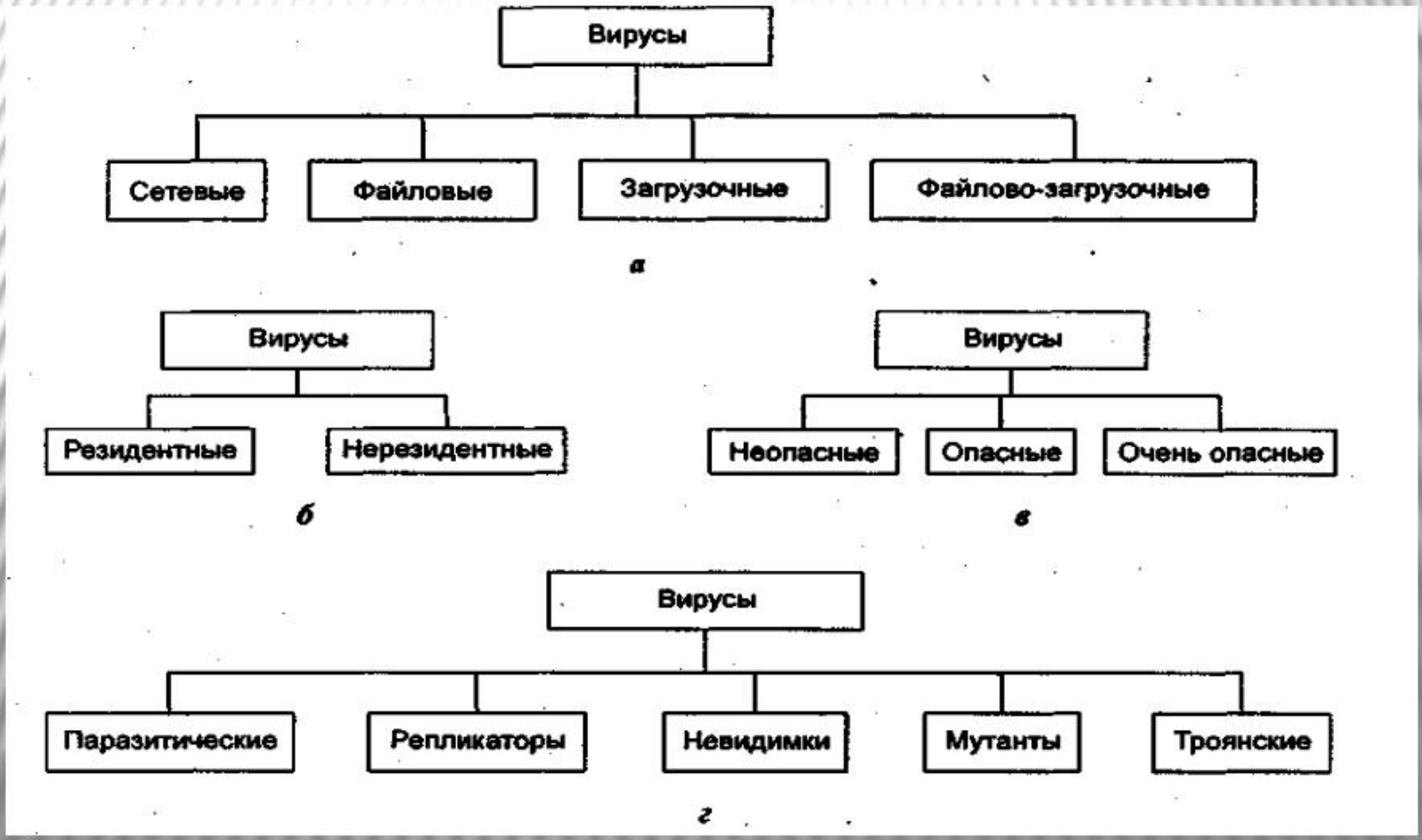
ПО СПОСОБУ РАБОТЫ (АЛГОРИТМУ)

- ТРОЯНСКИЙ
- СТЕЛС-ВИРУС
- ПОЛИМОРФНЫЕ
- МАКРОВИРУСЫ

назад

Классификация компьютерных вирусов

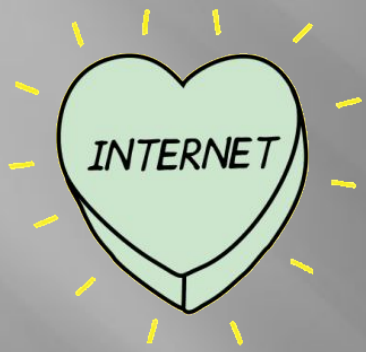
а - по среде обитания; б - по способу заражения;
в - по степени воздействия; г - по особенностям алгоритмов



назад

Загрузочные вирусы

Загрузочные вирусы заражают загрузочный сектор гибкого или жесткого диска.



При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и отдают управление не оригинальному коду загрузчика, а коду вируса. Профилактическая защита от таких вирусов состоит в отказе загрузки операционной системы с гибких дисков и установке в BIOS компьютера защиты загрузочного сектора от изменений.

В 1986 году началась первая эпидемия загрузочного вируса. Вирус-невидимка «Brain» «заражал» загрузочный сектор дискет. При попытке обнаружения зараженного загрузочного сектора вирус незаметно «подставлял» его незараженный оригинал.

назад

Файловые вирусы

Файловые вирусы внедряются в исполняемые файлы (командные файлы *.bat, программы *.exe, системные файлы *.com и *.sys, программные библиотеки *.dll и др.) и обычно активируются при их запуске.

После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т.е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы. По способу заражения файловые вирусы разделяют на перезаписывающие вирусы, вирусы-компаньоны и паразитические вирусы.

Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами. В 1999 году началась эпидемия файлового вируса Win95.CIH, названного «Чернобыль» из-за даты активации 26 апреля. Вирус уничтожал данные на жестком диске и стирал содержание BIOS.

назад

Макро-вирусы

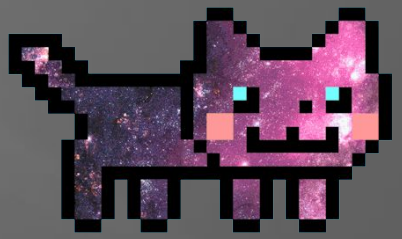
Макро-вирусы заражают документы, созданные в офисных приложениях. Макро-вирусы являются макрокомандами (макросами) на встроенном языке программирования Visual Basic for Applications (VBA), которые помещаются в документ.

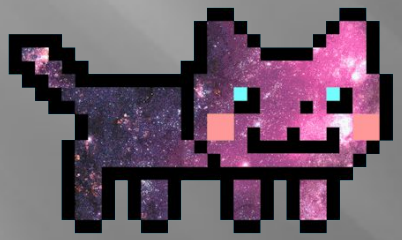
Профилактическая защита от макро-вирусов состоит в предотвращении запуска вируса (запрете на загрузку макроса). Макро-вирусы являются ограниченно- резидентными, т.е. они находятся в оперативной памяти и заражают документ, пока он открыт. Макро-вирусы заражают шаблоны документов. В 1995 году началась эпидемия первого макро-вируса «Concept» для текстового процессора Microsoft Word. Макро-вирус «Concept» до сих пор широко распространен.

назад

Скрипт-вирусы

Скрипт-вирусы – активные элементы (программы) на языках JavaScript или VBScript, которые могут содержаться в файлах Web-страниц. Заражение локального компьютера происходит при их передаче по Всемирной паутине с серверов Интернета в браузер локального компьютера.





Профилактическая защита от скрипт-вирусов состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер. В 1998 году появился первый скрипт-вирус VBScript.Rabbit, заражающий скрипты Web-страниц, а в мае 2000 года грянула глобальная эпидемия скрипт-вируса «LoveLetter».

назад

Типы вредоносных программ

- КОМПЬЮТЕРНЫЕ ВИРУСЫ
- СЕТЕВЫЕ ЧЕРВИ
- ТРОЯНСКИЕ ПРОГРАММЫ
- ПРОГРАММЫ ПОКАЗА РЕКЛАМЫ
- ПРОГРАММЫ-ШПИОНЫ
- ХАКЕРСКИЕ УТИЛИТЫ

назад

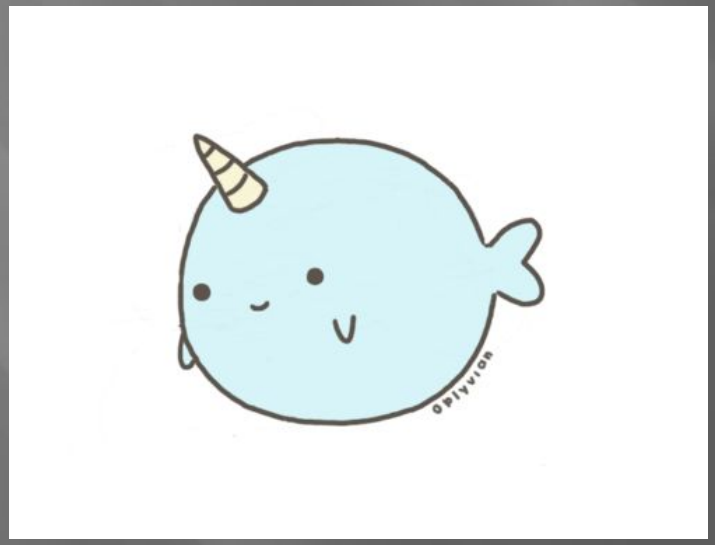
Антивирусные программы

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

назад

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



назад

Действия при наличии признаков заражения компьютера

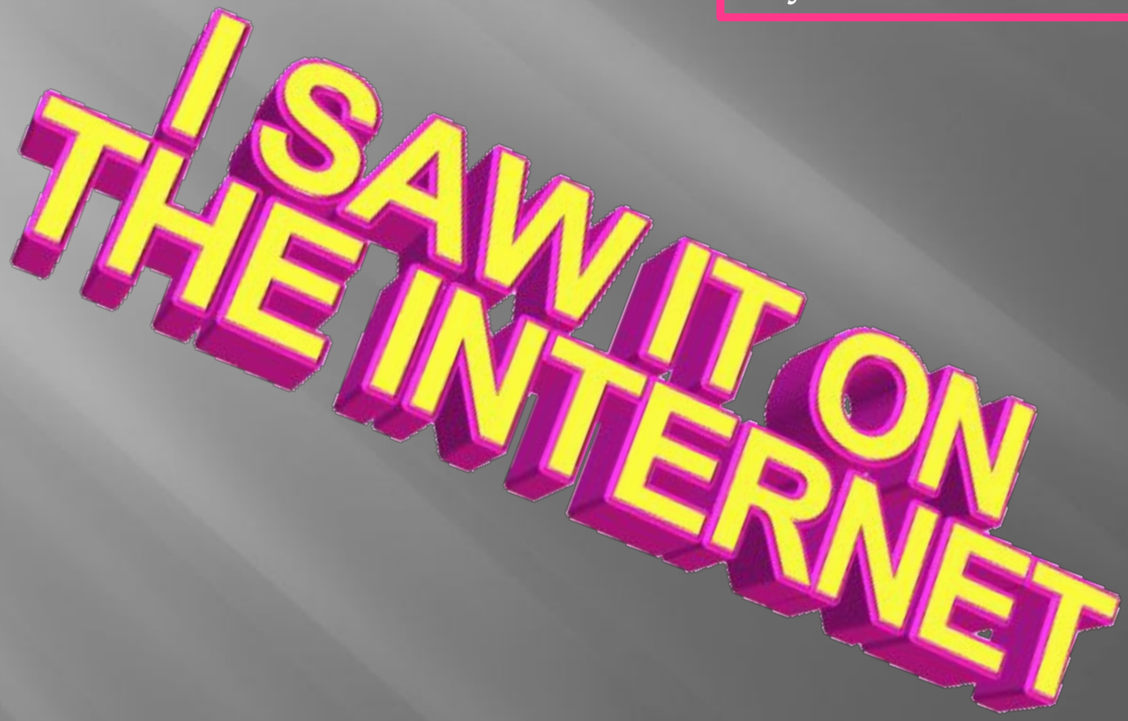
1. Сохранить результаты работы на внешнем носителе
2. Отключить компьютер от локальной сети и Интернета, если он к ним был подключен
3. Загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows (если компьютер выдает ошибку, когда вы его включаете)
4. Запустить антивирусную программу

назад

Спам и защита от него

Спам (от англ. spam) это массовая автоматическая рассылка рекламных электронных сообщений, со скрытым или фальсифицированным обратным адресом. Спам распространяется по компьютерным сетям с использованием электронной почты и систем интерактивного общения (типа ICQ), а также по мобильным сетям с использованием службы SMS-сообщений.

Спам приходит потому, что электронный адрес получателя стал известен спамерам (рассыльщикам спама). Спамеры стремятся получить подтверждение, что почтовый адрес действительно используется (в этом случае поток спама может



назад

Рекламный спам

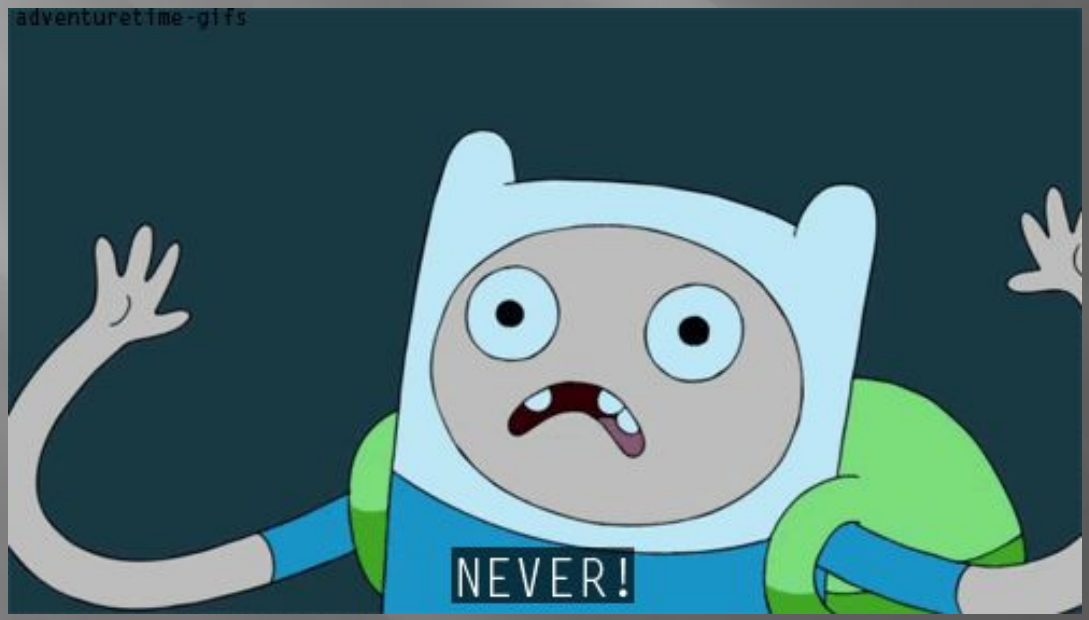
Рекламный спам используют некоторые компании, занимающиеся легальным бизнесом, для рекламы своих товаров или услуг. Р ассылку рекламного спама чаще заказывают компаниям (или лицам), которые на этом специализируются.

Привлекательность такой рекламы заключается в ее сравнительно низкой стоимости и большом охвате потенциальных клиентов. С помощью спама часто рекламируют продукцию, о которой нельзя сообщить другими способами, например оружие, порнографию, лекарственные средства с ограничениями по обороту, ворованную информацию (базы данных), контрафактное программное обеспечение и т. п.

назад

Защита от спама

В силу массового характера спамовые почтовые рассылки затрудняют работу информационных систем и ресурсов, создавая для них бесполезную нагрузку. Для борьбы со спамом используются антиспамовые фильтры, которые могут быть установлены как на локальных компьютерах пользователей, так и на почтовых серверах провайдеров.

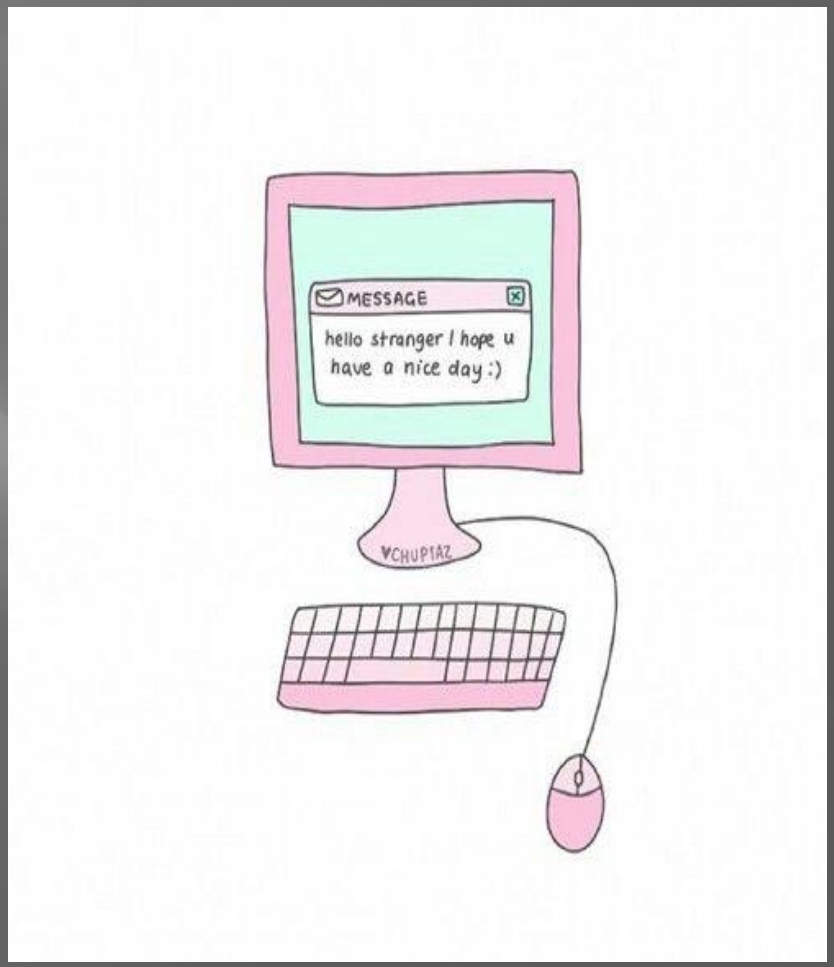


Антиспамовые фильтры анализируют содержание письма или пытаются опознать спамера по электронному адресу. Для затруднения автоматической фильтрации спамовые сообщения часто искажаются, вместо букв используются похожие по начертанию цифры, русские буквы заменяются на латинские, а в случайных местах добавляются пробелы.

назад

Защита компьютерных сетей

Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью межсетевого экрана, или брандмауэра (от англ. firewall). Межсетевой экран позволяет: блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов (определенных IP-адресов или доменных имен); не допускать проникновение на защищаемый компьютер сетевых червей (почтовых, Web и др.); препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере. Межсетевой экран может быть реализован как аппаратно, так и программно. Межсетевые экраны



назад

Основные меры по защите от вирусов

Для того, чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:

- оснастите свой компьютер современными антивирусными программами, и постоянно обновляйте их версии
- перед считыванием с дискет информации, записанной на других компьютерах,

всегда проверяйте эти дискеты на наличие вирусов, запуская антивирусные программы своего компьютера

- при переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами

назад

- периодически проверяйте на наличие вирусов, жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив операционную систему с защищенной от записи системной дискеты

- всегда защищайте свои дискеты от записи при работе на других компьютерах, если на них не будет производиться запись информации

- обязательно делайте архивные копии на дискетах ценной для вас информации
- не оставляйте в кармане дисковода А дискеты при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами

назад

Принцип работы антивирусных программ.

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.

назад

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).

назад

Антивирусные программы

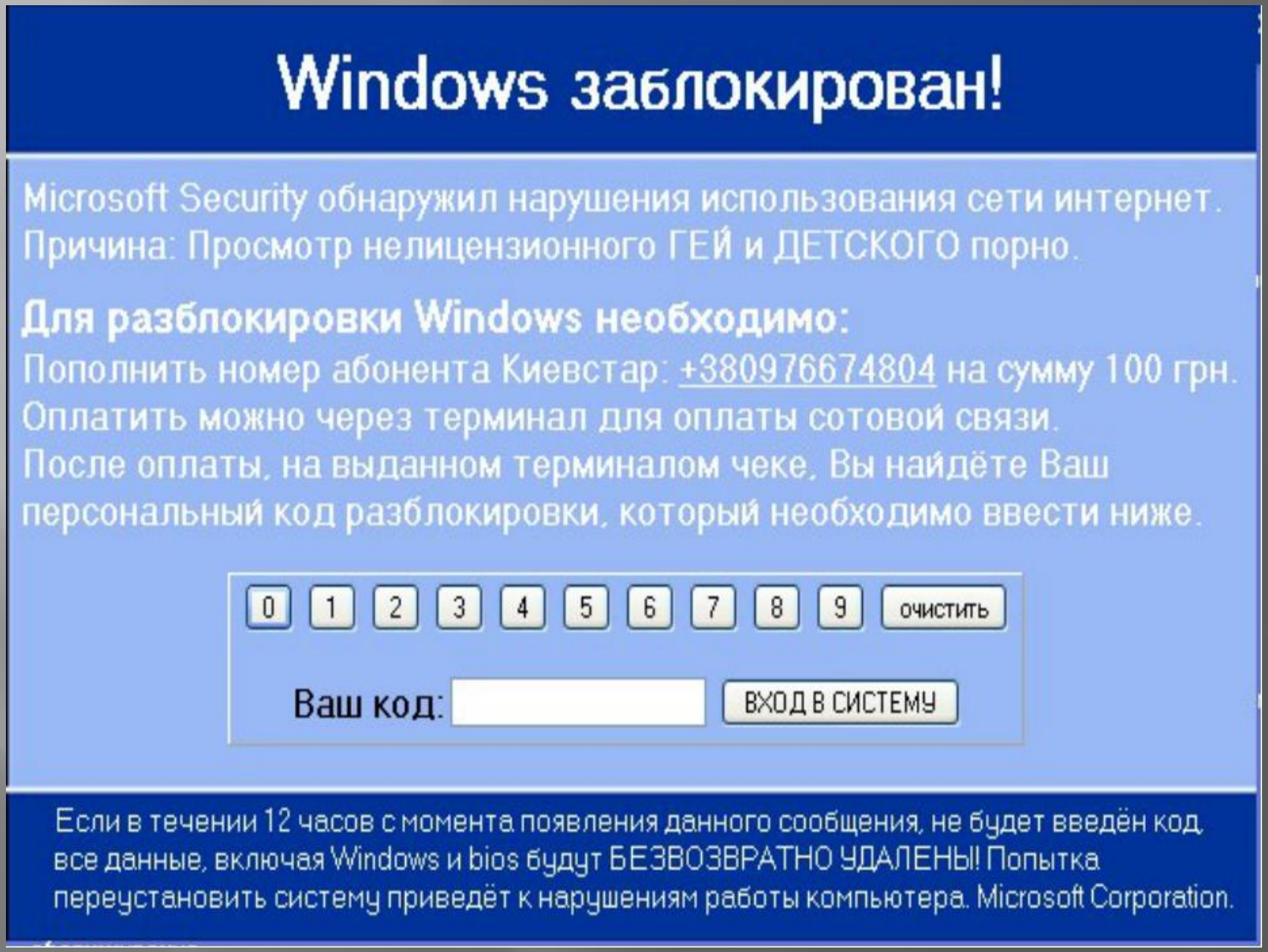
Самые популярные и широко используемые антивирусные программы для защиты компьютеров: AVG, Kaspersky, NOD 32, Dr. Web и многие другие.

назад

Пути проникновения вирусов

- Глобальная сеть Internet
- Электронная почта
- Локальная сеть Компьютеры «Общего назначения»
- Пиратское программное обеспечение
- Ремонтные службы
- Съемные накопители

назад


Windows заблокирован!
Microsoft Security обнаружил нарушения использования сети интернет.
Причина: Просмотр нелицензионного ГЕЙ и ДЕТСКОГО порно.
Для разблокировки Windows необходимо:
Пополнить номер абонента Киевстар: +380976674804 на сумму 100 грн.
Оплатить можно через терминал для оплаты сотовой связи.
После оплаты, на выданном терминалом чеке, Вы найдёте Ваш персональный код разблокировки, который необходимо ввести ниже.
0 1 2 3 4 5 6 7 8 9 очистить
Ваш код:
ВХОД В СИСТЕМУ
Если в течении 12 часов с момента появления данного сообщения, не будет введён код, все данные, включая Windows и bios будут БЕЗВОЗВРАТНО УДАЛЕНЫ! Попытка переустановить систему приведёт к нарушениям работы компьютера. Microsoft Corporation.

КОМПЬЮТЕР ЗАБЛОКИРОВАН!

Ваш компьютер заблокирован за просмотр, копирование и тиражирование видеоматериалов содержащих элементы педофилии и насилия над детьми. Для снятия блокировки Вам необходимо оплатить штраф в размере 500 рублей на номер Билайн 8-965-347-15-40. В случае оплаты суммы равной штрафу либо превышающей ее на фискальном чеке терминала будет напечатан код разблокировки. Его нужно ввести в поле в нижней части окна и нажать кнопку "Разблокировать". После снятия блокировки Вы должны удалить все материалы содержащие элементы насилия и педофилии. Если в течение 12 часов штраф не будет оплачен, все данные на Вашем персональном компьютере будут безвозвратно удалены, а дело будет передано в суд для разбирательства по статье 242 ч.1 УК РФ.

Перезагрузка или выключение компьютера приведет к незамедлительному удалению ВСЕХ данных, включая код операционной системы и BIOS, с невозможностью дальнейшего восстановления.

Разблокировать

Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних.
Изготовление, хранение или перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних, а равно привлечение несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера лицом, достигшим восемнадцатилетнего возраста, - наказываются лишением свободы на срок от двух до восьми лет с ограничением свободы на срок до одного года либо без такового.


Windows заблокирован
Для разблокировки необходимо отправить смс с текстом
t7580620000 на номер 3649
введите полученный код
Активация
для разблокировки у вас есть
02:59:41
*попытка переустановить систему может привести к потере важной информации
и нарушениям работы компьютера.

Рынок антивирусных программ очень разнообразен

Источники

1. https://www.metod-kopilka.ru/page-4-1-1-18.html
2. http://www.myshared.ru/slide/927677/
3. https://www.metod-kopilka.ru/page-4-1-1-18.html
4. https://nsportal.ru/shkola/informatika-i-ikt/library/2012/05/08/prezentatsiya-virusy-i-antivirusnye-programmy-zashchita
5. https://videouroki.net/razrabotki/vredonosnye-i-antivirusnye-programmy.html
6. http://www.myshared.ru/slide/726465/
7. https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D0%BB%D0%B0%D0%B2%D0%BD%D0%B0%D1%8F_%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D0%B0
8. https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D1%82%D0%B5%D1%81,_%D0%96%D0%BE%D1%80%D0%B6_%D0%A8%D0%B0%D1%80%D0%BB%D1%8C
9. https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D1%80%D1%85%D0%BD%D0%B8%D0%B9_%D0%A0%D0%B5%D0%B9%D0%BD
10. https://www.metod-kopilka.ru/page-4-1-1-18.html