1.1 ինչ է համակարգչային վիրուսը,

Համակարգչային վիրուսը դա մեքենայական ծրագիր է կամ ծրագրի մասնիկ, որը ընկնելով համակարգչի մեջ պատճենում է ինքն իրեն և տարածվում է մի համակարգչից մյուսը՝ վարակը տարածելով ֆայլից ֆայլ և համակարգչից համակարգիչ: Այն կարող է նաև ջնջել կամ վնասել համակարգչային տվյալները՝ առանց ձեր ուղղակի միջամտության կամ գիտության և հակառակ ձեր ցանկության:

Համակարգչային վիրուսների շարքին հաճախ սխալմամբ դասում են բազմաթիվ վնասակար ծրագրային միջոցներ (malicious software-MALWARE), որոնք իրականում վիրուսներ չեն, կարող են ունենալ կամ չունենալ վերարտադրվելու հատկություն և շատ հաճախ կարող են զգալի վնաս հասցնել օգտագործողին և նրա կողմից օգտագործվող համակարգին: Այնուամենայնիվ այս վնասակար ծրագրերը նույնպես դիտարկվում են որպես անցանկալի և դրանք շատ հաճախ դիտվում են վիրուսների հետ մեկ շարքում:

Ծրագրային վնասակար միջոցների թվին են պատկանում՝

- որդերը (WORMS),
- գովազդային՝ օժանդակվող ծրագրային միջոցները (Advertising-supported software-ADWARE),
- հետախուզական՝ գաղտնի ծրագրային միջոցները (Spy Software-SPYWARE),
- դեպի օգտագործողի համակարգիչ չարտոնված մուտքի շնորհման՝ գաղտնի աշխատող ծրագրային միջոցները (Root Kit-ROOTKIT),
- կեղծ անվանումով և օրինական ծրագրի դիմակով աշխատող՝ իրականում ծածուկ վնաս հասցնող ծրագրային միջոցները (Trojan Horse-TROJAN),
- իրականում վնասակար՝ օգտագործողի համակարգչի համար օգտակար ծրագրի դիմակի տակ աշխատող և այդ ,օգտակարությունըե ամեն կերպ խարդախությամբ լավ կողմից ներկայացնող (գովազդող) ծրագրային միջոցները (scaring software- SCAREWARE),
- ինտերնետային հանցագործության համար ստեղծված որևիցե վնասակար ծրագրային միջոց (վիրուս) (crime software-CRIMEWARE):

Համակարգչային վիրուսները կցվում են որևէ ծրագրի կամ ֆայլի դրանց աշխատանքի ժամանակ: Սակայն վիրուսները անպայմանորեն չեն վարակում բոլոր աշխատող ֆայլերը: Շատ հաճախ վիրուսներից շատերը գրվում են միայն մեկ կամ մի քանի տեսակի ֆայլերի համար: Ավելին, վիրուսներից շատերը վարակում են ոչ թե օգտագործողի կողմից ստեղծված, այլև շատ հաճախ՝ հենց համակարգային ֆայլերը: Որքան երկարատև է վիրուսը աշխատում համակարգչում այնքան ավելի ու ավելի շատ ֆայլեր է այն վարակում: Տարածվելով մի ֆայլից մյուսին, և համապատասխան պահի սպասելով, վարակը կարող է կցվել էլեկտրոնային նամակին կամ վարակելով ցանցային ֆայլային համակարգը անցնել ցանցի ներսում գտնվող հաջորդ համակարգչին:

1.Ինչ է համակարգչային վիրուսը_____

_____

_____

2.Թվարկել այլ վնասակար
միջոցներ_____

_____
_____
_____

1.2 վիրուսների հիմնական հատկությունները

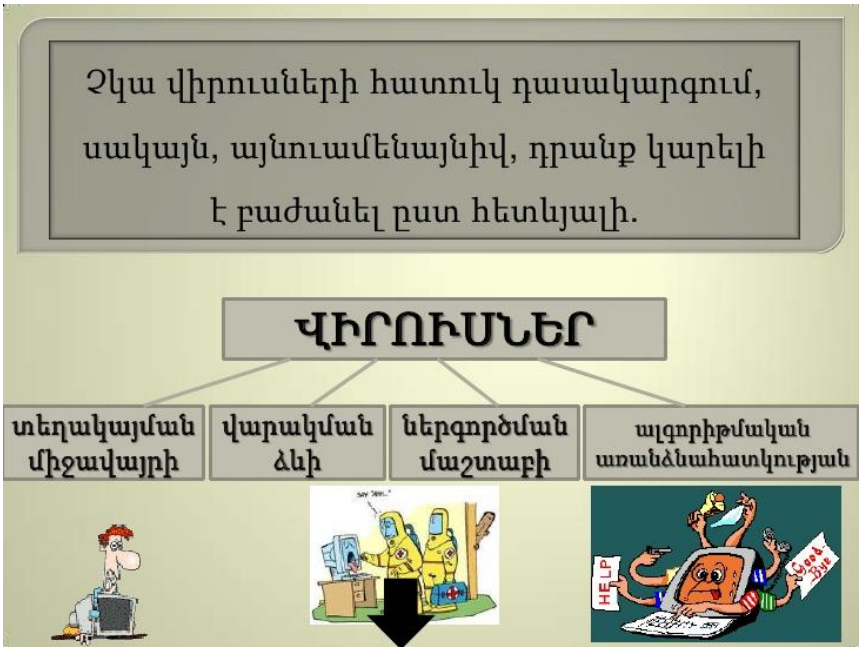
Վիրոսով վարակված ֆայլի ակտիվացման ժամանակ ղեկավարումը միանգամից փոխանցվում է վիրուսին, որը կատարում է իր ավերիչ գործողությունները, նաև զուգահեռ կցվում է այլ ծրագրերին և ֆայլերին։ Այնուհետև տեխնոլոգիապես կատարվում է հետադարձ այն գործողություններին, որոնք կատարվել են համակարգչի վրա։ Համակարգչի բարձր և արագ գործողության ժամանակ նմանատիպ շեղումը օգտագործողի համար մնում է աննկատ։ Հասցված վնասը կարող է նկատվել ոչ միանգամից։ Վիրուսի ներկայության արտաքին դրսևորումները համակարգչի մեջ կարող են լինել ամենատարբեր տեսակների.

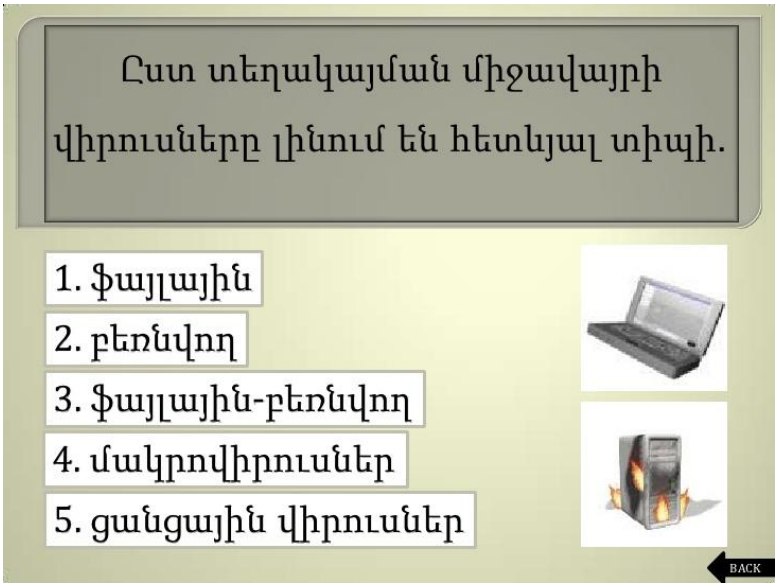
- էկրանի մարում
- չնախատեսված հաղորդագրության հայտնվումը էկրանի վրա
- չնախատեսված պահանջ՝ ձայնագրության սկավառակից հանել պաշտապանությունը
- վարակված ֆայլերի ստեղծման ժամանակի և ամսաթվի փոփոխություն
- էկրանի վրայից տառերի կորչելը (երբեմն երաժշտության ուղեկցությամբ)
- որոշ ծրագրային ֆայլերի անհետացում ուրբաթ օրերին որոնք ընկնում են ամսի 13-ին
- աշխատանքի անսովոր վթարային ավարտ
- տեղեկատվական ֆայլեր կործանում կամ մասնակի վնասում
- համակարգչի աշխատանքի դանդաղեցում
- ստեղմանաշարից ներմուծման արգելափակում
- սիմվոլների շրջում էկրանի վրա
- տվյալների գրանցման արգելափակում կոշտ սկավառակի վրա
- համակարգչի վարքի դրսևորման այլ անսովոր ձևեր

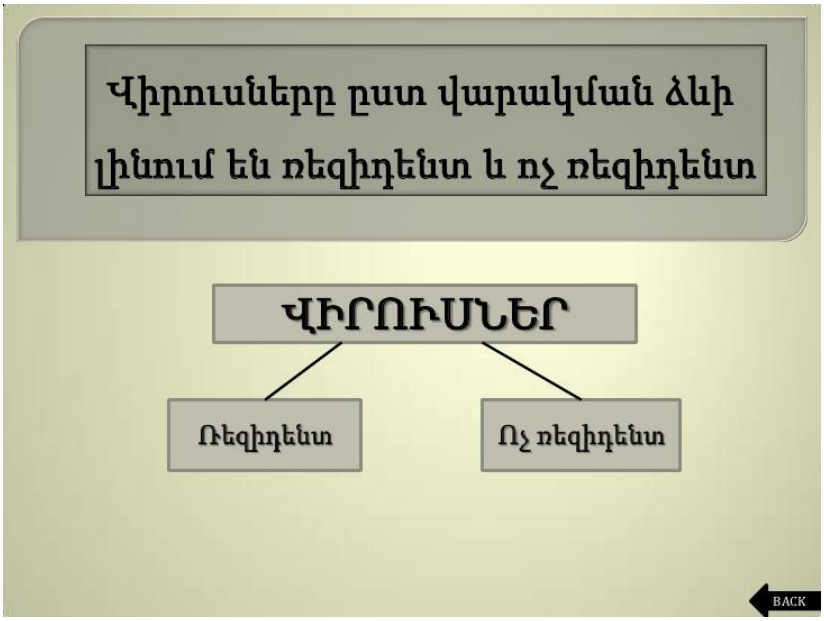
1.Թվարկել վիրուսների հիմնական հատկությունները
_____

_____
_____
_____
_____
_____
_____

1.3 Վիրուսների դասակարգումը

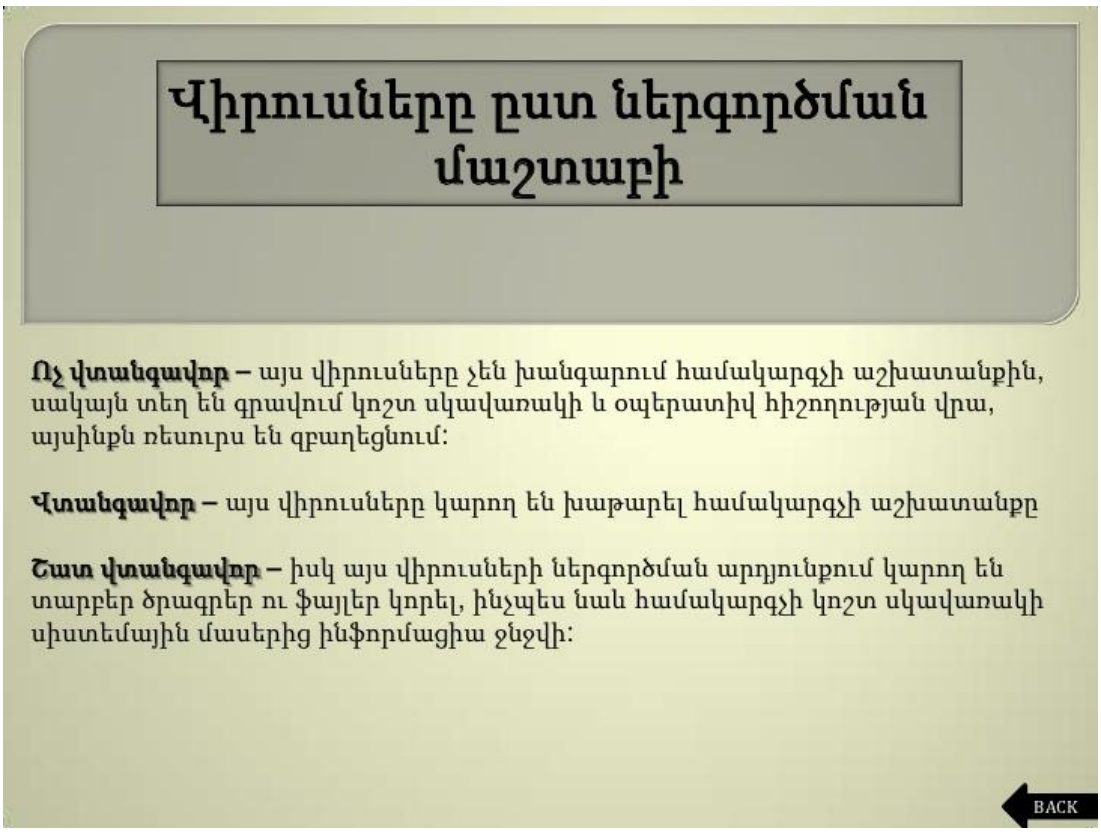


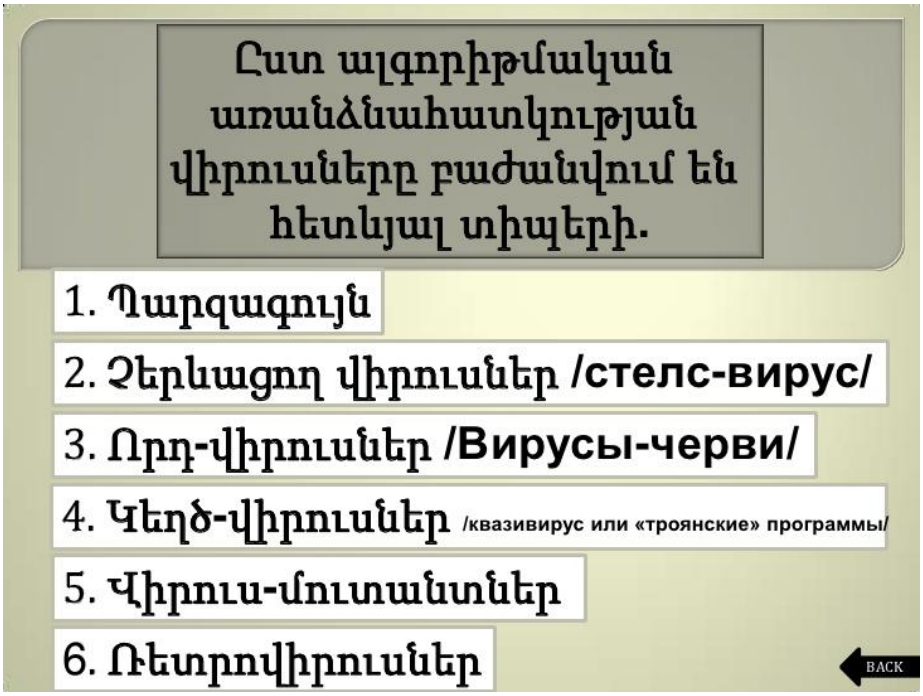




Ռեզիդենտ վիրուսները համակարգչի վարակման ժամանակ թողնում են իրենց ռեզիդենտ մասը օպերատիվ հիշողության մեջ: Այս վիրուսները կարող են ակտիվ մնալ մինչև համակարգչի անջատումը կամ վերաբեռնավորումը:

Ոչ ռեզիդենտ վիրուսները համակարգչի վարակման ժամանակ չեն թողնում իրենց ռեզիդենտ մասը օպերատիվ հիշողության մեջ: Որոշ վիրուսներ թողնում են հատվածներ հիշողության մեջ, որոնք հետագայում ընդունակ չեն բազմանալու:





1. Ավարտել նախադասությունը՝ ընտրելով տարբերակներից մեկը:
   1.1. Համակարգչային վիրուսների հիմնական տիպերն են_____
   a. Սարքային, ծրագրային, բեռնավորվող
   b. Ֆայլային, բեռնավորվող, մակրովիրուսներ, ցանցային
   c. Ֆայլային, ծրագրային, մակրովիրուսներ
   1.2. Վիրուսները դասակարգվում են ըստ_____
   d. տեղակայման միջավայրի, առանձնահատկության, տեղակայման մասշտաբի
   e. ներգործման մասշտաբի, վարակման ձևի, տարածման արագության
   f. Վարակման ձևի, տեղակայման միջավայրի, ալգորիթմական առանձնահատկության, ներգործման մասշտաբի
2. Ավարտել նախադասությունները՝

Վիրուսներն ըստ վարակման ձևի լինում են_____

_____

Վիրուսներն ըստ ներգործման աստիճանի լինում են_____

_____

1.4 Վիրուսով վարակվելու ճանապարհները

Համակարգչի մեջ վիրուսի ներթափանցման ճանապարհները

Համակարգչի մեջ վիրուսի ներթափանցման հիմնական ճանապարհներն.

- տարբեր տեսակի ինֆորմացիայի կրիչների՝ CD դիսկերի, USB ֆլեշների, դիսկետաների և այլ կրիչներով
- համակարգչային ցանցերի միջոցով
- այլ միջոցներով

Վիրուսների տարածումը արգելափակում են նաև այսպես կոչված միջնապատերը՝ Firewall: Դրանք հատուկ ծրագրեր են, որոնք անհրաժեշտության դեպքում արգելափակում են տարբեր «կասկածելի» ծրագրերի աշխատանքը՝ թույլ չտալով դրանց կասկածելի գործողությունները:

Վիրուսի ներթափանցման նշանները

- Մինչ այդ նորմալ աշխատող ծրագրի ոչ ճիշտ աշխատանքը, կամ աշխատանքի դադարումը
- Համակարգչի դանդաղ աշխատանքը
- Օպերացիոն համակարգերի աշխատանքի խաթարումը
- Ֆայլերի ու կատալոգների անհայտացումը, կամ դրանց պարունակության աղավաղումը
- Ֆայլերի մոդիֆիկացիաների ամսաթվի և ժամանակի փոփոխությունը
- Ֆայլերի չափերի փոփոխությունը
- Ֆայլերի քանակի անսպասելի շատացումը սկավառակի վրա
- Ազատ օպերատիվ հիշողության չափի էական փոքրացումը
- Էկրանին չնախատեսված հաղորդագրությունների և նկարների հայտնվելը
- Չնախատեսված ձայնային ազդանշանների առկայությունը
- Համակարգչի հաճախակի կախվելը
- և այլն

1.Լրացնել բաց թողած բառերը

1. Համակարգիչը վարակելուց հետո՝ վիրուսը կարող է »_____« ու »հարձակման անցնել«
   որոշակի իրադարձությունից հետո միայն:
2. Վիրուսի հիմնական աղբյուր կարող է հանդիսանալ օպերացիոն _____ում թաքնված
   վիրուսը:
3. Վիրուսով վարակված լինելու մասին կարող են վկայել ազատ օպերատիվ հիշողության ծավալի _____ը:
4. Վիրուսի հիմնական_____ կարող է հանդիսանալ վիրուսակիր սկավառակը:

2.Ընտրել ճիշտ պատասխանները: Վիրուսների ներթափանցման նշաններ են հանդիսանում.

1. Համակարգչի հաճախակի կախումը
2. Ազատ հիշողության տարածքի փոքրացումը
3. Ֆայլերի քանակի զգալի ավելացումը
4. Համակարգչի դանդաղ աշխատանքը
5. Հակավիրուսային ծրագրի բացակայությունը

1.5 Վիրուսով վարակման ենթակա հիմնական ֆայլերի ընդլայնումները,

Համակարգչային վիրուսները իրարից տարբերվում են նրանով, թե ինչպիսի օբյեկտներում են նրանք տեղավորվում, այսինքն ինչ են վարակում: Որոշ վիրուսներ կարող են վարակել միանգամից մի քանի օբյեկտներ: Վիրուսների մեծամասնությունը տարածվում են վարակելով կատարողական ֆայլերը՝ ֆայլեր որոնք ունեն exe և com ընդլայնումներ: Այս վիրուսները կոչվում են ֆայլային: Վիրուսը, որը գտնվում վարակված կատարողական ֆայլերում, սկսում է իր աշխատանքը այն ծրագրի բեռնման ժամանակ, որում գտնվում է ինքը: Մեկ այլ վիրուսների տարածված տեսակ, որը ներխուժում կոշտ սկավառակի սկզբնական սեկտոր, որտեղ գտնվում է օպերացիոն համակարգը բեռնող ծրագիրը: Այսպիսի վիրուսները կոչվում են բեռնային վիրուսներ: Այս վիրուսները սկսում են իրենց աշխատանքը համակարգչի բեռնման ժամանակ: Բեռնային վիրուսները համարվում են ռեզիդենտ և վարակում են համակարգչի մեջ տեղակայված սկավառակները: Որոշ վիրուսներ կարողանում են վարակել դրայվերներ: Դրայվերում գտնվող վիրուսը սկում է իր աշխատանքը տվյալ դրայվերի բեռնման (CONFIG.SYS ֆայլից) ժամանակ: Սովորաբար վիրուսները, որոնք վարակում են դրայվերները վարակում են նաև կատարողական ֆայլերը, քանի որ այլ կերպ այդ վիրուսները չէին կարողանա տարածվել: Շատ հազվադեպ են հանդիպում վիրուսներ, որոնք վարակում են համակարգային DOS ֆայլերը (IO. SYS կամ MSDOS.SYS): Սովորաբար այդպիսի վիրուսները վարակում են նաև սկավառակի բեռնման սեկտորները, քանի որ այլ կերպ նրանց չի հաջողվի տարածվել: Հազվադեպ են հանդիպում վիրուսներ, որոնք վարակում են հրամանային ֆայլերը: Սովորաբար այդպիսի վիրուսները

հրամանային ֆայլի հրամանների միջոցով ձևակերպում են սկավառակի վրա կատարող ֆայլ, բաց են թողնում այն, այնուհետև տեղի է ունենում վիրուսների բազմացումն ու տարածումը, որից հետո ֆայլը մաքրվում է սկավառակից: Այս վիրուսները սկսում են իրենց աշխատանքը հրամանային ֆայլի կատարման ժամանակ, որտեղ նրանք գտնվում են: Վիրուսը իրենից ներկայացնում է ծրագիր, այդ պատճառով օբյեկտները, որոնք ծրագրային կոդ չեն պարունակում, չեն կարող վարակվել վիրուսով: Այդպիսի օբյեկտները կարող են միայն վրուսների հետևանքով փչանալ: Այդպիսի օբյեկտների թվում են պատկանում հասարակ խմբագիր-ծրագրերի կողմից ստեղծված փաստաթղթերը և տվյալների բազաների ֆայլերը:

Ընտրել ճիշտ տարբերակները.

1. Որ ֆայլերը կարող են վարակվել վիրուսով
    1. Գրաֆիկական
    2. Ծրագրերը և փաստաթղթերը
    3. Ձայնային ֆայլերը
    4. Տեսաֆայլերը
2. Վիրուսի հիմնական աղբյուր չի կարող հանդիսանալ
    - վիրուսակիր ֆայլ պարունակող սկավառակը,
    - վիրուսով վարակված կոշտ սկավառակը,
    - նոր տեղադրված մոդեմը:
3. Վիրուսով վարակման ենթակա հիմնական ֆայլերի ընդլայնումներն են

    _____

    _____

    _____

1.6 Համակարգչային վիրուսների տարածման ձևերը:

Եթե համակարգիչների զարգացման սկզբնական շրջանում վիրուսները տարածվում էին սկավառակների միջոցով, ապա այսօր սկավառակներին փոխարինում է Էլեկտրոնային փոստը: Ամեն օր էլեկտրոնային փոստի միջոցով փոխանցվում է միլիոնավոր հաղորդագրություններ, որոնց մեծ մասը վարակված է վիրուսով: Ցավոք էլեկտրոնային հաղորդագրություններում ներդրված ֆայլերը նաև կարող են շատ վտանգավոր լինել համակարգիչների համար: Ինչու՞մ է կայանում ներդրված ֆայլերի վտանգը: Այդպիսի ֆայլի փոխարեն օգտագործողին կարող են ուղարկել վիրուս կամ Տրոյան ծրագիր, երբեմն Microsoft Office ծրագրերով ստեղծված փաստաթուղթ (*.doc, *.xls), վարակված համակարգչային վիրուսով: Բաց թողնելով ստացված ծրագիրը կատարման համար, օգտագործողը կարող է սկզբնայնացնել վիրուսը, կամ ակտիվացնել համակարգչում Տրոյան ծրագիրը: Դեռ ավելին փոստային ծրագրի ոչ ճիշտ կարգավորումից կամ նրանում եղած սխալներից, ներդրված ֆայլերը կարող են մեխանիկորեն բացվել ստացված նամակները ընթերցելիս: Այս դեպքում, եթե չձեռնարկել ոչ մի պաշտպանողական միջոց, ապա վիրուսների ներխուժումը համակարգիչ ժամանակի գործ է: Հնարավոր են վիրուսների ներխուժման այլ փորձեր համակարգիչ էլեկտրոնային փոստի միջոցով: Օրինակ կարող են ուղարկել հաղորդագրություններ HTML տեսքով, որում ներդրված լինի ActiveX ղեկավարման տրոյան էլեմենտը: Բացելով այդպիսի հաղորդագրություն դուք կարող եք բեռնել այդ էլեմենտը ձեր համակարգիչ, որից հետո նա դանդաղորեն սկսում է կատարել իր ՙչար՚ գործը:

Ընտրել ճիշտ պատասխանը կամ պատասխանները

1. Վիրուսի համակարգիչ ներթափանցման հիմնական ճանապարհներն են
    1. Ճկուն սկավառակները
    2. Համակարգչային ցանցերը
    3. Հիվանդ օգտվողը
    4. Word-ում և Excel-ում ստեղծված ֆայլերը
2. Համակարգիչը վիրուսով կարող է վարակվել հետևյալ գործընթացում.
    1. Սկավառակի ֆորմատավորման ժամանակ
    2. Ֆայլերի հետ աշխատելու ժամանակ
    3. Համակարգչի անջատման ժամանակ
    4. Պրինտերով տպելու ժամանակ

1.7 Վիրուսների դեմ պայքարի պրոֆիլակտիկ միջոցառումներ

Հիմնականում օգտագործողի համար վտանգավոր է համարվում վիրուսի այն գործողությունը, ինչպիսին է կոշտ սկավառակի ֆորմատավորումը, որը բերում է կոշտ սկավառակի վրա պահպանվող ինֆոմացիայի կորստի: Քանի որ վիրուսի ներխուժումից ոչ մի օգտագործողի համակարգիչ ապահովված չէ, հետևաբար վիրուսների կողմից հասցվող վնասները նվազագույնի հասցնելու համար անհրաժեշտ է պահպանել մի քանի հասարակ կանոններ:

1. Ամեն մի սկավառակ, եթե այն եղել է այլ համակարգչի վրա, անհրաժեշտ է ստուգել կամայական հակավիրուս ծրագրով: Այդպիսի ծրագրերը կարող են ոչ միայն հայտնաբերել վիրուսը այլ նաև կարող են բուժել սկավառակը: Հատկապես վերաբերվում է խաղային ծրագրերին, քանի որ վիրուսների մեծ մասը տարածվում են հենց խաղերի միջոցով:
2. Նմանատիպ ստուգումները անհրաժեշտ է կատարել այն ֆայլերի համար, որոնք գալիս են ցանցի միջոցով:
3. Հակավիրուսային ծրագիրը շատ արագ ծերանում է: դրա համար խորհուրդ է տրվում հաճախակիորեն այն թարմացնել նոր տարբերակով: Սովորաբար այդպիսի թարմացումները տևում են մեկ շաբաթից մինչ երեք ամիս:
4. Վիրուսի բացահայտման ժամանակ պետք չէ կատարել չմտածված գործողություններ քանի որ դա կարող է բերել այնպիսի ինֆորմացիայի կորստի, որը դեռ կարելի է փրկել: Այդ ժամանակ ամենից ճիշտ է անջատել համակարգիչը, որպեսզի կանգնեցվի վիրուսի գործունեությունը: Այնուհետև բեռնել համակարգիչը օպերացիոն համակարգի էտալոնային սկավառակից: Որից հետո պետք է բաց թողնել հակավիրուսային ծրագիրը: Եթե ամեն ինչ ճիշտ է կատարվել, ապա հակավիրուսային ծրագիրը օգտագործողին տեղեկացնում է համակարգչից վիրուսների բացակայման մասին:

Վերջին շրջանում ցանցում աշխատելիս հատկապես էլեկտրոնային փոստից օգտվելիս, հաճախակի են դարձել վիրուսների ներխուժումը համակարգիչ փոստային հաղորդագրությունների միջոցով: Այդ պատճառով այստեղ նույնպես անհրաժեշտ է պահպանել մի քանի հասարակ կանոններ.

1. Նամակներին կպած ֆայլերը պետք չէ բացել, եթե չգիտես թե ումից է ուղարկված և ինչ է պարունակում։
2. Նամակներին կպած ֆայլերը պետք չէ բացել, որոնք ուղարկված են հակավիրուսային լաբորատորիաներից։ Լաբորատորիաները երբեք ֆայլեր չեն ուղարկում։
3. Նամակներին կպած ֆայլերը պետք չէ բացել, եթե նամակի թեման և ինքը նամակը դատարկ են։
4. Ոչնչացնել բոլոր կասկածելի ֆայլերը:

Թվարկել վիրուսների դեմ պայքարի մի քանի միջոցառում

1. _____
2. _____
3. _____
4. _____
5. _____

Ընտրել ճիշտ տարբերակը: Վիրուսի հիմնական աղբյուր չի կարող հանդիսանալ

1. վիրուսակիր ֆայլ պարունակող սկավառակը,
2. վիրուսով վարակված կոշտ սկավառակը,
3. նոր տեղադրված մոդեմը:

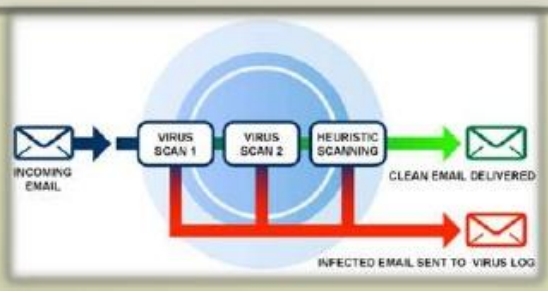
1.8 Համակարգչային վիրուսների տարածման դեմ պայքարի եղանակները:

Համակարգչային վիրուսներից հասցրած վնասներից պաշտպանվելու մեթոդները

- Ինֆորմացիայի ոչնչացումը – այսինքն ֆայլերի պատճենների պահպանումը
- Պատահական և անծանոթ ծրագրերի օգտագործումից խուսափելը
- Եթե մինչ այդ ուրիշ մարդիկ էին աշխատում տվյալ համակարգչով, ապա համակարգչի վերաբեռնավորումից խուսափելը
- Նոր ստացած ֆայլերի պարտադիր ստուգումը
- Լոկալ դիսկերի և ֆայլերի պարբերաբար ստուգումը
- Անջատել տարբեր կրիչների ինքնաբեռնավորման ռեժիմը
- Ուրիշից ստացված Word –ի կամ նմանատիպ ֆայլերը բացելիս նպատակահարմար է սեղմած պահել [Shift] կոճակը: Այդ ժամանակ ոչ մի վիրուս էլ չի աշխատի:
- և այլն

ՀԱԿԱՎԻՐՈՒՍԱՅԻՆ ԾՐԱԳՐԵՐ

Հակավիրուսները վիրուսներից պաշտպանվելու համար գրված հատուկ ծրագրեր են, որոնց նպատակն է հայտնաբերել վիրուսը, բուժել վարակված ֆայլերն ու դիսկերը, հայտնաբերել և կանխել վիրուսներին հատուկ կասկածելի գործողությունները:



1.Թվարկել համակարգչային վիրուսների դեմ պայքարի մի քանի եղանակ_____

_____
_____
_____
_____
_____

2.1 Հակավիրուսային ծրագրեր

Ներկայումս վիրուսակիր ծրագրերի դեմ հակավիրուսային ծրագրեր կան, որոնք հնարավորություն են տալիս ստուգել վիրուսի առկայությունը, հայտնաբերել վարակված ֆայլերը, վերականգնել («բուժել») դրանք: Եթե վիրուսով վարակված ֆայլը վիրուսի կողմից այնպիսի փոփոխությունների է ենթարկվել, որ հնարավոր չէ վերականգնել, ապա համակարգչից օգտվողի ցուցումով դրանք կարող են ջնջվել:
Dr.Web, NOD32, Norton AntiVirus, Kaspersky Anti-Virus, Avast ծրագրերը ներկայումս լայնորեն կիրառվող հակավիրուսային միջոցներից են: Dr.Web-ը լայնորեն տարածված հակավիրուսային ծրագիր է, որը ունակ է բարձր հավանականությամբ բացահայտել նույնիսկ անհայտ վիրուսները:
NOD32-ը շատ արագ աշխատող հակավիրուսային ծրագիր է, որն արդյունավետ կերպով համակարգիչը պաշտպանում է հնարավոր վիրուսներից և, այսպես կոչված՝ «լրտեսական» ծրագրերից: Վերջիններս այնպիսի ծրագրեր են, որոնք հաճախ գովազդային ծրագրերի տեսքով Ինտերնետային ցանցով մուտք գործելով համակարգիչ՝ թաքնված կերպով տարատեսակ տեղեկություններ են հավաքում և ուղարկում տվյալ ծրագրերի տերերին: NOD32-ը միակ հակավիրուսային ծրագիրն է, որը վերջին 7 տարիներին գործարկելիս բացահայտել է *բոլոր* վիրուսները:
Norton Antivirus-ը նույնպես աշխարհում ամենակիրառվող հակավիրուսային միջոցներից է: Այս ծրագիրը գտնում և ոչնչացնում է վիրուսները, ավտոմատ կերպով մեկուսացնում է «լրտես» ծրագրերը, չի թույլատրում «վարակված» նամակներ տարածել, բացահայտում է օպերացիոն համակարգում թաքնված «սպառնալիքները», պաշտպանում համակարգիչը ինտերնետային «որդերից». ինտերնետային «որդերը» վիրուսակիր ծրագրեր են, որոնք իրենց պատճենները
տարածում են լոկալ կամ ինտերնետային ցանցերի միջոցով:
Kaspersky Anti-Virus-ը նույնպես ամենատարածվածներից է: Կիրառվող հատուկ մշակված ալգորիթմի շնորհիվ այս ծրագիրը նույնպես անսխալ կողմնորոշվում է վիրուսներ ախտորոշելիս, ընդ որում՝ ի հայտ է բերում անգամ դեռևս անհայտ նոր վիրուսները: Ծրագիրը կարողանում է «բռնել» նաև այնպիսի վիրուսներ, որոնք ներդրվում են Microsoft Office-ի փաստաթղթերում:

1.Նշվածներից ո՞ր ծրագրերն են հակավիրուսային
1. AVP, DrWeb, Norton AntiVirus.
2. MS-DOS, MS Word, AVP.
3. MS Word, MS Excel, Norton Commander.

2. Համակարգչային վիրուսը ……
1. Հատուկ ծրագիր է, որն ունակ է բազմանալու
2. Սկավառակների ստուգման միջոց է
3. Վիրուսներին հետևելու ծրագիր է
4. Ֆայլ է, որը թողարկման ժամանակ վարակում է մյուսներին

3.Ինչի վրա է հիմնված հակավիրուսային ծրագրի աշխատանքը.

1. Վիրուսով հարձակմանը սկզբին սպասելու
2. Ծրագրային կոդը հայտնի վիրուսների հետ համեմատելու
3. Վարակված ֆայլերը հեռացնելու

2.2 Հակավիրուսային ծրագրի տեղադրում (scan)

Այժմ մանրամասն ուսումնասիրենք Avast հակավիրուսային ծրագրի աշխատանքը: Avast-ը կարողանում է գտնել ինչպես համակարգչի կոշտ սկավառակի վրա, այնպես էլ հիշողության մեջ և սկավառակի բեռնավորիչ սեկտորներում եղած վիրուսները: Այս ծրագիրը ավտոմատ կերպով ստուգում է ստացված նամակները:
Avast-ի լավ հատկություններից է նաև այն, որ դրա թարմ տարբերակները կարելի է ստանալ Ինտերնետի միջոցով՝ ավտոմատ: Ընդ որում՝ այս ծրագիրն ունի պարզ ու հասկանալի երկխոսային համակարգ և կիրառման մատչելի եղանակ:
Avast-ը գործարկվում է երկու եղանակով՝ Home Edition – մասնավոր օգտագործման նպատակով՝ անվճար, և Profesional Edition – կազմակերպությունների համար՝ վճարովի:
Avast հակավիրուսային ծրագիրը տեղադրելով համակարգչի վրա՝ օգտագործողը ազատվում է լրացուցիչ այլ հակավիրուսային միջոցներ օգտագործելու անհրաժեշտությունից:
Avast հակավիրուսային ծրագիրը համակարգչին տեղադրելու համար նախ այցելեք http://abast.ru կայքը, ծանոթացեք ծրագրի առանձնահատկություններին, ապա http://abast.ru/Free_Avast_home_edition_download.htm էջից բեռնավորեք setuprus.exe ֆայլը: Սրանից հետո Avast-ը կառաջարկի համակարգիչը վերաբեռնավորել, որի ընթացքում ծրագիրը կստուգի համակարգչի ողջ համակարգը:

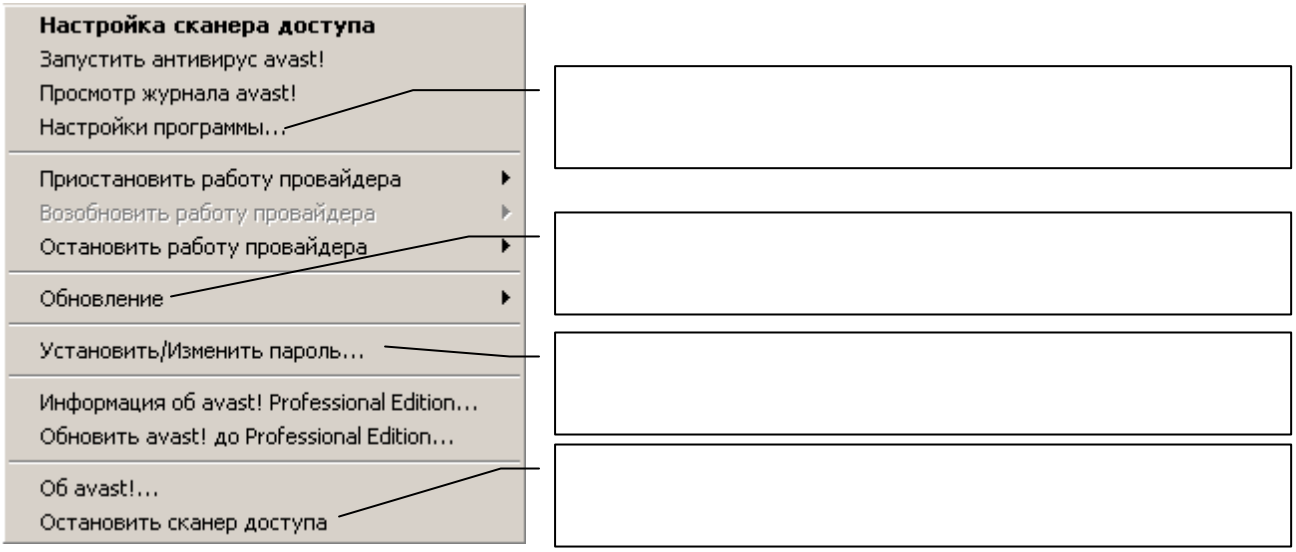
Պատասխանել հարցերին

4. Ինչ հակավիրուսային ծրագրեր գիտեք_____
   _____
   _____
5. Ինչ եղանակներով կարելի է տեղադրել հակավիրուսային ծրագիրը_____
   _____
   _____
6. Ինչ եղանակներով է գործարկվում Avast-ը_____
   _____
   _____

2.3 Հակավիրուսային ծրագրի կառավարման ենթատեքստային մենյու

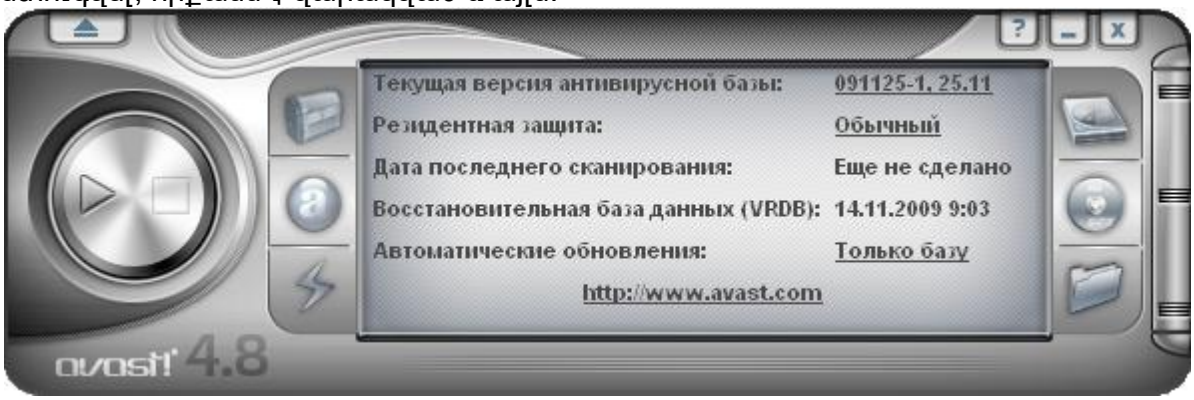
Համակարգչի բեռնավորումից հետո էկրանի ներքին աջ անկյունում (ժամացույցի մոտ) հայտնվում է տարբերանշանը: Եթե այն պտտվում է, ապա դա վկայում է այն մասին, որ համակարգիչը պաշտպանության տակ է: Այդ տարբերանշանի տիրույթում մկնիկի աջ սեղմակով բացված ենթատեքստային մենյուի միջոցով կարելի է կառավարել հակավիրուսային ծրագրի աշխատանքը՝ աշխատեցնել Avast հակավիրուսային ծրագիրը՝ *ԻՈտցրՅՈՅՖ ...*, ժամանակավորապես դադարեցնել ու անհրաժեշտության դեպքում նորից թողարկել հակավիրուսային ծրագրի բաղադրիչ տարրերից ցանկացածը՝ *ԿՐՈՏրՅՈվՏՉՈՅՖ ...*, սահմանել ծրագրի աշխատանքային ռեժիմները՝ ԾՈրՑՐՏռՍՈ տՐՏչՐՈՎՎo ..., զանազան տեղեկություններ ստանալ ծրագրի մասին՝ *Կո ՈՉՈրՅ* և այլն:

Լրացնել վանդակները



2.4 Հակավիրուսային ծրագրի թողարկում

ԻՈտցրՑՈՑՖ ՈվՑՈՉՈՐցր ... հրամանն ընտրելիս նախ իրականացվում է բեռնավորված ծրագրերի և հիշողության ստուգում, որից հետո համակարգը ներկայացնում է հակավիրուսային ծրագրի երկխոսային պատուհանը (նկ.2), որտեղ կարելի է ընտրել ստուգման ենթակա օբյեկտը, ստուգելու եղանակն ու տեսնել ստուգման արդյունքը՝ որքանն է ստուգվել, որքանն է վարակված և այլն:



(նկ.2), Վիրուսների ստուգման երկխոսային պատուհան

Վիրուս հայտնաբերելու գործընթացն սկսելուց առաջ նախ պետք է երկխոսային պատուհանի աջ մասում եղած կոճակների օգնությամբ ընտրել ստուգման ենթակա տեղամասը:
Համակարգչի կոշտ սկավառակները ստուգելու համար անհրաժեշտ է ընտրել (*ԽՏՍՈաՖվօպ ՊՈրՍՈ*) կոճակը:
Ճկուն սկավառակների և CD դիսկետի պարունակությունները ստուգելու նպատակով պետք է ընտրել (*ԻՎպվվօպ վՏրՈՑպսՈ*) կոճակը:
Բացատրել վիրուսների ստուգման երկխոսական պատուհանի կառուցվածքը_____

_____

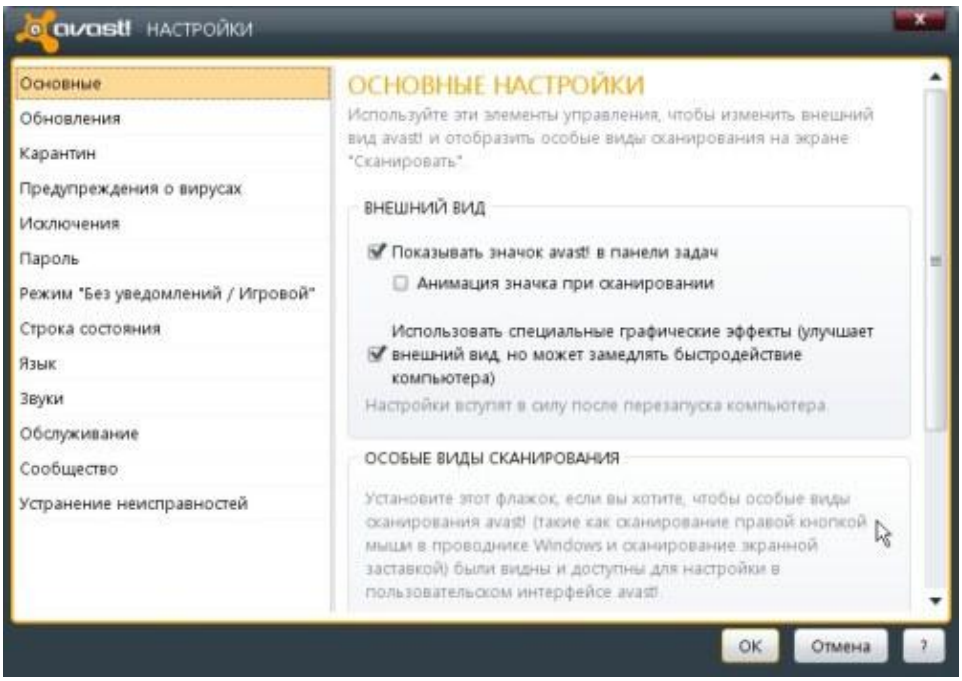
_____

_____

_____

_____

2.5 Հակավիրուսային ծրագրի կարգաբերում



Այս պատուհանում տեղադրված են ծրագրի արտաքին տեսքի ղեկավարման էլեմենտները:.

Գրել ղեկավարման էլեմենտների նշանակությունը

Внешний вид

- "Показывать значок avast! в панели задач" – _____
  _____

- "Анимация значка при сканировании" – _____
  _____

- "Использовать специальные графические эффекты" –_____
  _____

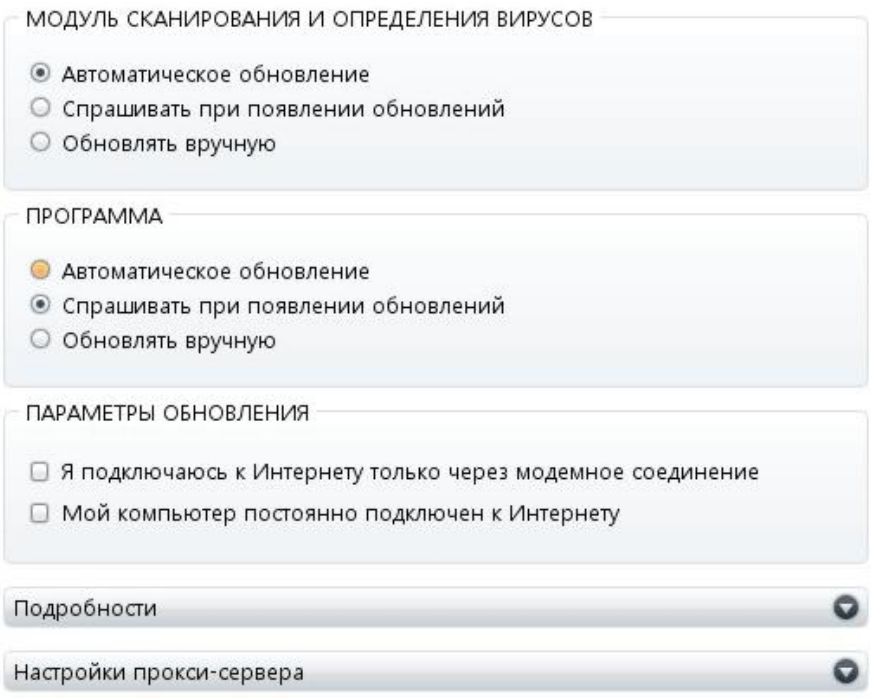
Եթե տեղադրված է Показывать особые виды сканирования в пользовательском интерфейсе avast!" նշիչը, ապա այս ստուգումները կհայտնվեն ստանդարտ ստուգումների ցուցակում

- Автоматически открывать результаты сканирования после его завершения նշիչը երբ տեղադրված է, ապա ստուգումից հետո ավտոմատ կբացվի ստուգման արդյունքներ պատուհանը:

2.6 Թարմացնել արդեն տեղադրված հակավիրուսային ծրագիրը

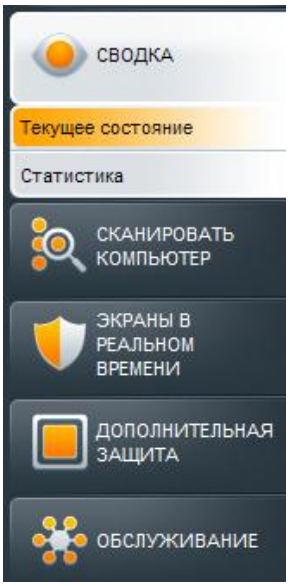
Հակավիրուսային ծրագիրն ունի թարմացման հնարավորություն, որը կարելի է կարգաբերել: Մենք կարող ենք տեղադրել ավտոմատ թարմացում, թարմացում ձեռքով, կամ անհրաժեշտության դեպքում:

Գրել թարմացման պարամետրերը



2.7 Կատարել վիրուսով վարակված օբյեկտի զննում

Հակավիրուսային ծրագրի երկխոսական պատուհանի ձախ մասում ուղղաձիգ դասավորությամբ գտնվում է գլխավոր ընտրացուցակը խոշոր կոճակներով:



Сводка. Այստեղ հավաքված է ծրագրի կոմպոնենտների հիմնական ինֆորմացիան և վիճակագրությունը:

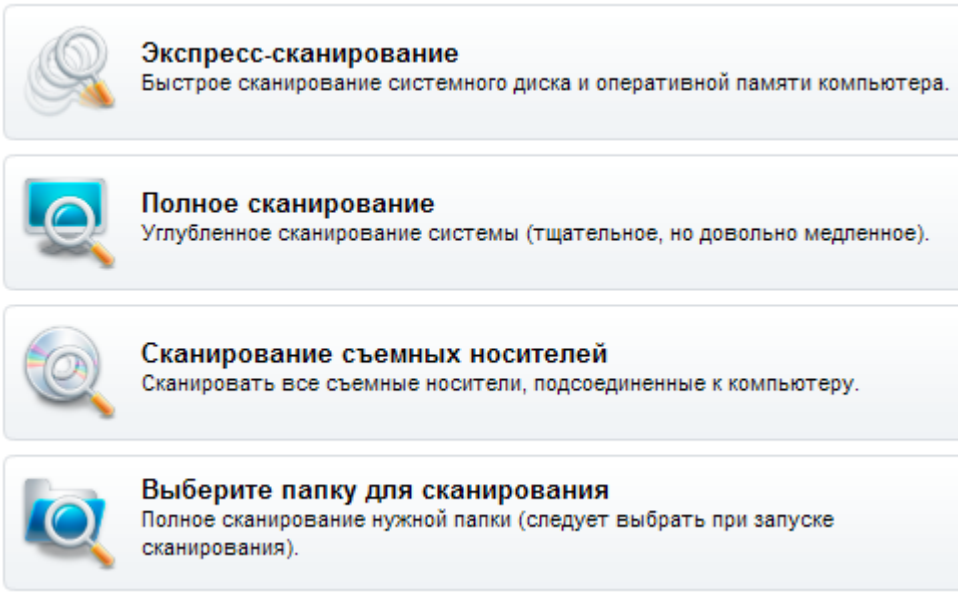
Сканировать компьютер. Վիրուսների ստուգման տարբերակները. Հենց հիմա, համակարգչի բեռնավորումից հետո, ինչպես նաև նախորդ ստուգումների արդյունքները:

Экраны в реальном времени. Այստեղից կարելի է թողարկել տարբեր գործընթացների պաշտպանությունը:

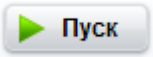
Дополнительная защита. Լրացուցիչ պաշտպանություն:

Համակարգիչը ստուգելու համար կատարել հետևյալ քայլերը.

Գլխավոր ընտրացուցակում ընտրել "Сканировать компьютер" կոճակը, որից հետո ծրագիրը կառաջարկի 4 տարբերակներ

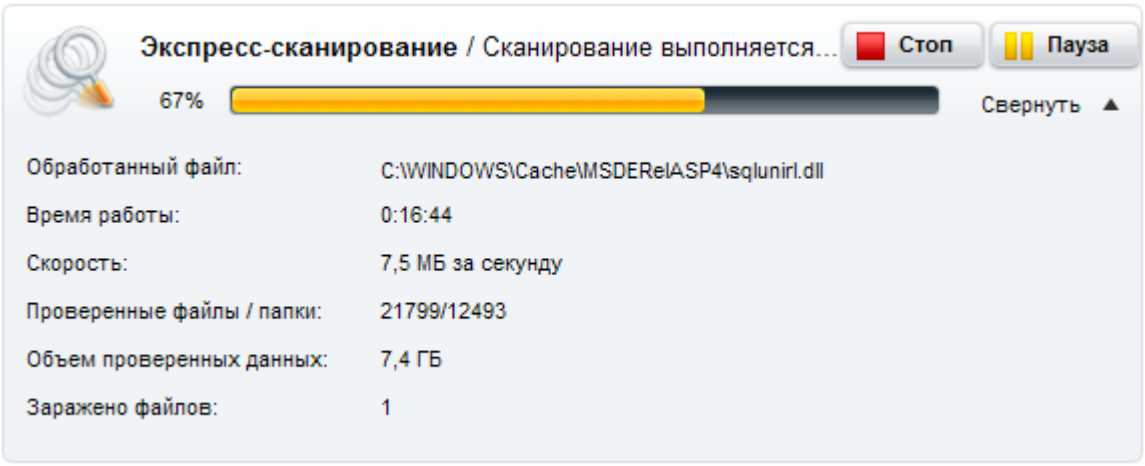


- **Экспресс-сканирование.** Համակարգի արագ ստուգում
- **Полное сканирование.** Բոլոր ֆայլերի ստուգում
- **Сканирование съемных носителей.** Արտաքին կրիչների ստուգում
- **Выберите папку для сканирования.** Թղթապանակների ստուգում

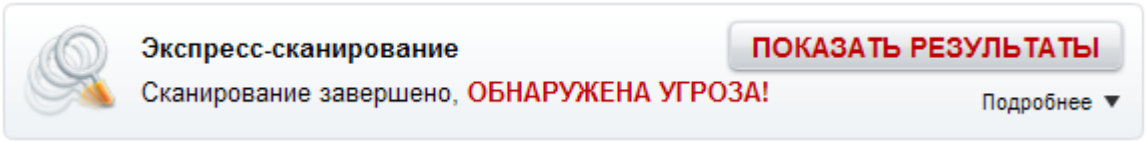
Ընտրություն կատարելուց հետո սեղմել 

կոճակը:

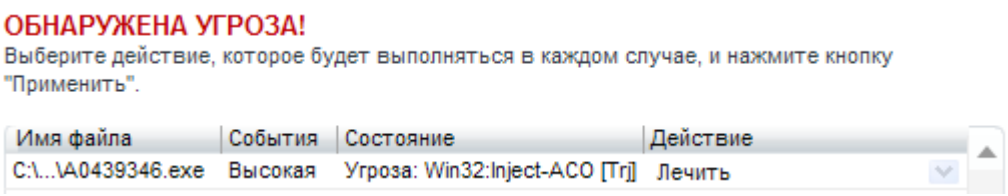
Կբացվի հետևյալ պատուհանը



Աստուգումից հետո կցուցադրվի ստուգման արդյունքները



Սեղմելով "Показать результаты" կոճակը կտեսնենք վտանգի հայտնաբերումը.



1. Ինչ պետք է ունենալ կոշտ սկավառակի ստուգման համար
    - Պաշտպանված ծրագիր

- Բեռնավորող ծրագիր
- Հակավիրուսային ծրագրով ֆայլ
- Համակարգչում տեղադրված հակավիրուսային ծրագիր

2. Թվարկել հակավիրուսային ծրագրով ֆայլերի ստուգման քայլերը

_____

_____

_____

_____

_____

_____

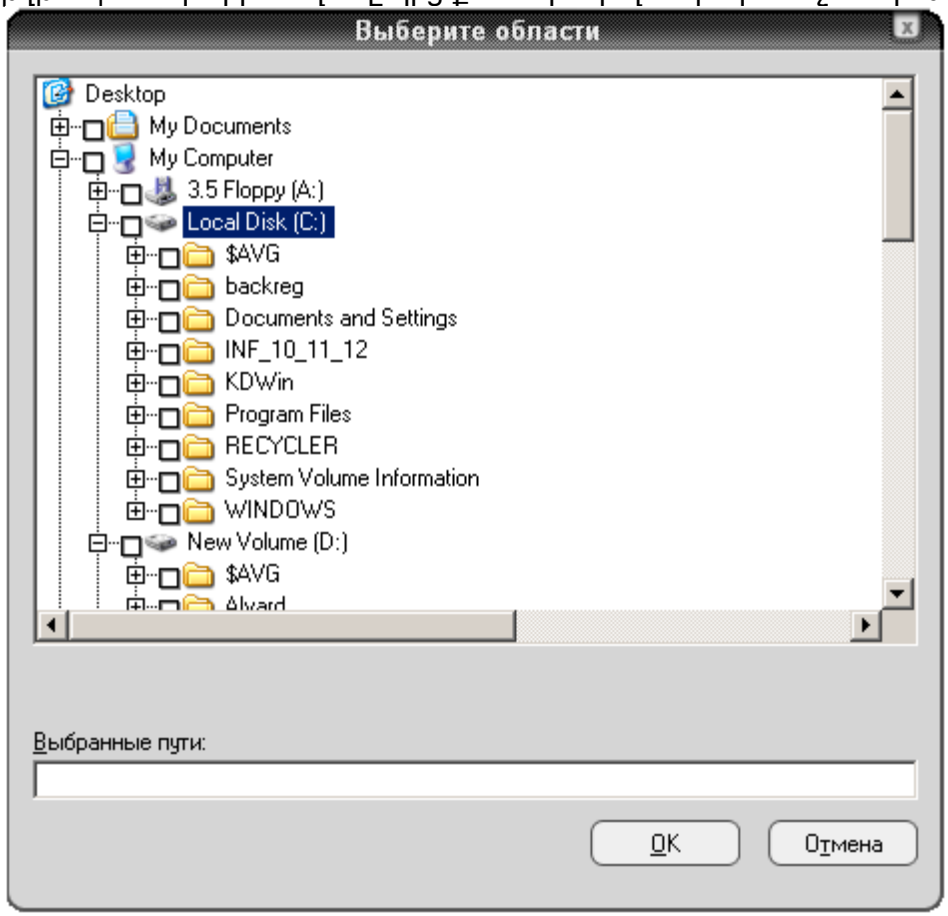
_____

_____

_____

2.8 Առանձին թղթապանակների ստուգում

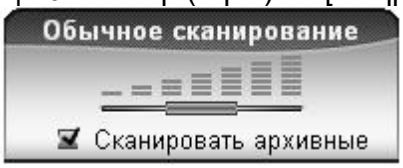
Առանձին թղթապանակներ ստուգելու համար անհրաժեշտ է ընտրել (*ՁonՏՐ ՍՈՍՄՈ*) կոճակն ու բացված պատուհանում (նկ.3) մկնիկի ձախ սեղմակով ստուգման ենթակա թղթապանակների անվանը կից քառակուսի վանդակում նշում կատարել:



Նկ. 3. Թղթապանակների ընտրության պատուհան
Ստուգել համակարգչի MyDocuments թղթապանակիը և գրել արդյունքների մասին
_____
_____
_____
_____
_____
_____

2.9 Ստուգման զգայնության ընտրություն

Ստուգման զգայնությունը (խորությունը) կարելի է սահմանել այդ նպատակին ծառայող պատուհանի (նկ. 4) սողնակի տեղաշարժմամբ:



Նկ. 4. Ստուգման զգայնության ընտրություն

Avast հակավիրուսային ծրագիրը հնարավորություն է տալիս ընտրել զգայնության հետևյալ 3 մակարդակներից որևէ մեկը.

- o *ևՍրտՐպրր րՍՈվՈՐՏՉՈվՈպ* - արագ, մակերեսային ստուգում,
- o *ԿոօփվՏպ րՍՈվՈՐՏՉՈվՈպ* - սովորական, միջին ստուգում,
- o *կՏսվՏպ րՍՈվՈՐՈՉՈվՈպ* - բոլոր ֆայլերի մանրամասն ստուգում:

Արխիվային ֆայլերը ստուգելու նպատակով անհրաժեշտ է նկ. 4-ում բերված պատուհանի *ԿՑՍՐօՉՈՑՖ ՈՐւՈՉվօպ* դաշտում նշում կատարել:

*Վիրուս հայտնաբեր*ելու գործընթացն սկսելու համար անհրաժեշտ է սեղմել (*ԻՈտգրՑՈրՑՖ*) կոճակը:

Որպեսզի հակավիրուսային ծրագրի աշխատանքն ընթանա ակտիվ ծրագրի աշխատանքին համընթաց՝ այսպես կոչված՝ ֆոնային ռեժիմում, պետք է Avast-ի ծրագրի աշխատանքի ընթացքում ծրագրի երկխոսային պատուհանի վրա մկնիկի աջ սեղմակի սեղմում կատարել և բացված ենթատեքստային պատուհանում ընտրել *կպՐպՒՑՈ Չ ԻՏվՏՉօՒ ՐպՋՈվ* հրամանը: Ֆոնային ռեժիմին անցնելիս վիրուսների ստուգման գործընթացը դանդաղ կընթանա, որովհետև այս դեպքում համակարգիչը կատարման առաջնահերթությունը տալիս է ակտիվ ծրագրին:

2.10 Վիրուսների հեռացում

Վիրուս հայտնաբերելիս հակավիրուսային ծրագիրը մի քանի տարբերակներ է առաջարկում (նկ. 5).

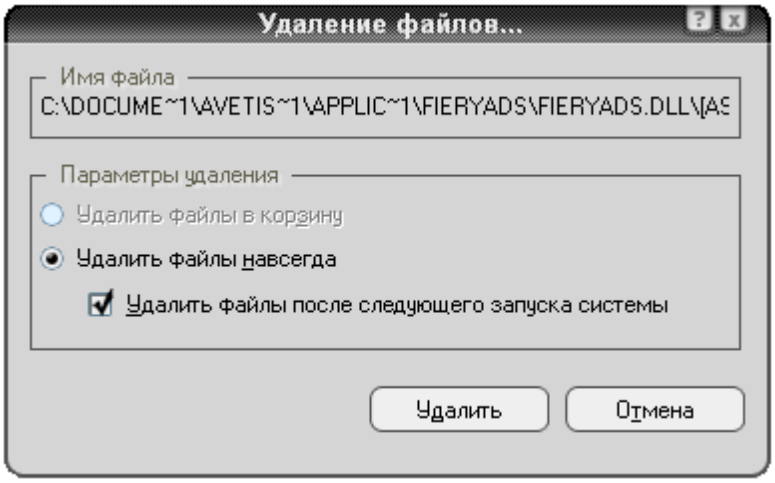
- o կպՐպՈՎպվՏՉՈՑՖ... - անվանափոխել ֆայլը,
- o ձՊՈսՈՑՖ... - հեռացնել ֆայլը,
- o Թ ղՐՈվՈսՈՔպ... - հայտնաբերված վիրուսակիր ֆայլը տեղափոխել նման ֆայլերի պահեստարան՝ հետագայում բուժելու, ջնջելու կամ տեղափոխելու համար,
- o ծՈփպչՏ վպ ՊպսՈՑՖ - շարունակել ստուգումը՝ ֆայլը թողնելով անփոփոխ:

Նկ. 5. Վիրուսի առկայության մասին նախազգուշացնող պատուհան

Ֆայլը ջնջելուց օպերացիոն համակարգը պահանջում է ընտրել ստորև բերված տարբերակներից որևէ մեկն ու սեղմել ՅՊՈՍՌՑՖ կոճակը.

o ՅՊՈՍՌՑՖ ԻՈՋսօ Չ ՍՏՐՉՌՎց - հեռացված ֆայլն ուղղարկել Recycle Bin,

o ՅՊՈՍՌՑՖ ԻՈՋսօ ՎՈՉրաչՊՈ - ֆայլը հեռացնել ընդմիշտ:

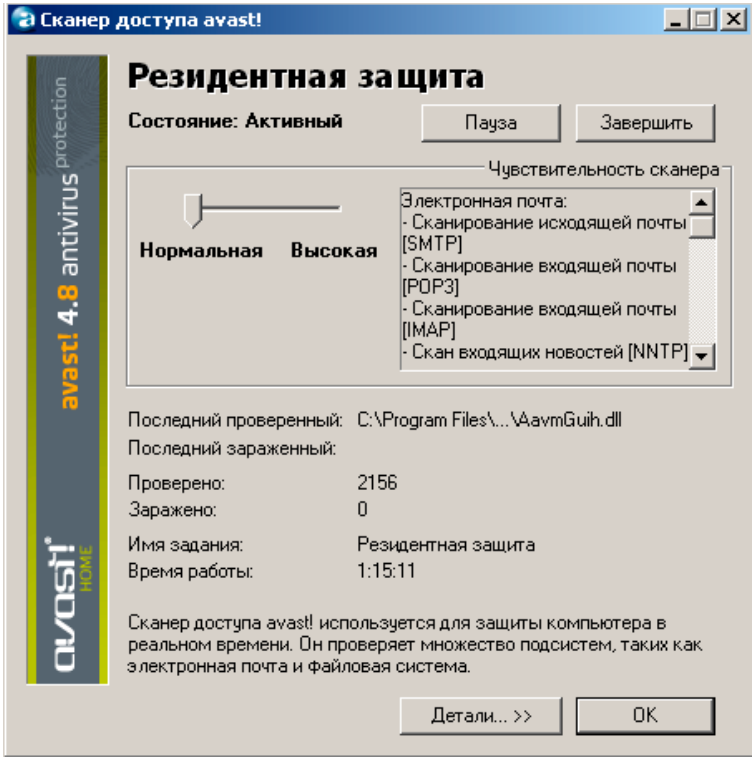


Նկ. 6. Ֆայլը ջնջելու ձևն ընտրելու պատուհան

Ստուգումն ավարտելուց հետո Avast-ը հաղորդագրություն է տալիս ստուգման արդյունքի վերաբերյալ:

Avast-ի տարբերանշանի տիրույթում մկնիկի ձախ սեղմակի օգնությամբ բացվում է ռեզիդենտային պաշտպանության պատուհանը: Avast-ի ռեզիդենտային ծրագիրը համակարգչի աշխատանքի ողջ ընթացքում անընդհատ վերահսկում է օպերատիվ հիշողությունն ու բոլոր աշխատող ծրագրերը՝ հետևելով կասկածելի գործընթացներին: Ծրագիրն ավտոմատ ակտիվանում է համակարգիչը միացնելուց անմիջապես հետո:

Ռեզիդենտային պաշտպանությունն ընդհատելու, դադարեցնելու կամ զգայնությունը փոփոխելու համար անհրաժեշտ է մկնիկի ցուցիչը տեղադրել հակավիրուսային ծրագրի տարբերանշանի վրա, սեղմել ձախ սեղմակն ու բացված պատուհանում (նկ.7) ընտրել անհրաժեշտ տարբերակները:



Նկ. 7. Ռեզիդենտային պաշտպանության ղեկավարման պատուհան

Ընտրել ճիշտ տարբերակները

1. Ո՞ր վիրուսներն են իրենց «գաղտնի» աշխատանքի ընթացքում մի համակարգչից տեղեկություններ հավաքելով՝ դրանք Ինտերնետով այլ համակարգիչ ուղարկում:
   - ֆայլային,
   - բեռնավորվող,
   - տրոյական:
2. Հակավիրուսային ծրագրերից չէ
   - Dr.Web ,
   - Norton Antivirus ,
   - Norton Commander:
3. Հակավիրուսային ծրագիրը վիրուս հայտնաբերելիս չի առաջարկում
   - անվանափոխել ֆայլը,
   - բեռնավորել ֆայլը,
   - հեռացնել ֆայլը:

3. Ֆայլերի, թղթապանակների պաշտպանում ծածկագրով:

3.1.Փաստաթղթերի պաշտպանությունը

Պաշտպանությունը թույլ է տալիս ամբողջովին արգելել փաստաթղթի մատչելիությունը,այնպես էլ սահմանափակել այլ օգտագործողնների կողմից փաստաթղթի ձևափոխման հնարավորությունը:

Office- ծրագրերը հագեցած չեն վիրուսներից պաշտպանվելու հնարավորություններով: Հակավիրուսային ծրագրեր կարելի է ինքնուրույն հայթայթել և տեղակայել համակարգչում:

Մակրովիրուսներ և պաշտպանությունը նրանցից

MS Office փաստաթուղթը կարող է պարունակել մակրոսներ (**VBA** լեզվով յուրահատուկ ծրագրեր են), որոնց նպատակը տվյալների հետ աշխատանքի պարզեցումն ու ավտոմատացումն է: Ինչպես ցանկացած ծրագիր, մակրոսներն էլ կարող են վարակվել վիրուսներով:**MS Office** առնձնահատկությունը բացվող փաստաթղթերում մակրոսների հանդեպ եռամակարդակ պաշտպանության համակարգն է: Կախված ընտրված պաշտպանության մակարդակից **(Security Level) Office** հավելվածների վարքը փաստաթղթերի բացման ժամանակ տարբեր է:

MS Office փաստաթղթերում պաշտպանվածության մակարդակները

1. Ընտրեք **Tools/Macros/Security** հրամանը:
2. **Security** երկխոսության պատուհանում բացեք **Security Level :** Տեղակայեք փոխանջատիչը պահանջվող դիրքում:
   - **High(բարձր).** նշանակում է, որ փաստաթղթի բացման ժամանակ կարող են կատարվել միայն հուսալի աղբյուրների կողմից թվային ստորագրություն ունեցող մակրոսները: Եթե մակրոսները թվային ստորագրություն չունեն, դրանք ավտոմատ կերպով անջատվում են:
   - **Medium (միջին)** փաստաթղթի բացման ժամանակ օգտագործվողը նախազգուշացվում է: Նա ինքնուրույն պետք է որոշի մակրոսներն անջատել թ՞ե ոչ: Եթե աղբյուրները որոնցից ստեղծվել է փաստաթուղթը, վստահելի են, ապա նախազգուշացում չի տրվում և մակրոսները չեն անջատվում:
   - **Low (ցածր)** ենթադրում է որ մակրովիրուսներ գոյություն չունեն; Բոլոր մակրոսները անկախ ծագումից և թվային ստորագրության առկայությունից միանում են առանց նախազգուշացման:

1. ԻՆչ է մակրոսը:_____

_____

_____

_____

2.Մակրովիրուսներից պաշտպանության մակարդակները

_____

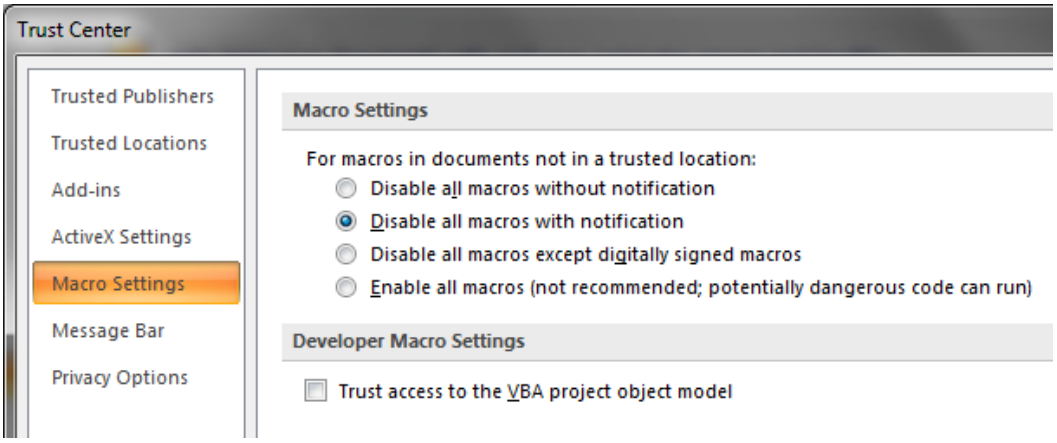
_____

_____

_____

_____

Բացատրել հետևյալ պատուհանի կառուցվածքը.

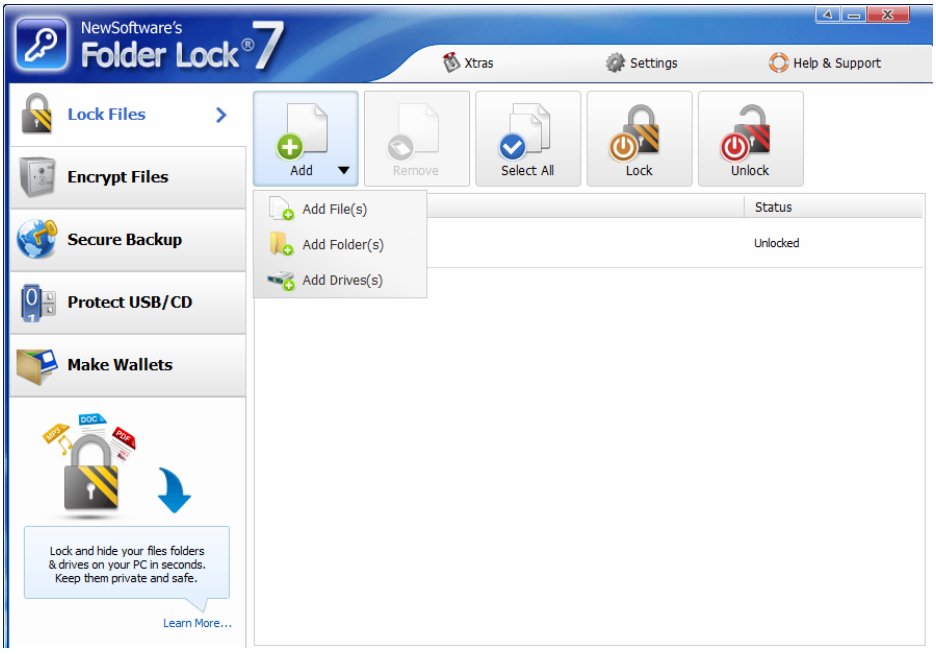


3.2.Թղթապանակների պաշտպանում ծածկագրով: Folder Lock ծրագիրը

Թղթապանակները Folder Lock ծրագրով պաշտպանելու համար կատարել հետևյալ քայլերը:

1. Թողարկել Folder Lock ծրագիրը:

2. Enter Master Password դաշտում ներմուծել ծածկաբառը և սեղմել OK կոճակը:



3. Բացված պատուհանի Add ընտրացուցակից ընտրել AddFolder կետը:

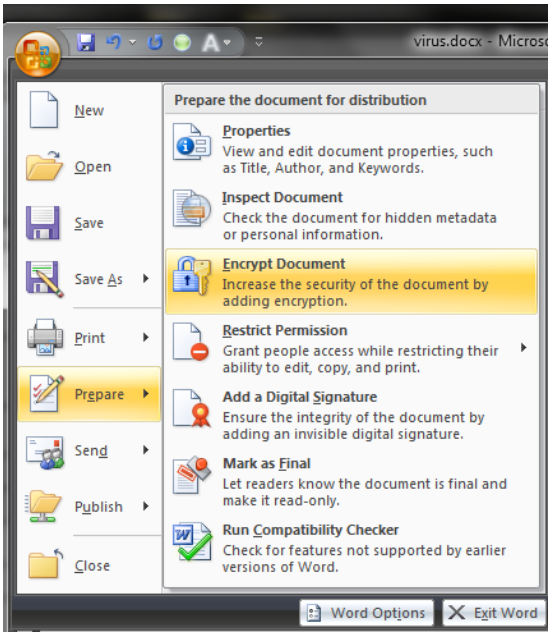
4. Բացված պատուհանից ընտրել ցանկացած թղթապանակը և սեղմել Ok կոճակը:
5. Թղթապանակը կհայտնվի ընտրման տարածքում: Նշել այն և սեղմել Lock կոճակը:
6. Արդյունքում թղթապանակը կանհետանա:
7. Այն մենք կարող ենք տեսնել միայն Folder Lock ծրագրի պատուհանում:

Folder Lock ծրագրի օգնությամբ ինքնուրույն թողարկեք Protect USB/CD հրամանը և բացատրեք քայլերը.

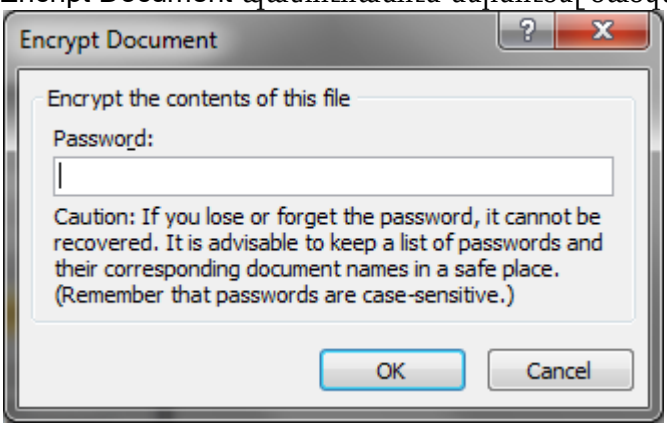
1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

3.3. Word-ի և Excel-ի փաստաթղթերի պաշտպանում ծածկագրով

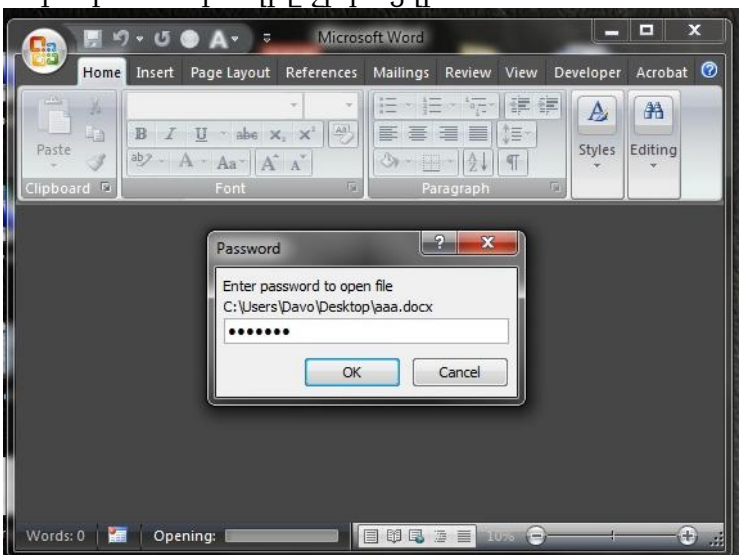
Word-ի և Excel-ի փաստաթղթերը ծածկագրով պաշտպանելու համար թողարկել Prepare→Encript Document հրամանը:



Encript Document պատուհանում ներմուծել ծածկագիրը և սեղմել Ok կոճակը:



Փաստաթուղթը փակել: Փաստաթղթի հաջորդ բացման ժամանակ կբացվի ծածկագրի պատուհանը, որտեղ պետք է հավաքել փաստաթղթի ծածկագիրը: Եթե սխալ բառ հավաքվի, ապա փաստաթուղթը չի բացվի:



1.Փաստաթղթերի պաշտպանության միջոցները

_____

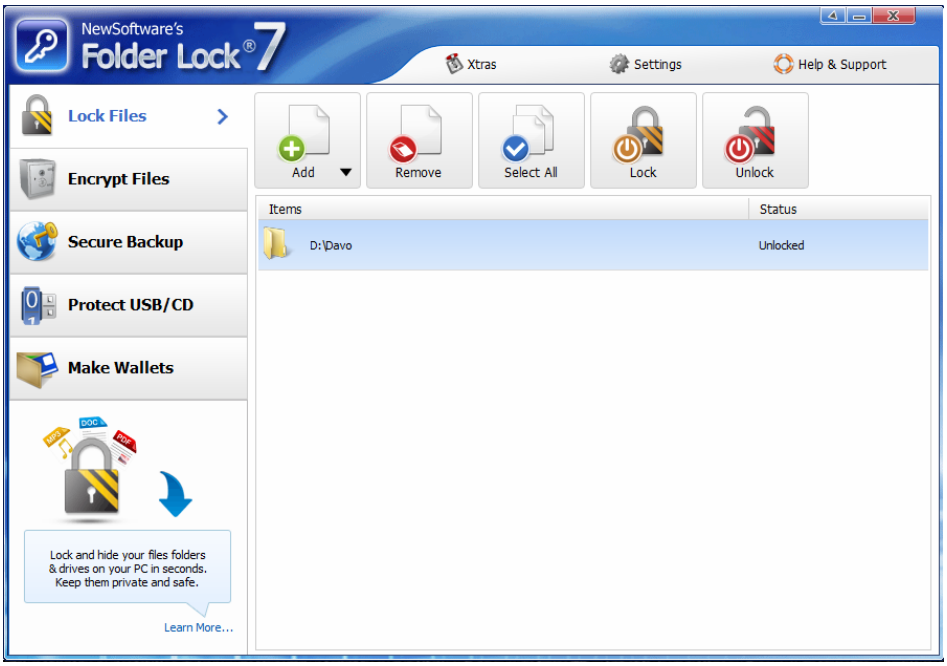
_____

2.Թվարկել փաստաթուղթը ծածկագրով պաշտպանելու քայլերը

3.4. Հեռացնել ծածկագրերը

Թղթապանակների ծածկագիրը հեռացնելու համար

1. թողարկել Folder Lock ծրագիրը,
2. ներմուծել ծածկաբառը,
3. բացված պատուհանում ընտրել թղթապանակը, որը պետք է պաշտպանությունից հանել
4. սեղմել Unlock կոճակը: Արդյունքում թղթապանակը դուրս կգա պաշտպանությունից:



Ինքնուրույն բացատրել փաստաթղթերի ծածկագրերի հեռացումը

_____

_____

_____

_____

1.MsWord ծրագրում ստեղծել ֆայլ և այն պաշտպանել ծածկագրով: Գրել բացատրությունը

_____

_____

_____

_____

_____

1.MsExcel ծրագրում ստեղծել ֆայլ և այն պաշտպանել ծածկագրով: Գրել բացատրությունը

_____

_____

_____

_____

_____

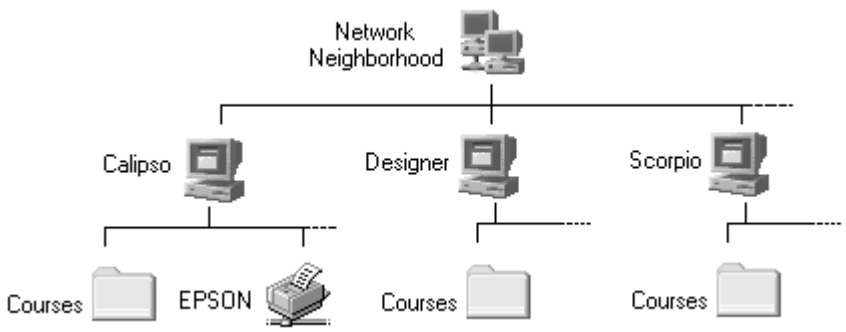
4.Օգտագործողների իրավունքների սահմանում

4.1.Տեղային Ցանցի Կազմակերպում

Տեղային ցանցերի տարբեր համակարգերի կազմակերպման սկզբունքներն ու համագործակցության կանոնակարգերը շատ նման են

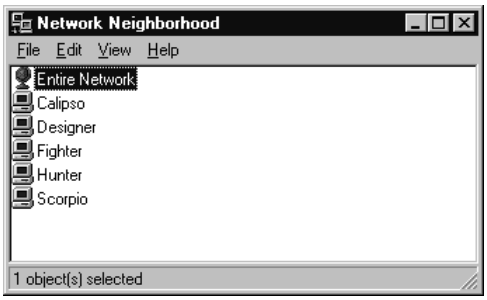
Ցանցերում ռեսուրսները՝ օբյեկտները, բաժանվում են, և քոմփյութերները կարող են դիմել ու համատեղ օգտագործել այլ քոմփյութերների ռեսուրսները: Ցանցային ռեսուրսներն ընդգրկում են ցանցային քոմփյութերների բաժանելի բոլոր ռեսուրսները՝ օբյեկտները, և կազմակերպված են հիերարխիական կառուցվածքներով:

Ցանցային քոմփյութերներն ունենում են հատուկ անուններ. Դիցուք ցանցը կազմված է Calipso, Designer, Scorpio…քոմփյութերներից, ուր Calipso-ին միացված է ցանցային տպիչը (Epson մակնիշի) և ցանցի բոլոր քոմփյութերների կոշտ սկավառակներն ունեն Courses բաժանելի թղթապանակները: Ցանցի հիերարխիական կառուցվածքն ընդգրկում է բաժանելի բոլոր ռեսուրսները (Courses թղթապանակներն ու Epson տպիչը նեռարյալ) և կարող է ունենալ ստորև բերված տեսքը (տրված են կառուցվածքի միայն վերևի մակարդակները):

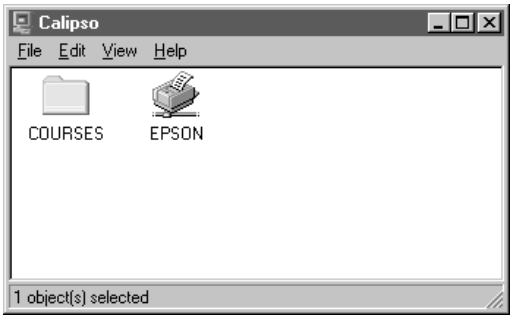


Ցանցային ու Մենաշնորհային Դիմում

Ցանցի հիերարխիական կառուցվածքը կազմվում է ցանցային քոմփյութերների բաժանելի օբյեկտներից: Ցանցային կառուցվածքը արտապատկերվում է Desktop պատուհանի *Network Neighborhood* (Ցանցային հարևանություն) նշանի շրխկացումով: Արտապատկերվում է պատուհան ցանցային քոմփյութերների նիշերով, որը բերված ցանցի դեպքում կարող է ունենալ հետևյալ տեսքը.

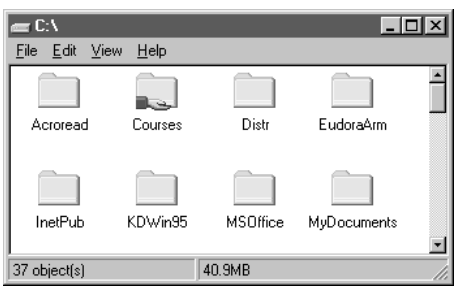


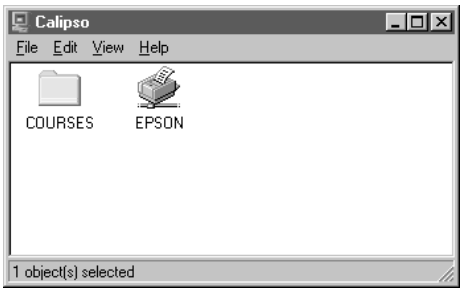
Ցանցային քոմփյութերները կարող են ունենալ բաժանելի ռեսուրսներ, որոնք արտապատկերվում են Network Neighborhood պատուհանի քոմփյութերների նիշերի հետագա շրխկացումներով: Այսպես, Calipso նիշի շրխկացումով արտապատկերվում է պատուհան Calipso քոմփյութերի բաժանելի ռեսուրսների՝ Courses թղթապանակի ու Epson տպիչի նիշերով:



Desktop աշխատանքային սեղանի Network Neiborhood ու My Computer նիշերին համադրված են համապատասխանաբար ցանցային ու տվյալ քոմփյութերի ռեսուրսները: Դրանց շրխկացումներով իրագործվում են ռեսուրսներին դիմելու ցանցային ու 'մենաշնորհային' եղանակները, և օգտագործողը ստանում է ցանցի բոլոր քոմփյութերների բաժանելի ռեսուրսներին կամ միայն 'սեփական' ռեսուրսներին դիմելու և օգտագործելու հնարավորությունը:

Այսպես, Calipso քոմփյութերի Desktop պատուհանում My Computer նիշի շրխկացումով արտապատկերվում են ու մատչելի դառնում տվյալ քոմփյութերի (և միայն դրա) բոլոր ռեսուրսները: Միևնույն ժամանակ, նույն Calipso քոմփյութերի Desktop պատուհանի Network Neiborhood ու արտապատկերվող պատուհանի Calipso նիշերի շրխկացումներով արտապատկերվում ու մատչելի են դառնում Calipso քոմփյութերի բաժանելի ռեսուրսները՝ Courses թղթապանակն ու Epson տպիչը:





Ցանցի Օգտագործողները

Ցանցերում հատուկ ձևով գրանցվում են ցանցի մասնակիցները, որոնք կարող են դիմել և օգտագործել ցանցային ռեսուրսները, փոխանակել ինֆորմացիա և թողարկել այլ քոմփյութերների ծրագրերը:

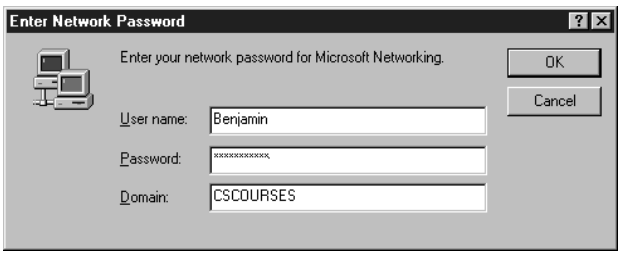
Ցանցային օգտագործողներին համադրվում են Անուններ ու Ծածկանուններ (Password): Այսպես, ցանցում գրանցված օգտագործողները կարող են ունենալ հետևյալ անուններն ու ծածկանունները.

Benjamin 9Benthos9

Administrator98QQ89

Guest1 Anonymous

Ամենասկզբում՝ քոմփյութերի միացման պահին, արտապատկերվում է հատուկ երկխոսական պատուհան, որի դաշտերում օգտագործողը ներանցում է գրանցման իր անունն ու ծածկանունը: Օրինակ, պատուհանը, որի դաշտերում գրանցված է “Benjamin” անունն ու “9Benthos9” ծածկանունը, ունենում է հետևյալ տեսքը.



Ծածկանունը ներմուծելու ժամանակ իրական նիշերը արտապատկերվում են աստղանիշերով, իսկ ծածկանունը մնում է անտեսանելի կողմնակի դիտորդների համար:

Օգտագործողը իր անունն ու ծածկանունը ներանցելուց հետո OK ստեղնի շրխկացումով ավարտում է երկխոսությունն ու ստանում է ցանցում աշխատելու հնարավորություն:

Չգրանցված օգտագործողները (անուններ ու ծածկանուններ չունեցողները) կարող են Esc ստեղնի սեղմումներով հրաժարվել ցանցային աշխատանքից և օգտագործել միայն տվյալ քոմփյութերի ռեսուրսները:

Առաջադրանք

Ստեղծել տեղային ցանց, որի քոմփյութերների անուններն են.

Calipso, Designer, Fighter, Hunter, Scorpio

Ցանցում գրանցված են օգտագործողներ, որոնց անուններն են.

guest1, guest2, guest3...

այդ բոլորին տրված է ընդհանուր ծածկանուն.

anonymous

Բոլոր քոմփյութերները կոշտ սկավառակների Courses թղթապանակներում ունեն վարժեցողական ինֆորմացիոն ռեսուրսներ

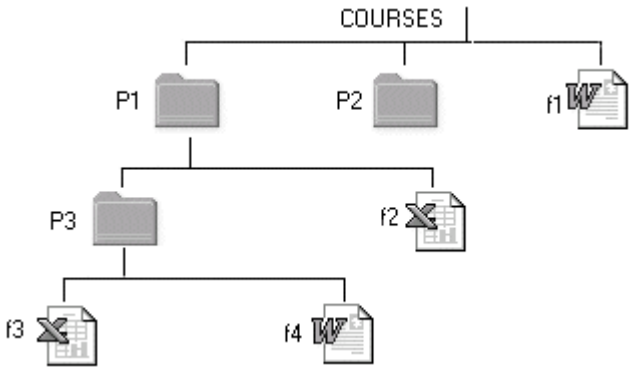
Calipso քոմյութերին միացրած է Epson տպիչը, որի միջով կարող է իրագործվել ցանցային տպումը

Գրել բացատրությունը_____

4.2.Ռեսուրսների Բաժանում: Ընդհանուր Տեղեկություններ

Ցանցային քոմփյութերների ռեսուրսների մի մասը կարող է *Բաժանելի* (Shared) լինել ու դիտվել, մատչելի լինել ցանցի այլ քոմփյութերների համար: Մնացած անբաժանելի ռեսուրսները անտեսանելի են և ոչ մատչելի: Ինֆորմացիոն ռեսուրսները բաժանվում են թղթապանակների մակարդակով եթե թղթապանակը բաժանելի է, ապա մատչելի են ու կարող են դիտվել և մշակվել բաղկացուցիչ ֆայլերը:

Դիցուք ցանցային քոմփյութերներից մեկի Courses ֆայլային կառուցվածքն ունի ստորև բերված տեսքը, և Courses ու P3 թղթապանակները բաժանելի են, իսկ P1 ու P2-ը՝ ոչ: Այդ դեպքում ցանցային բոլոր օգտագործողների համար բաժանելի թղթապանակների ֆայլերը՝ f1, f3, f4 տեսանելի են ու կարող են դիտվել և մշակվել, իսկ անբաժանելի թղթապանակի f2 ֆայլը ամտեսանելի է. դրա դիտումն ու մշակումը անհնար է:



Ցանցային եղանակով աշխատելու ժամանակ կարող են դիտվել ու մշակվել միայն բաժանելի ռեսուրսները: Բաժանելի յուրաքանչյուր ռեսուրսին համադրվում են դիմելու իրավունք ունեցող օգտագործողները՝ գրանցվածների թվից: Մնացածների համար տվյալ ռեսուրսը թեպետ տեսանելի է, սակայն մատչելի չէ:

Յուրաքանչյուր օգտագործողի համար մատչելի ռեսուրսը կարող է բերվել Լրիվ Դիմելու (Full Acces) կամ Միայն Ընթերցելու (Read Only) մակարդակների, երբ բաղկացուցիչ ֆայլերի տվյալները օգտագործողը կարող է փոփոխել կամ միայն ընթերցել:

Ցանցային քոմփյութերի մեջ ձևավորվում են դիմումի հատուկ աղյուսակներ, ուր գրանցվում են տեղեկություններ տվյալ քոմփյութերի բաժանելի ռեսուրսների, առանձին օգտագործողների դիմելու իրավունքների ու մակարդակների մասին: Դիցուք Calipso քոմփյութերում բաժանելի ռեսուրսներն են Courses ու P3 թղթապանակները: Նրա դիմելու աղյուսակը կարող է ունենալ հետևյալ տեսքը.

Օգտագործող	Ռեսուրս	Դիմելու մակարդակ
Administrator	P3 թղթապանակ	Full Access
Administrator	Courses թղթապանակ	Full Access
Benjamin	P3 թղթապանակ	Read Only

Guest1	Courses թղթապանակ	Full Access

Administrator օգտագործողն ունի P3 ու Courses թղթապանակներին դիմելու լիիրավ իրավունք ու կարող է փոփոխել, լրացնել, ուղղել բաղկացուցիչ փաստաթղթերը՝ f1, f3, f4 ֆայլերը: Benjamin օգտագործողը կարող է միայն ընթերցել P3 թղթապանակի փաստաթղթերը՝ f3, f4 ֆայլերը, իսկ Guest1-ը՝ փոփոխել Courses թղթապանակի փաստաթղթերը՝ f1 ֆայլը:

Բերված աղյուսակում նշված են օգտագործողներից միայն երեքը, իսկ բացակայում են մյուսները, որոնց համար Calipso քոմփյութերի ռեսուրսներին դիմելը արգելված է: Նրանք, այլ քոմփյութերներով աշխատելիս կարող են միայն տեսնել Calipso-ի բաժանելի ռեսուրսները, սակայն դրանք անմատչելի են մնում:

Առաջադրանք

Desktop պատուհանի Network Neiborhood, այնուհետև առանձին քոմփյութերների նիշերի շրխկացումներով արտապատկերել ցանցային ռեսուրսներ ներկայացնող պատուհանը

Desktop պատուհանի ու My Computer նիշի շրխկացումով արտապատկերել տվյալ քոմփյութերի ռեսուրսները ներկայացնող պատուհանը

Արտապատկերված պատուհանների բաղկացուցիչ օբյեկտների շրխկացումներով ստանալ ու դիտել ցանցային ու մենաշնորհային կառուցվածքի տարրերն ու եզրակացություններ անել դիմումի համեմատական հնարավորությունների մասին

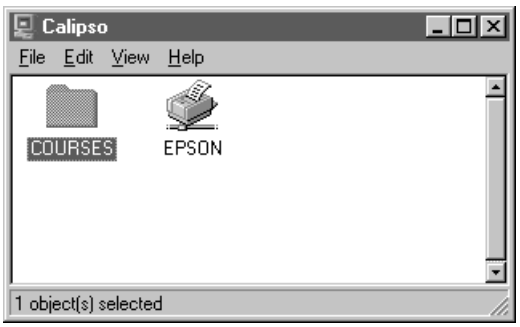
Գրել բացատրությունը_____

_____
_____
_____
_____
_____

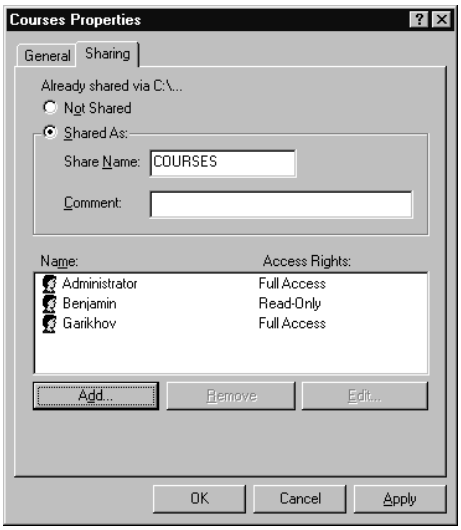
4.3.Ռեսուրսների Բաժանում: Համագործակցության Համակարգ

Սկզբնական վիճակում, ցանցային մասնակիցների համար ցանցային քոմփյութերի բոլոր ռեսուրսները անբաժանելի են, անտեսանելի և անմատչելի: Օգտագործողը, որը մուտք է գործում *My Computer* կառուցվածքի միջոցով, աշխատում է մենաշնորհային եղանակով, տիրապետում է տվյալ քոմփյութերի ռեսուրսներին ու կարող է դրանք բաշխել՝ դարձնել բաժանելի, օգտագործողներին տալ դիմելու իրավունքներ ու մակարդակներ: Օգտագործվում է File վայր ընկնող մենյուի *Sharing* (բաժանում) հատուկ հրամանը:

Թղթապանակը նախապես ակտիվացվում է, այնուհետև թողարկվում է Sharing հրամանը, որը կարող է թողարկվել ինչպես File վայր ընկնող մենյուից, այնպես էլ ենթատեքստայինից: Դիցուք Calipso քոմփյութերի արմատական թղթապանակում ակտիվացված է Courses թղթապանակը:



Sharing հրամանը արտապատկերում է *Properties* (հատկություններ) հատուկ պատուհանը, որի վերնամասում կան *Not Shared* ու *Shared As* հատուկ կոճակները, որոնց շրխկացումներով ակտիվացված թղթապանակը բերվում է անբաժանելի կամ բաժանելի վիճակի: Այսպես, Not Shared կոճակի շրխկացումով ցանցային օգտագործման համար ռեսուրսը դառնում է անբաժանելի, անտեսանելի և անմատչելի:

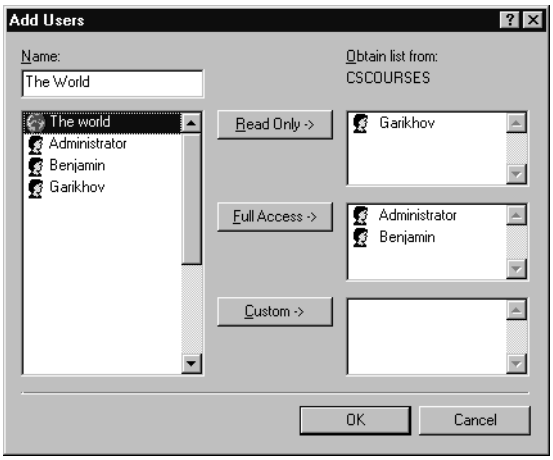


Պատուհանի կենտրոնում արտապատկեված են ռեսուրսին դիմելու իրավունք ունեցողների ցուցակն ու դիմելու մակարդակները (Full Access, Read only): Այսպես, բերված պատուհանում Courses թղթապանակը բաժանելի է (սեղմված է Shared As կոճակը) ու Administrator ու Benjamin օգտագործողները կարող են դիմել դրան: Administrator-ն լրիվ դիմումի իրավունք (Full Access) ունի, իսկ Benjamin-ը՝ միայն ընթերցելու (Read only):

Properties պատուհանն ունի հատուկ միջոցներ, որոնց օգնությամբ կարող են հեռացվել, վերանշանակվել ու փոփոխվել օգտագործողների դիմումի իրավունքն ու մակարդակը:

Օգտագործողների ցուցակի տարրերի ակտիվացումով ու *Remove* (հեռացում) ստեղնի հետագա շրխկացումով համապատասխան օգտագործողները հեռացվում են դիմելու իրավունքներ ունեցողների ցուցակից, և ռեսուրսը նրանց համար դառնում է անմատչելի:

Նոր օգտագործողները դիմելու իրավունք են ստանում, և ցուցակին ավելացվում են *Add* (ավելացում) հատուկ կոճակի օգնությամբ: Այդ կոճակի շրխկացումով արտապատկերվում է հատուկ *Add Users* (ավելացնել օգտագործողներ) պատուհանը, ուր տրվում է ցանցում գրանցված օգտագործողների ցուցակն և դիմելու մակարդակների կոճակները (Read only, Full Access):



Օգտագործողների ցուցակի կետերի ընտրությամբ ու շրխկացումներով համապատասխան օգտագործողը ստանում է տվյալ ռեսուրսին դիմելու իրավունքը, իսկ դիմելու մակարդակների կոճակների շրխկացումներով (Read only, Full Access) նրանց տրվում են դիմելու մակարդակներ:

Բաժանելի ռեսուրսների ցուցակներում բացակայող օգտագործողների համար ռեսուրսները թեպետ տեսանելի են, սակայն մատչելի չեն: Դիմելու փորձերը մերժվում են, և համակարգը ձևավորում է “Access Is denied” (դիմումն արգելված է) հատուկ հաղորդումը:

Առաջադրանք

My Computer նիշի շրխկացումով արտապատկերել ’սեփական’ քոմփյութերի հիերարխիական կառուցվածքը և Courses թղթապանակում ստեղծել վարժեցողական մի քանի թղթապանակ ու ֆայլ Վարժեցողական կառուցվածքի թղթապանակները բերել բաժանելի ու անբաժանելի վիճակների: Ցանցային առանձին մասնակիցներին (guest1, guest2..) տալ դիմելու իրավունքներ ու մակարդակներ (Full Acces, Read only).

Ակտիվացնել թղթապանակներն ու օգտագործել Sharing հրամանը:

Գրել բացատրություն _____

_____

_____

_____

_____

_____