ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

НИЗОМИЙ НОМИДАГИ ТОШКЕНТ ДАВЛАТ

ПЕДАГОГИКА УНИВЕРСИТЕТИ

ФИЗИКА - МАТЕМАТИКА ФАКУЛЬТЕТИ

«Ҳимояга рухсат этилсин»

Факультет декани ф.-м.ф.н.,доц.

_____ Д.Юнусова

«____» _____2012 йил

5140100-«Математика ва информатика» таълим

йўналиши IV курс 401 гуруҳ талабаси

ЮСУПОВА Ирода Бахтиёровнанинг

«ФАЙЛЛАРНИ АРХИВЛАШ ВА КОМПЬЮТЕР ВИРУСЛАРИДАН САҚЛАНИШ ДАСТУРЛАРИ БИЛАН ИШЛАШ МЕТОДИКАСИ» мавзусидаги

БИТИРУВ МАЛАКАВИЙ ИШИ

Талаба: _____ И.Юсупова

Илмий раҳбар: «Информатика ва ТАТ» кафедраси доценти
_____ Б.И.Холдоров

Тақризчи: «Информатика ва ТАТ» кафедраси катта ўқитувчиси
_____ И.Мамаражабов

Тақризчи: А.А.Хўжаев номидаги Республика дизайн КХК информатика ўқитувчиси
_____ Б.Халилова

«Ҳимояга рухсат этилсин»

«Информатика ва ТАТ» кафедраси

мудири п.ф.н. доц._____ М.Э.Мамаражабов

«____» _____2012 йил

Тошкент 2012

Мундарижа

КИРИШ

Битирув малакавий иши мавзусининг долзарблиги. Бугунги кунда деярли ҳар дақиқада сайёрамизнинг турли бурчакларида ўзгаришлар, янгиланишлар, кутилган ва кутилмаган воқеа-ҳодисалар содир бўлмоқда. Ҳар бир кунимиз кучли ахборот оқими остида кечмоқда. Биз уйда, ишда ва жамоат жойларида, энг кўпроғи таълим жараёнида ахборот оқимидан хабардор бўлиш, янги билимлар ва изланишлар натижаларидан хабардор бўлиш эҳтиёжи вужудга келади. Замон шуни тақозо қилаяптики, инсоният ахборот оқимидан узилган ҳолда нормал фаолият юрита олмайди. Замонавий тараққиёт босқичида ҳаётни англаш, уни ўрганиш, таҳлил қилиш ва тадбиқ қилиш ахборотларни йиғиш ва ўзлаштириш, саралаш ва қайта ишлаш орқали кечади. [1]

Юқоридагидан келиб чиқиб айтиш мумкинки, инсоннинг билимлилик даражаси, эгаллаган маълумоти ҳам маълум давр мобайнида шахс томонидан ўзлаштирилган ахборотларнинг кўп ёки озлиги билан белгиланади.

Президентимиз республикамиз мустақилликка эришиш арафасидан таълим тизимига, ёшларни таълим олиш, юксак интеллектуал салоҳиятли, бой дунёқарашга эга баркамол авлод бўлиб етишишларига алоҳида эътибор қаратдилар: “Фанга истеъдодли ёшларнинг кириб келишини таъминлаш учун комплекс тадбирлар туркумини амалга ошириш зарур. Бу борада олий мактабнинг, ҳатто, умумий таълим мактабларининг фаолиятини тубдан қайта қуриш керак.”[2]

Президентимиз таълимнинг жамият ривожидаги ўрнига “Шуни унутмаслигимиз керакки, келажагимиз пойдевори билим даргоҳларида яратилади, бошқача айтганда, ҳалқимизнинг эртанги куни қандай бўлиши фарзандларимизнинг бугун қпндай таълим ва тарбия олишига боғлиқ”. [2]

Бугунги кунда барча соҳалар каби таълим соҳасида ҳам компьютер тизимлари ва унда сақланаётган оддий ахборотларни ҳимоялаш сиёсати ва дастурини амалга ошириш жараёнига эътиборни қаратиш зарурлигини шарт

қилиб қўйди. Шу боис хозирги кунда таълим муассасаларида ахборот хавфсизлиги соҳасида таълим бераётган ўқитувчилар, ўқувчилар ва компьютер синфларига хизмат кўрсатувчи ходимлар ахборотларнинг бузилиши, ўғирланиши ва йўқотилишига таҳдид солувчи айрим хужумларга қарши кураш учун нафақат ахборотларни ҳимоялаш воситаларига эга бўлиши, балки уларни ишлатиш принципларини тушуниш, ахборот хавфсизлиги ҳақидаги асосий тушунчаларни, операцион тизим ва компьютер тармоқларидаги ахборотларни ҳимоялаш, ахборот хавфсизлиги бўйича асосий қонун ва стандартларни, ахборотларни шифрлашнинг асосий алгоритмларини ва умуман ҳимоялаш усулларини пухта билишлари зарур.

Компьютер тизимларида ахборотни ҳимоя қилиш муаммоси улар яратилиши билан деярли бир вақтнинг ўзида, ёмон ниятли ҳаракатларнинг натижасида келиб чиқди. Шу туфайли ҳам замонавий ахборотлашган жамиятда ахборотлардан фойдаланиш борасида ахборотни ҳимоя қилиш бўйича ўзига хос муаммоларни ҳам ечишга тўғри келади. Бу борада ахборотнинг махфийлиги ва бутунлигини таъминлаш учун керакли техник ва дастурий воситалардан самарали фойдаланишни ташкил қилиш, ҳозирги куннинг муҳим масалаларидан бири эканлигини ҳаммамизга маълум. Ахборотни тасодифий хавфлардан ҳимоя қилишнинг энг самарали усуллари файлларни архивлаш ва компьютерга тушувчи вируслардан сақланиш дастурлари билан ишлаш ҳисобланади.

Бизнинг битирув малакавий ишимизда ҳам айнан шу мавзу- файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш методикаси тўғрисида фикр юритилган.

Илмий янгилиги:

- файлларни архивлаш дастурлари ва компьютер вирусларидан сақланиш дастурларининг дидактик аспектларининг назарий таҳлил қилинганлиги;

- информатика фанини ўқитишнинг назарий дарсларида файлларни архивлаш ва компьютр вирусларидан сақланиш дастурлари билан ишлаш методикаси;

- информатика фанини ўқитишнинг лаборатория машғулотларида ва мустақил ишларни бажаришда файлларни архивлаш ва компьютр вирусларидан сақланиш дастурлари билан ишлаш методикаси.

Битирув малакавий ишининг амалий аҳамияти. Информатика фанини ўқитишда файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш методикасидан фойдаланилса,талабаларда ахборотларни ҳимоя қилиш, унинг бузилиши, йўқотилишига таҳдид солувчи айрим хужумларга қарши курашиш, ахборотларни ҳимоялаш воситаларини ишлатиш принципларини тушуниш, ахборот хавфсизлиги ҳақидаги асосий тушунчаларни, операцион тизим ва компьютер тармоқларидаги ахборотларни ҳимоялаш ва умуман ҳимоялаш усулларини пухта билишлари ҳақидаги билимлари тезда шаклланади, шунингдек талабаларнинг кўникма ва малакалари ошади.

Битирув малакавий ишининг мақсади файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлашни ўргатиш.

Битирув малакавий ишининг вазифалари:

- файлларни архивлаш ва компьютер вирусларидан сақланиш дастурларини билан танишиб чиқиш, илмий адабиётларни таҳлил қилиш, умумлаштирилган хулосалар чиқариш;

- файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлашнинг дидактик жиҳатларини асослаш;

- файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлашни ўргатишда замонавий педагогик технологиялар ва интерфаол усуллардан фойдаланиш;

- файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлашни ўргатишда замонавий педагогик технологиялар

ва интерфаол усулларни фойдаланиб ўқитишнинг таълим технологиясини ёритиш.

Битирув малакавий ишининг объекти - информатика ўқув фани доирасида файлларни архивлаш дастурлари, компьютер вируслари ва улардан ҳимоя дастурларини ўқитиш жараёни.

Битирув малакавий ишининг предмети –ўқувчиларда файлларни архивлаш ва компьютер вирусларидан сақланиш дастурларини ўқитиш методикаси.

Битирув малакавий иши кириш, 2та боб ва 5 та параграф, хулоса ва фойдаланилган адабиётлар рўйхатидан ташкил топган. **Биринчи бобда** файлларни архивлаш, файлларни архивлаш дастурлари ва компьютер вируслари турлари ва вируслардан сақланиш дастурларининг аҳамияти, компьютер вирусларидан ҳимоя қилиш йўллари ҳақида маълумотлар берилган. Битирув малакавий ишимизнинг **иккинчи бобида** эса, информатика ва ахборот технологиялари фанининг назарий дарсларида, лаборатория машғулотларида файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш методикаси, ахборотларни ҳимоя қилиш бўйича кўрсатма ва тавсиялар берилган. **Иккинчи боб сўнгида** эса битирув малакавий ишининг педагогик тажриба-синов натижалари келтирилган.

I – БОБ. ФАЙЛЛАРНИ АРХИВЛАШ ВА КОМПЬЮТЕР ВИРУСЛАРИДАН САҚЛАНИШ ДАСТУРЛАРИ

1.1. Файлларни архивлаш дастурлари ва уларнинг аҳамияти

Компьютердан фойдаланиш жараёнида турли сабабларга кўра магнит дисклардаги маълумотлар ўчирилиши ёки зарарланиши мумкин. Бу магнит дискини ишдан чиқиши, файлларнинг нотўғри таҳрири ёки файлни эҳтиётсизлик оқибатида ўчирилиши, ёки компьютер вирусининг зарари натижасида юз беради. Шу сабаб бундай кўнгилсизликларнинг олдини олиш учун фойдаланувчи файлларнинг архив нусхасини олиб туриш, ҳамда уларни керак бўлганда яна тиклаш мумкин бўлади. Ундан ташқари компьютерга антивирус дастурларини жойлаштириб, керак бўлганда хавф сезилган папкаларни текширишдан ўтказиб туриш лозим бўлади.

Компьютер хотирасида фойдаланувчи ишлаши учун керак бўлган кўплаб файллар сақланади. Бу файллар баъзан эҳтиётсизлик оқибатида ёки бошқа сабаблар, масалан, компьютер вируси зарари натижасида ўчирилиб кетилиши мумкин. Шунинг учун керакли файлларнинг нусхасини архивли файлга жойлаб қўйиш мақсадга мувофиқ. Файлларни архивлаш натижасида нафақат файлларнинг ўчирилиб кетилиши олди олинади, балки дискларда бўш жой кўпаяди. Файлларни архивлаш натижасида дискларда матнли файллар учун 60–70 фоиз, бажарилувчи файллар учун 20–30 фоиз бўш жой тежалади.

Архивлаш деганда, файл ёки файллар гуруҳининг сиқилган ҳолда битта файлга жойлашиши тушунилади. Архивли файлларда асосан компьютер хотирасида узоқ муддатли сақланувчи ва муҳим бўлган дастурлар сақланади. Маьлумотларни хажм жихатдан кичрайтириш учун архивлаш дастурларидан фойдаланиш мумкин. Архивлаш натижасида бир нечта файл, хатто каталоглар сиқилган ҳолда бир файлга бирлаштирилади, архив файлни очиш натижасида улар ўз ҳолатига қайтарилади.

Файлларни архивли нусхасини яратиш учун махсус архивловчи дастурлардан фойдаланилади. Бу дастурлар дискетадаги жойни тежайди ва архив файлидан фойдаланишда қулайликлар яратади. Архивловчи дастурлар файл нусхасини дискда сиқиб жойлаштиради, файлларни архивдан олиш ва архив мундаражасини кўриш имконини беради.

Архивлаш дастурлари — дискда жойни тежаш максадида файллар хажмини кичрайтиришга имкон берувчи дастурлар. Улар турлича куринишда ишлатилса-да, ишлаш тамойили бир хил: файлларда айнан такрорланадиган ўринлар мавжуд бўлиб, уларни дискда тўлиқ сақлаш мазмунсиздир. Архивлаш дастурларининг вазифаси такрорланадиган шундай бўлакларни топиб, уларнинг ўрнига бошқа бирор маълумотни ёзиш ҳамда уларнинг кетма-кетлигини аниқ кўрсатишдан иборатдир. Бундан кўринадики, турли файллар учун уларнинг сиқилганлик даражаси турлича бўлади. Масалан, 80-90%, график ахборотлар 60-70%, расм файллар 20-30%, бажарилувчи файллар эса 10-20% га сиқилади. Дастурлар ифодаланган файллар эса жуда кам — 1% га якин сиқилади. Ўртача қилиб айтганда архивлаш дастурлари файллар хажмини 1,5 — 2 баробар қисқартиришга имкон беради.

Архивли файл бир неча файлларнинг сиқилган ҳолда бир файлга жойлашган мажмуидир. Архив файл мундарижага эга. Унда файллар номи, охирги ўзгартириш вақти ва санаси, файлнинг дискдаги ва архивдаги ҳажми ва текшириш коди ҳақидаги маълумот берилади.

Архивлаш дастурлари анчагина. Улар қўлланиладиган математик усуллар, архивлаш, архивни очиш тезлиги ва энг асосийси, сикиш самарадорлиги билан бир-биридан фарқ қилади. Архивлаш дастурларидан етарли даражада тез ва яхши ишлайдиганлари PKZIP, LHARC, **ARJ, RAR** дастурларидир.

Архив файл ягона файлга бирлаштирилган бир ёки бир неча файлнинг сиқилган холдаги куриниши бўлиб, ундан керакли холларда файлларни дастлабки кўринишдан чиқариб олиш мумкин. Архив файл ундаги файллар

номларини кўрсатувчи мундарижага эга бўлади. Архивда жойлашган ҳар бир файл ҳақида маълумот берувчи мундарижада қуйидагилар жойлашган бўлади:

— файл номи;

— файл жойлашган каталог ҳақида маълумот;

— файл ўзгартирилганлигини кўрсатувчи сана ва вақт;

— файлнинг дискдаги, архивдаги ўлчами ва параметрлари.

Архивловчи дастурлар ва уларнинг имкониятлари

MS DOS тизимида кўп ишлатиладиган архиваторларга қуйидаги архивлаш дастурлари киради:

Arj дастури. Бу дастур формати қуйидагича берилади:

Arj <буйруқ> <архив файли номи> ><Файллар номи>

Бунда:

Буйруқ - дастур бажарилиши лозим бўлган вазифа турини англатади. Масалан, а- файлларни архивга қўшиш, е-файлларни архивдан тиклаш. Агар файллар номи берилмаса катологдаги барча файлларни битта архивга киритади.

Масалан:arj a test, arj a doc.

Файлларни тиклашга мисол:arj e test.arj;arj e pe2.arj.

Pkzip ва Pkunzip дастури. Бу дастур формати қуйидагича:

Pkzip<Режим><Архив файл номи><Файллар номи>

Файллар номи - архивга кирувчи файллар рўйхати бўлиб улар вергул билан ажратилади.

Режим «-» ёки «/» белгиси билан бошланиб қуйидаги вазифаларни аниқлайди:

-A- архивга барча файлларни киритади.

-U- архивга янги файлни киритади;

-M- файлларни архивга кўчиради;

-D- архивдаги файлни ўчиради.

Агар режим кўрсатилмаса «А»- режим тушунилади.

Мисоллар:

Pkzip -a test - бу буйруқ барча жорий катологдаги файлларни архивга жойлайди.

Pkzip -a doc *.doc - бу буйруқ жорий катологдаги барча doc кенгайтмага эга файлларни архивга жойлайди.

Pkunzip дастури формати қуйидагича:

Pkunzip<Режим><Архив файл номи><Файллар номи>

Параметрлари:

Архив номи- файлларни қайта тикланаётган архив номи кўрсатилади.

Файллар номи- тикланиши керак файллар номи.

Режимлар:

-x- файлларни архивдан олиш;

-v- архивдаги файллар таркибини кўриш.

Мисоллар:Pkunzip -x- test.zip;Pkunzip -v- test.zip.

Агар режим қўйилмаса -x- режим ишлайди.

Компьютерда файлларни архивлаш учун махсус архивловчи дастурлар мавжуд. Windows операцион тизимида файлларни архивлаш учун қуйидаги дастурлардан фойдаланилади: **WinRar, WinZip, WinArj** ва ҳоказо. Бу архивловчи дастурлар бир-биридан сиқиш даражаси, тезлиги, умуман олганда имкониятлари билан фарқланади. Кенг тарқалган архивловчи дастурлар деярли бир хил имкониятга эга, яъни бири иккинчисидан барча параметрлари бўйича устунлик қилолмайди. Бир дастур тез ишласа, бошқаси файлларни яхши сиқиш даражасини таъминлайди. Архивли файлларни номлаш ҳам худди оддий файллар каби амалга оширилади ва қайси архивловчи дастур ишлатилганига қараб, махсус кенгайтмага эга бўлади. Архивли файл мундарижага эга, унда қандай файллар сақланаётганлиги кўрсатилади. Архив мундарижасида қуйидаги маълумотлар сақланади:

- файл номи;

- файл сақланувчи каталог тўғрисида маълумот;
- файлнинг охирги марта қайта ишланган санаси ва вақти;
- файлнинг дискдаги ва архивдаги ўлчами;
- архивнинг тўлиқлигини текширишда ишлатиладиган ҳар бир файлнинг циклик текшириш коди.

Windows тизимида кўп ишлатиладиган архиваторга **Winrar** дастури киради. Бу дастур Windows тизимига ўрнатиладиган дастур бўлиб, у ўрнатилганда контекст менюсига янги буйруқ бўлиб қўшилади. Бирор папкани белгилаб контекст менюсидан Дабавить в архив… буйруғи берилса папкадаги барча файллар сиқилган .rar кенгайтмали битта архив файлига бирлашади. Агар мулоқот дарчасидан zip танланмаси белгиланса .zip кенгайтмали архив файли бўлади.

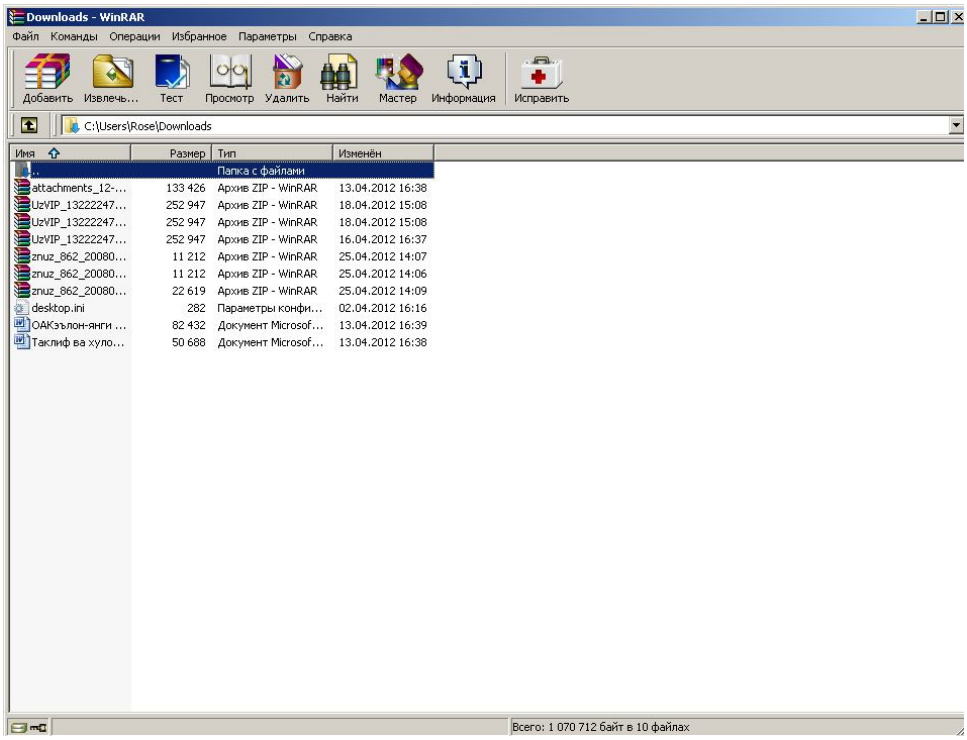
Windows тизимида бу дастурлардан ташқари файлларни қисилган ҳолда ёзиб сақлаш учун махсус zip папка яратиш усули ҳам мавжуд. Бу папкани яратиш учун керакли файллар ажратилиб, контекст менюси чақирилиб “отправить” буйруғига кириш ва zip папка буйруғини бериш етарли.

Windows операцион тизимида файлларни архивга нусхалаш

Windows операцион тизимида файлларни архивлаш учун қуйидаги дастурлардан фойдаланилади: **WinRar, Winzip, WinArj** ва ҳоказо.

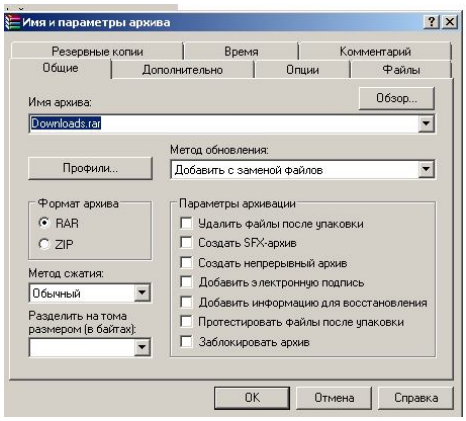
Архивлаш дастурларидан фойдаланиш учун ҳар бир шахсий компьютерларнинг системасига архивлаш дастурлари ўрнатилган бўлиши шарт. Компьютер системасига дастурни ўрнатиш учун дастурнинг диструбути ёки пакетли дастуридан фойдаланилади. Дастур тизимга ўрнатилгандан кейин ихтиёрий ахборотни архивлашимиз мумкин. **WinRar** дастурини ишга тушириш қуйидаги буйруқлар орқали амалга оширилади: **ПУСК → Программы→WinRar.**

WinRar дастури ишга тушгандан сўнг, экранда унинг асосий ишчи ойнаси пайдо бўлади(1-расм).



1-расм. WinRar дастури ишчи ойнаси.

Ишчи ойнадан архивланиши керак бўлган диск аниқланади, масалан, **C:** диск. Сўнгра, архивланиши керак бўлган файллар белгиланади ва **Добавить** тугмачаси босилади. Натижада, экранда архив номи ва архивлаш параметрларини ўрнатиш мулоқот ойнаси пайдо бўлади(2-расм).



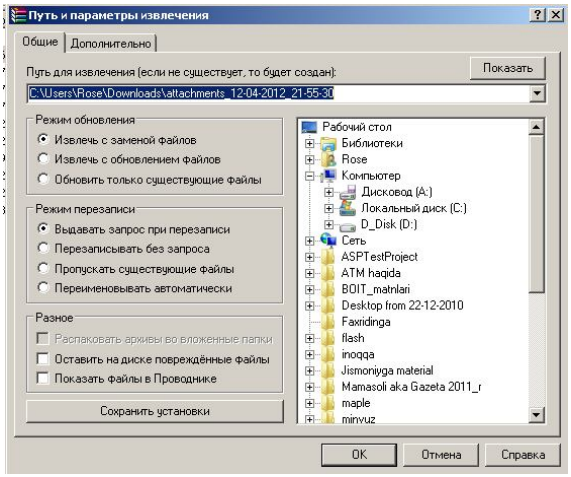
2-расм. Архив номи ва параметрларини ўрнатиш ойнаси.

Архив дарчасида архивли файлга ихтиёрий ном берилади. **Формат архива** дарчасида архивлашнинг кенгайтма тури танланади(rar ёки zip). **Метод сжатия** дарчасида файлларни архивга жойлаштиришда сиқиш усулларидан бири танланади(**Без сжатия, Скоростной, Быстрый**,

Обычный, Хороший, Максимальный), масалан, **обычный. Метод обновления** дарчасида архивли файлга яна бошқа файлларни жойлаштириш мумкин. **Размер словаря** дарчасида қуйидаги қийматлардан бири танланади: 64, 128, 256, 512 ва 1024 Килобайт. Бу қийматларнинг ошиши файлларни архивлашда сиқиш дарачасини оширади. Сиқиш даражасини ошириш кўп хотира ҳажми ва кўп вақт талаб қилади. Барча архивлаш параметрлари ўрнатилгандан кейин ОК тугмачаси босилади ва натижада, диск мундарижасида архивли файл номи пайдо бўлади.

Windows операцион тизимида файлларни архивдан қайта тиклаш

Файлларни архивдан тиклаш учун дастлаб архивли файл танланади ва менюдан **Извлечь в** буйруғи танланади ва «сичқонча» тугмачаси босилади. Экранда файлларни тиклаш йўли параметрларини кўрсатувчи мулоқот ойнаси пайдо бўлади(3-расм) ва фойдаланувчи қуйидаги буйруқларни кетма-кет бажаради.



3-расм. Файлларни архивдан тиклаш ойнаси.

Путь извлечения дарчасида файлларни дискнинг қайси жойига тиклаш йўли кўрсатилади.

Режим обновления дарчасида қуйидагилар бажарилади:

- **Извлечь с заменой файлов**- барча белгиланган файллар тикланади;

- **Извлечь с обновлением файлов**- папкада йўқ ёки архивдаги нусхаси янги бўлган белгиланган файллар тикланади;

- **Обновить существующие файлы-** папкада бор, лекин архивдаги нусхаси янги бўлган белгиланган файллар тикланади. Бу ҳолда дискда мавжуд бўлмаган файллар тикланмайди.

Режим перезаписи дарчасида қуйидагилар бажарилади:

- **Запрось при перезаписи-**агар архивдаги файллар уларнинг нусхаси жойлашган папкага тикланаётган бўлса, у ҳолда мулоқот ойнаси пайдо бўлади ва унда **«Файл мавжуд. Қайта ёзиш зарурми?** сўроғи чиқади. Фойдаланувчи **Ҳа** ёки **ЙЎҚ** дан бирини танлайди;

- **Перезаписать без запроса** –сўроқсиз файлларни тиклайди;

- **Пропустить существующие файлы-** папкада мавжуд файллар тикланмайди.

1.2. Компьютер вируслари турлари ва вируслардан сақланиш дастурларининг аҳамияти

Ҳозирги кунда компьютердан фойдаланувчилар олдида катта муаммо - вируслардан ҳимояланиш муаммоси туради. Ҳозирда фанга 30000 дан ортик компьютер вируслари маълум. Компьютер вируси термини биринчи бўлиб 1984 йилда АКШ Лехайс университети ходими Ф.Коуэн томонидан киритилди. Лекин вирус дастурларининг пайдо бўлиши 70 йиллардан бошланган. Биринчи вирус дастури 1970 йили америкада IBM-360/370 компьютерларида қайд этилган ва бу вирус Christmas tree деб номланган.

Биринчи вируслар унча зарарли бўлмаган ва у фойдаланувчини огоҳлантирган. Масалан, фойдаланувчидан у ёки бу саволга жавоб сўраган ва жавоб нотуғри берилган ҳолда дискдаги файлларнинг ўчириши ҳақида огоҳлантирган. Кейинроқ компьютер техникаси ва унинг дастурий таъминоти ривожланиб борган сари вируслар ҳам ривожланиб ўзларининг кодларини беркитиш ҳолатларига ўтган. Бундай вируслар куринмас (stealth) вируслар деб ном олган. 1990 йилга келиб шундай вируслар пайдо булдики, улар ўз кодларини доимий равишда ўзгартира олиш қобилиятига эга бўлди. Бундай вируслар «полиморф вирус»лар деб ном олди. Компьютер вирусларини дунё бўйлаб тарқашига интернет тармоғи катта ҳисса қўшди. Бунинг натижасида бутун бошли интернет вируслар синфи пойдо бўлди. Бу вируслар синфи «Троян» деб ном олди. Улар компьютерларга унча зарар келтирмасада интернет тармогига уланиш логин ва паролларини, махфий ахборотлар паролларини ўғирлай бошлади. 1998-1999 йилларга келиб Melissa, Win95.CIH каби вируслар дунё бўйича миллиондан ортиқ компьютерни ишдан чиқарди. Бу вируслар каттик дискларни ва бош платаларни ишдан чиқарди.

Компьютер вируси - бу ҳажм жиҳатдан унча катта бўлмаган дастур бўлиб, у ўзидан бошқа дастурларга нусха кўчиради ва шу тариқа купайиб, компьютерда сақланаётган ахборотларнинг йўқолишига, баъзи ҳолларда

компьютерларнинг ишдан чиқишига сабаб булади. Барча вируслар қуйидаги учта умумий хоссага эга бўлади:

1. Ўз-ўзидан кўпайиб кетиш;
2. Кўринмаслик;
3. Режалаштирилмаган ҳолда ҳаракат қилиш.

Вирус дастурлари профессионал дастурчилар томонидан баъзан охирини ўйламаган ҳолда, баъзан атайлаб кайсидир компанияга зарар етказиш мақсадида ёзилади. Вируслар хавфли ва хавфсиз вирусларга бўлинади. Вирус дастурларининг кўпчилиги унча зарар келтирмайдиган хавфсиз вируслар ҳисобланади. Масалан WinFile вируси. Улар ўз-ўзидан кўпайиб дискда жойни қискаришини келтириб чиқаради. Колган вируслар хавфли вируслар ҳисобланиб файлларни ўчириб ташлаш, маълумотларни шифрлаб ташлаш каби зарар етказувчи вируслардир. Ҳозирда вирус ёзаётган ва антивирус ёзаётган дастурчилар орасида ким зўрга жанг ҳам бормокда. Бунинг натижасида оддий фойдаланувчилар зарар кўриб қолмокда.

Компьютерларнинг вируслар билан зарарланиши асосан вирус тарқатувчи дастурлар ёрдамида амалга ошади. Вирус тарқатувчи дастурлар ўзидаги вирусни бошқа дастурга нусхасини кўчиради. Кейин вирус билан зарарланган дастур ўз навбатида бошқа бир дастурни зарарлайди. Бу жараён такрорланиб бориб компьютердаги кўпгина дастур файллар вирус билан зарарланиб қолади. Компьютерларнинг вирус билан зарарланиш белгилари – файл ҳажми ортиб кетиши, дастур бажарилиш тезлиги секинлашиши, дискдаги маълумотларнинг тўлиқ ёки қисман йўқолиб қолишлари ва бошқа оддий бўлмаган ҳолатлар ҳисобланади.

Вируслар бир-биридан қайси объектни зарарлашга мўлжалланганлиги билан фарқланади. Улар асосан буйруқли файлларга (кенгайтмаси .BAT), тизим билан бирга юкланувчи драйвер дастурларга (.SYS, .BIN) ва бажарилувчи иккили кодлардаги дастурларга (.EXE, .COM) зарар етказиш учун

мўлжалланган бўлади. Берилганлар сақланадиган файлларга, масалан матнли файлларга вируслар кам зарар келтиради.

Ҳамма компьютер вируслари ҳам бир хил тарзда ҳаракат қилмайди. Уларнинг кўпайиши ва компьютерингизни зарарлаш усуллари ҳам турлича. Ҳозирги кунга келиб компьютерга зарар етказувчи программалар ва вирус турлари жуда кўп.

Вирусларни ёзилиш алгоритмига кўра қуйидаги гуруҳларга ажратиш мумкин:

1.***Юкланувчи (битли) вируслар(Bootsector viruses)*** флоппи дискларни, винчестерларни юкланиш (BOOT ёки Master Boot) секторларига жойлашиб олади. Кейин вирус ўзини кодини бошланғич юкланишда сақланаётган тизимга, ҳамда ва уларни юкланувчи секторга ёзади. Бу вируслар компьютернинг ишлай бошлаши (загрузка) учун фойдаланиладиган қаттиқ дискнинг махсус қисмини ишдан чиқаради. Бу вирус компьютерни зарарлаганидан кейин компьютер ишламай қолиши мумкин. Одатда бу вируслар флоппи дисклар орқали тарқалади.

2.***Кўринмас вируслар (Stealth)*** амалий дастурлар таркибига кириб олади ва ДОСга мурожат қилганда зарарланган файлларни зарарланмаган қисмини кўрсатади. Шунинг учун ДОС орқали уларни топиш мумкин бўлмай қолади.

3.***Полиморф вируслар(Polymorphic viruses)*** – уларни қидириб топиш анча мушкул иш ҳисобланади. Чунки улар доимий кодга эга бўлмайди. Бу вируслар нафақат ўз-ўзидан кўпаяди, балки кўпайган пайтда ўзларининг кодларини ҳам ўзгартириб туришади. Ўзгарувчан вирусларни аниқлаш ҳам баъзи антивируслар учун қийин кечиши мумкин.

4.***Йулдош вируслар*** - бу турли вируслар бўлиб файлларни ўзгартирмайди. Ишлаш алгоритмига кўра, улар EXE файллар учун йулдош файллар ташкил этади. Йулдош файлнинг номи асосий файл номи била бир хил бўлиб кенгайтмаси COM бўлади. Бунга мисол килиб WinFile вирусини келтириш мумкин.

5.***«Вирусы-черви»*** - бу турдаги вируслар компьютер тармоғи орқали тарқалиувчи вируслар ҳисобланади. Улар тармоқ орқали компьютер хотирасига кириб олиб, бошқа компьютерлар тармоқ адресини аниқлайди ва бу адрес бўйича бошқа копьютерга ўзининг нусхасини жўнатади. Бу турдаги вирусга мисол тариқасида «Corner» номли вирусни келтириш мумкин. Бу вирус электрон почта орқали тарқайди.

6.***Чувалчанг вируслар (Worms)*** – Чувалчанг вируслар ўз номига мос равишда жуда тез ўз-ўзидан кўпаядиган вируслардир. Одатда бу вируслар интернет ёли интранет тармоқлари орасида тарқалади. Тарқалиш усули сифатида электрон хатлар ёки бошқа тез тарқалувчи механизмлардан фойдаланади. Улар ҳақиқатан ҳам компьютердаги маълумотлар ва компьютер хавфсизлигига катта зиён етказади. Чувалчанг вируслар операцион тизимнинг нозик жойларидан фойдаланиш ёки зарарланган электрон хатларни очиш йўли билан компьютерингизга ўрнашиб олиши мумкин.

7.***Оператив хотирада яшовчи вируслар (Memory Resident Viruses)*** - Бу вируслар компьютерингизнинг оператив хотирасида (RAM) яшайди ва зарарли ҳаракатини амалга оширади. Одатда уларни ишга тушириш учун бошқа вирусдан фойдаланилади. Улар ўзларининг ишга тушишга ёрдам берган вирус ёпилган бўлса ҳам компьютер хотирасида қолади, шунинг учун ҳам уларга юқоридаги ном берилган.

8.***Рооткит вируслари (Rootkit viruses)*** **–** Рооткитлар вируслар орасида ўзларининг энг хавфлилиги ва яширинишга усталиги билан алоҳида ажралиб туради. Рооткитлар компьютерни ёвуз ҳакерлар томонидан қўлга олиниши учун фойдаланилади. Баъзи рооткитларни антивирус программалари ҳам аниқлай олмайди, чунки улар ўзларини оператив тизим файллари сифатида кўрсатишади. Рооткитлар одатда троянлар томонидан компьютерга ўрнатилади.

9.***Вақт бомбаси вируслари (Time or Logic Bombs)*** – Бу вируслар муайян сана ёҳуд пайт келганида ёки фойдаланувчи томонидан муайян ҳаракат амалга оширилганида ишга тушадиган вируслардир. Мисол учун Кулги кунида(1 апрел) ёки Янги йилда компьютерингиздаги маълумотларни ўчириб ташлаб сизга “совға” тақдим этиши мумкин.

10. ***Паразит вируслар*** – бу вируслар ўзларини нусхасини кўчириш орқали файллар ва диск секторларидаги маълумотларни ўзгартириб ташлайди.

11. ***Студентлар вируси*** – кўп холларда резидент бўлмаган ва кўп хотоликлардан иборат бўлган вируслар.

12. ***"Троян отлари" вируси(Trojan Horses) -*** керакли дастурлар ичига кириб олиб ҳар бир буйруқ берилганда қахшатгич зарба бера олади. У компьютер ва унинг сетлари орқали кўпайиб сезиларли зарарларни пайдо қилади. Қадимги юнонларнинг Трояга юришлари даврида қўллаган ҳийласи, яъни трояликларни отга ишқибоз эканлигидан фойдаланиб, уларга катта ёғоч от совға қилишлари ва бу отнинг трояликлар мағлубиятига олиб келиши воқеасидан олинган ном. Ҳозирда троя оти ибораси “ҳосиятсиз совға” деган маънони билдиради. Компьютер ва интернет дунёсида троянлар “ҳосиятсиз программа” деб номланиши мақсадга мувофиқ. Троянлар одатда интернет орқали тарқалади. Троянлар компьютерга ўрнашиб олиб, дастлаб фойдали программа сифатида ўзларини таништирадилар, лекин уларнинг асл вазифаси фойдаланувчига номаълумлигича қолади. Яширин равишда улар ўзларининг яратувчиси (cracker – ёвуз ҳакер) томонидан белгиланган ҳаракатларни амалга оширадилар. Троянлар ўз-ўзидан кўпаймайди, лекин компьютер хавфсизлигини ишдан чиқаради: троянлар керакли маълумотларни ўчириб юбориши, компьютердаги маълумотларни керакли манзилга жўнатиши, компьютерга интернетдан рухсатсиз уланишларни амалга ошириши мумкин.

13.***"Макро" вируслари(Macro viruses)*** - асосан маълумотларн қайта ишлашга тусқинлик қилади ва матн муҳаррирларига зарар етказади. Улар Microsoft Word, Excel ва Access муҳаррирларида тайёрланган ҳужжатларда кўплаб учраб туради. Масро вируслар бу – ўзларининг тарқалиши учун бошқа бир программанинг макро дастурлаш тилидан фойдаланадиган вируслардир. Улар одатда Microsoft Word, Excel хужжатларини зарарлайди.

14.***Уяли телефонлар учун вируслар.*** ILOVEYOU номли вирус уяли телефонлар учун мулжалланган. У 2000 йилда Испанияда энг йирик Telefonika уяли алока тармогида биринчи булиб тарқалди. У телефонни бузмайди, аммо алоқани қийинлаштиради

Компьютер вирусининг кўп таърифлари мавжуд. Биринчи таърифни 1984 йили Фред Коэн берган: "Компьютер вируси — бошқа дастурларни, уларга ўзини ёки ўзгартирилган нусхасини киритиш орқали, уларни модификациялаш билан захарловчи дастур. Бунда киритилган дастур кейинги кўпайиш қобилиятини сақлайди". Вируснинг ўз-ўзидан кўпайиши ва ҳисоблаш жараёнини модификациялаш қобилияти бу таърифдаги таянч тушунчалар ҳисобланади. Компьютер вирусининг ушбу хусусиятлари тирик табиат организмларида биологик вирусларнинг паразитланишига ўхшаш.

Ҳозирда компьютер вируси деганда қуйидаги хусусиятларга эга бўлган дастурий код тушунилади:

- аслига мос келиши шарт бўлмаган, аммо аслининг хусусиятларига (ўз-ўзини тиклаш) эга бўлган нусхаларни яратиш қобилияти;

- хисоблаш тизимининг бажарилувчи объектларига яратилувчи нусхаларнинг киритилишини таъминловчи механизмларнинг мавжудлиги.

Таъкидлаш лозимки, бу хусусиятлар зарурий, аммо етарли эмас. Кўрсатилган хусусиятларни ҳисоблаш мухитидаги зарар келтирувчи дастур таъсирининг деструктивлик ва сир бой бермаслик хусусиятлари билан тўлдириш лозим.

Вирусларни қуйидаги асосий аломатлари бўйича туркумлаш мумкин:

- яшаш макони;
- операцион тизим;
- ишлаш алгоритми хусусияти;
- деструктив имкониятлари.

Компьютер вирусларини яшаш макони, бошқача айтганда вируслар киритилувчи компьютер тизими объектларининг хили бўйича туркумлаш асосий ва кенг тарқалган туркумлаш ҳисобланади (4-расм).

Компьютер вирусларининг яшаш макони

Файл	Юкланувчи	Макро	Тармок
Бажариладиган файллар (exe.com.bat)	Дискнинг юкланувчи (Boot) сектори	Хужжатлар WORD (.doc)	Тармок протоколлари
Эгизак файллар	Тизимли юкловчи сектори	Хужжатлар Excel (.xls)	Тармок командалари
Файллар уртасидаги алока (лин к-вируслар)	Актив boot-секторга курсаткич	Office хужжатлари	Электрон почта

4-расм. Яшаш макони бўйича компьютер вирусларининг туркумланиши.

Вирусларнинг хаёт даври. Ҳар қандай дастурдагидек компьютер вируслари хаёт давринининг иккита асосий босқичини сақланиш ва бажарилиш босқичларини ажратиш мумкин.

Сақланиш босқичи вируснинг дискда у киритилган объект билан биргаликда шундайгина сақланиш даврига тўғри келади. Бу босқичда вирус вирусга қарши дастур таъминотига заиф бўлади, чунки у фаол эмас ва ҳимояланиш учун операцион тизимни назорат қила олмайди.

Компьютер вирусларининг *бажарилиш даври,* одатда, бешта босқични ўз ичига олади:

1. Вирусни хотирага юклаш.
2. Қурбонни қидириш.
3. Топилган қурбонни захарлаш.
4. Деструктив функцияларни бажариш.
5. Бошқаришни вирус дастур-элтувчисига ўтказиш.

Вирусни хотирага юклаш. Вирусни хотирага юклаш операцион тизим ёрдамида вирус киритилган бажарилувчи объект билан бир вақтда амалга оширилади. Масалан, агар фойдаланувчи вирус бўлган дастурий файлни ишга туширса, равшанки, вирус коди ушбу файл қисми сифатида хотирага юкланади. Оддий ҳолда, вирусни юклаш жараёни-дискдан оператив хотирага нусхалаш бўлиб, сўнгра бошқариш вирус бадани кодига узатилади. Бу ҳаракатлар операцион тизим томонидан бажарилади, вируснинг ўзи пассив ҳолатда бўлади. Мураккаброк вазифаларда вирус бошқаришни олганидан сўнг ўзининг ишлаши учун қўшимча харакатлар бажариши мумкин. Бу билан боғлик иккита жихат кўрилади.

Биринчиси вирусларни аниқлаш муолажасининг максимал мураккаблашиши билан боғлиқ. Сақланиш босқичида баъзи вируслар ҳимояланишни таъминлаш мақсадида етарлича мураккаб алгоритмдан фойдаланади. Бундай мураккаблашишга вирус асосий баданини шифрлашни киритиш мумкин.

Аммо фақат шифрлашни ишлатиш чала чора ҳисобланади, чунки юкланиш босқичида расшифровкани таъминловчи вирус қисми очиқ кўринишда сақланиши лозим. Бундай холатдан қутилиш учун вирусларни ишлаб чиқувчилар расшифровка қилувчи кодини "мутациялаш" механизмидан фойдаланади. Бу усулнинг мохияти шундан иборатки, объектга вирус нусхаси киритилишида унинг расшифровка қилувчига тааллуқли қисми шундай модификацияланадики, оригинал билан матнли фарқланиш пайдо бўлади, аммо иш натижаси ўзгармайди.

Кодни мутациялаш механизмидан фойдаланувчи вируслар *полиморф вируслар* номини олган. Полиморф вируслар (polymorphic)-қийин аниқланадиган вируслар бўлиб, сигнатураларга эга эмас, яъни таркибида бирорта ҳам кодининг доимий қисми йўқ. Полиморфизм файлли, юкламали ва макровирусларда учрайди.

Стелс-алгоритмлардан фойдаланилганда вируслар ўзларини тизимда тўла ёки қисман беркитишлари мумкин. стелс-алгоритмларидан фойдаланадиган вируслар — ***стелс-вируслар*** (Stealth) деб юритилади. Стелс вируслар операцион тизимнинг шикастланган файлларга мурожаатини ушлаб қолиш йўли билан ўзини яшаш маконидалигини яширади ва операцион тизимни ахборотни шикастланмаган қисмига йўналтиради.

Иккинчи жихат ***резидент вируслар*** деб аталувчи вируслар билан боғлиқ. Вирус ва у киритилган объект операцион тизим учун бир бутун бўлганлиги сабабли, юкланишдан сўнг улар, табиий, ягона адрес маконида жойлашади. Объект иши тугаганидан сўнг у оператив хотирадан бўшалади. Бунда бир вақтнинг ўзида вирус хам бўшалиб сақланишнинг пассив босқичига ўтади. Аммо баъзи вируслар хили хотирада сақланиш ва вирус элтувчи иши тугашидан сўнг фаол қолиш қобилиятига эга. Бундай вируслар резидент номини олган. Резидент вируслар, одатда, фақат операцион тизимга рухсат этилган имтиёзли режимлардан фойдаланиб яшаш маконини захарлайди ва маълум шароитларда зараркунандалик вазифасини бажаради. Резидент вируслар хотирада жойлашади ва компьютер ўчирилишигача ёки операцион тизим қайта юкланишигача фаол ҳолда бўлади.

Резидент булмаган вируслар фақат фаоллашган вақтларида хотирага тушиб захарлаш ва заракунандалик вазифаларини бажаради. Кейин бу вируслар хотирани бутунлай тарк этиб яшаш маконида қолади.

Таъкидлаш лозимки, вирусларни резидент ва резидент бўлмаганларга ажратиш фақат файл вирусларига тааллуқли. Юкланучи ва макровируслар-резидент вирусларга тегишли.

Қурбонни қидириш. Қурбонни қидириш усули бўйича вируслар иккита синфга бўлинади. Биринчи синфга операцион тизим функцияларидан фойдаланиб фаол қидиришни амалга оширувчи вируслар киради. Иккинчи синфга қидиришнинг пассив механизмларини амалга оширувчи, яъни дастурий файлларга тузоқ қўювчи вируслар тааллуқли.

Топилган қурбонни захарлаш. Оддий ҳолда захарлаш деганда қурбон сифатида танланган объектда вирус кодининг ўз-ўзини нусхалаши тушунилади.

Аввал файл вирусларининг захарлаш хусусиятларини кўрайлик. Бунда иккита синф вируслари фарқланади. Биринчи синф вируслари ўзининг кодини дастурий файлга бевосита киритмайди, балки файл номини ўзгартириб, вирус бадани бўлган янги файлни яратади. Иккинчи синфга қурбон файлларига бевосита кирувчи вируслар тааллуқли. Бу вируслар киритилиш жойлари билан характерланади. Қуйидаги вариантлар бўлиши мумкин:

Файл бошига киритиш. Ушбу усул MS-DCSmon^ *com*-файллари учун энг қулай ҳисобланади, чунки ушбу форматда хизматчи сарлавҳалар кўзда тутилган.

Файл охирига киритиш. Бу усул энг кўп таркалган бўлиб, вируслар кодига бошқаришни узатиш дастурнинг биринчи командаси *(com)* ёки файл сарлавхасини *(exe)* модификациялаш орқали таъминланади.

Файл ўртасига киритиш. Одатда бу усулдан вируслар тузилмаси олдиндан маълум файлларга (масалан, *Command.com* файли) ёки таркибида бир хил қийматли байтлар кетма-кетлиги бўлган, узунлиги вирус жойлашишига етарли файлларга татбиқан фойдаланади.

Юклама вируслар учун захарлаш босқичининг хусусиятлари улар киритилувчи объектлар — қайишқоқ ва қаттиқ дискларнинг юкланиш секторларининг сифати ва қаттиқ дискнинг бош юклама ёзуви (MBR) орқали аниқланади. Асосий муаммо-ушбу объект ўлчамларининг чегараланганлиги.

Шу сабабли, вируслар ўзларининг қурбон жойида сиғмаган қисмини дискда сақлаши, ҳамда захарланган юкловчи оргинал кодини ташиши лозим.

Макровируслар учун захарлаш жараёни танланган хужжат-қурбонда вирус кодини сақлашдан иборат. Баъзи ахборотни ишлаш дастурлари учун буни амалга ошириш осон эмас, чунки хужжат файллари форматининг макропрограммаларни сақлаши кўзда тутилмаган бўлиши мумкин.

Деструктив функцияларни бажариш. Деструктив имкониятлари бўйича безиён, хавфсиз, хавфли ва жуда хавфли вируслар фарқланади.

Безиён вируслар - ўз-ўзидан тарқалиш механизми амалга оширилувчи вируслар. Улар тизимга зарар келтирмайди, фақат дискдаги бўш хотирани сарфлайди холос.

Хавфсиз вируслар — тизимда мавжудлиги турли таассурот (овоз, видео) билан боғлиқ вируслар, бўш хотирани камайтирсада, дастур ва маълумотларга зиён етказмайди.

Хавфли вируслар — компьютер ишлашида жиддий нуқсонларга сабаб бўлувчи вируслар. Натижада дастур ва маълумотлар бузилиши мумкин.

Жуда хавфли вируслар — дастур ва маълумотларни бузилишига ҳамда компьютер ишлашига зарур ахборотни ўчирилишига бевосита олиб келувчи, муолажалари олдиндан ишлаш алгоритмларига жойланган вируслар.

Бошкаришни вирус дастур - элтувчисига ўтказиш. Таъкидлаш лозимки, вируслар бузувчилар ва бузмайдиганларга бўлинади.

Бузувчи вируслар дастурлар захарланганида уларнинг ишга лаёқатлигини сақлаш хусусида қайғурмайдилар, шу сабабли уларга ушбу босқичнинг маъноси йўқ.

Бузмайдиган вируслар учун ушбу босқич хотирада дастурни коррект ишланиши шарт бўлган кўринишда тиклаш ва бошқаришни вирус дастур-элтувчисига ўтказиш билан боғлиқ.

Вируслар ва зарар келтирувчи дастурларни тарқатиш каналлари.

Компьютерлар ва корпоратив тармоқларни ҳимояловчи самарадор тизимни яратиш учун қаердан хавф туғилишини аниқ тасаввур этиш лозим. Вируслар тарқалишнинг жуда хилма-хил каналларини топади. Бунинг устига эски усулларга янгиси қўшилади.

Тарқатишнинг классик (мумтоз) усуллари. Файл вируслари дастур файллари билан биргаликда дискетлар ва дастурлар алмашишда, тармоқ каталогларидан, Web- ёки FTP — серверлардан дастурлар юкланишида тарқатилади. Юклама вируслар компьютерга фойдаланувчи захарланган дискетани дисководда қолдириб, сўнгра операцион тизимни қайта юклашида тушиб қолади. Юклама вирус компьютерга вирусларнинг бошқа хили орқали киритилиши мумкин. Макрокоманда вируслари MicroSoft Word, Excel, Access файллари каби офис хужжатларининг захарланган файллари алмашинишида тарқалади.

Агар захарланган компьютер локал тармоққа уланган бўлса вирус осонгина файл-сервер дискларига тушиб қолиши, у ердан каталоглар орқали тармоқнинг барча компьютерларига ўтиши мумкин.

Шу тариқа вирус эпидемияси бошланади. Вирус тармоқда шу вирус тушиб қолган компьютер фойдаланувчиси хуқуқлари каби хуқуққа эга эканлигини тизим маъмури унутмаслиги лозим. Шунинг учун у фойдаланувчи фойдаланадиган барча каталогларга тушиб қолиши мумкин. Агар вирус тармоқ маъмури ишчи станциясига тушиб қолса оқибати жуда оғир бўлиши мумкин.

Электрон почта

Ҳозирда Internet глобал тармоғи вирусларнинг асосий манбаи ҳисобланади. Вируслар билан захарланишларнинг аксарияти MicroSoft Word форматида хатлар алмашишда содир бўлади. Электрон почта макрокоманда вирусларини тарқатиш канали вазифасини ўтайди, чунки ахборотлар билан бир қаторда кўпинча офис хужжатлари жўнатилади.

Вируслар билан захарлаш билмасдан ва ёмон ниятда амалга оширилиши мумкин. Масалан, макровирус билан захарланган мухарриридан фойдаланувчи ўзи шубха килмаган ҳолда, адресатларга захарланган хатларни жўнатиши мумкин. Иккинчи тарафдан нияти бузуқ одам атайин электрон почта орқали ҳар қандай хавфли дастурий кодни жўнатиши мумкин.

Троян Web-сайтлар. Фойдаланувчилар вирусни ёки троян дастурни Internet сайтларининг оддий кузатишда, троян Web-сайтни кўрганида олиши мумкин. Фойдаланувчи браузерларидаги хатоликлар кўпинча троян Web-сайтлари фаол компонентларининг фойдаланувчи компьютерларига зарар келтирувчи дастурларни киритишига сабаб бўлади. Троян сайтни кўришга таклифни фойдаланувчи оддий электрон хат орқали олиши мумкин.

Локал тармоқлар.

Локал тармоқлар ҳам тезликда захарланиш воситаси ҳисобланади. Агар ҳимоянинг зарурий чоралари кўрилмаса, захарланган ишчи станция локал тармоққа киришда сервердаги бир ёки бир неча хизматчи файлларни захарлайди. Бундай файллар сифатида Login.com хизматчи файлни, фирмада қўлланилувчи Excel-жадваллар ва стандарт хужжат-шаблонларни кўрсатиш мумкин. Фойдаланувчилар бу тармоққа киришида сервердан захарланган файлларни ишга туширади, натижада вирус фойдаланувчи компьютеридан фойдалана олади.

Зарар келтирувчи дастурларни тарқатишнинг бошқа каналлари.

Вирусларни тарқатиш каналларидан бири дастурий таъминотнинг қароқчи нусхалари ҳисобланади. Дискетлар ва CD-дисклардаги ноқонуний нусхаларда кўпинча турли-туман вируслар билан захарланган файллар бўлади. Вирусларни тарқатиш манбаларига электрон анжуманлар ва FTP ва BBS файл-серверлар ҳам тааллуқли.

Вирусга қарши дастурлар

Компьютер вирусларини аниқлаш ва улардан химояланиш учун махсус дастурларнинг бир неча хиллари ишлаб чиқилган бўлиб, бу дастурлар

компьютер вирусларини аниқлаш ва йўқотишга имкон беради. Бундай дастурлар вирусга қарши дастурлар деб юритилади. Умуман, барча вирусга қарши дастурлар захарланган дастурларнинг ва юклама секторларнинг автоматик тарзда тикланишини таъминлайди.

Вирусларга қарши дастурлар фойдаланадиган вирусларни аниқлашнинг асосий усуллари қуйидагилар:

- эталон билан таққослаш усули;
- эвристик таҳлил;
- вирусга қарши мониторинг;
- ўзгаришларни аниқловчи усул;
- компьютернинг киритиш/чиқариш базавий тизимига (BIOSra) вирусга қарши воситаларни ўрнатиш ва х.

Эталон билан таққослаш усули энг оддий усул бўлиб, маълум вирусларни қидиришда ниқоблардан фойдаланади. Вируснинг ниқоби-мана шу муайян вирусга хос коднинг қандайдир ўзгармас кетма-кетлигидир. Вирусга қарши дастур маълум вирус ниқобларини қидиришда текширилувчи файлларни кетма-кет кўриб чиқади (сканерлайди). Вирусга қарши сканерлар факат ниқоб учун белгиланган, олдиндан маълум вирусларни топа олади. Оддий сканерлар компьютерни янги вирусларнинг суқилиб киришидан химояламайди. Янги дастурни ёки юклама секторини захарлашда кодини тўла ўзгартира олувчи шифрланувчи ва полиморф вируслар учун никоб ажратиш мумкин эмас. Шу сабабли сканер уларни аниқламайди.

Эвристик тахлил. Компьютер вируси кўпайиши учун хотирада нусхаланиш, секторга ёзилиш каби қандайдир муайян ҳаракатларни амалга ошириши лозим. Эвристик таҳлиллагичда бундай харакатларнинг рўйхати мавжуд. Эвристик тахлиллагич дастурларни ва диск ва дискет юклама секторларини, уларда вирусга хос кодларни аниқлашга уринган ҳолда, текширади. Тахлиллагич захарланган файлни топиб, монитор экранига

ахборот чиқаради ва шахсий ёки тизимли журналга ёзади. Эвристик таҳлил олдин маълум бўлмаган вирусларни аниқлайди.

Вирусга қарши мониторинг. Ушбу усулнинг моҳияти шундан иборатки, компьютер хотирасида бошқа дастурлар томонидан бажарилувчи шубхали ҳаракатларни мониторингловчи вирусга қарши дастур доимо бўлади. Вирусга қарши мониторинг барча ишга туширилувчи дастурларни, яратилувчи, очилувчи ва сақланувчи хужжатларни, Internet оркали олинган ёки дискетдан ёки ҳар қандай компакт-дискдан нусхаланган дастур ва хужжатларнинг файлларини текширишга имкон беради. Агар қандайдир дастур хавфли харакатни қилишга уринмоқчи бўлса, вирусга қарши монитор фойдаланувчига хабар беради.

Компьютерларнинг киритиш/чикариш базавий тизимига (BIOS***га) вирусга қарши воситаларни ўрнатиш.*** Компьютерларнинг тизимли платасига вируслардан химоялашнинг оддий воситалари ўрнатилади. Бу воситалар қаттиқ дискларнинг бош юклама ёзувига ҳамда дисклар ва дискетларнинг юклама секторларига барча мурожаатларни назоратлашга имкон беради. Агар қандайдир дастур юклама секторлар таркибини ўзгартиришга уринса, ҳимоя ишга тушади ва фойдаланувчи огохлантирилади. Аммо бу химоя жуда хам ишончли эмас.

Вирусга қарши дастурларнинг хиллари. Вирусга қарши дастурларнинг қуйидаги хиллари фарқланади:

- дастур-фаглар (вирусга қарши сканерлар);
- дастур-тафтишчилар (CRC-сканерлар);
- дастур-блокировка қилувчилар;
- дастур-иммунизаторлар.

Дастур-фаглар энг оммавий ва самарали вирусга қарши дастур ҳисобланади. Самарадорлиги ва оммавийлиги бўйича иккинчи уринда дастур-тафтишчилар туради.

Одатда, бу иккала дастур хиллари битта вирусга қарши дастурга бирлаштирилади, натижада унинг қуввати анчагина ошади. Турли хил блокировка қилувчилар ва иммунизаторлар ҳам ишлатилади.

Дастур-фаглар **(**сканерлар) вирусларни аниқлашда эталон билан таққослаш усулидан, эвристик таҳлиллашдан ва бошқалардан фойдаланади. Дастур-фаглар оператив хотира ва файлларни сканерлаш йули билан муайян вирусга характерли бўлган ниқобни қидиради. Дастур-фаглар нафақат вируслар билан захарланган файлларни топади, балки уларни даволайди ҳам, яъни файлдан дастур-вирус баданини олиб ташлаб, файлни дастлабки холатига қайтаради. Дастур-фаглар аввал оператив хотирани сканерлайди, вирусларни аниқлайди ва уларни йўқотади, сунгра файлларни даволашга киришади. Файллар ичида вирусларни катта сонини қидиришга ва йўқ қилишга аталган дастур-фаглар, яъни полифаглар ҳам мавжуд.

Дастур-фаглар иккита категорияга бўлинади: универсал ва ихтисослаштирилган сканерлар. Универсал сканерлар сканер ишлаши мўлжалланган операцион тизим хилига боғлиқ бўлмаган ҳолда, вирусларнинг барча хилларини қидиришга ва зарарсизлантиришга мўлжалланган. Ихтисослаштирилган сканерлар вирусларнинг чегараланган сонини ёки уларнинг бир синфини, масалан макровирусларни зарарсизлантиришга аталган. Фақат макровирусларга мўлжалланган ихтисослаштирилган сканерлар MS WORD ва Excel мухитларида хужжат алмашиниш тизимини ҳимоялашда энг қулай ва ишончли ечим ҳисобланади.

Дастур-фаглар сканерлашни "бир зумда" бажарувчи мониторинглашнинг резидент воситаларига ва фақат сўров бўйича тизимни текширишни таъминловчи резидент бўлмаган сканерларга ҳам бўлинади. Мониторинглашнинг резидент воситалари тизимни ишончлироқ химоялашни таъминлайди, чунки улар вируслар пайдо бўлишига даров реакция кўрсатади, резидент бўлмаган сканер эса вирусни аниқлаш қобилиятига фақат навбатдаги ишга туширилишида эга бўлади.

Дастур-фагларнинг афзаллиги сифатида уларнинг универсаллигини кўрсатиш мумкин. Дастур-фагларнинг камчилиги сифатида вирусларни қидириш тезлигининг нисбатан катта эмаслигини ва вирусга қарши базаларнинг нисбатан катта ўлчамларини курсатиш мумкин. Ундан ташқари, янги вирусларнинг доим пайдо бўлиши сабабли дастур-фаглар тездан эскиради ва улар версияларининг мунтазам янгиланиши талаб этилади.

Дастур-тафтишчилар (CRC-сканерлар) вирусларни қидиришда ўзгаришларни аниқловчи усулдан фойдаланади. CRC-сканерлар дискдаги файллар/тизимли сектордагилар учун CRC-йиғиндини (циклик назорат кодини) хисоблашга асосланган. Бу CRC-йиғиндилар вирусга қарши маълумотлар баъзасида файллар узунлиги, саналар ва охирги модификацияси ва бошқа параметрлар хусусидаги қўшимча ахборотлар билан бир қаторда сақланади. CRC-сканерлар ишга туширилишида маълумотлар базасидаги маълумот билан реал ҳисобланган қийматларни таққослайди. Агар маълумотлар базасидаги ёзилган файл хусусидаги ахборот реал қийматларга мос келмаса, CRC-сканерлар файл ўзгартирилганлиги ёки вирус билан захарланганлиги хусусида хабар беради. Одатда холатларни таққослаш операцион тизим юкланишдан сўнг дархол ўтказилади.

CRC-сканерларнинг камчилиги сифатида уларнинг янги файллардаги вирусларни аниқлай олмаслигини кўрсатиш мумкин, чунки уларнинг маълумотлар базасида бу файллар хусусидаги ахборот мавжуд эмас.

Дастур-блокировка *қилувчилар* вирусга қарши мониторинглаш усулини амалга оширади. Вирусга қарши блокировка қилувчилар резидент дастурлар булиб, вирус хавфи вазиятларини тўхтатиб қолиб, у хусусида фойдаланувчига хабар беради. Вирус хавфи вазиятларига вирусларнинг кўпайиши онларидаги характерли чақириқлар киради. Блокировка қилувчиларнинг афзалликлари сифатида вируслар кўпайишининг илк босқичида уларни тўхтатиб қолишини кўрсатиш мумкин. Бу айниқса, кўпдан бери маълум вируснинг мунтазам пайдо бўлишида мухим ҳисобланади.

Аммо, улар файл ва дискларни даволамайди. Блокировка қилувчиларнинг камчилиги сифатида улар химоясининг айланиб ўтиш йўлларининг мавжудлигини ва уларнинг "хираликлигини" (масалан, улар бажарилувчи файлларнинг харқандай нусхаланишига уриниш хусусида мунтазам огохлантиради) кўрсатиш мумкин. Таъкидлаш лозимки, компьютер аппарат компоненти сифатида яратилган вирусга қарши блокировка қилувчилар мавжуд.

Дастур-иммунизаторлар — файллар захарланишини олдини олувчи дастурлар икки хилга булинади: захарланиш хусусида хабар берувчи ва вируснинг қандайдир хили бўйича захарланишни блокировка қилувчи. Биринчи хил иммунизаторлар, одатда, файл охирига ёзилади ва файл ишга туширилганда ҳар марта унинг ўзгаришини текширади. Бундай иммунизаторлар битта жиддий камчиликка эга. Улар стелс-вирус билан захарланишни аниқлай олмайдилар. Шу сабабли бу хил иммунизаторлар хозирда ишлатилмайди.

Иккинчи хил иммунизаторлар тизимни вируснинг маълум тури билан захарланишдан ҳимоялайди. Бу иммунизатор дастур ёки дискни шундай модификациялайдики, бу модификациялаш уларнинг ишига таъсир этмайди, вирус эса уларни захарланган деб қабул қилади ва суқилиб кирмайди. Иммунизациялашнинг бу хили универсал бўлаолмайди, чунки файлларни барча маълум вируслардан иммунизациялаш мумкин эмас. Аммо бундай иммунизаторлар чала чора сифатида компьютерни янги ноъмалум вирусдан, у вирусга қарши сканерлар томонидан аниқланишига қадар, ишончли химоялаши мумкин.

Вирусга қарши дастурнинг сифат мезонлари. Вирусга қарши дастурни бир неча мезонлар бўйича баҳолаш мумкин. Қуйида бу мезонлар муҳимлиги даражаси пасайиши тартибда келтирилган:

- ишончлилик ва ишлаш қулайлиги фойдаланувчилардан махсус харакатларни талаб этувчи техник муаммоларнинг йўқлиги; вирусга қарши

дастурнинг ишончлилиги энг мухим мезон ҳисобланади, чунки хатто энг яхши вирусга қарши дастур сканерлаш жараёнини охиригача олиб бора олмаса, у бефойда ҳисобланади;

- вирусларни барча тарқалган хилларини аниқлаш фазилати, ички файл-хужжатлар/жадвалларни (MS Office), жойлаштирилган ва архивланган файлларни сканерлаш, вирусга қарши дастурнинг асосий вазифаси-100% вирусларни аниқлаш ва уларни даволаш;

- барча оммавий платформалар (DOS, Windows 95/NT, Novell NetWare, OS/2, Alpha, Linux ва х.) учун вирусга қарши дастур версияларининг мавжудлиги; суров буйича сканерлаш ва "бир зумда" сканерлаш режимларининг борлиги, тармоқни маъмурлаш имкониятли сервер версияларининг мавжудлиги.

- Вирусга қарши дастурнинг кўп платформалилиги мухим мезон ҳисобланади, чунки муайян операцион тизимга мўлжалланган дастургина бу тизим функцияларидан тўла фойдаланиш мумкин. Файлларни "бир зумда" текшириш имконияти хам вирусга қарши дастурларнинг етарлича мухим мезони ҳисобланади. Компьютерга келувчи файлларни ва қўйилувчи дискетларни бир лахзада ва мажбурий текшириш вирусдан захарланмасликка 100%-ли кафолат беради. Агар вирусга қарши дастурнинг сервер вариантида тармоқни маъмурлаш имконияти бўлса, унинг қиймати янада ошади.

- ишлаш тезлиги. Вирусга қарши дастурнинг ишлаш тезлиги хам унинг мухим мезони ҳисобланади. Турли вирусга қарши дастурларда вирусни кидиришнинг ҳар хил алгоритмларидан фойдаланилади. Бир алгоритм тезкор ва сифатли булса, иккинчиси суст ва сифати паст бўлиши мумкин.

Химоянинг профилактика чоралари. Хар бир компьютерда вируслар билан захарланган файллар ва дискларни ўз вақтида аниқлаш, аникланган вирусларни тамомила йукотиш вирус эпидемиясининг бошка компьютерларга тарқалишининг олдини олади. Хар қандай вирусни аниқлашни ва йук килишни кафолатловчи мутлок ишончли дастурлар мав-

жуд эмас. Компьютер вируслари билан курашишнинг мухим усули ўз вақтидаги профилактика ҳисобланади.

Вирусдан захарланиш эхтимоллигини жиддий камайтириш ва дисклардаги ахборотни ишончли сақланишини таъминлаш учун қуйидаги профилактика чораларини бажариш лозим:

- факат қонуний, расмий йул билан олинган дастурий таъминотдан фойдаланиш;

- компьютерни замонавий вирусга қарши дастурлар билан таъминлаш ва улар версияларини доимо янгилаш;

- бошқа компьютерларда дискетда ёзилган ахборотни ўқишдан олдин бу дискетда вирус борлигини ўзининг компьютеридаги вирусга қарши дастур ёрдамида доимо текшириш;

- ахборотни иккилаш. Аввало дастурий таъминотнинг дистрибутив элтувчиларини сақлашга ва ишчи ахборотни сақланишига эътибор бериш;

- компьютер тармоқларидан олинувчи барча бажарилувчи файлларни назоратлашда вирусга қарши дастурдан фойдаланиш;

- компьютерни юклама вируслардан захарланишига йўл қўймаслик учун, операцион тизим ишга туширилганида ёки кайта юкланишида дисковод чўнтагида дискетани қолдирмаслик.

Вирусга қарши дастурларнинг ҳар бири ўзининг афзалликларига ва камчиликларига эга. Факат вирусга қарши дастурларнинг бир неча хилини комплекс ишлатилиши мақбул натижага олиб келиши мумкин.

Қуйида вирусдан захарланиш профилактикасига, вирусларни аниқлаш ва йўкотишга мулжалланган баъзи дастурий комплекслар тавсифланган.

AVP (Антивирус Касперского Personal) — Россиянинг вирусга қарши пакети. Пакет таркибига қуйидагилар киради:

- Office Guard — блокировка килувчи, макровирусдан 100% химояланишни таъминлайди;

- Inspector — тафтишчи, компьютердаги барча узгаришларни кузатади, вирус фаоллиги аникланганида дискнинг асл нусхасини тиклашга ва зарар келтирувчи кодларни чикариб ташлашга имкон беради;

- Monitor — вирусларни ушлаб колувчи, компьютер хотирасида доимо хозир булиб, файллар ишга туширилганида, яратилишида ёки нусхаланишида уларни вирусга қарши текширади;

- Scanner — вирусга қарши модул, локал ва тармоқ дисклар таркибини кенг кўламли текшириш имконини беради. Сканерни кул ёрдамида ёки берилган вақтда автоматик тарзда ишга тушириш мумкин.

Пакет ёрдамида электрон постани вирусга қарши фильтрлаш ва почта корреспонденциясини комплекс текшириш амалга оширилади. Вирусга қарши базани янгилаш Internet оркали бажарилади.

Dr.Web — Россиянинг вирусга қарши оммавий дастури, Windows 9x/NT/2000/XP учун мулжалланган булиб, файлли, юклама, ва файл-юклама вирусларни қидиради ва зарарсизлантиради. Дастур таркибида резидент қоровул SpIDer Guard, Internet орқали вирус базаларини янгилашнинг автоматик тизими ва автоматик текшириш жадвалини режалаштирувчи мавжуд. Почта файлларини текшириш амалга оширилган.

Dr.Web да ишлатилувчи алгоритмлар хакида маълум бўлган барча вирус хилларини аниқлашга имкон беради. Dr.Web дастурининг мухим хусусияти — оддий сигнатурли қидириш натижа бермайдиган мураккаб шифрланган ва полиморф вирусларни аниқлаш имкониятидир.

Symantec Antivirus — Symantec компаниясининг корпоратив фойдаланувчиларга таклиф этган вирусга қарши махсулоти тўплами.

Symantec махсулотидан ишчи жойларининг умумий сони 100 ва ундан ортиқ бўлганида ва бўлмаганда битта Windows NT/2000/NetWare сервери мавжудлигида фойдаланиш мақсадга мувофиқ ҳисобланади. Ушбу пакетнинг башқалардан ажралиб турадиган хусусияти қуйидагилар:

- бошкаришнинг иерархик модели;

- янги вирус пайдо бўлишига реакция килиш механизмининг мавжуд-лиги.

AntiVir Personal Edition — вирусга қарши дастур AVP, Dr.Web ва Х.лар имкониятларидек имкониятларга эга. Дастур комплектига қуйидагилар киради:

- дискларни сканерловчи;
- резидент қоровул;
- бошкариш дастури;
- режалаштирувчи.

Дастур Internet дан юкланувчи файлларни сканерлайди. Internet оркали янгиланишларни автоматик тарзда текшириш ва юклаш функцияси хам мавжуд. Дастур хотирани, юкланиш секторини текширишда ва унда вируслар буйича кенг кўламдаги маълумотнома мавжуд.

Компьютер вирусларидан ҳимояланишнинг 11 та йўли

Интернет ва компьютер технологиялари ривожланиб бораётган даврда ўз компьютеримизни вируслардан етарлича ҳимоя қила олишни ҳам билиш керак. Компютерга вирус тушиб, унга қарши курашгандан кўра, ўша вирусни компьютерга туширмасликка ҳаракат қилиш лозим.

Маълумки, вируслар компьютерга ўрнашиб олар экан, компьютердаги маълумотларга жуда катта зиён етказиши мумкин. Оддий уй фойдаланувчиси учун компьютерга вирус тушиши катта муаммо бўлмаслиги мумкин, чунки бундай вазиятда одатда кўриладиган чора Windows ОТ қайта ўрнатиш ҳисобланади, лекин операцион тизимни ҳам қайта ўрнатиш ва созлашга анча вақт кетади. Ҳозирги пайтда эса вақт олтинга тенг.

1. Ишончли ва самарали антивирус программасидан фойдаланинг.

Бу маслаҳатга компьютер ишлатиб бошлашданоқ амал қилиш лозим. Компьютер интернетга уланманганмаган бўлсада, яхши антивируснинг компьютерда ишлаб туриши маълумотларнинг хавфсизлиги ва компьютер ишлаши барқарорлигини таъминлайди. “Қайси антивирус яхши?” деган

савол сизни қийнаши мумкин. Ҳозирги кунда машҳур антивирусларнинг ҳаммаси ҳам самарали ҳисобланади, сиздан уларнинг вақтида вирусларни аниқлаш базасини янгилаб туриш ва тўғри созлаш талаб қилинади, холос.

2. Spyware (айғоқчи) ва бошқа зарарли программаларга (malware) қарши керакли чоралар кўриш лозим.

Антивирус программалари баъзида вируслар, ***Spyware*** ва бошқа зарарли программаларга қарши курашда ёрдамга муҳтожлик сезиши мумкин, яъни биргина антивирус кучи билан зарарли программаларга қарши курашиб бўлмайди. Антивирусга қўшимча тарзда Ad-aware ёки Spybot Search & Destroy, AVZ va a2 HijackFree программаларидан фойдаланиш тавсия этилади.

3. Шубҳали ва зарарланган сайтлардан эҳтиёт бўлинг.

Зарарланган сайтга кириш компьютерга вирус тушишига олиб келади. Ҳозирги кунда сайтларнинг зарарланганлиги тўғрисида қидирув машиналари (Google) маълумот бера олади, яъни сиз Google қидирув натижалари орасидан зарарланган сайтларга киришни хоҳласангиз, Google бу ҳақда сизни огоҳлантиради. Мисол учун, www. google.co.uz га кириб, бирор-бир веб-сайт адресини теринг ва қидирув натижасидаги тавсияга қаранг.

4. Электрон почтага келган хатларга қўшилган (аттачед) файлларни ҳеч қачон антивирус текширмасидан олдин очманг.

Ҳозирги кунда электрон почта вируслар тарқалашининг энг асосий воситаси ҳисобланган учун фақат ва фақат антивирус томонидан текширилган хатларни очиб ўқинг.

5. Антивирус программанинг автоматик тарзда компьютерингизни вируслардан текшириб туришни таъминлаши керак.

Ҳозирги кунда кўпгина антивирус программаларида бу хусусият мавжуд, шунинг учун камида икки кундан бир компьютерингизни автоматик текшириб туришга антивирус программангизни созлашингиз керак. Бу усул энг янги вирусларнинг компьютерингизга ўрнашиб қолишини олдини олади.

6. Интернетда компьютерга сақлаб олаётган файллардан эҳтиёт бўлинг.

Агар интернетдан фаол фойдаланадиган бўлсангиз, деярли ҳар куни компьютерингизга янги программа, мусиқа ёки клип сақлаб оласиз ва бу жараёнда ҳам эҳтиёткорликни эсдан чиқарманг. Янги сақлаб олинган файлларни (одатда .exe, .zip, .rar кенгайтмали) антивирус программаси билан текширинг.

7. Янгилаш, Янгилаш, Янгилаш

Кўпгина программалар вақт ўтган сайин янгиланишга (update) муҳтожлик сезади. Windows ОТ ҳам вақти-вақти билан янгиланиб туриши керак. Бу жараён одатда автоматик тарзда кечади ва операцион тизимнинг ҳакерлар томонидан аниқланган нозик жойларини (loopholes) ёпади. Янгиланган операцион тизим барқарор ишлаш гаровидир. Антивирус ва бошқа хавфсизликни таъминлайдиган программаларни ҳам янгилаб туришни эсдан чиқарманг.

8. Компьютер ишлаш тизимини бироз бўлсада тушиниш ва ўрганишга ҳаракат қилинг.

Ҳозирги кунда энг муаммоли вазият. Кўпчилик компьютер фойдаланувчилари компьютер аслида қандай ишлаши ҳақида умуман тасаввурга эга эмаслар. Компютердан фойдалана бошлаган кунингизданоқ, унинг ишлаш тизими ҳақида билимингизни ошириб боринг. Бу билимингиз кейинчалик вирусларга қарши курашда, компьютерда ишлаш самарадорлигига ва, умуман, кейинги ҳаётингизда катта ёрдам беради. Ёвуз ҳакерлар компьютер саводсизлигингиздан фойдаланишига йўл қўйманг!

9. Контрафакт (Cracked) программалардан фойдаланманг.

Бу маслаҳат келажак фойда беради. Тўғри, ҳозирда кўпчилик фойдаланувчилар пуллик программалар сотиб олишга унчалик ошиқмайдилар, чунки пуллик бўлсада, аллақачон “даволанган” – регистратсия калитлари (ключ) мавжуд бўлган программалар интернетда

жуда кўп. Бу программаларда вирус йўқлигига ҳеч ким кафолат беролмайди, шунинг учун иложи борича, текин бўлган программалардан фойдаланинг. Текин программалардан фойдаланиб компьютерда одатий ишларни қандай амалга оширишни кейинги мақолаларда кўрсатиб ўтаман.

10. Fayervoldan фойдаланинг.

Агар фаерволдан фойдаланишга билимингиз етарли бўлса, Microsoft компаниясининг эмас, бошқа программа ишлаб чиқарувчиланринг фаерволларидан фойдаланинг.

11. Интернетда янги вирус эпидемияси тарқалганида компьютерингизни етарлича ҳимоя қилишга тайёр туринг.

Бундай вазиятда иложи борича, электрон хатларга қўшилган файлларни очманг, янги шубҳали сайтлардан программалар сақлаб олманг. Чат программаларида (Mail.ru Agent, ICQ) юборилган файлларни қабул қилманг. Антивирус программаларининг янгиланганлигига ишонч ҳосил қилинг.

Компютерда вирус борлигини қандай билса бўлади ва вирусларга қарши нима қилиш керак?

Компютер вируслари операцион тизимда ўрнашиб олганлигини билиш унчалик осон эмас, агар бу вируслар троян ёки рооткит бўлса, умуман, уларнинг мавжудлигини нафақат фойдаланувчи, балки антивирус программалари ҳам сезмаслиги мумкин.

Компютерга вирус асосан икки йўл орқали ўрнашиб олиши мумкин.

Биринчи ва энг кенг тарқалгани йўл бу – зарарланган флеш ёки бошқа портатив дискларни компьютерингизга улаш, шунинг учун бегона флешни компьютерга улашдан олдин, антивирус программаси билан текширинг.

Иккинчи йўли бу – интернетда зарарланган сайтларга кириш, чат давомида шубҳали файлларни олиш ёҳуд очиш ёки p2p тизимидан келадиган файллардаги вирусларнинг компьютерингизга ўрнашиб олишидир. Интернетга уланишдан олдин, компьютерингиз хавфсизлигига етарлича

ишонч ҳосил қилиш керак. Бунинг учун антивирус программаси ишлаб турган бўлиши, вирусларни аниқлаш базаси янгиланган бўлиши лозим.

Компютер фойдаланувчилари “бахтига” компьютерингизга ўрнашиб олган вирус ўзи бир нечта белгилар билан ўзини билдириб қўяди. Бу белгилар, одатда, қуйидагича бўлади:

1. Компьютерингиз одатдагига қараганда секин ишлай бошлайди.
2. Компьютерингизнинг буйруқларга жавоб бериш тезлиги камаяди ва тез-тез қотиб қола бошлайди.
3. Компьютерингиз тез-тез ўчиб ёна бошлайди.
4. Сиз компьютердан фойдаланиш пайтида ғалати хатоликлар, меню ва хабарларга дуч кела бошлайсиз.
5. Компьютерингиздаги айрим программалар ишламай қолади ёки тез-тез хатоликга дуч кела бошлайди.
6. Компьютердан принтер орқали хужжат чоп етиш тизими ишдан чиқади.

Агар компьютерингизга вирус тушган деб ўйласангиз, қуйидаги маслаҳатларга амал қилинг:

1. Компютерингиз интернетга уланган бўлса, дарҳол интернет алоқасини узинг, чунки баъзи-бир вируслар интернет орқали сизнинг компьютерингизга янада кўп зарар етказиши мумкин.

2. Ўзингизга энг муҳим ва керакли маълумотни (хужжатлар, суратлар ва бошқа файллар) захирага олинг, яъни флеш ёки CD/DVD дискларига ёзиб олинг.

3. Компютерингизда антивирус программаси бўлмаса, ўрнатинг. Иложи бўлса, ўзингизнинг компьютердан эмас, бошқа диск ёки флешда олиб келиб ўрнатинг ва вирусларни аниқлаш базасини янгиланг. Агар антивирус программа бўлса, албатта, вирусларни аниқлаш базаси янгиланг.

4. Янгиланган вирусларни аниқлаш базасига эга антивирус билан компьютернинг қаттиқ дискини текширинг.

5. Антивирус программаси ишлаб чиқарувчи сайтига кириб, вирусни компьютердан ўчиришга ёрдам берадиган махсус ёрдамчи программалар бўлса, улар ёрдамида ҳам компьютерни вируслардан тозаланг.

6. Агар компьютер қаттиқ дискидаги маълумотлар ўчиб кетган бўлса, маълумотларни қайта тиклаш бўйича компьютер устасига мурожаат қилинг. Уста қаттиқ дискни текшириб, ундаги маълумотларни қайта тикламагунича қаттиқ дискга янги маълумот ёзманг.

II – БОБ. ФАЙЛЛАРНИ АРХИВЛАШ ВА КОМПЬЮТЕР ВИРУСЛАРИДАН САҚЛАНИШ ДАСТУРЛАРИ БИЛАН ИШЛАШ МЕТОДИКАСИ

2.1. Информатика ва ахборот технологиялари фанининг назарий дарсларида файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш методикаси

Замонавий педагогик технологиялар ва ахборот технологияларини ўқув жараёнида қўллаш ўқитувчиларни ўз устида кўпроқ ишлашга (ўқув материалларини тайёрлаш: маъруза, семинар, лаборатория машғулотларга доир назарий материаллар тайёрлаш, тажриба ишларига доир материалларни тўплаш, таҳлил қилиш, дарс жараёнига тегишли объектлар учун имитацион моделидан фойдаланиш, мавзулар бўйича савол-жавоблар ва бошқа материалларни тайёрлаш) мажбур қилса, талабаларнинг дарсга қизиқишини, фаоллигини ошиши, ақлий ривожланиши ва онгли равишда муносабатда бўлишга ундайди, бунда таълим сифати яхшиланади, ўқитиш самарадорлиги ошади.

Касб ҳунар коллежларида ўқитиладиган информатика фанида файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш учун қуйидагича соат тақсимланган:

1-жадвал

Мавзу номи	Маъруза машғулоти (соат)	Амалий машғулот (соат)
Файлларни архивлаш ва архив файлларни очиш. Архивлашнинг қўшимча имкониятлари	2	2
Компьютер вируслари ва уларни даволаш	2	2

Маъруза машғулотларида “Файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш” мавзусини ўқитиш методикасини келтирамиз.

Машғулотнинг мақсадлари. Файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлашни ўргатиш. Ахборот хавфсизлигини таъминлаш тушунчаларини бериш.

Тарбиявий: касбий фаолиятига доир билимларни чуқур эгаллаш, жамият олдида бурч ва маъсулиятни сезишни тарбиялаш.

Ривожлантирувчи: билимларни қўллай билишни шакллантириш, мантиқий фикрлаш ва мустақил ишлаш кўникмаларини ривожлантириш.

Таянч тушунча ва иборалар: Ахборот хавфсизлиги, файл, каталог, интерфейс, архивлаш дастури, антивирус дастури.

Педагогик вазифалар: ахборот хавфсизлиги тушунчасига таъриф бериш; файлларни архифлаш ҳақида маълумот бериш; компьютер вируслари тушунчасига таъриф бериш ва уларнинг турлари ҳақида маълумот бериш; антивирус дастурлари ҳақида маълумот бериш.

Машғулотнинг шакли: маъруза (80 дақиқа).

Машғулот методи: маъруза, тушунтириш, инструкция бериш, намойиш, компьютерли ўқитиш, блиц-сўров, диаграмма- Венна.

Ўқитиш воситалари: маъруза матни, компьютер, компьютер слайдлари, доска

Ўқитиш шакллари: фронтал, коллектив иш

Жиҳоз: мультимедиа проектор, компьютерлар, топшириқ вариантлари.

Машғулотдан кутиладиган натижалар. Ўқитувчи: талабаларда назарий билимларни амалда қўллай олишни шакллантириш, оқилона бошқариш, зериктирмаслик, доимий назорат ва адолатли баҳолаш, қисқа вақт ичида кўп нарсага эришиш, талабаларнинг эвристик фаолиятини ошириш.

Талаба: олинган билимларни тизимлаштириш ва амалда қўллаш, мустаҳкамлаш ва баҳо олиш, гуруҳ бўлиб ишлаш кўникмасини ҳосил қилиш, мустақил, мантиқий ва дадил фикрлашга ўрганиш.

Назарий дарсларда файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш методикаси 7 та босқичдан иборат бўлиб, булар қуйидагилар:

БИРИНЧИ БОСҚИЧ. Дарсларга тайёрланишда энг аввало талабаларнинг берилган муайян дарсларга тайёргарлиги автоматлаштирилган ҳолатда талабаларнинг маъруза дарслари мавзуси билан боғлиқ назарияни билиши; муайян маълумотларни билиши; уй вазифаларининг тўғри бажарилганлиги текширилади. Бундан ташқари, бу босқичда талабаларнинг маъруза дарсларида зарур бўлган назарий билимларни фаоллаштириш мақсадга мувофиқдир. Бунинг учун бир маълумотнинг ўзи параллел барча дисплейларда бир вақтнинг ўзида ҳамма талабаларга кўрсатилади, яъни кадрлар бирин-кетин ўтказилади. Кадрнинг чидамлилик вақти қўрсатилаётган материалнинг мураккаблигига боғлиқ ишлаш вақти билан яъни 15 – 20 секунд тенглаштирилиши шарт.

Бироқ паст ўзлаштирадиган талабалар дарснинг бу босқичида дастлабки ўрнатилган маълумотлардан фойдаланишлари учун, уларга мурожаат қилишни маъруза дарсининг бутун даври мобайнида рухсат бериш мақсадга мувофиқдир. Ўқитувчи файлларни архивлаш ва компьютер вирусларидан сақланиш дастурларини ўрнатади ва ишга туширади. Талабалар эса диққатни жамлаб, ўқитувчи фаолиятини кузатади. Бу босқичда асосий мақсад талабаларнинг диққатини жамлаш бўлиб, жорий ишларни амалга оширган ҳолда, уни 5-10 минут билан чегаралаш мумкин.

ИККИНЧИ БОСҚИЧ. Бу босқичда ўқитувчи мавзуни эълон қилади, фанни мақсад ва вазифалари, мавзу режалари, ундаги таянч тушунчалар, маъруза мазмуни, кутилаётган натижалар билан талабаларни таништиради. Олдинги мавзу билан жорий мавзуни боғлайди. Талабалар бу босқичда

ўқитувчи берган маълумотларни тинглайдилар, мавзуни ёзиб оладилар ва ўқитувчи талабаларда келтирилган ахборотларга нисбатан кучли мотивацияни шакллантириш зарур.

Блиц-сўров усулида мавзу бўйича маълум бўлган тушунчаларни санаб беришни сўрайди. (1.1-илова)

Фаоллаштирувчи саволлар:

1. Файлларни архивлаш деганда нимани тушунасиз?
2. Қандай архивлаш дастурларини биласиз?
3. Қандай компьютер вируслари ва уларнинг турларини биласиз?
4. Компьютер вирусларидан сақланиш дастурларининг вазифаси нимадан иборат?

Талабалар эса тушунчаларни санаб берадилар. Бу босқичга 10 минут вақт ажратилади.

УЧИНЧИ БОСҚИЧ. Бу босқичда ўқитувчи талабаларга файлларни архивлашнинг афзаллиги ва компьютер вирусларини турлари, уларнинг компьютерга тушиш сабаблари ҳақида умумий маълумот беради Сўнгра файлларни архивлаш дастурларини қўллаб файлни сиқиш, компьютер вирусларидан сақланиш дастурлари ёрдамида компьютерни вируслардан тозалашни кўрсатиб беради. Дарсларнинг самарадорлигини оширишда:

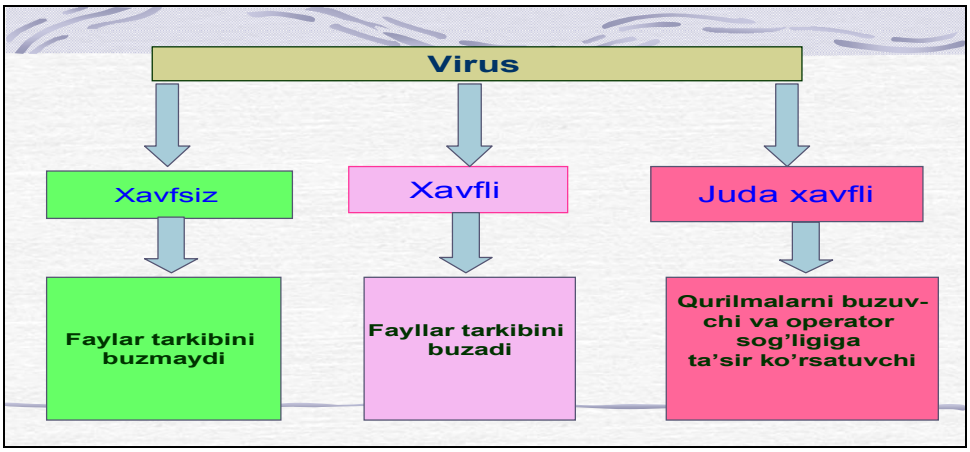
- дарсда фойдаланилаётган усулларнинг бир хиллигини йўқотиш;
- етарлича дастурли ўргатиш элементларини дарсда қўллаш;
- дарсда вақтдан фойдаланиш рационаллигини таъминлаш;
- муаммоли ўқитиш элементларини кўпроқ қўлланилиши;
- дарсда видеофильм, мультимедиа воситаларидан кўпроқ фойдаланиш мақсадга мувофиқ.

Бунда ўқитувчининг нутқи муҳим оддий, тушунарли, эмоционал нутқга эга бўлиши керак. Асосий эътиборни янги тушунчалар, таянч ибораларни тушунтиришга қаратиш, ортиқча сўзларни ишлатмаслиги керак. Бу

босқичнинг асосий мақсади - талабаларда келтирилган ахборотларни илмий билимларни тизимли равишда бериш, уларда ижодий изланувчанликни, ижтимоий ҳамкорликни ривожлантириш.

Жараён компьютер слайдларини намойиш қилиш билан олиб борилади.(1.2 - илова)

1.2 - илова



Fayllar tarkibini buzmaydigan viruslar.

Tezkor xotira qurilmasida ko'payuvchi.	Operatorni ta'sirlantiruvchi	Tarmoq viruslar

Operatorni ta'sirlantituvchi

Qurilmalarni ishdan chiqaruvchi	Terminalda xabar chiqaruvchi	Tovushli effektlarni hosil qiluvchi	Ish tartibini o'zgartiruvchi
- protsessor			-klaviatura
- xotira	-matnli	-ohang	
-MD, vinchestor			-displey
- printer	- grafikli	- nutq sintezi	
- port PS-232			- printer
Displey		- maxsus effektlar	
- klaviatura			- port PS-232

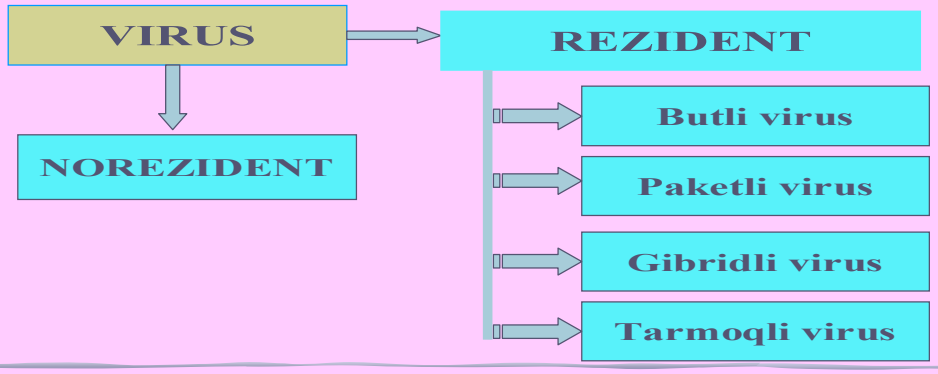
Fayl tarkibini buzuvchi viruslar

Foydalanuvchining ma'lumotlar va dasturlarini buzuvchi		Tizim ma'lumotlarini buzuvchi
Dasturlarni buzuvchi	Ma'lumotlarni bizuvchi	Disk sohasini buzuvchi
Dasturlarning boshlang'ich yozuvlarini buzuvchi	Ma'lumotlar bazalarini buzuvchi	Diskning mantiqiy tarkibini buzish
Bajariluvchi dasturlarni buzuvchi	Matnli xujjatlarni buzuvchi	Ma'lumot tashuvchilarning tarkibini buzuvchi
Kompilyatorlarning qism dasturlar to'plamini buzuvchi	Grafik tasvirni buzuvchi	
	Elektron jadvalni buzuvchi	

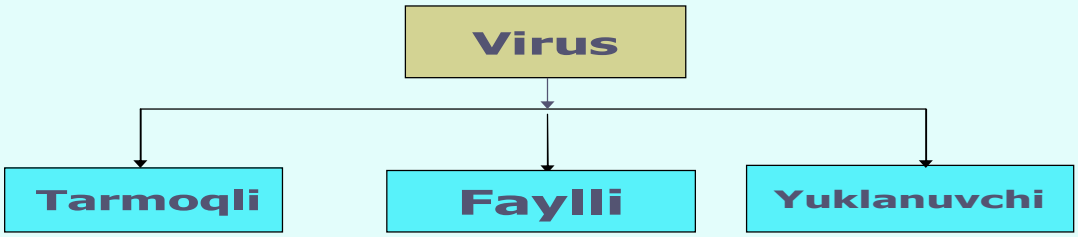
Operator va qurilmalarga ta'sir etuvchi viruslar

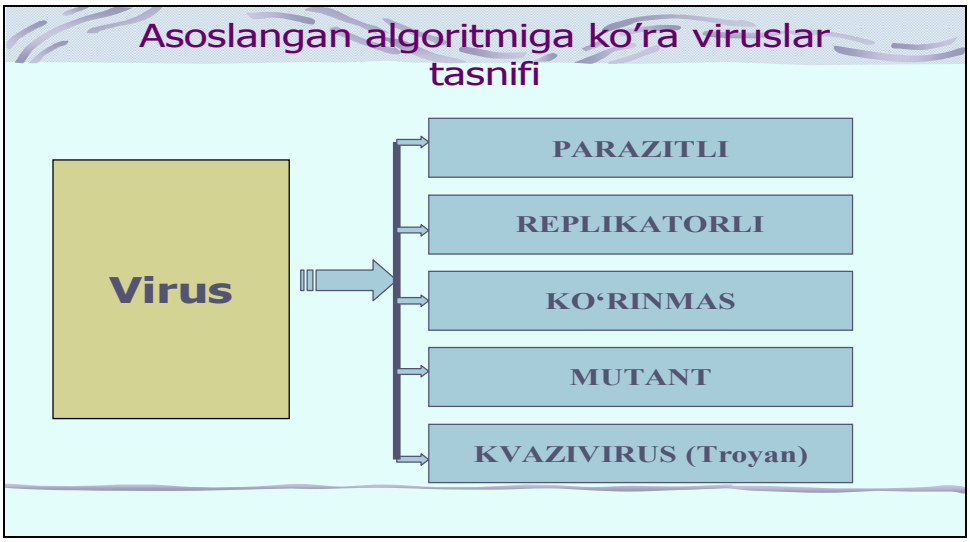
Qurilmalarni buzuvchi				Operatorga ta'sir etuvchi
Displeyning lyuminafor qatlamini Kuydiruv chi	Kompyuternin Mikrosxemasini ishdan chiqaruvchi	Printerni ishdan chiqaruv chi	MDni buzuv chi	Operator texnikasiga ta'sir etuvchi

ZARARLASH USULI BO'YICHA VIRUSLARTASNIFI



Joylashgan muhiti bo'yicha viruslar tasnifi





Бу босқичга 25 дақиқа вақт ажратилади.

ТЎРТИНЧИ БОСҚИЧ. Таҳлил босқичида ўқитувчи талабалар томонидан киритилган ғояларнинг қизғин таҳлил қилиниши учун шароит яратади. Талабалар ахборотларнинг баъзи жиҳатларини аниқлашга ва киритилган ғояларни, фикрларни қизғин таҳлил қилиб, энг тўғри ғоя ва фикрларни аниқлаб оладилар. Бу босқичда талабаларнинг дарс давомида ўрганиш, билим олиш фаоллигини ошириш, уларнинг шахсий фикрларини дадил айтишига, эркин, мантиқий фикрлашини ривожлантиришга эришилади. Талабаларда муаммо моҳиятини тўғри идрок қилиш, кенг мантиқий фикрлаш учун барча имкониятларидан фойдаланадилар.

Талабалар эса тинглайдилар. Тарқатма материаллар тўпламида келтирилмаган қирраларини конспект қилиб борадилар. Ҳар бир таянч тушунча ва ибораларни муҳокама қиладилар. Мавзу бўйича билимларни долзарблаштирувчи саволларга(1.3-илова) жавоб берадиларва мавзуни Т-схема(1.4-илова) бўйича муҳокама қиладилар. Барча ахборотни тизимлаштирадилар.

Мавзу бўйича билимларни долзарблаштирувчи савол

1.3 -илова

Катта ҳажмдаги файллар билан ишлаш муаммоси ва унинг ечимлари.

Йўналтирувчи саволлар:

1. Катта ҳажмдаги файллар билан ишлашдаги ноқулайликлар.
2. Катта ҳажмдаги файлларнинг компьютер хотирасинининг кўп қисмини банд этиши.
3. Катта ҳажмдаги ахборотни дискеталарга ёзиш муаммоси
1-муаммо. Катта ҳажмдаги файллар билан ишлашдаги ноқулайликлар
1. Файлдаги ахборотни иккита файлга жойлаштириб ишлаш.
2. Файлни архивлаш
2-муаммо. Катта ҳажмдаги файлларнинг компьютер хотирасинининг кўп қисмини банд этиши.
1. Катта оператив хотирага эга бўлган компьютердан фойдаланиш
2. Файлни архивлаш
3-муаммо. Катта ҳажмдаги ахборотни дискеталарга ёзиш муаммоси
1. CD-R, CD-RW дискларидан фойдаланиш
2. Файлни архивлаш

Т-схема

Архив файлнинг афзалликлари ва камчиликлари

1.4 -илова

Афзалликлар	Камчиликлар

Бу босқичга 15 дақиқа вақт ажратилади.

БЕШИНЧИ БОСҚИЧ. Назорат босқичида талабаларнинг маърузадаги таянч тушунчалар, янги билимлар қандай ўзлаштирилганлиги назорат қилинади. Бунда ўқитувчи электрон (компьютерлар орқали) ёки қоғоз (тарқатма материал) вариант бўйича тестлардан фойдаланади. Талабалар мавзудаги асосий таянч тушучаларни ўрганадилар ва уларда фаоллик, ижодкорлик ҳисси ривожланади, ўз хатоларини тузатиш ва янада яхши билим олишга интилиш ошади. Бу босқичга 15 дақиқа вақт ажратилади.

«Блиц-сўров» саволлари савол-жавоб вақтида тўлдирилади.

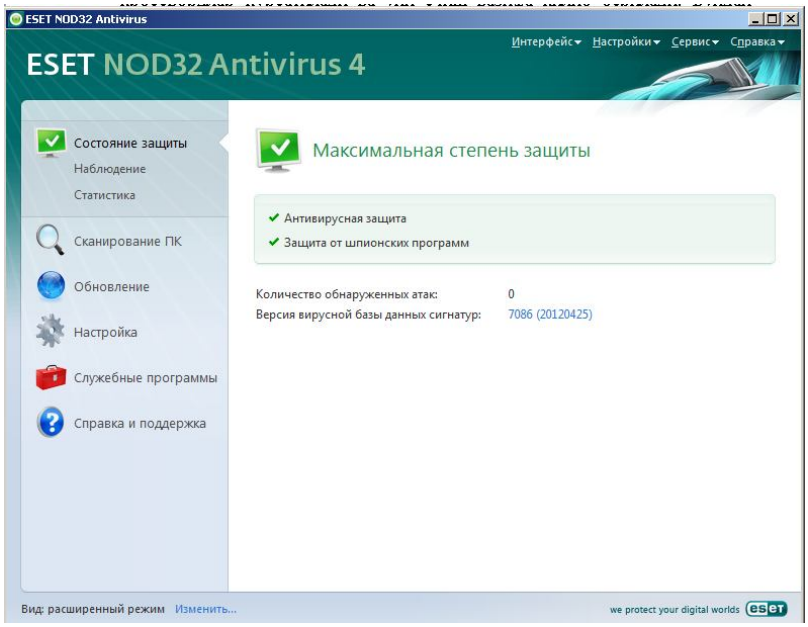
№	Саволлар	Жавоблар
1.	WinZIP архиватори WinRAR архиваторидан нимаси билан фарқ қилади?	

2.	WinRAR архиваторининг ишчи столи асосий элементларини санаб беринг.	
3.	Архиваторларнинг яна қандай функцияларини биласиз?	
4.	Архив файл оддий файлдан нимаси билан фарқ қилади?	

ОЛТИНЧИ БОСҚИЧ. Вазифа босқичида талабаларга тестлар ёки кроссвордлар кўрсатилади ва уни ечиш вазифа қилиб берилади. Бундан ташқари, фанга доир, мавзу бўйича интернет тармоғидан керакли материаллар тўплаш, таҳлил қилиш ва улардан фойдаланиш, фан бўйича фойдали сайтлар номи, мавзудаги таянч тушунчалар асосида кроссворд тузиш вазифалари берилади. Бу босқичда талабалар вазифаларни тушуниб, уларни бажариш масъулиятини ҳис қилишлари керак. Бу босқичга 5 дақиқа вақт ажратилади.

Топшириқ

ESET NOD 32 антивирусида ишлашни ўрганиш



ЕТТИНЧИ БОСҚИЧ. Якуний босқич бўлиб, ўқитувчи мавзу хулосасини айтади ва дарсга якун ясайди. Маъруза дарсининг бу босқичи ўтказилган ишларнинг таҳлили ва муҳокамасига бағишланади.

Файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлашда барча турдаги лаборатория машғулотлари учун универсал методик тавсияларни ишлаб чиқиш қийинчиликлар туғдиради. Шунга қарамасдан, муайян шартларга боғлиқ бўлмаган ҳолда лаборатория машғулотлари умумий мантиқий тузилишга эга бўлиб, ҳар бири ўз ичига 7 та босқични олади: машғулотларга тайёрланиш, машғулотга доир намуна масала ечиш ва тушунтириш, топшириқлар, топшириқларни бажариш ва билимларни фаоллаштириш, таҳлил, баҳолаш ва якун, лаборатория машғулотлари учун ҳам шундай босқичлар мавжуд.

2.2. Информатика ва ахборот технологиялари фанининг лаборатория машғулотларида файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш методикаси

Бугунги кунда телекоммуникацион технологиялар фаннинг барча соҳаларига, техникага, дунёнинг барча мамлакатларида инсонларнинг ижтимоий ва шахсий турмуш тарзларига яна кўпроқ кириб бормоқда.

Бундан ташқари информатикани ўқитиш жараёнида амалий фаолиятга тайёрлаш вазифасини тўғри ҳал этишга эришиш учун информатика курсининг илмийлигини ошириш лозим. Фақатгина тўғри ва чуқур хулосалар қила олсагина, ўқувчилар ҳар бир масалани ечишга танқидий ва ижодий ёндаша оладилар, янги муаммолар олдида ўзларини йўқотиб қўймайдилар ва турли шарт-шароитларда унумли фаолият кўрсата оладилар. Шунингдек, лаборатория иши ўқувчиларнинг дунёқарашини ошириши ва уни янги фактлар билан бойитиши билан бир қаторда, информатикадан билим даражаларини оширади, чуқур, тўлиқ ва мустаҳкам бўлишини таъминлайди.

Информатика ва ахборот технологиялари фанини ўқитиш қўйидаги мақсадларни кўзда тутади:

- бўлажак ўқитувчиларни информатика фанини ижодий ўқитиш ва ўзларининг амалий фаолиятларида янги педагогик ва ахборот технологияларини қўллаш бўйича билим, кўникма ва малакалари билан қуроллантириш;
- бўлажак ўқитувчиларни информатика соҳаси бўйича турли-туман шаклдаги синф ва синфдан ташқари ишларни ташкил этиш ва ўтказишга тайёрлаш;
- бўлажак ўқитувчиларни таълим соҳасини ахборотлаштиришнинг йўллари ва улкан истиқболлари ҳақида тасаввурларини ривожлаштириш ва ҳамда чуқурлаштириш.

Бўлажак информатика ўқитувчиси ўсиб келаётган авлоднинг умумтаълим мактаблари, академик лицей ва касб-ҳунар коллежларида

ўқитиладиган информатика ва ахборот технологиялари фанларининг аҳамиятини, унинг мазмунини ажратиш тамойилларини, шунингдек, информатика фанининг бошқа фанлар билан алоқадорлигини тушуниши зарур.

Лаборатория машғулотларида “Файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш” мавзусини ўқитиш методикасини келтирамиз.

Машғулотнинг мақсадлари. Файлларни архивлаш ва компьютер вирусларидан саыланиш дастурлари турлари билан танишиш. Архивлаш ва антивирус дастурлари билан ишлашни ўрганиш.

Тарбиявий: касбий фаолиятига доир билимларни чуқур эгаллаш, жамият олдида бурч ва маъсулиятни сезишни тарбиялаш.

Ривожлантирувчи: билимларни қўллай билишни шакллантириш, мантиқий фикрлаш ва мустақил ишлаш кўникмаларини ривожлантириш.

Машғулотнинг шакли: лаборатория (80 дақиқа).

Машғулот методи: компьютерли ўқитиш ва «кичик гуруҳлар» бўлиб ишлаш.

Жиҳоз: проектор, интернетга уланган компьютерлар, дастурий таъминотлар бўйича сайтлар рўйхати, топшириқ вариантлари.

Машғулотдан кутиладиган натижалар. Ўқитувчи: талабаларда назарий билимларни амалда қўллай олишни шакллантириш, оқилона бошқариш, зериктирмаслик, доимий назорат ва адолатли баҳолаш, қисқа вақт ичида кўп нарсага эришиш, талабаларнинг эвристик фаолиятини ошириш.

Талаба: олинган билимларни тизимлаштириш ва амалда қўллаш, мустаҳкамлаш ва баҳо олиш, гуруҳ бўлиб ишлаш кўникмасини ҳосил қилиш, мустақил, мантиқий ва дадил фикрлашга ўрганиш.

Машғулотнинг бориши

Ташкилий қисм. Ўқитувчи синфдаги ўқувчиларни 4—5 ўқувчидан иборат гуруҳларга ажратади.

Билимларни фаоллаштириш: барча талабаларга ижодий вазифа берилган.

1-БОСҚИЧ. **Тайёргарлик (10 дақиқа).**

Ўқитувчи фаолияти: талабаларни лаборатория машғулот мавзуси, ишнинг асосий мақсади тадқиқот соҳасининг локал кўринишларини моделлаш, уларнинг умумий бўлган концептуал моделга бирлаштириш кераклигини тушунтиради ва талабаларни 5 та кичик гуруҳга ажратади. Ҳар бир кичик гуруҳ 5 та талабадан иборат.

Талаба фаолияти: талабалар 4-6 кишидан иборат кичик гуруҳларга бирлашадилар ва машғулот методини тушуниб оладилар.

Кутилаётган натижа: талабаларда келтирилган ахборотга нисбатан кучли мотивацияни шакллантириш.

2-БОСҚИЧ. Намуна масала ечиш ва тушунтириш (15 дақиқа).

Ўқитувчи ҳар бир гуруҳга, Дастурий таъминотлар бўйича сайтлар рўйхатини ёки файлларни архивлаш ва компьютер вирусларидан сақланиш дастурларининг ўрнатгичини беради ва қуйидаги вазифани бажаришни тавсия этади:

–файлларни архивлаш дастурий таъминотини ўрнатиш, уларнинг турларини ва бир-биридан устунлик тарафини ёзиб бориш;

–турли(матнли, овозли, видео, бажарилувчи ва х.) файлларни архивлашни бажариш, архивлашни турли параметрлар бўйича бажариш, фарқларини кузатиш ва ёзиб бориш;

–компьютер вирусларидан сақланиш дастурий таъминотини ўрнатиш, уларнинг турларини ва бир-биридан устунлик тарафини ёзиб бориш;

–компьютер вирусларидан сақланиш дастури ёрдамида компьютерни вирусдан тозалаш;

–компьютерни замонавий вирусга қарши дастурлари ва улар версияларини янгилаш;

–диск ва флешкаларни вируслардан текшириш.

3-БОСҚИЧ. Топшириқ (5 дақиқа). Ўқитувчи фаолияти: топшириқни гуруҳларга тарқатади, масаланинг қўйилишини тушунтиради ва топшириқни бажариш учун кетадиган вақтни белгилайди. Ўқувчилар гуруҳларда ишлайдилар. Ўқитувчи уларни назорат қилиб, тўғрилаб, ёрдам бериб туради.

4-БОСҚИЧ. Топшириқни бажариш ва билимларни фаоллаштириш (20 дақиқа). Ўқитувчи фаолияти: талабаларнинг иш фаолиятини кузатади, ишлаш жараёнида айрим ноаниқликларни бартараф қилади, берилган саволларга жавоб беради. Талаба фаолияти: топшириқни бажариш мобайнида ўз билимларини амалиётда қўллайди. Кутилаётган натижалар: талабаларда мустақил ишлаш, билимни амалда қўллаш, ижодкорлик, ўз фаолиятини тўғри ташкил қилиш, мантиқий фикрлаш, ташаббускорлик, фаолликни шакллантириш.

5-БОСҚИЧ. Таҳлил (20 дақиқа). Ўқитувчи фаолияти: талабалар йўл қўйган хатоларни тузатиш, хато билим ўзлаштириш олдини олиш, талабалар фаолиятини таҳлил қилиш. Талаба фаолияти: ишлаб чиқилган топшириқни тақдимот орқали тушунтирадилар ва ўз камчиликларини тузатадилар. Ҳар бир гуруҳ ўзлари бажарган ишни тақдим этади. Тақдимот жараёнида савол-жавоб бўлиши мумкин.

Кутилаётган натижа: талабаларда хатоларни бартараф қилиш, ўзининг тўғри фикрини исботлш, мантиқий фикрлаш ва ижодкорликни шакллантириш.

6-БОСҚИЧ. Баҳолаш (5 дақиқа). Машғулот ниҳоясида ўқитувчи хулоса ясайди ва ҳар бир гуруҳ ишини баҳолайди.

7-БОСҚИЧ. **Якун (5 дақиқа).** Ўқитувчи уй вазифаларни топширади, уйда мавзуни такрорлаш, вазифага ижодий ёндашиш кераклигини ва кейинги машғулотга тайёрланиб келишларини айтиб, машғулотни якунлайди.

Келтирилган методика орқали лаборатория машғулотларни ўтказиш талабаларда олинган билимларни тизимлаштириш ва назарий билимларни амалда қўллаш малакасини оширишга, мустаҳкамлашга, якка ва гуруҳ бўлиб

ишлаш кўникмасини ҳосил қилишга, мустақил, мантиқий ва дадил фикрлашни ўрганишга олиб келади.

Топшириқларни бажариш давомида талабалар сайтлардан маълумотномадан фойдалангандек, керакли маълумотларни оладилар, янги мавзу билан олдиндан танишадилар, олган билимлардан самарали фойдаланадилар. Бу ўз навбатида талабаларда юқори ақлий, илмий салоҳиётнинг ривожланишига олиб келади. Янги педагогик технология ва ахборот технологиялари асосида лаборатория машғулотларни олиб бориш, талабаларнинг фанга бўлган қизиқишини янада оширади.

2.3. Педагогик тажриба-синов натижалари ва уларнинг таҳлили

Амалиёт, билишнинг асоси деб таъкидлаш, назариянинг нисбий ривожланишини инкор этмайди, лекин муайян назариянинг ҳақиқатга тўғри келишини тажриба тасдиқлайди.

Тадқиқот ишининг асосий ҳолатларини тажриба-синовдан ўтказиш бир неча босқичда, 2011-2012 ўқув йиллари мобайнида олиб борилди. Бўлажак кичик мутахассисларда ахборот хавфсизлиги билимларни шакллантириш муаммосини ҳал қилиш мақсадида Тошкент шаҳри Учтепа туманидаги Республика Дизайн КҲК да тажриба - синов ишлари ўтказилди.

Биринчи босқичнинг (2011-2012) асосий мақсади, танланган муаммони дизайн йўналишдаги КҲК ларида информатика дарсларида ўқувчиларнинг ахборот хавфсизлиги бўйича билимлари қандай даражада эканлигини ўрганиш, ўқувчиларда ахборот тушунчаси ва уни хавфсизлигини таъминлаш билимларнинг шаклланганлик даражасини аниқлаш мезонларини ишлаб чиқишдан иборат бўлди.

Тажриба-синов ишларининг иккинчи босқичида (2011-2012 йй.) ўқувчиларда файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш билимлари шаклланганлик даражасининг дастлабки ҳолати аниқланди, ахборот хавфсизлиги билимларни шакллантириш имкониятлари изланди. Шу мақсадда илғор педагогик тажрибалар ўрганилди, умумлаштирилди, ахборот хавфсизлигини таъминлаш бўйича турли мазмундаги топшириқлар системаси ишлаб чиқилди. Тажрибанинг бошланишида ўзлаштириш даражалари бир-бирига яқин бўлган ўқувчилар гуруҳлари иштирок этишди.

Файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш билимларнинг шаклланганлигини аниқлаш учун уч даражали (юқори, ўрта, паст) мезондан фойдаланилди. Педагогик тажриба-синовда иштирок этган 148 нафар талабанинг экспериментал тайёргарлик даражаси

талаблар бўйича баҳоланганда: 18 нафар (11,2%) талаба «юқори», 64 нафар (43%) талаба «ўрта», 66 нафар (45,8%) талаба «паст» натижаларга эришди. Бундан ўқувчиларда файлларни архивлаш ва компьютер вирусларидан сақланиш билимларнинг шаклланганлик даражасини ошириш лозим, деган хулосага келинди.

Иккинчи босқичнинг асосий мақсадидан яна бири бўлган файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш билимларни шакллантириш методикасини ишлаб чиқиш ва апробациядан ўтказишга қаратилди. Биринчи босқичдаги хулосаларга таянган ҳолда, тавсия этилаётган методикага тузатишлар киритилди. Масалалар ечиш билан боғлиқ бўлган топшириқларни бажаришда муаммоли саволлардан фойдаланилди. Бундай муаммоли вазиятлар яратилиши натижасида, ўқувчилар ўзларида етишмаётган ахборот хавфсизлигини таъминлаш бўйича билимларни шакллантиришга эҳтиёж сезиб, ўқиш мотивлари вужудга келгач, ахборот хавфсизлиги бўйича билимлар шакллантирилди. Тажриба-синов ишларининг натижалари умумлаштирилди, математик статистика Хи квадрат (χ^2) методидан [10] фойдаланиб, сифат ва миқдорий жиҳатдан ишлов берилди. Тадқиқот ишида тақдим этилган файлларни архивлаш ва компьютер вирусларидан сақланиш билимларни шакллантириш методикаси, ўқувчиларнинг билим сифатини ошириш, мустақил ишлаш фаолиятларини ташкил қилиш нуқтаи назаридан мақсадга мувофиқ деб топилди.

Тажрибада иштирок этаётган гуруҳларни саралаш ва уларда ахборот хавфсизлиги бўйича билимларнинг шаклланганлик даражасини аниқлаш мақсадида тажриба-синов ўтказилиб, юқоридаги мезонлар асосида баҳоланди. Баҳолаш натижаларини 2-жадвалда келтирамиз.

2-жадвал

Ўқувчиларда файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш билимлар шаклланганлик

даражасининг дастлабки ва кейинги ҳолати

Ўқув йили	**Тажриба - синовгача (а-қисм)**				**Тажриба-синовдан кейин (б-қисм)**			
2011-2012	Ўқувчилар сони	юқори	ўрта	паст	Ўқувчилар сони	юқори	ўрта	паст
	148	18	64	66	148	38	78	32
	%	12.2	43.2	44.6	%	25.7	52.7	21.6

Олинган натижаларнинг таҳлилидан ўқувчиларда файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш билимларнинг шаклланганлик даражасини ошириш лозим, деган хулосага келинди.

Тадқиқот ишининг кейинги босқичида унда тажриба ва назорат гуруҳлари танланди. Танланган гуруҳлардаги ўқувчиларда файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш билимларнинг шаклланганлик даражасини аниқлаш учун ҳар бир талабага алоҳида индивидуал равишда мустақил бажариши керак бўлган топшириқлар берилди ва уларнинг жавоблари таҳлил қилинди.

Олиб борилган педагогик тажриба синов ишларига статистик таҳлил беришда χ^2-статистика усулидан фойдаланилди.

Бизнинг тажрибаларимизда $C=3$ га тенг бўлганлиги учун қуйидаги формула асосида ҳисоблаш ишларини олиб борамиз

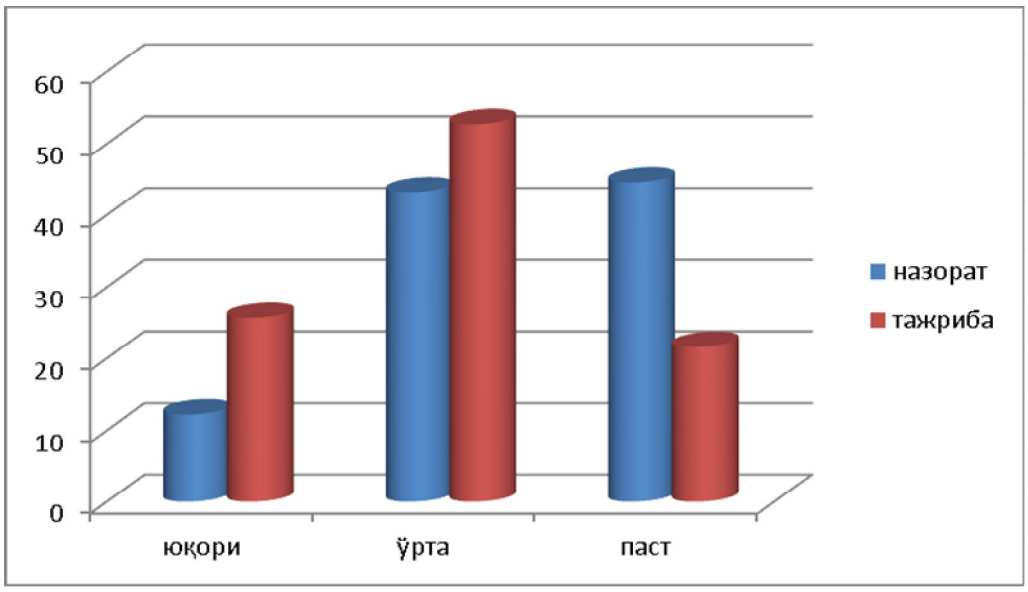
$$T = \frac{1}{n_1 n_2}\left(\frac{\left(n_1 O_{21} - n_2 O_{11}\right)^2}{O_{11} + O_{21}} + \frac{\left(n_1 O_{22} - n_2 O_{12}\right)^2}{O_{12} + O_{22}} + \frac{\left(n_1 O_{23} - n_2 O_{13}\right)^2}{O_{13} + O_{23}} \right) \qquad (3.2)$$

Информатика курсини ўқишга киришишидан аввал ўқувчиларда файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари

билан ишлаш билимларнинг шаклланганлик даражасини аниқлаш мақсадида ҳар бир талабага индивидуал равишда синов топшириқлар берилди. Бу синов топшириқларга ўқувчилар томонидан берилган жавоблар статистикаси (3.2) формула ёрдамида ҳисобланди.

Ҳисоб натижаларига кўра 2011-2012 ўқув йилида $T = 0,454 < T_{кр} = 6,00$ бўлганлиги учун нолинчи гипотеза қабул қилинади. Бундан кўринадики, танланган гуруҳларда тажрибадан олдинги ўтказилган синов ишларидаги билим даражалари деярли фарқ қилмайди. Худди шу каби ҳисоб-китобларни тажриба ўтказилгандан кейинги синов топшириқларидан олинган натижалар асосида амалга оширамиз. Демак, ҳисоблаш натижаларига кўра $T = 7,886 > T_{кр} = 6,00$ бўлганлиги учун нолинчи гипотеза инкор қилиниб, H_1 гипотеза қабул қилинади. Бошқача айтганда, назорат гуруҳи ўқувчиларига нисбатан тажриба гуруҳи ўқувчиларининг ўзлаштириш даражаси юқори бўлиб, бу олиб борилган тадқиқот ишлари самарали эканлигини кўрсатади.

Тажриба-синов даврида файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш билимларнинг шаклланганлик даражасини баҳолаш натижалари тажриба гуруҳларида «юқори» даража 12,2% дан 25,7% гача, «ўрта» даража 43,2% дан 52,7% гача ошди, «паст» даража эса 44,6% дан 21,6% гача камайди (2-жадвал, б қисм). Бу натижа-ларнинг назорат гуруҳларидаги натижаларга нисбатан юқори эканлигини қуйидаги гистограммадан кўриш мумкин.



5-расм. Файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш билимларнинг шаклланганлик даражаси гистограммаси

Гистограммадаги маълумотларга кўра:

2011/2012 ўқув йили учун: $T_{куз} = 7,77$; $T_{куз} > T_{крит} = 5,991$

Тажрибадан кейинги натижаларда $T_{куз} > T_{крит}$ эканлигидан кўринадики, олинган натижаларнинг ишончлилик даражаси юқори экан. Бундан тажриба ва назорат гуруҳлари ўқувчиларининг файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш билимларидаги фарқ статистик аҳамиятга эга, деган хулосага келдик. Демак, биз тавсия этган ўқитиш методикаси анъанавий олиб борилган ўқитиш методикасига нисбатан самарали эканлиги математик-статистика усуллари орқали исботланди.

ХУЛОСА

Ахборот ва у билан боғлиқ информацион технологиялар жамиятнинг ривожида жуда катта рол ўйнамокда. Малакали бўлган ҳар бир ходим – ўқитувчи, ҳуқуқшунос, мухандис, иқтисодчи, журналист ва ҳ.к. - ҳозирги кунга келиб маълумотлар тўпламини қийинчилик билан бошқара оляпти. Шунинг билан биргаликда информатикада информацион технологиялар, яъни инсон мехнатини қисман ёки тўла енгиллаштиришга қаратилган технологиялар кўплаб яратилмокда. Ушбу технологиялар ёрдамида таълим тизимида мавжуд бўлган, таълим жараёнлари тўғрисидаги ресурслар, ҳамда турли бошқариш тизимларида тўпланувчи ахборотлар ва бу ахборотларнинг бутунлигини ҳимоялаш ва унга турли компьютер вируслари тушишини олдини олиш ҳозирги замон компьютер технологиясидан фойдаланувчилар олдига жуда кўп муҳим бўлган муаммоларни қўяди.

Информатика ва ахборот технологиялар фанида “Файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш” бўйича назарий ва лаборатория дарсларини ташкил этиш жараёнида замонавий педагогик технологиялар ва интерфаол усуллардан фойдаланиш ўрганилаётган мавзунинг яна кенг қамровли тушиниб олишига, билим, кўникма ва малакаларнинг мустаҳкамланишига олиб келади.

Хулоса ўрнида шуни айтиш мумкин, “Файлларни архивлаш ва компьютер вирусларидан сақланиш дастурлари билан ишлаш” методикасини ишлаб чиқиш дарсларни мазмунли ташкил этилишида ва талабаларда ўзлаштириш кўрсаткичларини ошириш ҳамда мустаҳкам билим олишларига ёрдам беради.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1.“Ахборот технологиялари соҳасида кадрлар тайёрлаш тизимини такомиллаштириш тўғрисидаги Ўзбекистон Республикаси Президенти қарори. “Халқ сўзи” газетаси, 2005, 3-июн.

2. И.А.Каримов, “Ўзбекистон мустақилликка эришиш остонасида”, Тошкент, “Ўзбекистон”, 2011, 440 б.

3.Ўзбекистон Республикасининг “Ахборотлаштириш тўғрисида”ги қонуни. “Халқ сўзи”. 11 феврал, 2004 й.

4.«Ахборот-коммуникация технологияларини янада ривожлантиришга оид қўшимча чора-тадбирлар тўғрисида» Ўзбекистон Республикаси Президентининг 2005 йил 8 июлдаги–117-сон қарори.

5.«Таълим ҳақида» конун // Халқ таълими. 1997. №5. С.4-16.

6.Кадрларни тайёрлаш миллий дастури // Халқ таълими. 1998. №1. С.5-41.

7.А.Парпиев, А.Марахимов, Р.Ҳамдамов, У.Бегимкулов, М.Бекмурадов, Н.Тайлоқов. Янги ахборот технологиялари. /Олий таълим муассасалари учун. ЎзМЭ давлат илмий нашриёти.-Т.: 2008, 118 б.

8.Абдуқодиров А. А. Теория и практика интенсификации подготовки учителей физико-математических дисциплин. Аспект использования компьютерных средств в учебно-воспитательном процессе: Автореф…докт.пед.наук. - Т., 1990. – 39 с.

9.Абдуқодиров А. А.. ва бошк.. Ахборот технологияси фани буйича касб-ҳунар коллежлари учун ўқув дастури. - Тошкент: 2000.- 8 бет.

10.Абдуқодиров А. А.. ва бошк. Ахборот технологиялари.: Академик лицей ва касб –ҳунар коллежлари учун дарслик. / Абдукодиров А., Хаитов А., Шодиев Р. - Тошкент: Ўзбекистон, 2001.- 250 бет.

11.Арипов М. ва бошқ. Информатика: Касб-ҳунар коллежлари учун дарслик. - Тошкент: 2002. – 203 бет.

12.Ахмедов А., Тайлоқов Н. Информатика: Академик лицей ва касб–ҳунар коллежлари учун дарслик. - Тошкент: Ўзбекистон, 2001. - 272 бет.

13. Информатика. Базовый курс. Под редакцией С.В.Симоновича Санк-Петербург. 2001г.

14. В. Пассиков. Защита компьютерной информации. М.: Наука. 2001г.

15.Ахроров Ш. С. Педагогические основы формирования информационной и учебно-технической культуры будущих учителей в системе педагогического образования: Дисс. … док.пед.наук. - Т., 1994. – 301 с.

16.Боқиев Р. Компьютерлаштирилган укув жараёнининг инсон-машина системаси сифатидаги айрим муаммолари // Педагогик таълим. 2000. №1. 93-94 бетлар.

17.Боқиев Р. Академик лицей ва касб-ҳунар коллежларида информатика таълими ҳақида // Лицей ва академик лицейларда таъмин тизимини тақомиллаштириш. Илмий услубий маколалар тўплами. - Тошкент, 2000. 2 – 4 бетлар.

18.Гейн А. Г. Изучение информационного моделирования как средство реализации межпредметных связей информатики с дисциплинами естественнонаучного цикла: Автореф. ... канд.пед.наук. - М., 2000

19.Хайитов А. Г. Система дидактических упражнений по ОИВТ для 8-9 классов: Автореф. дис. канд. пед. наук. - Т.. 1996.

20.Аширова А.И. “Ахборот тизимларини лойиҳалаш” фанидан дастурий қобиқ яратиш ва таълимда фойдаланиш методикаси: Автореф…к.п.н.-Т.: ТДПУ, 2009.

21.Юлдашев У. Ю, Боқиев Р. Р. и др. Информатика таълими концепцияси ҳақида// Академик лицей ва касб-ҳунар коллежларида физика, математика ва информатика фанларини ўқитишни тақомиллаштириш мавзусидаги республика илмий-амалий конференция материаллари. - Тошкент: ТДПУ, 2000.

22.Юлдашев У. Ю, Боқиев Р. Р., Закирова Ф. М. Информатика.: Касб-ҳунар коллежлари учун дарслик. - Тошкент: Ғ.Ғулом номидаги нашриет. 2002.

23.Юлдашев У. Ю, Закирова Ф. М. и др. Задания для лабораторных работ по курсу информатика. - Т.: ТГПУ, 2002.

24.Юлдашев У. Ю, Закирова Ф. М. и др. Microsoft Access 97. - Т.: ТГПУ, 2002.

25.Зокирова Т.А., Машарипов А.К., Мусаева М.А., Иброҳимов Э.У. Web дастурлаш. Ўқув қўлланма. Тошкент- 2006.

26.Глушаков С.В. и др. «Работа в сети Интернет»: Учебный курс. М.: АСТ,2001г.

27.Закирова Т.А., Ходиева Р.М. Основы HTML. Учебное пособие. ТГЭУ. Ташкент–2006 г.

28. «Академик лицей ва касб хунар коллежларида физика, математика ва информатика фанларини ўқитишни такомиллаштириш истиқболлари» Республика илмий – амалий конференцияси материаллари.Тошкент, 2010 йил.

29.Ўзбекистон Республикасининг конституцияси. - Т.:Ўзбекистон. 1992. –

30.http://www.ziyonet.uz – Ўзбекистон Республикаси ахборот-таълим тармоғи.

31.http://diamond.stup.ac.ru /ENG/F4/Direct/4.html – «Таълимда янги ахборот технологиялари» номли Россия таълим сайти.

32.www.search.re.uz – Ўзбекистон ахборотларни излаб топиш тизими.

33.www.ictcouncil.gov.uz - Компьютерлаштиришни ривожлантириш бўйича Вазирлар Махкамаси мувофиқлаштирувчи Кенгашининг сайти.

34.www.ecsoman.edu.ru – Россия Федерацияси Олий ўқув юртларида ўқитилаётган фанлар бўйича ўқув-услубий комплекслар.

ИЗОҲЛИ ЛУҒАТ

Access	Ахборотга муносабат(кириш). Ахборот билан танишиш ё у билан бирор ахборот жараёнини амалга ошириш.
Access object	Муносабат (кириш) обекти. Муносабат тури ва даражаси аниқ қоидалар асосида чеклаб қўйилган ахборот технологияси елементи ва обекти.
Active attack	Тажовуз. Хавфсизликка таҳ диднинг йузага чиқиши.
Active threat	Хавфсизликка тахдид. Қасддан тизимнинг холатини ёмонлаштиришга қаратилган муайян турдаги хавф хатарнинг маълум ехтимоллиги.
ASCII	ASCII тўпламига кирувчи 7 битли стандарт босма символларда ёзилиб иккили саноқ тизимида кодланган ахборот. Бу кўринишдаги ахборот ҳар қандай тармоқ канали орқали узатишга ярайди.
Authentication information	Аутентификатсия ахбороти. Муайян ахборот манбаининг ё уни эгасининг аслини билиб олиш учун ишлатиладиган ахборот. Бундай ахборот сифатида рақамли имзо, хужжат изи, манбаъ изи ва ш.ў. бўлиши мумкин.
Authentication	Аутентификатсия. Муайян ахборот манбаининг ё уни эгасининг аслини билиб олиш. Бу мақсадда носимметрик криптотизимдан фойдаланилганда ҳужжатнинг аслини (келиб чиқишини) хужжат тузувчининг рақамли имзоси воситасида аниқлаб олинади. Аутентификатсия кенг маънода қаралганда ахборотнинг манбаъидан қатъий назар унинг фақат ички тузилмаси асосида бутунлигини аниқлашдир.

Authorized access	Рухсатли муносабат(кириш). Ахборотга ва ахборот технологияси елементларига нисбатан белгилаб қўйилган чеклов қоидаларига риоя қилинган ҳолда фаол муносабатда бўлиш.
Certify	Калитни сертификатсиялаш. Бирор кимсанинг ошкора калитини рақамли имзо билан тасдиқлаш.
Certifying Authority	Ваколатли сертификатор. Калитни сертификациялаш ва буни умумий маълумотлар базасига киритиш ҳуқуқига эга бўлган ишончга сазовор шахс (ё шахслар).
Confidentiality mark	Махфийлик грифи. Хужжатлаштирилган ахборотнинг махфийлик даражасини кўрсатувчи реквизит (масалан, ўта махфий, махфий, пинхона, хизматда фойдаланиш учун, ошкора).
Cryptographic method	Криптографик метод. Ахборотни шифрлашга асосланган химоялаш усули.
Data destruction	Ахборотни йўқ қилиш. Ахборотни тасодифий хато туфайли ё қасддан моддий ташувчидан ўчириб йубориш ёкм ташувчиси билан бирга ўғирлаб кетиш.
Data falsification	Ахборотни сохталаштириш. Ахборот жараёнлари давомида ахборот мазмунини қастдан бузиб ўзгартириш.
Data protection	Ахборот химояси. Ахборотнинг пинхоналиги, бутунлиги ва қобиллигини таъминлашга қаратилган ҳуқуқий, сиёсий, ташкилий, техникавий ва дастурий тадбирлар мажмуи.
Decryption	Шифрни очиш. Шифрланган ахборотни тушунарли шаклга айлантириш. Бунинг учун махфий калитдан фойдаланилади.

Digest	рақамли из(дайджест). Ахборотнинг ихчам бир томонлама хисобланадиган функтсияси ёки файлнинг назорат жамламаси. Ахборот ўзгарса дайджест ҳам ўзгаради.
Digital Signature	Рақамли имзо. Ахборотнинг рақамли изи(дайджести)нинг шу ахборотнинг хақиқийлигини тасдиқловчи субъектнинг махфий калити билан шифрланган шакли. Рақамли имзо шу субъектга тегишли еканига ишонч хосил қилиш учун ахборотнинг рақамли изини ҳаммага маълум бўлган функтсия асосида ҳисоблаб топиб, натижани рақамли имзо эгасининг ошкора калити билан очилган имзоси билан таққослаш (верификатсиялаш) етарли.
Documented information	Хужжатлаштирилган ахборот. Моддий ташувчида акс етган ва уни белгиловчи реквизитларга эга бўлган муайян ахборот.
Encryption	Шифрлаш. Ахборотни ундан хабардор бўлиши лозим бўлмаган шахслар учун мутлақо тушунарсиз шаклга келтириш амали, химоя усули .
Enforcement	Мажбурлаш. Фойдаланувчи ёки ижрочига нисбатан моддий ёки жиноий жавобгарлик тахдиди остида ахборот жараёнлари коидаларининг бажарилишига еришишга асосланган химоя усули.
Identification	Идентификатсия. Кўрсатилган идентификаторни унинг эгасига такдим етилган идентификатор билан таккослаш.
Identifier	Идентификатор. Ахборот жараёни субекти , воситаси ва обекти(ахборот)га такдим етиладиган, факат унга бириктирилган ноёб белги, символлар қатори.

Information procedure	Ахборот жараёни. Ахборотни яратиш, олиб йиғиш, сақлаш, ҳимоялаш, излаш, узатиш, тақсимлаш, ундан фойдаланиш ёки унга ишлов бериш жараёнларидан бири.
Information (data) integrity	Ахборотнинг бутунлиги. Ахборотнинг ахборот жараёнлари давомида уни берухсат ўзгартириш ёки йўқотишга йўл қўймаслик хоссаси.
Information availability	Ахборот қобиллиги. Ахборотнинг унга нисбатан рухсат берилган ахборот жараёнларини бажарилишига яроқлик ва тайёрлик хоссаси.
Information distortion	Ахборот бузилиши. Ахборотнинг ахборот жараёнлари давомида халал берувчи ташқи таъсирлар ё жараён воситалари ва иштирокчиларининг тасодифий хатолари ё қасддан қилинган ишлар туфайли ўзгариб қолиши.
Information modification	Ахборот модификатсияси. Ахборот мазмуни ё хмиқдорининг ахборот жараёнлари давомида ўзгариши.
Information security	Ахборот хавфсизлиги. Ахборотниниг ва ахборот жараёнларини амалга ошириш воситаларининг маълум турдаги тасодифий ва қасддан қилинадиган таҳдидлардан ҳимояланганлик ҳолати
Information security service	Ахборот хавфсизлигини таъминлаш тизими. Ахборот хавфсизлигини таъминловчи сиёсий, ҳуқуқий, ташкилий, техникавий ва дастурий тадбирлар, воситалар ва меёрлар тизими.
Information user	Ахборот фойдаланувчиси. Ахборот билан бирор ахборот жараёнини амалга оширувчи субъект (шахс, ташкилот).

Information's security	Ахборотнинг хавфсизлиги. Ахборотнинг тасодифий ё қасддан қилинадиган таҳдидларга қарши пинхоналикни, бутунликни ва қобилликни сақлаб қолиш хоссаси.
Key	Калит. Шифрлаш, шифрни очиш, рақамли имзо қўйиш ва верификатсия(ишониб олиш)да ишлатиладиган рақамли код. Калитлар носимметрик криптотизимларда жуфт(ошкора ва маҳфий) холда ҳосил қилинади ва боғламларда сақланади. Симметрик криптотизимларда фақат битта(маҳфий) калит ишлатилади. Аралаш криптотизимларда калитлар жуфтига қўшимча тарзда маҳфий сеанс алити ишлатилади.
Passiv threat	Хавфсизликка нофаол тахдид. Тизим холатини бузмасдан туриб ундан ахборотнинг бегоналарга берухсат чиқиб кетиш хавфи.
Password	Парол. Амалий муносабат бошлаш учун ишлатиладиган, субектнинг сири хисобланадиган идентификатор. Тизимга кириш учун клавиатура тугмаларини босиш кетма кетлиги.
Regulation	Тартибга солиш. Ахборотга берухсат муносабатда булишни минимумга келтиришга қаратилган технологияга асосланган химоя усули.
Screening	Экранлаш. Тармоклараро екран(бранмауер)нинг рухсат етилмаган ташки ахборот окимларини утказмай ички тармок хавфсизлигини саклаш вазифаси.
Security audit	Хавфсизликни текшириш. Ахборот тизими ва тармоғининг ҳамда ахборотларнинг хавфсизлик холатини текшириб баҳолаш.

Security model	Хавфсизлик модели. Ахборот хавфсизлиги сиёсатининг формал ифодаси.
Security policy	Хавфсизлик сиёсати. Ахборот хавфсизлигини таминлашга ва тажовуз оқибатларини тугатишга қаратилган меёрлар мажмуи.
Trojan horse	Троян оти. Субъектнинг қонуний ваколатларидан фойдаланиб ахборотга берухсат муносабатда бўлишга имкон берувчи қўшимча пинхона вазифаларни амалга оширувчи дастур.
Trusted	Ишончли. Очиқ калит ишончли, агар уни сиз ё бирор сиз вакил етган кимса сертификатсиялаган бўлса.
Trusted computer system	Химояланган компйутер тизими. Химоя воситалари мажмуи ўрнатилган компйутер тизими.
Unauthorized access	Берухсат муносабат. Субъект томонидан ахборотга ва ахборот воситаларига нисбатан чеклаб куйилган қоидаларнинг бузилиши.
Unauthorized action	Беруҳсат фаолият. Субъектнинг ахборот жараёнларини амалга ошириш қоидаларига зид фаолияти.
Vulnerability	Ахборот заифлиги. Ахборотнинг уни пинхоналиги, бутунлиги ё қобиллигига путур етказувчи таъсирларга дош беролмаслик хоссаси.