ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЬЛИМ ВАЗИРЛИГИ

ҚАРШИ МУҲАНДИСЛИК ИҚИСОДИЁТ ИНСТИТУТИ

Факултети: Мухандис техника

Таълим йўналиши: “Ер усти транспорт тизимлари ва уларнинг эксплуатцияси”

І-босқич **Т-141 гуруҳ** талабаси Ўролов Жонибекнинг

“Информатика ва Ахборот технологиялари” фанидан

Компьютер вируслари ва вирусга қарши воситалар

мавзуси бўйича бажарган

РЕФЕРАТИ

Бажарди: Ж.Ўролов

Қабул қилди: С.Н.Хусанов

Қарши 2013

Компьютер вируслари ва вирусга қарши воситалар

Режа:

Кириш

I. Назарий қисм

1. Компьютер вируси ҳақида тушунча. Вирусларнинг моҳияти, пайдо бўлиши ва тарқалишининг асосий белгилари
2. Компьютер вирусларини таснифланиши
3. Компьютер вирусларидан ҳимоя қилиш усуллари
4. Боб.Вирусларни пайқаш ва улардан ҳимоя қилиш дастурлари. Уларнинг ва тавсифлари.
5. Компьютер вирусларидан ҳимоя қилиш учун асосий чоралар

II. Хулоса

III. Фойдаланган адабиётлар

Кириш

Компьютер вируси ўлчами буйича катта бўлмаган,махсус ёзилган дастурдан иборат бўлиб, у ўзини бошқа дастурларга «ёзиб қўйиши», шунингдек, компьтерда турли нохуш амалларни бажара олиши мумкин. Бундай дастур ишлашни бошлаганда дастлаб бошқарувни вирус олади. Вирус бошқа дастурларни топади ва унга «юқади»,шунингдек, қандайдир зарарли амалларни (масалан, дискдаги файл ёки файлларнинг жойлашиш жадвалини бузади, тезкор хотирани «ифлослайди»)бажаради.

Вирус жойлашган дастур одатдагидек ишини давом эттиради. Ташқаридан дастурнинг касалланганлиги билинмайди. Кўп турдаги вируслар шундай тузилганки, касалланган дастурни ишга туширганда вирус компьютер хотирасида доимий қолади ва вақти-вақти билан дастурларни касаллайди ва компьютерда зарарли амалларни бажаради.

Мавжуд бўлган вирусларнинг кўпчилиги ядро системали файлларни афзал кўрадилар,чунки кўп замонавий компьютерларда файллар системаси бир хил юкланади масалан вируслар аксарият холларда ,**Command.com** файлига бирлаштирлади ва **DIR** буйруғи билан бошқа диск ва директорияларга тарқалади.Кўп холларда системанинг зарарланиши киритиш ва чиқариш жараёнига мурожаат қилганда рўй беради

Аслини олганда, вируслар системаларга бирикиб кетиш учун ҳар қандай йўлларни ишлатишади, шунинг учун ҳам зарарланмайдиган ситемалар йўқдир.

Компьютерларга вирусларнинг кириб кетишининг асосий йўли бўлиб зарарланган дискеталар ҳизмат қилади.Вируслар борган сайин бешавқат ва ҳеч нарсадан қўрқмайдиган бўлиб бормоқда,ҳатто энг етук вирусларга қарши дастурлар ҳам улар билан курашишга ожизлик қилмоқдалар. Шундай вируслар мавжудки,улар энергияга боғлиқ бўлмаган хотирага яшириниб олиб,системани тозалашда жуда катта қийинчиликлар туғдирадилар. Ҳатто ҳақиқий фирма белгисига эга бўлган,сиқилган дастур ҳам вирусдан ҳоли эканлигига ҳеч ким кафиллик бера олмайди.Вирусларни **CD ROM** дискларнинг штамповка жараёнида ҳам ўрнашганлик ҳоллари мавжуддир.

Вирус фаолияти асосан 4 та фазага эга;

- ухлаш фазаси;
- кўпайиш фазаси;
- ишга киришиш фазаси;
- вайрон қилиш фазаси.

Вирус ихтирочиси аста-секинлик билан фойдаланувчининг ишончини қозониш мақсадида,ухлаш фазасини ишлатиши мумкин,чунки бунда вирус кўпаймайди ва маълумотларни бузмайди. Хозирги кунда 20000 дан ортиқ компьютер вируслари мавжуд бўлиб, улар компьютерда маълумотларни ишончли сақланишига хавф солади ва компьютер ишлаш жараёнида турли муаммолар келиб чиқишига сабаб бўлади. Шу боис компьютер вируслари, уларнинг турлари, етказадиган зарарлари ҳамда улардан ҳимояланиш учун кўриладиган чоралар билан таниш бўлиш мухим

1. Компьютер вируси ҳақида тушунча. Вирусларнинг моҳияти, пайдо бўлиши ва тарқалишининг асосий белгилари

ШК ларнинг оммавий қўлланилиши, бахтга қарши, компьютерларнинг меъёрда ишлашига тўсқинлик қиладиган, файлли структурани, дискларни бузадиган ва компьютерда сақланадиган ахборотга талофат етказадиган ўз-ўзидан ишлаб чиқариладиган дастур вирусларни пайдо бўлиши билан алоқадордир. Битта компьюютерга кириб олиб, компьютер вируси бошқа компьютерларга тарқалиш қобилиятига эгадир.

Компьютер вируси нима

Компьютер вируси - махсус ёзилган дастур бўлиб, компьютерда ишлашда барча мумкин бўлган ҳалақитларни яратиш, файлларни ва каталогларни бузиш дастурлари ишдан чиқариш мақсадида ҳисоблаш тизимларига, компьютернинг тизимли соҳаларига, файлларга тадбиқ, қилинадиган, узларининг нусхаларини яратиш, бошқа дастурларга ўз-ўзидан бирикиб оладиган хоссаларга эгадирлар.

Ичида вирус жойлашган дастур **“зарарланган”** (“юқтирилган) деб аталади.

Бундай дастур ўз ишини бошлаганда, олдин бошқаришни вирус ўз қўлига олади. Вирус бошқа дастурларни топади ва “зарар-лантиради”, ҳамда бирор-бир зарарли ишларни бажаради (масалан, файлларни ёки дискда файлларни жойлашиш жадвалини бузади, тезкор хотирани “кирлантиради” ва х.к.) Вирусни ниқоблаш учун бошқа дастурларни зарарлантириш ва зарар етказиш бўйича ишлар ҳар доим ҳам эмас, айтайлик маълум бир шартлар бажарилганда, бажарилиши мумкин. Вирус унга керакли ишларни бажаргандан кейин у бошқаришни ўзи жойлашган дастурга узатади ва у дастур одатдагидай ишлай бошлайди. Шу билан билан бирга ташқи кўринишдан зарарланган дастурнинг ишлаши зарарланмаганники каби кўринади.

Вирусларнинг кўпгина кўринишлари шундай тузилганки, зарарлангандан дастур ишга туширилганда вирус компьютер хотирасида ҳар доим қолади ва вақти-вақти билан дастурларни зарарлантиради ва компьютерда зарарли ишларни бажаради.

Вируснинг барча ҳаракатлари етарлича тез бажарилиши мумкин ва бирор-бир хабарни бермайди, шунинг учун фойдаланувчи компьютерда бирорта одатдан ташқари ишлар бўлаётганини пайқаши жуда мушкулдир.

Компьютерда нисбатан кам дастурлар зарарланган бўлса вируснинг борлиги деярли сезиларсиз бўлади. Лекин бирор вақт ўтиши билан компьютерда қандайдир ғалати ҳодисалар рўй бера бошлайди, масалан:

- баъзи дастурлар ишлашдан тўхтайдилар ёки нотўғри ишлай бошлайдилар;
- экранга бегона хабарлар ёки белгилар чиқарилади;
- компьютерда ишлаш жиддий секинлашади;
- баъзи бир файллар бузилиб қолади ва х. к;

Бу вақтга келиб, қоидага кўра, фойдаланувчи ишлаётган етарлича кўп (ёки хатто кўпчилик) дастурлар вируслар билан зарарланган, баъзи бир файллар ёки дисклар эса ишдан чиққан ҳисобланади. Бундан ташқари, фойдаланувчи компьютеридаги зарарланган дастурлар дискеталар ёрдамида ёки локал тармоқ бўйича фойдаланувчининг ҳамкасбларини ва ўртоқларини компьютерига ўтиб кетган бўлиши мумкин.

Вирусларнинг баъзи бир кўринишлари ўзларини янада хавф-лироқ тушадилар. Улар бошланишда катта миқдордаги дастурларни ёки дискларни билдирмасдан зарарлантирадилар, кейин эса жуда жиддий шикастланишларни келтириб чиқаради, масалан, компьютердаги бутун қаттиқ дискни форматлайди. Дастур-вирус сезиларсиз бўлиши учун у катта бўлмаслиги керак. Шунинг учун, қоидага кура, вируслар етарлича юқори малакали дастурловчилар томонидан Ассемблер тилида ёзилади.

Компьютер вирусларини пайдо бўлиши ва тарқатилиши сабаблари, бир томондан, инсон шахсиятининг психологиясида ва унинг ёмон хислатларида яширинади (ҳаваслар, қасос олишлари, тан олинмаган ижодкорларни мансабпарастлиги, ўзининг қобилиятларини конструктив қўллашни имконияти йўқлиги), иккинчи томондан эса, ҳимоя

қилишнинг аппарат воситаларини ва шахсий компьютернинг операцион тизими томонидан қарши ҳаракатларни йўқлиги билан боғлиқдир.

Кўпчилик давлатларда қабул қилинган компьютер жиноятлари билан кураш ва вируслардан ҳимоя қилишнинг махсус дастур воситаларини ишлаб чиқиш тўғрисидаги қонунларга қарамасдан, янги дастур-вирусларнинг, сони доимо ошиб бормоқда. Бу шахсий компьютер фойдаланувчисидан вируслар табиати, вируслар билан зарарланиш усуллари ва улардан ҳимоя қилиш услублари тўғрисидаги билимларни талаб этади.

Вирусларни компьютерга кириб олинишини асосий йўллари олинадиган дисклар (эгилувчан ва лазерли), ҳам компьютер тармоқлари ҳисобланади. +аттиқ дискни вируслар билан зарарланиши компьютерни вирусни ўзида сақлаган дискетадан юклаганда амалга ошиши мумкин. Бундай зарарланиш тасодифий бўлиши мумкин, масалан, дискетани А: дисководдан чиқариб олмасдан ва компьютерни қайта юкланганда, бунда дискета тизимли бўлмаслиги ҳам мумкиндир. Дискетани зарарлантириш жуда оддийроқдир. Унга вирус, ҳаттоки агар дискетани зарарланган компьютерни дисководига қўйилганда ва, масалан, унинг мундарижасини ўқилганда, тушиши мумкин.

Зарарланган диск - бу юкланиш секторида дастур-вирус жойлашган дискдир.

Вирусни ўз ичига олган дастур ишга туширилгандан кейин бошқа файлларни зарарлантириш мумкин бўлиб қолади. Энг кўпроқ вируслар билан дискнинг юкланадиган сектори ва .EXE,.COM,.SYS ёки /BAT кенгайтмасига эга бўлган бажариладиган файллар зарарланадилар. Жуда ҳам кам матнли ва графикли файллар зарарланадилар.

Зарарланган дастур - бу унга тадбиқ қилинган дастур-вирусни ўз ичига олган дастурдир.

Компьютер вируси билан зарарланишда ўз вақтида уни пайқаш жуда муҳимдир. Бунинг учун вирусларни пайдо бўлишини асосий белгилари тўғрисида билимларга эга бўлиш керак. Уларга қуйидагилар тегишли бўлиши мумкин:

- олдин муваффақиятли ишлаган дастурларнинг ишлашини тўхташи ёки нотўғри ишлаши;
- компьютернинг секин ишлаши;
- операцион тизимни юклашни имкони йўқлиги;
- файлларни ва каталогларни йўқолиб қолиши ёки уларнинг мазмунини бузилиши;
- файлларни ўзгартирилганлик санасини ва вақтини ўзгариши;
- дискда файллар сони бехосдан жуда ошиб кетиши;
- бўш тезкор хотирани ўлчамини жиддий камайиши;
- экранга кўзга тутилмаган хабарларни ёки тасвирларни чиқариш;
- кўзда тутилмаган товушли хабарларни бериш;
- компьютер ишлашида тез-тез бўладиган осилиб қолишлар ва бузилишлар.

Таъкидлаш керакки, юқорида санаб ўтилган ҳодисалар вирусларни келиб чиқиш билан бўлиши мажбурий эмас, бошқа сабабларнинг оқибатлари ҳам бўлиши мумкин. Шунинг учун компьютер ҳолатини тўғри диагностикалаш ҳар доим мушкулдир.

Вирус билан зарарланган ва бузилган файллар

Компьютер вируси компьютерда мавжуд бўлган дисклардаги исталган файлни етарлича ўзгартириши ва бузиши мумкин. Лекин файлларнинг баъзи бир турларини вирус “зарарлантириши” мумкин. Бу билдирадики, вирус бу файлларга “тадбиқ” қилиниши мумкин, яъни уларни шундай ўзгартирадики, улар вирусни ўз ичида сақлайдилар ва бу вирус баъзи бир ҳолатларда ўзининг ишини бошлаши мумкин.

Таъкидлаш лозимки, дастурларнинг ва хужжатларнинг матн-лари, маълумотлар базасининг ахборотли файллари, жадвалли процессорларнинг жадваллари ва бошқа шунга ўхшаш файллар вирус билан зарарланиши мумкин эмас, бу файлларни вируслар фақат бузиши мумкин.

Вирус билан “зарарланиши” мумкин бўлган файлларнинг турлари қуйидагилардир:

1. **Бажариладиган файллар**, яъни .COM ва .EXE кенгайтмали файллар, ҳамда бошқа дастурлар бажарилганда юкланадиган оверлокли (такрорланадиган) файллардир. Зарарланган бажариладиган файллардаги вирус шу вирус жойлашган дастур ишга туширилганда ўзининг ишини бошлайди. Вирус билан зарарланишнинг энг хавфлиси DOS буйруқли процессорини-COMMAND.COM дастурини зарарланишидир, чунки бу вирус DOS нинг исталган буйруғи бажарилганда ишлайди ва исталган бажариладиган дастур зарарланади (агар вирус уни зарарлантира олса).

2. **Операцион тизимни юкловчиси ва қаттиқ дискни асосий юкловчи ёзуви.** Бу соҳаларни бузадиган, қоидага кўра, икки қисмдан ташкил топган бўлади, чунки ушбу катта бўлмаган қайд қилинган диск соҳаларида вирус дастурини бутунлай жойлаштириш мушкулдир. Уларга сиғмайдиган вирус қисми, “бузилган” деб эълон қилинадиган, дискнинг бошқа қисмида жойлашади. Бундай вирус операцион тизим бошланғич юкланганда ўзининг ишини бошлайди ва резидент бўлиб қолади, яъни компьютер хотирасида доимий жойлашади.

3. +урилмаларнинг драйверлари, яъни CONFIG.SYS файлининг Device қилишда кўрсатиладиган файллар. Уларда жойлашган вируслар ҳар сафар мос қурилмага мурожаат қилганда ўзининг ишини бошлайди.

4. DOC тизимининг тизимли файллари (MS DOS да улар IO.SYS ва MSDOS.SYS деб аталади, PS DOS да - IBMBIO.COM ва IBMDOS.COM, DR DOSда эса - DRBIOS.SYS ва DRDOS.SYS деб аталади). Бу файлларнинг зарарланиши эҳтимоли камроқдир, лекин назарий жиҳатдан мумкиндир, чунки улар дискнинг узлуксиз қисмида, файлларни жойлаштириш учун ажратилган бошланғич қисмида, жойлашиши керак. Шунинг учун бу файлларга вирусларни жойлашиши учун, IO.SYS ва MSDOS.SYS файлларидан кейин келадиган бошқа файллар банд қиладиган жойни дискда бўшатиш керак, бу эса етарлича мураккабдир. +оидага кўра, вируснинг ҳар бир маълум тури файлларнинг фақатгина битта ёки иккита типини зарарлантириши мумкин. Кўпрок .COM файлларни зарарлантирадиган вируслар учрайди, тарқалиши бўйича иккинчи ўринда-.EXE файлларни ҳам зарарлантирадиган вируслар учрайди. Баъзида компьютерлар дискеталарнинг юкланадиган секторлари орқали тарқатиладиган вируслар билан зарарлантирадилар.

2. Компьютер вирусларини таснифланиши

Ҳозирги вақтда 60000 тадан ортиқ дастурли вируслар маълумдир. Уларни қуйидаги белгилар бўйича таснифлаш мумкин:

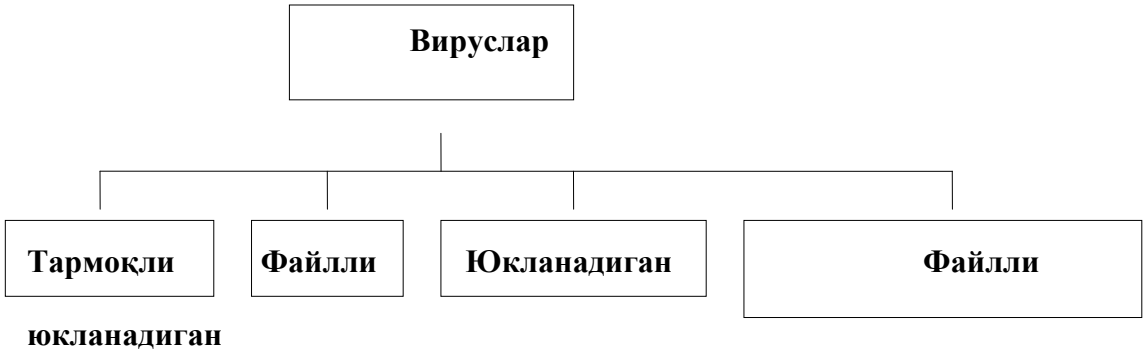
а) яшаш муҳити бўйича;

б) зарарлантириш усули бўйича;

в) таъсир этиши бўйича;

г) алгоритмнинг хусусиятлари бўйича;

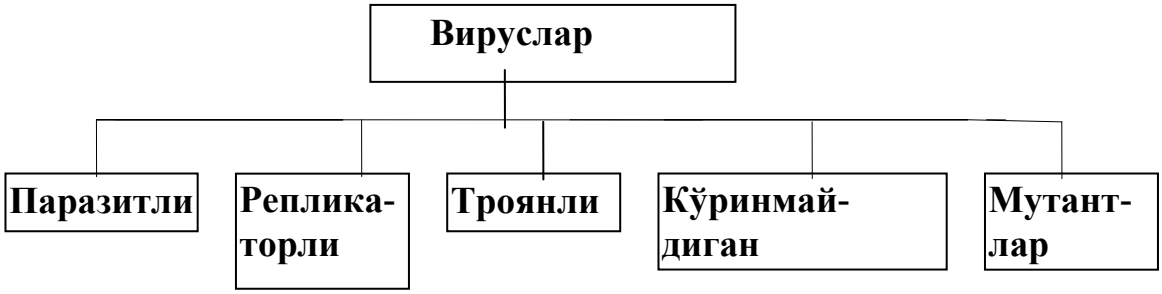
А) Яшаш муҳити бўйича вирусларнинг таснифлаши



Б) Зарарлантириш усули бўйича вирусларнинг таснифланиши

В) Таъсир этиш даражаси бўйича вирусларнинг таснифланиши

Г) Алгоритмларнинг хусусиятлари бўйича вирусларнинг таснифланиши



Яшаш муҳитига боғлиқ равишда вирусларни тармоқли, файлли, юкланадиган ва файлли-юкланадиган турларга бўлиш мумкин.

Тармоқли вируслар турли компьютер тармоқлари бўйича тарқаладилар. Дискетадан эмас, балки локал ёки глобал тармоқдан тарқатиладиган бу вируслар бажарадиган

дастурларни зарарлантирмайдилар. Улар ҳимоя қилишнинг тармоқ воситалари орқали кириб олиш учун мослашгандирлар ва тармоқда юқори тарқалиш тезлигига эгадир.

Тармоқли вирусларнинг энг кенг тарқалган тури **компьютер "чувалчанглари"** ҳисобланади, улар дастурли коднинг "бошқа жинсли" қисми бўлиб, компьютер тармоғини барча участкаларида юқори тезликда тарқаладилар.

Компьютер "чувалчанглари" тизимнинг жиддий бузилишларига олиб келмайди. Вирус "чувалчанг" сифатида Worm дастурини келтириш мумкин, у ўзининг нусхаларини тарқатиш учун ўзининг дастурли кодини Интернет тармоғи бўйича электрон хабарларга иловалар кўринишида жўнатади. Бу вирус бажариладиган HAPPУ99. EXE файлида жойлашади.

Файлли вируслар асосан бажариладиган модулларга, яъни .COM ва .EXE кенгайтмаларга эга бўлган файлларга, тадбиқ қилинади. Файлли вируслар бошқа турдаги файлларга ҳам тадбиқ қилиниши мумкин, лекин бунда улар бошқаришни узатадилар, ва, демак, кўпайиш қобилиятини йўқотадилар. Файлли вируслар компьютердан компьютерга файлларда кўчиб ўтадилар ва юқори зарарлантириш хоссасига эга.

Зарарланган дастурни ҳар сафар ишга туширилганда вируснинг ўз-ўзини нусхалаши бўлиб утади.

Юкланадиган вируслар- дискнинг юкланадиган секторига (Boot сектор) ёки тизимли дискни юклаш дастурини ўз ичига олган секторга (Master Boot Record) тадбиқ қилинади. Улар файлли вируслардан шуниси билан фарқланадики, тизимдан тизимга юкланадиган сектор орқали кўчиб ўтади ва дискеталарни ва қаттиқ дискларни фақат Boot-секторларини зарарлантиради. Бу вирусли дастурлар кичик ўлчамларга эга (512 байтдан ошиқроқ).

Файлли юкланадиган вируслар - файлларни ҳам, дискларнинг юкланадиган секторларини ҳам зарарлантиради. Бу турдаги вирусларни яратиш учун одатда мураккаб алгоритмлар ва технологиялар ишлатилади.

Зарарлантириш усули бўйича вируслар резидентли ва резидентли бўлмаган бўлади.

Резидентли вирус компьютерни зарарлантирганда тезкор хотирада ўзининг резидентли қисмини қолдиради, бу қисм кейин операцион тизимни зарарланган объектларга (файлларга, дискларнинг юкланадиган секторларига) мурожаатини ушлаб олади ва уларга тадбиқ қилинади. Резидентли вируслар хотирада жойлашади ва компьютерни ўчиргунгача ёки қайта юклагунгача актив ҳисобланади.

Резидентли бўлмаган вируслар компьютер хотирасини зарарлантирмайдилар ва чегараланган вақт ичида актив ҳисобланади.

Таъсир этиш даражаси бўйича вирусларни қуйидаги кўринишларга бўлиш мумкин

1. Хавфсиз - улар компьютер ишлашига ҳалақит бермайдилар, лекин бўш тезкор хотирани ва дисклардаги хотираларни сиғимини камайтиради, бундай вирусларнинг ишлаши бирорта графикли ёки товушли самараларда намоён бўлади.

2. Хавфли - улар компьютер ишлашида турли бузилишларга олиб келиши мумкин.

3. Жуда хавфли - уларнинг таъсирида дастурлар йўқолади, маълумотлар ўчиб кетади, дискнинг тизимли соҳаларидаги ахборотлар ўчирилиб юборилади.

Алгоритмнинг хусусиятлари бўйича вирусларни уларнинг турли-туманлигини катталиги туфайли таснифлаш мушкулроқдир.

Паразитли вируслар оддийроқдир, улар файлларнинг ва диск секторларининг мазмунини ўзгартирадилар, ва етарлича енгил пайқалиши ва йўқотилиши мумкин.

Чувалчанглар деб аталадиган **вирус репликаторларни_**таъ-кидлаш керак, улар компьютер тармоқлари бўйича тарқаладилар, тармоқ компьютерларининг адресларини ҳисоблайдилар ва бу адреслар бўйича ўзларининг нусхаларини ёзадилар.

Стелс-вируслар деб аталадиган **кўринмайдиган вируслар** маълумдир, уларни пайқаш ва зарарлантириш жуда мушкулдир, чунки улар операцион тизимни зарарланган

файлларга ва диск-ларнинг секторларига мурожаат қилишни ушлаб оладилар ва ўзининг танасини ўрнига дискнинг зарарланмаган қисмларини қўяди.

Шифрлаш-қайта шифрлаш алгоритмларини ўз ичига олган вирус-мутантларни пайқаш жуда мушкулдир, шу алгоритмлар ҳисобига бир хил вируснинг нусхалари битта ҳам такрорланмайдиган байтлар занжирига эга эмас.

Квазивирусли ёки **“троянли”** дастурлар деб аталадиган вируслар ҳам мавжуддир, улар ўз-ўзидан тарқалиш хоссасига эга бўлмасаларда, лекин жуда хавфлидир, чунки улар фойдали дастур остида ниқобланиб, юкланадиган секторни ва дискларнинг файлли тизимини бузадилар.

3. Компьютер вирусларидан ҳимоя қилиш усуллари

Компьютер вирусларидан ҳимоя қилишнинг учта чегараси мавжуддир:

-вирусларни кириб келишини бартараф этиш;

-агар вирус барибир компьютерга кирган бўлса, вирус ҳужумини бартараф этиш;

-агар ҳужум барибир амалга ошган бўлса, бузувчи оқибатларни бартараф этиш.

Ҳимоя қилишни амалга оширишни учта усули мавжуддир:

-ҳимоя қилишнинг дастурли усуллари;

-ҳимоя қилишнинг аппаратли усуллари;

-ҳимоя қилишнинг ташкилий усуллари.

Муҳим маълумотларни ҳимоя қилиш масаласида кўпинча маиший ёндашиш ишлатилади: “касалликни даволагандан кўра унинг олдини олган яхшироқ”. Афсуски, айнан у энг бузувчи оқибатларни келтириб чиқаради. Компьютерга вирусларни кириб олиш йўлида баррикадаларни яратиб олиб, уларнинг мустахкамлигига ишониб ва бузувчи ҳужумдан кейинги ҳаракатларга тайёр бўлмасдан қолмаслик керак. Шу билан бирга, вирусли ҳужум - бу муҳим маълумотларни йўқотишни ягона бўлмаган ва хаттоки кенг тарқалмаган сабабидир. Шундай дастурли узилишлар мавжудки, улар операцион тизимни ишдан чиқариши мумкин, ҳамда шундай аппаратли узилишлар борки, улар қаттиқ дискни ишлашга лаёқатсиз қилиб қўйиш қобилиятига эгадирлар. Ўғрилаш, ёнғин ёки бошқа фавқулодда ҳолатлар натижасида муҳим маълумотлар билан биргаликда компьютерни йўқотиш эҳтимоли ҳар доим ҳам мавжуддир. Шунинг учун хавфсизлик тизимини яратишни биринчи навбатда “охиридан” бошлаш керак - исталган таъсирни, у вирус ҳужуми, хонада ўғрилик ёки қаттиқ дискни физик ишдан чиқиши бўлишидан қатъий назар, бузувчи оқибатларини бартараф этишдан бошлаш керак.

Маълумотлар билан ишончли ва хавфсиз ишлашга фақат шундагина эришиладики, агар исталган кутилмаган ҳодиса, шу жумладан компьютерни тўлиқ физик ишдан чиқариш ҳам, халоқатли оқибатларга олиб келмаслиги керак.

Вирусга қарши ҳимоя қилиш воситалари

Ахборотни ҳимоя қилишнинг асосий воситаси энг муҳим маълумотларни заҳирали нусхалаш ҳисобланади. Юқорида санаб ўтилган сабабларнинг исталгани бўйича ахборотни йўқотиш ҳолатида қаттиқ дисклар қайта форматланади ва янгидан ишлатишга тайёрланади. ”Тоза” форматланган дискка дистрибьютив ихчам-дискдан операцион тизим ўрнатилади, кейин эса унинг бошқаруви остида барча керакли дастурли таъминот ўрнатилади, уларни ҳам дистрибьютив ташувчилардан олинади. Компьютерни тиклаш заҳирадаги ташувчилардан олинадиган маълумотларни тиклаш билан якунланади.

Маълумотларни заҳиралашда яна шуни инобатга олиш керакки, барча рўйхатдан ўтган ва паролли маълумотларни, Интернетнинг тармоқли хизматларига мурожаат қилиш учун, алоҳида сақлаш керак. Уларни компьютерда сақламаслик керак. Одатдаги сақлаш жойи - бўлим рахбарининг сейфидаги хизмат кундалигидир. Ахборотни заҳирали нусхалаш бўйича тадбирлар режасини тузиб олиб заҳирали нусхалар компьютердан алоҳида сақланиш кераклигини инобатга олиш керак. Яъни масалан, уша компьютернинг алоҳида қаттиқ дискида ахборотни заҳиралаш фақатгина хавфсизлик иллюзиясини яратади.

Муҳим, лекин махфий бўлмаган маълумотларни нисбатан янги ва етарлича ишончли усули уларни Интернетда узоклашган серверларда Web-папкаларда сақлаш ҳисобланади. Фойдаланувчи маълумотларини сақлаш учун бўш жойни (бир неча Мбайтгача) текинга берадиган хизмат турлари мавжуддир.

Махфий маълумотларни заҳирали нусхаларини сейфда сақланадиган ташқи ташувчиларда, иложи борича алоҳида биноларда, сақланади. Заҳирали нусхалашни ташкилий режасини ишлаб чиқишда турли жойларда сақланадиган, иккитадан кам бўлмаган заҳирали нусхаларни яратиш кераклигини инобатга олиш керак. Нусхалар ўртасида **ротация** амалга оширилади. Масалан, хафта давомида ҳар куни заҳирали А комплектнинг ташувчиларга маълумотларни нусхалайди, бир хафтадан кейин эса уларни Б комплект билан алмаштириладилар, ва х.к.

Ахборотни ҳимоя қилишнинг ёрдамчи воситалари вирусга қарши дастурлар ва аппаратли ҳимоя қилиш воситалари ҳисобланади. Масалан, бош платада уланиш жойини оддийгина ўчириб қўйиш ДЭ++ сини қайта дастурланадиган (флэш - BIOS) микросхемасини ўчиришни амалга ошириш имконини бермайди, бунда бу ишни ким амалга оширишига: компьютер вирусими, ёмон ниятли одамми ёки тартибсиз фойдаланувчими, боғлиқ эмасдир.

Вирусга қарши ҳимоя қилишнинг етарлича кўп дастур воситалари мавжуддир.

Вирусдан ҳимоя қилиш учун ишлтиш мумкин:

-ахборотни ҳимоя қилишнинг умумий воситалари, улар магнит дискларини физик бузишдан кафолатлаш, каби, нотўғри ишлайдиган дастурлар ёки фойдаланувчиларнинг нотўғри ҳаракатлари каби фойдалидир;

-вирус билан зарарланиш эҳтимолини камайтириш имконини берадиган профилактик чоралар;

-вируслардан ҳимоя қилиш учун махсус дастурлар.

Ахборотни ҳимоя қилишни умумий воситалари нафақатгина вирусдан ҳимоя қилиш учун фойдали эмас. Бу воситаларнинг иккита асосий тури мавжуддир:

-ахборотни нусхалаш-файлларнинг ва дискларнинг тизимли соҳаларини нусхаларини яратиш;

-мурожаат қилишни чеклаш-ахборотни рухсат этилмаган ишлатишни бартараф этиш, хусусан, вируслардан дастурларни ва маълумотларни ўзгаришлардан ҳимоя қилишдан, нотўғри ишлайдиган дастурлардан ва фойдаланувчиларнинг нотўғри ҳаракатларидан ҳимоя қилишдан.

Ахборотни ҳимоя қилишни умумий воситалари вируслардан ҳимоя қилиш учун жуда муҳимлигига қарамасдан, уларнинг ўзлари етарли эмас. Вируслардан ҳимоя қилиш учун махсус дастурларни қўллаш ҳам керакдир.

Бу дастурларни бир нечта турларга бўлиш мумкин: детекторлар, вакцина (иммунизаторлар), докторлар (ораш), тафтишчилар (файлларда ва дискларнинг тизимли соҳаларида ўзгаришларни назорат қилиш дастурлари), доктор-тафтишчилар ва фильтрлар (вируслардан ҳимоя қилиш учун дастурлар).

Вируслардан компьютерларни ва маълумотларни хавфсизлигига хисса қўшиш бўйича бирин ўрин, шубхасиз, **маълумотларни нусхалаш,** ҳисобланади. Вирус билан компьютер зарарланганда ҳали ҳам ҳеч бўлмаганда маълумотларнинг бир қисмини тиклаш мумкин, лекин агар компьютерда қаттиқ диск бузилса, унда нима қилмоқ керак? Бундан ташқари, нусхалари архивда мавжуд бўлган дастурлар ва маълумотлар исталганча бузилганда, қўшимча уларни турли “докторлар” билан даволашни амалга оширишга интилмасдан, архивдан тўғри нусхаларини нусхалаш мақсадга мувофиқдир.

Хавфсизликка ҳисса қўшиш бўйича иккинчи ўринга **маълумотларга мурожаат қилишни чеклашни** қўйиш мумкин. Агар аксарият кўпчилик ишлатиладиган дастурлар тўплами ёзишдан ҳимоя қилинган мантикий дискда жойлашган бўлса, унда вирус билан зарарланганда бу тўпламлар бузилмайдилар ва зарарланиш оқибатларини бартараф этиш учун нисбатан кам уринишлар талаб этилади.

Дастур-тафтишчилар (вирус билан зарарланишни олдиндан пайқаш) учинчи ўринда турадилар, улар дастурларнинг ва маълумотларнинг бутунлигини аниқлайдилар. Бундай текшириш вируснинг борлигини, у ҳам кўп нарсаларни бузишга улгурмасдан олдин, энг бошланғич босқичда пайқаш имконини беради.

Дастур фильтрлар тўртинчи ўринда турадилар. Бу дастурлар кўплаб вирусларни (ҳаммасини бўлмаса ҳам), улар хали кўп нарсаларни бузишга ёки зарарлантиришга улгурмасдан олдин, энг бошланғич босқичда пайқаш имконини беради. Antivirus ва Flu Shot Plus туридаги дастурлар дастур-фильтрларга тегишлидир.

Дастур-детекторлар бешинчи ўринда турадилар, улар янги олинган дастур таъминотида вирусларнинг мавжудлигини текшириш учун ишлатилади.

Дастур-докторлар (фаглар) олтинчи ўринда (умуман биринчида эмас) жойлашган. Уларни, бузилган дастурни нусхаси архивда бўлмаганда, ва уни бошқа усул билан олиш қийин бўлган ҳоллардагина қўллаган маъқулроқ. Бундан ташқари, агар дастур-фаг ишлатилаётган бўлса, унда кейин тикланган файлни дастур-тафтишчи билан албатта текшириш керак бўлади (тушунарлики, агар бу файл тўғрисидаги ахборот олдиндан сақланган бўлса), лекин ҳар доим ҳам дастур-доктор тўғри даволайвермайди.

Ва ниҳоят, энг охирги ўринда **доктор-вакциналар** жойлашган. Дунёда минглаб вируслар мавжуд бўлган шароитларда айнан компьютер зарарланадиган вирусдан файлни ҳимоя қилиш эҳтимоли жуда ҳам кичкинадир. Ва бундан ташқари, дастурни ёзувдан ҳимоя қилинган дискетага жойлаштириш янада самаралироқдир.

Жуда кўп фойдаланувчилар таъкидламоқдаларки, вируслардан ҳимоя қилиш учун вирусларни пайқайдиган ва уларни йўқотадиган дастурларни иложи борича кўпроқ (яъни дастур-детекторларни ва докторларни) йиғиш керак, ҳимоя қилишнинг бошқа чораларини инобатга олмаслик мумкин: вирус қачон пайдо бўлса, унда бу дастурлардан тўғри келадиган “дорини” танлаш балки мумкин бўлади. Шу билан бирга вирусдан келадиган зарарни камайтириш учун тиббиёт ходимлари қадимдан гапириб келаётган қоидага риоя қилиш керак: «касални даволагандан кўра унинг олдини олган яхшироқ».

Вирус билан зарарланишга қарши профилактика

Бу параграфда компьютерни вирус билан зарарланиш эҳтимолини камайтириш, ҳамда, агар барибир вирус билан зарарланиш бўлиб ўтган бўлса, ундан келадиган зарарни минимумга олиб келиш чоралари кўриб чиқилади. Албатта, вирус билан зарарланишга қарши профилактика учун кўриб чиқилган барча воситаларни эмас, балки фақатгина сиз керакли деб ҳисобланган воситаларнигина ишлатиш керак.

1. Ўзгартирмайдиган файлларни ўзида сақлаган дискеталарда ёзувдан ҳимоя қилувчи кесилган жойини елимлаб қўйиш керак. қаттиқ дискда ёзувдан ҳимоя қилинган мантикий дискни яратиш ва унга ўзгартирилмасдан, фақат ишлатиладиган дастурларни ва файлларни жойлаштириш керак.

2. Вирусдан ҳимоя қилиш учун резидентли дастур-фильт-рларни ёки доимо, ёки бу мумкин бўлган ҳамма вақтда ишлатиш мақсадга мувофиқдир.

3. Дискеталарнинг юкланадиган секторлари орқали тарқаладиган вирус билан зарарланишдан халос бўлиш учун қаттиқ дискдан компьютерни қайта юклашдан олдин А: дисководда бирорта дискета йўқлигига ишонч ҳосил қилинг. Агар у ерда дискета бор бўлса, унда қайта юклашдан олдин дисковод эшигини очиб қўйинг.

4. Агар сиз компьютерни дискетадан қайта ишлашни хохласангиз, фақатгина операцион тизимли ёзишдан ҳимоя қилинган “эталон” дискетадан фойдаланинг.

5. DOS бошланғич юкланганда бажариладиган AUTOEXEC.BAT буйруқли файлига, параметр сифатида файлларнинг унча катта бўлмаган рўйхатини кўрсатган ҳолда, файлларда ўзгаришларни текшириш учун дастур-тафтишчини чақиришни қўйиш мақсадга мувофиқдир.

6. Сиз яратган ёки ўзгартирган файлларни даврий равишда архивлаш керак. Файлларни архивлашдан олдин, компьютерда вирус йўқлигига ишонч ҳосил қилиш ва

архивга бузилган ёки зарарланган файлларни жойлашишидан халос бўлиши учун, вирус борлигини аввалроқ диагностика қилиш учун дастурни бажариш мақсадга муваффиқдир.

7. Бошқа компьютерлардан дастур таъминотини кўчириб ёзиш керак эмас, чунки у вирус билан зарарланган бўлиши мумкин.

8. Сиз бирорта дастур махсулотини ёки ҳужжатни олганингиздан ёки ишлаб чиққанингиздан кейин мос файлларнинг эталонли архивли нусхасини яратиш керак, унинг ёрдамида бу файлларни компьютер вирус билан зарарланганда енгилгина тиклаш мумкин бўлади.

9. Ташқаридан олиб келинган дискеталарни ишлатишдан олдин дастур-детектор ёрдамида вирус борлигига текшириш керак. Буни хаттоки, сиз бу дискеталарда фақатгина маълумотли файлларни ишлатишни истаган ҳолатларингизда ҳам фойдалидир - сиз вирусни қанчалик тез пайқасангиз, шунчалик яхшидир.

10. Компьютерда ишлашга беона шахсларни, айниқса агар улар ўзларининг дискеталарига эга бўлмасалар, қаровсиз қолдирмасдан рухсат бермаслик керак. Жуда кўп ҳолларда компьютерни вирус билан зарарланиш сабаби дискетада олиб келинган, кимдир уни компьютерда 10-15 минут ўйнаган компьютер ўйини ҳисобланади. Агар компьютерга тасодифий шахсларни мурожаат қилишдан халос бўлишнинг имкони бўлмаса (масалан, ўқув марказида), компьютернинг қаттиқ дискида жойлашган барча ёки деярли барча дастурларни ёзишдан ҳимоя қилинган дискда жойлаштирилган мақсадга мувофиқдир.

11. Агар компьютер қаттиқ дискда эга бўлса, ҳар доим ишончли жойда “тизимли” дискетага, яъни DOS операцион тизимини юклаш мумкин бўлган дискетага эга бўлиш керак.

12. Турли компьютер вирусларни пайқаш ва йўқотиш учун дастурларни йиғиб бориш керак. Бу дастурларни ишончли жойда сақланиш керак бўлган дискетага жойлаштириш керак. Бу дискета билан биргаликда уни ишлатиш бўйича йўриқномани сақлаш мақсадга мувофиқдир. Дастурларни танлаб олишда “миқдор сифатни алмаштирмайди” деган қоидани ёддан чиқармаслик керак ва фақатгина:

-ўзига яхши тавсиянома берган;

- вирусларнинг кенг диапазонига ёки бошқа дастурлар билан “ушлаб олинмайдиган” вирусларга мўлжалланган;

-ўзларида вируслар йўқлигига текширилган дастурларнигина йиғиш керак

4. Вирусларни пайқаш ва улардан ҳимоя қилиш дастурлари. Уларнинг ва тавсифлари.

Компьютер вирусларини пайқаш, ўчириш ва улардан ҳимоя қилиш учун махсус дастурларнинг бир нечта турлари ишлаб чиқилган, улар вирусларни пайқаш ва йўқотиш имконини беради. Бундай дастурлар **вирусга қарши** дастурлар деб аталади.

Вирусга қарши дастурларнинг қуйидаги турлари мавжуд:

1) дастур-детекторлар;
2) дастур-докторлар ёки фаглар;
3) дастур-тафтишчилар;
4) дастур-фильтрлар;
5) дастур-вакциналар ёки иммунизаторлар.

Вирусга қарши дастурларнинг турлари

Дастур-детекторлар маълум бир вирус учун тавсифли бўлган байтлар кетма-кетлигини (вирус сигнатуралари) тезкор хотирада ва файлларда қидиришни амалга оширилади, ва вирусни пайқаганда мос хабарни беради. Бундай вирусга қарши дастурларнинг камчилиги шундаки, улар фақат бундай дастурларнинг ишлаб чиқувчиларига маълум бўлган вирусларнигина топа оладилар.

Дастур-докторлар ёки **фаглар,** ҳамда **дастур-вакциналар** нафақатгина вируслар билан зарарланган файлларни топмасдан, балки уларни “даволайди” ҳам, яъни файлдан дастур-вирус танасини ўчирадилар, файлларни бошланғич ҳолатга қайтарадилар. Фаглар ўзининг ишини бошида тезкор хотирада вирусларни қиди-ради, уларни йўқотади ва фақат кейингина файлларни “даволашга” ўтади. Фаглар орасида **ярим фагларни** ажратиш мумкин, улар катта миқдордаги вирусларни қидириш ва йўқотиш учун мўлжалланган дастур-докторлардир. **Aidstest, Scan, Norton Antivirus** ва **Doctor Web** энг машҳур полифаглар ҳисобланадилар. Янги вируслар доимо пайдо бўлиб боришини инобатга олиб, дастур-детекторлар ва дастур-докторлар тезда эскирадилар, ва уларнинг версияларини доимо янгилаб бориш талаб этилади.

Дастур-тафтишчилар вируслардан ҳимоя қилишнинг энг ишончли усулларига тегишлидир. Тафтишчилар, компьютер вирус билан зарарланмаганда, каталогларнинг дастурларини ва дискнинг тизимли соҳаларини бошланғич қийматини эслаб қоладилар, кейин эса даврий равишда ёки фойдаланувчининг хохиши бўйича жорий ҳолатни бошланғич ҳолат билан таққослайди. Пайқалган ўзгаришлар видеомонитор экранига чиқарилади. +оидага кўра, ҳолатларни тақ-қослаш опкрацион тизим юклангандан кейин бирданига амалга оширилади. Таққослашда файл узунлиги, циклик назорат қилиш коди (файлнинг назорат йиғиндиси), ўзгартириш санаси ва вақти, бошқа параметрлар текширилади. Дастур-тафтишчилар етарлича ривожланган алгоритмларга эга, стелс-вирусларни пайқайдилар, ва ҳаттоки текширилаётган дастур версияларини ўзгаришларини вирус томонидан киритилган ўзгаришлардан фарқини пайқайдилар.

Россияда кенг тарқалган **“Диалог-Наука”** фирмасининг **Adinf** дастури дастур-тафтишчилар қаторига киради.

Дастур-фильтрлар ёки “қоровуллар”-бу, компьютер ишлашида вируслар учун тегишли бўлган шубоали ҳаракатларни пайқаш учун мўлжалланган, унча катта бўлмаган резидентли дастурлардир. Бундай ҳаракатлар бўлиши мумкин:

1) .COM ва .EXE кенгайтмали файлларни тўғрилашга интилишлар;

2) файллар атрибутларини ўзгартириш;

3) абсолют адрес бўйича дискка тўғридан тўғри ёзиш;

4) дискнинг юкланадиган секторларига ёзиш;

5) резидент дастурни юклаш.

Бирор дастур томонидан кўрсатилган амалларни бажаришга интилиш бўлганда “қоровул” фойдаланувчига хабар юборилади ва мос амалларни таъқиқлашни ёки рухсат беришни таклиф этади. Дастур-фильтрлар жуда фойдалидир, чунки улар вирусни уни пайдо бўлишини бошланғич босқичларида, кўпайгунга кадар пайқаш қобилиятига эгадир. Аммо улар файлларни ва дискларни “даво-ламайдилар”. Вирусларни йўқотиш учун бошқа дастурларни, масалан фагларни, қўллаш талаб этилади. Дастур-қоровулларнинг камчиликларига уларнинг жонга тегишини “(масалан, улар бажарилаётган файлни нусхалашга ихтиёрий интилиш тўғрисида доимо огоҳлантириб турадилар), ҳамда бошқа дастур таъминоти билан мумкин бўлган келишмовчиликларни келтириш мумкин. Дастур-фильтрга мисол тариқасида MS DOS операцион тизимининг утилитларини тўпламини таркибига кирувчи **Vsafe** дастурини келтириш мумкин.

Вакциналар ёки иммунизаторлар - бу файлларни зарарланишини бартараф этувчи резидентли дастурдир. Вакциналарни вирусни “даволайдиган” дастур докторлар йўқ бўлганда қўлланилади. Вакциналаш фақатгина маълум бўлган вируслардан мумкиндир. Вакцина дастур ёки дискни шундай ўзгартирадики, бу уларнинг ишлашида акс эттирилмайди, вирус эса уларни зарарланган деб қабул қилади ва шунинг учун тадбиқ этилмайди. Хозирги вақтда дастур-вакциналар чекланилган қўлланишга эгадирлар.

Вируслар билан зарарланган файлларни ва дискларни ўз вақтида пайқаш, ҳар бир компьютерда пайқалган вирусларни тўлиқ йўқотиш вирус эпидемиясини бошқа компьютерларга тарқалишини олдини олиш имконини беради.

5. Компьютер вирусларидан ҳимоя қилиш учун асосий чоралар

Компьютерни компьютер вируслари билан зарарланишини олдини олиш ва дискларда ахборотларни ишончли сақлашни таъминлаш учун қуйидаги қоидаларга риоя қилиш керак:

-компьютерни замонавий вирусга қарши дастурлар, масалан Aidstest ёки Doctor Web, билан таъминланг ва уларнинг версияларини доимо янгилаб боринг;

-бошқа компьютерларда ёзилган ахборотларни дискетадан ўқишдан олдин ўзингизни компьютердаги вирусга қарши дастурни ишга тушириб бу дискеталарни вирус борлигига доимо текширинг;

-ўзингизни компьютерингизга архивланган кўринишдаги файлларни кўчириб ўтишда, текшириш соҳасини хозиргина ёзилган файллар билан чеклаган ҳолда, уларни қайта архивлангандан кейин тезда қаттиқ дискда текширинг;

-олдиндан ОТ ни ёзишдан ҳимоя қилинган тизимли дискетадан юклаб, файлларни, хотираларни ва тизимли соҳаларни ёзишдан ҳимоя қилинган дискетадан вирусга қарши дастурларни ишга тушириб компьютернинг қаттиқ дискларини вируслар борлигига даврий равишда текшириб боринг;

-бошқа компьютерда ишлаганда ўзингизни дискетани, агар уларга ахборотни ёзиш амалга оширилмаса, ёзишдан ҳар доим ҳимоя қилинг;

-Сиз учун муҳим бўлган ахборотларни архивли нусхаларини дискеталарда албатта яратинг;

-компьютерни юкланадиган вируслар билан зарарланишини олдини олиш учун операцион тизимни қайта юклашда ёки компьютерни улашда А: дисководда дискетани қолдирманг;

-компьютер тармоқларидан олинадиган барча бажарадиган файлларни назорат қилиш учун вирусга қарши дастурларни ишлатинг.

-Aidstest ва Doctor Web дастурларини қўллашни юқори хавф-сизлигини таъминлаш учун **Adinf** диск текширувчисини ҳар куни ишлатиб бориш керак.

1. “Диалог-наука” хиссадорлик жамиятини вирусга қарши тўплами

Компьютер вируслари билан курашишнинг кўплаб замонавий воситалари орасида “Диалог-наука” ҳиссадорлик жамиятини (ҲЖ) вирусга қарши тўплами устунликка эгадир, унга тўртта дастур махсулоти киради: **Aidstest** ва **Doctor Web** (қисқача Dr Web) полифаглари, диск тафтишчиси **Adinf** ва даволовчи **Adinf Cure Module** блоки. Бу вирусга қарши дастурларни қандай ва қачон қўлланишини қисқача кўриб чиқамиз.

A. Aidstest дастур - полифаг

Aidstest - бу жуда ҳам кенг тарқалган 1300 дан ортиқ компьютер вирусларини пайқаш ва йўқотиш имкониятига эга бўлган дастурдир. Aidstest версиялари янги вируслар тўғрисидаги ахборот билан доимий равишда янгиланиб ва тўлдирилиб бормокда.

Aidstest ни ишга тушириш учун қуйидаги буйруқни бериш керак:

Aidstest <path>[<options>]

бу ерда: **path** - диск номи, тўлиқ ном, файл спецификацияси, файллар гурухининг ниқоби:

*- қаттиқ дискнинг барча бўлимлари

**- тармоқ ва CDROM дискларини қўшган ҳолда барча дисклар.

Options - қуйидаги калитларнинг исталган комбинацияси:

F- зарарланган дастурларни тўғрилаш ва бузилганларини ўчириш;

G- барча файлларни кетма-кет текшириш (фақатгина .COM, .EXE ва SYS ларни эмас);

H- бузилган вирусларни қидириш учун ctkin ишлаш;

X- вирус структурасида бузилишлар бўлган барча файлларни ўчириш;

Q- бузилган файлларни ўчиришга рухсат сўраш;

R- кейинги дискектани қайта ишлашни таклиф этмаслик.

Мисол 1. **AISTEST B: /F/G/Q**

B: дискни “даволаш” ва текшириш учун вирусга қарши Aidstest дастурини ишга тушириш, пайқалган зарарланган дастурлар тўғриланади. Агар файлни тўғрилашга имкон бўлмаса, унда дастур уни ўчиришга рухсат сўрайди.

Doctor Web дастур-полифаг

Бу дастур, энг аввало, компьютер оламида нисбатан яқинда пайдо бўлган полиморфли вируслар билан курашиш учун мўлжалланган. Дискларни текшириш ва пайқалган вирусларни ўчириш учун мўлжалланган. Дискларни текшириш ва пайқалган вирусларни ўчириш учун Dr.Web ни ишлатиш Aidstest дастурига тўлиқ ўхшашдир. Бунда текширишни дубллаш деярли бўлмайди, чунки Aidstest ва Dr.Web дастурлари вирусларнинг турли тўпламлари билан ишлайдилар.

Dr.Web дастури Aidstest кучи етмайдиган мураккаб вируслар мутантлар билан самарали курашиши мумкин. Aidstest дан фарқли равишда Dr.Web дастури хусусий дастурли коддаги ўзгаришларни пайқаш, ҳамда “вакцинали беркитишни” енгиб ўтган ҳолда шифрланган ва ихчамлаштирилган файлларга кириб янги, ноъмалум вируслар билан зарарланган файлларни самарали аниқ-лаш қобилиятига эгадир. Бу кучли эвристик таҳлилчи мавжудлиги ҳисобига эришилади.

Эвристик таҳлил режимида Dr.Web дастури вируслар учун ҳарактерли бўлган янги ёки унга номаълум вирусларни пайқашга интилиб файлларни ва дискларнинг тизимли соҳаларини тадқиқот этади. Агар шундай вируслар топилса, унда объект номаълум вирус билан зарарланганлиги тўғрисида огоҳлантириш берилади.

Эвристик таҳлилни учта даражаси кўзда тутилган. Эвристик таҳлил режимида ёлғон ишлашлар, яъни зарарланмаган ҳисобланмаган файлларни детекторлаш мумкиндир. “Эвристика” даражаси ёлғон ишлашлар мавжудсиз кодни таҳлил қилиш даражаси кўринишига эгадир. Эвристик таҳлилчининг ишлашини биринчи иккита даражаси тавсия этилади.

Эвристик таҳлилни учинчи даражаси файлларни яратилишини “шубхали” вақтига уларни қўшимча текширишни кўзда тутади. Файллар зарарланишида баъзи бир вируслар ушбу файлларнинг зарарганлик белгиси каби яратилишнинг нотўғри вақтини ўрнатади. Масалан, зарарланган файллар учун секундлар 62 қийматга эга бўлиши мумкин, яратилиш йили эса 100 йилга кўпайтирилиши мумкин.

Вирусга қарши Dr.Web дастурини етказиб бериш таркибига яна унинг имкониятларини кенгайтирадиган дастурнинг асосий вирусли тўпламига файл қўшимчалар ҳам кириши мумкин.

Dr.Web дастури билан икки режимда ишлаш мумкин:

-меню ва мулоқот ойнасини ишлатиб тўлиқ экранли интерфейс режимида;

-буйруқ қатори орқали бошқариш режимида.

Бир марталик доимий бўлмаган қўллаш учун биринчи режим қулайроқдир, лекин дискеталарнинг доимий кириш назорат қилиш мақсадида доимий қўллаш учун яхшиси иккинчи режимини қўллаган маъқулдир.

Иккинчи режимни ишлатганда Dr.Web нинг мос ишга тушириш буйруғи Norton Commander операцион қобиғини фойдаланувчисини менюсига ёки махсус буйруқли файлга киритилган бўлиши мумкин.

Dr.Web ни ишга тушириш учун буйруқ қатори қуйидаги кўринишга эга:

Dr.Web [диск:] [йўл] [калитлар]

бу ерда **диск:** - қаттиқ дискни мантиқий қурилмаси ёки эгилувчан дискни физик қурилмаси, масалан, F: ёки A:

*- қаттиқ дискдаги барча мантиқий қурилмалар;

йўл - бу талаб этилаётган файлларнинг йўли ёки ниқоби.

Энг муҳим калитлар:

/ AL-берилган қурилмадаги барча файлларнинг диагностикаси;

/ CU [P] - дискларни ва файлларни “даволаш”, топилган вирусларни ўчириш;

P- фойдаланувчининг тасдиқлаши билан вирусларни ўчириш;

/ DL-тўғилаб даволашни имкони бўлмаган файлларни ўчириш;

/ HA [даража]- файлларни эвристик таҳлил қилиш ва уларда номаълум вирусларни қидириш, бу ерда [даража] 0,1,2 қийматларни қабул қилиш мумкин;

/ CL - буйруқли қатор режимида дастурни ишга тушириш, файлларни ва тизимли соҳаларни тестлашда тўлиқ экранли интерфейс ишлатилмайди;

/ QU- тестлашдан кейин тезда DOS га чиқиш.

Агар Dr.Web нинг буйруқли қаторида бирорта ҳам калит кўрсатилмаган бўлса, унда жорий сўров учун барча ахборот DRWEB. EXE жойлашган каталогда жойлашган DRWEB.INI конфигурация файлидан ўқилади. Конфигурация файли тестлаш учун зарур бўлган параметрларни сақлаш буйруғи ёрдамида Dr.Web дастури билан ишлаш жараёнида ишлатилади.

Мисол-2: **DrWeb B: / AL/ CUP/ HA1/QU/CL**

B: дискни текшириш ва даволаш учун Dr.Web вирусга қарши дастурини ишга тушириш.

Тўлиқ экранли интерфейс режимида Dr. Web дастури билан ишлаш технологияси

Тўлиқ экранли интерфейс режимида ишга тушириш учун буйруқ қаторига фақат дастур номини киритиш етарлидир. Дастур юклангандан кейин компьютернинг тезкор хотирасини тестлаш, агар у компьютернинг тезкор хотирасини тестлаш, агар у компьютернинг олдинги ўрнатилишида ўчирилмаган бўлса, бошланади. Тестлашнинг бориши тестлаш ойнасида акс эттирилади. Хотирани тестлаш тугагандан кейин тўхташ амалга оширилади. Дастур ишлашини, агар экраннинг юқори қаторида жойлашган асосий менюдан фойдаланилса, давом эттириш мумкин. Менюни активлаштириш учун F10 клавишини босиш керак. Асосий меню қуйидаги режимларга эга:

Dr.Web ТЕСТ НАСТРОЙКИ ДОПОЛНЕНИЯ

Исталган режимни танлашда мос қисмменю очилади.

Dr.Web қисмменюси DOS га вақтинчалик кириш, Dr.Web дас-тури ва унинг муаллифи тўғрисида қисқача ахборотни олиш ёки дастурдан чиқиб кетиш имконини беради.

ТЕСТ қисмменюси файлларни тестлашни ва “даволашни” асосий амалларини бажариш, ҳамда бажарилган ишлар тўғрисида ҳисоботларни кўриб чиқиш имконини беради.

Настройки қисмменюси мулоқот ойналари ёрдамида дастурни созлаш параметрларини ўрнатиш, қидиришни йўлларини ва ниқобларини ўрнатиш ва параметрларни DRWEB.INI конфигурация файлида сақлаш учун хизмат қилади.

ДОПОЛНЕНИЯ қисмменюси дастурнинг асосий вирусли базасига, унинг имкониятларини кенгайтирадиган файл-қўшимчаларни қўшиш учун ишлатилади.

Дискнинг вирусга қарши тафтишчиси Adinf

Adinf тафтишчиси стелс-вирусларни, вирус-мутантларни ва бугунги кунгача номаълум вирусларни қўшган ҳолда исталган вирусларни пайдо бўлишини пайқаш имконини беради.

Adinf дастури эслаб қолади:

- юкланадиган секторлар тўғрисидаги ахборотни;
- бузилган кластерлар тўғрисидаги ахборотни;
- файлларнинг узунлиги ва назорат йиғиндиларини;
- файлларни яратилиш санаси ва вақтини.

Компьютерни бутун ишлаши давомида Adinf дастури бу тавсифларни сақланганлиги кузатиб боради. Ҳар кунги назорат қилиш режимда Adinf дастури ҳар куни компьютер

биринчи марта уланганда автоматик равишда ишга туширилади. Айниқса вирусга ўхшаш ўзгаришлар кузатиб борилади, улар тўғрисида тезда огоҳлантириш берилади. Файлларни бутунлиги назорат қилишдан ташқари Adinf дастури қисмкаталогларни яратишни ва ўчиришни, файлларни яратишни, ўчиришни, силжитишни ва қайта номлашни, янги бузуқ кластерларни пайдо бўлишини, юкланадиган секторларини сақла-ганлигини ва кўплаб бошқа нарсаларни кузатади. Вирусни тизимга тадбиқ қилиш учун мумкин бўлган барча жойлар ёпиб қўйилади. Adinf дастури, DOS ни ишлатмасдан BIOS га тўғридан-тўғри мурожаат қилиб дискни секторлари бўйича ўқиган ҳолда текширади. Шу усул туфайли Adinf текширишлари ниқобланувчан стелс-вирусларни аниқлайди ва дискни текширишни юқори тезлигини таъминлайди.

Adinf Cure Module даволовчи блоки

Adinf Cure Module - бу компьютерни янги вирусдан “даво-лашга” ёрдам берадиган дастур бўлиб, у бу вирус маълум бўлган Aidstest ёки Dr.Web полифагларни янги версияларини кутиб турмайди. Adinf Cure Module дастури, вирусларни кўплаб турлари борлигига қарамасдан уларни файлларга тадбиқ қилишни унчалик кўп бўлмаган турлича усуллари мавжудлиги далилини ишлатади. Меъёрий ишлаш вақтида, доимий равишда ишга туширишда Adinf тафтишчиси Adinf Cure Module дастурига охирги марта ишга туширилгандан бери қайси файллар ўзгарганлиги тўғрисида хабар беради. Adinf Cure Module дастури бу файлларни таҳлил қилади ва ўзининг жадвалларига, вирус билан зарарланганда файлларни тиклаш учун керак бўладиган, ахборотни ёзиб қўяди. Агар зарарланиш бўлиб ўтган бўлса, унда Adinf тафтишчиси ўзгаришларни пайқайди ва Adinf Cure Module дастурини яна чақиради, у зарарланган файлни таҳлил қилиш ва уни ёзиб қўйилган ахборот билан тақ-қослаш асосида файлнинг бошланғич ҳолатини тиклашга ҳаракат қилади.

Дастур махсулотларини ҳимоя қилиш

Дастур маҳсулотлари бир қатор сабабларга кўра ҳимоя қилишнинг муҳим объекти ҳисобланади.

Биринчидан, улар юқори малакали мутахассисларнинг, баъзида ўнлаб ёки хаттоки юзлаб одамларнинг интеллектуал мехнати махсулоти ҳисобланади.

Иккинчидан, бу махсулотларни лойиҳалаш жараёни моддий ва мехнат ресурсларини сезиларли ҳаракатлари билан боғлангандир, қимматбахо компьютер жиҳозларини ва илмий - техникавий технологияларни ишлатишга асосланган.

Учинчидан, бузилган дастур таъминотини тиклаш анчагина мехнат сарфини талаб этади, ҳисоблаш техникаси жиҳозларини ишламай туриб қолиш эса ташкилотлар ва жисмоний шахслар учун нохуш натижаларга олиб келиши мумкин.

Дастур махсулотларини ҳимоя қилиш қуйидаги мақсадларни кўзда тутади:

- фойдаланувчиларнинг алоҳида тоифаларини дастур махсулотлари билан ишлаш учун рухсат этилмаган мурожаат қилишни чеклаш;
- маълумотларни қайта ишлашни меъёрда олиб бориш мақсадида дастурларни олдиндан режалаштирилган бузилишини инкор қилиш;
- дастур махсулотини ишлаб чиқарувчиларни нуфузини бузиш мақсадида дастурларни олдиндан режалаштирилган ўзгартирилишни инкор қилиш;
- дастурларни рухсат этилмаган ададлашни (нусхалашни) инкор қилиш;
- дастурларни мазмунини, структурасини ва ишлаш механизмини рухсат этилмаган ўрганишни инкор қилиш.

Дастур махсулотлари турлича объектларнинг одамни, техник воситаларни, махсус дастурларни, атроф муҳитни ва бошқаларни рухсат этилмаган таъсирларидан ҳимоя қилиниши керак.

Одамлар дастур махсулотига шу дастур махсулотини ҳужжатларини ёки машина ташувчисининг ўзини ўғрилаш ёки физик йўқотиш, дастур воситаларини ишлаш қобилиятини бузиш йўли билан таъсир этиши мумкин.

Техник воситалар (аппаратура) компьютерга ёки узатувчи муҳитга уланиш йўли билан дастурларни ўқиш, қайта шифрлаш, ҳамда уларни физик бузишни амалга ошириши мумкин.

Махсус дастурлар ёрдамида дастур махсулотини вирус билан зарарлантириш, уни рухсат этилмаган нусхалаш, унинг маъносини рухсатсиз ўрганиш ва амалга ошириши мумкин.

Ва нихоят, **атроф-муҳит** аномал ҳодисалар ёрдамида (электромагнит нурланишни кўпайиши, ёнғин, сув тошқини ва бошқалар.) дастур махсулотини физик бузиш амалга оширилиши мумкин.

Дастур махсулотларини ҳимоя қилишни энг оддий ва мумкин бўлган усули уларга қуйидаги усуллар билан мурожаат қилишни чеклаш ҳисобланади:

- дастурлар ишга тушганда уларни пароль билан ҳимоя қилиш;
- калит дискетани ишлатиш;
- компьютернинг киритиш - чиқариш портига уланадиган махсус техник қурилмани (электрон калитни) ишлатиш.

Дастурларни рухсат этилмаган нусхалашдан сақлаш мақ-садида ҳимоя қилишнинг махсус дастурли воситалари:

- дастур ишга тушириладиганмуҳитни идентификациялаш;
- рухсат этилган инсталляцияларни ва нусхалашларни бажарилишини миқдорини ҳисобини олиб бориш;
- тизимларнинг ишлаш алгоритмларини ва дастурларини ўрганишга қарши туриш (хаттоки ўз-ўзини бузишгача) керак.

Дастур махсулотлари учун самарали ҳимоя қилиш чоралари қуйидагилар ҳисобланадилар:

- ишга тушрадиган дискетани ностандарт шакллантириш;
- қаттиқ дискда дастурларни жойлашган жойини қатъий белгилаш;
- киритиш-чиқариш портига қўйиладиган электрон калитга боғланиш;
- BIOS номерига боғланиш ва бошқалар.

Дастур маҳсулотларини ҳимоя қилиш хуқуқий усуллар билан ҳам албатта амалга ошириши керак, уларнинг қаторига келишувлар ва шартномаларни, патентли ҳимоя қилишни, муаллифлик хуқуқини, технологик ва ишлаб чиқариш махфийлигини ва бошқаларни киритиш мумкин.

Вирус билан қуйидаги турдаги файллар зарарланиши мумкин:

- Бажарилувчи файллар**: COM** ва **EXE** кўринишидаги файллар.

-Файлларнинг зарарлайдиган вируслар файл вируслари дейилади. Бажарилувчи файллардаги вируслар шу файлга тегишли бўлган дастур ишлаганда ўз фаолиятини бошлайди.

- Операцион системанинг юкловчиси ва қаттиқ дискнинг асосий юкловчи ёзувлардан иборат файллар. Бу соҳаларни зарарлайдиган вируслар юкловчи ёки бут вируслар дейилади. Бундай вируслар компьютер юкланиши билан ишлай бошлайди ва у резидентлик ҳолатига ўтади, яъни доим компьютер хотирасида сақланади. **Тарқалиш механзми**- компьютерга қўйиладиган дискетларни юкловчи ёзувларини зарарланиши. Буларда жойлашган вируслар шу қурилмалар, қурилмалар драйверлари, яъни ҳар хил қурилмалар ишини таъминловчи дастурларга мурожат қила бошлаганда ишга тушади. Дискдаги файл системани ўзгартирадиган вируслар.

Одатда бундай вируслар **DIR** деб аталади. Бу вируслар дискнинг бирор бир соҳасида файлларнинг охири сифатида яширинадилар. Улар кўрсаткичлар бошини ёзув охирига олиб ўтиб қўяди ва **NDD** (Norton Disk Doktor) билан текширганда дискнинг бузулганлиги маълум бўлади.

Кўринмас ва ўзи дифференциалланувчи вируслар.

Кўп вируслар ўзини сездирмаслик учун системада **DOS** га мурожат қила

бошлаганда файлларни худди олдинги ҳолатидек ишланишини таъминлайдилар. Кўринмас вируслар шундай тарзда харакат қилади. Ўзи дифференциалланувчи вируслар эса ўз шаклини такомиллаштиради. Кўп вируслар бошқалар унинг ишлаш механзмини сезиб қолмасликлари учун ўзининг катта қисмини кодланган ҳолда сақлайди. Бу албатта бундай вирусларини топишда қийинчиликлар туғдиради.

BOOT-вируслар.

Баъзида дискетдан хеч нарса кўчирмасдан ҳам, ундан қандайдир дастурни юкламай туриб вирус билан зарарланиш мумкун. Масалан **STONE** ёки **MARS** каби вируслар мавжудки, улар компьютерни ёқишингиз билан ёки қайта юклаганингизда, ичида дискет қолиб кетган бўлса, зарар етказиши аниқ. Бундай вируслар **BOOT**-вируслар дейилади. **BOOT Sector**-.юкланувчи соха деган сўздан келиб чиққан. Компьютер ёқилиши билан дискет орқали юкланишга харакат қилади,агар компьютерда юкланиш дискети бўлмаса,бунинг уддасидан чиқа олмайди.Лекин дискет қандай бўлишидан қатъий назар,**BOOT**-вируслар компьютерни бемалол зарарлайди,шунинг учун эхтиёткорлик талаб қилинади.

Компьютер зарарланганда бирқанча ғаройиб ходисалар юз беради:

-Баъзи бир дастурлар ишламайди ёки ёмон ишлай бошлайди;

-Экранга бошқа ҳабарлар ёки символлар чиқа бошлайди;

-Компьютер ишлаш секинлашади;

-Баъзи бир файллар бузилади ёки уларнинг хажми ортиқча ҳар хил ёзувларни қўшиш ҳисобига ўзгаради, катталашади;

-Оператив хотиранинг бўш жойи қисқаради; системали дискетдан дастурларни юклаш қийинлашади, ёки умуман юкланмайди ва х.к.

Компьютер вирусларидан ҳимоялашнинг энг яхши ҳимоя тури-вирусларни қай тарзда таъсир этишини билишдир. Вируслар оддий дастурлар бўлиб, бирон ғароиб кучга эга эмаслар.

Компьютер вируслар билан зарарланиши учун ундаги бирон-бир зарарланган дастур ишлаши талаб қилинади. Шунинг учун компьютернинг бирламчи зарарланиши қуйидаги ҳолларда рўй беради:

-Компьютердаги вирус билан зарарланган дастурлар юкланиши (COM, BAT ёки EXE файллар) ёки модули зарарланган дастурни ишлатилиши;

-Компьютерга вирусли дискетнинг юкланиши;

-Компьютерга зарарланган **ОС** ёки қурилмаларнинг зарарланган драйверларнинг ўрнатилиши;

Вируслардан қуйидаги усуллар билан ҳимояланиши мумкин:

-Дискетдан ўқилаётганда албатта вирус борлигини антивируслар ёрдамида текшириш;

-Ахборот нусхаларини кўчириш шунингдек дисклар ва ахборотни сақлаш учун ишлатиладиган умумий қоидалардан фойдаланиш, дискларни жисмоний зарарланишидан, дастурларни эса бузилишидан сақлаш;

-Ахборотдан ноқонуний фойдаланишни чеклаш, хусусан дастур ва маълумотларни вируслар таъсиридан ўзгаришидан, нотўғри ишлатилган дастурлар ва фойдаланилувчиларнинг нотўғри харакатларидан ҳимоя қилиш;

-Вируслар билан зарарланиш эҳтимолини камайтирувчи чора-тадбирлар;

-Вируслар билан курашувчи махсус дастурлардан (антивируслар) фойдаланиш.

Вирусдан кўриладиган зарарларга қуйидагиларни мисол қилиб кўрсатиш мумкин:

- Компьютер қаттиқ диски ёки тезкор хотирасининг ифлосланиши-вируси дастур кўпайиши жараёнида бутун қаттиқ дискни ўзининг нуқталари ёки бошқа белгилари билан тўлдириши мумкин.
- Буларни у тезкор хотирага ҳам ёзиши ва шу билан унинг хажмини камайтириши мумкин;

- Файллар жойлашиш жадвалининг бузилиши. У бузилса, дискдан керакли файл ва катологни ўқиш мумкин бўлмайди;
- Юкланиш секторидаги маълумотларнинг бузилиши. Юкланиш сектори дискдаги махсус дастур бўлиб, унинг бузилиши диск ишини тўхтатиб қўяди;
- Дискни қайта форматлаш-дискдаги барча ахборот бутунлай йўқолади;
- Дискка бирон хабар чиқариши ёки бирон куйни ижро этиши мумкин. Кўп холларда бу хабар тушунарсиз бўлади;
- Компьютернинг ўз-ўзидан қайта юкланиши;
- Тугмачалар мажмуи ишни тўхтатиб қўйиши;
- Дастурли ва маълумотли файллар мазмунининг ўзгариши.

Вирус маълумотларини иҳтиёрий равишда аралаштириб қўяди.

Оддий вирусдан зарарланишни вирусга қарши дастурлар ёрдамида осон аниқлаш мумкин,(мураккаб тузилишга эга) вирусларни бу усул билан аниқлаш қийин, чунки улар ўз-ўзини нусхалашда кўринишини ўзгартиради. Макрослар билан ишлайдиган иловалар макровируслар билан зарарланиши мумкин. Макровируслар-маълумот билан бирга ўргатиладиган буйруқлардир. Бундай иловаларга мисол қилиб, **WORD, EXCEL** ва **POSTSRIPTER** интерпроекторларини кўрсатиш мумкин.

Улар маълумотлар файлини очаётганида макровирус билан зарарланади.

Илгари фақат дисклар вирус билан зарарланар эди. Чунки вируслар дисклар орқали компьютердан компьютерга ўтар эди. Янги **BBS** вируслари эса модем орқали тарқаладиган бўлди. Интернетнинг пайдо бўлиши вирусларга қарши курашнинг анъанавий усуллари фойда бермайдиган яна битта каналнни ҳосил бўлишига олиб келди.

Вируслар билан зарарланиш эҳтимоли компьютерда янги файллар ва иловаларнинг пайдо бўлиш частотасига мос равишда ортади. Компьютердаги маълумотларнинг аҳамияти қанчалик зарур бўлса, вирусга қарши хавфсизлик чоралари шунчалик юқори бўлиши керак.

Бу нарсаларга бефарқ бўлиш нафақат катта моддий зарар кўриш, балки ташкилот ёки фирманинг бундан кейинги фаолияти масаласини ҳам ўртага қўйиш мумкин.

Шуни эсдан чиқармаслик керакки, вируслар, одатда фойдаланувчининг бирор амали (масалан иловаларни ўрнатиш, тармоқдан файлларни ўқиш, электрон алоқани ўрнатиш ва ҳ.к) натижасида пайдо бўлади. Шунинг учун маълумотлар кириш жойига махсус фильтрлар ўрнатилиши зарур. Бундай қурилмалардан бири Symantic корпорацияси маҳсулидир. **Symantic** битта машина ўрнига бутун корпоратив тармоқни комплекс ҳимоялаш ғоясини илгари суради. Вируснинг корпоратив тармоққа кириш нуқтаси исталган нуқтада браузердан то ишчи станциягача бўлиши мумкин.

Шунинг учун назорат барча босқичларда амалга оширилади. Вирусга қарши **Symantic** дастурий таъминоти **Dynamic Document Revion** корпорацияси технологиясида бажарилган ва **E-mail** вирусларига ҳам қарши кураш олиб боради.

Вирусга қарши дастурли таъминот ишининг алоҳида хусусиятлари шундаки, вирусга қарши дастурлар омборини ўз вақтида янгилаб туриш керак. Бундан ташқари бошқа турдаги вируслар ҳам мавжуд. Вируслардан ҳимоя қилишда ахборотни ҳимоя қилишнинг умумий воситаларидан фойдаланиш кифоя қилмайди. Бунинг учун махсус дастурлардан фойдаланиш зарур бўлади. Бу дастурларни бир неча курсга ажратиш мумкин бўлади: детекторлар, вакциналар (иммунизаторлар), докторлар, ревизорлар (файл ва дискларнинг тизимини соҳаларидаги ўзгаришларни назорат қилувчи дастурлар). Доктор-ревизорлар ва фильтрлар (вирусдан ҳимояланиш учун мўлжалланган резидент дастурлар).

Ревизор дастурлар-дастлаб дастур ва тизимли соҳаси ҳақидаги маълумотларни хотирага олади, сўнгра уларни дастлабкиси билан солиштиради. Мос келмаган ҳоллар ҳақида фойдаланувчига маълум қилади. Масалан, **CRCLIST** ва **CRCTEST** дастурлар.

Фильтр дастурлар ва резидент дастурлар компьютернинг тезкор хотирасида резидентдай жойлашади ва вируслар томонидан зарарни кўпайтириш ва зиён етказиш

мақсадида операцион тизимга қилинадиган мурожаатларни ушлаб қолиб, улар ҳақида фойдаланувчига маълум қилади. Вирусга қарши дастурлар қувватига қараб, бир неча турга бўлинади.

1. **AIDSTEST**- вирусларни аниқлаш ва йўқотиш учун мўлжалланган вирусга қарши кўп қиррали дастур (хар хафтада янгиланиб туради).
2. **Doctor WEB (Dr.Web)** –янгидан яратилган, маълум ва номаълум вирусларни аниқлаш ва йўқотиш учун ишлатиладиган вирусга қарши дастур. У архивланган ва вакциналанган файлларда ҳам вирусларни аниқлай олади. (хар ойда ўртача 2 марта янгиланади).
3. **ADINF**- дискдаги барча ўзгаришларни назорат қилувчи, дискларнинг вирусга қарши ревизор дастури (бир йилда бир неча марта янгиланади. Дискдаги барча дастурларнинг физик камчиликларини назорат қилади. Дискнинг тизимли сохасини ва файллар ҳолатини эслаб қолади ва қайта юклашда дискдаги ўзгаришларни аниқлайди, агар бирор ҳавфли ўзгаришлар аниқланса, фойдаланувчига бу хақда хабар беради.
4. **SHERIF** - қаттиқ дискдаги операцион тизим дастурлар ва маълумотлар файлини 100% кафолат билан ҳимояловчи резидент дастур. Бу дастурлар асосан **MS DOS** муҳитида ишлатилади.)

(уларни Windows муҳитига мослаш ҳам мумкун). Амалда юқоридагилардан биттасидан фойдаланиш мақсадга мувофиқдир. Бирор дастурни ўрнатиб уни доимий равишда янгилаб борилса, фойдалироқ бўлади.

Компьютерга вирус юққанда (ёки юққанлик ҳақида гумон бўлса) қуйидаги қоидаларни эсда тутиш ва қўллаш лозим.

1. Дастлабки, қарши кураш қарорларини қабул қилишга шошилмаслик керак. Ўйламасдан қилинган харакатлар тиклаш мумкин бўлган файлларнинг бир қисмини йўқотишгина эмас, балки компьютерни яна қайта касаллантиришга олиб келиш мумкин.
2. Вирус ўзининг бузғунчилигини давом этирмаслиги учун компьютерни ўчириш лозим.
3. Компьютер касалланиши ва даволаниши кўринишни аниқлашга мўлжалланган барча амалларни ёзишдан ҳимояланган операцион тизимли диск билан компьютерни ишга тушириш орқалигина бажариш мумкин.

Dr.Web дастуридан фойдаланиш билан танишиб чиқамиз. Бу дастур 32 битли **Windows** туркумидаги операцион системалар учун мўлжалланган бўлиб қисқача **Dr.Web 32 W** деб аталади. У кенг тарқалган антивирус дастурларидан биридир. **Doctor Web** хар доим янгиланишда бўлади. **Doctor Web** да ишни бошлаш учун жойлашган катологдан **Dr.Web. exe** дастури компьютерга юкланади. Натижада экранда қуйидаги ҳолат пайдо бўлади. Бунда экраннинг энг юқори қисмида **Dr.Web.** Анти вирус дастурининг менюси пайдо бўлади. Унинг ёрдамида вақтинча **Dr.Web** дан чиқиб туриш (временўй вўход), дастурдан чиқиш (Вўход) ва дастур ҳақида (о программе) буйруқларини бажариши мумкин.

Менюнинг тест бўлимидаги хотирани текшириш (тест памяти), текшириш (тестирование), даволаш (лечение), статистика (статистика), файл ҳисоботи (Файл отчёта) мавжуд. Мулоқот ойнасида **путь для лечение** даволаш йўли кўрсатилади.

Временўй вўход (вақтинча чиқиш) буйруғи ёрдамида **Dr.Web** дан вақтинча чиқиб турилади.

Настройка ёрдамида **Dr.Web** дастурининг параметирлари созланади.

Менюдан фойдаланиб, қандай файлларни текшириш билан боғлиқ бўлган барча параметрлар ўрнатилади. Сўнгра **«Тест»** даги **«Лечение»** кўрсатмасини танлаш ва **Ctrl** ва **F5** тугмаларини биргаликда босиш орқали вируслардан даволаш жараёнини бошлаб юборилади. Дастур хотиранинг кўрсатилган қисмини текшириб, мавжуд вирусларни даволашга харакат қилади ва иш охирида мос ҳисоботни чиқаради.

III. Хулоса

Компьютер тизимларини ривожланиши билан янада янги компьютер вируслари пайдо бўлмоқда, шунга мос равишда турли хил антивирусли тизмлар ва воситалар ҳам пайдо бўлмоқда. Одатда вируслар компьютер тизимида сақлаётган дастур таъминотини ва/ёки маълумотларни ўзгартиради ёки йўқ килади. Зарар келтирадиган дастурларга биологик вирусларнинг хоссалари интилишдир.

Компьютер вирусларини шаклларини ва турли - туманлигини кўп қирралилиги тавсифли схемаларда турли хил белгилар бўйича келтирилгандир. Айниқса «мантиқий бомбалар», «троян отлари», «чувалчанглар» каби вирусларни таъкидлаш жоиздир.

Шак-шубхасиз, махсус антивирусли воситаларни ишлаб чиқиш ва ишлатиш долзарбдир. Антивирусли воситалар вирусдан зарарланиш окибатларини аниқлаш (сканерлаш, ўзгаришларни пайқаш усули, эвриетик тахлил этиш, аппарат - дастурли антивирусли воситалар ва хакозо) ва йук килиш масалаларини ечади, шу билан бир каторда файлларни ва хотира сохаларини, юкланиш секторларини тиклайди.

Антивирусли дастурлардан детектор, ревизор (тафтишли) ва «коровул» дастурларини таъкидлаб утиш мумкин.

Компьютер вирусларидан ҳимоя қилишнинг асосий чораларидан дастур махсулотларини расмий йўл билан ишлатишни келтириш мумкин. Алоҳида таъкидлаш керакки, антивирусли воситалар доимо янгиланиб бориши керак, бунда ташқаридан келадиган янги дастурларга ва файлларга алохида эътиборни қаратиш керак.

Таъкидлаб ўтамизки, дастур махсулотларини вируслардан химоя қилишнинг ахамияти жуда каттадир. Бундай ҳимоя, оддий вируслардан ташқари, албатта хуқуқий усуллар билан амалга оширилиши керакдир.

Вирусга қарши дастур, юкланадиган вирус, компьютер вируси, вирус-мутант, кўринмайдиган вирус (стелс-вирус), хавфсиз вирус, резидент бўлмаган вирус, хавфли вирус, жуда хавфли вирус, паразит (текинхур) вирус, резидент вирус, вирус-реплиқатор (чу-валчанг), тармоқли вирус, троян вируси, файл вируси, зарарланган дастур, зарарланган диск, дастур-вакцина, дастур-доктор (фаг), дастур-детектор, дастур-тафтишчи, дастур-фильтр (қоровул), Aidstest ва Doctor Web дастур-полифаглари.

III. Фойдаланган адабиётлар.

1. Тайлоков Н.И., Ахмедов А.Б. "IBM PC компьютерлари". Тошкент 2001й.
2. Рахмонкулова С.И. "IBM PC шахсий компьютерларида ишлаш". Тошкент 1996й.
3. Гуломов С.С. ва бошкалар "Ахборот тизимлари ва технологиялари". Тошкент 2000й.
4. Имамов Э.З., Фаттахов М. "Ахборот технологиялари. "Тошкент" 2002й.
5. Узоков З.У. "Информатика ва ахборот технологиялари" маъруза матнларининг электрон версияси. Карши 2002й.
6. Маллаев А.Р., Носиров Б.Н., Ганиев Р.Р. "Компьютер куникмалари". Тасвирли укув кулланманинг электрон версияси. Карши 2002й.
7. Носиров Б.Н. "Компьютер куникмалари". Услубий кулланма. Карши 2000й.
8. Алимов Р.Х. ва бошқ. Ахборотлар технологияси асослари. – Т.:ТДИУ, 2003.
9. Ғуломов С.С. ва бошқ. Иқтисодий информатика. - Т.:ТДИУ, 1999.
10. Ғуломов С.С. ва бошқ. Миллий иқтисодда ахборот тизимлари ва технологиялари. - Т.:ТДИУ, 2004.
11. http://www.referat.uz
12. http://vlibrary.freenet.uz

.