Տեղեկատվության անվտանգության հիմունքներ

Համակարգչային վիրուսներ

Դաս 1. Համակարգչային վիրուս

Հիշեցնենք, որ համակարգչային վիրուսը ծրագրավորողների կողմից գրված, «ինքնաբազմացման» ունակությաթբ օժտված փոքրածավալ ծրագիր է, որը կարող է համակարգչի աշխատանքում տարբեր անցանկալի երևույթների պատճառ դառնալ՝ սկսած «ամենաանմեղներից». էկրանին բերվող պատկերի աղավաղում, երաժշտական հոլովակների ցուցադրում և այլն, մինչև լրջորեն վնասելը՝ համակարգչային տվյալների ոչնչացում և նույնիսկ համակարգչի առանձին միկրոսխեմաների անսարքության առաջացում: Համակարգիչը վարակելուց հետո վիրուսը կարող է «թաքնվել» ու «հարձակման անցնել» սկսած որոշակի իրադարձությունից՝ շաբաթվա որևէ օրվանից, կոնկրետ ամսաթվից, կիրառական որևէ ծրագրի թողարկումից, փաստաթուղթ բացելուց:

Վիրուսի հիմնական աղբյուր կարող է լինել.

- վիրուսակիր ֆայլ պարունակող սկավառակը,
- համակարգչային ցանցը, այդ թվում՝ էլեկտրոնային փոստն ու ինտերնետը,
- վիրուսով վարակված կոշտ սկավառակը,
- օպերացիոն համակարգում թաքնված վիրուսը:

Վիրուսով վարակված լինելու մասին կարող են վկայել հետևյալ ախտանիշները.

- ազատ օպերատիվ հիշողության ծավալի անհիմն փոքրացումը,
- համակարգչի աշխատանքի և բեռնավորման գործընթացի դանդաղումը,
- ֆայլի պարունակության փոփոխությունը,
- ֆայլի ծավալի և վերջին վերափոխման ամսաթվի փոփոխությունը,
- տեքստային փաստաթղթի աղավաղումը,
- աշխատող կիրառական ծրագրի վթարային ելքը,
- օպերացիոն համակարգի ինքնավերաբեռնավորումը,
- օպերացիոն համակարգի բեռնավորման սխալները,
- ֆայլերն անհրաժեշտ թղթապանակներում պահպանելու անհնարինությունը,
- ֆայլերի բազմաթիվ կրկնօրինակների ավտոմատ ստեղծումը և այլն:

Դաս 2. Վիրուսի առկայությունը բնորոշ <<ախտանիշներ>>

Վիրուսով վարակված լինելու մասին կարող են վկայել հետևյալ <<ախտանիշները>>.

- ազատ օպերատիվ հիշողության ծավալի անհիմն փոքրացումը,
- համակարգչի աշխատանքի նբեռնավորման գործընթացի դանդաղումը,
- ֆայլի պարունակության փոփոխությունը,
- ֆայլի ծավալի և վերջին վերափոխման ամսաթվի փոփոխությունը,
- տեքստային փաստաթղթի աղավաղումը,
- աշխատող կիրառական ծրագրի վթարային ելքը,
- օպերացիոն համակարգի ինքնավերաբեռնավորումը,
- օպերացիոն համակարգիբեռնավորման սխալները,
- ֆայլերն անհրաժեշտ թղթապանակներում պահպանելու անհնարինությունը,
- ֆայլերիբազմաթիվ կրկնօրինակների ավտոմատ ստեղծումը և այլն:

Դաս 3. Վիրուսով վարակվելու հիմնական աղբյուրները

Վիրուսի հիմնական աղբյուր կարող է լինել.

- վիրուսակիր ֆայլ պարունակող սկավառակը,
- համակարգչային ցանցը, այդ թվում՝ էլեկտրոնային փոստն ու ինտերնետը,
- վիրուսով վարակված կոշտ սկավառակը,
- օպերացիոն համակարգում թաքնված վիրուսը:

Դաս 4. Վիրուսի հիմնական հատկությունները

Համակարգիչը վիրուսով վարակվելուց հետո համակարգչում առաջանում են մի շարք խնդիրներ՝

ա) համակարգչի աշխատունակության նվազում (այն սկսում է դանդաղ աշխատել՝ երկար «մտածել»),
բ) համակարգչով աշխատելու ընթացքում օպերացիոն համակարգի ավտոմատ վերաբեռնավորում,
գ) տեքստային փաստաթղթերի աղավաղում,
դ) կիրառական ծրագրերի աշխատանքի վթարային ելք,
ե) ճկուն և կոշտ սկավառակների վրա եղած ֆայլերի բազմաթիվ կրկնօրինակների ստեղծում և այլն:

Դաս 5. Վիրուսների դասակարգումը

Տարբերում են վիրուսների հետևյալ տիպերը.

- ֆայլային վիրուսներ. սրանք վարակում են ճկուն ու կոշտ սկավառակների վրա եղած ծրագրերն ու փաստաթուղթ պարունակող ֆայլերը,
- բեռնավորվող վիրուսներ. սրանք վնասում են կոշտ ու ճկուն սկավառակների համակարգչային տիրույթները,
- տրոյական վիրուսներ. սրանք իրենց «գաղտնի» աշխատանքի ընթացքում մի համակարգչից տեղեկություններ հավաքելով՝ ինտերնետով դրանք այլ համակարգիչ են ուղարկում և այլն:

Դաս 6. Ֆայլային վիրուսներ

<u>ֆայլային վիրուսներ</u> (երբեմն զանազանում են սրանց ծրագրային և մակրովիրուսային տարբերակները). սրանք վարակում են սկավառակների վրա եղած ծրագրեր և փաստաթղթեր պարունակող ֆայլերը: Վերջերս հատկապես տարածում են գտել այնպիսի մակրովիրուսներ, որոնք ունակ են ներդրվելու միանգամից մի քանի հավելվածներում. այդպիսին է, օրինակ Nriplicate անունը կրողվիրուսը:Նման վիրուսակիր ծրագրի աշխատանքը սկսելուց հետո վիրուսը տեղակայվում է համակարգչի օպերատիվ հիշողության մեջ և կարող է մինչև մեքենան անջատելը վարակել այդ ընթացքում կիրառված ծրագրերը:

Դաս 7. Բեռնավորվող վիրուսներ

Բեռնավորվող վիրուսներ. սրանք վնասում են սկավառակների այն տիրույթները, որոնք ծառայում են օպերացիոն համակարգի բեռնավորման համար: Նման վիրուսի օրինակ է հայտնի Win95CIH «Չեռնոբիլ» անվամբ վիրուսը, որը1998 թվականի գարնանը հազարավոր համակարգիչներ շարքից հանեց:

Դաս 8. Տրոյական վիրուսներ

Տրոյական վիրուսներ. սրանք այն վտանգավոր վիրուսներն են, որոնք ունակ են «գաղտնի» աշխատելու: Այդ ընթացքում կարող են ոչ միայն համացանց մտնելուՁեր գաղտնաբառը, այլև վարկային կտրոնի համարն իմանալ, այնուհետև այդ տեղեկություններն համացանցով այլ համակարգիչ ուղարկել: Հիմնավորվելով վերջինիս վրա՝ նման վիրուսներն այնուհետև սկսում են գործել Ձեր անունից:

Դաս 9. Համակրագչային վիրուսների տարածման ձևերը

Վիրուսի հիմնական աղբյուր կարող է լինել.

- վիրուսակիր ֆայլ պարունակող սկավառակը,
- համակարգչային ցանցը, այդ թվում՝ էլեկտրոնային փոստն ու ինտերնետը,
- վիրուսով վարակված կոշտ սկավառակը,
- օպերացիոն համակարգում թաքնված վիրուսը:

Դաս 10. Համակարգչային վիրուսների տարածման դեմ պայքարի եղանակները

Ինչպե՞ս պաշտպանվել վիրուսներից:
Նախ՝ պետք է հնարավորինս սահմանափակել համակարգչին առնչվող մարդկանց քանակը՝ այդ նպատակով հատուկ նշանաբան կիրառելով: Սակայն ամենակարևորը՝ պետք է ունենալ և ժամանակ առ ժամանակ կիրառել **հակավիրուսային միջոցներ**: Նման ծրագրերը հնարավորություն են տալիս հայտնաբերել վարակված ֆայլերը, վերականգնել («բուժել») դրանք՝ հեռացնելով վիրուսակիր մասերը: Գոյություն ունեն նաև հատուկ հակավիրուսային ծրագրեր, որոնք ամեն անգամ սկավառակին դիմելիս ստուգում են դրա վրա վիրուսի առկայությունը և հայտնաբերելիս՝ հայտնում այդ մասին: Որոշ դեպքերում մինչև «բուժելը» ֆայլը վիրուսի կողմից այնպիսի փոփոխությունների է ենթարկված լինում, որ այլևս այն չի հաջողվում վերականգնել. նման ֆայլերը պետք է ջնջվեն, ոչնչացվեն:

Միշտ պետք է հակավիրուսային ծրագրով ստուգենք համակարգչին միացնվող արտաքին հիշողության կրիչները, որոնք եթե միացվում են մի քանի համակարգիչների կարող են իրենց մեջ պարունակել համակարգչային վիրուսներ:

Եթե աշխատում ենք համացանցով միշտ պետք է հակավիրուսային ծրագրի բազան թարմ վիճակում լինի, որ կարողանա հայտնաբերել համացանցում օրեցոր ավելացող վիրուսները:

Դաս 11. Պաշտպանում համակարգչային վիրուսներից

Ներկայումս վիրուսակիր ծրագրերի դեմ կիրառվող բազմաթիվ 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 այն հնարավոր չէ վերականգնել, ապա օգտվողի ցուցումով այն կարելի է ջնջել: Լայնորեն կիրառվող հակավիրուսային միջոցներից են Kaspersky, Dr. Web 7, ESET NOD32, Norton Int. Security, BitDefender, Comodo, Aviraև Avast փաթեթները:

Դաս 12. Հակավիրուսային ծրագրեր

Ներկայումս վիրուսակիր ծրագրերի դեմ կիրառվող բազմաթիվ **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 այն հնարավոր չէ վերականգնել, ապա օգտվողի ցուցումով այն կարելի է ջնջել:

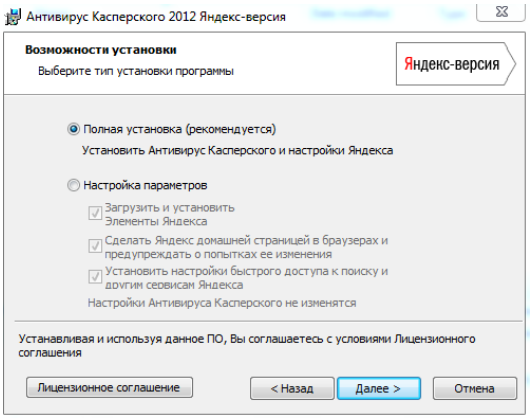
Dr.Web, NOD32, Norton AntiVirus, Kaspersky Anti-Virus, Avast ծրագրերը ներկայումս լայնորեն կիրառվող հակավիրուսային միջոցներից են:
Dr.Web-ը լայնորեն տարածված հակավիրուսային ծրագիր է, որը մեծ հավանականությամբ ունակ է բացահայտել նույնիսկ անհայտ վիրուսները:
NOD32-ը շատ արագ աշխատող հակավիրուսային ծրագիր է, որն արդյունավետ կերպով համակարգիչը պաշտպանում է հնարավոր վիրուսներից և, այսպես կոչված, «լրտեսական» ծրագրերից, 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 առկա վիրուսները, ավտոմատ կերպովմեկուսացնում է «լրտես» ծրագրերը, չի թույլատրում «վարակված» նամակներտարածել, բացահայտում է օպերացիոն համակարգում թաքնված «սպառնալիքները», համակարգիչը պաշտպանում ինտերնետային «որդերից», որոնք վիրուսակիր ծրագրեր են, և իրենց պատճենները տարածում են լոկալ կամ ինտերնետային ցանցերի միջոցով:
Kaspersky Anti-Virus-ը նույնպես ամենատարածվածներից է: Կիրառվող հատուկ մշակված ալգորիթմի շնորհիվ այս ծրագիրն անսխալ կողմնորոշվում է վիրուսներ ախտորոշելիս, ընդ որում՝ ի հայտ է բերում անգամ դեռևս անհայտ նոր վիրուսներ: Ծրագիրը կարողանում է «բռնել» նաև այնպիսի վիրուսներ, որոնք ներդրվում են Microsoft Office-ի փաստաթղթերում:
Avast-ը կարողանում է գտնել ինչպես համակարգչի կոշտ սկավառակի վրա,

այնպես էլ հիշողության մեջ և սկավառակի բեռնավորիչ սեկտորներում եղած վիրուսները: Այս ծրագիրն ավտոմատ ստուգում է ստացված նամակները: **Avast**-ի դրականհատկություններից է նաև այն, որ թարմ տարբերակները կարելի է ստանալ ինտերնետի միջոցով: Ընդ որում՝ այս ծրագիրն ունի պարզ ու հասկանալի երկխոսային համակարգ և կիրառման մատչելի ձև:
վճարովի:

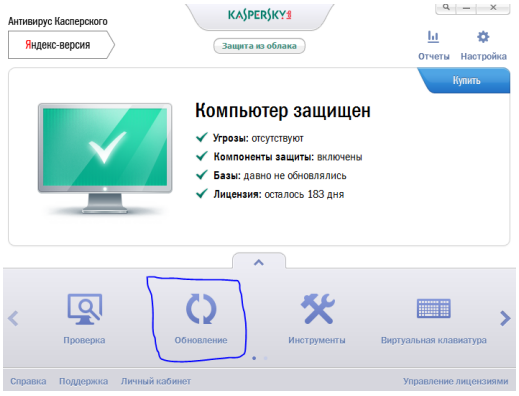
Հակավիրուսային ծրագրեր

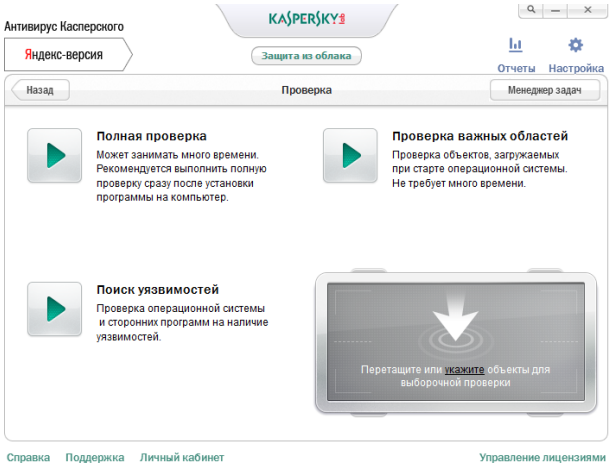
Դաս 1. Kaspersky Anti-Virus
Դաս 2. Kaspersky Anti-Virus-ի տեղադրում
Դաս 3. Kaspersky Anti-Virus-ի թարմացում
Դաս 4. Kaspersky Anti-Virus -ով համակարգչի կամ ֆայլի զննում

Kaspersky Anti-Virus-ը ամենատարածվածներից է: Կիրառվող հատուկ մշակված ալգորիթմի շնորհիվ այս ծրագիրն անսխալ կողմնորոշվում է վիրուսներ ախտորոշելիս, ընդ որում՝ ի հայտ է բերում անգամ դեռևս անհայտ նոր վիրուսներ: Ծրագիրը կարողանում է «բռնել» նաև այնպիսի վիրուսներ, որոնք ներդրվում են Microsoft Office-ի փաստաթղթերում:
Հակավիրուսային ծրագիրը տեղարելու համար կրկնակի սեղմում ենք ինստալացիոն փաթեթի վրա(որը նախօրոք բեռնում ենք պաշտոնական կայքից) և հետևում քայլերին սեղմելով Next այնուհետև Finish:



Հակավիրուսային ծրագիրը միշտ պետք է թարմ բազա իր մեջ պարունակի, որպեսզի կարողանա գտնել ամենավերջին ստեղծված վիրուսները: Հիմնականում եթե համակարգչը միացված է համակագչին թարմացումը կատարվում է ավտոմատ:





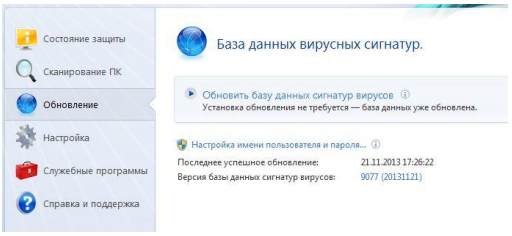
Համակարգչում վիրուս փնտրելու համար հակավիրուսային ծրագիրը առաջարկում է մի քանի տարբերակ՝ արագ, ամբողջական, կարևոր օբյեկտների, կամ մենք ենք ընտրում ֆայլը, տեղափոխելով հատուկ դաշտի մեջ կամ բացելով այդ դաշտից:

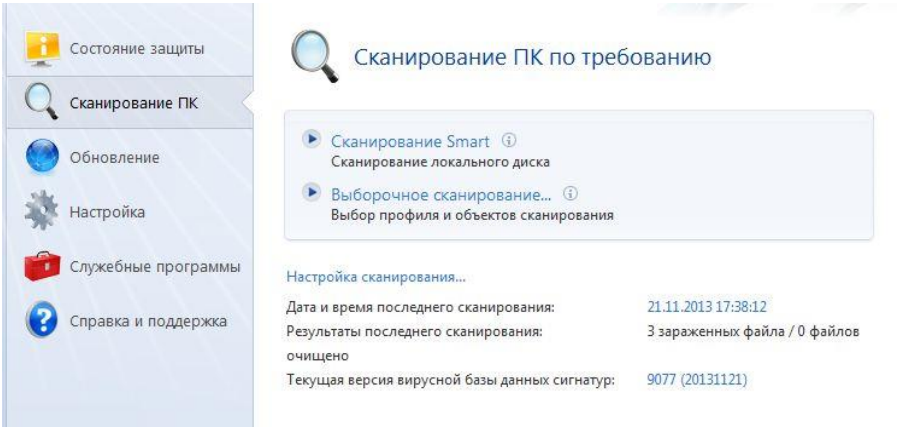
Դաս 5. ESET Smart Security
Դաս 6. ESET Smart Security-ի տեղադրում
Դաս 7. ESET Smart Security-ի թարմացում
Դաս 8. ESET Smart Security-ով համակարգչի կամ ֆայլի զննում

Հակավիրուսային ծրագիրը տեղարելու համար կրկնակի սեղմում ենք ինստալացիոն փաթեթի վրա(որը նախօրոք բեռնում ենք պաշտոնական կայքից) և հետևում քայլերին սեղմելով Next այնուհետև Finish:

Հակավիրուսային ծրագիրը միշտ պետք է թարմ բազա իր մեջ պարունակի, որպեսզի կարողանա գտնել ամենավերջին ստեղծված վիրուսները: Հիմնականում եթե համակարգչը միացված է համակագչին թարմացումը կատարվում է ավտոմատ:

Կարելի է նաև ձեռքով թարմացնել հակավիրուսային ծրագրի բազան:



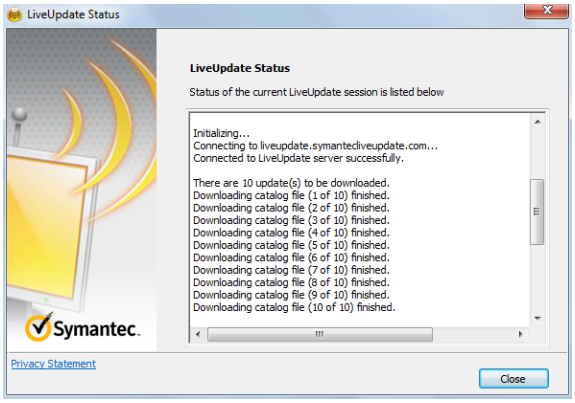


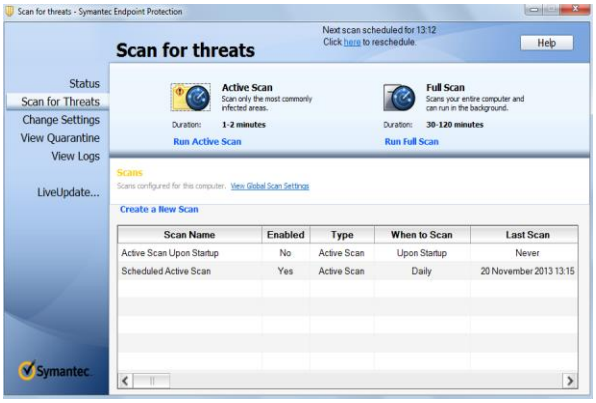
Համակարգչում վիրուս փնտրելու համար հակավիրուսային ծրագիրը առաջարկում է մի քանի տարբերակ՝ ամբողջական զննում և ընտրովի այսինքն մենք ենք ընտրում ֆայլը, և սկանավորում:

Դաս 9. Symantec Endpoint protection
Դաս 10. Symantec Endpoint protection-ի տեղադրում
Դաս 11. Symantec Endpoint protection-ի թարմացում
Դաս 12. Symantec Endpoint protection-ով համակարգչի կամ ֆայլի զննում

Հակավիրուսային ծրագիրը տեղարելու համար կրկնակի սեղմում ենք ինստալացիոն փաթեթի վրան հետևում քայլերին սեղմելով Next այնուհետև Finish: Ի տարբերություն մյուս հակավիրուսային ծրագրերի այս ծրագիրը ունի սերվեր և խաճախորդ տեսակներ, հաճախորդը նախատեսված է անհատական համակարգիչների համար, իսկ սերվերը նախատեսված է համակարգչային ցանցերում տեղակայելու համար:

Թարմացումը կտարվում է ձեռքով սեղմելով LiveUpdate

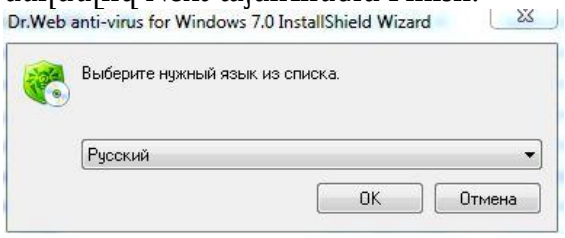


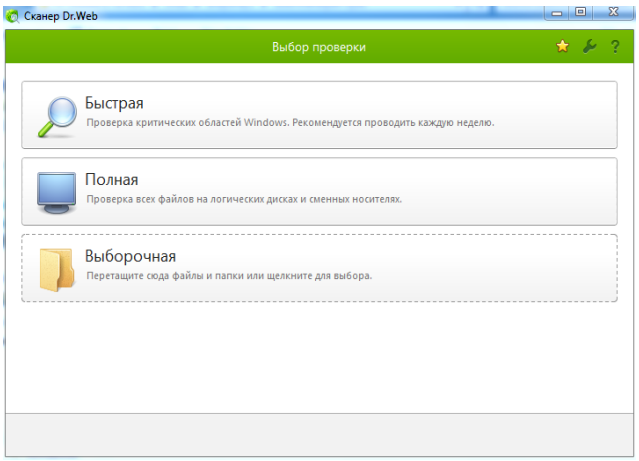


Համակարգչում վիրուս փնտրելու համար հակավիրուսային ծրագիրը առաջարկում է մի քանի տարբերակ՝ ակտիվ մասերի և ընտրովի այսինքն մենք ենք ընտրում ֆայլը, և սկանավորում:

Դաս 13. Dr.Web AntiVirus
Դաս 14. Dr.Web AntiVirus-ի տեղադրում
Դաս 15. Dr.Web AntiVirus-ի թարմացում
Դաս 16. Dr.Web AntiVirus-ով համակարգչի կամ ֆայլի զննում

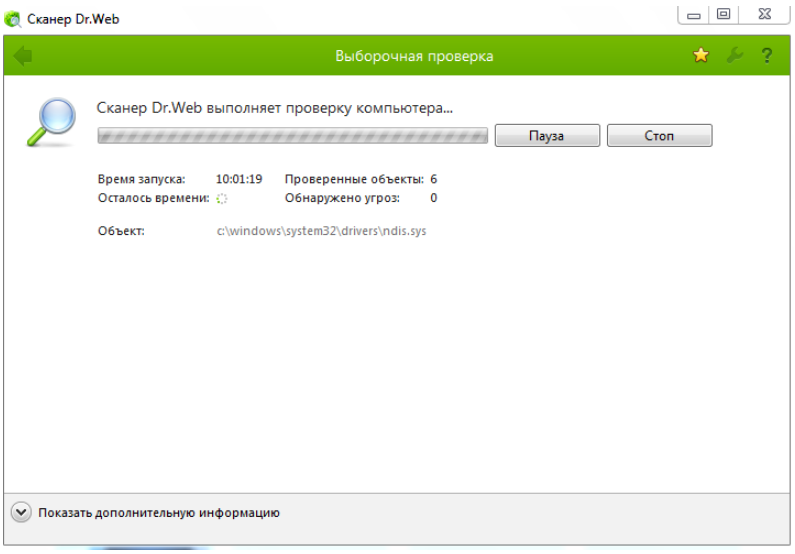
Dr.Web-ը լայնորեն տարածված հակավիրուսային ծրագիր է, որը մեծ հավանականությամբ ունակ է բացահայտել նույնիսկ անհայտ վիրուսները:
Հակավիրուսային ծրագիրը տեղարելու համար կրկնակի սեղմում ենք ինստալացիոն փաթեթի վրա(որը նախօրոք բեռնում ենք պաշտոնական կայքից) և հետևում քայլերին սեղմելով Next այնուհետև Finish:





Հակավիրուսային ծրագիրը միշտ պետք է թարմ բազա իր մեջ պարունակի, որպեսզի կարողանա գտնել ամենավերջին ստեղծված վիրուսները: Հիմնականում եթե համակարգչը միացված է համակագչին թարմացումը կատարվում է ավտոմատ:

Կարելի է նաև ձեռքով թարմացնել հակավիրուսային ծրագրի բազան



Համակարգչում վիրուս փնտրելու համար հակավիրուսային ծրագիրը առաջարկում է մի քանի տարբերակ՝ արագ,ամբողջական զննում և ընտրովի այսինքն մենք ենք ընտրում ֆայլը, և սկանավորում:

Դաս 17. Norton AntiVirus

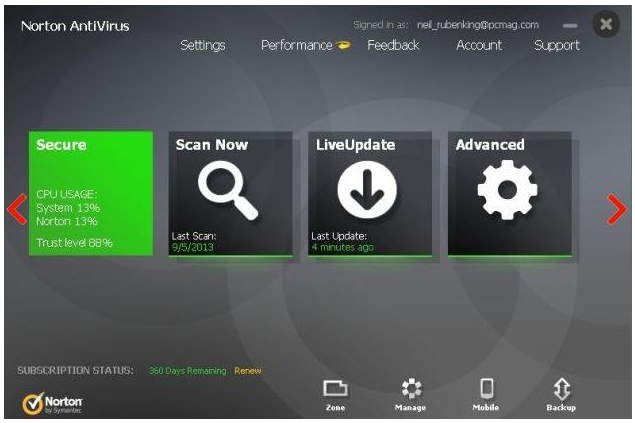
Դաս 18. Norton AntiVirus-ի տեղադրում

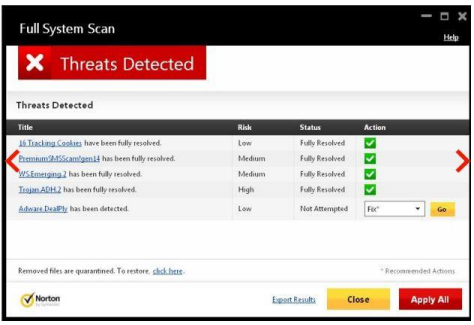
Դաս 19. Norton AntiVirus-ի թարմացում

Դաս 20. Norton AntiVirus -ով համակարգչի կամ ֆայլի զննում

Norton Antivirus-ը նույնպես աշխարհում ամենակիրառվող հակավիրուսային միջոց-ներից է: Այս ծրագիրը գտնում և ոչնչացնում է առկա վիրուսները, ավտոմատ կերպովմեկուսացնում է «լրտես» ծրագրերը, չի թույլատրում «վարակված» նամակներտարածել, բացահայտում է օպերացիոն համակարգում թաքնված «սպառնալիքները», համակարգիչը պաշտպանում ինտերնետային «որդերից», որոնք վիրուսակիր ծրագրեր են, և իրենց պատճենները տարածում են լոկալ կամ ինտերնետային ցանցերի միջոցով:
Հակավիրուսային ծրագիրը տեղարելու համար կրկնակի սեղմում ենք ինստալացիոն փաթեթի վրա(որը նախօրոք բեռնում ենք պաշտոնական կայքից) և հետևում քայլերին սեղմելով Next այնուհետև Finish:

Հակավիրուսային ծրագիրը միշտ պետք է թարմ բազա իր մեջ պարունակի, որպեսզի կարողանա գտնել ամենավերջին ստեղծված վիրուսները: Հիմնականում եթե համակարգչը միացված է համակագչին թարմացումը կատարվում է ավտոմատ:

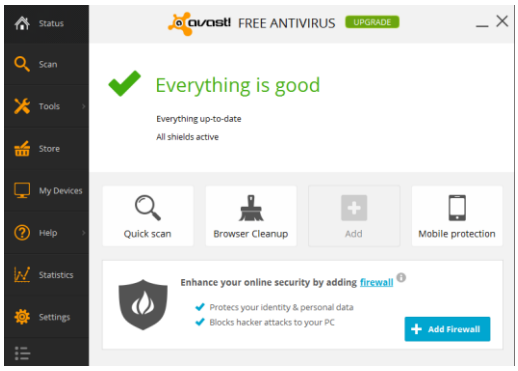




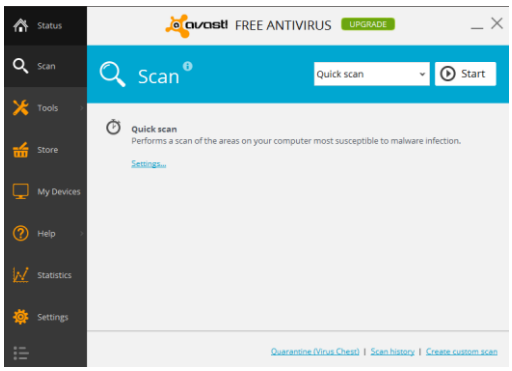
Համակարգչում վիրուս փնտրելու համար հակավիրուսային ծրագիրը առաջարկում է մի քանի տարբերակ՝ արագ,ամբողջական զննում և ընտրովի այսինքն մենք ենք ընտրում ֆայլը, և սկանավորում:

Դաս 21. Avast AntiVirus
Դաս 22. Avast AntiVirus-ի տեղադրում
Դաս 23. Avast AntiVirus -ի թարմացում
Դաս 24. Avast AntiVirus -ով համակարգչի կամ ֆայլի զննում

Avast-ը կարողանում է գտնել ինչպես համակարգչի կոշտ սկավառակի վրա, այնպես էլ հիշողության մեջ և սկավառակի բեռնավորիչ սեկտորներում եղած վիրուսները: Այս ծրագիրն ավտոմատ ստուգում է ստացված նամակները: Avast-ի դրականհատկություններից է նաև այն, որ թարմ տարբերակները կարելի է ստանալ ինտերնետի միջոցով: Ընդ որում՝ այս ծրագիրն ունի պարզ ու հասկանալի երկխոսային համակարգ և կիրառման մատչելի ձև:
վճարովի:

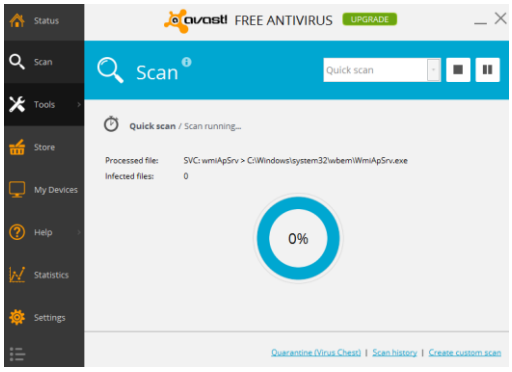


Հակավիրուսային ծրագիրը տեղարելու համար կրկնակի սեղմում ենք ինստալացիոն փաթեթի վրա(որը նախօրոք բեռնում ենք պաշտոնական կայքից) և հետևում քայլերին սեղմելով Next այնուհետև Finish:



Հակավիրուսային ծրագիրը միշտ պետք է թարմ բազա իր մեջ պարունակի, որպեսզի կարողանա գտնել ամենավերջին ստեղծված վիրուսները:

Հիմնականում եթե համակարգչը միացված է համակագչին թարմացումը կատարվում է ավտոմատ:



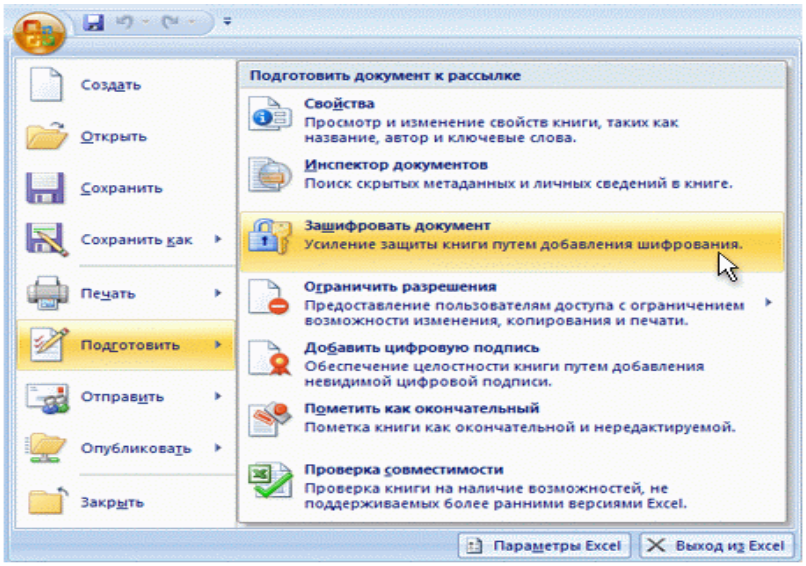
Համակարգչում վիրուս փնտրելու համար հակավիրուսային ծրագիրը առաջարկում է մի քանի տարբերակ՝ ամբողջական զննում և ընտրովի այսինքն մենք ենք ընտրում ֆայլը, և սկանավորում:

Ֆայլերի, թղթապանակների ծածկագրում

Դաս 1-3. Ֆայլը պաշտպանել ծածկագրով

Microsaft Office ֆայլերը կոդավորելու համար՝ File-Save As-Tools-General Options դաշտում մուտքագրում ենք ծածկագիրը և պահպանում: Ծածկագիրը ջնջելու համար պետք է նույն դաշտից հեռացնենք ծածկագիրը և պահպանենք ֆայլը:

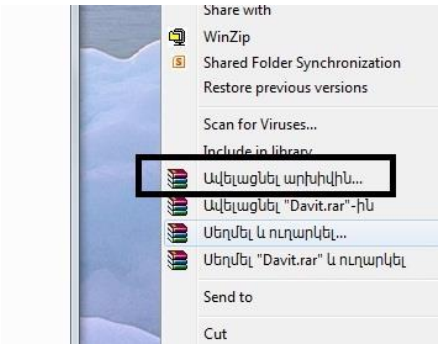
Կոդավորման մեկ այլ եղանակ պատկերված է նկարում



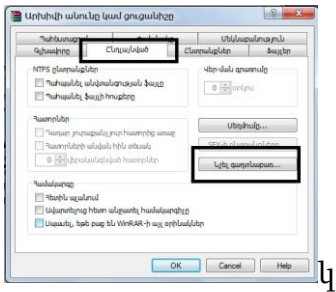
Առաջադրանք: Ստեղծել ֆայլ և կոդավորել այն: Հեռացնել և փոփոխել կոդը:

Դաս 4-6. Թղթապանակը պաշտպանել ծածկագրով

Թղթապանակը ծածկագրով պաշտպանելու համար կան հատուկ ծրագրեր: Օր. WinRar ծրագրով կարող ենք կոդավորենք և արխիվացնենք ֆայլը:



Պետք է անհրաժեշտ թղթապանակի վրա մկնիկի աջ ստեղնով սեղմենք և ընտրեք նկարում պատկերված հրամանին: Այնուհետև



կատարում նկարած ֆայլերը:

Թղթապանակները ծածկագրելու համար կան բազմաթիվ ծրագրեր: Օր. Password Protect USB շատ պարզ ծրագիր է և հեշտությամբ կարողանում ենք ծածկագրել թղթապանակը և հեռացնել ծածկագիրը:

Դաս 7. Ֆայլի ծածկագրի փոփոխում, հեռացում

Microsaft Office ֆայլերը կոդավորելու համար՝ File-Save As-Tools-General Options դաշտում մուտքագրում ենք ծածկագիրը և պահպանում: Ծածկագիրը ջնջելու համար պետք է նույն դաշտից հեռացնենք ծածկագիրը և պահպանենք ֆայլը, փոփոխելու համար նույն դաշտում փոխում ենք ծածկագիրը և պահպանում:

Առաջադրանք: Ստեղծել ֆայլ և կոդավորել այն: Հեռացնել և փոփոխել կոդը:

Դաս 8. Ֆայլի ծածկագրի փոփոխում

Microsaft Office ֆայլերը կոդավորելու համար՝ File-Save As-Tools-General Options դաշտում մուտքագրում ենք ծածկագիրը և պահպանում: Ծածկագիրը ջնջելու համար պետք է նույն դաշտից հեռացնենք ծածկագիրը և պահպանենք ֆայլը, փոփոխելու համար նույն դաշտում փոխում ենք ծածկագիրը և պահպանում:

Առաջադրանք: Ստեղծել ֆայլ և կոդավորել այն: Հեռացնել և փոփոխել կոդը:

Դաս 9. Ֆայլի ծածկագրի հեռացում

Microsaft Office ֆայլերը կոդավորելու համար՝ File-Save As-Tools-General Options դաշտում մուտքագրում ենք ծածկագիրը և պահպանում: Ծածկագիրը ջնջելու համար պետք է նույն դաշտից հեռացնենք ծածկագիրը և պահպանենք ֆայլը:

Առաջադրանք: Ստեղծել ֆայլ և կոդավորել այն: Հեռացնել և փոփոխել կոդը:

Դաս 10. Թղթապանակի ծածկագրի փոփոխում, հեռացում

Դաս 11. Թղթապանակի ծածկագրի փոփոխում

Դաս 12. Թղթապանակի ծածկագրի հեռացում

Դասի նպատակը՝ ուսանողը կարողանա ներկայացնի և կատարի թղթապանակի ծածկագրի փոփոխումը, հեռացումը

Password Protect USB շատ պարզ ծրագիր է և հեշտությամբ կարողանում ենք ծածկագրել թղթապանակը և հեռացնել ծածկագիրը:

Lock folders դաշտով ընտրում ենք մեզ անհրաժեշտ թղթապանակը և ծածկագիր տեղադրում: Թղթապանակի տեսքը փոխվում է՝

Unlock folders –ի միջոցով ընտրում ենք թղթապանակը և հեռացնում ծածկագիրը: Այնուհետև կարող ենք փոխել և նոր ծածկագիր օգտագործենք:

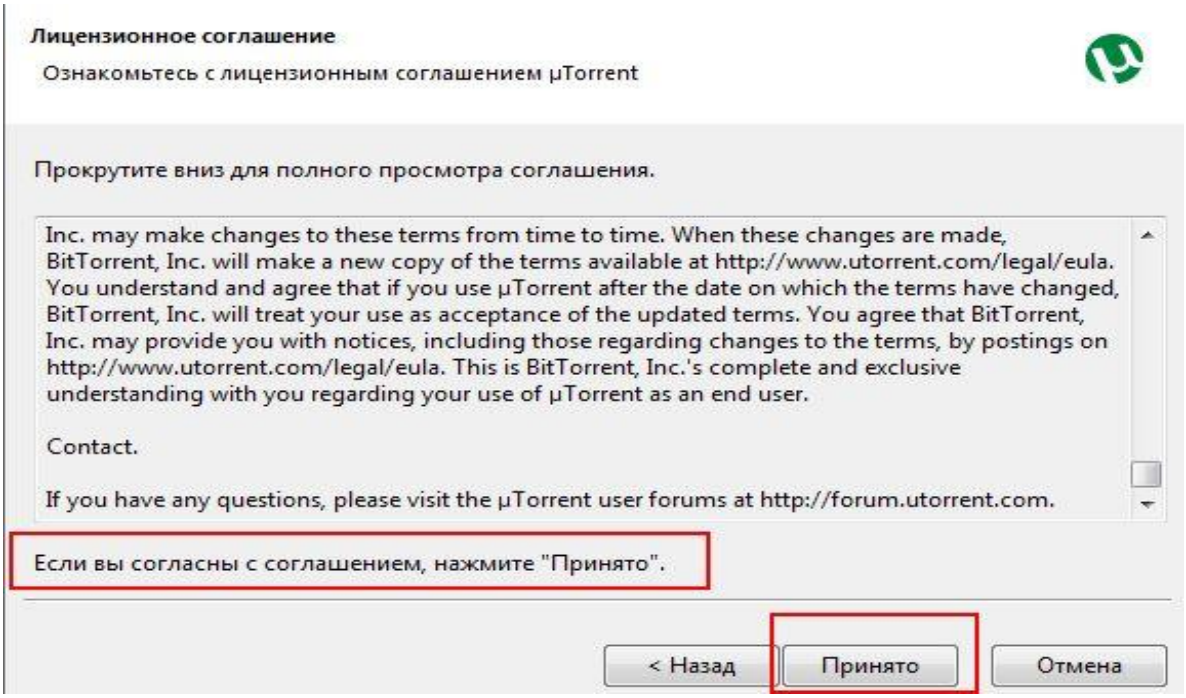
Ծրագրերի օգտագործողների իրավունքներ

Դաս 1. Տվյալներ և ծրագրեր օգտագործողների իրավունքներ
Դաս 2. Ըստ իրավական կարգավիճակի ծրագրերի հիմնական խմբերը
Դաս 3. Լիցենզավորված ծրագրեր
Դաս 4. Պայմանականորեն անվճար ծրագրեր
Դաս 5. Ազատ տարածվող ծրագրեր
Դաս 6. Հեղինակային իրավունքի նորմեր

Երբ մենք հանդես ենք գալիս որպես ծրագիր կամ որևէ տվյալ օգտագործող մենք ձեռք ենք բերում որոշակի իրավունքներ և պարտականություններ, որոնք ամրագրված են այն պայմանագրում, որը կնքում ենք տվյալ ծրագիրը տեղադրելու ժամանակ: Այդ պայմանները կարող են տարբեր լինել պայմանավորված ծրագրերը արտադրող ընկերություններից: Մենք պետք է ուշադիր լինենք թե ինչի հետ ենք համաձայնվում ծրագիրը տեղադրելու ժամանակ և չխախտենք այդ պայմանները:

Ըստ իրավական կարգավիճակի ծրագրերի լինում են լիցանզավորված, պայմանականորեն անվճար և ազատ տարածվող:

Եթե մենք ներբեռնում ենք համակարգչային ծրագիր և տեղադրում ենք մեր համակարգչում, ապա տեղադրելիս մենք կնքում ենք իրավաբանական պայմանագիր՝ լիցենզավորված ծրագիր տարածող ընկերության հետ, և այդ պայմանագիրը ավարտվում է մեր կողմից ծրագիրը ջնջելուց հետո: Ծրագիրը տեղադրելուց հետո մենք իրավունք չունենք այդ ծրագիրը մոդիֆիկացիայի ենթարկել, թարգմանել, փոփոխել, այդ նույն հիմքով նմանատիպ ծրագիր ստեղծել, այդ ծրագրով անօրինական գործողություններ կատարել: Ցանկացած ծրագիր տեղադրելուց առաջ պետք է ուշադիր կարդանք Лицензионное соглашение, եթե համաձայն ենք պայմանների հետ նոր սեղմենք Принято և շարունակենք ծրագրի տեղադրումը համակարգչում: Իսկ հետագայում այդ ծրագիրը օգտագործելիս չպետք է խախտենք իրավաբանական պայմանագիր, որը կնքել ենք ծրագիրը ստեղծած ընկերության հետ:



Կան ծրագրեր, որոնք "ազատ տարածվող" են և գործում են լիարժեք: Օր. Google Chrom, Google Earth, Skype, և այլն: "Ազատ տարածվող" ծրագրերում արտադրողի կողմից կարող է ավելացվել այլ ծրագրեր (бραузер, mail.ru агент, bing որոնման համակարգ և այլն): Պետք է ծրագիրը տեղադրելու ժամանակ ուշադիր կարդալ և անջատել այդ ծրագրերը եթե մեզ հարկավոր չեն:

Այն փաթեթներն ու ծրագրերը, որոնք "ազատ տարածվող" չեն ներկայացված են լինում Demo տարբերակով կամ ունեն գործածության որոշակի ժամկետ (հիմնականում 30 օր): Վերջիններիս լիարժեք տարբերակները վճարովի են, և կարող են ձեռք բերվել դրանց հեղինակների կայքերից: Օր. համակարգչային անտիվիրուսները, օպերացիոն համակարգերը և այլն:

Կան նաև պայմանականորեն ազատ տարածվող ծրագրեր: Դրանց տարածումը կախված է ծրագիրը արտադրող ընկերության հայեցողությունից:

Հեղինակ է ճանաչվում այն ֆիզիկական անձը կամ կազմակերպությունը, ով ստեղծել է ծրագիրը:

Հեղինակային իրավունքի առանձնահատկությունը կայանում է նրանում, որ հեղինակային իրավունքն առաջանում է ստեղծագործության ստեղծման փաստի ուժով, այն պահից, երբ անձն (կազմակերպությունը) իր ստեղծագործական կարողությունների շնորհիվ ստեղծում է հեղինակային իրավունքի որեւէ օբյեկտ, որը դառնում է երրորդ անձանց համար հասանելի, դա պատկանում է իրեն՝ հեղինակային իրավունքով, պաշտպանվում հեղինակային իրավունքի նորմերով: Հեղինակային իրավունքի խախտումը առաջացնում է պատասխանատվություն օրենքի առջև: Այնպես որ պետք է ուշադիր լինենք և չխախտենք այն ծրագրերի հեղինակային իրավունքները, որոնք օգտագործում ենք:

Առաջադրանք: Տեղադրել որևէ ծրագիր համակարգչում և ուսումնասիրել այն պայմանագիրը, որը կնքում ենք այդ ընկերության հետ: