ЎЗБЕКИСТОН РЕСПУБЛИКАСИ

ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

НАМАНГАН МУҲАНДИСЛИК-ПЕДАГОГИКА ИНСТИТУТИ

Алишер Анваров

МАЪЛУМОТЛАРНИ МУҲОФАЗА ҚИЛИШ

ФАНИДАН
Тажриба ишлари тўплами

УСЛУБИЙ КЎРСАТМА

НАМАНГАН

Маълумотларни муҳофаза қилиш фанидан услубий кўрсатма Информатика ва АТ Касб таълими йўналиши талабалари учун мўлжалланган.

Тузувчи: **АЛИШЕР АНВАРОВ**

Ушбу маърузалар курси «Информатика ва АТ» кафедраси умумий йиғилишида муҳокама қилинган.
(__-мажлис баёни_____2006 й.)

,

Автоматлашган ахборот тизимларида хамда маълумотларни мухофаза килиш воситалари

Ишнинг максади: Талабаларда Автоматлашган ахборот тизимларида хамда маълумотларни мухофаза килиш воситалари ҳакида кискача назарий маълумотлар ва амалий куникмалар хосил килиш

Аниқлаштирилган ўқув мақсадлари.Талаба бу мавзуни тўла ўзлаштиргандан сўнг:

- ❖ Маълумотларни муҳофаза қилиш ҳақидаги тамойилларни билади;
- ❖ Система хавфсизлигининг асосий принципларини бўлакларга бўлиб, таъриф бера олади;
- ❖ Система ташкил этувчиларининг бутунлиги – система хусусиятларинини талқин эта олади;
- ❖ Информациянинг ишончлилиги принципларини қайси синфга мансублигини тасаввур эта олади;
- ❖ Система ташкил этувчисидан фойдаланувчанлиги ўртасидаги ўзаро алоқадорликни аниқлайди, боғланишларни таҳлил қила олади.

НАЗАРИЙ МАЪЛУМОТЛАР

Ҳозирги пайтда компьютер системаларида маълумотларни муҳофаза қилишни таъминлаш масаласи долзарб масалалардан бири бўлиб қолмоқда.

Информациянинг ҳаммаси ҳам ҳимояга муҳтож эмас. Шунинг учун

информация ўз характерига кўра критик ва нокритик информацияга бўлинади.

Критик информация фойдаланувчининг шахсий ишлаб топган маълумотлари бўлиб, хизматчи информация, савдо-сотиққа оид сирларни ўз ичига олувчи информация ёки махфийликнинг турли кўриниш ёки шаклларига оид информация ва ҳ. бўлиши мумкин.

Бу бобда критик маълумотларни муҳофаза қилиш билан боғлиқ масалаларга эътибор қаратилади.

Айни пайтда компьютер техникасидан фойдаланувчиларнинг ҳаммаси ҳам бу масалаларнинг муҳимлигини англаб етмайдилар. Мамлакатимизнинг бозор иқтисодига ўтиши кўплаб фирма ва банкларнинг ташкил этилишига олиб келди, бу фирма ва банкларнинг самарали ишини эса компьютерларсиз ташкил этиб бўлмаслиги ҳаммага аён. Компьютер техникасидаги ҳар қандай бузилиш ўша фирма ёки ташкилот учун жиддий йўқотишларга олиб келиши мумкин. Шунинг учун ҳам маълумотларни муҳофаза қилиш масаласига жиддий ёндашмоқ зарур.

Системанинг хавфсизлиги деганда, унинг фойдаланувчи ёки эгаларига, турли қасддан ёки тасодифий қилинган таъсирлар натижасида, катта талофотлар етказишга бардош бера олиш хусусияти тушунилади. Бошқача сўз билан айтганда, система хавфсизлиги деганда унинг иш жараёнининг бир маромда кетишига халақит берувчи тўсиқлар, тасодифий ёки атайдан пухта ўйланган халақитлар, шунингдек, унинг ташкил этувчиларини ўғирлаш, ўзгартириш ёки бузишга қаратилган уринишларга қарши ҳимоя қобилияти тушунилади.

Системанинг хавфсизлигига 3 та асосий принципларни таъминлаш билан эришилади:

1) ***Система ташкил этувчиларининг бутунлиги*** – система хусусиятларининг унинг иш жараёнида ўзгармаслиги. Эксплуатация жараёнида система администратори томонидан бир қатор фойдали ўзгартиришлар ўтказилади ва бу ўзгартиришларнинг кам-кўсти тўлдирилиб охиригача етказилади (масалан - WinNT системасига қўшимча тўлатувчи пакетни ўрнатиш), лекин бунда талаб қилинган хусусиятлар ўзгармайди - илгаригидек фойдаланувчини идентификация қилиш ва унинг системадаги ишини таъминлаши керак.

2) ***Информациянинг ишончлилиги*** – бу информациянинг шундай хусусиятики, бунда у системанинг фақат рухсат этилган ва текширувдан ўтган субъектларигагина (фойдаланувчилар, программалар, жараёнлар ва ҳ.) маълум бўлади.

3) ***Система ташкил этувчисидан фойдаланувчанлиги*** – фақат муаллиф субъектларнинг система ташкил этувчисидан ихтиёрий пайтда фойдалана олиш хусусияти. Бошқача айтганда, системанинг ҳар бир фойдаланувчиси идентификация қилинган ва фойдаланувчининг фойдаланиш даражасига мувофиқ ҳолда система ташкил этувчиларидан фойдаланишга рухсат этилган бўлиши керак. Бунда фойдаланиш даражаси хизматчининг хизмат мавқеи билан эмас, балки унинг қатъий функционал мажбуриятлари билан аниқланади.

Маълумки, ҳозирда компьютер ва компьютер системалари автоном ҳолда кам фойдаланилади. Улар одатда бир-бирлари билан локал, корпоратив ва глобал тармоқлар орқали боғланади. Компьютер

системаларининг маълумотлар базасида катта ҳажмдаги информация шаклланган. Унинг йўқолиши, бузилиши ёки берухсат фойдаланилиши катта иқтисодий талофотларни келтириб чиқариши мумкин. Бундан четлашиш мақсадида берухсат фойдаланишлардан информацияни ҳимоя қилишнинг ҳар хил системалари қўлланилади.

Самарадорлиги юқори информацияни ҳимоя қилиш системасини ишлаб чиқиш аввало, бу системанинг концепциясини аниқлаш керак. Тадқиқот ўтказишда ва моделлаштиришда информацияни ҳимоя қилувчи восита юқори даражадаги ҳимоя қобилиятига эга эканлигини исботлаши лозим.

Информацияни ҳимоя қилувчи системаларнинг кўпгина моделлари ишлаб чиқилган. Бироқ энг кўп фойдаланиладиган моделлар қуйидагилардир:

1. **Белла ва Ла-Падула**; бунда фойдаланиш ҳуқуқини чеклаш воситаларини қуриш учун фаол субъектлар S ва пассив субъектлар Q тушунчалари киритилади. Ушбу ҳолда субъектлар фойдаланишнинг ҳар хил ҳуқуқларига эга бўладилар. Бундай модел гоҳида “фойдаланиш ҳуқуқини чеклашнинг матрицали модели” деб ҳам юритилади;
2. **Денинг модели** – ҳар хил даражадаги махфийликка эга ҳужжатлар билан ишлашда информацияни ҳимоя қилиш воситасининг кўп сатҳли иерархик модели; бу ерда информацияни ҳимоя қилишнинг концентрлашган халқаси тушунчаси киритилади. Ички халқаларда – максимал махфийлик даражаси мавжуд бўлиб, ташқи қурилма (периферии)га яқинлашган сари махфийлик даражаси камаяди;
3. **Лендвер модели** - шундай компьютер тармоқларида фойдаланиладики, бундай тармоқдаги маълумотларни муҳофаза қилиш информацияни киритиш-чиқариш операцияларининг ҳимояси билан таъминланади.

Кўпгина реал вақт масштабида ишлайдиган мавжуд операцион системалар учун Белла ва Ла-Падула ҳимоя системаси концепциясидан фойдаланилади. Бу моделда фойдаланиш диспетчерининг қўлланилиши талаб этилади. Информацияни ҳимоя қилиш системасининг ўзи эса учлик кўринишида тасвирланади:

$$Zк(S,Q,P)$$

бу ерда:

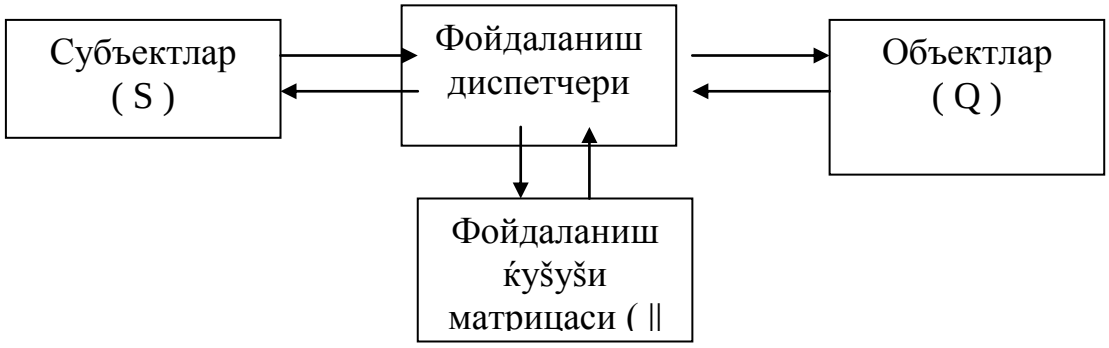
S – фойдаланувчилар ва улар программаларидан иборат субъектлар ҳамда ўзидан-ўзи пайдо қилувчи жараёнлар, процедуралар ва б.;

Q – субъектлар билан сўров олиб бориши мумкин бўлган системанинг объект (ресурслари) тўплами; объектларга

программалар, процедуралар, маълумотлар дисклари, томлар, файллар, алоҳида файл ёзувлари ва қурилмалар мансуб;

P – субъектларнинг объектлардан фойдаланиш ҳуқуқлари тўплами.

Информацияни ҳимоя қилиш системасининг умумий структураси 1-расмда келтирилган.



Битта процедура бир вақтда ҳам субъект, ҳам объект бўлиб чиқиши мумкин. Фойдаланиш ҳуқуқи битли векторлар билан аниқланади. Ҳар бир бит таъқиқлаш (запрет) ёки рухсат беришни аниқлайди: R, E, W, M, A, O; бу ерда R – ўқиш, E – таҳрирлаш, W – ёзиш, A – администратор, O – тўлиқ мулкдор (полний собственник).

Фойдаланишнинг минимал ҳуқуқи тўрт бит билан аниқланади: R, E, W, M. Фойдаланиш ҳуқуқини фойдаланиш администратори аниқлайди ва ҳеч қайси фойдаланувчи ||P|| матрицадан фойдаланиш имконига эга эмас, лекин уни ўзгартириши мумкин.

Кўпроқ ишончли ҳақиқийликка мос модел сифатида ўйин ҳимоя моделлари ифодаланади, яъни бундай моделларда камида иккита томон мавжуд бўлади. Биринчи томон информацияни ҳимоя қилиш системасини, иккинчи томон эса биринчи томон воситасида қурилган ҳимояни эгаллаш системасини қуради.

Шундай бўлишига қарамасдан кўпгина атакалар ва берухсат фойдаланишга бўлган ҳаракатлар пассив (яъни фойдаланувчи ҳақида информация йиғиш ва нусхалаш) ҳисобланади ва ўзида фаол атакага тайёр потенциал бузғунчини ошкор қилиши ҳам мумкин.

Ҳимоя системасини ишлаб чиқиш ҳимоя қилиниши лозим бўлган системанинг ўзини ишлаб чиқиш билан бирга олиб борилиши керак. Ҳимоя системасини яратиш тажрибаси қуйидаги асосий принципларни ажратиш имконини беради. Улар лойиҳалашда эътиборда бўлиши керак.

1. ***Ҳимоя механизмининг соддалиги.*** Бу принцип шунга асосланганки, лойиҳалашда ва эксплуатацияда юзага чиққан айрим хатолар фойдаланишнинг эътиборга олинмаган йўлларини аниқлашга имкон беради. Шунга асосан ҳимоянинг аппарат ва программ

воситаларини синчиклаб тестлаш керак, бироқ амалиётда бундай текширувнинг фақат содда ва ихчам схемалар учун имконияти мавжуд.

2. *Информациянинг четга чиқиб кетиши мумкин бўлган ҳамма каналларнинг ёпиқлиги*. Бу принцип ҳар қандай объектга бўладиган ҳар қандай мурожаат ҳуқуқини (ваколатини) текширишга мўлжалланган ва ҳимоя системасининг асоси ҳисобланади.

Бу принципни ҳисобга олган ҳолда, фойдаланишни бошқариш масаласи умумсистема сатҳида ечилиши лозим. Бунда ишга тушириш, бузилишлардан сўнг қайта тиклаш, ажратиш ва профилактик хизмат кўрсатиш каби иш режимлари эътиборга олинади. Маълумотларга бўладиган ҳар қандай мурожаат манбаини ишончли аниқлашни таъминлаши зарур.

3. *Ҳимоя механизмининг жиддий бўлмаган махфийлиги*. Кенг фойдаланишга мўлжалланган ҳимоя системасини амалга ошириш деталларини яшириши шарт эмас. Ҳимоя самарадорлиги потенциал бузғунчиларнинг маҳоратига боғлиқ бўлмаслиги керак. Чунки пароллар рўйхати ҳимоясини таъминлаш анча содда кечади. Ҳимоя механизмининг махфий эмаслиги зарур ҳолларда, унинг мутахассислар орасидаги кенг муҳокама субъекти бўлиши имконини беради.

4. *Фойдаланувчилар ҳуқуқ ва ваколатларининг тақсимланиши*. Компьютер тармоқлари ва системаларида бир қанча ҳимоя калитларининг мавжудлиги қачонки фойдаланишга бўлган ҳуқуқ бир қатор шартлар бажарилиши билан аниқланган ҳолатдагина қулайлик туғдиради.

5. *Минимал ваколат*. Ҳар қандай фойдаланувчи ва программа учун топширилган ишни бажариш учун зарур бўлган ваколатнинг минимал доираси аниқланган бўлиши керак. Шунга кўра тасодифий бузилишларга сабаб бўладиган зарарлар маълум миқдорда камайиши мумкин.

6. *Ҳимоя механизмининг максимал ихтисослаштирилганлиги*. Фойдаланувчилар орасида информация алмашишини истисно қилиш мақсадида ҳимоя схемасини лойиҳалашда бир неча фойдаланувчилар учун умумий бўлган параметрлар ва ҳимоя механизми характеристикаси сонини минимумга олиб келиш мақсадга мувофиқ.

7. *Психологик жозибадорлик*. Ҳимоя системасини эксплуатация қилиш содда бўлиш лозим. Фойдаланувчининг ҳимоя системаси ҳақидаги тасаввурлари унинг фактларга асосланган имкониятлари билан қанчалик мос тушса, қўллаш жараёнида хатолар шунчалик кам бўлади. Айрим сунъий тилларнинг ҳимоя системасига мурожаат қилишда фойдаланилиши қўшимча хатолар манбаи бўлиб хизмат қилади. Юқорида санаб ўтилган принципларнинг айримларига асосланган системани қуришда уларни амалга оширишда

сарфланадиган катта харажатлар билан боғлиқ жиддий тўсиқлар юзага келади. Шунинг учун ҳимоя системаларини лойиҳалашдаги муҳим фактор сифатида унинг иқтисодий самарадорлигини кўрсатиш мумкин.

Шуни эсда тутиш лозимки, фаолиятнинг алоҳида тармоқлари (банк ва молия институтлари, информацион тармоқлар, давлат бошқарув системалари, мудофаа ва махсус хизмат структуралари) маълумотлар хавфсизлиги бўйича махсус чора-тадбирлар кўришни талаб қилади ва бу тармоқларда ечилаётган масалаларнинг характери ва аҳамиятига мос ҳолда информацион системанинг ишлаш ишончлилигига бўлган талаблар жуда юқори бўлади.

Маълумотларни муҳофаза қилиш масаласини кўриб чиқишда, даставвал, маълумотларни ўринсиз (номатлуб, номаъқул) ўзгартириш ёки йўқотишга олиб келувчи рухсатсиз фойдаланиш ёки бузишнинг турлари билан танишиб чиқиш лозим. Бундай жиддий таҳдидлардан қуйидагиларни келтириш мумкин:

- жиҳоз (қурилма) ларнинг бузилиши: кабель системасининг бузилиши, электр манбаининг ўчиб-ёниши, диск системасининг бузилиши, маълумотларни архивлаш системасининг бузилиши, серверлар, ишчи станция

- лар, тармоқ карталарининг бузилиши;
- программа таъминотининг нотўғри ишлаши оқибатида келиб чиқадиган информация йўқолиши, программа таъминотининг носозлиги натижасида маълумотларнинг ўзгариб кетиши ёки йўқ бўлиб кетиши, системанинг компьютер вируслари билан зарарланиши натижасида маълумотларнинг йўқолиши ва ҳ.;
- рухсатсиз фойдаланиш билан боғлиқ йўқотишлар: информациядан рухсатсиз нусха олиш, йўқотиш ёки қалбакилаштириш, махфий, сир тутилиши лозим бўлган информацияни бегона кишиларга таништириш;
- архив маълумотларини нотўғри сақлаш билан боғлиқ йўқотишлар;
- хизматчи шахс ёки фойдаланувчининг хатолари: маълумотларни ўзи билмаган ҳолда ўзгартириш ёки йўқотиб юбориш, маълумотларнинг йўқолишига ёки бузилишига олиб келувчи программа ёки аппарат таъминотидан нотўғри фойдаланиш.

Бу таҳдидлардан келиб чиқиб, информацияни ҳимоялашнинг барча турларини қуйидаги 3 та синфга бўлиш мумкин:

- ***физик ҳимоялаш воситалари:*** кабель системасини, электр манбаи системасини ҳимоялаш воситалари, ҳимоялашнинг аппарат воситалари, архивлаш, дискли массивлар ва ҳ.;

- ***ҳимоялашнинг программа воситалари:*** антивирус программалари, ваколатларни (фойдаланиш имкониятларини) чеклаш системаси, фойдаланишни назорат қилувчи программа воситалари;
- ***ҳимоялашнинг маъмурий чора-тадбирлари:*** бинога киришни назорат қилиш, фирма ёки ташкилотнинг хавфсизлигини таъминлаш стратегиясини ишлаб чиқиш, фавқулодда ҳолатларда ҳаракат қилиш режаларини тузиб чиқиш ва б..

Бундай синфлаш шартли эканлигини унутмаслик лозим, чунки Ҳозирги замонавий технологиялар аппарат-программ ҳимоя воситалари билан бир йўналишда ривожланиб бормоқда. Бундай аппарат-программ воситаларидан, хусусан, вируслардан ҳимояланиш, фойдаланишни назорат қилиш ва ҳ. кенг тус олмоқда.

Банкларда нақд пуллар йиғилгани каби компьютерда ҳам информациянинг тўпланиши ҳам информацияни ҳимоялаш мақсадида назоратни янада кучайтиришни талаб қилади.

Юридик масалалар, хусусий сир, махфий маълумотлар, миллий хавфсизлик - буларнинг барчаси тижорат ва ҳукумат ташкилотларида ички назоратни кучли ташкил этишни талаб қилади. Бу йўналишдаги ишлар янги «Маълумотларни муҳофаза қилиш» фанининг пайдо бўлишига олиб келди. Маълумотларни муҳофаза қилиш бўйича мутахассис ташкилотда йиғилган информациянинг бутунлиги, махфийлиги, фойдаланишга яроқлилигини таъминлашга қаратилган маълумотларни муҳофаза қилиш системасини ишлаб чиқиш, йўлга қўйиш ва ишлатиш ишларига масъулдир. Унинг вазифаларига информацион ресурсларни физик (техник воситалар, алоқа каналлари ва узоқлаштирилган компьютерлар) ҳамда мантиқий (маълумотлар, амалий программалар ва операцион системалар) ҳимоялашни таъминлаш киради.

Информацияни ҳимоялаш системасини яратиш мураккаблиги шундаки, маълумотлар компьютердан ўғирланиши билан бир вақтда ўз жойида қолиши ҳам мумкин, яъни баъзи маълумотларни йўқотиш ёки ўзгартириш эмас, балки бутунича нусха кўчириб олиб кетишнинг ўзи кифоя қилади.

Маълумотларни муҳофаза қилишни таъминлаш - қиммат ҳамда катта сарф-харажатларни талаб қиладиган иш бўлиб, воситаларни сотиб олиш ёки ўрнатишга қанча сарф-харажат қилинмасин, мос таъминот системасининг ишга лаёқатли ҳолатини ва оқилона хавфсизлик чегарасини малакали аниқлаш шунчалик қийин бўлади. Агар локал тармоқ умумий фойдаланилувчи кўп сонли информация файллари, қимматбаҳо рангли принтерлар ёки лицензион программа воситаларидан биргаликда фойдаланиш мақсадида ишлаб чиқилган

бўлса, у ҳолда информацияни ҳатто минимал шифрлаш ёки дешифрлаш ҳам талаб қилинмайди.

Информацияни ҳимоялаш воситаларини лойиҳалаш, сотиб олиш ёки ўрнатишни етарлича таҳлилларни олиб бормасдан туриб амалга ошириш керак эмас. Таваккални таҳлил қилиш кўплаб факторлар (ишнинг бузилишининг пайдо бўлиши, ишнинг бузилишининг пайдо бўлиш эҳтимоллиги, тижорат йўқотишлардан зарар кўриш, системанинг тайёргарлиги коэффициентининг камайиши, жамоат муносабатлари, юридик муаммолар) нинг объектив баҳоларини бериши ҳамда хавфсизликнинг мос турларини ва даражаларини аниқлаш учун информация тақдим этиши шарт. Тижорат ташкилотларининг барчаси маълум даражада кўп бўлган критик корпоратив информацияни катта-катта ҳисоблаш системаларидан олиб, очиқ система воситаларига узатишда хавфсизлик системасидан фойдаланиш ва уни йўлга қўйишда янги, ҳали номаълум бўлган мураккаб муаммоларга дуч келадилар. Ҳозирда кўплаб ташкилотларда тижорат маълумотларини бошқариш учун юқори қувватли, тақсимланган маълумотлар базаси ва клиент/сервер технологиясидан фойдаланилмоқда. Тақсимланишнинг ўсиши билан бирга бу маълумотларга рухсатсиз кириш ва уларни бузиш имкониятлари ҳам кўпайиб бормоқда.

Компьютер системасининг хавфсизлигига эришиш жараёнида системага таъсир этиши мумкин бўлган барча ҳолатларни таҳлил ва прогноз қилиш керак. Системага кўрсатиладиган таъсирлар 2 турга фарқланади - ***тасодифий*** ва ***атайдан (қасддан) қилинган таъсирлар***.

ТОПШИРИКЛАР

1. Алока тизимларида ахборотларни ҳимоялаш ҳакида маълумотли ҳужжат тайёрланг.
2. Электрон ҳужжат ларни юридик аҳамиятини ҳимоялаш ҳакида маълумотли ҳужжат тайёрланг.
3. Ахборотларни чикиб кетишни ҳимоялаш ҳакида маълумотли ҳужжат тайёрланг.
4. Хисоблаш ускуналарини компьютернинг ахборот нурланишларидан ҳимоялаш ҳакида маълумотли ҳужжат тайёрланг.
5. Кимматли банк ахборотларидан рухсатсиз нусха кучириш ва таркатилишидан ҳимоялаш ҳакида маълумотли ҳужжат тайёрланг.
6. Дастурий таъминотнинг яхлитлигини назорат килиш ҳакида маълумотли ҳужжат тайёрланг.

7. Пластик карточкалар тамойили ҳақида маълумотли ҳужжат тайёрланг.
8. Хакерлар ва крэкерлар ҳақида маълумотли ҳужжат тайёрланг.
9. «Ахборотлар уруши» ҳақида маълумотли ҳужжат тайёрланг.
10. Система хавфсизлиги принциплари ҳақида маълумотли ҳужжат тайёрланг.
11. Ҳимоя системалари моделлари ҳақида маълумотли ҳужжат тайёрланг.
12. информацияни ҳимоялашни 3 та синфи ҳақида маълумотли ҳужжат тайёрланг.
13. Тасодифий таъсирлар ҳақида маълумотли ҳужжат тайёрланг.
14. Рухсатсиз кириш (фойдаланиш) ҳақида маълумотли ҳужжат тайёрланг.
15. имтиёзлардан ноконуний фойдаланиш РК, РФ
16. Системани бузиш параметрлари
17. Критик информация ҳақида маълумотли ҳужжат тайёрланг.
18. Диск ва каналларни резервлаш ҳақида маълумотли ҳужжат тайёрланг.
19. Серверни кайнок резервлаш ҳақида маълумотли ҳужжат тайёрланг.
20. Системани касддан килинган таъсирлар ҳақида маълумотли
21. Программа модулига яшириш (туйнуклар) ҳақида маълумотли ҳужжат тайёрланг.

Компьютер вируслари ва уларни яратишдан кўзланган мақсад.
Вирус турлари ва ишлаш принциплари.

AVP умумий характеристикаси.

Аниқлаштирилган ўқув мақсадлари.Талаба бу мавзуни тўла ўзлаштиргандан сўнг:

- ❖ Компьютер вируслари ҳақидаги тамойилларни билади;
- ❖ Резидент ва норезидент вирусларини бўлакларга бўлиб, таъриф бера олади;
- ❖ Уяли телефонлар учун вируслар хусусиятларинини талқин эта олади;
- ❖ Windows 98 карокчилик нусхалари билан таркаладиган

Вирус қайси синфга мансублигини тасаввур эта олади;
Уз-узини ҳимоялаш рецептлар
ўртасидаги ўзаро алоқадорликни аниқлайди, боғланишларни таҳлил қила олади.

НАЗАРИЙ МАЪЛУМОТЛАР

Компьютер вируслари. Бу нима ва унга карши кандай курашиш керак? Бу мавзуга унлаб китоблар ва юзлаб маколалар ёзилган. Компьютер вирусларига карши минглаб профессионал мутахассислар кўплаб компанияларда иш олиб боришмокда. Бу мавзу ута қийин ва мухимки кўп эътиборни талаб килмокда. Компьютер вируси информацияни йукотиш сабабларидан бири ва асосийси бўлиб колмокда. Вируслар кўплаб ташкилот ва компанияларни ишларини бузишга олиб келганлиги маълум. Шуи дай маълумотлар мавжудки, Нидерландия госпиталларидан бирида беморга компьютер куйган ташхис буйича истеъмол килинган дори окибатида бемор оламдан утган. Бу компьютер вирусининг иши булган.

Эътиборсизлик билан килинган ишдан компьютер тезда вирус билан зарарланади. Инсон касаллик вируси билан зарарланса иссиклиги узгариши, вазни узгариши, холсизланиш ва огрикнинг пайдо булиши кузда тутилади. Компьютер вируси билан зарарланган компьютерларда куиидагилар кузатилади: дастурларнинг ишлашининг секинлашиши, файлларци хажми узгаради, гайритабиий ва баъзи бир номаълум хатоликлар, маълумотлар ва система файллари йукотилиши. Баъзи вируслар зарарсиз кўпаяди, лекин куркинчли эмас. Бу вируслар экранга хато маълумот кикаради. Аммо, бир турдаги вируслар хужум килувчи,

яъни, ёмон асоратлар колдирувчи хисобланади. Масалан, вируслар қаттиқ дискдаги информацияларни ўчирибташлайди.

Вирус нима?

Машхур «доктор» лардан бири Д.Н.Лозинский вирусни котибага ухшатади.

Тартибли котибани фараз килсак, у ишга келади ва столидаги бир кунда килиши керак булган ишларни - қоғозлар катламини куради. У бир варогни кўпайтириб бир нусхасини узига иккинчисини кейинги кушни стол га куяди. Кейинги столдаги котиба хам камида икки нусхада кўпайтириб, яна бир котибага утказади. Натижада конторадаги биринчи нусха бир неча нусхаларга айланади. Баъзи ну ехал ар яна кўпайиб бошка столларга хам утиши мумкин.

Компьютер вируслари тахминан шундай ишлайди, факат қоғозлар урнида энди дастурлар, котиба бу - компьютер. Биринчи буйруқ «кучириш-нусха олиш» булса, компьютер буни бажаради ва вирус бошка дастурларга утиб олади. Агар компьютер бирор зарарланган дастурни ишга туширса вирус бошка дастурларга таркалиб бориб бутун компьютерни эгаллаши мумкин.

Агар бир дона вируснинг кўпайишига 30 секунд вакт кетса, бир соатдан кейин бу 1000000000 дан ортиб кетиши мумкин. Аниқроги компьютер хотирасидаги буш жойларни банд килиши мумкин.

Худди шундай вокеа 1988 йили Америкада содир булган. Глобал сет оркали узатилаётган информация оркали вирус бир компьютердан бошкасига утиб юрган. Бу вирус Моррис виру си деб аталган.

Маълумотларни вирус кандай йук килиши мумкин деган саволга шундай жавоб бериш мумкин:

1. Вирус нусхалари бошка дастурларга тез кўпайиб утиб олади;
2. Календар буйича 13-сана жума кунга тугри келса

ҳамма ҳужжатларни йук килади (учиради).

Буни ҳаммага маълум «Jerusalem» («Time» вируси хам деб аталади) вируси жуда «яхши» амалга оширади.

Кўп холларда билиб булмайди, вирус каердан пайдо булди.

Компьютер вируслари - кўпаювчи, дастурларни **{|Ц||га** кучиб олиши, ёмон окибатлар келтириб чикарувчи дастурлардир. Лекин улар катъий бир куринишда булиши белгилаб куйилмаган.

Вирусни Аниқланиши шундаги, у компьютер системасида жойлашиб ва кўпайиб боришига боғлиқ. Мисол учун, назарий жихатдан оператив системада вирус даволаб булмайди. Бажарувчи коднинг сохасини тузиш ва узгартириш таъкикланган система мисол булиши мумкин.

Вирус хосил булиши учун бажарилувчи кодлар кетма-кетлиги маълум бир шароитда шаклланиши керак. Компьютер вирусининг хоссаларидан

бири уз нусхаларини компьютер тармоқлари оркали бажарилувчи объектларга кучиради. Бу нусхалар хам уз-узидан кўпайиш имкониятига эга.

Компьютер вируслари кандай хосил булади?

Биологик вируслардан фаркли уларок, компьютер вирусларини инсон томонидан тузилади. Вируслар компьютер фойдаланувчиларига катта зарар етказади. Улар компьютер ишини тухтатади ёки қаттиқ дискдаги маълумотларни учиради. Вирус системага бир неча йуллар билан тушиши мумкин: дискеталар, дастур таъминот юкланган CD-ROM, тармоқ интерфейси ёки модемли богланиш, глобал Internet тармогидаги электрон почта.

Дискета виру с дан зарарланиши осон. Зарарланган компьтерга дискетни солиб укитилганда дискнинг бош секторига вирус тушади.

Internet маълумотлар алмашинишига катта имконият яратади. Лекин, компьютер вируслари ва зарарли дастурлар таркалиши учун яхши муҳит яратади. Албатта InternetzjaH олинган барча маълумотларда вирус бор деб булмайди. Компьютерда ишловчи кўпчилик мутахассислар ва операторлар кабул килинадиган маълумотларни вируслардан текширишни доимо бажаради. Interne^a ишлаётган ҳар бир киши учун яхши антивирус ҳимоя зарур. «Касперский лабораторияси» техник таъминот хизмати статистикасига кура, вируслардан зарарланган ҳолатларнинг 85% и электрон почта оркали содир булган. 1999 йилга нисбатан хозирги кунда бу курсаткич 70 % ташкил этади. «Касперский лабораторияси» электрон почталарга яхши антивирус ҳимояси кераклигини таъкидлайди.

Вирус тузувчиларга электрон почта жуда кулай. Амалиёт шуни курсатадики, оммабоп дастурлар, операцион системалар, маълумотларни узатиш технологиялари учун вируслар кўплаб тузилмокда. Хозирда электрон почта бизнес ва бошка сохаларда мулокот учун асосий восита бўлиб колмокда. Шунинг учун вирус тузувчилари электрон почтага диккатини каратмокда.

Вирус пайдо булиш белгилари.

Зарарланган компьютерда энг мухими вирусни Аниқлаш. Бунинг учун вирусни асосий белгиларини билиш керак:

1. Функционал дастурларни ишини тухтатиш ёки нотўғри ишлаши;
2. Компьютерни секин ишлаши;
3. ОС ни юкланмаслиги;
4. Файл ва каталогларни йуколиши ёки улардаги маълумотларни бузилиши;

5. Файллар модификайиясининг сана ва вактининг узгариши;
6. Файл хажмининг узгариши;
7. Дискдаги файллар микдорининг кескин кўпайиши;
8. Буш оператив хотира хажмининг кескин камайиши;
9. Кутилмаган маълумотлар ва тасвирларнинг экранга чикиши;
10.Кутилмаган товушларнинг пайдо булиши;
11 .Компьютернинг тез-тез осилиб колиши.

Юкоридаги белгилар бошка сабабларга кура хам булиши мумкинлигини эслатиб утамиз.

Кискача тарих.

80-йилларда IBM-PC билан ишлаган кишилар булса 1987-89 йиллардаги вирусларни таркалишини унутишганича йук. Экрандаги ҳарфлар ҳар хил
куринишда бузилган ва фойдаланувчилар оммаси мутахассисларга дисплейларини олиб кела бошлашган. Кейинчалик компьютер «Yankee Doodle» деб номланган узга ерлик вирусини чалишни бошлаган. Лекин, буни тузатишни хеч ким ташламади, жуда тез хал булди. Бу унлаб вируслар туплами эди.

Шундай килиб, вируслар файлларни зарарлай бошлади. «Brain» ва экранда шариклар пайдо килувчи «Pingpong» вируслари Boot-сектор устидан хам голиб чикишди. Бу ҳаммаси IBM-PC дан фойдаланувчиларга унчалик ёкмади ва антивируслар пайдо булди. Биринчи антивиру ел ар дан бири ANTI-KOT: афсонавий Олег Котик узининг антивирусининг биринчи версияси дунё юзини курди. У 4 та вирусни йук килди. Афсуски, ANTI-KOT MSDOS комбинациясидан фойдаланиб файл охирида «Time» вирусини Аниқлаиди. Бошка антивируслар эса .com ва .exe кенгайтмали файлларнинг ҳар бир ҳарфигача занжирлайди.

Вакт утиши билан вируслар кўпайиб бормокда. Буларнинг ҳаммаси бир-бирига ухшаш, хотирага урнашади, сектор ва файлларга богланади, файлларни, дискет ва винчестерларни йук килади. Биринчилардан бўлиб, «Frodo.4096» вируси оммабоп бўлиб чикди. Бу вирус INT2Ih ни эгаллаб, DOS га мурожаат этилганда зарарланган файл худди хеч нарса бўлмагандай холда куриниш берган. Аммо, бу MSDOS устидан урнашиб хукмини утказган. Бир йил хам утмасданок «электр сувараклар» DOS ядросига урнашиб олишган. Куринмас вирус «Deast.512» деб аталган. Куринмаслик фикри кўпайиб ривожланиб
борди: 1991 йил ёзида компьютер улати - вирус «Dir_n» пайдо булди. Бирок куринмасларга карши кураш содда: RAM ни даволаб хотиржам булиш мумкин.

Шундай вируслар хам келиб чикдики, улар узларини шифрлаб олиш имкониятига эга булишди. Бу вирусларни даволаш ва йук килиш учун

махсус кием дастурлар яратиш керак булган. Лекин бунга хеч ким эътибор бермади, токи бу вирусларнинг янги авлодлари келиб чикмагунча.

Вируслар классификацияси.

Хозирги даврда 5000 дан ортик вирус дастурлар маълум. Буларни куйидагича классификацига ажратиш мумкин:

• Фаолият муҳитига караб;
• Зарарлантириш усулига караб;
• Ҳаракатланишига караб;
• Алгоритмнинг аҳамиятига караб.

Фаолият муҳитидан келиб чиккан холда вирусларни сетли, файлли, юкланувчи каби турларга булинади. Сетли вируслар ҳар-хил сетли компьютерларда таркалади. Файлли вируслар бажарилувчи файлларга таркалади. Бу файллар .com ва .exe булган файллар. Файлли вируслар бошка турдаги файлларни хам зарарлантириши мумкин. Бунда файллар бошкарувни кабул килмайди, имконият даражасини йукотади. Юкланувчи вируслар дискнинг юкловчи секторида таркалади ёки секторнинг узида жойлашади. (Boot sektor)

Вируслар зарарлантириш усулига караб резидент ва резитент бўлмаганларга булинади. Резидент вируслар зарарланган компьютерлар оператив хотирасига узининг юкумли бир кисмини колдириб кетади. Качонки, оператив хотирага мурожаат килинганда у ишга тушади ва таркалади. Резидент вируслар компьютерни учирилгунча ва перезагрузка килингунча актив ҳолатда булади. Резидент бўлмаган вируслар компьютер хотирасини зарарлантирмайди, балки белгиланган вакт чегарасида актив ҳолатга утади.

Ҳаракатланишига караб вируслар куйидаги турларга булинади:

• Хавфсиз, компьютерда ишлашга халакит бермайди. Лекин, буш булган оператив хотира ва дискдаги хотирани камайтиради. Бундай вируслар график ва овоз эффектларида пайдо булади.
• Хавфли вируслар компьютер ишини бузишга олиб келади.
• Жуда хавфли вируслар дастурларни йукотилишига, маълумотларни ва диск системасини учиб кетишига олиб келади.

Алгоритмнинг аҳамиятига караб вируслар куйидаги группаларга булинади:

1. «Хамжихат-йулдошлар» - файлларни узгартирмайдиган вируслар. Бу вируслар EXE кенгайтмали файлларга кушимча нусха олиб, бу нусхани .com ёки .bat кенгайтмали файл килиб ёзиб куяди. Бундай файлга мурожаат этилганда биринчи .com ёки .bat кенгайтмали файл ишга тушади сунгра эса вирус .exe кенгайтмалисини ишга тушириб юборади.

2. "Чувалчанг-лукмалар" - бу вируслар компьютер сетларига таркайди, файл ва диск секторларини узгартирмайди. Улар компьютер сети оркали хотирага киради. Бошка вируслар адресларини топиб уларга уз нусхаларини ёзиб куяди. Бундай вируслар баъзида файллар тузади, лекин умуман компьютер ресурсларига мурожаат килмайди.
3. "Паразит" вируслар - нусхаларини диск сектори ва файлларга узгартириб таркатади. Бу вируслар юкоридагилардан фаркланади.
4. "Талаба" вируслари - жуда кўп хатоликлар келтириб чикарувчи хисобланади. Улар ҳар-хил ҳарфларни пай до килиши кутилади.
5. "Куринмас Стелс" вируси - узининг имкониятидан келиб чикиб оператив системада файлларни зарарлантириб уз урнига бошка маълумотларни куйиб "кочиб колади". Бу вируслар АВП (антивирус программалари) ни алдаб кетади.
6. "Полиморфик-ажина-мутантлар" вируси -етарлича тутиш қийин булган вируслар хисобланади. Улар Аниқ бир жойда турмайди (кучиб юради). Кўп холларда полиморфик вируслар узининг бир хил нусхасига эга булмайди.
7. "Троян отлари" вируси - керакли дастурлар ичиг-я кириб олиб ҳар бир буйруқ берилганда какшатгич зарба бера олади. У компьютер ва унинг сетлари оркали кўпайиб сезиларли зарарларни пай по ,. килади. '
8. "Макро" вируслари - асосан маълумотларн кайта ишлашга тускинлик килади ва матн муҳаррирларига зарар етказади. Хозирги вактда Microsoft Word, Excel ва Access муҳаррирларида тайёрланган ҳужжатларда кўплаб учраб туради.

Уяли телефонлар учун вируслар.

ILOVEYOU номли вирус уяли телефонлар учун мулжалланган. 2000 йилда Испанияда энг йирик Telefonika уяли алока тармогида бу вирус таркалди. Вирус мобил телефонлар учун мулжалланган бўлиб, матнли маълумотни узатади. У телефонии бузмайди, аммо алокани қийинлаштиради. Бу вирус дунё буйлаб таркалишига йул куйилмади, аммо Handheld асбоблар деб аталувчи портатив компьютерлар тармогини зарарлантирувчи янги турдаги вирусларни яратиш учун асос булиши мумкин.

Windows 98 карокчилик нусхалари билан таркаладиган вирус.

Карнеги-Меллон университета компьютер ходисаларига жавоб берувчи гурух мувофиклаштириш маркази хабарига кура 2000 йил бошида янги вирус пайдо булди. Бу Trojan.kill троян вируси бўлиб, яна -Inst98 деган номга хам эга. У С: дискдаги ҳамма маълумотларни учиради. Дастлаб у Microsoft Windows 98 операцион тизимининг крокчилик нусхаларида учради, бирок вирус электрон почта ва биргаликда фойдаланилаётган тармоқ дисклари оркали хам таркалиши мумкин. Хабар берилишича,

вирус 5682 байт улчамдаги INSTALL.EXE файлида булади. Ушбу файл KEYB.COM клавиатура жойлашиш файлига кучирилади.

REMOTE EXPLORER дастури

1998 йил 17- декабрда MCI/ WorldCom ички тармоқка Remote Explorer номли вирус хужум килди. Бунинг окибатида бир канча сайтлар ва бир неча минг серверлар ва ишчи станциялар зарарланди. Вирус функциясига кура узини System 32ғdrivers га нусхасини хосил килади ва «Remote Exp1огег»хизмати каби узини урнатади шундан сунг узини бошка машиналарга нусха куринишини бошлайди. (факатгина NT тармогида).

Вирус иш бажариш жараёнида бажарувчи файлларни зарарлаши билан биргаликда, танланган матнли файлларни хам ихтиёрий тарзда шифрлайди. Бу фаолият шанба 15:00 дан якшанба 6:00 гача булган даврда кучаяди.

Remote Explorer вируси трояплар туридаги вирусларга кушиш мумкин, чунки компьютер кайта юкланганда у йуколади ва вирус зарарланиши учун уни одатда тезда ишга тушириш керак.

«Чернобўль» вируси

1999 йил 26-апрель куни «Чернобўль» вируси туфайли дунё буйича компьютер фожиаси содир булди. Зарарланган компьютерлар ҳакида Англия, Швеция, Туркия, Япония, Россия, Жанубий Корея, Хиндистон, Мальта, Финлендия, Янги Зеландия ва бошка мамлакатлардан хабар келди. Евро Осиё

китъасининг мамлакатлари катта зарар курди. Умумман олганда тахминан 600000 машина ишдан чикди. Жанубий кореяда 300000 та Хитойда 100000 та, Россияда 100000 та Америкада асосан хусусий сектор, мактаблар ва университетлар (1000) зарарланди.

CIN номли вирус винчестирдаги барча маълумотларни ўчирибташлайди. У Windows 95/98 да ишлайди. Асосий таркалиш йули - электрон почта ва зарарланган дискеталар. Вирус EXE файлларга ёпишиб олади ва из колдирмайди, чунки анъанавий Аниқлаш усулларидан кочиш учун «Space Filler» хусусиятларидан яхши фойдаланади. Вирус куйидагича ишлайди: Hard drive (қаттиқ диск)нинг файл тартиби ёзиладиган соханинг маълумотнинг ўчирибюборади. Бу маълумотсиз система файлларни курмайди сунгра BIOS (Basic input Output System)ra таъсир килиб, ОС ни зарарлайди. Бу эса винчестирдаги маълумотларниинг умуман учиришга олиб келади

Компьютер качон зарарланиши номаълум. Вирусни кенг таркалиши ойлаб давом этган булиши мумкин. Вирус 26-апрель куни ишга тушди. 1986 йил 26-апрель Чернобил фожеаси содир булган кун билан устма-уст тушганлиги учун

Антивирус программалар.

Компьютер вирусларидан ҳимояланиш, уларни йук килиш ва Аниқлаш учун бир неча махсус программалар яратилган. Бундай программалар антивируслар деб аталади. Антивирус программалари турларга булинади:

- программа детекторлар;
- доктор-программалар ёки фаги;
- ревизор программалар;
- филтрловчи программалар;
- вакцина ёки иммунитет программалар.

Детектор-программалар - Аниқ вируснинг ҳарактерли ҳолатини кидиради. Оператив хотира ёки файлдаги керакли маълумотни Аниқлайди. Бундай антивирусларнинг камчилиги шундаки, улар узларига маълум булган вируснигина Аниқлайди.

Доктор-программалар ёки фаги хамда вакцина-программалар нафакат вирусларни Аниқлайди балки, даволайди, файлдаги вирус танасини учиради, файлни асл ҳолатича саклаб колади. Доктор программалар кўп микдордаги вирусларни Аниқлаш ва йук килиш имкониятига эга. Бундай программаларга: AVP, AidsTest? Scan? Norton Antivirus, Doctor Web киради.

Янги вируслар пайдо булган сари юкоридаги антивирусларнинг янги версиялари ишлаб чикиш талаб этилади.

Ревизор программалар - вируслардан ишончли ҳимоя воситаси хисобланади. Ревизорлар дастурларни, каталоглар ва дискнинг система булими .ҳолатини компьютер вирусдан зарарланмасдан аввал эслаб колади. Шундан кейин, фойдаланувчининг хохишига биноан олдинги ва кейинги ҳолатларни солиштиради. Узгарган ҳолатларни экранга чикаради. Файлларни ҳолатини солиштиришда унинг узунлиги, модификация вакти ва санаси, хамда бошка параметрини солиштиради. Ревизор программалар етарлича мураккаб алгоритмларни хатто стелс-вирусларни хам йук килади, вирус бузиб юборган файлларни уз ҳолатига келтиради. Бундай антивирусга кўп таркалган Россиянинг Adinf программаси мисол булади.

Фильтр-программалар ёки «тозаловчи» узида кўп бўлмаган резидент дастурларни мужассамлаштиради. Компьютернинг шубхали ва вирус ҳарактернўй берувчи ишини Аниқлайди. Бундай ҳолатларга:

1. COM ва EXE кенгайтмали файллар тартиби буйича;
2. Файл атрибутларини узгарганига караб;
3. Аниқ манзил оркали дискка ёзиш буйича;
4. Дискнинг юкловчи секторига ёзиш буйича;
5. Резидент программанинг юкланишига караб.

Бирор бир программанинг ишлаш давомида «тозаловчи» ишнинг рухсат этилиши ёки мумкин эмаслиги ҳакида маълумот беради. Фильтр-программалар фойдали хисобланади, у вирусни кўпайиб улгурмасидан олдин Аниқлаш имкониятини беради. Факат улар диск ва файлларни олмайди. Вирусларни йук килиш учун бошка программалар керак булади.

Вакцина ёки иммунитет программалар зарарланган файлларни даволайди. Вакциналар доктор-программалардан яхширок даволайди. Вакцина факат машхур вирусларни Аниқлайди, бунда вирус вакциналанган файл ёки дискни олиб зарарлай олмай колади. Хозирда вакциналар кам кулланилади. Зарарланган файл ва дисклардан, ҳар бир вирус тушган компьютерлардан узокрок юриш вирус эпидемиясидан сакланиш демакдир.

AntiViral Toolkit Pro антивирус программаси.

AVP фойдаланувчи учун кулай интерфейсга эга. Кўплаб кулайликларни фойдаланувчи узи белгилайди ва шу билан бирга жуда кўплаб таркалган вирусларни йук кила оладиган антивирус базасига эга.

AVP нинг иш режими куйидагича: Оператив хотира назорати. Файллар ва архивлар назорати.

Master Boot Record - система сектори, юкловчи сектор ва диск таблица назорати.

AntiViral Toolkit Pro ишининг аҳамиятли томони куйидагича:

- Турли хил вирусларни йук килади, шу билан бирга уз-узини шифрловчи, куринмас ва стеле вирусларни, макро ва Word, Excel ҳужжатлари вирусларини хам йук килади.
- Упаковкаланган файлларни ичини текширади.
- Архивланган файлларни ичини текширади.
- Юмшок диск, локал, сетли ва CD-ROM дискларни текширади.
- Номаълум вирусларни текширади.
- Ортикча текшириш режими.
- Объект ичидаги узгаришларни текшириш.

AVP программаси марказий бошкарув компьютеридан автоматик равишда ишлатиш кулайдир. Бунинг учун, автоматик бошкарув буйругини тузиш талаб этилади. Баъзи бир антивирусларни кискача ҳарактеристикаси.

Dr Solomon's Antivirus Toolkit

Вирусларни Аниқлаш ва уларни йукотиш буйича энг яхши курсаткичларга эга , шуниниг учун хам нархи киммат. Нархи юкорилигига карамай (85$) бу дастур «энг яхши танлов» номига сазовор булди. McAfee фирмасининг VimsScan дастури кўпрок «ёввойи» вирус-ларни учиради. Dr Solomon's Antivims Toolkit

дастурининг интерфейсида ихтиёрий антивирус функциялар, барча маълум вирусларни тулик маълумоти ва уларнинг зараралари ҳакида маълумотлар мавжуд. Бу дастур пакетига таркибига кирувчи юкловчи дискета Bullet («Сехрли ук») ихтимёрий системада вирусларни тез Аниқлайди ва йук килади. Бупакетниниг камчилиги ҳакида янги маълумотларни тармоқ оркали юклай олмаслиги хамда янги версияларни алмаштириш йилига 4 марта булади.

F-Prot Professional

Бу дастур вирусларни яхши Аниқлайди, кенг созлаш имкониятига эга, вирусларни Аниқлаганда электорн алока оркали хабар беради. Дастур камчилиги янги весриялар билан алмаштиришда паролни зарурлиги ва дастурни кайтадан урнатиш зарурлигидир. Вирусларни Аниқлаш буйича утказилган тестда 99 % вирусларни Аниқлади, лекин улардан 78 % ни учира олди. Бу дастур пакетида доимий текширувда кайси дисклар , папкалар ва файллар булиши ёки булмаслиги имкониятлари мавжуд. Бу эса вактдан ютади яъни аввал текширилган файлларни ташлаб утиши хисобига.

IBM AntiVirus v.2.5.

Вирусларни Аниқлашда катта имкониятга эга бўлиб, 1 та пакетда турли операцией системалар билан ишлаш версиялари мавжуд. Дастур камилиги вирусни учиришда консерватив (эскича) усулдан фойдаланиши. Вирусларни янги типини Аниқлашдазамонавий технологиядан фойдаланилади.Пакет нархи 49 % бўлиб, «ёввойи» вирусларни яхши Аниқлайди ва йук килади.

IBM AntiVirus вирус дастури агарда зарарланган файл вирус учиришда бузилиб кетса , у холда бу вирусни учирмайди. Бундай ҳолатда зарарланган файл умуман учирилади ва файлни резерв нусхасидан кайтадан юкланади. IBM AntiVirus дастури шундай ишлаш хисобига «ёввойи» вирусларни 32 % ни учира оладиАммо бошка дастурлар каби , IBM AntiVirus дастури юкловчи секторни заралантирувчи вирусларни 100 % учиради. Афзаллиги: янги версиялар урнатиш учун зарур файллар IBM WEB - сервер оркали олиш мумкин ва уларни урнатиш учун дастур кенг имкониятли менюга эга. Бу дастур пакетида Windows 95, 3.x , DOS ва OS / 2 системалар учун версиялар мавжуд. ENTERPRISE EDITION итшбилармонлари учун дастур пакетида Windows NT система учун версияси хам мавжуд.

Me Afee VirusScan for Windows 95

Вирусларни яхши йук килади, турли операцией системалар билан ишлай олади, энг арзон дастур. Камчилиги: вирусларни яхши Аниқлай олмасли-ги ва янги версиялар учун кушимча хак туланиши. Me Afee VirusScan - машхур антивирус пакетларидан бири хисобланади.

Утказилган тест натижаларига кура Symantec фирмасининг Norton Anti Virus дастури 13 та макровирусларни ушлади, McAfee VirusScan 12 та макровирус ушлади, 1та яъни Imposter номли кам учрайдиган вирусни ушлай олмади. Virus Scan дастури файлли вирусларни «ёввойи» турларини қийин Аниқлайди. Текширув натжаларига кура дастур файлли вирусларни 93 % ни Аниқлади. Агарда ба дастур эффетивлиги юкори булганда эди, у яхши пакет хисобланар эди. Дастурни осон ва тез система параметрларига мослаштириб урнатиш мумкин, бунда дастур параметрларини уз ихтёрингизга кура узгартиришингиз мумкин.
Virus Scan нархи 45$ бўлиб, Windows 95, 3.x ва NT , DOS ва OS / 2 асосий операцион системалар учун версиялари мавжуд. Аммо дастурни имкониятларин кенгайтириш учун кушимча хак тулаш керак. Маълумотлар базаларини янгиланган версияларни WEB да ишлатиш мумкин, лекин McAfee WEB - сахифасига кура янги версияларни компания техник таъминотини хам олиш шарти билан ишлатиш мумкин. Кайд килинган фойдаланувчилар биринчи навбатда уч ой давомида бир марта янги версияни бепул о лиши мумкин. Шуи дан сунг 49 $ га бир йилга тузилган шартнома асосида чекланмаган микдорда дастур янги версияларни ва вирусларни янги белгиларини , хамда доимий телефон маслахатларини олиш мумкин.

Norton AntiVirus 2.0 for Windows 95

Афзаллиги вирусларни жуда яхши Аниқлайди, ажойиб интерфейс, автоматик янгиланиш. Камчилиги: «ёввойи» вирусларни 77 % ни йук килади. Бу дастур тез, ишончли ва содда мулокотли бўлиб, фойдаланувчи учун жуда кулай Мутахассислар эса узларига мослаштириб олиши мумкин.
Norton AntiVirus дастурининг интерфейсида Live Update функцияси мавжуд. Бу функция Web оркали дастурни ва вируслар белгилар тупламини янгилаши мумкин Шу билан бирга вируслар билан кураш Устаси (Virus Repair Wizard) Аниқланган вирус ҳакида тулик маълумот беради хамда уни йук килиш усулларни танлаш имконини беради. Бу усуллар : вирусларни автоматик равишда йук килиш ; боскичма-боскич йук килиш, бу холда учириш жараенини бошкариш мумкин.
Thunder Byte AntiVirus Utilites.
Афзаллиги: файлли вирусларни яхши Аниқлайди, текширишни жуда кулайлиги. Камчилиги: вирусларни учириши қийинрок, янги фойдаланувчилар учун учириш жараёни мураккаб. Биринчи бор Караганда, Thunder Byte AntiVirus Utilites дастури (100 $) янги вирус белгиларни Web юклаш иконият ига эга. Дастур чукуррок урганилганда, у пакетда одатдаги аъзи бир функциялар йук , аммо бир катор янги мукаммал функцияларга эга. Бу дастур Windows 95 системасининг

«Проводник» дастурига ухшаш интерфейсига эга бўлиб, бошка пакетларда мавжуд бўлмаган бир катор кулайликларга эга. Текширишда сиз алохида дискларни , файлларни ёки папкаларни белгилашингиз мумкин. Thunder Byte утказилган тест натижаларига кура юкловчи сектордаги вирусларни 100% ни Аниқлайди, аммо уларни учира олмайди. Шу билан бирга дастур сикилган файлларни текширмайди, бу эса архивланган файлдаги вирусни Аниқланмаслигига олиб келади. Thunder Byte дастури компьютерда чекланган (корпоратив) ҳолатда фойдали булиши мумкин. Файлли вирусларни (макро - вируслардан ташкари) учиришдан аввал TBCLEAN номли алохида DOS утилитали дискета хосил килиш керак. Дискетадан юкланиш, текшириш жараёнида хотирадаги вирусни фаоллашишига имкон камаяди, чунки бунда зараланган юкловчи сектор ва файлларга мурожат булмайди.

Евгений Касперский Антивирус дастури

AntiViral Toolkit Pro by Eugene Kaspersky (AVP) Microsoft кор-порациясининг тест лабораториясида сертификатланган ва "Desig-ned for Microsoft Windows95/NT", " Designed for Microsoft Win-dows 98/NT " белгиларни олган. Бу системанинг махсулотларидан бири, AVP for Windows'98? Secure Computing (АКШ ва Буюк Бри-тания) компьютер хавфсизлиги журналининг тест лабораториясида IN-the-Wild вирусларни детектирлаш буйича текширилди ва «CheckMark» белгисини олди. Бундан ташкари , AVP бошка халка-ро сертификат ва совринларга (ICSA компьютер хавфсизлиги хал-каро америка корпорацияси соврини) эга. AVP антивирус системаси таркибига бир нечта дастурлар киради:

- DOS, WINDOWS 3.XX, Windows 95/98/NT , OS/2 операцион тизимлар да ишчи станциялар учун AVP версияларидан ;
- AVP инспектори - дискни узгаришлардан ҳимояловчи ревизор ;
- AVP for Novell Netware ва AVP for Windows NT -серверлар учун AVP версиялари ;
- Брэндмауэр (Firewall - 1) лар учун Интернетда антивирус ҳимоя.

AVP умумий ҳарактеристикаси.

Умуман система:

- Файллардаги, юклаш секторлардаги ва оператив хотирадаги барча мавжуд турдаги файлларни излайди ва учиради ;
- «Сикилган» файлларда (PKLITE, LZEXE, DIET, COM2EXE ва бошка дастурлар форматларида) вирусларни Аниқлайди ва учиради ;
- ZIP, ARJ, LHA, RAR форматлардаги архив файлларни текширади ;

• Машхур электрон алока системалар учун локал алока кутиларни вирусга текширади;
• Эвристик механизм ёрдамида номаълум вируслар ва 32-разрядли вирусларни излайди ;
• Ностандарт заралайдиган ва файлларни бузувчи вирусларни Аниқлаш учун сканерлаш ҳолати мавжуд.

Ишчи станцияларни ҳимоялаш.

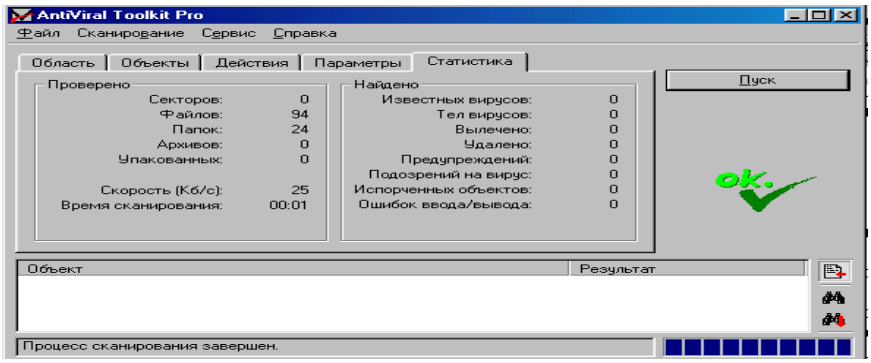
Winfows 95, 98 , NT ва OS / 2 лар учун AVP версиялари рези-дент монитор ёрдамида фонли режимда доимий ҳимояни таъмин-лайди.

DOS учун AVP версияси 2 вариантда мавжуд : интерфейс билан ва буйруқ сатри курининшида (AVPLITE). AVPLITE аввалги машиналарда (INTEL 286) хам ишлаши мумкин. AVPLITE - AVP туркумидаги бошка сканерлар имкониятларига эга.

AVP INSPECTOR дастури ишчи станцияларга кушимча ҳимояни таъминлайди. Бу дискни узгаришлардан ҳимояловчи ревизор.Дастур Windows 95/98/NT бошчилигида ишлаб, файллар ва директориялардаги, системали секторлардаги барча узгаришларни Аниқлайди.Дастур ажойиблиги, вирус хисобига ва вирус хисобига бўлмаган файлдаги узгаришини Аниқлай олиши.Масалан, AVP Inspector ёрдамида системанинг иш фаолияти (Системали реестр) боғлиқ булган ресурслардаги узгаришларни Аниқлаш мумкин. AVP Inspector сканерлаш (текшириш) вактини тежайди, чунки AVP сканери факат узгарган файлларни текширади. Бундан ташкари, дастур вирус туфайли зарарланган ва бузилган файллар ёки секторларни узи тиклаш имкониятига эга.

AVP Inspector кулай график интерфейс (GUI), кўп максадли иш юритиш, кўп окимлилик, соф 32-разрядилилик, IOS (киритиш-чикариш супервизори ёки 32-битли драйвер) драйвери оркали тугридан-тугри физик ва мантикий дискларга мурожаат килиш имкониятларига эга.

Серверларни антивирус ҳимоялаш.



Корпоратив тармоқларга кирган вируслар кўпрок салбий таъсир утказади. Шуни хисобига, кўплаб компаниялар унлаб, баъзида юзлаб миллион дбллар йукотади.

AVPN (ёки NorellNetware учун Касперкий антивирус) - бу сканер, хам фильтр бўлиб, доимо сервердаги файлларни назорат килиб туради. AVPN сканер ҳолатида
NorellNetware (3.11 версиядан бошлаб ва IntranetWare файл-серверида жойлашган) файлдаги вирусларни излайди, фильтр ҳолатида файлларни назорат килади, яъни файлларни укишда, ишга туширишда ва серверга ёзишда текширади.
AVPN зарарланган файлларни Аниқлагандан сунг уларни бошкарувчисига курсатмасига биноан, файллар дискдан ўчирибюборилиши, курсатилган жойга файлни кучириши, файл номини узгартириши мумкин. Агар да зарурат тугилса AVPN ишчи станцияни тармоқдан узиб, тармоқ администраторига хабар жунатади. AVPN нинг сканер ҳолатида битта тармоқ жойлашган узокдаги сервер томларини хам текширади.
Бундан ташкари, AVPN янги антивирус базаларини юклашга имкон беради ёки антивирус база маълумотларини AVPN дан чиқмасдан туриб тулик алмаштиришга имкон беради.
Тармоқ бошкарувчиси, AVPN билан ишлаш мобайнида унга янги созлашларни киритиши ва хотирага саклаши мумкин. Шу билан бирга ишчи станциядан дастурни ишаг тушириши ва бошкариши мумкин. AVPNHH сканер сифаьтда фойдаланилаётганда бошкарувчи уни жадвал асосида хамда ихтиёрий вакт мобайнида ишлатиши мумкин.
AVP for Windows NT Server дастури хам янги кулайликларга эга. Унинг ёрдамида система бошкарувчи тармоқдаги антивирус хавфсизлик стратегиясининг марказлашган холда бошкариши мумкин.
Бу дастур ишчи станциялардаги ва серверлардаги AVP функциясини текширишга имкон беради, хамда битта ишчи жойидан бутун тармоқ билан бошкаришга имкон беради. Хусусан, тармоқнинг барча объектларини мослаштиради. Дастур бошкарувчи тармоқнинг жорий ҳолати ҳакида тулик хисобот тузади ва ҳар бир ишчи станция учун автоматик янгилаш утказади.

Брэндмауэрлар учун антивирус.

Брэндмауэрлар хам ҳимоя учун тузилади. Тармоқ рухсатсиз киришга тускинлик килгани билан доимо хам вирусларни йукота олмайди. Касперский лабораторияси, CVP (масалан, ChekPoint Fire Wall-1) протоколини таъминловчи, ихтиёрий брэндмауэрлар учун AVP for Fire Wall дастурини яратади.

AVP for Fire Wall - бу антивирус сервери бўлиб, HTTP, FTP, SMTP ва бошка протоколлар буйича кабул килинаётган файлларни текширади. Вирус Аниқланган ҳолатда, у файлни даволайди, зарарланган файл

узатилиши тухтатилади, файлни алохида каталогга жойлайди ва бошкарувига алока оркали хабар беради.

Уз-узини ҳимоялаш рецептлар:

! Энг яхши ҳимоя компьютерга вирусни якинлаштирмаслик.

- умумий доимо текшириб туриш ;
- дискетга ёзиш ҳимоясини урнатиш ;
- янги юкланган файлларни текширмасдан ишлатмаслик;
- шахсий компьютер «беркитиб» куйиш;
- доимо антивирус дастурини янгилаб бориш.

Антивирус дастурларини тест натижалари:

Антивирус дастури	Платфор-ма	Аниқлан ган «ёв-войи» вирус-лар, %	Учирил-ган «ёв-войи» вирус-лар, %
DrSolomon's AntiVirus Toolkit	Windows 95	100	89
F - Prot Proffessional	Windows 95	99	78
IBM Anti Vims v.2.5	Windows 95	96	32
McAfee Virus Scan	Windows 95	93	90
Norton Anti Virus v. 2.0	Windows 95	100	77
Thunder Byte Antivirus Utilites	Windows 95	95	60
Touchstone PC - Cillin II	Windows 95	100	80
McAfee Virus Scan	Windows NT	92	59

Norton Anti Vims v. 2.0	Windows NT	100	76

"**Троя тулпори**" - бу шундай программаки, у асосан ҳужжат ларда ёзилмаган қўшимча ҳаракатларни бажаради. қадимги Рим Троя тулпорининг аналоги бўлмиш "Троя тулпори" шубҳа ўйғотмайдиган қобиқ программаларга таъсир кўрсатиб, автоматлаштирилган система хавфсизлигига таъсир кўрсатувчи жиддий таҳдид ҳисобланади. Характерига кўра "Троя тулпори"пакет режимида ишловчи программа воситалари ёрдамида амалга ошириладиган фаол таҳдидлар турига киради. У системанинг ихтиёрий объектига тахдид солиши мумкин. Энг хавфлиси - опосредованнўй таъсир, яъни "Троя тулпори" бир фойдаланувчи ваколатлари доирасида ҳаракат қилади, лекин бошқа фойдаланувчи борасида эса унинг шахсини аниқлаш мумкин эмас.

"Троя тулпори" хавфи асосан кейинчалик система фойдаланувчиларига таклиф этиладиган (инъом этиладиган, сотиладиган ёки алмаштириладиган) зарарсиз программага у ёки бу усул билан қушилган қушимча командалар блокига таъсир этишидадир. Бу командалар блоки бирор шарт (ой, йил, кун, вақт, ташқи команда) киритилганда ёки бажарилганда ишга тушади. Бундай программани ишга туширувчи ўзи ва ўзи билан бирга бутун системани ҳавф остида қолдиради.

Агар «троя тулпори»ни ишга туширган фойдаланувчи кенг имтиёзлар наборига эга бўлса, бу ҳолда унинг хавфи анча юқори бўлади. Бундай ҳолларда «троя тулпори» ни тузган ва ўзлаштирган ҳамда кенг имтиёзлар наборига эга бўлмаган бузғунчи бошқаларнинг қўли билан рухсатсиз имтиёзли функцияларни бажариши мумкин. Ёки, масалан, бундай программани ишга туширган фойдаланувчининг маълумотлар набори бузғунчини жуда қизиқтириб қолиши мумкин, бунда бузғунчининг ҳатто кенг имтиёзлар наборига эга бўлмаслиги унинг системага рухсатсиз таъсирларига тўсиқ бўла олмайди. Бунга мисол қилиб, 1999 йил январда Интернетда пайдо бўлган текин тарқатилувчи Screen saver (заставка) ни олиш мумкин, у компьютерда DES алгоритми асосидаги шифрловчи программани қилиришни амалга оширади ва агар уни топса, шифрлаш калитларининг алмашиниш жараёнини назорат қилиб, бу калитларни электрон почта орқали Хитойдаги аноним-серверга узатади. Ундан ҳимояланишнинг радикал услуби – бу программани ижро этишда берк муҳитни ташкил этишдир. Айниқса ташқи Интернет ва ички тармоқларни лоақал протоколлар сатҳида бир-биридан ажратиш (агарда бу жараён физик сатхда амалга оширилса янада яхши бўларди) лозим. Шунингдек, имтиёзли ва

имтиёзсиз фойдалнувчилар турли к¢ринишдаги, индивидуал равишда сақланиши ва ҳимояланиши шарт б¢лган программалар билан ишлагани маъқул. Бу тадбирлардан фойдаланган ҳолдагина «троя тулпори» каби программаларнинг қабул қилиниши камаяди.

Вируслар. Ҳозирда компьютер вирусига дуч келмаган бирорта ҳам система администратори ёки фойдаланувчини топиб бўлмайди. Creative Strategy Research фирмаси томонидан ўтказилган тадқиқот натижаларига кўра сўров ўтказилганда 451 мутахассисдан 64% и вирусга дуч келганини маълум қилишади. Ҳозирги кунда маълум бўлган минглаб вирусларга ҳар ойда 100-150 штаммдан келиб қўшилмоқда.

Вирус – бу шундай программаки, у бир программадан иккинчисига тез тарқала олиш хусусиятига эга б¢либ, бошқа программаларнинг таркибига ¢зининг программа таркибини ¢згартирувчи хусусиятларини қ¢шиб қ¢яди. Вируснинг 2 та асосий хусусияти характерланади:

- ¢зидан-¢зи к¢пайиш: унинг бирор маълумот т¢пловчи ёки элтувчи таркибида яшаш даврида камида битта нусхага к¢пайиш хусусияти;
- ҳисоблаш жараёнига халақит бериш – тирик табиатдаги вирусларга хос паразитлик хусусияти.

Вируслар ҳам «троя тулпори» каби фаол таъсир этувчи программа б¢либ, қуйидаги 4 та қисмдан иборат структурага эга б¢лади:

1-қисм – программа кодини акс эттиради, вирус унинг ёрдамида ЭҲМ хотирасига тушади;

2-қисм – вируснинг д иск хотирасига, улардаги файллар ва юклаш секторига к¢чирилиш ишини таъминлайди;

3-қисм – вируснинг ¢з фаолиятини ишлаш шарт-шароитларини ¢з ичига олади;

4-қисм – вируснинг асосий иши – бузғунчилик фаолиятини алгоритмини ¢з ичига олади.

Компьютер вируслари ишлаш соҳасига қараб:

1. Компьютер системасидаги информацияни зарарловчи;
2. Компьютер системаларига инфекция юқтирувчи;
3. Компьютер системалари ва тармоқларининг ишини батамом тугатувчи турларга б¢линади.

Ҳозирги пайтда вирусларнинг синфланиши, уларда қулланиладиган вирусни юқтириш усуллари, уларга қарши курашиш чора-тадьирлари яхши ¢рганилмоқда.

Вируслардан ҳимояланишда икки томондан ёндашиш мумкин:

- мустақил, алоҳида масала сифатида;
- автоматлаштирилган системанинг умумий хавфсизлигининг бир жиҳати сифатида.

Бу ёндашувларнинг иккиси ҳам ¢зининг алоҳида хусусиятларига ва мос равишда масалани ечишнинг ¢зига хос усулларига эга.

Вирусга қарши курашнинг бир томони сифатида Ҳозирги пайтда вирусга қарши программалар системаси ишлаб чиқилмоқда. Уларнинг к¢пчилиги мос тиббий атамалар: «Вакцина», «Антитоксин», «Интерферон» ва ҳ. атамалар билан аталмоқда. Умуман олган вирусга қарши прграммаларни 3 гуруҳга ажратиш мумкин:

1. Фильтловчи программалар;
2. Вирус детекторлар (вирус ушловчилар, ревизор программалар, инфекцияга қарши программалар);
3. Фаг программалар.

Фильтрловчи программалар – заҳарланишни бартараф этиш учун ишлаб чиқилган программалар. Улар компьютер хотирасига жойлашиб олиб вируснинг уринишларини ва сигналларини кузатиб, олиб бораётган ишларини назорат қилади.

Вирус детекторлар – система ҳолатининг фото тасвирини олиб, уни доимий иш фаолияти ҳолати билан таққослаб туради. Агарда бирор ¢згариш содир б¢лса, хавф т¢ғрисидаги сигналини беради. Бошқа ревизор программалар математик формулалар ёрдамида программа ва маълумотлар бутунлигини аниқлаб берувчи назорат кодлари йиғиндисини ҳисоблаш га асосланади.

Фаг программалар – оддий вирусларни топиб, илдизини й¢қотишга ¢ргатилган программалар. Улар к¢проқ эски вирусларни топиб й¢қотишга қулайдир.

Олиб борилган чора-тадбирлар натижасида, юқорида келтирилган программаларнинг фаолияти натижасида охирги пайтларда вируслар билан зарарланиш ва бузилиш масштабини камайтиришга эришилди. Лекин бу программаларнинг тараққиёти вирусларнинг тараққий этишига ета олмаяпти. Сўнгги йилларда компьютер вирусларидан ҳимояланишнинг истиқболли йўлларидан бири сифатида аппарат ва программ ҳимоя усулларининг биргаликда ташкил этилишидан фойдаланилмоқда. Бундай аппарат-программ воситаларга компьютернинг стандарт кенгайтириш слотларига ўрнатиладиган махсус вирусга қарши платаларни мисол қилиш мумкин. Масалан, Intel корпорацияси 1994 йилдаёқ компьютер тармоқларини вирусдан ҳимоялашнинг истиқболли технологияси - Intel EtherExpress PRO/10 қурилмасини таклиф қилган эди. Intel EtherExpress PRO/10 қурилмаси компьютернинг бутун системасини ОС юклангунга қадар текшириб чиқувчи вирусга қарши программага ҳам эга.

«қурт» - вируслардан фарқли равишда ¢з нусхасини ахборот элтувчида қолдирмайдиган, тармоқ орқали тарқалувчи программалар.

«қурт» тармоқнинг бирор зарарланган узелини аниқлаш механизмидан фойдаланган ҳолда, ¢зининг танаси ёки бирор қисмини ушбу узелга узатади ҳамда шу пайтнинг ¢зида ишга тушади ёки бирор пайт пойлаб ишга тушади. Бундай турдаги программаларнинг энг машҳури – «Моррис қурти» б¢либ, 1988 йилда Интернет халқаро тармоғига катта зарар етказган.

«қурт»нинг тарқалиши учун энг қулай шароит бу – тармоқ фойдаланувчиларининг бир-бирига д¢стона, ишонувчан муносабатларидир. Ундан ҳимояланишнинг энг яхши усули бу тармоқдан рухсатсиз фойдаланишга қарши эҳтиёт чораларини қ¢ллашдир.

Хуллас, «троя тулпори», «қурт», вирус программалар каби зарарли программалардан ҳимояланиш учун программаларни ижро этишнинг берк муҳитини ташкил этиш, ижро этилувчи файлларга киришни чеклаш, ишлатилаётган программа воситаларини тестлаш ва ҳ. ни амалга ошириш зарур.

Фойдаланилган сайтлар рўйхати

- www.securityfocus.com-портал: материалў по безопасности
- www.sans.org-Институт SANS: статьи по безопасности, проектў
- www.xforce.iss.net-база даннўх уязвимостей, материалў по безопасности
- www.packetfactory.net-сайт разработчиков библиотеке
- blacksun.box.sk/ tutorials.html-аспектам сетевой безопасности работў с сетевўх сервисов.
- www.phrack.com - журнал «Phrack»
- www.cerias.purdue.edu-Центр информационной безопасности Университет Пурду , архив программного обеспечения