Министерство образования и науки Республики Казахстан
Лицей при Казахской Головной Архитектуно Строительной Академии

Проект

На тему:Антивирусы

Алдибекова Куралай Алиевна

Алматы 2016год

Антивирус — программное средство, предназначенное для борьбы с вирусами
Как следует из определения, основными задачами антивируса является:
Препятствование проникновению вирусов в компьютерную систему
Обнаружение наличия вирусов в компьютерной системе
Устранение вирусов из компьютерной системы без нанесения повреждений другим объектам системы
Минимизация ущерба от действий вирусов

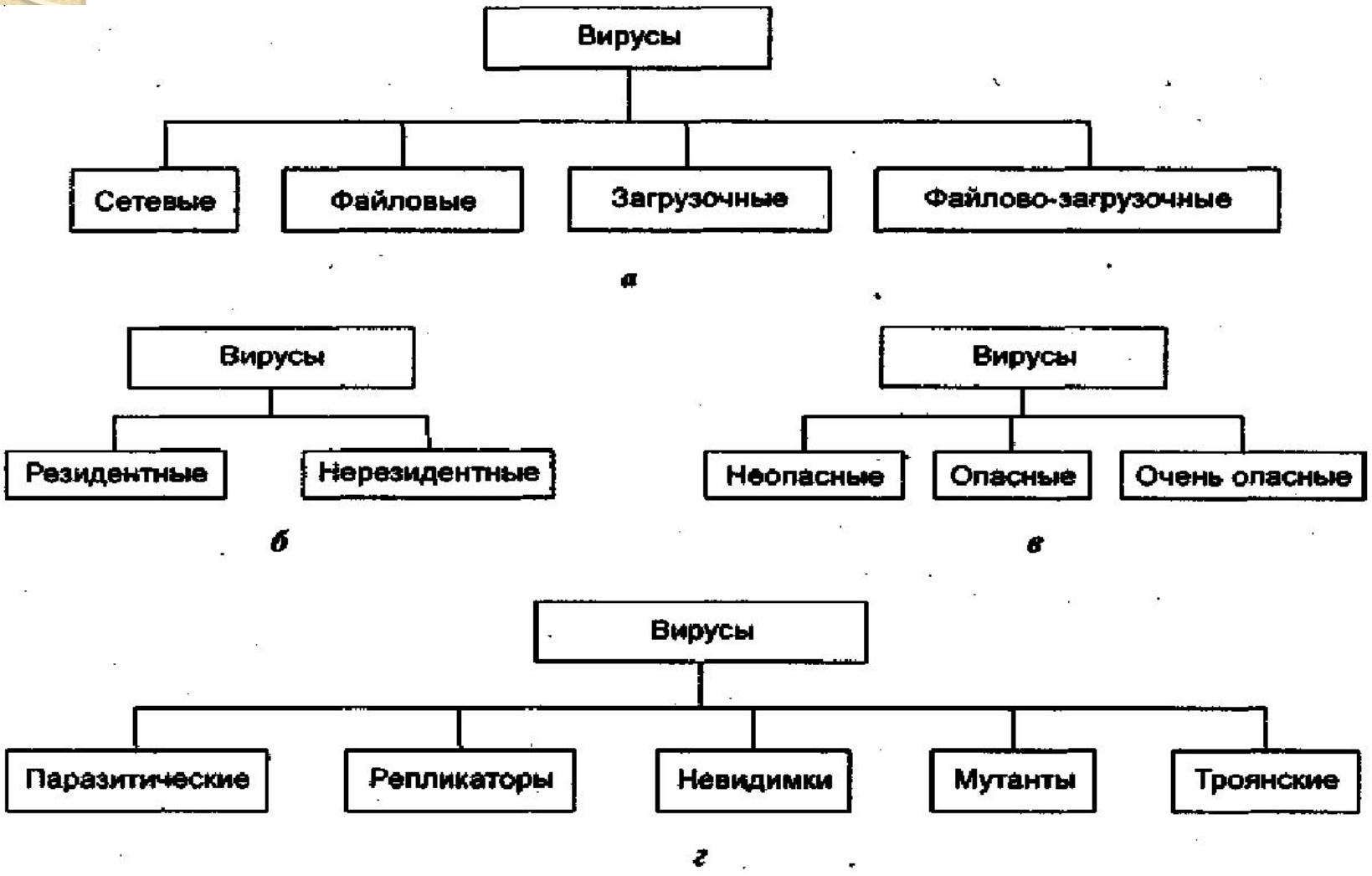
Компьютерные вирусы, как таковые, впервые появились в 1986 году, хотя исторически возникновение вирусов тесно связано с идеей создания самовоспроизводящихся программ. Одним из "пионеров" среди компьютерных вирусов считается вирус "Brain", созданный пакистанским программистом по фамилии Алви. Только в США этот вирус поразил свыше 18 тыс. компьютеров. В начале эпохи компьютерных вирусов разработка вирусоподобных программ носила чисто исследовательский характер, постепенно превращаясь на откровенно вражеское отношение к пользователям безответственных, и даже криминальных "элементов".

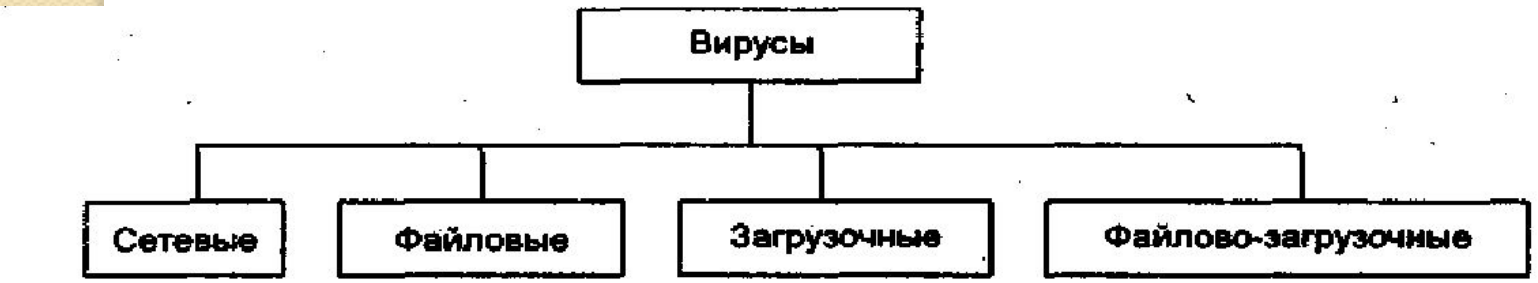
Основные признаки проявления вирусов

- Прекращение работы или неправильная работа ранее успешно функционировавших программ
- Медленная работа компьютера
- Невозможность загрузки операционной системы
- Исчезновение файлов и каталогов или искажение их содержимого
- Изменение даты и времени модификации файлов
- Изменение размеров файлов
- Частые зависания и сбои в работе компьютера
- Неожиданное значительное увеличение количества файлов на диске
- Существенное уменьшение размера свободной оперативной памяти
- Вывод на экран непредусмотренных сообщений или изображений
- Подача непредусмотренных звуковых сигналов

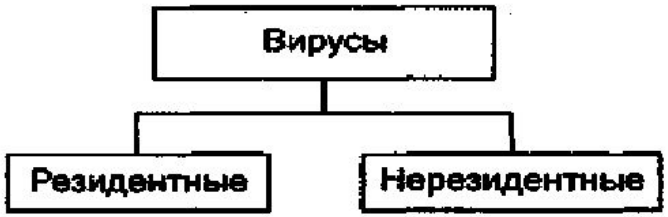
Классификация компьютерных вирусов

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

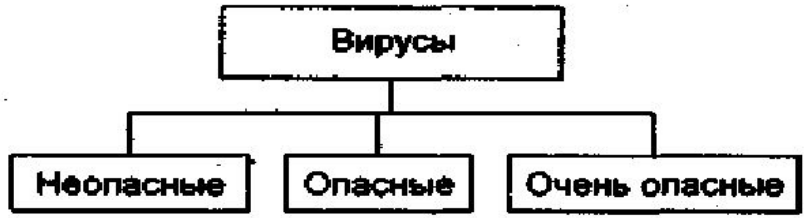



Вирусы
Сетевые
Файловые
Загрузочные
Файлово-загрузочные

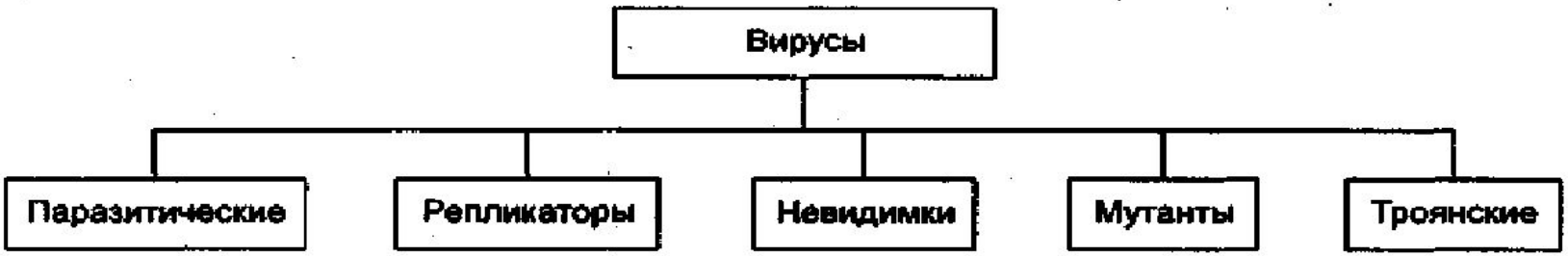
а


Вирусы
Резидентные
Нерезидентные

б


Вирусы
Неопасные
Опасные
Очень опасные

в


Вирусы
Паразитические
Репликаторы
Невидимки
Мутанты
Троянские

г

ПУТИ ПРОНИКНОВЕНИЯ ВИРУСОВ

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

По способу заражения:

Резидентные (такой вирус при инфицировании ПК оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение ОС к объектам заражения и поражает их. Резидентные вирусы живут до первой перезагрузки ПК)

Нерезидентные (не заражают оперативную память и могут быть активными ограниченное время)

По степени воздействия:

Неопасные (как правило эти вирусы забивают память компьютера путем своего размножения и могут организовывать мелкие пакости – проигрывать заложенную в них мелодию или показывать картинку);

Опасные (эти вирусы способны создать некоторые нарушения в функционировании ПК – сбои, перезагрузки, глюки, медленная работа компьютера и т.д.);

Очень опасные (опасные вирусы могут уничтожить программы, стереть важные данные, убить загрузочные и системные области жесткого диска, который потом можно выбросить)

По особенностям алгоритма:

Паразитические (меняют содержимое файлов и секторов диска. Такие вирусы легко вычисляются и удаляются);

Мутанты (их очень тяжело обнаружить из-за применения в них алгоритмов шифрования. Каждая следующая копия размножающегося вируса не будет похожа на предыдущую);

Репликаторы (вирусы-репликаторы, они же сетевые черви, проникают через компьютерные сети, они находят адреса компьютеров в сети и заражают их);

Троянский конь (один из самых опасных вирусов, так как трояны не размножаются, а воруют ценную (порой очень дорогую) информацию – пароли, банковские счета, электронные деньги и т.д.);

Невидимки (это трудно обнаружимые вирусы, которые перехватывают обращения ОС к зараженным файлам и секторам дисков и подставляют вместо своего незараженные участки.

Ремонтные службы

Достаточно редко, но до сих пор вполне реально заражение компьютера вирусом при его ремонте или профилактическом осмотре. Ремонтники — тоже люди, и некоторым из них свойственно наплевательское отношение к элементарным правилам компьютерной безопасности.

Съемные накопители

В настоящее время большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны.

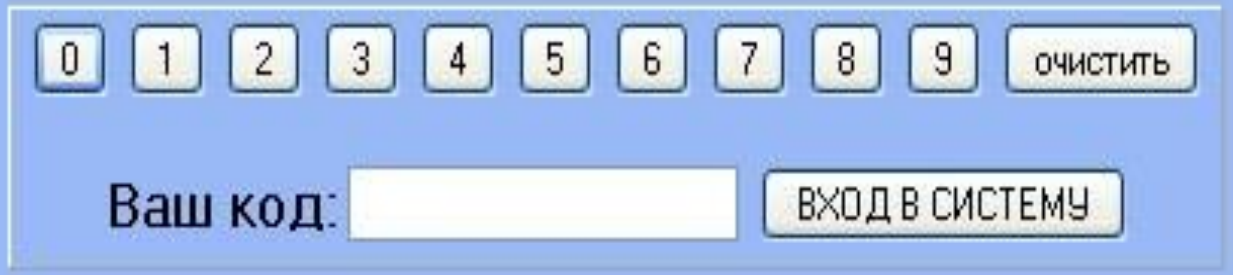
Trojan.Winlock (Винлокер) — семейство вредоносных программ блокирующих или затрудняющих работу с операционной системой, и требующих перечисление денег злоумышленникам за восстановление работоспособности компьютера. Впервые появились в конце 2007 года. Широкое распространение вирусы-вымогатели получили зимой 2009—2010 года, по некоторым данным оказались заражены миллионы компьютеров, преимущественно среди пользователей русскоязычного Интернета. Второй всплеск активности такого вредоносного ПО пришелся на май 2010 года.

Троянский конь - это вредоносное программное обеспечение, которое, без ведома владельца персонального компьютера может предоставить доступ к его данным или по определенному адресу выслать вашу персональную информацию. Кроме этого, вы даже себе и подумать не можете, что эта программа является "трояном" подобного рода законспирированы под приложения.

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.



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.

вирус

- **Вирус** представляет собой самовоспроизводящуюся программу, - которая способна внедрять свои копии в файлы, загрузочные сектора дисков и документы; приводить к нарушению нормального функционирования компьютера. Копии вирусной программы также сохраняют способность дальнейшего распространения.

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.

Как защититься от вирусов

1. установите на свой ПК современную антивирусную программу.
2. перед просмотром информации принесенной на флэш-карте (дискете) с другого компьютера проверьте носитель антивирусом;
3. после разархивирования архивных файлов сразу проверьте их на вирусы (не все антивирусные программы могут искать вредоносный код в архивах или могут делать это не корректно);
4. периодически проверяйте компьютер на вирусы (если активно пользуетесь Интернетом – запускайте раз в неделю, а то и чаще);
5. как можно чаще делайте резервные копии важной информации (backup);
6. используйте совместно с антивирусной программой файервол (firewall) если компьютер подключен к Интернет;
7. настройте браузер (программа просмотра Интернет страниц – IE, Opera и т.д.) для запрета запуска активного содержимого html-страниц.


eset
NOD 32
antivirus system


NANO
antivirus


AVG


Microsoft
Security Essentials


AVIRA