ՍԵՐԳԵՅ ԱՎԱՆԵՍՅԱՆ, ՕԼՅԱ ՂՈՒԼՅԱՆ, ՋԱՐԻՆԵ ԱԲԳԱՐՅԱՆ

ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ

ՈՒՍՈՒՄՆԱԿԱՆ ՁԵՌՆԱՐԿ

ԳՈՐԻՍ 2024

ՈՒՍՈՒՄՆԱԿԱՆ ՁԵՌՆԱՐԿ

Տեղեկատվության անվտանգություն

«Տեղեկատվության անվտանգություն» ուսումնական ձեռնարկը քննարկվել և հավանության է արժանացել Գորիսի պետական քոլեջի Մաթեմատիկայի, ինֆորմատիկայի և տնտեսագիտության ամբիոնի նիստում:

Հեղինակային խումբ

Սերգեյ Վլադիմիրի Ավանեսյան. Գորիսի պետական քոլեջի Մաթեմատիկայի, ինֆորմատիկայի և տնտեսագիտության ամբիոնի դասախոս:

Օլյա Մենիկի Ղուլյան. Գորիսի պետական քոլեջի Մաթեմատիկայի, ինֆորմատիկայի և տնտեսագիտության ամբիոնի վարիչ, դասախոս:

Զարինե Վաղարշակի Աբգարյան. Գորիսի պետական քոլեջի Մաթեմատիկայի, ինֆորմատիկայի և տնտեսագիտության ամբիոնի դասախոս:

ՆԵՐԱԾՈՒԹՅՈՒՆ

Տեղեկատվական գործոնն առաջնային նշանակություն ունի մարդկային կենսագործունեության գրեթե բոլոր ոլորտներում: Տեղեկատվական անվտանգությունը (անգլերեն Information Security, երբեմն կրճատվում է որպես InfoSec) ազգային անվտանգության կարևոր բաղադրիչ է և նրա խնդիրը արդի հիբրիդային պատերազմների ռազմավարությունում և մարտավարությունում կարևորագույն, իսկ հաճախ՝ որոշիչ դերակատարում ունեցող տեղեկատվական-հոգեբանական պատերազմների և գործողությունների արդյունավետ դիտարկումն է, քանի որ արդի աշխարհում պատերազմները մղվում են ոչ միայն զենքի և բանակների կիրառմամբ, այլև որպես ժամանակակից զենք օգտագործվում է ինվորմացիան: Ըստ չինացի ռազմական տեսաբան և մտածող Սուն Ցըզիի՝ «Հմուտ պատերազմողն օտար բանակը հպատակեցնում է առանց ճակատամարտի»: Տեղեկատվական պատերազմները պայքարի ձևեր են, որոնք նպատակ են հետապնդում հասնել հակառակորդի հոգեբանական կայունության խարխլմանը, ավանդույթների քայքայմանը, արժեքային կողմնորոշումների փոփոխմանը, ինչպես նաև ազգային գիտակցության խարխլմանը, իր համար անհրաժեշտ ինֆորմացիոն դաշտ ի ստեղծմանը: Տեղեկատվական անվտանգության (ՏԱ) արդյունավետությունը մեծապես պայմանավորված է տեղեկատվական ոլորտի վերաբերյալ հանրության գիտելիքներով, ընդհանրական մտավոր ռեսուրսներով և դրանց խելամիտ համակարգմամբ ու կառավարմամբ: Տեղեկատվական անվտանգության հիմնական նպատակն է տվյալների անվտանգության ապահովումը:

ԳԼՈՒԽ 1. ՏԵՂԵԿԱՏՎՈՒԹՅՈՒՆՆ ԱՆՑՅԱԼՈՒՄ, ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ ԵՎ ՏԵՂԵԿԱՏՎԱԿԱՆ ՊԱՏԵՐԱԶՄՆԵՐ, ՄԱՐՏԱՀՐԱՎԵՐՆԵՐԸ ԿԻԲԵՌՏԱՐԱԾՔՈՒՄ

1. «ՏՐՈՅԱԿԱՆ ՁԻ» ԳՈՐԾՈՂՈՒԹՅՈՒՆԸ

Հոմերոսի «Իլիական» պոեմի մագաղաթե ամենահին ձեռագիրը, X դար։

Ռազմական ոլորտի փորձագետների գնահատականներով, մարդկությունն իր պատմության ընթացքում վարել է մոտ 15 հազար մեծ և փոքր պատերազմներ (միայն 2000–2010թթ. տեղի է ունեցել ավելի քան 150 հակամարտություն) և ընդամենը 300 տարի է ապրել լիակատար խաղաղության պայմաններում: Տեղեկատվահոգեբանական գործոնը, բնականաբար, այս կամ այն չափով դերակատարում է ունեցել գրեթե բոլոր պատերազմներում ու քաղաքական զարգացումներում, և այդ գործոնի նշանակությունը, տեղեկատվական հեղափոխություններին զուգընթաց՝ մշտապես աճել է: Արդի ժամանակաշրջանում տեղեկատվական գործոնը, հանդիսանալով այսպես կոչված «փափուկ ուժի» և «հիբրիդային պատերազմների» կարևորագույն բաղադրամասը, վճռորոշ դերակատարում է ձեռք բերել աշխարհաքաղաքական, աշխարհատնտեսական ու հասարակական գործընթացներում: Հենց այս հանգամանքներով է պայմանավորված այն իրողությունը, որ XX դարի վերջին քառորդում մշակվեցին տեղեկատվական անվտանգության, քաղաքականության ու պատերազմների տեսական և գործնական հայեցակարգերը, որոնք կլուսաբանվեն հաջորդ գլխում:

Միևնույն ժամանակ, արդի տեսությունները ձևավորվել են անցյալում իրագործված տեղեկատվական գործողությունների համալիր վերլուծության և դրանց արդյունքների ընդհանրացման հիման վրա: Հավելենք, որ անցյալում իրագործված տեղեկատվական գործողություններում կիրառված մեթոդներից շատերն առայսօր չեն կորցրել իրենց հրատապությունը և այս կամ այն ձևափոխությամբ կիրառվում են արդի ժամանակաշրջանում նույնպես: Հայտնի է նաև, որ ցանկացած կենսագործունեության ոլորտի վերաբերյալ պատկերացումները բավական թյուր կլինեին, եթե ժամանակակիցները չվերլուծեին պատմական նախադեպերը և դասեր չքաղեին դրանցից: Պատահական չէ, որ «ժամանակների միջև կապի պահպանումը» տեղեկատվական անվտանգության կարևորագույն խնդիրներից է, և այս թեմային դեռ կանդրադառնանք:


«Լաոկոոնը և որդիները», մարմարե քանդակ, Վատիկան:

Վերոնշյալի համատեքստում այս գլխում խիստ համառոտ կներկայացվեն անցյալում կատարված ուշագրավ տեղեկատվական գործողությունները և որոշ հասարակարգերին բնորոշ՝ տեղեկատվական քաղաքականության հետ կապված զարգացումները:

Որպես հեռավոր պատմական անցյալում իրականացված տեղեկատվական գործողության դասական օրինակ հաճախ հիշատակվում է Տրոյայի գրավման՝ Ոդիսևսի մշակած և իրագործած պլանը (մ.թ.ա. XII դար): Սակայն այդ իրադարձությունը դիտարկվում է որպես հակառակորդին ապատեղեկացնելու գործողություն, ո՛չ ավելին: Մինչդեռ ավելի հանգամանալի վերլուծությունը թույլ է տալիս բացահայտել մտահղացման խորությունն ու հույների ռազմավարական

մտածողության բարձր մակարդակն այն հեռավոր ժամանակներում:


Տրոյական ձի:

Ինչպես նկարագրում է Հոմերոսն (մ.թ.ա. VIII դար) իր հանճարեղ «Իլիական» էպիկական պոեմում, հույները մոտ տասը տարի պաշարել էին Տրոյան, բայց քաղաքը գրավել չէր հաջողվում: Նրանց ջանքերը, թերևս, այդպես էլ ապարդյուն կմնային, եթե Ոդիսևսը չառաջարկեր մի փայլուն գաղափար: Ըստ նրա մտահղացման՝ հույները մի հսկայական փայտե ձի պատրաստեցին (մեզ բոլորիս հայտնի «տրոյական ձին»), որի մեջ տեղավորեցին հույն զինվորների ընտրյալ մի ջոկատ: Հետո աքեացիների (Աքեացիներ էին անվանում հունական ամենահին ցեղերից մեկին, և Հոմերոսն ընդհանրական առումով հաճախ հենց այդպես էր կոչում հույներին) զորքը հավաքեց վրանները, բեռնեց նավերն ու թողեց ծովափը, բայց ուղևորվեց ոչ թե դեպի Հունաստան, այլ Տրոյային մոտ կղզիներից մեկը՝ ափին թողնելով «փայտե ձին»:

Պարզամիտ տրոյացիները, ուրախանալով հույների «փախուստով», սկսեցին հետաքրքրությամբ ուսումնասիրել փայտե նժույգը՝ չհասկանալով դրա իմաստն ու նպատակը: Այսինքն՝ Ոդիսևսի ապատեղեկատվական գործողության մեջ կարևոր տեղ էր զբաղեցնում հոգեբանական ներգործության հայտնի էֆեկտը, երբ այս կամ այն երևույթը չհասկանալը, որպես կանոն, շփոթեցնում, ապակողմնորոշում է մարդկանց և նրանց դրդում չմտածված քայլերի. նման դրսևորումներ մենք տեսնում ենք նաև այսօր: Հենց այդ պահին էլ սկսվում է գործողության երկրորդ փուլը. իր առաջադրանքն է սկսում կատարել Իլիոնում Ոդիսևսի գաղտնի գործակալ Սինոնը: Նա սկսում է «օգնել» տրոյացիներին «հասկանալ» իրավիճակը՝ նրանց համոզելով, որ «տրոյական ձին» Աթենաս աստվածուհու նվերն է, դրա համար էլ պետք է քանդել ամրոցի պատը, «ձին» մտցնել Տրոյա և պահել որպես սրբություն: Բոլոր հատկանիշներից ելնելով՝ Սինոնին պետք է համարել որպես առաջին «ազդեցության գործակալը» և «գործակալ ագիտատորը» միաժամանակ. չէ՞ որ նրան հաջողվեց իր պերճախոսությամբ ազդել «որոշումների ընդունման» գործընթացի վրա: Ակնհայտ է, որ առանց Սինոնի ջանքերի հունական պլանը հազիվ թե իրականանար: Բայց դա դեռ ամենը չէր:

«Փայտե ձին» Տրոյա մտցնելուն ընդդիմացավ քուրմ Լաոկոոնը՝ հայտարարելով, թե դա հույների հերթական նենգությունն է և քաղաքին մեծ դժբախտություն կբերի: Այլ խոսքով՝ իմաստուն քուրմը, որը նաև կանխատեսման շնորհ ուներ, փորձում էր պաշտպանել Տրոյայի շահերը և հակաագիտացիա վարել Սինոնի դեմ: Գուցե Լաոկոոնի խոսքերն ազդեցություն ունենային, եթե (ըստ Հոմերոսի) այդ պահին ծովից դուրս չգային երկու մեծ օձեր և չխեղդեին քրմին ու նրա որդիներին (մեկ այլ, ավելի դաժան վարկածով՝ օձերը սպանեցին միայն նրա որդիներին, որպեսզի Լաոկոոնը ողջ կյանքում սգար նրանց մահն ու զղջար արածի համար): Կասկած չի հարուցում, որ օձերի հետ կապված պատմությունն առասպելաբանական այլաբանություն է: Իրականում, ամենայն հավանականությամբ, Ոդիսևսը կանխատեսել էր իրադարձությունների նման ընթացքը և, Սինոնի տիպի ազդեցության գործակալներից բացի, Տրոյայում ձևավորել էր նաև «հատուկ գործակալական խումբ», որի խնդիրն էր Սինոնի ընդդիմախոսներին չեզոքացնելը: Նրանք կատարեցին առաջադրանքը և ինչ-որ ձևով վերացրին Լաոկոոնին: Այսպիսով, ակնհայտ երևում է այն ճշմարտությունը, որ եթե երկրի անվտանգության համակարգը թերի է, ապա լավ կազմակերպված «ազդեցության գործակալներին» հաճախ հաջողվում է չեզոքացնել նրանց, ովքեր պաշտպանում են իրենց «ազգային շահերը»: Լաոկոոնի ողբերգական մահը վճռորոշ գործոն է հանդիսանում տրոյացիների համար, որպեսզի

վերջիններն ընդունեն Սինոնի առաջարկը. քաղաքի պատերը քանդվում են, և փայտե ձին տեղ է գտնում քաղաքում:

Եթե փոքր-ինչ առաջ անցնենք, ապա կարելի է տեսնել, որ Ոդիսևսի գործողությունը համապատասխանում է արդեն XX դարում ընդունված «տեղեկատվական պատերազմների» բնութագրմանը, համաձայն որոնց՝ նման պատերազմների նպատակներից է նաև այն, որպեսզի հակառակորդն ընդունի տեղեկատվական պատերազմ վարողի համար ձեռնտու որոշումներ: Մեկ այլ սկզբունքային նմանություն ևս. արդի իրողություններում, ինչպես և Տրոյական պատերազմի դարաշրջանում, հատուկ ծառայությունների գործառույթներում նկատվում է տեղեկատվական-հոգեբանական գործողությունների մասնաբաժնի էական աճ: Բավական է նշել, որ համաձայն փորձագիտական գնահատականների՝ արդի ժամանակաշրջանում ԱՄՆ Կենտրոնական հետախուզական վարչության (ԿՀՎ) ֆինանսական միջոցների գերակշիռ մասը ծախսվում է հենց նման նպատակներով:

Մնացածն արդեն, ինչպես ընդունված է ասել, տեխնիկայի գործ էր: Գիշերը զինված հույները դուրս են գալիս «տրոյական ձիուց», վերացնում են իրենց «հաղթանակը» տոնող և, թերևս, այդ պատճառով ոչ այնքան սթափ տրոյացի պահապաններին և նախապես պայմանավորված ազդանշան են տալիս մերձակա կղզում թաքնված հույներին, որոնք և շտապում են Տրոյա: Շարունակությունը հատուկ մեկնաբանությունների կարիք չունի:

Սակայն չի կարելի բացառել նաև այն վարկածը, համաձայն որի՝ «տրոյական ձին» (հատկանշական է, որ այդպես են այսօր կոչվում նաև որոշակի տիպի համակարգչային վիրուսները):

Հոմերոսի ստեղծագործական երևակայության արգասիքը եղած լինի: Եվ իսկապես, իրականում դժվար է պատկերացնել նման հսկայական «նժույգի» կառուցումը, նրա ներսում բազմաթիվ զինված մարտիկների տեղավորումը, այդ «նժույգի» տեղափոխումը Տրոյա և հետագա գործողությունները: Չի կարելի բացառել, որ մեծ պոետն այդ պատմությամբ պարզապես գեղարվեստորեն ներկայացրել է բազմաքայլ, այդ թվում նաև տեղեկատվա-հոգեբանական գործողությունների միջոցով ամրացված քաղաքները գրավելու՝ այն ժամանակ կիրառվող հունական ռազմավարությունը: Թերևս, այդ քաղաքական մշակույթի համատեքստում պետք է դիտարկել Մակեդոնիայի թագավոր Փիլիպոս Մակեդոնացուն (մ.թ.ա. IV դար, որն ավելի հայտնի է որպես Ալեքսանդր Մակեդոնացու հայր) վերագրվող այն ասացվածքը, թե քաղաքը գրավելու համար անհրաժեշտ է ոչ թե զորք ուղարկել, այլ «ոսկով բեռնված ավանակ»՝ նկատի ունենալով, որ քաղաքը կարելի է անհամեմատ ավելի դյուրին գրավել, եթե հնարավոր լինի ոսկով կաշառել նրա պաշտպաններին:

Նմանատիպ գործողությունների վերաբերյալ տեղեկատվության կուտակումը, համակարգումը և վերլուծումն էապես նպաստեցին ռազմարվեստի և դրա հետ զուգակցված տեղեկատվական գործողությունների հետագա զարգացման գործընթացին:

2. ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ. ՄԱՐՏԱՀՐԱՎԵՐՆԵՐԻ ԵՎ ՊԱՏԱՍԽԱՆՆԵՐԻ ՀԱՄԱԿԱՐԳԸ

Տեղեկատվական հինգերորդ հեղափոխության արդի ժամանակաշրջանում տեղեկատվական ոլորտում ընթացող զարգացումները և դրանց ուղեկցող տեղեկատվական պատերազմները համակել են ողջ գլոբալ հարթությունը: Տեսական և գործնական հարթություններում դա հանգեցրել է նոր հասկացությունների և հայեցակարգերի ձևավորմանը, որոնք և համառոտ կլուսաբանվեն այս գլխում:

Վերոնշյալի համատեքստում առանցքային նշանակություն է ձեռք բերել տեղեկատվական անվտանգություն (ՏԱ) հասկացությունը, որն ազգային անվտանգության (ԱԱ) կարևորագույն բաղադրամասն է հանդիսանում:

Անվտանգություն հասկացությունը, թվացյալ պարզության հետ մեկտեղ, խիստ ընդգրկուն է և գործնականորեն ներառում է հասարակության ու առանձին անհատների կենսագործունեության բոլոր ոլորտները: Ամեննին պատահական չէ, որ գրականության մեջ կարելի է հանդիպել այդ եզրի ամենատարբեր մեկնությունների և սահմանումների: Օրինակ, հաճախ կարելի է հանդիպել հետևյալ ձևակերպմանը. «Ազգային անվտանգությունն ազգի ընդունակությունն է՝ պահպանելով իր հիմնարար արժեքները հնարավորինս նվազագույն կորուստներով՝ բավարարել այն պահանջները, որոնք անհրաժեշտ են ինքնապաշտպանության, ինքնավերարտադրման և ինքնակատարելագործման համար»: Լինելով բավական ընդգրկուն՝ միևնույն ժամանակ այս սահմանումը փոքր-ինչ ստատիկ բնույթ է կրում և լիարժեք չի արտահայտում հարափոփոխ միջավայրի ազդեցությունները: Այդ իսկ պատճառով անդրադառնանք նաև անվտանգության փիլիսոփայության ստեղծման գործում մեծ ավանդ ունեցող Առնոլդ Թոյնբիի (1889-1975թթ.) ձևակերպումներին:


Առնոլդ Ջոզեֆ Թոյնբի (1889-1975թթ.):

Եթե փորձենք փոքր-ինչ ընդհանրացնել Թոյնբիի դասական մոտեցումները, ապա քաղաքակրթությունների, պետությունների, հասարակությունների և անգամ անհատների անվտանգությունն ապահովվում է նրանց՝ մարտահրավերների և դրանց տրվող պատասխանների բարդ համակարգում գործելու ունակությամբ: Հայտնի է Թոյնբիի ասույթը, թե քաղաքակրթությունների կործանման պատճառը եղել է նրանց անկարողությունը՝ ադեկվատ արձագանքելու իրենց նետված մարտահրավերներին: Նկատենք, սակայն, որ մարտահրավերները որոշ իրադրություններում կարող են ընկալվել նաև որպես դրական հանգամանք, քանի որ դրանք ստուգում, փորձաքննում են անվտանգության համակարգի հուսալիությունը և, մարտահրավերներին արժանիորեն դիմագրավելու նպատակով, մոբիլիզացնում են հանրության հոգևոր, մտավոր, ռազմաքաղաքական ու նյութական ռեսուրսները:

Թոյնբիի վերոնշյալ դատողությունները կիրառելի են նաև ՏԱ ոլորտում: Վերջինիս շրջանակները երբեմն նեղացվում են, մինչդեռ այն ծավալուն հասկացություն է և առաջին մոտավորությամբ ներառում է այն ամենը, ինչ վերաբերում է.

- ազգի, պետության, հասարակության և անհատի հոգևորհոգեբանական, մտավոր, գիտելիքային և կրթական ոլորտների արդյունավետ զարգացման, կառավարման ու ապահովության խնդիրներին:
- պետության, հասարակության և անհատի տեղեկատվականտեխնոլոգիական համակարգերի արդյունավետ զարգացման ու ապահովության խնդիրներին:

Այս և նման մոտեցումների հիման վրա մասնագիտական գրականությունում առաջարկվել են ՏԱ բազմաթիվ սահմանումներ: Օրինակ՝ «Տեղեկատվության և այն ապահովող ենթակառուցվածքների պաշտպանվածությունը պատահական կամ միտումնավոր ազդեցություններից»: ՏԱ-ն սահմանվում է նաև որպես «Ներազդող սպառնալիքների և դրանց արդյունավետ հակազդելու գործընթացների միջև հավասարակշռության պահպանման գործընթաց»: Ելնելով Թոյնբիի անվտանգության փիլիսոփայության դրույթներից և շեշտելով անվտանգության խնդիրներում գիտակրթական-տեխնոլոգիական ռեսուրսների ու հանրության ընդհանրական հմտությունների որոշիչ կարևորությունը՝ ՏԱ-ը կարելի է սահմանել նաև հետևյալ կերպ.

«Տեղեկատվական անվտանգությունը պետության և հասարակության գիտելիքային-տեխնոլոգիական անհրաժեշտ ռեսուրսների ստեղծման միջոցով հանրության անվտանգությունը և զարգացումն ապահովելու ունակությունն է տեղեկատվական մարտահրավերներ-պատասխաններ գործընթացում»:

Հայկական հանրության տեղեկատվական անվտանգության առանձնահատկությունները. ՏԱ ոլորտին վերաբերող մոտեցումներում և սահմանումներում պետք է հաշվի առնել, որ դրանք միշտ չէ, որ ունիվերսալ բնույթ են կրում, քանի որ հաճախ վճռորոշ նշանակություն ունեն այն քաղաքակրթական և աշխարհաքաղաքական միջավայրերը, որոնցում կիրառվում են ՏԱ այս կամ այն դրույթները։ Օրինակ, Հայկական հանրությանը վերաբերող ՏԱ խնդիրներում անհրաժեշտ է հաշվի առնել հետևյալ իրողությունները.

- Հայաստանը ներկայացնում են երկու պետություններ՝ Հայաստանի Հանրապետությունը և Լեռնային Ղարաբաղի (Արցախի) Հանրապետությունը։
- Հայկական Սփյուռքի մեծ մասը, սփռված լինելով տարբեր երկրներում, գտնվում է իր բնակության վայրի (օրինակ՝ Ռուսաստանի կամ Միացյալ Նահանգների) քաղաքական, մշակութային և տեղեկատվական ազդեցության տակ։
- Հայկական հանրությունը ներառում է տարադավան (Հայ Առաքելական եկեղեցու հետևորդներից բացի առկա են նաև կաթոլիկություն, ուղղափառություն և բողոքականություն դավանող հայկական համայնքներ) և տարակրոն (Արևմտյան Հայաստանում և Մերձավոր Արևելքի որոշ երկրներում բնակվում են իսլամացված հայեր) հատվածներ։ Հայկական հանրության այս հատվածներին բնորոշ են հոգեկերտվածքային բնույթի առանձնահատկություններ, որոնք անհրաժեշտ է հաշվի առնել տեղեկատվական քաղաքականություն վարելիս։
- Պատմական Հայաստանի որոշ հատվածներում բնակվում են հայեր, որոնք ավանդաբար համարում են, որ ապրում են իրենց հայրենիքում (օրինակ՝ Ջավախքում, Արևմտյան Հայաստանի ու Մերձավոր Արևելքի որոշ շրջաններում), և այս գործոնը նույնպես պետք է ուշադրության արժանանա։

Ինչպես տեսնում ենք, ՏԱ տեսանկյունից Հայկական հանրությունն ունի բավական լուրջ հիմնախնդիրներ։ Բնակության տարաբնույթ միջավայրերն առանձին հայկական համայնքներին և կազմակերպություններին երբեմն թելադրում են այս կամ այն ազգային խնդրի վերաբերյալ կիրառել տեղեկատվական մարտավարություն, որը միշտ չէ, որ համընկնում է հայկական հանրության այլ հատվածների մոտեցումների հետ։ Միևնույն ժամանակ, նման մարտավարական տարաձայնությունները նույնպես կարելի է ընդունել և օգտագործել որպես տեղեկատվական ռեսուրս։ Ընդհանրական գաղափարա–տեղեկատվական դաշտի առկայության, ինչպես նաև արդի համակարգչային-ցանցային համագործակցության հնարավորությունների լիարժեք օգտագործման պարագայում այդ բազմակարծությունը կարելի է և անհրաժեշտ է ծառայեցնել հայկական պետությունների ու հանրության շահերին։ Ավելին, տեղեկատվական ռեսուրսների նման «սփռվածությունը» և «ցանցային» բնույթը որոշակի առավելություններ են ընձեռում հայկական հանրությանը, որին չեն տիրապետում մեր որոշ մրցակիցները։

Բոլոր պարագաներում ակնհայտ է, որ տեղեկատվական անվտանգության մշակվող կամ առաջարկվող «հայկական» հայեցակարգերը պետք է հաշվի առնեն վերոնշյալ կարևոր հանգամանքները, այլապես չեն կարող լիարժեք համարվել։ Մինչդեռ Սփյուռքի տեղեկատվական ռեսուրսների հաշվառումը և համապատասխան օգտագործումը կնպաստեն, որպեսզի ողջ Հայկական հանրությունն արժանավայել պատասխանի անվտանգության բազում մարտահրավերներին, որոնցից շատերը տեղեկատվական բնույթի են։

3. ԿԻԲԵՌՏԱՐԱԾՔ ԵՎ ԿԻԲԵՌՄԱՐՏԱՀՐԱՎԵՐՆԵՐ

Նախորդ գլուխներում ՏԱ խնդիրները հիմնականում դիտարկվել են տեղեկատվության բովանդակային բաղադրիչի համատեքստում: Միևնույն ժամանակ, տեխնոլոգիական զարգացումների արդյունքում տեղեկատվական ոլորտում առաջանում են ուղղություններ, որոնք ձևավորում են տեղեկատվական նոր միջավայր և նոր տիպի սպառնալիքներ: Այս գլխում համառոտակի կդիտարկվեն այդ նոր մարտահրավերների առանձնահատկությունները և դրանց դիմակայելուն ուղղված անհատական ու օրենսդրական միջոցները:

Գլոբալ դերակատարում ձեռք բերած համացանցը և նրա հետ համակցված թվային տեխնոլոգիաները ձևավորել են նոր միջավայր՝ կիբեռտարածք, որի տակ հասկացվում է այն համակարգչային-համացանցային երևակայական, վիրտուալ դաշտը, որտեղ անձը կորցնում է իրական և արհեստական կառուցված աշխարհները տարբերելու ունակությունը:

Այլ տեսանկյունից են մեկնաբանում այդ եզրը ռազմական ոլորտի փորձագետները, համաձայն որոնց՝ կիբեռտարածք ասելով հասկացվում է «փոխկապակցված տեղեկատվական-տեխնոլոգիական ենթակառուցվածքների ցանց, որը ներառում է համացանցը, հեռահաղորդակցման և համակարգչային համակարգերն ու նրանց մեջ ներառված պրոցեսորները»:

Նկատենք, որ կիբեռեզրի հաստատվելը ՏԱ բառապաշարում պատահական չէ, քանի որ կիբեռնետիկան (հունարեն՝ կառավարման արվեստ) ենթադրում է գիտության այն ոլորտը, որտեղ ուսումնասիրում են կառավարման բարդ համակարգերում (լինեն դրանք մեքենաներ, կենդանի օրգանիզմներ կամ մարդկային հանրություններ) տեղեկատվություն ստանալու և հաղորդելու, պահելու և վերամշակելու խնդիրները:

Համացանցային, թվային տեխնոլոգիաների միջոցով ստեղծված կիբեռտարածքն աննախադեպ մեծ հնարավորություններ է ընձեռում մարդկային շփման ու տեղեկատվության փոխանակման համար, և այդ տեսանկյունից մարդկության զարգացման համար կարևորագույն գործոն է հանդիսանում: Համաձայն որոշ հետազոտողների մոտեցումների, կիբեռտարածքում ընթացող գործընթացներին բնորոշ է յուրահատուկ գաղափարախոսություն՝ այսպես կոչված Netism (ցանցականություն), որի հենքը, հաշվի առնելով նման տարածքում անձի զանազան ինքնարտահայտումների գրեթե անսահմանափակ հնարավորությունները, ծայրահեղականացված ազատականությունն է կամ այսպես կոչված հիպերլիբերալիզմը: Նման գաղափարական բովանդակություն ունեցող տարածքում իրական աշխարհի հետ կապը կորցրած անձը՝ homo virtualicus-ը, կարող է լիովին բավարարվել կիբեռտարածքի ընձեռած հնարավորություններով և չընկալել իրական աշխարհում տեղի ունեցողը: Թերևս այս հանգամանքով կարելի է բացատրել, որ կիբեռտարածքի «քաղաքացիների» պարագայում գրեթե չի գործում տոտալիտար համակարգերում գործող այն կանոնը, համաձայն որի, երբ մատուցվող քարոզչության բովանդակության և իրականության միջև տեղի է ունենում խզում, ապա հասարակությունը սկսում է ըմբոստանալ տիրող համակարգի դեմ: Այդ իսկ պատճառով լիովին «ազատականացված» homo virtualicus-ը կարող է հաճախ անտարբեր լինել իրական կյանքում հաստատվող տոտալ գաղափարախոսության և բարքերի նկատմամբ ու չձեռնարկել որևէ ջանք դրանք փոխելու նպատակով: Այս առիթով նշենք, որ վիրտուալ տարածքում այս կամ այն խնդրի վերաբերյալ հայտնվող «ֆեյքերը» ավելի քան անարդյունավետ են և ի լրումն ստանում են հերքող պատասխաններ տարաբնույթ բոտերի միջոցով: Մինչդեռ հայտնի է, որ ցանկացած քաղաքական համակարգի համար հասարակական վերահսկումից դուրս գալը հղի է ծանր սոցիալական և քաղաքական հետևանքներով:

Ակնհայտ է, որ առանձին անհատների նման լայն իրավունքներն ինչ պես իրական, այնպես էլ վիրտուալ հարթությունում, գրեթե անխուսափելիորեն ոտնահարում են այլոցիրավունքները: Այդ պատճառով դժվար վե րահսկելի այդ տարածքն այսօր հանդիսանում է հարթակ ոչ միայն օրեն քի

հետ երբեմն աղերս չունեցող քաղաքական գործողությունների, այլև զուտ քրեական բնույթի արարքների համար: Հատկանշական է, որ վերջիններս, չնայած իրենց վիրտուալ բնույթին, հանգեցնում են միանգամայն «նյութականացված» հետևանքների:

Վերոնշյալի համատեքստում նշենք, որ ներկայում շուրջ 130 երկրներում գործում են ցանցահենների կամ, ինչպես նրանց ընդունված է անվանել՝ հաքերների 5 խմբեր, որոնք շարունակաբար նոր վնասակար ծրագրեր են մշակում և տարեկան կատարում են մի քանի հարյուր միլիոն կիբեռհարձակում: Դրանց նպատակն է ֆինանսական-տնտեսական վնաս պատճառել «պայմանական հակառակորդներին»՝ մրցակից բիզնես կազմակերպություններին, կամ էլ ուղղակի անձնական շահույթ ստանալ: Նման հարձակումներից ԱՄՆ-ը 2016թ. կորցրել է $108 մլրդ, Չինաստանը՝ $60 մլրդ, իսկ Գերմանիան՝ $58 մլրդ: Ընդհանուր առմամբ համացանցային հանցագործությունների հետևանքով համաշխարհային տնտեսության վնասները 2016թ. կազմել են $575 մլրդ, սակայն արդեն 2017-ին սպասվում է, որ կիբեռգրոհների արդյունքում ընդհանուր առմամբ համաշխարհային տնտեսությանը կպատճառվի մոտ $1.0 տրլն-ի վնաս (համաշխարհային ՀՆԱ-ի մոտ 2%-ը): Նկատենք նաև, որ ներկայացված տվյալներում ներառված չեն այն հսկայական գումարները, որոնք ծախսվում են նման հարձակումներից պաշտպանվելու նպատակով:

Բայց խնդիրը միայն այն չէ, որ կատարվում են զուտ ֆինանսական մեքենայություններ: Կիբեռհարձակումները թույլ են տալիս շարքից դուրս բերել արդյունաբերական կառույցները. համաձայն «Կասպերսկու լաբորատորիայի» հրապարակած տվյալների, 2016թ. համաշխարհային արդյունաբերական ոլորտ համակարգի 27.5%-ում հայտնաբերվել են վնասակար ծրագրեր: Այս ոլորտում առանձնապես վտանգավոր են հարձակումները միջուկային ենթակառուցվածքների վրա: Օրինակ, 2009-2010թթ. կազմակերպվեց կիբեռգրոհների շարք Իրանի միջուկային օբյեկտների վրա, որոնց կառավարման համակարգում ներմուծված «Stux net» տիպի վիրուսները ոչնչացրին ուրան հարստացնող շուրջ 1000 ցենտրի ֆուգ: Ակնհայտ է, որ նման հարձակումների կարող են ենթարկվել, մասնավորապես, նաև ատոմակայանները, ինչը կարող է հանգեցնել հումանիտար և էկոլոգիական աղետների: Հատկանշական է, որ ինչպես 1986թ. Չեռնոբիլի, այնպես էլ ավելի ուշ՝ 2011թ. ճապոնական Ֆուկուսիմա-1 ԱԷԿ-ներում պատահած վթարների պատճառը, համաձայն որոշ վարկածների, այլ երկրների կողմից կատարված նպատակաուղղված գործողություններն են:

Ինչպես տեսնում ենք, կիբեռհարձակումները դարձել են տարածված երևույթ, և տրամաբանական է, որ ընձեռված հնարավորություններից լայնորեն օգտվում են նաև քաղաքական ոլորտում: Կիբեռգործողությունները և դրանց համակարգված համախումբը՝ կիբեռպատերազմները (այս պես կոչված պատերազմի հինգերորդ ոլորտը՝ ցամաքից, ծովից, օդից և տիեզերքից հետո), թույլ են տալիս, մասնավորապես, մեծ արդյունավետությամբ ներազդել պայմանական հակառակորդի հիմնական կրիտիկական ենթակառուցվածքի՝ կառավարման համակարգի վրա: Այսպիսով, չնայած տեխնոլոգիական յուրահատկություններին, բովանդակային առումով կիբեռգործողությունները և կիբեռպատերազմներն ընդհանրական տեղեկատվական գործողությունների ու պատերազմների մասն են կազմում և ենթարկվում են համապատասխան դասական սահմանումներին:

Միևնույն ժամանակ, կիբեռտարածքում ընթացող պատերազմները, շնորհիվ իրենց, ինչպես արդեն նշել ենք, «նյութականացված» արդյունքների, երբեմն ավելի զորեղ են ազդում աշխարհաքաղաքական զարգացումների վրա, քան իրական հարթությունում կատարվող տեղեկատվական գործողությունները: Նման իրողությանը նպաստում է նաև այն հանգամանքը, որ խիստ դժվար է պարզել, թե ովքեր են կիբեռգործողություններ իրականացնողները. հայտնի է, որ այսօր բացահայտվում է կիբեռհանցագործությունների ընդամենը 3-4%-ը: Սակայն անգամ բացահայտումից հետո պետք է հաշվի առնել, որ կոնկրետ հաքերային խմբավորումը կարող է ենթարկվել կամ ուղղորդվել ոչ միայն պետական հատուկ նշանակության ծառայությունների և կառույցների կողմից: Հաճախ այդ հաքերները կատարում են ոչ պետական կազմակերպությունների պատվերը կամ էլ

գործում են անկախ՝ հետևելով իրենց համոզմունքներին և պատկերացումներին: Բոլոր պարագաներում պետք է արձանագրել, որ կիբեռգործողություններ կատարողների և դրանց պատվիրատուների նույնականացումը տեխնիկապես ավելի դժվար խնդիր է, քան ավանդական տեղեկատվական գործողությունների պարագայում:

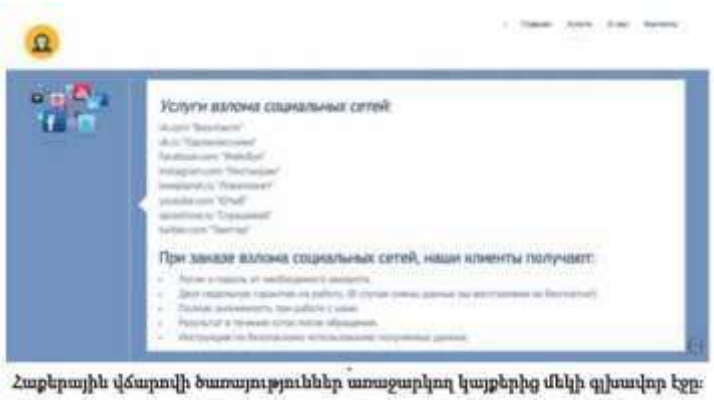
Այս վերջին հանգամանքները մեծ հնարավորություններ են ստեղծում տարաբնույթ քաղաքական շահարկումների համար, և արդյունքում նման հարձակումները հանգեցնում են լարվածության անգամ խոշոր տերությունների հարաբերություններում: Դրա վկայություններից է, օրինակ, ՌԴ-ԱՄՆ հարաբերությունների սրացումը՝ պայմանավորված 2016թ. ամերիկյան նախագահական ընտրություններում «ռուսական հաքերների» կողմից կատարված «միջամտություններով»: Այդ միջադեպը փաստացի չհաստատվեց, սակայն որոշակի քաղաքական կողմնորոշումներ ունեցող ԶԼՄ-ի բուռն արձագանքի շնորհիվ հասարակությունում ձևավորված մթնոլորտն առիթ տվեց ԱՄՆ վարչակազմին արտաքսել երկրից ռուս դիվանագետների մի մեծ խմբի:

Տեղեկատվական համալիր գործողություններով պայմանավորված՝ վերոնշյալ և բազում նման քաղաքական զարգացումների թիվն արդի ժամանակահատվածում շեշտակի աճում է: Արդյունքում՝ երբեմն որոշ ոչ պետական կառույցներ, ելնելով իրենց կորպորատիվ շահերից, կարող են իրագործել համալիր տեղեկատվական գործողություններ, որոնք կարող են ուղղորդել այս կամ այն երկրի քաղաքական ղեկավարության դիրքորոշումները, մինչդեռ անցյալում համարվում էր, որ արտաքին տեղեկատվական քաղաքականությունը պետական կառույցների մենատիրությունն է: Այս իրողություններից ելնելով՝ որոշ փորձագետներ հակված են կարծել, որ արդի ժամանակաշրջանում ոչ թե «պատերազմն է քաղաքականության շարունակությունը այլ միջոցներով» (համաձայն ռազմարվեստի դասական Կառլ ֆոն Կլաուզևիցի հայտնի սահմանման), այլ հաճախ «քաղաքականությունն է հանդիսանում տեղեկատվական պատերազմների շարունակությունն այլ միջոցներով»:

Միևնույն ժամանակ, կիբեռհարձակումները մեծ վտանգ են ներկայացնում ոչ միայն խոշոր պետությունների, այլև շարքային օգտատերերի համար:

4. ԱՆՁՆԱԿԱՆ ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀԻՄՈՒՆՔՆԵՐ

Ինչպես հայտնի է, այսօր ձևավորվել է հաքերային հարձակումների ծառայությունների հսկայական սև շուկա: Մասնավորապես այսպես կոչված «Մութ ցանցում» (Darknet) գործում են բազմաթիվ անոնիմ կայքեր, որտեղ կարելի է պատվիրել տարբեր տիպի հաքերային հարձակումներ՝ սկսած ընտանեկան բնույթի գործողություններից, ուղղված սոցցանցերի օգտատերերի դեմ, մինչև լուրջ կորպորատիվ հարձակումները, երբ կորզվում է գաղտնի տեղեկատվություն կամ էլ իրականացվում համակարգի խափանում: Նման խմբերը համացանցում գովազդում են իրենց ծառայությունները, ինչպես դա անում է բազմաթիվ երկրների ուժային կառույցներին հաքերային ծառայություններ մատուցող իտալական The Hacking Team հաքերային կազմակերպությունը, կամ էլ գործում են անոնիմ (տե՛ս նկարում):



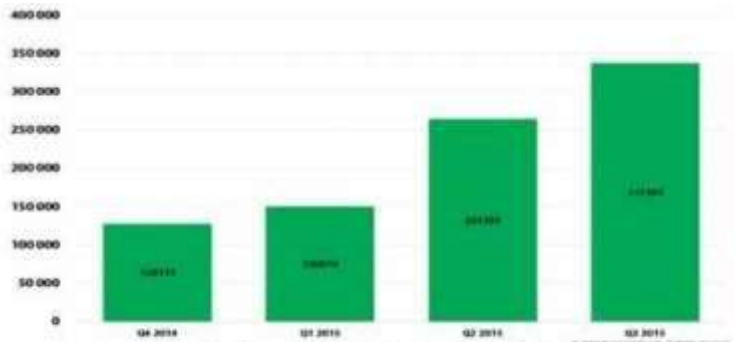
Հաքերային վճարովի ծառայություններ առաջարկող կայքերից մեկի գլխավոր էջը:

Հարձակումներ կատարող հաքերային խմբավորումները կարելի է բաժանել մի քանի տիպի.

- Իրենց «Սև գլխարկ» (Black Hat) անվանող վարձկան հաքերներ, որոնք պատրաստ են երրորդ կողմի պատվերով իրականացնել ցանկացած տիպի հարձակում
- Սեփական պետությանը ծառայող հաքերներ, որոնք իրականացնում են հարձակումներ պետական պատվերով
- Կիբեռլրտեսներ, որոնք աշխատում են մեծ կորպորացիաների և կազմակերպված հանցավոր խմբերի պատվերով
- Կիբեռահաբեկիչներ, որոնք իրականացնում են գործողություններ նույն դրդապատճառներով, ինչ ավանդական ահաբեկչական խմբերը
- Այսպես կոչված հաքտիվիստներ (hacktivist)՝ քաղաքական, կրոնական կամ հասարակական ոլորտների ակտիվիստներ, որոնք իրենց բողոքը դրսևորում են հաքերային հարձակումների միջոցով։

Հարձակվող խմբերի բազմազանությունն այնպիսին է, որ թիրախ կարող է հանդիսանալ յուրաքանչյուրը։ Հաճախ օգտատերերը չեն պատկերացնում, թե ինչ պատճառով հաքերները կարող են իրենց թիրախավորել։ Հասկանալի է, որ քաղաքական գործիչները, իրավապաշտպանները, բիզնեսմենները, լրագրողները կարող են հանդիսանալ անմիջական թիրախներ։ Նույնիսկ համացանցի «շարքային» օգտատերը կարող է հանդիսանալ թիրախ, քանի որ.

- Հաքերները հաճախ իրականացնում են զանգվածային ավտոմատացված հարձակումներ՝ հնարավորինս մեծ քանակի անձնական տվյալներին տիրանալու համար, և այդ պարագայում յուրաքանչյուրը կարող է տուժել հաքերային գրոհից
- Այսօր շատերն էլեկտրոնային առևտուր են կատարում, և հարձակվողները փորձում են նրանցից գումար կորզել
- Համացանցում ստեղծվում են տարատեսակ ծրագրեր և մեթոդներ, որոնց միջոցով հաքերները գումար են շորթում։ Օրինակ, այսպես կոչված շորթող վիրուսների (Ransomware) միջոցով, որոնք համակարգչի ֆայլերը գաղտնագրում են, իսկ հաքերները դրանք վերադարձնում են տիրոջը միայն գումարի դիմաց, և նման հարձակումների թիվը ժամանակի հետ աճում է (տե՛ս նկարում)։
- Հաքերային ծառայությունների սև շուկան այսօր բավական մատչելի է և թույլ է տալիս պատվիրել հարձակումներ յուրաքանչյուրին յուրաքանչյուրի դեմ։



Ransomware տիպի վիրուսների կողմից հարձակումների թվի աճը մեկ տարվա ընթացքում (ըստ *Kaspersky Lab* տվյալների)։

Բացի այդ, անհատը կամ կազմակերպությունը կարող է թիրախ հանդիսանալ պետական ուժային կառույցների, մեծ կորպորացիաների կողմից։ Հայաստանի պարագայում կարևոր գործոն են հանդիսանում նաև այլ երկրների, հատկապես Ադրբեջանի և Թուրքիայի հատուկ ծառայությունները։ Արդյունքում՝ հազարավոր հայաստանցիներ և սփյուռքահայեր շարունակաբար տուժում են ադրբեջանական հաքերներից։

Իրական վտանգներն այսօր չպետք է թերագնահատել։ Ամերիկյան հետախուզության նախկին գործակալ Էդվարդ Սնոուդենի բացահայտումները վկայում են այն մասին, որ ԱՄՆ և Մեծ Բրիտանիայի հատուկ ծառայություններն օգտագործում են բոլոր հնարավոր մեթոդները՝ անհատներին ու կազմակերպություններին հետևելու նպատակով։ ԱՄՆ Ազգային անվտանգության գործակալությունը (National Security Agency (NSA)), բրիտանական Հաղորդակցությունների կառավարական շտաբը (Government Communications Headquarters (GCHQ)) կանադական,

ավստրալական և նորզելանդական հատուկ ծառայությունների հետ համատեղ ստեղծել են լրտեսական գլոբալ համակարգ, որը թույլ է տալիս հետևել գրեթե բոլոր անհատներին, որոնք օգտվում են հեռախոսից կամ համակարգչից: Հատուկ ծառայությունները հաքերային հարձակումներ են կատարում օգտատերերի վրա և լայնորեն օգտվում են տեղեկատվություն ստանալու ծառայություններ տրամադրող հարթակների հնարավորություններից, նույն Google-ից կամ Facebook-ից:

Սնոուդենը հետախուզական փաստաթղթերը բացահայտել է մինչև 2013թ.: Հասկանալի է, որ դրանից հետո հատուկ ծառայություններն ավելի են ընդլայնել իրենց հնարավորությունները: 2017թ. մարտին Wikileaks-ը հրապարակեց ԱՄՆ Կենտրոնական հետախուզական վարչության ցանցահենային ծրագրերի և գործողությունների վերաբերյալ նոր տվյալներ, համաձայն որոնց՝ լրտեսական այս գործակալությունը նույնպես օգտագործում է տեխնիկական հնարքներ անհատներին և կազմակերպություններին հետևելու և տեղեկատվություն կորզելու համար: Սակայն միայն ամերիկյան, բրիտանական հետախուզությունները չէ, որ իրականացնում են հաքերային լայնամասշտաբ գործողություններ, այսօր նման լրտեսական համակարգեր ձևավորվում են նաև այլ երկրներում:

Հաշվի առնելով վտանգների բազմազանությունը՝ այսօր գրեթե յուրաքանչյուր օգտատեր կարող է դառնալ հարձակման թիրախ: Սակայն կիբեռվտանգների մի զգալի մասից կարելի է խուսափել՝ որոշակի կանոնների հետևելու պայմանով:

5. ՀԱՄԱԿԱՐԳՉԻ ԵՎ ՇԱՐԺԱԿԱՆ ՍԱՐՔԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆ

Պետք է հաշվի առնել, որ համակարգչային ծրագրային ապահովման սխալ ընտրությունն արդեն իսկ կարող է պարունակել լուրջ վտանգներ: Բացի այդ, կարևոր է նաև ծրագրային ապահովման հետ ճիշտ աշխատանք վարել և այն պարբերաբար թարմացնել:

Համակարգչի պաշտպանությունը. այս խնդրում առաջնային դերակատարում ունի օպերացիոն համակարգը (Operation System): Այսօր ամենատարածված և ամենախոցելի օպերացիոն համակարգն է Microsoft Windows-ը: Այս համակարգի կառուցվածքային յուրահատկությունները հանգեցնում են նրան, որ հաքերային խմբերը հիմնական վիրուսները ստեղծում են հենց Windows-ի համար և այս համակարգում են փնտրում խոցելիություններ: Հարկ է նշել, որ այսօր պետք է խուսափել Windows-ի XP, 7 տարբերակից, քանի որ այն այլևս չի թարմացվում և դրա տեղադրումը համակարգիչը դարձնում է շատ խոցելի հարձակումների համար: Ցավոք, Հայաստանում 2016թ. տվյալներով, գրեթե ամեն հինգերորդ համակարգչի վրա (ներառյալ կրթական հաստատություններում) տեղադրված է Windows 7 համակարգը: Միևնույն ժամանակ, Windows-ի 10-րդ թարմացումն անվտանգության տեսանկյունից դրական պետք է համարել:

Համեմատաբար ավելի անվտանգ են OS X և Linux օպերացիոն համակարգերը: Դրանցից ամենաանվտանգը մատչելի կիրառման համար համարվում են Linux օպերացիոն համակարգերը: Մասնավորապես, այդ ընտանիքի Ubuntu օպերացիոն համակարգն անվճար է և կարող է ներբեռնվել ubuntu.com կայքից: Տվյալ համակարգն ինքնին շատ ավելի պաշտպանված է, քան մնացած ավելի տարածված օպերացիոն համակարգերը, հարձակումների մեծ մասը տվյալ համակարգի համար վտանգավոր չէ:

Իսկ Apple արտադրանքի լայն տարածումը շուկայում կենտրոնացնում է իր հանդեպ հաքերների ուշադրությունը: Արդյունքում՝ վերջին տարիներին Apple-ի դեմ հարձակումների թիվը կտրուկ աճել է: Իհարկե, կատարյալ պաշտպանված օպերացիոն համակարգ չկա, միշտ հնարավոր են թաքնված խոցելիություններ, որոնք կարող են օգտագործել հաքերները: Բայց այն կարելի է դարձնել առավել

պաշտպանված այսպես կոչված կիբեռանվտանգության հիգիենայի կանոններին հետևելու պարագայում:

Օպերացիոն համակարգի պաշտպանությունը ենթադրում է երկու կարևոր կետ.

- Այն պետք է լինի լիցենզիոն, եթե խոսքը վճարովի համակարգերի մասին է
- Համակարգը պետք է միշտ թարմացնել:

Հակառակ պարագայում օպերացիոն համակարգում կարող են հայտնվել վտանգավոր խոցելիություններ, որոնք թիրախ կհանդիսանան հանցագործների համար: Ինչ վերաբերում է թարմացումներին, ապա միշտ պետք է համոզված լինել, որ չեն անջատված ավտոմատացված թարմացումները (Update): Եթե օպերացիոն համակարգը չի կատարում թարմացումներն ինքնուրույն, ավտոմատացված կարգով, ինչպես դա կատարվում է Windows-ի դեպքում, ապա հարկավոր է պարբերաբար ստուգել թարմացումների բաժինը և դրանք ներբեռնել ու տեղադրել համակարգչի վրա: Թարմացումների միջոցով օպերացիոն համակարգ ստեղծող կազմակերպությունները վերացնում են նոր հայտնաբերված խոցելիությունները: Մինչդեռ երկար ժամանակ չթարմացված օպերացիոն համակարգը կարող է դառնալ խիստ խոցելի հարձակումների համար: Նույնիսկ մի քանի շաբաթ չթարմացված օպերացիոն համակարգը կարող է լուրջ վտանգ ներկայացնել, քանի որ պարբերաբար հայտնի են դառնում վտանգավոր խոցելիություններ, որոնք զանազան հաքերային խմբեր սկսում են կիրառել իրենց հարձակումներում:

Ոչ լիցենզիոն, «կոտրված» Windows օպերացիոն համակարգն ինքնին մեծ խնդիր է օգտագործողի համար, քանի որ նմանատիպ համակարգերն ինչ-որ պահից դադարում են թարմացվել: Նույնիսկ լինում են դեպքեր, երբ նման Windows-ները տարածվում են հենց հաքերների կողմից և պարունակում են ներդրված վիրուսներ կամ այլ վտանգներ:

Այսպիսով, պետք է օգտագործել միայն օրինական Windows, և համակարգիչ գնելիս պետք է համոզվել, որ ձեզ տրվում է լիցենզիոն օպերացիոն համակարգով սարք: Նույնը վերաբերում է համակարգչի վրա տեղադրված ծրագրային ապահովմանը. այն պետք է լինի լիցենզիոն և թարմացված: Միևնույն ժամանակ, կարելի է օգտվել նաև անվճար Linux օպերացիոն համակարգերից: Այս հարցում պետք է հաշվի առնել, որ լիցենզիոն վճարովի ծրագրերը հաճախ օգտագործում են «կոտրելուց» հետո, որպեսզի դրանք անվճար տեղադրվեն համակարգչի վրա: Նման դեպքում օգտվողը վտանգի տակ է հայտնվում, քանի որ այդպիսով ծրագրային ապահովումը կարող է խոցելի լինել և, ի լրումն, կարող է պարունակել հաքերների կողմից ներդրված վտանգավոր ծրագրեր ու վիրուսներ: Այս խնդիրը հիմնականում առաջանում է տնային համակարգիչների հետ կապված, քանի որ օգտվողները գերադասում են չծախսել մեծ գումարներ ծրագրերի համար:

Սակայն վերոնշյալ խնդիրն ունի այլ, ավելի խոհեմ լուծում. տնային պայմաններում օգտագործելու համար գրեթե բոլոր վճարովի ծրագրերն ունեն անվճար փոխարինողներ (իհարկե, խոսքը լուրջ, պրոֆեսիոնալ գործիքների մասին չէ): Այսպես, օրինակ, ամենատարածված Microsoft Office-ն ունի անվճար փոխարինող տարբերակ՝ LibreOffice, Photoshop-ի փոխարինող տարբերակ՝ Gimp և այլն: Հնարավոր է նաև գտնել փոխարինող անվճար ծրագրեր, որոնք գործում են այսպես կոչված «ամպային» տեխնոլոգիաների միջոցով, ցանցային տարբերակով: Օրինակ, Microsoft Office-ի անվճար փոխարինող կարող է հանդիսանալ ցանցային Google Drive փաթեթը, որն անվճար հասանելի է Gmailում գրանցված բոլոր օգտատերերին:

Այսօր առկա է այն մտայնությունը, թե բաց կոդերով ծրագրերը բարդ են օգտագործելու համար, մատչելի չեն, սահմանափակ հնարավորություններ ունեն և այլն: Մինչդեռ նմանատիպ ծրագրային ապահովումը բավական լայն կիրառություն է գտնում աշխարհում: Այսպես, Ռուսաստանի պետական համակարգում ներդրվում է սեփական արտադրության GosLinux համակարգ, Իսպանիայի զինված ուժերը և բազմաթիվ այլ խոշոր կառույցներ օգտվում են բաց կոդերով անվճար օպերացիոն համակարգերից, բոլոր օպերացիոն համակարգերի համար հասանելի LibreOffice փաթեթներից և

այլն։ Նշենք, որ Osalt.com կայքում ներկայացված են գրեթե բոլոր վճարովի ծրագրերի բաց կոդերով անվճար այլընտրանքային տարբերակները, որոնցից կարող է օգտվել յուրաքանչյուր օգտատեր՝ խուսափելով ծրագրերը «կոտրելու» և դրանք գողանալու վտանգավոր սովորությունից։

Վնասակար ծրագրերը, որոնք վարակում են համակարգիչները, լինում են բազմաթիվ տեսակների, տեխնիկական տարբերություններից ելնելով՝ դրանք կոչվում են որդեր (worm), տրոյաններ (troyan) և այլն։ Սակայն հանրային իրազեկման համար կարելի է դրանք բոլորն անվանել վիրուսներ։

Համակարգիչը պետք է պաշտպանվի հակավիրուսային ծրագրերով, քանի որ այն կարող է հարձակման ենթարկվել ինչպես ցանցի, այնպես էլ կրիչների միջոցով։ Այդ պատճառով համակարգչի վրա պետք է տեղադրված լինի միշտ թարմացվող հակավիրուսային ծրագիր։ Նույնիսկ մի քանի օր չթարմացված «հակավիրուսը» մեծ հավանականությամբ կարող է վտանգել համակարգիչը, քանի որ այսօր վիրուսային շուկան այնքան արագ է զարգանում, որ գրեթե ամեն օր հայտնվում են նոր սպառնալիքներ։ Մյուս վտանգն այն է, որ համակարգչի վրա տեղադրված «հակավիրուսի» գործողություններն օգտատերերը երբեմն կանգնեցնում են, քանի որ դա դանդաղեցնում է աշխատանքը։ Մինչդեռ «կանգնեցված» հակավիրուսային ծրագիրը պարզապես չի կատարում իր ֆունկցիաները։ Վիրուսներն իրենց հերթին հաճախ հարձակումն իրականացնում են հատկապես «հակավիրուսների» դեմ։ Եվ անջատված «հակավիրուսը», եթե համակարգիչը հասցրել է վարակվել, մեծ հավանականությամբ չի գտնի այդ վիրուսը միացնելուց հետո, քանի որ արդեն իսկ վնասված կլինի դրա կողմից։

Այսօր գոյություն ունեն ինչպես անվճար, այնպես էլ վճարովի հակավիրուսային ծրագրեր։ Անվճար տարբերակներից բավական տարածված են Avast, Avira, AVG, Microsoft Security Essentials և այլ նմանատիպ ծրագրերը, որոնք չեն զիջում վճարովիներին։ Սակայն պետք է հիշել, որ ոչ մի հակավիրուսային ծրագիր չի տրամադրում լիակատար պաշտպանություն։ Բոլոր դեպքերում, լինում են նորաստեղծ վիրուսներ, որոնց վերաբերյալ հակավիրուսային լաբորատորիաները դեռևս տեղեկատվություն չունեն, այդ պատճառով դրանք չեն իդենտիֆիկացվում։ Կասկածելի ֆայլերի կամ հղումների առկայության դեպքում դրանք կարելի է ներբեռնել Virustotal.com կայքում, որն իրականացնում է ստուգում 54 հայտնի հակավիրուսային ծրագրերի միջոցով՝ ավելի նվազեցնելով վարակվելու հնարավորությունը։

Համակարգչի անվտանգության առանձնահատուկ հարցերից մեկը դրա ֆիզիկական հասանելիությունն է այլ անձանց համար։ Եթե տանը մեկ համակարգչից օգտվում են մի քանիսը, ապա գերադասելի է յուրաքանչյուրի համար բացել առանձին հաշիվ (user profile)՝ ամեն մեկը պաշտպանված գաղտնաբառով։ Այն դեպքում, երբ համակարգչի վրա կա հաշիվների բաժանում, մեկ անձի դեմ հարձակումը չի անդրադառնում մյուսների վրա։ Եթե օգտագործվում է շարժական համակարգիչ՝ լափթոփ, ապա գերադասելի է այն ֆիզիկապես վերահսկել։ Սարքը պետք է կամ լինի ձեր հսկողության տակ, կամ ամրացված լինի սեղանին՝ հատուկ մալուխի միջոցով, ինչը թույլ չի տա համակարգիչը տեղաշարժել կամ տանել։

Համակարգիչը պարտադիր պետք է պաշտպանված լինի գաղտնաբառով, որի մուտքագրման ժամանակ ցանկալի է խուսափել այլ անձանց ներկայությունից։ Խնդիր կարող են հանդիսանալ նաև հանրային վայրերում տեղադրված վերահսկողության տեսախցիկները, որոնցից նույնպես կարող են գրանցել գաղտնաբառերը։

Շարժական սարքերի պաշտպանությունը. Շարժական սարքեր են հանդիսանում մոբիլ հեռախոսները և պլանշետները, որոնք նույնպես պարունակում են անձի վերաբերյալ շատ զգայուն տեղեկություններ։ Ավելին, հաճախ շարժական սարքերի վրա ավելի զգայուն տեղեկատվություն է պահեստավորվում, քան անձնական համակարգիչների՝ լուսանկարներ, բանկային տվյալներ և այլն։ Բացի այդ, հեռախոսը շատ դեպքերում մարդու անձը հաստատելու, միանշանակ իդենտիֆիկացնելու գործիք է։

Այսօր շարժական սարքերի վրա հիմնականում տեղադրվում է երկու օպերացիոն համակարգ՝ Android և iOS (տե՛ս նկարում)։ Այլ օպերացիոն համակարգերն այսօր աստիճանաբար լքում են համաշխարհային շուկան, այդ պատճառով դրանց անվտանգության խնդիրներին անդրադառնալը նպատակահարմար չէ։

Android և iOS սարքերը հիմնականում անվտանգ են, եթե պահպանվեն հետևյալ կանոնները.

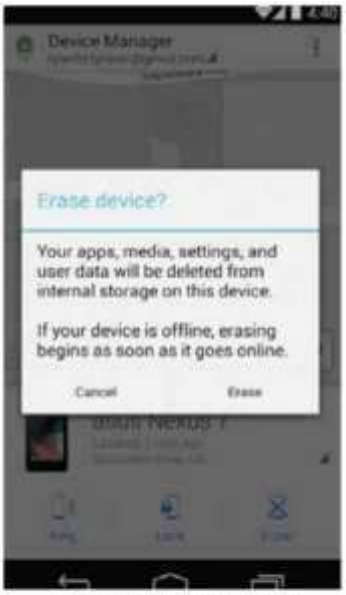
- Հավելվածներ (application) տեղադրել միայն պաշտոնական համացանցային խանութներից՝ Google Play և App Store։ Այլ կայքերից բեռնված ծրագրերը կարող են պարունակել թաքնված հնարավորություններ, որոնք թույլ կտան հաքերներին տիրանալ տեղեկատվությանը կամ հետևել ձեզ։ Այսինքն՝ դուք կարող եք ներբեռնել ծրագրեր, որոնք իրականում վիրուսային բնույթ ունեն։

Period	Android	iOS	Windows Phone	BlackBerry OS	Others
2015Q2	82.8%	13.9%	2.6%	0.3%	0.4%
2014Q2	84.8%	11.6%	2.5%	0.5%	0.7%
2013Q2	79.8%	12.9%	3.4%	2.8%	1.2%
2012Q2	69.3%	16.6%	3.1%	4.9%	6.1%

Հեռախոսների վրա տեղադրված օպերացիոն համակարգերի բաշխումը 2012-2015թթ.

- Հավելված տեղադրելիս հետևեք, թե ինչ տիպի տեղեկատվություն է ուզում ստանալ ձեզանից հավելվածը։ Եթե այն պահանջում է ձեր SMS-ների վերաբերյալ տեղեկատվություն կամ ուզում է միացնել խոսափողը, ապա հեռացրեք տվյալ ծրագիրը, քանի որ այն կարող է օգտագործվել լրտեսելու համար։ Ցավոք, այսօր սոցցանցերի կամ նմանատիպ այլ հավելվածները այնքան հնարավորություններ են պահանջում հեռախոսից, որ այս միջոցով միշտ չէ, որ հնարավոր է վտանգավոր ծրագիրը զատել անվտանգից։

Սարքը «կոտրել» (jailbreak, root) խորհուրդ չի տրվում, քանի որ այդ դեպքում սմարթֆոնը կամ պլանշետը դառնում են ավելի խոցելի։ Հիմնականում այս գործողությանը դիմում են զանազան վճարովի ծրագրերին կամ ծառայություններին անվճար տիրապետելու համար, բայց որպես հետևանք թուլացնում են հեռախոսի կամ պլանշետի պաշտպանողական համակարգը։



Device Manager հավելվածը թույլ է տալիս ինչպես գտնել ձեր սարքավորումը քարտեզի վրա, այնպես էլ վերացնել դրա վրա եղած ողջ անձնական տեղեկատվությունը։

Շարժական սարքի վրա պետք է միացված լինի այն հեռահար գտնելու և վրայի տեղեկատվությունը ոչնչացնելու հնարավորությունը։ Android-ի դեպքում դա Device Manager հավելվածն է, որը պետք է լրացուցիչ ներբեռնվի, քանի որ հեռախոսների և պլանշետների մեծ մասի վրա այն չկա հիմնական փաթեթի մեջ (տե՛ս նկարում)։ iOS-ի դեպքում դա Find My iPhone հավելվածն է։ Այս հավելվածները կառավարվում են անձնական հաշիվներով, համակարգչից կամ այլ շարժական սարքից և թույլ են տալիս ինչպես տեսնել սարքի հստակ տեղը, այնպես էլ վերացնել դրա վրայի տեղեկատվությունը, որպեսզի այն հասանելի չլինի այլ անձանց։ Հարկ է նշել, որ տեղեկատվության վերացումը տվյալ հավելվածների միջոցով լիարժեք չէ, եթե սարքավորման վրա առկա են արտաքին հիշողություն, փոփոխվող ֆլեշ քարտ։ Այդ դեպքում հեռացված տեղեկատվությունը բավական հեշտ հնարավոր է վերականգնել բոլորին հասանելի ծրագրերի միջոցով։

Սարքին պետք է միացված լինի սարքի արգելափակումը կոդի

միջոցով, որպեսզի այլ անձինք հնարավորություն չունենան հեշտությամբ ներթափանցել: Կարևոր է սարքը ֆիզիկապես վերահսկողության տակ պահել, եթե չեք գտնվում ձեր տանը՝ այն միշտ պետք է ձեզ մոտ լինի, քանի որ չվերահսկվող նույնիսկ մի քանի վայրկյանը բավական է դրա մեջ լրտեսական ծրագրեր ներդնելու համար:

Տեղեկատվության վերականգնումը և ոչնչացումը. Հարկ է իմանալ, որ տեղեկատվությունը համակարգչի, հեռախոսի կամ պլանշետի վրա չի անհետանում այն ջնջելուց հետո: Իրականում ջնջելուց հետո ֆայլերը մեծ հավանականությամբ հնարավոր է վերականգնել: Որքան ավելի երկար է ֆայլը մնում ջնջված, որքան ավելի շատ է աշխատում սարքը ջնջելուց հետո, այնքան վերականգնելու հավանականությունը նվազում է:

Ջնջված ֆայլերը վերականգնելու համար գոյություն ունեն բազմաթիվ վճարովի և անվճար ծրագրեր: Անվճարներից կարելի է նշել Recuva ծրագիրը Windows-ի համար, Mac-երի համար՝ TestDisk և PhotoRec, Linux-ի համար՝ R-Linux ծրագիրը:

Քանի որ ֆայլերը հնարավոր է վերականգնել, համակարգիչը կամ հեռախոսն ուրիշ մարդու փոխանցելուց կամ վաճառելուց առաջ պետք է վրայի տեղեկատվությունը ոչնչացնել հիմնովին: Հեռախոսների կամ պլանշետների վրա դա հնարավոր է կատարել գործարանային կարգավորումներին վերադառնալով. այդ դեպքում ֆայլերը վերականգնելի չեն, եթե դա չի իրականացվում մասնագետի կողմից հատուկ սարքավորումների միջոցով: Ինչպես արդեն նշվել է, այս գործողության հետևանքով տեղեկատվության վերացումը լիարժեք չէ, եթե սարքավորման վրա առկա են արտաքին հիշողություն, փոփոխվող ֆլեշ քարտ: Այդ դեպքում հեռացված տեղեկատվությունը կարելի է վերականգնել վերոնշյալ Recuva ծրագրով՝ քարտը միացնելով համակարգչին:

Ֆայլերը լիարժեք վերացնելու համար նույնպես պետք է կիրառվեն հատուկ ծրագրեր: Այսպես, Windows-ի համար գոյություն ունի CCleaner, Mac-երի համար գոյություն ունի ներդրված Disk Utility ծրագիր, Android համակարգի համար՝ Secure Wipe, Secure Delete ծրագրերը, iOS-ի համար՝ iPhone Data Eraser և այլ նմանատիպ հավելվածներ:

6. ՀԱՇԻՎՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆ

Այսօր օգտատերերի բոլոր հաշիվները (accounts)՝ առցանց բանկինգ (on-line banking), էլեկտրոնային փոստ, սոցիալական ցանցեր և այլն, հիմնվում են հիմնականում էլեկտրոնային հասցեների վրա, որոնք հանդիսանում են մարդուն իդենտիֆիկացնելու միջոց: Էլեկտրոնային հասցեն կրիտիկական խոցելի կետ է հանդիսանում. դրա դեմ հաջողված հարձակումն անմիջապես վտանգի տակ է դնում մարդու մյուս բոլոր հաշիվները: Այդ պատճառով գերադասելի է ունենալ մի քանի էլեկտրոնային հասցե.

- Գործնական և հանրային շփումների համար
- Անձնական, ընկերների և բարեկամների հետ շփվելու համար
- Գաղտնի էլեկտրոնային հասցե, որն օգտագործվում է այլ կայքերում գրանցվելու համար, օրինակ՝ Facebook, Twitter, Instagram և այլն
- Տեխնիկական օգտագործման հասցե, որը կիրառվում է անծանոթ, ոչ վստահելի կայքերի վրա գրանցվելու համար:

Գաղտնաբառերը հաշիվների պաշտպանության հիմնական բանալին են: Գաղտնաբառերի դեպքում կան մի քանի հիմնական կանոններ.

- Գաղտնաբառը պետք է պարունակի առնվազն 10 նիշ՝ ներառյալ փոքր և մեծ տառեր

- Գաղտնաբառը չպետք է պարունակի հեշտ գուշակվող տեղեկատվություն, օրինակ՝ ձեր ծննդյան թիվը, հեռախոսահամարը, երեխաների անունները և այլն
- Տարբեր հաշիվների գաղտնաբառերը երբեք չպետք է կրկնվեն։

Գաղտնաբառերի չկրկնվելու պահանջն ունի իր տրամաբանությունը։ Պարբերաբար հաքերներին հաջողվում է կորզել օգտատերերի տվյալները շտեմարանների տարբեր կայքերից։ Նման շտեմարանները պարբերաբար բոլորի համար հասանելի են դառնում համացանցում։ Եվ նման հարձակումների ենթարկվում են նույնիսկ վստահելի և մեծ կայքեր, օրինակ՝ Yahoo, Dropbox և այլն։ Եթե մարդը բոլոր հաշիվների վրա կիրառում է նույն գաղտնաբառը, ապա նման բացահայտումը վտանգում է նրա բոլոր գրանցումները։ Haveibeenpwned.com կայքից կարելի է տեղեկանալ՝ կա՞ արդյոք ձեր գաղտնաբառն արդեն իսկ հաքերների կողմից հրապարակված շտեմարաններում, թե՞ ոչ։ Այստեղ հնարավոր է նաև գրանցվել և նոր հաքերային բացահայտումների դեպքում տեղեկանալ էլեկտրոնային նամակի միջոցով, եթե ձեր գաղտնաբառը հայտնվի համացանցում բոլորին հասանելի տարբերակով։

Հասկանալի է, որ այսօր միջին օգտատերն արդեն իսկ ստիպված է հիշել տասնյակ գաղտնաբառեր։ Եվ բավական դժվար է լինում մտապահել, մանավանդ եթե մարդը պետք է տարբերվող գաղտնաբառեր ունենա։ Եթե չունեք իդեալական հիշողություն, այստեղ կա երկու հիմնական լուծում.

- Կիրառել գաղտնաբառերի ստեղծման հատուկ մեթոդներ, որոնք հասկանալի են միայն ձեզ;
- Օգտագործել գաղտնաբառերի կառավարման հատուկ ծրագրեր (password manager), որոնք մի տեղ են պահում դրանք, և պարտադիր չէ դրանք բոլորն անգիր հիշել։ Այդպիսի ծրագրեր են, օրինակ, LastPass-ը, Dashlane-ը, KeePassX-ը և այլն։

Այսօր գաղտնաբառերը կորցնելու մի շարք հնարավորություններ կան։ Այսպես.

- Վիրուսներով վարակված համակարգիչն արդեն իսկ վտանգ է, քանի որ դրանց միջոցով հաքերները կարողանում են ստանալ բոլոր գաղտնաբառերը։ Այս դեպքերից փրկում են հակավիրուսային ծրագրերը։
- Հանրային Wi-Fi կետերից օգտվելը նույնպես կարող է հանգեցնել հաշվի կորստի։
- Ինտերնետ ակումբներից, հանրային գրադարանների, կրթական հաստատությունների համակարգիչներից օգտվելը նույնպես կարող է բերել հաշիվների կորստի, քանի որ նմանատիպ համակարգիչները հաճախ լինում են վարակված և կորզում են ձեր տվյալները։ Պետք է խուսափել նման համակարգիչներով անձնական հաշիվները մուտքագրելուց։ Իսկ եթե ստիպված եք եղել, ապա գերադասելի է հնարավորինս շուտ վստահելի սարքից փոխել գաղտնաբառերը։ Իսկ ավելի գերադասելի է միշտ ունենալ միացված երկու փուլային մուտքի ընթացակարգը, ինչի մասին կխոսվի ստորև։
- Հաշվի կորուստը կարող է տեղի ունենալ նաև այլ, ոչ անձնական համակարգչից մուտք գործելու դեպքում՝ բրաուզերի (դիտարկիչ, browser) մեջ էլեկտրոնային հասցեն և գաղտնաբառը պահպանելու կամ հաշվից դուրս գալ մոռանալու պարագայում։ Նման վտանգներից խուսափելու համար ոչ անձնական համակարգչից կամ շարժական սարքից պետք է բրաուզերով մուտք գործել հատուկ ռեժիմով, որը չի պահպանում տվյալները պատուհանը փակելուց հետո։ Google Chrome-ի դեպքում դա միանում է որպես New Incognito Window (կամ ստեղնաշարով Ctrl+Shift+N), իսկ Firefox-ի դեպքում՝ որպես New Private Window, կամ ստեղնաշարով՝ Ctrl+Shift+P (տե՛ս նկարում)։

Google Chrome-ի դեպքում New Incognito Window պատուհանը բացելու քայլերը:

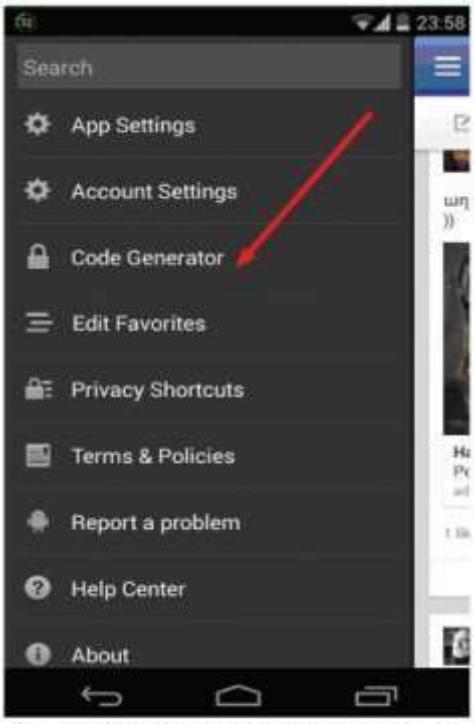
Այսօր ամենահուսալի պաշտպանության միջոցն է հանդիսանում երկփուլային մուտքի ընթացակարգը (Two-factor authentication), որը ենթադրում է գաղտնաբառի մուտքագրումից բացի՝ երկրորդ քայլով անընդհատ փոփոխվող կոդի մուտքագրում, որն օգտվողին տրամադրվում է կամ հատուկ բջջային հավելվածի, կամ կարճ հաղորդագրությունների միջոցով: Նման տարբերակով երկար ժամանակ աշխատում էին բանկերը, որոնք տրամադրում էին առցանց հաշիվների հետ աշխատելու հնարավորություն (on-line banking): Սակայն այսօր անհատների դեմ հարձակումներն այնքան են հաճախակիացել, որ բազմաթիվ ցանցային ծառայություններ ներմուծում են երկփուլային մուտքի տարբերակը բոլորի համար: Այսօր նման ֆունկցիա կարելի է միացնել Gmail, Yahoo, Yandex, Dropbox, Facebook, Twitter և տասնյակ այլ ծառայություններում, դրանց ցանկը կարելի է գտնել twofactorauth.org կայքում: Two-factor authentication-ի ակտիվացումը և կիրառումն անհամեմատ ավելի պաշտպանված է դարձնում օգտվողին: Այս համակարգը նշանակում է, որ եթե ուրիշի մոտ կա նույնիսկ ձեր գաղտնաբառը, նա չի կարող մտնել ձեր հաշիվ՝ առանց հատուկ կոդի, որն էլ անընդհատ փոխվում է: Ինչպես արդեն ասվեց, SMS-ներն այսօր արդեն վստահելի տարբերակ չեն հանդիսանում, և գերադասելի է օգտվել միայն հավելվածներից:

Google-ն ունի հատուկ հավելված երկփուլային մուտքի համակարգի համար՝ Google Authenticator: Այս հավելվածը թույլ է տալիս գեներացնել կոդն ինչպես Gmail-ի համար, այնպես էլ կցել դրան այլ կայքերի հաշիվները: Այսպիսով, մեկ հավելվածով հնարավոր է կարգավորել մուտքերը դեպի բազմաթիվ այլ հաշիվներ մյուս սոցցանցերում կամ այլ ծառայություններում, որոնք թույլ են տալիս նմանատիպ ծրագրերի կիրառումը: Կան ծառայություններ, որոնք թույլ չեն տալիս օգտվել երրորդ կողմի հավելվածներից և պահանջում են կիրառել միայն սեփական արտադրության ծրագիր: Նմանատիպ մոտեցում ունի Yandex-ը, որը հատուկ թողարկել է Yandex Key հավելվածը: Facebook հավելվածն ունի հենց իր մեջ ներդրված նման համակարգ, սակայն թույլ է տալիս օգտվել նաև երրորդ կողմի հավելվածներից, օրինակ՝ Google Authenticator-ից:

Որպես օրինակ ներկայացնենք Facebook հաշվի պաշտպանության հիմնական քայլերն ու կանոնները.

1. Վստահելի էլեկտրոնային հասցեին կցել հաշիվը: Հանրային հասանելի էլեկտրոնային հասցեների ծառայություններից այսօր ամենավստահելիներից են Gmail-ը կամ Hotmail-ը (Live.com): Գերադասելի է, որ դա լինի հատուկ միայն սոցիալական ցանցերի և այլ կայքերի գրանցումների համար էլեկտրոնային հասցե, որը դուք ուրիշներից գաղտնի եք պահում

2. Էլեկտրոնային բոլոր հասցեների և Facebook-ի գաղտնաբառերը պարտադիր պետք է տարբերվեն
3. Այցելել Facebook settings mobile և ավելացնել ձեր բջջային հեռախոսի համարը: Սա թույլ կտա հեռախոսն անվտանգ օգտագործել և ստանալ հաղորդագրություններ հնարավոր հարձակումների վերաբերյալ, արագ վերականգնել հաշիվը, եթե այն ենթարկվի հաքերային հարձակման
4. Մտնել Facebook-ի անվտանգության բաժին վերևի աջ անկյունից՝ settings բաժնից, ընտրելով security հատվածը և միացնել Login notifications: Այդ գործողությունից հետո, եթե ինչ-որ մեկն ուրիշ սարքից մուտք կգործի ձեր հաշիվ, դուք կստանաք հաղորդագրություն մուտքի մասին: Օգտատերն ինքը կարող է որոշել, թե ինչպես ստանա զգուշացումը՝ SMS-ով, թե էլեկտրոնային հասցեով, կամ երկուսից էլ միասին:
5. Ամենակարևոր գործողությունը Two-factor authentication երկփուլային մուտքերի համակարգի միացումն է: Միացվում է Login Approvals, այնուհետև ամեն անգամ նոր սարքով գաղտնաբառը մուտքագրելուց հետո անհրաժեշտ է մուտքագրել նաև հատուկ կոդ:



Facebook հավելվածում Code Generator-ը:

Նշենք, որ սմարթֆոնների վրա տեղադրված է Facebook հավելվածը: Այս դեպքում միացվում է Code Generator-ը, և հավելվածն ինքը կես րոպեն մեկ գեներացնում է նոր կոդ (տե՛ս նկարում): Հնարավոր է նաև միացնել այլ հավելվածներ, օրինակ՝ Google Authenticator:

7. ՑԱՆՑԱՅԻՆ ՀԻԳԻԵՆԱՅԻ ՀԻՄՆԱԿԱՆ ԿԱՆՈՆՆԵՐԸ

Ինչպես հայտնի է, կիբեռվտանգների տեսակները բավական արագ են բազմանում, իսկ հաքերները ձգտում են գտնել հարձակման նոր ձևեր, պաշտպանության համակարգերը շրջանցելու նպատակով: Այսինքն՝ այս պահին նկարագրված անվտանգության խնդիրները և դրանց լուծումները կես տարի հետո արդեն կարող են թարմացման կարիք ունենալ: Այս համատեքստում որպես անվտանգության գլխավոր կանոն պետք է ընդունել նոր գիտելիքների ձեռքբերումը և ոլորտի նորություններին հետևելը:

Ցանցային հիգիենայի մյուս կանոններն են.

- Երբեք չշտապել, ամեն քայլը կատարելուց առաջ մի պահ մտածել, չկատարել մեխանիկական գործողություններ. օգտվողները հաճախ վարակում են համակարգիչները կամ այլ սարքերը վիրուսներով, քանի որ ավտոմատ գործողություններ են կատարում, ինչից էլ օգտվում են ցանցահենները
    - Միշտ հաշվի առնել այն հանգամանքը, որ վիրտուալ աշխարհում հաքերները կարող են նմանակել ձեր ծանոթ կայքերը կամ օգտատերերին և նրանց անունից հաղորդակցվել ձեզ հետ:

Օգտատիրոջ անձնական տվյալները, գաղտնաբառերը կորզելու համար հաքերներն օգտագործում են մի շարք տարածված մեթոդներ: Դրանք ներառում են կեղծ նամակներ, որոնք առաջարկում են մտնել հղումով և մուտքագրել այս կամ այն ծառայության գաղտնաբառը: Նամակները կարող են գալ միանգամայն այլ հասցեից, ինչն ուշադիր լինելու պարագայում հեշտ բացահայտվում է:

Սակայն հաքերները կարող են նույնիսկ կեղծել էլեկտրոնային փոստի հասցեն և տպավորություն ստեղծել, թե նամակը ստացվել է, օրինակ, Facebook, Yahoo ծառայություններից: Էլեկտրոնային հասցեների մի շարք ծառայություններ թույլ են տալիս դյուրինությամբ կեղծել հասցեն, նման դեպքերում իրական առաքողի հասցեն կարելի է գտնել միայն էլեկտրոնային նամակի կողը դիտելիս: Ընդ որում, նամակի մեջ հնարավոր է կեղծել ոչ միայն առաքողի հասցեն, այլ նաև հղումների հասցեները՝ օգտվողի մոտ տպավորություն ստեղծելով, թե նա ուղղորդվում է դեպի լեգիտիմ կայք: Կեղծ կայքն արտաքնապես կարող է իդեալական կերպով նույնականացվել որևէ հայտնի սոցիալական ցանցի, էլեկտրոնային փոստի, ինտերնետ խանութի արտաքին տեսքին: Իսկ հասցեն կարող է պարունակել ծանոթ բառեր, օրինակ՝ facebook.com-ի փոխարեն կարող է լինել http://facedook.co.gp, որտեղ նմանակվում են լատիներեն b և d տառերը: Կամ հասցեն կարող է պարունակել facebook բառը, օրինակ՝ http://www.facebook.pcriot.com: Անուշադիր օգտատերը նման կայքում ներմուծում է իր էլեկտրոնային հասցեն և գաղտնաբառը՝ այդպիսով հանձնելով դրանք հաքերներին: Այս կիբեռմեքենայությունն ընդունված է կոչել ֆիշինգ (phishing): Նման հարձակումներից խուսափելու համար պետք է հիշել, որ ոչ մի որակյալ ծառայություն չի պահանջում նամակով մուտքագրել գաղտնաբառը:

Չի կարելի անզգուշորեն բացել հղումներ, որոնք եկել են անգամ ձեր վստահելի ընկերներից, քանզի հնարավոր է, որ ընկերոջ հաշիվն արդեն իսկ գտնվում է հաքերների վերահսկողության տակ, և տվյալ նամակը նա չի կազմել, այլ ուղարկվել է ձեզ չարագործների կողմից: Նման մեթոդներով ձեր ընկերների անունից նամակագրություն տարածելով՝ հաքերները վարակում են սոցիալական ցանցերի մեծաթիվ օգտատերերի: Դրանք հասարակության լայն շրջանակներում ավելի հայտնի են որպես «ֆեյսբուքյան վիրուսներ»:

Ողջամտության սկզբունքից ելնելով՝ արժե հետևել հետևյալ պարզ կանոնին.

- նամակներով կամ մեսենջերով չուղարկել գաղտնաբառեր կամ անձնական գաղտնի այլ տվյալներ պարունակող տեղեկատվություն: Եթե ստիպված եք նման հաղորդագրություններ ուղարկել, փորձեք դրանք բաժանել մի քանի մասի և հատվածներ ուղարկել տարբեր տիպի ծառայություններով: Ուղարկելուց հետո դրանք անպայման ջնջեք, իսկ հետո պարտադիր մաքրեք աղբամանը, նույնը պահանջեք նաև ստացող կողմից:

8. ԹՐԱՖԻԿԻ, ՀԵՌԱԽՈՍՆԵՐԻՑ ՀԱՂՈՐԴԱԳՐՈՒԹՅՈՒՆՆԵՐԻ ԵՎ ԶԱՆԳԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆ

TunnelBear VPN հավելվածը դիտարկչի (բրաուզերի) համար, *Chrome Web Store*.

Թրաֆիկի պաշտպանությունը. օգտատիրոջ այցելած կայքերի, ընթերցված հոդվածների ցանկը կարող է վերահսկվել, եթե չեն կիրառվում հատուկ պաշտպանական միջոցներ, մանավանդ եթե օգտվողն այցելում է կայքեր, որոնք պաշտպանված չեն https գաղտնագրմամբ: Պետք է հիշել, որ եթե կայքը չի միանում https տարբերակով, ապա դրա վրա չի կարելի մուտքագրել ոչ մի զգայուն տեղեկատվություն՝ գաղտնաբառեր, անձնական տվյալներ և այլն: Եթե https-ն ակտիվացված չէ կայքի վրա, ապա ողջ բովանդակությունը կարող է ազատ ընթերցվել երրորդ անձի կողմից:

Այսպիսով, եթե որևէ կայքում մուտքագրում եք ձեր անձնական տվյալները, լինեն գաղտնաբառը, անձնագրային տվյալները և այլն, ապա պետք է համոզվեք, որ կայքի վրա միացված է https արձանագրությունը: Դրա բացակայության դեպքում հեռացեք այդ կայքից և ոչ մի դեպքում մի մուտքագրեք ձեր տվյալները, քանի որ մեծ հավանականությամբ դրանք կհայտնվեն ուրիշի ձեռքում: Դա նաև նշանակում է, որ տվյալ կայքն անփույթ է վերաբերվում անձնական տվյալներին, ինչն արդեն իսկ մեծ խնդիր է օգտվողի համար:

Սրճարաններում, օդանավակայաններում հանրային WiFi կապից օգտվելիս նույնպես կարելի է կորցնել կարևոր տեղեկատվություն, օրինակ՝ գաղտնաբառեր, բանկային տվյալներ և այլն: Հաքերներն օգտագործում են նման հանրային կետերը օգտվողների դեմ հարձակումներ իրականացնելու համար: Այդ իսկ պատճառով, թրաֆիկը պաշտպանելու նպատակով օգտվում են հատուկ կապի գաղտնագրված այսպես կոչված թունելներից, որոնք թույլ չեն տալիս ուրիշներին տեսնել, թե դուք որ կայքերն եք այցելում, ինչ եք ընթերցում և ինչ տվյալներ եք փոխանցում: Դա իրականացվում է VPN (Virtual Private Network) ծառայության միջոցով, որը ստեղծում է գաղտնագրված թունելային կապ և դուրս է բերում ձեզ դեպի ցանց այլ կետից, հաճախ՝ նույնիսկ այլ երկրի տարածքից, այնպես, որ հնարավոր հարձակվողը չի տեսնում ձեր գործողությունները ցանցում և որ երկրից եք իրականում մտնում ինտերնետ:

Սա հիմնականում վճարովի ծառայություն է, որի վարձը հասնում է ամսական $3-10-ի: Սակայն, եթե սահմանափակ թրաֆիկ եք օգտագործում, կան անվճար լուծումներ: Դուք կարող եք VPN միացնել անմիջապես դիտարկչից, ինչն արվում է մեկ կտտոցով: Օրինակ՝ Google Chrome ամենատարածված դիտարկչի համար գոյություն ունեն մի շարք անվճար ծառայություններ՝ TunnelBear VPN, ZenMate, Hotspot Shield, որոնք ներբեռնվում են դիտարկչի հավելվածների Chrome Web Store խանութից: Բացի այդ, նույն ծառայությունները գործում են որպես համակարգչի համար ծրագրեր (տե՛ս նկարում):

Կարևոր է, որ նման ծրագրերը հասանելի են որպես հավելվածներ հեռախոսների և պլանշետների համար՝ Psiphon, Opera Free VPN, TunnelBear VPN, Hotspot Shield: Այսպիսով, հանրային ցանցից օգտվելիս անպայման պետք է միացնել VPN:

Ավելի լուրջ թրաֆիկի գաղտնագրման, սեփական անոնիմության ապահովման համար կարելի է օգտագործել Tor դիտարկիչը, որն այսօր համարվում է ամենաապահովներից մեկը: Այն հնարավոր է ներբեռնել Torproject.org կայքից:

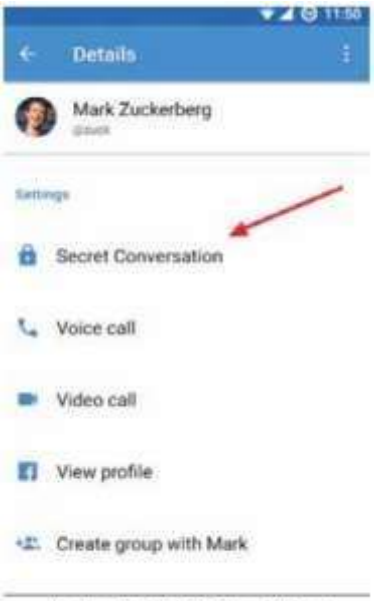
Հեռախոսներից հաղորդագրությունների և զանգերի պաշտպանությունը. SMS հաղորդագրությունները վտանգված են, քանի որ կարող են հասանելի դառնալ ինչպես հատուկ ծառայություններին, այնպես էլ օպերատորների աշխատակիցներին և այլ անձանց: Դրանց միջոցով գաղտնի կամ անձնական տեղեկատվություն չպետք է ուղարկվի:

Համարվում է, որ Facebook–ը և Skype-ը ինչ-որ չափով ապահովում են ձեր անվտանգությունը: Սակայն Էդվարդ Սնոուդենի բացահայտումները խոսում են այն մասին, որ այդ ծրագրերը նույնպես կարող են վերահսկվել: Facebook–ը և Skype-ը պարբերաբար համագործակցում են հատուկ ծառայությունների հետ, և հնարավոր է, որ օգտատերերի նամակագրությունը հայտնվի նրանց ձեռքում: Նշենք նաև, որ հաղորդագրությունները պահպանվում են տվյալ ծառայությունների սերվերների վրա նույնիսկ ձեր կողմից դրանք ջնջելուց հետո:

Վերոնշյալ հանգամանքներից ելնելով՝ կարևոր տեղեկատվության փոխանակման համար նախատեսված ծրագրերը պետք է համապատասխանեն հետևյալ պահանջներին.

- ստուգված լինեն երրորդ կողմի փորձագետների կողմից

- ներառեն արդիական գաղտնագրման մեթոդներ, որոնք ենթադրում են գաղտնագրում հենց սարքի վրա և գաղտնազերծում միայն ընդունող սարքի վրա, առանց միջանկյալ օղակների (End-to-end encryption)
- նման ծրագրերի միջոցով կատարված հաղորդագրությունները այնպես պետք է գաղտնագրվեն, որ ընթեռնելի չլինեն անգամ տվյալ ծառայության փորձագետների կողմից
- ծրագրերը պետք է հնարավորություն տան ոչնչացնել հաղորդագրությունները՝ չթողնելով դրանց օրինակներն այլ սարքավորումների վրա։



Facebook-ի մեսենջերում Secret Conversation միացնելու վահանակը

Այսօր արդիական գաղտնագրում են ներմուծել Whatsapp, Viber մեսենջերները (messenger)։ Facebook-ն իր հերթին ներմուծել է գաղտնագրված հաղորդագրությունների տարբերակ Secret Conversation հատուկ ծրագրի միջոցով (տե՛ս նկարում)։

Telegram մեսենջերն ունի հատուկ պաշտպանված հաղորդագրությունների տարբերակ secret chat ռեժիմում։ Այս տարբերակներում հաղորդագրությունները պաշտպանված են համարվում, և դեռ հայտնի չեն դեպքեր երրորդ անձանց կողմից դրանք գաղտնալսելու մասին։ Այսօր ամենաանվտանգ մեսենջերներից է համարվում Signal Private Messenger-ը (whispersystems.org)։

Վերոնշյալ նկատառումները վերաբերում են նաև հեռախոսային, ձայնային զանգերին։ Այստեղ նույնպես կան մի քանի հավելվածներ, որոնք թույլ են տալիս կատարել հեռախոսազանգեր, որոնք հնարավոր չէ գաղտնալսել։ Այստեղ կարելի է խորհուրդ տալ հետևյալ երկու զանգեր կատարելու ծրագրերը՝ նույն Signal Private Messenger-ը և Silent Phone (silentcircle.com)-ը։

***

Ինչպես արդեն բազմիցս նշել ենք, տեղեկատվական անվտանգության առաջնային նախապայմաններից են գիտելիքային ռեսուրսները։ Այս հանգամանքն առավել կարևոր է կիբեռանվտանգության ոլորտում, որտեղ փոփոխությունները և նորարարությունները կատարվում են խիստ արագ, և պետք է ունակ լինել դրանք ընկալելու և համապատասխանաբար կիրառելու համար։ Միևնույն ժամանակ, եթե անձը կամ կազմակերպությունը հանդիսանում են կարևոր, պետական նշանակություն ունեցող տեղեկատվության կրողներ, ապա անհրաժեշտ են ինստիտուցիոնալ բնույթի կառույցներ, որոնց խնդիրը պետք է լինի աջակցել նման օգտատերերին ինչպես խորհրդատվություններով, այնպես էլ համապատասխան ծրագրային միջոցներ տրամադրելով։

Վերը ներկայացված նյութերից հետևում է նաև, որ եթե ավանդական ԶԼՄ-ի միջոցով ձևավորված տեղեկատվական տարածքի վերահսկումը լուրջ խնդիր է, ապա հարափոփոխ կիբեռտարածքը կարգավորելուն միտված ջանքերը բախվում են անհամեմատ ավելի լուրջ խոչընդոտների։ Սակայն աշխատանքներ այդ ուղղությամբ, միևնույն է, կատարվում են։ Միջազգային հանրության կողմից կիբեռտարածքում իրավական նորմեր հաստատելու փորձերը կներկայացվեն ստորև։

9. ՎՆԱՍԱԿԱՐ ԾՐԱԳՐԵՐ

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 «օգտակարությունը» 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:

Իրենց պահելաձևից ելնելով վիրուսները բաժանվում են երկու խմբի.

- ռեզիդենտ
- ոչ ռեզիդենտ վիրուսների:

Ռեզիդենտ (կամ նույն է թե մշտապես տեղակայված) այս տեսակի վիրուսների վարակիչ կոդերը (վերարտադրվող մոդուլը) իրենց բեռնում են օպերատիվ հիշողության մեջ (ասել է թե մշտապես տեղակայվում են այնտեղ), որևէ վարակված ծրագրին կցված լինելով, և սպասում այնտեղ ակտիվ վիճակում այնքան ժամանակ մինչև օպերացիոն համակարգը կամ օգտագործողը չաշխատացնի այլ ծրագիր: Վերջինս վարակվելով, վերահսկողությունը հանձնում է արդեն նոր տիրոջը և սպասում իր հաջորդ «զոհին»:

Ռեզիդենտ վիրուսները հաճախ բաժանում են արագ վարակող կամ դանդաղ վարակող վիրուսների: Արագ վարակող ռեզիդենտ վիրուսները կարող են վարակել բոլոր այն ֆայլերը, որոնք այդ պահին սկսում են աշխատել: Նման դեպքում անգամ հենց ինքը հակավիրուսը, եթե չի հայտնաբերել, որ վիրուսի կիրառական մոդուլը նստած է հիշողության մեջ և այն չի վերացրել, կարող է պատճառ դառնալ ամբողջ համակարգչի ֆայլերի վարակմանը: Այդ դեպքում, հակավիրուսի ընդլայնված սքանավորման ժամանակ, յուրաքանչյուր ֆայլի վրա անցնելիս, ակտիվացնում է վերջիններիս դրանով իսկ թույլ տալով վիրուսին տեսնել և վարակել դրանք: Դանդաղները, հակառակը՝ փորձում են հնարավորինս քիչ ֆայլեր վարակել և դրանով իսկ անտեսանելի մնալ:

Ի տարբերություն ռեզիդենտ վիրուսների, ոչ ռեզիդենտները ունեն երկու մոդուլ՝ փնտրման և վերարտադրվելու: Երբ վիրուսը վարակում է համակարգիչը նրա փնտրման մոդուլը անմիջապես փնտրում է նոր ֆայլեր և գտնելով այն դիմում է վերարտադրման կամ վարակիչ մոդուլի օգնությանը, որպեսզի վերջինս վարակի այն:

Օգտագործողներից շատերը չեն էլ գիտակցում վիրուսի ներկայության մասին՝ չնայած որ հաճախ վիրուսների առկայությունը երևում է այս կամ այն ախտանշանից:

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:

Ֆայլային վիրուսներ

ֆայլային վիրուսներ (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 կրող վիրուսը: Նման վիրուսակիր ծրագրի աշխատանքը սկսելուց հետո վիրուսը տեղակայվում է համակարգչի օպերատիվ հիշողության մեջ և կարող է մինչև մեքենան անջատելը վարակել այդ ընթացքում կիրառված ծրագրերը:

Բեռնավորվող վիրուսներ

Բեռնավորվող վիրուսները վնասում են սկավառակների այն տիրույթները, որոնք ծառայում են օպերացիոն համակարգի բեռնավորման համար: Նման վիրուսի օրինակ է Win95CIH «Չեռնոբիլ» անվամբ վիրուսը, որը 1998-99 թվականներին 5 մլն. համակարգիչներ շարքից հանեց:

Տրոյական վիրուսներ

Տրոյական վիրուսներ. սրանք այն վտանգավոր վիրուսներն են, որոնք ունակ են «գաղտնի» աշխատել: Այդ ընթացքում կարող են ոչ միայն համացանց մտնելու Ձեր գաղտնաբառը, այլև վարկային կտրոնի համարն իմանալ, այնուհետև այդ տեղեկություններն համացանցով այլ

համակարգիչ ուղարկել: Հիմնավորվելով վերջինիս վրա՝ նման վիրուսներն այնուհետև սկսում են գործել Ձեր անունից:

Հարցեր և առաջադրանքներ

1. Համակարգչային վիրուս
2. Ծրագրային վնասակար միջոցներ
3. Վիրուսների խմբերը

10. ՎՆԱՍԱԿԱՐ ԾՐԱԳՐԵՐԻ ՏԱՐԱԾՄԱՆ ՁԵՎԵՐԸ

Համակարգչային վիրուսը ծրագիր է, որը կարող է ինքն իրեն պատճենել և տարածվել՝ վարակելով համակարգիչն առանց օգտագործողի թույլտվության կամ իմացության: Շատ հաճախ սխալմամբ վիրուս են ավնանում ցանկացած վնասակար ծրագիր:

Երբեմն համակարգչային վիրուսը կարող է նաև փոփոխել ինքն իրեն, կամ իր պատճենները կարող են փոփոխել իրենց, դրանք այսպես կոչված մետամորֆիկ վիրուսներ են: Դասական վիրուսները կարող են վարակել այլ համակագիչ միայն այն դեպքում, երբ վարակված ծրագիրը տեղափոխվում է այլ համակարգի վրա և աշխատեցվում է:

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:

Վիրուսներ

Ժամանակակից անհատական համակարգչով աշխատելիս օգտագործողներին (մանավանդ սկսնակ) կարող են հետապնդել շատ անհաջողություններ՝ տվյալների կորուստ, համակարգի կախում, համակարգչի առանձին մասերի խափանում և այլն: Պատճառներից մեկը կարող է հանդիսանալ վիրուսային ծրագրերի ներխուժումը համակարգչային համակարգ: Վիրուսները գրեթե ամենավտանգավոր թշնամիներն են համակարգչի համար: Այդ ծրագրերը կենսաբանական վիրուսների նման բազմանում են՝ գրանցվելով սկավառակի համակարգային տարածքում, կամ կցվելով ֆայլերին՝ կարող են կատարել տարբեր ոչ ցանկալի գործողություններ:

Այսօր ամենատարածված վիրուսների խումբը՝ մակրովիրուսներն են, որոնք վարակում են ոչ թե ծրագրերը, այլ Microsoft Office ընտանիքի ծրագրերով ստեղծված փաստաթղթերը: Վիրուսները համակարգիչ կարող են ներխուժել սկավառակների հետ կամ էլեկտրոնային փոստի հաղորդագրության հետ: Որպեսզի չդառնալ վիրուսների զոհը, ամեն մի օգտագործող պետք է իմանա համակարգչային վիրուսներից պաշտպանվելու սկզբունքները, քանի որ վիրուսները վերջնականապես ոչնչացնելու ոչ մի հույս չկա: Հին ժամանակներից հայտնի է, որ ցանակացած թույնի համար ուշ թե շուտ կգտնվի նրա հակաթույնը: Համակարգչային աշխարհում այդ հակաթույները կոչվում են հակավիրուսներ:

Համակարգչային վիրուսը հատուկ, որպես կանոն փոքր ծավալի ծրագիր է, որը կարող է գրանցել իր պատճենները համակարգչի համակարգային տարածքում, դրայվերներում, փաստաթղթերում և այլ տեղերում: Վիրուսի պատճենի ներխուժումը մեկ այլ ծրագիր կոչվում է վարակում, իսկ ծրագիրը, որը պարունակում է վիրուսը՝ կոչվում է վարակված:

Այսօր գիտությանը հայտնի է մոտ 40 հազար համակարգչային վիրուսներ և դրանք օրեցօր շատանում են: Բիոլոգիական վիրուսների նման համակարգչային վիրուսներին տարածվելու համար

անհրաժեշտ են «կրիչներե՝ առողջ ծրագրեր կամ փաստաթղթեր: Ինքը վիրուսը մեծ ծավալի ծրագիր չէ, հիմնականում չի գերազանցում մեգաբայթը: Այն պահին, երբ օգտագործողը ոչինչ չկասկածելով բաց է թողնում վարակված ծրագիրը, վիրուսը ակտիվանում է և սկսում է իր վտանգավոր գործունեությունը: Բացի ծրագրեր վնասելուց՝ կան ժամանակակից վիրուսներ, որոնք կարող են վնասել «երկաթը: Օրինակ. ոչնչացնում են BIOS-ի պարունակությունը, կամ վնասում են կոշտ սկավառակը:

Առաջին համակարգչային վիրուսները եղել են հասարակ և օգտագործողից չեն թաքնվել, այլ մոնիտորին արտապատկերել են նկարներ և կատակներ: Օրինակ. ասեք Կլիմանջարո լեռան բարձրությունը միլիմետրերով: Սխալ պատասխանի դեպքում կոչնչանան ձեր կոշտ սկավառակի բոլոր տվյալները: Բացահայտել այդպիսի վիրուսները դժվար չէր: Նրանք կպչում էին *.com և *.exe ֆայլերին փոփոխելով նրանց իսկական չափսերը: Հետագայում վիրուսները սկսեցին թաքցնել իրենց ծրագրային կոդը այնպես, որ ոչ մի հակավիրուս չէր կարողանում հայտնաբերել: Այդպիսի վիրուսները կոչվում էին ՝անտեսանելի 90-ական թվականներին վիրուսները սկսեցին արագ փոխել իրենց ծրագրային կոդը, այն թաքցնելով կոշտ սկավառակի տարբեր մասերում: Այդպիսի մուտանտ վիրուսները կոչվեցին՝ «Տրոյան վիրուսներ»: Վիրուսների տարածման մեջ մեծ ներդրում ունեցավ ինտերնետը: 1998-1999 թվականներին աշխարհը ցնցվեց մի քանի կործանիչ վիրուսային գրոհներից: Melissa Win95.CIH և Chernobyl վիրուսների գործունեության արդյունքում շարքից դուրս եկան մոտ 5մլն. համակարգիչներ ամբողջ աշխարհում: Այդ վիրուսները փչցնում էին համակարգչի կոշտ սկավառակը և ոչնչացնում էին մայրական հարթակի BIOS ծրագիրը:

Վտանգավոր և անվտանգ վիրուսներ

Վիրուսների մեծամասնությունը չեն կատարում ինչ-որ գործողություններ, բացի իրենց տարածումից (վարակելով այլ ծրագրեր, սկավառակներ և այլն) և երբեմն արտածում են հաղորդագրություններ, կամ վիրուսի հեղինակի կողմից ստեղծված այլ էֆեկտներ՝ խաղեր, երաժշտություններ, համակարգչի կախում, մոնիտորին հայտնվում են նկարներ, ստեղների ֆունկցիայի փոփոխում, համակարգչի աշխատանքի դանդաղեցում և այլն: Բայց այդ վիրուսները ինֆորմացիային լուրջ վնաս չեն հասցնում: Այդպիսի վիրուսները պայմանականորեն կոչվում են անվնաս: Ի դեպ, անվնաս վիրուսներն էլ կարող են պատճառել մեծ անհաջողություններ (օրինակ. համակարգչի վերաբեռնումը ամեն 5 րոպեն մեկ ձեզ թույլ չի տալիս հանգիստ աշխատել): Եթե տվյալների վնասումը կատարվում է պարբերաբար և դա չի ունենում ծանր հետևանքներ, ապա այդ վիրուսները կոչվում են վտանգավոր: Իսկ եթե վնասումը կատարվում է հաճախակի, կամ վիրուսները հասցնում են լուրջ վնասներ (կոշտ սկավառակի ֆորմատավորում, տվյալների սիստեմատիկ փոփոխում սկավառակի վրա և այլն) ապա այդպիսի վիրուսները կոչվում են շատ վտանգավոր:

Վարակվող օբյեկտներ

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 սկսում 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 ձնակերպում 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։

Հարցեր և առաջադրանքներ

1. Համակարգչի վիրուսը հիմնականում ո՞ր ընդլայնումով ֆայլերին է վարակում։
2. Ի՞նչ է համակարգչային վիրուսը։

11. ՎՆԱՍԱԿԱՐ ԾՐԱԳՐԵՐԻ ՏԱՐԱԾՄԱՆ ԴԵՄ ՊԱՅՔԱՐԻ ԵՂԱՆԱԿՆԵՐԸ

Վիրուսներից պաշպտպանվելու եղանակը

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։ Համակրգչի 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)
- աշխատանքի անսովոր վթարային ավարտ
- տեղեկատվական ֆայլերի կործանում կամ մասնակի վնասում
- ստեղմանաշարից ներմուծման արգելափակում
- ազատ օպերատիվ հիշողության ծավալի անհիմն փոքրացումը
- համակարգչի աշխատանքի և բեռնավորման գործընթացի դանդաղումը
- տեքստային փաստաթղթի աղավաղումը
- օպերացիոն համակարգի բեռնավորման սխալները
- ֆայլերի բազմաթիվ կրկնօրինակների ավտոմատ ստեղծումը և այլն։

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 սոցիալական կայքերից և էլեկտրոնային փոստից օգտվելիս, հաճախակի են դարձել վիրուսների ներխուժումը համակարգիչ փոստային հաղորդագրությունների միջոցով: Այս տեսակի վիրուսները կոչվում են սպամ: 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:

Հարցեր և առաջադրանքներ

1. Վիրուսների դրսևորումները համակարգչում
2. Վիրուսների համակարգիչ ներթափանցումը

12. ԾՐԱԳՐԵՐԻ ՕԳՏԱԳՈՐԾՈՂՆԵՐԻ ԻՐԱՎՈՒՆՔՆԵՐԸ, ՀԵՂԻՆԱԿԱՅԻՆ ԻՐԱՎՈՒՆՔԻ ՆՈՐՄԵՐԸ

Արման Քելինյանն աշխատում է թերթի խմբագրությունում: Նա պետք է հոդված պատրաստի համակարգչային տեխնոլոգիաների մասին: Արմանը որոշ տեղեկություններ է պատճենում մի կայքից ու օգտագործում դրանք իր հոդվածում: Սակայն, նա չի նշում այն աղբյուրը, որից պատճենել էր այդ տեղեկությունները: Հոդվածի հրապարակումից հետո Արմանին մեղադրանք է ներկայացվում հեղինակային իրավունքը խախտելու համար, որովհետև նա օգտագործել է մտավոր սեփականության օբյեկտը առանց սեփականատիրոջ թույլտվության:

Համացանցում հասանելի ցանկացած տեղեկություն մտավոր սեփականություն է համարվում, որն օրենքով այդ տեղեկությունը ստեղծողի սեփականությունն է: Օրինակ, երբ համակարգչից օգտվողը հոդված է հրապարակում որևէ կայքում, այդ հոդվածը համարվում է նրա մտավոր սեփականությունը: Որպես մտավոր սեփականության իրավատեր՝ նա բացառիկ իրավունքներ ունի վերահսկելու այդ նյութի օգտագործումը, ինչպես օրինակ՝

- պատճենումը, վերարտադրումը կամ տարածումը,
- իրավունքների համատեղ օգտագործումը կամ վաճառքը,
- իրավունքներից անհատույց հրաժարվելը:

Նշում.
Մտավոր սեփականության օբյեկտի նկատմամբ իրական իրավունքները կարող են տարբերվել՝ ըստ սեփականատիրոջ տրված թույլտվության:

Ոչ ոք իրավունք չունի օգտագործել մտավոր սեփականության օբյեկտը առանց սեփականատիրոջ թույլտվության: Գոյություն ունեն օրենքներ, որոնք պաշտպանում են անձի՝ մտավոր սեփականության օբյեկտի նկատմամբ իրավունքները: Դրանք հեղինակային իրավունքի մասին օրենքներն են: Այդ օրենքների խախտումը կարող է ունենալ իրավական հետևանքներ:

Հեղինակային իրավունքը խախտելը և այդ խախտումները կանխելը

Առանց սեփականատիրոջ համաձայնության հեղինակային իրավունքով պաշտպանված մտավոր սեփականության օբյեկտն օգտագործելը համարվում է հեղինակային իրավունքի խախտում: Ստորև ներկայացված են հեղինակային իրավունքի խախտման հնարավոր պատճառները և դրանցից խուսափելու միջոցները:

Գրագողություն

Որևէ մեկի աշխատանքը պատճենելը և այն, առանց աղբյուրին հղում կատարելու, օգտագործելը սեփական աշխատանքում կոչվում է գրագողություն: Պատկերացրեք մի իրավիճակ, երբ ստեղծել եք որևէ կայքում ցուցադրված գծապատկերի ճշգրիտ պատճենը: Այնուհետև այդ գծապատկերը զետեղել եք այլ կայքում՝ որպես սեփական ստեղծագործություն՝ առանց հղում կատարելու այն կայքին, որտեղից պատճենել եք այդ գծապատկերը: Դա համարվում է գրագողություն:

Շատ երկրներում որևէ մեկի աշխատանքը վերափոխելը և այն որպես բնօրինակ ներկայացնելը նույնպես գրագողություն է համարվում:

Հարցեր և առաջադրանքներ

1. Ո՞րն է մտավոր սեփականությունը
2. Հեղինակային իրավունքի խախտումը
3. Գրագողություն

13. ՀԵՂԻՆԱԿԱՅԻՆ ԻՐԱՎՈՒՆՔՈՎ ՊԱՇՏՊԱՆՎԱԾ ՆՅՈՒԹԵՐԸ ԵՎ ՆՅՈՒԹԵՐԻ ՕԳՏԱԳՈՐԾՈՒՄԸ

Ստորև նշված աղյուսակում ներկայացված է հեղինակային իրավունքով պաշտպանված նյութերի օգտագործման կանոնների խախտման այն հիմնական եղանակները, որոնց պետք է տեղյակ լինել և որոնցից պետք է խուսափել։

<u>Հեղինակային իրավունքի օբյեկտի օգտագործման կանոնների խախտում</u>

Երաժշտություն պատճենելը

Նկարագրություն

Շատ կայքեր երգերի ներբեռնման և համատեղ օգտագործման հնարավորություն են տալիս։ Սակայն, դրանց մի մասը կարող է երգերն անվճար ներբեռնելու հնարավորություն տրամադրելու իրավունք չունենալ։ Այդ կայքերից երգերի ներբեռնումը հեղինակային իրավունքով պաշտպանված երաժշտության օգտագործման կանոնների խախտում է։

Հեղինակային իրավունքով պաշտպանված երաժշտության օգտագործման կանոնների խախտում են համարվում հետևյալ գործողությունները՝

- առանց հեղինակային իրավունքի օբյեկտի սեփականատիրոջ թույլտվության կամ առանց հեղինակային վարձատրության վճարման կայքից հեղինակային իրավունքով պաշտպանված երաժշտություն ներբեռնելը,
- կայքից հեղինակային իրավունքով պաշտպանված երաժշտություններ բեռնելը և ներբեռնած երաժշտություն պարունակող ՍՍ–ներ կամ ԹԲՍ–ներ ստեղծելը,
- հեղինակային իրավունքով պաշտպանված ՍՍ–ներ կամ ԹԲՍ–ներ պատճենելը և այլ անձանց այդ պատճենները տրամադրելը,
- երգերի տարածումը հեշտացնող կայքերի միջոցով հեղինակային իրավունքով պաշտպանված երգեր տարածելը։

Առանց լիցենզիայի (թույլտվության) ծրագրաշար օգտագործելը

Նկարագրություն

Առանց հեղինակային իրավունքի իրավատիրոջ կողմից լիցենզիա կամ թույլտվություն ստանալու հեղինակային իրավունքով պաշտպանված ծրագրաշարի չթույլատրված պատճենումը համարվում է ծրագրաշարի գողություն։

Ծրագրաշարի գողությունից խուսափելու նպատակով անհրաժեշտ է տեղյակ լինել հետևյալ իրավիճակներին՝

- առանց իրավատիրոջ թույլտվության կամ հեղինակային վարձատրության վճարման կայքից հեղինակային իրավունքով պաշտպանված ծրագրաշարներ բեռնելը համարվում է ծրագրաշարի գողություն,
- ծրագրաշարի օրինական պատճենը գնելը, ծրագրաշար պատճենելը և այլ անձանց պատճենները բաժանելը նույնպես համարվում է ծրագրաշարի գողություն,
- որոշ համակարգիչ վաճառողներ համակարգիչներում տեղադրում են ծրագրաշարի չլիցենզավորված պատճեններ։ Դրա նպատակը լիցենզիայի համար նախատեսված գումարը խնայելն է։ Այնուամենայնիվ, չլիցենզավորված ծրագրաշարով համակարգիչներ գնելը նույնպես համարվում է ծրագրաշարի գողություն։ Այդ պատճառով, համակարգիչ գնելիս անհրաժեշտ է ունենալ համակարգչում նախօրոք տեղադրված կամ համակարգչի հետ վաճառված ծրագրաշարի համար լիցենզիային առնչվող փաստաթղթեր։

Պատկերանշանը պատճենելը

Նկարագրություն

Պատկերանշանը հեղինակային իրավունքով պաշտպանված նյութ է, որն օգտագործվում է հեղինակային իրավունքի իրավատիրոջ կողմից որպես նույնացման նշան: Առանց իրավատիրոջ թույլտվության պատկերանշանի պատճենումը կամ օգտագործումը անօրինական է: Օրինակ՝ այցեքարտի վրա Մայքրոսոֆթի պատկերանշանի օգտագործումն առանց Մայքրոսոֆթ ընկերության թույլտվության հեղինակային իրավունքի խախտում է:

Երբեմն հնարավոր է պատկերանշանն օգտագործելու թույլտվություն ունենալ, սակայն այդ օգտագործման նկատմամբ լինեն որոշակի սահմանափակումներ: Օրինակ՝ կարելի է Մայքրոսոֆթի պատկերանշանն օգտագործելու թույլտվություն ունենալ, որից հնարավոր է օգտվել բացառապես Մայքրոսոֆթի անունից գործարքներ կատարելու դեպքում: Իսկ, երբ Մայքրոսոֆթի պատկերանշանն օգտագործվում է անձնական նպատակներով գործարքներ կատարելու համար, ապա դա համարվում է հեղինակային իրավունքով պաշտպանված պատկերանշանի օգտագործման կանոնների խախտում:

Լրացուցիչ տեղեկություններ

Կայքից կարող է հնարավոր լինել ներբեռնել հեղինակային իրավունքով պաշտպանված տեղեկություններ, սակայն, նման տեղեկություններ ներբեռնելը կարող է իրավական հետևանքներ ունենալ: Սովորաբար կայքում հասանելի տեղեկությունները պաշտոնապես պաշտպանված են հեղինակային իրավունքով և կրում են հեղինակային իրավունքի վերաբերյալ ծանուցում կամ հեղինակային իրավունքի նշան: Սակայն, ցանկացած տեղեկության հետ հեղինակային իրավունքի վերաբերյալ ծանուցման կամ հեղինակային իրավունքի նշանի բացակայությունը չի նշանակում, որ տեղեկությունը պաշտպանված չէ հեղինակային իրավունքով: Հեղինակային իրավունքի ոլորտը կարգավորող՝ Միացյալ Թագավորության օրենսդրության համաձայն՝ մտքին կամ գաղափարին ֆիզիկական տեսք հաղորդելու դեպքում աշխատանքը ինքնաբերաբար դառնում է տվյալ անձին պատկանող՝ հեղինակային իրավունքով պաշտպանված օբյեկտ: Նմանապես, հեղինակային իրավունքի ոլորտը կարգավորող՝ ԱՄՆ օրենսդրության համաձայն՝ հեղինակային իրավունքի իրավատերը, նույնիսկ առանց սեփականության իրավունքի պաշտոնական գրանցման, հեղինակային իրավունքով պաշտպանված օբյեկտի նկատմամբ ունի բացառիկ իրավունքներ:

Հեղինակային իրավունքի ցանկացած խախտում պատժելի իրավախախտում է: Հեղինակային իրավունքի իրավատերը կարող է պատասխանատվության կանչել հեղինակային իրավունքին առնչվող օրենքները խախտող անձանց կամ խոշոր գումար պահանջել հեղինակային իրավունքի խախտումների դիմաց: Այդ պատճառով, որևէ կայքից տեղեկություններ ներբեռնելուց առաջ անհրաժեշտ է ծանոթանալ հեղինակային իրավունքին առնչվող միջազգային և տեղական օրենքներին:

Հեղինակային իրավունքով պաշտպանված օբյեկտի օրինական օգտագործումը

Ստորև նշված աղյուսակում ներկայացված է հեղինակային իրավունքով պաշտպանված օբյեկտների օրինական օգտագործման մի քանի եղանակ:

Օրինական օգտագործում

Ուսումնական նպատակներով հեղինակային իրավունքով պաշտպանված նյութն օգտագործելը

Նկարագրություն

Հեղինակային իրավունքով պաշտպանված նյութերից փոքր մասերի՝ ուսումնական նպատակներով օգտագործումը և դրանց աղբյուրը նշելը համարվում է հեղինակային իրավունքով պաշտպանված նյութի բարեխիղճ օգտագործում: Օրինակ՝ կարելի է փոքր հատվածներ օգտագործել գրքից՝ դպրոցում կամ քոլեջում հանձնարարված տնային

աշխատանքներում նշելով այդ գրքի անվանումը: Նմանապես, գրքի մասին գրախոսություններ կայացնելիս կարելի է գրքից մեջբերումներ կատարել:

Ներբեռնած նյութի փոխարեն հղումներ օգտագործելը

Նկարագրություն

Կայքերից նյութեր պատճենելու և աշխատանքում օգտագործելու փոխարեն կարելի է այդ նյութերին հղումներ կատարել: Օրինակ՝ կարող է անհրաժեշտություն առաջանալ հոդվածում նշել որոշակի կայքում պարունակվող բովանդակության մասին: Կայքից նյութերը պատճենելու փոխարեն կարելի է պարզապես տեղադրել հղում այդ կայքին: Այդ կերպ կարելի է ընդհանրապես խուսափել հեղինակային իրավունքով պաշտպանված նյութի գրագողությունից:

Հեղինակային իրավունքի իրավատիրոջ թույլտվությամբ հեղինակային իրավունքով պաշտպանված նյութն օգտագործելը

Նկարագրություն

Աշխատանքում կարելի է օգտագործել հեղինակային իրավունքով պաշտպանված նյութեր՝ հեղինակային իրավունքի իրավատիրոջից թույլտվություն ստանալուց հետո: Հեղինակային իրավունքով պաշտպանված նյութն օգտագործելու համար հիմնականում պահանջվում է գրավոր թույլտվություն:

Պետք է հաշվի առնել, որ հեղինակային իրավունքի իրավատերը իր հայեցողությամբ՝

- շնորհում կամ մերժում է հեղինակային իրավունքով պաշտպանված նյութն օգտագործելու թույլտվությունը,
- իրավունքներ է տալիս հեղինակային իրավունքով պաշտպանված ամբողջ նյութի կամ դրա որևէ մասի նկատմամբ,
- վարձատրության վճար է գանձում հեղինակային իրավունքով պաշտպանված նյութն օգտագործելու թույլտվություն տալու համար,
- սահմանում է պայմաններ և ժամկետներ՝ հեղինակային իրավունքով պաշտպանված նյութն օգտագործելու համար: Օրինակ՝ կարելի է ունենալ հեղինակային իրավունքով պաշտպանված ծրագրաշարը ներբեռնելու և տարածելու թույլտվություն, սակայն շահույթ ստանալու համար ծրագիրն օգտագործելու թույլտվություն չունենալ:

Եթե լրացել է նյութի նկատմամբ հեղինակային իրավունքի գործողության ժամկետը, կամ հեղինակային իրավունքով պաշտպանված նյութում օգտագործվող գաղափարը կամ գործընթացը հայտնի է բոլորին, նյութը կամ գաղափարը կարող է օգտագործվել առանց թույլտվություն ստանալու:

Հարցեր և առաջադրանքներ

1. Հեղինակային իրավունքով պաշտպանված երաժշտության օգտագործման կանոնների խախտում համարվող գործողությունները
2. Ծրագրաշարի գողությունից խուսափելու նպատակով անհրաժեշտ իրավիճակները
3. Պատկերանշան

Ծրագրերն՝ ըստ իրենց իրավական կարգավիճակի կարելի է բաժանել 3 խմբի՝

- լիցենզավորված,
- պայմանականորեն անվճար (shareware - պայմանականորեն),
- ազատ տարածվող (freeware - անվճար):

Լիցենզավորված ծրագրերի դիստրյուբյուտորները (պաշտոնական ներկայացուցիչները) տարածում են մշակողների կողմից ստեղծված ծրագրերը, վաճառում են, որոշակի գումարի դիմաց (սկավառակներ, որոնցից օգտագործողները տեղադրում են իրենց անհրաժեշտ ծրագրերը): Բավականին հաճախ ծրագրեր ստեղծողները ներկայացնում են զգալի զեղչեր իրենց ծրագրերի համար, տրամադրելով դպրոցներին և այն հաստատություններին, որտեղ մի շարք համակարգիչներ կան: Համաձայն լիցենզավորված պայմանագրի ծրագրերի մշակողները երաշխավորում են դրանց նորմալ աշխատանքը որոշակի օպերացիոն համակարգում և պատասխանատու են դրանց համար:

Որոշ մշակող ընկերություններ առաջարկում են օգտագործողներին պայմանականորեն անվճար ծրագրեր, դրանց գովազդի և շուկայում զարգացման համար: Օգտագործողին տրվում է ծրագրի տարբերակը որոշակի ժամկետով (նշված ժամկետի ավարտից հետո ծրագիրը դադարում է աշխատել, եթե դրա համար գումար չի վճարվում) կամ ծրագրի նույն տարբերակը հնարավորությունների որոշակի սահմանափակումով (վճարման դեպքում օգտագործողին հաղորդվում է կոդ, որը ակտիվացնում է ծրագրի բոլոր ֆունկցիաները):

Ազատ տարածվող ծրագրերի թվին են դասվում այն ծրագրերը, որոնք կարելի է ձեռք բերել համացանցին միանգամայն անվճար:

Ծրագրային ապահովման և համակարգչային տեխնիկայի շատ արտադրողներ հետաքրքրված են ծրագրային ապահովման լայնածավալ և անվճար տարածմամբ: Այսպիսի ծրագրային միջոցների շարքին կարելի է դասել հետևյալները.

- Նոր, կիսատ մշակված (бета) ծրագրերի տարբերակները (դա թույլ է տալիս այդ ծրագրերը լայնածավալ փորձարկել)
- Ծրագրային պրոդուքտները, որոնք հանդիսանում են սկզբունքորեն նոր տեխնոլոգիաների մասնիկ (դա թույլ է տալիս գրավել շուկան)
- Նախկինում թողարկված ծրագրերի հավելումները, որոնք ուղղում են տեղի գտած սխալները կամ ընդլայնում են հնարավորությունները
- Ծրագրերի հնացած տարբերակները
- Նոր սարքավորումների դրայվերները կամ արդեն գոյություն ունեցող դրայվերների կատարելագործված տարբերակները:

Ինֆորմացիայի իրավական հսկում

Ծրագրերի և տվյալների բազայի իրավական հսկում: Իրավական հսկումը ԷՀՄ-ի համար ամբողջ աշխարհում ընդունված և իրագործվող օրենք է, սակայն Հայաստանում այն ամբողջությամբ կամ կարելի է ասել ընդհանրապես չի կիրառվում: Օրենքի կողմից ներկայացված իրավական հսկումը տարածվում է ԷՀՄ-ի համար նախատեսված բոլոր ծրագրերի վրա (այդ թվում օպերացիոն համակարգեր և ծրագրային կոմպլեքսներ), որոնք կարող են արտահայտված լինել տարբեր լեզուներով և տարբեր տեսքով, որը նաև ընդգրկում է ծրագրավորման լեզվով գրված տեքստը և մեքենայական

կողը: Սակայն իրավական հսկումը չի տարածվում մտքերի և սկզբունքների վրա, որոնք գտնվում են ԷՀՄ-ի հիմքում, այդ թվում նաև ինտերֆեյսի և ալգորիթմի հիմքում ընկած մտքերն ու սկզբունքները:

ԷՀՄ-ի համար նախատեսված ծրագրերի հեղինակային իրավունքի և ճանաչման համար չի պահանջվում այն գրանցել ինչ-որ կազմակերպությունում: Հեղինակային իրավունքը ԷՀՄ-ի համար ծրագրեր ստեղծելու ժամանակ առաջանում է ինքնաբերաբար:

Իր իրավունքների մասին հայտարարելու համար ծրագիր ստեղծողը կարող է օգտվել հսկման նշաներից, որոնք բաղկացած են 3 էլեմենտներից.

- C տառից, որը գտնվում է շրջանակի կամ կլոր չակերտների մեջ ©
- Սեփականատիրոջ անունից
- Ծրագրի առաջին տարբերակի երևան գալու տարեթվից

Օրինակ՝ հեղինակային իրավունքի հսկման նշանը բոլորիս հայտնի Word տեքստային խմբագրիչի համար հետևյալն է.

© Корпорация Microsoft, 1993-2015.

Հեղինակին է պատկանում ծրագրի տարածման, վերարտադրության և այլ իրավունքներն ու իհարկե ծրագրում փոփոխություններ կատարելը:

Կազմակերպությունը կամ օգտագործողը ով օրինական տնօրինում է ծրագրի կրկնորինակին, կարող է այն անարգելք ձայնագրել և պահել ԷՀՄ-ի հիշողության մեջ:

Այն կազմակերպությունից կամ օգտագործողից, ով խախտում է հեղինակային իրավունքը ստեղծողը կարող է պահանջել վնասի փոխհատուցում նվազագույն աշխատավարձի 5000-ապատիկի կամ 50.000-պատիկի չափով:

Հարցեր և առաջադրանքներ

1. Որոնք են լիցենզավորված, պայմանականորեն անվճար և ազատ տարածվող ծրագրային միջոցները
2. Հեղինակային իրավունքի հսկման նշանները

15. ՀԱԿԱՎԻՐՈՒՍԱՅԻՆ ԾՐԱԳՐԵՐ

Ցանկացած այլ էլեկտրոնային սարքի նման՝ ամեն պահի համակարգիչը կարող է պատահաբար կամ դիտավորյալ վնասվել: Այդ վնասների մի մասը վերականգնման ենթակա չէ: Համակարգչի սարքաշարը, ծրագրաշարը և պահեստավորված տվյալները կարելի է զերծ պահել վնասներից՝ ձեռնարկելով որոշակի կանխարգելիչ միջոցներ:

Համակարգիչն օգտագործվում է կյանքի գրեթե բոլոր ոլորտներում: Համակարգիչն օգտագործվում է տարբեր նպատակներով, ինչպես օրինակ՝ տվյալներ պահեստավորելու, հաշվարկներ կատարելու, խաղեր խաղալու, երաժշտություն ունկնդրելու, համացանցում որոնումներ կատարելու, ինչպես նաև էլ. փոստի և զրույցի ծրագրերի միջոցով հաղորդակցվելու համար: Այնուամենայնիվ, համակարգիչը և դրանում պահեստավորված տվյալները կարող են վնասվել և ոչնչանալ: Այդ պատճառով անհրաժեշտ է պաշտպանել համակարգիչը վտանգներից, որոնք կարող են արտահայտվել բնական աղետների, մարդու կողմից գործած սխալների կամ վթարի արդյունքում առաջացած ֆիզիկական վնասի, կամ էլ

չարամիտ գործողությունների, ինչպես օրինակ՝ հակերների կողմից չթույլատրված մուտքի կամ վիրուսների հարձակումների ձևով: Համակարգիչը կարելի է պաշտպանել այդ վտանգներից՝ անվտանգության տարբեր միջոցներ ձեռնարկելու, ինչպես օրինակ՝ համակարգիչն անվտանգության համապատասխան կայանքներով և անվտանգության արդիացված ծրագրաշարով ապահովելու միջոցով: Ընտանիքի անդամները նույնպես պետք է տեղյակ լինեն անվտանգության միջոցների մասին՝ համակարգչի պաշտպանվածությունն ավելի լավ ապահովելու համար:

Ցանկացած թույնի դեմ վաղ թե ուշ կարելի է գտնել իր հակաթույնը: Այդպիսի հակաթույները համակարգչային աշխարհում դարձել են այն ծրագրերը որոնք կոչվում են հակավիրուսային ծրագրեր:

Այդ ծրագրերը կարելի է դասակարգել 5 խմբերի:

Ֆիլտրեր, հայտնաբերողներ, վերաքննիչներ, բժիշկներ և հակաթույնիչներ

Հակավիրուսային ֆիլտրերը դրանք այն ծրագրերն են, որոնք օգտվողին տեղեկացնում են այն մասին, երբ որևէ ծրագիր փորձում է ձայնագրվել սկավառակի վրա, նաև այլ կասկածելի գործողությունների մասին (օրինակ CMOS ծրագրի կարգավորումների փոփոխումը): Այդ ամենին զուգահեռ համակարգիչը օգտվողին լրացուցիչ հարցնում է տվյալ գործողության թույլատրման կամ արգելման մասին: Այս ծրագիրը ունիվերսալ է, քանի որ աշխատում է ոչ միայն հայտնի այլ նաև անհայտ վիրուսների դեմ, որը չի կարելի ասել հայտնաբերող հակավիրուսային ծրագրի հետ, որը ի տարբերություն ֆիլտրային հակավիրուսի աշխատում է միայն կոնկրետ վիրուսների դեմ, որոնք հայտնի էին եղել ծրագրավորողին այդ հակավիրուսը գրելու ժամանակ: Այնպիսի հակավիրուսները ինչպիսին է ֆիլտրային հակավիրուսը, շատ օգտակար են ներկա ժամանակներում, երբ ցանցում մեծ տարածում են գտել վիրուս-մուտանտները, որոնք չունեն մշտական կոդ: Բայց ֆիլտր-հակավիրուսները չեն կարող հակազդել այն վիրուսներին, որոնք ազդում են BIOS-ին, նաև BOOT վիրուսները որոնք ակտիվանում են մինչև հակավիրուսային ծրագրի միանալը: Տվյալ հակավիրուսի թերությունների շարքին է դասվում նաև այն, որ ինչ որ գործողություն իրականացնելու ժամանակ այն չափից շատ հարցումներ է անում, որոնց պատասխանելը շատ ժամանակատար է: Որոշ ֆիլտր-հակավիրուսների տեղադրման ժամանակ կարող են կոնֆլիկտներ առաջանալ որոշ բազային ծրագրերի հետ, որոնք ուղղակի կդադարեն աշխատել:

Ավելի մեծ տարածում ունեն հայտնաբերիչ-հակավիրուսները:Այս տեսակի ամենատարածված ներկայացուցիչներ են Kaspersky, Doctor Web, Nod, Avira, Avast հակավիրուսային ծրագրերը: Հայտնաբերիչ-հակավիրուսները նախատեսված են որոշակի վիրուսների համար: Դրանք հիմնված են վիրուսների կոդերի հերթականության համեմատությամբ, ստուգվող ծրագրերի կոդերի հետ:

Շատ հայտնաբերիչ-հակավիրուսներ կարողանում են նաև «բուժել» վարակված ֆայլերը կամ սկավառակները՝ջնջելով դրանցում գտնվող վիրուսները(բնականաբար «բուժվում» են միայն այն վիրուսները, որոնք մինչ այդ հայտնի են եղել հայտնաբերիչ-հակավիրուսին): Այս հակավիրուսային ծրագրերը պետք է մշտապես թարմացնել, քանի որ դրանք շատ շուտ են «հնանում» և չեն կարողանում հայտնաբերել նոր տեսակի վիրուսները:

Վերաքննիչ-հակավիրուսները: Դրանք այն ծրագրերն են, որոնք ստուգում են ֆայլերի և սկավառակի սիստեմային հատվածների տեղեկությունները և համեմատում են այդ նույն ֆայլերի արդեն նախորոք վերցված ինֆորմացիայի հետ: Այդ ամենի հետ մեկտեղ ստուգվում է BOOT-սեկտորը, FAT-ցուցակը նաև ֆայլերի երկարությունը, ստեղծման ժամանակը, ատրիբուտները և այլն: Անալիզի ենթարկելով վերաքննիչ-հակավիրուսի հրահանգները օգտվողը կարող է իմանալ արդյոք վիրուսի պատճառով են տեղի ունեցել փոփոխությունները թե ոչ:

Եվ վերջին խմբին են դասվում ամենաանարդյունավետ հակավիրուսները՝ հակաթույնիչներ: Հակաթույնիչները ներդնում են ֆայլի մեջ որևէ կոնկրետ վիրուս այնպես, որ իրական վիրուսը այն շրջանցում է կարծելով, որ այն արդեն վարակված է:

Հարցեր և առաջադրանքներ

1. Հակավիրուսային ծրագրերը քանի խմբի են դասվում և որո՞նք են դրանք:

16. ՀԱԿԱՎԻՐՈՒՍԱՅԻՆ ԾՐԱԳՐԵՐԻ ԱՇԽԱՏԱՆՔԸ

Հակավիրուսային ծրագրերը՝ ծրագրեր են, որոնց աշխատանքի հիմնական սկզբունքը կայանում է վիրուսներից կամ ավելի ճիշտ վտանգավոր ծրագրերից պահպանումը: Ցանկացած հակավիրուսային ծրագիր միավորում է գրեթե բոլոր հակավիրուսային տեխնոլոգիաները և վիրուսների դեմ պայքարի մեթոդները:

Հակավիրուսային պաշտպանման բոլոր մեթոդներից կարելի է տարանջատել երկու հիմնական խմբեր.

- Սիգնատյուրային (ստորագրային) մեթոդներ: Վիրուսների գտնման կոնկրետ մեթոդներ, հիմնված ֆայլի և վիրուսների հայտնի տարբերակների հետ համեմատության միջև:
- Էվրիստիկ մեթոդներ: Գտնման համեմատաբար ճիշտ մեթոդներ, որոնք թույլ են տալիս գրեթե 100 տոկոս ճշտությամբ ենթադրել, որ ֆայլը վարակված է:

Սիգնատյուրային անալիզ

Սիգնատյուրային (signature անգլերենից թարգմանաբար նշանակում է ստորագրություն) կամ էլ փոխաբերական իմաստով «բնութագրող գիծ, ինչ-որ մի բան որոշող»:

Սիգնատյուրային անալիզի աշխատանքը՝ գտնել յուրաքանչյուր վիրուսի բնութագրիչ գծերը, գտնել վիրուսը և համեմատել այդ բնութագրիչ գծերի հետ:

Վիրուսի սիգնատյուրը՝ փաթեթի առանձնահատկությունն է, որը թույլ է տալի միանշանակ ասել, որ ֆայլի մեջ վիրուս կա (ներառելով այն դեպքը, երբ ֆայլը ամբողջովին վիրուս է):

Հակավիրուսային բազա: Հակավիրուսային հայտնի ծրագրերի միախումբ: Սիգնատյուրների առանձնացման խնդիրը լուծում են համակարգչային վիրուսալոգիայի բնագավառի էքսպերտները, որոնք իվիճակի են վիրուսի կոդը դուրսբերել ծրագրի կոդից և բերել նրա բնութագրիչ գծերը մի տեսքի, որը հարմար է որոնման համար: Լավագույն հակավիրուսը կհամարվի այն հակավիրուսը, որի համար նոր վիրուսի սիգնատյուրան ավելի շուտ կարտադրվի:

Շատ հաճախ նմանատիպ վիրուսների ընտանիք գտնելու համար օգտագործվում է մեկ սիգնատյուրա և այդուհանդերձ համարել, որ սիգնատյուրների քանակը հավասար է գտնված վիրուսների քանակին սխալ կլինի: Սիգնատյուրների կարևորագույն հավելումն է՝ վիրուսի տեսակի ճշգրիտ և կոնկրետ որոշում: Այս միջոցը թույլ է տալիս մուտքագրել բազա ինչպես սիգնատյուրներ, այնպես էլ վիրուսի բուժման միջոներ: Եթե սիգնատյուրային անալիզը չպատասխաներ թե ինչ վիրուս է այն, բնականաբար բուժումը անհնարին կլիներ՝ շատ մեծ կլիներ ռիսկը, բուժման փոխարեն համակարգչից ջնջել անհրաժեշտ ինֆորմացիան:

Ժխտիչ հատկություններ: Սիգնատյուրաներ ստանալու համար անհրաժեշտ է ունենալ վիրուսի օրինակ: Հետևաբար սիգնատյուրային մեթոդը անպիտան է նոր վիրուսներից պաշտպանվելու համար, քանի որ մինչ վիրուսը չի հասել էքսպերտներին անալիզի համար, ստեղծել նրա սիգնատյուրան անհնար է: Վիրուսի, ինտերներտ ցանցում հայտնվելու և առանձին սիգնատյուրների ստեղծումից հետո սովորաբար անցնում է մի քանի ժամ և այս մի քանի ժամվա ընթացքում վիրուսը իվիճակի է վարակել ցանցում գտնվող բոլոր համակարգիչներին, որովհետև նոր վիրուսներից պաշտպանվելու համար օգնում են պաշտպանման հավելյալ միջոցները, որոնք դիտարկեցինք քիչ առաջ: Նաև էվրիստիկ մեթոդները, որոնք օգտագործվում են հակավիրուսային ծարգրերում:

Էվրիստիկ անալիզ

Վիրուսների որոնում, որոնք նման են հայտնի վիրուսներին:

Էվրիստիկա կոչվում է «գտնել»: Էվրիստիկ անալիզը հիմնված է (նման է իրականությանը) ենթադրությունների վրա, ըստ որոնց նոր վիրուսները նման են լինում արդեն ծանոթ վիրուսներին: Այդ իսկ պատճառով հակավիրուսային բազաներում լինում են մի քանի վիրուսների հայտնաբերման համար նախատեսված սիգնատյուրաներ: Հետևաբար էվրիստիկ մեթոդը հիմնված է այն ֆայլերի որոնման վրա, որոնք ոչ ամբողջական, սակայն մասամբ նմանվում են հայտնի վիրուսների սիգնատյուրաներին:

Առավելությունը. Հնարավորություն, գտնել նոր վիրուսները մինչև այն պահը, երբ նրանց համար կստեղծվեն սիգնատյուրաներ:

Թերությունը.

- Հավանականություն, երբ հակավիրուսը կարող է սխալմամբ գտնել վիրուս ֆայլում, մինչդեռ իրականում ֆայլը ամբողջապես մաքուր է: Այսպիսի դեպքերը կոչվում են կեղծ ահազանգեր
- Բուժելու հնարավորություն չունենալը, այն դեպքում, երբ հակավիրուսային համակարգը կեղծ ահազանգում է և վիրուսի տեսակի սխալ ախտորոշման պարագայում, բուժման փորձը կարող է հանգեցնել ինֆորմացիայի կորստի, իսկ դա անթույլատրելի է
- Ցածր էֆեկտիվություն: Դեպի իսկապես նորարարական վիրուսների դեմ պայքարը, որոնք առաջացնում են ավելի մեծ մասշտաբի վնասներ, այս տիպի էվրիստիկ անալիզը իսկապես քիչ պիտանի է

Տարօրինակ գործողություններ կատարող վիրուսների որոնում

Մյուս մեթոդը, որը հիմնված է էվրիստիկայի հիման վրա: Ենթադրվում է, որ վնաս հասցնող ծրագրերը այս կամ այլ կերպ ձգտում են վնաս հասցնել համակարգչին և հիմնված են հիմնական վնասակար գործողությունների հիման վրա: Օրինակ՝

- Ֆայլի ջնջում
- Ֆայլի մեջ ձայնագրում
- Համակարգային ռեեստերի (գրանցման) շրջանում ձայնագրում
- Լսման համար նախատեսված պորտի բացում
- Ստեղնաշարից մուտքագրված տվյալների որսում
- Նամակների ուղարկում

Այս տիպի յուրաքանչյուր գործողության առանձին կատարումը պատճառ չէ, որպեսզի ծրագիրը համարենք վնասակար: Սակայն այսպիսի գործողություններից մի քանիսի կատարումը՝ գրանցում է ինքը իրեն համակարգային ռեեստերի ավտոմիացման մեջ, գրավում է ստեղնաշարից մուտքագրված տվյալները և ուղարկում ինտերնետի ինչ-որ հասցեի, ուրեմն այս ծրագիրը, նվազագույնը կասկածելի է: Հիմնվելով այս սկզբունիք հիման վրա էվրիստիկ անալիզատորը միշտ հետևում է այն գործողություններին, որոնք կատարում են ծրագրերը:

Առավելությունները: Հնարավորություն, հայտնաբերել նախկինում անծանոթ վնասակար ծրագրերը, անգամ եթե դրանք այնքան էլ նման չեն ճանաչվածներին (համակարգիչ ներգործելու համար նոր թույլ հատվածներ, իսկ դրանից հետո կատարել արդեն իր համար ծանոթ վնասակար գործողություններ): Այսպիսի ծրագիրը կարող է բաց թողել առաջնային անալիզատորը, սակայն երկրորդայինը կարող է հայտնաբերել:

Թերությունները.

- Կեղծ միացումներ
- Բուժման անհնարինություն
- Ցածր էֆեկտիվություն

Հավելյալ միջոցներ

Հակավիրուսի հաջող աշխատանքի համար, որպեսզի հակավիրուսային միջոցները էֆեկտիվ լինեն, անհրաժեշտ են հավելյալ մոդուլներ, որոնք կատարում են օժանդակ գործառույթներ:

Ծրագրավորման մոդուլներ

Յուրաքանչյուր գործողության համար ընտրվում է ժամանակացույց, որը ամենաշատն է հարմար այդ տիպին: Գոյություն ունեն մի շարք գործողություններ, որոնք հակավիրուսը պետք է սիստեմատիկ կատարի՝ ստուգի ամբողջ համակարգիչը և թարմացնի հակավիրուսային բազան: Թարմացման մոդուլն էլ կատարում է այդ գործողությունը:

Կառավարման մոդուլ

- Կառավարման և կարգավորումների մոդուլ: Սա ինտերֆեյսային (ծրագրերի համակարգ) մոդուլ է, որի օգնությամբ կարելի է հարմար տեսքով մուտքի թույլտվություն ստանալ դեպի համեմատաբար կարևորագույն ֆունկցիաներ
- Հակավիրուսների մոդուլների կարգավորումների պարամետրորով
- Թարմացումների կարգավորումներով
- Թարմացումների սիստեմատիկ սկսման (запуск) և ստուգման կարգավորումներով
- Օգտագործողի հրամանով մոդուլների սկսումով
- Ստուգման պատասխաններով
- Դեպի այլ ֆունկցիաներ, կախված տվյալ հակավիրուսից

Այս տեսակի մոդուլից հիմանակ պահանջները

Հարման հասանելիություն դեպի կարգավորումներ, ինտուիտիվ հասկանալիություն, մանրամասն տեղեկատվական համակարգ, յուրաքանչյուր կարգավորման նկարագրություն, կարգավորումներ փոփոխելու արգելք, եթե համակարգչից օգտվում են մի քանի օգտագործողներ:

Այն հակավիրուսները, որոնք նախատեսված մեծ ցանցերի պաշտպանման համար, օժտված են հատուկ վարման մոդուլով: Այս տիպի վարման մոդուլի հիմնական հատկությունները.

- Հեռահար կարգավորման և վարման հնարավորություն: Անվտանգության անդմինիստրատորը կարող է առանց տեղից վերկենալու միացնել, անջատել կամ փոփոխել ցանցում միացված այլ համակարգիչների հակավիրուսային համակարգը
- Կարգավորումներ փոխելու արգելք: Վարման մոդուլը չի թույլատրում լոկալ օգտագործողին փոփոխել հակավիրուսի կարգավորումները կամ կանգնեցնել նրա աշխատանքը:

Կարանտին

Շատ հակավիոռսներ ունեն հատուկ տեխնոլոգիաներ, որոնք թույլ չեն տալիս կորցնել ինֆորմացիան հակավիրուսային համակարգի աշխատանքից հետո:

Ասենք թե ֆայլը հայտնաբերվել է էվրիստիկ անալիզի աշխատանքի շնորհիվ և ջնջվում է հակավիրուսային միջոցի կարգավորումների համաձայն: Սակայն էվրիստիկ անալիզատորը 100 տոկոսով չի հաստատում, որ տվյալ ֆայլը վարակված է, այսինքն կարող է լինել այնպես, որ հակավիրուսը կջնջի չվարակվա ֆայլը:

Այդ իսկ պատճառով մինչ ֆայլի ջնջումը կամ բուժումը, ավելի լավ կլինի պահպանել այդ ֆայլերի ռեզերվային տարբերակը: Այդ ժամանակ սխալ ջնջման դեպքում կարևոր ինֆորմացիայի կորուստ չի գրանցվի:

Հարցեր և առաջադրանքներ

1. Հակավիրուսային ծրագրերի պաշտպանման հիմնական մեթոդները և դրանց աշխատանքի սկզբունքը:

17. ՀԱԿԱՎԻՐՈՒՍԱՅԻՆ ԾՐԱԳՐԵՐԻ ՏԵՂԱԴՐՈՒՄԸ, ԹԱՐՄԱՑՈՒՄԸ, ՋՆՆՈՒՄԸ

Տարեցտարի համակարգչային վիրուսների թիվը երկրաչափական պրոգրեսիայով աճում է: Վերջին ժամանակաշրջանում այս սև արդյունաբերությունում նկատվում է մեծ չափերի ակտիվություն, կապված նրա հետ, որ համակարգիչների «կոտրումից» կարողացել են ստեղծել կոմերցիոն օգուտ: Եթե նախկինում վիրուսները կարողանում էին միայն «կախել» համակարգիչը, բացել CD-ROM-ը և կատարել ևս մի շարք այլ չարաճճիություններ, ապա այժմ միջոցներն ու մեթոդները դարձել են ավելի հարուստ կենսափորձ ունեցող, իսկ հարձակման օբյեկտները ավելի թանկարժեք: Ժամանակակից վիրուսների և Տրոյան ծրագրերի թիրախը արդեն ոչ թե չարաճճիությունն է, այլ անձնական ինֆորմացիայի գողանումը (այդ թվում էլեկտրոնային փոխերի), անցանկալի գովազդի ցուցադրումը, վարակված համակարգչի օգտագործումը որպես հարթակ DoS հարձակումների և այլնի համար: Եթե նախկինում վիրուսների տարածումը կատարվում էր հեղինակի խանդավառությունից ելնելով, ապա հիմա արդեն այդ խանդավառությունը հավասար է վիրուսների տարածումից ստացված հասույթին: Այս պարագայում արդեն համակարգչի օգտագործումը առանց հակավիրուսային պաշտպանման, նվազագույնը կդիտվի որպես չմտածված քայլ:

Հակավիրուսային ծրագիր տեղադրելը այնքան էլ դժվար չէ, դրանց թարմ տարբերակները կարելի է ներբեռնել հակավիրուսի պաշտոնական կայքից: Հակավիրուսի տեղադրումից հետո, որպես կանոն այն կարելի է օգտագործել որոշ ժամանակ անվճար, որի ավարտից հետո օգտագործողին կառաջարկվի գնել այդ ծրագիրը: Եթե հակավիրուսի համար օգտագործողը մտադրություն չունի գումար ծախսել, ապա կարելի է ձեռքբերել դրանց փորձնական կամ որոշ ֆունկցիաների սահմանափակումով տարբերակները:

Հակավիրուսի տեղադրման ընթացակարգը գրեթե ոչնչով չի տարբերվում այլ ծրագրերի տեղադրումից: Կա միայն երկու տարբերություն: Առաջինը՝ հակավիրուսի տեղադրումից հետո օգտագործողին կառաջարկվի վերամիացնել համակարգիչը, կատարել հակավիրուսի վերջնական կարգավորումներ և ամբողջական զննում (scan) և երկրորդը՝ հակավիրուսը չի կարելի տեղադրել մեկ այլ հակավիրուսի հետ զուգահեռ, այս քայլը ոչ թե ավելի կպաշտպանի համակարգիչը վիրուսներից, այլ կառաջացնի բազում ծրագրային կոնֆլիկտներ, հակավիրուսների ոչ նորմալ աշխատանք և ընդհանուր համակարգչի աշխատանքի խափանում: Այդ իսկ պատճառով մինչ նոր հակավիրուսի տեղադրելը, խորհուրդ է տրվում ջնջել բոլոր հին տարբերակները: Բացառություն է կազմում միայն հակավիրուսի թարմացումը, երբ օրինակ՝ Avast 2015-ը օգտագործողը ցանկանում է փոխարինել Avast 2016-ով: Այս պարագայում արդեն հակավիրուսը ինքնուրույն կատարում է փոփոխությունը:

Ընդհանուր առմամբ հակավիրուսի տեղադրման պրոցեսը բավականին պարզ է անգամ սկսնակ օգտագործողի համար, ավելի մեծ խնդիր է դրա ճիշտ տարբերակի ընտրությունը: Նաև անհրաժեշտ է իմանալ, որ հակավիրուսի տեղադրումով չի սահմանափակվում համակարգչի վիրուսներից ապահովագրումը: Ժամանակ առ ժամանակ անհրաժեշտ է կատարել համակարգի ամբողջական զննում, հետևել թարմացումների տեղադրմանը ժամանակին և ուշադիր կարդալ այն հաղորդագրությունները, որոնք գրում է հակավիրուսը:

Հարցեր և առաջադրանքներ

1. Ի՞նչ պետք է անել, եթե համակարգչում այս կամ այլ կերպ զգում եք վիրուսների առկայությունը:

Ցանկացած հակավիրուս պետք է պարունակի թարմացման մոդուլ, որպեսզի սիգնատյուրային (սիգնատյուրային անալիզը դա հակավիրուսային համակարգի աշխատանքի տեսակ է, որի մասին ավելի մանրամասն արդեն անցել ենք նախորդ թեմաներում) անալիզը էֆեկտիվ կարողանա պայքարել ամենավերջին վիրուսների դեմ: Հակավիրուսային էքսպերտները միշտ ստուգում և փորձարկում են նոր վիրուսները և թողարկում են դրանց դեմ սիգնատյուրները: Նոր սիգնատյուրների ստեղծումից հետո դրանք տեղադրվում են հակավիրուսների սերվերներում և հասանելի են դառնում բեռնման համար: Թարմացման մոդուլը դիմելով սերվերին և նոր թարմացումները գտնելով, ներբեռնում է դրանք համակարգիչ, հրամայելով հակավիրուսային մոդուլներին օգտագործել սիգնատյուրաների նոր ֆայլերը: Որոշ հակավիրուսային ընկերություններ հակավիրուսային թարմացումների համար ստեղծում են հատուկ արձանագրություններ:

Թարմացման մոդուլները տարբերվում են կարգավորումներով, այն դեպքերի համար, երբ թարմացման աղբյուրները անհասանելի են (սերվերների մի քանի հասցեները): Նաև կարող են կարգավորումներ լինել այնպես, որ թարմացման հայտերը ուղղարկվեն այնքան ժամանակ, մինչ սերվերը հասանելի կլինի: Այս երկու կարգավորումները կարող նաև լինել միաժամանակ:

Հարցեր և առաջադրանքներ

1. Հակավիրուսի թարմացման մոդուլը

Հակավիրուսային ծրագրերով զննում

Համակարգիչների հակավիրուսային պրոֆիլակտիկան և բուժումը ենթադրում է հետևյալ գործողությունները՝

- ծրագրերի գրանցումը իրականացնել միայն ներկայացուցիչներից
- ծրագրերի և մագնիսական սկավառակների փոխանակման սահմանափակում
- օպերատիվ հիշողության և մագնիսական սկավառակների պարբերական ստուգում հակավիրուսային ծրագրերի օգնությամբ
- հատուկ պաշտպանող ծրագրերի օգտագործում, որոնք համակարգիչը միացնելուց հետո, որպես ռեզիդենտ ծրագիր բեռնվում են օպերատիվ հիշողություն:

Գոյություն ունեն հազարավոր վիրուսներ և հարյուրավոր հակավիրուսային ծրագրեր, որոնցից առավել հայտնի են՝ Avast, Avira, Kaspersky, Dr.Web և այլն: Microsoft ընկերությունը MS-DOS-ի 6.0 տարբերակի մեջ ներգրավեր էլ Microsoft Antivirus ծրագիրը: Այդ ծրագիրը ներկայացված է երկու տարբերակներով՝ MS-DOS-ի և Windows-ի համար:

AVAST հակավիրուսային ծրագրի նախնական՝ ազատ, անվճար տարբերակը աշխատում է համակարգչում, ցուցաբերելով գերազանց արդյունքներ վիրուսների որոնման մեջ: AVAST-ն ունի վիրուսների փնտրման մի քանի տարբերակներ՝

- Համակարգչի արագ ստուգում
- Համակարգչի ամբողջական ստուգում
- Համակարգչին միացված բոլոր հիշող սարքերի ստուգում
- Առանձին ֆայլերի ստուգում

Այս հակավիրուսային ստուգումները ավարտելուց հետո հակավիրուսային ծրագիրը առաջարկում է անջատել և միացնել համակարգիչը և կրկին անգամ ստուգել համակարգչային բլոկը և բոլոր հիշող

սարքը, որոնք միացված են համակարգչին: Ջննումից հետո առաջացած բոլոր վարակված ֆայլերը հակավիրուսային ծրագիրը առանձնացնում է և առաջարկում դրանք կամ ջնջել, կամ տեղափոխել պահոց, կամ անտեսել, կամ էլ բուժել: Տարբերակներից մեկը ընտրելուց հետո այնդ վիրուսը տեղափոխվում է համապատասխան միջավայր: Եթե գտնված վիրուսների մեջ հայտնվում են ծրագրային ֆայլեր, հակավիրուսային համակարգը զգուշացնում է դրանց վարակվաց լինելու մասին և թե ինչ է նպատակահարմար դրանց հետ անել:

Հակավիրուսային ծրագրերը, մեր տարբերակում AVAST-ը, նաև աշխատում են համացանցային տիրույթում, ստուգելով URL հասցեները՝ վարակված են թե ոչ:

Գրեթե նույն սկզբունքով են աշխատում բոլոր հակավիրուսային ծրագրերը:

18. ՖԱՅԼԵՐԸ ԵՎ ՖԱՅԼԵՐԻ ՊԱՇՏՊԱՆՈՒՄԸ ԾԱԾԿԱԳՐՈՎ

Համակարգչի արտաքին հիշող սարքերի վրա պահպանվող ցանկացած ծրագիր կամ տվյալների հավաքածու ֆայլ է կազմավորում, որն ունենում է անվանում և ծավալ:

Արտաքին հիշող սարքի վրա որոշակի անվանումով պահպանված ինֆորմացիան անվանում են ֆայլ:

Ֆայլերի անվանումները կազմվում են երկու մասից, որոնք իրարից բաժանվում են կետով հետևյալ կերպ՝

անուն.ընդլայնում

օրինակ՝ Tetris.exe:

Ֆայլի անունը որոշակի քանակությամբ պայմանանշանների հաջորդականություն է, իսկ ընդլայնումը սովորաբար բնորոշում է, թե տվյալ ֆայլը, որ կիրառական ծրագրի աշխատանքի արդյունքում է ստեղծվել: Ֆայլի ընդլայնումը կարող է բաղկացած լինել մինչև երեք պայմանանշաններից:

Ֆայլը թողարկել նշանակում է այն բերել օպերատիվ հիշողություն և աշխատեցնել: Դրա համար անհրաժեշտ է մկնիկի ցուցիչը դնել ֆայլի անվանման կամ տարբերանշանի վրա ու ձախ սեղմակի կրկնակի սեղմում իրականացնել:

Երբ միևնույն նպատակին ուղղված տարբեր ֆայլեր են ստեղծվում, իմաստ է ունենում դրանք որևէ ձևով համախմբելու: Ենթադրենք, որոշել եք մաթեմատիկայի և հայ գրականության դասերը համառոտագրել և պահպանել համակարգչում: Բնական է, որ արժե ֆայլերի երկու խումբ ստեղծել, ոոնցից մեկը կհամախմբի մաթեմատիկայի, մյուսը՝ գրականության դասերի վերնագրերը: Ահա այդ խմբերն էլ, որոնք պարունակում են այս կամ այն նպատակին ուղղված ֆայլեի անվանումները, կոչվում են թղթապանակներ (Folder):

Ֆայլը ինֆորմացիայի էլեմենտների համախումբ է, որն ունի անուն և պահվում է ինֆորմացիայի կրիչի վրա – մագնիսական սկավառակի, ժապավենի կամ ցանկացած այլ հիշող սարքի մեջ: Ֆայլի կոշտ պատճենը կարելի է դուրս բերել թղթի վրա:

Ֆայլերը բաժանվում են երկու մասի – տեքստային և երկուական: Տեքստային ֆայլերը նախատեսված են մարդու կողմից կարդալու համար, իսկ տեքստային չհամարակալվող ֆայլերը՝ երկուական ֆայլերի անունները կարող են գրվել մեծատառերով, փեքրատառերով և խառը:

Սկավառակի վրա գտնվող յուրաքանչյուր ֆայլ ունի նշանակութուն, որը բաղկացած է երկու մասից՝ անունից և ընդլայնումից: Ֆայլի անունը կարող է պարունակել 1-ից մինչև 255 սիմվոլ (այսինքն 1բայթ): Ընդլայնումը անունից բաժանվում է կետով և բաղկացած է մինչև 4 սիմվոլներից: Օրինակ՝

COMAND.COM

AUTOEXEC.BAT

MAN.ZIP

MAN.DOC

Անունը և ընդլայնումը կարող են բաղկացած լինել մեծատառերից և փոքրատառերից, թվերից և հետևյալ սիմվոլներից՝

~ @ # $ % ( ) _ ` { } ''

Հետևյալ սիմվոլները չեն կարող կիրառվել ֆայլերի անունների մեջ: Օրինակ՝

\ / * « » < > |

Ֆայլի ընդլայնումը, որպես օրենք, նկարագրում է ֆայլի պարունակությունը: Ֆայլերի ընդլայնումների օրինակներ են.

exe, com – Execute բառից, որը նշանակում է կատարող կամ իրականացման պատրաստ ծրագիր,

bat – Batch բառից, որը նշանակում է փաթեթային կամ անվանում են հրամանային կամ ծրագրային ֆայլ,

doc, txt – տեքստային ֆայլեր,

chi – ChiWriter տեքստային խմբագրիչի փաստաթղթեր,

pas – պասկալ ալգորիթմական լեզվով ծրագրեր,

bas – Բեյսիկ ալգորիթմական լեզվով ծրագրեր,

for – Ֆորտրան ալգորիթմական լեզվով ծրագրեր

asm – ասեմբլեր ալգորիթմական լեզվով ծրագրեր

bak – ֆայլի պատճեն, որը ստեղծվում է ֆայլում փոփոխություններ կատարելուց հետո: Նշենք, որ այս ֆայլերը թույլ են տալիս անհրաժեշտության դեպքում վերականգնել տեքստային ֆայլը: Ֆայլի հետ աշխատանքից հետո, երբ կիրառողը կատարել է բոլոր փոփոխությունները, այն կարող է հեռացվել:

Ֆայլի անվան և ընդլայնումի մեջ մեծատառերը և փոքրատառերը համարժեք են, քանի որ օպերացիոն համակարգը փոքրատառերը ձևափոխում է մեծատառերի:

Սարքերի անունները չեն կարող օգտագործվել որպես ֆայլի անուն: Այդ անուններն են՝

PRN – տպիչ,

LPT1-LPT3 – 1-3 զուգահեռ միացման հանգույցներին միացված սարքեր (սովորաբար դրանք տպիչներ են),

AUX – ասինխրոն հաջորդական միացման հանգույցին միացված լրացուցիչ սարք,

COM1-COM3 – 1-3 ասինխրոն հաջորդական միացման հանգույցներին միացված սարքեր (մկնիկ, ստեղնաշար և այլն),

NUL - «դատարկ» սարք. Մուտքի-ելքի բոլոր գործողությունները այս սարքի համար անտեսվում են:

Եթե նույնիսկ վերը նշված անուններին ավելացվեն ընդլայնումներ, օպերացիոն համակարգը դրանք նույնպես կընդունի որպես սարքի անուն: Սակայն նշված անունները որպես ֆայլերի ընդլայնում կարելի է օգտագործել:

Հարցեր և առաջադրանքներ.

1. Համակարգչից օգտվելով գրել Microsoft Office Word, Microsoft Office Excel, Adobe Photoshop, Corel DRAW, Microsoft Office Access կիրառական ծրագրերի ընդլայնումները:

   _____

   _____

2. Ո՞ր անունները չեն թույլատրվում օգտագործել որպես ֆայլերի անուններ:
3. Սկավառակի վրա գտնվող յուրաքանչյուր ֆայլ քանի մասից է բաղկացած :
4. Արտաքին հիշող սարքի վրա որոշակի անվանումով պահպանված ինֆորմացիան անվանում են.

a) ընդլայնում,
b) ֆայլ,
c) տեքստային ֆայլ

Ֆայլերի պաշտպանումը ծածկագրով

Կարևոր փաստաթղթերը, ինչպես օրինակ՝ հարկերի վերաբերյալ փաստաթղթերը, պահեստավորվում են անվտանգ կերպով, որպեսզի դրանք չվնասվեն կամ չկորչեն: Անհրաժեշտ է նաև ապահովել, որպեսզի ոչ ոք չկարողանա օգտագործել այդ փաստաթղթերը առանց թույլտվության:

Համակարգչից պարբերաբար օգտվելու դեպքում դրանում պահեստավորվում են մեծ ծավալով տեղեկություններ: Այս տեղեկությունները կարող են ներառել հարկերի մասին մանրամասներ, անձնական նամակներ կամ ծառայողական նամակագրություն: Պետք է ապահովել, որ ոչ ոք առանց թույլտվության չկարողանա տեսնել այդ տեղեկությունները: Անհրաժեշտ է նաև ապահովել, որ այդ տեղեկությունները չվնասվեն:

Պատկերացրեք, թե համակարգչում գաղտնի նախագծի վերաբերյալ հաշվետվություն եք պահել: Այդ հաշվետվությունը պատրաստելու համար աշխատել եք մի քանի շաբաթ և այժմ պետք է այն ներկայացնեք ձեր ղեկավարին: Համակարգչում կա այդ հաշվետվության ընդամենը մեկ օրինակ և կարևոր է, որ այն չվնասվի կամ չջնջվի: Սակայն ձեր բացակայության ժամանակ մեկ այլ աշխատող օգտվել է այդ համակարգչից և ջնջել է նախագծի վերաբերյալ այդ հաշվետվությունը: Նման իրավիճակներից խուսափելու համար կարելի է միջոցներ ձեռնարկել համակարգչում պահվող տվյալները պաշտպանելու համար:

Օգտվողի նույնացման կատարում

Աշխատանքային միջավայրը և տվյալները վնասելու ռիսկը նվազեցնելու արդյունավետ եղանակ է թույլտվություն չունեցող անձանց կողմից համակարգիչ մուտք գործելու կանխումը:

Այն ապահովելու եղանակներից մեկը համակարգչից օգտվելու թույլտվություն ունեցողների համար առանձին հաշիվներ ստեղծելն է, ինչի արդյունքում յուրաքանչյուր օգտվող ստանում է համակարգիչ մուտք գործելու համապատասխան մակարդակ:

Օրինակ՝ Microsoft® Windows® XP Service Pack 2–ը հնարավորություն է տալիս օգտվողի հաշիվներ ստեղծել ընտանիքի բոլոր անդամների կամ այլ օգտվողների համար:

Հիմնական օգտվողն իր համար կարող է նախատեսել համակարգչից օգտվելու ավելի լայն արտոնություններ, իսկ, օրինակ, երեխայի հաշվի դեպքում կարող են կիրառվել որոշ սահմանափակումներ:

Օգտվողի անվան և գաղտնաբառի ստեղծում

Գաղտնաբառն օգտագործվում է որպես համակարգիչ մուտք գործելու բանալի: Գաղտնաբառն իմացող ցանկացած ոք կարող է մուտք գործել համակարգիչ և վնասել տվյալները:

Գաղտնաբառն անհրաժեշտ է գաղտնի պահել: Գաղտնաբառը մուտքագրելիս անհրաժեշտ է ուշադիր լինել, որպեսզի ոչ ոք այն չտեսնի: Գաղտնաբառը պետք չէ հայտնել ուրիշներին:

Պետք չէ գրել գաղտնաբառը և թողնել այն համակարգչի վրա կամ գրասեղանին: Եթե կա որևէ կասկած, որ գաղտնաբառը բացահայտվել է, այն անհրաժեշտ է անհապաղ փոխել, քանի դեռ ոչ ոք այն սխալ չի օգտագործել:

Երբ համակարգիչը միացված է և չի գտնվում հսկողության տակ, համակարգչի ծրագրաշարին կամ դրանում պահվող տվյալներին կարող է վնաս հասցվել: Նման դեպքերը կանխելու համար համակարգչից որոշ ժամանակով հեռանալուց առաջ անհրաժեշտ է ժամանակավորապես կողպել այն:

Համակարգիչը կողպելը

Երբ համակարգիչը կողպվում է, այն անմիջապես թաքցնում է էկրանին ցուցադրվող բովանդակությունը և թույլ չի տալիս որևէ գործողություն կատարել, քանի դեռ այն չի ապակողպվել՝ օգտվողի ճիշտ անվան և գաղտնաբառի համակցությունը մուտքագրելու միջոցով:

Համակարգիչը կողպելու համար անհրաժեշտ կոնկրետ քայլերը կախված են օգտագործվող գործավար համակարգից: Օրինակ՝ Windows XP Service Pack 2–ն օգտագործելիս համակարգիչը կարելի է կողպել՝ միաժամանակ սեղմելով CTRL+ALT+DEL ստեղները, այնուհետև կտտացնելով Windows Security պատուհանի Lock Computer կոճակին:

Անհրաժեշտ է նկատի ունենալ, որ ոչ բոլոր գործավար համակարգերն են հնարավորություն տալիս կողպել համակարգիչը:

Համակարգիչների և Համացանցի տարածման հետ մեկտեղ ի հայտ են գալիս բազմաթիվ եղանակներ, որոնց միջոցով կարող է վտանգվել համակարգչում պահվող անհատական տվյալների պաշտպանությունը: Համակարգչից օգտվողը և նրա ընտանիքի անդամները պետք է կանխեն անհատական տվյալների պաշտպանությանը սպառնացող այդ վտանգները: Կարելի է ձեռնարկել հետևյալ պարզ միջոցները՝ օգտվողի և նրա ընտանիքի անդամների անհատական տվյալներ ներխուժումից պաշտպանելու համար:

Ինքնությունը պաշտպանելը

Անհրաժեշտ է խուսափել անծանոթներին անձնական տեղեկություններ տրամադրելուց: Դա անհատական տվյալների պաշտպանության «ոսկե կանոնն» է: Էլ. փոստով հաղորդագրություններ փոխանակելիս կամ ճեպուղերձիչով զրուցելիս պետք է համոզված լինել, որ չեն բացահայտվում օգտվողի կամ նրան ծանոթ անձանց անհատական տվյալների մանրամասները: Բացի այդ, համակարգիչ և էլ. փոստի միացումներ մուտք գործելու համար անհրաժեշտ է օգտագործել հզոր գաղտնաբառեր:

Համակարգչում առկա տեղեկությունները և կարևոր տվյալները պարբերաբար պահուստավորելը

Խորհուրդ է տրվում պահուստավորել համակարգչում պահվող բոլոր տեսակի կարևոր և գաղտնի տեղեկությունները: Կարևոր տեղեկությունները կարող են ներառել փաստաթղթեր, տվյալների շտեմարաններ կամ կոնտակտային տվյալներ: Տվյալների պահուստավորման համար կարելի է օգտագործել տարբեր տեսակի պահուստավորման կրիչներ, օրինակ՝ սեղմասկավառակներ կամ այլ կոշտ սկավառակներ: Եթե համակարգչում պահվող տվյալները պարբերաբար պահուստավորվեն, ապա բնօրինակ տվյալները վնասվելու կամ ջնջվելու դեպքում կարելի է վերականգնել դրանք: Նաև խորհուրդ է տրվում պահուստավորված տվյալները պահեստավորել անվտանգ վայրում և սահմանափակել մուտքը այդ տվյալներ՝ օգտագործելով գաղտնաբառեր և գաղտնագրում:

Համակարգի ընթացիկ անվտանգությունը պարբերաբար ստուգելը

Անհրաժեշտ է պարբերաբար ստուգել համակարգչի ընթացիկ անվտանգության մակարդակը: Ժամանակակից գործավար համակարգերում կան ներկառուցված հատկություններ, որոնք օգնում են հետևել համակարգչի՝ անվտանգությանն ու անհատական տվյալների պաշտպանությանը սպառնացող տարբեր վտանգներից պաշտպանվելու կարողությանը: Օրինակ՝ Windows–ի անվտանգության կենտրոնը Windows XP Service Pack 2-ի բաղադրիչ է, որն օգնում է պահպանել հրապատի կայանքները, ստեղծել ծրագրաշարի արդիացման հերթացուցակներ և ստուգել համակարգչում տեղադրված հակավիրուսային ծրագրաշարի վավերությունը:

Վիրուսների դեմ ստուգումն ու ամեն օր աշխատեցնելը

Ամեն օր Համացանց մուտք գործելիս համակարգիչը կարող է վարակվել վիրուսներով: Այդ պատճառով կարևոր է, որ համակարգչում վիրուսների դեմ ստուգումն աշխատեցվի ամեն օր:

Անհրաժեշտ է նաև, որ համակարգչում տեղադրված հակավիրուսային ծրագրաշարը միշտ արդիացվի՝ համակարգիչը նոր վիրուսներից պաշտպանելու համար:
Հարցեր և առաջադրանքներ.

1. Օգտվողի նույնացման կատարում
2. Համակարգիչը կողպելը

19. ԳԱՂՏՆԱԳՐՈՒԹՅԱՆ ՀԻՄՆԱԿԱՆ ՀԱՍԿԱՑՈՒԹՅՈՒՆՆԵՐԸ

Գաղտնագրության հիմնական հասկացություններն հասկանալու համար, նախ պետք հասկանանք.

- Ինչո՞ւմ է կայանում գաղտնագրության համակարգի գաղափարը
- Կարո՞ղ է արդյոք գաղտնագրումը պաշտպանել ներթափանցումներից:

Տեղեկատվության գաղտնագրման փաստը չի պաշտպանում անիրավասու անձանց ներթափանցումներից, այլ միայն երաշխավորում է, որ նրանք չեն կարող հասկանալ տեղեկատվության բովանդակությունը:

Գաղտնագրային համակարգի օգտագործմամբ հաղորդագրության փոխանցման գործընթացը հետևյալն է.

Գաղտնագրության հիմնական հասկացություններն են.

Այբուբեն-տեղեկատվության կոդավորման համար օգտագործվող նիշերի վերջավոր բազմություն

Տեքստ-այբուբենի տարրերից կազմված կարգավորված հավաքածու

Գաղտնագիր-գաղտնագրային վերափոխման ալգորիթմով և բանալիով սահմանված գաղտնագրված տվյալների բազմության վրա բաց տվյալների բազմության արտապատկերման հակադարձելի վերափոխումների բազմություն

Ալգորիթմ-գաղտնագրերի կառուցման և օգտագործման կանոն

Գաղտնագրում-վերափոխման գործընթաց, որի արդյունքում ելակետային տեքստը, որը կրում է նաև բաց տեքստ անվանումը, փոխարինվում է գաղտնագրված տեքստով

Վերծանում-գաղտնագրմանը հակադարձ գործընթաց

Բանալի-տվյալների գաղտնագրային վերափոխման ալգորիթմի որոշ պարամետրերի կոնկրետ վիճակ (գաղտնի կամ բաց), որն ապահովում է տվյալ ալգորիթմի համար հնարավոր բոլոր տարբերակներից միայն մեկի ընտրությունը

Գաղտնահամակարգ-հաղորդագրությունների գաղտնագրման և վերծանման համար անհրաժեշտ ալգորիթմների, բանալիների և այլ միջոցների ամբողջություն

Հակառակորդ-հաղորդագրության բովանդակությանը ծանոթանալու կամ այն աղավաղելու փորձ կատարող կողմնակի անձ

Գրոհ-հակառակորդի գործողությունները գաղտնահամակարգին ընդեմ

Գաղտնակայունություն-գաղտնագրի կամ գաղտնահամակարգի հիմնական բնութագրիչ, որը սահմանում է նրա կայունությունը գաղտնավերլուծության մեթոդներով բացման հանդեպ

Համակարգի կոտրում-վիճակ, երբ հակառակորդը գտել է վերծանման բանալու որոշման գործնական միջոց:

Հակառակորդի նպատակը վերծանման բանալին ստանալն է և հաջողության դեպքում նա ունենում է նույն գիտելիքները, ինչ-որ հաղորդագրության օրինական ստացողը: Բանալիների փոխանցման և պահման անվտանգության ապահովումը հանդիսանում է գաղտնագրային համակարգի առավել կարևոր բաղկացուցիչ մասը:

20. ԳԱՂՏՆԱՀԱՄԱԿԱՐԳԵՐԻՆ ՆԵՐԿԱՅԱՑՎՈՂ ՊԱՀԱՆՋՆԵՐԸ

Տեղեկատվության պաշտպանության ժամանակակից գաղտնագրային համակարգերի համար ձևակերպված են հետևյալ համընդունելի պահանջները.

- գաղտնագրված տեքստը պետք է ընթերնելի լինի միայն վերծանման բանալու առկայության դեպքում
- գաղտնագրված տեքստի հատվածի և համապատասխան բաց տեքստի միջոցով օգտագործված բանալու որոծման համար անհրաժեշտ գործողությունների թիվը պետք է պակաս ճլինի հնարավոր բանալիների ընդհանուր թվից
- հնարավոր բանալիների լիակատար հատարկման (պերեբոր) եղանակով տեքստի վերծանման համար անհրաժեշտ գործողությունների թիվը պետք է ունենա խիստ ստորին գնահատանք և դուրս լինի ժամանակակից քոմփյութերային համակարգերի հնարավորություններից
- գաղտնագրման ալգորիթմների գիտենալը ճպետք է ազդի համակարգի գաղտնակայունության վրա
- բանալու աննշան փոփոխությունը պետք է առաջացնի գաղտնագրված տեքստի տեսքի էական փոփոխություններ
- գաղտնագրման ալգորիթմնի կառուցվածքային տարրերը պետք է լինեն անփոփոխ
- գաղտնագրված տեքստի երկարությունը պետք է հավասար լինի բաց տեքստի երկարությանը
- բոլոր հնարավոր բանալիներից ցանկացածը պետք է ապահովի տեղեկատվության հուսալի պաշտպանություն
- բանալու երկարության փոփոխությունը չպետք է բերի գաղտնագրման ալգորիթմի որակական վատթարացմանը

Այս պահանջների պահպանումը թույլ կտա ստեղծել տեղեկատվական անվտանգության ապահովման արդյունավետ և բավականաչափ գաղտնակայուն համակարգեր:

Գաղտնակայունության գնահատումը

Կարելի է ենթադրել, որ ցանկացած հակառակորդ գաղտնագրման համակարգերին վերաբերվող հնարավորինս մեծ տեղեկատվության է տիրապետում: Գաղտնահամակարգի անվտանգությունը պետք է սահմանվի միայն բանալու գաղտնիությամբ: Ալգորիթմների և նրանց իրականացման միջոցների փոփոխումը շատ թանկ է և ժամանակատար:

Համակարգի պաշտպանվածությունը չպետք է կախված լինի մի այնպիսի բանից, որը անհնար է արագ փոփոխել գաղտնի տեղեկատվության արտահոսքի դեպքում:

Գոյություն ունեն բազմաթիվ գաղտնագրային համակարգեր, որոնք տարբերվում են բարդության և պաշտպանվածության աստիճաններով:

Ո՞ր գաղտնահամակարգը ընտրել: Լավագույն պահանջվող գաղտնակայությունը ապահովող ամենաէժան համակարգն է:

Անվտանգության համակարգերի նախագծման հետ միաժամանակ պետք է ապահովել այդ համակարգերի գաղտնակայունության հիմնավորված քանակական գնահատականը:

Անհրաժեշտ է դիտարկել ամենավատթարագույն դեպքը, որը որոշվում է հետևյալ ենթադրություններով.

- հակառակորդը ունի լիակատար տեղեկատվություն գաղտնագրային համակարգերի մասին բացառությամբ գաղտնի բանալու
- հակառակորդը իր տրամադրության տակ ունի զգալի ծավալով գաղտնագրված տեքստ
- հակառակորդը իր տրամադրության տակ ունի բաց տեքստ, որը համապատասխանում է գաղտնագրված տեքստի մի որոշ ծավալին:

21. ԳԱՂՏՆԱՀԱՄԱԿԱՐԳԻ ՎՐԱ ԿԱՏԱՐՎՈՂ ԳՐՈՀՆԵՐԻ ՏԵՍԱԿՆԵՐԸ

Գրոհները կարող են տարբերվել հակառակորդի վարքի սցենարներով, կախված նրա տեղեկացվածության աստիճանից կարելի է առանձնացնել գրոհների հետևյալ տիպերը.

- Գորի միայն հայտնի գաղտնագրված տեքստի առկայության դեպքում
  - հակառակորդը տնօրինում է միայն մի քանի հաղորդագրությունների գաղտնագրված տեքստերին
  - հակառակորդը ունի կապի ուղիներին ֆիզիկական դիմման հնարավորություն, բայց չունի գաղտնագրման և վերծանման միջոցներին դիմելու հնարավորություն
- Գրոհ հայտնի բաց տեքստի առկայության դեպքում
  - հակառակորդը ոչ միայն հնարավորություն ունի դիմել որոշ հաղորդագրությունների գաղտնագրված տեքստերին, այլ նաև՝ դրանց բաց տեքստերին
  - գրոհի անցկացման հնարավորությունը պարզեցվում է տիպային փաստաթղթերի գաղտնագրման ժամանակ, երբ տվյալների որոշակի խմբեր կրկնվում են և հայտնի են
- Գրոհ բաց տեքստի ընտրության հնարավորության առկայության դեպքում
  - հակառակորդը հնարավորություն ունի ըստ ցանկության ընտրել տեքստերը, որոնք հետագայում կստանա գաղտնագրված տեսքով
  - գրոհի մեջ կարող են ներգրավվել գաղտնահամակարգից օգտվելու հնարավորություն ունեցող անձիք
- Գրոհ բաց տեքստի հարմարեցված ընտրությունով
  - հակառակորդը կարող է ոչ միայն ընտրել բաց տեքստը, որը հետագայում գաղտնագրվում է, այլ նաև կախված նախորդ գաղտնագրարդյունքներից փոխել իր ընտրությունը
  - հակառակորդին ընձեռում է ավելի մեծ հնարավորություններ
- Գրոհ ընտրված գաղտնագրված տեքստի օգտագործմամբ
  - հակառակորդը կարող է ընտրել տարբեր գաղտնագրված տեքստեր վերծանման համար
  - հատուկ հետաքրքրություն է ներկայացնում բաց բանալիով համակարգերի դեպքում
- Գրոհ բոլոր հնարավոր բանալիների հատարկման (պերեբոր) եղանակով
  - ենթադրում է հայտնի գաղտնագրված տեքստի օգտագործումը և իրականացվում է ստուգելով վերծանված բաց տեքստի իմաստավորված լնելը
  - պահանջում է առավելագույն հաշվողական հզորությունների ներգրավում
  - երբեմն կոչվում է ուժային գրոհ:

Գաղտնակայունության գնահատման համար կարելի է.

- ✓ ելնելով հակառակորդին մատչելի հաշվողական հզորություններից գնահատել յուրաքանչյուր բանալու վերլուծության համար պահանջվող ժամանակը
- ✓ դրա հիման վրա գնահատել բոլոր հնարավոր բանալիների հատարկման համար անհրաժեշտ ժամանակը:

Առաջին մոտարկումով (որևէ կարգի մեծությունների (կամ երկրաչափական առարկաների) մոտավոր արտահայտությունը ուրիշ՝ առավել հայտնի կամ ավելի պարզ մեծություններով (ապրոքսիմացիա)) համակարգը կարող է համարվել գաղտնակայուն, եթե բոլոր բանալիների հատարկման ժամանակը զգալիորեն մեծ է, քան տեղեկատվության գաղտնիության պահպանման անհրաժեշտ ժամանակը:

22. ՀԱՄԱԿԱՐԳՉԱՅԻՆ ՎԻՐՈՒՍԻ ՀԻՄՆԱԿԱՆ ՀԱՏԿՈՒԹՅՈՒՆՆԵՐԸ

Համակարգիչը վիրուսով վարակվելուց հետո համակարգչում առաջանում են մի շարք խնդիրներ՝

- համակարգչի աշխատունակության նվազում (այն սկսում է դանդաղ աշխատել՝ երկար «մտածել»),
- համակարգչով աշխատելու ընթացքում օպերացիոն համակարգի ավտոմատ վերաբեռնավորում,
- տեքստային փաստաթղթերի աղավաղում,
- կիրառական ծրագրերի աշխատանքի վթարային ելք,
- ճկուն և կոշտ սկավառակների վրա եղած ֆայլերի բազմաթիվ կրկնօրինակների ստեղծումէկրանի մարում
- չնախատեսված հաղորդագրության հայտնվում 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 ֆայլերի 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 և այլն:

23. ԿԵՍԱՐԻ ԳԱՂՏՆԱԳԻՐԸ

Կեսարի ձևափոխում կամ Կեսարի գաղտնագիր, որի ժամանակ այբուբենի տառերը դասավորվում են շրջանաձև, այսինքն՝ ա, բ, գ, ..., և, օ, ֆ, որին հաջորդում է ա-ն, հետո բ-ն և այդպես շարունակ: Սկզբնական տեքստի յուրաքանչյուր տառ փոխարինվում է նրան հաջորդող երրորդ տառով, այսինքն՝ ա-ն փոխարինվում է դ-ով, բ-ն՝ ե-ով, գ-ն՝ զ-ով, ..., ք-ն՝ ֆ-ով, և-ը՝ ա-ով, օ-ն՝ բ-ով և ֆ-ն՝ գ-ով:

Շեղումը կարող է լինել ոչ միայն 3 այլ կամայական թիվ 1-ից 39-ի սահմանում, ինչը կախված է այբուբենի տառերի քանակի հետ: Եթե կիրառվի անգլերեն լեզվի այբուբենը, ապա այդ շեղումը կարող է լինել 1-ից 26-ի սահմաններում:

«Բարև ընկեր Օրդյան» նախադասության կոդավորումից հետո կստանանք հետևյալ նախադասությունը՝ «Եդփա իչղըփ Բփէողչ», իսկ «գևուեջկ» բառը ապակոդավորելով կստանանք «ֆուտբոլ» բառը:

1	2	3	4	5	6	7	8	9	10
Ա	Բ	Գ	Դ	Ե	Զ	Է	Ը	Թ	Ժ
Ի	Լ	Խ	Ծ	Կ	Հ	Ձ	Ղ	Ճ	Մ
Յ	Ն	Շ	Ո	Չ	Պ	Ջ	Ռ	Ս	Վ
Տ	Ր	Ց	ՈՒ	Փ	Ք	և	Օ	Ֆ	

Առաջադրանքներ.

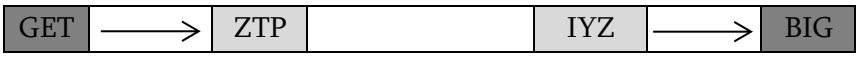
1. Օգտվելով Կեսարի ձևափոխությունից կոդավորիր նախադասությունները՝
   ա) ինֆորմատիկան գիտություն է,
   բ) ջուրը թափվեց սեղանին:
2. Ապակոդավորիր նախադասություններն օգտվելով Կեսարի ձևափոխությունից՝

   ա) ծչռ ժ զփցղձ զփղուդհուդղծչ,
   բ) զչղքֆի խղշդչըք նծպու խղշծչ:

24. ՊԱՐԶ ՓՈԽԱՐԻՆՄԱՆ ԳԱՂՏՆԱԳԻՐԸ

Կեսարի գաղտնագիրը պարզ փոխարինման գաղտնագրի մասնավոր դեպքն է:

Պարզ փոխարինման գաղտնագրի դեպքում կիրառվում է համապատասխանության աղյուսակը, որտեղ կարող է լինել մեկ բանալի երկու տարբեր ալգորիթմով: Օրինակ՝



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

Համապատասխանության աղյուսակը

Այժմ քննարկենք պարզ փոխարինման գաղտնագրի պարզագույն օրինակ.

1. Ընտրվում է որոշակի բանալու արտահայտություն՝

State Engineering University of Armenia

2. Այս բառակապակցությունից հեռացնելով բոլոր կրկնվող տառերը կստանանք բանալու սկզբնամասը՝

STAENGIRUVYOFM

3. Աշխատանքը հեշտացնելու համար նախօրոք գրված այբուբենից հեռացնում ենք վերը նշված սկզբնամասի տառերը: Արդյունքում ստանում ենք բանալու վերջնամասը՝

BCDHJKLPQWXZ

4. Բանալու սկզբնամասը և վերջնամասը միավորվում են և արդյունքում ստանում ենք նոր բանալին՝

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

Արդյունքում բանալիների քանակը որոշակիորեն կրճատվում է, բայց շարունակում է մնալ շատ մեծ:

Առաջադրանք.

1. Goris State College բառակապակցությունը կոդավորել օգտագործելով պարզ փոխարինման գաղտնագիրը

25. ԼԵԶՎԻ ՎԻՃԱԿԱԳՐՈՒԹՅՈՒՆԸ ԳԱՂՏՆԱԳՐՈՒԹՅԱՆ ՄԵՋ

Լեզվի վիճակագրությունն իրենից ներկայացնում է որոշակի ինֆորմացիա գաղտնագրության մեջ հաճախ օգտագործվող տառերի, դրանց հիստագրի, տառերի վիճակագրության, տառերի զույգերի օգտագործման վիճակագրության մասին:

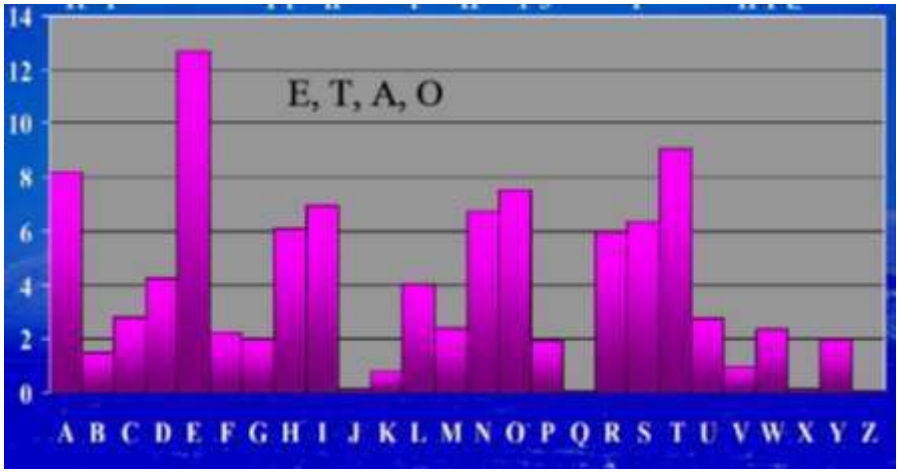
Քանի որ ինֆորմացիայի կոդավորման մեջ հիմնականում օգտագործվում է անգլերեն լեզվի այբուբենը, ապա բոլոր վիճակագրական տվյալները կապված են հենց սրա հետ:

Անգլերեն տեքստերում տառերի վիճակագրությունը հետևյալն է.

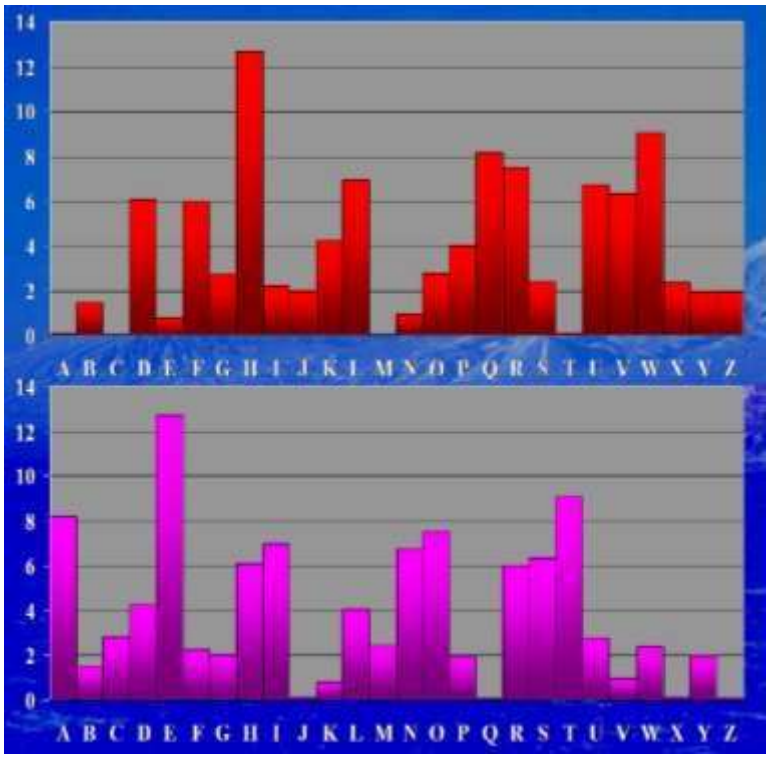
ՏԱՌ	ՏՈԿՈՍ	ՏԱՌ	ՏՈԿՈՍ	ՏԱՌ	ՏՈԿՈՍ
A	8,168	B	1,492	C	2,782
D	4,253	E	12,702	F	2,228
G	2,015	H	6,094	I	6,966
J	0,153	K	0,772	L	4,025
M	2,406	N	6,749	O	7,507
P	1,929	Q	0,095	R	5,987
S	6,327	T	9,056	U	2,758
V	0,978	W	2,360	X	0,150
Y	1,974	Z	0,074		

Բոլորից հաճախ օգտագործվում են E, T, A, O տառերը:

Անգլերեն տառերի վիճակագրության հիստագիրը հետևյալն է.



Գաղտնագրված տեքստում տառերի վիճակագրությունը հետևյալն է.



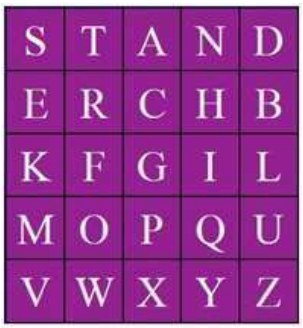
Անգլերեն լեզվում կարող է լինել 26*26=676 տառերի զույգ:

Տառերի զույգերի օգտագործման վիճակագրությունը հետևյալն է.

ԶՈՒՅԳ	ՏՈԿՈՍ	ԶՈՒՅԳ	ՏՈԿՈՍ	ԶՈՒՅԳ	ՏՈԿՈՍ
TH	6,3	AR	2,0	HA	1,7
IN	3,1	EN	2,0	OU	1,4
ER	2,7	TI	2,0	IT	1,4
RE	2,5	TE	1,9	ES	1,4
AN	2,2	AT	1,8	ST	1,4

Գաղտնագրված տեքստի վիճակագրական վերլուծությունը կարող է կիրառված գաղտնագրի վերաբերյալ որոշակի հետևություններ կատարելու հնարավորություն ընձեռել:

Փլեյֆեյրի գաղտնագիրը իրենից ներկայացնում է տառերի զույգերի գաղտնագրում իրականացնող գործնական գաղտնագիր:



Բանալի

Տեքստի նախնական ձևափոխում.

- բոլոր J-ի տառերը փոխարինել I-երով
- բաժանել տեքստը տառերի զույգերի
- եթե հերթական զույգը նույն տառերից է նրանց միջև ավելացնել Z տառը
- եթե վերջին զույգում մեկ տառ է, լրացնել այն Z տառով:

Գաղտնագրման կանոնները.

- եթե ընտրված բառակապակցության երկու տառը բանալու նույն տողի վրա են, ապա նրանցից յուրաքանչյուրը փոխարինվում է բանալիում իրենից աջ գտնվողով
- եթե երկու տառը նույն սյունում են, ապա նրանցից յուրաքանչյուրը փոխարինվում է իրենից ցածրով
- եթե երկու տառը տարբեր տողերում և սյուներում են, ապա նրանցից յուրաքանչյուրը փոխարինվում է իր տողի վրա մյուս տառի սյունում գտնվող տառով:

Ընդլայնված բանալի

Այժմ կոդավորենք հետևյալ բառակապակցությունն օգտվելով վերը նշված կանոններից.

GOOD BROOMS SWEEP CLEAN

GO OD BR OO MS SW EE PC LE AN

Քայլ 1.

Եթե հերթական զույգը նույն տառերից է նրանց միջև ավելացնել Z տառը:

Եթե վերջին զույգում մեկ տառ է, լրացնել այն Z տառով:

Եթե երկու տառը տարբեր տողերում և սյուներում են, ապա նրանցից յուրաքանչյուրը փոխարինվում է իր տողի վրա մյուս տառի սյունում գտնվող տառով:

GO OD BR OZ OM SZ SW EZ EP CL EA NZ
FP

Քայլ 2.

Եթե երկու տառը տարբեր տողերում և սյուներում են, ապա նրանցից յուրաքանչյուրը փոխարինվում է իր տողի վրա մյուս տառի սյունում գտնվող տառով:

GO OD BR OZ OM SZ SW EZ EP CL EA NZ
FP UT

Քայլ 3.

Եթե երկու տառը բանալու նույն տողի վրա են, ապա նրանցից յուրաքանչյուրը փոխարինվում է բանալիում իրենից աջ գտնվողով:

GO	OD	BR	OZ	OM	SZ	SW	EZ	EP	CL	EA	NZ
FP	UT	EC	UW	PO	DV	TV	BV	CM	BG	CS	DY

Վերծանման կանոնները.

- եթե երկու տառը բանալու նույն տողի վրա են, ապա նրանցից յուրաքանչյուրը փոխարինվում է բանալիում իրենից ձախ գտնվողով
- եթե երկու տառը նույն սյունում են, ապա նրանցից յուրաքանչյուրը փոխարինվում է իրենից վերինով
- եթե երկու տառը տարբեր տողերում և սյուներում են, ապա նրանցից յուրաքանչյուրը փոխարինվում է իր տողի վրա մյուս տառի սյունում գտնվող տառով:

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

Վերծանման բանալի

Վերծանում

Վերծանումը կատարվում է գաղտնագրման հակառակ գործողությունների հերթականությամբ.

- զույգերի վերծանում բանալիով
- ըստ տեքստի իմաստի
  - ավելորդ Z-երի հեռացում
  - բառերի ձևավորում զույգերից
  - ավելորդ I-երի փոխարինում J-երով:

FP	UT	EC	UW	PO	DV	TV	BV	CM	BG	CS	DY
GO	OD	BR	OZ	OM	SZ	SW	EZ	EP	CL	EA	NZ

GOOD BROOMS SWEEP CLEAN

Փլեյֆեյրի գաղտնագիրը լինելով երկտառ գաղտնագիր ունի ոչ շատ մեծ բանալի:

27. ՀՈՄՈՖՈՆԻԿ ԳԱՂՏՆԱԳԻՐԸ

Հոմոֆոնիկ գաղտնագիրն այբուբենի ընդլայնումն է մի քանի լրացուցիչ նիշերով, որն էլ իր հերթին «հավասար» է այլ այբուբենի օգտագործմանը:

Գաղտնագիրը կոչվում է հոմոֆոնիկ, եթե բաց տեքստի նույն տառին համապատասխանում են գաղտնագրված տեքստի մի քանի նիշեր:

Հոմոֆոնիկ գաղտնագրի հիմնական գաղափարը կայանում է հետևյալում.

Հոմոֆոնիկ գաղտնագրի ժամանակ օգտագործվում է աղյուսակ, որում նշված են տառեր և այդ տառերից յուրաքանչյուրին փոխարինում է որևէ թիվ այնպես, որ հակառակորդը գրոհիների

A	A	B	C	D	E	E	F	G	H	I	J	K	L	M	N
01	07	14	21	04	23	27	20	29	31	06	28	12	30	17	00

N	O	O	P	Q	R	R	S	T	T	U	V	W	X	Y	Z
18	26	19	09	10	25	13	02	08	24	22	05	16	15	11	03

ժամանակ չկարողանա վերծանել կամ գոնե դա դժվար լինի:

Ըստ այս աղյուսակի, եթե կոդավորենք ENGINE բառը կստացվի.

28. ԲԱԶՄԱԱՅԲՈՒԲԵՆ ԳԱՂՏՆԱԳԻՐ

Կրիպտոգրաֆիայի պատմությունը հաշվվում է արդեն չորս հազար տարի: Որպես կրիպտոգրաֆիայի պարբերականացման հիմնական հայտանիշ օգտագործվում են գաղտազերծման օգտագործվող մեթոդների տեխնոլոգիական հատկանիշները:

Առաջին շրջանը (մոտավորապես երրորդ հազարամյակ մ.թ.ա.) բնութագրվում է մեծամասամբ այբբենական կոդավորման օգտագործմամբ, այսինքն այդպիսի կոդավորման հիմնական դրույթն է՝ սկզբնական տեքստի այբուբենի տառերի փոխարինումը մեկ այլ այբուբենի նիշերով:

Երկրորդ շրջանը (IX դարից - մինչևXX դար) տարբերակվում էր բազմաայբուբենային կոդավորումների ներմուծմամբ:

Երրորդ շրջանը (XX դարի սկզբից, միչև նույն դարի կեսը) բնութագրվում է գաղտագորղների գործում էլեկտրոմեխանիկական սարքերի ներդրմամբ: Դրան զուգահեռ շարունակվում էր բազմաայբուբեն կոդավորումների օգտագործումը:

Չորրոդ շրջանը (XX դարի 70-ական թվականներից մինչև մաթեմատիկական կրիպտոգրաֆիայի անցում):

Բազմաայբուբեն կարելի է անվանել այն գաղտնագիրը, որում բաց տեքստի կոնկրետ տառը նրա դիրքից (կամ նախորդ տեքստից) կախված փոխարինվում է տարբեր այբուբենների նիշերով:

Գաղտնագրված տեքստի նույն նիշը կարող է ներկայացնել բաց տեքստի տարբեր տառեր:

Կիրառվող այբուբենի քանակը կոչվում է պարբերություն: Եթե պարբերությունը հավասար է 2-ի, ապա գաղտնագիրը համարժեք է տառերի զույգերի պարզ փոխարինմանը:

29. ՎԻԺԻՆԵՐԻ ԳԱՂՏՆԱԳԻՐԸ

Վիժների ձևափոխումը կամ գաղտնագիրգը, նույն Կեսարի ձևափոխությունն է տեղաշարժի փոփոխական մեծությամբ (Կեսարի ձևափոխությունում տեղաշարժի մեծությունը հիմնականում 3 է կամ ավելի բարդ գաղտնագրերում 1-26՝ անգլերեն լեզվի դեպքում, 1-39՝ հայոց լեզվի դեպքում), որտեղ օգտագործվում է բանալիային բառ: Բանալային բառն իր հերթին ձևավորում է տեքստի տառերի տեղաշարժի հաջորդականությունը: Օրինակ, «դիզել» բանալիային բառը ձևավորում է հետևյալ հաջորդականությունը՝ 4, 11, 6, 5, 12, 4, 11, 6, 5, 12, 4, 11, 6, 5, 12, ..., որտեղ 4, 11, 6, 5, 12 թվերը «դիզել» բառի տառերի հերթական համարներն են այբուբենում:

Օգտվելով այս ձևափոխությունից կոդավորենք «ես սովորում եմ կոդավորել» նախադասությունը: Նախ գրենք այբուբենի տառերը հերթականությամբ՝

1	2	3	4	5	6	7	8	9	10
Ա	Բ	Գ	Դ	Ե	Զ	Է	Ը	Թ	Ժ
Ի	Լ	Խ	Ծ	Կ	Հ	Ձ	Ղ	Ճ	Մ
Յ	Ն	Շ	Ո	Չ	Պ	Ջ	Ռ	Ս	Վ
Տ	Ր	Ց	ՈՒ	Փ	Ք	և	Օ	Ֆ	

Կազմենք հետևյալ աղյուսակը (Աղյուսակ 1), որն ունի 3 տող և 24 սյուն: 1-ին տողում գրենք «ես սովորում եմ կոդավորել» նախադասության տառերը առանձին սյուներում, 2-րդ տողում բանալային բառից ստացված հաջորդական թվերը, որոնք ցույց են տալիս, թե 1-ին տողի համապատասխան տառը քանի տառ պետք է տեղափոխել, իսկ 3-րդ տողում կստացվի կոդավորման արդյունքը՝ «թա փսգռդաչ ձո պվթխուփօժո»:

Աղյուսակ 1

ե	ս		ս	ո	վ	ո	ր	ու	մ		ե	մ		կ	ո	դ	ա	վ	ո	ր	ե	լ
4	11		6	5	12	4	11	6	5		12	4		11	6	5	12	4	11	6	5	12
թ	ա		փ	ս	գ	ռ	դ	ա	չ		ձ	ո		պ	վ	թ	խ	ու	փ	օ	ժ	ո

Օգտվելով Վիժների ձևափոխությունից ապակոդավորելով «խլյզելը» բառը, որում որպես բանալային բառ օգտագործվել է «դիզել» բառը, կստանանք «թակարդ» բառը:

Առաջադրանքներ:

1. Օգտվելով Վիժների ձևափոխությունից կոդավորի՛ր նախադասությունները՝
   ա) այսօր ամպամած է (բանալիային բառ՝ ավանակ)
   բ) կապուտաչյա Սևան (բանալիային բառ՝ բենզին)

2. Ապակոդավորի՛ր նախադասություններն օգտվելով Վիժների ձևափոխությունից՝
   ա) ըվ ռձփբջխչուրջ ըյ (բանալիային բառ՝ 3,1,21,12)
   բ) գնբաց խնջխնբպ թ (բանալիային բառ՝ 2, 1, 12)

Վերադասավորման գաղտնագրի դեպքում գաղտնագրումը կատարվում է հետևյալ կերպ.

1. Նախ ընտրվում է բառակապակցություն, որը պետք է գաղտնագրվի: Օրինակ՝

   Computer Systems and Informatics Department
2. Գաղտնագրման համար ընտրվում է բանալի թվի տեսքով, օրինակ՝ 5
3. Բաց տեքստը արտագրել հինգտառանի տողերով (Աղյուսակ 1)
4. Եթե վերջին տողում կա 5-ից պակաս տառ, ապա այն լրացնել Z-ով
5. Առաջին սյան տառերը գրել հաջորդաբար վերից վար, հետո երկրորդ սյան և այլն:

C	O	M	P	U
T	E	R	S	Y
S	T	E	M	S
A	N	D	I	N
F	O	R	M	A
T	I	C	S	D
E	P	A	R	T
M	E	N	T	Z

Աղյուսակ 1.

CTSAFTEMOETNOIPEMREDRCANPSMIMSRTUYSNADTZ

Վերադասավորման գաղտնագրի դեպքում վերծանումը կատարվում է հետևյալ կերպ.

1. Գրվում է բառը, որը պետք է գաղտնագրվի: Օրինակ՝

   CTSAFTEMOETNOIPEMREDRCANPSMIMSRTUYSNADTZ
2. Գաղտնագրված տեքստը բաժանել 5 տողերի, քանի որ գաղտնագրման դեպքում որպես բանալի ընտրել ենք 5 թիվը
3. Առաջին սյան տառերը գրել հաջորդաբար վերից վար, հետո երկրորդ սյան և այլն (Աղյուսակ 2)
4. Հեռացնել ավելորդ Z-ը և տեղադրել բացատները

COMPUTERSYSTEMSANDINFORMATICSDEPARTMENTZ

Computer Systems and Informatics Department

Բանալին պետք է լինի գաղտնագրված տեքստում տառերի թվի բաժանարար (a թվի բաժանարար կոչվում է այն թիվը, որի վրա a-ն բաժանվում է առանց մնացորդի):

C	T	S	A	F	T	E	M
O	E	T	N	O	I	P	E
M	R	E	D	R	C	A	N
P	S	M	I	M	S	R	T
U	Y	S	N	A	D	T	Z

Աղյուսակ 2

ԳՐԱԿԱՆՈՒԹՅՈՒՆ

1. David Kahn The Codebreakers — The Story of Secret Writing. — New York: Charles Scribner's Sons, 1967
2. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. — М.: Гелиос АРВ, 2002
3. S. Ա. Սոբոլյովա: ներածություն: «Գաղտնագրության պատմությունը Ռուսաստանում
4. Վ. Ժելնիկով: Գաղտնագրերի ի հյատ գալը: Գաղտնագրությունը պապիրուսիներից մինչև համակարգիչներ
5. Հայկական ծածկագրություն : Ա.Գ. Աբրահամյան, Երևան : Համալս. հրատ., 1978
6. F.L. Bauer, Decrypted Secrets, 2nd edition, 2000, Springer
7. Chris Savarese and Brian Hart, The Caesar Cipher
8. https://hy.m.wikipedia.org/wiki/%D4%B3%D5%A1%D5%B2%D5%BF%D5%B6%D5%A1%D5%A3%D6%80%D5%B8%D6%82%D5%A9%D5%B5%D5%B8%D6%82%D5%B6?fbclid=IwAR2o4xgDhQ34d4-p81YpZQEGXaGgejGtraekTOLVKEGWm9st24zXkoPcjO0
9. https://hy.m.wikipedia.org/wiki/%D4%BF%D6%80%D5%AB%D5%BA%D5%BF%D5%B8%D5%A3%D6%80%D5%A1%D6%86%D5%AB%D5%A1%D5%B5%D5%AB_%D5%BA%D5%A1%D5%BF%D5%B4%D5%B8%D6%82%D5%A9%D5%B5%D5%B8%D6%82%D5%B6
10. Ս.Մարտիրոսյան, Անձնական կիբեռանվտանգության հիմունքներ, Եր., «Նորավանք» ԳԿՀ, 2016, 62 էջ:
11. G K. Kostopoulus, Cyberspace and Cybersecurity, CRC Press, Taylor &Francis Group, Soca Raton, London – New York.
12. Է. Ա. Ղազարյան, Տեղեկատվական անվտանգության անգլերեն-ռուսերեն-հայերեն հանրագիտական բառարան, «Նորավանք» ԳԿՀ, Երևան, 2016:
13. Грамматчиков А., Вандышева О., Идет кибервойна народная, Эксперт, #5, с. 13, 2017.
14. Гриняев С., Поле битвы - киберпространство, Мн., Харвест, 2004.
15. G.Harutyunyan, Homo virtualicus in the context of post – democracy and information security, 21st Century, # 1(9), p. 5, 2011.
16. Черненко Е., Начало политической кибервойны, Россия в глобальной политике, #6, с. 134, 2016.

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ