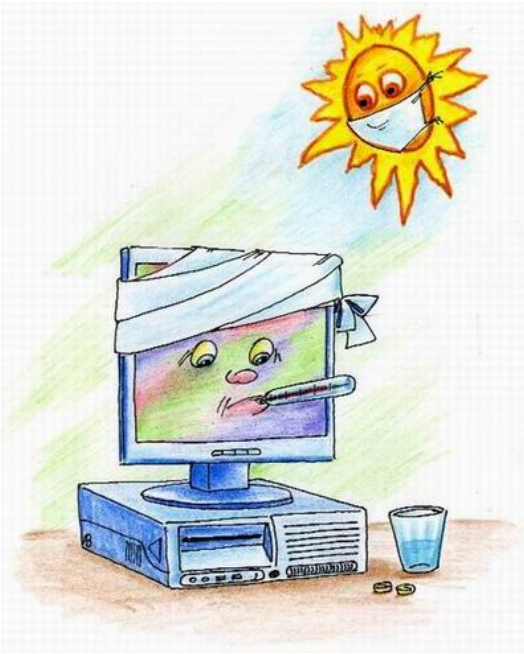
§ 2.3.Համակարգչային վիրուսներ և հակավիրուսային ծրագրեր

Առաջին վտանգը, որը կարող է հանդիպելհամակարգչին առնչվող յուրաքանչյուրին՝ *համակարգչայինվիրուսն* է: Համակարգչային վիրուսի առաջին «համաճարակը» տեղի ունեցավ *1986* թվականին, երբ *Brain* (ուղեղ) անվամբ վիրուսովսկսեցին «վարակվել» ճկուն մագնիսական սկավառակները: Ներկայումս հայտնի են մոտ*5* հազարից ավելի վիրուսներ, որոնք տարածվելով համակարգչային ցանցով՝ վարակում են դրանց հետ համագործակցող համակարգիչները:

Ընդհանուր առմամբ վիրուսը փոքրածավալ ծրագիր է, որիստեղծողներն



այնմեծապես օժտում են նաև «ինքնաբազմացման» ունակությամբ: Վիրուսակիր ծրագիրը կարող է ամենատարբեր գործողությունների «հեղինակ» հանդիսանալ՝ սկսած ամենաանմեղներից՝ էկրանին բերվող պատկերի աղավաղում, երաժշտական հոլովակների ցուցադրում և այլն, մինչև լրջորեն վնասելը՝ համակարգչային տվյալների ոչնչացում և նույնիսկհամակարգչի առանձին միկրոսխեմաների անսարքության առաջացում: Համակարգիչը վարակելուց հետովիրուսը կարող է «թաքնվել» ու «հարձակման անցնել» որոշակի իրադարձությունից՝ շաբաթվա որևէ օրվանից, կոնկրետ ամսաթվից, կիրառական որևէ ծրագրի աշխատելուց, փաստաթուղթ բացելուց հետո միայն:

Ասենք, որ տեքստային բնույթկրողֆայլերը վիրուսակիր չենլինում, սակայն վիրուսը կարող է փոփոխման ենթարկել դրանք:

Վիրուսակիր ծրագրերը կարող են տեղակայվել հաճախակի կիրառվող ծրագրային ֆայլերի տարբեր մասերում՝ դրանց սկզբում, միջնաբասում կամ վերջում:

Կախված այն բանից, թե ինչտիպի ծրագրեր են վարակում՝ վիրուսները կարելի է բաժանել հետևյալ տիպերի.

- ✓ *ֆայլային* (երբեմն զանազանում են սրանց *ծրագրային* և *մակրովիրուսային* տարբերակները). սրանք վարակում են սկավառակների վրա եղած ծրագրեր և փաստաթղթեր պարունակող ֆայլերը: Վերջերս հատկապես տարածում են գտելայնպիսի *մակրովիրուսներ*, որոնք ունակ են ներդրվելու միանգամից մի քանի հավելվածներում. այդպիսին է, օրինակ *Nriplicate*անունը

կրողվիրուսը:Նման վիրուսակիր ծրագրի աշխատանքը սկսելուցհետովիրուսը տեղակայվում է համակարգչի օպերատիվ հիշողության մեջ և կարող է մինչև մեքենան անջատելը վարակել այդ ընթացքում կիրառված ծրագրերը:

- ✓ *բեռնավորվող*. սրանք վնասում են սկավառակների այն տիրույթները, որոնք ծառայում են օպերացիոն համակարգի բեռնավորման համար: Նման վիրուսի օրինակ է հայտնի *Win95CIH* «Չեռնոբիլ» անվամբ վիրուսը, որը *1998* թվականի գարնանը հազարավոր համակարգիչներ շարքից հանեց:
- ✓ *տրոյական*. 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:

Իսկ ի՞նչ «ախտանիշներով» է բնորոշվում վիրուսի առկայությունը.

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:

Իսկինչպե՞ս պաշտպանվել նման վտանգ ներկայացնող 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:

Լայնորեն կիրառվող հակավիրուսային միջոցներից են *Kaspersky*, *Dr. Web 7, ESETNOD32, NortonInt. Security, BitDefender, Comodo, Aviraև Avast* փաթեթները:

Օգտակար է իմանալ

Համակարգիչները վիրուսակիր ծրագրերից պաշպանելու համար պետք է՝

- հակավիրուսային ծրագրերի օգնությամբ պարբերաբար ստուգել համակարգչի աշխատունակությունը,
- մինչև սկավառակներից ինֆորմացիա կարդալը՝ ստուգել դրա վրա վիրուսի առկայությունը,
- այլ համակարգիչներով աշխատելիս սկավառակները պաշտպանել դրանց վրա ինֆորմացիա գրանցելուց,
- արժեքավոր տվյալների ֆայլերի կրկնօրինակ ստեղծել,
- սկավառակը չթողնել սկավառակակրի մեջ,
- չօգտագործել անհասկանալի «պահվածքով» ծրագրեր,
- հակավիրուսային ծրագրերը պարբերաբար թարմացնել (փոխարինել դրանց նոր տարբերակներով):

Հարցեր և առաջադրանքներ

1. Նշեք մի քանի պատճառներ, որոնք նպաստում են համակարգչում պահպանվող ինֆորմացիայի խեղաթյուրմանը կամ ոչնչացմանը:
2. Թվարկեք համակարգչային ինֆորմացիան պաշտպանելու ձեզ հայտնի մի քանի կանոններ:
3. Ի՞նչ է համակարգչային վիրուսը:
4. Ի՞նչ տիպի համակարգչային վիրուսներ գիտեք:
5. Հակավիրուսային ծրագրերի ի՞նչ փաթեթներ են ձեզ հայտնի:
6. Համակարգչում առկա որևէ հակավիրուսային ծրագրի օգնությամբ ստուգեք ճկուն սկավառակը: