БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

Интернет

Интернет – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов.

Самые опасные угрозы сети Интернет

- Вредоносные программы
- Кража информации
- Халатность сотрудников
- Хакерские атаки
- Финансовое мошенничество
- Спам
- Аппаратные и программные сбои

Вирус

Компью́терный ви́рус — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).

КЛАССИФИКАЦИЯ

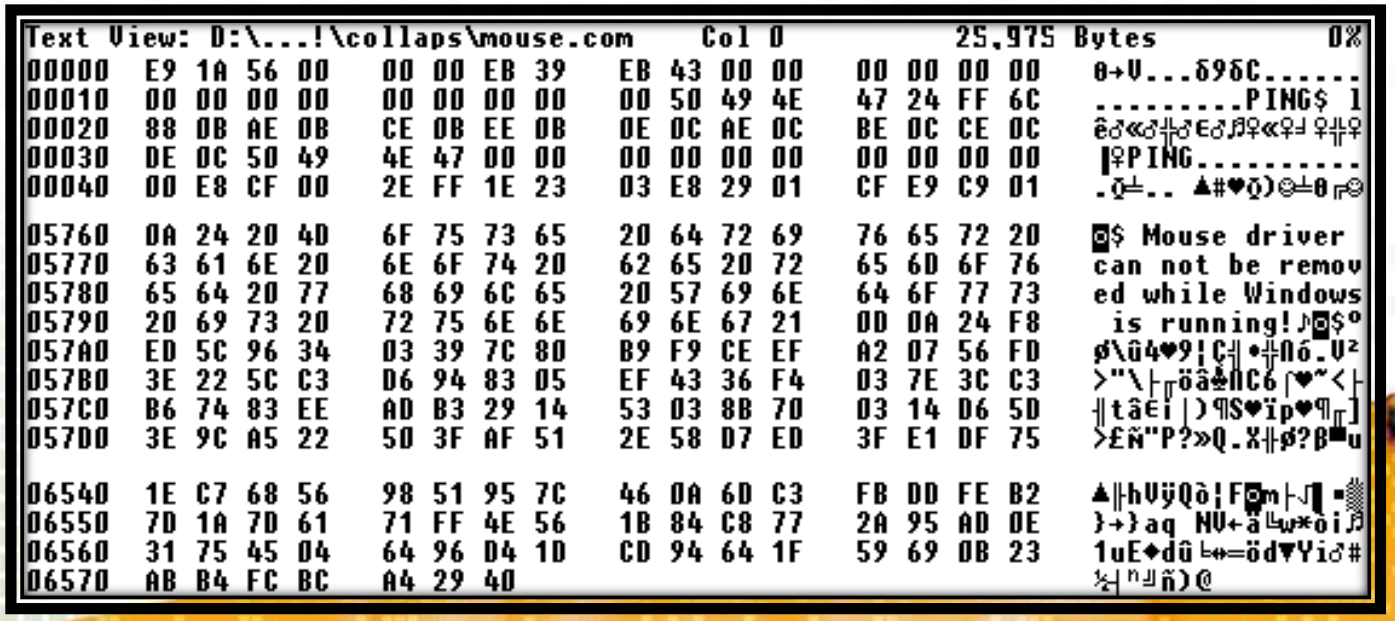
В настоящее время не существует единой системы классификации и именования вирусов.

Принято разделять вирусы на следующие группы.

ПО ПОРАЖАЕМЫМ ОБЪЕКТАМ

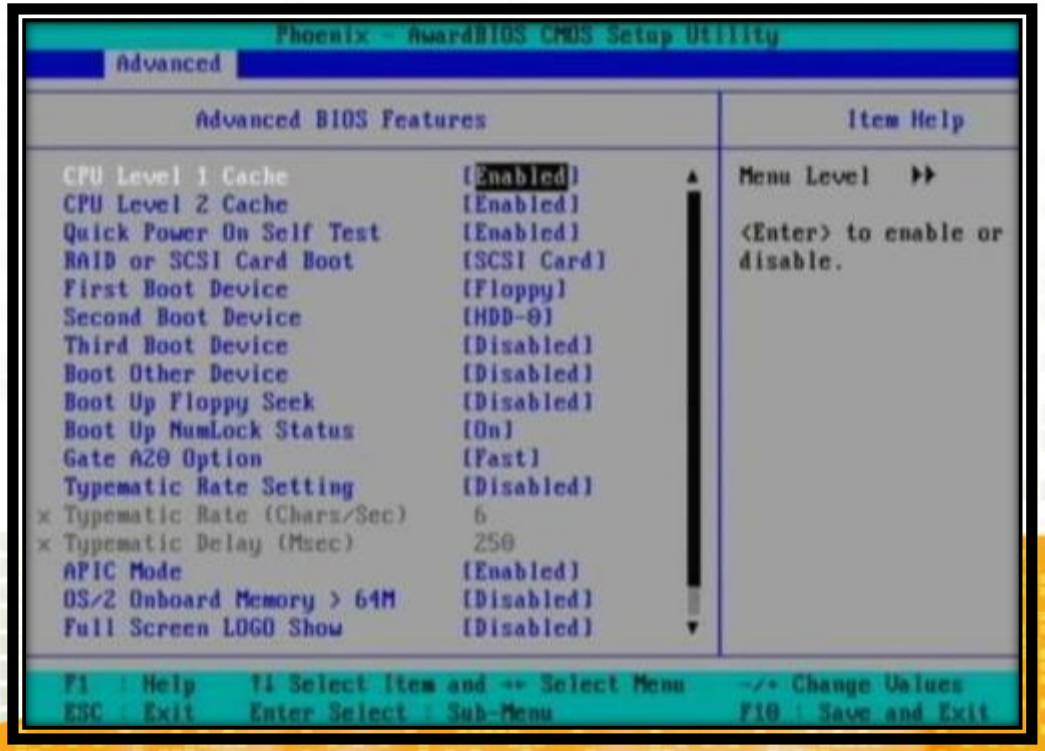
Файловые вирусы

- Это вирусы-паразиты, которые при распространении своих копий обязательно изменяют содержимое исполняемых файлов, при этом файлы, атакованные вирусом, в большинстве случаев полностью или частично теряют работоспособность)



Загрузочные вирусы

- Это компьютерные вирусы, записывающиеся в первый сектор гибкого или жесткого диска и выполняющиеся при загрузке компьютера.

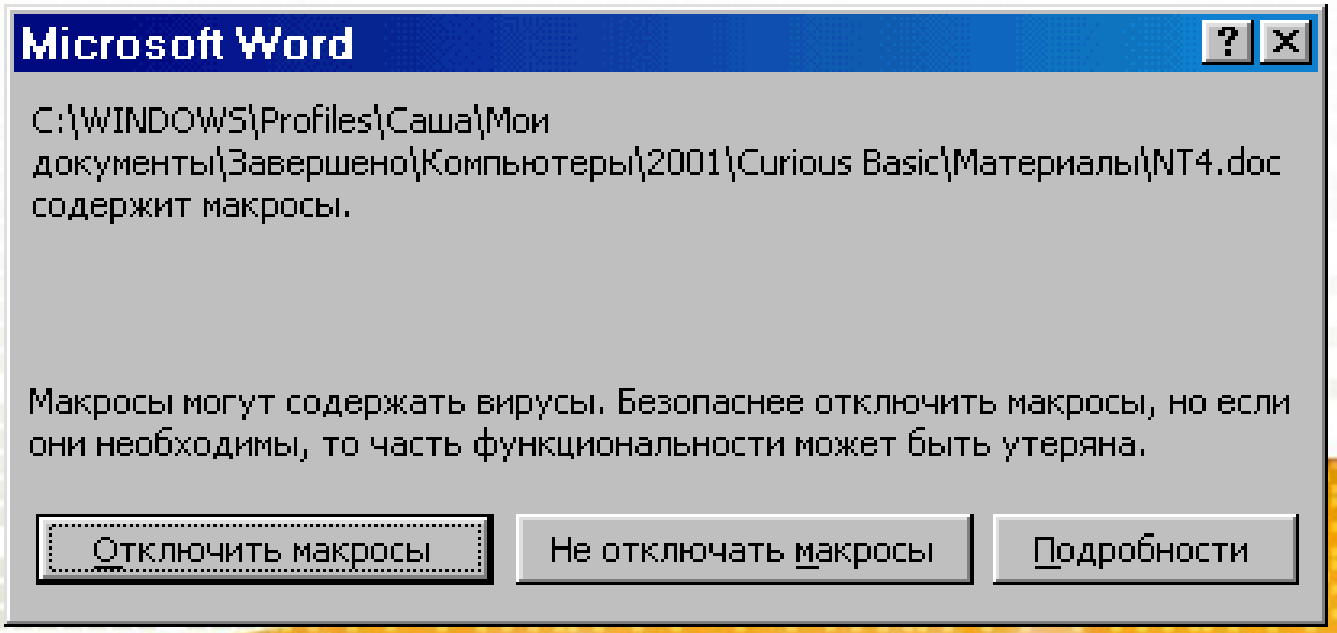


Скриптовые вирусы

- Требуют наличия одного из скриптовых языков (Javascript, VBScript) для самостоятельного проникновения в неинфицированные скрипты.

Макровирусы

- Это разновидность компьютерных вирусов разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office.



Вирусы, поражающие исходный код

- Вирусы данного типа поражают или исходный код программы, либо её компоненты (OBJ-, LIB-, DCU-файлы) а так же VCL и ActiveX компоненты.

```
text    segment    'code'
        assume     cs;text
        org    100h
Main    proc
        jmp    VStart          ;Переход на вирус
        db     'A'             ;Маркер заражённости
        mov    ax,4C00h
        int    21h             ;Завершение вирусоносителя

VStart: call   $+3             ;Определение начала вируса
        pop    bp
        sub    bp,offset VStart
        mov    di,100h
        lea    si,[bp+offset Orig]
        movsw                  ;Восстановление оригинального
        movsw                  ;начала заражённого файла

        mov    ax, 2524h
        lea    dx,[bp+New24h]
        int    21h
```

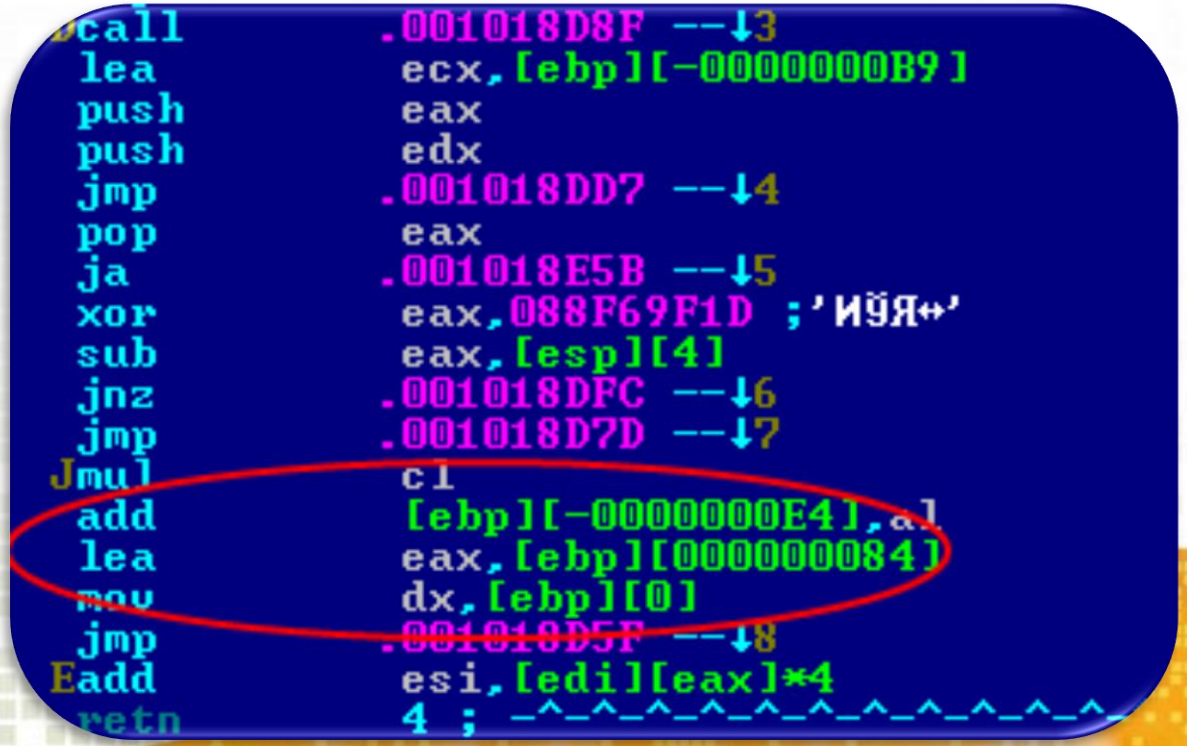
ПО ПОРАЖАЕМЫМ ОПЕРАЦИОННЫМ СИСТЕМАМ И ПЛАТФОРМАМ

- DOS
- Microsoft Windows
- Unix
- Linux

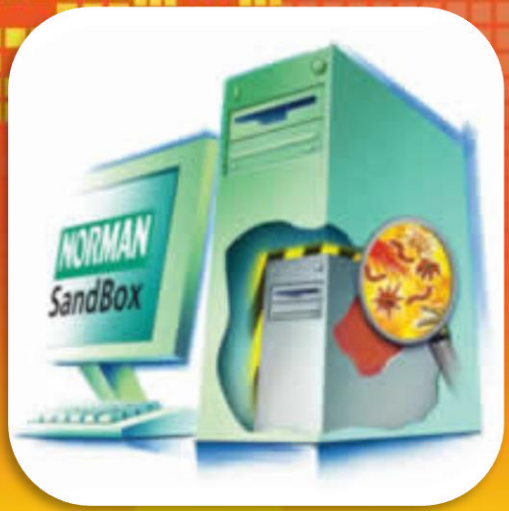
ПО ТЕХНОЛОГИЯМ, ИСПОЛЬЗУЕМЫМ ВИРУСОМ

Полиморфные вирусы

- Вирус, который при заражении новых файлов и системных областей диска шифрует собственный код.



Стелс-вирусы



- Вирус, полностью или частично скрывающий свое присутствие в системе, путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т.д.)

Руткит

- Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

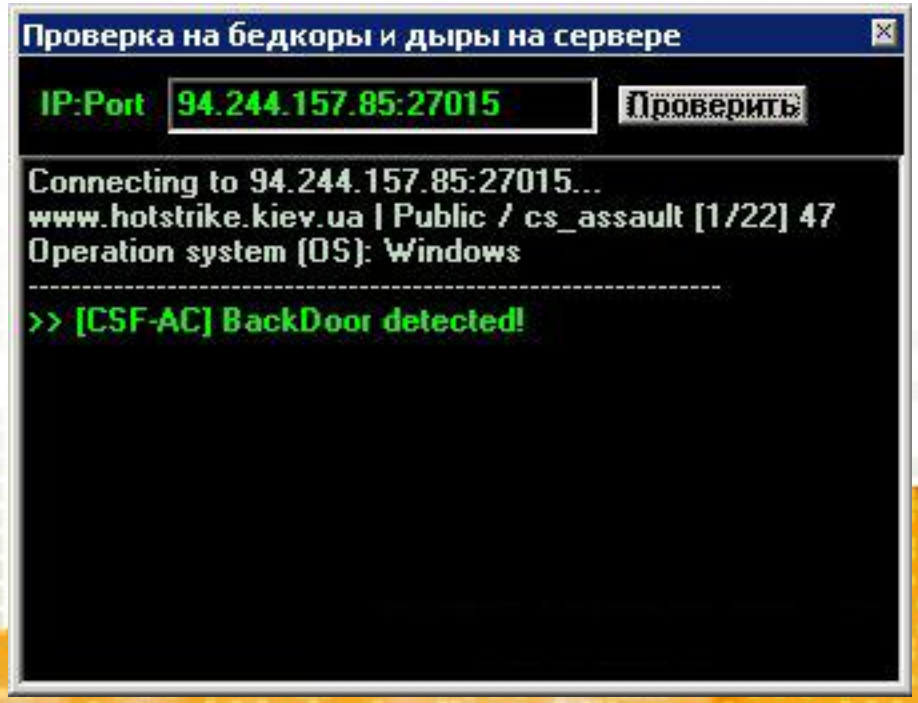
ПО ЯЗЫКУ, НА КОТОРОМ НАПИСАН ВИРУС

- ассемблер
- высокоуровневый язык программирования
- скриптовый язык
- и др.

ПО ДОПОЛНИТЕЛЬНОЙ ВРЕДОНОСНОЙ ФУНКЦИОНАЛЬНОСТИ

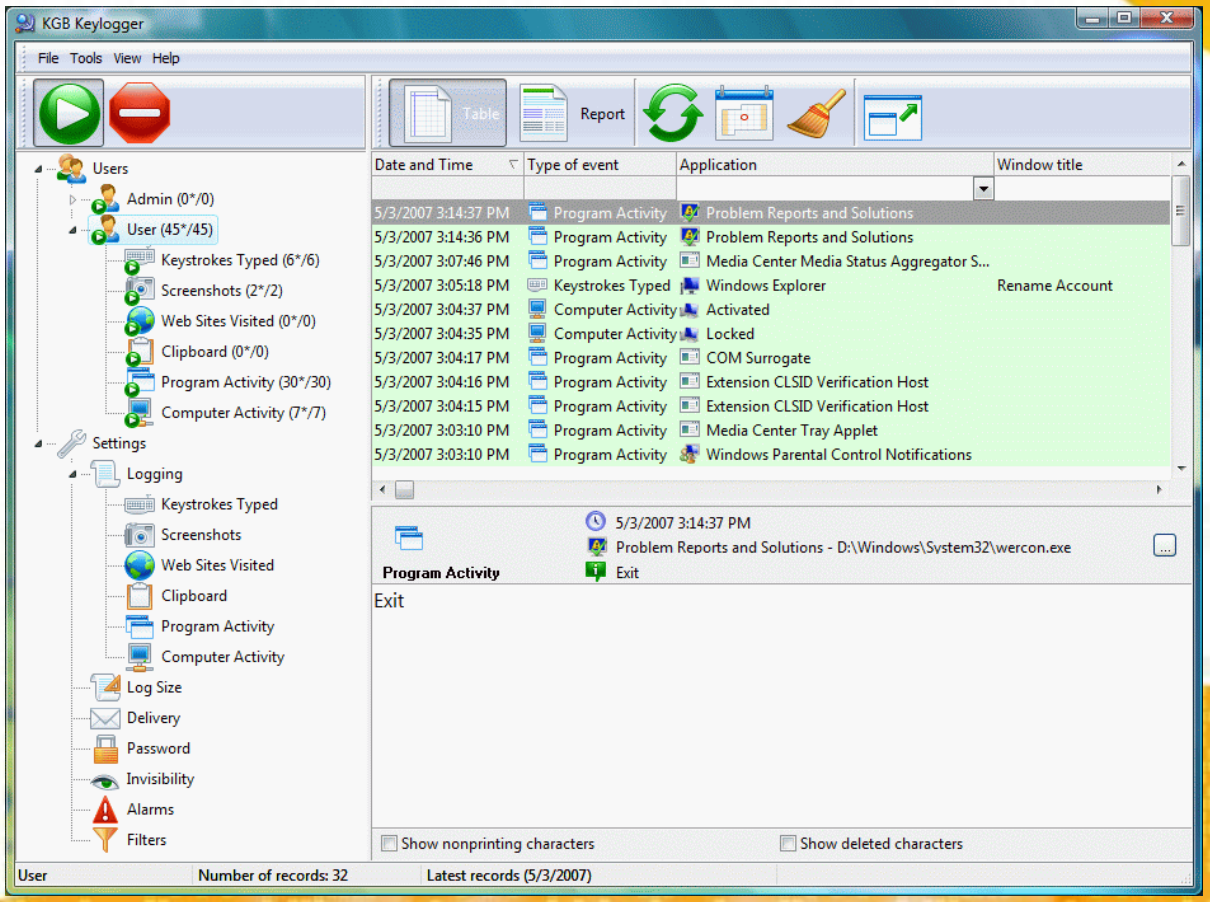
Бэкдоры

- Программы, которые устанавливает взломщик на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе.



Кейлоггеры

- Модули для перехвата нажатий клавиш на компьютере пользователя, включаемые в состав программ-вирусов.

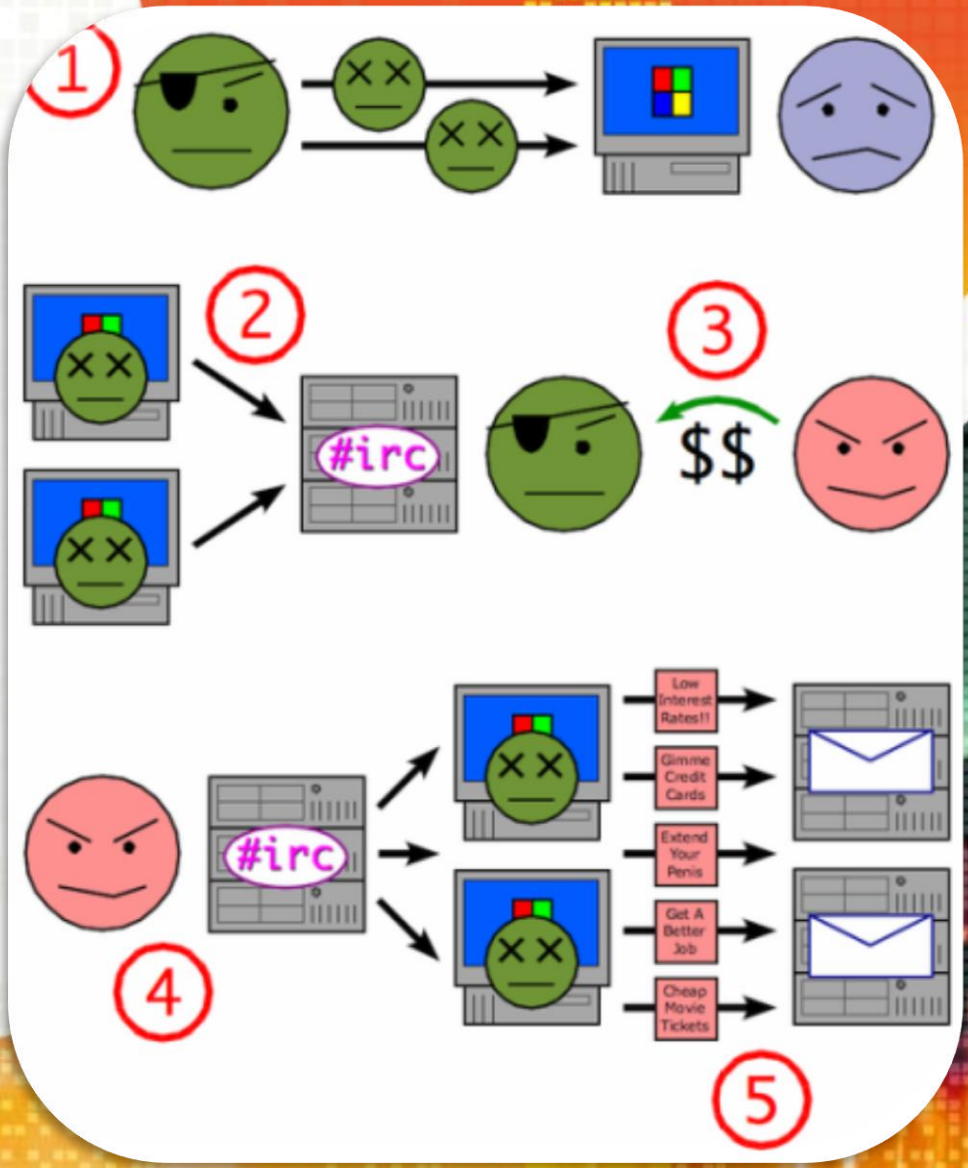


Шпионы

- Spyware — программное обеспечение, осуществляющее деятельность по сбору информации о конфигурации компьютера, деятельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя.

Ботнеты

- Это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением.
- Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.



ПРАВОВОЙ ЛИКБЕЗ

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (глава 28, статья 273)

Существует Доктрина информационной безопасности РФ, согласно которой в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, детскими порносайтами и обеспечению информационной безопасности в сетях ЭВМ.

Физкультминутка

Мы все вместе улыбнемся,
Подмигнем слегка друг другу,
Вправо, влево повернемся
И кивнем затем по кругу.
Все идеи победили,
Вверх взметнулись наши руки.
Груз забот с себя стряхнули
И продолжим путь науки.

БОРЬБА С СЕТЕВЫМИ УГРОЗАМИ

Установите комплексную систему защиты!

- Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам – фильтр и еще пару – тройку модулей для полной защиты вашего компьютера.
- Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур, лучше всего настроить программу на автоматическое обновление.

Будьте осторожны с электронной почтой!

- Не стоит передавать какую-либо важную информацию через электронную почту.
- Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения.
- Программы Microsoft Outlooku Windows Mail помогают блокировать потенциально опасные вложения.

Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari!

- Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera.
- IE до сих пор удерживает первую строчку в рейтинге популярности, но лишь потому, что он встроен в Windows.
- Opera очень популярна в России из-за ее призрачного удобства и реально большого числа настроек.
- Уровень безопасности сильно хромает как у одного, так и у второго браузера, поэтому лучше им и не пользоваться вовсе.

Обновляйте операционную систему Windows!

- Постоянно обновляйте операционную систему Windows.
- Корпорация Microsoft периодически выпускает специальные обновления безопасности, которые могут помочь защитить компьютер.
- Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа.

Не отправляйте SMS-сообщения!

- Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.
- При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.
- Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.

Пользуйтесь лицензионным программным обеспечением!

- Если вы скачиваете пиратские версии программ или свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить вирус на свой компьютер.
- Причем, чем программа популярнее, тем выше такая вероятность.
- Лицензионные программы избавят Вас от подобной угрозы!

Используйте брандмауэр!

- Используйте брандмауэр Windows или другой брандмауэр, оповещающий о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру.
- Он также позволяет запретить вирусам, червям и хакерам загружать потенциально опасные программы на компьютер.

Используйте сложные пароли!

- Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам.
- В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — 2-4 часа, но чтобы взломать семисимвольный пароль, потребуется 2-4 года.
- Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

Делайте резервные копии!

- При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена.
- Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве –флеш-карте, оптическом диске, переносном жестком диске.

Функция «Родительский контроль» обезопасит вас!

- Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.
- Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.

СПАСИБО ЗА ВНИМАНИЕ

Использованы материалы:

1. Мельников В.П. Информационная безопасность и защита информации: учеб.пособие для студентов высших учебных заведений; 3-е изд., стер.-М.: Издательский центр «Академия», 2008. – 336 с.
2. Википедия – свободная энциклопедия http://ru.wikipedia.org/wiki/Компьютерный_вирус
3. Безопасный компьютер и Интернет для детей: новая программа повышения квалификации преподавателей АПКиППРО //Microsoft в образовании. — [Электронный ресурс]. — Электрон. дан. – сор. 2008 – Режим доступа: http://www.ms-education.ru.

ИСПОЛЬЗОВАНЫ ИЗОБРАЖЕНИЯ:

- Слайд 2: http://news.ferra.ru/hard/2011/04/06/109949/
- Слайд 5: http://soft.compulenta.ru/529906/
- Слайд 7: http://www.frolov-lib.ru/antivirus/articles/mir_pk1/index.html
- Слайд 8: http://satwarez.ru/forum/65-184-1
- Слайд 9: http://www.securityscripts.ru/blogs/%D0%92%D0%B8%D1%80%D1%83%D1%81%D1%8B/virustotal-sobiraet-botnet.html
- Слайд 10: http://www.i2r.ru/static/449/out_6200.shtml
- Слайд 11: http://dic.academic.ru/dic.nsf/ruwiki/6162
- Слайд 15: http://infocom.uz/2010/06/14/samyiy-polimorfnyiy-virus/
- Слайд 16: http://strongweb.narod.ru/article_1.4.2.html
- Слайд 17: http://localname.ru/soft/rutkityi.html
- Слайд 19: http://casualuniverse.com/2012/05/rejting-yazykov-programmirovaniya-1h2012/
- Слайд 21: http://c-s.net.ua/forum/ipb.html?act=thanks&type=history&mid=24180&st=25
- Слайд 22: http://www.securitystronghold.com/gates/images/kgb-keylogger.jpg
- Слайд 23: http://www.brookfieldtec.com/computer-repair/protect-business-spyware/
- Слайд 24: http://ru.wikipedia.org/wiki/Ботнет
- Слайд 25: http://danko.ufanet.ru/news/kruglyj-stol-06-09-2012.html
- http://nnm.ru/blogs/Kvazar00900/za-samooboronu-ot-beshenogo-aziata-devushka-mozhet-poluchit-srok/page6/
- Слайд 27: http://www.islam.ru/content/analitics/1878
- Слайд 29: http://www.dokwork.ru/2012/01/blog-post.html
- Слайд 30: http://alduin.ru/antivirusnye_programmy.html
- Слайд 32: http://softwarez.su/programs/internet/browsers/page/6/
- Слайд 33: http://tipswin.ru/32-kak-otklyuchit-avtomaticheskoe-obnovlenie-v-windows-7.html
- Слайд 34: http://vorabota.ru/zaschita/kak-udalit-virus-sms-pri-pomoschi-onlayn-servisov-kaspersky-drweb-i-nod32.html
- Слайд 35: http://oboi-mira.ru/photo/3d_grafika/svoboda/3-0-3118
- Слайд 36: http://microinfo.ru/bezopasnost/13-ne-zapuskaetsya-brandmauer-windows.html
- Слайд 38: http://www.itshneg.ru/gides/kak-pravilno-delat-rezervnuyu-kopiyu-dannyx/
- Слайд 39: http://mini.butovonet.ru/deti.html
- Слайд 40: http://zontytrislona.ru/kartinki-smajliki-s-yazykom-2.html