

M. Çuriýew

MAGLUMATLARY GORAMAK

Ýokary okuw mekdepleri üçin okuw kitaby

*Türkmenistanyň Bilim ministrligi
tarapyndan hödürlenildi*

Aşgabat
Türkmen döwlet neşirýat gullugy
2013

Çüriýew M.

Ç 85 Maglumatlary goramak. Ýokary okuw mekdepleri üçin okuw kitaby. A.: Türkmen döwlet neşirýat gullugy, 2013.

Bu okuw kitaby kompýuterdäki maglumatlary goramagyň usullaryny öwretmäge gönükdirilendir. Kitapda maglumaty goramagyň 5 görnüşine – şifrlemäge, ýüklenilişi çäklendirmäge, parol arkaly goramaklyga, maglumaty gizlemek hem-de wiruslardan we troýanlardan goramaklyga sere-dilýär. Bu usullaryň häzirki wagtdaky ýetmezçilikleri, artykmaçlyklary we umumy peýdalylygy öwrenilýär, olary kämilleşdirmek üçin birnäçe görke-zmeler hem-de her bir usul üçin kompýuterde programma düzülip, onuň häsiýetlerine baha berilýär. Mundan başga hem gorag usullarynyň bilelikde ulanylyp dogry utgaşmasynyň peýdaly netijeleri görkezilýär.

Okuw kitaby öz düzüminde diňe maglumat beriji bölümleri saklaman, eýsem amaly taýdan peýdaly görkezmeleri we maslahatlary hem öz içine alýar.

Okuw kitaby kompýuter tehnologiýasy ugrunda işleýänler we okaýan-lar üçin niýetlenen hem bolsa, ondan beýleki höwesjeň adamlar hem peý-dalanyp bilerler.



**TÜRKMENISTANYŇ PREZIDENTI
GURBANGULY BERDIMUHAMEDOW**



TÜRKMENISTANYŇ DÖWLET TUGRASY



TÜRKMENISTANYŇ DÖWLET BAÝDAGY

TÜRKMENISTANYŇ DÖWLET SENASY

Janym gurban saňa, erkana ýurdum,
Mert pederleň ruhy bardyr köňülde.
Bitarap, garaşsyz topragyň nurdur,
Baýdagyň belentdir dünýäň önünde.

Gaýtalama:

Halkyň guran Baky beýik binasy,
Berkarar döwletim, jigerim-janym.
Başlaryň täji sen, diller senasy,
Dünýä dursun, sen dur, Türkmenistanym!

Gardaşdyr tireler, amandyr iller,
Owal-ahyr birdir biziň ganymyz.
Harasatlar almaz, syndyrmaz siller,
Nesiller döş gerip gorar şanymyz.

Gaýtalama:

Halkyň guran Baky beýik binasy,
Berkarar döwletim, jigerim-janym.
Başlaryň täji sen, diller senasy,
Dünýä dursun, sen dur, Türkmenistanym!

**Türkmenistanyň Prezidenti
Gurbanguly Berdimuhamedow:**

– Taze tehnologiýalar diňe bir önümçilikde öňegidişlikleri däl, eýsem, adamlaryň biri-birleri bilen habarlaşmagy, her şahsyýetiň jemgyýetde öz ornuny tapmagy, bilim derejesini ýokarlandyrmagy we taze nesli terbiýelemege üçin hem giň mümkinçilikleri döredýär.

GIRIŞ

Türkmenistanda garaşsyzlygyň ilkinji ýyllaryndan başlap dünýä tehnologiýalarynyň ösüşine örän uly gyzyklanma döredi. Sebäbi şol döwürde täzedan gurulýan döwletimiziň dürli pudaklarynda dünýä ösüşiniň iň taze gazananlarynyň, ýokary derejeli enjamlaryň, gurallaryň, öňdebaryjy usullaryň ornaşdyrylmagy ýurdumyzyň tiz we ýokary depginli ösmegi üçin gaty zerurdy. Şonuň üçin hem Türkmenistanda dürli tehnologiýalary öwrenmeklik boýunça uly işler alnyp barylýdy we häzir hem bu işler ýokary depginler bilen dowam etdirilýär.

Tehnologiýalary ulanmakdan öň olary öwrenmek zerurlygy ýüze çykýar. Tehnologiyalary öwrenmek ylmyň esasy wezipeleriniň biri bolup durýar. Tehnologiya hem öz gezeginde ylmyň ösmegine özüniň oňyn täsirini ýetirýär.

Ylym milli häsiýete eýe bolman, ol milli çäklerden daşyna çykýar. Ylym umumy adamzat häsiýete eýe bolup, onuň gazananlary birnäçe ýyllardan soň ähli ýurtlarda adaty ulanylýan zada öwrülýär. Şonuň üçin hem häzirki wagtda döwletleriň arasynda ylmy babatdaky özara hyzmatdaşlyklar ýokary derejede ýola goýulýar. Ony Türkmenistanyň mysalynda hem görmek bolýar. Ýurdumyzda soňky ýyllarda geçirilýän köp sanly halkara ylmy-amaly maslahatlar we sergiler munuň aýdyň mysalydyr.

Häzirki wagtda Türkmenistanda milli bilim ulgamynda düýpli özgertmeler geçirilýär. Şol özgertmeleriň baş maksady hem türkmen

ýaşlaryna dünýäniň iň ösen talaplaryna laýyk gelýän bilimleri elýeterli etmekden ybaratdyr.

Bilşimiz ýaly ylym – bilimden ýokarky başgaçakdyr. Gowy gurnalan bilim syýasaty bu – ylmyň daýanjydyr. Ýaşlary ylmy işlere çekmek – ýurdumyzda alnyp barylýan bilim syýasatynyň aýrylmaz we wajyp bölekleriniň biridir.

Çalt depginler bilen ösýän kompýuter tehnologiýalary biziň durmuşymyza degişli üýtgeşmeleri girizýär. Indi, köplenç „maglumat“ düşüňjesi ýörite bir harydyň belgilenmesi hökmünde ulanylýar. Şonda maglumatyň bahasy, köplenç, ony saklaýan kompýuter ulgamynyň bahasyndan ýokary bolýar. Maglumat örän gymmat we wajyp bolup ýa-da täjirçilik we döwlet syry hökmünde bolup bilýändigini sebäpli, şol maglumaty saklaýan, işläp bejerýän we geçirýän maglumat ulgamlaryna garşy dürli erbet maksatly hereketleriň bolmagy mümkindir. Şonuň üçin hem, maglumaty rugsatsyz elýeterlilikden, üýtgetmekden we ogurlamakdan goramagyň zerurlygy ýüze çykýar.

Okuw kitabynda kompýuterdäki maglumatyň goragynyň birnäçe usullaryna seredilýär. Olaryň ýetmezçilikleri we artykmaçlyklary hem-de umumy peýdalylygy öwrenilýär. Her bir usul üçin kompýuterde programma düzülip, onuň häsiýetlerine baha berilýär. Maglumaty goramagyň kriptografiýa, ýüklenilişi çäklendirme, parol arkaly goramak, maglumaty gizlemek, wiruslardan we troýanlardan goramak usullary seljerilýär.

Usullaryň her biri belli bir derejede özleriniň önünde goýlan maksatlaryny amala aşyrmaga niýetlenendir.

Kriptografiýa (şifrlmek) usulynyň manysy ençeme asyrlar bäri üýtgemän gelýär, esasy özgerişler diňe onuň tehniki serişdesine degip geçdi. Açyk maglumatlaryň (**plaintext**) şifrlenlen (şifrtkest, ciphertext) maglumatlara ýa-da şifrlenlen maglumatlaryň açyk maglumatlara açarlaryň ulanylmagynda belli bir kadalar boýunça bolup geçýän özgerişlere şifrlme (**encryption**) diýilýär. Şifrlmegiň birnäçe usullary bar. Kitapda olaryň has ýörgünlilerine seredilýär we olar boýunça düzülen programmalar seljerilýär.

Kompýuter programmalary – bu hem maglumatdyr. Şonuň üçin hem, programmalaryň goýberilmeginiň ýa-da ýüklenilmeginiň çäk-

lendirilmegi-de maglumatyň goragyna degişlidir. Kompýuterde ulanylýan programma önümlerini goramagyň bu usulynyň döränine köp wagt geçenok. Bu usul örän “ýaşdyr”. Emma muňa garamazdan, ol giňden ýaýrady. Dogrudan hem, programma taýdan üpjünçilik bilen meşgullanýan dünýä belli we näbelli söwda markalary bu usuly örän netijeli diýip hasaplaýarlar. Programmanyň goýberilişini wagt boýunça, sany boýunça we belli bir kompýuterde goýbermek bilen çäklendirmek bolýar. Kitapda bu usul üçin birnäçe programmalar düzülip olaryň netijeliligi seljerilýär.

Maglumaty goramagyň ýene bir usuly parol arkaly goragdyr. Bu usul gadymy usullaryň biridir. Ol gulp ýaly işleýär. Nädogry açar girizilende gulp açylmaýar, ýagny parol nädogry girizilende programma öz edýän mümkinçiliklerini hödürlemeýär. Dörediji programmany kämillik derejesine getirenden soň, programmanyň özüne simwollaryň yzygiderligini belläp goýýar. Ol yzygiderlilik parol hökmünde çykyş edýär. Nädogry simwollaryň yzygiderligi girizilende programma “käbir amallary amala aşyrýar”, ýagny programma ýa signal berýär ýa-da ýapylýar we kämahal özüni öçürip hem bilýär. Bu usulyň esasy ýetmezçilikleriniň biri paroly başga adamlaryň bilmekligidir. Okuw kitabynda oňa garşy usul hödürlenilýär.

Maglumaty goramaga ony gizleme usulyny hem degişli etmek mümkin. Dogrudan hem, görünmeýän zady ogurlamak, eýsem ulanmak mümkin däl. Kitapda şu usul üçin ýörite programma berlip, onuň mümkinçilikleri görkezilýär.

Häzirki wagtda tehnologiýanyň ösmegi bilen, maglumata bolan howplaryň ýene bir görnüşi – virus ýa-da troýan howpy emele geldi. Soňky döwürlerde virus döredijileriň “ussatlygy” has artdy, maksatlary bolsa erbetleşdi. Wirus hereket etmegi has “kämil” görnüşe geçip başlady. Kitapda wiruslaryň, şeýle hem häzirki wagtda olara garşy ulanylýan öndürijilikli meşhur antiwirus programmalarynyň işine baha bermek bilen, ýurdumyzda ýörite taýýarlanylýan antiwirus programmasy barada hem gürrüň edilýär.

Şeýle hem 2000-nji ýyldan bäri maglumaty goramak boýunça toplanan maglumatlar, ýerine ýetirilen tejribelikler, çykarylan netijeler jemlenilýär.

I. KRIPTOGRAFIÝA WE MAGLUMATLARY GORAMAK

1. Şifrlemegiň esaslary.
2. Şifrlemegiň görnüşleri.
3. Şifrlemegiň işleýşini ýazmaça beýan etmek.
4. XOR logiki operatoryny ulanmak arkaly şifrlemegi programmirleme arkaly amala aşyrmak.
5. Dürli görnüşli programmirlеме dillerini şifrlemegiň bir meselesini çözmek arkaly barlag geçirmek.

1.1. Şifrlemegiň esaslary

Asyrlaryň dowamynda material zatlar baradaky maglumatlar ol zatlaryň özlerinden pes bolmadyk derejede ähmiýete eýe bolupdyr. XXI asyr informatikanyň we informasiýa tehnologiýalarynyň asyrydyr. Häzirki zaman tehnologiýasy maglumatyň has uly mukdaryny ihermäge we saklamaga mümkinçilik berýär. Munuň amatly taraplary bilen bilelikde ters taraplary-da bardyr. Dürli sebäplere görä maglumat meselesinde “gowşaklyklar” ýüze çykyp başlady [7]:

- ýatda saklanylýan we iberilýän maglumatlaryň artyp barýan göwrümleri;
- Kompýuteriň resurslaryny, programmalary we maglumatlary ulanmaga ygtyýary bolan ulanyjylaryň toparlarynyň giňelmegi;
- Hasaplaýyş ulgamlaryny peýdalanma režimleriniň çylşyrymlaşdyrylmagy.

Şu sebäplere görä bu okuw kitabynda ihermekde we saklamakda rugsat edilmedik (REU) maglumatlary goramak meselesi has uly ähmiýete eýe bolup gelýär. Bu meseläniň düýbi – maglumaty goraýyş boýunça hünärmenleriň öz “garşydaşlaryna” garşy göreşindedir.

Şifrlemegiň iş alyp barýan algoritmleriniň häsiýetnamasy

| Algoritmiň ady | Açaryň ölçegi, bit | Blogyň ölçegi, bit | Inisializirlenme wektoryň ölçegi, bit | Şifrlemegiň gaýtalanmasynyň sany |
|----------------|--------------------|--------------------|---------------------------------------|----------------------------------|
| Lucipher | 128 | 128 | | |
| DES | 56 | 64 | 64 | 16 |
| FEAL-1 | 64 | 64 | 4 | |
| B-Crypt | 56 | 64 | 64 | |
| IDEA | 128 | 64 | | |
| ГОСТ 28147-89 | 256 | 64 | 64 | 32 |

Maglumatyň goralýşy – aşakdakylary üpjün edýän çäreleriň, usullaryň we serişdeleriň toplumydyr:

Kompýuteriň resurslaryna, programmalara we maglumatlara bolan REU-nyň mümkinçiliginiň bolmazlygy;

- maglumatyň bitewiliginiň barlanmagy;
- Programmalaryň rugsatsyz ulanylmagynyň mümkinçiliginiň bolmazlygy (programmalaryň göçürmeden goralýşy).

Maglumatyň iberilişiniň we ýatda saklanylyşynyň sanly usullaryna geçmek diskret (tekst, faks, teleks) we üznüksiz (gepleşik) maglumatyň goralýşy üçin unifikirlenen usullary we algoritmleri peýdalanmaga mümkinçilik döredýär.

Maglumatyň REU-syndan bolan goranmagyň peýdaly usuly – şifrleme (kriptografiýa).

Şifrleme (encryption) diýip açyk maglumatlaryň (plaintext) şifrlenlen (**şifrt tekst, ciphertext**) maglumatlara ýa-da şifrlenlen maglumatlaryň açyk maglumatlara açarlar ulanylanda belli bir kadalar boýunça bolup geçýän özgermesine aýdylýar. Inlisçe şifrleme/şifrden çykarma – **enciphering/deciphering**.

Kriptografiýa usullary arkaly aşakdakylary amal edip bolýar:

- maglumatyň şifrlenmesini;
- elektron ýazgynyň amala aşmagyny;
- şifrlemegiň açarlarynyň tertip boýunça paýlanylyşyny;

- maglumatyň tötänden ýa-da bilgeşleýin üýtgedilmeginden goramagy,

Şifrleme algoritmlerine şu talaplar bildirilýär:

- deşifrlemä we mümkin bolan modifikasiýa garşy maglumaty ýokary derejede goramak;
- maglumatyň goragy diňe açaryň bilinmeginde esaslanyl-malydyr we algoritmiň mälüm bolandygyna bagly bolmaly däl-dir (Kirkhoffyň düzgüni);
- başlangyç tekstiň ýa-da açaryň sähelçe üýtgemegi şifrlen-en tekstiň ep-esli üýtgemegine getirmelidir (“gorpyň” effekti);
- açaryň bahasynyň çägi bahalaryny yzly-yzyna basmak arkaly maglumatlaryň deşifrleme mümkinçiliginiň bolmazlygyny üp-jün etmeli;
- ýeterlikli tiz hereket etmekde algoritmiň amala aşmagynyň tygşytlylygy;
- maglumatlaryň açarsyz deşifrlenmesiniň bahasy maglumatlaryň bahasyndan artyk bolmalydyr.

Kriptologiýa gadymy ylymdyr, ony Ýuliý Sezar baradaky hekaýa bilen baglanyşdyrýarlar. Ýuliý Sezaryň (100-44 ýý. b.e.öň) Siseron (106-43 ýý. b.e. çenli) bilen we Gadymy Rimiň başga “abonentleri” bilen hat ýazyşmasy şifrlenýärdi. Sezaryň gaýtalanma çalşyrmalaryň şifri, maglumatdaky her bir harpy ondan belli bir harplaryň san aralygynda ýerleşýän harpa çalyşmakdan ybaratdyr. Elipbiý gaýta-lanýar, Z harpdan soň A harp gelýär. Sezar harpy ondan 3 harp aralyk-da duran harpa çalyşýar.

Häzirki wagtda kriptologiýada simwollar bilen harp görnüşde däl-de, olara degişli sanlar bilen işlemek kabul edilen. Şeýlelik bilen latyn elipbiýinde 0-dan (A harpa degişli) 25-e (Z harpa degişli) çenli sanlary ulanyp bileris. Başlangyç simwola degişli bolan sany x bilen, şifrlenende bolsa y bilen belgiläp, çalşyрма şifriniň ulanylyş düzgü-nini şeýle ýazyp bileris:

$$y = x + z \pmod{N}, \quad (1)$$

bu ýerde z – gizlin açar, N – elipbiýdäki simwollaryň sany, N -iň moduly boýunça goşulmasy bolsa adaty goşulma amalyna meňzeşdir. Emma adaty goşma N uly ýa-da kiçi netijäni berýän

bolsa, bu jemiň netijesi bolup, onuň N -e bölünmesiniň galyndysy bolýar.

Sezaryň şifrinde kabul edilen belgilerde gizlin açaryň bahasy 3 (Sezar Awgustyňkyda bolsa $z = 4$). Şeýle şifrler örän ýeňil açylýar, özem açary bilmek zerur hem däl şifrlemäniň algoritmini bilmek ýeterlikdir. Açary bolsa ýönekeý, yzly-yzyna basyşdyrmaklyk bilen (başgaça aýdylanda güýç hüjümi) tapyp bolýar. Kriptologiýa hem iki bölekden – şifrlemegiň usulyny ýa-da maglumatyň hakykylygyny, hem kriptogramalaryň şifrdan çykarmasyndan we çalşyrylmagyna seredýän kriptanalizden ybaratdyr. Ilkinji şifrleriň gowşaklygy birnäçe ýüzýyllyklara kriptografiýa işiniň daşynda gizlinlik atmosferasyny döretdi, kriptologiýanyň ylym hökmünde ösüşini saklady.

“Ylymdan ozalky” kriptografiýa iki müň ýyldan gowrak wagtyň dowamynda birnäçe gyzykly çözgütler bilen baýlaşdy. Ýönekeýje amal – çalşyрма elipbiý tertibi saklanmalary ýerine ýetirildi. Maglumatdaky simwollaryň ýerini çalşyrmaklyk (çalşyрма şifrleri) hem oňat amal edildi.

Kriptografiýa boýunça ilkinji ulgamlaryň iş hökmünde beýik arhitektör Leon Batista Albertiniň (1404–1472 ý.) işi hasaplanýandyr. XVII asyryň ortasyna çenli kriptografiýa we kriptanaliz boýunça işler has köpeldi. Şol döwürde Ýewropadaky şifrogrammalara degişli intrigalar örän gyzyklydyr. Olaryň arasyndan Fransua Wiýetiň (1540–1603 ý.) işlerini bellemek bolar. Ol fransuz koroly Genrih IV köşgünde kriptanaliz (ol döwürde bu ady götermeýärdi) bilen üstünlikli meşgullanypdyr.

Asyryň dowamyndaky kriptogramalaryň deşifrlenmesine aýry simwollaryň we olaryň birleşmeleriniň duş gelşiniň ýygýlykly analiziň kömegi barada aýtmak bolar. Tekstda aýry harplaryň duş geliş ähtimallyklary güýçli tapawutlanýandyrlar (rus dili üçin, meselem, “o” harpy “ф” harpyndan 45 esse köp duş gelişändir). Bu, bir tarapdan, hem açarlaryň açylmagyna, hem-de şifrleme algoritmleriniň analizi üçin esas bolup hyzmat edýär. Islendik ýönekeý çalşyрма simwolyň duş geliş ýygýlygyny bukmagy mümkin etmeýär. Emma maglumatyň nazaryýeti we artyklygyň derejesi entek dördilmedi we kriptografiýaň duşmany – ýygýlyk analizi bilen göreş üçin RANDOMIZASIÝA

hödürlenilýär. Onuň awtory Karl Fridrih Gauss (1777–1855 ý.) açylmaýan şifri döretdi diýip ýalňys hasaplanan.

Kriptologiýanyň taryhynda belli bolan şahsyýetleriň biri bolup gollandiýaly Ogýust Kerkhoff (1835–1903 ý.) çykyş edýär. Oňa ajaýyp “Kerkhoffyň düzgüni” degişlidir: şifriň berkligi diňe açaryň gizlinligi bilen kesgitlenmelidir. Bu düzgüniň döredilen wagtyny göz öňünde tutup, ony beýik açyşlaryň biri diýip hasaplap bolýar. Bu düzgün sifrlmegiň ALGORITMINIŇ gizlin dälidigini görkezýär.

Jilber Wernam (G.S. Vernam) 1926-njy ýylda açylyp bilmejek şifri hödürledi. Şifriň manysy (1) deňlemede her indiki simwol üçin z -niň täze ähmiýetini saýlamakdyr. Başgaça aýdylanda, gizlin açar diňe bir gezek ulanylýar. Eger şeýle açar tötänleýin saýlanýan bolsa, onda Şennonyň subutnamasyna laýyklykda 23 ýyldan soň şifr açylmaýan bolup galýar. Bu şifr “şifrbloknotlary” ulanmak üçin nazary esas bolup durýar. Olary giňişleýin ulanmak Ikinji jahan urşy ýyllarynda başlandy. Şifrbloknot bir gezek ulanylýan açarlaryň köp mukdaryny saklaýar. Ol açarlar maglumatlaryň şifrlenmesinde yzygiderli saýlanýlar. Wernamyň hödürlemesi welin, gizlin baglanyşygyň meselelerini çözmeýär: gizlin maglumatyň geçirilişiniň usulynyň deregine oňa UZYNLYGY bilen DEŇ BOLAN gizlin açaryň geçirilişiniň usulyny, ýagny başgaça aýdylanda açyk tekstde saklanýan simwollaryň sanyny saklaýan usuly.

1949-njy ýylda Klod Şennonyň “Gizlin ulgamlardaky baglanyşygyň taglymaty” diýen makalasy ylmy kriptologiýanyň esasyyny goýdy. Şennon käbirini “tötänleýin şifr” üçin sifrotekstiň belgiler sany üçin aşakdaky aňlatmany hödürledi:

$$H(Z)/(r \log N). \quad (2)$$

Eger kriptanalitik olary alyp bilse, onda çäklenmedik resurslarda ol açary dikeldip (we şifri açyp) bilýär. Bu ýerde $H(Z)$ – açaryň entropiýasy, r – açyk tekstiň artykmaçlygy, N – elipbiýiň ölçegi.

Arhiwatorlaryň tekst faýllary gysýandygy netijesinde adaty tekstiň uludygy bellidir. Sebäbi olaryň işi hem peseldilmeginden ybaratdyr (özem onuň has ýeňil aýrylýan böleginde). Adaty tekstiň möçberiniň 0,75 bolan ýagdaýynda we 56 bit açaryň ulanmagynda (DES tarapyndan hödürlenýän ýaly), kriptanalitigiň çäklenmedik

resurslarda açaryň dikeldilmegi üçin şifrotekstiň 11 simwoly ýeterlikdir. Has takygy aňlatma (2) islendik şifr üçin subut edilen däl-dir, emma belli bolan hususy ýagdaýlar üçin dogrudyr. Bu aňlatmadan, kriptanalitigiň işini diňe kriptosistemanyň kämilleşdirilmegi bilen däl-de, açyk tekstiň artykmaçlygynyň kemelmegi bilen hem kynlaşdyryp bolýanlygy baradaky netijä gelinýär.

Eger açyk tekstiň artykmaçlygyny nula çenli peseltseň, onda gysga açar hem kriptanalitigiň açyp bilmejek şifrini berer.

Şifrlemeden öňürti maglumaty statistiki kodirlemeden geçirmelidir (gysmaklykdan, arhiwasiýadan). Şonuň bilen maglumatyň ölçeği we artykmaçlygy peseler, entropiýa (bir simwola gabat gelyän maglumatyň ortaça mukdary) galar. Gysylan tekstde gaýtalanýan harplar we sözler ýok bolany sebäpli, deşifrleme (kriptanaliz) örän çylşyrymlaşdyrylar.

1.2. Şifrlemegiň görnüşleri

Şifrlemegiň algoritmleriniň klassifikasiýasy

- Simmetriki (gizlin, ýeke-täk açarly, bir açarly single-key).
- Akymly (maglumatyň akymynyň şifrlenmegi):
 - bir gezekli ýa-da üznüksiz açarly (infinite-key cipher);
 - gutarnykly açarly (Wernamyň ulgamy – Vernam);
 - galp tötänleýin sanlaryň generatoryň esasynda (GTS);
- Blokly (maglumatlaryň bloklaýyn şifrlenmesi):
 - ýerini üýtgetme şifri (permutation, P-bloklar);
 - çalşyрма şifri (substitution, S-bloklar);
- bir elipbiýli (Sezaryň kody);
- köp elipbiýli (Widženeriň şifri, Džefferson silindri, Uetstounyň diski, Enigma);
- Düzümleýin:
 - Lucifer (IBM firmasy, ABŞ);
 - DES (Data Encryption Standard, ABŞ);
 - FEAL-1 (Fast Enciphering Algorithm, Ýaponiýa);
 - IDEA/IPES (International Data Encryption Algorithm;

- Improved Proposed Encryption Standard, Ascom-Tech AG firmasy, Şweýsariýa);
- B-Crypt (British Telecom firmasy, Beýik Britaniýa);
- ГОСТ 28147-89 (СССР); * Skipjack (АВШ).
- Асимметрики (ачык аçarly, public-key);
- Diffie-Hellman DH (Diffie, Hellman);
- Раýwest-Şamir-Adleman RSA (Rivest, Shamir, Adleman);
- El-Gamal ElGamal.

Mundan başga-da, şifrlemegiň algoritmleri şifrlere (ciphers) we kodlara (codes) bölünýär. Şifrler aýratyn bitler, harplar, simwollar bilen işleýärler. Kodlary lingwistiki elementler bilen operirleýärler (bogunlar, sözler).

1.3. Şifrlemegiň işleýşini ýazmaça beýan etmek

Aşakdaky mysala seredeliň.

Mysal. Аşakda iňlis elipbiýiň harplary getirilen.

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Goý “MUGALLYM” diýen sözi şifrlemeklik gerek bolsun. Gizlin açar hökmünde biz $z = 3$ kabul edeliň (Sezaryň açaryny). Indi berlen sözüň her bir harpyny ondan 3 harp aralyk bilen yzda ýerleşen harpa çalşyralyň. Аşakda her harpyň kese çyzykdan soň çalşyryljak ähmiýeti görkezilen.

M – P, U – X, G – J, A – D, L – O, L – O, Y – B, M – P

Görşümüz ýaly “M” harpdan 3 harp yzda “P” harpy ýerleşen, beýleki harplar hem şol tertip bilen alynýar. “Y” harpy üçin birnäçe goşmaça ýagdaýlar emele gelýär. Ol elipbiýiň soňundan ikinji bolup ýerleşýär we yzyndan diňe “Z” harpy bar. Bu ýagdaýda sanaw elipbiýiň başyndan dowam etdirilýär, ýagny “Z” harpdan soň “A” harpy sanalyp, “B” harpy “Y” harpdan soň üçünji harp hökmünde alynýar.

Netijede “PXJDOOBP” harp yzygiderlilik alynýar.

Şeýlelik bilen “**MUGALLYM**” sözi “PXJDOOBP” bilen şifrlenýär. Geliň indi şifrlenenden sözi ony alyp okajak “abonentler” tapypdan şifrdan çykarylma amalyňa göz ýetireliň. Indi açary ($z=3$) bilýän islendik “abonent” şifrlenenden sözün her harpyny alyp onuň önünden 3 harp aralykda ýerleşen harpa çalsyp bilýär. Şeýlelik bilen:

P – M, X – U, J – G, D – A, O – L, O – L, B – Y, P – M

Bu ýerde hem “B” harpy bilen işlenende käbir goşmaça ýagdaýlar emele gelýär. Ondan öňde duran “A” harpy sanalýar, soňra sanaw elipbiýiniň soňundan dowam etdirilýär – “Z” harpy sanalýar we “Y” harpy üçünji harp bolup alynýar.

Netijede “**MUGALLYM**” sözünü alýarys.

Öz döwründe bu usul örän netijeli bolupdyr we belli bir derejede ýazylan maglumatlary gizlin saklamagy üpjün edýärdi. Emma wagtyň geçmegi bu usul kämilligi talap edýärdi. Sebäbi özge adam şifrlämegiň açaryny bilýän ýagdaýynda aňsatlyk bilen şifrlenenden maglumaty “aýdyňlaşdyryp” bilerdi.

Şonuň üçin hem harplaryň çalşyrylmagynyň has netijeli usullary döredi [8].

Şifrläme harplar arkaly däl-de, kompýuterdäki simwollaryň üsti bilen geçirilýär. Ekrandaky resminamanyň içine islendik simwol klawiatura arkaly girizilýär. Her bir simwoly girizmek üçin belli bir klawişa bar.

Klawiaturadaky klawişanyň basylmagy kompýutere signalyň ikilik san görnüşinde iberilmeginden ybarat. Ol san kod tablisasynda saklanylýar. Kod tablisasy – kompýuterde simwollaryň içki görkezilişi. Hemme döwletlerde standart hökmünde ASCII tablisasy (American Standart Code for Information Interchange) çykyş edýär. Bir simwolyň ikilik koduny saklamak üçin 1 baýt belenen. 1 baýt – 8 bit. Her bit 0 we 1 bahany kabul edýändigini göz önünde tutmak bilen, olaryň bir baýtda mümkin bolan yzygiderliginiň sany $2^8 = 256$. Şeýlelik bilen bir baýt arkaly 256 sany dürli kod kombinasiýasyny almak mümkin we olar arkaly 256 sany simwol görkezmek mümkin. Şol kombinasiýalar ASCII tablisany düzýärler.

ASCII standartynyň birinji 128 simwoly 0-dan 127-ä çenli – sanlar, latyn elipbiýiniň harplary, dolandyrys simwollary bilen kesgit-

lenýär. Ilkinji 32 simwol dolandyryňan bolýar we esasan dolandyrys buýruklary bermek üçin niýetlenen. Simwollaryň kod tablisasynyň ikinji bölegi amerikan standarty bilen kesgitlenmeýär we milli harplary görkezmek üçin niýetlenen.

Ýokardakylary has aýdyňlaşdyrmak üçin geliň latyn elipbiýiniň harplarynyň koduny ikilik we onluk sanda göreliň:

| Iňlis elipbiýiniň uly harpy | Ikilik sandaky kody | Onluk sandaky kody | Iňlis elipbiýiniň kiçi harpy | Ikilik sandaky kody | Onluk sandaky kody |
|--|------------------------------------|-----------------------------------|---|------------------------------------|-----------------------------------|
| A | 01000001 | 65 | a | 01100001 | 97 |
| B | 01000010 | 66 | b | 01100010 | 98 |
| C | 01000011 | 67 | c | 01100011 | 99 |
| D | 01000100 | 68 | d | 01100100 | 100 |
| E | 01000101 | 69 | e | 01100101 | 101 |
| F | 01000110 | 70 | f | 01100110 | 102 |
| G | 01000111 | 71 | g | 01100111 | 103 |
| H | 01001000 | 72 | h | 01101000 | 104 |
| I | 01001001 | 73 | i | 01101001 | 105 |
| J | 01001010 | 74 | j | 01101010 | 106 |
| K | 01001011 | 75 | k | 01101011 | 107 |
| L | 01001100 | 76 | l | 01101100 | 108 |
| M | 01001101 | 77 | m | 01101101 | 109 |
| N | 01001110 | 78 | n | 01101110 | 110 |
| O | 01001111 | 79 | o | 01101111 | 111 |
| P | 01010000 | 80 | p | 01110000 | 112 |
| Q | 01010001 | 81 | q | 01110001 | 113 |
| R | 01010010 | 82 | r | 01110010 | 114 |
| S | 01010011 | 83 | s | 01110011 | 115 |
| T | 01010100 | 84 | t | 01110100 | 116 |
| U | 01010101 | 85 | u | 01110101 | 117 |
| V | 01010110 | 86 | v | 01110110 | 118 |
| W | 01010111 | 87 | w | 01110111 | 119 |
| X | 01011000 | 88 | x | 01111000 | 120 |
| Y | 01011001 | 89 | y | 01111001 | 121 |
| Z | 01011010 | 90 | z | 01111010 | 122 |

Tablisadan görnüşi ýaly klawiaturada „A“ klawişasy basylan-da 01000001 ybarat signal berilýär, onuň onluk sandaky görnüşi 65. Şeýle hem tablisadan şol bir harpyň uly we kiçi görnüşiniň kodunyň tapawutlydygyny görmek mümkin. Klawiaturada her bir simwolyň öz kody bar, bu düzgün rus, türkmen we beýleki dilleriň elipbiýiniň harplaryna degişli bolup durýar.

Geliň indi şifrleme meselämize gaýdyp gelemiň. Her harpyň we simwolyň öz kodunyň bardygyny bilmek bilen, şol koduň üstünde belli bir amallar geçirilip, başga bir kod alyp, şol koda eýe bolan başga harpy almak mümkin. Eger şol amal, täze alnan harpyň üstünden geçirilip, başdaky harpymyzy almagy mümkin edýän bolsa, onda biziň şifremegiň bir usuly barada gürrüň edýändigimiz aýdyň.

1.4. XOR logiki operatoryny ulanmak bilen şifremegi programmirleme arkaly amala aşyrmak

Şol amallaryň biri XOR logiki operatory amala aşyrmagy mümkin edýär. Bu operator iki baýtyň (harpyň ýa-da simwollaryň) ýa-da sözüň arasynda her bit boýunça amalary geçirip bilýär. Her bit 0 ýa-da 1 bolýandygyny ýene bir gezek bellemek bilen, XOR operatoryň aşakdaky işleýşini görkezmek mümkin [9]:

| 1-nji bit | 2-nji bit | XOR amalyňyň netijesi |
|-----------|-----------|-----------------------|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Mysal hökmünde XOR amalyňy „A“ we „B“ harpyň üstünden ýerine yetireliň:

| | | | | | | | | |
|--------------------------------|---|---|---|---|---|---|---|---|
| A harpyň kody | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| B harpyň kody | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| XOR amalyndan soň alnan simwol | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |

Ýokardaky amalmyzyň netijesinde biz “00000011” (onluk san-da – 3) koda eýe bolan simwoly (tekstiň soňuny belgileýän simwol) alýarys. Alnan simwol bilen haýsy-da bolsa „A“ ýa-da „B“ harplaryň biriniň üstünde (meselem „B“ harpyň) XOR amaly gaýtadan geçiril-se, beýleki harp yzyna alynýar:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Tekstiň soňuny belgileýän simwol | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| B harpyň kody | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| XOR amalyndan soň alnan simwol (A harpy) | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |

Görşümüz ýaly „A“ harpyň kody emele geldi. Geliň indi belli bir sözi alyp, onuň her bir harpyny „B“ harpy ulanmak bilen XOR amalyndan geçirmek meselesine garalyň. Amalyň netijesinde emele gelen simwollaryň yzygiderligi şol sözün şifrlenен görnüşi bolup durar. Soňra şifrlenен görnüşi „B“ harpy ulanyp, gaýtadan XOR amalyndan geçirilen ýagdaýynda başdaky söz emele geler. Şeýlelik bilen şifrlеме we şifrden aýyrma amaly şol bir „B“ harpy we XOR amalyny ulanmak arkaly ýerine ýetirilýär.

Indi bolsa bir sözün deregine uly ýazgyny we „B“ harpyň deregine bir sözi (geljekde ol parol diýlip atlandyrylar) kabul edip, XOR amalyny ýerine ýetireliň. Bu ýagdaýda ýazgynyň birinji harpy parolyň birinji harpy bilen bile XOR amalyndan geçer. Ýazgynyň ikinji harpy parolyň ikinji harpy bilen we ş.m. parolyň harp sany yazgydan az bolandygy üçin parolyň iň soňky harpy ulanylandan soň, şifrlеме (XOR amaly) onuň birinji harpyndan dowam etdiriler we ş m. Şifrlenен ýazgydan üstünden öňki paroly ulanmak bilen XOR operatory gaýtadan ulanylan soň bolsa, başdaky ýazgy emele geler. Öňki parolyň deregine başga bir söz ulanylan ýagdaýynda XOR amaly öňki ýazgyny emele getirip bilmez. Bu bolsa şifrlenен ýazgynyň (maglumatyň) dogry şifrden aýrylmagyny gönümel parola bagly edip goýýar hem-de XOR amaly Sezaryň döwründäki şifrlemekden has ýokary derejede goýýar.

Parol näçe uzyn (harplary köp) bolsa, şonça hem şifrlемegiň ygtybarlygy ýokary bolýar.

Umuman aýdanyňda şifrlemek ýokarda aýdylanda ýa-da kodirlemek maglumaty goramagyň örän ýörgünli usullarynyň biridir. Diňe

ýazgy tarapdan bolman, onuň netijesi Assembler dilinde programma görnüşinde ýerine ýetirildi.

Bu ýerde Assembler programmirleme dili barada aýdyp geçmeli. Ýokary derejeli programmirleme dillerinde (Pascal, C, C++, Delphi, Jawa, Visual Basic we başg.) programmalaryň ençemesi ýazylandyr. Sebäbi bu programmirleme diller hünärmene taýyn bölekleri we usullary hödürleýärler, ýagny ulanyjy bilen baglanyşygy maşyn diliniň derejesinde däl-de, has ýokary derejede amala aşyrýar. Bu dillerde ýazylan kompýuter programmalary ýeterlikçe netijeli bolup, deňşdirilende tiz depginde işlenip taýýarlanylýar. Emma hünärmen oňa hödürlenýän taýyn bölekleri we usullary üýtgedip bilmeýär we olar onuň talabyna gabat gelmese programmanyň üstünde işlemegiň başga ýollaryny gözlemeli bolýar. Şeýle hem bu dilde ýazylan programmalar haýal işleýär we olaryň göwrümi (baýtdaky ölçegi) uly bolýar.

Assembler dili bu pes derejeli programmirleme dili bolup durýar. Sebäbi ol maşyn koduna iň golaý bolan pes derejeli baglanyşygy amala aşyrýar. Hünärmen assemblerde islendik bölekleri we usullary özi taýýarlaýar. Şol sebäpli assemblerde taýýarlanan programmalar tiz işleýär we olaryň göwrümi kiçi bolýar.

Programma barada aýdylanda bolsa, ol Assemblerde hem ýazylan bolsa, ulanyja onuň bilen işlemek aňsat we düşnükli bolar ýaly ýeterlikçe köp interfeýs bölekleri özünde jemleýär. Programma goýberilende, programmany ulanmak üçin parol („institut“ sözi) soralýar. Parol dogry girizilenden soň maglumaty şifrlenmeli faýlyň ady talap edilýär. Soňra şifrlenlen maglumaty saklaýan ikinji faýlyň ady soralýar. Mundan soň şifrlenmegiň paroly soralýar (bu paroly programmanyň goýberilişinde talap edilýän paroldan tapawutlandyrmalydyr). Bu parolyň esasynda şifrlenme ýerine ýetirilýär. Soňra programma maglumaty şifrlenýän öňki faýly öwürmegi soraýar. Programma işleýiş döwründe ulanyja onuň girizilen ady boýunça ýüzlenmegi amala aşyrýar.

Şifrleme usuly XOR operatory esasynda amala aşyrylýar. Bu operator iki simwolyň (şifrlenýän ýazgynyň we parolyň simwollary) koduny alýar, olaryň üstünde amal geçirip, ony üýtgedýär we netije-

de başga bir simwol emele gelýär. Başlangyç maglumaty almak üçin gaýtadan şifrlenen faýlyň ady girizilýär we öňki parol ulanylýar we programma tersine başlangyç maglumaty çykarýar.

Bu programmanyň artykmaç tarapy – ol diňe ýazgy faýllary däl-de, eýsem islendik faýllary şifrlemegi amala aşyrýar. Şeýlelik bilen şol faýllary şifrlemekden soň öňki maksatlary boýunça ulanmak mümkin bolmaýar (meselem, ýerine ýetirilmeli faýllary ((*.exe) goýberip bolmaýar, suratlary (*.jpg, *.psd we başg. görmek bolmaýar we ş.m.)).

Programmanyň ýazgysy aşakda getirilýär.

1.5 Dürli görnüşli programmirleme dilleri şifrlemegiň bir meselesiniň çözülişiniň üstünden barlag geçirmek

Programma listingi (shifr5.com)

| | |
|---|--------------|
| .model tiny | endm |
| .code | Start: |
| org 100h | mov ah,00 |
| Begin: | mov al,00 |
| .386 | int 10h |
| jmp start | mov ah,0bh |
| str10 db 20 dup (0) | mov bh,00 |
| db '\$' | mov bl,12 |
| fname db 11 dup (0),0 | int 10h |
| fname1 db 11 dup (0),0 | mov ah,09h |
| str1 db 1 dup (0) | mov bh,00 |
| db '\$' | mov bl,02 |
| b dw ? | int 10h |
| str6 db 8 dup (0) | mov ah,09h |
| str16 db 'Programma | Lea dx,Awtor |
| girmek uchin paroly girizin',10,13,'\$' | int 21h |
| str8 db 13,10,'Shifr- | mov cx,11 |
| leme programmasyna hosh geldi- | mov ah,09h |
| niz! ',10,13,'\$' | |

```

        str9    db    13,10,'Ady-
nyzy girizin',10,13,'$'
        str11   db    13,10,'Onki
fayly ','$'
        str111  db    13,10,'Siz
ochuryanizmi?',10,13,'$'
        str12   db    13,10,'Hawa
(ENTER), Yok (ESC)',10,13,'$'
        str13   db    13,10,'Indiki
seansa chenli ','$'
        str5    db    13,10,'Shi-
frlenjek faylyn adyny giri-
zin',10,13,'$'
        str7    db    13,10,'Shifr-
lenen faylyn ady',10,13,'$'
        str3    db    13,10,'Paroly
girizin',10,13,'$'
        str14   db    13,10,'Islen-
dik dumejige basyn',10,13,'$'
        str4    db    10 dup (0)
        str17   db    13,10,'$'
        m       dw    ?
        Parol   db    'institut'
        Awtor   db    'IMT kafe-
drasy, 2008 yyl.',10,13,'$'
        fhandle dw    0
        fhandle1 dw 0
        x       dw    ?
        msg1    db    'Fayly achyp
bilemok $'
        Zvezda macro
        mov     dl,42
        mov     ah,02h
        int     21h
        je      Loc05
        cmp     al,8
        jne     S01
        inc     cx
        dec     di

```

```

        Lea     dx,str16
        int     21h
        Lea     di,str6

```

Met1:

```

        mov     ah,07h
        int     21h
        cmp     al,13
        je      Met2
        stosb
        Zvezda
        Loop    Met1

```

Met2:

```

        mov     cx,11
        Lea     si,Parol
        Lea     di,str6

```

Met3:

```

        mov     al,byte ptr[di]
        cmp     byte ptr[si],al
        jne     Vyhod
        inc     di
        inc     si
        Loop    Met3

```

Metka:

```

        mov     ah,09h
        Lea     dx,str9
        int     21h
        mov     cx,20
        Lea     di,str10

```

Polzowatel:

```

        mov     ah,01h
        int     21h
        cmp     al,13
        cmp     al,8
        jne     S2
        inc     cx
        dec     di
        jmp     Imya1

```

S2:

```

    jmp     Polzowatel
S01:      stosb
    Loop   Polzowatel
Loc05:    mov     ah,06h
    mov     bh,07h
    mov     cx,0000
    mov     dx,184fh
    int     10h
    mov     ah,02h
    mov     bh,00
    mov     dh,00
    mov     dl,00
    int     10h
    mov     ah,09h
    Lea     dx,str8
int       21h
    mov     ah,09h
    Lea     dx,str10
    int     21h
    mov     cx,12
    mov     b,0
    mov     ah,09h
    Lea     dx,str5
    int     21h
    Lea     di,fname
Imya:    mov     ah,01h
    int     21h
    cmp     al,13
    je      Loc02
    cmp     al,8
    jne     S1
    inc     cx
    dec     di
    jmp     Imya
S1:      stosb

```

```

    stosb
    Loop   Imya1
Loc00:    mov     ah,09h
    Lea     dx,str3
    int     21h
    Lea     di,str4
    mov     cx,10
Loc01:    mov     ah,07h
    int     21h
    cmp     al,13
    je      Program
    cmp     al,8
    jne     S3
    inc     cx
    dec     di
    jmp     Loc01
S3:       stosb
    inc     b
    Zvezda
    Loop   Loc01
Program:  mov     ah,3ch
    mov     cx,00000000b
    mov     dx,offset fname1
    int     21h
    jc      error
mov fhandle1,ax
    mov     ah,3dh
    mov     al,00000000b
    mov     dx,offset fname
    int     21h
    jc      error
mov fhandle,ax
Loc000:

```


| | | | |
|--------------|-----------------|---------|-----------------|
| Loop | Imya | mov | ah,3fh |
| jmp | Loc02 | mov | bx,fhandle |
| Loc02: | | mov | cx,1 |
| mov | ah,09h | mov | dx,offset str1 |
| Lea | dx,str7 | int | 21h |
| int | 21h | push | ax |
| Lea | di,fname1 | | |
| mov | cx,12 | Loc11: | |
| Imya1: | | pop | cx |
| mov | ah,01h | push | cx |
| int | 21h | Lea | bx,str4 |
| cmp | al,13 | Lea | di,str1 |
| je | Loc00 | Lea | dx,str10 |
| | | int | 21h |
| Lupa4: | | mov | ah,09h |
| cmp | byte ptr[bx],0 | Lea | dx,str111 |
| je | Parol_bashy | int | 21h |
| | | mov | ah,09h |
| Lupa1: | | Lea | dx,str12 |
| mov | al,byte ptr[bx] | int | 21h |
| xor | byte ptr[di],al | mov | ah,07h |
| inc | bx | int | 21h |
| jmp | Lupa | cmp | al,27 |
| | | je | finite |
| Parol_bashy: | | mov | ah,41h |
| sub | bx,b | mov | dx,offset fname |
| jmp | Lupa4 | int | 21h |
| | | jc | error |
| Lupa: | | finite: | |
| mov | ah,40h | mov | ah,09h |
| mov | bx,fhandle1 | Lea | dx,str13 |
| pop | cx | int | 21h |
| mov | dx,offset str1 | mov | ah,09h |
| int | 21h | Lea | dx,str10 |
| jc | error | int | 21h |
| cmp | cx,1 | Vyhod: | |
| je | Loc000 | mov | ah,09h |
| exit1: | | Lea | dx,str14 |
| mov | ah,3eh | | |

| | | |
|----------------|-----------|-------------|
| mov bx,fhandle | | int 21h |
| int 21h | | mov ah,07h |
| jc error | | int 21h |
| exit: | | mov ah,4ch |
| mov ah,3eh | | int 21h |
| mov bx,fhandle | error: | |
| int 21h | | mov ah,09h |
| jc error | | lea dx,msg1 |
| mov ah,09h | | int 21h |
| Lea dx,str11 | | jmp finite |
| int 21h | end begin | |
| mov ah,09h | | |

Bölümde programmirleme dilleriniñ işlerini seljermek göz öñünde tutulýar. Ýokarda ýazylyan programmanyñ işini amala aşyryýan programmany Pascal programmirleme dilinde ýazmak meselesi goýulýar.

Aşakda şol programmanyñ programma kody getirilen

Programmanyñ listingi (shifot.exe)

```

Uses Crt;
Var
  fi,
  fo : File of byte;
  ch : Byte;
  j : Byte;
  i : Word;
  pass : string;
Begin
  If ParamCount = 3 Then
    Begin
      Clrscr;
      Assign(fi,ParamStr(1));Reset(fi);
      Assign(fo,ParamStr(2));ReWrite(fo);
      Pass:=ParamStr(3);
      i:=0;
    
```

```

While Not EOF(fi) do
    Begin
        Read(fi,ch); Inc(i);
        For j:=1 to length(pass) do
            ch:=(ch XOR Ord(Pass[j]));
        Write(fo,ch);
        { GotoXY(1,1);
        Write(i,' prosesdaky baytlar');}
    End;
Close(fi);
Close(fo);
End
Else WriteLn('Parametr tapylmady ');
End.
Aşakda biz deňeşdirme tablisany getirýäris:

```

| № | Programmirlleme dili | Programma kody | Maşyn kody |
|----|----------------------|----------------------------|----------------------------|
| 1. | Assembler | Shifr5.asm – 3 964 baýt | Shifr5.com – 940 baýt |
| 2. | Pascal | shifot.pas – 756 baýt | shifot.exe – 5 328 baýt |

Görnüş i ýaly, programma koduny düzmekde Pascal programmirlleme dili belli bir ýeňillikleri berýär. Sebäbi programma kodunyň kiçi bolmagy programma düzüjiden köp wag t talap etmeýär. Şeýle hem, Pascal diliniň birnäçe taýyn funksiýalary hödürleýändig i sebäpli, programma kodunda ýazylan sözler rezerwirlenen, ýagny ulanyjydan ugrukdyryjy usulda programmany düzme gi talap edýär. Bu hem oňa belli bir ýeňillikleri berýär. Assemblerde bolsa rezerwirlenen sözler az, bar hem bolsa olaryň uzynlygy köp derejede 4 simwoldan uzyn bolmaýar.

Şeýlelik bilen, programma kody, Assemblerde düzende programma dörediji ugrukdyrylmadyk köp söz toparlaryny (operatorlary) düzmeli bolýar we ondan has köp “akyl güýji” talap edilýär.

Programmanyň netijesinde bolsa (maşyn kody), düýpgöter başga ýagdaý bolýar. Pascal dilindäki programma kody Assemblerde ýazylan koddan näçe esse kiçi hem bolsa, şonça hem maşyn kodunda on-

dan uly bolýar. Bu örän täsin ýaly bolup görünýär, emma bu ýerde hiç hili üýtgeşik zat ýok.

Şu ýerde Pascal dilinde programma düzmegiň aňsatlygy belli bir derejede öz ýetmezçiliklerini bildirýär. Pascal dilindäki taýyn funksiýalary ulanmak ýeňil, emma olar örän uly huş ölçegine eýe bolýarlar. Sebäbi olar standart görnüşinde ýerine ýetirilen. Assemblerde bolsa köp funksiýalar programma düzüji tarapyndan özbaşdak döredilmeli bolýar we ol diňe gerekli häsiýetli funksiýalary döredýär. Şeýlelik bilen, ahyrky programma huş tutmak meselesinde tygşytly bolýar.

Kriptografiýa maglumat goragynyň örän gadymy usuly hem bolsa, ol öz ähmiýetini häzirki wagtda hem ýitirmeyär. Bu barada has giňişleýin reýestr baradaky bölümde gürrüň ediler.

Kriptografiýanyň häzirki zaman programmirleme bilen aýrylmaz baglanyşygy hem aýdyň. Programmirleme maglumaty şifrlemegi we şifrdan çykarmagy elde edilenden millionlarça esse tiz amala aşyrýar, belli bir derejede bu artykmaçlyk käbir oňaýsyz ýagdaýlara hem getirip bilýär – şifrleri „döwýän“ kriptanaliziň işini hem millionlarça gezek tizleşdirýär. Emma programmirlemegiň gorunda bu kemçilikleri düzetmek boýunça birnäçe serişdeler bar. Olaryň birini biz şu bölümiň çäginde peýdalandyk.

Şeýle hem bu bölümde kriptografiýa usulynyň netijeliligine ony amala aşyrmak üçin haýsy serişdäniň (programmirleme diliniň) alynýandygynyň täsir edýändigine göz ýetirildi. Şifreýji serişde näçe ölçegde kiçi bolsa, şonça hem şifrlenmek tiz amala aşyrylýar, bu diňe kriptografiýany programmirlemegiň kanuny däl-de, tutuş kompýuterdäki programmirlemegiň düzgünidir.

Şeýlelik bilen, programma düzmegiň aňsatlygy hem-de onuň işiniň netijeliligi we tizligi arasynda belli bir ortalyk ýagdaýa gelmek zerur. Netijeli we tiz programmany Assembler dilinde döretmek üçin 1-2 gün gerek bolmagy mümkin. Edil şol işi ýerine ýetirýän, emma biraz haýal işleýän we ölçegi uly bolan programmany, meselem, Pascal dilinde döretmek üçin 1-2 sagat gerek bolmagy mümkin. Şonuň üçin şu bölümiň netijeleri boýunça programmirleme dillerinde utgaşdyryp işlemek gerek, ýagny bir programmirleme diliniň koduny beýlekide ulanmak gerek.

Tejribe işleri

1. Simwollaryň ASCII koduny 8 baha artdyrmak bilen görkezilen teksti şifrlemek we şifrden çykarmak.
 2. Logiki operatorlary peýdalanyň şifrleýji programmalary döretmek.
 3. XOR logiki operatoryň kömegi bilen şifrleýji programmalary Pascal we C programmirleme dillerinde döredip, olary seljermeli.
 4. Şifremegiň usullaryny programmirleme dilinde amala aşyrmak arkaly seljermeli.
 5. Şifrlenlen faýly seljerýän ýönekeý programmany düzmeli.
-

II. DISKIŇ LOGIKI GURLUŞY HEM-DE MAGLUMATLARY GIZLEMEK

1. Diskiň logiki gurluşyny seljermek.
2. Faýllaryň diskde ýerleşişiniň düzgünini ulanmak arkaly maglumaty gizlemegiň mümkinçiligine baha bermek.
3. Maglumaty gizlemek üçin Assemblerde programma düzmek.

Maglumatlaryň goragy hemme wagt we islendik ugurda möhüm meseleleriň biri bolup durýar. Başga biriniň elýeterliginden ýa-da islenmeýän täsirden maglumaty goramak pikiri örän gadymy döwürde döräpdi. Jemgyýetiň ösüşi bilen, hususy eýeçiligiň, döwlet gurluşynyň, häkimiýet üçin göreşiň döremegi we soňra adamyň iş geriminiň ölçegleriniň giňelmegi bilen maglumat uly gymmata eýe bolýar. Özem diňe, şol wagtky ýa-da bolup biljek eýesine maddy, ylmy, syýasy, harby we ş.m. peýda getirip biljek maglumat has gymmatly bolup biler. Şol sebäpli adam gadymy döwürlerden bari maglumaty goramagyň üstünde işläp gelipdir. Her döwürde maglumatlary goramaklyk belli bir usul arkaly amala aşyrylyp, biziň döwrümize çenli olaryň birnäçesi gelip ýetipdir.

Maglumaty ýönekeý göterijileriň bolan döwründe, onuň goragy gurama usullar arkaly amala aşyrylyp, olar – elýeterligiň çaklandirilmegini, syryň aýdyňlaşdyrylany üçin belli jezanyň görülmegini göz önünde tutýardy. Wagtyň geçmegi bilen maglumat goralýşy kem-kemden kämilleşýär.

Gerodotyň aýtmagyna görä, eýýäm biziň eramyza çenli V asyrdan maglumaty kodirleme arkaly özgertmek ulanylýardy. Kodlar gadymy eýýamlarda kriptogramma görnüşinde emele gelipdir (grek dili boýunça – syr ýazgy). Spartanlylar ýörite mehaniki enjama eýediler, ol arkaly wajyp maglumatlary syryň bitewiligini üpjün edip ýöriteleýin ýazyp bolýardy. Hususy gizlin sözlük Ýuliý Sezarda hem bardy. Orta asyrlarda gizlin şifrleriň üstünde beýik şahslar hem işläpdir, olaryň içinde belli filosof Frensis Bekon, güýçli matematikler – Fransua Wiýet, Jerolamo Kardano, Jon Wallis dagylaryň bardygyny bellemelidir.

2.1. Diskiň logiki gurluşyny seljermek

EHM-leriň we ondan soňra bolsa kompýuterleriň döremegi adamyň durmuşyna düýpgöter täsir etdi. Maglumatyň saklanylmagy, görtermegi, iberilmegi, kodirlenmegi, okalmagy üýtgedi. Maglumatyň alyş-çalşygy tizlendi, maglumaty goramagyň mümkinçilikleri hem artdy. Tehnika näçe ösen hem bolsa, şonça hem onuň howplulygy galýar.

Ýokary hilli, gowy işleýän ulgam maglumatyň has üstünlikli ogurlanmagyna ýardam edip bilýär. Bu dürli sebäplere bagly bolup bilýär, emma, köplenç muňa goraýyş usulynyň ýetmezçiligi sebäp bolup durýar. Kodirleme we şifrleme, parol ulgamy, maglumat bilen işlemek boýunça çäklendirmeler – bularyň hemmesi häzirki wagtda giňden ulanylýar we olaryň netijeliligi belli bir derejede ony döredijileriň ussatlylyklaryna bagly bolup durýar.

Geliň indi maglumaty goramagyň başga usulyna seredeliň. Ýokzady (şol sanda maglumaty) ogurlap bolmaýar. Görünmeýän maglumat belli bir derejede ýok ýaly bolýar. Düşünşiňiz ýaly, biz maglumaty gizlemeklik barada gürrüň ederis.

Ilki maglumaty saklamagyň, ýazmagyň, okamagyň düzgünleri barada aýdyp geçmeli.

Kompýuter maglumaty – kompýuter huşunyň böleginde saklanylýar, ol faýl ýa-da bukja görnüşinde bolup biler. Faýllar kompýuteriň gaty diskinde ýa-da daşky maglumat ýygnaýjylarda (kompakt disklerde, flash huşda, çeýe magnit disklerde we başg.) ýerleşdirilip bilner.

Islendik maglumat ýygnaýjylarynda faýllaryň ýerleşmeginiň belli bir düzgüni bar. Şol düzgüni biz iň ýönekeý mysalda, çeýe magnit diskiň, ýagny 3,5 dýuým disketanyň içinde faýllaryň ýerleşmeginde göz ýetireliň. Ilki bilen belläp geçmeli zat, hemme çeýe magnit disketalarynda faýllary ýerleşdirmegiň FAT tablisasy ulanylýar.

Disketanyň üsti ýörite magnit gatlagy bilen örtülýär, maglumat ýazylýar we saklanylýar. Maglumat diskiň iki tarapyndan ýoljagazlar boýunça ýazylýar, şol ýoljagazlar tegelek görnüşde bolýar. Her

ýoljagaz sektora bölünýär. Her sektora bolsa baýtlaryň belli bir mukdary sygýar. Ol 512 baýta deň. Bilşimiz ýaly, bir baýt bu maglumatyň birligidir, ol bir simwoly (harpy, sany, beýleki dolandyryş belgileri) kesgitleýär.

Ýoljagazlaryň, sektorlaryň sanyny we sektoryň baýtdaky ölçegini bilip, çeyde diskiň göwrümini hasaplamak mümkin. Diskiň sektorlarynyň sany umumy görnüşde

$$\text{Sector_sany} = T * N * M$$

formula bilen hasaplanylýp bilner. Bu ýerde T-diskiň taraplarynyň sany; N – ýodajyklaryň sany, M – her bir ýodajykdaky sektorlaryň sany. Magnit diskleriň ýodajyklary MS-DOS, WINDOWS operasi-on ulgamlarynda işlänlende radiuslarynyň dürlüligine garamazdan, birmeňzeş sektorlary özlerinde saklaýarlar. Netijede diskde saklanylýp bilinjek maglumatlaryň mukdary

$$V = \text{Sector_sany} * 512$$

bu ýerde V – diskiň göwrümi. Biziň seredyňan 3,5 düýümlyk disketimiz üçin $T=2$, $N=80$, $M=18$.

$V = 2 * 80 * 18 * 512 = 1474560$ baýt = 1,44 Mbaýt (1Mbaýt = 1024Kbaýt, 1Kbaýt = 1024 baýt).

Diýmek, bir disketada 2880 sektor ýerleşýär. Bir sorag ýüze çykýar – şol sektorlaryň hemmesinde faýllar ýerleşýärmikä? Muňa jogap bermek üçin şulary bellemek gerek.

Diskdäki huşuň faýllar üçin paýlanmagynyň düzgünleri bar. Olaryň biri FAT (File Allocation Table) – faýllaryň tertipleniş tablisasy. Şol tablisa boýunça disketanyň:

- 0-njy sektory – ýükleniş sektor (boot sector);
- 1-18-nji sektorlary – dolandyryjy sektorlar (FAT);
- 19-32-nji sektorlary – bu diskdäki faýllaryň we bukjalaryň atlarynyň ýerleşýän sektorlary (diskiň mazmuny);
- 33-2879-njy sektorlary – maglumatyň (faýllaryň düzüminiň) ýerleşmegi üçin niýetlenen sektorlar [9].

Jemi 0-njy sektordan 2879-njy sektora çenli 2880 sektor bar.

2.2. Faýllaryň diskde ýerleşişiniň düzgünini ulanmak arkaly maglumaty gizlemegiň mümkinçiligine baha bermek

Diýmek, faýlyň ady bilen onuň saklaýan maglumaty aýry sektorlarda ýerleşýär. Geliň indi bir zada göz ýetireliň – eger disketadaky faýlyň adyny degişli sektordan aýryp, ony wagtlaýyn disketanyň başga sektorlaryna (meselem, soňky boş sektorlara) ýerleşdirsek, şol faýl disketanyň faýllarynyň hatarynda görnermikä? Ýok görünmez. Disketanyň huşunyň boş ýeriniň ölçegi hem şol faýlyň maglumatyny hasaba alman görkeziler. Faýl ýok edilen ýaly bolar. Emma disketanyň düzüminde onuň maglumaty saklanylýar. Eger faýlyň ady ýene öňki ýerine getirip ýerleşdirilse, onda şol faýl disketanyň düzüminde gaýtadan görner.

Ýokarda aýdylanlary göz önünde tutup, esasy maglumatyň (mümkin bolan ogryny gyzyklandyryp biljek maglumatyň) 33-2879-njy sektorlarda ýerleşdirilýändigine göz ýetirmek kyn däl. Şol maglumata degmän, disketanyň ilkinji 33 sektoryny (0-32-nji sektorlary) göçürüp, soňra ýok edip, disketada adatça boş bolýan soňky 33 sektora (2847-2789-nji sektorlara) ýazyp goýulsa, disketanyň içindäki faýllar we bukjalar görünmez. Disketanyň boş meýdany hem onuň doly ölçegine deň bolar – disketa edil formatirlenip, doly boş ýaly bolar.

Emma onuň içindäki maglumatlar hakykatdan hem bar bolsa we disketanyň soňuna ýazylan baýtlar gaýtadan öz 0-32-nji sektorlaryna ýazylsa, disketanyň faýl düzümi öňki ýagdaýa geler hem-de maglumatlaryň bitewidigine we ýok edilmändigine göz ýetirmek bolar.

Ýokarda görkezilen amallary ýerine ýetirmek üçin programmirleme dilinde programmany ýazmak mümkin. Amallar maşyn diliniň pes derejesinde ýerine ýetirilýändigini üçin programmany Assembler dilinde ýazmak amatly bolýar.

Programma disketadaky tutuş maglumaty (faýllary we bukjalary) gizleýär, maglumat gizlenenden soň programma ýene bir gezek goýberilen ýagdaýynda şol gizlenen maglumatlar gaýtadan görkezilýär. Maglumatyň gizlenendigini ýa-da görkezilýändigini kesgitlemek

üçin faýllaryň we bukjalaryň atlaryny saklaýan 19-njy sektoryň ilkinji baýty barlanylýar. Eger ol nola deň bolsa – diýmek, ilkinji 33 sektorlar göçürilip, boşadylypdyr we olary disketanyň soňundan öňki ýerine göçürmek gerek bolýar, eger nola deň bolmasa, onda gizleme amalyňy ýerine ýetirmeli bolýar.

Programmanyň ulanylyşy örän ýönekeý. Maglumat gizlenilmeli disketa degişli diskowoda goýulýar we programma goýberilýär. Netijede, disketanyň içi boş görkezilýär we özge adam özi üçin disketanyň içinde hiç hili peýdaly maglumaty tapmaýar. Maglumaty görmek üçin şol disketa diskowodda duran mahaly täzedan şol programma goýberilýär.

2.3. Maglumaty gizlemek üçin Assemblerde programma düzmek

Aşakda şol programmanyň doly ýazgysy getirilýär [10].

```
*****
;
;                               DISKHIDE.ASM                               ;
; A-diskdäki ilkinji 0-32 sektorlary in soňky 2847-2879 sektor-      ;
; lara ýazýar we başdaky 1-32 sektorlary nullaýar hem-de diskiň    ;
; label-ini bozýar (Label 0-sektoryň 2bh baýtyndan başlap 11      ;
; baýt tutýar).                                                    ;
; Eger-de 19-njy sektoryň ilkinji baýty 00 bolsa, onda 2847-2879    ;
; sektorlary 0-32 sektorlara ýazýar.   14.05.2008(3)                ;
*****
```

CODESG SEGMENT

ASSUME CS:CODESG

ORG 100H

START: JMP MAIN

;-----;

insert db 33 dup(512 dup('?'))

habar db '-----',10,13

db 'IMT kafedrası',10,13

db 'Orazberdi Nurgeldiyew',10,13

```

db 'Maksat Çürüyew',10,13
db '20.12.2003',10,13
db 'Version 1.0',10,13
db '-----'
db '$'

```

```

;-----;
.386 ;

```

```

MAIN PROC NEAR

```

```

    mov     ah,09
    lea     dx,habar
    int     21h
    mov     al,00 ; Diskowodyň nomeri(00-A, 01-B, 02-C)
    lea     bx,insert ; Okalan sektorlary saklamak üçin bufer
    mov     cx,01 ; Okalmaly sektorlaryň sany
    mov     dx,19 ; Başlangyç sektoryň sany
    int     25h ; Logiki sektory okamak

```

```

cmp     insert[0],00
je      ikinji

```

```

    mov     al,00
    lea     bx,insert
    mov     cx,33
    mov     dx,00
    int     25h

```

```

    mov     al,00
    lea     bx,insert
    mov     cx,33
    mov     dx,2847
    int     26h ; Logiki sektory ýazmak

```

```

    mov     cx,33*512
    mov     si,00
m1:
    mov     insert[si],00

```

```

inc     si
loop    m1
mov     al,00
lea     bx,insert
mov     cx,32
mov dx,01
int     26h
mov     al,00
lea     bx,insert
mov     cx,01
mov     dx,00
int     25h
mov     insert[2bh+0],4eh
mov     insert[2bh+1],4fh
mov     insert[2bh+2],20h
mov     insert[2bh+3],4eh
mov     insert[2bh+4],41h
mov     insert[2bh+5],4dh
mov     insert[2bh+6],45h
mov     insert[2bh+7],20h
mov     insert[2bh+8],20h
mov     insert[2bh+9],20h
mov     insert[2bh+10],20h
mov     al,00
lea     bx,insert
mov     cx,01
mov     dx,00
int     26h
jmp     tamam

```

ikinci:

```

mov al,00
lea bx,insert
mov cx,33
mov dx,2847
int 25h

```

```

        mov    al,00
        lea    bx,insert
        mov    cx,33
mov dx,00
        int    26h      ; Logiki sektory ýazmak
tamam:
        MOVAH,4CH
        INT    21H
MAIN ENDP
;-----;
;-----;
CODESG  ENDS
        END START

```

Bu programma 3,5 düýmlyk magnit diskleri üçin taýýarlanyldy. Bu programmadaky ululyklaryň bahalaryny üýtgetmek bilen, ony islendik diskler üçin hem ulanmak bolar.

Bu bölümde maglumatlaryň gizlenmegine ony goramak hökmünde seredildi.

Dogrudan hem, görünmeýän maglumat barada ýörite habary bolmadyk adam ony ogurlamaga çalyşmaz, bu bolsa ygtybarly goraglaryň biridir. Bu usul amala aşyrylanda Assembler programmirleme diliniň ulanylmagy bolsa, Assembler diliniň häzirki wagtda hem ileri tutulmagynyň alamaty bolýar.

Assembler dili diňe bir ýöne programmirmek taýdan däl, eýsem barlag işlerini geçirmek üçin hem örän wajyp serişdeleriň biri bolup durýar. Sebäbi ol hasaplaýyş ulgamynda bolup geçýän prosesleri obýektiw ýagdaýda derňemegi mümkin edýär.

Tejribe işleri

1. FAT düzgünini peýdalanyň flesh ýadynyň içindäki faýllary gizleýän we görkezýän programmany döretmeli.
2. NTFS düzgüninde faýllaryň ýatda ýerleşişini özbaşdak seljermeli.

III. PAROL GORAGYNYŇ KÄBIR MESELELERI

1. Parol simwollarynyň yzygiderligi.
2. Parol yzygiderligini barlap döwmegiň esaslary.
3. Paroly döwmekligi programmirlеме arkaly gurnamagyň häzirkі zaman meseleleri.
4. Programmirlеме dilleriniň deňeşdirilişi.
5. Paroly döwmeklige garşy usullary düzmek.
6. Parolyň döwürmeginiň önüni alýan programma kody.

Bilşimiz ýaly, häzirkі zaman goragynyň aglaba bölegi parol esasynda amala aşyrylýar. Bu usul gadymy usullaryň biridir. Ol gulp ýaly işleýär. Nädogry açar girizilende gulp açylmaýar. Şol açar köplenç simwollaryň (harplaryň, sanlaryň, nyşanlaryň) yzygiderliginden ybarat. Harplar barada gürrüň edilende – bir açarda dürli dilleriň harplaryny ulanmak bolýar.

Häzirkі wagtda tehnologiýalaryň ösmegi parol goragyny kämilleşdirmeklige uly mümkinçilikleri döredýär, emma, belli bir derejede, parol goragynyň döwürmegine howplaryň hem artmagy gaty ähtimaldyr. Hakykatda, häzirkі wagtda parol goragy meselesinde, paroly döwmek bilen meşgullanýan adamlarda has köp mümkinçilikler bar. Bu şular bilen düşündirilýär:

I. Gadymy döwürlerde gulpy açmak üçin dogry açary ýa-da onuň göçürmesini ulanypdyrlar. Häzirkі zaman parol goragy köp derejede kompýuter tehnologiýasynyň meseleleri bilen bagly. Köplenç parol goragynyň ulanylmagyny biz aşakdaky ýagdaýlarda görýäris:

- a) kompýuteriň fiziki ulgamyna girmek üçin (SETUP BIOS);
- b) windows ýa-da başga amallar ulgamyna girilende;
- ç) amaly programmalara ýa-da Internede girilende;
- d) dürli programmalarda paroly çalşyrylanda;
- e) käbir başga ýagdaýlarda.

Görşümüz ýaly, parol goragy köplenç programma derejesinde amala aşyrylan. Şol sebäpli onuň açylmagy (döwürmegi) hem amaly programmalar arkaly amala aşyrylýar.

3.1. Parol simwollarynyň yzygiderligi

Amaly programmalar arkaly döwmegiň ýönekeý usuly – adaty ýagdaýda açaryň (parolyň) simwollaryny yzygiderli tertipleşdirip gulpa (paroly sorayan programma) goýup barlamak – parolyň simwollaryny toplaşdyrmak usuly (метод перебора символов пароля).

Meselem, „maksat“ parolyny döwmek üçin yzygiderli aşakdaky 6 simwoldan ybarat bolan harplaryň yzygiderligini dowam etdirmeli:

- | | |
|--------------|--------------|
| 1. „aaaaaa“ | 26. „aaaaaz“ |
| 2. „aaaaab“ | 27. „aaaaba“ |
| 3. „aaaaac“ | 28. „aaaabb“ |
| | 29. „aaaabc“ |
| | |
| 52. „aaaabz“ | ... „abaaaa“ |
| 53. „aaaaca“ | |
| 54. „aaaacb“ | ... „baaaaa“ |
| 55. „aaaacc“ | |
| | ... „maaaaa“ |
| 78. „aaaacz“ | |
| | ... „makaaa“ |
| ... „aaabaa“ | ... „maksaa“ |
| | |
| ... „aabaaa“ | ... „maksat“ |

Ýokarky mysaldan görşümüz ýaly, parolyň yzygiderligi ilkibaşda elipbiýiň ilkinji harpynyň düzüminden (aaaaaa) başlanýar we yzygiderligiň iň ahyrky (altynjy) harpy elipbiý tertibinde üýtgeýär (a,b,c,...,z). Soňky 6-njy orundaky harp elipbiý tertibinde doly üýtgäninden soň, 5-nji orundaky harp elipbiý tertibinde üýtgäp başlaýar – ýöne 5-nji harpyň her bir çalşyrylmazyndan öň, 6-njy orundaky harplar doly elipbiý tertibinde üýtgemeginiň gaýtalanyşyny amala aşyrýar.

Mundan beýläk 4-nji orundaky, soňra 3-nji orundaky, 2-nji orundaky, 1-nji orundaky harplar tä 1-nji orunda „m“ harpyna ýetilýänçä çalşyrylýar. Soňra „maaaaa“, ..., „makaaa“, ..., „maksaa“, ..., yzygiderligi tä „maksat“ tapylýançä dowam etdirilýär.

Geliň indi şu ýerde „maksat“ açaryny tapmak üçin simwollaryň yzygiderliginiň näçe sanysynyň gerekdigini seljereliň. Munuň üçin belli bir derejede matematiki hasaplamalary ýerine ýetirmek zerur bolar.

Ilkibaşda meseläni aňsatlaşdyralyň.

a) Goý, bize 6 sany simwoldan ybarat bolan parol berlen bolsun. Simwollar 0,1,2,3,4,5,6,7,8,9 bolup bilýär, ýagny sanlardan ybarat. Parolyň mümkin bolan yzygiderliginiň sanyny kesgitlemeli.

Bu ýagdaýda parolyň yzygiderliligi aşakdaky ýagdaýda bolar:

| | |
|---------------|-------------------|
| 1. „000000“ | |
| 2. „000001“ | 1000. „000999“ |
| 3. „000002“ | |
| 4. „000003“ | 10000. „009999“ |
| | |
| 10. „000009“ | 100000. „099999“ |
| | |
| 100. „000099“ | 1000000. „999999“ |

Netijede, diňe sanlardan ybarat bolan 6 simwolly yzygiderliligiň 1000000 sanysy bolup biljekdigi görünýär.

Indiki hasaplamalarymyzy aňsatlaşdyrmak üçin biz belli bir formulamyzy girizeliň.

Eger parolyň simwoly bolup biljekleriň sanyny x bilen, parolyň uzynlygyny bolsa (parol yzygiderligindäki simwollaryň sany) y bilen belgilesek, aşakdakylary beýan etmek mümkin:

$$x = 10 \text{ (0,1,2,3,4,5,6,7,8,9)}$$

$$y = 6 \text{ (parol = xxxxxx)}$$

$$N = x^y \quad (1)$$

bu ýerde, N – parol bolup biljek 6 simwoldan ybarat yzygiderliligiň sany

Şeýlelik bilen, meselämiziň çözgüdi $N = 10^6 = 1000000$ [11];

b) “maksat” paroly ýagdaýynda mesele çylşyrymlaşýar, biz bu ýerde sanlar bilen däl-de latyn (iňlis) elipbiýi bilen iş salyşýarys. Bilşimiz ýaly, iňlis dilinde 26 harp bar, şeýlelik-de (1) formulany ulanmak bilen:

$$x = 26$$

$$y = 6$$

$$N = 26^6 = 308915776.$$

Netijede, 308915776 sany mümkin bolan parol yzygiderligini alýarys, ýagny “aaaaaa” bilen “zzzzzz” yzygiderligiň çäginde 308915776 sany ýazgy bar. Şolaryň arasynda hem biziň parolymyz – “maksat”.

Indi bolsa “maksat” ýazgynyň “aaaaaa” – “zzzzzz” çäginde haýsy orunda ýerleşýändigini anyklalyň, sebäbi hemme yzygiderliligi barlamak zerur däl – barlag diňe parol anyklanýança dowam etdiriler.

Parolymyzyň 6 harpdan ybaratdygy sebäpli “maksat” sözünüň ornuny kesgitlemek üçin aşakdaky hasaplamalary ýerine ýetireliň:

Onluk san ulgamyndan bilşimiz ýaly:

$$999999 = 9 \cdot 10^5 + 9 \cdot 10^4 + 9 \cdot 10^3 + 9 \cdot 10^2 + 9 \cdot 10^1 + 9.$$

Biziň ýagdaýymyzda iňlis elipbiýi 26 harpdan ybarat şol sebäpli aşakdakyny ýazmak bolar:

$$n(\text{maksat}) = n(m) \cdot 26^5 + n(a) \cdot 26^4 + n(k) \cdot 26^3 + n(s) \cdot 26^2 + n(a) \cdot 26^1 + n(t), \quad (2)$$

bu ýerde $n()$ – belli bir simwolyň elipbiýdäki tertip belgisi, özem a – elipbiýiň 0-njy elementi bolup durýar, şeýlelik bilen:

$$n(m) = 12, n(a) = 0, n(k) = 10, n(s) = 18, n(t) = 19$$

(2) formulany ulanmak bilen alýarys:

$$\begin{aligned} & 12 \cdot 26^5 + 0 \cdot 26^4 + 10 \cdot 26^3 + 0 \cdot 26^2 + 18 \cdot 26^1 + 19 = \\ & = 142576512 + 175760 + 468 + 19 = 142752759. \end{aligned}$$

Netijede, “maksat” ýazgysy umumy yzygiderlikde 142752759-njy bolup durýar.

3.2. Parol yzygiderligini barlap döwmekligiň esaslary

Geliň indi kompýuter arkaly şol yzygiderlikleri barlamak üçin programmanyň koduny taýýarlalyň:

procedure TForm1.Button1Click(Sender: TObject);

```
label 1;
var
  str:array [1..6] of char;
  i,i1,i2,i3,i4,i5,i6:integer;
  t:word;
  j:longint;
Present: TDateTime;
Year, Month, Day, Hour, Min, Sec, MSec: Word;
```

```
begin
  Present:= Now;
  DecodeTime(Present,Hour, Min, Sec, Msec);
  t:=Min*60+Sec;
  for i1:=97 to 122 do
```

```
  begin
    str[1]:=chr(i1);
    for i2:=97 to 122 do
```

```
      begin
        str[2]:=chr(i2);
        for i3:=97 to 122 do
```

```
          begin
            str[3]:=chr(i3);
            for i4:=97 to 122 do
              begin
                str[4]:=chr(i4);
                for i5:=97 to 122 do
```

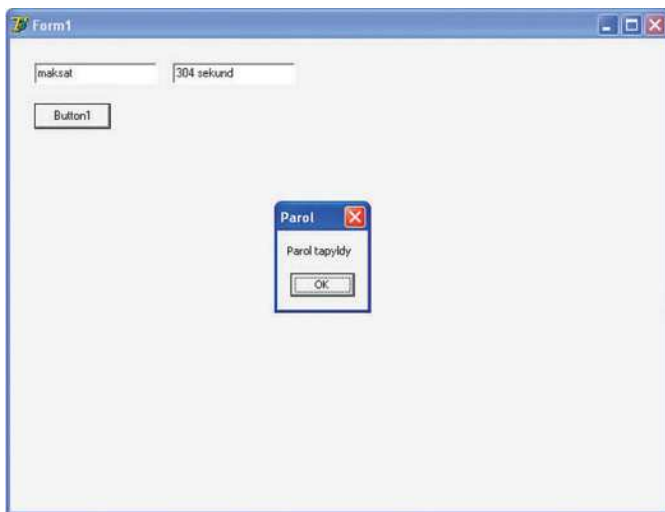
```
                  begin
                    str[5]:=chr(i5);
                    for i6:=97 to 122 do
                      begin
                        str[6]:=chr(i6);
```

```

if (str=edit2.Text) then
begin
Present:= Now;
DecodeTime(Present,Hour, Min, Sec, Msec);
edit2.Text:=inttostr(Min*60+Sec-t)+' sekund';
Edit1.Text:=str;
showmessage('Parol tapylady');
Goto 1;
end;
end;
end;
end;
end;
end;
1:
end;

```

Ýokarda görkezilen programmanyň kody iňlis elipbiýiniň kiçi harplarynyň 6 mukdarda doly gaýtalanmagyny (“aaaaaa”-dan “zz-zzzz” çenli) amala aşyrýar. Edit2.text komponentde parol ýazylýar



3.1-nji surat. Paroly deňeşdirip anyklamak

(meselem „maksat“), soňra Button1 düwmejige basylýar (ýokarda görkezilen programma – onuň basylmagynyň prosedurasynyň kody) we barlagda parolyň üstünden barlan ýagdaýynda bu barada habar berilýär. Barlagyň wagty görkezilýär hem-de Edit1 komponentde tapylan parol görkezilýär (3.1-nji surat).

Görşümüz ýaly, gerek bolan sözi tapmak üçin 304 sekunt gerek boldy. Indi gözlegiň birligini kesgitlemek boýunça hasaplamalary geçireliň.

3) Iki özenli prosessorly (her özeniň ýygylgy 2Gh), işjeň huşy 2Gb bolan kompýuter arkaly iňlis dili elipbiýiniň kiçi harplaryndan ybarat bolan 6 harplyk zygiderliliginiň 10 000 000, 20 000 000, 30 000 000 sany toplumlarynyň näçe wagtda kesgitlenýändigini anyklamaly;

Görkezilen kompýuterde programma arkaly goýberilen barlamalaryň netijesinde aşakdaky netijeleri alýarys:

10 000 000 – 7, 12, 12, 12, 12, 12, 13, 12, 12, 12 sek

20 000 000 – 26, 33, 33, 33, 33, 33, 34, 33, 33, 33 sek

30 000 000 – 54, 55, 55, 55, 55, 54, 55, 54, 55, 55 sek

Ýokarkylara göz ýetirmek bilen aşakdaky netijeleri çykarmak bolýar:

a) Her toplumu kesgitlemek üçin 10 sany tejribe geçirildi. Olaryň deň dældigine göz ýetirmek mümkin, meselem 10 000 000 sany zygiderligiň tejribesinde ilkinji synagda 7 sekunt, galan ýagdaýlarda bolsa 12 we 13 sekunt wagt gerek boldy. Bu uly aratapawudy şol wagt kompýuteriň başga meseleler bilen işleýändigi sebäpli düşündürmek bolýar. Dürli wagtda kompýuteriň kuwwaty meseleler üçin deň paýlanmaýar. Birinji synagda kompýuter birneme „boş“, ýagny kän bir ýüklenmedik ýagdaýda bolansoň, 10 000 000 sany zygiderlilik 7 sekuntda barlanyldy. Şol ýagdaý 20 000 000 toplum üçin hem gäytalandy – başda 26 sekunt, soňra bolsa 33 we 34 sekunt (ilkibaşda 1 gezek 10 000 000 toplum, soňra 20 000 000 toplum barlanyldy, indiki synaglar bolsa bir toplumyň içinde doly geçirilip, soň indiki toplumda amala aşyryldy).

b) 10 000 000 zygiderliliği barlamagyň wagtynyň iki esseligi 20 000 000 zygiderliliği barlamagyň wagtyna deň däl (12+12 sek. we

33 sek.), bu bolsa kompýuter tarapyndan yzygiderlikleri barlanmagyň dowamynda onuň kuwwatynyň peselmegi bolup geçýär (ol hem 10 000 000 we 20 000 000 toplumlarynyň wagtynyň goşulyp 30 000 000 wagty bilen deňeşdirilende hem görünýär 12+33 sek we 55 sek.), bu bolsa barlagyň hemişe bir depginde alnyp barylmaýandygyny aňladýar.

Ýokardakylary seljermek bilen, belli bir anyk barlagyň birligini kesgitlemek (meselem, 1 sekuntda näçe yzygiderligiň barlanýandygyny) mümkin däl, munuň üçin birnäçe synaglary geçirmek zerur, özem diňe bir kompýuterde däl-de, biri-birinden tapawutlanýan kompýuterlerde.

3-nji mysalda görkezilen kompýuterimizde 142752759-njy orunda duran „maksat“ sözüni kesgitlemek üçin 304 sekunt gerek, diýmek şol kompýuterde 1 sekuntda ortaça $142752759/304=469581$ sany yzygiderlilik barlanylýp bilinýär.

Geliň şol kompýuterde tutuş „aaaaaa“ – „zzzzzz“ yzygiderliligini doly barlap çykalyň. Netijede, 308915776 sany yzygiderligi barlap çykamak üçin 659 sekunt gerek bolýar, diýmek bu ýagdaýda 1 sekuntda ortaça $308915776/659=468765$ sany yzygiderlilik barlanylýar.

Mundan ýokarky mysal bilen deňeşdirenimizde tapawudy kän bir uly däl. Emma ol maşyn ulgamy üçin şeýledir, adam üçin 900-e golaý yzygiderligi elde barlamak üçin birnäçe sagat gerek bolýar.

Ýokarda aýdyşymyz ýaly, wagt birliginde maşyn tarapyndan ulgamyň yzygiderlikleri barlamagyň sanyny kesgitlemäge dogry baha bermek üçin tejribäni birnäçe maşynda ýerine ýetirmek zerur.

4. Bir özenli prosessorly (ýygylgy 2,8Gh), işjeň huşy 256Mb bolan DELL firmasynyň kompýuteri arkaly iňlis dili elipbiýiniň kiçi harplaryndan ybarat bolan 6 harplyk yzygiderliliginiň „maksat“ sözüne çenli barlamagyň wagtyny kesgitlemeli.

Barlagyň netijesinde programma 753 sekunt görkezdi, diýmek 1 sekuntda ortaça $142752759/753=189579$ sany yzygiderlilik barlanylýar, 3-nji mysaldaky kompýuteriň netijeleri bilen deňeşdirilende örän uly tapawudy berýär.

5. Iki özenli prosessorly (her özeniň ýygylgy 3,16Gh), işjeň huşy 4Gb bolan kompýuter arkaly iňlis dili elipbiýiniň kiçi harp-

laryndan ybarat bolan 6 harplyk yzygiderliliginiň „maksat“ sözüne çenli barlamagyň wagtyny kesgitlemeli:

Barlagyň netijesinde programma 189 sekunt görkezdi, diýmek 1 sekuntda ortaça $142752759/189=755306$ sany yzygiderlilik barlanylýar. Bu netije örän ýokary. Adam üçin bu tizligi göz önüne getirmek örän kyn. Bir sekundyň dowamynda 755306 söz barlanyp geçilýär şol sözleriň barlagyny ekranda görmek mümkin däl.

Şu ýerde bir zada üns bermek gerek, sebäbi barlagyň dowamynda ýene bir täsin netije çykaryldy. Harp yzygiderlikleriniň barlagy ekrana çykaryp amala aşyrylanda örän pes netijeler berildi, meselem „arslan“ sözüni, ondan öňki duran hemme yzygiderlikleri ekranda görkezip barlag geçirilende 207 sekunt wagt görkezildi, emma ekranda görkezmän barlag geçirilende 17 sekunt wagt görkezildi (barlaglar 3-nji mysaldaky kompýuterde geçirildi).

Şol sebäpli hemme ýokarda görkezilen barlaglar, barlanylýan yzygiderlikleri ekranda görkezilmän amala aşyryldy, şol sebäpli hem ýokary netijeler alyndy.

Indiki hasaplamalara geçmezden ön parol barlamagyň usullarynyň aşakdaky meselelerine göz ýetireliň:

a) parol döwüjiler elmydama örän kuwwatly kompýuterleri ulanýar;

b) parolyň barlagy kompýuteriň in kuwwatly ýagdaýynda, ýagny hiç bir başga meseleler goýberilmän amala aşyrylýar (köplenç kompýuter ýaňy işledilen mahalyndan uzak wagtda däl), ýagny 3-nji mysalda 10 000 000 sany yzygiderlilik barlanylanda 7 sekunt, diýmek şol ýagdaýda 1 sekuntda ortaça $10000000/7=1\,428\,571$ yzygiderlilik barlanylýar, bu bolsa 5-nji mysaldaky kuwwatly kompýuteriň netijesinden hem ýokary;

c) paroly barlamak üçin sözlükler peýdalanylýar. Köplenç parol goýýan adamlar harp yzygiderligi däl-de, taýyn sözi ulanýarlar, meselem adyny, ýa-da başga bir durmuşda ulanýan sözüni, olar bolsa sözlüklerde saklanylmagy mümkin. Umuman, her diliň sözlüğünde 100 000 golaý söz bar. Kompýuteriň kuwwatyny hasaba almak bilen dünýädäki hemme sözlükleri barlamak üçin kompýuter üçin 1 minutdan hem az wagt gerek. Şol sebäpli parolyň tiz wagtda tapylmagynyň önüni almak üçin bu sözleri ulanmaklyk teklipe edilmeýär;

d) Házirki wagtda birnäçe özenli kompýuterleriň ulanylmagy hasaplamalary yzygiderli däl-de, parallel amala aşyrmagy mümkin edýär. Meselem, yzygiderlikleriň barlagyny diňe başdan däl-de, şol bir wagtda yzdan başa çenli, ortadan başa we yza amala aşyrmagy mümkin edýär, ýagny parol yzygiderligiň soňunda ýerleşen bolsa, meselem „wwwwww“, oňa başdan ýetmek üçin köp wagt gerek bolar, takmynan 600 sekunt, barlag bir wagtda yzdan başa çenli amala aşyrylanda bolsa 40 sekuntndan köp däl, ýa-da parol eýsem „maksat“ bolanda, ortadan başa çenli barlagy amala aşyrmak üçin 30 sekuntndan köp wagt gerek bolmaýar.

e) Parol yzygiderligini barlamakda ulanylýan programmanyň haýsy programmirleme dilinde ýazylandygy hem uly orun tutýar, sebäbi Assembler we C++ has ýokary tizlikleri hödürleýärler, Delphi programmirleme dili esasy obýekte gönükdirilen dil bolmak bilen, ulgamlaryň tizlikde birneme yza galýar [12].

3.3. Paroly döwmekligi programmirleme arkaly gurnamagyň häzirki zaman meseleleri

Delphi dilinde ýazylan programmany deňeşdirmek üçin C++ programmirleme dilinde ýazylan programma aşakda getirilen.

Bu programma belli bir parol yzygiderligini girizmegi talap edýär, soňra ony barlap anyklamak üçin öz hyzmatyny hödürleýär. Onuň iş düzgüni mundan ýokarky programma ýaly. Ol hemme iňlis elipbiýiniň harplaryny toplumlaýyn goýuşdyryp dogry parol bilen deňeşdirýär. Eger parol tapylsa, onda ony döwmek üçin näçe wagtyň gerek boýandygyny kesgitleýär.

Programma listingi (wzlom.exe)

```
#include <stdio.h>
#include <conio.h>
#include <string.h>
#include <stdlib.h>
main()
```

```

{
clrscr();
randomize();
char *p,*c,b;
int i,j,k,m;
for (i=0;i<4;++i)
p[i]=random(25)+'A';
printf(«4 belgili paroly girizmeli (meselem, SDFG):\n»);
l2:
printf(«Menýu saýlamaly:\n»);
printf(«Parol girizmek üçin 1 basmaly\n»);
printf(«Döwmek usulyny işletmek üçin 2 basmaly\n»);
printf(«Çykmak üçin 3 basmaly\n»);
b=getch();

if (b=='1')
{
clrscr();
printf(«Paroly girizmeli:»);
gets(c);
if (!strcmp(p,c))
{
printf(«Parol dogry»);
goto l1;
}
clrscr();
printf («Parol nädogry\n»);
goto l2;
}
if (b=='2')
{
long int tm;
tm=time(0);
for (c[0]='A';c[0]<='Z';++c[0])
for (c[1]='A';c[1]<='Z';++c[1])

```



```

for (c[2]='A';c[2]<='Z';++c[2])
for (c[3]='A';c[3]<='Z';++c[3])
{
//printf(c);
//printf(« «);
if (kbhit()) goto l1;
if (!strcmp(p,c))
{
clrscr();
printf(«\nParol tapyldy – %s»,c);
printf(«\n gerek bolan wagt %ld sekunt»,time(0)-tm);
getch();
goto l1;
}
}
}
}
l1:
}

```

3.4. Programmirleme dilleriniň deňeşdirilişi

Programmirleme dilleriniň öndürijiligini barlamak üçin Assembler, C++, Delphi dillerinde ýazylmaly programmalaryň önünde bir meseläni goýalyň.

Mesele. Inlis elipbiýiniň harplaryndan ybarat bolan 6 simwolly paroly döwmek üçin Iki özenli prosessorly (her özeniň ýygylgy 2,00Gh), işjeň huşy 2Gb bolan noutbuk ulanylýar. 1 sekuntda barlanylýan parollaryň sany her dilde ýazylan programma üçin aýratyn görkezmeli.

Belli bir barlag işlerinden soň aşakdaky netijeleri alýarys:

| № | Programmirleme dili | Programmanyň ölçegi | 1 sekuntda barlanylýan parollaryň sany |
|----|---------------------|---------------------|--|
| 1. | Turbo Assembler | 976 baýt | 1 182 786 |
| 2. | Turbo C++ | 16 Kbaýt* | 787 532 |
| 3. | Borland Delphi | 400 Kbaýt* | 485 943 |

* 1Kbaýt = 1024 baýt

Ýokardaky tablisadan görnüşi ýaly, Assembler we C++ dilleri gowy netijeleri berýär. Emma häzirki wagtda obýekte göni gurşawlaryň has giňden ýaýramagy bilen ýokary derejeli dillerde döredilen önümleri parol sorayan programmalara gönümel birikdirip bolmaýar. Sebäbi olar obýekte gönükdirilen däl, şol sebäpli Delphi dilini meýbury ýagdaýda ulanmak gerek, onuň tizliginiň pesdigini – obýekte gönükdirilmek bilen, ulgamlaryň işe birneme ikinji orun berilýär, ulgamlaryň işe bolsa göni wagt aralygynda hasaplama işleri degişlidir.

Ýokardakylary hasaba almak bilen, şu ýerde biz wagtyň birliğinde Delphi programmirleme dilinde döredilen programma arkaly barlanylýan simwollaryň yzygiderliliginiň takmyny mukdaryny kesgitläliň.

Häzirki wagtdaky kuwwatly kompýuterlerde, ol hemme meselelerden azat bolan mahaly (diňe paroly barlamaklyga gönükdirilen bolsa) 1 sekuntda 10 000 000 golaý simwollaryň yzygiderliligini barlamak mümkin, eger biz parallel hasaplamalary ulansak (bir wagtda başdan soňa çenli, soňdan başa çenli, ortadan başa çenli, ortadan soňa çenli) bu tizligi 1 sekuntda 40-50 milliona ýetirip bolýar.

Şeýlelikde, islendik simwollar yzygiderliliginiň wagtyň birliğinde barlanyp bilinjek sany kesgitlenildi.

6) Kompýuter ulgamynda parol barlanyp, onuň döwürmeginiň ähtimallygyny häzirki ýagdaý boýunça kesgitlemek.

Mundan öňki mysallarda biz ýa onluk ulgamynyň sanlaryny, ýa-da inlis elipbiýiniň harplaryny parolyň mümkin bolan simwollary hökmünde ulandyk. Hakykatda şol simwollar hökmünde çykyş edip biljek elementler gaty kän.

- a) İnlis elipbiýiniň uly we kiçi harplary – 52 sany;
- b) Rus diliniň uly we kiçi harplary – 66 sany;
- c) Sanlar – 10 sany;
- d) Dyngy belgiler we beýleki nyşanlar – takmynan 50 sany.

Şeýlelik bilen, biziň ygtyýarymyzda 180-e golaý simwol.

(1) formula boýunça 6 simwolly paroly kesgitlemek üçin yzygiderlikleriň aşadaky mukdaryny kesgitlemek gerek:

$$x = 180$$

$$y = 6$$

$$N=180^6= 34\,012\,224\,000\,000$$

Görşümüz ýaly astronomik san emele geldi.

Ýokarda kesgitleän wagtyň birliginde barlanylýan yzygiderliligiň mukdaryny (50 000 000 sany/s) ulanmak bilen aşakdaky hasaplamlary geçirýäris:

$$34\,012\,224\,000\,000 / 50\,000\,000 = 680244,48 \text{ sekunt};$$

$$680245 / 60 = 11307 \text{ minut};$$

$$11307 / 60 = 188,9568 \text{ sagat};$$

$$189 / 24 = 7,87 \approx 8 \text{ gün}.$$

Diýmek, eger parol “sowatly” düzülip goýlan bolsa, ony doly ýagdaýda kesgitlemek üçin aňryçäk 8 gün gerek, emma, ol ondan gaty ir “ýykylmagy” mümkin, Sebäbi bu ýagdaýda biz paroly iň soňky tapyljak yzygiderlik hökmünde kesgitledik. Hakyky ýagdaýda bolsa ol beýle bolman bilýär we yzygiderlikleriň arasynda ilkinjileriň ýa-da ortanjylaryň hatarynda bolup, onuň açylmagy üçin birnäçe sekunt ýa-da minut gerek bolmagy hem mümkin.

Parol goragy häzirki wagtda gorag tehnologiýasynda orän wajyp orny eýeleýär. Onuň hyzmatyndan orän möhüm maglumat çeşmeleri peýdalanýar. Ol orän gymmatly maglumatlaryň goraýjysy bolup bilýär. Şol sebäpli bu meselä gaty uly üns berilýär.

3.5. Paroly döwmeklige garşy usullary düzmek

Parol goragy üçin hödürülenjek täze usul düýpgöter özgertmelere eltýär, “terezi jamyny” paroly döwüjä garanynda parolyň eýesine tarap çekýär.

Bu usul düşündirilende gaty aňsat, işlenip düzülende we amala aşyrylanda bolsa çylşyrymly. Şol usul boýunça ýörite programma işlenip düzüldi.

Dogrudan hem, biziň döwrümüzde parolyň çylşyrymlylygyna garamazdan, olary döwüp açýan programmalaryň sany sansyzdyr. Olaryň iş düzgünleri ýokarda aýdyşymyz ýaly, simwollaryň yzygiderliligini tiz toplam parol hökmünde hödürlemektir. Parolyň dördiliş usulyna garamazdan simwol yzygiderliligi tötänleýin dogry toplan-sa – onda parol açylýar. Bu parol ulgamynyň iň uly ýetmezçiligidir.

Muny ýeňmeklik üçin parolyň simwol yzygiderligine wagty goýmaklyk göz önünde tutuldy. Mysal üçin şu programmada, parolyň her simwoly biri-birinden 5 sekuntadan galman toplanymalydyr. Eger bir gezek şol wagtdan artykmaç toplanýş bolsa, parol bitinlikde ýalňyş bolýar. Meselem, “maksat” parolynda 3-nji “k” simwol 2-nji “a” simwoldan soň 6 sekunt wagt geçen soň toplansa – parol ýalňyş görkezzer. Bu usul köp mümkinçilikleri döredýär. Eger paroly dogry bilseler hem, wagt aralygynda simwollar berlen wagta “sygmasalar” parol döwüji programmalaryň işi netijesiz bolýar.

3.6. Parolyň döwürmeginiň önüni alýan programma kody

Programma 4 proseduradan ybarat. Hemme ululyklar globaldyr (proseduranyň içinde kesgitlenýän üýtgeýänlere lokal üýtgeýänler diýilýär): **s** – paroly saklamak üçin ulanylýar (parol – maksat), **s1** – paroly barlamaklyk üçin, programmanyň işleýşiniň dowamynda düzümini ütgedýär, gysgaça aýdylanda, klawiaturadaky ýygñalan simwollaryň toplumy oña göçürilýär, **a** – wagt sanawjysyny (sçýotçigini) her simwol toplanýlandan soň täzelemek üçin ulanylýar, **i** – toplanýlan simwollaryň sanyny sanamak üçin ulanylýar (ähmiýeti programmanyň ýerine ýetirilişiniň dowamynda 6-dan ýokary bolmaýar, **j** – wagtyň geçmegini görkezýär.

TForm1.FormCreate – formanyň açylyş prosedurasy. Onda ilkinji parametrlar kesgitlenilýär.

TForm1.FormKeyPress – formada klawişa basylyş prosedurasy (formanyň KeyPreview häsiýeti True bolmalydyr). Bu ýerde **ENTER** basylymaklygy barlanýar – girizilen simwollaryň yzygiderliligi takyklyga barlanýar we netije boýunça **TRUE** ýa-da **FALSE** ekrana çykarylýar. Soňra hemme parametrlar (üýtgeýänler) başlangyç derejesine goýulýar.

TForm1.Edit1KeyPress – bu prosedura **s** setiri simwol yzygiderliligi bilen ädimleýin doldurylýar. Bu ýerde birnäçe şert bardyr. Olaryň birinde toplanýlan simwollaryň sanynyň (i) çäkden geçmekligi we **ENTER** basylymaklygy (onuň kody – 13) barlanýar. Şert

ýetse onda dolandyrys **TForm1.FormKeyPress** prosedurasyna aýtmazlyk boýunça geçýär, ýetmese, onda simwolyň toplanlyşyndan öňki wagty barlanýar (j). Eger wagt çäkten geçilen bolsa, programma ýygnaýan simwolyň koduny üýtgedýär (ony birlik sana artyk edip goýýar).

TForm1.Timer1Timer – prosedurasy wagt bilen işi alyp bar-maklygy amala aşyrýar (hasaplaýjyny her simwol toplanýlandan soň täzelemekligi, wagty ekrana çykarmaklygy we ş.m.)

```
var
Form1: TForm1;
s,s1:string;
i,j:integer;
a:boolean;
implementation
{$R *.dfm}
procedure TForm1.FormCreate(Sender: TObject);
begin
s:='maksat';i:=0;s1:='";a:=false;j:=0;
end;
procedure TForm1.FormKeyPress(Sender: TObject; var Key: Char);
begin
if ord(key)=13 then begin
Edit1.Text:='";
if s=s1 then Label2.Caption:='TRUE'
else Label2.Caption:='FALSE';
s1:='";i:=0;a:=false;
end;
end;
procedure TForm1.Edit1KeyPress(Sender: TObject; var Key: Char);
Label 1;
begin
if (i=6) or (ord(key)=13)then Goto 1
else
begin
inc(i);
```

```

if (j>5) and (i>1) then s1:=s1+chr(ord(key)+1)
else s1:=s1+key;
a:=true;
end;
1:
end;
procedure TForm1.Timer1Timer(Sender: TObject);
Label 1;
begin
if a=true then begin a:=false;j:=0;Goto 1;end;
Label3.Caption:=inttostr(j);
Timer1.Interval:=1000;inc(j);
1:
end;
end.

```

Ýokardaky programmanyň bir ýetmezçiligi bar. Ol rugsatsyz elýeterlikden gorap bilmeýär. Dogrudan hem, döwüji programmalara garşy ony ulanmaklyk amatly, emma paroly bilýän başga adama garşy (programmanyň eýesi däl) amatly däl. Paroly bilýän adam dogry paroly 5 sekuntadan gijä galman toplam programma girip biler.

Şol sebäpli ikinji programmanyň üstünden iş alnyp barylýdy. Bu programma ýokarkydan programma kody boýunça kän bir tapawutlanmaýar. Emma has ýokary netijeliligi berýär. Tapawutly ýeri hem şu ýerdedir:

TForm1.Edit1KeyPress – prosedurasynda yzygider simwollaryň toplanlymagynyň wagty 1 sekuntadan köp we 3 sekuntadan az bolmaly diýlen şert goýlandyr.

Netijede, paroly bilýän adam dogry wagtda simwollaryň yzygiderligini ýerleşdirip bilmez – ol ony derrew girizjek bolar – bu bolsa ýalňyşlyga ýol berler.

```

var
Form1: TForm1;
s,s1:string;
i,j:integer;
implementation
{$R *.dfm}

```

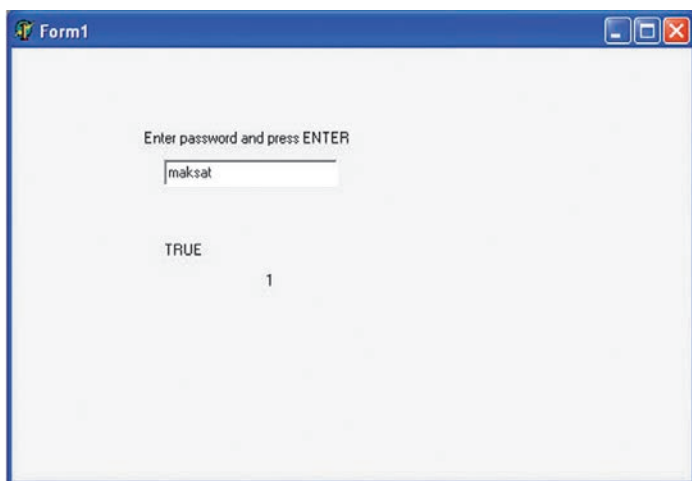
```

procedure TForm1.FormCreate(Sender: TObject);
begin
s:='maksat';i:=0;s1:="";j:=0;
end;
procedure TForm1.FormKeyPress(Sender: TObject; var Key: Char);
begin
if ord(key)=13 then begin
Edit1.Text:="";
if s=s1 then Label2.Caption:='TRUE'
else Label2.Caption:='FALSE';
s1:="";i:=0;
end;
end;
procedure TForm1.Edit1KeyPress(Sender: TObject; var Key: Char);
Label 1;
begin
if (i=6) or (ord(key)=13)then Goto 1
else
begin
inc(i);
if (j<1) or (j>3) and (i>1) then s1:=s1+chr(ord(key)+1)
else s1:=s1+key;
j:=0;
end;
1:
end;
procedure TForm1.Timer1Timer(Sender: TObject);
begin
Label3.Caption:=inttostr(j);
Timer1.Interval:=1000;inc(j);
end;
end.

```

Ýokarky usul parol goragynyň ýykylmagynyň öňüni alýar, sebäbi diňe adatdan daşary ýagdaýda paroly dogry kesgitlän adam, ony dogry wagtda girizip programmany açmagy mümkin. Bu ýagdaýlar

bolsa, parolyň eýesi paroly girizmekligi gizlin ýagdaýda saklamagy amala aşýran ýagdaýda bolmazlygy hem mümkin.



3.2-nji surat. “maksat” parolyň simwollary 1 we 3 sekundyň aralygynda girizilende parol dogry girizildi diýlip bellenilýär (**TRUE**)



3.3-nji surat. “maksat” parolyň haýsy-da bir simwoly 1 we 3 sekundyň aralygynda girizilmän, meselem 3 sekunt geçen soň girizilen mahaly parol nädogry girizildi diýlip bellenilýär (**FALSE**)

Geliň indi parolyň hem-de her simwolyň ondan öňki simwoldan bolan wagt aralygyny nirede saklamak barada meseläni öňde goýalyň. Bu elbetde reýestr.

Onuň belli bir açarlarynyň birinde her simwollaryň aralyklarynyň we parolyň saklanylmagy, olary faýl görnüşinde kompýuteriň huşunda ýerleşdirmekden azat edýär. Bilşimiz ýaly, faýl görnüşü elýeterlikden goramak babatda belli bir gowşaklyklara ýol berýär, reýestriň açarlary belli bir sebäplere görä şol gowşaklyklara ýol bermeýär. Emma muňa garamazdan, biziň gizlin saklajak bolýan zatlarymyzy has netijeli gizlemek üçin olary şifrlemek gerek. Bu barada bolsa biz şu okuw kitabyň beýleki bölümlerinde gürrüň ederis.

Bu bölümde parol goragyna seredilipdi.

Dogry, parol goragyny döwmekligiň dürli usullary öň hem bardy. Emma kompýuter tehnologiýasynyň ýaýramagy bilen bu ugurdaky “döwüji” tehnologiýalaryň has ýokary depginde ösmegi dowam etdirilýär. Paroly döwmek meselesi köp şertlere bagly. Olaryň hemmesini biz ýokarda sanap geçdik, emma oňa garamazdan, oňa garşy uniwersal usul peýdalanmak bolar. Parolyň simwollarynyň arasynda wagt aralygyň goýulmagy paroly 4 ölçeg ýagdaýa getirýär.

Tejribe işleri

1. Inlis elipbiýiň kiçi harplaryndan ybarat bolan dürli söz parollary barlamak üçin harp yzygiderliklerini seljermeli.
2. Parol girizmekligi talap edýän ýönekeý programmany döretmeli.
3. Paroly faýldan okaýan we ony üýtgetmegi mümkin edýän programmany düzmeli.
4. Assembler dilinde paroly seljerýän programmany döretmeli.

IV. KOMPÝUTER PROGRAMMALARYNYŇ GOÝBERILMEGINI ÇÄKLENDIRMEK

1. Programmalaryň goýberilişiniň çäklendirilmeginiň gorag hökmünde seredilmegi.
2. Programmalaryň goýberilişini çäklendirmegi seljermek:
 - Programmalaryň goýberilişini wagt boýunça çäklendirmek;
 - Programmalaryň goýberilişiniň sanyny çäklendirmek;
 - Programmalary diňe bir kompýuterde goýbermek.
3. Programmalaryň goýberilişini programmirleme arkaly amala aşyrmak.
4. Programmirleme serişdelerine barlag geçirmek.
5. Programmalary çäklendirmek üçin programmirleme dilleri utgaşdyryp ulanmak meselesi.

Kompýuter tehnologiýasynyň häzirki wagtda ýokary depginler bilen ösmegi onuň iň wajyp ugurlarynyň biri bolan – programma üpjünçiliginiň giňden ýaýramagyna getirdi. Häzirki wagtda programmalaryň örän köp mukdary peýda boldy we olaryň görnüşleriniň sany hem artdy.

Programmalar häzirki wagtda örän ýokary gyzyklanmalara eýe bolýar. Programma üpjünçiligini düzüjileriň ummasyz köp sany emele geldi.

Häzirki wagtda ylmyň ähli pudaklarynda alymlaryň ylmy-barlag işlerinde ol ýa-da başga maksatlar bilen programma üpjünçiliginiň ulanylýandygy bellidir.

Medisina, dilşynaslyk, himiýa, nebit-gaz, geologiýa, gurluşyk we başg. pudaklara degişli ylmyň ugurlarynda dürli programmalar ulanylýar. Olar köplenç ýöriteleşdirilen görnüşinde bolýar hem-de diňe şol ylmyň pudagynda ulanylýar. Bu bolsa şol programma üpjünçiligini düzen hünärmenleriň toparyna ykdysady taýdan uly bir düşewünt getirmeyär. Şol sebäpden programmasyna awtorlyk hukugyna ýa-da patente eýe bolan programma düzüjiler, öz önüminiň goragy ugrunda XX asyryň 90-njy ýyllarynda işläp başladylar.

Maglumaty goramagyň bu usulynyň emele gelmeginiň esasy sebäbini aşakdaky ýagdaýdan yzarlamak mümkin:

Programma düzüji belli bir öndürijilikli, kompýuter program-masyny kesgitlenen wagt aralygynda işläp düzýär. Şol kompýuter programmany düzmek üçin sarp eden wagtyňy, peýdalanylan tehniki serişdeleriň bahasyny, siňdirilen akyl zähmetini hem-de şol kompýu-ter programmasynyň şol wagtdaky ähmiýetini we netijeliligini hasaba almak bilen programma düzüji öz önüminiň bahasyny kesgitleýär. Öz döreden programmasyny degişli edaralarda gorap hem-de awtorlyk hukugyna ýa-da patente eýe bolup, programma düzüji öz önümini ýerlemäge başlaýar. Önümiň birlik bahasyny kesgitläp hem-de umu-my girdejiniň möçberini bellemek bilen, programma düzüji öz kom-pýuter programmasynyň näçe mukdarda (ýagny, näçe disk çykarylyp) satylmalydygyny kesgitleýär.

Kompýuter tehnologiýasynyň ösüşi, programmalary ulanmakda has giň mümkinçilikleri döretdi. Maglumat göçüriji enjamlaryň ös-megi (ýagny disk okaýjylaryň), maglumaty bir maglumat göterijiden beýlekä kynçylyksyz göçürmegi amala aşyrmaga mümkinçilik döred-ýär. Bu bolsa zerur bolan kompýuter programmasynyň bir maglumat göterijiden (ýagny diskden) çäksiz mukdarda beýleki maglumat gö-terijilere göçürilmegini aňladýar. Şeýlelik bilen, satylan kompýuter programmasynyň bir nusgasyndan çäksiz mukdary hiç hili girdeji bermän ýerlenip bilýär. Bu bolsa programma düzüjiniň ykdysady ýagdaýynyň peselmegine getirip biler.

Şol sebäpden hem biziň döwrümüzde kompýuter programma-larynyň rugsatsyz ulanmazlygy ugrunda täze gorama usullary döre-dilip başlandy.

4.1. Programmalaryň goýberilişiniň çäklendirilmeginiň gorag hökmünde seredilmegi

Programma – bu maglumatyň bir görnüşidir. Emma resminama ýa-da başga beýan ediş maglumatyň görnüşlerinden tapawutlylykda, ol goýberilmek we ýerine ýetirmek häsiýetine eýe bolýar. Şol sebäp-li programmalary edil beýleki maglumatyň görnüşleri ýaly, diňe bir

şifrlemek ýa-da parol goýmak arkaly däl-de, eýsem goýberilişini çäklendirmek arkaly hem goramak mümkin.

Bu bölümde, kompýuteri goramagyň iň „ýaş“ hasaplanylýan usulyna, ýagny kompýuter programmalarynyň goýberilişini çäklendirmeklige seredilýär.

Programmanyň goýberilmegini çäklendirmeklik şeýle ugurlary öz içine alýar: goýberilmegi wagt boýunça çäklendirmek, goýberişleriň sanyny çäklendirmek, kompýuter programmasynyň diňe bir iş ýerinde (kompýuterde) goýberilmegi.

4.2. Programmalaryň goýberilişini çäklendirmegi seljermek

Programmalary çäklendirmek üçin programmirleme dilleri utgaşdyryp ulanmak meselesine soňky wagtlar seredilip başlandy.

Programmanyň goýberilmegini wagt boýunça çäklendirmek bu ugurda iň ilkinji emele gelen usullaryň biridir. Onuň ulanylyşy aşakdaky netijeleri berýär:

Programma düzüji kompýuter programmasyny taýýarlap we awtorlyk hukugyna eýe bolup, onuň koduna birneme üýtgediş girizýär. Ol koduň maksady – programmanyň diňe belli bir wagtyň aralygynda işlemegidir. Meselem 3 aý. Bu möhlet geçenden soň programma özüniň iş ukybynyň tamamlanandygy barada habar berýär.

Bu ýagdaýda kompýuter programmasyny ulanyjy programma düzüjiden habar tutup programmany işletmek üçin ylalaşyga gelmeli bolýar. Bu usulyň artykmaçlygy programma ilki başda erkin ýaýradylýar. Şol programma bilen, belli bir synag möhletiň dowamynda işläninden soň, ulanyjy şol programma oňa gerekdigini ýa-da gerek dälidigi barada netije çykaryp, şol programmanyň işiniň möhletini uzaltmak üçin tölemeli bolýar. Bu bolsa programma düzüjiniň satuwa çykarjak önüminiň köp mukdarynyň ýerlenmegini aňladýar. Sebäbi her bir ulanyjy diňe özündäki programmasy üçin işleýiş möhleti uzaldýar. Şol programmanyň beýleki nusgalary üçin ol degişli däl, sebäbi düzüji bir programmanyň ähli nusgalaryny belgiläp çykýar we şol belgiler üçin aýratyn möhleti uzaldyşy işläp düzýär.

Geliň, indi programmanyň goýberilişiniň möhlet boýunça çäklendirilmeginiň ülnüsine has düýpli seredeliň [13].

Programma kompýutere gurnalýar, soňra onuň ilkinji goýberilmegi amala aşyrylýar, şonda ýadyň içine belli bir maglumat ýazgy hökmünde geçirilýär. Şol ýazgy köplenç programmanyň ilkinji goýberilmegiň senesini saklaýar. Bu ýazgy belli bir gizlin faýla ýa-da reýestriň bir açaryna ýazylyp bilýär (ikinjisi has amatly). Özünüň ulanylyşynyň dowamynda programma şol döredilen faýlyň ýa-da reýestriň açaryna girip görýär hem-de özüniň ilkinji goýberilen senesi bilen häzirki wagtyň arasyndaky geçen möhleti kesgitleýär. Soňra şol möhlet çäk möhlet bilen deňeşdirilýär (meselem programma 3 aý işlemeli bolsa çäk möhlet 90 güne deň). Eger çäk möhletden ýokary geçilen bolsa, bu barada habar berilýär hem-de programma düzüji bilen habarlaşmak maslahat berilýär.

Ýokarky ülni matematiki diline geçirenimizde aşakdaky hasaplamalary almak mümkin:

Mysal. Programma 2009-njy ýylyň ýanwar aýynyň 12-ne ilkinji gezek goýberildi. Onuň çäk möhleti 3 aý, ýagny 90 gün. Biz şol programmany 2010-njy ýylyň fewral aýynyň 10-yna goýberen ýagdaýyndaky onuň barlama hasaplamalaryny getirmeli.

Goý d – programmanyň ilkinji gezek goýberilen günü (12), m – aýy (12), y – ýyly (2009) bolsun.

Onda d_1 – barlanylýan gün (10), m_1 – aý (02), y_1 – ýyly (2010) bolsun.

t – çäk möhleti ol 90-a deň t_1 – programmanyň barlanylýan gününe çenli ulanylan möhleti.

Şeýlelikde, şulary alýarys:

$$t_1 = (y_1 - y) * 365 + (m_1 - m) * 30 + (d_1 - d). \quad (1)$$

5.1. formula boýunça şeýle hasaplamalar amala aşyrylýar:

$$t_1 = (2010 - 2009) * 365 + (2 - 12) * 30 + (10 - 12) = 365 - 300 - 2 = 64$$

Şeýlelik bilen $t > t_1$ (çäk möhletinden heniz geçilenok), şol sebäpden programma ulanylyşy dowam etdirilýär.

Biz bu ýerde ýylda 365 gün, aýda bolsa 30 gün edip şertleýin aldyk, sebäbi ýalňyşlyk gitse-de ol 1-2 günden köp bolmaýar, şol sebäpli oňa ýol berilýär.

Eger programma mart aýynyň 5-den soň goýberilen ýagdaýynda çäk möhletinden ýokary geçilýär we programma öz işini bes edýär:

$$t_1 = (2010-2009) * 365 + (3-12)*30 + (6-12) = 365 - 270 - 5 = 90 = t.$$

Elbetde, möhleti barlaýan programma kody, onuň başynda ýerleşdirilmelidir, sebäbi çäk möhletinden geçilendigi tassyklanandan soň, ol öz mümkinçiliklerini hödürlemeli däl [14].

Aşakda programmanyň goýberilişiniň adaty ýönekeýje mysaly Pascal programmirleme dilinde ýazylyp görkezilen.

4.3. Programmalaryň goýberilişini programmirleme arkaly amala aşyrmak

Wrema3.exe programması.

Bu programma öz goýberişini wagta baglap goýýar. Belli wag geçenden soň ýalňyşlyk barada habar berýär.

Ilkibaşda biz programmanyň düzüminde programma haýsy wagtdan bäri sanap başlamalydygyny kesgitleýäris – ýyly (y), soňra aýy (m) we günü (d), mundan soň biz programmanyň möhlet boýunça t çäginde kesgitleýäris. Mysal üçin: programma 2009-njy ýylyň awgust aýynyň 25-inden sanawy başlaýar. Şol wagtdan 1 ýyl, ýagny 365 gün geçen soň ol öz goýberişini çäklendirýär (ýalňyşlyk barada habar berýär). Bularyň hemmesi hemişelikdir (const). Olary diňe dörediji başlangyç ýazgyda üýtgedip biler.

Soňra üýtgeýänleriň sanawy gidýär, y1, m1, d1 (s1 ulanylmaýar) degişlikde häzirki ýyly, aýy, günü belgilemek üçin ulanylýar.

GetDate funksiýasy arkaly biz häzirki ýyly, aýy, we günü tapýarys. Soňra ýörite formula boýunça biz programmanyň sanap başlaýan wagtyndan häzirki wagty aýyryarys we çäk bilen barlaýarys, eger çäk geçilen bolsa onda 1 belgisine gidilýär we ýalňyşlyk barada habar berilýär we programmadan çykylyar. Eger kiçi ýa-da deň bolsa, onda häzirki sene çykarylyar – bu programmanyň heniz işewürligini görkezýär, sebäbi çäk möhletinden geçilenok.

Programmanyň listingi

```
uses dos,crt;
label 1,2;
const
y=2008; m=8; d=25; t=366;
var
ch:char;
y1,m1,d1,s1,t1:word;
BEGIN
  clrscr;
  GetDate(y1,m1,d1,s1);
  if (y1-y)*365+(m1-m)*30+(d1-d)>365 then goto 1
  else
    begin
      writeln('Hazirki sene – ',d1,', ',m1,', ',y1);
      goto 2;
    end;
  1: writeln('Programmanyň mohleti gecdi');
  2: write('Programmadan cykmak ucun ISLENDIK DUWMA bas-
maly');
  ch:=readkey;
END.
```

Wrema4.exe programmasy.

Indiki görkeziljek programma mundan ýokarda görkezilenden birneme tapawutlanýandyr. Bu programma goýberilende özüniň ilkinji gezek goýberilýändigini barlaýar. Bu barlag **C:\reg** faýlyň bardygyny ýa-da ýoklugy esasynda amala aşyrylýar. Eger şol faýl ýok bolsa programma ony gizlin ýagdaýda döredýär we onuň içine şol wagtky senäni (ýyl, aý, gün tertibinde) hem-de çäk möhletini (deslapdan ol 365-e deň) girizýär. Ýagny başlangyç sene bilen çäk möhlet programmanyň kodunda däl-de, aýratyn çeşmede ýerleşdirilýär.

Eger faýl ilkinji gezek goýberilmeýän bolsa (ýagny **reg** faýly bar bolsa), onda şol faýl açylýar we onuň içinden **y**, **m**, **d**, **t** üýtgeýän ululyklary ýatda saklanylan programmanyň ilkinji goýberilen senesi ýyl, aý, gün tertibinde hem-de çäk möhleti ýazylýar.

Programma şeýle hem çäk möhletini üýtgetmek mümkinçiligini hödürleýär. Ony üýtgetmek diňe paroly dogry girizmek arkaly mümkin. Parol – “maksat”.

Parol nädogry girizilende programma işlemekligi dowam etmekligi hödürleýär (eger çäk möhleti rugsat etse). Programmanyň işjeňligi häzirki senäniň çykarylmany bilen kesgitlenýär (eger görkezilse onda programmanyň möhleti geçenok).

Parol dogry girizilen mahalynda reg faýlyň içinde täze girizilmeli çäk möhleti ýazylyar.

Programmanyň listingi

```
uses dos,crt;
label 1,2,metka1,metka2,metka3,start,start1,error,Prog;
var
i:integer;
ch:char;
fi:file of word;
y1,m1,d1,s1,y,m,d,t:word;
p,l,c,fname:string;
BEGIN
  clrscr;
  p:='maksat';
  l:='C:\';
  fname:='reg';
  chdir(l);
  assign(fi,fname);
  {$I-}
  reset(fi);
  {$I+}
  if IOResult<>0 then goto error;
  read(fi,y);
  read(fi,m);
  read(fi,d);
  read(fi,t);
  close(fi);
```



```

    goto Prog;
error:
    rewrite(fi);
    GetDate(y,m,d,s1);
    t:=365;
    write(fi,y);
    write(fi,m);
    write(fi,d);
    write(fi,t);
    close(fi);
Prog:
    writeln('6-simwolly paroly girizin we ENTER basyn');
    read(c);
    asm
    start:
        Lea di,p
        Lea si,c
        mov cx,6
    start1:
        mov al,byte ptr[si]
        cmp byte ptr[di],al
        jne metka1
        inc si
        inc di
        Loop start1
        jmp metka2
    end;
metka2:
    writeln('Parol dogry');
    writeln('Gun sany boyunca cagi girizin');
    reset(fi);
    for i:=1 to 3 do read (fi,t);
    readln(t);
    write(fi,t);
    close(fi);

```

```

    goto metka3;
metka1:
    writeln('Parol nadogry, islemekligi dowam ediberin!');
metka3:
    GetDate(y1,m1,d1,s1);
    if (y1-y)*365+(m1-m)*30+(d1-d)>t then goto 1
    else
        begin
            writeln('Hazirki sene – ',d1,',',m1,',',y1);
            goto 2;
        end;
    1: writeln('Programmanyn mohleti gecdi');
    2: write('Programadan cykmak ucun ISLENDIK DUWMA bas-
maly');
    ch:=readkey;
END.

```

Şu iki kiçi mysalda programmanyň goýberilmeginiň wagt boýunça çäklendirilmeginiň in ýönekeý, emma esasy usul düzüji tilsimleri görkezilen.

Elbetde, bu programma kodlarynyň şu ýagdaýda ulanylmagy belli bir derejede programmanyň goragyny ýeterlik derejede üpjün edip bilmez, emma indiki bölümde awtor tarapyndan hödürlenen usulyýeti düşündürmek üçin gowy usuly-görkezme bolup biler.

Programmalaryň goýberilişini wagt boýunça çäklendirmede meselem, çäk möhleti 3 aý bolanda dürli ulanyjylaryň şertleri deň bolmaýar. Sebäbi käbir ulanyjylar 3 aýyň dowamynda programmany birnäçe ýüz gezek goýberip bilýär, käbirileri bolsa birnäçe ýa-da eýsem birden köp däl hem bolmagy mümkin.

Bu ýagdaýy düzetmek üçin soňky ýyllarda programmalaryň goýberilmeginiň ýene bir çäklendirilmesiniň usuly – goýberilmegini çäklendirmek sany işlenip düzüldi.

Ulanjy programmany satyn alýar we ony ulanyp başlaýar. Mysal üçin, 100-nji goýberişden soň (çäk sany 100-e deň) programma öz işiniň möhletini uzaltmak barada habar berip, işini bes edýär. Bu ýagdaýda ulanyjylar şol programmany deň ýagdaýda kesgitli mukdarda

goýberip ulanýarlar hem-de şol programma işlerinde gerek bolan mahaly onuň iş möhletini (goýberiş sanyny) satyn alyp artdyrýarlar, eýsem ony üznüksiz ýagdaýa hem ýetirip bilýärler.

Goýberilmegi çäklendirmegiň bu usulynyň ülnüsi aşakdakylardan ybarat.

Edil mundan öňki usuldaky ýaly, programma ilkinji gezek goýberilende kompýuteriň huşunda belli bir ýazgynyň faýla ýa-da reýestriň açaryna ýazylmagy amala aşyrylýar. Emma bu gezek sene ýa-da çäk möhleti ýazylan, şol programmanyň goýberilmeginiň aňryçäk sany ýa-da programmanyň ilkinji goýberilendigi bellenilýär (ýagny 1-lik san ýazylýar). Programmanyň ulanylyşynyň dowamynda şol ýazgy üýtgäp durýar, meselem, ikinji gezek goýberilende, ýazgyda 2, üçünji gezekde 3 we ş.m. ýazylyp gidýär. Şol ýazgy tä programmanyň goýberilmeginiň çäğine ýetilýänçä (meselem 100-e çenli) üýtgäp durýar hem-de programma 100 gezek goýberilenden soň, şol ýazgy üýtgemeyär we programma öz goýberilişini bes edýär.

Ýokarky ülnüni matematiki diline geçirilende aşakdaky hasaplamalary almak mümkin:

Mysal. Programmanyň goýberilmegi 100 gezege niýetlenen. Ol 25-nji gezek goýberilýär. Ol goýberilende barlama hasaplamalaryny geçirmeli.

Goý, **n1** – programmanyň häzirki wagta çenli goýberilendiginiň sany, **n** – goýberilmegiň çäk sany bolsun.

Onda **n1** = 25, **n** = 100.

$n > n1$, şonda **n1** = **n1** + 1,

şeylelik bilen, her bir goýberiliş bilen ýazgynyň içindäki san birlige artdyrylýar, tä 100-e deň bolýançä.

Calculýator.exe programmasy.

Bu programma Delphi 6.0 programmirleme dilinde ýerine ýetirildi. Bu programma döredilende 80% iş kalkulýatoryň ýerine ýetirýän funksiýalaryna, galan 20% bolsa bu programmanyň goralýşyna sarp edildi.

Programma diňe 3 gezek ýerine ýetýär. Ony gaýtadan işletmek üçin, onuň döredijisine ýüzlenmeli.

Sorag ýene bir ýerde ýüze çykmagy mümkin – programma özünüň näçe gezek ýerine ýetirilendigini nähili bilýär?

Muny amala aşyrmagyň birnäçe usullary bar. MS-DOS operasion sistemasyna has giň ýaýran usullaryň biri sanaýjyny (sçýotçigi) daşky özbaşdak faýla (gizlin, ýazgy faýlda) baglaşdyrmakdyr. Ol faýly bir gizlin ýerde saklamaly. Bu usuly diňe ýönekeý ulanyjylara garşy ulanmak mümkin. Kompýuterlere belet adamlar haçan-da bolsa onuň syryny bilmegi mümkin. Şol sebäpli esasy maksat – hemme ýokardakylara syn edip, uniwersal usuly tapmak.

Windows operasion sistemasy köp mümkinçilikleri berýär. Windows operasion sistemasynyň reýestri bar. Ol “Regedit” diýlip atlandyrylýar. Ol münlerçe açarlardan we bukjalardan ybaratdyr.

Programma göni reýestr bilen işleýändir.

Ilkinji gezek goýberilende ol reýestriň içine girýär. Soňra HKEY_LOCAL_MACHINE bölüme geçýär. System\ ýol boýunça hereket edýär. Bu ýerde ol ‘234’ setiri gözleýär we onuň düzümini okaýar. Eger onuň düzümi boş bolsa (setir ýok) onda özünüň ilkinji gezek goýberilendigine “düşünýär”, bu setiri döredýär we onuň içine 2-lik sany ýazyp goýýar. Soň indiki gezek goýberilende ol şol setiriň düzümini okap, şol düzümiň (sanyň) bahasyny birlik sana kemeldýär – tä “0” çenli. Ol setiriň düzüminiň ähmiýeti “0” bolan ýagdaýynda ýalňyşlyk barada maglumat berýär we programma elýeterligi togtadýar.

Döredijiniň mümkinçiliklerini görkezmek üçin şeýle bir kod döredildi. Ýalňyşlyk barada penjire çykan mahalynda iňlis “m” harpyny klawiatura arkaly basylanda programma ony işläp, indiki goýberilişden başlap ol ýene-de 3 gezek goýberilmek ukybyna eýe bolýar we ş.m.

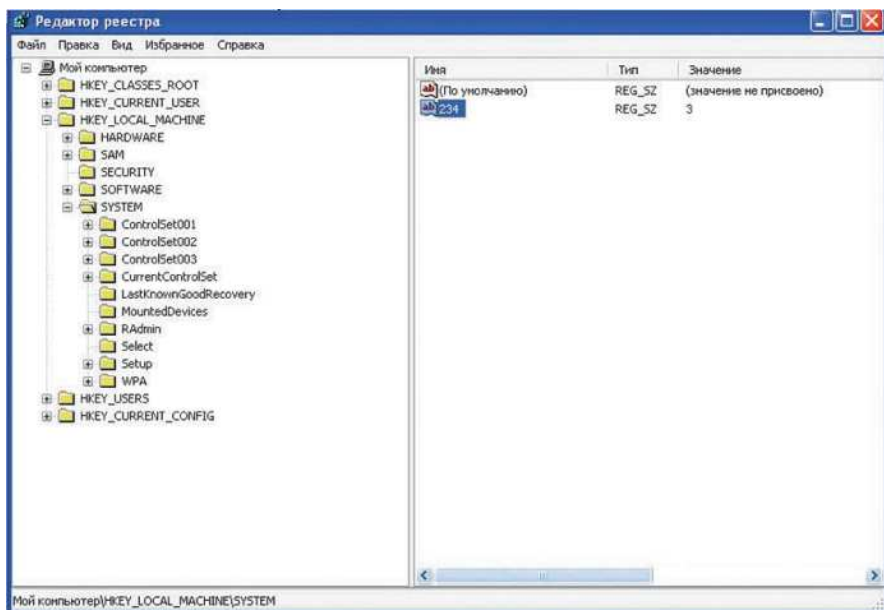
Indi bolsa programmanyň düşündirilişine geçeliň.

Programmanyň döredilişiniň hemme taraplaryna degip geçmän, diňe onuň goralýşyna göz ýetireliň. Regedit bilen işlemegi mümkin etmek üçin Proýektiň (Delfide hemme iş Project diýlip atlandyrylýar) esasy penjiresiniň modullar belgisinde (**uses**) “registry” diýen ýazgyny ýazmaly. Programmanyň goýberilişini netijeli çäklendirmek üçin TTimer obýekti Formanyň üstüne ýerleşdirilýär. TTimer obýekti programmanyň goýberilişiniň dürli wagt aralygynda nämeleriň bolup

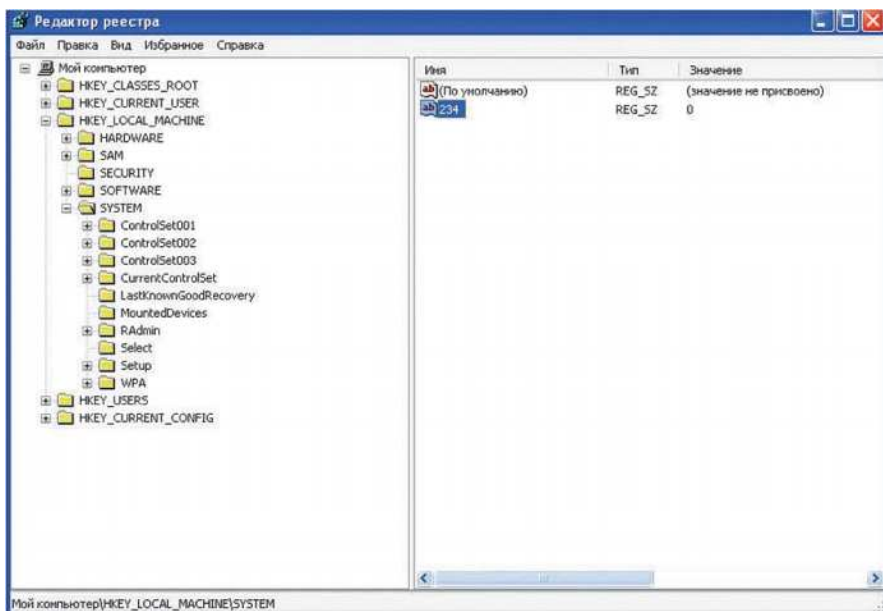
geçýändigine jogap berýär. Bu obýektiň prosedurasynda biz hemme üýtgeýänleri belgileýäris. Olaryň arasynda iň esasysy R üýtgeýän ululykdyr. Onuň tipi – **TRegistry**. Ondan başga hem biz **fi** – **string** we **m** – **integer** üýtgeýänleri belgileýäris.

fi bize reyestriň içindeki ‘234’ atly açaryň düzümini okamak üçin gerek bolýar. Mysal üçin programma ilkinji gezek goýberilende **fi** boş bolýar (sebäbi ‘234’ açar döredilmedik). Hemme indiki goýberilişlerde **fi** ululygyň düzümi boş bolmaýar (sebäbi ilkinji gezek goýberilende programma ‘234’ açary döredip, onuň içine ‘3’ simwoly ýazýar), ol okalýar we san formatyna geçirilýär, sebäbi ‘234’ açaryň düzümi setirde bolýar.

San formatyny amala aşyrmak üçin **m** ulanylýar (**m:=StrToInt(fi)**). Ol üýtgeýäniň üstünde esasy iş alnyp barylýar, onuň ähmiýeti **dec** operatory arkaly birlik sana kemelýär. Soňra **m** ululyk setir formatyna geçirilýär (**fi:=IntToStr(m)**) we ol reyestrdäki gerek bolan ‘234’ açaryň setirine ýazylýar.



4.1-nji surat. HKEY_LOCAL_MACHINE bölümiň **System** bölümçesinde ‘234’ açary döredilip, onuň içine setir görnüşinde ‘3’ ýazylýar (goýberilmegin çäk sany)



4.2-nji surat. ‘234’ açaryň içinde ‘0’ ýazgy (programma işini bes edýär)



4.3-nji surat. Form1 esasy formanyň penjiresi

Eger ‘234’ açaryň düzümi ‘0’ bolsa täze Forma goýberilýär (Form3.Show) we esasy forma ýapylýar – Form1.Close.

Form3 goýberilmeginiň esasy maksady ulanyja programmanyň goýberilmeginiň çäginäň tamamlanandygyny görkezmekdir.



4.4-nji surat. Form3 penjiresiniň goýberilmegi

Gaýtadan 3 gezek goýberişi amala aşyrmak üçin Ýalňyşlyk barada habar berýän penjiräniň (Form3) KeyPreview häsiýetini **True** edip goýmaly. Soňra şol formanyň OnKeyPress hereket etmeginde FormKeyPress prosedurasynda “m” klawişasy basylanda reýestre girip, gerek bolan setiri açyp onuň içine “3” ýazmaly.

Geliň, indi Regedit bilen Delphiniň üsti bilen işlemäge seredeliň.

Registriň üýtgeýänini belgiläp (R:TRegistry), reýestri programma üsti bilen açylýar – R:=TRegistry.Create. Soňra – gerek bolan bölümi açyp – R.RootKey:=HKEY_LOCAL_MACHINE ýol saýlanylýar – R.OpenKey(System, true). Bu ýerde “true” şu ýolda ýazgysy ýazmak mümkin ýa-da ýok diýen belgini kesgitleýär. Gerek bolan setiri okamak üçin – fi:=R.ReadString('234') saýlanylýar. Setire ýazmak üçin – R.WriteString('234','2') saýlanylýar.

Goýberilişi çäklendirmäge göni degişli programma kody ýarym goýy we ýapgyt şrift bilen bellenilendir.

Programmanyň listingi

Unit1

| | |
|------------------------------|--|
| unit Unit1; | Dialogs, Menus, StdCtrls, Buttons, ComCtrls, ExtCtrls; |
| interface | |
| | type |
| uses | TForm1 = class(TForm) |
| Windows, Messages, SysUtils, | Button1: TButton; |
| Variants, Classes, Graphics, | Button2: TButton; |
| Controls, Forms, Registry, | Button3: TButton; |

```

Button4: TButton;
MainMenu1: TMainMenu;
N1: TMenuItem;
N2: TMenuItem;
N3: TMenuItem;
N4: TMenuItem;
Button5: TButton;
Button6: TButton;
Button7: TButton;
Button8: TButton;
Button9: TButton;
Button10: TButton;
Button11: TButton;
Button12: TButton;
Button13: TButton;
Button14: TButton;
Button15: TButton;
Button16: TButton;
Button19: TButton;
Button20: TButton;
Button21: TButton;
BitBtn1: TBitBtn;
Button18: TButton;
Button22: TButton;
Button23: TButton;
Memo1: TMemo;
BitBtn2: TBitBtn;
Panel1: TPanel;
Timer1: TTimer;
Bevel1: TBevel;
Bevel2: TBevel;
Bevel3: TBevel;
procedure N2Click(Sender:
TObject);
procedure Button6Click(Sender:
TObject);

```

```

procedure Button7Click(Sender:
TObject);
procedure Button8Click(Sender:
TObject);
procedure Button9Click(Sender:
TObject);
procedure
Button10Click(Sender: TObject);
procedure
Button11Click(Sender: TObject);
procedure
Button13Click(Sender: TObject);
procedure
Button12Click(Sender: TObject);
procedure
Button14Click(Sender: TObject);
procedure
Button15Click(Sender: TObject);
procedure
Button16Click(Sender: TObject);
procedure FormCreate(Sender:
TObject);
procedure Button1Click(Sender:
TObject);
procedure Button5Click(Sender:
TObject);
procedure
Button22Click(Sender: TObject);
procedure Button2Click(Sender:
TObject);
procedure Button3Click(Sender:
TObject);
procedure BitBtn1Click(Sender:
TObject);
procedure
Button21Click(Sender: TObject);

```



```

procedure Button4Click(Sender:
TObject);
procedure
Button19Click(Sender: TObject);
procedure
Button20Click(Sender: TObject);
procedure BitBtn2Click(Sender:
TObject);
procedure
Button18Click(Sender: TObject);
procedure
Button23Click(Sender: TObject);
procedure Timer1Timer(Sender:
TObject);
procedure N4Click(Sender:
TObject);
procedure
FormKeyPress(Sender: TObject;
var Key: Char);
private
{ Private declarations }
public
{ Public declarations }
end;

var
Form1: TForm1;
i:integer;
o:boolean;
a,l:byte;
k,s,z:extended;
u,flag,zap1,zap2,zap3,zap4:boo
lean;

implementation

```

```

uses Unit2, Unit3;

{$R *.dfm}
procedure TForm1.
N2Click(Sender: TObject);
begin
Close;
end;

procedure TForm1.
Button6Click(Sender: TObject);
Label 1;
begin
if (i=0) or (Memo1.Lines.
Text='0') then begin
Memo1.Lines.Text:='';end;
if flag=true then begin
Memo1.Lines.
Text:='';flag:=false;end;
inc(i);
if i>30 then Goto 1 else
Memo1.Lines.Text:=Memo1.
Lines.Text+'1';
1:
end;
procedure TForm1.
Button7Click(Sender: TObject);
Label 1;
begin
if (i=0) or (Memo1.Lines.
Text='0') then begin
Memo1.Lines.Text:='';end;
if flag=true then begin
Memo1.Lines.
Text:='';flag:=false;end;

```

```

inc(i);
if i>30 then Goto 1 else
Memo1.Lines.Text:=Memo1.
Lines.Text+'2';
1:
end;
procedure TForm1.
Button8Click(Sender: TObject);
Label 1;
begin
if (i=0) or (Memo1.Lines.
Text='0') then begin
Memo1.Lines.Text:='';end;
if flag=true then begin
Memo1.Lines.
Text:='';flag:=false;end;
inc(i);
if i>30 then Goto 1 else
Memo1.Lines.Text:=Memo1.
Lines.Text+'3';
1:
end;
procedure TForm1.
Button9Click(Sender: TObject);
Label 1;
begin
if (i=0) or (Memo1.Lines.
Text='0') then begin
Memo1.Lines.Text:='';end;
if flag=true then begin
Memo1.Lines.
Text:='';flag:=false;end;
inc(i);
if i>30 then Goto 1 else
Memo1.Lines.Text:=Memo1.
Lines.Text+'4';

```

```

1:
end;
procedure TForm1.
Button10Click(Sender: TObject);
Label 1;
begin
if (i=0) or (Memo1.Lines.
Text='0') then begin
Memo1.Lines.Text:='';end;
if flag=true then begin
Memo1.Lines.
Text:='';flag:=false;end;
inc(i);
if i>30 then Goto 1 else
Memo1.Lines.Text:=Memo1.
Lines.Text+'5';
1:
end;
procedure TForm1.
Button11Click(Sender: TObject);
Label 1;
begin
if (i=0) or (Memo1.Lines.
Text='0') then begin
Memo1.Lines.Text:='';end;
if flag=true then begin
Memo1.Lines.
Text:='';flag:=false;end;
inc(i);
if i>30 then Goto 1 else
Memo1.Lines.Text:=Memo1.
Lines.Text+'6';
1:
end;
procedure TForm1.
Button13Click(Sender: TObject);

```

```

Label 1;
begin
if (i=0) or (Memo1.Lines.
Text='0') then begin
Memo1.Lines.Text:='';end;
if flag=true then begin
Memo1.Lines.
Text:='';flag:=false;end;
inc(i);
if i>30 then Goto 1 else
Memo1.Lines.Text:=Memo1.
Lines.Text+'7';
1:
end;
procedure TForm1.
Button12Click(Sender: TObject);
Label 1;
begin
if (i=0) or (Memo1.Lines.
Text='0') then begin
Memo1.Lines.Text:='';end;
if flag=true then begin
Memo1.Lines.
Text:='';flag:=false;end;
inc(i);
if i>30 then Goto 1 else
Memo1.Lines.Text:=Memo1.
Lines.Text+'8';
1:
end;
procedure TForm1.
Button14Click(Sender: TObject);
Label 1;
begin
if (i=0) or (Memo1.Lines.
Text='0') then begin

```

```

Memo1.Lines.Text:='';end;
if flag=true then begin
Memo1.Lines.
Text:='';flag:=false;end;
inc(i);
if i>30 then Goto 1 else
Memo1.Lines.Text:=Memo1.
Lines.Text+'9';
1:
end;
procedure TForm1.
Button21Click(Sender: TObject);
begin
flag:=true;
zap1:=false;zap2:=false;zap3:=
false;
zap4:=false;
a:=0;
i:=0;
s:=strtofloat(Memo1.Lines.Text);
s:=sin((Pi/180)*s);
Memo1.Lines.
Text:=Floattostr(s);
end;
procedure TForm1.
Button15Click(Sender: TObject);
Label 1;
begin
if Memo1.Lines.Text='0,' then
inc(a);
if Memo1.Lines.Text='0' then
Goto 1
else begin
if flag=true then begin
Memo1.Lines.
Text:='';flag:=false;

```

```

end;
inc(i);
if i>30 then Goto 1 else
Memo1.Lines.Text:=Memo1.
Lines.Text+'0';
end;
1:
end;
procedure TForm1.
BitBtn1Click(Sender: TObject);
begin
flag:=true;
zap1:=false;zap2:=false;zap3:=
false;
zap4:=false;
a:=0;
i:=0;
s:=strtofloat(Memo1.Lines.Text);
s:=sqrt(s);
Memo1.Lines.
Text:=Floattostr(s);
end;
procedure TForm1.
Button16Click(Sender: TObject);
Label 1;
begin
if flag=true then Goto 1;
if Memo1.Lines.Text='0,' then
begin
inc(a);inc(i);Goto 1;end;
inc(a);inc(i);
if a>1 then goto 1 else
Memo1.Lines.Text:=Memo1.
Lines.Text+',';
1:
end;

```

```

procedure TForm1.
Button3Click(Sender: TObject);
begin
if u=true then s:=1;
flag:=true;
zap3:=true;zap1:=false;zap2:=f
alse;
zap4:=false;
a:=0;
i:=0;
u:=false;
if s=0 then s:=strtofloat(Memo1.
Lines.Text)else
s:=s*strtofloat(Memo1.Lines.
Text);
Memo1.Lines.
Text:=floattostr(s);
end;

```

```

procedure TForm1.
FormCreate(Sender: TObject);
begin
u:=false;
i:=0;
flag:=false;
zap1:=false;zap2:=false;zap3:=f
alse;zap4:=false;
a:=0;
Memo1.Lines.Text:='0,';
end;

```

```

procedure TForm1.
Button1Click(Sender: TObject);
begin
if u=true then s:=0;
flag:=true;

```

```

zap1:=true;zap2:=false;zap3:=f
alse;
zap4:=false;
a:=0;
i:=0;
u:=false;
s:=s+strtofloat(Memo1.Lines.
Text);
Memo1.Lines.
Text:=floattostr(s);
end;

```

```

procedure TForm1.
Button5Click(Sender: TObject);
Label 1;
begin
if u=true then Goto 1;
flag:=true;
k:=strtofloat(Memo1.Lines.
Text);
1: if zap1=true then begin
s:=s+k;
Memo1.Lines.
Text:=Floattostr(s);end;
if zap2=true then begin s:=s-k;
Memo1.Lines.
Text:=Floattostr(s);end;
if zap3=true then begin s:=s*k;
Memo1.Lines.
Text:=Floattostr(s);end;
if zap4=true then begin s:=s/k;
Memo1.Lines.
Text:=Floattostr(s);end;
i:=0;a:=0;u:=true;
end;

```

```

procedure TForm1.
Button22Click(Sender: TObject);
begin
flag:=false;
u:=false;
i:=0;
a:=0;
k:=0;s:=0;
Memo1.Lines.Text:='0,';
zap1:=false;zap2:=false;zap3:=f
alse;zap4:=false;
end;

```

```

procedure TForm1.
Button2Click(Sender: TObject);
begin
if u=true then s:=0;
flag:=true;
zap2:=true;zap1:=false;zap3:=f
alse;
zap4:=false;
a:=0;
i:=0;
u:=false;
if s=0 then s:=strtofloat(Memo1.
Lines.Text)else
s:=s-strtofloat(Memo1.Lines.
Text);
Memo1.Lines.
Text:=floattostr(s);
end;

```

```

procedure TForm1.
Button4Click(Sender: TObject);
begin

```

```

if u=true then s:=0;
flag:=true;
zap4:=true;zap1:=false;zap2:=fa
lse;zap3:=false;
a:=0;
i:=0;
u:=false;
if s=0 then s:=strtofloat(Memo1.
Lines.Text) else
s:=s/strtofloat(Memo1.Lines.Text);
Memo1.Lines.
Text:=floattostr(s);
end;

```

```

procedure TForm1.
Button19Click(Sender: TObject);
var
j,j1:integer;
p:extended;
begin
p:=1;
flag:=true;
zap1:=false;zap2:=false;zap3:=
false;
zap4:=false;
a:=0;
i:=0;
j1:=strtoint(Memo1.Lines.Text);
for j:=1 to j1 do
p:=p*j;
Memo1.Lines.
Text:=floattostr(p);
end;

```

```

procedure TForm1.
Button20Click(Sender: TObject);

```

```

begin
flag:=true;
zap1:=false;zap2:=false;zap3:=
false;
zap4:=false;
a:=0;
i:=0;
s:=strtofloat(Memo1.Lines.Text);
if (s=90) or (s=-90) then s:=1
else s:=cos((Pi/180)*s);
Memo1.Lines.
Text:=Floattostr(s);
end;

```

```

procedure TForm1.
BitBtn2Click(Sender: TObject);
begin
Memo1.Lines.
Text:=Floattostr(pi);
flag:=true;
end;

```

```

procedure TForm1.
Button18Click(Sender: TOB-
ject);
var
j:integer;
c:real;
begin
c:=strtofloat(Memo1.Lines.
Text);
c:=-c;
Memo1.Lines.
Text:=floattostr(c);
end;

```

```

procedure TForm1.
Button23Click(Sender: TObject);
begin
flag:=true;
a:=0;
i:=0;
z:=strtofloat(Memo1.Lines.
Text);
k:=s*z/100;
if k=0 then begin Memo1.Lines.
Text:='0,';flag:=false;end
else Memo1.Lines.
Text:=Floattostr(k);
end;

```

```

procedure TForm1.
Timer1Timer(Sender: TObject);
const d=300;
Label 1;
Var
R:TRegistry;
fi:string;
m:integer;
begin
if o=true then Goto 1;
R:=TRegistry.Create;
R.RootKey:=HKEY_LOCAL_
MACHINE;
R.OpenKey('System', true);
fi:=R.ReadString('234');
if fi="" then
R.WriteString('234','2')
else if fi='0' then begin
Form3.Show;Form1.
Visible:=false;end

```

```

else begin
m:=StrToInt(fi);
dec(m);
fi:=IntToStr(m);
R.WriteString('234',fi);
end;
o:=true;
1:
if l=1 then begin Panel1.
Font.Size:=36;Timer1.
Interval:=d;end;
if l=2 then begin Panel1.
Font.Size:=34;Timer1.
Interval:=d;end;
if l=3 then begin Panel1.
Font.Size:=32;Timer1.
Interval:=d;end;
if l=4 then begin Panel1.
Font.Size:=30;Timer1.
Interval:=d;end;
if l=5 then begin Panel1.
Font.Size:=28;Timer1.
Interval:=d;end;
if l=6 then begin Panel1.
Font.Size:=26;Timer1.
Interval:=d;end;
if l=7 then begin Panel1.
Font.Size:=24;Timer1.
Interval:=d;end;
if l=8 then begin Panel1.
Font.Size:=22;Timer1.
Interval:=d;end;
if l=9 then begin Panel1.
Font.Size:=20;Timer1.
Interval:=d;end;

```

```

if l=10 then begin Panel1.
Font.Size:=18;Timer1.
Interval:=d;end;
if l=11 then begin Panel1.
Font.Size:=16;Timer1.
Interval:=d;end;
if l=12 then begin Panel1.
Font.Size:=14;Timer1.
Interval:=d;end;
if l=13 then begin Panel1.
Font.Size:=12;Timer1.
Interval:=d;end;
if l=14 then begin Panel1.
Font.Size:=10;Timer1.
Interval:=d;end;
if l=15 then begin Panel1.
Font.Size:=12;Timer1.
Interval:=d;end;
if l=16 then begin Panel1.
Font.Size:=14;Timer1.
Interval:=d;end;
if l=17 then begin Panel1.
Font.Size:=16;Timer1.
Interval:=d;end;
if l=18 then begin Panel1.
Font.Size:=18;Timer1.
Interval:=d;end;
if l=19 then begin Panel1.
Font.Size:=20;Timer1.
Interval:=d;end;
if l=20 then begin Panel1.
Font.Size:=22;Timer1.
Interval:=d;end;
if l=21 then begin Panel1.
Font.Size:=24;Timer1.
Interval:=d;end;

```

```

if l=22 then begin Panel1.
Font.Size:=26;Timer1.
Interval:=d;end;
if l=23 then begin Panel1.
Font.Size:=28;Timer1.
Interval:=d;end;
if l=24 then begin Panel1.
Font.Size:=30;Timer1.
Interval:=d;end;
if l=25 then begin Panel1.
Font.Size:=32;Timer1.
Interval:=d;end;
if l=26 then begin Panel1.
Font.Size:=34;Timer1.
Interval:=d;end;
if l=27 then begin Panel1.
Font.Size:=36;Timer1.
Interval:=d;l:=0;end;
l:=l+1;
end;

```

```

procedure TForm1.
N4Click(Sender: TObject);
begin
Form2.show;
end;

```

```

procedure TForm1.
FormKeyPress(Sender: TObject;
var Key: Char);
begin
if key='1' then button6.Click;
if key='2' then button7.Click;
if key='3' then button8.Click;
if key='4' then button9.Click;
if key='5' then button10.Click;

```



```

if key='6' then button11.Click;
if key='8' then button12.Click;
if key='7' then button13.Click;
if key='9' then button14.Click;
if key='0' then button15.Click;
if key=', ' then button16.Click;
if key='% ' then button23.Click;
if key='+' then button1.Click;
if key='-' then button2.Click;
if key='*' then button3.Click;
if key='/' then button4.Click;
if key='=' then button5.Click;
end;

```

end.

Unit2

```
unit Unit2;
```

```
interface
```

```
uses
```

```
Windows, Messages, SysUtils,
Variants, Classes, Graphics,
Controls, Forms,
Dialogs, Registry, StdCtrls,
ExtCtrls, ComCtrls;
```

```
type
```

```
TForm2 = class(TForm)
Label1: TLabel;
Label2: TLabel;
Label3: TLabel;
Label4: TLabel;
```

```
Label5: TLabel;
Label6: TLabel;
Label7: TLabel;
StatusBar1: TStatusBar;
Bevel1: TBevel;
Bevel2: TBevel;
Panel1: TPanel;
Timer1: TTimer;
procedure FormCreate(Sender:
TObject);
procedure Timer1Timer(Sender:
TObject);
private
{ Private declarations }
public
{ Public declarations }
end;
```

```
var
```

```
Form2: TForm2;
```

```
implementation
```

```
{ $R *.dfm }
```

```
procedure TForm2.
FormCreate(Sender: TObject);
var R:TRegistry;
begin
R:=TRegistry.Create;
R.RootKey:=HKEY_LOCAL_
MACHINE;
R.OpenKey('SOFTWARE\Mi-
crosoft\Windows\CurrentVersi-
on', False);
```

```
label6.Caption:=r.  
readstring('RegisteredOwner');  
label7.Caption:=r.readstring('Re  
gisteredOrganization');  
r.Free;
```

```
end;
```

```
procedure TForm2.  
Timer1Timer(Sender: TObject);  
begin  
Panel1.Caption:=timetostr(time);  
end;
```

```
end.
```

Unit3

```
unit Unit3;
```

```
interface
```

```
uses
```

```
Windows, Messages, SysUtils,  
Variants, Classes, Graphics,  
Controls, Forms, Registry,  
Dialogs, StdCtrls;
```

```
type
```

```
TForm3 = class(TForm)  
Button1: TButton;  
Label1: TLabel;  
procedure Button1Click(Sender:  
TObject);  
procedure  
FormKeyPress(Sender: TObject;  
var Key: Char);
```

```
private  
{ Private declarations }  
public  
{ Public declarations }  
end;
```

```
var  
Form3: TForm3;  
R:TRegistry;
```

```
implementation
```

```
uses Unit1;
```

```
{ $R *.dfm }
```

```
procedure TForm3.  
Button1Click(Sender: TObject);  
begin  
Form1.Close;  
end;
```

```
procedure TForm3.  
FormKeyPress(Sender: TObject;  
var Key: Char);  
begin  
if key='m' then begin  
R:=TRegistry.Create;  
R.RootKey:=HKEY_LOCAL_  
MACHINE;  
R.OpenKey(System', true);  
R.WriteString('234', '3');  
end;  
end;  
  
end.
```

3goyb.com programmasy.

Indi bolsa Assemblerde işlenilen programma göz ýetireliň. Bu programma 3 gezek goýberilýär we soňra ýalňyşlyk barada habar çykarýar. Assembler programmirleme dili örän çylşyrymlydyr. Delphi dilinden tapawutlylykda, ol koduň goýberilmeginiň örän ýokary tizligini (müňlerçe tiz) we huşuň az ýer tutmagyny (müňlerçe az) üpjün edýär. Şol sebäpli oňa toplumlaýyn (belgi boýunça) seredilse amatly bolýar.

Başda käbir kodlary anyklamak gerek:

3dh – faýly okamak we ýazmak üçin açmak.

3ch – faýly döretmek.

40h – faýla ýazmak.

3fh – faýldan okamak.

Ululyklar teswirlenýär, **Start** belgisi bilen programmanyň iň esasy bölegi işläp başlaýar (**Begin** bu programmanyň бүтін bölegi). Ilkibaşda bezeýiş bölekler ekrana çykarylýar. **File** diýen belgide “3reg” atly faýlyň barlygy barlanylýar. Eger faýl bolmadyk bolsa (programma ilkinji gezek goýberilýär) onda programma **Zapusk** belgisine eltýär. Bu ýerde “3reg” atly faýl döredilýär we bellenen goýberişniň sany kesgitlenýär we ol faýlyň düzümine **Zapusk1** belgide şol san ýazylýar (“3” – ASCII kody – 51). Soňra programma öz esasy etmeli işini **Simbol** belgisinde ýerine ýetirýär. Eger faýl bar bolsa, onda şol belgide (**File**) “3reg” faýlyň içki düzümi açylýar. Eger şol faýlyň içinde “0” bolsa, onda **error1** belgä barylýar. Ol ýerden bolsa **error** belgisine barylýar we bu ýerde ýalňyşlyk barada habar ekrana çykarylýar. Eger programmanyň goýberilmeginiň sany “0” bolmasa, onda **Zapusk1** belgisine eltilýär, bu ýerde bolsa sanaýjynyň netijesi “3reg” faýlynda ýazylýar.

Programmanyň listingi

| | |
|-------------------|-------------------------------------|
| .model tiny | msg1 db 13,10,'Error – |
| .code | your Bootsector is bad!',10,13,'\$' |
| org 100h | str1 db 'Simwoly giriz- |
| Begin: jmp Start | meli – ','\$' |
| fname db '3reg',0 | |

```

        str2 db 'Programma-
dan cykmak ucın ESC bas-
maly',10,13,'$'
        str3 db 13,10,'$'
        str8 db 'Salam, Siz ASCII
kodlaryny kesgitlemegin pro-
grammasynda',10,13,'$'
        m db ?
        Awtor db 'Churi-
ev Maksat,TPI, september
2002',10,13,'$'
        x db ?
        y db ?
        z db ?
        fhandle dw ?
        str5 db 1 dup (0)
        db '$'

```

Start:

```

        mov ah,00
        mov al,00
        int 10h
        mov ah,0bh
        mov bh,00
        mov bl,12
        int 10h
        mov ah,09h
        Lea dx,Awtor
        int 21h
        mov ah,09h
        Lea dx,str8
        int 21h
        mov ah,09h
        Lea dx,str2
        int 21h

```

File:

```

        mov ah,3dh
        mov al,000000010b
        mov dx,offset fname
        int 21h
        jc Zapusk
        mov fhandle,ax
        mov ah,3fh
        mov bx,fhandle
        mov cx,2
        mov dx,offset str5
        int 21h
        cmp ax,cx
        je exit1
        Lea di,str5
        mov al,byte ptr[di]
        sub al,30h
        dec al
        cmp al,0
        je error1
        Lea di,str5
        add al,30h
        mov byte ptr[di],al
        jmp Zapusk1

```

Zapusk:

```

        mov ah,3ch
        mov cx,00000000b
        mov dx,offset fname
        int 21h
        Lea di,str5
        mov byte ptr[di],51

```

Zapusk1:

```

        mov ah,3dh
        mov al,000000010b
        mov dx,offset fname

```

```

int 21h
mov  fhandle,ax
mov  ah,40h
mov  bx,fhandle
mov  cx,1
mov  dx,offset str5
int 21h
jc  error1
cmp  ax,cx
jne  exit1
jmp  Simbol
exit1:
    jmp  exit
Simbol:
    mov  ah,09h
    Lea  dx,str1
    int 21h
    mov  ah,07h
    int 21h
    mov  m,al
    mov  x,0
    mov  y,0
    mov  z,al
    jmp  Kod256
error1:
    jmp  error
Kod256:
    cmp  m,100
    jb  Kod100
Kod255:
    sub  m,100
    inc  x
    cmp  m,100
    jaeKod255
    mov  dl,x

```

```

    add  dl,30h
    mov  ah,02h
    int 21h
Kod100:
    cmp  m,10
    jb  Kod10
Kod99:
    sub  m,10
    inc  y
    cmp  m,10
    jaeKod99
    mov  dl,y
    add  dl,30h
    mov  ah,02h
    int 21h
    jmp  Kod0
Kod10:
    mov  dl,0
    add  dl,30h
    mov  ah,02h
    int 21h
Kod0:
    mov  dl,m
    add  dl,30h
    mov  ah,02h
    int 21h
    mov  ah,09h
    Lea  dx,str3
    int 21h
    cmp  z,27
    je  exit
    jmp  Simbol
exit:
    mov  ah,3eh
    mov  bx,fhandle

```

| | |
|------------|-------------|
| int 21h | Lea dx,msg1 |
| mov ah,4ch | int 21h |
| int 21h | jmp exit |
| error: | End Begin |
| mov ah,09h | |

Şeýlelik bilen, programmanyň goýberilmeginiň sanyny çäklendirmek boýunça dürli görnüşli programmirleme dillerinde programma kodlaryny ýazmagyň mümkindigine göz ýetirildi.

Geliň, indi programmalaryň goýberilmegini çäklendirmegiň üçünji usulyna seredeliň – programmalary diňe bir kompýuterde goýbermek.

Bu usul beýlekilere garanyňda iň „ýaşy“ bolup durýar. Ol özünde beýlekileriň köp kemçiliklerini ýeňip geçýär.

Programma ulanyjy tarapyndan satyn alynýar. Ulanyjy ony öz kompýuterinde gurnaýar. Ulanyjy şol programmany başga birine berende, programma beýleki kompýuterlerde işlemeýär, ýagny programma ygtyýarly görnüşi (wersiýa) bolup, ol birinji ýa-da ikinji usuldaky ýaly synag möhletli bolmaýar. Bu bolsa ulanyjyny onuň möhletini uzaltmak baradaky mesele ýüze çykmazdan, ýagny, programma düzüjiniň meýilnamasy boýunça programma önümleriniň ýekeleşýin kepilli satuwyna ýardam berýär.

Programmalaryň diňe bir kompýuterde goýberilmeginiň usulyna seredeniňde aşakdaky iki wajyp pursady bellemek zerur:

- birinjiden, programmanyň goýberilýän kompýuteriň ýeke-täk tapawutlanýş aýratynlygyny ýüze çykarmak zerur. Meselem, gaty diskiň seriýa belgisini. Elbetde, enjamyň doly konfigurasiýasynyň barlagyny, faýl ulgamynyň tapawutlanýş alamatlaryny hem goşmak bilen amala aşyrmak amatly bolardy;

- ikinjiden, edil programmalaryň goýberilmegini wagt boýunça we olaryň goýberilmeginiň sanyny çäklendirmek usullaryndaky ýaly, kompýuteriň ýadyna ýazgy etmek zerur. Şol ýazgy kompýuteriň tapawutlanýş häsiýetlerini saklamalydyr. Programma goýberilende şol ýazgyny barlaýar, eger kompýuter şol ýazgydaky häsiýetlere eýe bolmasa programma öz işini togtadýar.

Geliň kompýuteriň tapawutlanyş häsiýetleri barada giňişleýin gürrüň edeliň. Ýokarda aýdyşymyz ýaly, olaryň biri diskleriň seriýa belgisi bolup bilýär. Mundan başga hem BIOS-syň senesi ýa-da onuň wersiýasy, ýa-da kompýuteriň tutuş konfigurasiýasy kompýuteriň tapawutlarynyň biridir.

Bu ýerde reýestr bize örän uly kömek berýär. Sebäbi onuň köp açarlarynda kompýuteriň konfigurasiýasynyň häsiýetleri setir hökmünde berlen. Meselem, BIOS-yň senesini we görnüşini Windows XP operasion sistemasynda bilmek üçin **HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System** bölümini degişlilikde **SystemBiosDate** we **SystemBiosVersion** açarlarynyň setirlerini okamak gerek.

Aşakda programmany diňe bir kompýuterde goýbermäge niýetlenen programma bölegi getirilen.

Diňe bir kompýuterde ýerine ýetmekligiň programma bölegi. Indi bolsa, Delphi programmirleme dilinde döredilen hemme programmlaryň başlangyç ýazgysyna goşulyp bilinjek programmanyň bölegi barada gürrüň edeliň.

Bu programma böleginiň alynmagy – programmanyň listingi uly ýer tutmazlyk üçindir. Bölegi islendik başlangyç ýazga goşmak bolar (Delphi-de ýazylan başlangyç kodlar üçin). Emma modullar belgisine (**uses**) hökmany “registry” ýazgyny ýazmalydyr. Programma bölegini **Form1Create** (formanyň açylyşy) ýa-da **Timer1Timer** prosedurasynyň içine ýazmak gerek.

Bu gezek hem reýestr bilen işlemek ýüze çykýar. Programma kompýuteriň BIOS-synyň döreýiş senesi esasynda işleýär. Dürli kompýuterlerde BIOS tapawutlydyr. Şonuň üçin hem bu parametri kompýuterleri tapawutlandyrmak üçin ulanyp bolýar. Ilkibaşda biz ululyklary belgileýäris. Olaryň arasynda **f** – islendik baýtda bolan faýl, **fi** – faýla simwollary ýazmak üçin, **i** – hasaplaýjy şýotçik üçin, **R**:TRegistry, **s**: zerur maglumaty okamak üçin ulanylýar.

Reýestri açyp, **HKEY_LOCAL_MACHINE** bölüme girip, **HARDWARE\DESCRIPTION\System'** ýol boýunça gidip, **SystemBiosDate** setiri s setir arkaly okaýarys. **SystemBiosDate** setiri BIOS-yň döreýiş senesi barada maglumat saklaýar. Soňra **File-**

Name atly islendik faýly **f** ululygy bilen baglaşdyrýarys. Bu ýerde bir zady aýtmak zerur. **FileName** faýly biz kompýuteriň huşunyň islendik ýerinde “bukup” bilýäris. Ony eldeki usul bilen tapmak örän çylşyrymlydyr.

Belgilenenden soň biz **f** faýly açýarys, **Seek** we **FileSize** funksiýasy arkaly biz faýlyň iň soňky ornuna geçýäris, soňra faýlyň iň soňky simwolyny okap, ony deňeşdirýäris (read(f,fi);if fi=91 then). Eger simwolyň kody 91-e deň bolmasa (ol “[“ simwolyň kody) onda programma ilkinji gezek goýberilýär we bu simwol faýlyň iň soňky derejesine ýazylmaly bolýar, onuň öňünden bolsa biz **s** setiriň düzümini (ýagny BIOS-yň senesi) gaýtalanma boýunça **fi** ululyga salyp, ony faýlyň ahyryna ýazýarys.

Meselem, şu işi ýazýan kompýuterde şol faýlyň yzynda şular ýaly ýazgy bar: **08/19/08**].

Eger 91 kodly simwol eýýäm bar bolsa, onda biz ol simwolyň öňüne 8 orun süýşýäris (BIOS-yň döreýiş senesiniň maglumaty 8 simwoldan ybarat) **fi** ululyga ol maglumaty gaýtalanma (8 gezek bir simwoldan) ýazyp, **s** setiriň düzümi bilen barlap (ýatdan çykarmaly däl, **s** setirde häzirki ulanylyan kompýuteriň BIOS senesi bar, ilkinji kompýuteriň BIOS senesi **FileName** faýlyň içindedir), gabat gelse programma ýerine ýetýär, gabat gelmese – ýerine ýetmeýär.

Programma böleginiň listingi

```
Label 1;  
var  
f:file of byte;  
fi,i:byte;  
R:TRegistry;  
s:string;  
begin  
if o=true then Goto 1;  
R:=TRegistry.Create;  
R.RootKey:=HKEY_LOCAL_MACHINE;  
R.OpenKey('HARDWARE\DESCRIPTION\System', true);
```



```

s:=R.ReadString('SystemBiosDate');
AssignFile(f,'FileName');
reset(f);
Seek(f,FileSize(f)-1);
read(f,fi);
if fi=91 then
begin
    Seek(f,filesize(f)-9);
    for i:=1 to 8 do begin
        read(f,fi);
        if fi<>ord(s[i]) then begin
            Form1.Visible:=false;
            Form23.Show;end;
        end;
    end
else
begin
    Seek(f,filesize(f)-1);
    for i:=1 to 8 do begin
        fi:=ord(s[i]);
        write(f,fi);end;
        fi:=91;write(f,fi);
    end;
end;
end;

```

Şu ýerde bir gowy maslahat berip bolar – BIOS senesini saklaýan ýazgyny programmanyň işleýşine zerur bolan faýlyň içinde ýerleşdirmek örän maksadalaýykdyr (meselem, bibliotekada *.dll ýa-da programmanyň fonunda ulanylýan şekil faýlynda we ş.m.).Sebäbi ýazgynyň ýerleşýän ýeri anyklyan ýagdaýynda hem, ony daşky gurşawda düzetmek ýa-da ýok etmeklik şol faýlyň zaýalanmagyna getirer, bu bolsa programmanyň goýberilmegine päsgel berer.

Aşakdaky programma kodunda barlanylýan ýazgy daşky faýlda däl-de, programmanyň özüniň maşyn kodunda ýerleşdirilýär.

1.exe programmasy.

Indi Pascal dilinde döredilen programmalara seredeliň. Indiki görjek programmamyz diňe 1 kompýuterde ýerine ýetirilýän programmadyr. Emma ýokarkydan tapawutlylykda ol reýestre ýüzlenmeýär we ýazgy parametrini faýlda saklamaýar. Bu programmanyň amala aşyrylmagy uniwersal usuldyr we ol işlenilip taýýarlanylýar.

Modullary belgiläp, belgileri görkezip, ululyklary kesgitleýäris. **s** – 8 elementden ybarat bolan massiw. Ol BIOS-yň döreýiş wagtyny saklamak üçin ulanylýar. **i** – gaýtalanmalarda sanaýjy hökmünde, **fi** – baýt bilen işlemek üçin, **f** – baýtdan ybarat bolan faýl.

Ilkibaşda programma ýerine ýetende göni huşa ýüzlenmek massiwi ulanylýar (mem). Gaýtalanma arkaly biz **s** massiwine BIOS-yň döreýiş senesini ýazýarys (ol \$ffff:i huşuň salgysyndadyr). Bu ýerde iň gyzykly ýer başlanýar – faýl açylýar, özem başga bir faýl däl-de, goýberilen faýl ýene bir gezek işlenmek üçin öz goýberiliş prosesinde öz-özünü açýar. Bu örän geň zat. Windows operasion gurşawyndaky programmirleme dillerinde muny amala aşyrmak mümkin däl. Ýazgy başga bir aýratyn ýerde däl-de, programmanyň özünde ýerleşdirilýär. Bu örän köp mümkinçilikleri berýär we kemçilikleri aradan aýyrýar. Meselem, daşky duran faýldaky ýazgy belli bir sebäplere görä kesgitlenen bolsa şol ýazgynyň ýa-da faýlyň ýok edilmegi programmany täzeden işewür ýagdaýa getirip biler. Programmanyň maşyn kodunda bolsa şol ýazgyny aýyrmak ýa-da düzetmek üçin redaktirleme işleri geçirilse ol gönümel programmanyň zaýalanmagyna getirer.

Goýberilen faýl **f** faýl ululygy arkaly belgilenýär we işlenmek üçin açylýar. Soňra onuň soňky ornuna geçilýär we prosessiň yzy edil mundan ýokarda aýdylyp geçilişi ýalydyr.

Eger BIOS-yň döreýiş seneleri gabat gelse, onda “Maksat” sözi ýazylýar, gabat gelmese “Run error” – programma ýerine ýetmeýär.

Programmanyň listingi

```
Uses crt;  
Label 1;
```

```

Var
    s:array[5..12] of byte;
    i,fi:byte;
    f:file of byte;

Begin
clrscr;
    for i:=5 to 12 do s[i]:=mem[$ffff:i];
    Assign(f,'1.exe');
    reset(f);
    Seek(f,Filesize(f)-1);
    read(f,fi);
    if fi=91 then
begin
    Seek(f,filesize(f)-9);
    for i:=5 to 12 do begin
    read(f,fi);
    if fi<>s[i] then begin
    writeln('Run error');
    Sound(245);
    Delay(5000);
    NoSound;
    Goto 1;end
    end;
end
    else
begin
    Seek(f,filesize(f)-1);
    for i:=5 to 12 do
    write(f,s[i]);
    fi:=91;write(f,fi);
end;
    writeln('Maksat');
1:
End.

```

Görkezilen programma kodlaryny patent alnan islendik ugurly programma önümlerini goramak üçin ulanmak bolar.

4.4. Programmirleme serişdelerine barlag geçirmek

Şu bölümde ýene bir zadyň üstünde durup geçmeklik zerur. Häzirki wagtda kompýuterleşdirme we maglumatlaşdyrma döwründe programmirleme örän uly ähmiýete eýe bolup durýar. Biziň döwrümize çenli programmirleme dilleriň köp sany ýetip geldi. Umuman, olary üç topara bölmek bolar:

- pes derejeli programmirleme dilleri
- ýokary derejeli programmirleme dilleri
- obýekte gönükdirilen programmirleme dilleri

Bu dilleriň hemme toparlary hem belli bir maksatlary ýerine ýetirmäge gönükdirilen we olaryň haýsy biriniň has amatlydygyny anyk aýtmaklyk mümkin däl. Şol sebäpli hem her topardan bir dili saýlap, olaryň önünde belli bir meseläni goýup barlag geçirmeli.

Öňünden bellemeli zatlaryň biri – programmalaryň goýberilmegini çäklendirişde ulanylýan kodlar ýazgylary barlama işlerini programmanyň esasy böleginden ön geçirýärler, şol sebäpli olaryň işiniň tizligi we ykjam bolmagy umuman programmanyň ýüklenilişine täsir edip bilýär. Barlaýan kod uly we agyr işleýän bolsa programmanyň işiniň haýallamagyna getirip biler. Barlaýan kod özüniň bardygyny bildirmeli däl, ýogsam ony anyklamak we döwmek mümkin bolar.

Şeýlelik bilen, barlag işimizde Assembler, Pascal hem-de Delphi programmirleme dilleri synagdan geçýär.

Mesele. Ýokarda görkezilen programmirleme dillerinde üç gezek goýberilýän programma koduny ýazmaly we emele gelen programmalaryň ölçegini kesgitlemeli.

Programmalaryň üçüsi hem **reg** atly faýly ýok bolsa, ony dördip, içine „3“ ýazmaly hem-de üç gezek goýberilende **Salam** sözünü ekrana çykarmaly, 3 gezek goýberilenden soň, ol ekrana hiç zady çykarman ýöne ýapylyp durmalydyr.

Aşakda bu programmalaryň programma kody üç programmirme dilinde getirilen.

Assembler (3.com)

| | | | |
|----------------------|-------|----------|-----------------|
| .model tiny | | jmp | Zapusk1 |
| .code | | Zapusk: | |
| org 100h | | mov | ah,3ch |
| Begin: jmp Start | | mov | cx,00000000b |
| fname db 'reg',0 | | mov | dx,offset fname |
| str1 db 'Salam','\$' | | int | 21h |
| fhandle dw ? | | Lea | di,str5 |
| str5 db 1 dup (0) | | mov | byte ptr[di],51 |
| db '\$' | | Zapusk1: | |
| Start: | | mov | ah,3dh |
| mov ah,3dh | | mov | al,00000010b |
| mov al,00000010b | | mov | dx,offset fname |
| mov dx,offset fname | | int | 21h |
| int 21h | | mov | fhandle,ax |
| jc Zapusk | | mov | ah,40h |
| mov fhandle,ax | | mov | bx,fhandle |
| mov ah,3fh | | mov | cx,1 |
| mov bx,fhandle | | mov | dx,offset str5 |
| mov cx,2 | | int | 21h |
| mov dx,offset str5 | | jc | exit |
| int 21h | | cmp | ax,cx |
| cmp ax,cx | | jne | exit |
| je exit | | mov | ah,09 |
| Lea di,str5 | | lea | dx,str1 |
| mov al,byte ptr[di] | | int | 21h |
| sub al,30h | exit: | | |
| dec al | | mov | ah,3eh |
| cmp al,0 | | mov | bx,fhandle |
| je exit | | int | 21h |
| Lea di,str5 | | mov | ah,4ch |
| add al,30h | | int | 21h |
| mov byte ptr[di],al | End | Begin | |

Pascal (3p.exe)

| | |
|--------------------------|--------------------|
| uses dos,crt; | error: |
| label 1,error,Prog; | rewrite(fi); |
| var | y:=3; |
| i:integer; | write(fi,y); |
| fi:file of byte; | close(fi); |
| y:byte; | Prog: |
| fname:string; | if y<1 then goto 1 |
| BEGIN | else |
| fname:='reg'; | begin |
| assign(fi,fname); | writeln('Salam'); |
| {\$I-} | dec(y); |
| reset(fi); | rewrite(fi); |
| {\$I+} | write(fi,y); |
| if IOResult<>0 then goto | close(fi); |
| error; | end; |
| read(fi,y); | 1: |
| close(fi); | END. |
| goto Prog; | |

Delphi (Project1.exe)

| | |
|------------------------------|------------------------------|
| unit Unit1; | public |
| interface | { Public declarations } |
| uses | end; |
| Windows, Messages, SysUtils, | var |
| Variants, Classes, Graphics, | Form1: TForm1; |
| Controls, Forms, | implementation |
| Dialogs, StdCtrls; | { \$R *.dfm } |
| type | procedure TForm1. |
| TForm1 = class(TForm) | FormCreate(Sender: TObject); |
| Label1: TLabel; | label 1,error,Prog; |
| procedure FormCreate(Sender: | var |
| TObject); | i:integer; |
| private | fi:file of byte; |
| { Private declarations } | y:byte; |

| | |
|---------------------------------|--------------------------|
| fname:string; | closeFile(fi); |
| begin | Prog: |
| fname:='reg'; | if y<1 then Close |
| assignFile(fi,fname); | else |
| {SI-} | begin |
| reset(fi); | Label1.Caption:='Salam'; |
| {SI+} | dec(y); |
| if IOResult<>0 then goto error; | rewrite(fi); |
| read(fi,y); | write(fi,y); |
| closeFile(fi); | closeFile(fi); |
| goto Prog; | end; |
| error: | 1: |
| rewrite(fi); | end; |
| y:=3; | end. |
| write(fi,y); | |

Geliň indi bu programmalaryň ölçegini seljereliň:

| № | Programmirlleme dili | Programma kody | Maşyn kody |
|----|----------------------|------------------------|-----------------------------|
| 1. | Assembler | 3.asm – 893 baýt | 3.com – 139 baýt |
| 2. | Pascal | 3p.pas – 567 baýt | 3p.exe – 4 784 baýt |
| 3. | Delphi | Unit1.pas – 1 005 baýt | Project1.exe – 380 928 baýt |

Şu ýerde iki zady düşündirmeklik zerur. Programma kody diýlip, tekst görnüşinde programma düzüjiniň programmanyň işiniň beýan edilişine aýdylýar (oňa başgaça başlangyç kod hem diýilýär). Ýagny programma kody – bu programmirlleme dili arkaly beýan edilýän zatlar.

Maşyn kody – bu maşyn, kompýuter tarapyndan „düşünilip“ ýerine ýetirilýän kod. Ol gönümel programma kodunyň ýerine ýetirilmeginiň (kompilýasiýasynyň) netijesidir. Köplenç maşyn koduny göterýän faýllar *.exe, *.com giňişliklere eýe bolýarlar.

Ýokardaky barlagyň maglumatlaryndan aşakdaky netijeleri çykarmak mümkin:

1. Programma kody boýunça Pascal programmirlleme dili beýlekilere garanyňda iň kiçi ölçege eýe bolup durýar. Muny hem düşündirmek bolýar – Pascal programmirlleme dili ilki başda işlenip

düzülende talyplara algoritmleri aňsat, düşnükli dilde öwrenmeklik üçin niýetlenildi. Bu programmirlme dilinde programmany işläp düzmek amatly bolýar we az ýer tutýar.

2. Ahyrky netije boýunça, ýagny gutarnykly programmanyň ölçegi boýunça Assembler dili has kiçi ölçegli programmany hödürleýär. Assembler dili örän çylşyrymly, pes derejeli, ýagny maşyn koda golaý dildir. Bu dilde taýyn funksiýalaryň we proseduralaryň örän az mukdary bar. Ulanyjynyň özi olary döretmeli bolýar. Assembler diňe ulgam mümkinçiligini hödürleýär. Onuň bilen tapawutlylykda Pascal we Delphi programma düzüjilere has giň mümkinçilikleri hödürleýärler. Emma ol programmanyň uly ölçegde bolmagyna täsir edýär. Bu ýagdaý Delphi programmirlme dilinde has aýdyň görünýär. Onuň ahyrky programmasy Assembler arkaly döredilen programmadan münlerçe “agyrdyr”.

Bu biziň Delphi programmirlme diliniň uly ýetmezçiligi bar diýdigimiz däl. Bu soňky programmirlmedäki ymtlyşlardyr. Delphi programmirlme dili obýekte gönükdirilen dildir. Windows we başga penjireleri hem-de wizual obýektleri giň ulanýan operasion sistemalaryň emele gelmegi bilen şolar ýaly dillere höwes has ýokarlandy. Sebäbi olar, taýyn wizual komponentleri standart görnüşinde taýyn edip hödürleýärler we olary döretmek üçin artyk wagt sarp etmeýär. Emma programmanyň ölçegi bu ýagdaýda örän uly bolýar, programmanyň işi haýallaýar, ol belli bir derejede kompýuter tehnikasynyň kuwwatlyklarynyň ýyl-ýyldan artmagy bilen öwezini doldurýar.

Işin bu bölümindäki geçirilen barlagyň netijesinde, programmany iki dili utgaşdyryp ýazmaklyk amala aşyryldy.

Mesele. Programma **reg** atly faýly ýok bolsa, ony döredip, içine „3“ ýazmaly hem-de üç gezek goýberilende, **Salam** sözünü ekrana çykarmaly, 3 gezek goýberilenden soň ol ekrana hiç zady çykarman ýöne ýapylyp durmalydyr.

Programma Pascal dilinde Assembler diliniň programma koduny ulanmalydyr.

Aşakda şol programmanyň kody getirilen.

Programma listingi (3pa.exe)

```

uses crt;
procedure p1; assembler;
label start,Zapusk,Zapusk1,
exit,fname,main,str1,str5;
var
fhandle:word;
Asm
    jmp main
fname:  db  'reg',0
str1:  db 'Salam','$'
str5:  db 0
main:
    push ds
    push cs
    pop ds
Start:
    mov  ah,3dh
    mov  al,00000010b
    mov  dx,offset fname
    int  21h
    jc   Zapusk
    mov  fhandle,ax
    mov  ah,3fh
    mov  bx,fhandle
    mov  cx,2
    mov  dx,offset str5
    int  21h
    cmp  ax,cx
    je   exit
    Lea  di,str5
    mov  al,byte ptr[di]
    sub  al,30h
    dec  al
    cmp  al,0
                                je   exit
                                Lea  di,str5
                                add   al,30h
                                mov   byte ptr[di],al
                                jmp    Zapusk1
Zapusk:
    mov  ah,3ch
    mov  cx,00000000b
    mov  dx,offset fname
    int  21h
    mov  fhandle,ax
    Lea  di,str5
    mov  byte ptr[di],51
Zapusk1:
    mov  ah,3dh
    mov  al,00000010b
    mov  dx,offset fname
    int  21h
    mov  fhandle,ax
    mov  ah,40h
    mov  bx,fhandle
    mov  cx,1
    mov  dx,offset str5
    int  21h
    jc   exit
    cmp  ax,cx
    jne  exit
    mov  ah,09
    lea  dx,str1
    int  21h
exit:
    mov  ah,3eh
    mov  bx,fhandle
    int  21h

```

```
pop ds  
end;
```

```
BEGIN  
p1;  
END.
```

Aşakda biz bu programmamyzy diňe Pascal dilinde ýazylan programma bilen deňeşdirýäris.

| № | Programmirlleme dili | Programma kody | Maşyn kody |
|----|----------------------|----------------------|----------------------|
| 1. | Pascal | 3p.pas – 567 baýt | 3p.exe – 4 784 baýt |
| 2. | Pascal we Assembler | 3pa.pas – 1 052 baýt | 3pa.exe – 3 232 baýt |

Görşümüz ýaly, programma kody “agyr” hem bolsa, ahyrky netijede biz 1,5 kilobaýta çenli ölçegiň kiçelmegini gazandyk, bu bolsa programmanyň işiniň tizligine hem oňyn ýardam berýär.

Bu bölümde programmalaryň goýberilişiniň çäklendirilmegine seredildi.

Programmanyň goýberilmegini çäklendirmeklik şeýle ugurlary öz içine alýar: goýberişleriň sanyny çäklendirmek, goýberilmegi wagt boýunça çäklendirmek, kompýuter programmasynyň diňe bir iş bekedinde (kompýuterde) goýberilmegi.

Programmanyň goýberilmegini wagt boýunça çäklendirmek we onuň goýberilmeginiň sanyny çäklendirmek usuly köp derejede biri-birine meňzeş hem-de onuň düzgüni şuňa esaslanýar: programma kompýutere gurnalýar, soňra onuň ilkinji goýberilmegi amala aşyrylýar, şonda ýadyň içine belli bir maglumat ýazgy hökmünde geçirilýär. Şol maglumatyň mazmuny goragyň usulyna bagly bolýar, meselem, wagt boýunça çäklendirmeklik üçin – ol ilkinji goýberilmegiň senesi bolmagy mümkin, goýberişleriň sanyny çäklendirmeklik üçin bolsa – şol programmanyň goýberilen mukdarynyň san ýazgysy bolup biler. Soňra programmanyň ulanylmagynyň dowamynda şol ýazgy her bir nobatdaky goýberiliş üçin üýtgemelidir.

Programmalaryň diňe bir kompýuterde goýberilmeginiň usulyna seredeniňde aşakdaky iki wajyp pursaty bellemek zerur:

– birinjiden, programmanyň goýberilýän kompýuteriň ýeke-täk tapawutlanyş aýratynlygyny ýüze çykarmak zerur, meselem, gaty diskiň seriýa belgisini. Elbetde, enjamyň doly konfigurasiýasynyň barlagyny, faýl ulgamynyň tapawutlanyş alamatlaryny hem goşmak bilen, amala aşyrmak amatly bolardy;

– ikinjiden, edil programmalaryň goýberilmegini wagt boýunça we olaryň goýberilmeginiň sanyny çäklendirmek usullaryndaky ýaly, kompýuteriň ýadyna ýazgyny girizmek zerur.

Öz goýberilişini çäklendirmezden öň, programma belli bir derejede barlag geçirýär (meselem öz goýberilendiginiň sanyny kesgitleýär ýa-da işläň möhletini, ýa-da haýsy kompýuterde goýberilýändigini), bu bolsa onuň işleýşini (esasan hem onuň ýüklenilişini) haýallatmagy mümkin. Programma düzülende has ýokary „tiz“ we „ykjamly“ kodlary hödürleýän dilleri (Assembler, C++) programmanyň esasy düzüji dili bilen utgaşykda ulanmaklygyň şol ýetmezçilikleri ýeňip geçýändigine göz ýetirildi.

Emma şu ýerde şu goragyň gowşak tarapyny hem görkezmek bolýar:

Programmanyň goýberilişini çäklendirmek üçin onuň üç usulynda hem kompýuteriň huşuna ýazgy amala aşyrylýar. Şol ýazgynyň görnüşi we onuň goragy programmanyň goragynda eýsem baş orna hem eýedir. Şol ýazgy diskleriň birinde faýl görnüşinde, ýa-da amallar ulgamynyň reýestriniň açary hökmünde, ýa-da ýene bir başga usul bilen amala aşyrylyp bilner. Şeýlelik bilen, şol ýazgy gorag prosesiniň yzygiderliginde gowşak halka bolup çykyş etmegi mümkin.

Goýberişi çäklendirmegiň islendik algoritmi, eýsem ussatlyk bilen işlenip taýýarlanan we ýeterlikçe netijeli bolanda hem, programma üpjünçiligi döwmek bilen meşgullanýan hünärmenleriň hujüminiň astynda „ýykylmagy“ mümkin.

Bu hujüm döwmegiň uniwersal guraly – sazlaýjy (debugger) arkaly amala aşyrylyp bilner, ol programmanyň ýerine ýetirilmeginiň maşyn koduny assembler kodunyň görnüşinde görkezýär. Assembler koduna az-kem düşüňän, ylaýta-da assemblerde programmalaryň düzülmegi bilen meşgullanýan adam üçin çäklendirmegi barlamagyň

ýazgysy saklanylýan diskdäki faýla ýa-da reýestriň açaryna bolan ýoly kesgitlemeklikde, eýsem tutuş barlagyň özüni assembler koduny düzetmek arkaly üýtgetmeklikde kân bir uly kynçylyklar ýüze çyk-maz.

Debuggerlerden goranmak barada bolsa indiki bölümde gürrüň ediler.

Tejribe işleri

1. Diňe 10 gezek goýberilýän programmany döretmeli.
 2. Diňe 6 aý işleýän programmany döretmeli.
 3. Diňe bir kompýuterde goýberilýän programmany döretmeli.
 4. 1-nji işde görkezilen programmany üç programmirleme dilde döre-dip, olary seljermeli.
 5. 2-nji işde görkezilen programmany üç programmirleme dilde döre-dip, olary seljermeli.
 6. 3-nji işde görkezilen programmany üç programmirleme dilde döre-dip, olary seljermeli.
-

V. DEBAGGER-SAZLAÝJYLARDAN GORANMAK

1. OllyDebug sazlaýjynyň mümkinçilikleri.
2. OllyDebug sazlaýjyny programmalaryň goragyny döwmekde ulanmagyň esaslary.
3. Debuggerleri ulanman maşyn kodundaky gizlin maglumatlary kesgitlemek.
4. OllyDebug programmasynda programmalaryň seljerilmesiniň mysallary.
5. Maşyn koduny debuggerlerden we beýleki hüjümlerden goramak:
 - Ýaşyrmaly maglumatlary reýestrde ýerleşdirmek we olary faýlyň programmanyň maşyn kodunyň içindäki maglumatlar bilen baglaşdyrmak;
 - Olara bolan ýollary maşyn kodunda şifrlemek;
 - Programmada şertli geçişleri ýaşyrmak;
 - Boş geçişleri guramak;
 - Debugger arkaly goýberilendigi barada habar berýän programma koduny düzmek.

Mundan öňki bölümlerde biz maglumat goragynyň birnäçe usullaryna seredip geçdik. Olaryň her biriniň artykmaçlygy bar hem bolsa, ýetmezçilikleri hem az däl. Bu ýetmezçilikler şol gorag usullaryň her biri üçin aýratyn hem bolsa, olary birleşdirýän ýetmezçilik hem bardyr. Bu debugger arkaly hüjümdir.

Sazlaýjylaryň köp dürli görnüşleri bar: SoftICE, OllyDebug, IDA we ş.m. Windows-platformalar üçin bar bolanlaryň hemmesiniň arasynda has meşhur bolup Numega firmasynyň SoftICE önümi çykyş edýär. Onuň in esasy aýratynlygy bolup, goragyň 0-njy halkasynda işlemeklik çykyş edýär. Gorag halkalary Intel firmasynyň 32-derejeli prosessorlaryň gurluşlarynda ýerine ýetirilýän programmalaryň özara we amallar ulgamy bilen baglaşmagyny çäklendirmek üçin ulanylýar. Adatça, amallar ulgamy hemme beýleki ýerine ýetirilýän programmalara bolan doly elýeterlilik hukugyna eýe, sebäbi ol goragyň 0-njy halkasynda işleýär, ulgamlaryň meseleler 1-nji we 2-nji halkalarda, goşundylar 3-nji halkada işleýär. Goýberilen goşundylary bölekleyin

dolandyrmagy goragyň 1-nji we 2-nji halkalaryndan amala aşyrmak mümkin. Hut şeýle ýagdaýda sazlaýjylaryň köpüsi işleýär. SoftICE amallar ulgamynyň özeni ýüklenmezden öň ýüklenýär we diňe ulgam tarapyndan ýerine ýetirilýän hemme meseleleri gözegçilikde saklamak, eýsem amallar ulgamynyň özüni hem gözegçilikde saklamagy mümkin edýär.

Kitabyň bu bölümünde esasy maksat – debuggerler arkaly programmalaryň goragynyň döwürmegini amala aşyrmak däl-de, ony seljermek, seljermeginiň esasynda oňa garşy programma kodlary işläp düzmek. Munuň üçin ýönekeý hasaplanylýan, emma şol bir wagtda öndürililikli bolan debugger-sazlaýjy – OllyDebug programmasynyň işine serediler.

5.1. OllyDebug sazlaýjynyň mümkinçilikleri

OllyDbg – bu duýgur interfeýsi bolan assembler derejesinde seljirme işlerini geçirýän 32-bit sazlaýjy. Ol has hem başlangyç kod elýetersiz ýa-da siz kompilyator bilen kynçylyk çekýän halatyňyzda peýdaly bolýar.

Talaplary – Windows 95, 98, ME, NT ýa-da 2000, XP, seven operasion sistemalarynda Pentium toparynyň islendik kompýuterinde işleýär. Emma onuň amatly işi üçin ýygylgy azyndan 300 MGs bolan prosessor gerek bolýar. Eger goşmaça pluginler ulanyljak bolsa onda, 128 Mb we ondan ýokary RAM ulanmak zerur.

Goldanylýan prosessorlar – OllyDbg hemme 80x86, Pentium, MMX, 3DNow!, Athlon goldaýar, mundan başga hem SSE buýruklary we degişli maglumatlaryň formatlaryny goldaýar. Emma SSE2 goldamaýar.

Sazlamasy. Programmanyň işini 100-den gowrak opsiýalar goldaýarlar.

Maglumatlaryň formatlary. Dampnyň penjirelerini, maglumatlaryny hemme adaty formatlarda görkezýärler: HEX, ASCII, UNICODE, 16- we 32 derejeli bitin/bitin däl/hex sanlary, ýüzýän oturly 32/64/80-bit, salgylanmany, dizassemblirlämäni (MASM, IDEAL ýa-da HLA), PE at ýazgysyny ýa-da maglumatlar blogunyň akymyny.

Kömek. Bu faýl OllyDbg düşünmek we ulanmak üçin zerur bolan esasy maglumaty saklaýar. Eger sizde Windows API boýunça maglumat bar bolsa (Win32.hip awtor hukuklary boýunça girizilmedik), siz ony berkidip ulgamlayn çagyryşlar barada şol pursatdaky maglumaty alyp bilýärsiňiz.

Goşundynyň goýberilmegi. Siz ýerine ýetirilýän faýly buýruk setirinde saýlap, menýuda saýlap, OllyDbg-e faýly süýşürüp, soňky sazlanýlan programmany gaýtadan goýberip ýa-da eýýäm goýberilen goşunda goşulyp bilýärsiňiz. OllyDbg şol wagtky sazlamany goldaýar. Gurnama gerek däl, siz OllyDbg çeýe diskden goýberip bilýärsiňiz!

DLL sazlamak. OllyDbg bilen dinamiki birikdirilýän bibliotekalaryň (DLL) sazlanmasyny amala aşyryp bolýar. OllyDbg awtomatiki ýagdaýda kiçi ýerine ýetirilýän faýly goýberýär, oňa ol bibliotekany ýükleýär hem-de onuň eksportyny çagyrmagy mümkin edýär.

Sazlanyş maglumaty we faýllary sazlamak. OllyDbg MICROSOFT we Borland Formatdaky sazlamalar baradaky maglumaty okaýar. Bu maglumat öz içine başlangyç teksti we funksiýalaryň, bellikleriň, global we statiki üýtgeýänleriň atlaryny alýar. Dinamiki (stek) üýtgeýänleriň we düzümleriň goldanylmagy örän çäklendirilendir.

Koduň aşakdan ýagtylandyrylmagy. Dizassembler buýruk-laryň dürli görnüşlerini (geçişleri, şertli geçişleri, stege ýerleşdiriş we çykaryş, proseduralaryň çagyrylmagy, ileri tutulýan we ýol berilmeýän gaýtaryşlar) hem-de dürli operandlary (umumy, FPU/SSE ýa-da segment/ulgam registrleri, stekdäki ýa-da başga huşdaky huş operandlary, hemişelikler) aşagyndan ýagtylandyryp bilýär. Şeýle hem ýagtylandyrmagyň ulanyjynyň ülnülerini döretmek mümkin.

Akymlar. OllyDbg köp akymly goşundylary sazlap bilýär. Bir akymdan beýlekä geçmek, akymly duruzmak, dikeltmek we ýok etmek ýa-da olaryň ileri tutulmagyny üýtgetmek bolýar. Akymlaryň penjiresi her akym üçin ýalňyşlyklary görkezýär (meselem, GetLast-Enot funksiýasyna çagyryşy gaýtarýarlar).

Seljeriş. Seljeriji – OllyDbg-iň iň wajyp bölekleriniň biridir. Ol proseduralary, gaýtalanýşlary, gaýtadan geçirijileri, tablisalary, koda

ornaşdyrylan hemişelikleri we setirleri, çylşyrymly gurnawlary, API-funksiýalaryň çagyryşlaryny, funksiýanyň parametrleriniň sanyny, importyň öýjüklerini we ş.m. tanaýar. Seljeriş ikilik kody has aňsat okalýan edýär, sazlamany aňsatlaşdyrýar we nädogry düşünmekligiň we näsazlyklaryň ähtimallygyny azaldýar. Ol kompilyatordan ugur almaýar hem-de deň derejede islendik PE-programma bilen işleýär. Kömekçi düşündirişleri goýmak arkaly seljerişini netijelerini gowulandyrmak bolýar.

Obýektleriň skaneri. OllyDbg bibliotekanyň ýa-da obýektiň modullaryny (faýllary) skanirleýär (ikisini hem OMF we COFF formatlarynda), kody çykarýar, onuň sazlanylýan programmada ýerleşýän ýerini segmentleýär hem-de kesgitleýär.

Import edilýän bibliotekalaryň skaneri. Käbir DLL öz simwolaryny diňe ordinallar (ordinal) bilen eksport edýär. Olar bolsa, adam gözi tarapyndan kabul etmek üçin amatsyz. Eger importyň degişli bibliotekasy bar bolsa, OllyDbg ordinallary simwol atlaryna geçirýär.

UNICODE doly goldamak. ASCII setirlerine elýeterli bolan hemme amallar UNICODE setirlerine hem degişlidir we tersinedir.

Atlar. OllyDbg sazlama baradaky maglumatdan hemme import we eksport edilen simwollary we atlary Microsoft we Borland formatlarynda hem görkezýär. Obýektleriň skaneri bibliotekalaryň funksiýalaryny tanamagy mümkin edýär. Öz bahaňy we belligiňi goşup bolýar. OllyDbg şeýle hem köp hemişelikleriň simwolik atlaryny bilýär, meselem habar penjireleriň, koduň ýalňyşlyklarynyň ýa-da derejeleriň meýdanlarynyň hem-de olary belli funksiýalaryň çagyryşlaryna dekodirleýär.

Belli funksiýa. OllyDbg köp ulanylýan Si we Windowsyň API funksiýalarynyň ady boýunça 2300-e golaýyny tanaýar we olaryň parametrlerini dekodirleýär. Öz teswirlemelerini goşmak ýa-da belli bir dekodirlemegi bellemek mümkin. Belli funksiýadaky ýazgy bilen kesilme nokatlary (breakpoint) goýup we parametrleri faýla ýazyp bolýar.

Çagyryşlar. OllyDbg stega ýüzlenilende, eýsem eger sazlama baradaky maglumat elýetersiz bolanda hem-de proseduralar standart däl girişleri we tamamlanyşlary ulananda hem goşundynyň işini kesip bilýär.

Stek. Stack penjiresinde, OllyDbg gaýtaryşyň salgysyny we ýazgynyň düzüm gurluşyny tanamak üçin ewristikany peýdalanýar. Emma olaryň öňki çagyryşyň galyndy bolup bilmekligine gaty üns bermeli. Eger programma belli funksiýada duruzylan bolsa, stegiň penjiresi hakyky parametrleri dekodirleýär.

SEH zynjyrlary. Stek SE hendlleriň yzygiderliligini yzarlaýar we görkezýär. Doly yzygiderlilik aýry penjirede elýeterlidir.

Gözleg. Örän köp mümkinçilikler hödürlenýär. Buýrugyň (takyk ýa-da takyk däl) ýa-da buýruklaryň yzygiderliginiň gözlegi, hemişelikler üçin, ililik sandaky ýa-da ýazgyly setir (hökmany üznüksiz bolmadyk) üçin, salga, hemişelige ýa-da salgy aralygyna salgylanýan hemme buýruklar üçin, saýlanylan ýerleşiş ýere bolan hemme geçişler üçin, belli bir prosedurany çagyryan hemme funksiýalar ýa-da şol proseduranyň çagyryan hemme zatlary üçin, hemme agzalýan ýazgyly setirler üçin, dürli modullaryň hemme çagyryşlary üçin, atlar üçin, huşuň bitewi tertipleşdirilmeginde ýaşyrylan ililik sandaky yzygiderlikler üçin gözleg. Eger ýerleşiş ýerleriň köp sany tapylan bolsa, olaryň arasynda tiz süýşmek bolýar.

Penjireler. OllyDbg sazlanýlan goşundy arkaly döredilýän hemme penjireleri sanap geçýär we penjirelere, toparlara eýsem saýlanylan habara ýa-da habarlaryň toparyna gözegçilik nokatlaryny gurnaýar.

Resurslar. Eger Windowsyň API funksiýasy setir resursyna salgylanýan bolsa, OllyDbg ony çykarýar we görkezýär. Beýleki görnüşleriň goldawy berkidilen resurslaryň, dampyň we ililik san arkaly redaktirlemeginiň sanawy bilen çäklendirilen.

Gözegçilik nokatlary (oreikpointler). OllyDbg gözegçilik nokatlaryň hemme adaty görnüşlerini goldaýar: ýönekeý üzülmeleri, şertli üzülmeleri, maglumaty žurnala ýazýan üzülmeleri (meselem, işleýiş parametrleri ýazýanlar), huşa ýazmak we elýeterlik üçin gözegçilik nokatlary, apparat gözegçilik nokatlary (diňe Windows ME/NT/2000). Ädimleýin sazlamanyň iň aňryçäk ýagdaýynda, INT3 gözegçilik nokady modulda, her bir buýrukda goýlup bilner. Windows NT operasion sistemasyny işledýän 500 MGs prosessorda OllyDbg bir sekuntda 5000 golaý üzülmeleri işläp bejerip bilýär.

Synçylar we gözegçiler. Synçylar – her gezek programma duruzylan ýagdaýynda bahalandyrylýan aňlatmalar. Registrleri, hemişelikleri, salgy aňlatmalary, islendik çylşyrymly algebraik amallary ulanmak mümkin. Siz ASCII we UNICODE setirleri deňeşdirip bilýärsiňiz. Gözegçiler – bu iki indeksi saklaýan hem-de massiwleri we düzüm gurluşlary dekodirlemegi mümkin edýän iki ölçegli tablisa görnüşinde görkezilýän synçylar.

Ýerine ýetiriliş. Programmany, onuň kömekçi böleklerine girmek bilen ädimleýin ýa-da olary bir gezekde ýerine ýetirip bolýar. Programmany indiki gaýtaryşa çenli ýa-da görkezilen ýere çenli ýerine ýetirip bolýar, ýa-da ýerine ýetirişe meňzetme edip bolýar. Goşundy ýerine ýetirilende onuň üstünde doly gözegçilik ulanyjyda saklanylýar hem-de ol huşy görüp, gözegçilik nokatlary goýup, eýsem kody şol ýagdaýda üýtgedip hem bilýär. Islendik wagtda, ulanyjy sazlanýlan programmany durzup ýa-da gaýtdan goýberip bilýär.

Ädimleýin sazlama. Ädimleýin sazlama şol wagta çenli haýsy buýruklaýň ýa-da proseduralaryň ýerine ýetirilendigini görkezýär, şonuň bilen, ol ulanyja kodunyň hemme şahamçalaryny barlamagy mümkin edýär. Ädimleýin sazlama gözegçilik nokady her saýlanylan buýrukda gurnaýar hem-de buýruga ýetilenden soň ony ýok edýär.

Gönümel ugur belleýiş (Run trace). Ugur belleýiş (trassirovka) programmany ädimleýin ýerine ýetirýär we onuň ýerine ýetirilişini uly tegelek buferde ýazýar. Bu protokol hemme registrleri (SSE-den başgasyny), baýdaklary we akymyň ýalňyşlyklaryny, habarlary we belli funksiýalaryň dekodirlenen parametrlerini saklaýar. Öz-özünü üýtgedýän koduň sazlamasyny aňsatlaşdyrjak asyl nusga buýruklary ýatda saklamak bolýar. Sazlamanyň bes edilmeginiň şertini kesgitlemek mümkin – munuň üçin salgylaryň aralygyny, aňlatmany ýa-da buýrugy girizmek gerek. Sazlamanyň maglumatyny faýlda saklap hem-de programmanyň iki garaşsyz ýerine ýetirilmegini deňeşdirmek mümkin. Ugur belleýiş millionlarça buýruklaýň ýerine ýetirilmeginiň wagt boýunça taryhyny jikme-jik gaýtdan seljermegi mümkin edýär.

Ugrukdyrys. Ugrukdyryjy belli bir buýrugyň ugur belleýşiň buferinde näçe gezek duş gelyändigini sanaýar. Ugrukdyryjyň kömegi bilen, koduň haýsy böleginiň ýerine ýetirilmeginiň iň köp wagt alyandygyny bilmek bolýar.

Düzedişleri girizmek. Gurnalan assembler awtomatiki ýagdaýda, mümkin bolan, iň gysga kody saýlaýar. Ikilik sandaky redaktor maglumatlary şol bir wagtda ASCII, UNICODE we on altlyk formalarda görkezýär. Şeýle hem köne adaty bolan göçürme we göçürilen zady goýma elýeterli. Awtomatiki ätiýaçlyk nusga üýtgemeleri ýatymagy mümkin edýär. Üýtgemeleri gönümel ýerine ýetirilýän faýla göçürmek mümkin, eýsem OllyDbg kesgitlenen ýalňyşlyklary düzedýär. OllyDbg programmanyň sazlamanyň beýleki işleýşindäki hemme düzedişlerini ýatda saklaýar. Olary klawişalara birnäçe gezek basmak arkaly ulanmak ýa-da ýok etmek mümkin.

Öz-özünü çykarýan faýllar. SFX faýly sazlanýlanda, köplenç arhiwatoryň üstünde geçip gönümel programma girilýän ýerde durmaklyk gerek bolýar. OllyDbg hakyky girişiň ýerini kesgitlemäge synanyşyk edip, SFX faýlynyň sazlamasyny geçirýär. Köplenç goranylan arhiwlerde SFX faýlyň sazlanmasy şowsuz bolýar. Giriş tapylandan soň OllyDbg arhiwden çykaryjynyň üstünden has tiz we ygtybarly geçip bilýär.

Programma bolan goşmaçalar. OllyDbg-e usuly goşmak, ýa-da öz goşmaçaňy ýazmak mümkin. Programma bolan goşmaçalar maglumatlaryň hemme esasy düzümlerine ýüzlenýär, OllyDbg-iň bar bolan penjirelerine menýulary we ýarlyklary goşýarlar hem-de 100-den gowrak goşmaça API funksiýalaryny peýdalanýarlar. API pluginleri gowy resmileşdirilendir. Standart distributiv programma bolan iki goşmaçany öz içine alýar: Buýruk setiri we goşmaça sahy-palary.

UDD OllyDbg tutuş programmany – ýa-da modul bilen bagly bolan maglumaty aýratyn faýlda saklaýar we modul gaýtadan ýüklenende ony dikeldýär. Bu maglumat öz içine bellikleri, düşündirişleri, gözegçilik nokatlary, synçylary, seljermäniň maglumatlaryny, şertleri we ş.m. alýar.

OllyDbg programması:

- hiç haçan sazlamadan başga beýleki prosesleri yzarlamaga ýa-da tor müşderi, ýa-da serwer ýaly hereket etmäge, ýa-da islendik beýleki kompýutere hiçi hili usul bilen maglumatlary ibermäge (eger olar ulanyjy tarapyndan görkezilen uzakdaky faýllar bolmasa) synanyşyk etmeýär, islendik görnüşli troýan aty ýaly hereket etmeýär;
- eger anyk ýagdaýda gerek bolmasa ulgamyň reýestrini okamaýar, üýtgetmeýär, talap edilýän bu modifikasiýalar aşakdaky 6 sany açar bilen çäklendirilen:

HKEY_CLASSES_ROOT\exefile\shell\OpencOllyDbg HKEY_CLASSES_ROOT\exefile\shell\Open cOllyDbg\command
HKEY_CLASSES_ROOT\dlfile\shell\Open cOllyDbg
HKEY_CLASSES_ROOT\dlfile\shell\OpencOllyDbg\command
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AeDebug\Debugger
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AeDebug\Auto

- ulgam bukjalarynda faýllary döretmeýär, gaýtadan ýazmaýar we üýtgetmeýär;

- eger anyk ýagdaýda gerek bolmasa, islendik kompýuterde hiç hili ýerine ýetirilýän faýly ýa-da DLL, gönümel OllyDbg goşmak bilen üýtgetmeýär;

- diňe ulanyjy tarapyndan anyk talap edilen ýagdaýynda sazlamanyň hereketlerini bellige alýar (**ollydbg.ini** ýa-da ***udd** faýllarda sazlama maglumaty bilen ýatda saklanylýan Faýllaryň Wag taryhyndan başga). Ulanyjynyň rugsady bolmazdan OllyDbg faýllary diňe özüniň ýerleşýän bukjasynda döredýär we üýtgedýär;

Ýokarda agzalanlar kepillendirilýän hem bolsa soňky döwürde debaggerler, hususanda OllyDbg köp halatda hünärmenler tarapyndan programmalary sazlamak üçin däl-de, olaryň goragyny döwmek we rugsatsyz çäksiz ulanmak ýa-da satmak üçin peýdalanylýar.

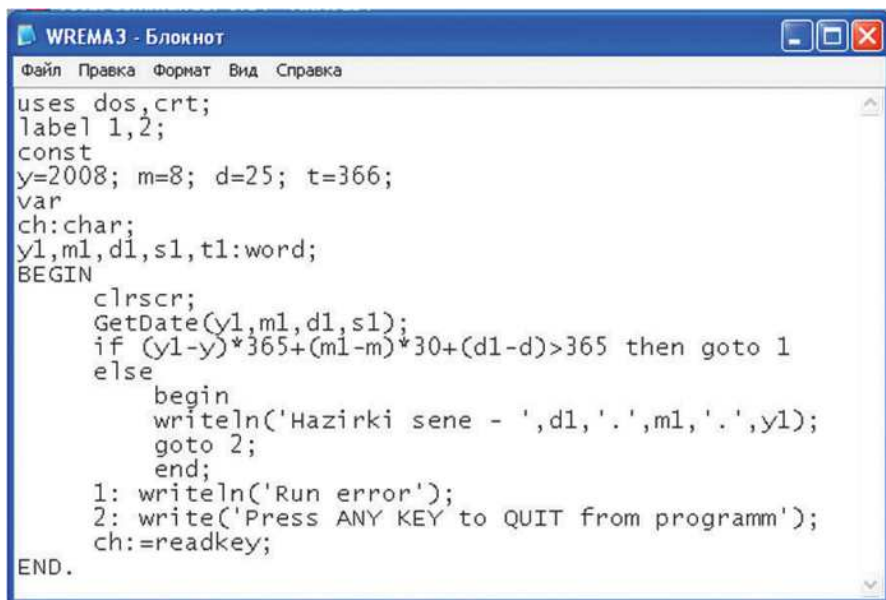
Geliň sazlaýjynyň döwmek maksady üçin ulanmagynyň esaslaryny seljereliň.

Bilşimiz ýaly, programma ahyrky görnüşde maşyn koduna eýe bolýar. Maşyn kody programma kody bilen tapawutlykda ulanyjy

üçin, eýsem islendik adam üçin örän düşnüksiz, sebäbi biziň üçin adaty bolan harplar we sanlar ýa-da beýleki ýazuw simwollar bilen bilelikde ol ýerde dolandyryjy simwollaryň şekilleri hem ulanylýar, üstesine-de harplar we sanlar adam dilindäki adaty zygiderlikde däl-de (söz ýa-da sözlem) diňe kompýutere düşünikli zygiderlikde ýerleşdirilen.

5.1-nji suratda belli bir programma kodunyň kompilyasiýasy esasynda emele gelen maşyn koduny, ony döreden programma kody bilen deňeşdirilýär.

Görşümüz ýaly, programma kody bilen oňa degişli maşyn kody düýpgöter tapawutlanýandyr. Programma koduna eýe bolan hünärmen, hiç hili kynçylyk çekmän programmanyň işleýşini üýtgedip bilýär. Ýagny üýtgedilen programma kody, degişlilikde maşyn kodunyň üýtgemegine getirýär. Kompýuter üçin maşyn kodundaky baýtlar „düşnükli“ bolup durýar, olaryň belli bir zygiderlikleri buýruklary döredýär, programma kody bolsa ulanyjy tarapyndan programmirme dilinde ýazylan ýazgy bolup durýar, programma kody öz-özünden



```
uses dos,crt;
label 1,2;
const
y=2008; m=8; d=25; t=366;
var
ch:char;
y1,m1,d1,s1,t1:word;
BEGIN
  clrscr;
  GetDate(y1,m1,d1,s1);
  if (y1-y)*365+(m1-m)*30+(d1-d)>365 then goto 1
  else
    begin
      writeln('Hazirki sene - ',d1,'.',m1,'.',y1);
      goto 2;
    end;
  1: writeln('Run error');
  2: write('Press ANY KEY to QUIT from programm');
  ch:=readkey;
END.
```

5.1-nji surat. Wrema3.pas (programma kody)



5.2-nji surat. Wrema3.exe (maşyn kodunyň parçasý)

ýerine ýetirilip bilmeýär, ony hökman kompillirmek gerek, ýagny maşyn koduna geçirmek gerek.

Satuwda we ulanyşda biz elmydama maşyn kodundaky programma bilen işleýäris. Programmanyň düzüjisi hiç haçan onuň ýany bilen programma koduny bermeýär. Şol sebäpden satyn alnan programmanyň işini öz islegiň boýunça üýtgedip bolmaýar. Emma programma koduna eýe bolan ýagdaýynda, islendik programma düzüp bilýän adam programmany üýtgetmekde uly mümkinçiliklere eýe bolardy.

5.2. OllyDebug sazlaýjyny programmalaryň goragyny döwmekde ulanmagyň esaslary

Programmirlmegiň ösmegi bilen, programmanyň maşyn koduny üýtgetmeklik boýunça örän köp islegler döredi. Şol islegleriň köpelmegine programma goragynyň şeýle görnüşleriniň döremegi

ýardam berdi: programmanyň goýberilmeginiň çäklendirilmegi, parol goragynyň kompýuter görnüşleri.

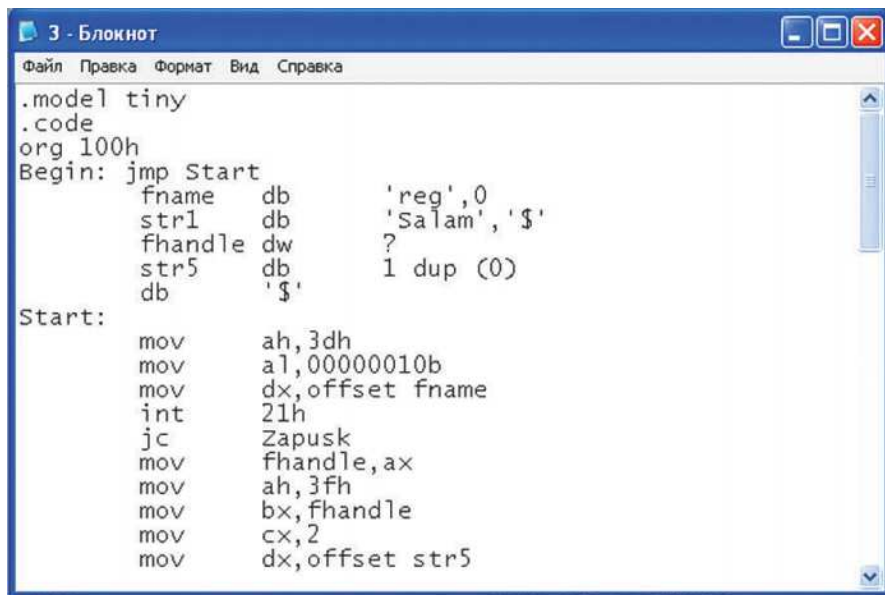
Programmalaryň belli bir wagtda geçmegi bilen işlemeginiň bes edilmegi, olaryň maşyn kodunda belli bir bölekleriň şoňa jogap berýändigini barada pikirleriň kemala gelmegine getirdi.

Adaty ulanyjylar muňa hiç hili täsir edip bilmeýän bolsa, programma düzüp bilýänler bu ýagdaý bilen razy bolup bilmediler.

Ökde programma düzüjiler maşyn koduna golaý bolan programmirleme diline ýüz tutup başladylar. Şu ýagdaýda Assembler ulgamlaryn programmirleme diliniň gaýtadan „kemala gelmegi“ bolup geçdi. Fortran, Pascal, Basic, C++ we beýleki dilleriň giňden ýaýramagy Assembler dilini ikinji orna süýşürdi. Bu ol dilleriň ulanyja has golaýdygy, ýagny ýokary derejeli dil bolýandygy bilen düşündirilýärdi.

Emma XX asyryň ahyrlarynda programma goraglarynyň kämilleşmegi, olary ýokary derejeli diller bilen däl-de, maşyn koduna golaý diller bilen işläp döwmeklik mümkinçilikleri döredildi.

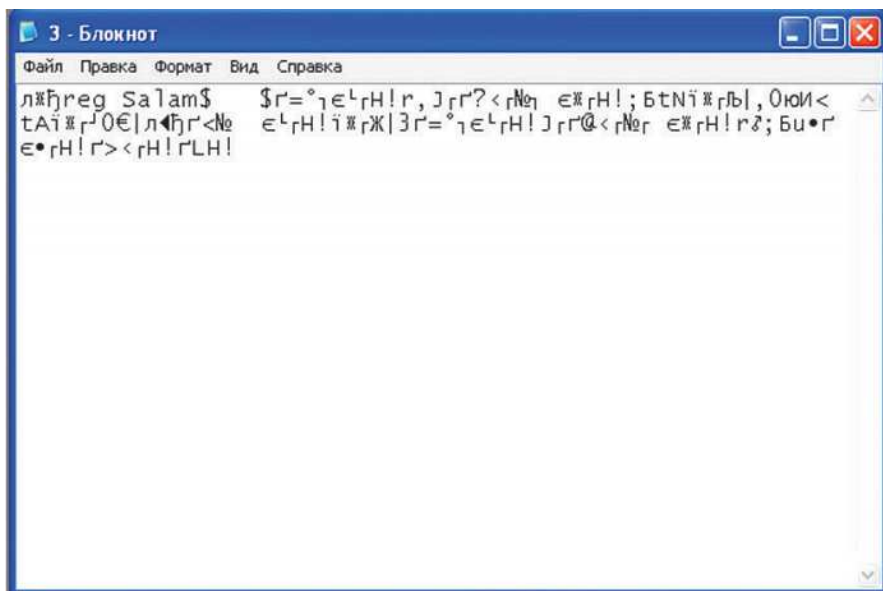
Bu ýagdaýda islendik maşyn koduny assemblere geçirip bilýän debaggerleriň, ýagny sazlaýjylaryň ähmiýeti ýokarlandy.



```
.model tiny
.code
org 100h
Begin: jmp Start
        fname db      'reg',0
        str1  db      'Sałam', '$'
        fhandle dw     ?
        str5  db      1 dup (0)
        db    '$'

Start:
        mov     ah,3dh
        mov     al,00000010b
        mov     dx,offset fname
        int     21h
        jc      Zapusk
        mov     fhandle,ax
        mov     ah,3fh
        mov     bx,fhandle
        mov     cx,2
        mov     dx,offset str5
```

5.3-nji surat. 3.asm (Assemblerdäki programma kody)



5.4-nji surat. 3.com (maşyn kody)

Assembler dili örän çylşyrymly programma koduny hödürleýän hem bolsa, maşyn kody bilen deňeşdirilende ol anyk düşnükli bolup görünýändir.

Görşümüz ýaly, islendik ýokary derejeli ýa-da obýekte gönükdirilen dilinde döredilen programmanyň maşyn koduny assembler diline geçirmeklik, şol programmany üýtgetmeklik mümkinçiligini döredýär.

Şol sebäpli öň ulanyjylaryň öz programmalaryny sazlamak üçin ulanylýan debuggerler, häzirki wagtda özge programmalary döwmek üçin ulanylyp başlandy.

Debuggerleriň içinde programmalaryň edýän işini seljermek üçin örän uniwersal gural bar – gurnalan dizassembler, ýagny islendik maşyn kody assembler koduna geçirýän programma.

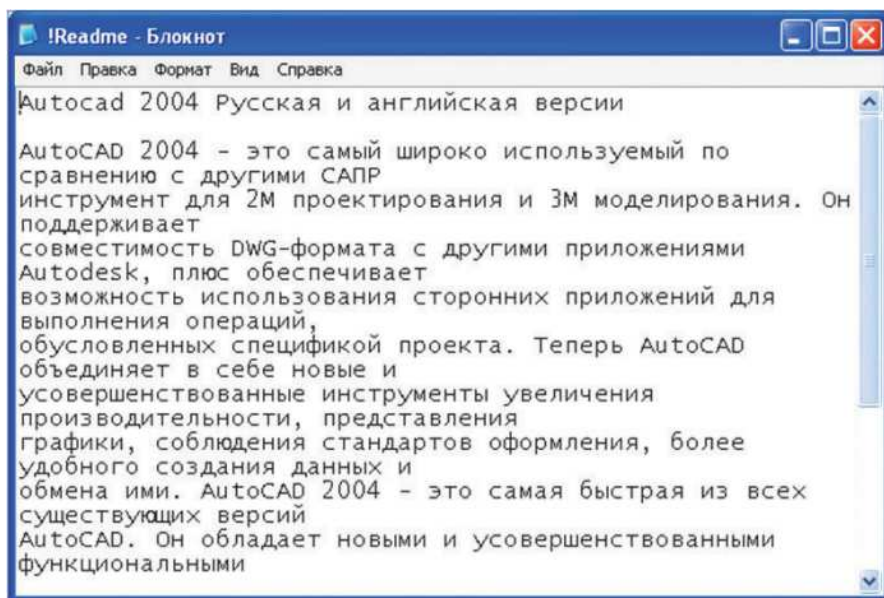
Häzirki zaman debuggerleriň (meselem OllyDbg programma-synyň) içinde diňe bir dizassemblerden başga, ýüzlerçe seljeriş, düzediş, anyklaýyş, gözleýiş, goýberiş gurallary bar. Şol sebäpli, OllyDbg işine düşýän, assembler kody bilen işläp, ony seljerip bilýän adam üçin goragyň häzirki zaman kämil usuly bilen goranylan

programmany „döwmek“ (ýagny üýtgetmek, çäksiz ulanylar ýaly etmek we ş.m.) uly bir kynçylyk döretmez.

Emma maşyn koduny programma kodunyň üstünden geçip düzetmekligiň synanyşyklary debuggerler döredilmezden öň hem bardy. Şol sebäpli debuggerler bilen barlag işlere geçmezden öň şol synanyşyklara seretmeli.

5.3. Debuggerleri ulanman maşyn kodundaky gizlin maglumatlary kesgitlemek

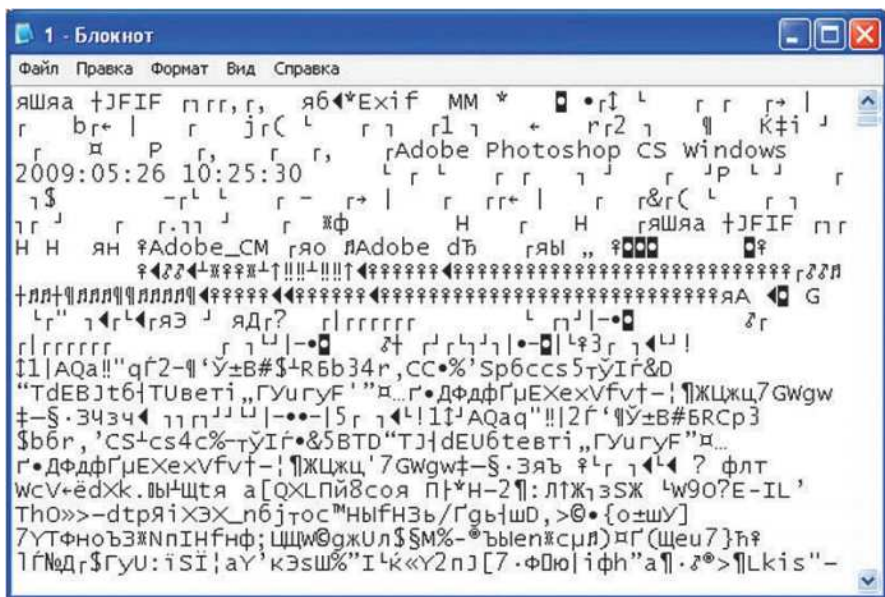
Bilşimiz ýaly, kompýuteriň ýadynda islendik zady saklamak üçin, ony baýt düzümine getirmeli (baýt = 8 bit, her bit bolsa ýa 0 ýa-da 1 bolup bilýär, ýagny san görnüşinde bolmaly). Şol sebäpli kompýuterde ulanylýan maglumatlaryň hemme görnüşleri – ýazgy, saz, şekil, wideo ýa-da maşyn kodundaky programma bolsun – faýl görnüşinde bolýar. Bu faýllar degişli gurluşlar arkaly adaty görnüşine geçirilýär (koderler we dekoderler arkaly) – saz faýllary owazlanýar, grafiki faýllary – şekillenýär, programmalar – goýberilýär.



5.5-nji surat. !Readme.txt – ýazgy faýly



5.6-nji surat. Rob D – Clubbed To Death.mp3 – saz faýly



5.7-nji surat. 1.jpg – şekil faýly

Bu faýllary degişli gurluşlar arkaly däl-de, başga usul arkaly görmegiň uniwersal programmasy bar – bu baýt editordyr (notepad, edit we beýl.). Olar islendik faýly, onuň maglumat görnüşine garamazdan, baýt görnüşinde görkezýärler.

Meselem, **notepad** (bloknót) programmasy arkaly şu yzygiderlikde – ýazgy, saz, şekil, wideo, ýerine ýetiriji programma ýaly faýllary ýokardaky suratlarda göreliň.

Ýokardaky suratlardan aşakdaky netijeleri çykarmak bolýar:

- baýt görnüşinde hemme tekst ýazgylary hemme 5 faýlda hem üýtgemän görkezilýär;

- operatorlar, funksiýalar, ýerine ýetirilýän owaz, şekil, wideo bölekler düşüniksiz maşyn kod görnüşinde görkezilýär.

Şeýlelik bilen, programmanyň peýdalanýan ýazgy yzygiderliliklerini notepad programmasy bilen görmek mümkin.

Geliň indi gorag meselesinde programmanyň ulanyp biljek tekst maglumatlaryny sanap geçeliň:

- simwollaryň yzygiderlilik bolan parol;
- programmanyň çäklendirilmegi baradaky maglumatyň saklanýan faýlyna bolan ýol;
- seriýa belgiler ýa-da ygtyýarlyk kodlar we ş.m.

Bu kitapda programmalaryň goragy boýunça birnäçe programmalar görkezilýär. Geliň indi olaryň maşyn koduny **notepad** programmasy arkaly seljereliň:

Mysal. Goýberilende parol soraýan programmany Pascal programmirleme dilinde döredip, onuň soraýan parolyny **notepad** programmasy bilen kesgitlemeli (käbir operasion sistemalarda amala aşmaýar).

Aşakdaky programma parol soraýar, eger girizilen parol „maksat“ bolsa ol „Parol dogry“ diýip ýazýar, dogry däl bolsa „Parol nädogry“ diýip ýazýar.

Parol.pas (programmanyň listingi)

```
uses crt;  
var  
c:string;ch:char;
```

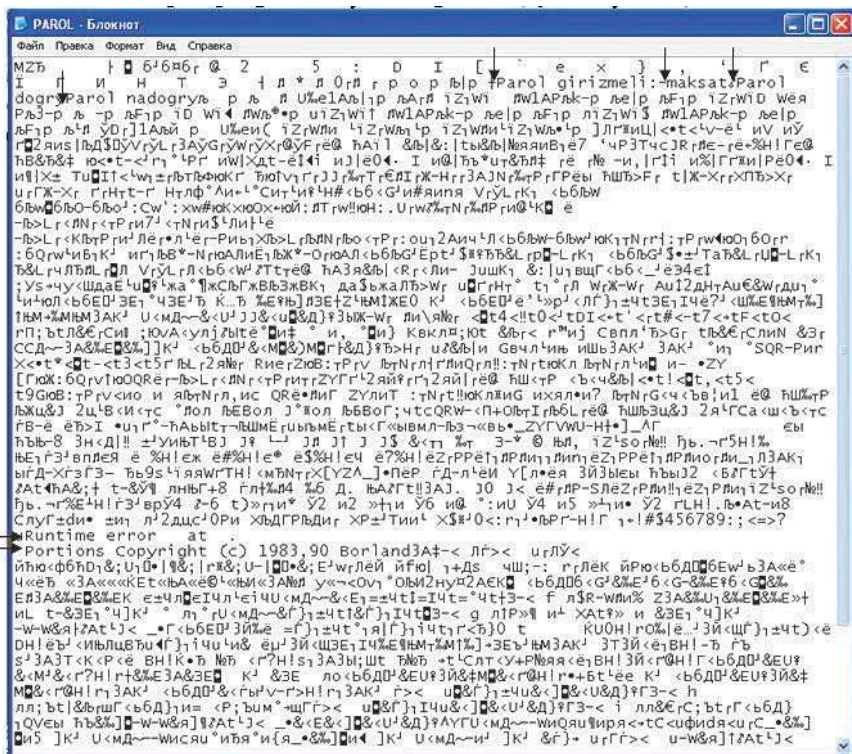
```

Begin
clrscr;
writeln('Parol girizmeli:');
read(c);
if c='maksat' then writeln('Parol dogry')
else writeln ('Parol nadogry');
ch:=readkey;
end.

```

Indi şu programma kody esasynda döredilen parol.exe programmanyň düzümini **notepad** programmasy bilen göreliň (aşakdaky surat)

Suratdan görşümüz ýaly, maşyn kodunda diňe birnäçe ýazgyny okamak mümkin (gara oklar bilen görkezilen). Olar: Paroly girizme-



5.10-njy surat. Parol.exe programmasynyň maşyn kody

li:, maksat, parol dogry, parol nädogry, Runtime error, Portions Copyright (c) 1983, 90 Borland.

Şeýlelik bilen, programmanyň goýberişde berýän jogaplaryny aýyrmak bilen biz näbelli „maksat“ sözünü kesgitleýäris. Dogrudan hem „maksat“ sözi parol bolup durýar.

Ýene bir mysal getireliň.

Mysal. Goýberilmegi san boýunça çäklendirilen (meselem 3 gezek goýberilmeli) hem-de näçe gezek goýberilendigini belli bir faýlda saklaýan programmany Assembler dilinde ýazmaly.

Aşakda programma kody getirilen programmamyz 3 gezek ýerine ýetirilýär (her gezek ol „Salam“ sözünü ekrana çykarýar), özüniň ýerine ýetirilmeli sanyny ol „C:\reg.txt“ ýolunda ýerleşen faýlda saklaýar.

Note.asm (programma kody)

```
.model tiny
.code
org 100h
Begin: jmp Start
      fname db      'c:\reg.txt',0
      str1  db      'Salam','$'
      fhandle dw      ?
      str5  db      1 dup (0)
      db    '$'
Start:
      mov   ah,3dh
      mov   al,00000010b
      mov   dx,offset fname
      int   21h
      jc    Zapusk
      mov   fhandle,ax
      mov   ah,3fh
      mov   bx,fhandle
      mov   cx,2
      mov   dx,offset str5
```

```

int    21h
cmp    ax,cx
je     exit
Lea    di,str5
mov    al,byte ptr[di]
sub    al,30h
dec    al
cmp    al,0
je     exit
Lea    di,str5
add    al,30h
mov    byte ptr[di],al
jmp    Zapusk1

```

Zapusk:

```

mov    ah,3ch
mov    cx,00000000b
mov    dx,offset fname
int    21h
Lea    di,str5
mov    byte ptr[di],51

```

Zapusk1:

```

mov    ah,3dh
mov    al,000000010b
mov    dx,offset fname
int    21h
mov    fhandle,ax
mov    ah,40h
mov    bx,fhandle
mov    cx,1
mov    dx,offset str5
int    21h
jc     exit
cmp    ax,cx
jne    exit
mov    ah,09

```

```

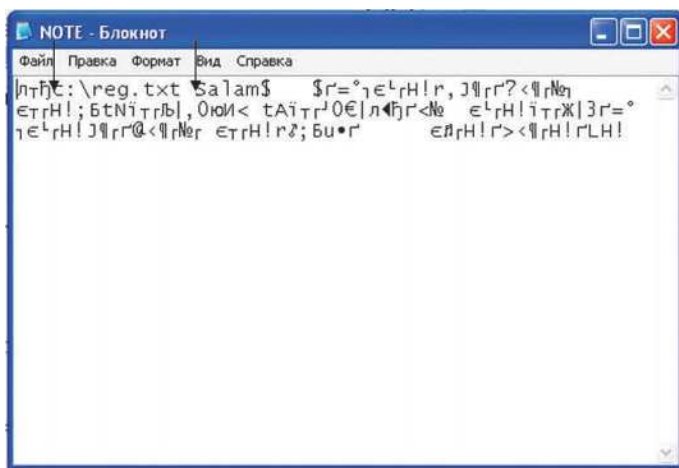
        lea    dx,str1
        int    21h
exit:
        mov    ah,3eh
        mov    bx,fhandle
        int    21h
        mov    ah,4ch
        int    21h
End      Begin

```

Elbetde, goýberilmegiň sanynyň nirede ýerleşýändigi barada diňe programma düzüji bilýär. Şol sebäpli şol ýoly kesgitlemek üçin ýene-de **notepad** programmasy ulanylýar. Netije 5.11-nji suratda görkezilendir:

Gysga seljermeden soň şu sözler kesgitlenýär: **c:\reg.txt, Salam**. Bu ýerde programmanyň goýberilmeginiň san çäginin C:\reg.txt faýlynda ýerleşýändigi aýdyň. Indi bu faýly tapyp onuň içine has ulurak sany goýmak bilen, bu programmanyň goýberilmeginiň sanyny programmany düzüjä ýüzlenmän dolandyrmak bolar.

Emma seredilen programmalar örän ýönekeýje we sada dilde ýazylan. Häzirki wagtda ulanylýan obýekte gönükdirilen programmirleme dilleri (meselem Delphi), şeýle bir uly maşyn kodlaryny emele



5.11-nji surat. Note.com programmasynyň maşyn kody

getirýär we olaryň içinde şeýle bir ýazgylar we setirler kân, eýsem ony **notepad** programmasy arkaly seljermek örän kyn we örän köp wagty alýar. Şeýle hem parol ýa-da faýllara bolan ýollar diňe tekst arkaly görkezilmän hem bilýär. Şol sebäpli programmalaryň goragyny döwmek bilen meşgul bolýan hünärmenler debaggerlere ýüzlenip başladylar.

Bu bölümde ýokarda belleýşimiz ýaly, esasy maksat programmalaryň goragyndan nähili üstün geçmekligi öwretmek däl-de, şol programmalaryň goragynyň haýsy sebäplere görä „ýykylmagyny“ kesgitlemek we şol maglumatlary ulanmak arkaly debagger „hüjümine“ garşy degerli usul tapmakdyr.

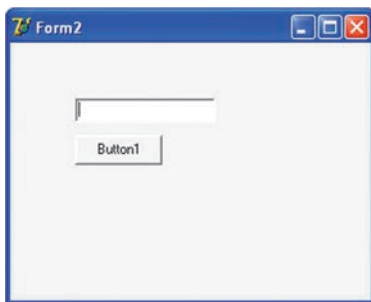
5.4. OllyDebug programmasynda programmalaryň seljerilmesiniň mysallary

OllyDbg programmasyň „döwüji“ mümkinçiliklerini seljermek üçin aşakdaky mysaly ýerine ýetirmeli.

Mysal. Delphi programmirleme dilinde goýberilende, paroly girizmekligi talap edýän programmany düzmeli we ony OllyDbg programmasynda seljermeli.

Aşakdaky suratda programma goýberilende paroly girizmekligi talap edýän penjiräniň çykarylmagy görkezilen (dogry parol – merdan).

Parol dogry girizilen ýagdaýynda penjire ýapylýar we „DELPHI“ diýip uly harplar bilen ýazylan başga penjire açylýar (esasy penjire).



5.12-nji surat. Parol talap edýän penjire



5.13-nji surat. Parol dogry girizilende açylýan esasy penjire

Ýokardaky programmanyň programma kody aşakda getirilýär. Ol iki esasy bölekden ybarat Unit1.pas – esasy penjiräniň kody we Unit2.pas – parol girizmekligi talap edýän penjiräniň kody.

Project1.exe programma kody

unit Unit1;

interface

uses

Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
Forms,
Dialogs, StdCtrls;

type

TForm1 = class(TForm)

Label1: TLabel;

procedure FormShow(Sender: TObject);

private

{ Private declarations }

```

public
    { Public declarations }
end;

var
    Form1: TForm1;

implementation
uses Unit2;

{$R *.dfm}

procedure TForm1.FormShow(Sender: TObject);
begin
    form2.ShowModal;
end;

end.

unit Unit2;
interface
uses
    Windows, Messages, SysUtils, Variants, Classes, Graphics,
    Controls, Forms,
    Dialogs, StdCtrls;

type
    TForm2 = class(TForm)
        Edit1: TEdit;
        Button1: TButton;
        procedure FormClose(Sender: TObject; var Action:
            TCloseAction);
        procedure Button1Click(Sender: TObject);
    private
        { Private declarations }

```

```

public
    { Public declarations }
end;
const c='merdan';
var
    Form2: TForm2;
implementation
uses Unit1;
{$R *.dfm}

procedure TForm2.FormClose(Sender: TObject; var Action:
TCloseAction);
begin
if edit1.Text<>c then Form1.close;
end;

procedure TForm2.Button1Click(Sender: TObject);
begin
Close;
end;
end.

```

Ýokardaky programma koduna şeýle gysgaça düşündiriş bereliň: **Unit1** böleginde **procedure TForm1.FormShow(Sender: TObject)** prosedurasy **form2.ShowModal** buýrugy goýberýär. Bu buýruk Form2 penjiräniň **Unit2** koduny ilkinji goýbermegi tabşyrýar. Bu ýagdaýda **Form2** penjiresi (paroly girizmekligi talap edýän penjire) ýapylýança, **Form1** (DELPHI sözüni saklaýan) penjire bilen işläp bolmaýar. Şol sebäpli **Unit2** koduna has ünsli seredeliň, sebäbi **Unit1** kody başga hiç bir işi ýerine ýetirmeýär.

Unit2 kodundaky **const c='merdan'** ýazgysy c hemişelige parolyň bahasyny dakýar (ýagny OllyDbg goýberilende biziň esasy maksadymyz şol bahany tapmaklykdyr).

procedure TForm2.Button1Click(Sender: TObject) prosedurasy (**Button1** düwmejige basylanda işleýär) **Edit1** tekst setirine parol girizilenden soň, Form2 penjiresini ýapmaklygy göz önünde tutýar.

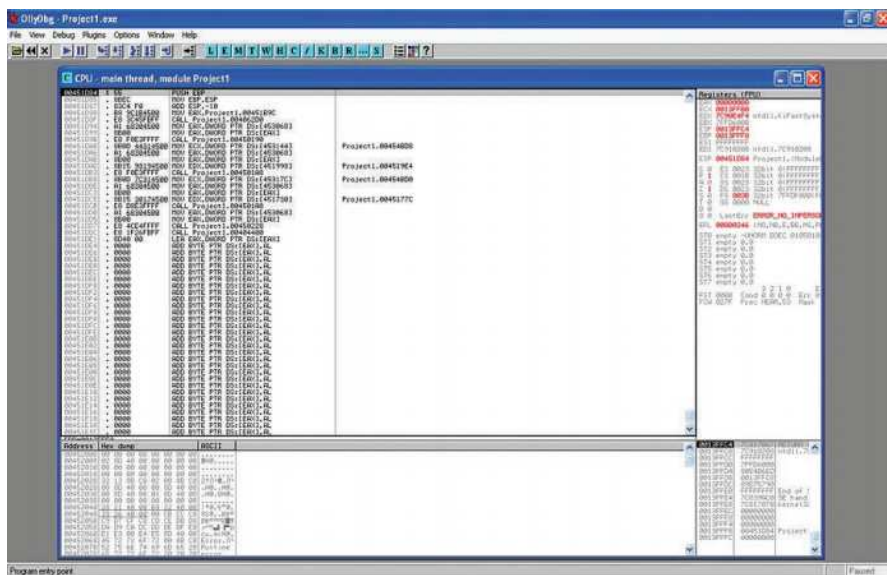
Parolyň dogry ýa-da dogry dälidigini **procedure TForm2. FormClose(Sender: TObject; var Action: TCloseAction)** prosedurasy kesgitleýär. Bu prosedura **Form2** penjiresi ýapylanda ýerine ýetirmeli buýruklary saklaýar, ýagny:

if edit1.Text<>c then Form1.close;

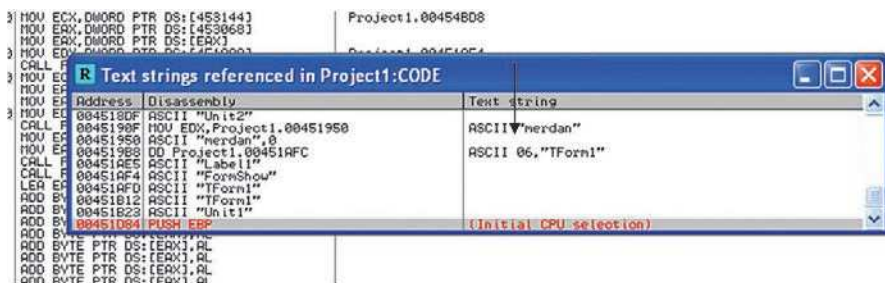
Görşümüz ýaly, **Edit1** setiriň bahasy **c** hemişeligiň bahasy bilen gabat gelmese, esasy **Form1** penjiresi hem ýapylmalydygy kesgитlenýär, ýagny tutuş programmamyz öz işini tamamlayar, parol dogry bolanda bolsa **Form2** penjiresiniň diňe ýeke özi ýapylýar we dolandyryş gaýtadan **Form1** penjiresine geçýär.

Programma düzülden soň, OllyDbg goýberip **File-Open** menýu yzygiderliginden peýdalanyň biziň programmamyzyň assemblerdäki koduna seredeliň.

Indiki ädim esasy penjirede syçanjygyň sag düwmejigine basyp, kontekst menýudan **Search for – All referenced text strings** buýrugy saýlamaly. Netijede programmamyzda ulanylan hemme tekst setirleri getirýän penjire açylýar. Biziň parolymyzyň hem merdan sözi



5.14-nji surat. OllyDbg programmasynyň esasy penjiresinde Project1.exe programmasynyň assemblere geçirilen kody



5.15-nji surat. Hemme ulanylýan tekst ýazgylary görkezilýän penjire

bolýandygyny hasaba almak bilen işiň netijesini 5.15-nji suratda görýäris.

Görşümüz ýaly, biziň parolymyz örän aňsat ýagdaýda anyklanyldy. Ýagny biziň programmamyzyň goragy „döwüldi“.

5.5. Maşyn koduny debuggerlerden we beýleki hüjümlerden goramak

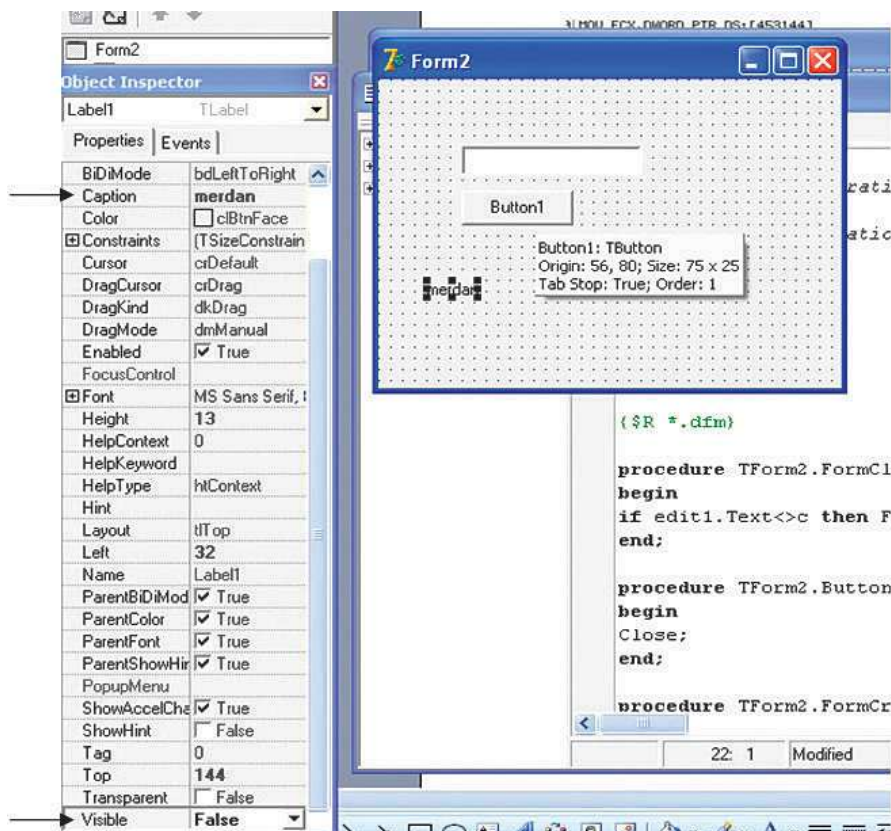
Geliň programmamyza birneme üýtgetmeleri girizeliň. Ýagny parolymyz c hemişeliginde däl-de, Delphiniň komponenti bolan **Label1**-de ýerleşdirilen bolsun. Bu komponentiň **Caption** (ýazgysyny) we **Visible** (penjire goýberilende görünmekligini) aşakdaky suratdaky ýaly üýtgedýäris (5.16-njy surat).

Indi programma debuggerde seljerilende 5.17-nji suratdaky netijäni alýarys.

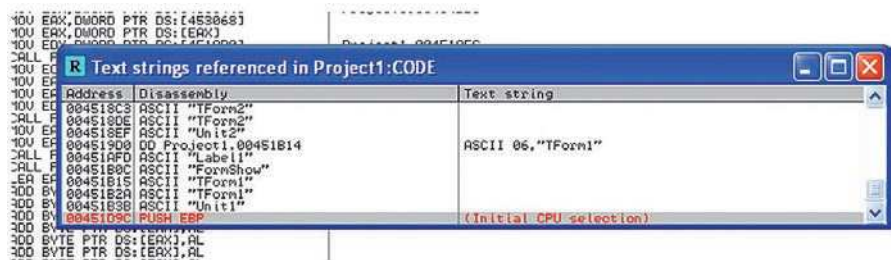
Şeýlelik bilen, debuggerlere garşy göreşmäge bir usuly kesgitledik:

programmanyň kodunda göni setir ululyklara salgylanmaly däl-de, olaryň deregine programmirleme diliniň öz tekst komponentlerini ulanmaly we olary degişli gizlemegi amala aşyrmaly.

Emma güýçli programma döwüjiler üçin bu garşylyk ýeterlik derejede görülmezligi mümkin. Şonuň üçin, ýokarky bendimize aşakdakylary goşmak gerek:



5.16-njy surat. Label1 ululyga merdan sözi dakylýar
we ol görünmez ýaly edilýar



5.17-nji surat. Parol kesgitlenmeýär

hemme girizilen parollary ýa-da faýllara bolan ýollary şifrlemeli.

Şifrlemegiň usullaryna öňki bölümde seredilipdi.

Meselem, programma kody maşyn koduna geçirilmezden öň hemme okalyp bilinjek maglumatlar XOR operatory arkaly şifrlenmeli. Maşyn kody işlän mahaly olaryň hemmesi düşnüksiz ýagdaýda bolar, programma özüne gerek mahaly olary XOR operatory gaýtadan ulanmak arkaly düşnükli ýagdaýa getirip ulanyp bilýär.

Emma has ussat döwüjiler debugger arkaly şifrleniş we şifrdan çykarylýş prosesleri anyklap, dogry maglumaty düşnükli ýagdaýda alyp bilýärler. Şol sebäpli aşakdaky bendiň goşulmagy teklipl edilýär:

hemme parollary, çäklendiriş ýazgylary we ş.m. daşky faýllarda däl-de, programmanyň öz maşyn kodunyň içinde saklamaklyk teklipl edilýär.

Dogrudan hem, debuggeri ulanyp, özüne gerekli maglumatlary aljak ýa-da üýtgetjek bolan ýagdaýda, programma döwüji şol programmanyň maşyn kodunyň assemblere salynmadyk, ýagny göni Delphi programmirleme diliniň görünyän (wizual) komponentler häsiýetini üýtgetmäge çalşar. Emma bu ýagdaýda ol gaýtarylmasyz programmany bozar hem-de öz beýleki synanyşyklaryny dowam etdirmip bilmez. Onuň programmanyň birnäçe nusgasyny saklap galmagy mümkin we nobatdaky nusga zaýalanandan soň, indikiniň üstünden synag geçirip başlamagy mümkin. Bu ondan köp wagty we resurslary talap etmegi mümkin hem bolsa, programma bolan howpy aradan aýyrmaz. Şol sebäpli ýene bir bent teklipl edilýär:

programmanyň maşyn kodunyň içindäki maglumatlara parallel ýagdaýda ulgamyň reýestrinde olaryň göçürmelerini saklamak.

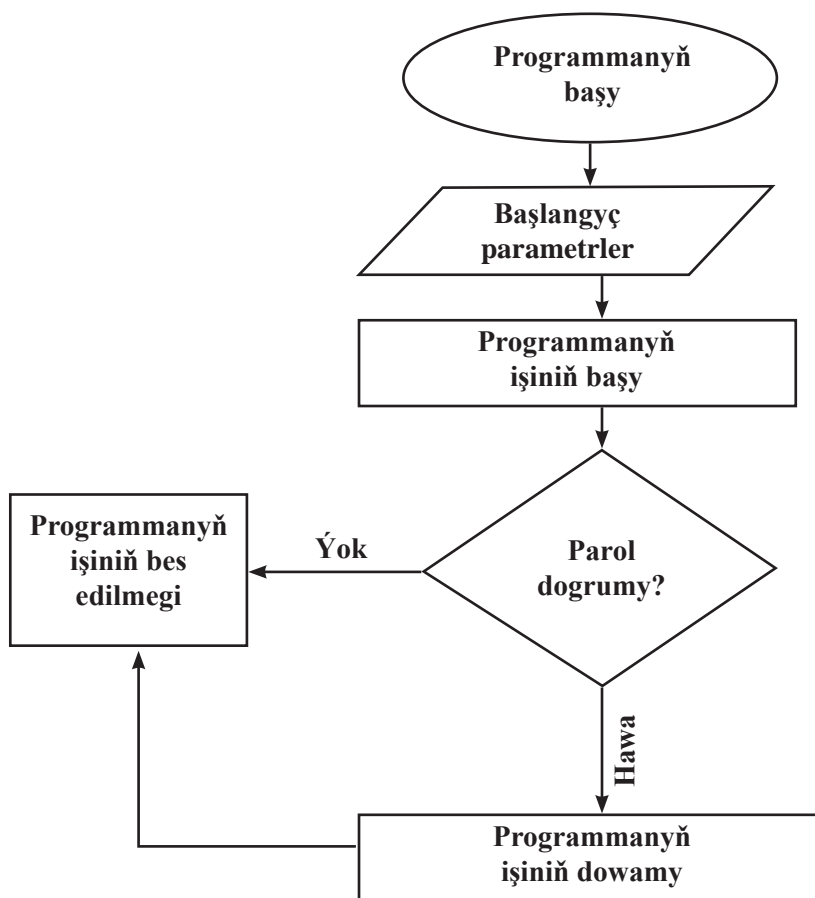
Bu ýagdaýda parallel yzarlama programma döwüjiniň mümkinçiliklerini çäklendirýär, eger ol belli bir sebäplere görä maşyn kodundaky maglumatlary özüne gerek ýagdaýyna getirip bilse hem (örän mümkin däl), programmany sazlanýandan soň, goýberen mahaly, ol elbetde, reýestrdäki maglumatlar bilen gabat gelmez. Bu ýagdaýda programma öz-özünü ýok etmek mehanizmini goýberip biler we programma döwüji hiç zatsyz galyp biler.

Emma OllyDbg sazlaýjynyň örän köp mümkinçilikleri bar. Meselem, programma döwüji programmanyň işleýşi baradaky gizlenen

maglumatlar bilen gyzyklanman, diňe şertli geçişler bilen meşgul bolmagy mümkin. Onuň üçin şol maglumatlaryň dogrudygynyň ýa-da nädogrudygynyň anyklamaklyk üçin programmanyň içinde nirä eltýändigini bilmeklik ýeterlidir.

Muňa düşünmek üçin, şulary beýan etmek gerek.

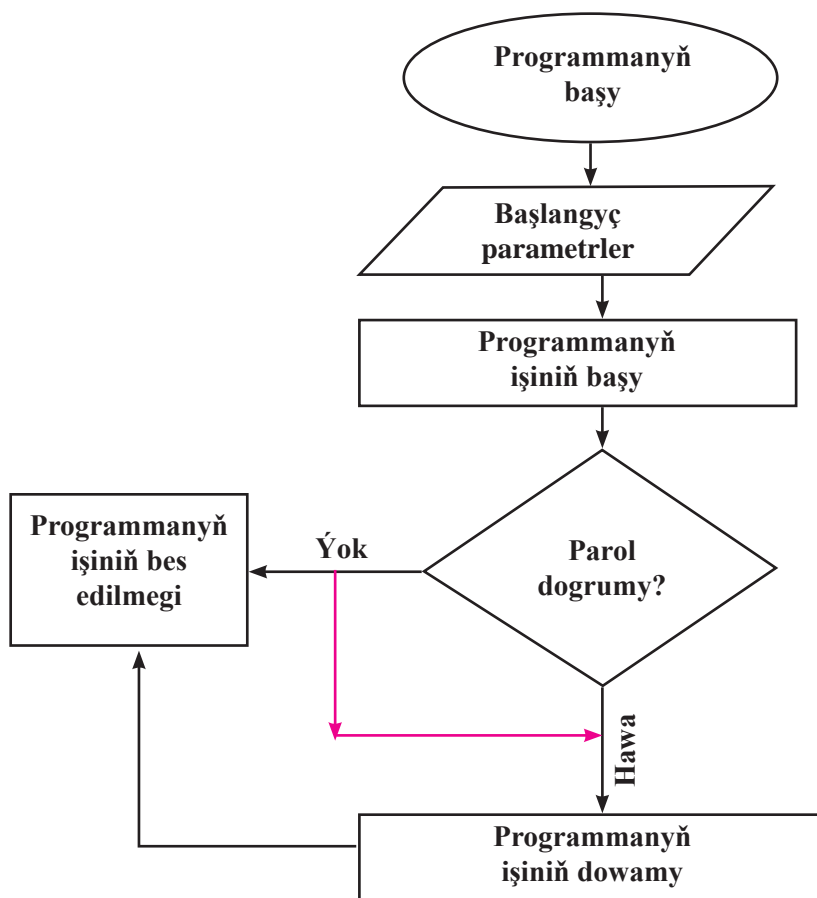
Meselem, adaty ýagdaýda programma parol dogry girizilen ýagdaýynda özüniň içindäki belli bir ýere geçip bilýär, parol dogry däl bolsa, onda başga ýere, meselem programmanyň işinden çykylyan ýere geçip bilýär (aşakdaky blok shema).



5.18-nji surat. Programmanyň goragynyň adaty işlemegi

Şeýlelik bilen, programma döwüji paroly anyklaman, sazlaný-
ýan programmanyň işini aşakdaky blok-shema boýunça üýtgedip bil-
ýär.

Shemadan görnüşi ýaly, parol dogry däl hem bolsa, geçiş şol
bir programmanyň işiniň dowam edýän ýerinde amala aşyrylýar
(gyzyl oklar). Bu programma „döwmekde“ bir döwür rewolýusiýa
bolupdy. Dogrudan hem, paroly bilmek gerek däl, programmanyň
goýberilmeginiň sanyny üýtgetmek gerek däl, diňe bir şertiň ýerine
ýetmeýän ýagdaýyny şertiň ýerine ýetýän ýagdaýy bilen bilelikde bir
dogry ugurdan goýbermek ýeterlikdir.



5.19-njy surat. Sazlaýjy arkaly üýtgedilen programmanyň işi

Emma programma döwüji şertiň barlanylýandygyny nähili kesgitleýär? OllyDbg ýüzlerçe API funksiýalary tanamagy başarýar, şeýle hem programma döwüjiler örän güýçli strateglerdir. Olar ýaltanman programmanyň işini ädimleýin debaggerde seljerýärler we gerekli koduň setiri tapylandan soň ony ussatlyk bilen üýtgetmegi başarýarlar.

Şertli geçiş bir zadyň başga zat bilen deňeşdirilmesi (meselem, dogry parolyň girizilen tekst bilen deňeşdirilmegi) esasynda amala aşyrylýar. Assembler dilinde ähli deňeşdirmeler **CMP** arkaly amala aşyrylýar. Mundan soň şertli geçişler amala aşyrylýar:

ja – eger uly bolsa;
jb – eger kiçi bolsa;
je – eger deň bolsa;
jae – eger uly ýa-da deň bolsa;
jbe – eger kiçi ýa-da deň bolsa;
jne – eger deň bolmasa;
jna – eger uly bolmasa
jnb – eger kiçi bolmasa
jnae – eger uly ýa-da deň bolmasa
jnbe – eger kiçi ýa-da deň bolmasa
jz – eger nol bolsa;
jnz – eger nol bolmasa;
we başg.

CMP operatory arkaly registrler deňeşdirilende programma döwüjiler haýsy maglumatyň haýsy registrde ýerleşýändigini kesgitleýärler. Meselem, **if** şertli operator assembler diline geçirilende **CMP** görnüşine eýe bolýar. Ýokarda agzalanlary hasaba almak bilen debaggerlere garşy aşakdaky bendi teklip etmek bolar:

Şertli geçişleri gizlemek gerek, olary düzümlü ýagdaýa getirmeli.

Meselem, biz **if** operatory arkaly **Label1**-de ýerleşen dogry paroly **Edit1**-de girizilen tekst bilen deňeşdirenimizde olary gönümel deňeşdirmän, ilki başda olaryň içinde ýerleşen sözüň her simwolynyň ASCII koduny kesgitlep, olary birine goşup soňra deňeşdirmek belli bir netijeleri bermegi mümkin.

Mysal. Parolyň simwollarynyň ASCII kodlaryny kesgitläp, olary jemlemeli we soňra girizilen tekstiň simwollarynyň ASCII kodlarynyň jemi bilen deňeşdirmeli.

Goý, biziň dogry parolymyz **merdan** bolsun, şeýlelik bilen:

Label1.Caption[1] = m = ASCII kody = 109

Label1.Caption[2] = e = ASCII kody = 101

Label1.Caption[3] = r = ASCII kody = 114

Label1.Caption[4] = d = ASCII kody = 100

Label1.Caption[5] = a = ASCII kody = 97

Label1.Caption[6] = n = ASCII kody = 110

S = 109 + 101 + 114 + 100 + 97 + 110 = **631**

Edit1-de bolsa maksat girizilen bolsa, aşakdakylary alýarys:

Edit1.Text[1] = m = ASCII kody = 109

Edit1.Text[2] = a = ASCII kody = 97

Edit1.Text[3] = k = ASCII kody = 107

Edit1.Text[4] = s = ASCII kody = 115

Edit1.Text[5] = a = ASCII kody = 97

Edit1.Text[6] = t = ASCII kody = 116

S1 = 109 + 97 + 107 + 115 + 97 + 116 = **641**

Şeýlelik bilen, $S \neq S1$ şerti ýerine ýetmeýär (diýmek, parol nädogry).

Programma döwüjiler üçin dogry şertiň indi nirede amala aşyrylýandygy hem-de **S** we **S1** ululyklaryň hakykatda näme üçin ulanylýandygyny anyklamak gaty kyn bolar.

Emma bu ýerde ýene bir goşmaça barlaglary goşmak gerek, sebäbi 631 jemleýji koda şular ýaly yzygiderlikler eýe bolup durýar – **nadrem** (**merdan** sözüniň ters ýazylyşy), **iiiiij** we münlerçe başgalar. Şol sebäpli aşakdaky bendi goşmak maksadalaýykdyr:

Goşmaça barlaglary we deňeşdirmeleri geçirmek gerek, üstesine-de boş barlaglary we deňeşdirmeleri, boş geçişleriň örän köp sanlysyny programmada gurnamak gerek.

Boş barlaglaryň we deňeşdirmeleriň, şeýle hem boş geçişleriň köp sany, programma döwüjiniň işini birneme bulaşdyrmagy mümkin. Sebäbi, assembler kody anyk barlaglary geçirmäge mümkinçilik

bermeýär we onuň örän uly göwrümlü bolmagy programma döwüjiniň yzarlama işini ýalňyş şertli geçişler boýunça eltmegi mümkin.

Eger belli bir sebäplere görä ýokarda agzalan çäreler hem kömek bermese, onda ýene bir maslahaty teklip edip bolar:

DebuggerPresent funksýasyny ulanmaklyk.

Bu funksiýa programmanyň sazlaýjy tarapyndan goýberilýändigini kesgitlemegi amala aşyrýar. Bu ýagdaýda islendik hereketleri ýerine ýetirip bilýär – debuggeri ýapyp, ýok etmekden başlap öz-özünü ýok etmektige çenli. Aşakda şol funksiýanyň ýazgysy getirilen.

function DebuggerPresent: boolean;

type

TDebugProc = function: boolean; stdcall;

var

Kernel32: HMODULE;

DebugProc: TDebugProc;

begin

Result := False;

Kernel32 := GetModuleHandle('kernel32.dll');

if Kernel32 <> 0 then

begin

 @DebugProc := GetProcAddress(Kernel32, 'IsDebuggerPresent');

 if Assigned(DebugProc) then

 Result := DebugProc;

end;

end;

Bu bölümiň ahyrynda bir programma koduna seredeliň. Bu programma kody belli bir möhletiň dowamynda işlemegi göz önünde tutýar. Çäk möhleti reýestrde hem-de programmanyň maşyn kodunda saklanylýar. Soňkyny amala aşyrmak gaty çylşyrymly, sebäbi Windows operasion sistemasy programma işläp duran mahaly gönümel öz maşyn koduna ýazmaklygy amala aşyrmaga mümkinçilik bermeýär. Emma sistema birnäçe aldamak usuly bilen ol ýerine ýetirildi. Şeýle hem faýllara we reýestriň açaryna bolan ýollar gönümel Delphi programmirleme diliniň Label komponentlerinden şifrlenlen görnüşinde

amala aşyrylýar. Bu programma kodunda ýokarda agzalan hemme usullar amala aşyrylan. Tejribede barlanyldy: bu programma kodunyň goragyny OllyDbg programmasy arkaly döwmek, eger mümkin däl bolmasa-da, örän kyn bolar. Aşakda onuň esasy bölegi getirilen. Bu programma koduny programmanyň görünýän (wizual) komponentleri bilen tanyşman ulanmak mümkin däl.

procedure TForm1.FormShow(Sender: TObject);

```
Label 1,2;  
var  
la:array of byte;  
ra:array [1..9] of byte;  
k:longint;  
FileName:string;  
ks:integer;  
reg:TRegistry;  
begin  
if DebuggerPresent then  
    begin  
        ShowMessage('Programmany döwjek bolýarlar!!!');  
        Label5.Caption:='6';  
        goto 2;  
    end;  
Present:= Now;  
DecodeDate(Present, Year, Month, Day);  
DecodeTime(Present,Hour, Min, Sec, Msec);  
ks:=0;Randomize;  
  
for i:=1 to length(Label2.Caption) do  
j[i]:=chr(ord(Label2.Caption[i])-3);  
h:=j;  
Label2.Caption:=h;  
  
for i:=1 to length(Label3.Caption) do  
j1[i]:=chr(ord(Label3.Caption[i])-5);
```

```

h1:=j1;
Label3.Caption:=h1;
for i:=1 to length(Label6.Caption) do
j[i]:=chr(ord(Label6.Caption[i])-5);
h2:=j;
Label6.Caption:=h2;
for i:=1 to length(Label7.Caption) do
j1[i]:=chr(ord(Label7.Caption[i])-6);
h3:=j1;
Label7.Caption:=h3;

```

```

IF FileExists(h)=true THEN

```

```

BEGIN

```

```

assignFile(b,h);

```

```

i:=0;

```

```

FileMode:=fmOpenRead;

```

```

reset(b);

```

```

while not eof(b) do

```

```

    begin

```

```

        SetLength(la, Length(la) + 1);

```

```

        read(b,la[i]);

```

```

        inc(i);

```

```

    end;

```

```

    CloseFile(b);

```

```

    FileMode:=fmOpenReadWrite;

```

```

    k:=i;

```

```

    for i:=0 to k-1 do

```

```

        begin

```

```

            Reg := nil;

```

```

            TRY

```

```

                reg := TRegistry.Create;

```

```

                reg.RootKey := HKEY_LOCAL_MACHINE;

```

```

                reg.LazyWrite := false;

```

```

            if (la[i]-ord(Label5.caption[1])=0) and (la[i+1]-ord(Label5.caption[1])=0) and (la[i+2]-ord(Label5.caption[1])=0) then

```

```

begin
  if (la[i+3]-ord(Label5.Caption[2])=0) and (la[i+4]-ord(Label5.
Caption[2])=0) and (la[i+5]-ord(Label5.Caption[2])=0) and (la[i+6]-
ord(Label5.Caption[2])=0) then
    begin
      reg.OpenKey(h2,false);
      if reg.ValueExists(h3)=true then
        begin
          if Assigned(Reg) then Reg.Free;
          Form1.Close;
        end;
      la[i+3]:=Day;
      la[i+4]:=Month;
      la[i+5]:=Year;
      la[i+6]:=49;
      la[i+8]:=((60*hour)+min) div 256;
      la[i+9]:=((60*hour)+min) mod 256;
      for f:=1 to 9 do
        begin
          ra[f]:=random(255);
          ks:=ks+ra[f];
        end;

      for f:=1 to 9 do Label4.Caption:=Label4.Caption+chr(ra[f]);
      reg.WriteString(h3,Label4.Caption);
      reg.CloseKey;

      la[i+10]:=ks div 256;
      la[i+11]:=ks mod 256;
    end
  else
    begin
      reg.OpenKey(h2,false);
      Label4.Caption:=reg.ReadString(h3);
      reg.CloseKey;
    end
  end
end

```



```

for f:=1 to 9 do
ks:=ks+ord(Label4.Caption[f]);
Label4.Caption:=inttostr(ks);
Label5.Caption:=inttostr(la[i+10]*256+la[i+11]);
if ks - (la[i+10]*256+la[i+11])<>0 then Close;
if la[i+6]-ord(Label1.caption[8])>0 then
begin
//Form1.Hide;
Form2.Label3.Caption:=inttostr(strtoint(Label5.Caption)*3);
Form2.showmodal;
end;
if form2.Label2.Caption='5' then
begin
la[i+6]:=49;ks:=0;
reg.OpenKey(h2,false);
for f:=1 to 9 do
begin
ra[f]:=random(255);
ks:=ks+ra[f];
end;
la[i+10]:=ks div 256;
la[i+11]:=ks mod 256;
Label4.Caption:="";
for f:=1 to 9 do Label4.Caption:=Label4.Caption+chr(ra[f]);
reg.WriteString(h3,Label4.Caption);
reg.CloseKey;
Label5.Caption:='6';
end;

```

```

if (la[i+3]-day<>0) or (la[i+4]-month<>0) or (la[i+5]-(year mod
256)<>0) then
begin
la[i+3]:=Day;
la[i+4]:=Month;
la[i+5]:=Year;

```

```

        inc(la[i+6]);
    end
else
    begin
        if (la[i+8]*256+la[i+9])-(hour*60+min)>0 then
            begin
                inc(la[i+6]);
                la[i+8]:=((60*hour)+min) div 256;
                la[i+9]:=((60*hour)+min) mod 256;
            end;
        end;
    end;
end;
reg.free;
except
if Assigned(Reg) then Reg.Free;
END;
end;
RenameFile(h,h1);
rewrite(b);
for i:=0 to k-1 do
write(b,la[i]);
CloseFile(b);
END;
FileName := changefileext(paramstr(0), '.bat');
assignFile(a, FileName);
rewrite(a);
writeln(a, '1');
writeln(a, format('Erase «%s»', [Label3.Caption]));
writeln(a, format('If exist «%s» Goto 1', [Label3.Caption]));
writeln(a, format('Erase «%s»', [FileName]));
closefile(a);
ShellExecute(Handle, 'Open', PChar(FileName), nil, nil, sw_hide);
SHChangeNotify(SHCNE_ASSOCCHANGED, SHCNF_IDLIST,
nil, nil);

```

```
2:
if label5.Caption='6' then Close;
end;
```

Bu bölümde hâzirki zaman maglumaty goramagyň iň gowşak tarapyna, ýagny debugger arkaly hüjümiň astynda maglumat goragynyň islendik görnüşiniň “ýykylyp” bilmegine seredildi.

Şeýle hem, bu bölümde amala aşyrylan işleriň netijesi hökmünde aşakdakylary bellemek bolar (olar wajyplygy boýunça yzygiderli ýerleşdirilen):

- debuggerPresent funksiýasyny ulanmaklyk;
- goşmaça barlaglary we deňeşdirmeleri geçirmek gerek, üstesine-de boş barlaglary we deňeşdirmeleri, boş geçişleriň örän köp sanlysyny programma gurnamak gerek;
- şertli geçişleri ýaşyrmak gerek, olary düzümlü ýagdaýa getirmeli;
- programmanyň maşyn kodunyň içindäki maglumatlarda parallel ýagdaýda ulgamyň reýestrinde olaryň göçürmelerini saklamak;
- hemme parollary, çäklendiriş ýazgylary we ş.m. daşky faýllarda däl-de programmanyň öz maşyn kodunyň içinde saklamaklyk teklipe edilýär;
- hemme ýaşyrylan parollary ýa-da faýllara bolan ýollary şifrlmeli;
- programmanyň kodunda gönümel setir ululyklara salgylanmaly däl-de, olaryň deregine programmirlene diliniň öz tekst komponentlerini ulanmak gerek we olary degişli ýaşyrmagy amala aşyrmaly.

Eger debugger arkaly hüjümden maglumat goragynyň hemme görnüşleri zeper çekýän bolsa, onda şol hüjüme garşy olary utgaşykda ulanmak gerek. Bu bölüm hem şoňa şaýat boldy, sebäbi debuggerlere garşy şifrlmegi, parol goragyny, çäklendirmegi reýestriň üsti bilen amala aşyrmak peýdalanyldy.

Tejribe işleri

1. Assembler dilinde ýazylan gorag programmanyň koduny Notepad programmasynda seljermek.
 2. Pascal dilinde ýazylan gorag programmanyň koduny Notepad programmasynda seljermek.
 3. C dilinde ýazylan gorag programmanyň koduny Notepad programmasynda seljermek.
 4. Delphi dilinde ýazylan gorag programmanyň koduny Notepad programmasynda seljermek.
 5. Assembler dilinde ýazylan gorag programmanyň koduny OllyDbg programmasynda seljermek.
 6. Pascal dilinde ýazylan gorag programmanyň koduny OllyDbg programmasynda seljermek.
 7. C dilinde ýazylan gorag programmanyň koduny OllyDbg programmasynda seljermek.
 8. Delphi dilinde ýazylan gorag programmanyň koduny OllyDbg programmasynda seljermek.
 9. Ýönekeý dizassembler programmasyňy ýazmaly.
-

VI. REÝESTR GORAGY ÜPJÜN EDIJI HÖKMÜNDE

1. Reýestriň gurluşy.
2. Reýestriň wezipeleri.
3. Reýestriň uniwersal häsiýetini barlagdan geçirmek we onuň maglumaty goramagyň usullarynda ulanmagyň mümkinçiligi.
4. Reýestriň awtoýükleniş bölümlerini seljeriş hem-de onuň wirus hüjüminiň goldawy hökmünde ulanylmagy.
5. Reýestri seljermek arkaly prosesleriň arasyndan we ulgam bukjasyndan wiruslaryň komponentlerini ýok etmek.

Geliň indi ýene bir wajyp bölümleriň biri bolan – Windowsyň reýestri bilen tanşalyň. Bu gural Windows amallar ulgamynyň kadaly işlemeginde uly orny tutýar. Reýestrdäki kemçilikler Windows amallar ulgamynda ýüze çykyan näsazlyklaryň sebäbi bolup bilýär. Eger deňeşdirip aýtsak, Windows amallar ulgamy üçin reýestr, edil kompýuter üçin BIOS ýalydyr.

Reýestr möçberi boýunça ägirt uly zat. Ony doly teswirlemeklik mümkin zat däl. Hiç bir edebiýatda reýestriň edýän işi barada anyk maglumatlar getirilmýär. Eger has düşnükli dilde aýtsak – Windows-da her bir sazlama we dolandyryş işleri geçirilende, ol reýestre ýazylýar we soňra amallar ulgamy reýestri okap, ony ýerine ýetirýär. Meselem, aýdalyň, gurluşlar ulgamynda bir gural wagtlaýyn öçürildi. Şonuň öçürilmegi göni reýestre ýazylýar. Kompýuter öçürilip, soňra işledilenden soň, Windows amallar ulgamy öz reýestriňi okaýar we hemme ön geçirilen üýtgemeleri öz işinde amala aşyrýar. Şol sebäpden hem, indiki ýüklenende şol öçürilen gural, öçürilen ýagdaýda galýar. Şol guralyň öçürilendigi baradaky maglumat reýestrde düzedilse, onda gurluşlar ulgamynda sazlama işini geçirmän hem, Windowsyň indiki ýüklenişinde şol gural işläp ýaly edip bolýar. Şeýlelik bilen, reýestr görkezme berýän ýazgy guraly bolýar, şol guralda görkezme üýtgedilen bolsa, amallar ulgamy şol üýtgetmä görä işleri geçirýär.

Reýestre has dogry düşünmek üçin, ol barada biraz maglumat almaly we sazlamalaryň anyk ýagdaýlaryny görmek gerek, şol sebäpli, şol yzygiderlikde düşündirme berip başlalyň.

6.1. Reýestriň gurluşy

Windowsyň reýestri – 5 sany kök bölümlerden (root keys) ybarat: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS we HKEY_CURRENT_CONFIG.

Her bölüm bahasy bolan elementleri – parametrleri (value entries), şeýle hem onuň içine girýän bölümleri saklap bilýär (subkeys). Bu düzgüne düşünmek üçin faýl ulgamyna meňzetme getirmek mümkin. Reýestriň düzümindäki bölümler kataloglara meňzeş, bahasy bolan elementler — faýllara. Kök bölümleriň hemmesiniň ady HKEY_ setirden başlanýar, her bir kök bölümüň teswirlenmesi bolsa, aşaky tablisada getirilen [15].

| Kök bölümüň ady | Teswirleme |
|--------------------|--|
| 1 | 2 |
| HKEY_LOCAL_MACHINE | Kompýuter ulgamy barada global maglumaty saklaýar, şol maglumatyň içine apparat serişdeleri we amallar ulgamy baradaky maglumatlar, şol sanda şinanyň kysymy, ulgam huşy, gurluşlaryň draýwerleri we ulgam goýberilende dolandyryjy maglumatlar girýär. Bu bölümde saklanylýan maglumat ulgamydaky hemme ulanyjlara täsir edýär. Reýestriň köpbaşgançaklylygyň iň ýokary derejesinde bu bölüm üçin üç sany lakam bar: HKEY_CLASSES_ROOT, HKEY_CURRENT_CONFIG we HKEY_DYN_DATA. |
| HKEY_CLASSES_ROOT | Goşmaça programmalaryň we faýllaryň görnüşleriniň arasyndaky assosiasiýalary saklaýar. Mundan başga hem, bu bölüm OLE (Object Linking and Embedding) maglumatyny saklaýar, ol COM obýektleri bilen assosirlenen. Bu bölümüň parametrleri HKEY_LOCAL_MACHINE\Software\Classes bölümde ýerleşen parametrlere gabat gelýär. |

| 1 | 2 |
|---------------------|--|
| HKEY_CURRENT_CONFIG | <p>Şol wagtky ulanylýan apparat profili üçin konfigurasiýa maglumatlaryny saklaýar. Apparat profilleri özi bilen HKEY_LOCAL_MACHINE kök bölümiň Software we System bölümleriň maglumatlary bilen bellenen serwisleriň we gurluşlaryň standart konfigurasiýasyna girizilen üýtgemeleriň toplумы bolup durýar. HKEY_CURRENT_CONFIG bölümde diňe üýtgemeler görkezilýär. Mundan başga hem, bu bölümiň parametrleri HKEY_LOCAL_MACHINE\ System\CurentControlSet\ HardwareProfites\Curent bölümünde emele gelýär.</p> |
| HKEY_CURRENT_USER | <p>Şol mahal ulgamda bellige alnan ulanyjynyň profilini saklaýar, şol sanda daşky gurşawyň üýtgeýänlerini, iş meýdanyň sazlamalaryny, toruň, printerleriň we goşmaça programmalaryň sazlamasynyň parametrlerini saklaýar. Bu bölüm özi bilen HKEY_USERS\ username bölümüne salgylanma bolup durýar, şol ýerde username — şol mahal ulgama giren (bellige alnan) ulanyjynyň ady.</p> |
| HKEY_USERS | <p>Hemme işlenen ýagdaýda ýüklenilen ulanyjy profilleri, şol sanda HKEY_CURRENT_USER, şeýle hem deslapdan duran profili saklaýar. Serwere daşlaşdyran elýeterligi alýan ulanyjylar bu bölümde saklanylýan profilere eýe däl; olaryň profilleri olaryň öz kompýuterindäki reýestrine ýüklenýär. HKEY_USERS bölümü \Default, şeýle hem her ulanyjynyň howpsuzlyk kesgitlendirijisi bilen (Security ID) kesgitlenýän beýleki bölümleri içinde saklaýar.</p> |

Reýestriň maglumatlary, reýestriň bölümünde ýerleşen parametrlar görnüşinde saklanylýar. Her parametr at bilen, maglumatyň görnüşi we baha bilen häsiýetlendirilýär.

| Maglumatlaryň görnüşi | Teswirleme |
|-----------------------|--|
| REG_BINARY | Ikilik san görnüşdäki maglumatlar. Apparat komponentleriň köpüsi ikilik san görnüşindäki maglumaty saklaýarlar. Reýestriň redaktory bu maglumaty on altylyk san formatynda görkezýärler. |
| REG_DWORD | Maglumatlar uzynlygy 4 baýt bolan baha görnüşinde görkezilýär. Maglumatlaryň bu görnüşini gurluşlaryň draýwerleriniň we serwisleriň parametrleriniň köpüsi ulanylýar. Reýestriň redaktorlary bu maglumatlary ikilik, on altylyk we onluk san formatynda görkezip bilýär. |
| REG_EXPAND_SZ | Maglumatlaryň giňelýän setiri. Bu setir özi bilen, goşmaça programma tarapyndan çagyrylanda çalşyrylyp bilinjek üýtgeýäni saklaýan tekst bolup durýar. |
| REG_MULTI_SZ | Köp setirli meýdan. Adam tarapyndan görünmäge amatly bolan formatdaky tekst setirleriň sanawy bolup durýan bahalar adatça maglumatlaryň şu görnüşine eýe bolýarlar. Setirler NULL simwoly bilen bölünen. |
| REG_SZ | Adam tarapyndan görmäge amatly bolan formatdaky tekst setiri. Komponentleriň teswirlemesi bolup durýan bahalarda hut şu maglumatlaryň görnüşi berilýär. |

6.2. Reýestriň wezipeleri

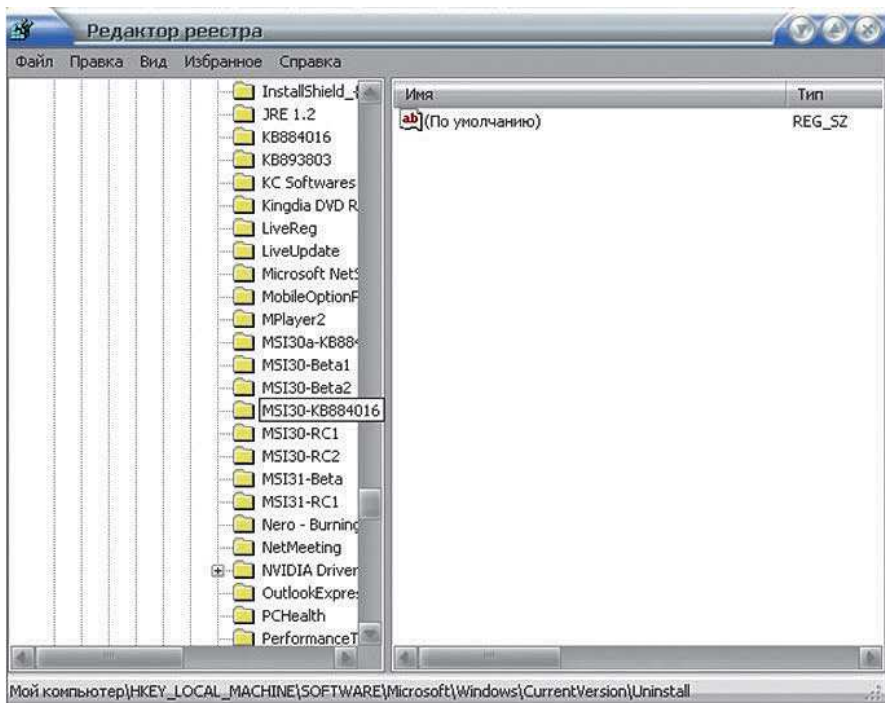
Windows amallar ulgamyna ulanyjynyň ýerine ýetirýän işlerine baglylykda birnäçe programmalaryň gurnalmagy mümkin. Olaryň sanawyny görmek üçin, şeýle hem olary ulgamdan aýyrmak, olaryň

düzümlerine goşmaça girizmek üçin Dolandyryş paneline girmeli (“Пуск – Настройки – Панель управления” buýrukларыň uzygiderliligini ýerine ýetirmeli).

Panelde „Установка и удаление программ“ nuşana basmaly. Açylan penjirede amallar ulgamyna gurnalan programmalaryň sany görkeziler. Olaryň her birine basylan ýagdaýynda gapdalynda olary ýok etmek ýa-da başga amalyň ýerine ýetirilmegini amala aşyran düwmejik emele gelýär. Kähalatlarda programma ýok edilýär, onuň faýllary hem amallar ulgamyndan ýok edilýär, emma onuň ady şol sanawdan aýrylmaýar.

Bu ýagdaýda Windowsyň reýestrini ulanmak gerek. Reýestre girmek üçin „Пуск – Выполнить“ buýrugyny ýerine ýetirmeli. Açylan penjiräniň tekst ýazmagy hödürleýän setirinde **regedit** diýip ýazmaly we OK düwmejige basmaly.

6.1-nji suratda açylan Windowsyň reýestriniň düzümini görmek bolýar. Düzümi boýunça ol edil bukjalaryň agaç düzümine meňzeýär.



6.1-nji surat. Reýestriň gurluşy

Islendik bölümiň düzümine girýän beýleki düzüm bölekleri görmek üçin şol bölümiň çep gapdalyndaky duran “+” nyşanyna basmaly. Netijede, onuň düzümine girýän beýleki bölekler görüner. Eger bölümiň gapdalynda “+” nyşany bolmasa, onda onuň düzümine bölüm girmeyär. Eger bölümiň gapdalyndaky nyşana basman özüne basylsa, onda şol bölümiň içindäki parametrleri görmek bolýar.

Göz önünde tutan amalymyzy ýerine ýetirmek üçin HKEY_LOCAL_MACHINE kök bölüminiň gapdalyndaky “+” nyşanyna basýarys. Netijede, onuň içine girýän beýleki bölümler açylar. Şeýle usul bilen SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall yzygiderlilik bilen bölümleriň gapdalyndaky nyşana basmaly. Uninstall bölümünde ýerleşen bölümlere seredilse olaryň köpüsiniň atlary Windows amallar ulgamyna gurnalan programmalaryň atlaryna gabat gelyändirler (6.1-nji surat).

Bu ýerde bölümleriň arasynda, ulgamdan ýok edilen, emma „Установка и удаление программ“ penjiredäki sanawda ady galan programmanyň adyny tapyp, ony ýok edip bolýar. Munuň üçin, şol bölümi syçanjyk bilen belläp, onuň sag düwmejigi bilen çagyrylýan kontekst menýudan degişli buýrugy çagyrmaly.

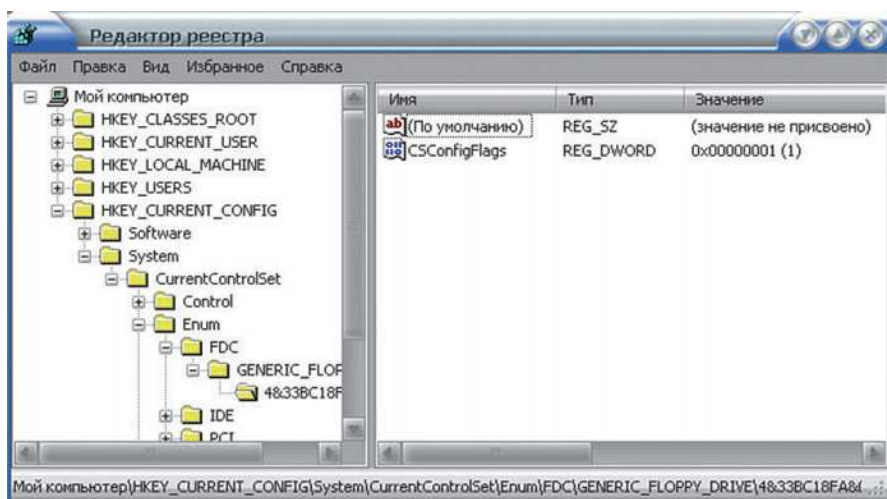
Netijede, Uninstall bölüminden onuň içine girýän belli bir bölüm ýok edilse, şol bölümiň adyny göterýän programmanyň ady „Установка и удаление программ“ penjiräniň sanawyndan aýrylar.

Indi beýleki mysala garalyň. Windows-yň Gurluşlar ulgamyndan (Диспетчер устройств) bir guraly, meselem, **Floppy disk drive** gurluşy (çeýe magnit diskleri – disketalary okaýan), kontekst menýudan degişli buýrugy çagyryp wagtlaýyn öçürmeli. Şu ýagdaýda Windowsyň reýestrine girmeli we aşaky bölümleriň yzygiderliligini açmaly:

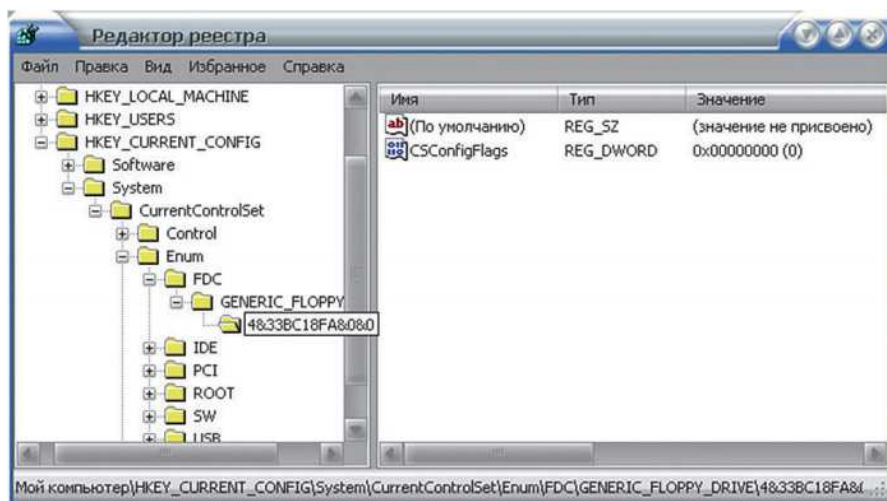
HKEY_CURRENT_CONFIG\System\CurrentControlSet\Enum\FDC\GENERIC_FLOPPY_DRIVE\4&33BC18FA&0&0. Soňky bölümiň özüne basmaly (6.2-nji surat).

Bu ýerde bahasy görkezilen diňe bir parametr bar. Onuň bahasy ikilik sanda 00000001 deň. Reýestriň penjiresini ýapmaly.

Indi bolsa öçürilen guraly gurluşlar ulgamyndan gaýtadan işletmeli.



6.2-nji surat. Gurluşlary sazlamak



6.3-nji surat. Gurluşlary işletmek

Ýene reýestri açyp ýokarda görkezilen yzygiderligi açmaly. Netijäni 6.3-nji suratda görmek bolar.

Ýokarky parametriň bahasy üýtgäp 00000000 deň bolupdyr. Şeýlelik bilen, gurluşyň şu parametriniň gapdalynda 00000001-lik bahanyň durmagy, onuň öçürilendigini aňladýar. Adaty ýagdaýda

00000000 baha durmaly. Eger 6.2-nji we 6.3-nji suratlara üns berip se-redilse, Floppy disk drive gurluşdan başga penjirede beýleki gurluşlar hem bar. Sebäbi, HKEY_CURRENT_CONFIG\System\CurrentControlSet yzygiderlikde ýerleşýän Enum bölümünde kompýuteriň käbir beýleki gurluşlarynyň ýagdaýy belenilýär.

Şu mysaly seljerip, amallar ulgamynda belli bir üýtgemeler we sazlamalar ýerine ýetirilende, olaryň netijeleri hökmany Windowsyň reýestrine ýazylýandygyny göz önümize getirmek kyn däl. Başgaça aýdylanda, reýestr maglumat saklaýjy ulgam bolup çykyş edýär.

Köp sazlamalar we üýtgemeler gös-göni, käbirleri bolsa diňe kompýuter öçürilenden soň gaýtadan işlenende ýa-da gaýtadan ýük-leme berlenden soň herekete girip başlaýar. Şol iki ýagdaýda hem reýestre ýazgy geçirilýär. Windows amallar ulgamy işläp başlanda ol reýestri okaýar hem-de mundan öňki goýberişde edilen sazlamalary ýene herekete girizýär we şu ýagdaý elmydama Windows amallar ulgamy işlenende bolup geçýär. Şol sebäpli, ulgamda bir gezek edilen sazlamalar uzak wagtlap, olar tä üýtgedilýänça ýa-da ýatyrylýança hereket edip bilýär. Diýmek, reýestr diňe maglumat saklaýjy däl-de, eýsem buýruk beriji ulgam bolup hem çykyş edýär.

6.3. Reýestriň uniwersal häsiýetini barlagdan geçirmek we onyň maglumaty goramagyň usullarynda ulanmagyň mümkinçiligi

Geliň indi reýestriň uniwersal häsiýetine göz ýetireliň. Ýokarda belleýşimiz ýaly, reýestr huşda ýerleşen operasion ulgamlaryň düzümine meňzeş gurluşa eýe bolup durýar. Bukjalar hökmünde reýestriň bölümlerini kabul etmek bolýar, faýllar hökmünde bolsa onuň açarlaryny. Reýestriň açarynda edil faýldaky ýaly, belli bir maglumaty saklap bolýar. Ol maglumatyň görnüşi islendik bolup bilýär – tekst, ililik san, on altylyk san we ş.m.

Mundan öňki bölümlerde goragyň birnäçe usullary gözden geçirildi. Olaryň käbir belli gorag parametrini (dogry paroly, goýberilişň çäk möhletini, çäk sanyny, kompýuteriň häsiýetnamasyny) saklaýan

ýazgynyň huşa ýazylmagyny amala aşyrýar. Şol ýazgynyň ýerleşýän ýerini we içindäki maglumatyny diňe programmany düzüji adam bil-melidir. Köplenç şol ýazgy gizlin faýlyň içinde ýerleşdirilýär.

Ýokardaky bölümleriň birinde gizlin ýazgynyň faýlyň içinde ýerleşdirilmeginiň kemçilikleri seljerilipdi.

Dogrudan hem ýazgy, programma kompýutere gurnalandan soň, ilkinji gezek goýberilende ýazylýar. Islendik adam şol günü kesgitläp, ulgamyň hödür edýän gözleg serişdelerinden peýdalanyň, sene boýunça faýlyň gözlegini amala aşyryp bilýär hem-de gizlin faýly tapyň bilýär.

Reýestrde açaryň gözlegini sene boýunça amala aşyryp bolmaýar. Bu bolsa şol ýazgynyň belli bir açarda ýerleşendigin, sene boýunça kesgitläp bolmaýandygyny aňladýar.

Köplenç faýllaryň içini debaggerler ýa-da notepad programmasy arkaly seljerip onuň ýazgysyny kesgitleýärler.

Reýestriň düzümini debagger ýa-da faýlyň baýt düzümini görkezýän programma serişdeler bilen görmek mümkin däl.

Köplenç güýçli kriptanalitikler faýlyň gözlegini onuň düzümi boýunça, çalşyryjy simwollar arkaly (? – bir simwolyň ýerine, * – birnäçe simwollaryň ýerine) örän netijeli gözlegi amala aşyryp bilýärler.

Reýestrde bolsa, hiç hili çalşyryjy simwollary kesgitlemek bolmaýar.

Faýl ulagamynda gözleg parametrlerine gabat gelýän birnäçe faýllary bir gözlegde tapmak bolýar. Bu bolsa şol faýllary seljermek arkaly ýaşyrylan ýazgynyň kesgitlenmegine getirmegi mümkin.

Reýestrde açarlaryň gözlegi yzygiderli amala aşyrylýar, ýagny bir açar tapylýar, ony görüp ikinjini gözlege goýbermeli bolýar. Bu hem gizlin ýazgynyň gözlegini haýalladýar.

Iň uly operasion sistemanyň faýl ulgamynda faýllaryň sany häzirki wagtda umuman 1000 000-dan ýokary geçmeýär. Şeýle hem operasion sistemanyň gözleg serişdeleri faýlyň gözlegini onuň giňişligi

boýunça (*.exe, *.com, *.txt, *.doc we ş.m.) amala aşyrmak bolýar. Bu bolsa ýazgynyň gözlegini aňsatlaşdyrýar.

Reýestrde umuman açarlaryň sany islendik operasion sistemanyň içindäki faýllaryň sanyndan köp, şeýle hem açarlaryň giňişligi bolmansoň, gözleg çylşyrymlaşýar.

Faýllarda maglumaty ýaşyrmak üçin şifrlemegi peýdalanmak gerek bolýar.

Reýestrde ýazgyny şifrlemek zerurlygy ýüze çykmaýar, sebäbi ýazgyny ikillik san ulgamyna ýa-da on altlyk san ulgamyna geçirmek arkaly, ol awtomatiki şifrlenýär.

Ýazgynyň faýla ýazylmagy belli bir derejede az hem bolsa belli bir wagty talap edýär, ol bolsa programmanyň operatiw huşa ýüklenmegini, ýagny goýberilmegini haýalladyp biler.

Reýestre ýazgynyň ýazylmagy bolsa, faýla ýazylmaktan tiz amala aşyrylýar, bu bolsa programmanyň goýberilmegini haýallatmaýar hem-de birnäçe açarda ýazgylary ýazyp olaryň barlagyny amala aşyrmagy mümkin edýär.

Reýestriň şeýle uniwersal häsiýetleri ony goramagyň dürli usullarynda, goragyň bir halkasy hökmünde ulanylmagyna mümkinçilik berýär we goragy ýokary hilli we netijeli edýär.

6.4. Reýestriň awtoýükleniş bölümlerini seljeriş hem-de onuň wirus hüjüminiň goldawy hökmünde ulanylmagy

Reýestriň iň wajyp bölegi hökmünde – bu awtoýükleniş bölümlerini saklanylmagy. Kompýuter işlenenden soň, Windows operasion sistemasy ýüklenende reýestriň maglumaty okalyp başlanylýar. Şol sebäpli, käbir programmalaryň atlaryny we olaryň ýerleşýän ýerini aýratyn bir reýestriň bölümünde görkezmek bilen şol programmalaryň awtomatiki ulanyjy gatnaşmazdan goýberilmegini gazanyp bolýar.

Reýestriň düzüminde awtoýükleniş amala aşyryan bölümler aşakda getirilen:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

«Whatever»=>c:\runfolder\program.exe»

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]

«Whatever»=>c:\runfolder\program.exe»

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\000x]

«RunMyApp»=>||notepad.exe»

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

«Whatever»=>c:\runfolder\program.exe»

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]

«Whatever»=>c:\runfolder\program.exe»

HKEY_LOCAL_MACHINE kök bölümde ýerleşen awtoýükleniş bölümlerindäki parametrlər amallar ulgamynda döredilen hemme ulanyjylar üçin degişli bolup durýar.

HKEY_CURRENT_USER kök bölümdäki awtoýükleniş bölümlerine ýazylan parametrlər bolsa, diňe haýsy ulanyjynyň işiniň dowamynda reýestre ýazylan bolsa, şol ulanyjynyň amallar ulgamyna giren mahaly ulanylýar.

Indi mysal hökmünde Windows amallar ulgamy açylanda Microsoft Word programmasy awtomatiki, ulanyjy goýbermezden açylar ýaly etmek pikiri emele gelse, şu amallary ýerine ýetirmeli.

- reýestre girmeli;
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run yzygiderlige girmeli;
- Run bölümüne basmaly;
- reýestriň sag böleginde parametrleriň ýazylan ýerinde syňanjygyň sag düwmejigini basyp kontekst menýuny çagyry-

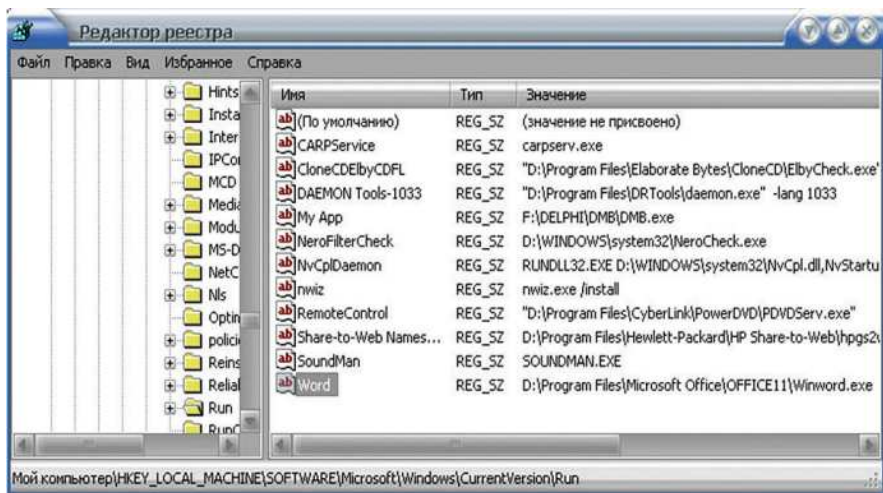
maly we “Создать” bendiniň “Строковый параметр” kömekçi bendini saýlamaly;

- täze emele gelen parametriň adyny girizeliň, meselem “Word” we Enter klawişasyny basmaly;
- syçanjygyň çep düwmejigi bilen parametriň adyna iki gezek tiz basyp, parametriň bahasyny girizmegiň penjiresini çagyrmaly. Bu penjirede aşaky setirde Word programmasynyň goýberiji Winword.exe faýlynyň ýerleşýän ýerini görkezmek gerek.

Bellik. Bilşimiz ýaly – Microsoft Office programmalar toplu-my gurnalanda, onuň faýllary Windows amallar ulgamynyň gurnalan diskinde ýerleşýän Program Files bukjasynda ýerleşýär. Bu bukjada Microsoft Office bukjasy ýerleşýandır. Microsoft Office öz gezeginde içinde bukjalary saklaýar. Şol bukjalaryň arasynda Office11 (12,13,14 we m.b.) bukjasy bolmaly. Onuň içinde bukjalaryň we faýllaryň arasynda Winword.exe faýly bar (onuň nyşany edil, Word programmasynyň resminamalary ýaly “W” harpyny saklaýandyr).

– Indi bahany ýazmagy hödürleýän setire degişlikde şu yzygiderliligi ýazalyň: C:\Program Files\Microsoft Office\OFFICE11\Winword.exe.

Netijäni 6.4-nji suratda görmek bolar.



6.4-nji surat. Programmalary awtomatik goýbermek

Görşümüz ýaly, täze parametr döredilen. Indi Windows amallar ulgamy gaýtadan ýüklenilse, Microsoft Word programmasynyň penjiresi açylar we täze boş resminama awtomatiki açylar. Bu ýagdaý amallar ulgamynda döredilen hemme ulanyjylara täsir eder. Eger diňe bir ulanyja ýokarky amaly degişli etmek üçin, onda ýokarky amalyň ikinji ädiminde `HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion\ Run` yzygiderligi açmaly. Galan ädimler üýtgemeýär.

Operasion sistema ýüklenende ulanyjy tarapyndan goýberilmän, özi ýüklenmeli islendik programma kadaly işlemek üçin şu usuldan peýdalanýar.

Emma bu usuly başga garaşylmadyk obýektler hem peýdalanýandyr.

Ylmy tehniki ösüşiň täze geň döredijiligi – ýörite kompýuter bozujylar: hakerler we krekerler. Hakerler (Hacker, iňlis) – kompýuter huliganlary, olar başga kompýutere girip bilendiklerinden lezzet alýarlar. Bir wagtda olar maglumat tehnikaýy örän gowy bilýärler. Telefon we öý kompýuterleri arkaly olar ykdysadyýetiň, ylmy gözleg merkezleriň, banklaryň hemme güýçli kompýuterleri bilen baglanyşykly maglumat iberiş torlaryna birikýärler.

Geň zat, emma ýokary hilli birleşmeleri gowy işleýän ulgam maglumatyň has üstünlikli ogurlanmagyna ýardam eder. Erbet soňunyň önüni almak üçin, diňe goragy netijeli amala aşyрман, eýsem yzarlama we howpsuzlygy dolandyрма funksiyalaryna edil kompýuter torlaryna goýlan ähmiýeti goýmalydyr. Hakerler öz klublaryny döredýärler, mysal üçin, Gamburgyň “Haos-kompýuter” kluby, öz býulletenlerini ýaýradýarlar, onlarça “elektron poçta gapyrjaklar” arkaly maglumat bilen paýlaşýarlar. Kodlar, parollar, tehniki maglumat, çagyryşlar we ş.m. – hemmesi “poçta gapyrjaklaryň” üstünden geçýär. Hakerleriň tapawutly görnüşi – krekerler (Cracker, iňlis – döwüp açýan ogry). Hakerlerden tapawutlylykda, krekerler maglumaty kompýuter arkaly ogurlanlarynda, bütün informasion maglumat banklaryny alyp çykarýarlar.

Soňky döwürlerde giňişleýin ýaýradysa kompýuter howpunyň täze görnüşi ýüze çykýar – kompýuter wiruslarynyň döredilmegi, olar bolup diňe kesgitlenen signal boýunça işläp başlaýan ýörite işlenip düzülen programmalar çykyş edýär. Şonuň bilen hem, wirus edil kesel dörediji ýaly köpeldilip bilinýär. Şeýle wiruslar bilen programmalaryň “zäherlenmeginiň” netijesi dürli hili ýitgi ýagdaýyna getirip biler.

Häzirki wagtda, kompýuter tehnikasynyň dünýäde has güýçli depginli ösmegi bu tehnologiýalaryň adamyň durmuşynda has köp ornaşandygyny görkezýär.

Emma bu, öz gezeginde adamyň tehnika, esasan hem kompýuter tehnikasyna bagly bolmagyny hem artdyrýar. Bu bolsa tehnika-da ýüze çykýan käbir näsazlyklaryň örän amatsyz ýagdaýlara getirip biljekdiginiň alamaty bolup durýar.

Şol näsazlyklary döretmeklikde we olaryň netijelerini has amatsyz ýagdaýa getirip biljek wiruslar “öňdebaryjy” orunlarda barýar diýsek ýalňyşmarys. Wirus düşünjesiniň dürli kesgitlemesi bar. Olaryň hemmesi dürli derejede dogry, emma biri-birine doly laýyk gelmeýärler. Bu ýerde bir zady bellemek gerek, wirus diýlip, aňsat we bildirmän ýaýraýan hem-de kompýuteriň işini programma-laýyn, käwagt bolsa tehniki taýdan bozýan programmalarla aýdylýar.

Kompýuterleri wiruslardan goramakda antiwirus programmalaryň orny örän uludyr. DrWeb, MCCafy, Kaspersky, Norton Antivirus, Symantec ýaly programmalar bu önümçilikde öňdebaryjy orunlary tutýarlar. Emma bu programmalaryň ygtyýarnamasyz we döwrlüp açylan wersiýalarynyň ýaýramagy, şeýle hem antiwiruslary döretmeklikde käbir kemçilikleriň we ýetmezçilikleriň bolmagy wiruslardan doly howpsuzlygy üpjün etmeklikde belli bir ýetmezçilikleri döredýär.

6.5. Reýestri seljermek arkaly prosesleriň arasyndan we ulgam bukjasyndan wiruslaryň komponentlerini ýok etmek

Geliň indiki bölüme geçmezden, başda wiruslaryň ýaýraýyş düzgünlerine seredip geçeliň. Soňky döwürlerde maglumat göterijileriň görnüşleri artdy. Olaryň köpüsine wiruslaryň geçmegi aňsat bolýar. Meselem, floppy (çeýe) diskleri we flash huşy alsak. Esasan hem soňkyny. Flash huş soňky döwürlerde has elýeterli boldy we köp ulanyjylar bu maglumat göterijini öz işlerinde peýdalanýarlar.

Wiruslaryň soňky görnüşleri hut flash huş gurluşlaryna ýaýramaklygy amala aşyrýarlar. Şu ýerde bir zady bellemek gerek. Köp ýagdaýlarda köp ussatlygy bolmadyk ulanyjylar hem wirus düşmegiň önüni alyp bilýär.

Geliň mysal getireliň. Köplenç wiruslaryň düşmegi ulanyjynyň ýönekeýje ýalňyşy bilen bolup geçýär. Köp halatda wirus goýberijilere basylmazdan wirus ýaýramaýar. Şol sebäpli wirus goýberijiler ulanyjynyň ünsüni çekip biljek görnüşinde ýerine ýetirilýär, meselem, gyzykly oýnuň adyny göterýärler ýa-da näbellilik alamaty (Новая папка, New Folder), adam bolsa näbelliligi öwrenmegi gowy görýär. Şeýle ýagdaýda şol faýllara basylýar we wirus goýberiji işläp başlaýar.

Bellik: Köplenç wirusy goýberiji programma wirusdan aýry bolup, diňe wirusy ýaýratmagy amala aşyryp durýar we özi bilen hiç hili başga howpy getirmeýär we näsazlyklary döretmeýär.

Ýene bir ýagdaýa seredeliň. Flash huşy USB portuna dakylan ýagdaýda kompýuter ony kesgitleýär we awto goýberiş işläp başlaýar, soňra flash huş gurluşyň ady Мой компьютер bölümünde beýleki diskleriň arasynda görkezilýär. Şol ýagdaýda kompýuterde ýa-da flash huşunda **autorun.exe** atly wirus goýberiji bar bolsa hem-de flash huşuň bukjalaryny we faýllaryny görmek üçin onuň adyna syçanjygyň çep düwmejigi bilen iki gezek basylsa onda kompýuterdäki ýa-da flash huşdaky şol wirus goýberiji wirusyň hereketlenmegini ýola goýar we kompýuterdäki wirus flash huşa geçýär we tersine. Şu ýerde bir zady belläp geçeliň, köp halatda wirus goýberiji

we virus programmasy bir faýl bolup durmaýar. Şu ýagdaýda wirusy kesgitlemek, eýsem ony ýok etmek has çylşyrymly bolup durýar.

Wirus dörediji tarapyndan wirusy goýberiji programma taýýarlana-da – şeýle pikir gelmeli – ol görünýän, elýeterli we kiçi bolmaly, şeýle hem ulanyjynyň ünsüni çekip biljek ada eýe bolmaly hem-de degişli nyşana eýe bolmaly.

Şonuň üçin, nätanyş oýunlara, eýsem nätanyş faýllara basmaly däl-dir, flash huşy açylanda syçanjygyň çep düwmejigi bilen iki däl-de bir gezek basyp, soňra onuň çep düwmejigi arkaly kontekst menýusyny çagyryp Open ýa-da **Открыть** bendini saýlap açmak gerek.

Wirus dörediji virus goýberiji programmasyna ýene bir wezipäni ýükleýär – oňa basylandan soň ol Windowsyň reýestrine ýazgy ýazýar. Ol ýazgy reýestriň awtoýükleniş bölümlerine – HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE we HKEY_USERS kök bölümleriniň SOFTWARE \Microsoft \Windows \CurrentVersion \Run ýolunda ýazylyp galýar. Ol ýazgynyň maksady – Windowsyň proseslerine rezident (görünmeýän we bildirmeýän) programmany ýüklemeklik. Ol programma – wirusy goldawçy programma diýlip atlandyrylýar.

Bellik. Wirusy goldawçy programma hem virus programmasyndan köplenç aýry edilip hiç hili bozuýy işleri bitirmeýär. Onuň esasy wezipesi – virus programmasy ýüze çykarylanda we ony ýok etjek bolanda päsgelçilik bermeklik. Meselem, virus ýok ediljek bolanda, ulgam habar beriş penjiresini açyp şeýle habar berýär: “Не могу удалить приложение, оно занято другим процессом или пользователем” – programmany ýok edip bilemok, ol başga proses ýa-da ulanyjy tarapyndan ulanylýar, ýa-da şuna meňzeş habarlaryň başgalaryny bermegi hem mümkin.

Windows ýüklenenden soň, beýleki awto ýüklenýän programalaryň arasynda ýüklenip, wirusy goldawçy programma virus programmanyň alyp barýan hereketlerini goldaýar. Wirus dörediji wirusy goldawçy programmany döredende wirusyň we wirusy goýberijiniň ýagdaýyny elmydama gözegçilikde saklamak wezipesini oňa berkidýär. Wirusy goldaýjy programmasy amallar ulgamyň

prosesleriniň arasynda iş ýagdaýda bolup, wirusy goýberijiniň we wirusyň ýerleşýän ýerine wagtal-wagtal salgylanýar we wirus goýberiji programma ýok edilende, ol ony gaýtadan döredýär, wirus ýok ediljek bolsa, ol ýok etmäge ýol bermeýär we bu barada dürli habarlary berýär. Hemme bu amallar wirus döredijiniň “ussatlykly” iş başaryandygynyň netijesi bolup durýar.

Windowsyň reýestriniň awtoýükleniş bölümleri arkaly çagyrylyp wirusy goldaýjy maksatnama elmydama Windows amallar ulgamy işlän mahaly, iş ýagdaýynda bolup durýar.

Ýokarda agzalanlar jemlenende aşakdaky netijelere gelmek bolýar:

Bozuýjy işleri amala aşyrmak üçin wirus dörediji tarapyndan üç programma ýazylmagy mümkin:

- wirusy goýberiji
- wirusy goldaýjy
- wirus

Bular aýry hem bolsalar, bitewilikde işleri alyp barýarlar we öz wagtynda dogry tertipde ýok edilmeseler gaty kän erbetçilikleri ýerine ýetirip bilerler. Käwagt üç programmanyň işini biri ýerine ýetirýär, bu ýagdaýda ony kesgitlemeklik birneme aňsat bolýar.

Geliň indi ýokarda görkezilen wirus toplumyny ýok etmegiň dogry tertibi barada gürrüň edeliň. Windows amallar ulgamynda birnäçe prosesler işleýär. Olaryň her biri bir wezipäni ýerine ýetirýär. Wagtal-wagtal meseleleriň dispetcherini açyp (Ctrl+Alt+Del), prosesleriň düzümine gözegçilik etmeli. Esasan hem öz ulanyjyňyzyň adyndan goýberilenlere. Henize çenli, wirus döredijileriň ussatlyklarynyň belli bir derejede örän ýokary daldigi sebäpli, wiruslar Windowsyň spesifikasi ulanyjylaryň (System, Local Service, Network Service) adyndan goýberilip bilinmeýär. Eger bir üýtgeşik prosesi kesgitleseňiz, haýal etmän windowsyň reýestrine girip, eýýäm belli bolan awto ýükleýji bölümleriň parametrlerinden onuň adyny tapmaly, we onuň nireden goýberilýändigini parametriň bahasyndan görüp (6.4-nji surat), onuň gaty diskiň huşunda ýerleşýän ýerine barmaly. Eger prosesi goýberýän faýl şübheli ýa-da ön kesgitlän wirusyň häsiýetnamalaryna eýe bolsa aşakdaky ädimleri ýerine ýetirmeli:

– ilki başda rezidentlik işini alyp barýan wirus goldaýjy programma ýok edilmeli. Sebäbi, ol beýleki iki maksatnamanyň ýok edilmegine päsgel berer.

– wirus goldaýjy ýok edilen soň, wirus goýberiji programmalar ýok edilýär.

– soňra Windowsyň reýestriniň awtoýükleýji bölümlerine girmek, wirusy goldaýjy programmany çagyryjy parametrler ýok edilmeli.

– şol ýerden wirusyň ýerleşýän ýeri görüp wirus ýok edilýär.

Bu ädimler 100%-den 95% ýagdaýlarda kömek edýär we wiruslaryň aýrylmagy doly möçberde bolup geçýär.

Şu düzgüne köp wiruslaryň ýok edilmegi degişli. Wiruslaryň ýaýramagy köp derejede meňzeş usulda amala aşyrylýan bolsa hem, bozujylyk işi babatda bolsa her wirus öz maksatlaryny yzarlaýar, olar dürli bolup biler. Indiki bölüm anyk wiruslara, olaryň bitirýän işlerine we olary ýok etmegiň ädimlerine degişli.

Görşümüz ýaly, reýestr bozujy programmalar arkaly peýdalanylýan hem bolsa, ol arkaly bozujy programmalary yzarlap we ýok edip bolýar.

Geliň şu ýerde reýestri programmirlemek meselesine seredeliň. Reýestr bu operasion ulgamyň açyk kodydyr. Şol sebäpli ol belli bir derejede programmirleme dillerine elýeterli. Reýestri programmirlemegiň dürli maksatlary bar – ýagny onuň içinde ulgam barada dürli takyk maglumatlar bar hem-de şol maglumatlary ulanyjylara görkezmek programmalary döretmek bolýar (Tweaker).

Ýokardakylary amala aşyrmak üçin programmirleme dilinde reýestre elýeterligi almak gerek. Seljeriş üçin işimizde obýekte gönükdirilen programmirleme dilleriň biri bolan Borland Delphi dilini peýdalanarys.

Delphi dilinde ilki bilen ulanjak bolýan Formanyň kod sahypasynda modullaryň bölümünde (**uses**) **Registry** sözi ýazmaly. Şeýlelik bilen, reýestri degişli Formada ulanmaga mümkinçilik alynýar.

Soňra reýestriň ululygy lokal ýa-da global üýtgeýänleriň bölümünde girizilýär:

Var

reg:TRegistry;

Şeýlelik bilen, **reg** ululygy geljekde reýestr bilen dürli amallary amala aşyrmak üçin kesgitlenilýär.

Programma kodunda reýestr ululygyny reýestriň içine girmek üçin aşakdaky amallardan geçirmeli (ýagny reýestre girişi döretmek, esasy açarlaryň birini saýlamak, köp nokatly ýerde zerur bolan amallar görkezilýär, soňra bolsa degişli açarlary ýapmak bilen reýestri boşatmaly):

Reg := nil;

try

reg := TRegistry.Create;

reg.RootKey := HKEY_CURRENT_USER;

reg.LazyWrite := false;

.....

reg.CloseKey;

except

if Assigned(Reg) **then** Reg.Free;

end;

Reýestriň açarlaryny okamak we olara ýazmak üçin aşakdakylary beýan etmeli (reýestrde setir we san görnüşinde maglumatlar bilen işleşmek üçin degişli ululyklary girizmeli, köp nokatly ýerde ýokarda görkezilen reýestre giriş amallary görkezilmeli, **OpenKey** funksiýasy esasy açaryň içindäki görkezilen ýol boýunça açara girmekligi amala aşyrýar – açar ýoly apostroflaryň içine salynmalydyr, **ReadString** we **ReadInteger** funksiýalary görkezilen açaryň içinde degişli setir we san parametrlerden okamagy we degişli ululyklara şol alnan bahalary dakmagy amala aşyrýar):

Var

s:string;

a:integer;

.....

Reg.**OpenKey**(Açaryň ýoly, false);

meselem, Açaryň ýoly = ,SOFTWARE\Microsoft‘

```
s:=Reg.ReadString(setir Parametr);  
a:=Reg.ReadInteger(san Parametr);  
Reg.WriteString(setir Parametr, s);  
Reg.Writeinteger(san Parametr,a);
```

Şeýle hem, käbir açarlary ýok etmeklik zerur bolmagy mümkin, munuň üçin aşakdaky amallary ýerine ýetirmek gerek (**ValueExists** funksiýasy ýaýyň içinde parametriň, **KeyExists** funksiýasy bolsa açaryň bardygyny kesgitleýär, **DeleteValue** we **DeleteKey** degişlilikde görkezilen parametri we açary ýok etmegi amala aşyrýar):
If reg.**ValueExists**(parametr)=true **then** reg.**DeleteValue**(parametr);
If reg.**KeyExists**(açar)=true **then** reg.**DeleteKey**(açar);
meselem,
if reg.**ValueExists**('DisallowRun')=true **then** reg.**DeleteValue** ('DisallowRun');
if reg.**KeyExists**('DisallowRun')=true **then** reg.**DeleteKey** ('DisallowRun');

Reýestri programmirlmegiň ýokarda görkezilen esasy funksiýalary peýdalanmak bilen operasion ulgamyň işini dürli ugurlarda sazlamak we düzetmek mümkin. Munuň üçin diňe reýestriň açarlarynyň işini bilmek zerur.

Şeýlelik bilen, operasion sistemanyň reýestri umuman sistemada uly rol oýnaýandygyna göz ýetirildi. Reýestriň giň mümkinçiliklerini seljermek arkaly onuň maglumat goragynyň dürli usullarynda – programmalaryň goýberilmegini çäklendirmekde, parol goragynda we başg. ulanylmagyna mümkinçilik berýär. Reýestriň gorag halkasy hökmünde çykyş etmegi şol goragy ýokary derejeli edýär.

Şeýle hem, diňe peýdaly programmalar arkaly peýdalanman, reýestr virus hüjüminiň hem halkasy hökmünde çykyş etmegi mümkin. Onuň awtoýükleniş bölümleri virus hüjümini başlamak we dowam etdirmek üçin ulanylýar. Emma şeýle bolsa hem, ters amallary amala aşyrmak – reýestri barlamak, tapylan açarlary ulanyp virus prosesleri we virus faýllary ýok etmek arkaly virus hüjümini saklamak mümkin. Bu barada indiki bölümde has giňişleýin gürrüň edilär.

Tejribe işleri

1. Microsoft Office toplumynyň programmalaryny awtomatiki ýüklenýaly etmeli.
 2. Programmirleme dili arkaly reýestriň bölümini döretmeli.
 3. Programmirleme dili arkaly reýestriň açaryny döretmeli.
 4. Programmirleme dili arkaly reýestriň bölümini ýok etmeli.
 5. Programmirleme dili arkaly reýestriň açaryny ýok etmeli.
 6. Programmirleme dili arkaly operasion sistemanyň parametrlerini kesgitlemek.
 7. Programmirleme dili arkaly kompýuteriň parametrlerini kesgitlemek.
-

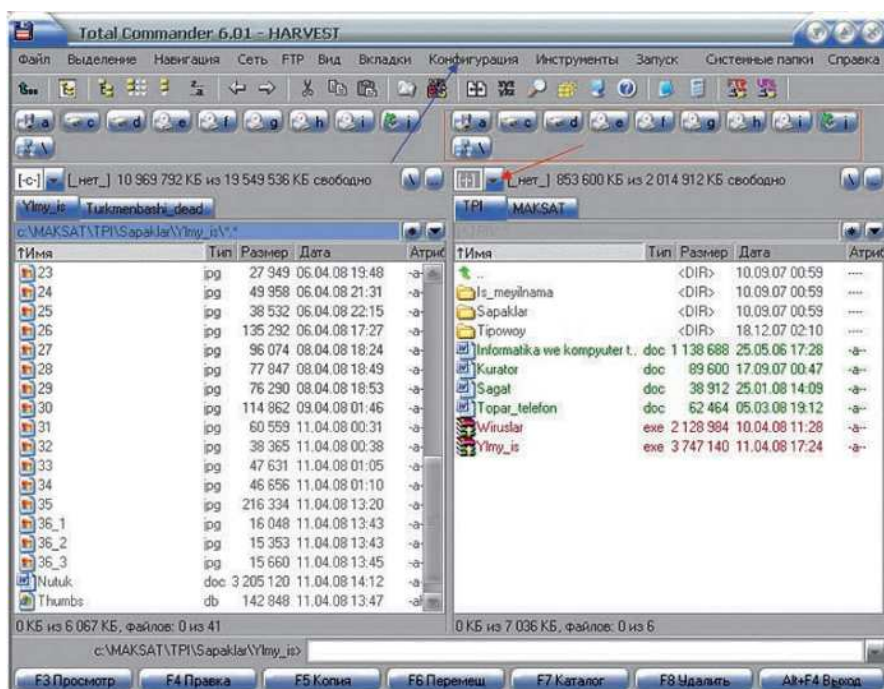
VII. WIRUSLARA WE TROÝANLARA GARŞY GÖREŞ

1. Total Commander faýl menejeriň işi;
2. Dürli wiruslaryň işini seljermek we olary aýyrmak boýunça programma gözükdirmeleri döretmek;
3. Antitroýan.exe türkmen antiwirus programmasynyň döredilmegi.

7.1. Total Commander faýl menejeriň işi

Bu bölümde köp işleri Total Commander arkaly ýerine ýetirmeli bolar. Ilkibaşda ol barada birneme teswirleme bereliň.

Suratdan görşüňiz ýaly, faýl menejer iki bölege bölünen, iki tarapda hem diskleriň düzümi (bukjalary we faýllary) görkezilen. Dis-

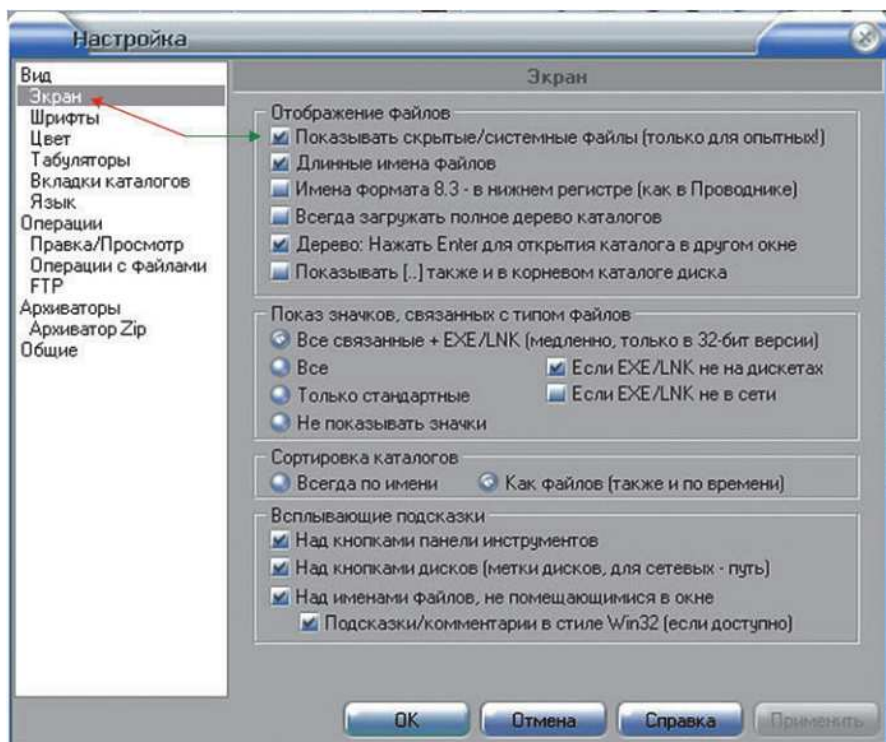


7.1-nji surat

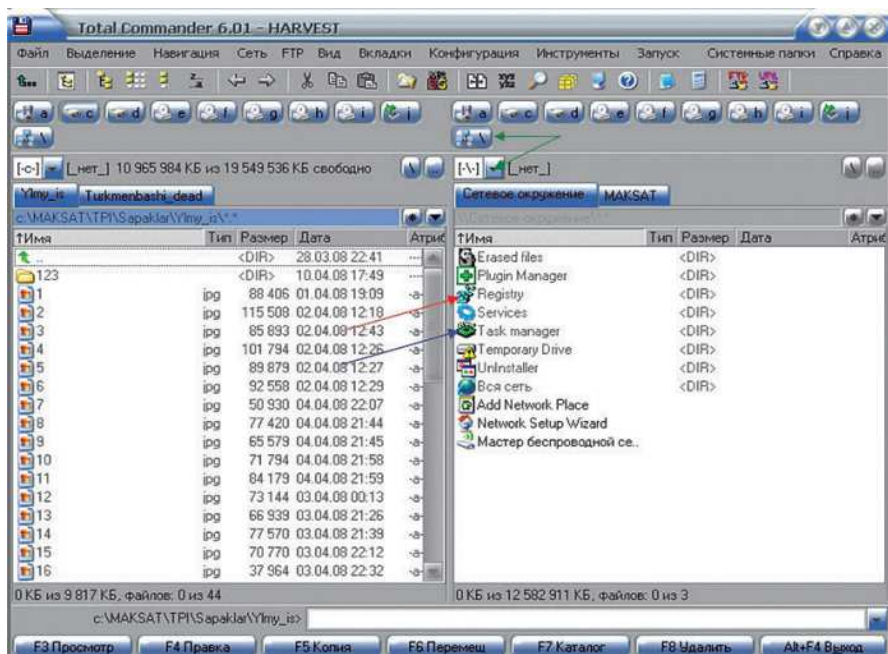
kleri saýlamak üçin suratda gyzyk ok bilen görkezilen sanawy görkezýän gök düwmejigi arkaly ýa-da gyzyk gönüburçlugyň içine alnan düwmejikler arkaly saýlamak mümkin (adatça diskleriň atlary – [-a-], [-b-] we ş.m. bilen belgilenen).

Bu faýl menejeriň amatly tarapy “Проводник” ulgamyň ähli kontekst menýusyny ulanmagy mümkin edýär. Meselem, islendik faýly ýa-da bukjany belläp, oňa syçanjyk bilen bir gezek basyp, soňra sag düwmejige basylsa adaty faýlyň ýa-da bukjanyň kontekst menýusy ýüze çykar.

Ýene-de bir amatlylyk – faýllaryň bir diskden beýlekä, penjireleri açman geçirilme mümkinçiligi (bir bölekde belläp F5 klawişasyna basyp beýleki bölege ibermeklik). Faýllary we bukjalary ýok etmeklik F8 düwmejigi arkaly amala aşyrylýar, emma munuň üçin Delete klawişasyny hem ulanmak mümkinçiligi bar. Bu ýagdaýda ýok edilen



7.2-nji surat



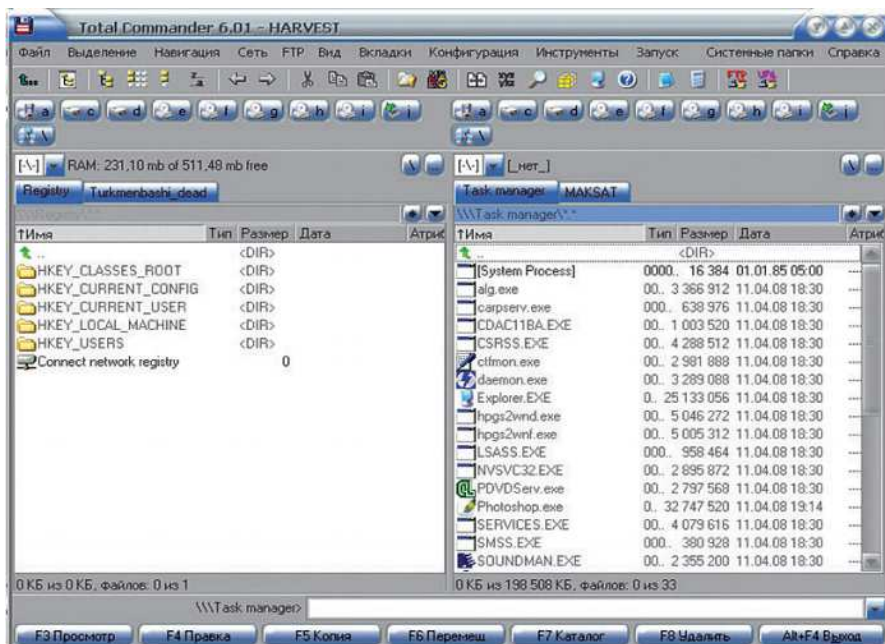
7.3-nji surat

bukja ýa-da faýl “Корзина” ýok edilýär. Eger Shift klawişasyna basylyp Delete klawişasyna basylsa (Shift+Del), onda faýl “Корзина” iberilmän göni huşdan ýok edilýär.

Total Commander faýl menejerinde islendik atributy bolan (buklan, ulgamlayýn) faýly ýa-da bukjany görmek mümkinçiligini dolandyrmak mümkin. Munuň üçin menejeriň iň ýokarsynda ýerleşen menýu setirinde “Конфигурация” atly menýu girmeli (gök ok bilen görkezilen). Bu ýerde “Настройка” bendi saýlamaly. Netijede, aşaky penjire açylar.

Penjirede “Экран” atly goşmaçany saýlaýarys (gyzyl ok bilen görkezilen). Onuň panelinde iň ýokarky ýaşyl ok bilen görkezilen bendiň gapdalyndaky ak inedördüljigine belgini goýýarys. Şeýlelik bilen, islendik faýl ýa-da bukja ekranda görner.

Bu faýl menejeriň iň peýdaly mümkinçiligi bolup gönümel reýestre we meseleler dispetçerine çykmaklykdyr.



7.4-nji surat

Munuň üçin diskleriň sanawyny görkeziji gök düwmejige ýa-da üç birleşen kompýuteriň şekilini we “\” belgini saklaýan düwmejige basmaly (ikisi hem ýaşyl ok bilen görkezilen).

Netijede, 7.3-nji suratyň sag bölegindäki elementleri peýda bolar. Bu ýerde reýestre girmek üçin gyzyk ok bilen görkezilen Registry elemente, Meseleler dispetçerine girmek üçin bolsa gök ok bilen görkezilen Task manager elemente basmaly. Geliň faýl menejeriň çep böleginde Registry elementine, sag böleginde bolsa Task manager elementine basalyň.

Netijede, 7.4-nji suratdaky penjire açylar. Görşüňiz ýaly, çep bölekde adaty reýestriň bölümleri, sag bölekde bolsa prosesleriň sanawy ýerleşdirilen. Bu düzgünde bölümleri ýok etmek üçin F8, Delete ýa-da Shift+Delete klawişalaryny ulanmak bolýar.

7.2 Dürli wiruslaryň işini seljermek we olary aýyrmak boýunça programma gözökdirmeleri döretmek

Windows amallar ulgamy giňden ýaýrandygy sebäpli, onuň kadaly işini bozmak boýunça münlerçe wiruslar we beýleki bozujy programmalar ýazylandyr. Antiwirus programmalary köp derejede olardan goranmagy amala aşyrýarlar, emma olar wirus girmezden öň öňüni alyş işleri netijeli geçirmegi başaryp, wirus düşen ýagdaýynda köp halatlarda güýcsüz hem bolup bilýärler. Bu bölümde öz döwründe hiç bir antiwirus programmasy tarapyndan doly aýrylyp bilmän, eldeki usul bilen aýrylan bozujy programmalaryň sanawy getirilen.

Game.exe

Alyp barýan işi – her ýarym minutdan çeyde diskiň gurluşyna ýüzlenýär we içinde disketa bar bolan ýagdaýynda, oňa 300 Kb deň bolan Game.exe atly faýly ýükleýär. Diskowod boş bolsa hem, yzygiderli oňa ýüzlenmegi dowam etdirýär, şeýle edip ony zaýalaýar. Disketa ýazylan Game.exe faýly bolsa öz gezeginde wirus goýberiji bolup galýar. Oňa iki gezek syçanjyk ýa-da bir gezek Enter bilen basylsa wirus goýberilýär.

Köp antiwiruslar bu wirusy anyklap bilmediler. Wirusy ýok etmek üçin Ctrl-Alt-Del düwmejigiň yzygiderligini bir wagtda basyň, netijede meseleler Dispetçeriň (Диспетчер задач) penjiresi açylar. Penjiräniň ýokary böleginde 5 sany goşmaça bar (Windowsyň wersiýasyna görä az bolmagy mümkin) Bu ýerde prosesleriň goşmaçasyny (Процессы) basyp açyň. Ekranda işläp duran prosesleriň sanawy açylar. Prosesleriň arasynda iki sany **explorer.exe** atly proses bardyr. Şularyň biri hakyky Windowsyň öz ýüklendirijisi beýlekisi bolsa wirus goldawçysy. Köplenç olaryň haýsy biridigini tanap bolmaýar. Biri diňe uly harplar, beýlekisi diňe kiçi, ýa-da birinji harpy uly harp bilen ýazylan bolup durýar. Olary kesgitlemek üçin olaryň operatiw huşda tutýan göwrümüne seretmeli. Ýalan **explorer.exe** prosesi kiçi bolmaly.

Emma bu ýagdaýda diňe wirus goldawçysyny aýyrдыgymyz bolýar. Sebäbi Windows indiki gezek ýüklenende ikinji explorer atly wirus prosesi gaýtadan ýüklenir. Munuň öňüni almak üçin reýestri

goýberýäris. Reýestriň düzüminde HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run bu k j a ýoly bilen bukjalary açyşdyryp iň soňky Run atly bukjada Explorer.exe goýbermek baradaky setiri ýok etmeli. Explorer.exe hiç haçan Run arkaly awto ýüklenmegi amala aşyрмаýar ol Windowsyň başga ýoly arkaly ýüklenýär.

Bu ýagdaýda, wirus doly ýok edildi diýip bolýar.

Explorer.exe

Bu wirus programmasy başga bir zerur prosesiniň adyny göterip, öz hereketlerini bildirmezlik bilen işlemegi amala aşyrýar. Dogrudan hem onuň bitirýän işini daşky alamatlardan bilmek, eýsem bozuýy hereketleri kesgitlemek örän çylşyrymly bolup durýar. Emma hemme zat açylýan pikir bilen, ýerine ýetirilýär. Biz hem bu bozuýy programmany ýüze çykaralyň.

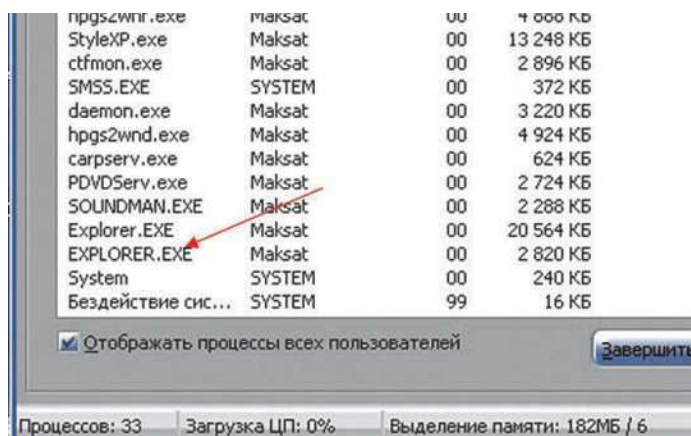
Hemme hereketler hakyky wagtda wirusy goýbermek we ony ädimleýin ýok etmekligi görkezmek bilen amala aşyrylýar.

Explorer.exe faýlyň özi bukulanylýan, ulgamlayýn we diňe okamak atributlaryna eýe. Bu atributlar ony ulanyjynyň gözünden ýaşyrmagy, tapylyan ýagdaýyndan hem ýok etmeklige päsgel bermek we antiwirus programmalar bilen gizlenmäge mümkinçilik berýär.

Bu faýl ulanyjynyň özi oňa basmasa hereket etmeýär. Geliň oňa syçanjygyň düwmeji bilen iki gezek basalyň we Windows amallary ulgamyny gaýtadan ýüklenişe goýbereliň.

Windows amallary ulgamynyň ýüklenmegi öňkünden birneme haýallaýar we ol ýüklenenden soň “Мои документы” atly penjire öz-özünden açylýar. Lokal diskleri barlap görýäris. Görünýän başga üýtgeşikler bildirmeýär.

Onda prosesleri barlap göreliň munuň üçin Meseleler dispetcherini çagyralyň (Ctrl+Alt+Del) we onuň “Процессы” atly goşmaçasyna gireliň. Bu ýerde bolsa käbir üýtgemeler bize garaşýandyr. Ýagny prosesleriň sanawynda explorer adyny göterýän iki sany proses bardyr (7.5-nji surat). Olaryň biri hakyky gerekli proses, beýlekisi bolsa ýalan gerekmez (gyzyl ok bilen görkezilen – ýalan prosesi). Şol sebäpli haýal etmän şol prosesi degişli usul bilen ýok etmeli.



7.5-nji surat

Soňra Windowsyň reýestrine adaty usul bilen girip, HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run yzygiderlige geçmeli we Run bölümiň üstüne basmaly. Bu ýerde awtoýükleniş programmalaryň düzümine täze iki sanysy goşulan. Şol prosesleriň ikisi hem şübheli. Öňki bölümlerde belleýşimiz ýaly Explorer prosesi hiç haçan reýestriň bu bölümlerinden ýüklenmeýär. Şol sebäpli bu ýazgyny ýok etmeli. Ikinji ýazgy – wscft.exe ol hem ýok edilmeli prosesi ýükleýiş ýazgysynyň biri.

Bu prosesleri goýbermeli faýllara bolan ýol iki ýazgydada anyk görkezilmändir (ikisinde hem olaryň diňe atlary görkezilen). Bu ýagdaýda “Пуск-Найти- Файлы и папки” bendini saýlap, gözlegiň penjiresini çagyrmaly. Bu ýerde hem Файлы и папки bendi gaýtadan saýlamaly. Penjiräniň çep böleginde açylan paneliň ýokarky setirinde şol faýllaryň atlaryny (explorer.exe ýa-da wscft.exe) ýazmaly.

| Имя | Тип | Значение |
|-------------------|--------|--|
| ab (По умолчанию) | REG_SZ | (значение не присвоено) |
| ab CTFMON.EXE | REG_SZ | D:\WINDOWS\system32\ctfmon.exe |
| ab EXPLORER.EXE | REG_SZ | EXPLORER.EXE |
| ab STYLEXP | REG_SZ | D:\Program Files\TGTSoft\StyleXP\StyleXP.exe -Hide |
| ab wscft.exe | REG_SZ | wscft.exe |

7.6-njy surat

Gözlegiň netijesinde **explorer.exe** atly diňe bir faýl tapylar. Ol hem Windows bukjasynda ýerleşen dogry faýl, ikinjiniň ady bilen hiç hili faýl tapylmaýar.

Diýmek, bu prosesler, hakyky exploreriň resurslaryny ulanyp goýberilýär. Indi Windowsy gaýtadan ýükläliň we ol ýüklenenden soň “Мои документы” atly penjire öz-özünden ýene açylýar. Eger Windows amallar ulgamy birnäçe gezek ýüklenip barlanylsa, şol penjire ýüze çykanda käbir kemçiliklerini ýüze çykarmagynyň mümkindigine göz ýetirmek bolýar. Meselem, käwagt şol penjiräni ýapjak bolsak, ol jogap bermän bilýär we bu ýagdaýda ony meseleler dispetçerini çagyryp ýok etmeli bolýar.

“Мои документы” penjiräniň açylyp durmagy wirusyň heniz doly aýrylmandygynyň alamaty bolup durýar. Muny barlamak üçin meseleler dispetçerine girmeli. Meseleler dispetçerine girilenden soň prosesleriň arasynda ikinji **explorer.exe** prosesiň ýokdugyna göz ýetirmeli. Bu nähili ýagdaýka (bozuý proses ýok welin?)

Emma munuň öz düşündirilişi bar. Reýestre girip HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon yzygiderliligine gireliň we Winlogon bölümüne geçmeli.

Suratda iki ýazga ünsi çekmek zerur (7.7-nji surat – gyzykly oklar bilen bellenen). Indi virus goýberilmezden öňki şu bölümüň parametrlerini görmeli (7.4-nji surat).

7.8-nji suratdan görnüşi ýaly, virus goýberilenden soň, Shell diýip parametr bölüme goşulýar we Userinit parametriň bahasy bir-

| | | |
|----------------------|---------|---|
| SFCDisable | REG_... | 0x00000000 (0) |
| SfcQuota | REG_... | 0xffffffff (4294967295) |
| Shell | REG_SZ | Explorer.exe |
| ShowLogonOptions | REG_... | 0x00000000 (0) |
| ShutdownWithoutLogon | REG_SZ | 0 |
| System | REG_SZ | |
| UIHost | REG_SZ | D:\Program Files\TGTSoft\StyleXP\CurrentLogon.EXE |
| Userinit | REG_SZ | userinit.exe,EXPLORER.EXE |
| VmApplet | REG_SZ | rundll32 shell32,Control_RunDLL "sysdm.cpl" |
| WinStationsDisabled | REG_SZ | 0 |

7.7-nji surat

| | | |
|----------------------|---------|---|
| SFCDisable | REG_... | 0x00000000 (0) |
| SfcQuota | REG_... | 0xffffffff (4294967295) |
| ShowLogonOptions | REG_... | 0x00000000 (0) |
| ShutdownWithoutLogon | REG_SZ | 0 |
| System | REG_SZ | |
| UIHost | REG_SZ | D:\Program Files\TGTSoft\StyleXP\CurrentLogon.EXE |
| Userinit | REG_SZ | D:\Windows\System32\userinit.exe |
| VmApplet | REG_SZ | rundll32 shell32,Control_RunDLL "sysdm.cpl" |
| WinStationsDisabled | REG_SZ | 0 |

7.8-nji surat

neme üýtgeýär (7.7-nji sur. ser.). Geliň şol parametrleri öňki bolşuna getireliň (Shell ýok edilýär, Userinit bolsa degişli redaktirlenýär).

Windows amallar ulgamy gaýtadan ýüklenenden soň, hemme zat adaty bolup, başga hiç penjireler ýüze çykmaýar we iş meýdanyň özi ekranda peýda bolýar. Wirus, atlary dünýä belli bolan DrWeb, MCCafy, Kaspersky, Norton Antivirus, Symantec antiwirus programmalary tarapyndan aýrylanda, “Мои документы” atly penjire çykmagyny dowam edýär hem-de bu usulyň şeýle ýagdaýda artykmaçlygyny görkezýär.

Bu ýerde ýene bir amaly ýerine ýetirmegi ýatdan çykarmaly däl. D:\Windows\System32 bukjasyndan Explorer.exe faýlyny ýok etmeli. Ol eýýäm howply däl hem bolsa, reýestrde ony işletmek barada degişli ýazgy bolsa, birneme ýaramaz amallary ýerine ýetirmegi mümkin.

ntdetect.com

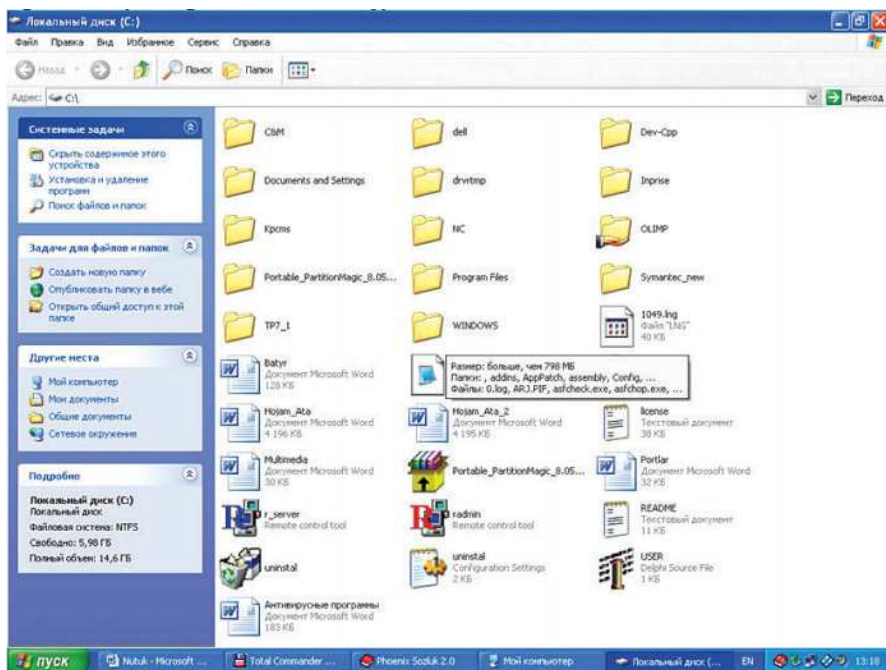
Geliň indi, awtoýükleniş faýllary döredip işleýän bozujy programmalaryň işine seredeliň. Olaryň arasynda aýratyn ony **ntdetect.com** programmasy tutýar. Bu programma özi bilen dolandyryjy lokal diskde (Windows amallar ulgamy gurnalan diskde) ýerleşýän hakyky Ntdetect.com programmasyna meňzetme bolup ulanyjynyň ýa-da ulgam administratoryň ünsüni çekmezlik üçin atlandyrylan. Ol özi bukulan, ulgamlayyn we diňe okamak atributlara eýe hem-de ulgamlayyn faýlyň nyşanyny göterýär.

Ol goýberilen mahaly, ekranda hiç hili daşky alamatlar görünmeýär. Windows amallar ulgamy gaýtadan ýüklenişe goýberilýär we

ol ýüklenenden soň ekrana tor baglanyşygy barada habar berilýär. Bu özi bilen eýýäm bir üýtgeşme bolandygynyň alamaty bolup durýar.

Indi, lokal disklerdäki faýllaryň sanawyny barlamaly. Sebäbi bu programma olaryň her birinde iki faýl – **autorun.inf** we **ntdelect.com** faýllary döredýär. Şeýle hem kompýutere flash huşy çatylanda ol awtoýüklenende oňa bu iki faýllardan başga RECYCLER bukjasy emele geler. Lokal disklerde bu faýllar ýok edilse hem, olar her gezek emele gelip durar. Flash huşunda bolsa şol faýllar we RECYCLER bukjasy ýok edilen ýagdaýda bir wagt olar emele gelmeýär, emma flash huşy öçürilip, gaýtadan çatylsa we onuň awtoýüklenişi bolup geçse olar awtomatiki ýene flash huşa ýazylar.

Şu ýerde ünsi bir zada çekmeli. Bu virus örän mekirlik bilen hereket edýär. Ýokarda faýllaryň döremegini, eger “Мой компьютер” hödürleýän bukja düzümi arkaly ýa-da “Проводник” ulgamy arkaly görmeklige synanyssak ýokarda ady agzalan faýllaryň hiç biri hem görünmez (7.9-njy surat).



7.9-njy surat

7.10-njy surat.

Ussatly ulanyjylar bilýändir, suratdaky penjiräniň ýokarky menýu setirinden “Сервис” menýuny saýlap onuň „Свойства папки“ bendine basylyp açylan „Вид” penjirede „Показывать скрытые и системные файлы“ parametri işledilse, hemme bukulan we ulgamlaryň bukjalary we faýllar görkeziler. Emma bozuýy programma „Свойства папки“ bendini ýok edýär we gerek bolan faýllary görüp bolmaýar.

Bu ýerde Total Commander programmasyny ulanmak gerek. Ol hemme atributly faýllary görmekligi amala aşyrmagy mümkin edýär.

Aşakda şol **Autorun.inf**, **ntdelect.com** faýllaryň we RECYCLER bukjasyň Total Commander programmasynyň penjiresindäki daşky görnüşleri görkezilen.

Indi beýleki wiruslara we bozuýy programmalara seredilende, deslapdan Total Commanderiň penjiresi ulanylýandygyny göz önünde tutmak gerek.

Faýllaryň ýok edilmeginden soň, olaryň gaýtadan döreme ýagdaýy seljerilse, amallar ulgamyň proseslerinde bir prosesniň goýberilip şol faýllaryň ýagdaýyny yzarlaýandygy aýdyň bolup durýar. Şol proses wirusy goldaýjy programma bolup durýar. Şeýlelik bilen, **autorun.inf** we **ntdelect.com** programmalary – wirusy goýberiji programmasy bolup durýar.

Autorun.inf faýly mundan başga hem başga wezipeleri ýerine ýetirýär. Bu bozuýy programmalar bilen “ýokuşan” kompýuter birnäçe gezek gaýtadan ýüklenenden (öçürilip işlenenden) soň, meselem ýene üç günden soň, Iş meýdanyndan “**Мой компьютер**” nyşanyna basyp lokal disklere (meselem, C we D disklere) ýa-da flash gurluşa syçanjyk bilen iki gezek basyp giriljek bolanda, onda adaty olaryň bukjalaryna girilmezde, başga penjireler açylar (7.11-nji surat) ýa-da hiç hili täsir bolmaz.

Bu ýagdaýda gerek bolan lokal diski ýa-da flash gurluşy syçanjygyň çep düwmejigi bilen bir gezek basyp belläp, soňra onuň sag düwmejigini basyp kontekst menýuny çagyryp, ol ýerden “Открыть” buýrugy saýlap basmaly. Bu ýagdaýda şol diskiň buk-



7.11-nji surat

jalar düzüminiň penjiresi açylmagy mümkin. Eger bu hem kömek etmese, onda diňe bir mesele galýar – Autorun.inf faýly ýok etmek. Emma ol, ýok edilenden soň, ýene emele gelmez ýaly – ilkibaşda virus goldaýjy programmany prosesleriň arasyndan kesgitläp ýok etmek gerek.

Indi bolsa aşakdaky tertipde bozuýjy programmany ýok etmegiň ädimlerini aşakdaky tertipde beýan edeliň.


I. İlkibaşda meseleler dispetcherine girip, prosesleriň arasynda McaUpdate.exe prosesi ýok etmeli. Indi bir tarapdan, virus goldaýjy ýok edilen ýaly. Emma virus goýberiji programmalar lokal disklerden ýok edilýän hem bolsa, olar ýene emele gelip durýandyr. Diýmek, ýene bir proses bar. Prosesleriň sanawyna seredip görülse, başga bir şübheli proses ýok ýalydyr. Bu ýagdaýda ýeke-ýekeden ulanyjyňyzyň adyndan goýberilen prosesleri ýok edip, soňra virus goýberiji programmalary disklerden ýok edip, olaryň gaýtadan eme-

le gelyändigini ýa-da gelmeýändigini barlamak mümkin. Emma köp wagt ýitirmän, bu tejribäniň öň ýerine ýetirilib, şol prosesniň anyklanandygyny aýtmak bolar. Ol – explorer.exe. Bu ýerde prosesleriň sanawynda şol atly diňe bir proses bar, ol hem hakykatdaky proses, ýogsam iş meýdanyň elementleri ekranda görünmezdi, ol nähili wirus goldaýjy bolup bilýär diýen soragyň ýüze çykmagy mümkin.

Muňa jogap hökmünde şulary aýtmak bolar: esasy wirus goldawjy proses **McaUpdate.exe**, ol wagtlaýyn beýleki prosese – explorer.exe prosesine öz işini „tabşyrýar” we özi ýok edilse hem, **explorer.exe** prosesi onuň işini dowam edýär. Eger **explorer.exe** prosesi ýok edilip, gaýtadan ýüklenilse, ulgam kadaly işläp başlar we wirus goýberiji programmalar ýok edilenden soň, gaýtadan emele gelmez.

II. Wirus goldaýjy we wirus goýberiji programmalar ýok edilen-den soň, indi diňe reýestriň ýazgysynda olar baradaky maglumatlary ýok edip wirus programmasynyň ýoluny kesgitläp ony ýok etmek galdy.

Ilkibaşda reýestre girip, HKEY_CURRENT_USER\Software\Microsoft\ Windows\ CurrentVersion\Run yzygiderlige girip Run bölümiň üstüne basmaly.

| | | |
|--|--------|--|
|  (По умолчанию) | REG_SZ | (значение не присвоено) |
|  авпа | REG_SZ | D:\WINDOWS\system32\avpa.exe |
|  CTFMON.EXE | REG_SZ | D:\WINDOWS\system32\ctfmon.exe |
|  STYLEXP | REG_SZ | D:\Program Files\TGTSoft\StyleXP\StyleXP.exe -Hide |

7.12-nji surat

Eger, reýestriň awtoýükleýji bölümleriniň parametrleri hemişelik gözegçilikde saklanylsa, onda şübheli parametri kesgitlemeklik kyn bolmaz. Ol gyzyk bilen görkezilen avpa atly parametr. Onuň bahasynda ýüklenýän wirusa eltýän ýol we wirus faýlynyň ady görkezilen. Ntdelect.com faýly goýbermezden öň reýestrde bu parametr ýokdy. Ony ýok etmeli.

Indi, reýestrde hemme işler ýerine ýetirilen hem ýaly. Öň ýerine ýetirilen tejribeden belli edildi, ýene bir ýazgy bar, ol HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersi-

on\policies\Explorer\Run yzygiderlikde Run bölümünde parametr hökmünde ýerleşýär.



7.13-nji surat

Ol parametr 7.13-nji suratda gyzyl ok bilen görkezilen. Üns berilse ol hem ön prosesleriň arasyndan ýok edilen McaUpdate.exe faýlyň ýerleşýän ýerini görkezýär. Ol hem virus programmasy bolup durýar. Özem onuň ýerleşýän bukjasyňyň we parametriň ady onuň virus barlaýjy hökmünde çykyş edýändigini görkezjek bolýar we ulanyjynyň ünsüni çekmejek bolýar. Bu parametri ýok etmeli.

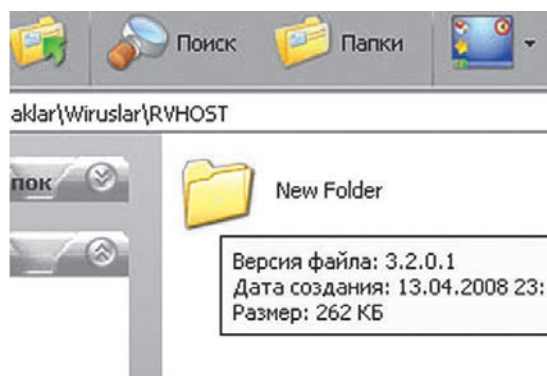
III. Reýestr arassalanandan soň, we wiruslara bolan ýollar kesgitlenenden soň olary diňe ýok etmek galýar, şol sebäpli D:\Windows\Sytem32\avpo.exe we D:\Program Files\Network Associates\VirusScan\MCAUpdate.exe ýollar arkaly degişli bozuýy programmalary ýok etmeli, ikinji ýagdaýda bolsa tutuş Network Associates bukjasyňy ýok etmek gerek. Avpo.exe faýlyňy ýok etjek bolanymyzda, eger onuň ýaýnnda avpo0.dll faýly bar bolsa, ony hem ýok etmek gerek.

Bu bozujynyň virus barlaýjy programma hökmünde çykyş etmegi we onuň birnäçe virus goýberiji, virus goldaýjy programmalary ulanmagy, mundan başga hem öz işine explorer.exe prosesi birikdirmegi, virus programmalaryň ikisiniň gatnaşmagyny amala aşyrmagy, ony çylşyrymlylaryň hataryna goşmaga mümkinçilik berýär.

Rvhost.exe

Bu bozuýy programma has çylşyrymly bolup, onuň ýok edilmeginde ilki başda birneme päsgelçilikler döreýärdi. Bozuýy toplum ulanyjynyň öz ýalňyşlygy bilen goýberilýär.

Esasan bu virus flash gurluşdan geçýär. Meselem şol virus bilen “ýokuşan” kompýutere arassa flash gurluşy çatylýar. Onuň awtomatiki ýüklenişi işläp başlaýar we onuň bukjalar we faýllar düzümini görkezmek boýunça penjireler açylýar. Şol mahal kompýuterden flash huşuň içine virus goýberiji programmalar ýazylyp başlaýar. Özem olar her bir bukja ýazylyp şol bukjanyň adyny göterýärler.

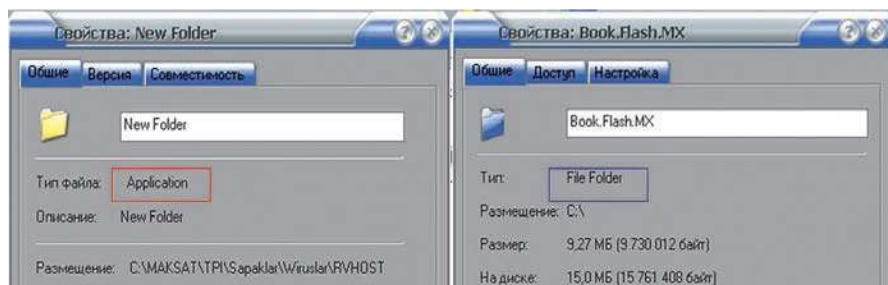


7.14-nji surat

Ulanyjy öz flash gurluşyny öz ýa-da başga arassa kompýuterine getirýär we oňa çatýar we Flash gurluşyň içine girip bukjalaryň içini açyp başlaýar. Birden ol bukjanyň içinde täze bir bukjany görýär (7.14-nji surat).

Ol oňa basýar. Emma ekrana bolsa hiç zat çykmaýar, kompýuter işlände birneme haýallaýar. Ulanyjy üns bermän öz işini dowam etdirýär.

Emma şol pursatdan başlap, kompýuteriň tordaky bilelikde ulanylýan bukjalarynyň we flash gurluşyň içindäki bukjalaryň içine virus goýberiji faýllaryň ýazylmagy güýçli depginde başlanýar. Prosesleriň sanawyna virus goldaýjy RVHOST.exe programmasy goşulýar, Kompýuteriň dolandyryjy diskiniň içindäki Windows we Windows\System32 bukjalaryna Rvhost.exe faýly ýazylýar. Reýestriň awtoýükleniş bölümlerine degişli ýazgylar ýazylýar.



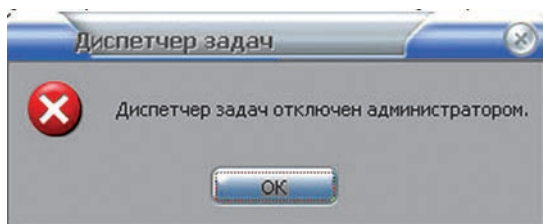
7.15-nji surat

Geliň şu ýerde *7.14-nji suratda* görkezilen faýlyň ýa-da bukjanyň häsiýetlerini görelin. Munuň üçin şol “bukjany” syçanjygyň çep düwmejigi bilen bir gezek basyp bellälin, soňra onuň sag düwmejigi bilen kontekst menýuny çagyryp, ol ýerde “Свойства” bende basalyň.

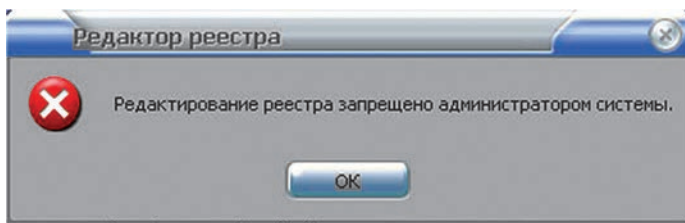
Ýokarky suratyň çep böleginde şol “bukjanyň” häsiýetiniň penjire bölegi, sag böleginde bolsa hakyky bukjanyň häsiýetleriniň penjire bölegi görkezilen. Görşüňiz ýaly çep bölekde ýalan bukjanyň görnüşi Application diýlip ýazylan. Ol bolsa goýberilýän (.exe faýllary) belgileýär. Hakyky bukja File Folder (faýllaryň bukjalary) diýlip belgilenmeli. Üns berilse, in bärkisi olaryň nyşanlary hem deň gelmeýär. Windows amallar ulgamyna dürli efektleri ulanmak bolýar, şol sanda hem bukjalaryň nyşanlaryny üýtgedýän efektler. Şol efektler şu bozuýy programmalaryň bukja nyşanlaryna täsir etmeýär. Şu maglumaty ulanyp hem, virus goýberiji programmany beýleki bukjalardan tapawutlandyryp kesgitlemek mümkin.

Wirusyň goýberilendigi bu indi hakykat – indi ony aýyrmak gerek. Ilkibaşda yzygiderlik bilen meseleler dispetçerine Ctrl+Alt+Del basyp girýäris. Emma oňa girmegiň deregine şeýle habar berilýär (*7.16-njy surat*).

Ol habar meseleler dispetçeriniň öçürilendigi baradadyr. Esasy guralymyzyň biri bozuýy toplумы tarapyndan ýapylan. Indi ikinji



7.16-njy surat



7.17-nji surat

esasy guralymyz bolan reýestre gireliň we ol ýerden zerur amallary ýerine ýetireliň.

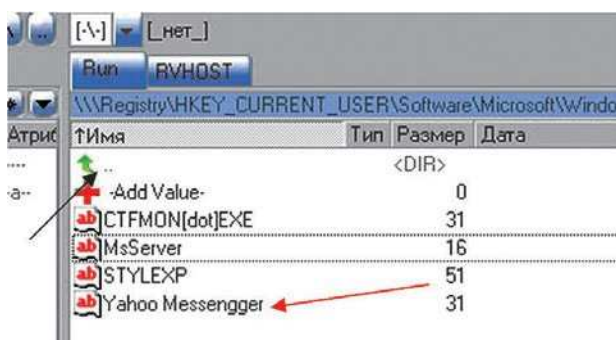
Emma indiki gadagan ediji habaryň çykmagy bozuýy toplumyň biziň garşymyza gowy taýýarlanandygyny görkezýär. Emma Total Commander faýl menejeri bu ýagdaýda uly kömek berýär. 7.3-nji suratda görkezilen düwmejige basyp bozuýy toplumy aýyrmaklygy aşakdaky yzygiderlikde başlalyň.

I. Değişli düwmejige basyp (7.3-nji surat), Task manager bende basalyň. Netijede 7.4-nji suratyň sag bölegindäki prosesleriň sanawy çykar, olaryň hatarynda bukja nyşanly RVHOST.exe prosesleriň ikisi bardyr. Olaryň ikisini hem ýok etmeli. Şeýlelik bilen wirus goldawjysy ýok edilýär.

II. Indi Task manager bendinden çykmaly. Munuň üçin prosesleriň iň ýokarkysynyň üstünde iki nokatly ýere basmaly. Registry bendine girmeli. Netijede, 7.4-nji suratyň çep bölegindäki kök bölümleriň düzümi çykar. HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Run yzygiderlik bilen gideliň we Run bölümüniň içine gireliň.

Bu ýerde gyzyk bilen görkezilen parametri ýok etmeli. Bu ýerde onuň diňe ady görkezilen we wirusyň programma eltýän ýoluny biz görüp bilmeýäris.

Emma şu ýerde, bir zady bellemek gerek. Wirus dörediji adam ussatly ulanyjy bolandygy üçin bilýär – reýestriň HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Po-



7.18-nji surat

| Имя | Тип | Значение |
|----------------|-----------|-------------------------|
| (По умолчанию) | REG_SZ | (значение не присвоено) |
| DisableTaskMgr | REG_DWORD | 0x00000001 (1) |

7.19-njy surat

licies bölümünde täze System bölümünü döredip onuň içine DisableTaskmgr parametri döredip bahalaryň tipini we ähmiýetini 7.19-njy suratdaky ýaly edip ýazyp goýsa, onda meseleler dispetçeri ýokarda görkezilen ýaly ýapylar (7.16-njy surat).

Eger bu bölümde DisableRegistryTools parametr döredilip edil şol ýokardaky ýaly onuň bahasy girizilse, onda 7.17-nji suratdaky ýaly reýestr hem elýeterli bolmaz.

Geliň indi 7.18-nji surata gaýdyp geleliň. Bu parametri ýok etmezden öň, bir bölüm ýokary galalyň. Bir bölüm ýokary galmak üçin, edil bir bukja ýokary galmak üçin ýaly iň ýokarky parametriň ýokarsyndaky iki nokatly setire basmak gerek. Netijede Run bölümüniň üstünde Policies bölümü durandyr, onuň içine girip System bölümü görmek bolar. Onuň içine girip 7.20-nji suratda görkezilen iki parametri görmek bolar. Ol ikisini ýok etmek gerek, emma has dogrusy bir bölüm ýokary galyp tutuş System bölümünü ýok etmeli.

Indi adaty usul bilen reýestre girjek bolalyň. Netijede, reýestr açylandyr. Ctrl+Alt+Del klawişalaryny basyp meseleler dispetçerine

| \\Registry\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System | | | |
|--|-----|--------|----------|
| Имя | Тип | Размер | Действие |
| <DIR> | | | |
| + Add Value- | | 0 | |
| DisableRegistryTools | | 4 | |
| DisableTaskMgr | | 4 | |

7.20-nji surat

| Имя | Тип | Значение |
|-----------------|--------|--|
| (По умолчанию) | REG_SZ | (значение не присвоено) |
| CTFMON.EXE | REG_SZ | D:\WINDOWS\system32\ctfmon.exe |
| STYLEXP | REG_SZ | D:\Program Files\TGTSoft\StyleXP\StyleXP.exe -Hide |
| Yahoo Messenger | REG_SZ | D:\WINDOWS\system32\RVHOST.exe |

7.21-nji surat

| | | |
|----------------------|-----------|-------------------------|
| SystemRestore | REG_DWORD | 0 |
| SFCDisable | REG_DWORD | 0x00000000 (0) |
| SfcQuota | REG_DWORD | 0xffffffff (4294967295) |
| Shell | REG_SZ | Explorer.exe RVHOST.exe |
| ShowLogonOptions | REG_DWORD | 0x00000000 (0) |
| ShutdownWithoutLogon | REG_SZ | 0 |

7.22-nji surat

hem girmek bolýar. Reýestre girip, HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Run yzygiderlik bilen gideliň we Run bölümiň içine geçmeli (7.21-nji surat).

Suratdan görşümüz ýaly, bizi gyzyklanýan parametrdde Rvhost.exe faýla bolan ýol görkezilen. Şol ýoly belläp bu parametri ýok etmeli. Reýestrden çykmazdan öň HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \Winlogon yzygiderlilik bilen gidip Winlogon bölümiň içini barlap görmeli (7.22-nji surat).

Bu bölümiň parametrleriniň arasynda Shell parametri ýok etmeli.

III. Reýestr arassalandan soň 7.21-nji suratdan bellenen ýol boýunça RVHOST.exe faýly ýok etmeli. Eger proseslerden deň atly virus goldawjy aýrylmadyk bolanda bu faýlyň ýok edilmegini amala aşyrmak mümkin bolmazdy.

RVHOST.exe faýlyň adyny gözlege bermeli (*Пуск-Найму-Файлы и папки-Файлы и папки*). Gözlegiň parametrlerinde “Дополнительные параметры-Поиск в скрытых файлах и папках” parametri goýmaly we gözlegi goýbermeli. Netijede Windows bukjasynda hem RVHOST.exe faýly bardyr. Ony hem ýok etmeli. Şu usul örän peýdaly. Munuň üçin reýestre girip “*Правка-Найму*” menýu yzygiderligini ýerine ýetirmeli we açylan penjirede gerek bolan gözlegiň adyny ýazyp gözlegi goýbermeli.

Şu amallar bilen bu bozuýjy programmanyň işi doly togtadylan.

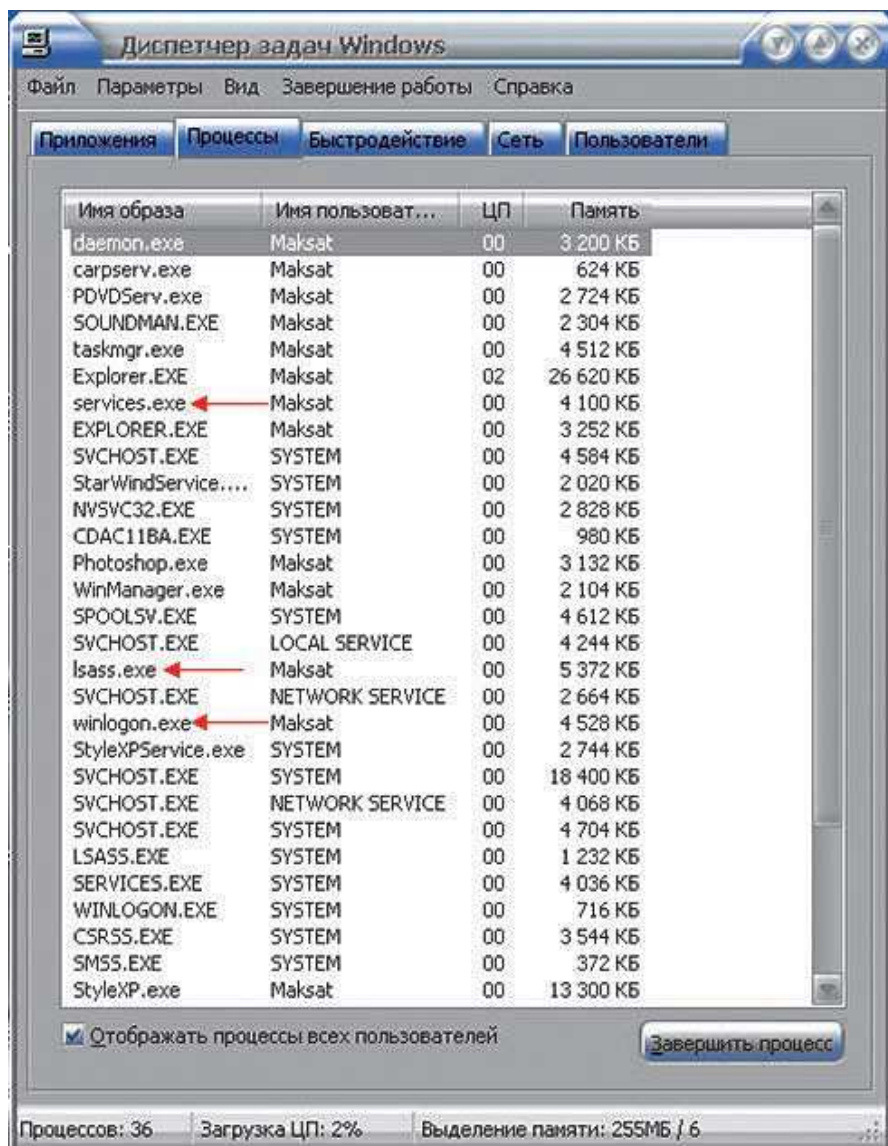
NorBtok.exe

Gezek indi tejribelikde duş gelen bozuýjylaryň arasynda has kyn ýok edilýänine geldi.

Wirus goýberiji edil mundan öňki, Rvhost.exe we Scvvhos.exe bozuýjy toplumlaryňky ýalydyr. Ol bukjanyň nyşanyny göterýär, özi

.exe giňişlikli goýberilýän faýl bolup durýar (7.15-nji surat). Onuň göwrümi 80Kb golaý.

Geliň indi şoňa basyp, bozuýy toplumy “azatlyga” goýbereliň we kompýuteri gaýtadan ýükläliň. Windows amallar ulgamy doly ýükle-



7.23-nji surat

nenden soň, amallar ulgamyň birneme haýal işläp durandygy bildirip durar. Eger reýestre girjek bolsak, onda 7.17-nji suratdaky habar berler. Şeýlelik bilen, ýene-de, bozuýy programma biziň iş gurallarymyz boýunça “urgy edýär”.

Geliň indi Meseleler dispetçerine girjek bolalyň (Ctrl+Alt+Del). Emma meseleler dispetçeri ýapylmandyr we ondan gyzykly maglumaty almak mümkin (7.23-nji surat).

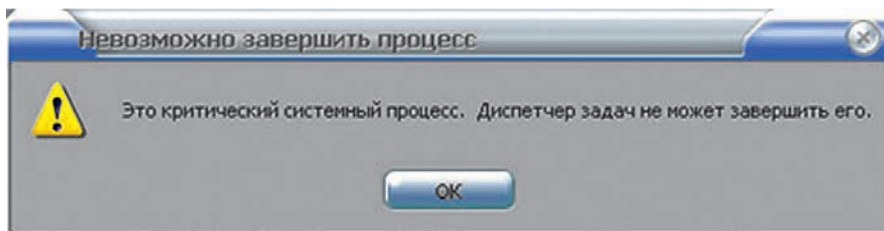
Gyzyl oklar bilen täze emele gelen prosesleri görmek mümkin, üns berilse olar System ulanyjy tarapyndan goýberilen LSASS.EXE, SERVICES.EXE we WINLOGON.EXE prosesleriň atlaryny görterýärler. Emma olar, ulgamyň ulanyjysy bolan Maksat ulanyjynyň ady bilen goýberilen. Bu prosesleriň virus goldaýjy bolup durýandygyna göz ýetirmek kyn dälmi kä diýip pikir edýäris.

Indi bolsa geliň bozuýy programmanyň ýok edilmegini ädimleýin amala aşyrylmagynyň tertibini yzarlalyň.

I. Ilkibaşda virus goldaýjy programmalaryň ýok edilmeginden başlalyň. Emma ýok edilmeli prosesleri belläp, degişli düwmejige basyp ýok etjek bolsak 7.24-nji suratdaky habar berilýär.

Bu habaryň mazmuny, ýok edip bilmeýändigini habar bermekden ybarat.

Bozuýy programma proseslere elýeterligi ýapmadyk hem bolsa, onuň bu hereketleri özümizi bu ýagdaýda hiç zada ukypsyz hasap etmäge mümkinçilik döredýär. Emma biziň elimizde Total Commander bar we meseleler dispetçerine degişli düwmejige basyp (7.3-nji surat), Task manager bende basalyň. Netijede, 7.4-nji suratyň sag bölegindäki prosesleriň sanawy çykar, olaryň hatarynda bukja nyşanly bar bolan prosesleriň hemmesini (lsass.exe, services.exe we winlogon.exe, bar bolsa beýlekilerini hem) ýok etmek gerek. Bu ýerde bize hiç



7.24-nji surat

hili habar berilmedi. Onda ýokarky habar wirus dörediji tarapyndan diňe meseleler dispetçeri üçin göz önünde tutulan eken. Şeýlelik bilen, wirus goldaýjylar ýok edilen.

II. Geliň indi, reýestriň açylmagyny amala aşyralyň. Munuň üçin Total Commanderiň üsti bilen reýetriň düzümini açyp HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion\Policies yzygiderligi bilen gidip Policies bölümüne girip System bukjasyyny ýok etmek gerek. Netijede reýestrimiz açylar.

Indi reýestre adaty usul bilen (*Пуск-Выполнить*, soňra setirde regedit ýazyp OK basyp) gireliň we HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion\Run yzygiderligi bilen Run bölüme gireliň (7.25-nji surat).

Bu ýerde gyzyk bilen görkezilen parametri şübheli diýip kesgitläp, onuň bahasyny ýatda saklaýarys – **D:\Documents and Settings\Maksat\Local Settings\Application Data\smss.exe**. Soňra bu parametri ýok edýäris.

Indi bolsa HKEY_LOCAL_MACHINE \Software \Microsoft \Windows \CurrentVersion\Run yzygiderligi bilen Run bölüme gireliň (7.26-njy surat). Bu ýerde hem gyzyk bilen görkezilen bir täze

| Имя | Тип | Значение |
|----------------|--------|---|
| (По умолчанию) | REG_SZ | (значение не присвоено) |
| CTFMON.EXE | REG_SZ | D:\WINDOWS\system32\ctfmmon.exe |
| STYLEXP | REG_SZ | D:\Program Files\TGTSoft\StyleXP\StyleXP.exe -Hide |
| Tok-Cirrhatus | REG_SZ | "D:\Documents and Settings\Maksat\Local Settings\Application Data\smss.exe" |

7.25-nji surat

| Имя | Тип | Значение |
|-----------------------|--------|--|
| (По умолчанию) | REG_SZ | (значение не присвоено) |
| Bron-Spizaetus | REG_SZ | "D:\WINDOWS\INF\norBtok.exe" |
| CARPService | REG_SZ | carpserv.exe |
| CloneCD\ElbyCDFL | REG_SZ | "D:\Program Files\Elaborate Bytes\CloneCD\ElbyCheck.exe" /L ElbyCDFL |
| DAEMON Tools-1033 | REG_SZ | "D:\Program Files\DRTools\daemon.exe" -lang 1033 |
| IMJPMIG8.2 | REG_SZ | msime80.exe |
| NeroFilterCheck | REG_SZ | D:\WINDOWS\system32\NeroCheck.exe |
| NvCplDaemon | REG_SZ | RUNDLL32.EXE D:\WINDOWS\system32\NvCpl.dll,NvStartup |
| nwiz | REG_SZ | nwiz.exe /install |
| RemoteControl | REG_SZ | "D:\Program Files\CyberLink\PowerDVD\PDVDServ.exe" |
| Share-to-Web Names... | REG_SZ | D:\Program Files\Hewlett-Packard\HP Share-to-Web\hpgs2wnd.exe |
| SoundMan | REG_SZ | SOUNDMAN.EXE |

7.26-njy surat

| d:\Documents and Settings\Maksat\Local Settings\Application Data | | | | |
|--|-------|-----------|----------------|------|
| Имя | Тип | Размер | Дата | А |
| Bron.tok-3-14 | <DIR> | | 14.04.08 20:08 | ---- |
| Help | <DIR> | | 08.08.06 21:31 | ---- |
| Macromedia | <DIR> | | 23.11.07 23:39 | ---- |
| Microsoft | <DIR> | | 05.07.06 22:34 | ---- |
| Oblivion | <DIR> | | 09.01.07 22:26 | ---- |
| Ok-SendMail-Bron-tok | <DIR> | | 14.04.08 20:16 | ---- |
| PCHealth | <DIR> | | 15.07.07 20:17 | ---- |
| Symantec | <DIR> | | 18.12.07 17:55 | ---- |
| TechSmith | <DIR> | | 12.09.07 23:08 | ---- |
| WMTtools Downloaded Files | <DIR> | | 02.12.07 18:34 | ---- |
| csrss | exe | 81 920 | 08.01.08 09:09 | -a- |
| DCBC2A71-70D8-4DAN-E.. | ini | 64 512 | 14.04.08 02:06 | -a- |
| GDIPFONTCACHEV1 | DAT | 77 776 | 30.01.08 20:48 | -a- |
| IconCache | db | 2 643 154 | 11.04.08 00:18 | -al |
| inetinfo | exe | 81 920 | 08.01.08 09:09 | -a- |
| lsass | exe | 81 920 | 08.01.08 09:09 | -a- |
| services | exe | 81 920 | 08.01.08 09:09 | -a- |
| smss | exe | 81 920 | 08.01.08 09:09 | -a- |
| winlogon | exe | 81 920 | 08.01.08 09:09 | ---- |

7.27-nji surat

şübhelili parametri görýäris. Onuň bahasyny hem ýatda saklaýarys – **D:\WINDOWS\INF\norBtok.exe**.

Soňra bu parametri ýok edýäris.

III. Indi alnan **D:\Documents and Settings\Maksat\Local Settings\Application Data\smss.exe** we **D:\WINDOWS\INF\norBtok.exe** ýollar boýunça degişli wirus programmalary ýok etmäge başlaýarys.

Birinji ýol bilen gidenimizde Total Commanderi ulanmaklyk maksada laýykdyr. Netijede 7.27-nji suraty görmek bolar. Bu ýerde gyzyly oklar we gyzyly gönüburçlugaň içinde ýok edilmeli elementler görkezilen. Üns berseňiz bu ýerde prosesleriň sanawynda ýok edilen prosesleriň atlaryny göterýän faýllar hem bar. Hut şolar hem prosesleri goýberýän faýllar bolup durýar. Eger prosesleriň sanawyndan degişli wirus goldawjylar ýok edilmedik bolsa, bu faýllary ýok etmek mümkin bolmazdy. Bularyň hemmesini ýok edýäris.

Indi D:\WINDOWS\INF bukjasyna girýäris we norBtok.exe faýly ýok edýäris.

Indi hemme amallar ýerine ýetirilen ýaly. Işimiziň netijesini barlamak üçin kompýuteri gaýtadan ýükleýäris.

Windows amallar ýüklenilenden soň, bozuýy toplумыň ýene öňki ýagdaýynda işläp durandygyna göz ýetirmek bolýar. Şeýlelik bilen, bozuýy toplумыň bir bölegini goýberipdiris. Geliň gowy pikir edip göreliş. Reýestriň hemme awtoýükleniş bölümleri arassalanypdy. Emma Windowsyň programmalary goýberýän bukjasy biziň ünsümüzden gaçypdyr. Ony görmek üçin “Пуск-Программы-Автозагрузка (ýa-da Sturtup)” buýrugyny ýerine ýetirmeli we onuň içinden **Empty.pif** (ýe-ne de özüni bukmak üçin başga bir grafiki faýlyň giňişligini alypdyr) faýly ýok etmeli we hemme öňki gaýtalan amallarymyzy täzeden gaýtalamaly.

DiňeMenSeniSöýýän.exe

Tehnologiýanyň ýaramaz taraplarynyň ösüşi Türkmenistandan hem sowulyp geçmedi. Dünýäde wirus ýazylmagynyň ösmegi, Türkmenistandaky wirusçylaryň döremegine getirdi.

Olaryň döreden programma „önümleri“ dünýädäki „kärdeşleriňkiden“ hili we ýaramaz işleriniň netijeligi boýunça pes gelmeýär. Şol wiruslara garşy göreşmekligi kynlaşdyrýan ýene bir zatlaryň biri – meşhur daşary ýurt antiwiruslar tarapyndan bu wirusyň öz döwründe kesgitlenmeýändigidir.

Bu wirusyň ýerine ýetirýän işleri hem-de ýaýradlyşy tejribe taýdan öwrenildi. Tejribeler birnäçe kompýuterlerde we operasion sistemalarda geçirildi. Tejribeleriň esasynda şol wirusy eldeki ýagdaýda ýok etmegiň usuly işlenip düzüldi hem-de Delphi programmirleme dilinde oňa programma kody düzüldi. Aşakda şol programma kody getirilendir.

```
procedure TForm1.Button34Click(Sender: TObject);
```

```
begin
```

```
WinDirP := StrAlloc(MAX_PATH);
```

```
Res := GetWindowsDirectory(WinDirP, MAX_PATH);
```

```
if Res > 0 then
```

```

WinDir := StrPas(WinDirP);
{Proses}
KillTask('Mss.exe');
KillTask('Svchîst.exe');
{Reyestr}
Reg := nil;
  try
    reg := TRegistry.Create;
    reg.RootKey := HKEY_Local_Machine;
    reg.LazyWrite := false;
    reg.OpenKey('Software\Microsoft\Windows\CurrentVersion\Run',
    false);
    if reg.ValueExists('AA')=true then reg.DeleteValue('AA');
    if reg.ValueExists('AA1')=true then reg.DeleteValue('AA1');
    reg.CloseKey;
    reg.free;
  except
    if Assigned(Reg) then Reg.Free;
end;
  {Files}

```

```

If FileExists(Windir+'\System32\MSS.exe')=true then
begin
FileSetAttr(Windir+'\System32\MSS.exe',0);
DeleteFile(Windir+'\System32\MSS.exe');
end;
If FileExists(Windir+'\System32\svchîst.exe')=true then
begin
FileSetAttr(Windir+'\System32\svchîst.exe',0);
DeleteFile(Windir+'\System32\svchîst.exe');
end;
for i:=67 to 82 do
Begin
if FileExists(chr(i)+':\DineMenSeniSoyyan.exe') then
begin

```

```

FileSetAttr(chr(i)+':\DineMenSeniSoyyan.exe',0);
DeleteFile(chr(i)+':\DineMenSeniSoyyan.exe');
end;
if FileExists(chr(i)+':\autorun.inf') then
begin
FileSetAttr(chr(i)+':\autorun.inf',0);
DeleteFile(chr(i)+':\autorun.inf');
end;
End;
end;

```

Wirus aşakdaky işleri ýerine ýetirýär:

Operasion sistemada işläp başlanyndan soň, ol **Mss.exe** we **Svchost.exe** prosesleri işledýär. Bu virus hüjüminiň beýlekilerden tapawudy – onuň iki prosesiniň hem parallel işläp, biri-birini goramagydyr. Meselem onuň biri ýok edilen mahaly, ikinji bu ýagdaýy barlap ony gaýtadan dikeldip ýetişýär. Barlama we dikeltme şeýlebir ýokary tizlikde amala aşyrylýar, eýsem ulanyjy iki prosesin bardygyny bilse hem, olary meseleler dispetçerinden ýok edip ýetişmeýär. Munuň üçin, programmirmlemegi ulanmaly. Programmanyň tizliginde diňe programma işläp bilýändir.

Ýokarda görkezilen programma kodunda, iki proses biri-birinde örän ýokary ýygylykda ýok edilýär. Ikinji proses birinjisini dikeldip ýetişmeýär.

Wirus reýestrde hem öz yzyny galdyrýar. HKEY_Local_Machine\Software\ Microsoft\ Windows\CurrentVersion\Run bölüminde AA we AA1 açarlary döredýär. Ol açarlaryň bahasynda – **Mss.exe** we **Svchist.exe** faýllara bolan ýol görkezilen, ýagny operasion sistema ýüklenen mahaly şol iki virus faýly iki sany virus prosesini goýberýär.

Ýokarda görkezilen programma kody şol ýazgylary kesgitläp ýok edýär, soňra şol ýazgylarda görkezilen ýoly yzarlap Windows\System32 ulgamlaryň bukjasynda degişli virus faýllary ýok edýär.

Mundan başga hem, hemme lokal disklerde hem-de şol mahal çatylan maglumat göterijilerden virus goýberiji bolan **DineMenSe-**

niSoyyan.exe faýly hem-de onuň meýilnamalaşdyryjysy bolan **auto-run.exe** faýllary ýok edilýär.

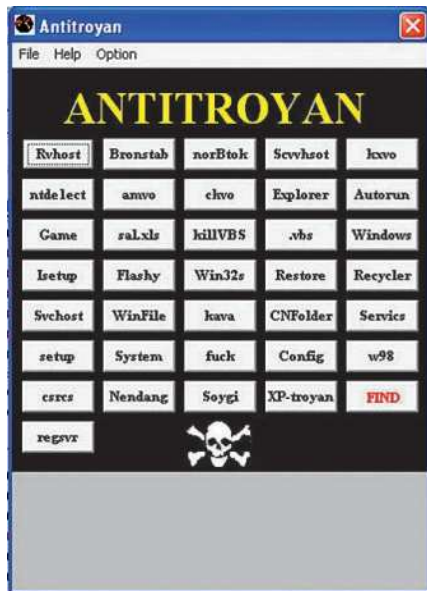
Şeýlelik bilen görkezilen virus doly operasion sistemadan ýok edilýär.

7.3. Antitroyan.exe türkmen antiwirus programmasynyň döredilmegi

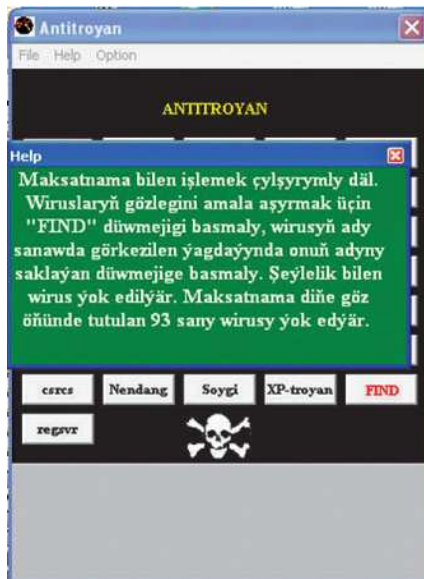
Ýokarda ady agzalan bozuýy programmalaryň toplumyna garşy antiwirus programmasynyň mysaly hökmünde şekili aşakda görkezilen programma döredildi. Bu programma türkmen dilinde bolmak bilen 100-e golaý wirusyň we troýanlaryň ýok edilmegini üpjün edýär.

Programma doly türkmen dilinde özüni ulanmak barada düşündiriş berýär.

Programma Borland Delphi 7 programmirleme dilinde işlenip düzüldi. Umuman aýdylanda programma bozuýy toplumyň bir böle-



7.28-nji surat



7.29-njy surat

gini tapyp, göni beýlekilerini ýok etmegi amala aşyrýar hem-de kompýuterde käbir galyndy bolan faýllary hem ýok edýär.

Programmanyň bozujy toplumlary aýyrmaklyk boýunça ýerine ýetirýän işi öň bellenen yzygiderlikde amala aşyrylýar:

I. Meseleler dispetçerindäki prosesleriň sanawynda virus goldaýjy proses ýok edilýär.

II. Reýestre girilýär we onuň awtoýükleýji bölümlerinde bozujy programmalaryň ýüklenmegi baradaky ýazgylar ýok edilýär we wirusyň programmalara eltýän ýollar kesgitlenýär.

III. Wirus goýberiji we bozujy faýllar lokal disklerden we flash gurluşyndan (çatylan bolsa) aýrylýar.

Programmanyň programma kody örän uludyr. Ol 100 sahypadan hem köp. Şol sebäpli, onuň, iň esasy bölegi bolan wiruslary gözleýji we seljeriji böleginiň koduny (Find düwmesi) getirilýär.

procedure TForm1.BitBtn1Click(Sender: TObject);

Label 1,2,3,4;

Var

j:integer;

Temp:string;

begin

d1:=true;

j:=0;

WinDirP := StrAlloc(MAX_PATH);

Res := GetWindowsDirectory(WinDirP, MAX_PATH);

if Res > 0 then

WinDir := StrPas(WinDirP);

If FileExists(Windir+"System32\autorun.i")=true then

begin

FileSetAttr(Windir+"System32\autorun.i",0);

DeleteFile(Windir+"System32\autorun.i");

end;

If FileExists(Windir+"System32\autorun.in")=true then

begin

FileSetAttr(Windir+"System32\autorun.in",0);

DeleteFile(Windir+"System32\autorun.in");

```

end;
Memo1.Lines.Clear;j:=0;
{Reyestr amallary}
Reg := nil;
try
reg := TRegistry.Create;
reg.RootKey := HKEY_CURRENT_USER;
reg.LazyWrite := false;

reg.OpenKey('Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders',
false);
Temp:=reg.ReadString('Local Settings')+'\Temp';
reg.CloseKey;
reg.OpenKey('Control Panel\International',
false);
if reg.ReadString('sTimeFormat')='FUCK YOU!' then
begin
Memo1.Lines.Add('fuck.exe');
inc(j);
end;
reg.CloseKey;
Reg.free;
except
if Assigned(Reg) then Reg.Free;
end;
If FileExists(Windir+'\System32\Rvhost.exe')=true then
begin
Memo1.Lines.Add('Rvhost.exe');
inc(j);
end;
If FileExists(Windir+'\System32\Scvvhsot.exe')=true then
begin
Memo1.Lines.Add('Scvvhsot.exe');
inc(j);

```

```

end;
If FileExists(Windir+"\System32\amvo.exe")=true then
begin
Memo1.Lines.Add('amvo.exe');
inc(j);
end;
If FileExists(Windir+"\System32\avpo.exe")=true then
begin
Memo1.Lines.Add('ntdelect.com');
inc(j);
end;
If FileExists(Windir+"\System32\algssl.exe")=true then
begin
Memo1.Lines.Add('sal.xls.exe');
inc(j);
end;
If FileExists(Windir+"\INF\norBtok.exe")=true then
begin
Memo1.Lines.Add('norBtok.exe');
inc(j);
end;
If FileExists(Windir+"\System32\explorer.exe")=true then
begin
Memo1.Lines.Add('Explorer.exe');
inc(j);
end;
Reg := nil;
try
reg := TRegistry.Create;
reg.RootKey := HKEY_LOCAL_MACHINE;
reg.LazyWrite := false;

reg.OpenKey('Software\Microsoft\Windows\CurrentVersion\Run',
false);
if reg.ValueExists('Explorer.exe')=true then

```

```

begin
reg.DeleteValue('Explorer.exe');
Memo1.Lines.Add('Game.exe');
inc(j);
end;
reg.CloseKey;
reg.free;
except
if Assigned(Reg) then Reg.Free;
end;
If FileExists(Windir+'\ShellNew\bronstab.exe')=true then
begin
Memo1.Lines.Add('Bronstab.exe');
inc(j);
end;

If FileExists(Windir+'\KesenjanganSosial.exe')=true then
begin
Memo1.Lines.Add('Nendang');
inc(j);
end;
If FileExists(Windir+'\System32\killVBS.vbs')=true then
begin
Memo1.Lines.Add('killVBS.vbs');
inc(j);
end;
if FileExists(chr(i)+':\n2de.cmd') then
begin
Memo1.Lines.Add('n2de.cmd');
inc(j);
end;

If FileExists(Windir+'\System32\xpbootnt.exe')=true then
begin
Memo1.Lines.Add('setup.exe');

```



```
inc(j);  
end;
```

```
If FileExists(Windir+"\System32\drivers\services.exe")=true then  
begin  
Memo1.Lines.Add('services.exe');  
inc(j);  
end;
```

```
If FileExists(Windir+"\regsvr.exe")=true then  
begin  
Memo1.Lines.Add('regsvr');  
inc(j);  
end;  
if FileExists(Windir+"\System32\imapd.exe") then  
begin  
Memo1.Lines.Add('Isetup.exe');  
inc(j);  
end;  
if FileExists(Windir+"\System32\vbe') then  
begin  
Memo1.Lines.Add('.vbs');  
inc(j);  
end;  
if FileExists(Windir+"\System32\Flashy.exe') then  
begin  
Memo1.Lines.Add('Flashy.exe');  
inc(j);  
end;  
if FileExists(Windir+"\security\services.exe') then  
begin  
Memo1.Lines.Add('Win32s.exe');  
inc(j);  
end;
```

```
If FileExists(Windir+'\System32\ckvo.exe')=true then  
begin  
Memo1.Lines.Add('ckvo.exe');  
inc(j);  
end;
```

```
If FileExists(Windir+'\System32\kxvo.exe')=true then  
begin  
Memo1.Lines.Add('kxvo.exe');  
inc(j);  
end;
```

```
If FileExists(Windir+'\MsDoStray.com')=true then  
begin  
Memo1.Lines.Add('Windows.exe');  
inc(j);  
end;
```

```
for i:=67 to 82 do  
if DirectoryExists(chr(i)+':\RESTORE') then  
begin  
Memo1.Lines.Add('RESTORE');  
inc(j);Goto 1;  
end;  
1:  
for i:=67 to 82 do  
if DirectoryExists(chr(i)+':\RECYCLER') then  
begin  
Memo1.Lines.Add('RECYCLER');  
inc(j);Goto 2;  
end;  
2:  
for i:=67 to 82 do  
if DirectoryExists(chr(i)+':\CONFIG') then  
begin
```

```
Memo1.Lines.Add('CONFIG');  
inc(j);Goto 3;  
end;
```

```
3:  
for i:=67 to 82 do  
if DirectoryExists(chr(i)+':\SYSTEM') then  
begin  
Memo1.Lines.Add('SYSTEM');  
inc(j);Goto 4;  
end;
```

```
If FileExists(Windir+'\System\svchost.exe')=true then  
begin  
Memo1.Lines.Add('svchost.exe');  
inc(j);  
end;
```

```
If FileExists(Windir+'\System32\autorun.bat')=true then  
begin  
Memo1.Lines.Add('autorun.bat');  
inc(j);  
end;
```

```
If FileExists(Windir+'\Mstray.exe')=true then  
begin  
Memo1.Lines.Add('WINFILE.EXE');  
inc(j);  
end;  
If FileExists(Windir+'\System32\kavo.exe')=true then  
begin  
Memo1.Lines.Add('kava');  
inc(j);  
end;
```

```
If FileExists(Temp+'\services.exe')=true then  
begin  
Memo1.Lines.Add('CNFolder');  
inc(j);  
end;
```

```
If FileExists(Windir+'\System32\olhrwef.exe')=true then  
begin  
Memo1.Lines.Add('w98');  
inc(j);  
end;
```

```
If (FileExists(Windir+'\System32\mss.exe')=true) or  
(FileExists(Windir+'\System32\svchîst.exe')=true) then  
begin  
Memo1.Lines.Add('Soygi');  
inc(j);  
end;
```

```
If FileExists(Windir+'\System32\csrçs.exe')=true then  
begin  
Memo1.Lines.Add('csrçs');  
inc(j);  
end;
```

```
If FileExists(Windir+'\System32\com.run')=true then  
begin  
Memo1.Lines.Add('XP-troyan');  
inc(j);  
end;  
ScandirFind(WinDir+'\System32\','EXE',1515280);  
if FileExists(troyanDir+troyan)=true then  
begin  
Memo1.Lines.Add('XP-troyan');  
inc(j);
```

end;

4:

if j=0 then

if opsiya=false then Memo1.Lines.Strings[j]:='Wirus tapylmady'

else Memo1.Lines.Strings[j]:='Âèðóñû íà íàéääû';

end;

procedure TForm1.Help2Click(Sender: TObject);

begin

Form3.ShowModal;

end;

procedure TForm1.Button11Click(Sender: TObject);

Var

AppData:string;

begin

error:="";

WinDirP := StrAlloc(MAX_PATH);

Res := GetWindowsDirectory(WinDirP, MAX_PATH);

if Res > 0 then

WinDir := StrPas(WinDirP);

{Proses}

KillTask('WScript.exe');

KillTask('dxdlg.exe');

KillTask('imapd.exe');

{Reyestr}

Reg := nil;

try

reg := TRegistry.Create;

reg.RootKey := HKEY_LOCAL_MACHINE;

reg.OpenKey('SOFTWARE\Microsoft\Windows\CurrentVersion\
policies\Explorer\Run',

false);

```

if reg.ValueExists('imapd')=true then
reg.DeleteValue('imapd');
reg.CloseKey;
{Folder Options parametri dikeldyar}

reg.OpenKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Ex-
plorer\Advanced\Folder\Hidden\SHOWALL',
false);
reg.Writeinteger('DefaultValue',1);
reg.Writeinteger('CheckedValue',1);
reg.CloseKey;

reg.OpenKey('SOFTWARE\Microsoft\Windows NT\CurrentVersi-
on\Winlogon',
false);
if reg.ValueExists('Shell')=true then
reg.DeleteValue('Shell');

reg.WriteString('Userinit',WinDirP+'\System32\userinit.exe');
reg.CloseKey;
reg.RootKey := HKEY_CURRENT_USER;
reg.LazyWrite := false;

reg.OpenKey('Software\Microsoft\Windows\CurrentVersion\Explo-
rer\Shell Folders',
false);
AppData:=reg.ReadString('AppData');
reg.CloseKey;
reg.free;
except
if Assigned(Reg) then Reg.Free;
end;
for i:=66 to 72 do
Begin
if FileExists(AppData+'\dxdlls\imapd'+chr(i)+''.dll') then

```

```

begin
FileSetAttr(AppData+"\dxdlls\imapd'+chr(i)+'.dll',0);
DeleteFile(AppData+"\dxdlls\imapd'+chr(i)+'.dll');
end;
if FileExists(AppData+"\dxdlls\imapd'+chr(i)+'.exe') then
begin
FileSetAttr(AppData+"\dxdlls\imapd'+chr(i)+'.exe',0);
DeleteFile(AppData+"\dxdlls\imapd'+chr(i)+'.exe');
end;
End;
If FileExists(AppData+"\dxdlls\imapd.exe')=true then
begin
FileSetAttr(AppData+"\dxdlls\imapd.exe',0);
DeleteFile(AppData+"\dxdlls\imapd.exe');
end;
If FileExists(AppData+"\dxdlls\boot.vbs')=true then
begin
FileSetAttr(AppData+"\dxdlls\boot.vbs',0);
DeleteFile(AppData+"\dxdlls\boot.vbs');
end;
If FileExists(AppData+"\dxdlls\dxdlg.exe')=true then
begin
FileSetAttr(AppData+"\dxdlls\dxdlg.exe',0);
DeleteFile(AppData+"\dxdlls\dxdlg.exe');
end;
If FileExists(AppData+"\dxdlls\isetup.exe')=true then
begin
FileSetAttr(AppData+"\dxdlls\isetup.exe',0);
DeleteFile(AppData+"\dxdlls\isetup.exe');
end;
If DirectoryExists(AppData+"\dxdlls')=true then
RemoveDir(AppData+"\dxdlls');
If FileExists(Windir+"\System32\boot.vbs')=true then
begin
FileSetAttr(Windir+"\System32\boot.vbs',0);

```

```

DeleteFile(Windir+'\System32\boot.vbs');
end;
If FileExists(Windir+'\System32\dxdlg.exe')=true then
begin
FileSetAttr(Windir+'\System32\dxdlg.exe',0);
DeleteFile(Windir+'\System32\dxdlg.exe');
end;
If FileExists(Windir+'\System32\wproxp.exe')=true then
begin
FileSetAttr(Windir+'\System32\wproxp.exe',0);
DeleteFile(Windir+'\System32\wproxp.exe');
end;
If FileExists(Windir+'\System32\imapd.exe')=true then
begin
FileSetAttr(Windir+'\System32\imapd.exe',0);
DeleteFile(Windir+'\System32\imapd.exe');
end;
If FileExists(Windir+'\System32\isetup.exe')=true then
begin
FileSetAttr(Windir+'\System32\isetup.exe',0);
DeleteFile(Windir+'\System32\isetup.exe');
end;
for i:=66 to 72 do
Begin
if FileExists(Windir+'\System32\imapd'+chr(i)+'.dll') then
begin
FileSetAttr(Windir+'\System32\imapd'+chr(i)+'.dll',0);
if DeleteFile(Windir+'\System32\imapd'+chr(i)+'.dll')=false then
if opsiya=false then
error:='The file is ' +Windir+'\System32\imapd'+chr(i)+'.dll cannot
delete. Close and restart program and press «Isetup» button'
else error:='Ôàée ' +Windir+'\System32\imapd'+chr(i)+'.dll íà
óääëÿàõñÿ. Çàêðíéòà è íãðàçàíõñòèòà ïðíãðàìíó (êîíüðòàð) è íàæíèòà
êîíüèò «Isetup»';
end;

```



```

if FileExists(Windir+'\System32\imapd'+chr(i)+'.exe') then
begin
FileSetAttr(Windir+'\System32\imapd'+chr(i)+'.exe',0);
DeleteFile(Windir+'\System32\imapd'+chr(i)+'.exe');
end;
if FileExists(chr(i)+':\explorer.exe') then
begin
FileSetAttr(chr(i)+':\explorer.exe',0);
DeleteFile(chr(i)+':\explorer.exe');
FileSetAttr(chr(i)+':\autorun.inf',0);
DeleteFile(chr(i)+':\autorun.inf');
FileSetAttr(chr(i)+':\setup.exe',0);
DeleteFile(chr(i)+':\setup.exe');
end;
End;
if error<>" then ShowMessage(error);
end;

```

Kitabyň bu böleginde durmuşda has köp düş gelýän bozujy toplumlaryň teswirlenilişi getirildi. Bilkastlaýyn döredilýän näsazlyklaryň islendik zada zeper ýetirip bilýändigini hemmeler bilýär. Şol sebäpli, wirus döredijiler tarapyndan döredilen bozujy toplumlar barada has giň gürrüň edildi.

Operasion sistemada goýberilen bozujy programmalaryň hemmesi wirus bolman, olaryň arasynda troýanlar hem bar. Şol sebäpli, umumylaşdyryp olara bozujy programmalar diýlip kitabyň ýazgysynda bellenildi.

Bu bozujy toplumlary antiwirus programmalaryny ulanman aýyrmak boýunça görkezmeler şekillendirip görkezildi. Bu bölümde ady agzalan daşary ýurt antiwirus programmalaryň köpüsi wirusyň düşmeginiň önüni almakda netijeli işi ýerine ýetirip, wirus kompýutere düşen soň, olar ony kesgitlese hem, köp halatlarda ony doly aýyrmaklygy başarmaýarlar.

Tejribe işleri

1. Reýestri bekleýän programmany düzmeli.
 2. Meseleler dispetçerini bekleýän programmany düzmeli.
 3. Reýestri işledýän programmany düzmeli.
 4. Meseleler dispetçerini işledýän programmany düzmeli.
 5. Islendik prosesi ýok edýän programmany düzmeli.
 6. Islendik faýly ýok edýän programmany düzmeli.
 7. Islendik bukjany ýok edýän programmany düzmeli.
-

PEÝDALANYLAN EDEBIÝATLAR

1. *Gurbanguly Berdimuhamedow*. Garaşsyzlyga guwanmak, Watany, halky söýmek bagtdyr. Aşgabat, 2008.
2. Türkmenistanyň Prezidenti Gurbanguly Berdimuhamedowyň Umumymilli „Galkynyş“ Hereketiniň we Türkmenistanyň Demokratik partiýasynyň nobatdan daşary V gurultaýlarynyň bilelikdäki mejlisinde sözlän sözi. Aşgabat, 2007.
3. *Gurbanguly Berdimuhamedow*. Türkmenistan – sagdynlygyň we ruhubelentligiň ýurdy. Aşgabat, 2009.
4. *Gurbanguly Berdimuhamedow*. Ösüşiň täze belentliklerine tarap. Saýlanan eserler. I tom. Aşgabat, 2008.
5. *Gurbanguly Berdimuhamedow*. Ösüşiň täze belentliklerine tarap. Saýlanan eserler. II tom. Aşgabat, 2009.
6. *Hipson P.* Mastering Windows Xp Registry, SYBEX, 2002
7. Введение в криптографию / Под ред. В.В. Яценко. СПб.: МЦНМО, 2001.
8. *O. Nurgeldiýew, M. Çuriýew*. „Kompýuterde maglumatlary goramak meselesi“, Täze Galkynyşlar we beýik özgertmeler zamansynyň ylmy gadamlary ylmy konferensiýada edilen nutuklaryň gysgaça beýany, 25.04.2009ý., Aşgabat, Ylym. 2009ý. sah 33-35.
9. *Путер Абель*. Ассемблер и программирование для IBM PC. Перевод с английского. Технологический институт Британская Колумбия, 2003.
10. *O. Nurgeldiýew, M. Çuriýew*. „Diskiň logiki gurluşy hem-de kompýuterdäki maglumatlary gizlemek“, Türkmenistanda ylym we tehnika žurnaly. №4, 2008ý., sah 72-78.
11. *Çuriýew M., Komolsew I.* Häzirki wagtda kompýuterdäki maglumatlary goramagyň käbir meseleleri. „Täze Galkynyşlar eýýamynda täze tehnologiýalary önümçilige ornaşdyrmagyň ylmy esaslary“ atly Halkara ylmy maslahatyň nutuklarynyň gysgaça beýany. „Fizika, matematika, nanotehnologiýa, informasion tehnolo-

- logiýalary“ bölümçesi (2009ý. 12-14 iýuny), „Ylym“ neşirýaty, Aşgabat, 2009ý.
- 12.** *Marco Cantu* – Mastering Delphi 7, Sybex, 2003.
- 13.** *I. Komolsew, M. Çuriyew.* Sazlaýjylardan goranmak we kompýuter programmalarynyň goýberilmegini çäklendirmek. „Täze Galkynyş eýýamynyň ylmy we bilim dünýäniň ylym-bilim ulgamynda“ atly halkara ylmy maslahatyň nutuklarynyň gysgaça beýany. „Tehniki ylymlar, täze tehnologiýalar, ylmy barlaglary guramak we dolandyrmak“ bölümçesi (2009ý. 9-11 sentýabr), „Ylym“ neşirýaty, Aşgabat, 2009ý., sah 486-489.
- 14.** *Karl Maria Michael de Leeuw, Jan Bergstra* – The History of Information Security: A Comprehensive Handbook, Elsevier Science, 2007.
- 15.** Реестр Microsoft Windows XP. Справочник профессионала, Джерри Хонейкэтт, М.: Эком, 2003.

MAZMUNY

| | |
|------------|---|
| Giriş..... | 7 |
|------------|---|

I. KRIPTOGRAFIÝA WE MAGLUMATLARY GORAMAK

| | |
|---|----|
| 1.1. Şifrlemegiň esaslary..... | 10 |
| 1.2. Şifrlemegiň görnüşleri | 15 |
| 1.3. Şifrlemegiň işleýşini ýazmaça beýan etmek | 16 |
| 1.4. XOR logiki operatoryny ulanmak bilen şifrlemegi programmirlеме arkaly amala aşyrmak..... | 19 |
| 1.5. Dürli görnüşli programmirlеме dilleri şifrlemegiň bir meselesiniň çözülişiniň üstünden barlag geçirmek..... | 22 |

II. DISKIŇ LOGIKI GURLUŞY HEM-DE MAGLUMATLARY GIZLEMEK

| | |
|---|----|
| 2.1. Diskiň logiki gurluşyny seljermek | 31 |
| 2.2. Faýllaryň diskde ýerleşişiniň düzgünini ulanmak arkaly maglumaty gizlemegiň mümkinçiligine baha bermek..... | 33 |
| 2.3. Maglumaty gizlemek üçin Assemblerde programma düzmek..... | 34 |

III. PAROL GORAGYNYŇ KÄBIR MESELELERI

| | |
|--|----|
| 3.1. Parol simwollarynyň yzygiderligi..... | 39 |
| 3.2. Parol yzygiderligini barlap döwmekligiň esaslary..... | 41 |
| 3.3. Paroly döwmekligi programmirlеме arkaly gurnamagyň häzirki zaman meseleleri..... | 47 |
| 3.4. Programmirlеме dilleriniň deňeşdirilişi | 49 |
| 3.5. Paroly döwmeklige garşy usullary düzmek | 51 |
| 3.6. Parolyň döwürmeginiň önüni alýan programma kody..... | 52 |

IV. KOMPÝUTER PROGRAMMALARYNYŇ GOÝBERILMEGINI ÇÄKLENDIRMEK

| | |
|--|----|
| 4.1. Programmalaryň goýberilişini çäklendirilmeginiň gorag hökmünde seredilmegi | 59 |
|--|----|

| | |
|---|----|
| 4.2. Programmalaryň goýberilişini çäklendirmegi seljermek | 60 |
| 4.3. Programmalaryň goýberilişini programmirlеме arkaly amala aşyrmak | 62 |
| 4.4. Programmirlеме serişdelerine barlag geçirmek | 92 |

V. DEBAGGER-SAZLAÝJYLARDAN GORANMAK

| | |
|--|-----|
| 5.1. OllyDebug sazlaýjynyň mümkinçilikleri | 102 |
| 5.2. OllyDebug sazlaýjyny programmalaryň goragyny döwmekliginde ulanmagyň esaslary | 110 |
| 5.3. Debuggerleri ulanman maşyn kodundaky gizlin maglumatlary kesgitlemek | 113 |
| 5.4. OllyDebug programmasynda programmalaryň seljerilmesiniň mysallary | 121 |
| 5.5. Maşyn koduny debuggerlerden we beýleki hüjümlerden goramak | 126 |

VI. REÝESTR GORAGY ÜPJÜN EDIJI HÖKMÜNDE

| | |
|---|-----|
| 6.1. Reýestriň gurluşy | 142 |
| 6.2. Reýestriň wezipeleri | 144 |
| 6.3. Reýestriň uniwersal häsiýetini barlagdan geçirmek we onuň maglumaty goramagyň usullarynda ulanmagyň mümkinçiligi | 148 |
| 6.4. Reýestriň awtoýükleniş bölümlerini seljeriş hem-de onuň wirus hüjüminiň goldawy hökmünde ulanylmagy | 150 |
| 6.5. Reýestri seljermek arkaly prosesleriň arasyndan we ulgam bukjasyndan wiruslaryň komponentlerini ýok etmek | 155 |

VII. WIRUSLARA WE TROÝANLARA GARŞY GÖREŞ

| | |
|--|-----|
| 7.1. Total Commander faýl menejeriň işi | 162 |
| 7.2. Dürli wiruslaryň işini seljermek we olary aýyrmak boýunça programma gözükdirmeleri döretmek | 166 |
| 7.3. Antitroyan.exe türkmen antiwirus programmasynyň döredilmegi | 188 |
| Peýdalanylan edebiýatlar | 203 |

Maksat Çüriýew

MAGLUMATLARY GORAMAK

Ýokary okuw mekdepleri üçin okuw kitaby

Redaktor

A. Ekiýewa

Surat redaktory

G. Orazmyradow

Tehniki redaktor

O. Nurýagdyýewa

Neşir üçin jogapkär

Ş. Baýramow

Çap etmäğe rugsat edildi 06.12.13. Ölçeği 60x90¹/₁₆.
Edebi garniturasy. Şertli çap listi 13,0. Şertli reňkli ottiski 44,25.
Hasap-neşir listi 9,54. Çap listi 13,0. Sargyt 2717. Sany 1000.

Türkmen döwlet neşirýat gullugy.
744000. Aşgabat, Garaşsyzlyk şaýoly, 100.

Türkmen döwlet neşirýat gullugynyň Metbugat merkezi.
744004. Aşgabat, 1995-nji köçe, 20.