

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА
МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

Самарқанд давлат университети

Нурмаматов М.Қ

АХБОРОТЛАРНИ ҲИМОЯЛАШ



Ўқув-услубий мажмуа

**5110700– «Информатика ўқитиш методикаси» таълим
йўналиши 1-босқич талабалари учун**

САМАРҚАНД-2019

Ўзбекистон республикаси олий ва ўрта махсус таълим вазирлиги
Самарқанд давлат университети

Амалий математика ва информатика
«Ахборотлаштириш технологиялари» кафедраси

Рўйхатга олинди:

№ _____

«___» _____ 2019 й.

Тасдиқлайман:

Ўқув ишлари бўйича проректор

_____ проф.А.С.Солеев

«___» _____ 2019 й.

**”Ахборотларни ҳимоялаш” фанидан ўқув
услубий мажмуа**

Билим соҳаси: 100000 –гуманитар соҳа

Таълим соҳаси: 130000 - математика

**Таълим йўналиши: 5110700 – «Информатика ўқитиш
методикаси»**

Самарқанд - 2019

Фаннинг ўқув услубий мажмуаси ишчи ўқув режа ва ўқув дастурига мувофиқ ишлаб чиқилди.

Тузувчилар: СамДУ «Ахборотлаштириш технологиялари» кафедраси ассистенти Химматов И.Қ.

СамДУ «Ахборотлаштириш технологиялари» кафедраси ассистенти Нурмаматов МҚ.

Такризчилар:

Кобиров С. С. - СамДУ «Ахборотлаштириш технологиялари» кафедраси дотсенти, т.ф.н.

Ўринбоев Э. - СамДУ «Амалий математика ва комплекс дастурлаш» кафедраси дотсенти, т.ф.н.

Ўқув услубий мажмуа «Ахборотлаштириш технологиялари» кафедрасининг « » _____ йилдаги №__ йиғилишида муҳокама қилинди ва факултет илмий кенгашида тасдиқлаш учун тавсия қилинди.

Кафедра мудири:

проф. И.И.Жуманов

Ўқув услубий мажмуа “Амалий математика ва информатика” факултети ўқув-услубий кенгашининг «__»_____ 201_ йилдаги №_ йиғилишида муҳокама этилди ва фойдаланишга тавсия қилинди.

Факултет кенгаши раиси:

Келишилди: Ўқув услубий бошқарма бошлиғи:

Фаннинг ўқув-услубий мажмуаси тузилмаси
Мундарижа

1.	Аннотатсия	
2.	Силлабус	
3.	Фанининг ўқув дастури	
4.	Фанининг ишчи ўқув дастури	
5.	Модулни ўқитишда фойдаланиладиган интерфаол таълим методлари	
6.	Таълим технологияси: Машғулотларнинг педагогик технологияси ва технологик харитаси	
7.	Ўқув материаллари : Маъруза матни	
8.	Амалиёт машғулотлар учун масала ва машқлар тўплами.	
9.	Амалий машғулотлар бўйича топшириқлар ва уларни бажариш учун курсатмалар	
10.	Мавзулар бўйича намойиш дастурлари (презентация)	Файл
11.	Оралик назорат учун тест саволлари	
12.	Яқуний назорат учун саволлар	
13.	Мустақил таълим мавзулари ва уни бажариш бўйича тавзиялар	
14.	Атамалар	
15.	Адабиётлар рўйхати	

Аннотация

2002 йилда 30 майда Ўзбекистон Республикаси Президенти томонидан ПФ №3080 «Компьютерлаштириш ва ахборот – коммуникация технологияларини янада ривожлантириш ҳақидаги» қарори ва «Компьютерлаштириш ва ахборот – коммуникация технологияларини 2002-2010 йилларгача ривожлантириш дастури»га асосан республикамизда Компьютер ва ахборот технологияларини ривожлантириш, уларни халқ хўжалигида самарали қўллаш – долзарб масалага айланган. Телекоммуникация тўрлари, берилганларни узатиш, Интернет хизматларига кириш воситалари ривожланиб такомиллаштирилмоқда.

Ҳозирги кунда фан-техникани жадал сураатлар билан ривожланиши натижасида турли мураккаб жараёнларни, уларни математик нуқтаи назардан тасаввур қилиш, моделларини тузиш, алгоритм ва программа таъминотини яратиш нафақат назарий жиҳатдан, балки амалий жиҳатдан ҳам долзарб бўлган муаммолардан бири ҳисобланади. Фан назарий ва амалий қисмлардан иборат бўлиб, маълумотлар базаси билан ишлаш долзарб масала ҳисобланади.

«Ахборотларни ҳимоялаш» фани табиий фундаментал фанлар мажмуасига тааллуқли бўлиб, талабалар уни II семестрда ўрганишади.

« Ахборотларни ҳимоялаш » фанининг бош мақсади талабаларга ахборотларни ҳимоялашни ўргатишдир. Бу мақсадда уларга ахборот хавфсизлиги ҳақида умумий тушунчалар бериш ва ахборот хавфсизлигини таъминлашни ўргатишдан иборат. Ҳавфсизлик муаммоларини ҳал этиш учун бир қатор фундаментал билимларни муваффақиятли ўзлаштириш учун зарур бўладиган таянч билимларни беради.

Фаннинг вазифаси –

- ❖ Талабаларда компьютер тармоқлари ва тизимларида ахборот хавфсизлиги тўғрисидаги билимларни шакллантириш;
- ❖ Ахборотни ҳимоя қилишнинг назарий, амалий ва услубий асосларини бериш;
- ❖ Талабаларга компьютер тармоқлари ва тизимларида ахборот хавфсизлигини таъминлашнинг замонавий усуллари ва воситаларини қўллашни амалий жиҳатдан ўргатиш;
- ❖ Талабаларни ахборотни ҳимоя қилиш бўйича ишлаб чиқарилган турли хил дастурий маҳсулотлардан эркин фойдалана олиш имконини берадиган билимлар билан таъминлаш;

« Ахборотларни ҳимоялаш» фанидан ўқув услубий мажмуа амалий математика ва информатика таълим йўналишида билим олаётган бакалавриатура талабаларига мўлжалланган.

Силлабус
Берилганлар базасини бошқариш тизимлари фанининг қисқача тафсиви

ОТМнинг номи ва жойлашган манзили:	Самарқанд давлат университети	Университет хиёбони, 15					
Кафедра:	Ахборотлаштириш технологиялари	“Амалий математика ва информатика” факултети таркибида					
Таълим соҳаси ва йўналиши:	110000-педагогика	5110700 –Информатика ўқитиш методикаси					
Фанни (курсни) олиб борадиган ўқитувчи тўғрисида маълумот:	Асс.М.К.Нурмаматов	e-mail		mehridinnur@gmail.com			
Дарс вақти ва жойи:	Амали математика ва информатика ўқув биноси 18 аудитория	Курснинг давомийлиги:	Ўқув йили давомида				
Индивидуал график асосида ишлаш вақти:	Душанба, пайшанба ва шанба кунлари 14 ³⁰ дан 17.00 гача						
Фанга ажратилган Соатлар	Аудитория соатлари					Мустақил таълим	
	Маъруза	14	амалиёт	18	Л		
Фаннинг бошқа фанлар билан боғлиқлиги (пререквизитлари):	“Ахборотларни химоялаш”, “Компьютер тармоқлари”						

Фаннинг мазмуни

Фаннинг долзарблиги ва қисқача мазмуни:	Фанни ўқитишдан мақсад ва вазифаси – талабаларга ахборотларни химоялашни ўргатиш, уларда ахборот хавфсизлиги тўғрисидаги билимларни шакллантириш, ахборотни химоя қилишнинг назарий, амалий ва услубий асосларини бериш, ахборот хавфсизлигини таъминлашнинг замонавий усуллари ва воситаларини қўллашни амалий жихатдан ўргатиш, ишлаб чиқарилган турли хил дастурий махсулотлардан эркин фойдалана олиш имконини
--	---

	берадиган билимлар билан таъминлашдан иборатдир.
Талабалар учун талаблар	- ўқитувчига ва гуруҳдошларга нисбатан ҳурмат билан муносабатда бўлиш; - университет ички тартиб - интизом қоидаларига риоя қилиш; - уяли телефонни дарс давомида ўчириш; - берилган уй вазифаси ва мустақил иш топшириқларини ўз вақтида ва сифатли бажариш; - кўчирмачилик (плагиат) қатъиян ман этилади; - дарсларга қатнашиш мажбурий ҳисобланади, дарс қолдирилган ҳолатда қолдирилган дарслар қайта ўзлаштирилиши шарт; - дарсларга олдиндан тайёрланиб келиш ва фаол иштирок этиш; - талаба ўқитувчидан сўнг, дарс хонасига - машғулотга киритилмайди; - талаба рейтинг баллидан норози бўлса эълон қилинган вақтдан бошлаб 1 кун мобайнида апелляция комиссиясига мурожат қилиши мумкин
Электрон почта орқали муносабатлар тартиби	Профессор-ўқитувчи ва талаба ўртасидаги алоқа электрон почта орқали ҳам амалга оширилиши мумкин, телефон орқали баҳо масаласи муҳокама қилинмайди, баҳолаш фақатгина университет ҳудудида, ажратилган хоналарда ва дарс давомида амалга оширилади. электрон почтани очиш вақти соат 15.00 дан 19.00 гача

**ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ
ВАЗИРЛИГИ
САМАРҚАНД ДАВЛАТ УНИВЕРСИТЕТИ**

Рўйхатга олинди:

**Тасдиқлайман
Ўқув ишлари бўйича проректор**

№ _____

«____» _____ 2019 йил

2019 йил "____" _____

**АХБОРОТЛАРНИ ҲИМОЯЛАШ
ФАНИНИНГ
ИШЧИ ЎҚУВ ДАСТУРИ**

Билим соҳаси : 100000- «Гуманитар соҳа»

Таълим соҳаси : 130000 – «Математика»

**Таълим
йўналиши: 5110700 - «Информатика ўқитиш
методикаси»**

Самарқанд-2019

Фаннинг ишчи ўқув дастури ўқув, ишчи ўқув режа ва ўқув дастурига мувофиқ ишлаб чиқилди.

Тузувчи: - «Ахборотлаштириш технологиялари»
кафедраси ассистенти Химматов И.Қ.

Такризчилар: СамДУ «Ахборотлаштириш технологиялари»
кафедраси ассистенти

СамДУ «Ахборотлаштириш технологиялари»
кафедраси доценти Қобилов С.С.
СамДУ «Математик моделлаштириш ва
комплекс дастурлаш» кафедраси доценти
Ўринбоев Э.

Фаннинг ишчи ўқув дастури СамДУ «Ахборотлаштириш технологиялари» кафедрасининг 2019 йил “___” _____ даги “___” – сон йиғилишда муҳокамадан ўтган ва факультет кенгашида муҳокама қилиш учун тавфсия этилган.

Кафдра мудири: _____ Жуманов И.И.

Фаннинг ишчи ўқув дастури СамДУ Амалий математика ва информатика факультет кенгашида муҳокама этилган ва фойдаланишга тавфсия қилинган. (2019 йил “___” _____ даги “___” -сонли баённома).

Факультет кенгаши раиси _____ **Ахатов А.Р.**
“___” _____

Келишилди: Ўқув услубий
бошқарма бошлиғи: “___” _____ **Холхўжаев А.**

Кириш

Ушбу дастур “Информатика ўқитиш методикаси” таълим йўналишидаги талабаларни Ахборот хавфсизлиги фанидан чуқур билим эгаси бўлишига қаратилган. Ахборотларни ҳимоялашнинг криптография соҳасидаги масалаларни эчиш, ахборот хавфсизлиги сиёсати, архитектураси ва стратегияси криптографик алгоритмларни таҳлил қилиш, улар ёрдамида шифрлаш амаллари, электрон рақамли имзо, идентификация схемалари ҳақида тушинча берилади ва улардан фойдаланиш ўргатилади.

Фаннинг мақсад ва вазифалари

Фанни ўқитишдан мақсад - талабаларда ахборотларни ҳимоя қилишнинг замонавий усуллари ҳақида мос билим, қўникма ва малакасини шакллантириш.

Фаннинг вазифаси - талабаларга ахборот хавфсизлиги сиёсати, архитектураси ва стратегияси, замонавий компьютер технологиялари асосида шифрлаш, электрон рақамли имзо алгоритмларини назарий ва дастурий таъминотини ўрганишдан иборат.

Фан бўйича талабаларнинг малакасига қўйиладиган талаблар

«Ахборотларни ҳимоялаш» ўқув фанини ўзлаштириш жараёнида амалга ошириладиган масалалар доирасида бакалавр:

- замонавий ахборот жамияти очик ахборот тизимининг ахборот соҳасида глобаллашув жараёни;
 - Ахборотларни ҳимоялаш асосларини ўрганиш имкониятини берувчи асосий тушинчалар ва терминлар;
 - Оммавий ахборот тизимларининг очиклиги шароитида шахс, жамият ва давлатнинг ахборот хавфсизлигини, хусусан, ахборот-психологик хавфсизлигини таъминлаш соҳасидаги фаолияти мақсад, вазифалар ва йўналишлари;
 - ахборотлаштириш соҳасидаги таҳдидлардан инсон, жамият ва давлатнинг ахборот-психологик жихатдан муҳофазалашнинг моҳияти;
- Ахборот экспансияси кучайиши шароитида оммавий ахборот соҳасида шахс, жамият ва давлатга ахборот-психологик таҳидларга нисбатан қарши фаолиятининг шакл ва услублари ҳақида тасавурга эга бўлиши;
- талаба катта ахборот массивларини маънавий, сиёсий, маъқуравий нуқтаи назардан ҳамда шахс, жамият ва давлат хавфсизлиги жихатидан таҳлил қила олишлари.

Ўқув режадаги бошқа фанлар билан боғлиқлиги

«Ахборотларни ҳимоялаш» фани умумқасбий фан ҳисобланиб, 2-семестрда ўтилади. Дастурни амалга ошириш ўқув режасида режалаштирилган умумқасбий фанлар (информатиканинг назарий асослари,

программалаш асослари) фанларидан этарли билим ва кўникмаларга эга бўлишлари талаб этилади.

Фаннинг ишлаб чиқаришдаги ўрни

Ишлаб чиқаришнинг турли жабхаларига оид ахборотларни ишончли саклаш, уларни ҳар хил бузувчилар, ҳакерлардан ҳимоялаш жуда ҳам долзарб ҳисобланади. Глобал компютер тармоклари пайдо бўлгандан кейин ахборотларни ҳимоя қилиш янада қийинлашди. Эндиликда тармок орқали юқори даражада ҳимояланмаган тизимларни бузуб кириш ёки ишдан чиқариш ҳам мумкин бўлиб қолди. Тизим хавфсизлигини таъминлаш учун бу муаммоларга комплекс тарзда ёндашиш керак.

Хозирда яратилган крипто­ти­зим­лар катта ҳажмдаги турли табиатли ахборотларни ҳимоялаш учун унинг самарали воситалар сифатида тан олинган. Шу билан бирга банк, молия, солиқ ва божхона тизимининг ишлари берилганлар базасини тизимлари ёрдамида автоматлаштирилган ва ахборотларни ҳимоялаш усуллари­дан фойдаланилади (шифрлаш, электрон рақамли имзо ва бошқалар).

Фанни ўқитишда замонавий ахборот ва педагогик технологиялар

Талабаларнинг “ Ахборотларни ҳимоялаш ” фанини ўзлаштиришлари учун ўқитишнинг илғор ва замонавий усуллари­дан фойдаланиш, янги информатсион-педагогик технологияларни тад­бик қилиш муҳим аҳамиятга эгадир. Фанни ўзлаштиришда дарслик, ўқув ва услубий қўлланмалар, маъруза матнлари, таркатма материаллар, электрон материаллар, виртуал стендлар ҳамда компютер технол­гияларидан фойдаланилади. Маъруза ва амалий дарсларда мос равишда мунозара, блитс-сўров ва кичик гуруҳларда ишлаш каби илғор педагогик технология­ли­дан фойдаланилади.

Шахсга йўналтирилган таълим. Бунда келгусидаги мутахассис фаолияти билан боғлиқ ўқитиш, масалалар, мавзулар ишчи дастурда қўрилиши кераклиги назарда тутилган.

Тизимли ёндошув. “Информатика ўқитиш методикаси” таълим йўналишининг барча белгилари мужассам этилиши, барча фанларнинг ўзаро боғланганлиги ва таълим технологиясининг яхлитлиги назарда тутилган.

Фаолиятга йўналтирилган ёндошув. Мазкур дастурда келгусидаги мутахассис сифатларини шакллантириш, активлаштириш ва унинг барча қобилияти ва ташаббусқорлигини очишга этибор берилган.

Диалогик ёндошув. Фаннинг амалиёт дарсларида шахснинг ўз-ўзини фаоллаштириш, ўзини кўрсата олиш каби ижодий фаолиятларини ривожлантириш назарда тутилган.

Ҳамкорликдаги таълимни ташкил қилиш. Талабаларнинг қуйилган масала эчимларини олишда биргаликдаги ишлашни жорий этиш зарурлиги эътиборга олинган.

Муаммоли таълим. Таълим олувчи фаолиятини активлаштириш учун фан дастури билан боғлиқ кизикарли мавзулар муҳокама қилинишлиги, бунда илмий билимнинг обектив қарама-қаршилиги, уни ҳал этиш усуллари,

амалий фаолиятга уларни қўллаш масалаларни муҳокама қилиш назарда тутилган.

Ахборотни такдим қилишнинг замонавий воситалари ва усулларини қўллаш - янги компьютер ва ахборот технологияларни ўқув жараёнига қўллаш.

Ўқитишнинг мавзулари ва техникаси. Маъруза, муаммоли таълим, кейс-технология, пинборд, парадокс ва лойихлаш усуллари, амалий ишлар.

Ўқитишни ташкил этиш шакллари. Диалог, мулоқот, ҳамкорлик, ўзаро ўрганишга асосланган фронтал, коллектив ва гуруҳ.

Ўқитиш воситалари. Дарслик, маъруза матни, электрон китоб, электрон ўқув қўлланмалар, электрон ўйинлар ва шу билан бир каторда компьютер ва ахборот технологиялари.

Коммуникация усуллари. Тингловчилар билан оператив тескари алоқага асосланган бевосита ўзаро муносабатлар.

Тескари алоқа усуллари ва воситалари: кузатиш, блис-сўров, оралик, жорий, якуний назорат тахлили.

Бошқариш усуллари ва воситалари: ўқув машғулотни бошқаришнинг белгилаб берувчи технологик харита қўринишидаги ўқув машғулотларини режалаштириш, қўйилган мақсадга эришишда ўқитувчи ва тингловчининг биргаликдаги ҳаракати, аудитория машғулотлари ва мустақил ишлар назорати.

Мониторинг ва баҳолаш. Курс охирида тест топшириқлари ёки ёзма иш вариантлари бўйича талабалар билимлари баҳоланади.

Айрим мавзулар бўйича талабалар билим баҳолаш тест асосида ва компьютер ёрдамида бажарилади. Интернет тармоғидаги расмий иктисодий кўрсаткичларидан фойдаланилади, таркатма материаллар тайёрланади, таянч сўз ва иборалар асосида оралик ва якуний назоратлар ўтказилади.

Маъруза қисми

т/р	Мавзулар номи	Маъруза
1	Замонавий ахборотлашган жамият. Асосий тушунчалар ва тарифлар. Ахборотларни ҳимоялашнинг асосий ҳавфлари	2
2	Вируслар ва антивируслар.	2
3	Ахборотларни стенографик ҳимоялаш усуллари	2
4	Ахборотларни криптографик ҳимоялаш усуллари.	2

5	Симметрияли криптоанизим асослари	2
6	Асимметрик криптоанизим асослари.	2
7	Электрон рақамли имзо	2
	Жами	14

Асосий қисм: Фаннинг услубий жиҳатдан узвий кетма-кетлиги

Асосий қисмда (маъруза) фанни мавзулари мантикий кетма-кетликда келтирилади. Ҳар бир мавзунинг моҳияти асосий тушунчалар ва тезислар орқали очиб берилади. Бунда мавзу бўйича талабаларга ДТС асосида етказилиши зарур бўлган билим ва кўникмалар тула қамраб олиниши керак.

Асосий қисм сифатига қўйиладиган талаб мавзуларнинг долзарблиги, уларнинг иш берувчилар талаблари ва ишлаб чиқариш эҳтиёжларига мослиги, мамлакатимизда бўлаётган ижтимоий-сиёсий ва демократик ўзгаришлар, иқтисодиётни эркинлаштириш, иқтисодий-ҳуқуқий ва бошқа соҳалардаги ислохатларнинг устувор масалаларини қамраб олиши ҳамда фан ва технологияларнинг сўнгги ютуқлари эътиборга олиниши тавсия этилади.

Маъруза машғулотлари Фаннинг назарий машғулотлари мазмуни

Ахборотларни химоялаш кириш, фаннинг асосий тушунчалари ва мақсади, ахборотларга нисбатан хавф-хатарлар таснифи, химоянинг бузилиши; химоя хизмати; ахборот хавфсизлиги фаолият соҳалари.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим. Бинго, блиц, нилуфар гули, меню, алгоритм, мунозара, ўз-ўзини назорат.

Адабиётлар: А1, А3, А4, А5, Қ1, Қ3, Қ4, Қ8

Химояланган дастурий таъминот ахборотини асосий даражалари ва вазибалари.

Ахборотларни химоялашда бузувчининг модели, бўлиши мумкин бўлган тахдидларни олдини олиш, мақсадлар ва усулларга боғлиқ ҳолда ахборот хавфсизлигини бузувчилар категориялари, компьютер тизимлари ва тармоқларида хавфсизлик моделлари, Белла ва Ла-Падула модели, Деннинг модели, Ландвер модели.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим. Бинго, блиц, нилуфар гули, меню, алгоритм, мунозара, ўз-ўзини назорат.

Адабиётлар: А1, А3, А2, А4, А5, Қ1, Қ3, Қ4, Қ7

Ахборотни ҳимоялашнинг криптографик усуллари.

Криптографиянинг асосий қоидалари ва таърифлари, шифрлаш усулларининг туркумланиши, симметрик (махфий) ва асимметрик (очик) калитли шифрлаш тизимлари, алмаштириш (подстановка) усулларининг моҳияти, полиалфавитли алмаштириш усуллари, шифрлашнинг аддитив усуллари, RSA алгоритми.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим. Бинго, блиц, нилуфар гули, меню, алгоритм, мунозара, ўз-ўзини назорат.

Адабиётлар: А1, А2, А3, А4, А5, Қ1, Қ3, Қ4, Қ8

Ахборот хавфсизлигининг стратегияси ва архитектураси.

Ахборотларни химоялашда соҳасида ҳуқуқий бошқариш, ахборот хавфсизлигининг ташкилий – маъмурий таъминоти, ахборот хавфсизлиги бўйича стандартлар ва спецификациялар, ахборот хавфсизлигининг ҳуқуқий таъминоти, ахборот хавфсизлигининг халқаро ва миллий ҳуқуқий меъёрлари, ҳуқуқий бошқариш предметлари, ахборот химоясининг ҳуқуқий режими, ахборот хавфсизлигининг ташкилий-маъмурий таъминоти, маъмурий тадбирлар.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим. Бинго, блиц, нилуфар гули, меню, алгоритм, мунозара, ўз-ўзини назорат.

Адабиётлар: А1, А3, А4, А5, Қ1, Қ3, Қ4, Қ8

Ахборотларни химоялашда таҳдидлар, уларнинг таснифи ва таҳлили

Химоялашни адаптив бошқариш концепцияси. Химояланишни таҳлиллаш. Хужумларни аниқлаш.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим. Бинго, блиц, нилуфар гули, меню, алгоритм, мунозара, ўз-ўзини назорат.

Адабиётлар: А1, А3, А4, А5, Қ1, Қ3, Қ4, Қ8

Идентификация ва аутентификация.

Асосий тушунчалар ва туркумланиши, идентификация, аутентификация, фойдаланувчиларнинг ҳақиқийлигини аниқлаш, авторизация, маъмурлаш, маълумотларни узатиш каналларини химоялашда субъектларнинг ўзаро аутентификацияси, парол, сертификатлар ва рақамли имзолар, пароллар асосида аутентификациялаш, сертификатлар асосида аутентификациялаш, фойдаланувчиларни биометрик идентификациялаш ва аутентификациялаш.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим. Бинго, блиц, нилуфар гули, меню, алгоритм, мунозара, ўз-ўзини назорат.

Адабиётлар: А1, А3, А4, А5, Қ1, Қ3, Қ4, Қ8

Ахборотларни ҳимоялашнинг заифлиги

Электрон почтадан фойдаланиш ва E-mail асослари. E-mailдаги мавжуд муаммолар. Электрон почтада мавжуд хавфлар ва улардан ҳимоялаш.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим. Бинго, блиц, нилуфар гули, меню, алгоритм, мунозара, ўз-ўзини назорат.

Адабиётлар: А1, А3, А4, А5, Қ1, Қ3, Қ4, Қ8

Конфиденциаллик, бутунлик ва фойдаланувчанликни чеклаш

Электрон тўловлар тизими асослари. Идентификацияловчи шахсий номерни ҳимоялаш. POS тизими хавфсизлигини таъминлаш. Банкоматлар хавфсизлигини таъминлаш. Ахборотларни ҳимоялашнинг асосий воситалари.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим. Бинго, блиц, нилуфар гули, меню, алгоритм, мунозара, ўз-ўзини назорат.

Адабиётлар: А1, А3, А4, А5, Қ1, Қ3, Қ4, Қ8

Компьютер вируслари, зараркунанда дастурлар ва уларни ҳимоялаш механизмлари

Электромагнит нурланиш ва таъсирланишлардан ҳимояланишнинг пасив усуллари. Электромагнит нурланиш ва таъсирланишлардан ҳимояланишнинг актив усуллари.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим. Бинго, блиц, нилуфар гули, меню, алгоритм, мунозара, ўз-ўзини назорат.

Адабиётлар: А1, А3, А4, А5, Қ1, Қ3, Қ4, Қ8

Ахборот ҳимоясининг криптографик усуллари

Компьютер вируслари ва уларнинг классификацияси. Вируслар билан курашиш методлари ва воситалари.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.

Адабиётлар: А1, А4, А6, Қ2, Қ3

Криптографик тизимларни ташкиллаштириш

Криптографиянинг асосий қоидалари ва таърифлари, шифрлаш усулларининг туркумланиши, симметрик (махфий) ва асимметрик (очик) калитли шифрлаш тизимлари, алмаштириш (подстановка) усулларининг моҳияти, полиалфавитли алмаштириш усуллари, шифрлашнинг аддитив усуллари, RSA алгоритми.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим. Бинго, блиц, нилуфар гули, меню, алгоритм, мунозара, ўз-ўзини назорат.

Адабиётлар: А1, А2, А3, А4, А5, Қ1, Қ3, Қ4, Қ8

Ахборот хавфсизлиги соҳасида халқаро стандартлар

Компьютер вируслари ва уларнинг классификацияси. Вируслар билан курашиш методлари ва воситалари.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.

Адабиётлар: А1, А4, А6, Қ2, Қ3

Электрон рақамли имзо

Электрон ҳужжатларни аутентификацияла Рақамли имзони шакллантириш муолажаси. Рақамли имзони текшириш муолажаси

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим. Бинго, блиц, нилуфар гули, меню, алгоритм, мунозара, ўз-ўзини назорат.

Адабиётлар: А1, А3, А4, А5, Қ1, Қ3, Қ4, Қ8

Амалий машғулотларнинг тавсия этиладиган мавзулари:

- 1. Ахборотларни ҳимоялаш усуллари Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3
- 2. Симметрик ўрин алмаштири алгоритмлари ёрдамида шифрлаш мисол**
Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.
Адабиётлар: А1, А4, А6, Қ2, Қ3
- 3. Ахборотларни ҳимояларининг бузилишлари ва унинг оқибатлари шифрлашга мисол Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3
- 4. Вернам, Гаммалаш ҳамда Уитстоннинг “иккилик квадрат” шифрлаш усуллари ёрдамида шифрлаш мисол**
Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.
Адабиётлар: А1, А4, А6, Қ2, Қ3
- 5. Идентификациялаш ва аутентификациялаш усуллари мисол**
Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.
Адабиётлар: А1, А4, А6, Қ2, Қ3

6. **Очиқ калитли криптолизимлар алгоритмларини дастурлаш мисол Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3
7. **Компьютер вируслари ва улардан ҳимояланиш Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3
8. **Windows 7 ОТ ни хавфсиз ишлаши учун ОТда «Фойдаланувчилар қайд ёзувларини яратиш ва созлаш. Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3
9. **Гамильтон маршрутига асосланган шифрлаш Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3
10. **Windows 7 ОТнинг «Хавфсизлик параметрлари»ни созлаш Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3
11. **Аналитик усулларга асосланган шифрлаш алгоритми Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3
12. **Windows 7 ОТнинг хавфсизлик аудити сиёсати параметрларини созлаш Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3
13. **Электрон рақамли имзо Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3
14. **Windows 7 ОТда дастурлардан фойдаланишни чеклаш сиёсати Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3
15. **Cloud Computing технологиясида маълумотлар хавфсизлигини таъминлаш усуллари.Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.**
Адабиётлар: А1, А4, А6, Қ2, Қ3

16. Антивирус дастурларини ўрнатиш ва хавфсизлик параметрларини созлаш Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, БББ жадвали, кластер усули.

Адабиётлар: А1, А4, А6, Қ2, Қ3

№	Амалий машғулоти мавзулари	Ажратилган соат
1	Антивирус Касперский 6.0. дастурини ўрнатиш ва созлаш, базани янгилаш	2
2	Классик симметрик криптолизимлар	2
3	Ўрин алмаштириш усули	2
4	Шифрлаш жадваллари	2
5	Сехрли квадратларни қўллаш. Трисемус шифрлаш жадвали.	2
6	Плейфейр биграмма шифри. Хилл криптолизими.	2
7	Вижинер жадвали	2
8	Очиқ калитли криптолизимлар	2
9	Електрон рақамли имзо алгоритми	2
	Жами	18

Мустақил ишлар мавзулари

Ахборотларни химоялаш бўйича Ўзбекистон Республикасида ишлаб чиқилган қонунлар, фармойишлар ва қарорлар. Ахборот-коммуникация технологияларига бўладиган таҳдидлар. Зарар келтирадиган вирусли дастурлар. Ахборотни шифрлаш бўйича ишлаб чиқилган хорижий давлатлар стандартлари. Хорижий давлатлар электрон рақамли имзо алгоритмлари. Ахборотларни химоялашда аутентификация ва идентификация. Тармоқлараро экран технологияси. Химояланган виртуал хусусий тармоқлар VPN. Ахборот-коммуникацион тизимларга суқилиб киришларни аниқлаш. Компьютер вируслари ва вирусдан химояланиш усуллари. Симсиз алоқа тизимларида ахборотни химоялаш. Ахборотни рухсатсиз фойдаланишлардан химоялаш.

т.р	Лаборатория машғулоти мавзулари	Соат
1	1-Лаборатория машғулоти Дастурларни компьютер вирусларидан химоялаш 1. Масаланинг қўйилиши ва унинг таҳлили 2. Замонавий антивирус дастурларидан фойдаланиш усуллари 3. Лаборатория ишини якунлаш ва ҳисобот тайёрлаш	6

2	2-Лаборатория машғулот Ахборотларни стенографик ҳимоялаш усуллари 1. Масаланинг кўйилиши ва унинг тахлили 2. Замонавий антивирус дастурларидан фойдаланиш усуллари 3. Лаборатория ишини яқунлаш ва ҳисобот тайёрлаш	6
3	3-Лаборатория машғулот Симметрияли криптолизим асослари 1. Масаланинг кўйилиши ва унинг тахлили 2. Замонавий антивирус дастурларидан фойдаланиш усуллари 3. Лаборатория ишини яқунлаш ва ҳисобот тайёрлаш	6
4	4-Лаборатория машғулот Вижинер жадвали ва Сезар усули. Гамильтон маршрутларига асосланган шифрлаш 1. Масаланинг кўйилиши ва унинг тахлили 2. Полиалфавитли вижинер жадвалини (матрицасини) қўллаган ҳолда ва Сезар шифрлаш усуллари асосида маълумотларни шифрлаш дастурларини тузиш 3. Лаборатория ишини яқунлаш ва ҳисобот тайёрлаш	6
5	Лаборатория ишлари натижалари тақдимотини яратиш. Лаборатория ишлари ҳимояси	4
	Жами	28

Дастурнинг информатсион-услугий таъминоти.

Мазкур фанни ўқитиш жараёнида таълимнинг замонавий методлари, педагогик ва ахборот-коммуникация технологияларни қўллаш назарда тутилган:

- маъруза дарсларида замонавий компьютер технологиялари ёрдамида презентацион ва электрон-дидактик материаллардан;
 - амалий машғулотларида замонавий компьютер синфларидан фойдаланиш кўзда тутилган. Шунингдек бугунги куннинг асосий маълумотлар олиш базаси сифатида Интранет ва Интернет тизимида уланган бўлиши ва университет порталига маълумотларни жойлаштириш имконияти мавжуд бўлиши лозим.
- “Ахборот ҳавсизлиги” фанидан талабалар билимини рейтинг тизими асосида баҳолаш мезони

"Ахборотларни ҳимоялаш" фани бўйича рейтинг жадваллари, назорат тури, шакли, сони ҳамда ҳар бир назоратга ажратилган максимал балл, шунингдек жорий ва оралик назоратларининг саралаш баллари ҳақидаги маълумотлар фан бўйича биринчи машғулотда талабаларга эълон қилинади.

Фан бўйича талабаларнинг билим савияси ва ўзлаштириш даражасининг Давлат таълим стандартларига мувофиқлигини таъминлаш учун қуйидаги назорат турлари ўтказилади:

- **жорий назорат (ЖН)** - талабанинг фан мавзулари бўйича билим ва амалий кўникма даражасини аниқлаш ва баҳолаш усули. Жорий назорат фаннинг хусусиятидан

келиб чиққан ҳолда амалий машғулотларда оғзаки суров, тест утказиш, суҳбат, назорат иши, коллеквиум, уй вазифаларини текшириш ва шу каби бошқа шаклларда ўтказилиши мумкин;

- **оралиқ назорат (ОН)** - семестр давомида ўқув дастурининг тегишли (фанларнинг бир неча мавзуларини ўз ичига олган) бўлими тугаллангандан кейин талабанинг назарий билим ва амалий кўникма даражасини аниқлаш ва баҳолаш усули. Оралиқ назорат бир семестрда икки марта ўтказилади ва шакли (оғзаки, ёзма) ўқув фанига ажратилган умумий соатлар ҳажмидан келиб чиққан ҳолда белгиланади;

- **якуний назорат (ЯН)** - семестр якунида муайян фан бўйича назарий билим ва амалий кўникмаларни талабалар томонидан ўзлаштириш даражасини баҳолаш усули. Якуний назорат тест шаклида ўтказилади.

ОН ўтказиш жараёни кафедра мудири томонидан тузилган комиссия иштирокида мунтазам равишда ўрганиб борилади ва уни ўтказиш тартиблари бузилган ҳолларда, **ОН** натижалари бекор қилиниши мумкин. Бундай ҳолларда **ОН** қайта ўтказилади.

Олий таълим муассасаси раҳбарининг буйруғи билан ички назорат ва мониторинг бўлими раҳбарлигида тузилган комиссия иштирокида **ЯН** ни ўтказиш жараёни мунтазам равишда ўрганиб борилади ва уни ўтказиш тартиблари бузилган ҳолларда, **ЯН** натижалари бекор қилиниши мумкин. Бундай ҳолларда **ЯН** қайта ўтказилади.

Талабанинг билим савияси, кўникма ва малакаларини назорат қилишнинг рейтинг тизими асосида талабанинг фан бўйича ўзлаштириш даражаси баллар орқали ифодаланади.

Фан бўйича талабаларнинг семестр давомидаги ўзлаштириш курсаткичи 100 баллик тизимда баҳоланади.

Ушбу 100 балл баҳолаш турлари бўйича қуйидагича тақсимланади: Я.Н.-30 балл, қолган 70 балл эса Ж.Н.-35 балл ва О.Н.-35 балл қилиб тақсимланади.

Балл	Баҳо	Талабаларнинг билим даражаси
86-100	Аъло	Хулоса ва қарор қабул қилиш. Ижодий фикрлай олиш. Мустақил мушоҳада юрита олиш. Олган билимларини амалда қўллай олиш. Моҳиятини тушунтириш. Билиш, айтиб бериш. Тасаввурга эга бўлиш.
71-85	Яхши	Мустақил мушоҳада қилиш. Олган билимларини амалда қўллай олиш. Моҳиятини тушунтириш. Билиш, айтиб бериш. Тасаввурга эга бўлиш.
55-70	Кониқарли	Моҳиятини тушунтириш. Билиш, айтиб бериш. Тасаввурга эга бўлиш.
0-54	Кониқарсиз	Аниқ тасаввурга эга бўлмаслик. Билмаслик.

Фан бўйича саралаш бали 55 баллни ташкил этади. Талабанинг саралаш балидан паст бўлган ўзлаштириш рейтинг дафтарчасида қайд этилмайди.

Талабаларнинг ўқув фани бўйича мустақил иши жорий, оралиқ ва якуний назоратлар жараёнида тегишли топшириқларни бажариши ва унга ажратилган баллардан келиб чиққан ҳолда баҳоланади.

$$\text{Талабанинг фан бўйича рейтинги қуйидагича аниқланади: } R = \frac{V \cdot O}{100}$$

бу ерда: V- семестрда фанга ажратилган умумий укув юкламаси (соатларда); О`-фан буйича узлаштириш даражаси (балларда).

Фан буйича жорий ва оралик назоратларга ажратилган умумий баллнинг 55 фоизи саралаш балл ҳисобланиб, ушбу фоиздан кам балл туплаган талаба якуний назоратга киритилмайди.

- Жорий **ЖН** ва оралик **ОН** турлари буйича 55бал ва ундан юкори бални туплаган талаба фанни узлаштирган деб ҳисобланади ва ушбу фан буйича якуний назоратга кирмаслигига йул куйилади.

- Талабанинг семестр давомида фан буйича туплаган умумий бали хар бир назорат туридан белгиланган коидаларга мувофик туплаган баллари йигиндисига тенг.

- **ОН** ва **ЯН** турлари календар тематик режага мувофик деканат томонидан тузилган рейтинг назорат жадваллари асосида утказилади. **ЯН** семестрнинг охириги 2 хафтаси мобайнида утказилади.

- **ЖН** ва **ОН** назоратларда саралаш балидан кам балл туплаган ва узрли сабабларга кура назоратларда катнаша олмаган талабага кайта топшириш учун, навбатдаги шу назорат туригача, сунгги жорий ва оралик назоратлар учун эса якуний назоратгача булган муддат берилади.

- Талабанинг семестрда **ЖН** ва **ОН** турлари буйича туплаган баллари ушбу назорат турлари умумий балининг 55 фоизидан кам булса ёки семестр якуний жорий, оралик ва якуний назорат турлари буйича туплаган баллари йигиндиси 55 балдан кам булса, у академик карздор деб ҳисобланади.

- Талаба назорат натижаларидан норози булса, фан буйича назорат тури натижалари эълон килинган вақтдан бошлаб бир кун мобайнида факультет деканига ариза билан мурожаат этиши мумкин. Бундай холда факультет деканининг тақдимномасига кура ректор буйруги билан 3 (уч) аъзодан кам булмаган таркибда апелляция комиссияси ташкил этилади.

- Апелляция комиссияси талабаларнинг аризаларини куриб чикиб, шу куннинг узида ҳулосасини билдиради.

- Баҳолашнинг урнатилган талаблар асосида белгиланган муддатларда утказилиши ҳамда расмийлаштирилиши факультет декани, кафедра мудури, укув-услугий бошкарма ҳамда ички назорат ва мониторинг булими томонидан назорат килинади.

Талабалар ОН дан туплайдиган балларнинг намунавий мезонлари

№	Курсаткичлар	ОН баллари	
		макс	1-ОН (тест)
1	Дарсларга катнашганлик даражаси. Маъруза дарсларидаги фаоллиги, конспект дафтарларининг юритилиши ва туликлиги.	10	0-10
2	Талабаларнинг мустакил таълим топшириқларини уз вақтида ва сифатли бажариши ва узлаштириш.	10	0-10
3	Оғзаки савол-жавоблар, коллоквиум ва бошқа назорат турлари натижалари бўйича	15	0-15
Жами ОН баллари		35	0-35

№	Курсаткичлар	Ж
		макс
1	Дарсларга катнашганлик ва узлаштириши даражаси. Амалий машгулотлардаги фаоллиги, амалий машгулот дафтарларининг юритилиши ва ҳолати	10
2	Мустакил таълим топшириқларининг уз вақтида ва сифатли бажарилиши. Мавзулар бўйича уй вазифаларини бажарилиш ва узлаштириши даражаси.	10
3	Езма назорат иши ёки масалаларга тузадиган дастурига мувофиқ	15
Жами ЖН баллари		35

Якуний назорат “Тест” шаклида белгиланган, якуний назорат 30 баллик “Тест” вариантлари асосида ўтказилади ва якуний назорат қуйидаги жадвал асосида амалга оширилади:

№	Кўрсаткичлар	ЯН баллари	
		Макс	Ўзгариш оралиғи
1	Фан бўйича якуний назорат	30	0-30
	Жами	30	0-30

Якуний назоратда “Тест”ларни баҳолаш мезони

Якуний назорат “Тест” шаклида амалга оширилади, синов тест саволларидан иборат базадан олинган кўп вариантли усулда ўтказилади. Ҳар бир вариантда назарий ва амалий топшириқлардан ташкил топган 50 та савол танлаб олинади. Саволлар фан бўйича таянч сўз, иборалар ҳамда амалий топшириқлар асосида тузилган бўлиб, фаннинг барча мавзуларини ўз ичига қамраб олган.

Тест синови бўйича умумий ўзлаштириш кўрсаткичини аниқлаш учун 30 ни тўғри жавоблар йиғиндисига кўпайтириб 50 га бўламиз ва натижада талабанинг якуний назорат бўйича ўзлаштириш бали келиб чиқади.

5. Адабиётлар

- 1. С.С.Қосимов. Ахборот технологиялари. Ўқув қўлланма. – Тошкент. "Алоқачи", 2006.**
- 2. С.К.Ғаниев, М.М. Каримов. Хисоблаш системалари ва тармоқларида информация химояси. Олий ўқув юрт.талаб. учун ўқув қўлланма.-Тошкент Давлат техника университети, 2003.**
- 3. В.И. Завгородний. Комплексная защита информации в компьютерных системах: Учебное пособие.-М: Логос; ПБОЮЛ Н.А.Егоров, 2001.**

5.2. Қўшимча адабиётлар

- 1. Г.Н. Устинов. Основы Информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия "Безопасность".-М.:СИНТЕГ, 2000.**
- 2. Мерит Максим, Девид Поллино. Безопасность беспроводных сетей. Информационные технологии для инженеров.-Москва. 2004.**
- 3. А. Соколов, О. Степанюк. Защита от компьютерного терроризма. Справочное пособие. БХВ-Петербург. Арлит, 2002.**
- 4. А.М. Астахов. Аудит безопасности информационных систем. //Конфидент.-2003.-№1,2.**

5.3. Интернет сайтлари

1. [www.ulstu.ru/people/SOSNIN/umk/Image Recognition and _Scene_Analysis/chapters/ch](http://www.ulstu.ru/people/SOSNIN/umk/Image_Recognition_and_Scene_Analysis/chapters/ch)
2. ocrai.narod.ru
3. e-smirnov.narod.ru
4. <http://dimacs.Rutgers.edu/>
5. [l. h ttp://epubs, s i am. or g/s am -bi n/dbq, toclic s t/S I.DM A](http://epubs.siam.org/sam-bi n/dbq, toclic s t/S I.DM A)
6. <http://www.uni-bonn.de/logic/world.html>
7. [http://www.vspub.com/jomals/jn- isMatapp.hi:iiil](http://www.vspub.com/jomals/jn-isMatapp.hi:iiil)
8. <http://7/dmoz.org/Scitnce/Math/logic/>
9. <http://www.allbesLru/cataJog/aL3al63744.26>
10. <http://nit.it-SofLm/2003/tezic;y/artigles/296.lrtm>
11. [http://www.niY- shop,iu/books/29955.html.](http://www.niY-shop,iu/books/29955.html)

ЎЗБЕКИСТОН RESPUBLIKASI
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

Рўйхатга олинди:

№ 505130200

2018 йил « 7 » ой



Ўзбекистон Республикаси Олий
ва ўрта махсус таълим вазирлигининг
2018 йил « 7 » ой 6-сони буйруғи билан
тасдиқланган

АХБОРОТЛАРНИ ХИМОЯЛАШ

фанининг

ЎҚУВ ДАСТУРИ

Билим соҳаси: 100 000 – Гуманитар соҳа
Таълим соҳаси: 130 000 – Математика
Таълим йўналиши: 5130200 – Амалий математика ва информатика

Фаннинг ўқув дастури Олий ва ўрта махсус, касб-хунар таълими йўналишлари бўйича ўқув-услубий бирлашмалари фаолиятини мувофиқлаштирувчи Кенгашининг 2014 йил « 4 » 01 даги « 1 »-сонли мажлиси баёни билан маъқулланган.

Фаннинг ўқув дастури Мирзо Улугбек номидаги Ўзбекистон Миллий университетида ишлаб чиқилди.

Тузувчилар:

- Б.Ф. Абдурахимов** - Механика-математика факультети «Информатика ва тадбикий дастурлаш» кафедраси профессори, ф.-м.ф.д.
А.С.Матякубов - Механика-математика факультети «Информатика ва тадбикий дастурлаш» кафедраси доцент в.б., ф.-м.ф.н.

Такризчилар:

- М.Арипов** - ЎзМУ механика-математика факультети «Информатика ва тадбикий дастурлаш» кафедраси профессори, ф.-м.ф.д.
Т. Қодиров - А.Аллоний номидаги ХТХКТМОМИ АТЎ кафедраси доценти, ф.-м.ф.и.

Фаннинг ўқув дастури Мирзо Улугбек номидаги Ўзбекистон Миллий университети услубий кенгашида кўриб чиқилган ва тавсия қилинган (2014 йил « 26 » 14 даги « 6 »-сонли баённома).

Кириш

Ушбу дастур "Амалий математика ва информатика" йўналишидаги талабаларнинг Ахборотларни химоялаш фанидан чуқур билим эгаси бўлишига қаратилган. «Ахборотларни химоялашнинг криптография соҳасидаги масалаларни ечиш, ахборот хавфсизлиги сиёсати, архитектураси ва стратегияси, криптографик алгоритмларни таҳлил қилиш, улар ёрдамида шифрлаш амаллари, электрон рақамли имзо, идентификация схемалари ҳақида тушунча бериладиган ва улардан фойдаланиш ўргатилади. Компьютерларнинг техник ва дастурий таъминотининг доимий равишда янгиланиб, такомиллашиб бориши ҳамда бу фанга қиянаётган янгиланларни ҳисобга олган ҳолда, ҳар йили дастурга қўшимча ва ўзгартiriшлар киритилиши кўзда тутилади.

Ўқув фанининг мақсад ва вазифалари

Фанни ўқитишдан мақсад – талабаларда ахборотларни химоя қилишнинг замонавий усуллари ҳақида мос билим, кўникма ва малакасини шакллантириш.

Фанининг вазифаси – талабаларга ахборот хавфсизлиги сиёсати, архитектураси ва стратегияси, замонавий компьютер технологиялари асосида шифрлаш, электрон рақамли имзо алгоритмларини назарий ва дастурий таъминотини ўргатишдан иборат.

Фан бўйича талабалар билим, кўникма ва малакаларига қўйиладиган талаблар

"Ахборотларни химоялаш" ўқув фанини ўзлаштириш жараёнида амалга ошириладиган масалалар доирасида бақалавр:

- замонавий ахборот жамияти очик ахборот тизимининг ахборот соҳасида глобаллашуви жараёни;
- ахборот хавфсизлиги асосларини ўрганиш имкониятини берувчи асосий тушунчалар ва терминлари;
- оммавий ахборот тизимларининг очиклиги шаронтида шахс, жамият ва давлатнинг ахборот хавфсизлигини, хусусан, ахборот-психологик хавфсизлигини таъминлаш соҳасидаги фаолиятнинг мақсад, вазифалар ва йўналишлари;
- ахборотлаштириш соҳадаги таҳдидлардан инсон, жамият ва давлатнинг ахборот-психологик жиҳатдан муҳофазланишининг моҳияти;
- ахборот экспанцияси кучайиши шаронтида оммавий ахборот соҳасида шахс, жамият ва давлатга ахборот-психологик таҳдидларга нисбатан қарши фаолиятнинг шакл ва услублари ҳақида тасаввурга эга бўлиши;
- талаба катта ахборот маънавларини маънавий, сиёсий, мафкуравий нуқтан назардан ҳамда шахс, жамият ва давлат хавфсизлиги жиҳатидан таҳлил қила олиши;

- касбий фаолият объектлари бўлган ҳуқуқий муносабатлар жараёнида хавфсизлик таъминлашнинг инобатга олиш;
- ахборот таҳдидларини аниқлаш ва олдини олиш, ахборот хавфсизлигини нуқтан назардан аҳмийатли бўлган стратегик масалаларни таҳлил қилишнинг *билиши ва улардан фойдалана олиши*;
- талабалар ўзлари эгалланган билимлардан ҳуқуқий тажрибада фойдалана олиш;
- оммавий ахборот тизимларининг очиклиги шариғида Ўзбекистон Республикаси ахборот хавфсизлигига таҳдидларнинг турларини фарқлаш ва баҳолай олиш;
- Ўз касбий мажбуриятларига ижодий ёндашув ва мустақил тафаккур кўникмаларига;
- касбий фаолиятнинг мос соҳаларида ахборот хавфсизлигини таъминлашнинг барча чора-тадбирларига оид ахборотлар оқимидан позитив маълумотларни танлай билиш;
- ахборотлаштириш шариғида ахборот телекоммуникация очик тизимларидаги ахборотлардан олинган хулосаларни меҳнат самараси учун йўналтира билиш;
- ахборот хавфсизлигини таъминлашга оид норматив-ҳуқуқий ҳужжатлар билан ишлай олиш *кўникмаларига эга бўлиши керак*.

Фаннинг ўқув режадаги бошқа фанлар билан ўзаро боғлиқлиги ва услубий жиҳатдан узвий кетма - кетлиги

«Ахборотларни ҳимоялаш» фани ихтисослик фани ҳисобланиб, 5-семестрда ўқитилади.

Дастурни амалга ошириш ўқув режасида режалаштирилган умумкасбий фанлар (математик анализ, информатиканинг назарий асослари, программалаш асослари) фанларидан етарли билим ва кўникмаларга эга бўлишлик талаб этилади.

Фаннинг ишлаб чиқаришдаги ўрни

Ишлаб чиқаришнинг турли жиҳатларига оид ахборотларни ишончли сақлаш, уларни ҳар хил бузғунчилар, ҳакерлардан ҳимоялаш жуда ҳам долзарб масала ҳисобланади. Глобал компьютер тармоқлари пайдо бўлгандан кейин ахборотларни ҳимоя қилиш янада қийинлашди. Эндиликда тармоқ орқали юқори даражада ҳимояланмаган тизимларни бузиб кириш ёки ишдан чиқариш ҳам мумкин бўлиб қолди. Тизим хавфсизлигини таъминлаш учун бу муаммоларга комплекс тарзда ёндашиш керак.

Ҳозирда яратилган криптотизимлар катта ҳажмдаги турли табиатли ахборотларни ҳимоялаш учун энг самарали воситалар сифатида тан олинган. Шу билан бирга, банк, молия, солиқ ва бошқона тизимларининг ишларини берилганлар базасини бошқариш тизимлари ёрдамида автоматлаштирилган ва ахборотларни ҳимоялаш усулларидан фойдаланади (шифрлаш, электрон рақамли имзо ва бошқалар). Масалан, интернет тизимида фаолият

кўрсатувчи серверларнинг катта қисми, хусусан, тижорат ва пул ўтказиш серверларининг иши маълум криптоалгоритмлар асосида шифрлаш, электрон рақамли имзо қўлланилган ҳолда ташкил этилган.

Фанни ўқитишда замонавий ахборот ва педагогик технологиялар

Талабаларнинг «Ахборотларни химоялаш» фанини ўзлаштиришлари учун ўқитишнинг илғор ва замонавий усуллардан фойдаланиш, яъни информатик – педагогик технологияларни талқин қилиш муҳим аҳамиятга эгадир. Фанни ўзлаштиришда дарслик, ўқув ва услубий қўлланмалар, маъруза матнлари, таркатма материаллар, электрон материаллар ҳамда компьютер технологиялари (C, C++, Delphi, Internet) дан фойдаланилади. Маъруза ва амалий дарсларда мос равишдаги мунозара, блиц-сўров ва кичик гуруҳларда ишлаш каби илғор педагогик технологияларидан фойдаланилади.

Асосий қисм

Фанининг назарий машғулоти мазмуни

Кириш. Ахборот хавфсизлигининг роли ва ўрни. Ахборот хавфсизлиги соҳалари. Ахборот хавфсизлиги сифати. Ахборот хавфсизлиги архитектура-си ва стратегияси. Ахборот хавфсизлиги категориялари. Ахборот хавфсизли-ги моделлари. Ахборотларга «ҳужум»нинг асосий кўринишлари ва манбалари. «Бузиш»нинг энг кўп тарқалган усуллари.

Ахборот хавфсизлиги асослари. Ахборот тизимлари, криптоалгоритмлар классификацияси. Асосий тушунчалар: криптология, криптография, криптоанализ, шифр, криптограмма, очик матн, ёпиқ матн, калит, криптоалгоритм ва криптографик алгоритм. Химояланган информацияни узатишнинг умумий тизими: жўнатувчи, қабул қилувчи, алоқа канали, бузгунчи.

Ахборот хавфсизлигини таъминлашнинг классик усуллари. Алмаштириш шифри тушунчаси. Жадвали алмаштиришлар. Вертикал алмаштириш, горизонтал алмаштириш, иккили алмаштириш. Магик квадратларни қўллаш. Алмаштириш шифрлари криптоанализи. Шифрларни алмаштириш тушунчаси. Цезар шифри. Цезарнинг афини тизими. Клод Шеннон назарияси. Ротор машиналар. Стеганография. Скремблерлар.

Ахборот хавфсизлигида криптографик усуллар. Ахборот хавфсизлиги криптографик усуллари. Ахборот хавфсизлиги стандартлари. Криптографиянинг математик асослари. Ахборотлар назарияси. Сонлар назарияси. Параметрлар дигресси. Хэш-функциялар. Криптология асослари. Алгоритм ва калитлар. Криптоалгоритм. Криптоанализ. Алгоритм хавфсизлиги. Симметрик алгоритмлар. Очик калитли алгоритмлар. Симметрик алгоритмлар. Rijndael алгоритми. Симметрик тизимларда калитнинг узатилиши. Очик калитли криптосистемалар. Рюкзак алгоритми. RSA системаси. El-Gamal системаси. Криптографик протоколлар. Калитларни алмаштириш Диффи-Хелман алгоритми.

Электрон рақамли имзо ва идентификация схемалари, ГОСТ, DSA, El-Gamal алгоритмлари. Хабарларни аутентификация ва идентификацияси. Аутентификация ва идентификация муаммолари, Feige-Fiat-Shamir схемаси. Бир нечта очик калитли криптография. Яширин канал.

Илоҳ: Ишчи дастурни шакллантириш жараёнида мазкур машғулоти турига ишчи ўқув режада ажратилган соат ҳажмига мос мавзулар тандаб ўқитиш тавсия этилади.

Амалий машғулотларни ташкил этиш бўйича кўрсатма ва тавсиялар

Амалий машғулотларнинг мақсади назарий олинган билимлар асосида амалий топшириқларни бажара олиш кўникмаларини ҳосил қилишдан иборат. Талабалар ахборотларни ҳимоялаш усулларини амалий масалаларга қўллашда фойдаланишни ўрганадилар. Амалий машғулотларни ташкил этиш бўйича кафедра профессор – ўқитувчилари томонидан кўрсатма ва тавсиялар ишлаб чиқилади. Унда талабалар асосий мазмун мавзулари бўйича олган билим ва кўникмаларини амалий масалаларни ечиш орқали янада бойитиладилар. Шунингдек, дарслик ва ўқув қўлланмалар асосида талабалар билимларини мустахкамлашга эришиш, таркатма материаллардан фойдаланиш, илмий мақолалар ва тезисларни чоп этиш орқали талабалар билимини ошириш, масалалар ечиш, мавзулар бўйича кўргазмани қуроллар тайёрлаш ва бошқалар тавсия этилади.

Амалий машғулотларнинг тахминий мавзулари рўйхати

1. Алмаштириш методи билан матнларни шифрлаш ва очиш.
2. Оддий алмаштириш усули билан матнларни шифрлаш ва очиш. Криптограммани битта калитда шифрлаш, яшириш, Стеганография. Скремблерлар.
3. Рюкзак, RSA, El-Gamal алгоритмларидан фойдаланиб шифрлаш. Калитлар алмаштириш Диффи-Хелман алгоритми.
4. ГОСТ, DSA, El-Gamal алгоритмлари ёрдамида электрон рақамли имзо қўйиш.
5. Feige-Fiat-Shamir схемаси.
6. Бир нечта очик калитли криптографик алгоритмлардан фойдаланиш.
7. Яширин канал орқали маълумотлар жўнатиш.

Илоҳ: Амалий машғулоти соатлари ҳажмларидан келиб чиққан ҳолда ишчи дастурда мазкур мавзулар ичидан амалий машғулоти мавзуларни шакллантирилади.

Мустақил таълимни ташкил этишнинг шакли ва мазмуни

Талаба мустақил таълимнинг асосий мақсади – ўқитувчининг раҳбарлиги ва назоратида муайян ўқув ишларини мустақил равишда бажариш учун билим ва кўникмаларини шакллантириш ва ривожлантириш.

Талаба мустақил ишнинг ташкил этишда қуйидаги шакллардан фойдаланади:

- айрим назарий мавзуларни ўқув адабиётлари ёрдамида мустақил ўзлаштириш;
- берилган мавзулар бўйича ахборот (реферат) тайёрлаш;
- таркатма материаллар бўйича маърузалар қисmini ўзлаштириш;
- автоматлаштирилган ўргатувчи ва назорат қилувчи тизимлар билан ишлаш;
- талабанинг ўқув-илмий-тадқиқот ишларини бажариш билан боғлиқ бўлган бўлимлари ва мавзуларни чуқур ўрганиш;
- фаол ва муаммоли ўқитиш услубидан фойдаланиладиган ўқув машғулотлари;
- масофавий (дистанцион) таълим;
- назарий билимларни амалиётда қўллаш;
- макет, модел ва намуналар яратиш;
- илмий мақола, анжуманга маъруза тайёрлаш ва ҳ.к.

Тавсия этилаётган мустақил ишларнинг мавзулари

1. С тилида дастурлаш.
2. Алмаштириш шифри дастури.
3. Цезар шифрига дастур тузиш.
4. Стеганография.
5. Рюкзак, RSA, El-Gamal алгоритмларига дастур тузиш.
6. ГОСТ, DSA электрон рақамли имзо алгоритмларига дастур тузиш.

Илоҳ: Мустақил таълим соатлари ҳажмларидан келиб чиққан ҳолда ишчи дастурда мазкур мавзулар ичидан мустақил таълим мавзулари шакллантирилади.

Дастурининг инфор­мация – услубий таъминоти

Мазкур фанни ўқитиш жараёнида таълимнинг замонавий методлари, педагогик ва ахборот-коммуникациялари технологиялари қўлланилиши назарда тутилган.

- маъруза дарсларида замонавий компьютер технологиялари ёрдамида презентацион ва электрон-дидактик технологиялардан;
- шифрлаш ва шифрни очиш мавзуларида, амалий машғулотларда ақлий ҳужум, кичик гуруҳлар мусобақалари, гуруҳли фикрлаш педагогик технологияларидан қўллаш назарда тутилади.

Фойдаланиладиган адабиётлар рўйхати Асосий адабиётлар

1. «Ахборотлаштириш тўғрисида» Ўзбекистон Республикасининг қонуни, 11.12.2003 йилдаги № 560-III-сон

2. «Электрон рақамли имзо тўғрисида» Ўзбекистон Республикасининг қонуни, 11.12.2003 йилдаги № 562-II-сон
3. «Электрон ҳужжат айланиши тўғрисида» Ўзбекистон Республикасининг қонуни, 29.04.2004 йилдаги № 611-II-сон
4. «Электрон тижорат тўғрисида» Ўзбекистон Республикасининг қонуни, 29.04.2004 йилдаги № 613-II-сон
5. «Ахборотлаштириш ва маълумотлар узатиш соҳасида қонунга ҳилоф ҳаракатлар солиқ этганидн учун жавобгарлик қучайтирилганлиги муносабати билан Ўзбекистон Республикасининг айрим қонун ҳужжатларига ўзгариш ва қўшимчалар киритиш тўғрисида» Ўзбекистон Республикасининг қонуни, 25.12.2007 йилдаги №ЗРУ_137-сон
6. Каримов И.А., «Экономическое обозрение № 6, 2002г.», «Информационные технологии на службе развития» ru.infocom.uz/more.php
7. Ганиев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Тошкент, 2009 й., 407 б.
8. Гулжамол С.С. «Основы информационной безопасности.» Тошкент, 2004 г.
9. Арипов М., Пуловченко Ю. «Основы криптологии», Тошкент, 2003 г.
10. Брисе Шнайер «Прикладная криптография», М., 2000 г.
11. Иргалиева Д.Я. Ахборот хавфсизлиги. Тошкент, ТАТУ, 83 б.
12. Ашвин Б. «Защита компьютерной информации». Москва, 2006 г.
13. Зима В. «Безопасность глобальных сетей». Москва, 2001 г.
14. А. В. Фролов. Антивирусная защита: Учебное пособие для защиты информационных ресурсов. 2004 г. <http://frolov-lib.ru/books/av/index.html>

Қўшимча адабиётлар

1. O'zDSt 2009, Shiftlash, Xeshlash funksiyasi. Elektron raqamli imzo.
2. Арно Саюмова «Криптография с открытым ключом», М., 1995 г.
3. Денни Кани «Взломы кодов», М., 2000 г.
4. В. В. Яценко «Введение в криптографию», М., 1999 г.
5. В.П.Кузьминов «Криптографические методы защиты информации», Новосибирск, 1998 г.
6. В. Жельников «Криптография от папируса до компьютера», М., 1995 г.

Электрон манбалар

1. <http://www.intuit.ru>
2. <http://www.zjyonet.uz>
3. <http://www.nuu.uz>, <http://www.tuit.uz>
4. <http://www.cerit.uz>, <http://www.unicon.uz>
5. <http://www.uzinfocom.uz>
6. <http://www.ceit.uz>, <http://www.securitylab.ru>
7. <http://www.wikipedia.org>, <http://www.cryptopro.ru>
8. <http://www.itsecurity.com>, <http://www.cert.org>
9. <http://www.cryptobook.rsu.ru>

Кириш

5521900 - Информатика ва ахборот технологияси, 5523600 - Электрон тижорат, 5523500 - Ахборот хавфсизлиги, 5524400 - Мобил алоқа тизимлари, 5522000 - Радиотехника, 5522100 - Телевидение, радиоалоқа ва телерадиоэшиттириш, 522200 - Телекоммуникация, 5320200 - Ахборотлаштириш ва кутубхонашунослик, 5140800 – “Амалий математика ва информатика”, 5140900- Касб таълими (информатика ва ахборот технологияси), 5140900- Касб таълими (телекоммуникация), 5340100- Иқтисодиёт (тармоқлар бўйича), 5340200- Менежмент (соҳалар бўйича), 5811200- Сервис (ахборот сервис), 5811300- Сервис (электрон ва компьютер техникаси бўйича), 5840200- Почта хизмати таълим йўналиши бўйича бакалаврни тайёрлаш ўқув режасида «Ахборотларни ҳимоялаш» ўқув фани махсус фанлар таркибига киритилган.

Ушбу намунавий ўқув дастурида « Ахборотларни ҳимоялаш » фанига тегишли бўлган барча мавзулар бўйича талабаларга Давлат таълим стандартлари асосида етказилиши шарт бўлган минимум билимлар ва кўникмалар тўла қамраб олинган.

Фанни ўқитилишидан мақсад: криптографияни статистик усулларини ўрганиш ва улар асосида ахборотни ҳимоялаш қобилиятларини эгаллаш.

Талабалар ахборотни ҳимоялаш ва криптография асослари ҳақида тушунчага эга бўлишлари керак, ҳамда ахборотни ҳимоялаш дастурий ва техник воситаларини ишлатиш қобилиятига эга бўлишлари керак.

Фанни ўқитиш «Информатика», «Алгоритмик тиллар», «Ахборотни ҳимоялаш асослари» фанлари асосида олиб бориши керак. Ўқитиш жараёнида талабалар назарий сонли усуллар асосида криптоtahlil қобилиятларини эгаллайдилар.

Ахборотларнинг эҳтимолли- статистик моделлари ва уларнинг энтропияли хоссалари

Дискрет ахборотлар ва уларнинг эҳтимолли моделлари. Энтропия функционал ва унинг хоссалари. Шартли энтропия ва унинг хоссалари. Стационар символли кетма-кетликнинг нисбий энтропияси. Марков символли кетма-кетликнинг энтропияли характеристикалари. Узлуксиз ахборотлар манбалари ва уларнинг энтропияли хоссалари.

Криптологияда ахборотлар назарияси усуллари

Дискрет ахборотлар стационар манбасининг асимптотик хоссалари. Символли кетма- кетликнинг энтропияли турғунлиги. Шеннон бўйича ахборот миқдори ва унинг хоссалари. Криптотизимлар Шеннон моделлари. Симметрик криптотизимлар турғунлиги назарий-информацион баҳолари.

Тасодифий ва псевдотасодифий кетма-кетликларни статистик тестлаш

Текис тарқалган тасодифий кетма-кетлик ва унинг хоссалари. Тасодифий ва псевдотасодифий кетма-кетликларни статистик тестлаш универсал алгоритми. n-сериялар тести. Интерваллар тести. Умумлашган покер-тест. “Купон йиғувчи” тести. Алмаштиришлар тести. Кесишувчи n-грамм тести. Иккилик матрицалар рангларига асосланган тест. Спектрал тестлар. Тасодифий силжишлар тестлари. Маурер универсал статистик тести. Энтропиялар ошишига асосланган тестлар. Лемпел – Зив сиқиш алгоритмига асосланган тест. Чизиқли мураккабликка асосланган тест. Скаляр кўпайтма экстремал статистикасига асосланган тест. Дельта кўпайтма экстремал статистикасига асосланган тест. Тасодифийликни алгоритмик аниқлаш.

Псевдотасодифий кетма-кетликларни генерация қилиш алгоритмлари

Генерация алгоритмлари классификацияси. Чизиқли ва мультипликатив конгруэнт генераторлар. Ночизиқ конгруэнт генераторлар. Чеки майдонда рекуррентлар. Тескари алоқали силжитиш чизиқли регистрлари томонидан яратиладиган кетма-кетликлар. Фибоначчи генераторлари. Бир томонлама функциялар асосида криптотурғун генераторлар. Сонлар назариясига асосланган криптотурғун генераторлар. Элементар псевдотасодифий кетма-кетликларни “яхшилаш” усуллари. Макларен - Марсальи усуллари билан генерация алгоритмларини комбинация қилиш. ЛФСР-генераторларини комбинация қилиш. Тасодифий параметрларга эга конгруэнт генератор.

Оқимли криптотизимлар

Асосий тушунчалар. Рекуррент кетма-кетликлар. Чизиқли рекуррент кетма-кетликлар. Чизиқли рекуррент кетма-кетликлар параметрларини баҳолаш. Чизиқли мураккаблик. Чизиқли рекуррент кетма-кетликлар бошланғич ҳолатини аниқлаш. Кетма-кетликларни комбинация қилиш. Корреляцион криптотахлил.

Симметрик тизимлар криптотахлили математик усуллари

Криптотахлил вазибалари ва принциплари. “Синаб кўриш” усули ва унинг мураккаблиги. Статистик қарор қабул қилиш назариясига асосланган криптотахлил усуллари. Айирмалли криптотахлил. Чизиқли криптотахлил.

Амалий машғулотлар

Ахборотларнинг эҳтимолли- статистик моделлари ва уларнинг энтропияли хоссалари. Криптологияда ахборотлар назарияси усуллари. Тасодифий ва псевдотасодифий кетма-кетликларни статистик тестлаш. Псевдотасодифий кетма-кетликларни генерация қилиш алгоритмлари. Оқимли криптотизимлар. Симметрик тизимлар криптотахлили математик усуллари.

Лаборатория иши

Ахборотларнинг эҳтимолли- статистик моделларини дастурлаш. Криптологияда ахборотлар назарияси усулларини дастурлаш. Тасодифий ва псевдотасодифий кетма-кетликларни статистик тестлаш. Псевдотасодифий кетма-кетликларни генерация қилиш алгоритмларини дастурлаш. Оқимли криптотизимларни дастурлаш. Симметрик тизимлар криптотахлилларини дастурлаш

Мустақил иш

Криптографиянинг статистик усуллари ривожланиш босқичлари билан танишиш. Криптографияда статистик усуллардан фойдаланиш йўллари. Квант криптографияси асослари. Ассимметрик тизимлар тахлили статистик усулларининг замонавий ҳолати.

Дарслик ва ўқув қўлланмалари рўйхати

Асосий

1. Коблиц, Н. Курс теории чисел и криптографии - М., Научное издательство ТВП, 2001 г., 260 стр. (перевод с английского).
2. Яценко В.В. Введение в криптографию. МЦМО, 2003
3. Масленников. Практическая криптография БХВ – СПб 2003
4. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф. 2002.
5. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком . 2002
6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных кн. 1.-М.: Энергоатомиздат. -1994.-400с.
7. Вербицкий О.В. Вступление к криптологии.- Львов.: Издательство науково-техничной литературы.-1998.-300с.
8. Диффи У. Первые десять лет криптографии с открытым ключом //ТИИЭР, т. 76(1988)б Т56 с. 54-74.

Қўшимча

1. Герасименко В.А., Скворцов А.А., Харитонов И.Е. Новые направления применения криптографических методов защиты информации.- М.: Радио и связь.-1989.-360с.
2. Миллер В. Использование эллиптических кривых в криптографии .: -1986.-417-426с.
3. Галатенко В.А. Информационная безопасность. –М.: Финансы и статистика, 1997. –158 с.
4. Грегори С. Смит. Программы шифрования данных // Мир ПК –1997. -№3. -С.58 - 68.
5. Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров. –М.: Наука, 1995. –208 с.
6. Терехов А. Н., Тискин А. В. // Программирование РАН. –1994. -Н 5 -С. 17—22.
7. Криптология – наука о тайнописи // Компьютерное обозрение. –1999. -№3. –С. 10 – 17.
8. Баричев С. В. Криптография без секретов. –М.: Наука, 1998. –120 с.

Интернет маълумотлари

1. [**"Организация и технология защиты информации"**](http://сесуритй.аспу.ру/индекс) сесуритй.аспу.ру/индекс.
2. [**Криптографические алгоритмы | Безопасность**](http://либ.кбсу.ру/елиб/диск/компресс) либ.кбсу.ру/елиб/диск/компресс

МАШҒУЛОТЛАРНИНГ ПЕДАГОГИК ТЕХНОЛОГИЯСИ

МОДУЛНИ ЎҚИТИШДА ФОЙДАЛАНИЛАДИГАН ИНТЕРФАОЛ ТАЪЛИМ МЕТОДЛАРИ

“SWOT-таҳлил” методи

Методнинг мақсади: мавжуд назарий билимлар ва амалий тажрибаларни таҳлил қилиш, таққослаш орқали муаммони ҳал этиш йўллари топишга, билимларни мустаҳкамлаш, такрорлаш, баҳолашга, мустақил, танқидий фикрлашни, ностандарт тафаккурни шакллантиришга хизмат қилади.

S-(strength)	• Kuchli tomonlari
W – (weakness)	• Zaif, kuchsiz tomonlari
O – (opportunity)	• Imkoniyatlari
T – (threat)	• To'siqlar

Намуна: Маълумотларнинг ахборот моделлари, ахборотни структуралаш ва тасвирлаш муаммосининг SWOT таҳлилини ушбу жадвалга туширинг.

С	Маълумотларнинг ахборот моделларидан фойдаланишнинг кучли томонлари	Ушбу Маълумотларнинг ахборот моделлари ахборотни структуралаш масалаларни ечишда мурожаат этилади.
W	Маълумотларнинг ахборот моделларидан фойдаланишнинг кучсиз томонлари	ахборотни структуралаш ва тасвирлашнинг структураси мураккаблиги.
O	Windows OT дан фойдаланишнинг имкониятлари (ички)	Маълумотларнинг ахборот моделлари ахборотни структуралаш ва тасвирлашда хатоликларни бартараф этишда мукамал муҳит ҳисобланади.
T	Тўсиқлар (ташқи)	Маълумотлар хавфсизлигининг тўлақонли таъминланмаганлиги

Хулосалаш» (Резюме, Веер) методи

Методнинг мақсади: Бу метод мураккаб, кўптармоқли, мумкин қадар, муаммоли характеридаги мавзуларни ўрганишга қаратилган. Методнинг моҳияти шундан иборатки, бунда мавзунинг турли тармоқлари бўйича бир хил ахборот берилади ва айна пайтда, уларнинг ҳар бири алоҳида аспектларда муҳокама этилади. Масалан, муаммо ижобий ва салбий томонлари, афзаллик, фазилат ва камчиликлари, фойда ва зарарлари бўйича ўрганилади. Бу интерфаол метод танқидий, таҳлилий, аниқ мантиқий фикрлашни муваффақиятли ривожлантиришга ҳамда ўқувчиларнинг мустақил ғоялари, фикрларини ёзма ва оғзаки шаклда тизимли баён этиш, ҳимоя қилишга имконият яратади. “Хулосалаш” методидан маъруза машғулотларида индивидуал ва жуфтликлардаги иш шаклида, амалий ва семинар машғулотларида кичик гуруҳлардаги иш шаклида мавзу юзасидан билимларни мустаҳкамлаш, таҳлили қилиш ва таққослаш мақсадида фойдаланиш мумкин.

Metodni amalga oshirish tartibi:



trener tinglovchilarni 5-6 kishidan iborat kichik guruhlariga ajratadi;



trening maqsadi, shartlari va tartibi bilan ishtirokchilarni tanishtirgach, har bir guruhga umumiy muammoni tahlil qilinishi zarur bo'lgan qismlari tushirilgan tarqatma materiallarni tarqatadi;



har bir guruh o'ziga berilgan muammoni atroflicha tahlil qilib, o'z mulohazalarini tavsiya etilayotgan sxema bo'yicha tarqatmaga yozma bayon qiladi;



navbatdagi bosqichda barcha guruhlar o'z taqdimotlarini o'tkazadilar. Shundan so'ng, trener tomonidan tahlillar umumlashtiriladi, zaruriy axborotlar bilan to'ldiriladi va mavzu yakunlanadi

Намуна:

Моделлар					
Иерархик		тармоқли		реятсион	
Афзаллиги	камчилиги	Афзаллиги	камчилиги	афзаллиги	камчилиги
Хулоса:					

“Кейс-стади” методи

«Кейс-стади» - инглизча сўз бўлиб, («сасе» – аниқ вазият, ходиса, «стади» – ўрганмоқ, таҳлил қилмоқ) аниқ вазиятларни ўрганиш, таҳлил қилиш асосида ўқитишни амалга оширишга қаратилган метод ҳисобланади. Мазкур метод дастлаб 1921 йил Гарвард университетида амалий вазиятлардан иқтисодий бошқарув фанларини ўрганишда фойдаланиш тартибида қўлланилган. Кейсда очик ахборотлардан ёки аниқ воқеа-ходисадан вазият сифатида таҳлил учун фойдаланиш мумкин. Кейс ҳаракатлари ўз ичига қуйидагиларни қамраб олади: Ким (Who), Қачон (When), Қаерда (Where), Нима учун (Why), Қандай/ Қанақа (How), Нима-натижа (What).

“Кейс методи” ни амалга ошириш босқичлари

Иш босқичлари	Фаолият шакли ва мазмуни
1-босқич: Кейс ва унинг ахборот таъминоти билан таништириш	✓ якка тартибдаги аудио-визуал иш; ✓ кейс билан танишиш(матнли, аудио ёки медиа шаклда); ✓ ахборотни умумлаштириш; ✓ ахборот таҳлили; ✓ муаммоларни аниқлаш
2-босқич: Кейсни аниқлаштириш ва ўқув топшириғни белгилаш	✓ индивидуал ва гуруҳда ишлаш; ✓ муаммоларни долзарблик иерархиясини аниқлаш; ✓ асосий муаммоли вазиятни белгилаш
3-босқич: Кейсдаги асосий муаммони таҳлил этиш орқали ўқув топшириғининг ечимини излаш, ҳал этиш йўллари ишлаб чиқиш	✓ индивидуал ва гуруҳда ишлаш; ✓ муқобил ечим йўллари ишлаб чиқиш; ✓ ҳар бир ечимнинг имкониятлари ва тўсиқларни таҳлил қилиш; ✓ муқобил ечимларни танлаш
4-босқич: Кейс ечимини ечимини шакллантириш ва асослаш, тақдимот.	✓ якка ва гуруҳда ишлаш; ✓ муқобил вариантларни амалда қўллаш имкониятларини асослаш; ✓ ижодий-лойиха тақдимотини тайёрлаш; ✓ якуний хулоса ва вазият ечимининг амалий аспектларини ёритиш

Кейс. Берилган топшириқ асосида дастур алгоритми тузилиб C++ дастурлаш тилида дастур матни ёзилди. Дастурни асм.туит.уз сайтига юборилганда “компилятсияда ҳатолик” хабари чиқди. Яъни Система ечимни қабул қилмади.

Keysni bajarish bosqichlari va topshiriqlar:

- Keysdgi muammoni keltirib chiqargan asosiy sabablarni belgilang (individual va kichik guruhda).
- Xatolikni bartaraf etuvchi ishlar ketma-ketligini belgilang (juftliklardagi ish).

«ФСМУ» методи

Технологиянинг мақсади: Мазкур технология иштирокчилардаги умумий фикрлардан хусусий хулосалар чиқариш, таққослаш, қиёслаш орқали ахборотни ўзлаштириш, хулосалаш, шунингдек, мустақил ижодий фикрлаш кўникмаларини шакллантиришга хизмат қилади. Мазкур технологиядан маъруза машғулотларида, мустаҳкамлашда, ўтилган мавзунини сўрашда, уйга вазифа беришда ҳамда амалий машғулот натижаларини таҳлил этишда фойдаланиш тавсия этилади.

Технологияни амалга ошириш тартиби:

- қатнашчиларга мавзуга оид бўлган якуний хулоса ёки ғоя таклиф этилади;
- ҳар бир иштирокчига ФСМУ технологиясининг босқичлари ёзилган қоғозларни тарқатилади:

F	• Fikringizni bayon eting
S	• Fikringizni bayoniga sabab ko'rsating
M	• Ko'rsatgan sababingizni isbotlab misol keltiring
U	• Fikringizni umumlashtiring

- иштирокчиларнинг муносабатлари индивидуал ёки гуруҳий тартибда тақдимот қилинади.

ФСМУ таҳлили қатнашчиларда касбий-назарий билимларни амалий машқлар ва мавжуд тажрибалар асосида тезроқ ва муваффақиятли ўзлаштирилишига асос бўлади.

Намуна.

Фикр: Дастурий таъминот компютернинг асосий таркибий қисми ва асосий тамойилларидан биридир”.

Топширик: Мазкур фикрга нисбатан муносабатингизни ФСМУ орқали таҳлил қилинг.

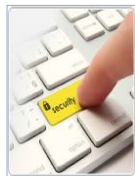
“Ассесмент” методи

Методнинг мақсади: мазкур метод таълим олувчиларнинг билим даражасини баҳолаш, назорат қилиш, ўзлаштириш кўрсаткичи ва амалий кўникмаларини текширишга йўналтирилган. Мазкур техника орқали таълим олувчиларнинг билиш фаолияти турли йўналишлар (тест, амалий кўникмалар, муаммоли вазиятлар машқи, қиёсий таҳлил, симптомларни аниқлаш) бўйича ташхис қилинади ва баҳоланади.

Методни амалга ошириш тартиби:

“Ассесмент” лардан маъруза машғулотларида талабаларнинг ёки катнашчиларнинг мавжуд билим даражасини ўрганишда, янги маълумотларни баён қилишда, семинар, амалий машғулотларда эса мавзу ёки маълумотларни ўзлаштириш даражасини баҳолаш, шунингдек, ўз-ўзини баҳолаш мақсадида индивидуал шаклда фойдаланиш тавсия этилади. Шунингдек, ўқитувчининг ижодий ёндашуви ҳамда ўқув мақсадларидан келиб чиқиб, ассесментга қўшимча топшириқларни киритиш мумкин.

Намуна. Ҳар бир катакдаги тўғри жавоб 5 балл ёки 1-5 балгача баҳоланиши мумкин.



Test

- **1.10⁻⁸ aniqlikda natijani chop etish qanday bajariladi?**
- A. `printf("%.8f",x)`
- B. `cout<<x`
- C. `cout<<("%.8f",x)`



Qiyosiy tahlil

- **Dasturiy ta'minot mahsulotlardan foydalanish ko'rsatkichlarini tahlil qiling?**



Tushuncha tahlili

- **STD qisqartmasini izohlang.**



Amaliy ko'nikma

- **Ma'lumotlarning axborot modellarini aniqlash va unga misollar keltiring.**

“Инсерт” методи

Методнинг мақсади: Мазкур метод ўқувчиларда янги ахборотлар тизимини қабул қилиш ва билмларни ўзлаштирилишини енгиллаштириш мақсадида қўлланилади, шунингдек, бу метод ўқувчилар учун хотира машқи вазифасини ҳам ўтайди.

Методни амалга ошириш тартиби:

- ўқитувчи машғулотга қадар мавзунинг асосий тушунчалари мазмуни ёритилган инпут-матнни тарқатма ёки тақдимот кўринишида тайёрлайди;

- янги мавзу моҳиятини ёритувчи матн таълим олувчиларга тарқатилади ёки тақдирот кўринишида намоиш этилади;
- таълим олувчилар индивидуал тарзда матн билан танишиб чиқиб, ўз шахсий қарашларини махсус белгилар орқали ифодалядилар. Матн билан ишлашда талабалар ёки қатнашчиларга қуйидаги махсус белгилардан фойдаланиш тавсия этилади:

Белгилар	1-матн	2-матн	3-матн
“В” – таниш маълумот.			
“?” – мазкур маълумотни тушунмадим, изоҳ керак.			
“+” бу маълумот мен учун янгилик.			
“– ” бу фикр ёки мазкур маълумотга қаршиман?			

Белгиланган вақт якунлангач, таълим олувчилар учун нотаниш ва тушунарсиз бўлган маълумотлар ўқитувчи томонидан таҳлил қилиниб, изоҳланади, уларнинг моҳияти тўлиқ ёритилади. Саволларга жавоб берилади ва машғулот якунланади.

“Тушунчалар таҳлили” методи

Методнинг мақсади: мазкур метод талабалар ёки қатнашчиларни мавзу бўйича таянч тушунчаларни ўзлаштириш даражасини аниқлаш, ўз билимларини мустақил равишда текшириш, баҳолаш, шунингдек, янги мавзу бўйича дастлабки билимлар даражасини ташхис қилиш мақсадида қўлланилади.

Методни амалга ошириш тартиби:

- иштирокчилар машғулот қоидалари билан таништирилади;
- ўқувчиларга мавзуга ёки бобга тегишли бўлган сўзлар, тушунчалар номи туширилган тарқатмалар берилади (индивидуал ёки гуруҳли тартибда);
- ўқувчилар мазкур тушунчалар қандай маъно англатиши, қачон, қандай ҳолатларда қўлланилиши ҳақида ёзма маълумот берадилар;
- белгиланган вақт якунига етгач ўқитувчи берилган тушунчаларнинг тугри ва тўлиқ изоҳини ўқиб эшиттиради ёки слайд орқали намоиш этади;
- ҳар бир иштирокчи берилган тугри жавоблар билан ўзининг шахсий муносабатини таққослайди, фарқларини аниқлайди ва ўз билим даражасини текшириб, баҳолайди.

Намуна: “Модулдаги таянч тушунчалар таҳлили”

Тушунчалар	Сизнингча бу тушунча қандай маънони англатади?	Қўшимча маълумот
Файл	Макро дериктиваларни белгилаш	а дирестиве тхат дефинес а масро.
каталог	Бир соурсе файл ичида бошқа бир файлаг мурожатни амалга ошириш механизми	а мечанизм фор техтуал инслусион оф оне <u>соурсе</u> <u>филе</u> инто анотхер.
тизим	адд-анд-ассигн оператори; масалан $a+=b$ вазифази жиҳатдан $a=a+b$ билан бир хил	адд-анд-ассигн <u>оператор</u> ; $a+=b$ ис роугхлй эквивалент то $a=a+b$.
опен	Дастур жодини ўзида жамловчи файл	<u>филе</u> сонтаининг <u>деф</u> <u>инитионс</u> .
сопй	Дастур жодини ўзида жамловчи файл	<u>филе</u> сонтаининг <u>деф</u> <u>инитионс</u> .
делете	Сарлавха файли	<u>хеадер филе</u>
адресс	Ҳотира манзили	а <u>меморй</u> лосатион

Изоҳ: Иккинчи устунчага қатнашчилар томонидан фикр билдирилади. Мазкур тушунчалар ҳақида қўшимча маълумот глоссарийда келтирилган.

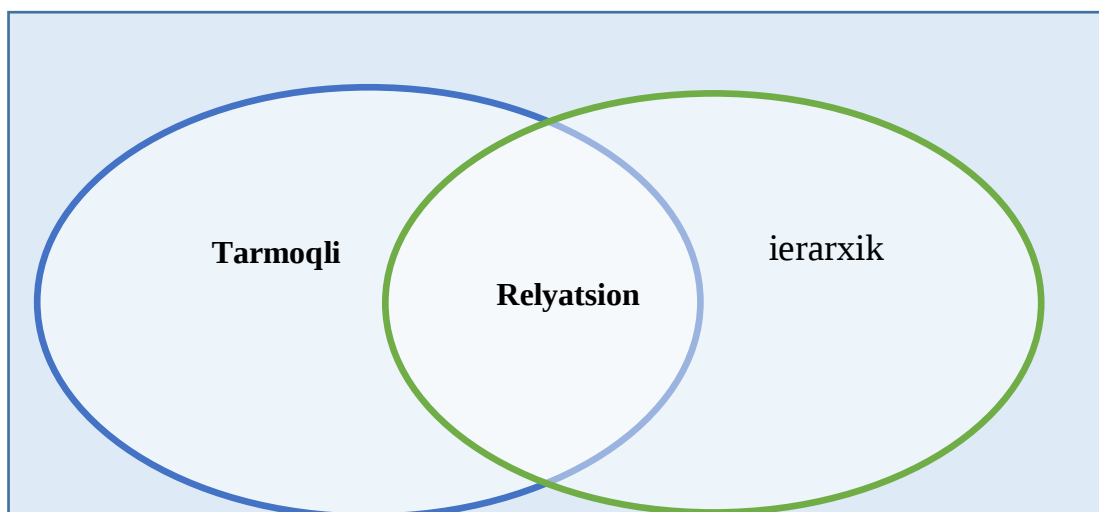
Венн Диаграммаси методи

Методнинг мақсади: Бу метод график тасвир орқали ўқитишни ташкил этиш шакли бўлиб, у иккита ўзаро кесишган айлана тасвири орқали ифодаланади. Мазкур метод турли тушунчалар, асослар, тасавурларнинг анализ ва синтезини икки аспект орқали кўриб чиқиш, уларнинг умумий ва фарқловчи жиҳатларини аниқлаш, таққослаш имконини беради.

Методни амалга ошириш тартиби:

- иштирокчилар икки кишидан иборат жуфтликларга бирлаштириладилар ва уларга кўриб чиқиладиган тушунча ёки асоснинг ўзига хос, фарқли жиҳатларини (ёки акси) доиралар ичига ёзиб чиқиш таклиф этилади;
- навбатдаги босқичда иштирокчилар тўрт кишидан иборат кичик гуруҳларга бирлаштирилади ва ҳар бир жуфтлик ўз таҳлили билан гуруҳ аъзоларини таништирадилар;
- жуфтликларнинг таҳлили эшитилгач, улар биргалашиб, кўриб чиқиладиган муаммо ёхуд тушунчаларнинг умумий жиҳатларини (ёки фарқли) излаб топадилар, умумлаштирадилар ва доирачаларнинг кесишган қисмига ёзадилар.

Намуна: Ахборотни моделлари бўйича



“Блис-ўйин” методи

Методнинг мақсади: ўқувчиларда тезлик, ахборотлар тизмини таҳлил қилиш, режалаштириш, прогнозлаш кўникмаларини шакллантиришдан иборат. Мазкур методни баҳолаш ва мустаҳкамлаш мақсадида қўллаш самарали натижаларни беради.

Методни амалга ошириш босқичлари:

1. Дастлаб иштирокчиларга белгиланган мавзу юзасидан тайёрланган топшириқ, яъни тарқатма материалларни алоҳида-алоҳида берилади ва улардан материални синчиклаб ўрганиш талаб этилади. Шундан сўнг, иштирокчиларга тўғри жавоблар тарқатмадаги «якка баҳо» колонкасига белгилаш кераклиги тушунтирилади. Бу босқичда вазифа якка тартибда бажарилади.

2. Навбатдаги босқичда тренер-ўқитувчи иштирокчиларга уч кишидан иборат кичик гуруҳларга бирлаштиради ва гуруҳ аъзоларини ўз фикрлари билан гуруҳдошларини таништириб, баҳслашиб, бир-бирига таъсир ўтказиб, ўз фикрларига ишонтириш, келишган ҳолда бир тўхтамга келиб, жавобларини «гуруҳ баҳоси» бўлимига рақамлар билан белгилаб чиқишни топширади. Бу вазифа учун 15 дақиқа вақт берилади.

3. Барча кичик гуруҳлар ўз ишларини тугатгач, тўғри ҳаракатлар кетма-кетлиги тренер-ўқитувчи томонидан ўқиб эшиттирилади, ва ўқувчилардан бу жавобларни «тўғри жавоб» бўлимига ёзиш сўралади.

4. «Тўғри жавоб» бўлимида берилган рақамлардан «якка баҳо» бўлимида берилган рақамлар таққосланиб, фарқ булса «0», мос келса «1» балл қуйиш сўралади. Шундан сўнг «якка хато» бўлимидаги фарқлар юқоридан пастга қараб қўшиб чиқилиб, умумий йиғинди ҳисобланади.

5. Худди шу тартибда «тўғри жавоб» ва «гуруҳ баҳоси» ўртасидаги фарқ чиқарилади ва баллар «гуруҳ хатоси» бўлимига ёзиб, юқоридан пастга қараб қўшилади ва умумий йиғинди келтириб чиқарилади.

6. Тренер-ўқитувчи якка ва гуруҳ хатоларини тўпланган умумий йиғинди бўйича алоҳида-алоҳида шарҳлаб беради.

7. Иштирокчиларга олган баҳоларига қараб, уларнинг мавзу бўйича ўзлаштириш даражалари аниқланади.

(80 МИНУТЛИК ДАРСНИ ТАШКИЛ ҚИЛИШ ТАҚСИМОТИ)

ДАРС ТУРИ : МАЪРУЗА; КУРС : 2

ДАРСНИНГ ХРОНО ХАРИТАСИ – 80 МИНУТ

1. ТАШКИЛИЙ ҚИСМ: ХОНАНИНГ ТОЗАЛИГИ, ЖИҲОЗЛАНИШИ, САНИТАРИЯ ҲОЛАТИ

(2 МИНУТ).

2. ТАЛАБАЛАР БИЛИМИНИ БАҲОЛАШ: ЎТИЛГАН МАВЗУНИ ҚИСҚАЧА ТАКРОРЛАШ ТАЛАБАЛАР

БИЛАН САВОЛ - ЖАВОБ ЎТКАЗИШ (10 МИНУТ).

3. ЯНГИ МАВЗУНИНГ БАЁНИ: МАВЗУНИ ЖОНЛИ - МУЛОҚАТЛИ ТУШИНТИРИШ (55 МИНУТ).

4. МАВЗУНИ ЎЗЛАШТИРИШ ДАРАЖАСИНИ АНИҚЛАШ: ШУ МАВЗУ БЎЙИЧА ҚИСҚА САВОЛ-

ЖАВОБ ЎТКАЗИШ (8 МИНУТ).

5. УЙГА БЕРИЛАДИГАН ТОПШИРИҚЛАР ВА АДАБИЁТЛАР МУҲОКАМАСИ: ТОПШИРИҚЛАР, АДАБИЁТЛАР ВА ИНТЕРНЕТ – РЕСРУСЛАРИНИ ТАҲЛИЛ ҚИЛИШ (5 МИНУТ).

ФАН БЎЙИЧА КАЛЕНДАР РЕЖА

САМАРҚАНД ДАВЛАТ УНИВЕРСИТЕТИ

2017/2019 ўқув йили 2-семестрида 5110700 – Информатика ўқитиш методикаси бакалавриат йўналишлари талабаларига «Ахборотлаштириш технологиялари» кафедраси ўқитувчилари томонидан ўтиладиган «Ахборотларни ҳимоялаш» фани ишчи дастурининг машғулотлар тури бўйича бажарилишининг

КАЛЕНДАР РЕЖАСИ

Маърузачи доцент И.Н. Туракулов
Амалий машғулотлар И.Қ.Химматов

Т. р.	Маш-ғулот тури	Мавзу номи	Ажра-тилган соати	Бажарилган -лиги		Ўқитувчи имзоси
				Сана	Соат-лар сони	
1	2	3	4	5	6	7
1	Маъ-Руза	Замонавий ахборотлашган жаимят. Асосий тушунчалар ва тарифлар. Ахборотларни ҳимоялашнинг асосий хавфлари	2			
1	Маъ-Руза	Вируслар ва антивируслар.	2			
1	Маъ-Руза	Ахборотларни стенографик ҳимоялаш усуллари	2			
1	Маъ-Руза	Ахборотларни криптографик ҳимоялаш усуллари.	2			
1	Маъ-Руза	Симметрияли криптиотизим асослари	2			
1	Маъ-Руза	Асимметрик криптиотизим асослари.	2			
1	Маъ-Руза	Электрон рақамли имзо	2			
1	Амалий	Антивирус Касперский 6.0. дастурини ўрнатиш ва созлаш, базани янгилаш	2			
1	Амалий	Классик симметрик криптиотизимлар	2			
1	Амалий	Ўрин алмаштириш усули	2			
1	Амалий	Шифрлаш жадваллари	2			
1	Амалий	Сехрли квадратларни қўллаш. Трисемус шифрлаш жадвали.	2			
1	Амалий	Плейфейр биграмма шифри. Хилл криптиотизими.	2			
1	Амалий	Вижинер жадвали	2			

1	Амаллий	Очиқ калитли криптотизимлар	2			
1	Амаллий	Електрон рақамли имзо алгоритими	2			
		Жами	32			

Факультет декани

проф. А.Р. Ахатов

Кафедра мудири

проф. И.И.Жуманов

МАЪРУЗАЛАР МАТНИ

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

Самарқанд давлат университети

«Ахборотлаштириш технологиялари» кафедраси

И.Қ.Химматов

«АХБОРОТЛАРНИ ҲИМОЯЛАШ»

фанидан

МАЪРУЗАЛАР МАТНИ

САМАРҚАНД – 2019 йил

Ушбу маърузалар матни факултет услубий кенгашида куриб чиқилган ва
фойдаланишга тавсия этилган «___»_____2019_й.

Тузувчи: Самарқанд давлат университети «Ахборотлаштириш
технологиялар» кафедраси ассистенти
т.ф.н., асс. И.Қ. Химматов

Ушбу маърузалар матни «Ахборотлаштириш технологиялари»
кафедраси йиғилишида куриб чиқилган ва фойдаланишга тавсия этилган
«___»_____2019 й.
Баённома №_____

Кафедра мудири:

проф. И.И.Жуманов

СЎЗ БОШИ

Тез ривожланиб бораётган компьютер ахборот технологиялари бизнинг кундалик ҳаётимизнинг барча жабхаларида сезиларли узгаришларни олиб кирмокда. Хозирда “ахборот тушунчаси” сотиб олиш, сотиш, бирор бошка товарга алмаштириш мумкин булган махсус товар белгиси сифатида тез-тез ишлатилмокда. Шу билан бирга ахборотнинг бахоси куп холларда унинг узи жойлашган компьютер тизимининг бахосида бир неча юз ва минг баробарга ошиб кетмокда. Шунинг учун тамомила табиий холда ахборотни унга рухсат этилмаган холда киришдан, касддан ўзгартиришдан, уни ўғирлашдан, йўқотишдан ва бошка жиноий характерлардан ҳимоя қилишга кучли зарурат тугилади.

Компьютер тизимлари ва тармокларида ахборотни ҳимоя остига олиш деганда, берилаётган, сакланаётган ва қайта ишланилаётган ахборотни ишончилигини тизимли тарзда таъминлаш мақсадида турли восита ва усулларни куллаш, чораларни куриш ва тадбирларни амалга оширишни тушуниш қабул қилинган.

Ахборотни ҳимоя қилиш деганда:

- Ахборотнинг жисмоний бутунлигини таъминлаш, шу билан бирга ахборот элементларининг бузилиши, ёки йук қилинишига йул қуймаслик;
- Ахборотнинг бутунлигини саклаб қолган холда, уни элементларини қалбақлаштиришга (узгартиришга) йул қуймаслик;
- Ахборотни тегишли ҳукукуларга эга булмаган шахслар ёки жараёнлар орқали тармокдан рухсат этилмаган холда олишга йул қуймаслик;
- Эгаси томонидан берилаётган (сотилаётган) ахборот ва ресурслар фақат томонлар уртасида қилишилган шартномалар асосида кулланилишига ишониш қабила тушунилади.

Юқорида таъкидлаб утилганларнинг барчаси асосида компьютер тармоклари ва тизимларида ахборот хавфсизлиги муаммосининг долзарблиги ва муҳимлиги қелиб чиқади. Шунинг учун ҳозирги курс Республикаимизнинг олий ва урта махсус уқув муассасалари уқув режаларида муносиб урин эгаллайди.

Ушбу курснинг вазифалари:

- Талабаларда компьютер тармоклари ва тизимларида ахборот хавфсизлиги тугрисидаги билимларни шакллантириш;
- Ахборотни ҳимоя қилишнинг назарий, амалий ва услубий асосларини бериш;
- Талабаларга компьютер тармоклари ва тизимларида ахборот хавфсизлигини таъминлашнинг замонавий усуллари ва воситаларини куллашни амалий жихатдан ургатиш;
- Талабаларни ахборотни ҳимоя қилиш бўйича ишлаб чиқарилган турли хил дастурий махсулотлардан эркин фойдалана олиш имконини берадиган билимлар билан таъминлаш;

Курсни узлаштириш натижасида талаба қуйидагиларни билиши шарт;

- компьютер тармоклари ва тизимларидаги ахборот хавфсизлигига таҳдид солиши кутилаётган хавф хатарнинг моҳиятини ва оқибатларини тушуниши;
- компьютер тармоклари ва тизимларида ахборотни ҳимоя қилиш бўйича қўйиладиган асосий талаблар ва асосларни ушлаштириш;
- компьютер тармоклари ва тизимларида ахборот хавфсизлигини таъминлашда қўлланиладиган замонавий усуллар ва воситаларни билиш;
- тизимларда ахборот бутунлиги ва ишқўчлигини бузувчи вируслар ва бошқа манбалар мавжудлигини тизимли текширишни таъминлаш ва уларни зарарсизлаштириш бўйича чораларни қўриш;
- ахборотни ҳимоя қилишда қўлланиладиган замонавий амалий тизимлар ва дастурий маҳсулотларни ишлата олиш.

**1-МАВЗУ: Замонавий ахборотлашган жаймиёт. Асосий
тушунчалар ва тарифлар. Ахборотларни химоялашнинг асосий
хавфлари**

1. Ахборотларни химоялаш фанига кириш;
2. Ахборотларга нисбатан хавф-хатарлар таснифи.
3. Химоялаш тизимининг комплекслилиги. Ахборотларни ташкилий химоялаш
элементлар.
4. Ахборот тизимларида маълумотларга нисбатан хавф-хатарлар

Ахборотларни химоялаш фанига кириш

Тез ривожланиб бораётган компьютер ахборот технологиялари бизнинг кундалик ҳаётимизнинг барча жабхаларида сезиларли узгаришларни олиб кирмокда. Хозирда “ахборот тушунчаси” сотиб олиш, сотиш, бирор бошқа товарга алмаштириш мумкин булган махсус товар белгиси сифатида тез-тез ишлатилмокда. Шу билан бирга ахборотнинг баҳоси куп холларда унинг узи жойлашган компьютер тизимининг баҳосида бир неча юз ва минг баробарга ошиб кетмокда. Шунинг учун тамомила табиий холда ахборотни унга рухсат этилмаган холда киришдан, касддан узгартиришдан, уни уФирлашдан, йукотитдан ва бошқа жиноий характерлардан химоя қилишга. кучли зарурат туФилади. Аммо, жамиятнинг автоматлаштиришнинг юкори даражасига интилиши уни фойдаланиладиган ахборот технологияларнинг хавфсизлиги савиясига боФлик қилиб қуяди. Хдкикатан, компьютер тизимларининг кенг куламда ишлатилиши доимо ушиб боровчи ахборот хажмини ишлатиш жараёнларини автоматлаштиришга имкон берсада, бу жараёнларни агрессив таъсирларга нисбатан ожиз қилиб қуяди ва, демак, ахборот технологиялардан фойдаланувчилар олдида янги муаммо-ахборот хавфсизлик муаммоси кундаланг булди. Хавфсизлик муаммоси, аслида, янги муаммо эмас, чунки хавфсизлигини таъминлаш ҳар кандай тизим учун, унинг мураккаблиги, табиатидан катъий назар, бирламчи вазифа ҳисобланади. Аммо, химояланувчи объект ахборот тизими булса, ёки агрессив таъсир воситалари ахборот шаклда булганда, химоянинг мутлок янги технологияларини ва усулларини яратишга туФри келади. Маълумотларни химояловчи усуллар ҳамда ҳакерларга қарши ҳаракат воситалар мажмуасини белгилаш мақсадида компьютер хавфсизлиги атамаси ишлатила бошланди.

Маълумотларни ишловчи таксимланган тизимларнинг пайдо булиши хавфсизлик масаласига янгича ёндашишнинг шаклланишига олиб келди. Маълумки, бундай тизимларда тармоқлар ва коммуникацион ускуналар фойдаланувчиларнинг терминаллари билан марказий компьютерлар уртасида маълумотлар алмашишга хизмат килади. Шу сабабли маълумотлар узатилувчи тармоқларни химоялаш зарурияти туФилди ва шунинг билан бирга тармоқ хавфсизлиги атамаси пайдо булди.

Ахборотнинг муҳимлик даражаси кадим замонлардан маълум. Шунинг учун ҳам кадимда ахборотни химоялаш учун турли хил усуллар кулланилган. Улардан бири - сирли ёзувдир. Ундаги хабарни хабар юборилган манзил эгасидан бошқа шахс уқий олмаган. Асрлар давомида бу санъат - сирли ёзув жамиятнинг юкори табақалари, давлатнинг элчихона резиденқиялари ва разведка миссияларидан ташқарига чикмаган. Факат бир неча ун йил олдин ҳамма нарса тубдан узгарди, яъни ахборот уз қийматиға эға булди ва кенг тарқаладиган махсулотға айланди. Уни эндиликда ишлаб чиқарадилар, саклайдилар, узатишади, сотадилар ва сотиб оладилар. Булардан ташқари уни уФирлайдилар, бузиб талқин этадилар ва сохталаштирадилар. Шундай қилиб, ахборотни химоялаш зарурияти туФилади.

Ахборотни химоя қилиш деганда:

- Ахборотнинг жисмоний бутунлигини таъминлаш, шу билан бирга ахборот элементларининг бузилиши, ёки йуқ қилинишиға йул қуймаслик;

- Ахборотнинг бутунлигини сақлаб қолган уолда, уни элементларини калбакилаштиришга (узгартиришга) йул қуймаслик;
- Ахборотни тегишли ҳуқуқуларга эга бўлмаган шахслар ёки жараёнлар орқали тармоқдан рухсат этилмаган ҳолда олишга йул қуймаслик;
- Эгаси томонидан берилаётган (сотилаётган) ахборот ва ресурслар фақат томонлар уртасида келишилган шартномалар асосида қулланилишига ишониш кабилар тушунилади.

Юқорида таъкидлаб утилганларнинг барчаси асосида компьютер тармоқлари ва тизимларида ахборот хавфсизлиги муаммосининг долзарблиги ва мууимлиги келиб чиқади. Компьютер тизимлари ва тармоқларида ахборотни уимоя остига олиш деганда, берилаётган, сақланаётган ва қайта ишланилаётган ахборотни ишончлилигини тизимли тарзда таъминлаш мақсадида турли восита ва усулларни қуллаш, чораларни куриш ва тадбирларни амалга оширишни тушуниш қабул қилинган.

Ушбу курснинг вазифалари:

- Талабаларда компьютер тармоқлари ва тизимларида ахборот хавфсизлиги туфрисидаги билимларни шакллантириш;
- Ахборотни химоя қилишнинг назарий, амалий ва услубий асосларини бериш;
- Талабаларга компьютер тармоқлари ва тизимларида ахборот хавфсизлигини таъминлашнинг замонавий усуллари ва воситаларини қуллашни амалий жихатдан ургатиш;
- Талабаларни ахборотни химоя қилиш бўйича ишлаб чиқарилган турли хил дастурий махсулотлардан эркин фойдалана олиш имконини берадиган билимлар билан таъминлаш;

Бирлашган тармоқларда ишлаш хавфсизлигининг мураккаблигига қуйидаги мисоллар орқали ишонч уосил қилиш мумкин.

- Ахборотни узатишда хавфсизликни таъминлашга қуйиладиган талабларни бевосита қуйидаги атамалардан аниқлаш мумкин: конфиденциалик, аутентификация, яхлитликни сақлаш, ёлгоннинг мумкин эмаслиги, фойдаланувчанлик, фойдаланувчанликни бошқариш.
- Куп уолларда яратувчи эътиборидан четда қолган уимоя тизимининг камчиликларини аниқлаш мақсадида муаммога қарши томоннинг нуқтаи назаридан қараш лозим. Бошқача айтганда, уимоянинг у ёки бу механизми ёки алгоритмини яратишда мумкин бўлган қарши чораларни уам куриш лозим.
- Химоя воситаларидан барча қарши чоралар мажмуасини уисобга олган уолда фойдаланиш лозим.
- Хавфсизликни таъминлаш чоралари тизими яратилганидан сунг бу чораларни қачон ва қаерда қуллаш масаласини ечиш лозим. Бу физикавий жой (маълум уимоя воситасини қуллаш учун тармоқ нуқтасини танлаш) ёки хавфсизликни таъминловчи мантиқий занжирдаги жой (масалан, ахборот узатувчи протокол сатхи ёки сатхларини танлаш) бўлиши мумкин.

Химоя воситалари, одатда, маълум алгоритм ва протоколдан фарқланади. Уларга биноан барча уимоядан манфаатдор ахборотининг қандайдир қисми махфий бўлиб қолиши шарт (масалан, шифр калити куринишида). Бу эса уз навбатида бундай махфий ахборотни яратиш, тақсимлаш ва уимоялаш усулларини ишлаб чиқиш заруриятини тугдиради.

Махфий ва қимматбауо ахборотларга рухсатсиз киришдан уимоялаш энг мухим вазифалардан бири саналади. Компьютер эгалари ва фойдаланувчиларнинг мулки ууқуқларини уимоялаш - бу ишлаб чиқарилаётган ахборотларни жиддий иқтисодий ва бошуа моддий уамда номоддий зарарлар келтириши мумкин бўлган турли киришлар ва угирлашлардан уимоялашдир. Хозирги кунда хавфсизлиكنинг бир қанча йуналишларини қайд этиш мумкин. (1-расм)

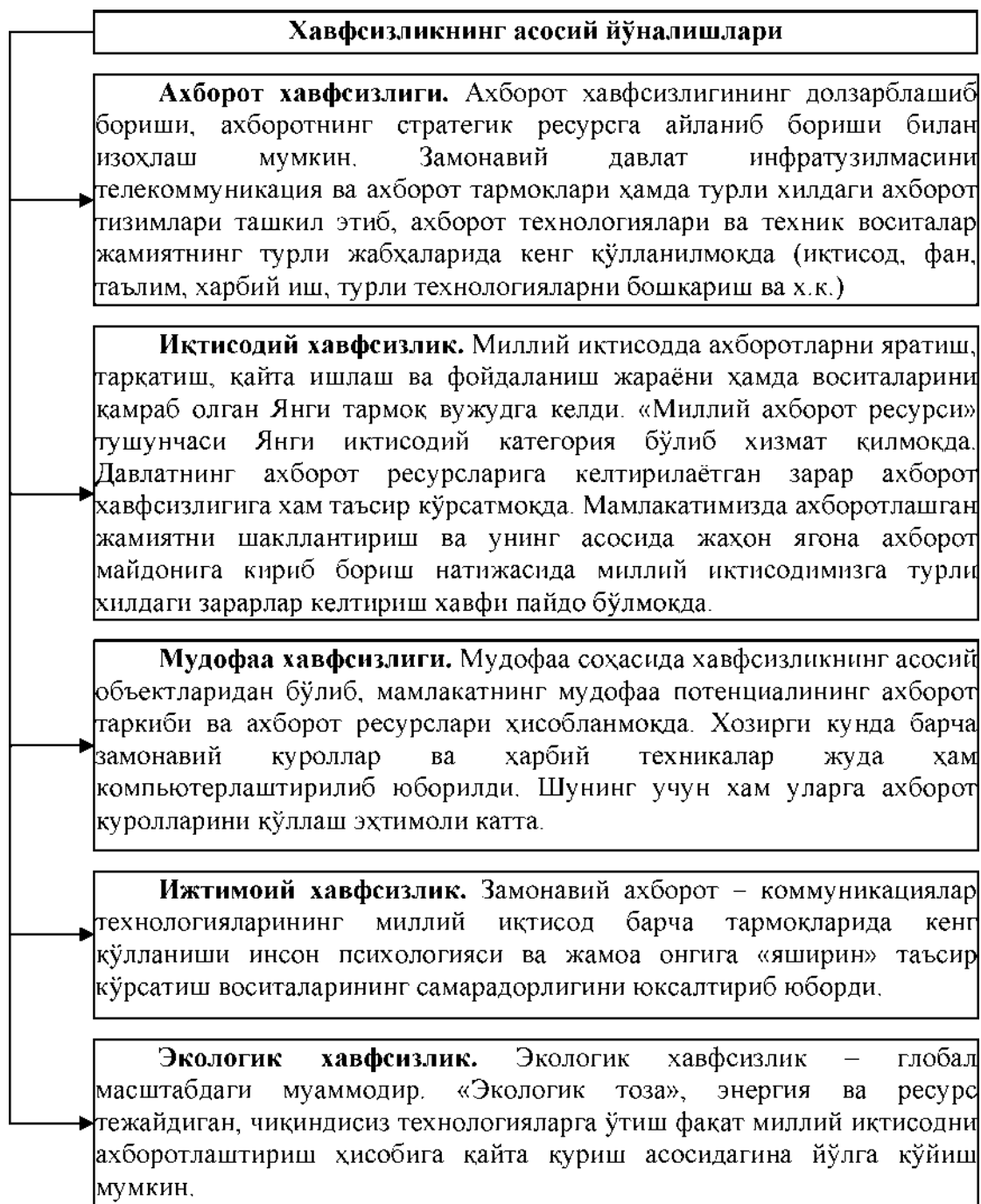
Ахборот хавфсизлиги деб, маълумотларни йуқотиш ва узгартиришга

йуналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан ҳар қандай ташувчиларда ахборотнинг уимояланганлигига айтилади. Илгариги хавф фақатгина конфиденциал (махфий) хабарлар ва ҳужжатларни угирлаш ёки нусха олишдан иборат булса, уозирги пайтдаги хавф эса компьютер маълумотлари туплами, электрон маълумотлар, электрон массивлардан уларнинг эгасидан рухсат сурамасдан фойдаланишдир. *Булардан ташқари, бу ҳаракатлардан моддий фойда олишга интилиш ҳам ривожланди.*

Ахборотнинг ҳқмояси деб, бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлиги, ишончилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатъий регламентланган динамик технологик жараёнга айтилади.

Ахборотни уимоялашнинг мақсадлари қуйидагилардан иборат:

- ахборотнинг келишувсиз чиқиб кетиши, угирланиши, йуқотилиши, узгартирилиши, сохталаштирилишларнинг олдини олиш;
- шахс, жамият, давлат хавфсизлигига булган хавф - хатарнинг олдини олиш;
- ахборотни йуқ қилиш, узгартириш, сохталаштириш, нусха кучириш, тусиқлаш буйичарухсат этилмаган ҳаракатларнинг олдини олиш;
- ҳужжатлаштирилган ахборотнинг миқдори сифатида ҳуқуқий тартибини таъминловчи, ахборот захираси ва ахборот тизимиға ҳар қандай ноқонуний аралашувларнинг қуринишларининг олдини олиш;
- ахборот тизимида мавжуд булган шахсий маълумотларнинг шахсий махфийлигини ва конфиденциаллигини сақловчи фуқароларнинг конституцион ҳуқуқларини уимоялаш;
- давлат сирини, қонунчиликка мос ҳужжатлаштирилган ахборотнинг конфиденциаллигини сақлаш;
- ахборот тизимлари, технологиялари ва уларни таъминловчи воситаларни яратиш, ишлаб чиқиш ва қуллашда субъектларнинг ҳуқуқларини таъминлаш.



Ахборотларга нисбатан хавф-хатарлар таснифи

Хавфсизлик сиёсатининг энг асосий вазифаларидан бири уимоя тизимида потенциал хавфли жойларни кидириб топиш ва уларни бартараф этиш ҳисобланади. Текширишлар шуни курсатадики, тармоқдаги энг катта хавфлар — бу рухсатсиз киришга мулжалланган махсус дастурлар, компьютер вируслари ва дастурнинг ичига жойлаштирилган махсус кодлар булиб, улар компьютер тармоқларининг барча объектлари учун катта хавф тугдиради.

Ташкилотнинг ҳимоялаш тизимига булган уақиқий зутиёжини аниқлаш ва хавфсизликнинг мавжуд барча хилма-хил чораларидан кераклигини танлашда турли ёндашишлардан фойдаланилади. Бундай ёндашишлардан бири ахборот уимоясининг куйидаги учта жиҳатига асосланган.

1. Химоянинг бузилишлари. Корхонага тегишли ахборотни сақлаш ва ишлатиш хавфсизлигига зарар келтирувчи уар қандай ҳаракатлар.
2. Химоя механизми. Химоянинг бузилишларини аниқлаш ва бартараф этиш,

уамда бузилишлар оқибатини йўқотиш механизмлари.

3. Химоя хизмати. Маълумотларни ишлаш тизимлари ва корхонага тегишли ахборотни ташиш хавфсизлиги савиясини кутаришга мулжалланган сервис хизмати.

Химоянинг бузилиши. Компьютер тизими ёки тармоги уимоясини бузишга уринишларни компьютер тизимини ахборотни таъминловчи объект сифатида куриш орқали классификациялаш мумкин. Умумий уолда қандайдир манбадан(масалан, файл ёки хотира қисми) ахборот оқимининг адресатга (масалан, бошқа файл ёки бевосита фойдаланувчи) узатилиши кузатилади. Шу нуқтаи назардан қуйидаги хужумларни фарқлаш мумкин:

- Узиш (разъединение);
- Ушлаб қолиш (перехват);
- Турлаш (модификация);
- Сохталаштириш (фальсификация).

Узиш (разъединение). Тизим ресурси йўқ қилинади, ахборотдан фойдаланувчанлик бузилади. Бундай бузилишларга мисол тариқасида ускунанинг ишдан чиқиши, алоқа линиясининг узилиши ёки файлларни бшқарувчи тизимнинг бузилишини курсатиш мумкин.

Ушлаб қолиш (перехват). Ресурсдан рухсат берилмаган фойдаланишга йул очилади. Натижада ахборотнинг махфийлиги (конфиденциаллиги) бузилади. Бундай фойдаланувчилар физик шахс, программа ёки компьютер булиши мумкин. Бундай бузилишларга мисол тариқасида маълумотларни ушлаб қолиш мақсадида алоқа кабелига уланиш ва файллардан ёки программалардан ноқонуний нусха кучиришни курсатиш мумкин.

Турлаш (модификация). Ресурсдан нафақат ноқонуний фойдаланишга йул очилади, балки ресурс бузгунчи томонидан узгартирилади. Натижада ахборотнинг яхлитлиги бузилади. Бундай бузилишларга мисол тариқасида файлдаги маълумотлар мазмунини узгартирилишини, программанинг вазифалари ва характеристикаларини узгартириш мақсадида уни модификациялашни, тармоқ орқали узатилаётган ахборотлар мазмунини узгартирилишини ва у. курсатиш мумкин.

Сохталаштириш (фальсификация). Тизимга сохта объект киритилади. Натижада ахборотнинг аслига тугрилиги (аутентичностлиги) бузилади. Бундай бузилишларга мисол тариқасида тармоқ орқали ясама маълумотларни узатиш ёки файлга ёзувларни кушишни курсатиш мумкин.

Юқорида келтирилган бузилишлар пассив ва актив хужум атамалари буйича классификацияланганида пассив тахдидга ушлаб қолиш(перехват) мансуб булса, узиш(разъединение), турлаш(модификация) ва сохталаштириш(фальсификация) актив тахдидга мансуб эканлигини куриш қийин эмас.

Пассив хужумлар натижасида узатилаётган маълумотлар ушлаб қолинади ёки мониторинг амалга оширилади. Бунда бузгунчининг мақсади узатилаётган ахборотни ушлаб қолишдир. Пассив бузилишларни иккита гуруҳга ажратиш мумкин- ахборотлар мазмунини фoш этиш ва маълумотлар оқимини тахлил этиш.

Ахборотлар мазмунини фoш этиш нима эканлиги маълум. Телефон орқали сухбатда, электрон почта ахборотида ёки узатилаётган файлда мууим ёки махфий ахборот булиши мумкин. Табиийки, бундай ахборот билан бу ахборот мулжалланмаган шахсларнинг танишиши мақбул эмас.

Химоянинг пассив бузилишларини аниклаш жуда кийин, чунки уларда маълумотларга қандайдир узгартиришлар киритиш кузда тутилмайди. Аммо, бундай хил бузилишларни олдини олишни амалга оширса булади. Шу сабабли пассив бузилишлар холида эътиборни уларни аниклашга эмас, балки уларни олдини олишга каратиш лозим.

Маълумотлар оқимини тахлили мукамалроқ хисобланади. Фараз қилайлик, биз ахборот ёки бошқа узатилувчи маълумотлар мазмунини шундай маскировка қилайликки, бузгунчи ахборотни уз ихтиёрига киритганида уам ундаги ахборотни чиқариб

ололмасин. Купинча ахборот мазмунини маскировка қилишда шифрлаш қўлланилади. Аммо, ахборот мазмуни шифрлаш ёрдамида ишончли тарзда беркитилган бўлсада, бузгунчида узатилувчи маълумотларнинг узига уос алотоматларини кузатиш имконияти қолади. Масалан, узатувчини ва ахборотларни узатишга ишлатилувчи узелларни, ахборотлар узунлигини ва уларнинг алмашинув частотасини аниқлаш мумкин. Бундай ахборот маълумотлар алмашинувидан кузланган мақсадни аниқлашда жуда уам қўл келиши мумкин.

Актив хужумлар натижасида маълумотлар оқими узгартирилади ёки сохта оқимлар уосил қилинади. Бундай бузилишларни туртта гуруҳга ажратиш мумкин: имитация, тиклаш, ахборотни турлаш (модификациялаш), хизмат курсатишдаги ҳалаллар.

Имитация деганда объектнинг узини бошқа объект қилиб курсатиши тушунилади. Одатда имитация актив бузилишларнинг бошқа бир хилининг уриниши билан биргаликда бажарилади. Масалан, бузгунчи тизимлар алмашинаётган аутентификация маълумотларининг оқимини ушлаб қолиб сунгра аутентификация ахборотларининг уақиқий кетма-кетлигини тиклаши мумкин. Бу эса ваколати чегараланган объектнинг узини ваколати кенгроқ объект қилиб курсатиши (имитация) орқали ваколатини кенгайтиришига имкон беради.

Тиклаш деганда маълумотлар блокини пассив ушлаб қолиб, кейин уни рухсат берилмаган натижани уосил қилиш мақсадида ретранслякия қилиш тушунилади.

Маълумотларни модификациялаш деганда рухсат берилмаган натижани уосил қилиш мақсадида қонуний ахборот қисмини узгартириш, ёки ахборот келиши кетма-кетлигини узгартириш тушунилади.

Хизмат курсатишдаги халаллар алоқа ёки уларни бошқарувчи воситаларнинг нормал ишлашига тусқинлик қилади. Бундай бузилишларда муайян мақсад кузланади: масалан, объект маълум адресатга йуналтирилган барча ахборотларни тухтатиб қолиши мумкин. Яна бир мисол, тармоқни атайин ахборотлар оқими билан ортиқча юклаш орқали ёки тармоқни ишдан чиқариш йули билан барча тармоқ ишини блокировка қилиш.

Ҳимоянинг актив бузилишларини бутунлай олдини олиш жуда мураккаб, чунки бунга факат барча алоқа воситаларини узлуксиз физик химоялаш орқали эришиш мумкин. Шу сабабли химоянинг актив бузилишларида асосий мақсад уларни оператив тарзда аниқлаш ва тездан тизимнинг ишга лаёқатлилигини тиклаш бўлиши шарт. Бузилишларнинг уз вақтида аниқланиши бузФунчини тухтатиш вазифасини ҳам утайди, ва бу вазифани бузилишлардан оғохлантириш тизимининг қисми деб қуриш мумкин.

Химоя механизмлари

Амалиётда ишлатиладиган химоя механизмларининг аксарияти криптография усулларига асосланган. Шифрлаш ёки шифрлашга яқин ахборотни узгартиришлар маълумотларни химоялаш усуллари ҳисобланади.

Химоя хизмати

Амалиётда қўлланиладиган химоя вазифалари тупламларидан бирига қуйидагилар киради: конфиденциаллик, аутентификациялаш, яхлитлик, ёлгоннинг мумкин эмаслиги, фойдаланувчанлик, фойдаланувчанликни бошқариш.

Конфиденциаллик. Конфиденциаллик маълумотлар оқимини пасив хужумлардан химоя қилишга хизмат қилади. Ахборотлар мазмунининг муҳимлиликка қараб химоянинг бир неча сатҳлари урнатилиши мумкин. Кенг маънодаги уимоя хизмати ихтиёрий иккита фойдаланувчи уртасида узатиловчи барча маълумотларни маълум вақт мобайнида химоясини таъминлаши лозим. Масалан, агар икки тизим уртасида виртуаль алоқа урнатилган бўлса бундай кенг маънодаги химоя фойдаланувчилар маълумотлари узатилгандаги ҳар қандай йуқолишларга тусиқ бўла олади. Тор маънодаги химоя хизмати алоҳида ахборотни ёки ҳатто ахборотнинг алоҳида қисмини химоясини таъминлай олади. Аммо бундай чораларнинг самараси кенг маънодаги уимоя хизматиға нисбатан кам,

уларни амалга ошириш эса баъзида мураккаб ва қиммат булиши мумкин.

Конфиденциалликнинг яна бир жиҳати маълумотлар оқимини унинг аналитик тадқиқ қилинишидан химоялашдир. Аналиик тадқиқ деганда алоқа тизимидаги ахборотлар тавсифига тааллуқли ахборот манбаини, адресатни, ахборотлар узатиладиган частотани, ахборотлар улчамини ва х. бузФунчи томонидан билишга уриниш тушунилади.

Аутентификация. Аутентификация хизмати ахборот манбаини ишончли идентификациялашга мулжалланган. Масалан, бирор хавф тугрисида сигнал берилганида аутентификация хизматининг вазифаси бу сигналнинг манбаи уақиқатан уам сигнал узатувчи эканлигини текширишдан иборат булади. Ташки интерактив алоқада, масалан, терминал ёрдамида бош узелга уланишдаги сервис хизматининг икки жиуатини ажратиш мумкин. Биринчидан, боғланиш урнатилишида аутентификация воситалари алоқада иштирок этувчиларнинг ҳақиқий (эканликларига) кафолат бериши лозим. Иккинчидан, кейинги маълумот алмашинувида бу воситалар маълумотлар оқимиға қандайдир учинчи томоннинг аралашishiға йул қўймаслиги лозим.

Яхлитлик. Яхлитлик конфиденциаллик каби ахборотлар оқимиға, алоҳида ахборотға ёки хатто ахборот қисмиға тааллуқли булиши мумкин. Бу ҳолда ҳам жами оқимни химоялаш мақсадға мувофиқ уисобланади. Ахборот яхлитлигини боғланишлар асосидаги химояловчи воситалар ахборот оқими билан иш куради ва қабул қилинган ахборотларнинг узатилганиға камаймасдан, қушилмасдан дастлабки узатиш кетма-кетлиги бузилмасдан, қайтаришларсиз аниқ мос келиши кафолатини таъминлайди. Бу воситалар маълумотлар бузилиши химоясини ҳам таъминлайди. Шундай қилиб, ахборот яхлитлигини боғланишлар асосидаги химояловчи воситалар ахборот оқимини модификациялашдан ҳамда хизмат курсатишдаги ҳалаллардан химояловчи воситаларни уз ичига олади.

Ахборот яхлитлигини боғланишлар урнатилмагандаги химояловчи воситалар алоҳида ахборотлар билан иш куради ва ахборотларни фақат модификациялашдан химоялашни таъминлайди.

Яхлитликни химояловчи воситаларнинг актив ҳужумға қарши туриши хисобға олинса бузилишларни олдини олиш эмас, балки бузилишларни аниқлаш муҳим хисобланади. Яхлитликнинг бузилиши аниқланганидан сунг бундай хизмат фақат бузилиш содир булганлигини хабарлаши мумкин, бузилган ёки йуқолган ахборотни тиклаш эса бошқа программ воситалари ёки оператор томонидан амалға оширилади. Умуман, автоматик тиклаш воситаларидан фойдаланиш афзал хиобланади.

Ёлгоннинг мумкин эмаслиги. Ёлгоннинг мумкин эмаслигини кафолатловчи воситалар узатувчи ва қабул қилувчининг ахборотлар узатилганлиги ҳақиқат эканлигидан тонишларига имкон бермаслиги керак. Шундай қилиб, агар ахборот ишонч қозонмаган узатувчи томонидан юборилган булса, қабул қилувчи ахборот худди шу узатувчи томонидан юборилганлигини исбот қилиш имкониятиға эға булиши зарур.

Ресурслардан фойдаланувчанлик. Бузилишларнинг купгина хиллари ресурслардан фойдаланувчанликни йуқолишиға ёки улардан фойдаланишнинг қийинлашишиға олиб келади. Бунда баъзи ҳолларда аутентификация ва шифрлаш каби автоматлаштирилган қарши чоралар самара берса, баъзи ҳолларда бузилишларни олдини олиш ёки тизим фойдаланувчанлигини тиклаш учун маълум физикавий уаракатлар талаб қилинади.

Фойдаланувчанликни бошқариш. Фойдаланувчанликни бошқариш деганда алоқа каналлари орқали тармоқ узелларидан, иловалардан фойдаланишни чегаралаш ва назорат қилиш имконияти тушунилади. Бундай назоратда ҳар бир объект узининг ваколат доирасига эға булганлиги сабабли объектларнинг ресурслардан фойдаланишға уринишларининг ҳар бирида объектларни идентификациялаш имконияти мавжуд булиши керак.

Ҳимоялаш тизимининг комплекслилиги. Ахборотларни ташкилий ҳимоялаш элементлар

Ҳимоя тизимининг комплекслилигига ундан ҳуқуқий, ташкилий, муҳандис-техник ва дастурий – математик элементларининг мавжудлиги билан эришилади. Элементлар нисбати ва уларнинг мазмуни ташкилотларнинг ахборотни ҳимоялаш тизимининг ўзига хослигини ва унинг такрорланмаслигини ҳамда бузиш қийинлигини таъминлайди.

Аниқ тизимни кўп турли элементлардан иборат, деб тасаввур қилиш мумкин. Тизим элементларининг нафақат унинг ўзига хослигини, балки ахборотнинг қимматлилигини ва тизимнинг қийматини ҳисобга олган ҳолда белгиланган ҳимоя даражасини аниқлайди.

Ахборотни ҳуқуқий ҳимоялаш элементи ҳимоялаш чораларининг ҳақли эканлиги маъносида ташкилот ва давлатларнинг ўзаро муносабатларини юридик мустаҳкамлаш ҳамда персоналнинг ташкилот қимматли ахборотини ҳимоялаш тартибига риоя қилиши ва ушбу тартибни бузилишида жавобгарлиги тасаввур қилинади.

Ахборотларни ташкилий ҳимоялаш элементлари

Ҳимоялаш технологияси персонални ташкилотнинг қимматли ахборотларини ҳимоялаш қоидаларига риоя қилишга ундовчи бошқариш ва чеклаш характериға эга бўлган чора-тадбирларни ўз ичига олади.

Ташкилий ҳимоялаш элементи бошқа барча элементларни ягона тизимга боғловчи омил бўлиб ҳисобланади. Кўпчилик мутахассисларнинг фикрича, ахборотларни ҳимоялаш тизимлари таркибида ташкилий ҳимоялаш 50-60% ни ташкил қилади. Бу ҳол кўп омилларга боғлиқ, жумладан, ахборотларни ташкилий ҳимоялашнинг асосий томони амалда ҳимоялашнинг принципи ва усуллари бажарувчи персонални танлаш, жойлаштириш ва ўргатиш ҳисобланади.

Ахборотларни ҳимоялашнинг ташкилий чора - тадбирлари ташкилот хавфсизлиги хизматининг меъёрий услубий ҳужжатларида ўз аксини топади. Шу муносабат билан кўп ҳолларда юқорида кўрилган тизими элементларининг ягона номи – ахборотни ташкилий – ҳуқуқий ҳимоялаш элементини ишлатадилар.

Ахборотларни муҳандис – техник ҳимоялаш элементи – техник воситалар комплекси ёрдамида ҳудуд, бино ва қурилмаларни кўриқлашни ташкил қилиш ҳамда техник текшириш воситаларига қарши суғуруш ва фаол кураш учун мўлжалланган. Техник ҳимоялаш воситаларнинг нархи баланд бўлсада, ахборот тизимини ҳимоялашда бу элемент муҳим аҳамиятга эга.

Ахборотни ҳимоялашнинг дастурий – математик элементи компьютер, локал тармоқ ва турли ахборот тизимларида қайта ишланадиган ва сақланадиган қимматли ахборотларни ҳимоялаш учун мўлжалланган.

Ахборотни ишончли ҳимоя механизмини яратишда ташкилий тадбирлар муҳим рол ўйнайди, чунки конфиденциал ахборотлардан рухсатсиз фойдаланиш асосан, техник жиҳатлар билан эмас, балки ҳимоянинг элементар қоидаларини эътиборга олмайдиган фойдаланувчилар ва ходимларнинг жинойткорона ҳаракатлари, бепарволиги, совуққонлиги ва маъсулиятсизлиги билан боғлиқ.

Ташкилий таъминот конфиденциал ахборотдан фойдаланишга имкон бермайдиган ёки жиддий қийинчилик туғдирувчи ижрочиларнинг ишлаб-чиқариш ва ўзаро муносабатларини меъёрий-ҳуқуқий асосида регламентлашдир.

Ташкилий тадбирларга қуйидагилар киради:

- хизматчи ва ишлаб чиқариш бино ва хоналарни лойиҳалашда, қуришда ва жиҳозлашда амалга ошириладиган тадбирлар. Бу тадбирларнинг асосий мақсади ҳудудга ва хоналарга яширинча кириш имконини йўқотиш; одамларнинг ва транспортнинг юриши назоратининг қулайлигини таъминлаш; фойдаланишнинг алоҳида тизимига эга бўлган ишлаб-чиқариш зоналарини яратиш ва х.;

- ходимларни танлашда амалга ошириладиган тадбирлар. Бу тадбирларга ходимлар билан танишиш, конфиденциал ахборот билан ишлаш қоидалари билан ишлашни ўргатиш, ахборот химояси қоидасини бузганлиги учун жавобгарлик даражаси ва х. билан таништириш киради;

- ишончли пропуск режимини ва ташриф буюрувчиларнинг назоратини ташкил қилиш;

- хона ва ҳудудларни ишончли қуриқлаш;

- ҳужжатлар ва конфиденциал ахборот элтувчиларини сақлаш ва ишлатиш, шу жумладан қайд этиш, бериш, бажариш ва қайтариш тартибларига риоя қилиш;

- ахборот химоясини ташкил этиш, яъни муайян ишлаб чиқариш жамоаларида ахборот хавфсизлигига жавобгар шахсни тайинлаш, конфиденциал ахборот билан ишловчи ходимлар ишини мунтазам текшириб туриш.

Бундай тадбирлар ҳар бир муайян ташкилот учун ўзига хос хусусиятга эга бўлади.

Ташкилий тадбирларнинг талайгина қисмини ходимлар билан ишлаш эгаллайди. Мулкчиликнинг турли шаклларига эга бўлган корхона ходимлари билан ишлашда ташкилий тадбирлар, умумий ҳолда қуйидагиларни ўз ичига олади:

- ишга қабул қилишда суҳбат. Суҳбат натижасида номзоднинг мос бўш жойга қабул қилиниши мақсадга мувофиқлиги аниқланади;

- муайян корхонада конфиденциал ахборот билан ишлаш қоидалари ва муолажалари билан танишиш; ишга қабул қилинувчи корхона тижорат сирларини сақлаши бўйича тилхат ва фирма сирларини ошкор қилмасликка ваъда беради;

- ходимларни конфиденциал ахборот билан ишлаш қоидалари ва муолажаларига ўқитиш. Ходимларни ўқитишда нафақат ишлаб-чиқариш кўникмаларига эга бўлиш ва уларни юқори даражада сақлаш, балки уларни саноат (ишлаб чиқариш) махфийлиги ахборот хавфсизлиги, интеллектуал мулк ва тижорат сирлари химояси талабларини бажариш зарурлигига қатъий ишонч руҳида тарбиялаш кўзда тутилади. Мунтазам ўқитиш раҳбарият ва ходимларнинг корхона тижорат манфаатларини химоя қилиш масалалари бўйича билимдонлик даражасини ошишига имкон яратади;

- ишдан бушаётганлар билан суҳбат. Суҳбат давомида ишдан бушаётган ходимнинг фирма сирларини фош қилмасликка қатъий ваъда бериши лозимлиги таъкидланади ва бу ваъда, одатда, тилхат орқали расмийлаштиради.

Тадбирларнинг муҳим йўналишларидан бири иш юритиш ва ҳужжат юритиш тизимини пухта ташкил этиш ҳисобланади. Бу эса ўз иш юритиш тартибини, ҳужжатларни қайдлаш, ишлаш, сақлаш, йўқотиш ва мавжудлигини ҳамда тўғри бажарилишини назорат қилишни таъминлайди. Тизимни амалга оширишда ҳужжатлар хавфсизлигига ва ахборот конфиденциаллигига алоҳида эътибор бериш лозим.

Ахборотни ҳужжатлаштириш қатъий белгиланган қоидалар ёрдамида амалга оширилади. Бу қоидаларнинг асосийлари ГОСТ 6.38-90 "Ташкилий-бошқарувчи ҳужжатлар тизими. Ҳужжатларни расмийлаштиришга талаблар", ГОСТ 6.10.4-84 "Унификацияланган ҳужжатлар тизими. Ҳисоблаш техника воситалари орқали яратилувчи машина элтувчиларидаги ва машинограммалардаги ҳужжатларга ҳуқуқий куч бериш" кабилар баён этилган. Бу ГОСТларда ахборотга ҳужжат ҳуқуқини берувчи 31 та реквизитлар кўзда тутилган, аммо бу реквизитларнинг барчасининг ҳужжатда мавжудлиги шарт эмас. Асосий реквизит – матн. Шу сабабли, ҳар қандай раво баён этилган матн ҳужжат ҳисобланади ва унга ҳуқуқий куч бериш учун сана ва имзо каби муҳим реквизитларнинг мавжудлиги кифоя.

Автоматлаштирилган ахборот тизимларидан олинган ҳужжатлар учун алоҳида тартиб қўлланилади. Бунда, маълум ҳолларда, масофадан олинган ахборот электрон имзо билан тасдиқланади. Ахборотни химоялаш учун барча ташкилий тадбирларни таъминловчи махсус маъмурий хизматни яратиш талаб қилинади. Унинг штат структураси, сони ва таркиби фирманинг реал эҳтиёжлари, ахборотининг конфиденциаллик даражаси ва хавфсизлигининг умумий ҳолати орқали аниқланади.

Маъмурий тадбирларга қуйидагилар киради:

- операцион тизимнинг тўғри конфигурациясини мададлаш;
- иш журналларининг назорати;
- пароллар алмашишининг назорати;
- химоя тизимида "рахна"ларни аниқлаш;
- ахборотни химояловчи воситаларни тестлаш.

Тармоқ операцион тизимининг тўғри конфигурациясини мададлаш масаласини, одатда, тизим маъмури хал этади. Маъмур операцион тизим (одамлар эмас) риюя қилиши лозим бўлган маълум қоидаларни яратади. Тизимни маъмурлаш – конфигурация файллари тўғри тузишдир. Бу файлларда (улар бир нечта бўлиши мумкин, масалан тизимнинг ҳар бир қисмига биттадан файл) тизим ишлаши қоидаларининг тавсифи бўлади.

Хавфсизлик маъмури компьютер тармоғи ҳолатини оператив тарзда (тармоқ компьютерлари химояланиши ҳолатини кузатиш орқали) ва оператив бўлмаган тарзда (ахборот химояси тизимидаги воқеаларни қайдловчи журналларни таҳлиллаш орқали) назоратлаш лозим. Ишчи станциялар сонининг ошиши ва турли-туман компонентлари бўлган дастурий воситаларнинг ишлатилиши ахборот химояси тизимидаги ходисаларни қайдлаш журналлар ҳажмини жиддий ошишига олиб келади. Журналлардаги маълумотлар ҳажми шунчалик ошиб кетиши мумкинки, маъмур улар таркибини жоиз вақт мобайнида таҳлиллай олмайди.

Тизим заифлигининг сабаби шундаки, биринчидан, фойдаланувчини аутентификациялаш тизими фойдаланувчи исмига ва унинг паролига (кўз тўридан фойдаланиш каби экзотик ҳоллар бундан мустасно), иккинчидан, фойдаланувчи тизимида тизимни маъмурлаш ҳукуқи берилган супервизорнинг (супервизор) мавжудлигига асосланади. Супервизор паролини сақлаш режимининг бузилиши бутун тизимдан рухсатсиз фойдаланиш имконини яратади.

Ундан ташқари бундай қоидаларга асосланган тизим-статик, қотиб қолган тизим. У фақат қатъий маълум ҳужумларга қарши тўра олиши мумкин. Олдиндан кўзда тутилмаган қандайдир янги таҳдиднинг пайдо бўлишида тармоқ ҳужуми нафақат муваффақиятли, балки тизим учун кўринмайдиган бўлиши мумкин. Шунинг учун, муассасада ишлатилувчи ахборотнинг қайсиси химояга мухтож эканлигини аниқ тасаввур қилиш муҳим ҳисобланади. Мавжуд ахборотни таҳлиллашдан бошлаш лозим. Бу муолажалар ахборот химоясини таъминлаш бўйича тадбирларни дифференциаллаш имконини беради ва натижада, сарф-харажатларнинг қисқаришига сабаб бўлади.

Ахборот химояси тизимини эксплуатация қилиш босқичида хавфсизлик маъмурининг фаолияти фойдаланувчилар ваколатларини ўз вақтида ўзгартиришдан ҳамда тармоқ компьютерларидаги химоя механизмларини созлашдан иборат бўлади. Фойдаланувчилар ваколатларини ва компьютер тармоқларида ахборотни химоялаш тизимини созлашни бошқариш муаммоси, масалан, тармоқдан марказлаштирилган фойдаланиш тизимидан фойдаланиш асосида хал этилиши мумкин. Бундай тизимни амалга оширишда тармоқ асосий серверида ишловчи махсус фойдаланишни бошқарувчи сервердан фойдаланилади. Бу сервер марказий химоя маълумотлари базасини локал химоя маълумотлари базаси билан автоматик тарзда синхронлайди. Фойдаланишни бошқаришнинг бу тизимида фойдаланувчи ваколати вақти-вақти билан ўзгартирилади ва марказий химоя маълумотлари базасига киритилади, уларнинг муайян компьютерларда ўзгариши навбатдаги синхронлаш сеансида вақтида амалга оширилади.

Ундан ташқари фойдаланувчи паролини ишчи станцияларининг бирида ўзгартирса, унинг янги пароли марказий химоя маълумотлари базасида автоматик тарзда аксланади, ҳамда бу фойдаланувчи ишлашига рухсат берилган ишчи станцияларга узатилади.

Химоялаш тизимининг комплекслиги

Химоя тизимининг комплекслигига унда ҳукукий, ташкилий, муҳандис – техник ва дастурий – математик элементларнинг мавжудлиги билан эришилади. Элементлар

нисбати ва уларнинг мазмуни ташкилотларнинг ахборотни ҳимоялаш тизимининг ўзига хослигини ва унинг такрорланмаслигини ҳамда бузиш қийинлигини таъминлайди.

Аниқ тизимни кўп турли элементлардан иборат, деб тасаввур қилиш мумкин. Тизим элементларининг мазмуни нафақат унинг узига хослигини, балки ахборотнинг қимматлилигини ва тизимнинг қийматини ҳисобга олган ҳолда белгиланган ҳимоя даражасини аниқлайди.

Ахборотни ҳуқуқий ҳимоялаш элементи ҳимоялаш чораларининг ҳақли эканлиги маъносида ташкилот ва давлатларнинг узаро муносабатларини юридик мустаҳкамлаш ҳамла персоналнинг ташкилот қимматли ахборотини ҳимоялаш тартибига риоя қилиши ва ушбу тартибни бузилишида жавобгарлиги тасаввур қилинади.

Ахборотларни ташкилий ҳимоялаш элементлари

Ҳимоялаш технологияси персонални ташкилотнинг қимматли ахборотларини ҳимоялаш қоидаларига риоя қилишга ундовчи бошқариш ва чеклаш характериға эға бўлган чора-тадбирларни ўз ичига олади.

Ташкилий ҳимоялаш элементи бошқа барча элементларни ягона тизимға боғловчи омил бўлиб ҳисобланади. Кўпчилик мутахассисларнинг фикрича, ахборотларни ҳимоялаш тизимлари таркибида ташкилий ҳимоялаш 50—60 % ни ташкил қилади. Бу ҳол кўп омилларға боғлиқ, жумладан, ахборотларни ташкилий ҳимоялашнинг асосий томони амалда ҳимоялашнинг принципи ва усулларини бажарувчи персонални танлаш, жойлаштириш ва ургатиш ҳисобланади.

Ахборотларни ҳимоялашнинг ташкилий чора – тадбирлари ташкилот хавфсизлиги хизматининг меъёрий услубий ҳужжатларида уз аксини топади. Шу муносабат билан кўп ҳолларда юқорида кўрилган тизим элементларининг яғана номи — ахборотни ташкилий - ҳуқуқий ҳимоялаш элементини ишлатадилар.

Ахборотларни муҳандис – теҳиик ҳимоялаш элементи — теҳник воситалар комплекси ёрдамида ҳудуд, бино ва қурилмаларни куриқлашни ташкил қилиш ҳамда теҳник текшириш воситаларига қарши суғт ва фаол кураш учун мулжалланган. Теҳник ҳимоялаш воситаларининг нарҳи баланд бўлсада, ахборот тизимини ҳимоялашда бу элемент муҳим аҳамиятға эға.

Ахборотни ҳимоялашнинг дастурий – математик элементи компьютер, локал тармоқ ва турли ахборот тизимларида қайта ишланадиган ва сақланадиган қимматли ахборотларни ҳимоялаш учун мулжалланган.

Ахборот тизимларида маълумотларға нисбатан хавф-хатарлар

1. Ахборот урушлар ва киберҳужумлар
2. Ахборот-коммуникацион тизимлар ва тармоқларда таҳдидлар ва заифликлар

Ахборот урушлар ва киберҳужумлар

Хавфсизлик – хар куни биз тўкнашадиган ҳаётимизнинг жихати: эшикни қулфлаймиз, қимматбаҳо нарсаларни бегона кўзлардан беркитамиз ва ҳамённи дуч келган жойда қолдирмаймиз. Бу "рақамли дунёға" ҳам расм бўлиши шарт, чунки хар бир фойдаланувчининг компютери қароқчи ҳужуми объекти бўлиши мумкин.

Коммерция ташкилотлари хавфсизликни таъминлаш ўзининг биринчи галдаги вазифаси эмас, балки уни таъминлашға сарф этиладиган харажатларни муқаррар бало деб ҳисоблаб келганлар. Қандайдир даражада бу "оқилона иш": ниҳоят, усиз ҳам иш бажаришда тўсиқлар тўлиб-тошиб ётибдику?! Аммо фирманинг барча корпоратив биноларига кеча-кундуз киришға рухсат беришға журъат этувчи ақли жойида "саноат капитанлари"ни кўрганмисиз? Албатта, йўқ! Хатто кичкина компания биносининг кириш йўлида сизни қоровул, ёки киришни чегараловчи ва назоратловчи тизими қарши олади. Ахборотни ҳимоялаш эса хали кўнгилдагидек эмас. Ахборотни қандай йўқотиш мумкинлигини ва бу қандай оқибатларға олиб келишини барча ҳам тушунавермайди.

Йирик ўйинчилар яхшигина сабоқ олдилар: хакерлар Яҳоо!, Амазон.ком каби компанияларга ва ҳатто космик тадқиқот агентлиги НАСАга ката зарар етказдилар. Хавфсизлик хизмати бозорининг энг йирик номоёндаларидан бири РСА Сесуритй, харқандай таҳдидга қарши чора борлиги хусусидаги ўйламасдан қилган баёнотидан бир неча кундан кейин, ҳужумга дучор бўлди.

Одатда одамлардан ёки предметлардан чиқадиган ва зарар етказадиган таҳдидлар қуйидаги синфларга бўлинади: *ички ёки ташқи* ва *структураланган* (маълум объектга қарши) ёки *структураланмаган* ("кимга Худо беради" кабилида адресланувчи). Масалан, компьютер вируслари "ташқи структураланмаган таҳдидлар" сифатида туркумланади ва тамомила оддий ҳисобланади. Қизиғи шундаки, фойдаланувчилар ўзининг компьютерини муайян нишон деб ҳисобламайдилар, улар ўзларини яхшигина химоялангандек сезадилар. Керакли химоя даражаси аксарият ҳолларда ишингизнинг ҳолатига боғлиқ. Агар ташкилотингиз ёки компаниянгиз қандайдир таъйиқ нишони бўлса, агар сиз миллий энергетик ресурсларни тақсимловчи ёки миллий алоқа тармоқларига хизмат қилувчи давлат инфраструктураси таркибида бўлсангиз, оддий террористлар бомбаларини ва пистолетларини четга қўйиб, турли-туман дастурий воситалар ёрдамида ташкилотингизга электрон ҳужумни амалга ошириш масаласини кўрадилар. Иккинчи томондан, савдо-сотик ва маркетинг бўйича оддий ташкилот хусусида сўз борса, фақат мижозлар руйхатини ўғриловчи хизматчиларингиз тўғрисида, қалбаки кредит карточкалари бўйича товар олувчи фирибгарлар, тармоғингизга прејскурантлардан фойдаланиш мақсадида қирувчи рақиблар, Веб-сайтнингизни таъмағирлик мақсадида бузувчилар ва шунга ўхшашлар тўғрисида қайғуришингизга тўғри келади.

Аммо, ваҳимага ўрин йўқ. Биринчи навбатда кундалик эҳтиёж чоралари кўрилиши лозим. Ахборотга эга бўлишнинг энг оммабоп усули оддий ўғрилик. Сиз иш столингизда кечага мумайгина пулни қолдириб кетмайсизу. Нима учун боқувчингиз-шахсий компьютер хавфсизлигини таъминлашга озгина вақт сарф қилмайсиз? Бу нафақат аппарат воситаларига, балки маълумотларга ҳам тааллуқли. Маълумотларни ўғирлатиш ёки йўқотиш катта, баъзида, тузатиб бўлмайдиган зарар келтиради.

Маълумки, тизим маъмурлари барча махфий материаллардан фойдаланиш имконига эга ва, одатда, компания фойдасидан ўз улушларига эга эмаслар. Шу сабабли худди улар ташкилот хавфсизлигига таҳдид сола олувчилар ичида энг каттаси ҳисобланадилар. Таъкидлаш лозимки, компания ишга қирувчиларни синчиклаб текширади. Худди шундай, хавфсизлик хизматини таъминловчиларга, айниқса маслаҳат бериш, режалаштириш ва муъмурлашни тавсия этувчиларга диққат билан қараш лозим.

Цивилизация ривожининг замонавий босқичида ахборот нафақат жамоат ва давлат институтлари фаолиятида, балки ҳар бир инсон ҳаётида ҳал қилувчи ролни уйнайди. Кўз олдимизда жамиятнинг ахборотлашиши шиддат билан ва кўпинча олдиндан билиб бўлмайдиган тарзда ривожланмоқда. Биз эса унинг ижтимоий, сиёсий, иқтисодий ва бошқа оқибатларини тушуниб етишга бошлаймиз, ҳолос. Жамиятимизнинг ахборотлашиши ягона дунё ахборот маконининг яратилишига олиб келадики, бу макон доирасида ахборотни йиғиш, ишлаш, сақлаш ва субъектлар – инсонлар, ташкилотлар, давлатлар ўртасида алмашиш амалга оширилади.

Равшанки, сиёсий, иқтисодий, илмий-техникавий ва бошқа ахборотларни тезликда алмашиш имконияти жамият ҳаётининг барча соҳаларида ва айниқса ишлаб чиқаришда ва бошқаришда янги технологияларнинг қўлланилиши сўзсиз фойдалидир. Аммо, саноатнинг тезликда рифожланиши Ер экологиясига таҳдид сола бошлади, ядро физикаси соҳасидаги ютуқлар ядро уруши хавфини тўғдирди. Ахборотлаштириш ҳам жиддий муаммолар манбаига айланиши мумкин.

Урушлар доимо бўлган. Вақт ўтиши билан урушни олиб бориш бутун бир фанга айланди. Харқандай фандагидек урушда ўзининг тарихи, ўзининг қондаси, машҳур намоёндалари, ўзининг методологияси пайдо бўлди.

Замонавий уруш ғояси жуда илдамлаб кетди. Энди унинг макони – бутун ер шари. Уруш локал қароқчи ҳужумидан бир неча давлатларни вайрон қилувчи глобал муаммога айланди.

Турли мамлакатларнинг ҳарбий доктриналарида электрон қурол ривожини режалари ва махсус вазифаларга мўлжалланган дастурий таъминот тўғрисида эслатишлар кўзга ташланмоқда. Турли разведка манбаларидан келаётган ахборотнинг таҳлили натижасида ҳулоса қилиш мумкинки, баъзи бир давлатларнинг раҳбарлари ҳужумкор кибер-дастурларни яратишни молияламоқдалар.

Ахборот урушига оддий воситалар ёрдамида ҳарбий ҳаракатлар самара бермайдиган ҳолларга нисбатан стратегик альтернатива сифатида қаралмоқда.

Ҳарбийлар томонидан киритилган *ахборот уруши* атамаси реал, қирғинли ва емирувчи ҳарбий ҳаракатлар билан боғлиқ шафқатсиз ва хавфли фаолиятни англатади. Бу урушнинг алоҳида қирралари-штаб уруши, электрон уруши, психологик амаллар ва ҳ.

Харқандай уруш, ахборот уруши шу жумладан, замонавий қурол ёрдамида олиб борилади. Ахборот қуроли ёрдамида, уруш олиб бориловчи барча қуроллардан фарқли ўлароқ, эълон қилинмаган ва кўпинча дунёга кўринмайдиган урушларни олиб бориш мумкин (олиб боришмоқда ҳам). Бу қуролнинг таъсир объектлари – иқтисодий, сиёсий, ижтимоий ва ҳ. каби жамият ва давлат институтлари. Маълумотларни узатиш тармоқларининг келажак жанглари майдонига айланиши аллақачон эътироф этилган.

Ахборот қуроли ҳужумда ва мудофаада "электрон тезлик" билан ишлатилиши мумкин. У энг илғор технологияларга асосланган бўлиб, ҳарбий низоларни дастлабки босқичида ҳал этилишини таъминлайди ҳамда умуммақсад кучларнинг қўлланилишини истисно қилади. Ахборот қуроли қўлланишининг стратегияси ҳужумкор характерга эга. Аммо хусусий заифлик нуқтаи назари мавжуд, айниқса фуқаролик секторида. Шу сабабли бундай қуролдан ва ахборот терроризмидан ҳимояланиш муаммоси ҳозирда биринчи ўринга чиққан. Фойдаланувчиларига дунё тармоқларида ишлашни таъминловчи мамлакатларнинг миллий ахборот ресурсларининг заифлиги – ҳар икки томонга хавфли нарсаси.

Ахборот қуроли деганда ахборот массивларини йўқотиш, бузиш ёки ўғирлаш воситалари, ҳимоялаш тизимини йўқотиш, қонуний фойдаланувчилар фаолиятини чегаралаш асбоб-ускуналар ва бутун компьютер тизими ишлаши тартибини бузиш воситалари тушунилади.

Ҳозирда ҳужумкор ахборот қуроли сифатида қуйидагиларни кўрсатиш мумкин:

- *компьютер вируслари* – кўпайиш, дастурларда ўрнашиш, алоқа линиялари, маълумотларни узатиш тармоқлари бўйича узатилиш, бошқариш тизимларини ишдан чиқариш ва шунга ўхшаш қобилиятларга эга;

- *манتيқий бомбалар* – сигнал бўйича ёки ўрнатилган вақтда ҳаракатга келтириш мақсадида ҳарбий ёки фуқаро инфраструктураларига ўрнатиловчи дастурланган қурилмалар;

- *телекоммуникация тармоқларида ахборот алмашинувини босириши воситалари*, давлат ва ҳарбий бошқарув каналларида ахборотни сохталаштириш;

- *тестли дастурларни бетарафлаштириши воситалари*;

- объект дастурий таъминотида айбоқчилар томонидан атайин киритилувчи турли хил *хатоликлар*.

Универсаллик, махфийлик, дастурий-аппарат амалга оширилишининг ҳар хиллиги, таъсирининг кескинлиги, қўлланилишининг вақти ва жойини танлаш имконияти, ниҳоят, фойдалилиги ахборот қуролини ҳаддан ташқари хавфли қилади. Бу қуролни, масалан, интеллектуал мулкни ҳимоялаш воситасига ўхшатиб ниқоблаш мумкин. Ундан ташқари, у ҳатто уруш эълон қилмасдан ҳужум ҳаракатларини автоном тарзда олиб бориш имконини беради.

Замонавий жамиятда ахборот қуролини ишлатиш ҳарбий стратегияси фуқаро сектори билан узвий боғланган. Ахборот қуролининг, унинг таъсири шакли ва

усулларининг пайдо бўлиши ва қўлланиши хусусиятларининг турли-туманлиги ундан химояланишнинг мураккаб масалаларини вужудга келтирди.

Ахборот қуроли қўлланилишини олдини олиш ёки қўлланиши оқибатларини бартараф қилиш учун қуйидаги чораларни кўриш лозим:

- ахборот ресурсларининг физик асосини ташкил этувчи моддий-техник объектларни химоялаш;

- маълумотлар базалари ва банкларининг меёрий ва муттасил ишлашини таъминлаш;

- ахборотдан рухсатсиз фойдаланишдан, уни бузилишидан ёки йўқ қилинишидан химоялаш;

- ахборот сифатини сақлаш (ўз вақтидалиги, аниқлиги, тўлаллиги ва фойдаланувчанлиги).

Давлатнинг дунё очик тармоғига уланишининг иқтисодий ва илмий-техник сиёсатини ахборот хавфсизлиги орқали кўриш лозим. Бу очик, фуқароларнинг ахборотга ва интеллектуал мулкга эга бўлиш қонуний ҳуқуқини сақлашга мўлжалланган сиёсат мамлакат ҳудудида тармоқ асбоб-ускуналарини унга ахборот қуроли элементларининг киришидан сақлашни кўзда тутиш лозим. Бу муаммо ҳозирда, чет эл ахборот технологияларини оммавий сотиб олинаётган пайтда ўта муҳимдир.

Маълумки, дунё ахборот маконига уланмасдан мамлакат иқтисодини ривожлантириб бўлмайди. Интернет тармоғи томонидан таъминланган ахборот ва ҳисоблаш ресурсларидан оператив фойдаланишни давлатчиликни, фуқаролик жамияти институтларини мустаҳкамлаш, ижтимоий инфраструктураларининг ривожланиш шартлари сифатида талқин этиш мумкин.

Аммо мамлакатнинг халқаро телекоммуникация тизимида ва ахборот алмашинувида иштирокининг ахборот хавфсизлиги муаммосини комплекс ҳал қилмасдан мумкин эмаслигини аниқ тасаввур этиш лозим. Айниқса хусусий ахборот ресурсларини химоялаш муаммоси ахборот ва телекоммуникация технологиялар соҳасида ривожланган мамлакатлардан технологик орқада қолаётган мамлакатлар учун жиддий ҳисобланади.

Ахборот қуралини ишлаб чиқишни ва уни ишлатишни химиявий ва бактериологик қурол каби тақиқлаш эҳтимолдан узоқ. Худди шу каби кўпгина мамлакатларнинг ягона глобал ахборот маконини шакллантириш бўйича уринишларини чегаралаб бўлмайди.

Тизим маъмури учун химоянинг мақбул даражасини таъминлашнинг ягона усули-ахборотга эга бўлиши, чунки ҳозирча ахборот ҳужумига энг тез реакция берадиган инсон ҳисобланади. Демак, ахборотни химоялаш маъмуруларининг ўқитишга ва профессионал ўсишига сарф-харажат ахборот ҳужумларига қарши турувчи энг самарали восита ҳисобланади.

Ахборот-коммуникацион тизимлар ва тармоқларда таҳдидлар ва заифликлар

Тармоқ технологиялари ривожининг бошланғич босқичида вируслар ва компьютер ҳужумларининг бошқа турлари таъсиридаги зарар кам эди, чунки у даврда дунё иқтисодининг ахборот технологияларига боғлиқлиги катта эмас эди. Ҳозирда, ҳужумлар сонининг доимо ўсиши ҳамда бизнеснинг ахборотдан фойдаланиш ва алмашишнинг электрон воситаларига боғлиқлиги шароитида машина вақтининг йўқолишига олиб келувчи хатто озгина ҳужумдан келган зарар жуда катта рақамлар орқали ҳисобланади. Мисол тариқасида келтириш мумкинки, фақат 2003 йилнинг биринчи чорагида дунё микёсидаги йўқотишлар 2002 йилдаги барча йўқотишлар йиғиндисининг 50%ини ташкил этган.

Корпоратив тармоқларда ишланадиган ахборот, айниқса, заиф бўлади. Ҳозирда рухсатсиз фойдаланишга ёки ахборотни модификациялашга, ёлғон ахборотнинг муомалага кириши имконининг жиддий ошишига қуйидагилар сабаб бўлади:

- компьютерда ишладиган, узатиладиган ва сақланадиган ахборот хажмининг ошиши;
- маълумотлар базасида муҳимлик ва махфийлик даражаси турли бўлган ахборотларнинг тўпланиши;
- маълумотлар базасида сақланаётган ахборотдан ва ҳисоблаш тармоқ ресурсларидан фойдаланувчилар доирасининг кенгайиши;
- масофадаги ишчи жойлар сонининг ошиши;
- фойдаланувчиларни боғлаш учун Интернет глобал тармоғини ва алоқанинг турли каналларини кенг ишлатиш;
- фойдаланувчилар компьютерлари ўртасида ахборот алмашинувининг автоматлаштирилиши.

Ахборот хавфсизлигига таҳдид деганда ахборотнинг бузилиши ёки йўқотилиши хавфига олиб келувчи химояланувчи объектга қарши қилинган ҳаракатлар тушунилади. Олдиндан шуни айтиш мумкинки, сўз барча ахборот хусусида эмас, балки унинг фақат, мулк эгаси фикрича, коммерция қийматига эга бўлган қисми хусусида кетяпти.

Замонавий корпоратив тармоқлар ва тизимлар дучор бўладиган кенг тарқалган таҳдидларни таҳлиллаймиз. Ҳисобга олиш лозимки, хавфсизликка таҳдид манбалари корпоратив ахборот тизимининг ичида (ички манба) ва унинг ташқарисида (ташқи манба) бўлиши мумкин. Бундай ажратиш тўғри, чунки битта таҳдид учун (масалан, ўғирлаш) ташқи ва ички манбаларга қарши ҳаракат усуллари турлича бўлади. Бўлиши мумкин бўлган таҳдидларни ҳамда корпоратив ахборот тизимининг заиф жойларини билиш хавфсизликни таъминловчи энг самарали воситаларни танлаш учун зарур ҳисобланади.

Тез-тез бўладиган ва хавфли (зарар ўлчами нуқтаи назаридан) таҳдидларга фойдаланувчиларнинг, операторларнинг, маъмурларнинг ва корпоратив ахборот тизимларига хизмат кўрсатувчи бошқа шахсларнинг атайин қилмаган хатоликлари киради. Баъзида бундай хатоликлар (нотўғри киритилган маълумотлар, дастурдаги хатоликлар сабаб бўлган тизимнинг тўхташи ёки бўзилиши) тўғридан тўғри зарарга олиб келади. Баъзида улар нияти бузук одамлар фойдаланиши мумкин бўлган нозик жойларни пайдо бўлишига сабаб бўлади. Глобал ахборот тармоғида ишлаш ушбу омилнинг етарлича долзарб қилади. Бунда зарар манбаи ташкилотнинг фойдаланувчиси ҳам, тармоқ фойдаланувчиси ҳам бўлиши мумкин, охиригиси айниқса хавфли.

Зарар ўлчами бўйича иккинчи ўринни ўғирлашлар ва сохталаштиришлар эгаллайди. Текширилган ҳолатларнинг аксариятида ишлаш режимлари ва химоялаш чоралари билан аъло даражада таниш бўлган ташкилот штатидаги ходимлар айбдор бўлиб чиқдилар. Глобал тармоқлар билан боғланган қувватли ахборот каналининг мавжудлигида, унинг ишлаши устидан етарлича назорат йўқлиги бундай фаолиятга қўшимча имкон яратади.

Хафа бўлган ходимлар (хатто собиқлари) ташкилотдаги тартиб билан таниш ва жуда самара билан зиён етказишлари мумкин. Ходим ишдан бўшаганида унинг ахборот ресурсларидан фойдаланиш ҳукуки бекор қилиниши назоратга олиниши шарт.

Хозирда ташқи коммуникация орқали рухсатсиз фойдаланишга атайин қилинган уринишлар бўлиши мумкин бўлган барча бузилишларнинг 10%ини ташкил этади. Бу катталик анчагина бўлиб туюлмаса ҳам, Интернетда ишлаш тажрибаси кўрсатадики, қарийб ҳар бир Интернет-сервер кунига бир неча марта суқилиб кириш уринишларига дучор бўлар экан. Хавф-хатарлар таҳлил қилинганида ташкилот корпоратив ёки локал тармоғи компьютерларининг ҳужумларга қарши туриши ёки бўлмаганида ахборот хавфсизлиги бузилиши фактларини қайд этиш учун етарлича химояланмаганлигини ҳисобга олиш зарур. Масалан, ахборот тизимларини химоялаш Агентлигининг (АҚШ) тестлари кўрсатадики, 88% компьютерлар ахборот хавфсизлиги нуқтаи назаридан нозик жойларга эгаки, улар рухсатсиз фойдаланиш учун фаол ишлатишлари мумкин. Ташкилот ахборот структурасидан сасофадан фойдаланиш ҳоллари алоҳида кўрилиши лозим.

Химоя сиёсатини тузишдан аввал ташкилотда компьютер мухити дучор бўладиган хавф-хатар баҳоланиши ва зарур чоралар кўрилиши зарур. Равшанки, химояга таҳдидни назоратлаш ва зарур чораларни кўриш учун ташкилотнинг сарф-харажати ташкилотда активлар ва ресурсларни химоялаш бўйича ҳеч қандай чоралар кўрилмаганида кутиладиган йўқотишлардан ошиб кетмаслиги шарт.

Умуман олганда, ташкилотнинг компьютер мухити икки хил хавф-хатарга дучор бўлади:

1. Маълумотларни йўқотилиши ёки ўзгартирилиши.
2. Сервиснинг тўхтатилиши.

Таҳдидларнинг манбаларини аниқлаш осон эмас. Улар нияти бузуқ одамларнинг бостириб киришидан то компьютер вирусларигача турланиши мумкин.

Бунда инсон хатоликлари хавфсизликка жиддий таҳдид ҳисобланади. 1.1-расмда корпоратив ахборот тизимида хавфсизликнинг бузилиш манбалари бўйича статистик маълумотларни тасвирловчи айланма диаграмма келтирилган



1.1-расм. Хавфсизликнинг бузилиш манбалари.

1.1.-расмда келтирилган статистик маълумотлар ташкилот маъмуриятига ва ходимларига корпоратив тармоқ ва тизими хавфсизлигига таҳдидларни самарали камайитириш учун ҳаракатларни қаерга йўналтиришлари зарурлигини айтиб бериши мумкин. Албатта, физик хавфсизлик муаммолари билан шуғулланиш ва инсон хатоликларининг хавфсизликка салбий таъсирини камайитириш бўйича чоралар кўрилиши зарур. Шу билан бир қаторда корпоратив тармоқ ва тизимга ҳам ташқаридан, ҳам ичкаридан бўладиган ҳужумларни олдини олиш бўйича тармоқ хавфсизлиги масаласини ечишга жиддий эътиборни қаратиш зарур.

Ахборот тизимларида маълумотларга насбатан хавф-хатарлар

Компьютер тизими (тармоги)га зиён етказиши мумкин бўлган шароит, ҳаракат ва жараёнлар компьютер тизими (тармоги) учун хавф - хатарлар, деб ҳисобланади.

Автоматлаштирилган ахборот тизимларига тасодифий таъсир кўрсатиш сабаблари таркибига қуйидагилар киради.



Маълумки, компьютер тизим (тармоғ)ининг асосий компонентлари — техник воситалари, дастурий - математик таъминот ва маълумотлардир.

Назарий томондан бу компонентларга нисбатан тўрт турдаги хавфлар мавжуд, яъни узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш:

— узилиш — қандайдир ташки ҳаракатлар (ишлар, жараёнлар)ни бажариш учун ҳозирги ишларни вақтинча марказий процессор қурилмаси ёрдамида тухтатишдир, уларни бажаргандан сўнг процессор олдинги ҳолатга қайтади ва тўхтатиб қуйилган ишни давом эттиради. Ҳар бир узилиш тартиб рақамига эга, унга асосан марказий процессор қурилмаси қайта ишлаш учун қисм – дастурни қидириб топади. Процессорлар икки турдаги узилишлар билан ишлашни вужудга келтириши мумкин: дастурий ва техник. Бирор қурилма фавқулудда хизмат кўрсатилишига муҳтож бўлса, унда техник узилишлар пайдо бўлади. Одатда бундай узилиш марказий процессор учун қутилмаган ҳодисадир. Дастурий узилишлар асосий дастурлар ичида процессорнинг махсус буйруқлари ёрдамида бажарилади. Дастурий узилишда дастур ўз – ўзини вақтинча тўхтатиб, узилишга тааллуқли жараёни бажаради.

— тутиб олиш — жараёни оқибатида ғаразли шахслар дастурий воситалар ва ахборотларнинг турли магнитли ташувчиларига киришни қулга киритади. Дастур ва маълумотлардан ноқонуний нусха олиш, компьютер тармоклари алоқа каналларидан номуаллифлик ўқишлар ва ҳоказо ҳаракатлар тутиб олиш жараёнларига мисол бўла олади.

— ўзгартириш — ушбу жараён ёвуз ниятли шахс нафақат компьютер тизими компонентларига (маълумотлар тупламлари, дастурлар, техник элементлари) киришни қулга киритади, балки улар билан манипуляция (ўзгартириш, кўринишини ўзгартириш) ҳам килади. Масалан, ўзгартириш сифатида ғаразли шахснинг маълумотлар тўпламидаги маълумотларни ўзгартириши, ёки умуман компьютер тизими файлларини ўзгартириши, ёки қандайдир қўшимча ноқонуний қайта ишлашни амалга ошириш мақсадида фойдаланилаётган дастурнинг кодини ўзгартириши тушунилади;

— сохталаштириш — ҳам жараён саналиб, унинг ёрдамида ғаразли шахслар тизимда ҳисобга олинмаган вазиятларни ўрганиб, ундаги камчиликларни аниқлаб, кейинчалик ўзига керакли ҳаракатларни бажариш мақсадида тизимга қандайдир сохта жараёни ёки тизим ва бошқа фойдаланувчиларга сохта ёзувларни юборади.

2-МАЪРУЗА. ВИРУСЛАР ВА АНТИВИРУСЛАР

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 қобилятини сақлайди". Вируснинг ўз-ўзидан кўпайиши ва ҳисоблаш жараёнини модификациялаш қобиляти бу таърифдаги таянч тушунчалар ҳисобланади. Компьютер вирусининг ушбу хусусиятлари тирик табиат организмларида биологик вирусларнинг паразитланишига ўхшаш.

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

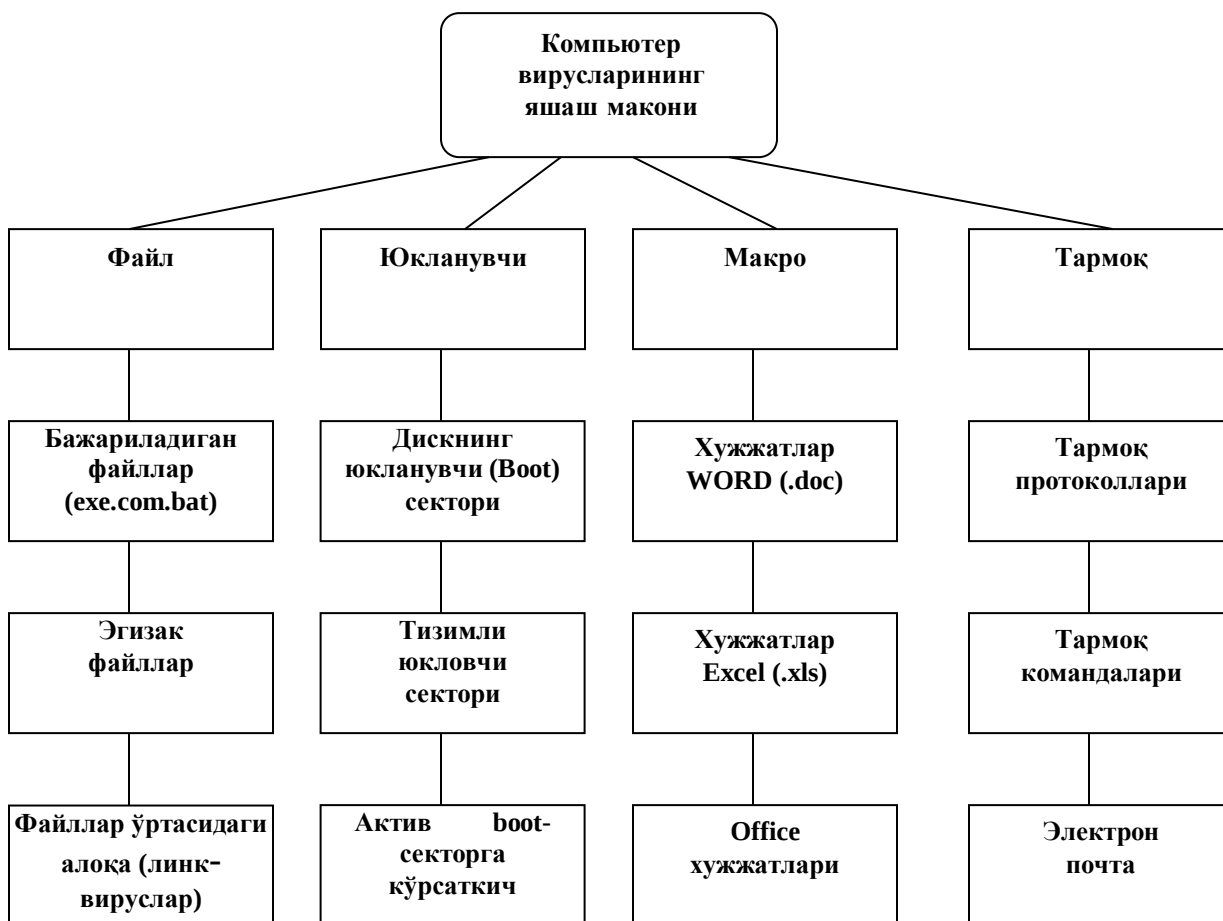
- аслига мос келиши шарт бўлмаган, аммо аслининг хусусиятларига (ўз-ўзини тиклаш) эга бўлган нусхаларни яратиш қобилияти;
- ҳисоблаш тизимининг бажарилувчи объектларига яратилувчи нусхаларнинг киритилишини таъминловчи механизмларнинг мавжудлиги.

Таъкидлаш лозимки, бу хусусиятлар зарурий, аммо етарли эмас. Кўрсатилган хусусиятларни ҳисоблаш муҳитидаги 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 (1-расм).



1-расм. Яшаш макони бўйича компьютер вирусларининг туркумланиши.

Файл вируслари бажарилувчи файлларга турли усуллар билан киритилади (энг кўп тарқалган вируслар хили), ёки файл-йўлдошларни (компаньон вируслар) яратади ёки файлли тизимларни (линк-вируслар) ташкил этиш хусусиятидан фойдаланади.

Юклама вируслар ўзини дискнинг юклама секторига (боот - секторига) ёки винчестернинг тизимли юкловчиси (Мастер Боот Ресорд) бўлган секторга ёзади. Юклама вируслар тизим юкланишида бошқаришни олувчи дастур коди вазифасини бажаради.

Макровируслар ахборотни ишловчи замонавий тизимларнинг макродастурларини ва файлларини, хусусан МисроСофт Ворд, МисроСофт Ехсел ва х. каби оммавий муҳаррирларнинг файл-хужжатларини ва электрон жадвалларини захарлайди.

Тармоқ вируслари ўзини тарқатишда компьютер тармоқлари ва электрон почта протоколлари ва командаларидан фойдаланади. Баъзи тармоқ вирусларини "қурт" хилидаги дастурлар деб юритишади. Тармоқ вируслари Интернет-қуртларга (Интернет бўйича тарқалади), ИРС-қуртларга (чатлар, Интернет Релей Чат) бўлинади.

Компьютер вирусларининг кўпгина комбинацияланган хиллари ҳам мавжуд, масалан – тармоқли макровирус тахрирланувчи хужжатларни захарлайди, ҳамда ўзининг нусхаларини электрон почта орқали тарқатади. Бошқа бир мисол сифатида файл-юклама вирусларини кўрсатиш мумкинки, улар файлларни ҳамда дискларнинг юкланадиган секторини захарлайди.

Вирусларнинг ҳаёт даври. Хар қандай дастурдагидек компьютер вируслари ҳаёт даврининг 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 химояланиш учун операцион тизимни назорат қила олмайди.

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

1. Вирусни хотирага юклаш.
2. Қурбонни кидириш.
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. Мураккаброқ вазибаларда вирус бошқаришни олганидан сўнг ўзининг ишлаши учун қўшимча ҳаракатлар бажариши мумкин. Бу билан боғлиқ иккита жихат кўрилади.

Биринчиси вирусларни аниқлаш муолажасининг максимал мураккаблашиши билан боғлиқ. Сақланиш босқичида баъзи вируслар химояланишни 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 очик кўринишда сақланиши лозим. Бундай ҳолатдан қутилиш учун вирусларни ишлаб чиқувчилар расшифровка қилувчи кодини "мутациялаш" механизмидан фойдаланади. Бу усулнинг моҳияти 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 (полйморпхис)-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* (Стеалтх) 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 ҳам бўшалиб сақланишнинг пассив босқичига ўтади. Аммо баъзи вируслар хили хотирада сақланиш ва вирус элтувчи иши тугашидан сўнг фаол қолиш қобилятига 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 холда бўлади.

Резидент бўлмаган 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. Юклануви ва макровирусларрезидент 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 холда захарлаш деганда қурбон сифатида танланган объектда вирус коднинг 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:

1. *Файл бошига киритиш.* Ушбу усул МС-ДОСнинг *com*-файллари учун энг қулай ҳисобланади, чунки ушбу форматда хизматчи сарлавхалар кўзда тутилган.

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

3. *Файл ўртасига киритиш.* Одатда бу усулдан вируслар структураси олдиндан маълум файлларга (масалан, *Сомманд.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 дисklarнинг юкланиш секторларининг сифати ва қаттиқ дискнинг бош юклама ёзуви (МБР) орқали аниқланади. Асосий муаммо-ушбу объект ўлчамларининг чегараланганлиги. Шу сабабли, вируслар ўзларининг қурбон жойида сиғмаган қисмини дискда сақлаши, ҳамда захарланган юкловчи оригинал кодини ташиши лозим.

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

Деструктив функцияларни бажариши. Деструктив имкониятлари бўйича беэиён, хавфсиз, хавфли ва жуда хавфли вируслар фаркланади.

Беэиён 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 эиён 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.

Бошқаришни 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.

Зарар келтирувчи дастурларнинг бошқа хиллари. Вируслардан ташқари зарар келтирувчи дастурларнинг куйидаги хиллари мавжуд:

- троян дастурлари;
- мантикий бомбалар;
- масофадаги компьютерларни яширинча маъмурловчи хакер утилиталари;
- Интернетдан ва бошқа конфиденциал ахборотдан фойдаланиш паролларини ўғирловчи дастурлар.

Улар орасида аниқ чегара йўқ: троян дастурлари таркибида вируслар бўлиши, вирусларга мантикий бомбалар жойлаштирилиши мумкин ва х.

Троян дастурлар ўзлари кўпаймайди ва тарқатилмайди. Ташқаридан троян дастурлар мутлақо беозор кўринади, хатто фойдали функцияларни тавсия этади. аммо фойдаланувчи бундай дастурни компьютерига юклаб, ишга туширса, дастур билдирмай зарар келтирувчи функцияларни бажариши мумкин. Кўпинча троян дастурлар вирусларни дастлабки тарқатишда, Интернет орқали масофадаги компьютердан фойдаланишда, маълумотларни ўғирлашда ёки уларни йўқ қилишда ишлатилади.

Мантикий бомба – маълум шароитларда зарар келтирувчи харакатларни бажарувчи дастур ёки унинг алохида модуллари. Мантикий бомба, масалан, маълум сана келганда ёки маълумотлар базасида ёзув пайдо бўлганида ёки йўқ бўлганида ва х. ишга тушиши мумкин. Бундай бомба вирусларга, троян дастурларга ва оддий дастурларга жойлаштирилиши мумкин.

Вируслар ва зарар келтирувчи дастурларни тарқатиш каналлари. Компьютерлар ва корпоратив тармоқларни химояловчи 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 ФТП – 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 МисроСофт Ворд, Ехсел, Ассесс файллари каби офис хужжатларининг захарланган файллари алмашилишида 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 тарика вирус эпидемияси бошланади. Вирус

тармоқда шу вирус тушиб қолган компьютер фойдаланувчиси ҳуқуқлари каби ҳуқуққа 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.

Хозирда Интернет глобал тармоғи вирусларнинг асосий манбаи ҳисобланади. Вируслар билан захарланишларнинг аксарияти МисроСофт Ворд форматида хатлар алмашишда содир бўлади. Электрон почта макрокоманда вирусларини тарқатиш канали вазифасини ўтайди, чунки ахборотлар билан бир қаторда кўпинча офис ҳужжатлари жўнатилади.

Вируслар билан захарлаш билмасдан ва ёмон ниятда амалга оширилиши мумкин. Масалан, макровирус билан захарланган муҳаррирдан фойдаланувчи ўзи шубҳа қилмаган ҳолда, адресатларга захарланган хатларни жўнатиши мумкин. Иккинчи тарафдан нияти бузук одам атайин электрон почта орқали харқандай хавфли дастурий кодни жўнатиши мумкин.

Троян Веб-сайтлар. Фойдаланувчилар вирусни ёки троян дастурни Интернет сайтларининг оддий кузатишда, троян Веб-сайтни кўрганида олиши мумкин. Фойдаланувчи браузерларидаги хатоликлар кўпинча троян Веб-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 химоянинг зарурий чоралари кўрилмаса, захарланган ишчи станция локал тармоққа киришда сервердаги бир ёки бир неча хизматчи файлларни захарлайди. Бундай файллар сифатида Логин.сом хизматчи файли, фирмада қўлланилувчи Ексел-жадваллар ва стандарт ҳужжат-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 СД-дисклардаги ноқунуний нусхаларда кўпинча турли-туман вируслар билан захарланган файллар бўлади. Вирусларни тарқатиш манбаларига электрон анжуманлар ва ФТП ва ББС файл-серверлар ҳам тааллуқли.

Ўқув юртларида ва Интернет-марказларида ўрнатилган ва умумфойдаланиш режимида ишловчи компьютерлар ҳам осонгина вирусларни тарқатиш манбаига айланиши мумкин. Агар бундай компьютерлардан бири навбатдаги фойдаланувчи дискетидан захарланган бўлса, шу компьютерда ишловчи бошқа фойдаланувчилар дискетлари ҳам захарланади.

Компьютер технологиясининг ривожланиши билан компьютер вируслари ҳам, ўзининг янги яшаш маконига мослашган ҳолда, такомиллашади. Хар қандай онда янги, олдин маълум бўлмаган ёки маълум бўлган, аммо янги компьютер асбоб-ускунасига мўлжалланган компьютер вируслари, троян дастурлари ва қуртлар пайдо бўлиши мумкин. Янги вируслар маълум бўлмаган ёки олдин мавжуд бўлмаган тарқатиш каналларидан ҳамда компьютер тизимларга татбиқ этишнинг янги технологияларидан фойдаланиши мумкин. Вирусдан захарланиш хавфини йўқотиш учун корпоратив тармоқнинг тизим маъмури, нафақат вирусга қарши усуллардан фойдаланиши, балки компьютер вируслари дунёсини доимо кузатиб бориши шарт.

3 – МАВЗУ: АХБОРОТЛАРНИ СТЕГАНОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ

1. *Замонавий компьютер стенографияси;*
2. *Конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш.*
3. *Стенографик дастурлар тўғрисида қисқача маълумот*
4. *Компьютер стенографияси истикболлари*

Замонавий компьютер стеганографияси

Рухсат этилмаган киришдан ахборотни ишончли ҳимоялаш муаммоси энг илгаритдан мавжуд ва ҳозирги вақтгача ҳал қилинмаган. Махфий хабарларни яшириш усуллари қадимдан маълум, инсон фаолиятининг бу соҳаси стеганография деган ном олган. Бу сўз грекча Стеганоc (махфий, сир) ва Грапхй (ёзув) сўзларидан келиб чиққан ва «сирли ёзув» деган маънони билдиради. Стенография усуллари, эҳтимол, ёзув пайдо бўлишдан олдин пайдо бўлган (дастлаб шартли белги ва белгилашлар қулланилган) бўлиши мумкин.

Ахборотни ҳимоялаш учун кодлаштириш ва криптография усуллари қўлланилади.

Кодлаштириш деб ахборотни бир тизимдан бошқа тизимга маълум бир белгилар ёрдамида белгиланган тартиб бўйича ўтказиш жараёнига айтилади.

Криптография деб махфий хабар мазмунини шифрлаш, яъни маълумотларни махсус алгоритм бўйича ўзгартириб, шифрланган матнни яратиш йўли билан ахборотга рухсат этилмаган киришга тусиқ қуйиш усулига айтилади.

Стеганографиянинг кринтографиядан бошқа ўзгача фарқи ҳам бор. Яъни унинг мақсади — махфий хабарнинг мавжудлигини яширишдир. Бу иккала усул бирлаштирилиши мумкин ва натижада ахборотни ҳимоялаш самарадорлигини ошириш учун ишлатилиши имкони пайдо бўлади (масалан, криптографик калитларни узатиш учун).

Компьютер технологиялари стенографиянинг ривожланиши ва мукаммаллашувига янги туртки берди. Натижада ахборотни ҳимоялаш соҳасида янги йўналиш — компьютер стеганографияси пайдо бўлди.

Глобал компьютер тармоқлари ва мультимедиа соҳасидаги замонавий прогресс телекоммуникация каналларида маълумотларни узатиш хавфсизлигини таъминлаш учун мўлжалланган янги усулларни яратишга олиб келди. Бу усуллар шифрлаш қурилмаларининг табиий ноаниқлигидан ва аналогли видео ёки аудиосигналларнинг сероблигидан фойдаланиб хабарларни компьютер файллари (контейнерлар)да яшириш имконини беради. Шу билан бирга криптографиядан фарқли равишда бу усуллар ахборотни узатиш фактининг ўзини ҳам яширади.

К.Шеннон сирли ёзунинг умумий назариясини яратдики, у фан сифатида стенографиянинг базаси ҳисобланади. Замонавий компьютер стеганографиясида иккита асосий файл турлари мавжуд: яшириш учун мўлжалланган хабар-файл, ва контейнер-файл, у хабарни яшириш учун ишлатилиши мумкин. Бунда контейнерлар икки турда бўлади: контейнер-оригинал (ёки «бўш» контейнер) - бу контейнер яширин ахборотни сақламайди; контейнер-натижа (ёки «тулдирилган» контейнер) — бу контейнер яширин ахборотни сақлайди. Калит сифатида хабарни контейнерга киритиб қуйиш тартибини аниқлайдиган махфий элемент тушунилади.

Компьютер стенографияси ривожланиши тенденциясининг таҳлили шуни кўрсатадики, кейинги йилларда компьютер стенографияси усуллари ривожлантиришга қизиқиш кучайиб бормоқда. Жумладан, маълумки, ахборот хавфсизлиги муаммосининг долзарблиги доим кучайиб бормоқда ва ахборотни ҳимоялашнинг янги усуллари кидиришга рағбатлантирилаяпти. Бошқа томондан, ахборот-коммуникациялар технологияларининг жадал ривожланиши ушбу ахборотни ҳимоялашнинг янги усуллари жорий қилиш имкониятлари билан таъминлаяпти ва албатта, бу жараённинг

кучли катализатори бўлиб умумфойдаланиладиган Интернет компьютер тармогининг жуда кучли ривожланиши ҳисобланади.

Ҳозирги вақтда ахборотни ҳимоялаш энг кўп қўлланилаётган соҳа бу — криптографик усуллардир. Лекин, бу йўлда компьютер вируслари, «мантикий бомба»лар каби ахборотий қуролларнинг криптовоситаларни бузадиган таъсирига боғлиқ кўп ечилмаган муаммолар мавжуд. Бошқа томондан, криптографик усулларни ишлатишда калитларни тақсимлаш муаммоси ҳам бугунги кунда охиригача ечилмай турибди. Компьютер стеганографияси ва криптографияларининг бирлаштирилиши пайдо бўлган шароитдан қутулишнинг яхши бир йўли булар эди, чунки, бу ҳолда ахборотни ҳимоялаш усулларининг заиф томонларини йўқотиш мумкин.

Шундай қилиб, компьютер стенографияси ҳозирги кунда ахборот хавфсизлиги бўйича асосий технологиялардан бири бўлиб ҳисобланади.

Замонавий компьютер стенографиясининг асосий ҳолатлари қуйидагилардан иборат:

- яшириш усуллари файлнинг аутентификацияланишлигини ва яхлитлигини таъминлаши керак;
- ёвуз ниятли шахсларга қўлланилувчи стеганография усуллари тўлиқ маълум деб фараз қилинади;
- усулларнинг ахборотга нисбатан хавфсизликни таъминлаши очик узаталадиган файлнинг асосий хоссаларини стенографик алмаштиришлар билан сақлашга ва бошқа шахсларга номаълум бўлган қандайдир ахборот — калитга асосланади;
- агар ёвуз ниятли шахсларга хабарни очиш вақти маълум бўлиб қолган бўлса, махфий хабарнинг ўзини чиқариб олиш жараёни мураккаб ҳисоблаш масаласи сифатида тасаввур қилиниши лозим.

Интернет компьютер тармогининг ахборот манбаларини таҳлили қуйидаги ҳулосага келишга имкон берди, яъни ҳозирги вақтда стенографик тизимлар қуйидаги асосий масалаларни ечишда фаол ишлатилаёпти:

- конфиденциал ахборотни рухсат этилмаган киришдан ҳимоялаш;
- мониторинг ва тармоқ захираларини бошқариш тизимларини енгиш;
- дастурий таъминотни никоблаш;
- интеллектуал эгаликнинг баъзи бир турларида муаллифлик ҳуқуқларини ҳимоялаш.

Замонавий компьютер стенографияси

Рухсат этилмаган киришдан ахборотни ишончли ҳимоялаш муаммоси энг илгаритдан мавжуд ва ҳозирги вақтгача ҳал қилинмаган. Махфий хабарларни яшириш усуллари қадимдан маълум, инсон фаолиятининг бу соҳаси стенография деган ном олган. Бу сўз грекча Стеганос (махфий, сир) ва Грапхй (ёзув) сўзларидан келиб чиққан ва «сирли ёзув» деган маънони билдиради. Стенография усуллари, эҳтимол, ёзув пайдо бўлишидан олдин пайдо бўлган (дастлаб шартли белги ва белгилашлар қўлланилган) бўлиши мумкин.

Ахборотни ҳимоялаш учун кодлаштириш ва криптография усуллари қўлланилади.

Кодлаштириш деб ахборотни бир тизимдан бошқа тизимга маълум бир белгилар ёрдамида белгиланган тартиб бўйича ўтказиш жараёнига айтилади.

Криптография деб махфий хабар мазмунини шифрлаш, яъни маълумотларни махсус алгоритм бўйича ўзгартириб, шифрланган матнни яратиш йўли билан ахборотга рухсат этилмаган киришга тусиқ қуйиш усулига айтилади.

Стенографиянинг кринтографиядан бошқа ўзгача фарқи ҳам бор. Яъни унинг мақсади — махфий хабарнинг мавжудлигини яширишдир. Бу иккала усул бирлаштирилиши мумкин ва натижада ахборотни ҳимоялаш самарадорлигини ошириш учун ишлатилиши имкони пайдо бўлади (масалан, криптографик калитларни узатиш учун).

Компьютер технологиялари стенографиянинг ривожланиши ва мукаммаллашувига янги туртки берди. Натижада ахборотни ҳимоялаш соҳасида янги йўналиш — компьютер стенографияси пайдо бўлди.

Глобал компьютер тармоқлари ва мультимедиа соҳасидаги замонавий прогресс телекоммуникация каналларида маълумотларни узатиш хавфсизлигини таъминлаш учун мўлжалланган янги усулларни яратишга олиб келди. Бу усуллар шифрлаш қурилмаларининг табиий ноаниқлигидан ва аналогли видео ёки аудиосигналларнинг сероблигидан фойдаланиб хабарларни компьютер файллари (контейнерлар)да яшириш имконини беради. Шу билан бирга криптографиядан фаркли равишда бу усуллар ахборотни узатиш фактининг ўзини ҳам яширади.

К.Шеннон сирли ёзувнинг умумий назариясини яратдики, у фан сифатида стенографиянинг базаси ҳисобланади. Замонавий компьютер стеганографиясида иккита асосий файл турлари мавжуд: яшириш учун мўлжалланган хабар-файл, ва контейнер-файл, у хабарни яшириш учун ишлатилиши мумкин. Бунда контейнерлар икки турда бўлади: контейнер-оригинал (ёки «бўш» контейнер) - бу контейнер яширин ахборотни сақламайди; контейнер-натижа (ёки «тулдирилган» контейнер) — бу контейнер яширин ахборотни сақлайди. Калит сифатида хабарни контейнерга киритиб қуйиш тартибини аниқлайдиган махфий элемент тушунилади.

Конфиденциал ахборотларни рухсатсиз киришдан ҳимоялаш

Бу компьютер стеганографиясини ишлатиш соҳаси конфиденциал ахборотларни ҳимоялаш муаммосини ечишда энг самарали ҳисобланади. Масалан, товушнинг энг кам аҳамиятли кичик разрядлари яшириладиган хабарга алмаштирилади. Бундай узгариш купчилик томонидан товушли хабарни эшитиш пайтида сезилмайди.

Саноат шпионлик тизимларининг мониторинг ва тармоқ захираларини бошқариш ҳаракатларига қарши йўналтирилган стенографик усуллар локал ва глобал компьютер тармоқлари серверларидан ахборотнинг ўтишида назорат ўрнатиш ҳаракатларига қарши туришга имкон беради.

Компьютер стеганографиясининг ҳозирги вақтда ишлатиладиган бошқа бир соҳаси дастурий таъминотни ниқоблашдир. Қачонки, дастурий таъминотни қайд қилинмаган фойдаланувчилар томонидан ишлатилиши ўринсиз бўлса, у стандарт универсал дастур маҳсулотлари (масалан, матнли муҳаррирлар) остида ниқобланиши ёки мультимедиа файллари (масалан, компьютер ўйинларининг мусикий иловаси)га яширилиши мумкин.

Стенографиядан фойдаланиладиган яна бир соҳалардан бири — бу муаллифлик ҳуқуқларини ҳимоялаш ҳисобланади. Компьютерли график тасвирларга махсус белги қуйилади ва у кузга кўринмай қатади. Лекин, махсус дастурий таъминот билан аниқланади. Бундай дастур маҳсулоти аллақачон баъзи журналларнинг компьютер версияларида ишлатилапти. Стенографиянинг ушбу йўналиши нафакат тасвирларни, балки аудио ва видеоахборотни ҳам қайта ишлашга мўлжалланган. Бундан ташқари унинг интеллектуал эгалигини ҳимоялашни таъминлаш вазифаси ҳам мавжуд.

Ҳозирги вақтда компьютер стенографияси усуллари икки асосий йўналиш бўйича ривожланмоқда:

- компьютер форматларининг махсус хоссаларини ишлатишга асосланган усуллар;
- аудио ва визуал ахборотларнинг сероблигига асосланган усуллар.

Стеганографик дастурлар тўғрисида қисқача маълумот

Windows операцион муҳитида ишловчи дастурлар:

- Стеганос фор Вин95 дастури ишлатишда жуда енгил бўлиб, айти пайтда файлларни шифрлаш ва уларни BMP, ДИВ, ВОС, WAB, АССИИ, HTML кен-гайтмали файллар ичига жойлаштириб яширишда жуда қудратли ҳисобланади;
- Сонтрабанд дастури 24-битли BMP форматдаги график файллар ичида ҳар қандай файлни яшира олиш имкониятига эга.

ДОС мухитида ишловчи дастурлар:

- Жстег дастури маълумотни ЖРГ форматли файллар ичига яшириш учун мўлжалланган;
- ФФЕнсоде дастури маълумотларни матнли файллар ичида яшириш имкониятига эга;
- СтегоДОС дастурлар пакетининг ахборотни тасвирда яшириш имконияти мавжуд;
- Винсторм дастурлар пакети РСХ форматли файллар ичига хабарни шифрлаб яширади.

ОС/2 операцион мухитида ишловчи дастурлар:

- Техто дастури маълумотларни инглиз тилидаги матнга айлантиради;
- Хиде4ПГП v1.1 дастури BMP, WAB, VOC форматли файллар ичига маълумотларни яшириш имкониятига эга.

Масинтош компьютерлари учун мўлжалланган дастурлар:

- Рананоид дастури маълумотларни шифрлаб, товушли форматли файл ичига яширади;
- Стего дастурининг РИСТ кенгайтмалли файл ичига маълумотларни яшириш имконияти мавжуд.

Компьютер стенографияси истикболлари

Компьютер стенографияси ривожланиши тенденциясининг таҳлили шуни кўрсатадики, кейинги йилларда компьютер стенографияси усуллари ривожлантиришга кизиқиш кучайиб бормоқда. Жумладан, маълумки, ахборот хавфсизлиги муаммосининг долзарблиги доим кучайиб бормоқда ва ахборотни химоялашнинг янги усуллари кидиришга рағбатлантирилаяпти. Бошқа томондан, ахборот-коммуникациялар технологияларининг жадал ривожланиши ушбу ахборотни химоялашнинг янги усуллари жорий қилиш имкониятлари билан таъминлаяпти ва албатта, бу жараённинг кучли катализатори бўлиб умумфойдаланиладиган Интернет компьютер тармогининг жуда кучли ривожланиши ҳисобланади.

Ҳозирги вақтда ахборотни химоялаш энг кўп қулланилаётган соҳа бу — криптографик усуллардир. Лекин, бу йўлда компьютер вируслари, «мантикий бомба»лар каби ахборотий қуролларнинг криптовоситаларни бузадиган таъсирига боғлиқ кўп ечилмаган муаммолар мавжуд. Бошқа томондан, криптографик усулларни ишлатишда калитларни тақсимлаш муаммоси ҳам бугунги кунда охиригача ечилмай турибди. Компьютер стеганографияси ва криптографияларининг бирлаштирилиши пайдо бўлган шароитдан қутулишнинг яхши бир йўли булар эди, чунки, бу ҳолда ахборотни химоялаш усуллариининг заиф томонларини йўқотиш мумкин.

Шундай қилиб, компьютер стенографияси ҳозирги кунда ахборот хавфсизлиги бўйича асосий технологиялардан бири бўлиб ҳисобланади.

Компьютер стенографиясининг асосий вазифалари

Замонавий компьютер стенографиясининг асосий ҳолатлари қуйидагилардан иборат:

- яшириш усуллари файлнинг аутентификацияланишлигини ва яхлитлигини таъминлаши керак;
- ёвуз ниятли шахсларга қўлланилувчи стеганография усуллари тўлиқ маълум деб фарз қилинади;
- усулларнинг ахборотга нисбатан хавфсизликини таъминлаши очик узаталадиган файлнинг асосий хоссаларини стенографик алмаштиришлар билан сақлашга ва бошқа шахсларга номаълум бўлган қандайдир ахборот — калитга асосланади;
- агар ёвуз ниятли шахсларга хабарни очиш вақти маълум бўлиб қолган бўлса, махфий хабарнинг ўзини чиқариб олиш жараёни мураккаб ҳисоблаш масаласи сифатида тасаввур қилиниши лозим.

Интернет компьютер тармоғининг ахборот манбаларини таҳлили куйидаги хулосага келишга имкон берди, яъни ҳозирги вақтда стенографик тизимлар куйидаги асосий масалаларни ечишда фаол ишлатилаяпти:

- конфиденциал ахборотни рухсат этилмаган киришдан ҳимоялаш;
- мониторинг ва тармоқ захираларини бошқариш тизимларини енгитиш;
- дастурий таъминотни ниқоблаш;
- интеллектуал эгаликнинг баъзи бир турларида муаллифлик ҳуқуқларини ҳимоялаш.

Конфиденциал ахборотларни рухсатсиз киришдан ҳимоялаш

Бу компьютер стеганографиясини ишлатиш соҳаси конфиденциал ахборотларни ҳимоялаш муаммосини ечишда энг самарали ҳисобланади. Масалан, товушнинг энг кам аҳамиятли кичик разрядлари яшириладиган хабарга алмаштирилади. Бундай узғариш купчилик томонидан товушли хабарни эшитиш пайтида сезилмайди.

Мониторинг ва тармоқ захираларини бошқариш тизимларини енгитиш

Саноат шпионлик тизимларининг мониторинг ва тармоқ захираларини бошқариш ҳаракатларига қарши йўналтирилган стенографик усуллар локал ва глобал компьютер тармоқлари серверларидан ахборотнинг ўтишида назорат ўрнатиш ҳаракатларига қарши туришга имкон беради.

Дастурий таъминотни ниқоблаш

Компьютер стеганографиясининг ҳозирги вақтда ишлатиладиган бошқа бир соҳаси дастурий таъминотни ниқоблашдир. Қачонки, дастурий таъминотни қайд қилинмаган фойдаланувчилар томонидан ишлатилиши ўринсиз бўлса, у стандарт универсал дастур маҳсулотлари (масалан, матнли муҳаррирлар) остида ниқобланиши ёки мультимедиа файллари (масалан, компьютер ўйинларининг мусиқий иловаси)га яширилиши мумкин.

Муаллифлик ҳуқуқларини ҳимоялаш

Стенографиядан фойдаланиладиган яна бир соҳалардан бири — бу муаллифлик ҳуқуқларини ҳимоялаш ҳисобланади. Компьютерли график тасвирларга махсус белги қуйилади ва у кузга кўринмай қатади. Лекин, махсус дастурий таъминот билан аниқланади. Бундай дастур маҳсулоти аллақачон баъзи журналларнинг компьютер версияларида ишлатилаяпти. Стенографиянинг ушбу йўналиши нафакат тасвирларни, балки аудио ва видеоахборотни ҳам қайта ишлашга мулжалланган. Бундан ташқари унинг интеллектуал эгалигини ҳимоялашни таъминлаш вазифаси ҳам мавжуд.

Ҳозирги вақтда компьютер стенографияси усуллари икки асосий йўналиш бўйича ривожланмоқда:

- компьютер форматларининг махсус хоссаларини ишлатишга асосланган усуллар;
- аудио ва визуал ахборотларнинг серобилигига асосланган усуллар.

4-МАРУЗА: АХБОРОТЛАРНИ КРИПТОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ

«Криптография» атамаси дастлаб «яшириш, ёзувни беркитиб қуймоқ» маъносини билдирган. Биринчи марта у ёзув пайдо булган даврлардаёқ айтиб ўтилган. Ҳозирги вақтда криптография деганда ҳар қандай шаклдаги, яъни дискда сақланадиган сонлар кўринишида ёки ҳисоблаш тармоқларида узатиладиган хабарлар кўринишидаги ахборотни яшириш тушунилади. Криптографияни рақамлар билан кодланиши мумкин бўлган ҳар қандай ахборотга нисбатан қўллаш мумкин. Махфийликни таъминлашга қаратилган криптография кенгроқ қўлланилиш доирасига эга. Аниқроқ айтганда, криптографияда қўлланиладиган усулларнинг ўзи ахборотни ҳимоялаш билан боғлиқ бўлган кўп жараёнларда ишлатилиши мумкин.

Криптография ахборотни рухсатсиз киришдан ҳимоялаб, унинг махфийлигини таъминлайди. Масалан, тулов варақларини электрон почта орқали узатишда унинг ўзгартирилиши ёки сохта ёзувларнинг қушилиши мумкин. Бундай ҳолларда ахборотнинг яхлитлигини таъминлаш зарурияти пайдо бўлади. Умуман олганда компьютер тармоғига рухсатсиз киришнинг мутлақо олдини олиш мумкин эмас, лекин уларни аниқлаш мумкин. Ахборотнинг яхлитлигини текширишнинг бундай жараёни, кўп ҳолларда, ахборотнинг ҳақиқийлигини таъминлаш дейилади. Криптографияда қўлланиладиган усуллар кўп бўлмаган ўзгартиришлар билан ахборотларнинг ҳақиқийлигини таъминлаши мумкин.

Нафақат ахборотнинг компьютер тармоғидан маъноси бузилмасдан келганлигини билиш, балки унинг муаллифдан келганлигига ишонч ҳосил қилиш жуда муҳим. Ахборотни узатувчи шахсларнинг ҳақиқийлигини тасдиқловчи турли усуллар маълум. Энг универсал процедура пароллар билан алмашувдир, лекин бу жуда самарали бўлмаган процедура. Чунки паролни қулига киритган ҳар қандай шахс ахборотдан фойдаланиши мумкин бўлади. Агар эҳтиёткорлик чораларига риоя қилинса, у ҳолда паролларнинг самарадорлигини ошириш ва уларни криптографик усуллар билан ҳимоялаш мумкин, лекин криптография бундан кучлироқ паролни узлуксиз ўзгартириш имконини берадиган процедураларни ҳам таъминлайди.

Криптография соҳасидаги охириги ютуқлардан бири — рақамли сигнатура — махсус хосса билан ахборотни тўлдириш ёрдамида яхлитликни таъминловчи усул, бунда ахборот унинг муаллифи берган очиқ калит маълум бўлгандагина текширилиши мумкин. Ушбу усул махфий калит ёрдамида яхлитлик текшириладиган маълум усулларан кўпроқ афзалликларга эга.

Криптография усулларини куллашнинг баъзи бирларини кўриб чиқамиз. Узатиладиган ахборотнинг маъносини яшириш учун икки хил ўзгартиришлар қўлланилади: кодлаштириш ва шифрлаш.

Кодлаштириш учун тез-тез ишлатиладиган иборалар тўпламини ўз ичига олувчи китоб ёки жадваллардан фойдаланилади. Бу иборалардан ҳар бирига, кўп ҳалларда, рақамлар тўплами билан бериладиган ихтиёрий танланган кодли суз тўғри келади. Ахборотни кодлаш учун худди шундай китоб ёки жадвал талаб қилинади. Кодлаштирувчи китоб ёки жадвал ихтиёрий криптографик ўзгартиришга мисол бўлади. Кодлаштиришнинг ахборот технологиясига мос талаблар — қаторли маълумотларни сонли маълумотларга айлантириш ва аксинча ўзгартиришларни бажара билиш. Кодлаштириш китобини тезкор ҳамда ташқи хотира қурилмаларида амалга ошириш мумкин, лекин бундай тез ва ишончли криптографик тизимни муваффақиятли деб булмайди. Агар бу китобдан бирор марта рухсатсиз фойдаланилса, кодларнинг янги китобини яратиш ва уни ҳамма фойдаланувчиларга тарқатиш зарурияти пайдо бўлади.

Криптографик ўзгартиришнинг иккинчи тури шифрлаш ўз ичига — бошланғич матн белгиларини англаб олиш мумкин бўлмаган шаклга ўзгартириш алгоритмларини камраб олади. Ўзгартиришларнинг бу тури ахборот-коммуникациялар технологияларига мос келади. Бу ерда алгоритмни ҳимоялаш муҳим аҳамият касб этади. Криптографик

калитни қўллаб, шифрлаш алгоритмининг ўзида ҳимоялашга бўлган талабларни камайтириш мумкин. Энди ҳимоялаш объекти сифатада фақат калит хизмат қилади. Агар калитдан нусха олинган бўлса, уни алмаштириш мумкин ва бу кодлаштирувчи китоб ёки жадвални алмаштиришдан енгилдир. Шунинг учун ҳам кодлаштириш эмас, балки шифрлаш ахборот-коммуникациялар технологияларида кенг қўламда қулланилмоқда.

Сирли (махфий) алоқалар соҳаси криптология деб айтилади. Ушбу сўз юнонча «крипто» — сирли ва «логос» — хабар маъносини билдирувчи сўзлардан иборат. Криптология икки йўналиш, яъни криптография ва криптотаҳлилдан иборат.

Криптографиянинг вазифаси хабарларнинг махфийлигини ва ҳақиқийлигини таъминлашдан иборат.

Криптотаҳлилнинг вазифаси эса криптографлар томонидан ишлаб чиқилган ҳимоя тизимини очишдан иборат.

Симметрияли криптотизим асослари.

Ҳозирги кунда криптотизимни икки синфга ажратиш мумкин:

- симметрияли бир калитлилик (махфий калитли);
- асимметрияли икки калитлилик (очиқ калитли).

Симметрияли тизимларда қуйидаги иккита муаммо мавжуд:

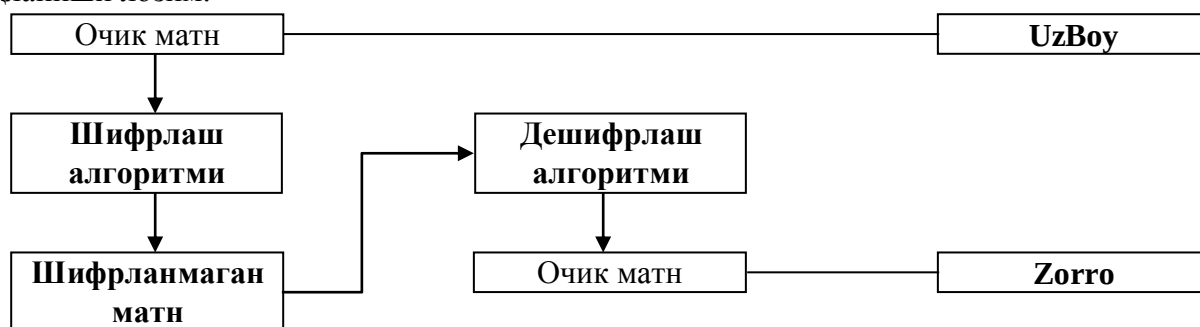
1) Ахборот алмашувида иштирок этувчилар қандай йўл билан махфий калитни бир-бирларига узатишлари мумкин?

2) Жўнатилган хабарнинг ҳақиқийлигини қандай аниқласа бўлади?

Ушбу муаммоларнинг ечими очиқ калитли тизимларда ўз аксини топди.

Очиқ калитли асимметрияли тизимда иккита калит қўлланилади. Бирдан иккинчисини ҳисоблаш усуллари билан аниқлаб бўлмайди.

Биринчи калит ахборот жўнатувчи томонидан шифрлашда ишлатилса, иккинчиси ахборотни қабул қилувчи томонидан ахборотни тиклашда қўлланилади ва у сир сақланиши лозим.



Ушбу усул билан ахборотнинг махфийлигини таъминлаш мумкин. Агар биринчи калит сирли бўлса, у ҳолда уни электрон имзо сифатида қуллаш мумкин ва бу усул билан ахборотни аутентификациялаш, яъни ахборотнинг яхлитлигини таъминлаш имкони пайдо бўлади.

Ахборотни аутентификациялашдан ташқари қуйидаги масалаларни ечиш мумкин:

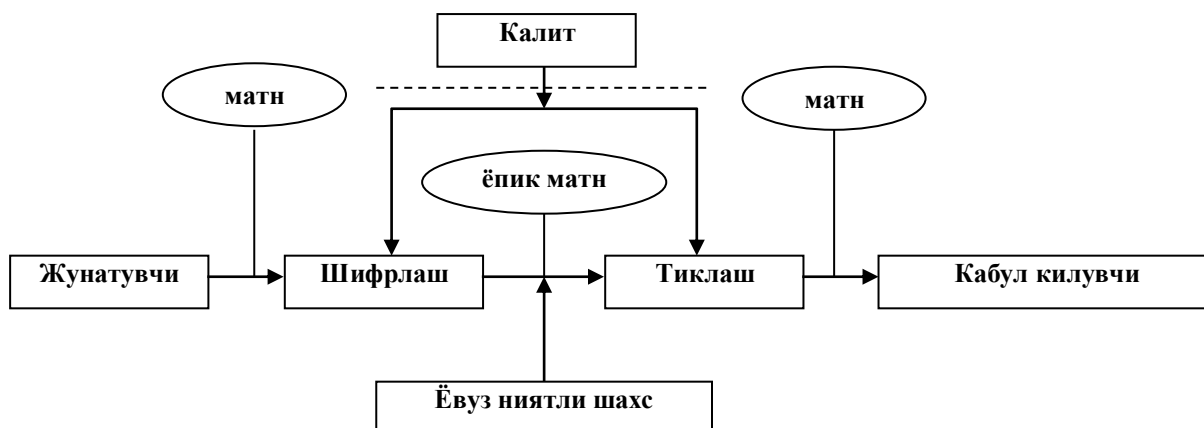
- фойдаланувчини аутентификациялаш, яъни компьютер тизими захираларига кирмоқчи бўлган фойдаланувчини аниқлаш;
- тармок абонентлари алоқасини урнатиш жараёнида уларни ўзаро аутентификациялаш.

Ҳозирги кунда ҳимояланиши зарур бўлган йўналишлардан бири бу электрон тўлов тизимлари ва Интернет ёрдамида амалга ошириладиган электрон савдолардир.

Криптография — маълумотларни ўзгартириш усуллариининг туплами бўлиб, маълумотларни ҳимоялаш бўйича қуйидаги иккита асосий муаммоларни ҳал қилишга йуналтирилган: махфийлик; яхлитлилик.

Махфийлик орқали ёвуз ниятли шахслардан ахборотни яшириш тушунилса, яхлитлилик эса ёвуз ниятли шахслар томонидан ахборотни ўзгартира олмаслик ҳақида далолат беради.

Криптография тизимини схематик равишда куйидагича тасвирлаш мумкин:



Бу ерла калит кандайдир химояланган канал оркали жунатилади (чизмада пунктир чизиклар билан тасвирланган). Умуман олганда, ушбу механизм симметрияли бир калитлик тизимига тааллуқлидир.

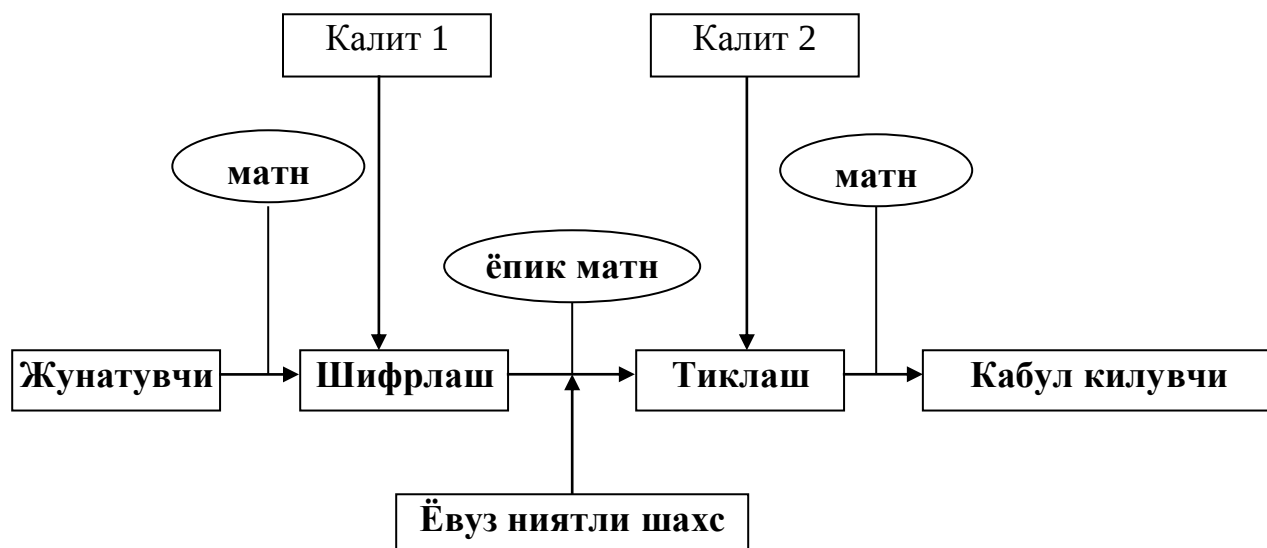
Ассимметрияли икки калитлик криптография тизимини схематик равишда куйидагича тасвирлаш мумкин:

Бу ҳолда химояланган канал бўйича очик калит жўнатилиб, махфий калит жўнатилмайд.

Ёвуз ниятли шахслар уз мақсадларига эриша олмаса ва криптотахлилчилар калитни билмасдан туриб, шифрланган ахборотни тиклай олмаса, у ҳолда криптотизим криптомуштаҳкам тизим деб айтилади.

Криптотизимнинг муштаҳкамлиги унинг калити билан аникланади ва бу криптотахлилнинг асосий қоидаларидан бири бўлиб ҳисобланади.

Ушбу таърифнинг асосий маъноси шундан иборатки, криптотизим барчаларга маълум тизим ҳисобланиб, унинг ўзгартирилиши кўп вақт ва маблағ талаб қилади, шу боис ҳам фақатгина калитни ўзгартириб туриш билан ахборотни химоялаш талаб қилинади.



Криптография нуктаи – назаридан шифр — бу калит демакдир ва очик маълумотлар тупламини ёпик (шифрланган) маълумотларга ўзгартириш криптография ўзгартиришлар алгоритмлари мажмуаси ҳисобланади.

Калит — криптография ўзгартиришлар алгоритмининг баъзи-бир параметрларининг махфий ҳолати булиб, барча алгоритмлардан ягона вариантини танлайди. Калитларга нисбатан ишлатиладиган асосий курсаткич булиб криптомуштаҳкамлик ҳисобланади.

Криптография химоясида шифрларга нисбатан куйидаги талаблар куйилади:

- етарли даражада криптомустахкамлик;
- шифрлаш ва кайтариш жараёнининг оддийлиги;
- ахборотларни шифрлаш окибатида улар хажмининг ортиб кетмаслиги;
- шифрлашдаги кичик хатоларга таъсирчан булмаслиги.

Ушбу талабларга куйидаги тизимлар жавоб беради:

- уринларини алмаштириш;
- алмаштириш;
- гаммалаштириш;
- аналитик узгартириш.

Уринларини алмаштириш шифрлаш усули буйича бошлангич матн белгиларининг матннинг маълум бир кисми доирасида махсус коидалар ёрдамида уринлари алмаштирилади.

Алмаштириш шифрлаш усули буйича бошлангич матн белгилари фойдаланилаётган ёки бошқа бир алифбо белгиларига алмаштирилади.

Гаммалаштириш усули буйича бошлангич матн белгилари шифрлаш гаммаси белгилари, яъни тасодифий белгилар кетма-кетлиги билан бирлаштирилади.

Тахлилий узгартириш усули буйича бошлангич матн белгилари аналитик формулалар ёрдамида узгартирилади, масалан, векторни матрицага купайтириш ёрдамида. Бу ерда вектор матндаги белгилар кетма-кетлиги булса, матрица эса калит сифатида хизмат килади.

5-МАЪРУЗА. **СИММЕТРИЯЛИ КРИПТОТИЗИМ АСОСЛАРИ.**

Ҳозирги кунда криптотизимни икки синфга ажратиш мумкин:

- симметрияли бир калитлилиқ (махфий калитли);
- асимметрияли икки калитлилиқ (очиқ калитли).

Симметрияли тизимларда куйидаги иккита муаммо мавжуд:

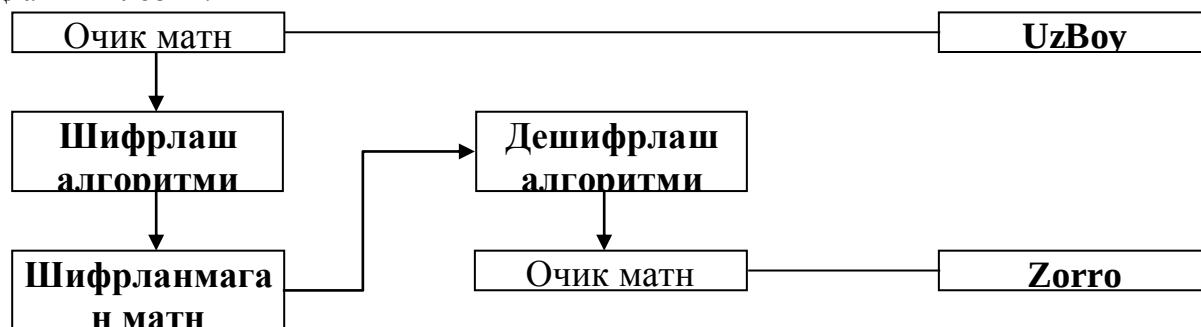
1) Ахборот алмашувида иштирок этувчилар қандай йўл билан махфий калитни бир-бирларига узатишлари мумкин?

2) Жўнатилган хабарнинг ҳақиқийлигини қандай аниқласа бўлади?

Ушбу муаммоларнинг ечими очиқ калитли тизимларда ўз аксини топди.

Очиқ калитли асимметрияли тизимда иккита калит қўлланилади. Бирдан иккинчисини ҳисоблаш усуллари билан аниқлаб бўлмайди.

Биринчи калит ахборот жўнатувчи томонидан шифрлашда ишлатилса, иккинчиси ахборотни қабул қилувчи томонидан ахборотни тиклашда қўлланилади ва у сир сақланиши лозим.



Ушбу усул билан ахборотнинг махфийлигини таъминлаш мумкин. Агар биринчи калит сирли бўлса, у ҳолда уни электрон имзо сифатида қуллаш мумкин ва бу усул билан

ахборотни аутентификациялаш, яъни ахборотнинг яхлитлигини таъминлаш имкони пайдо булади.

Ахборотни аутентификациялашдан ташқари қуйидаги масалаларни ечиш мумкин:

- фойдаланувчини аутентификациялаш, яъни компьютер тизими захираларига кирмоқчи бўлган фойдаланувчини аниклаш:

- тармок абонентлари алоқасини урнатиш жараёнида уларни ўзаро аутентификациялаш.

Ҳозирги кунда ҳимояланиши зарур бўлган йўналишлардан бири бу электрон тўлов тизимлари ва Интернет ёрдамида амалга ошириладиган электрон савдолардир.

Криптография — маълумотларни ўзгартириш усуллариининг туплами бўлиб, маълумотларни ҳимоялаш бўйича қуйидаги иккита асосий муаммоларни ҳал қилишга йуналтирилган: махфийлик; яхлитлилик.

Махфийлик орқали ёвуз ниятли шахслардан ахборотни яшириш тушунилса, яхлитлилик эса ёвуз ниятли шахслар томонидан ахборотни ўзгартира олмаслик ҳақида далолат беради.

Криптография тизимини схематик равишда қуйидагича тасвирлаш мумкин:



Бу ерда калит қандайдир ҳимояланган канал орқали жунатилади (чизмада пунктир чизиклар билан тасвирланган). Умуман олганда, ушбу механизм симметрияли бир калитлик тизимига тааллуқлидир.

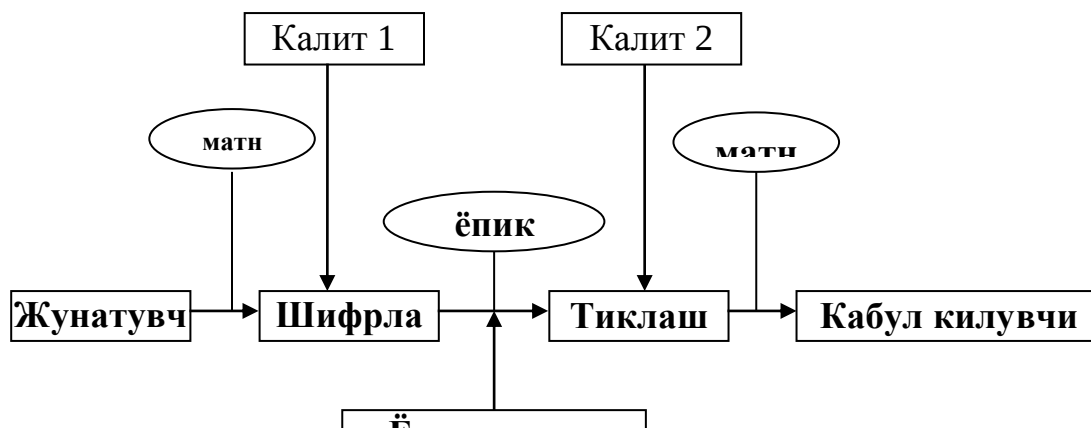
Ассимметрияли икки калитлик криптография тизимини схематик равишда қуйидагича тасвирлаш мумкин:

Бу ҳолда ҳимояланган канал бўйича очик калит жўнатилиб, махфий калит жўнатилмайд.

Ёвуз ниятли шахслар уз мақсадларига эриша олмаса ва криптотахлилчилар калитни билмасдан туриб, шифрланган ахборотни тиклай олмаса, у ҳолда криптотизим криптомустаҳкам тизим деб айтилади.

Криптотизимнинг мустаҳкамлиги унинг калити билан аникланади ва бу криптотахлилнинг асосий қоидаларидан бири бўлиб ҳисобланади.

Ушбу таърифнинг асосий маъноси шундан иборатки, криптотизим барчаларга маълум тизим ҳисобланиб, унинг ўзгартирилиши кўп вақт ва маблағ талаб қилади, шу боис ҳам фақатгина калитни ўзгартириб туриш билан ахборотни ҳимоялаш талаб қилинади.



Криптография нуктаи – назаридан шифр — бу калит демакдир ва очик маълумотлар тупламини ёпик (шифрланган) маълумотларга узгартириш криптография узгартиришлар алгоритмлари мажмуаси ҳисобланади.

Калит — криптография узгартиришлар алгоритмининг баъзи-бир параметрларининг махфий ҳолати бўлиб, барча алгоритмлардан ягона вариантини танлайди. Калитларга нисбатан ишлатиладиган асосий курсаткич бўлиб криптомустанхкамлик ҳисобланади.

Криптография химоясида шифрларга нисбатан куйидаги талаблар куйилади:

- етарли даражада криптомустанхкамлик;
- шифрлаш ва кайтариш жараёнининг оддийлиги;
- ахборотларни шифрлаш оқибатида улар ҳажмининг ортиб кетмаслиги;
- шифрлашдаги кичик хатоларга таъсирчан бўлмаслиги.

Ушбу талабларга куйидаги тизимлар жавоб беради:

- уринларини алмаштириш;
- алмаштириш;
- гаммалаштириш;
- аналитик узгартириш.

Уринларини алмаштириш шифрлаш усули буйича бошлангич матн белгиларининг матннинг маълум бир қисми доирасида махсус қоидалар ёрдамида уринлари алмаштирилади.

Алмаштириш шифрлаш усули буйича бошлангич матн белгилари фойдаланилаётган ёки бошқа бир алифбо белгиларига алмаштирилади.

Гаммалаштириш усули буйича бошлангич матн белгилари шифрлаш гаммаси белгилари, яъни тасодифий белгилар кетма-кетлиги билан бирлаштирилади.

Тахлилий узгартириш усули буйича бошлангич матн белгилари аналитик формулалар ёрдамида узгартирилади, масалан, векторни матрицага кўпайтириш ёрдамида. Бу ерда вектор матндаги белгилар кетма-кетлиги бўлса, матрица эса калит сифатида хизмат қилади.

Ўринларни алмаштириш усуллари

Ушбу усул энг оддий ва энг қадимий усулдир. Уринларни алмаштириш усулларига мисол сифатида куйидагиларни келтириш мумкин:

- шифрловчи жадвал;
- сеҳрли квадрат.

Шифрловчи жадвал усулида калит сифатида куйидагилар қўлланилади:

- жадвал улчовлари;
- суз ёки сузлар кетма-кетлиги;
- жадвал таркиби хусусиятлари.

Мисол.

Куйидаги матн берилган бўлсин:

КАДРЛАР ТАЙЁРЛАШ МИЛЛИЙ ДАСТУРИ

Ушбу ахборот устун буйича кетма – кет жадвалга киритилади:

К	Л	А	Л	И	Й	Т
А	А	Й	А	Л	Д	У

Д	Р	Ё	Ш	Л	А	Р
Р	Т	Р	М	И	С	И

Натижада, 4x7 улчовли жадвал ташкил килинади.

Энди шифрланган матн каторлар буйича аниқланади, яъни узимиз учун 4 тадан белгиларни ажратиб ёзамиз.

КЛАЛ ИЙТА АЙАЛ ДУДР ЁШЛА РРТР МИСИ

Бу ерда калит сифатида жадвал улчовлари хизмат килади.

Сеҳрли квадрат деб, катакчаларига 1 дан бошлаб сонлар ёзилган, ундаги ҳар бир устун, сатр ва диагональ буйича сонлар йигиндиси битта сонга тенг бўлган квадрат шаклидаги жадвалга айтиллади.

Сеҳрли квадратга сонлар тартиби бўйича белгилар киритилади ва бу белгилар сатрлар бўйича ўқилганда матн ҳосил бўлади.

Мисол.

4x4 улчовли сеҳрли квадратни оламир, бу ерда сонларнинг 880 та ҳар хил комбинацияси мавжуд. Қуйидагича иш юритамиз:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Бошланғич матн сифатида қуйидаги матнни оламир:

ДАСТУРЛАШ ТИЛЛАРИ

ва жадвалга жойлаштирамиз:

И	С	А	Л
У	Т	И	А
Ш	Р	Л	Л
Т	Р	А	Д

Шифрланган матн жадвал элементларини сатрлар бўйича ўқиш натижасида ташкил топади:

ИСАЛ УТИА ШРЛЛ ТРАД

Алмаштириш усуллари

Алмаштириш усуллари сифатида қуйидаги усулларни келтириш мумкин:

- Цезар усули;
- Аффин тизимидаги Цезар усули;
- Таянч сўзли Цезар усули ва бошқалар.

Цезар усулида алмаштирувчи ҳарфлар k ва силжиш билан аниқланади. Юлий Цезар бевосита $k = 3$ бўлганда ушбу усулдан фойдаланган.

$k = 3$ бўлганда ва алифбодаги ҳарфлар $m = 26$ та бўлганда қуйидаги жадвал ҳосил килинади:

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

Мисол.

Матн сифатида КОМПЮТЕР сузини оладиган булсак, Цезар усули натижасида куйидаги шифрланган ёзув хосил булади: НРПСБХWХУ.

Цезар усулининг камчилиги бу бир хил харфларнинг ўз навбатида, бир хил харфларга алмашишидир.

Аффин тизимидаги Цезар усулида хар бир харфга алмаштирилувчи харфлар махсус формула бўйича аникланади: $at+b \pmod m$, бу ерда a, b - бутун сонлар, $0 \leq a, b < m$, ЭКУБ (a, m)=1.

$m=26, a=3, b=5$ булганда куйидаги жадвал хосил килинади:

Т	0	1	2	3	4	5
3т+ 5	5	8	11	14	17	20

6	7	8	9	10	11	12
23	0	3	6	9	12	15

13	14	15	16	17	18	19
18	21	24	1	4	7	10

20	21	22	23	24	25
13	16	19	22	25	2

Шунга мос равишда харфлар куйидагича алмашади:

А	Б	С	Д	Е	Ф	Г	Х
Ф	И	Л	О	Р	У	Х	А

И	Ж	К	Л	М	Н	О	П
Д	Г	Ж	М	П	С	В	Й

Қ	Р	С	Т	У	В	W	Х
Б	Е	Х	К	Н	Қ	Т	W

Й	З
З	С

Натижада юкорида келтирилган матн куйидагича шифрланади:

ЖВПЙЗНКРЕ.

Хозирги вақтда компьютер тармокларида тижорат ахборотлари билан алмашишда учта асосий алгоритмлар, яъни ДЕС, СЛИППЕР ва ПГП алгоритмлари кулланилмоқда. ДЕС ва СЛИППЕР алгоритмлари интеграл схемаларда амалга оширилади. ДЕС

алгоритмининг криптомустахкамлигини куйидаги ммсол оркали хам баҳолаш мумкин: 10 млн. АКШ доллари харажат килинганда ДЕС шифрлаш очиш учун 21 минут, 100 млн, АКШ доллари харажат килинганда эса 2 минут сарфланади. СЛИППЕР тизими СКИПЖАСК шифрлаш алгоритмини уз ичига олади ва бу алгоритм ДЕС алгоритмидан 16 млн, марта кучлирокдир.

ПГП алгоритми эса 1991 йилда Филипп Циммерман (АКШ) томонидан ёзилган ва электрон почта оркали кузатиладиган хабарларни шифрлаш учун ишлатиладиган ПГП дастурлар пакети ёрдамида амалга оширилади, ФГП дастурий воситалари Интернет тармогида электрон почта оркали ахборот жунатувчи фойдаланувчилар томонидан шифрлаш мақсадида кенг фойдаланилмоқда.

ПГП (Преттй Гоод Привасй) криптография дастурининг алгоритми калитли, очик ва ёпик булади.

Очик калит куйидагича курунишни олиши мумкин:

```
EDF2lpI4—BEGIN PGP PUBLIC KEY BLOCK—
Version: 2.6.3i
mQCNazF1lgwAAEEANOVroJEWEq6npGLZTqssS5EScVUPV
aRu4ePLiDjUz6U7aQr
Wk45dIlg0797PFNVpCmRzQZcTxYl0ftyMHL/6ZF9wcx64jy
LH40tE2DOG9yqwKAn
yUDFpgRmoL3pbxXZx9lO0uuzlkAz+xU6OwGx/EBKYOKPTTt
DzSL0AQxLTyGZAAUR
tClCb2lgU3dhbnNvbiA8cmpzd2FuQHNIYXR0bGUtd2Vid29ya
3MuY29tPokAIQMF
h53aEsqJyQEB6JcD/RPxcg6g7tfHFi0Qiaf5yaH0YGEVoxcd-
FyZXr/ITz
rgztNXRUi0qU2MDEmh2RoEcDsIfGVZHSRpkCg8iS+35sAz
9c2S+q5vQxOsZJz72B
LZUFJ72fbC3fZZD9X9lMsJH+xxX9CDx92xm1IglMT25S0X
2o/uBAd33KpEI6g6xv
—END PGP PUBLIC KEY BLOCK—
```

Ушбу очик калит бевосита Веб саҳифаларда ёки электрон почта оркали очикчасига юборилиши мумкин. Очик калитдан фойдаланган жунатилган шифрли ахборотни ахборот юборилган манзил эгасидан бошқа шахс уқий олмайди. ПГП оркали шифрланган ахборотларни очиш учун, суперкомпьютерлар ишлатилганда бир аср хам камлик килиши мумкин.

Булардан ташқари, ахборотларни тасвирларда ва товушларда яшириш дастурлари хам мавжуд. Масалан, С-тооц дастури ахборотларни БМП, ГИФ, WAB кенгайтмали файлларда саклаш учун кулланилади.

Кундалик жараёнда фойдаланувчилар офис дастурлари ва архиваторларни куллаб келишади. Архиваторлар, масалан ПкЗип дастурида маълумотларни пароль ёрдамида шифрлаш мумкин. Ушбу файлларни очганда иккита, яъни лугатли ва тугридан-тугри усулдан фойдаланишади. Лугатли усулда бевосита махсус файлдан сузлар пароль урнига куйиб текширилади, тугридан-тугри усулда эса бевосита белгилар комбинацияси тузилиб, пароль урнига куйиб текиширилади.

Офис дастурлари (Ворд, Ексел, Ассесс) оркали химоялаш умуман тақлиф этилмайди. Бу борада мавжуд дастурлап Интернет да тусиксиз тарқатилади.

Такрорлаш учун саволлар

1. *Замонавий компьютер стенографияси истикболлари.*
2. *Компьютер стенографиясининг асосий вазифалари.*
3. *Конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш учун андай йўналишлар мавжуд?*
4. *Криптографиянинг асосий тушунчаларини таърифлаб бering.*

5. Ахборотларни криптографияли ҳимоялаш тамойиллари.
6. Уринларни алмаштириш ва алмаштириш усуллари қандай криптоизиларга тегишли?

7– МАВЗУ: ЭЛЕКТРОН РАКАМЛИ ИМЗО

1. Ўзбекистонда электрон ракамли имзо хақида тушунча;
2. Электрон ракамли имзо (ери)дан фойдаланиш бўйича ёўрикнома;
3. Электрон ракамли имзо тўғрисидаги конун.

Ўзбекистонда электрон ракамли имзо хақида тушунча;

Ўзбекистон Республикаси Президентининг 2005 йил 8 июлдаги «Ахборот-коммуникатсия технологияларини янада ривожлантиришга оид кўшимча чора-тадбирлар тўғрисида»ги ПК-117 сон Карори билан Ўзбекистон Республикаси алоқа, ахборотлаштириш ва телекоммуникатсия технологиялари давлат кўмитаси Электрон ракамли имзодан фойдаланиш соҳасидаги махсус ваколатланган орган деб белгиланган.

Электрон ракамли имзодан фойдаланиш соҳасидаги махсус ваколатланган органнинг асосий вазибалари ва функциялари:

* электрон ракамли имзодан фойдаланиш бўйича конун ҳужжатлари ва норматив ҳужжатларининг лойиҳаларини ишлаб чиқиш;

* давлат стандартларини ишлаб чиқиш ва белгиланган тартибда тасдиқлаш учун тақдим этиш, халқаро стандартлар жорий қилинишини ташкил қилиш, электрон ракамли имзодан фойдаланиш соҳасидаги тармок стандартлари, техник шартлар ва ушбу соҳадаги воситаларга кўйиладиган талабларни ишлаб чиқиш ва тасдиқлаш;

* электрон ракамли имзони жорий қилиш ва фойдаланиш масалалари бўйича давлат бошқаруви органлари ва хўжалик юритувчи субъектлар фаолиятини мувофиқлаштириш.

Электрон ракамли имзо калитларини Рўйхатга олиш марказларини рўйхатга олиш органининг асосий вазибалари ва функциялари қуйидагилар ҳисобланади:

* электрон ракамли имзо калитларини рўйхатга олиш марказларини белгиланган тартибда давлат рўйхатига олиш;

* электрон ракамли имзо калитларининг сертификатларини электрон ракамли имзо калитларини рўйхатга олиш марказларининг ваколатланган шахсларига бериш;

* электрон ракамли имзо калитларини рўйхатга олиш марказлари ваколатланган шахсларининг электрон ракамли имзо калитлари сертификатларининг ягона давлат реестрини юритиш;

* юридик ва жсмоний шахсларнинг мурожаати бўйича электрон ракамли имзо калитларини рўйхатга олиш марказлари ваколатланган шахсларининг электрон ракамли имзолари хақиқийлигини тасдиқлаш;

* электрон ракамли имзо калитларини рўйхатга олиш марказлари фаолиятининг назоратини амалга ошириш.

Вазифалар ва функцияларини бажаришда Электрон ракамли имзо калитларини рўйхатга олиш марказларининг рўйхатга олиш органи Ўзбекистон Республикасининг «Электрон ракамли имзо тўғрисида»ги Конуни ва Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2005 йил 26 сентябрдаги 215-сон қарори билан тасдиқланган Электрон ракамли имзо калитларини рўйхатга олиш марказларининг давлат рўйхатига олиш тартиби тўғрисидаги низомга амал қилади.

Бугунги кунга келиб, Ўзбекистонда ЭРИ калитларини рўйхатга олиш 10 та Марказ томонидан амалга оширилади. 2012 йилнинг 20 сентябр кунига республикада мавжуд бўлган амалдаги калитлар ва ЭРИ калитларини рўйхатга олиш марказлари томонидан берилган ЭРИ калитлари сертификатларининг умумий миқдори 271717 тани ташкил қилади.

ЕРИ рўйхатга олиш марказларининг реестри

Рўйхатга олиш марказлари сертификатларининг реестри

Аризалар шакллари

Электрон рақамли имзо (ЕРИ)дан фойдаланиш бўйича ёўрикнома

- ЕРИ нима ва у нега керак?
- ЕРИ олиш тартиби ва уни берувчи Марказлар
- ЕРИ кўллаш тартиби (ЕРИ модули (Е-имзо)ни ўрнатиш
- ЕРИ кўллаш соҳасидаги муносабатларни тартибга солувчи норматив-ҳукукий актлар

Хурматли фойдаланувчи!

Ягона портал Сизга Ўзбекистон Республикаси давлат органларига мурожаатларни электрон шаклда юбориш имкониятини тақдим этади. Шунинг билан Сизга эслатиб ўтамизки, электрон мурожаат ЭРИ билан имзоланиши шарт.

ЕРИ - имзонинг ёпик калитини кўллаган ҳолда ахборотнинг криптографик ўзгариши натижасида олинган ва имзонинг шаклланиш вақтидан бошлаб электрон ҳужжатдаги ахборотда ҳаттолик ёўклигини аниқловчи ҳамда имзо калити сертификатини имзо эгасига тааллуқлилигини текширувчи электрон ҳужжатнинг реквизити ҳисобланади.

ЕРИ электрон ҳужжатни имзолаган шахсни идентификатсиялаш учун мўлжалланган бўлиб, кўлда кўйилган имзонинг тўқис аналогини ҳисобланади ҳамда электрон ҳужжатда акс эттирилган ахборотнинг ўзгартирилмаслиги ва авторлигини тасдиқлаш учун кўлланилади. Шунингдек, “Жисмоний ва юридик шахсларнинг мурожаатлари тўғрисида”ги Ўзбекистон Республикаси қонунининг 6-моддасига мувофиқ, ЭРИ билан тасдиқланмаган мурожаатлар аноним мурожаатлар деб ҳисобланади.

ЕРИ олиш тартиби

ЕРИ Ўзбекистон Республикаси Давлат солиқ қўмитасининг Янги технологиялар илмий-ахборот маркази ва унинг ҳудудий бошқармалари томонидан 2 йилга берилади. ЭРИни яқин атрофдаги туман Давлат солиқ инспекцияси (ДСИ)да тўлов асосида олиш мумкин. ЭРИ учун энг кам ойлик иш ҳақининг 10% миқдорида тўлов суммаси ундирилади.

ЕРИ олиш учун қуйидаги ҳужжатларни тақдим этиш лозим:

- ЭРИ калити сертификати ва калитини олиш тўғрисидаги имзоланган ҳамда зарур ҳолларда муҳр билан тасдиқланган ариза (1-илова);

- Аризада кўрсатилган жисмоний шахс ёки юридик шахс вакилининг паспорти;

- ЭРИ калитларини яратиш хизмати учун тўлов тўланганлиги тўғрисидаги қвитантсия.

Эслатма. Аҳолига қулайлик яратиш мақсадида ЭРИ калитларини рўйхатдан ўтказиш учун ЦЛИЦК тизими орқали тўловни амалга ошириш ёўлга кўйилган. Бунинг учун телефонда *880*0113*СТИР*тўлов суммаси# УССД-бўйруғи терилади. Бунда:

СТИР - бу солиқ тўловчининг идентификатсион рақами;

Тўлов суммаси - энг кам ойлик иш ҳақининг 10% миқдорида (2016 йил 1 октябр ҳолатига кўра энг кам ойлик иш ҳақининг 10 фоизи 14 977 сўмни ташкил этади).

ЦЛИЦК орқали тўлов хизмати фақатгина жисмоний шахслар учун мавжуд бўлиб, у ЎЗР ДСИ ва унинг ҳудудий бошқармалари томонидан бериладиган ЭРИ учун амалга оширилади.

Тўлов амалга оширилгандан сўнг яқин ўртадаги ДСИга ташриф буюринг. ЭРИ калитларини ёзиш учун УСБ флеш-картасини олиб боришни унутманг.

ЕРИ модулини ўрнатиш тартиби

Ягона интерактив давлат хизматлари порталида (Ягона портал) электрон рақамли имзодан (ЕРИ) фойдаланилиши учун Э-ИМЗО махсус модули шахсий (иш ёки уй) компютерида ўрнатилиши лозим. Э-ИМЗО модулини ўрнатиш ёўрикномаси билан бу ерда танилиши мумкин. Шунингдек, фойдаланувчи ўзининг шахсий компютерини ЖРЕ нинг 1.7-версиясидан кам бўлмаган версияси ўрнатилганлигига ишонч ҳосил қилиши керак. Компютерда ОРАЦЛЕ ЖРЕ компонентлари мавжудлиги қандай текширилади? <[хтпс://еси.уз/индекс/хелп/жре?ланг=уз](http://esi.uz/index/help/jre?lang=uz)> Агар Сизнинг компютерингизда ЖРЕ иловаси мавжуд бўлмаса, уни ушбу ҳавола орқали юклаб олишингиз мумкин

Еслатма!!! Электрон мурожаатни имзолашда, ДСК томонидан берилган ЭРИ (электрон ракамли имзо) "ДСКЕЙС" номи остидаги папкада компьютернинг Ц ёки Д диск хотирасида (ёки USB флешкада) сакланган бўлиши лозим.

ЭЛЕКТРОН МУРОЖААТНИ ЭЛЕКТРОН РАКАМЛИ ИМЗО ОРКАЛИ ИМЗОЛАШ ТАРТИБИ

Мурожаатни ЭРИ билан имзолаш учун электрон мурожаатни юборишнинг сўнги қадамида «Имзо чекиш» тугмасига босинг.

1. «Имзо чекиш» тугмаси босилганида диалогли ойна очилади, бунда тегишли ЭРИ танланиши лозим.

2. Имзолаш муваффақиятли яқунланган тақдирда экранда «Шакл муваффақиятли имзоланди» ойнаси пайдо бўлади. Кейин «Юбориш» тугмасини босинг.

Мурожаатни ЭРИ ёрдамида имзолаш муваффақиятли яқунланди ва мурожаат тегишли давлат ташкилотига юборилди!

ЕРИ КЎЛЛАШ СОХАСИДАГИ МУНОСАБАТЛАРНИ ТАРТИБГА СОЛУВЧИ НОРМАТИВ-ХУКУКИЙ АКТЛАР

Ўзбекистон Республикасининг “ЭЛЕКТРОН РАКАМЛИ ИМЗО ТЎҒРИСИДА” ГИ КОНУНИ

Ўзбекистон Республикасининг “ЖИСМОНИЙ ВА ЮРИДИК ШАХСЛАРНИНГ МУРОЖААТЛАРИ ТЎҒРИСИДА” ГИ КОНУНИ

Ўзбекистон Республикасининг “ЭЛЕКТРОН ХУЖЖАТ АЙЛАНИШИ ТЎҒРИСИДА” >ГИ КОНУНИ

3. Электрон ракамли имзо тўғрисидаги қонун

(Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси, 2004 й., 1-2-сон, 12-модда)

1-модда. Ушбу Қонуннинг мақсади

Ушбу Қонуннинг мақсади электрон ракамли имзодан фойдаланиш соҳасидаги муносабатларни тартибга солишдан иборат.

2-модда. Электрон ракамли имзо тўғрисидаги қонун ҳужжатлари

Электрон ракамли имзо тўғрисидаги қонун ҳужжатлари ушбу Қонун ва бошқа қонун ҳужжатларидан иборатдир.

Агар Ўзбекистон Республикасининг халқаро шартномасида Ўзбекистон Республикасининг электрон ракамли имзо тўғрисидаги қонун ҳужжатларида назарда тутилганидан бошқача қоидалар белгиланган бўлса, халқаро шартнома қоидалари қўлланилади.

3-модда. Асосий тушунчалар

Ушбу Қонунда қуйидаги асосий тушунчалар қўлланилади:

электрон ракамли имзо - электрон ҳужжатдаги маъмур электрон ҳужжат ахборотини электрон ракамли имзонинг ёпик қалитидан фойдаланган ҳолда махсус ўзгартириш натижасида ҳосил қилинган ҳамда электрон ракамли имзонинг очик қалити ёрдамида электрон ҳужжатдаги ахборотда ҳатолик йўқлигини аниқлаш ва электрон ракамли имзо ёпик қалитининг эгасини идентификация қилиш имкониятини берадиган имзо;

Электрон ракамли имзонинг ёпик қалити - электрон ракамли имзо воситаларидан фойдаланган ҳолда ҳосил қилинган, факат имзо кўювчи шахснинг ўзига маълум бўлган ва электрон ҳужжатда электрон ракамли имзони яратиш учун мўлжалланган белгилар кетма-кетлиги;

Электрон ракамли имзонинг очик қалити - электрон ракамли имзо воситаларидан фойдаланган ҳолда ҳосил қилинган, электрон ракамли имзонинг ёпик қалитига мос келувчи, ахборот тизимининг ҳар қандай фойдаланувчиси фойдалана оладиган ва электрон ҳужжатдаги электрон ракамли имзонинг ҳақиқийлигини тасдиқлаш учун мўлжалланган белгилар кетма-кетлиги;

Электрон ракамли имзонинг ҳақиқийлигини тасдиқлаш - электрон ракамли имзонинг электрон ракамли имзо ёпик қалитининг эгасига тегишлилиги ва электрон ҳужжатдаги ахборотда ҳатолик йўқлиги текширилгандаги ижобий натижа;

Электрон хужжат - электрон шаклда кайд этилган, электрон ракамли имзо билан тасдиқланган ҳамда электрон хужжатнинг уни идентификатсия қилиш имконини берадиган бошқа реквизитларига эга бўлган ахборот.

4-модда. Электрон ракамли имзодан фойдаланиш соҳасини давлат томонидан тартибга солиш

Электрон ракамли имзодан фойдаланиш соҳасини давлат томонидан тартибга солишни Ўзбекистон Республикаси Вазирлар Маҳкамаси ва у махсус ваколат берган орган амалга оширади.

5-модда. Махсус ваколатли орган

Махсус ваколатли орган:

Электрон ракамли имзодан фойдаланиш стандартлари, нормалари ва қоидаларини ишлаб чиқади;

Электрон ракамли имзолар қалитларини рўйхатга олиш марказларини (бундан бўён матнда рўйхатга олиш маркази деб юритилади) давлат рўйхатидан ўтказди;

Рўйхатга олиш марказлари ваколатли шахсларига тегишли электрон ракамли имзолар қалитлари сертификатларининг ягона давлат реестрини юритади ҳамда юридик ва жисмоний шахсларнинг ундан эркин фойдалана олишини таъминлайди;

Рўйхатга олиш марказларининг ваколатли шахсларига электрон ракамли имзолар қалитлари сертификатларини беради;

Юридик ва жисмоний шахсларнинг мурожаатига биноан рўйхатга олиш марказлари ваколатли шахсларининг электрон ракамли имзоси ҳақиқийлигини тасдиқлайди; қонун ҳужжатларига мувофиқ бошқа ваколатларни амалга оширади.

6-модда. Рўйхатга олиш маркази

Рўйхатга олиш маркази махсус ваколатли органда давлат рўйхатидан ўтган ва ушбу Қонунда назарда тутилган вазифаларни бажараётган юридик шахсдир.

Рўйхатга олиш маркази:

Электрон ракамли имзоларнинг ёпик ва очик қалитларини яратади;

Электрон ракамли имзо ёпик қалити муҳофаза қилинишини таъминлайди;

Электрон ракамли имзолар қалитлари сертификатларининг реестрини юритади, унинг ўз вақтида янгиланишини ҳамда ундан юридик ва жисмоний шахсларнинг эркин фойдалана олиш имкониятини таъминлайди;

Юридик ва жисмоний шахсларга электрон ракамли имзолар қалитларининг сертификатларини электрон ҳужжатлар шаклида ва қоғоз ҳужжатлар шаклида беради; электрон ракамли имзолар қалитлари сертификатларининг амал қилишини тўхтатиб туради ва қайта тиклайди, шунингдек уларни бекор қилади;

Юридик ва жисмоний шахсларнинг мурожаатига биноан электрон ракамли имзолар қалитлари сертификатларининг қўчирма нусхалари берилишини, шунингдек электрон ракамли имзолар қалитларининг тўхтатиб турилган ва бекор қилинган сертификатлари тўғрисидаги маълумотлардан эркин фойдаланилишини таъминлайди;

Юридик ва жисмоний шахсларнинг мурожаатига биноан электрон ҳужжатлардаги электрон ракамли имзонинг ҳақиқийлигини тасдиқлайди;

Электрон ракамли имзоли қоғоздаги электрон ҳужжатларнинг қўчирма нусхаларини тасдиқлайди;

Электрон ракамли имзо қалитининг сертификатидан бундан бўён фойдаланиш имкониятига таъсир этиши мумкин бўлган ҳоллар ҳақида электрон ракамли имзо ёпик қалитининг эгасини хабардор қилади;

Электрон ракамли имзо ёпик қалитининг эгаларини электрон ракамли имзодан фойдаланиш қоидаларига ўқитиш имкониятини таъминлайди.

Рўйхатга олиш маркази билан юридик ва жисмоний шахслар ўртасидаги муносабатлар шартнома асосида амалга оширилади.

Рўйхатга олиш марказининг юридик ва жисмоний шахслар учун яратилган электрон ракамли имзоларнинг ёпик қалитларини сақлаши ҳамда электрон ракамли имзо қалитининг сертификатини бериш мақсадига тўғри келмайдиган маълумотларни сўраб олиши тақиқланади.

Рўйхатга олиш марказлари фаолиятининг тартиби Ўзбекистон Республикаси Вазирлар Маҳкамаси томонидан белгиланади.

7-модда. Электрон ракамли имзо билан қўлда ўзи қўйган имзонинг бир хил аҳамиятга эга эканлигини эътироф этиш шартлари

Электрон хужжатдаги электрон ракамли имзо айна бир вақтинг ўзида қуйидаги шартларга риоя этилган тақдирда қоғоз хужжатга қўлда ўзи қўйган имзо билан бир хил аҳамиятга эгадир, агар: электрон ракамли имзонинг ҳақиқийлиги тасдиқланган бўлса; электрон ракамли имзонинг ҳақиқийлиги тасдиқланган пайтда ёки имзолаш пайтини белгилувчи далиллар бўлганда электрон хужжат имзоланаётган пайтда электрон ракамли имзо калитининг сертификати амал қилиб турган бўлса; электрон ракамли имзодан электрон ракамли имзо калитининг сертификатида кўрсатилган мақсадларда фойдаланилаётган бўлса.

8-модда. Электрон ракамли имзо воситалари

Электрон ракамли имзо воситалари электрон хужжатда электрон ракамли имзо яратилишини, электрон ракамли имзонинг ҳақиқийлиги тасдиқланишини, электрон ракамли имзонинг ёпик ва очик калитлари яратилишини таъминлайдиган барча техникавий ва дастурий воситалардан иборат бўлади.

Электрон ракамли имзо воситалари қонун хужжатларида белгиланган тартибда сертификатлаштирилиши лозим.

9-модда. Электрон ракамли имзонинг ёпик калитларини ва очик калитларини яратиш

Электрон ракамли имзонинг ёпик калитлари ва очик калитлари юридик ва жисмоний шахслар томонидан ёки уларнинг муқожаатига биноан рўйхатга олиш маркази томонидан электрон ракамли имзо воситалари ёрдамида яратилиши мумкин.

10-модда. Электрон ракамли имзонинг ёпик калити эгаси

Электрон ракамли имзони яратган (электрон хужжатга имзо қўйган) ва рўйхатга олиш маркази томонидан унинг номига электрон ракамли имзо калити сертификати берилган жисмоний шахс электрон ракамли имзо ёпик калитининг эгаси бўлади.

Электрон ракамли имзо ёпик калитининг эгаси:

электрон ракамли имзонинг ёпик калитидан фойдаланиш устидан назоратни таъминлаши; электрон ракамли имзо калити сертификатини берган рўйхатга олиш марказига электрон ракамли имзонинг ёпик калитидан фойдаланиш режими бузилганлиги ёки бузилиши эҳтимоли борлиги тўғрисида хабар қилиши ва электрон ракамли имзо калити сертификатининг амал қилишини тўхтатиб туришни ёхуд мазкур сертификатни бекор қилишни талаб қилиши; ўзи вакил бўлган юридик шахснинг қайта ташкил этилиши ёки тугатилиши тўғрисида рўйхатга олиш марказига хабар қилиши шарт.

11-модда. Электрон ракамли имзо ёпик калити эгасининг жавобгарлиги

Электрон ракамли имзо ёпик калитининг эгаси ушбу Қонун 10-моддасининг иккинчи қисмида кўрсатилган мажбуриятларни бажармаганлиги оқибатида электрон ракамли имзонинг ёпик калитидан рухсатсиз тарзда фойдаланилиши туфайли этказилган зарар учун тегишли электрон ракамли имзо очик калитининг фойдаланувчиси олдида жавобгар бўлади.

12-модда. Электрон ракамли имзо очик калитининг фойдаланувчиси

Электрон ракамли имзонинг ҳақиқийлигини тасдиқлаш учун электрон ракамли имзонинг очик калитидан фойдаланаётган юридик ёки жисмоний шахс электрон ракамли имзо очик калитининг фойдаланувчиси бўлиши мумкин.

Электрон ракамли имзо очик калитининг фойдаланувчиси электрон ракамли имзонинг очик калити электрон ракамли имзо ёпик калитининг эгасига тегишлилигини ва электрон ракамли имзонинг ҳақиқийлигини текшириш учун электрон ракамли имзо калитининг сертификатини берган рўйхатга олиш марказига муқожаат этишга, шунингдек электрон ракамли имзонинг ҳақиқийлиги тасдиқланмаган ҳоллар ҳақида электрон ракамли имзо ёпик калитининг эгасига хабар қилишга ҳақли.

Электрон ракамли имзо очик калитининг фойдаланувчиси электрон ракамли имзо ёпик калити эгасининг шахси тўғрисидаги маълумотлар муқофаза қилинишини таъминлаши керак.

13-модда. Электрон ракамли имзо калитининг сертификати

Электрон ракамли имзо калитининг сертификати электрон ракамли имзонинг очик калити электрон ракамли имзонинг ёпик калитига мослигини тасдиқлайдиган ва электрон ракамли имзо ёпик калитининг эгасига рўйхатга олиш маркази томонидан берилган хужжатдан иборат бўлади. Электрон ракамли имзо калитининг сертификати электрон хужжат шаклида ва қоғоз хужжат шаклида тайёрланиши мумкин.

Электрон ракамли имзо калитининг сертификатида қуйидагилар кўрсатилиши керак: электрон ракамли имзо ёпик калитининг эгаси бўлган жисмоний шахснинг фамилияси, исми, отасининг исми;

агар электрон ракамли имзо ёпик калитининг эгаси юридик шахснинг вакили бўлса, шу юридик шахснинг номи;
унинг тартиб раками ва амал килиш муддати;
электрон ракамли имзонинг очик калити;
электрон ракамли имзонинг очик калитидан фойдаланишда ёрдам бериши мумкин бўлган электрон ракамли имзо воситаларининг номи;
мазкур сертификатни берган рўйхатга олиш марказининг номи ва жойлашган манзили;
электрон ракамли имзодан фойдаланиш мақсадлари тўғрисидаги маълумотлар;
электрон ракамли имзолар калитлари сертификатлари реестрининг электрон манзили.
Электрон ракамли имзо ёпик калитининг эгаси ташаббуси билан электрон ракамли имзо калити сертификатига бошқа маълумотлар ҳам киритилиши мумкин.

14-модда. Электрон ракамли имзо калитининг сертификатини бериш

Электрон ракамли имзо калитининг сертификати рўйхатга олиш маркази томонидан берилади.

Электрон ҳужжат шаклидаги электрон ракамли имзо калитининг сертификати берилаётганда у рўйхатга олиш маркази ваколатли шахсининг электрон ракамли имзоси билан тасдикланади.

Қоғоз ҳужжат шаклидаги электрон ракамли имзо калитининг сертификати икки нусхада расмийлаштирилади. Бундай сертификатнинг ҳар бир нусхаси рўйхатга олиш марказининг ваколатли шахси томонидан имзоланиши ва рўйхатга олиш марказининг муҳри билан тасдикланиши керак. Электрон ракамли имзо калити сертификатининг бир нусхаси электрон ракамли имзо ёпик калитининг эгасига берилади, бошқа нусхаси эса рўйхатга олиш марказида сақланади.

Электрон ҳужжатлар шаклидаги электрон ракамли имзолар калитлари сертификатларининг кўчирма нусхаларини беришга доир хизматлар рўйхатга олиш маркази томонидан бепул кўрсатилади.

15-модда. Электрон ракамли имзо калити сертификатининг амал килишини тўхтатиб туриш

Электрон ракамли имзо калити сертификатининг амал килиши электрон ракамли имзо ёпик калити эгасининг аризаси асосида, аризада кўрсатилган муддатга, лекин мазкур сертификатнинг амал килиш муҳлатидан кўп бўлмаган муддатга рўйхатга олиш маркази томонидан тўхтатиб турилиши мумкин.

Электрон ракамли имзо ёпик калити эгасининг электрон ракамли имзо калити сертификатининг амал килишини тўхтатиб туриш тўғрисидаги аризаси тушганда рўйхатга олиш маркази электрон ракамли имзолар калитлари сертификатларининг реестрига тегишли ёзув киритади ва айни бир вақтнинг ўзида бу ҳақда электрон ракамли имзо ёпик калитининг эгасини хабардор қилади.

Электрон ракамли имзо калити сертификатининг амал килиши тўхтатиб турилган муддат ичида рўйхатга олиш маркази электрон ракамли имзо ёпик калити эгасининг аризасига биноан мазкур сертификатнинг амал килишини қайта тиклаши мумкин.

16-модда. Электрон ракамли имзо калитининг сертификатини бекор қилиш

Электрон ракамли имзо калитининг сертификати электрон ракамли имзо ёпик калити эгасининг аризаси асосида рўйхатга олиш маркази томонидан бекор қилиниши мумкин.

Рўйхатга олиш маркази, электрон ракамли имзо ёпик калити эгасининг розилигидан қати назар, қуйидаги ҳолларда электрон ракамли имзо калитининг сертификатини бекор қилиши шарт, агар:

мазкур сертификатнинг амал килиш муддати тугаган бўлса;

электрон ракамли имзо калитининг сертификати берилишига асос бўлган ҳужжатнинг амал килиши тугатилганлиги аниқ маълум бўлса;

электрон ракамли имзо ёпик калитининг эгаси ушбу Қонун 10-моддасининг иккинчи қисмида назарда тутилган ўз мажбуриятларини бажармаган ҳоллар аниқланган бўлса.

Электрон ракамли имзо калити сертификатининг амал килишини тўхтатиб туриш муддати тугаган ва электрон ракамли имзо ёпик калити эгасининг уни қайта тиклаш ҳақида аризаси бўлмаган тақдирда ҳам электрон ракамли имзо калитининг сертификати бекор қилиниши керак.

Электрон ракамли имзо калитининг сертификатини бекор қилиш электрон ракамли имзо ёпик калити эгасининг аризаси олинган ёки ушбу модданинг иккинчи ва учинчи қисмларида баён қилинган ҳолатлар юзага келган кунда рўйхатга олиш маркази томонидан амалга оширилади.

Электрон ракамли имзо калитининг сертификатини бекор килиш тўғрисидаги ёзув рўйхатга олиш маркази томонидан электрон ракамли имзолар калитлари сертификатларининг реестрига киритилиб, бу ҳақда электрон ракамли имзо ёпик калитининг эгаси хабардор қилинади.

17-модда. Электрон ракамли имзо калитининг сертификатини рўйхатга олиш марказида сақлаш тартиби

Электрон ҳужжат шаклидаги электрон ракамли имзо калитининг сертификатини рўйхатга олиш марказида сақлаш тартиби ҳамда муддати рўйхатга олиш маркази ва электрон ракамли имзо ёпик калитининг эгаси ўртасидаги шартнома билан белгиланади.

Электрон ҳужжат шаклидаги электрон ракамли имзо калитининг бекор қилинган сертификати рўйхатга олиш марказида қамада уч йил сақланади.

Электрон ҳужжат шаклидаги электрон ракамли имзо калитининг сертификатини сақлаш муддати тугаганидан кейин, у рўйхатга олиш марказининг электрон ракамли имзолар калитлари сертификатларининг реестридан чиқарилади ва архивда сақлаш режимида ўтказилади.

Қўғоз ҳужжат шаклидаги электрон ракамли имзо калитининг сертификати қонун ҳужжатларида белгиланган тартибда сақланади.

Электрон ракамли имзо калитининг сертификати йўқолган тақдирда, рўйхатга олиш маркази электрон ракамли имзо калити сертификатининг дубликатини бериши мумкин.

18-модда. Рўйхатга олиш марказини тугатиш

Рўйхатга олиш маркази қонун ҳужжатларида белгиланган тартибда тугатилиши мумкин.

Рўйхатга олиш маркази тугатиш тўғрисида қарор қабул қилинган пайтдан эътиборан бир ой мобайнида бу ҳақда махсус ваколатли органга, шунингдек мазкур рўйхатга олиш марказининг электрон ракамли имзолар калитлари сертификатларининг реестрига киритилган электрон ракамли имзо ёпик калитларининг барча эгаларига хабар қилиши шарт.

Рўйхатга олиш маркази тугатилган тақдирда, мазкур рўйхатга олиш маркази томонидан берилган электрон ракамли имзолар калитларининг сертификатлари электрон ракамли имзо ёпик калитлари эгаларининг розилиги билан бошқа рўйхатга олиш марказларига топширилиши мумкин.

Бошқа рўйхатга олиш марказларига топширилмаган электрон ракамли имзолар калитларининг сертификатлари бекор қилинади ва махсус ваколатли органга сақлаш учун топширилиб, бу ҳақда электрон ракамли имзолар очик калитларининг фойдаланувчилари хабардор қилинади.

19-модда. Чет давлатларнинг электрон ракамли имзолар калитлари сертификатларидан фойдаланиш

Чет давлатларнинг электрон ракамли имзолар калитлари сертификатларидан фойдаланиш қонун ҳужжатларида белгиланган тартибда амалга оширилади.

20-модда. Мухр ўрнида ишлатиш

Мухр билан тасдиқланган ва электрон ҳужжатга айлантирилган қўғоз ҳужжатнинг мазмуни қонун ҳужжатларига ёки тарафларнинг қелишувига мувофиқ рўйхатга олиш маркази ваколатли шахсининг электрон ракамли имзоси билан ёки электрон ракамли имзо ёпик калити эгасининг электрон ракамли имзоси билан тасдиқланиши мумкин.

21-модда. Низоларни ҳал этиш

Электрон ракамли имзодан фойдаланиш соҳасидаги низолар қонун ҳужжатларида белгиланган тартибда ҳал этилади.

22-модда. Электрон ракамли имзо тўғрисидаги қонун ҳужжатларини бузганлик учун жавобгарлик

Электрон ракамли имзо тўғрисидаги қонун ҳужжатларини бузганликда айбдор шахслар белгиланган тартибда жавобгар бўладилар.

Фойдаланувчи учун қўлланма

Ҳужжат тўғрисида

Илтимос, ҳар қандай ҳатолар ёки тақлифлар ҳақида бизга хабар беринг. Тизим бугунги кунда жуда катта ва кичик ўзгаришларни бошидан кечирмоқда - бу ҳужжат Фактура.уз сайтидаги янгиликларни акс эттира олмайди. Шунинг учун тизимда ва фойдаланувчи қўлланмасида фарқ бўлиши мумкин, бундай ҳолларда ҳақиқат устунликка эга.

Мазмун

1. Ишга киришиш
1. Махсус модул электрон имзо
2. ЕРИ сертификати
1. Тизимда ишлашнинг соддалаштирилган сценарийси
2. ЁКошимча дастур
3. ЁТизимда ройхатдан отиш
4. Хисобингизни фаоллаштиринг
5. ЁРеквизитларни толдириш
6. Хамкорларнинг таклифи
2. Тизим интерфейси
3. Тизимнинг функционаллиги
1. Хужжатларни саклаш
2. Сават кандай ишлайди?
3. Хужжатлардаги имзоларни текшириш
4. ЁАтамалар ва тарифлар

Ишга киришиш

Биз тизимнинг ишлашини тушуниш учун, Фактура.уз модуллари коғоз хужжатларининг айланиши ва кайта ишлаш модулларини ишлаб чиқишни таклиф қиламиз. Тизимда қирувчи, чикувчи, коралама(), бўлимлари мавжуд, шу билан биргаликда тизимда хужжатларни ўчириш ва уларни кайта тиклаш имкониятлари бор.

Тизим билан ишлашнинг видео дарслари. Файллар мовер.уз (ТАСИХ) ва ёутубе.цом сайтларида сакланади.

Тизимда ишлаш учун нима керак?

1. ЕРИ билан ишлаш учун махсус модул электрон имзо. Юклаб олинг. <[хтttp://филес.фактура.уз/Е-ИМЗО-в3.41.exe](http://филес.фактура.уз/Е-ИМЗО-в3.41.exe)>.
2. Сизнинг ва хамкорларингизнинг солиқ хизмати томонидан бериладиган ўзбекча намунадаги электрон ракамли имзо сертификати.
3. Тизимда сиз ва хамкорларингизнинг рўйхатдан ўтиши.

Махсус электрон имзо модули

Электрон ракамли имзо системаси Ўзбекистонда ишлаб чиқилган бўлиб, ўзига хос алгоритмда ишлайди. Шу боис дунёдаги етук дастурий таминоат компаниялари хусусан Мицрософт, Мозилла, Гоогле ва шу қабилар Ўзбек алгоритми билан ишлаш модулларини такдим қилишга шошилаётгани йўқ. Яъни дунё микёсидаги электрон ракамли имзо тизими Ўзбекистонда ишлаб чиқарилган тизим билан фарқ қилгани учун, сизга бизнинг тизимни Э-имзо (юқоридаги хаволадан юклаб олиш мумкин) модули орқали ишлатишни тавсия этамиз. Файл ТАС-ИХ тармоғ`ида жойлаштирилган.

Корхоналарнинг бухгалтерлари электрон ракамли имзо сертификатларини ўзбек стандарти ёрдамида бир неча йиллар давомида давлат органларига ҳисобот топшириб келаётганлилари сабабли, Фактура.уз тизимини ишлатиш жараёнида ҳеч қандай қийинчиликлар юзага келмаслигига умид қилиб қоламиз.

Фирефокс браузерни учун қўшимча ўрнатиш босқичлари

- Фойдаланувчи браузерини энг сўнгги версиясига ўрнатинг ёки янгиланг.
- [Хтtps://127.0.0.1:64443](https://127.0.0.1:64443) манзилини очинг ва «Мен хавфни тушунаман» («Я понимаю риск») тугмасини босинг ва кейин «Истисно қўшиш» («Добавить исключение») тугмасини босинг.

ЕРИ сертификати

«Фактура.уз» тизими Ўзбекистон Давлат солиқ қўмитаси томонидан берилган ЭРИ сертификатларидан фойдаланади. Қўшимча маълумот учун [хтtps://солик.уз/уз/интерактиве/электрон_ракамли_имзо/](https://солик.уз/уз/интерактиве/электрон_ракамли_имзо/) га мурожаат қилинг.

Тизимда ишлашнинг соддалаштирилган сценарийси

Биз бир марта системанинг қандай ишлашини сўрашди. Биз қуйидагича қискача жавоб бердик: ҳар биримиз учун фойдали бўлади деб ўйлаймиз:

Савол: Сизнинг ресурсингиздан фойдаланиб, юридик шахс билан масофадан туриб шартномани имзолашим ва хизматим учун ҳақ олишим мумкинми?

Жавоб:

Иккала компания ҳам тизимда рўйхатдан ўтишлари керак:

- рўйхатдан ўтиш маълумотларини тўлдириш (ИНН, банк коди ва бошқалар);
- электрон почта манзилини фаоллаштириш;
- ЕРИ сертификатларини юклаб олиш;
- тизим томонидан юборилган таклифни имзолаш.

Тизимни тўлик қабул қилингандан сўнг ва оммавий офёртани имзолаб, бир тараф Менюдан (Новый документ) ҳужжатнинг сўнги вариантини юклайди. Сизнинг тарафингиздан (ИНН рақамингиз бўйича қидириш ёки қорхона номи бўйича қидирув) ва ҳужжатни имзолаш ва жўнатиш тугмаси босилади. Контрагент ҳужжатни қабул қилади ва рози бўлса ҳужжатни имзолайди. Бундан сўнг 3 тамонлама имзоланган шартнома (икки контрагент ва Система) ҳужжат

Архив папкасига жойлаштирилади.

Бундан ташқари, видео материалларни бизнинг сайтимида қўришингиз мумкин.

ЕРИ сертификатлари билан имзоланган ҳужжатда шартнома рақами ва саналари кўрсатилган. Ушбу маълумот асосида тўловчи банк ўтказмаси шаклини тўлдиради ва пулни ижрочиға ўтказиши. Шунда фактуралар орқали фактураларни ва бажариладиган ҳужжатларни юборишингиз мумкин.

Қўшимча дастур

Ҳужжатларни pdf форматда қўриш учун сизнинг компютерингизга тегишли дастурий таъминотни, масалан, Адобе Акробат Редер дастурини ўрнатишни тавсия қиламиз. Имзоланган ҳужжатлар, сертификатлар ва рақамли имзонинг ўзи zip архивларида сақланади. Ушбу архивларни қўриш ва очиш учун тизимингизда ўрнатилган бўлмаса zip архивлари билан ишлаш учун қўшимча дастурларга эҳтиёж сезилади.

Тизимда рўйхатдан ўтиш

Тизимда рўйхатдан ўтиш жараёни жуда осон ва енгил. Фойдаланувчиларни рўйхатдан ўтказиш жараёнини янада содда ва қулай қилиш учун биз рўйхатдан ўтишнинг иккита усулини тақдим этдик. Сертификат орқали тизимда рўйхатдан ўтишингиз ёки керакли майдонларни қўлда тўлдиришингиз мумкин.

Тизимда рўйхатдан ўтиш учун апп.фактура.уз/Аццоунт/Регистер <<http://апп.фактура.уз/Аццоунт/Регистер>> саҳифасига ўтинг. Ёки бизнинг веб-саҳифамизга қиринг, кейин рўйхатдан ўтиш саҳифасига ўтиш учун рўйхатдан ўтиш тугмасини босинг. Рўйхатга олиш саҳифасида, сизнинг ташкилотингиз маълумотларини кўрсатиши керак бўлган шаклни, шунингдек ҳисобингиз учун қириниш маълумотларини кўрасиз.

КАЙД:

Бизнинг тизимимизни ишлатишдан олдин Э-имзонинг энг сўнги версияси компютерингизда ўрнатилганлигига ишонч ҳосил қилинг. Бундан ташқари, Э-имзо ишлаш учун компютерингизда қамида этгинчи Жава-версиясини ўрнатиш керак.

Қейинчалик, тизимга босқичма-босқич топширилади.

(1) Браузерда <https://апп.фактура.уз/аццоунт/регистер> саҳифасига ўтинг.

(2) Тўлдириш шарт бўлган (Юлдузча билан кўрсатилган: *) қисмлар тўлдирилса форма юкланади.

Сертификатингиздан фойдаланиб рўйхатдан ўтинг

Сертификатдан фойдаланиб рўйхатдан ўтиш учун, рўйхатдан ўтиш ойнасида «ЕРИ ёрдамида рўйхатдан ўтиш» белгисини белгиланг.

Қейин очиладиған рўйхатда сертификатни танланг.

Сертификатингизни танлагандан сўнг, қуйидаги майдонларни сертификат маълумотингиз автоматик равишда тўлдирилади:

- Ташкилотнинг ИННси.
- Ташкилот номи.
- Фамилияси.
- Исм.
- Отасининг исми.

Юқоридаги майдонлар тизимдаги параметрлардан ўзгартирилиши мумкин.

Қуйидаги жойларни қўлда кўрсатиш керак бўлади:

- Е-почта манзили.
- Парол.
- Паролни қайта қиритинг.

- Мобил телефон раками.

Рўйхатга олиш жараёнини тугаллаш учун сиз «Оммавий офёртани ўқидим ва тўлик қабул қиламан» кутисини белгилашингиз керак.

Хисобингизни фаоллаштиринг

Кейинги қадам хисобни фаоллаштиришдир. Рўйхатдан ўтиш вақтида берган электрон почта манзилига ўтинг. Фактура.уз тизимидан активлаштириш учун ҳаволали мактуб олдингиз. Ҳеч хабар бўлмаса, бироз кутинг ёки электрон почта бўлимларидаги «Спам» жилдини текширинг.

Мактубни очинг ва «Манзилни тасдиқланг ва рўйхатдан ўтказинг!» тугмачасини босинг.

Тизим хисобингизни (хисоб қайдномасини) фаоллаштиради.

Ўз аккаунтингизни фаоллаштирганингиздан сўнг, дастурга кириш учун [хтtps://app.фактура.уз](https://app.фактура.уз) манзилига ўтинг

Тафсилотларни тўлдириш ва ЭРИ сертификатини қўшиш

Кейинги қадам - ЭРИ сертификатингизни қўшиш ва компаниянгизнинг барча банк ва ташкилий тафсилотларини тўлдиришдир. Барча керакли модулларни ўрнатганингизга ва сертификат (иккита файл ёки битта файл) ҳар қандай каттик дискнинг илдиз каталогида эканлигига ишонч ҳосил қилинг.

Корхонангизни банк реквизитларини толдиринг:

- Хисоб рақамини киритинг.
- Банкингизнинг МФО кодини киритинг.
- Банк номи сиз тақдим қилган МФО коди бўйича автоматик равишда кўрсатилади.

Махсус ҳисоб тўлдириш ихтиёрий. Агар сиз ушбу ҳисобга эга бўлмасангиз, ушбу майдонни ўтказиб юборинг.

Сўнг қуйидаги майдонни тўлдиринг ва сертификатингизни юкланг

- ОКОНХ коди
- ОКЕД учун код
- Давлат
- Вилоят
- Туман
- Кўча
- Уй
- Индекс

Сертификатни юклаш

Сертификатни юклаш учун системадаги сертификатингизни кераклиги ҳақидаги ҳаволани босинг ёки соғлама орақали юклашингиз мумкин

2016-йил август ойидан бошлаб Ўзбекистон Республикаси СТК қошидаги асосий рўйхатга олиш маркази пфх кенгайтмаси билан янги турдаги сертификатга ўтишни бошлади. Агар махсус электрон имзо модули ўрнатилган бўлса, тизим ушбу турдаги сертификат учун паролни сўрайди.

Оммавий офёртани имзолаш

Тизимдаги барча хизматлардан тўлақонлик фойдаланиш учун сиз оммавий офёртани имзолашингиз керак бўлади.

Таклифни имзолаш учун огоҳлантириш хабаридаги ҳаволани босинг ёки Киручи ҳужжатлар болими га ўтинг ва шартнома ҳужжатини топинг.

Ҳужжатни очинг, ва «Имзо ва юбориш» тугмасини босинг.

«Имзолаш ва Жонатиш» тугмасини босганингиздан сўнг ойна очилади. Сиз ушбу янги очилган ойнада ўз сертификатингизни танлашингиз керак.

Ҳамкорларнинг таклифи

Сизнинг бизнес ҳамкорларингиз (контрагентлар) ҳали Фактура.уз тизимида рўйхатдан ўтмаган бўлса, сиз уларни тизимга аъзо бўлишга таклиф қилишингиз мумкин. Ушбу нуктада Янги ҳужжат / Ҳужжат саҳифасида «Таклиф» тугмасини босинг.

Контакт маълумотларини киритинг ва «Таклифни жўнатиш» тугмасини босинг.

Тизим интерфейси

Электрон хужжат айланиши тизими билан ишлашнинг асосий интерфейси ыб-браузердир.

Интерфейс оддий ва ишлатиш учун кулай. Меню панели фойдаланувчи ўзи излаётган нарсаларни осонликча топиши учун мўлжалланган.

Тизимнинг функционалиги

Жўнатилмаган хужжат, биринчи навбатда, “Черновиклар “ папкасида яратилади, кейин контрагентга юборганингиздан сўнг, “Чикувчи”(Исходящие) папкасига ўтади.Контрагентнингиз жавоб берганидан сўнг “Кирувчи”(“Входящие”) папкага отади ва хужжат иккала томон томонидан Имзолангандан кейин “Архив”(“Архив”) папкасига отади. Хужжатнинг имзоланган версияси ёки юбориш учун имзоланган хужжат сифатида юборилиши мумкин.

Компаниянинг бошқа ходими билан келишиш учун юборилган хужжатлар «Рухсатнома»(«Согласование») папкасида жойлашган.

Хужжатларни сақлаш

Тизим имзоланган хужжатларни оммавий оферта белгиланган муддатда сақлашни режалаштирмакда. Шу билан бирга, биз имзоланган хужжатларнинг архивларини шахсий компютерларингизда сақлаймиз. Бунда куйидаги фикрлар сабабли бажариш керак.

- Фактура.уз маълумотлар сақлаш тизими эмас. Агар имзоланган электрон хужжатингиз бўлса, маълум бир вақт давомида сақланади. Агар лимит ёки сақлаш муддати ошиб кетган бўлса, хужжат автоматик равишда ўчирилади. Шундай қилиб, сиз ўзингизнинг манбаларингизга электрон хужжатларни сақлаш жараёнигизга катъий риоя қилишингиз керак.

- Фавқулудда вазиятлар юзага келиши мумкин, шунинг учун хужжатларингизни нусхаларини яратинг.

- Хар бир фирма хужжатларни сақлаш тартиби, лойиҳалар бўйича қимдир, қимгадир йил ва бошқалар. Аммо, Фактура.уз тизимида, имзоланган барча денгиз қисмлари «Архив» да сақланади, бу маълум бир даражага етганидан кейин ноқулайликка олиб келади. Шунинг учун хужжатни дастлаб ўзингиздан сақлашга ҳаракат қилинг.

Имзоланган электрон хужжат ЗИП архив файлининг ичида жойлашган хизмат маълумотлари билан биргаликда сақланади. Бундан ташқари, хужжатларни қўриш учун Адобе Акробат Редер ёки бошқалар каби ПДФ форматини қўллаб-қувватлайдиган дастур керак.

Сават қандай ишлайди?

Саватдан хужжатларни қайта тиклаб олиш

Саватка 4 хил қўринишдаги Электрон рақамли имзоланган хужжатлар тушиши мумкин.

(А) Бировнинг имзосиз хужжати (Б)Қарши томонга имзо қўймасдан ўз имзоси бўлган хужжат

(Ў) Қарши томоннинг имзоси билан ўз имзоси бўлмаган хужжат (Д) Ўз имзоси ва қарши томоннинг имзоси бўлган хужжат

Вариант (Ў) Қайта ишлаб чиқариш қутисидан тикланиши мумкин эмас. Агар контрагент сизни аллақачон имзоланган хужжатни юборса, сиз уни имзолашни рад этган сиз ва уни ўчириб қўйишингиз мумкин, лекин сиз ушбу хужжатнинг мазмунини қўришингиз мумкин.

Уни саватдан олиб ташлаш мумкинми?

Ҳа, сиз хужжатларни саватдан йўқ қилишингиз мумкин. Хужжатнинг ҳолатига қараб, тизим ва қарши томоннинг ўз нусхалари бўлиши мумкин.

Хужжатлардаги имзоларни текшириш

Хужжатни ва ЭРИ ни ўз ичига олган архивни текшириш учун куйидаги хаволани ишлатинг:

Ушбу линк фактура.уз ахборот сайтида ва тизимнинг манзили - апп.фактура.уз да такрорланади.

Адабиётлар:

1. Р.Х. Алимов, Б.Ю. Ходиев, К.А. Алимов, С.У. Усмонов, Б.А. Бегалов, Н.Р. Зайналов, А.А. Мусалиев, Ф. Файзиева, «Миллий иқтисодда ахборот тизимлари ва технологиялари», Ўқув қўлланма, Т. Шарқ, 2004 йил.
2. М.Т. Гафурова, Д.Ч. Дурсунов, В.И. Рапопорт, Б.Ю. Ходиев. Проектирование современных информационных технологий. Учебное пособие.-Тошкент, ТДИУ, 1994.-96 с.
3. Информационные системы в экономике: Учебник/Под ред. проф. В.В. Дика.-М.:Финансы и статистика,1996.-272 с.
4. Информатика: Учебник/Под ред. Н.В. Макаровой. -М.: Финансы и статистика, 1997.-768с.
5. Ғуломов С.С. ва бошқ. Иқтисодий информатика: Олий ўқув юртлирининг иқтисодий мутахассисликлари учун дарслик. —Т.: «Ўзбекистон», 1999. —528 б.
6. Козырев А.А. Информационные технологии в экономике и управлении: Учебник, 2-е изд. .—СПб.: Изд-во Михайлова В.А., 2001. —360 с.
7. Ходиев Б.Ю., Мусалиев А.А., Бегалов Б.А. Введение в информационные системы и технологии. Учебное пособие /Под ред. акад. С.С. Гулямова. —Т.:ТГЭУ, 2002. —156 с.
8. Шафрин Ю.А. Информационные технологии. —М.: Лаборатория Базовых Знаний, 1998. —704 с.
9. Петров Б.Н. Информационные системы. – СПб.: Питер, 2003. – 688с.:ил.

Кушимча адабиётлар:

1. Денинг В., Эссиг Г., Маас С. Диалоговые системы "Человек-ЭВМ". Адаптация к требованиям пользователя: Пер. с англ.- М.: Мир,1984.-112 с.,ил.
2. Компьютерлаштиришни янада ривожлантириш ва ахборот коммуникацион технологияларини жорий этиш туғрисида \Хабарнома. – 2002, №2.
3. Гафурова М.Т., Дурсунов Д.Ч. Стандартизация оформления дипломных, курсовых проектов и лабораторных работ: Методические указания.—Т.: ТДИУ,1988.—80 б.
4. Острейковский В.А. Информатика. М.: Высшая школа, 1999.
5. ИБМ ПС для пользователя. Фигурнов В.Э. М.: Инфра, 2001.
6. Рахмонкулова С.И. Шахсий компьютерда ишлаш. Тошкент - “Шарк”, 1998.
7. Джой Крейнак. Интернет. Санкт-Петербург, Питер, 1999.
8. www.питер.com
9. www.интуит.ру
10. www.ит-студй.ру
11. www.информатика.ру
12. www.еду.уз
13. www.реф.уз

6. АМАЛИЙ МАШГУЛОТЛАРГА ДОИР УСЛУБИЙ КЎРСАТМАЛАР

**ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА
МАХСУС ТАЪЛИМ ВАЗИРЛИГИ**

САМАРҚАНД ДАВЛАТ УНИВЕРСИТЕТИ

«Ахборотлаштириш технологиялари» кафедраси

**“АХБОРОТЛАРНИ ҲИМОЯЛАШ”
фанидан бакалавр йўналишлари талабалари учун
амалий ишларини бажариш бўйича**

УСЛУБИЙ КЎРСАТМА

Тузувчилар:

доцент И.Н. ТУРАКУЛОВ

ассистент И.К. ХИММАТОВ

Самарқанд – 2017

Ушбу услубий кўрсатма компьютер тизимлари ва тармоқларида ахборот хавфсизлигини таъминлаш билан боғлиқ масалаларни ечишда ахборотни ҳимоялаш технологияларининг ўрганиш ва кўриб чиқиш каби масалаларини қамрайди.

Услубий кўрсатмада лаборатория машғулотларига оид назарий маълумотлар, лаборатория машғулотлари топшириқлари мужассамлаштирилган. Бу лаборатория машғулоти талабаларни ахборотни криптографик ҳимоялаш усуллари: симметрик ва ассиметрик шифрлаш ва маълумотларни тармоқда хавфсизлигини таъминлаш масалалари устида тўхталиб ўтилган. Унда талабанинг билимини мустаҳкамлаш учун ўз-ўзини текшириш назорат саволлари ва адабиётлар рўйхати келтирилган.

Ушбу услубий кўрсатма “Ахборотлаштириш технорлогиялари” кафедраси мажлисида кўриб чиқилган ва маъқулланган.

(____ 2017 йил ____-баённома)

Услубий кўрсатма “Механика-математика” факультетининг илмий-услубий кенгашида тасдиқланган.

(____ 2017 йил ____-баённома)

Услубий кўрсатма Самарқанд давлат университети илмий-услубий Кенгашида тасдиқланган.

(____ 2017 йил ____-баённома)

©Самарқанд давлат университети, 2017 й.

КИРИШ

Компьютер технологияларининг, айниқса Интернетнинг жадал суръатлар билан кенг тарқалиши натижасида тармоқда маълумотларнинг кескин кўпайишига олиб келди. Бу маълумотларни тармоқда ҳимоялашда (маълумотлардан ижозатсиз фойдаланишнинг олдини олиш мақсадида) криптография усулларида фойдаланиш ва уларнинг янги алгоритмларни ишлаб чиқиш замонавий ҳамда актуал муаммолардан бири бўлиб ҳисобланади.

Компьютер технологияларининг тараққиёти криптографиянинг қўлланиш соҳасини кенгайтириб унга янги масалаларни қўйди.

Ҳозирги вақтда маълумотларни шифрлашда криптографик алгоритмларидан фойдаланиш мураккаб бўлмаган масалалардан бири бўлиб ҳисобланади. Чунки замонавий юқори босқичли алгоритмик тилларда яратилган дастурлар орқали берилган маълумотларни шифрлаб керакли жойга тармоқда узатиш тизимлари кўплаб яратилган ва улар фойдаланувчиларга қўл келмоқда. Аммо тармоқдаги криптографик усуллар билан шифланган маълумотларни очиш ва уларни бузиш ҳоллари ҳам мовжуд. Буларни олдини олиш мақсадида криптографик усулларнинг янги динамик алгоритмларини ишлаб чиқиш мақсадга мувофиқдир.

Ҳозирги вақтда криптографиянинг икки ишлатилиш соҳаси мовжуд: маълумотларни узатишда ҳимоялаш ва уларни сақлашда ҳимоялаш. Уларнинг ҳар бири криптографияга ўзининг хусусий талабларини қўяди ва муайян масалалар ечимида ўз тасдиғини топади.

1. Қисм. Назарий асослар

§1.1. Криптография

Маълумотларнидан ижозатсиз фойдаланишнинг олдини олиш мақсадида уни ўзгартириб ифодалаш қадимдан маълум. Унинг кўп сонли йўллари ва усуллари ишлаб чиқилган, такомиллаштирилган ҳамда улардан фойдаланиб келинмоқда. Информатика ва информацион технологияларнинг ривожланиши бу процесснинг тезлашига туртки бўлди. Бунинг асосий сабабларидан бири глобал тармоқларнинг пайдо бўлиши ва улардаги коммерцион (давлатлараро, харбий, иқтисодий, комерцион ва шахсий характерли) маълумотларни ўз вақтида ҳимоялаш, иккинчи томондан эса янги кучли компьютерларнинг ҳамда тармоқ технологияларининг ривожланиши натижасида кечаги очилиши мумкин бўлмаган криптографик тизимнинг ечими топилишидир.

Маълумотларни шакл ўзгартириш орқали ҳимоялаш муаммолари билан криптология (*крйитос* - яширин, *логос* - фан) ўрганади. Криптологиянинг маълумотларни ўзгартириб ифодалашнинг янги математик усулларини топиш ва улар устида изланишлар олиб боровчи бўлими криптография дейилади.

Компьютер технологияларининг, айниқса Интернетнинг жадал суръатлар билан кенг тарқалиши натижасида тармоқда маълумотларнинг кескин кўпайишига олиб келди. Бу маълумотларни тармоқда ҳимоялашда (маълумотлардан ижозатсиз фойдаланишнинг олдини олиш мақсадида) криптография усулларида фойдаланиш ва уларнинг янги алгоритмларни ишлаб чиқиш замонавий ҳамда актуал муаммолардан бири бўлиб ҳисобланади.

Компьютер технологияларининг тараққиёти криптографиянинг қўлланиш соҳасини кенгайтириб унга янги масалаларни қўйди.

Ҳозирги вақтда маълумотларни шифрлашда криптографик

алгоритмларидан фойдаланиш мураккаб бўлмаган масалардан бири бўлиб ҳисобланади. Чунки замонавий юқори босқичли алгоритмик тилларда яратилган дастурлар орқали берилган маълумотларни шифрлаб керакли жойга тармоқда узатиш тизимлари кўплаб яратилган ва улар фойдаланувчиларга қўл келмоқда. Аммо тармоқдаги криптографик усуллар билан шифланган маълумотларни очиш ва уларни бузиш ҳоллари ҳам мовжуд. Буларни олдини олиш мақсадида криптографик усулларнинг янги динамик алгоритмларини ишлаб чиқиш мақсадга мувофиқдир.

Ҳозирги вақтда криптографиянинг икки ишлатилиш соҳаси мовжуд: маълумотларни узатишда ҳимоялаш ва уларни сақлашда ҳимоялаш. Уларнинг ҳар бири криптографияга ўзининг хусусий талабларини қўяди ва муайян масалалар ечимида ўз тасдиғини топади.

Барча криптографик алгоритмлар симметрик ва асимметрик алгоритмларга бўлинади. Симметрик алгоритмларда маълумотларни шифрлаш ва уларни очиш битта калит сўзлари орқали содир этилади. Калит сўзларининг тез-тез янгиланиши маълумотларнинг кўпроқ ҳимояланганлигини кўрсатади. Калит сўзларининг тез-тез алмашинуви маълумотлар физик алмашинувиға таъсир этганлиги сабабли амалида ҳар бир узатиш вақти учун алоҳида калит сўзлари ишлаб чиқилади ва улар орқали маълумотлар шифрланади ва аслиға қайтарилади.

Асимметрик алгоритмлар яқинда пайдо бўлди ва криптографияда янги соҳа очди. Бу турдаги алгоритмлар икки қисмдан: шифрлаш учун калит ва шифрланган маълумотларни очиш учун калитдан иборат бўлади.

Асимметрик моделда ижозатсиз мурожаатларнинг олдини олиш мақсадида очик калитларни ҳақиқийлигини тасдиқлашнинг махсус усулларини (сертификация) ишлаб чиқиш талаб этилади. Бундан ташқари бу моделдан фойдаланилганда қўшимча маълумотлар алмашинувининг пайдо бўлиши ҳисобига тармоқнинг ишлаш тезлиги сезиларли даражада камаяди.

Юқоридагиларни ҳисобға олган ҳолда тармоқда маълумотларни ҳимоялашнинг криптографик усулларида қайси бирини танлаш

фойдаланувчининг ўзига ҳавола этилади.

Криптографикада маълумотларни шифрлашда ишлатиладиган кодларини яширинлишини таъминлаш муҳим рол ўйнайди. Чунки тармоқдаги маълумотга рухсатсиз кирувчида барча информациялар (криптограмма матн ва алгоритм ҳақида маълумот) ва дастурий воситалар мавжуд. Унга фақат бир нарса – калит сўзи (калит рақамлар) етишмайди. Бундай ҳолда калит сўзи (калит рақамлар)ни топиш учун мумкин бўлган барча ҳолатларни қараган ҳолда матнни очиб уни таҳлил қилиш керак. Бу энг секин бажариладиган, лекин тўғри йўлдир. Калит сўзлар узунлиги мумкин бўлган ҳолатларнинг сонини оширади ва натижада криптографиянинг турғунлигини сақлаш критерияси бўлиб ҳисобланади.

§1.2. Шифрлаш ва шифрларни очиш

Фараз қилайлик, жўнатувчи олувчига бирор хабар юбормоқчи. У бу маълумотни олувчидан бошқа бирор кишининг ўқиимаслигини ҳохлайди. Хабар очик матндан иборат бўлади. Бу очик матнни бегоналар ўқий олмайдиган ҳолга келтириб шакл алмаштиришга шифрлаш дейилади. Натижада шифрли-матн хабар ҳосил қилинади. Шифр-матнли хабарни тескари алмаштириб ўз ҳолига келтириш шифрларни очиш дейилади.

Очик матнли хабарларни ижозатсиз фойдаланувчиларлад ҳимоя қилиш йўллари ва усулларини ўрганувчи фан криптография деб аталади.

Криптография билан шуғулланувчи кишиларни криптографлар дейишади.

Криптотаҳлил бу– шифрланган матнли хабарни очиш (оригиналига мос келадиган матнни топиш) муаммолари билан шуғулланиш бўлиб бунлай соҳада фаолият кўрсатидиган кишиларни криптоаналитиклар деб аташадилар.

Фаннинг криптография ва криптотаҳлилни бирлаштирувчи бўлими криптология бўлиб ҳисобланади.

Шифлаш ва шифрларни очишнинг математик содда моделини қуйидагича тушинтириш мумкин:

Очиқ матнни Р ҳарфи (инглизча плаинтхт сўздан) билан белгилайлик. Очиқ матн матнли файл, битли тасвир, рақамлаштирилган мусиқа ва бошқалар бўлиши мумкин. Шифрли-матнни С ҳарфи билан (инглизча сипхертхт сўздан) белгилансин. Шифрли-матн ҳажми айрим ҳолларда асл матн ҳажмидан катта ёки кичик бўлиши мумкин. Шифрли-матн тармоқ орқали керакли жойга узатилиши ёки компьютер хотирасида сақланиши керак. Очиқ матнни шифрлаш ва шифрли-матнни олиш математикада қуйидаги функция билан аниқланади:

$$E(P) = C$$

Бу ерда Е шифрлаш алгоритми функцияси.

Шифрли-матнни очишни қуйидагича кўрсатиш мумкин:

$$D(C) = M$$

Шифрли-матнни очганда асл матн ҳосил бўлишини ҳисобга олиб қуйидаги ифодани кўрсатишимиз керак:

$$D(E(P)) = P$$

§1.3. Аутентификация, яхлитлик ва ишончлилик

Тармоқларда маълумотларни шифрлаб узатишда аутентификация, яхлитлик ва ишончлилик тушинчалари катта роль ўйнайди.

Аутентификация. Маълумотни қабул қилувчи маълумот кимдан келганини билиши ва унга ишонч ҳосил қилиши керак. Бу аутентификация дейилади.

Яхлитлик. Хабарни қабул қилувчи хабар узатилиши пайтида унга ўзгартиришлар киритилганлигини ёки уни бошқа хабар билан алмаштирганлигини аниқлаш хабарни яхлитлигини текшириш дейилади.

Ишончлилик. Хабарни юбуровчи шифрли-матнни ишончлигига кафил бўлади ва уни ишончоигини инкор этмайди.

Маълумотларни тармоқда узатишда юқорида келтирилган тушинчалар ката роль ўйнайди, чунки маълумот алмашинуви катта масофада иштирокчиларнинг бир-бирларини кўрмасдан ҳосил қилинади. Шунинг учун ҳар бир маълумот алмашинувида хабарнинг аутентификацияси, яхлитлиги ва

ишончлилиги таъминланган бўлмоғи зарур.

§1.4. Шифрлар ва калитлар

Шифрлаш ёки шифрлаш алгоритми деб аталувчи криптографик алгоритм шифрлашда ва шифрни очишда ишлатиладиган математиканинг оддий ёки махсус функциялардир. Бу функцияларнинг бири ахборотларни (матнлар ёки белгиларни) шифрлашда ишлатилса иккинчиси уни очишда ишлатилади.

Криптографик алгоритмнинг ишончлилиги фойдаланилган алгоритмнинг сирлигига боғлиқда бўлса шифрлашнинг бундай алгоритми чегараланган дейилади. Чегараланган алгоритмли шифрлаш замонавий криптографиянинг талабларига жавоб бермайди. Чунки маълумот алмашинувчиларнинг ҳар бирининг ўз алгоритмлари мовжуд бўлишлари керак ва уларга мос келувчи дастурий воситалар яратилган бўлиб стандарт дастурларнинг тузилиши шарт эмас.

Замонавий криптография бу масаланинг ечими сифатида бир ёки бирнеча алгоритмларни яратиш ва уларнинг дастурий воситаларини ишлаб чиқиш, улар учун яширин калитлар ўрнатишни тавсия қилади.

Калитлар K ҳариф билан белгиланади ва калитлар соҳаси деб аталувчи фазога қарашли қийматларнинг бири бўлади. Бу ҳолда шифрлаш функцияси E ва шифрлани очувчи функция D ҳам калит K га боғлиқ бўлади. Бу тушинчани қуйидаги ифодалар орқали ифодалаймиз:

$$E_K(P) = C$$

$$D_K(C) = P$$

Бу ерда ҳам қуйидаги тасдиқ ўринли бўлади:

$$D_K(E_K(P)) = P$$

Айрим криптографик алгоритмларда шифрлашда бир калит K_1 , шифрларни очишда бошқа калит K_2 ишлатилади. Бу ҳолда ҳам юқоридагидек ифодаларни ёзиш мумкин:

$$E_{K_1}(P) = C$$

$$D_{K_2}(C) = P$$

$$D_{k2}(E_{k1}(P)) = P$$

Калитлар ёрдамида шифрлаш алгоритмининг ишончилиги калитларнинг яширинлигига боғлиқ бўлиб алгоритмни яширишнинг ҳожати қолмайди.

§1.5. Шифрлашнинг симметрик алгоритмлари

Калитлар ёрдамида шифрлашнинг икки хили: симметрик ва асимметрик (очиқ калитлар) усули мавжуд.

Ахборотларни шифрлашда ва шифрларни очишда бита калитдан фойдаланиш, ёки шифрларни очишдаги калитни шифрлаш калитидан ҳосил қилиш симметрик алгоритмли криптография бўлиб ҳисобланади. У бир калитли алгоритм деб ҳам аталади.

Бир калитли алгоритмнинг ишончилиги калитнинг танланишига боғлиқ бўлади ва бу калит қаттиқ сир ҳолда сақланади.

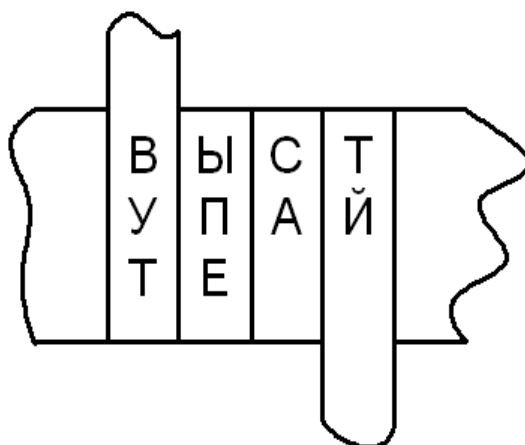
Симметрик алгоритмли шифрлашда юқорида келтирилган ифодалар ишлатилади:

$$E_k(P) = C$$

$$D_k(C) = P$$

§1.6. Шифрлашнинг айрим алгоритмлари

1. Қуйидаги шаклдаги алгоритмда бўйича шифрлашда ахборотлар бирор матрица шаклида ёзилади ва шифрланган матн матрицанинг устунлари бўйича ўқилади. Бундай алгоритмларни компьютерларда ижро этиш осон.

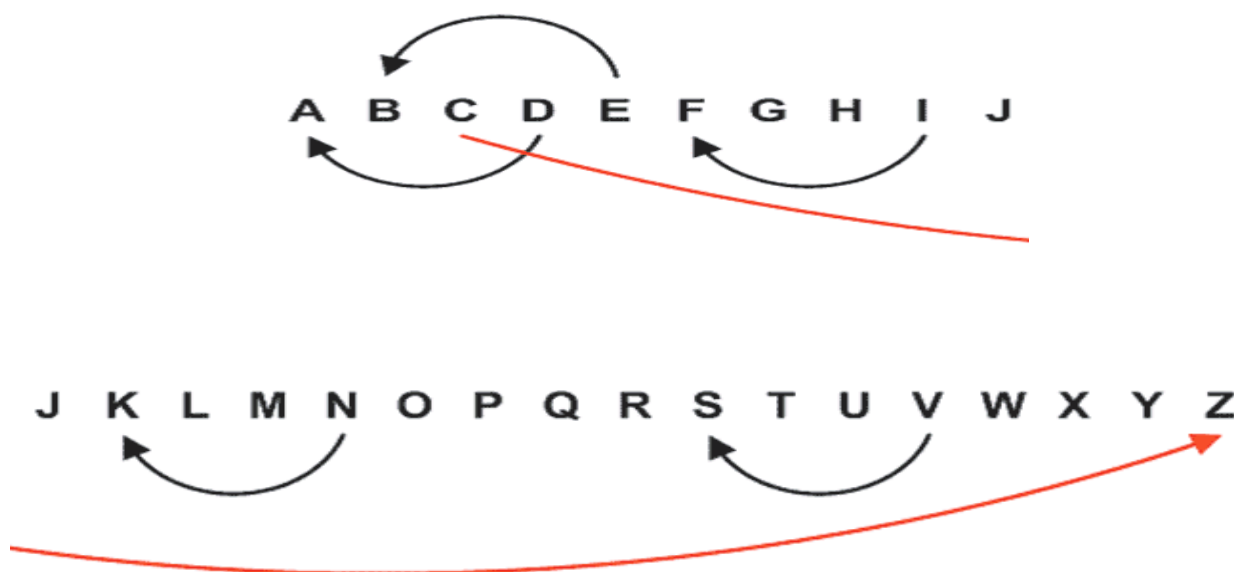


2. Бу алгоритмда ҳам маълумотлар жадвал кўринишида тасвирланиб шифрланиш пайтида берилган қоида асосида жадвалнинг элементлари

танланади. Масалан, $a(1,5)$, $a(2,5)$, $a(3,5)$ ва ҳакозо.

ν	π	η	ς	ε
λ	ϕ	μ	ρ	γ
	o	α	δ	ν
φ	β	ξ	σ	ω
ι	κ	τ	θ	χ

3. Матн сатри элементлари берилган қоида асосида шифрлаш пайтида ўз ўринларини алмаштиради. Масалан, 4-элемент 1-чи элемент ўрнига келади, 5-чи элемент 2-чи элемент ўрнига келади, 3-чи элемент эса охириги элемент ўрнига келади ва ҳакозо.



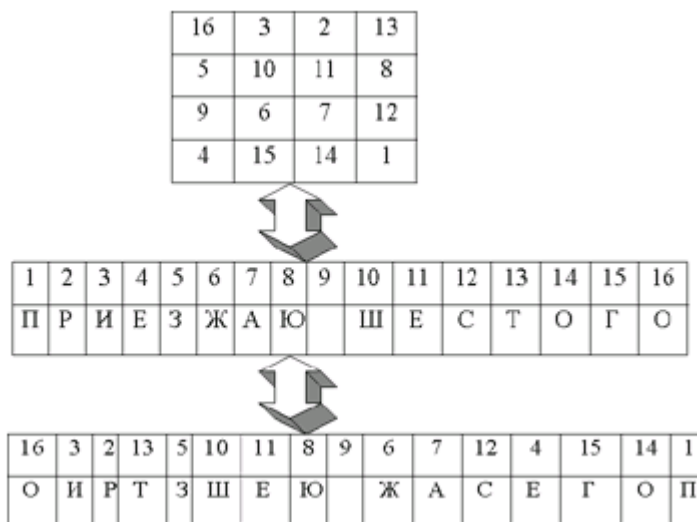
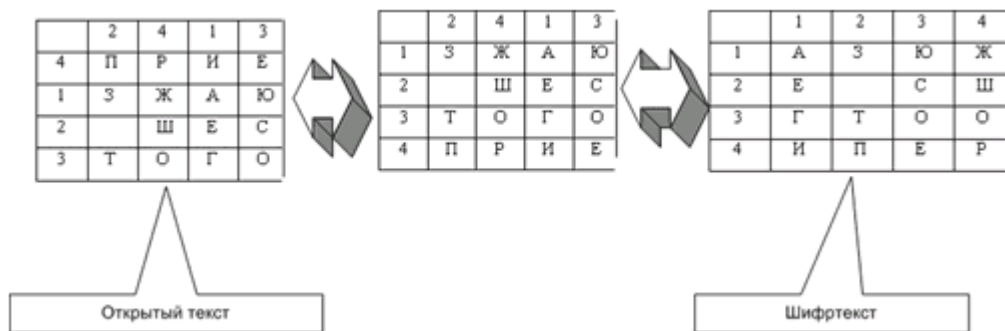
4. Шифрланадиган матн жадвалнинг устунлари бўйича тўлдирилади ва шифрлаш пайтида жадвал элементлари сатрлар бўйича ўқилади. Бу алгоритм дастурлашга қўлай бўладиган алгоритмлардан ҳисобланади.

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Л	У	Н	А	Т	И	К
4	7	5	1	6	2	3
Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

1	2	3	4	5	6	7
С	Н	Я	Н	Н	Б	О
Я	Е	Т	Е	О	О	Е
Е	П	Н	Я	В	Л	С
Щ	О	Ы	С	И	Е	Т
Е	Н	М	Н	Т	Е	А

5. Шифрлаш алгоритми шакл орқали кўрсатилмоқда.



А Б В Г Д Е Ё Ж З И Й К Л М Н . . . С Т У Ф . .

6. Шифрланадиган матн саҳифаси жадвал (матрица)га жойлаштирилади ва уни шифрлаш жадвал устунлари ва сатрлар номерлари комбинацияларидан иборат сонлар кетма-кетлигига боғлиқ бўлади.



Қуйида шифрлашнинг бошқа алгоритмларининг тасвирлари келтирилмоқда. Бу алгоритмларнинг айримлари кейинги мавзуларда ёритилади.



Р	Е	С	П	У	Б
Л	И	К	А	В	Г
Д	Ж	З	М	Н	О
Т	Ф	Х	Ц	Ч	Ш
Щ	Ъ	Ы	Э	Ю	Я

П У → У Б

С Т → Р Х

О Н → Д О

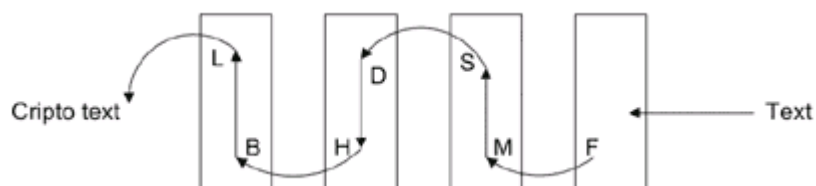
Л Ы → К Щ

Ч	_	В	Ы	П
О	К	:	Д	У
Г	Ш	З	Э	Ф
Л	Ъ	Х	А	,
Ю	Р	Ж	Щ	Н
Ц	Б	И	Т	Ь
.	С	Я	М	Е

Е	Л	Ц	:	П
.	Х	Ъ	А	Н
Ш	Д	Э	К	С
Ы	_	Б	Ф	У
Я	Т	И	Ч	Г
М	О	,	Ж	Ь
В	Щ	З	Ю	Р

О Ж → А Ц

А _ → Ъ Ф



§1.7. Очик калитли шифрлаш алгоритмлар

Очик калитли шифрлаш алгоритмлар (асимметрик алгоритмлар)ида шифрларни очишдаги калитлар шифрлашда ишлатиоган калитлардан тубдан фарқ килади ва уни сир сақлашнинг хожати йўқ.

Ҳозирги пайтда очик калитли критпографик алгоритмлар ичида энг яхши деб тан олнгани RSA (алгоритм яратувчиларининг номлари: Ривест, Шамир, Аделман) бўлиб ҳисобланади.

РСА алгоритмининг марказий қисмини бир жуфт очик калитни яратиш ташкил этади. Калитларни ҳосил қилиш қуйидагича содир этилади:

1. Тасодифий равишда иккита содда (фақат ўзига ва 1 га бутун бўлинадиган) сонлар танланади, p ва q , $p \neq q$.
2. Ҳисобланади
$$r = p * q.$$
3. Ҳисобланади
$$\phi = (p-1) * (q-1).$$
4. Очик (K_o) ва яширин (K_c) калитлар танланади. Бу калитлар ϕ га нисбатан ўзаро содда бўлиб $(K_o * K_c) \bmod \phi = 1$ шартни қаноатлантиришлари керак.

Очик калит K_o ҳақидаги маълумотларни шифрлаш учун қуйидагилар бажарилади:

1) Берилган матн блоklarга ажратилади, уларнинг ҳар бири $M(i) = 0, 1, \dots, n-1$ сон шаклида тасвирланган бўлишлари мумкин;

2) $M(i)$ кетма-кет сонларни қуйидаги формула бўйича шифрлаймиз $C(i) = (M(i)^{K_o}) \bmod n$, бу ердаги кетма-кет $C(i)$ сонлар шифрланган матнни аниқлайди.

Ушбу шифрланган маълумотларни яширин K_c калит билан очиш учун қуйидаги ишларни бажарамиз:

$$M(i) = (C(i)^{K_c}) \bmod n.$$

Натижада берилган матнни ифодалайдиган $M(i)$ сонлар тўплами ҳосил бўлади.

Мисол.

Қуйидаги “САБ” матнни очик калитли РСА алгоритми билан шифрлаш алгоритми келтирилади. Соддалик учун кичик сонлардан фойдаланамиз.

1. Танлаймиз $p=3$, $q=11$.
2. Ҳисоблаймиз $r=3*11=33$.
3. Ҳисоблаймиз $\phi=(p-1)*(q-1)=20$.

4. ϕ билан ўзаро содда бўлган махфий калит K_c ни танлаймиз, масалан $K_c=3$ бўлсин.

5. K_c ва ϕ асосида очиқ калит K_o ни ҳисоблаймиз.

K_o ни ҳисоблайдиган алгоритмнинг Паскаль алгоритмик тилдаги дастурини келтирамиз:

Програм PСA;

Вар

И, k_0, k_c, ϕ, y :интегер;

г, у, в:аррай[0..50] оф интегер;

БЕГИН

Рeadln(k_c, ϕ);

Г[0]:= ϕ ; г[1]:= k_c ;

У[0]:=1; у[1]:=0;

В[0]:=0; в[1]:=1;

и:=1;

whиle г[и]<> 0 до

бегин

г[и]:=у[и]* ϕ +в[и]* k_c ;

й:=г[и-1] див г[и];

г[и+1]:=г[и-1]-й*г[и];

у[и+1]:=у[и-1]-й*у[и];

в[и+1]:=в[и-1]-й*в[и];

енд;

k_0 :=в[и-1];

иф $k_0 < 0$ тхен k_0 := $k_0 + \phi$; wрителн(k_0);

ЕНД.

Натижа: $K_o=7$.

6. Шифрланадиган матнни 2...28 диапазондаги бутун сонлар кетма-кетлиги каби тасаввур этамиз. А ҳарфига 2 сони, В ҳарфига 3 сони, С ҳарфига 4 сони мос келсин. У ҳолда “САБ” матинни

қуйидаги кетма-кетлик шаклида тасвирлаш мумкин {5, 3, 4}.

Матнни очик калит $K_o=7$ орқали шифрлаймиз:

$$C_1 = (5^7) \bmod 33 = 78125 \bmod 33 = 14,$$

$$C_2 = (3^7) \bmod 33 = 2187 \bmod 33 = 9,$$

$$C_3 = (4^7) \bmod 33 = 16384 \bmod 33 = 16.$$

7. Шифрни махфий калит $K_c=3$ билан очиш учун қуйидаги {14, 9, 16} сонлар тўплами ҳосил бўлди. Ҳисоблаймиз:

$$M_1 = (14^3) \bmod 33 = 2744 \bmod 33 = 5,$$

$$M_2 = (9^3) \bmod 33 = 729 \bmod 33 = 3,$$

$$M_3 = (16^3) \bmod 33 = 4096 \bmod 33 = 4.$$

Натижада (“САБ”) матнига мос келувчи {5, 3, 4} сонлар тўплами ҳосил бўлди.

Ушбу алгоритмнинг мураккаблиги ва шифрни очишдаги қийинчилик танланадиган сонларнинг катталигига боғлиқда бўлади, масалан 200 та рақамдан иборат сон танланса махфий калитни ҳосил қилиш учун 10^{23} атрофидаги операцияларни бажариш талаб этилади.

§1.8. Криптоҳафли хужумлар

Криптоҳафли бу – шифрланган ахборотни қайта ишлаб унинг асл ҳолатини тиклашдан иборатдир. Муаффақиятли криптоҳафли натижасида нафақат шифрланган ахборотнинг асл ҳолатини балки унинг шифрлаш калитини ҳам ҳосил қилиши мумкин. Шунинг учун криптоҳафлини шифрланган ахборотларга нисбатан қилинган хужум деб қабул қилинади.

Криптоҳафлли хужумнинг 4 асосий типлари аниқланган:

1. Фақат шифрланган матнни билган ҳолда криптоҳафлли хужум.

Криптоҳафличида бир хил алгоритм билан шифрланган бир неча маълумотлар мавжуд. У шифрланган маълумотларни очиши ва

очик калитни топиб кейинги шифрланган маълумотларга қўллаши керак. Бу масаланинг математик моделини қуйидагича кўрсатиш мумкин:

Берилган

$$C_1=E_{k_1}(P_1), C_2=E_{k_2}(P_2), \dots, C_n=E_{k_n}(P_n)$$

Топиш керак

$$P_1, P_2, \dots, P_n \text{ ёки } k_1, k_2, \dots, k_n$$

2. Очик матнли билган ҳолда ҳужум. Криптоатаҳлилчи шифрланган маълумотларни ҳамда уларнинг очик матнларини билади. У шулар асосида калитни қўлга киритиш билан шуғулланади. Бу масаланинг математик ифодасини келтирамиз:

Берилган:

$$P_1, C_1 = E_{k_1}(P_1), P_2, C_2 = E_{k_2}(P_2), \dots, P_n, C_n = E_{k_n}(P_n).$$

Топилиши керак:

$$k_1, k_2, \dots, k_n.$$

3. Танланган очик матнли ҳужум. Криптоаналитик нафақат шифрланган ва очик матнли ахборотларни билади, балки бу ахборотларни маъносини ҳам чиқара олади. Бу ҳолда ҳам ундан калитни топиш талаб қилинади. Бу масаланинг математик модели ҳам юқорида келтирилганидек бўлади.
4. Танланган очик матнли адаптирлашган ҳужум. Бу ҳужум танланган очик матнли ҳужумнинг бир кўриниши бўлиб унда криптоаналитик шифрланган очик матнни танлабгина қолмайди, балки шифрлаш натижасига кўра танлашларни ҳам ўзгартириши мумкин.

§1.9. Шифрлаш алгоритмларининг мустаҳкамлиги

Ҳар хил криптографик алгоритмлар ҳар хил мустаҳкамликка эга бўлишади. Мустаҳкамлик криптоаналитикнинг шифрни қандай қийинчилик билан очишига боғлиқ. Шифрни очиш учун кетадиган вақт ва унга кетадиган

сарф-харажатлар катта бўлиб ахборотни сир сақлаш муддатидан кўп бўлса бундай алгоритмларни мустаҳкам деб ҳисобласа бўлади. Шифрланган ахборотлар ва уларнинг мустаҳкамлигига боғлиқ қуйидаги қоида мавжуд:

- Сир сақланадиган маълумотнинг баҳоси криптоаналитиклар томонидан шифрни очишга сарфланадиган харажатдан кам бўлмоғи керак.

Криптоаналитик ҳужумнинг мураккаблиги

Криптоаналитик ҳужумнинг мураккаблигини уч катталиқ билан характерлаш мумкин:

- Маълумотлар бўйича қийинлик. Муоффақиятли криптоаналитик ҳужум учун керакли маълумотларнинг етарлилиги.
- Ҳисоблашларнинг мураккаблиги. Муоффақиятли криптоаналитик ҳужум учун керакли вақтнинг етарлилиги.
- Хотиралар бўйича мураккаблик. Муоффақиятли криптоаналитик ҳужум учун керакли хотира майдонинг етарлилиги.

Криптоаналитик ҳужумнинг қийинлигини экспонентал функция кўринишда тасвирлаш қабул қилинган. Масалан, ҳужумнинг қийинлик даражаси^{2¹²⁸} бўлсин. Демак, шифрни очиш учун ^{2¹²⁸} та прерация бажарилиши керак экан.

§1.10. Шифрлашнинг алмаштириш ва ўрин алмаштириш алгоритмлари

Шифрлашнинг алмаштириш ва ўрин алмаштириш алгоритмлари кенг қўлланилади. Бунда элементлар бошқа элементлар билан алмаштирилади ёки элементлар ўз ўринларини алмаштириладилар.

§1.11. Алмаштирувчи шифрлар

Классик криптографияда алмаштирувчи шифрларнинг 4 хил кўриниши мавжуд:

1. Оддий алмаштириш ёки бир алфавитли алмаштириш (моноалпхабетис). Очиқ матннинг ҳар бир ҳарифи бирор символ билан алмаштирилади.
2. Омофонли алмаштириш (хомопхонис). Бунда оддий

алмаштиришдан фарқли равишда ҳар бир ҳарифлар бир неча символлар билан алмаштирилади.

3. Блокли алмаштириш (поляпҳабетис). Очиқ матн блокларга айлантирилади ва ҳар бир блок алоҳида символлар билан алмаштирилади.
4. Кўп алфавитли алмаштириш (полйграм). Бунда очиқ матннинг бирор симболи бир неча символлар ичидан танлангани билан алмаштирилади. Танланиш очиқ матн символининг ўрни билан аниқланади.

§1.12. Ўрин алмаштиришли шифрлаш

Бу алгоритмда очиқ матндаги символлар бошқалари билан алмаштирилмайди, балки уларнинг ўринлари алмаштирилади. Масалан, очиқ матн жалвалнинг сатрлари бўйича ёзилади ва ўқиш эса устунлари бўйича содир этилади.

Ўрин алмаштиришли шифрлашда икки карали ўрин алмаштиришлар ҳам содир этилиши мумкин. Бу ҳолат икки калитли шифрлаш дейилади.

Бевосита ўрин алмаштириш бўйича шифрлаш

Моноалпҳабетис синфига кирувчи тизимларда берилган матн символлари қатъий боғланган бошқа символлар билан алмаштирилади. Бундай тизимнинг криптографик калити жорий алфавитга мос келувчи янги ўрин алмаштириш жадвалидир. Бундай тизимнинг энг содда шифрлаш алгоритмида алфавитдаги ҳар бир ҳариф к позицияга сурилади, бу ерда к шифрлаш калитидир.

Цезарь алгоритми

Цезарь алгоритми ҳам шунга асосланган бўлиб уни қуйидаги ифода билан тасвирлаш мумкин:

$$E_k(i) = (i+k) \bmod 26.$$

Масалан, $k=3$ деб ҳисобланганда лотин алифбосида $i=0$ ўринда турадиган А ҳарфи $i=3$ ўринда турувчи Д ҳарфи билан алмаштирилади, чунки,

$$(i+k) \bmod 26 = (0+3) \bmod 26 = 3$$

Ёки лотин алифбосида $i=25$ ўринда турадиган з ҳарфи $i=2$ ўринда турувчи С ҳарфи билан алмаштирилади, чунки,

$$(i+k) \bmod 26 = (25+3) \bmod 26 = 2$$

Мисол.

Берилган матн: СРЙПТОГРАПҲЙАНДДАТАСЕСУРИТЙ.

Шифротекст :ФУБСЎРЖУДСКБДҚСГДЎДВҲФХУЛЎБ.

Шифрни очиш алгоритми қуйидагичадир

$$D_k(i) = (i+26-k) \bmod 26.$$

Ўрин алмаштиришнинг мураккаблашган усули

Юқорида келтирилган шифрлаш алгоритмини такомиллаштирамиз. Бунда берилган матн символлари позициялари калит k га кўпайтирилади. Унинг алгоритмини қуйидагича ифодалаш мумкин:

$$E_k(i) = (i*k) \bmod n,$$

Бу ерда i – берилган матн символи номери, n – берилган алфавитдаги символлар сони ($n=26$ лотин алифбоси учун ва $n=256$ АССИИ-кодлари учун). Силжитиш ва кўпайтиришга асосланган шифрлаш алгоритмининг ифодаси қуйидаги кўринишда бўлади:

$$E_k(i) = (i*k_1+k_0) \bmod n.$$

Криптографик тизимларнинг ҳомопхонис синифида бошланғич символни алмаштиришнинг бир нечта варианты аниқланган бўлади. Масалан, А ҳарфи 24, 35, 37 рақамлар билан, Б ҳарфи эса 41, 17, 76 рақамлар билан алмаштирилиши мумкин.

Криптографик тизимларнинг полялпҳабетис синфи бир қанча ҳар хил калитлардан фойдаланишга асосланган. Қуйидаги кўринишли берилган матн

$$X = x_1 x_2 x_3 x_4 \dots x_p x_{p+1} \dots x_{2p} \dots$$

$k_1, k_2, \dots, k_p$ калитлар орқали :

$$E_K(X) = E_{k_1}(x_1) E_{k_2}(x_2) \dots E_{k_p}(x_p) E_{k_1}(x_{p+1}) \dots E_{k_p}(x_{2p})$$

шакилда шифрланади.

Шундай алгоритмларнинг бирини ХВИ асрда француз Вигенер (Вигенере) таклиф этади.

Бу ерда калит K

$$K = k_1 k_2 \dots k_p,$$

шакилда тасвирланади. Бу ерда k_i ($1 \leq i \leq p$) берилган алфавитдаги силжишлардир.

Берилган матн символлари қуйидаги формула бўйича шифрланади

$$E_K(i) = (i + k_j) \bmod n,$$

бу ерда i – берилган матн символи номери, K_j - калит, $j \in \{1, \dots, p\}$.

Вижинернинг шифрлаш тизими.

Биринчи бўлиб Вижинер тизими 1586-йилда чоп этилган ва у кўп алфавитли тизимга нисбатан юқорироқ ўринда туради. Вижинер тизими Цезар шифрлаш тизимига қараганда мукамалроқ ҳисобланиб, унда калит ҳарфидан ҳарфга алмаштирилади. Бундай кўп алфавитли алмаштириш шифрини шифрлаш жадвали орқали ифодалаш мумкин. Қуйидаги биринчи жадвалда Вижинернинг латин алфавити учун мос келувчи жадвал кўрсатилган. Бу жадвалдан матнни шифрлаш ва уни очиш учун ишлатилади. Жадвалнинг иккита кириши бўлиб:

- Юқори қатордаги ҳарфлардан кирувчи очиқ ёзув учун фойдаланилади.
- Чап устундан эса калит ҳарфларидан фойданилади.

Мисол учун калит кетма-кетлигини p -деб олайлик, у ҳолда калит p -алфавитли p -сатрдан иборат бўлади.

$$\pi = (\pi_0, \pi_1, \dots, \pi_{p-1});$$

Вижинернинг шифрлаш тизимида очик матн $x=(x_0, x_1, \dots, x_{n-1})$ ва шифрланган матн $y=(y_0, y_1, \dots, y_{n-1})$ кўринишга эга. $\pi=(\pi_0, \pi_1, \dots, \pi_{p-1})$ калит ёрдамида қуйидагича муносабатда бўлади.

$$x=(x_0, x_1, \dots, x_{n-1}) \quad y=(y_0, y_1, \dots, y_{n-1});$$

$$(y_0, y_1, \dots, y_{n-1})=(\pi_0(x_0), \pi_1(x_1), \dots, \pi_{n-1}(x_{n-1}));$$

Юқоридаги ифодадан маълумки Вижинер жадвали орқали шифрлашда матннинг (ахборотнинг) ҳар бир ҳарфига мос келувчи калитнинг ҳар бир ҳарфи орқали уларнинг устун ва сатрлари кесишмасига мос келувчи ҳарфлар олинади.

Агар ўзбек алфавити ишлатилса, Вижинер матрицаси [36x36] ўлчамга эга бўлади.

АБВГД.....	ЎҚҒХ_
БВГДЕ.....	ҚҒХ_А
ВГДЕЖ.....	ҒХ_АБ
.....	_АБ
ВГ.....	ЯЎҚҒХ

Вижинер матрицаси.

Вижинер жадвали ёрдамида шифрлаш алгоритми қуйидаги қадамлар кетма-кетлигидан иборат.

1-қадам. Узунлиги M символли калит K ни танлаш.

2-қадам. Танланган калит K учун $[(M+1), P]$ ўлчамли шифрлаш матрицаси $T_{ш}=(b_{иж})$ ни қуриш.

3- қадам. Дастлабки матннинг ҳар бир символи $c_{ор}$ тагига калит символи k_m жойлаштирилади. Калит кераклича такрорланади.

4-қадам. Дастлабки матн символлари шифрлаш матрицаси $T_{ш}$ дан қуйидаги қоида бўйича танланган символлар билан кетма-кет алмаштирилади.

1) K калитнинг алмаштирилувчи $c_{ор}$ символга мос k_m символи аниқланади;

2) шифрлаш матрицаси $T_{ш}$ даги $k_m = b_{ж1}$ шарт бажарилувчи и қатор топилади.

3) $c_{ор} = b_{и1}$ шарт бажарилувчи ж устун аниқланади....

4) $c_{ор}$ символи $b_{иж}$ символи билан алмаштирилади.

5-қадам. Шифрланган кетма-кетлик маълум узунликдаги (масалан 4 символли) блоklarга ажратилади. Охирги блокнинг бўш жойлари махсус символ-тўлдирувчилар билан тўлдирилади.

Расшифровка қилиш қуйидаги кетма-кетликда амалга оширилади.

1-қадам. Шифрлаш алгоритмининг 3-қадамидагидек шифрматн тагига калит символлари кетма-кетлиги ёзилади.

2-қадам. Шифрматндан c_{1p} символлари ва мос калит символлари k_m кетма-кет танланади. $T_{ш}$ матрицада $k_m = b_{иж}$ шартни қаноатлантирувчи и қатор аниқланади. и-қаторда $b_{иж} = c_{1p}$ элемент аниқланади. Расшифровка қилинган матнда p - ўрнига $b_{иж}$ символи жойлаштирилади.

3-қадам. Расшифровка қилинган матн ажратилмасдан ёзилади. Хизматчи символлар олиб ташланади.

Агар калит сифатида <ВАЗА> сўзи танланган бўлса, шифрлаш матрицаси бешта қатордан иборат бўлади.

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_
ВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_АБ
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_
ЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_АБВГДЕЁЖ
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_

«ВАЗА» калити учун шифрлаш матрицаси.

Мисол. $K = \langle \text{ВАЗА} \rangle$ калити ёрдамида $T = \langle \text{БАЙРАМ КУНИ} \rangle$ дастлабки матни шифрлансин.

Шифрматн T_1 қуйидагича бўлади: ГАСРВМЖКХНП

Ўринларни алмаштириш усулларига мисол сифатида яна қуйидагиларни келтириш мумкин:

- шифрловчи жадвал;
- сеҳрли квадрат.

Шифрловчи жадвал усулида калит сифатида қуйидагилар қўлланилади:

- жадвал ўлчовлари;
- сўз ёки сўзлар кетма-кетлиги;
- жадвал таркиби хусусиятлари.

Мисол.

Қуйидаги матн берилган бўлсин:

КАДРЛАР ТАЙЁРЛАШ МИЛЛИЙ ДАСТУРИ

Ушбу ахборот устун бўйича кетма – кет жадвалга киритилади:

К	Л	А	Л	И	Й	Т
А	А	Й	А	Л	Д	У
Д	Р	Ё	Ш	Л	А	Р
Р	Т	Р	М	И	С	И

Натижада, 4x7 ўлчовли жадвал ташкил қилинади.

Энди шифрланган матн қаторлар бўйича аниқланади, яъни ўзимиз учун 4 тадан белгиларни ажратиб ёзамиз.

КЛАЛ ИЙТА АЙАЛ ДУДР ЁШЛА РРТР МИСИ

Бу ерда калит сифатида жадвал ўлчовлари хизмат қилади.

Сеҳрли квадрат деб, катакчаларига 1 дан бошлаб сонлар ёзилган, ундаги ҳар бир устун, сатр ва диагональ бўйича сонлар йиғиндиси битта сонга тенг бўлган квадрат шаклидаги жадвалга айтилди.

Сеҳрли квадратга сонлар тартиби бўйича белгилар киритилади ва бу белгилар сатрлар бўйича ўқилганда матн ҳосил бўлади.

Мисол.

4x4 ўлчовли сеҳрли квадратни оламир, бу ерда сонларнинг 880 та ҳар хил комбинацияси мавжуд. Қуйидагича иш юритамиз:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Бошланғич матн сифатида қуйидаги матнни оламир:

ДАСТУРЛАШ ТИЛЛАРИ

ва жадвалга жойлаштирамиз:

И	С	А	Л
У	Т	И	А
Ш	Р	Л	Л
Т	Р	А	Д

Шифрланган матн жадвал элементларини сатрлар бўйича ўқиш натижасида ташкил топади:

ИСАЛ УТИА ШРЛЛ ТРАД

§1.13. Роторли машиналар

Роторли машиналар очиқ матннинг ҳар бир симолини маълум бир позицияга суришдан иборат. Бундай шифрлаш дастурлаш учун осон бўлганидек криптоаналитиклар учун ҳам қийинчилик туғдирмайди.

§1.14. Бир марталик блокнотлар

Бир марталик блокнотлар энг мустаҳкам шифрлашлардан бири бўлиб ҳисобланади. Бу алгоритм бўйича шифрлашда узун тасодикий харфлар кетма-кетлигидан фойдаланилади. Тасодикий ҳарифлар кетма-кетлиги шифрлашда фақат бир марта ишлатилади. Шифрни очишда тасодикий харфлар кетма-кетлигидан иборат блокнот нусхаси ишлатилади. Ҳар бир янги алоқада янги тасодикий харфлар кетма-кетлиги фойдаланилади.

§1.15. Шифрлашнинг компьютерли алгоритмлари

Информатика ва информацион технологияларнинг ривожланиши криптографияга ҳам ўз таъсирини ўтказмоқда. Мутахассислар томонидан бир қанча компьютерлашган алгоритмлар яратилган. Бу алгоритмлар сифатида қуйидагиларни келтириш мумкин:

- Дата Енсрипцион Стандарт (ДЕС). АҚШ давлатининг стандарти бўлиб ҳисобланадиган симметрик алгоритм.
- RSA (Ривер, Шамир, Адиемам). Очик калитли шифрлаш алгоритми.
- ГОСТ 28147-89. Россиянинг давлат стандарти, симметрик шифрлаш алгоритми.

§1.16. Сир сақланадиган калит узунлиги

Симметрик криптосистемаларнинг мустаҳкамлиги унда ишлатилган алгоритм ва сир сақланадиган калитнинг узунлиги боғлиқ бўлади. Фараз қилайлик, идеал алгоритм мовжуд, уни ижозатсиз очиш учун фақат мумкин бўлган барча калитларни бирма-бир кўриб чиқиш керак. Криптоаналитиканинг бу ҳужуми тотал кўздан кечириш дейилади.

Агар сир сақланадиган калитнинг узунлиги 64 битдан иборат бўлса, 1 секундда 1 млн. калитни текширадиган суперкомпьютер барча мумкин бўлган имкониятларни 5 минг йилда текшириб бўлади.

II. Қисм. Амалий топшириқлар

Мавзу: Бевосита ўрин алмаштириш бўйича шифрлаш

Кириш. Ахборотларни қайта ишлаш жараёнларини автоматлаштириш воситалари, усуллари ва формалари мураккаблашуви ва ривожланиши бўйича уларни ахборот технологияларида уларни қўлланилиш хавфсизлик даражасидан ошиб бормоқда.

1.Ишдан мақсад: Симметрик криптолизимни асосий усулларини ўрганиш ва тадқиқ этиш.

2.Қисқача назарий маълумот:

Назарий маълумотлар услубий кўрсатманинг биринчи қисмида ҳамда мавзу бўйича ташкиллаштирилган адабиётларда келтирилган.

3. Ишни бажарилиш тартиби ва қўйилган вазифа:

Асосий матн шифрлаш усулларида бирида шифрлансин ва кадамма – кадам изохлансин.

Ҳисобот мазмуни:

Иш мавзуси.

Ишдан мақсад.

Шифрлаш алгоритмининг блок-схемаси.

Дастур матни.

Илова ва натижа

Умумий хулосалар

4. Топшириқ вариантлари

- **ВАРИАНТ №1.** «Самарқанд давлат университети» сўзи оддий ўрин алмаштириш усули билан шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №2.** «Самарқанд давлат университети» сўзи Цезарь усули билан шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №3.** «Самарқанд давлат университети» сўзи силжитиш ва кўпайтиришга асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №4.** «Самарқанд давлат университети» сўзи кўпайтириш ва силжитишга асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №5.** «Самарқанд давлат университети» матни 6*6 жадвалга жойлаштирилсин. Жадвал устунлари ўринларини

алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;

- **ВАРИАНТ №6.** «Самарқанд давлат университети» матни 6*6 жадвалга жойлаштирилсин. Жадвал сатрлари ўринларини алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №7.** «Самарқанд давлат университети» матни блоklarга ажратилсин. Ҳар бир блок номери силжитиш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №8.** «Самарқанд давлат университети» матни блоklarга ажратилсин. Ҳар бир блок номери кўпайтириш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №9.** «Самарқанд давлат университети» матни блоklarга ажратилсин. Ҳар бир блок номери айириш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №10.** «Самарқанд давлат университети» матни каррали силжитишга (силжитишлар символнинг жойлашган ўринлари номерига боғлиқда, масалан, калит $k=3$ да «Фан» сўзидаги «Ф» симболи 3+1 га, «а» симболи 3+2 га, «н» симболи эса 3+3 га силжийди) асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №11.** «Самарқанд давлат университети» матни тескари ўқиш ҳамда силжитиш алгоритми асосида шифрлансин ва шифр очилсин;
- **ВАРИАНТ №12.** «Самарқанд давлат университети» матни тескари ўқиш ҳамда кўпайтириш алгоритми асосида шифрлансин ва шифр очилсин;
- **ВАРИАНТ №13.** «Самарқанд давлат университети» матни тескари ўқиш ҳамда кўпайтириш ва силжитиш алгоритми асосида шифрлансин ва шифр очилсин;
- **ВАРИАНТ №14.** «Самарқанд давлат университети» матни 6*6 жадвалга жойлаштирилсин. Сатрлар ўрнига устунларни ёзиш орқали янги жадвал ҳосил қилинсин. Кейин эса сатрлари ўринларини алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №15.** «Самарқанд давлат университети» матни «сеҳирли квадрат» жадвали асосида шифрлансин ва шифр очилсин;

5. Назорат саволлари

1. Криптография мақсади ва вазифаси.

2. Оддий ўрин алмаштириш усули ва калит сўзли ўрин алмаштириш усули.
3. Икки марталик қайта қуйиш усули ва сеҳрли квадрат усули.
4. Цезар усули ва калит сўзли Цезар тизими.
5. Криптографиянинг симметрик ва асимметрик усуллари.
6. Электрон имзо.
7. Шифрлашнинг компьютерли алгоритмлари.
8. Шифрлаш алгоритмларининг мустаҳкамлиги
9. Криптоҳафизация хужумлар ва уларнинг типлари
10. Аутентификация, яхлитлик ва ишончлилиқ

Фойдаланилган адабиётлар

1. Жельников В. Криптография от папируса до компьютера. М.: АБФ, 1997. – 336с.
2. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001й.
5. Масленников А. Практическая криптография БХВ – СПб 2003й.
6. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002й.
8. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.

1. МУСТАҚИЛ ИШЛАР ТИЗИМИ

№	Мавзу номи	Со- ат	Топшириқлар	Ҳисо- бот шакли	Адабиёт лар
1	2	3		4	5
1	Ахборот ҳавфсизлигининг асосий тушунчалари ва уларни аниқлаштириш.	1	Ахборот ҳавфсизликнинг асосий мақсад ва вазифаларини ёритиб	Ёзма	[1-12]

			бериш		
2	Ҳавфсизликнинг мавжуд барча хилма-хил чораларидан фойдаланиш.	1	Ахборот хавфсизлигини таъминлаш чораларининг босқичлари ва даражалари	Ёзма	[1,12]
3	Ахборот ҳимоясининг бузулиши, ҳимоя механизми ва ҳимоя турлари.	1	Ахборот хавфсизлигига хавфларни ва хавфсизлик тизимлилигини таъминлаш усуллари	Ёзма	[1,12]
4	Ахборот хавфсизлиги моделлари Ҳавфсизлик моделлари. Ахборот хавфсизлиги тизимининг архитектураси.	1	Ҳавфсизлик моделлари бажарадиган вазифалари. Тизимнинг яшовчанлигини асослаш, унинг архитектураси, қурилишида фойдаланадиган асосий принциплар.	Ёзма	[3,12]
5	Криптографиянинг асосий қоидалари ва таърифлари. Симметрик шифрлаш тизими. Асимметрик шифрлаш тизими	1	Симметрик ва асимметрик шифрлаш тизимларнинг хусусиятлари. Шифрлаш усуллари.	Ёзма	[3,12]
6	Хэшлаш функцияси. Электрон рақамли имзо.	1	Хэшлаш функциясини қуриш принцип ва моделлари. Рақамли имзо файлини яратиш.	Ёзма	[3,12]
7	Криптографик калитларни бошқариш	1	Очқ, махфий, бир ва икки калитли тизимлар асосида криптографик алгоритмларни ишлаб чиқиш	Ёзма	[3,12]
8	Идентификация ва аутентификация. Асосий тушунчалар ва туркумланиши. Пароллар ва сертификатлар асосида аутентификациялаш	1	Оддий ва мураккаб пароллар. Идентификация ва аутентификация усуллари ривожланиши ва истиқболлари.	Ёзма	[3,12]
9	Интернет ва Интранетда ахборот хавфсизлиги Интернет тармоғи орқали узоқдаги ҳужумдан ҳимояланиш усуллари ва муҳитлари.	1	Локал ва глобал тармоқларда ички ва ташқи хавфлар таснифи. Глобал тармоғи орқали ҳужумлардан ҳимояланиш усуллари	Ёзма	[3,12]

10	Тармоқлараро экранлар Тармоқлараро экранларини функцияларининг хусусиятлари.	1	ФиреВалл тизимларини ташқил қилиш принциплари, турлари, вазифалари, дастурий таъминоти	Ёзма	[3,12]
11	Тармоқлараро экранларини асосий компоненталари. Маршрутлаштириш ва шлюзалар турлари. Кучлантирилган аутентификация.	1	Филтрлайдиган маршрутлаштиришлар. Тармоқ даражасининг шлюзи. Амалий даражасининг шлюзаси. Кучлантирилган аутентификация принципи	Ёзма	[3,12]
12	Тармоқлараро экранлар асосий схемалари. Экранлашган кўприк. Экранлашган қисм тармоқ..	1	Тармоқлараро экранлар базасида тармоқ ҳимоясининг асосий схемалари. Филтрлайдиган маршрутлаштириш кўприкларининг асоси. Экранлашган кўприк асосида тармоқлараро экран.	Ёзма	[4]
13	Тармоқлараро экранларни ҳимоялашнинг дастурли усуллари.	1	Тармоқлараро экран вазифасини бажарувчи дастурий таъминот риволаниш тарихи, мавжуд дастурлар шарҳи	Ёзма	
14	Компьютер вируслари, уларнинг классификацияси ва курашиш механизмлари	1	Компьютер вируслари ва уларнинг классификацияси. Вируслар билан курашиш. Компьютер тизимларнинг вируслар билан захарланиш профилактикаси.	Ёзма	
15	Операцион тизимлар ва тармоқлардаги ахборот ҳавфсизлиги усуллари ва воситалари.	1	Операцион тизимлар фаолиятига ҳавф хатарлар. Компьютер тармоқларида ахборот ҳавфсизлигини таъминлаш хусусиятлари	Ёзма	

16	Компьютер тармоқларида ахборот ҳимоясининг хусусиятлари	1	Ахборот ҳимояси нуқтаи назаридан компьютер тармоқларини корпоратив ва умумфойдаланувчи тармоқларга ажратиш	Ёзма	
	Жами	16			

8. ОРАЛИҚ ВА ЯКУНИЙ НАЗОРАТ САВОЛЛАРИ

1. Ахборот хавфсизлигининг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).

2. Ахборот хавфсизлигининг йуналишлари (иқтисодий, муҳофаа, ижтимоий, экологик).

3. Ахборот хавфсизлиги таснифи ва ахборот ҳимояси мақсадлари (ишончлилиқ, аниқлилиқ, назорат қилиш турлари).

4. Ҳимоялаш тизимининг элементлари (ҳукукий, ташкилий, муҳандис – техник, дастурий – математик).

5. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).

6. Вирус ҳақидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).

7. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).

8. Антивирус дастурлари (детекторлар, вакциналар, прививкалар, ревизорлар, мониторлар).

9. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).

10. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).

11. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)

12. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, никоблаш).

13. Криптография ҳақида асосий тушунчалар (махфийилиқ, ўзгартиришлар, кодлаштириш, шифрлаш).

14. Очиқ калитли симметрияли криптотизимлар (калит, симметрия, очиқ канал, махфий канал).

15. Икки калитли криптотизимлар (асимметрия, калит, очиқ, ёпиқ, аутентик канал, шифрлаш, дешифрлаш)

16. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).

17. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).

18. Сехрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).

19. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).

20. Тасодикий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодикий, калитли, жадвал, сатр, устун)

21. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).

22. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).

23. Уитсоннинг икки кавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).

24. Гаммалаш шифрлари ва тасодикий кетма-кетлик генератори (шифр, гамма, қуйиш, тасодикий сон, конгруэнт, рекуррент).

25. Тармоқлараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар оқими, қабул, трафикни йуналтириш, заиф қисмлар, баёнлаштириш, аутентификация).

26. Тармоқлараро экраннинг асосий компонентлари (фильтрловчи-йулловчи, шлюзлар, тармоқ даражаси, амалий даража).

27. Электрон туловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуқонлар, банқлар).

28. Яратиладиган дастурларни норасмий нусхалашдан ҳимоялаш асослари (дастур, норасмий, нусха, калит, кўрсаткичлар).

29. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).

30. Жихозлар регистри бўйича шахсий компьютер аппарат таркибини аниқлаш асослари (хотира, ячейка, разряд, қиймат, адаптер, диск юритувчи).

9. «АХБОРОТ ХАВФСИЗЛИГИ» ФАНИ БҲЙИЧА ОРАЛИҚ ВА ЯКУНИЙ НАЗОРАТ ВАРИАНТЛАРИ(БИЛЕТЛАР).

9.1 ОРАЛИҚ НАЗОРАТ БИЛЕТЛАРИ

1-вариант

1. Ахборот хавфсизлигининг асосий тушунчалари (ахборот хавфсизлиги, ахборотнинг ҳимояси, ахборотни турқумлари).

2. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)

3. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).

2-вариант

1. Ахборот хавфсизлигининг йуналишлари (иктисодий, муқофаа, ижтимоий, экологик).

2. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, никоблаш).

3. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).

3-вариант

1. Ахборот хавфсизлиги таснифи ва ахборот химояси мақсадлари (ишончлилиқ, аниқлилиқ, назорат қилиш турлари).
2. Криптография ҳақида асосий тушунчалар (махфийилиқ, ўзгартиришлар, кодлаштириш, шифрлаш).
3. Уитсоннинг икки қавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).

4-вариант

1. Ҳимоялаш тизимининг элементлари (ҳукукий, ташкилий, муҳандис – техник, дастурий – математик).
2. Очiq калитли симметрияли криптолизимлар (калит, симметрия, очiq канал, махфий канал).
3. Гаммалаш шифрлари ва тасодифий кетма-кетлик генератори (шифр, гамма, қуйиш, тасодифий сон, конгруэнт, рекуррент).

5-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).
2. Икки калитли криптолизимлар (асимметрия, калит, очiq, ёпиқ, аутентик канал, шифрлаш, дешифрлаш)
3. Тармоқлараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар оқими, трафикни йўналтириш, заиф қисмлар, баёнлаштириш, аутентификация).

6-вариант

1. Вирус ҳақидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).
2. Симметрияли криптолизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).
3. Тармоқлараро экраннинг асосий компонентлари (филтрловчи-йулловчи, шлюзлар, тармоқ даражаси, амалий даража).

7-вариант

1. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).
2. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).
3. Электрон тўловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуқонлар, банқлар).

8-вариант

1. Антивирус дастурлари (детекторлар, фақлар, вакциналар, прививкалар, ревизорлар, мониторлар).
2. Сеҳрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).
3. Яратиладиган дастурларни норасмий нусхалашдан ҳимоялаш асослари (дастур, норасмий, нусха, калит, кўрсаткичлар).
4. Цезарнинг Афинна тизими бўйича фамилия ва исмингизни шифрланг. Калит сифатида $t = (3 * t + 5) \bmod 26$ формуладан фойдаланинг.

9-вариант

1. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).
2. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).
3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).

10-вариант

1. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).
2. Тасодифий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодифий, калитли, жадвал, сатр, устун)
3. Жихозлар регистри бўйича шахсий компьютер аппарат таркибини аниқлаш асослари (хотира, ячейка, разряд, қиймат, адаптер, диск юритувчи).

11-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).
2. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).
3. Икки калитли криптотизимлар (асимметрия, калит, очик, ёпиқ, аутентик канал, шифрлаш, дешифрлаш).

12-вариант

1. Ахборот хавфсизлигининг йўналишлари (иқтисодий, муҳофаа, ижтимоий, экологик).
2. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).
3. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).

13-вариант

1. Ахборот хавфсизлиги таснифи ва ахборот ҳимояси мақсадлари (ишончлилиқ, аниқлилиқ, назорат қилиш турлари).
2. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).
3. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).

14-вариант

1. Ҳимоялаш тизимининг элементлари (хукукий, ташкилий, муҳандис – техник, дастурий – математик).
2. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)
3. Сехрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).

15-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).
2. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, никоблаш).

3. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).

16-вариант

1. Вирус ҳақидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).
2. Криптография ҳақида асосий тушунчалар (махфийилик, ўзгартиришлар, кодлаштириш, шифрлаш).
3. Тасодифий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодифий, калитли, жадвал, сатр, устун)

17-вариант

4. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).
5. Очик калитли симметрияли криптотизимлар (калит, симметрия, очик канал, махфий канал).
6. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).
7. Криптографиянинг калитли сўз бўйича жадвалли ўрин алмаштириш усули ёрдамида фамилия ва исмингизни 3 сатр бўйича шифрланг.

18-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).
2. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).
3. Тармоқлараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар окимини, қабул, трафикни йуналтириш, заиф қисмлар, баёнлаштириш, аутентификация).

19-вариант

1. Ахборот хавфсизлигининг йўналишлари (иктисодий, муҳофаа, ижтимоий, экологик).
2. Уитсоннинг икки қавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).
3. Тармоқлараро экраннинг асосий компонентлари (филтрловчи-йўлловчи, шлюзлар, тармоқ даражаси, амалий даража).

20-вариант

1. Ҳимоялаш тизимининг элементлари (хукукий, ташкилий, муҳандис – техник, дастурий – математик).
2. Электрон тўловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуконлар, банклар).
3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).

21-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).
2. Криптография ҳақида асосий тушунчалар (махфийилик, ўзгартиришлар, кодлаштириш, шифрлаш).

3. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).

22-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).

2. Очик калитли симметрияли криптотизимлар (калит, симметрия, очик канал, махфий канал).

3. Уитсоннинг икки кавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).

23-вариант

1. Вирус ҳақидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).

2. Икки калитли криптотизимлар (асимметрия, калит, очик, ёпик, аутентик канал, шифрлаш, дешифрлаш)

3. Гаммалаш шифрлари ва тасодикий кетма-кетлик генератори (шифр, гамма, қўйиш, тасодикий сон, конгруэнт, рекуррент).

24-вариант

1. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).

2. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).

3. Тармоқлараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар оқими, қабул, трафикни йуналтириш, заиф қисмлар, баёнлаштириш, аутентификация).

25-вариант

1. Антивирус дастурлари (детекторлар, фағлар, вакциналар, прививкалар, ревизорлар, мониторлар).

2. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).

3. Тармоқлараро экраннинг асосий компонентлари (филтрловчи-йулловчи, шлюзлар, тармоқ даражаси, амалий даража).

26-вариант

1. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).

2. Сехрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).

3. Электрон туловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуқонлар, банқлар).

27 -вариант

1. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).

2. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўйиш, таянч сўз).

3. Яратиладиган дастурларни норасмий нусхалашдан ҳимоялаш асослари (дастур, норасмий, нусха, калит, қўрсаткичлар).

28 –вариант

1. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)
2. Тасодифий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодифий, калитли, жадвал, сатр, устун)
3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).

29 -вариант

1. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, ниқоблаш).
2. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).
3. Жихоздар регистри бўйича шахсий компьютер аппарат таркибини аниқлаш асослари (хотира, ячейка, разряд, қиймат, адаптер, диск юритувчи).

30 -вариант

1. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).
2. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).
3. Гаммалаш шифрлари ва тасодифий кетма-кетлик генератори (шифр, гамма, қуйиш, тасодифий сон, конгруэнт, рекуррент).

9.2. ЯКУНИЙ НАЗОРАТ БИЛЕТЛАРИ

**Ўзбекистон Республикаси Олий ва Ўрта махсус таълим вазирлиги
Самарқанд давлат университети**

Йўналиш: 5110700 –

информатика ўқитиш методикаси

Ўқув йили: 2017-2019

Курс: 1

Семестр: 2

Фан: «Ахборотларни ҳимоялаш»

1-вариант

1. Ахборот хавфсизлигининг асосий тушунчалари (ахборот хавфсизлиги, ахборотнинг ҳимояси, ахборотни туркумлари).
2. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)
3. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).
4. Криптографиянинг калитли сўз бўйича жадвалли ўрин алмаштириш усули ёрдамида фамилия ва исмингизни 3 сатр бўйича шифрланг.

Кафедра мудири:

проф. И.И.Жуманов

2-вариант

1. Ахборот хавфсизлигининг йуналишлари (иқтисодий, муҳофаа, ижтимоий, экологик).

2. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, никоблаш).

3. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).

4. Белгилар сони 9 та булган (бушлик белгиси ҳисобланмайди) матнни танланг ва уни 3x3 сеҳрли квадрат ёрдамида шифрланг.

3-вариант

1. Ахборот хавфсизлиги таснифи ва ахборот ҳимояси мақсадлари (ишончлилиқ, аниқлилиқ, назорат қилиш турлари).

2. Криптография ҳақида асосий тушунчалар (махфийилиқ, ўзгартиришлар, кодлаштириш, шифрлаш).

3. Уитсоннинг икки қавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).

4. Криптографик шифрлашнинг Цезар усули ёрдамида $k=4$ бўлганда фамилия ва исмингизни шифрланг.

4-вариант

1. Ҳимоялаш тизимининг элементлари (ҳукукий, ташкилий, муҳандис – техник, дастурий – математик).

2. Очик калитли симметрияли криптотизимлар (калит, симметрия, очик канал, махфий канал).

3. Гаммалаш шифрлари ва тасодикий кетма-кетлик генератори (шифр, гамма, қуйиш, тасодикий сон, конгруэнт, рекуррент).

4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун компьютер турини аниқлайдиган дастур тузинг.

5-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).

2. Икки калитли криптотизимлар (асимметрия, калит, очик, ёпиқ, аутентик канал, шифрлаш, дешифрлаш)

3. Тармоқлараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар оқими, трафикни йўналтириш, заиф қисмлар, баёнлаштириш, аутентификация).

4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун операцион тизим версиясини аниқлайдиган дастур тузинг.

6-вариант

1. Вирус ҳақидаги тушунчалар (дастури, зарарланган, хавфли, хавфсиз).

2. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).

3. Тармоқлараро экраннинг асосий компонентлари (филтрловчи-йулловчи, шлюзлар, тармоқ даражаси, амалий даража).

4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун компьютердаги доимий хотирани ишлаб чиқилган санасини аниқлайдиган дастур тузинг.

7-вариант

1. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).
2. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).
3. Электрон тўловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуконлар, банклар).
4. Виженер жадвалидан фойдаланиб, исми шарифингизни шифрланг.

8-вариант

1. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).
2. Сехрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).
3. Яратиладиган дастурларни норасмий нусхалашдан ҳимоялаш асослари (дастур, норасмий, нусха, калит, кўрсаткичлар).
4. Цезарнинг Афинна тизими бўйича фамилия ва исмингизни шифрланг. Калит сифатида $t=(3*t+5) \bmod 26$ формуладан фойдаланинг.

9-вариант

1. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).
2. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).
3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).
4. Икки марталик ўрин алмаштириш усули билан шифрлашга мисол келтиринг.

10-вариант

1. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).
2. Тасодифий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодифий, калитли, жадвал, сатр, устун)
3. Жихозлар регистри бўйича шахсий компьютер аппарат таркибини аниқлаш асослари (хотира, ячейка, разряд, қиймат, адаптер, диск юритувчи).
4. Трисемус усули билан фамилия ва исмингизнинг туғри келадиган қисмини шифрланг.

11-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).
2. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).
3. Икки калитли криптотизимлар (асимметрия, калит, очик, ёпиқ, аутентик канал, шифрлаш, дешифрлаш).
4. Плеифер тизими бўйича биграммаларга бўлинадиган сўзни шифрланг.

12-вариант

1. Ахборот хавфсизлигининг йуналишлари (иқтисодий, муҳофаа, ижтимоий, экологик).
2. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).
3. Симметрияли криптизмларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).
4. Уитсоннинг икки квадратлари бўйича шифрлашга мисол келтиринг.

13-вариант

1. Ахборот хавфсизлиги таснифи ва ахборот ҳимояси мақсадлари (ишончлилиқ, аниқлилиқ, назорат қилиш турлари).
2. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).
3. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).
4. Цезарнинг таянчли сўз асосидаги шифрлаш тизимида $k=5$ ва ДИПЛОМАТ калитли сўзлар билан матнни шифрлашга мисол келтиринг.

14-вариант

1. Ҳимоялаш тизимининг элементлари (ҳукукий, ташкилий, муҳандис – техник, дастурий – математик).
2. Стеготизмнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)
3. Сехрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).
4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун компьютер турини аниқлайдиган дастур тузинг.

15-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).
2. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, никоблаш).
3. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).
4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун операцион тизим версиясини аниқлайдиган дастур тузинг.

16-вариант

1. Вирус ҳақидаги тушунчалар (дастури, зарарланган, хавфли, хавфсиз).
2. Криптография ҳақида асосий тушунчалар (махфийилиқ, ўзгартиришлар, кодлаштириш, шифрлаш).
3. Тасодиқий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодиқий, калитли, жадвал, сатр, устун)
4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун компьютердаги доимий хотирани ишлаб чиқилган санасини аниқлайдиган дастур тузинг.

17-вариант

1. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).

2. Очик калитли симметрияли криптотизимлар (калит, симметрия, очик канал, махфий канал).

3. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).

4. Криптографиянинг калитли сўз бўйича жадвалли ўрин алмаштириш усули ёрдамида фамилия ва исмингизни 3 сатр бўйича шифрланг.

18-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).

2. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).

3. Тармоқлараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар оқими, қабул, трафикни йуналтириш, заиф қисмлар, баёнлаштириш, аутентификация).

4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун компьютер турини аниқлайдиган дастур тузинг.

19-вариант

1. Ахборот хавфсизлигининг йўналишлари (иқтисодий, муҳофаа, ижтимоий, экологик).

2. Уитсоннинг икки қавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).

3. Тармоқлараро экраннинг асосий компонентлари (филтрловчи-йулловчи, шлюзлар, тармоқ даражаси, амалий даража).

4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун операцион тизим версиясини аниқлайдиган дастур тузинг.

20-вариант

1. Ҳимоялаш тизимининг элементлари (ҳукукий, ташкилий, муҳандис – техник, дастурий – математик).

2. Электрон тўловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуконлар, банклар).

3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).

4. Цезарнинг Афинна тизими бўйича фамилия ва исмингизни шифрланг. Калит сифатида $t = (3 * t + 5) \bmod 26$ формуладан фойдаланинг.

21-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).

2. Криптография ҳақида асосий тушунчалар (махфийлик, ўзгартиришлар, кодлаштириш, шифрлаш).

3. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).

4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун компьютердаги доимий хотирани ишлаб чиқилган санасини аниқлайдиган дастур тузинг.

22-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).
2. Очиқ калитли симметрияли криптолизимлар (калит, симметрия, очиқ канал, махфий канал).
3. Уитсоннинг икки кавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).
4. Криптографиянинг калитли сўз бўйича жадвалли урин алмаштириш усули ёрдамида фамилия ва исмингизни 3 сатр бўйича шифрланг.

23-вариант

1. Вирус ҳақидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).
2. Икки калитли криптолизимлар (асимметрия, калит, очиқ, ёпиқ, аутентик канал, шифрлаш, дешифрлаш)
3. Гаммалаш шифрлари ва тасодикий кетма-кетлик генератори (шифр, гамма, қуйиш, тасодикий сон, конгруэнт, рекуррент).
4. Белгилар сони 9 та бўлган (бўшлик белгиси ҳисобланмайди) матнни танланг ва уни 3x3 сеҳрли квадрат ёрдамида шифрланг.

24-вариант

1. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).
2. Симметрияли криптолизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).
3. Тармоқлараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар оқими, қабул, трафикни йуналтириш, заиф қисмлар, баёнлаштириш, аутентификация).
4. Цезарнинг Афинна тизими бўйича фамилия ва исмингизни шифрланг. Калит сифатида $t = (3 \cdot t + 5) \bmod 26$ формуладан фойдаланинг.

25-вариант

1. Антивирус дастурлари (детекторлар, фағлар, вакциналар, прививкалар, ревизорлар, мониторлар).
2. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).
3. Тармоқлараро экраннинг асосий компонентлари (филтрловчи-йулловчи, шлюзлар, тармоқ даражаси, амалий даража).
4. Уитсоннинг икки квадратлари бўйича шифрлашга мисол келтиринг.

26-вариант

1. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).
2. Сеҳрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).
3. Электрон туловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуқонлар, банқлар).
4. Цезарнинг таянчли сўз асосидаги шифрлаш тизимида $k=5$ ва ДИПЛОМАТ калитли сўзлар билан матнни шифрлашга мисол келтиринг.

27 -вариант

1. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).

2. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).

3. Яратиладиган дастурларни норасмий нусхалашдан ҳимоялаш асослари (дастур, норасмий, нусха, калит, кўрсаткичлар).

4. Криптографиянинг калитли сўз бўйича жадвалли ўрин алмаштириш усули ёрдамида фамилия ва исмингизни 3 сатр бўйича шифрланг.

28 –вариант

1. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)

2. Тасодикий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодикий, калитли, жадвал, сатр, устун)

3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).

4. Белгилар сони 9 та булган (бўшлик белгиси ҳисобланмайди) матнни танланг ва уни 3x3 сеҳрли квадрат ёрдамида шифрланг.

29 -вариант

1. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, ниқоблаш).

2. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).

3. Жихоздар регистри бўйича шахсий компьютер аппарат таркибини аниқлаш асослари (хотира, ячейка, разряд, қиймат, адаптер, диск юритувчи).

4. Икки марталик ўрин алмаштириш усули билан шифрлашга мисол келтиринг.

30 -вариант

1. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).

2. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).

3. Гаммалаш шифрлари ва тасодикий кетма-кетлик генератори (шифр, гамма, қўйиш, тасодикий сон, конгруэнт, рекуррент).

4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун компьютердаги доимий хотирани ишлаб чиқилган санасини аниқлайдиган дастур тузинг.

10. “АХБОРОТ ХАВФСИЗЛИГИ” ФАНИДАН ТЕСТ ТОПШИРИКЛАРИ

1. Компьютерни вируслардан ҳимоя қилишда хавфсизликни таъминловчи қандай дастурлар қўлланади?

А. Windows Ливе ОнеСаре

*Б. Антивирус ва антишпион дастурий таъминотлар, ҳамда брандмауэр.

С. Мисрософт га оид тасодикий манзил фильтри

Д. Барча жавоблар тўғри.

2. Шифрлаштириш сузининг маъноси нима ?

*А. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн шифрланган матн билан алмаштирилади.

Б. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн жадвал билан алмаштирилади.

С. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн лотинча матн билан алмаштирилади.

Д. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн инглизча матн билан алмаштирилади.

3. Дешифрлаштириш сўзининг маъноси нима?

А. Дешифрлаштириш – бу матн маълумотларини ўзгартириш учун иккилик коди.

*Б. Дешифрлаштириш – шифрлаштиришга тескари жараён. Калит асосида шифрланган матн ўз ҳолатига узгартирилади.

С. Шифрлаштириш – бу график маълумотларни ўзгартириш учун саккизлик коди.

Д. Шифрлаштириш – бу график ва матнли маълумотларни ўзгартириш учун саккизлик коди

4. Калит – бу?

А. калит – матнларни тўсиқларсиз шифрлаш ва дешифрлаш учун керак бўлган маълумот

*Б. калит – матнларни тўсиқларсиз шифрлаш ва дешифрлаш учун керак бўлган ахборот

С. калит – матнларни тўсиқларсиз шифрлаш ва дешифрлаш учун керак бўлган ҳужжат

Д. калит – матнларни тўсиқларсиз шифрлаш ва дешифрлаш учун керак бўлган файл

5. Криптографик тизим

А. Очiq матнни Т ўзгартириш оиласи. Ушбу оиланинг аъзолари К белги билан белгиланади (К– калит)

Б. Ёпиқ матнни Т ўзгартириш оиласи. Ушбу оиланинг аъзолари К белги билан белгиланади (К– калит)

*С. Очiq матнни Т ўзгартириш оиласи. Ушбу оиланинг аъзолари индекслаштирилади ва К белги билан белгиланади (К– калит)

Д. Барча жавоблар тўғри

6. Симметрик криптотизимларда шифрлаш ва дешифрлашда қандай калит ишлатилади?

*А. Бир хил калит

Б. алоҳида калитлар

- С. ҳар хил калитлар
- Д. барча жавоблар нотўғри

7. Очик калитли тизимда шифрлаш ва дешифрлаш учун қандай калит ишлатилади?

- А. очик
- *Б. очик ва ёпик
- С. ёпик
- Д. барча жавоблар нотўғри

8. Калитларни тақсимлаш ва калит билан бошқариш терминлари қайси жараёнда тааллуқли?

- А. Ахборотни чиқаришнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади
- Б. Ахборотни киритишнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади
- *С. Ахборотни қайта ишлашнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади
- Д. Ахборотни ёзишнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

9. Электрон имзо – бу

- А. жадвалга бириктирилган криптографик ўзгартириш бўлиб бошқа фойдаланувчи эгалик қилмоқчи бўлганда унинг муаллифи ва ҳаққонийлигини текширилади
- Б. файлга бириктирилган криптографик ўзгартириш бўлиб бошқа фойдаланувчи эгалик қилмоқчи бўлганда унинг муаллифи ва ҳаққонийлигини текширилади
- С. кутубхонага бириктирилган криптографик ўзгартириш бўлиб бошқа фойдаланувчи эгалик қилмоқчи бўлганда унинг муаллифи ва ҳаққонийлигини текширилади
- *Д. матнга бириктирилган криптографик ўзгартириш бўлиб бошқа фойдаланувчи эгалик қилмоқчи бўлганда унинг муаллифи ва ҳаққонийлигини текширилади

10. Криптомустаҳкамлик – бу

- *А. Шифрнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир
- Б. Идентификаторнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир
- С. Коднинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир
- Д. Код ва идентификаторнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир

11. Криптомустаҳкамликнинг қанақа кўрсаткичлари мавжуд

А. –мумкин бўлган калитлар сони; –крипто таҳлил учун керакли бошланғич вақт;

*Б. –мумкин бўлган калитлар сони; –крипто таҳлил учун керакли ўртача вақт;

С. –мумкин бўлган калитлар сони; –крипто таҳлил учун керакли охириги вақт;

Д. барча жавоблар тўғри

12. Ахборотни ҳимоялаш мақсадида шифрлашнинг эффективлиги қуйдагилардан боғлиқ

А. Тўғри жавоблар йўқ

Б. Шифрни криптомустаҳкамлиги ва идентификаторларнинг сирини сақлашдан

*С. Шифрни криптомустаҳкамлиги ва калитнинг сирини сақлашдан

Д. Шифрни криптомустаҳкамлиги ва коднинг сирини сақлашдан

13. Шифрланган маълумот ўқилиши мумкин фақат

*А. Калити берилган бўлса

Б. Коди берилган бўлса

С. Идентификатори берилган бўлса

Д. Шифри берилган бўлса

14. Шифрланган хабарнинг маълум қисми ва унга мос келувчи очиқ матн бўйича ишлатилган шифрлаш калитининг керакли жараёнлар сонини аниқлаш қуйдагилардан иборат

А. мумкин бўлган калитларнинг дискрет сонидан кам бўлмаган

*Б. мумкин бўлган калитларнинг умумий сонидан кам бўлмаган

С. мумкин бўлган калитларнинг ҳақиқий сонидан кам бўлмаган

Д. мумкин бўлган калитларнинг мавҳум сонидан кам бўлмаган

15. Шифрланган ахборотни шарҳлаб беришда мумкин бўлган калитларни танлаш йўли учун зарур жараёнлар сони қуйдагиларни ўз ичига олади

А. Юқоридан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқади

Б. Қуйидан баҳолаш қаттиқ талаб қилинмайди; замонавий компьютерлар имконият чегарасидан чиқади

*С. Қуйидан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқади

Д. Қуйидан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқмайди

16. Калитларни сезиларсиз ўзгартириш қуйдагиларга олиб келиши мумкин

А. Хато бир хил калитни ишлатганда шифрланган маълумот кўриниши сезиларли ўзгариш олади

Б. Хато бир хил калитни ишлатганда шифрланган маълумот кўриниши сезиларли ва сезиларсиз ўзгариш олади

С. Хато бир хил калитни ишлатганда шифрланган маълумот кўриниши сезиларсиз ўзгариш олади

*Д. битта ва бир хил калитдан фойдаланганда ҳам шифрланган хабарлар сезиларли даражада ўзгаришга эга бўлади

17. Шифрлаш алгоритмининг элементлари тузилиши қуйидагиларни ўз ичига олади

*А. доимий (ўзгармас)

Б. ихчам

С. энг кўп

Д. энг кам

18. Шифрлаш жараёнида маълумотга киритиладиган қўшимча битлар

А. тўлиқ бўлмаган ва ишончли яширинган бўлиши керак

*Б. тўлиқ ва ишончли яширинган бўлиши керак

С. тўлиқ бўлмаган ва ишончсиз яширинган бўлиши керак

Д. барча жавоблар тўғри

19. Шифрланган матннинг узунлиги

А. Шифрнинг узунлигига тенг бўлиши шарт

Б. Шифрнинг узунлигига тенг бўлмаслиги шарт

*С. Берилган матннинг узунлигига тенг бўлиши шарт

Д. Берилган матннинг узунлигига тенг бўлмаслиги шарт

20. Қуйидагилар бўлмаслиги керак

А. шифрлаш жараёнида мунтазам қўлланадиган идентификаторлар орасида содда ва осонгина аниқлаш мумкин бўлган боғлиқлик

Б. шифрлаш жараёнида мунтазам қўлланадиган шифрлар орасида содда ва осонгина аниқлаш мумкин бўлган боғлиқлик

С. шифрлаш жараёнида мунтазам қўлланадиган кодлар орасида содда ва осонгина аниқлаш мумкин бўлган боғлиқлик

*Д. шифрлаш жараёнида мунтазам қўлланадиган калитлар орасида содда ва осонгина аниқлаш мумкин бўлган боғлиқлик

21. Мумкин бўлган тўпламлардан олинган ҳар қандай калитлар қуйидагини таъминлайди

*а) ахборотни ишончли ҳимоялаш

б) компьютерни ишончли ҳимоялаш

с) файлни ишончли ҳимоялаш

д) ахборот ва файлни ишончли ҳимоялаш

22. Симметрик криптотизим учун қандай усуллар қўлланилади?

а) моноалфавитли алмаштириш, ўрнини алмаштириш, гаммирлаш

б) кўпалфавитли алмаштириш, ўрнини алмаштириш, гаммирлаш

- *с) ўрнини алмаштириш, гаммирлаш, блокли шифрлаш
- д) ўрнини алмаштириш, гаммирлаш, блокли идентификаторлар

23. Цезарь алмаштиришнинг мазмуни қандай изоҳланади?

- а) Цезарь алмаштириш блокли шифрлаш гуруҳига қарашли
- б) Цезарь алмаштириш гаммирлаш гуруҳига қарашли
- *с) Цезарь алмаштириш моноалфавитли гуруҳига қарашли
- д) Цезарь алмаштириш кўпалфавитли гуруҳига қарашли

24. Алмаштиришлар қуйидагиларга ажралади

- *а) моно ва кўпалфавитли
- б) моноалфавитли
- с) кўпалфавитли
- д) тўғри жавоб йўқ

25. Маълумотларни ҳимоя қилиш тушунчасига

- *а) маълумотларнинг тўлиқлигини сақлаш ва маълумотга киришини бошқариш киради
- б) файлнинг тўлиқлигини сақлаш киради
- с) шифрнинг тўлиқлигини сақлаш киради
- д) коднинг тўлиқлигини сақлаш киради

26. Компьютерга вируслар қандай кириб келади?

- а) Файллар орқали, тузатиш вақтида, электрон хатларга бириктирилган файллар орқали, тармоқда мавжуд зарарланган юкланувчи дастурлар орқали, интерактив хизматлар орқали
- *б) Файллар орқали, нусха кўчирганда, электрон хатларга бириктирилган файллар орқали, тармоқда мавжуд зарарланган юкланувчи дастурлар орқали, интерактив хизматлар орқали
- с) Файллар орқали, матнни териш орқали, электрон хатларга бириктирилган файллар орқали, тармоқда мавжуд зарарланган юкланувчи дастурлар орқали, интерактив хизматлар орқали
- д) барча жавоблар тўғри

27. Антивирус дастурларини синовдан ўтказиш билан қандай ташкилот шуғулланади?

- а) Интел, Селерон
- б) Селерон, ИБМ
- *с) Компьютер хавфсизлиги миллий ассоциацияси НССА (Национал Сомпютер Сесуритй Ассосиатион)
- д) ИБМ, ИНТЕЛ

28. Фойдаланувчиларни идентификация қилиш қуйидагиларни аниқлайди

- *а) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш шкаласини

- б) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш графигини
- с) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш пароллини
- д) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш кодини

29. Маълумотларни физик ҳимоялаш кўпроқ

- а) ташкилий ва нотаъкилий чораларга қарашлидир
- *б) ташкилий чораларга қарашлидир
- с) нотаъкилий чораларга қарашлидир
- д) туғри жавоб йўқ

30. Ахборотга кириш ҳуқуқини узатиш ва ҳимоя қилиш воситалари қуйидаги

- а) Файллар мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди
- б) Браузерлар мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди
- с) Дифференциаллашган мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди
- *д) Маълумотлар билан дифференциаллашган мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди

31. Ҳимоя қилишнинг асосий муаммолари қуйидагилардан иборат

- *а) Ахборотга киришга йўл қўймаслик
- б) Файлга киришга йўл қўймаслик
- с) Шифрга киришга йўл қўймаслик
- д) Кодга киришга йўл қўймаслик

32. Пароллар усули

- а) энг оммавий ва қиммат, лекин ишончли ҳимояни таъминлайди
- б) энг оммавий лекин операцияли тизимга киришни ишончли ҳимояни таъминлайди
- *с) энг оддий ва арзон, лекин ишончли ҳимояни таъминлайди
- д) энг мураккаб лекин ишончли ҳимояни таъминлайди

33. Дастурий пароллар усули қуйидагини ўз ичига олади

- а) модулар бўйича чеклашларни аниқловчи бошқа дастурий усулларни
- б) маҳсулотлар бўйича чеклашларни аниқловчи бошқа дастурий усулларни
- с) пакетлар бўйича чеклашларни аниқловчи бошқа дастурий усулларни
- *д) кўриниши ва объектга рухсат бўйича чеклашларни аниқловчи бошқа дастурий усулларни

34. Дастурий пароллар тизимини қандай тасаввур этиш мумкин?

- *а) ҳар хил фойдаланувчилар учун қаралган кириш (рухсат) турларини аниқлайдиган жадвалли бошқариш кўринишидан кириши(рухсат) бўлиб ҳисобланади
- б) ҳар хил фойдаланувчилар учун қаралган кириш (рухсат) турларини аниқлайдиган функция кўринишидан кириши(рухсат) бўлиб ҳисобланади
- с) ҳар хил фойдаланувчилар учун қаралган кириш (рухсат) турларини аниқлайдиган идентификатор кўринишидан кириши(рухсат) бўлиб ҳисобланади
- д) ҳар хил фойдаланувчилар учун қаралган кириш (рухсат) турларини аниқлайдиган жадвал ва функция кўринишидан кириши(рухсат) бўлиб ҳисобланади

35. Маълумотларни шифрлаш усули қуйидагилар учун жудаҳам фойдали бўлиши мумкин

- а) рухсатсиз кириш модулларини мураккаблаштирмаслик учун
- б) рухсатли кириш модулларини мураккаблаштириш учун
- *с) рухсатсиз кириш модулларини мураккаблаштириш учун
- д) тўғри жавоб берилмаган

36. Шифрлаш алгоритми орқали қуйидаги кўзда тутилади

- а) ҳар бир функцияни алмаштириш
- б) ҳар бир идентификаторни алмаштириш
- с) ҳар бир тизимнинг модулини алмаштириш
- *д) алфавитнинг ҳар бир ҳарфини сон билан алмаштириш

37. Автоматик қайта чакирув усули гоёси қуйидагидан иборат

- а) марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – шифр талаб этилади
- *б) марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – идентификацион код талаб этилади
- с) марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – шифр талаб этилмайди
- д) марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – парол ва шифр талаб этилади

38. Тизимни бузишнинг моҳияти нима?

- а) Хакерлик фаолиятининг шундай қуринишики, бунда фойдаланувчи юкори махоратга эга булмаган абонент сифатида тизимда руйхатдан утган булади.
- *б) Хакерлик фаолиятининг шундай қуринишики, бунда бузувчи юкори махоратга эга булмаган абонент сифатида тизимда руйхатдан утган булади.
- с) Хакерлик фаолиятининг шундай қуринишики, бунда абонент юкори махоратга эга булмаган абонент сифатида тизимда руйхатдан утган булади.
- д) Барча жавоблар тугри.

39. Узок (олис)лаштирилган масофадан бузиш нима?

- а) Хаваскорлик фаолияти
- б) Абонентлик фаолияти
- *с) Хакерлик фаолияти
- д) Фойдаланувчи фаолияти

40. Хакер (хаскер) нима?

- *а) хакер – бу булаётган ходисаларга кушилишни истайдиган одам учун умумий таъриф
- б) хакер – ШК фойдаланувчиси
- с) хакер – бу Интернет абоненти
- д) хакер – бу булаётган ходисаларга кушилишни истамайдиган одам учун асосий таъриф

41. Бузувчи (взломщик) нима?

- а) сраскер - хакер
- *б) сраскер – интродер (коида бузувчи)
- с) сраскер - Пинг
- д) сраскер - домаин

42. Тизимни бузишга ёки узгартиришга ҳаракат қиладиган одамлар ким деб аталади?

- *а) хакер, кракер
- б) хакер, фойдаланувчи
- с) абонент, кракер
- д) хаваскор, фойдаланувчи

43. “Инструтион Детестион Сйстем” нима?

- а) Хужумни аниклаш дастури
- б) Хужумни аниклаш модули
- *с) Хужумни аниклаш тизими
- д) Хужумни аниклаш пакети

44. Тармок даражасидаги аниклаш тизими қуйидагиларни текширади?

- *а) Тармок доирасидаги пакетлар ва ёвуз ниятлининг химояланадиган тизим ичига кириш ҳолатини аниклайди
- б) Тармок доирасидаги дастур ва ёвуз ниятлининг химояланадиган тизим ичига кириш ҳолатини аниклайди
- с) Тармок доирасидаги модул ва ёвуз ниятлининг химояланадиган тизим ичига кириш ҳолатини аниклайди
- д) барча жавоблар тугри

45. Қайси тизимлар мақсад ёмон ниятли кишиларни алдаш учун псевдо-сервислар билан ишлайди.

- *а) алмаштириш тизими
- б) регистрацион тизим
- с) хужумларни ушлаш тизими

д) бутунлигини назорат килиш тизимлари

46. Тармок даражасида химояланишнинг техник усуллари куйидагиларга булинадилар:

- *а) аппаратли, дастурли, аппарат-дастурли
- б) ташкиллаштирилган, тизимли, аппаратли
- с) аппарат-дастурли, тизимли, дастурли
- д) тугри жавоб йук

47. Ахборот химояси деганда куйидагилар тушунилади:

- *а) Бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик жараён
- б) Бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик процедураси
- с) Бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик услуги
- д) Барча жавоблар тугри

48. Ахборотлар тарқалиш канали – бу:

- а) Манбаларнинг ёпиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар ҳисобланадилар
- *б) Манбаларнинг очиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар ҳисобланадилар
- с) Манбаларнинг ёпиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар ҳисобланадилар
- д) Тугри жавоблар йук

49. Ахборотлар тарқалиш техник каналлари – бу:

- а) Акустик ва вироакустик, электрик, телеканаллар, оптик
- б) Акустик ва вироакустик, электрик, серверлар, оптик
- *с) Акустик ва вироакустик, электрик, радио каналлар, оптик
- д) Акустик ва вироакустик, электрик, теле каналлар, провайдерлар

50. Товушли ахборотлар тарқалишининг эҳтимоллик каналлари куйидагиларга булинади:

- а) Ер усти, радио тулкили, микросейсмик, электроакустик, оптоэлектро-акустик
- б) Ер усти, телекоммуникацион, микросейсмик, электроакустик, оптоэлектро-акустик

с) космик, радио тулкинли, микросейсмик, элетроакустик, оптоэлектро-акустик

*д) самовий, вибрацияли, микросейсмик, электроакустик, оптоэлектро-акустик

11. БАҲОЛАШ МЕЗОНЛАРИ ВА РЕЙТИНГ НАЗОРАТЛАРИ ГРАФИГИ

11.1. БАҲОЛАШ МЕЗОНЛАРИ

«Ахборотларни ҳимоялаш» фани бўйича жорий назоратларда талабалар билими ва амалий кўникма даржасини аниқлаш мезони

(мах балл – 35)

Максимал балл	Назорат қилинадиган ва баҳоланадиган иш турлари	Баҳолашда эътибор қаратиладиган жихатлар
1-жн		
7	Мавзулар бўйича назарий тайёргарлик даражаси ва дарсадаги фаоллик	Асосий тушунчалар, таърифлар, ахборот хавфсизлиги усуллари билиш, амалда қўллай олиш, моҳиятини тушуниш, ижодий фикрлай олиш, билимларни амалда қўллай олиш
7	Уйга берилган топшириқларни бажариш сифати	Топшириқларни тўғри ва тўлиқ бажариш, масалаларни ҳал қилишга ижодий ёндашиш, тушунтириб бера олиш
14	Назорат ишларини бажариш сифати	Топшириқларни тўғри ва тўлиқ бажариш, ижодий ёндашиш, мустақил фикрлаш, ечимни асослай олиш
7	Мустақил топшириқларни бажариш сифати	Берилган топшириқни тўғри ва тўлиқ бажариш, мустақил мулоҳаза юрита олиш, билимларни амалда қўллай олиш, масалага ижодий ёндашиш, моҳиятини тушуниш ва айтиб бера олиш
35		

«Ахборотларни ҳимоялаш» фани бўйича оралик ва якуний назоратларда талабалар билими ва амалий кўникма даржасини аниқлаш мезони

(ОН бўйича мах балл – 35, ЯН бўйича мах балл – 30)

Саволлар		ОН (мах балл)	ЯН (мах балл)	Баҳолашда эътибор қаратиладиган жихатлар
		1-ОН		
Назарий	1	7	6	Асосий тушунчалар, таърифлар, ахборот хавфсизлиги усуллари билиш, амалда қўллай олиш, моҳиятини тушуниш, тасаввур қилиш ва айтиб бера олиш, ижодий фикрлай олиш ва мустақил мулоҳаза юрита олиш
	2	7	6	
Амалий	3	7	6	Топшириқларни тўғри ва тўлиқ бажариш, ижодий ёндашиш, мустақил фикрлаш, ечимни асослай олиш, моҳиятини тушуниш
	4	7	6	
Мустақил иш	5	7	6	Саволга тўлиқ ва тўғри жавоб бериш, мисоллар билан асослаш, ижодий ёндашиш, моҳиятини тушуниш ва тушунтириб бера олиш

Жами	35	30	
------	----	----	--

«Ахборотларни ҳимоялаш» фани бўйича рейтинг назоратларида ўзлаштириш
кўрсаткичини аниқлаш мезони

ЖН	ОН	ЯН	Баҳолашларда эътибор қаратиладиган асосий жихатлар
31-35 балл	31-35 балл	27-30 балл	Асосий тушунча, таъриф, алгоритмларни тузиш, алгоритмларни амалга ошириш усуллари билиш, мохиятини тушуниш, ижодий фикрлай олиш, тасаввурга эга бўлиш, айтиб бера олиш, мустақил мулохаза юрита олиш, топшириқларни аниқ ва тўғри бажариш
25-30 балл	25-30 балл	22-26 балл	Асосий тушунча, таъриф, алгоритмларни тузиш усуллари билиш, ижодий ёндашишга ҳаракат қилиш, тасаввурга эга бўлиш, топшириқларни тўғри бажариш ва тушунтириш
19-24 балл	19-24 балл	17-21 балл	Асосий тушунча, таъриф, алгоритмларни билиш ва амалда қўллай олиш, мохиятини биров тушуниш ва тўлиқ бўлмаган тасаввурга эга бўлиш. Амалий топшириқларни деярли тўғри бажариш ва тушунтириб беришга ҳаракат қилиш.
0-19 балл	0-19 балл	0-15 балл	Асосий тушунча, таърифларни тўлиқ билмаслик ва амалда қўллай олмаслик, етарлича тасаввурга эга бўлмаслик ва тушунтира олмаслик, топшириқларни тўлиқ бажармаслик ва қўпол хатоликларга йўл қуйиш.

РЕЙТИНГ НАЗОРАТЛАРИ ГРАФИГИ

САМАРҚАНД ДАВЛАТ УНИВЕРСИТЕТИ АМАЛИЙ МАТЕМАТИКА ВА ИНФОРМАТИКА ФАКУЛЬТЕТИ

«Ахборотлаштириш технологиялари» кафедраси «Ахборотларни химоялаш» фани бўйича рейтинг назоратлари ГРАФИГИ

*Таълим йўналиши: Информатика ўқитиш методикаси (1-курс)
Умумий ўқув соати-60, шундан маъруза-14 соат, амалиёт-18 соат,
лабаратория иши – 28 соат*

2017-2019 ўқув йили
2-семестр

Ишчи ўқув дастуридаги мавзулар тартиб рақами	Умумий соат					Баҳолаш тури	Назорат шакли	Балл		Муддати (хафта)
	Маъруза	Амал.машғулот	Лабаратория	Мустақил иш	Жами			Макс. балл	Сарал. балл	
1-модул										
1-10	14	18	28		60	1-ЖБ	Кундалик назорат, Назорат ва лаборатория иши, уй иши	35		апрель 4-хафта
Қўшимча мавзу бўйича реферат						1-МБ	Химоя			
						1-ОБ	Ёзма назорат	35		
Жами	14	18	28		60			70	39	
						ЯБ	Ёзма	30		июль жадвал бўйича
						Жами		100	55	

12. ГЛОССАРИЙ

Ўзбекистон Республикаси
Олий ва ўрта махсус таълим вазирлиги

Самарқанд Давлат университети

**“Ахборотларни ҳимоялаш” фанидан
атамалар лўғати**

САМАРҚАНД - 2017 йил

Амалий дастурлар - фойдаланувчиларга компьютерда маълум амалларни бажаришга имкон берувчи дастурий воситалардир.

Антивируслар. Вирус-дастурларни излаб топувчи ва уларни зарарсизлантирувчи дастурий воситалардир.

Арифметик-мантикий мослама - барча арифметик ва мантикий амалларни бажаришга хизмат қилади. Қўшувчи сумматор ва маҳаллий бошқариш регистрларидан ташкил топган.

Архивлаш воситалари (ёки архиваторлар) - махсус усуллар билан файлларнинг ҳажмини қисиб, кичрайтиришга, яъни уларнинг архивларини ташкил қилишга хизмат қилувчи воситалардир.

Архивни янгилаш - архивдаги файлларнинг ескироқ версияси устига янги версиясини ёзиш.

Ахборот тармоғи - алоқа тизимларида компьютерларнинг бир-бири билан боғланиши.

Ахборот технологияси фани - ахборотларни жамлаш, сақлаш, узатиш ва шу жараёнларни амалга оширувчи техник воситаларни ишлатишни ўргатувчи фан.

Ахборот тизими - белгиланган мақсадга еришиш учун ахборотларни шакл ва мазмунига кўра турларга ажратиш, уларни сақлаш, излаш ва қайта ишлаш принциплари, қайта ишлашда қўлланиладиган усуллар, шахслар ҳамда воситаларнинг ўзаро боғланган мажмуи.

Баённома (протокол) - компьютерлар орасида маълумотларни узатиш тартиби ва форматини белгилувчи қоидалар мажмуи.

Белгили маълумот - алифбо-рақамли белгилар мажмуидан иборат маълумот тури.

Билимлар омбори - аниқ бир фан соҳасида тўпланган билимларни компьютерда тасвирлаш ва қайта ишланган ахборотларни сақлашга мўлжалланган модел.

Билимлар омборини бошқариш тизими - маълумотлар омборини яратиш, юритиш ва фойдаланишга мўлжалланган дастур ва тил воситалари мажмуи.

Биологик бошқариш - ҳайвонот оламининг сақланиши, кўпайиши ва ривожланишини режали равишда тартибга солиш мақсадида биологик тизимларга ўтказиладиган таъсирдир.

Биологик модел - объектлар ва уларнинг қисмларига хос биологик тузилиш, функция.

Бош калит - маълумотлар омборида саралаш ишларининг тез ва аниқ бажарилишига имкон берадиган жадвалнинг бир устуни.

Дастурий интерфейслар - компьютер қурилмалари билан фойдаланувчи ишлатаётган дастурларнинг ҳамжиҳатликда ишлашини таъминловчи воситалардир.

Диагностика воситалари. Компютер қурилмаларининг ва магнит дискларининг ишлаш қобилиятларини ва ҳолатларини текширувчи ҳамда улардаги нуқсонли жойларни аниқлаб, иложи борида тузатувчи воситалардир.

Фойдаланувчи интерфейси - берилган масалага мос интерфейсни танлаш.

Фойдаланувчи муҳити - интерфейс тушунчасининг бошқача номланиши.

Информатика - ахборотлаштириш жараёнларини ҳамда шу жараёнларни автоматлаштириш усулларини ўргатувчи фан сифатида намоён бўлмоқда.

Интеллект - инсоннинг тафаккур юритиш қобилиятидаги (ақл, онг).

Интеллектуал ахборотли излаш тизимлари - иш жойидан туриб билимлар омбордаги керакли ахборотни излашга имкон берадиган тизимлар.

Интеллектуал интерфейс - интерфейс тушунчасини бошқача номланиши.

Интеллектуал китоблар - имтиҳон олувчи китобларга ўхшаш бўлиб, бунда ўқувчиларнинг қобилиятлари, билим даражалари махсус тестлар ёрдамида уларнинг компютер билан мулоқати жараёнида аниқланади ва баҳоланади.

Интеллектуал тизимлар - инсоннинг мантикий фикрлаш усулини қўллаган ҳолда масалани ечадиган тизимлар.

Ишчи тизимлар - катта миқдордаги маълумотларни сақлаш, излаш, мураккаб ҳисоблашлар, моделлаштириш, дастурий таъминотни ривожлантиришга хизмат қиладиган воситалар.

Ишонтира олишлик хоссаси. Ҳар қандай информация бошқариш органи ишона оладиган даражада яъни бошқарилаётган объектнинг имконияти даражасида бўлиши керак. Имконият даражасидан четга чикувчи ҳар қандай информация бошқариш жараёнининг бузилишига олиб келади.

Кодлаш - узлуксиз сигнални рақамлар орқали ифодалаш жараёни.

Компютерли моделлаштириш - ҳодиса ва жараёнларнинг моделини компютерда куриш ва ўрганиш.

Маълумотлар базаси билан ишлаш воситалари. Турли маълумотлар базаларини ташкил қилиш, уларни бошқариш, улар устида турли амалларни бажариш (гуруҳлаш, тартибга солиш, нусха олиш ва ҳ.к.) ҳамда зарур маълумотларни турли мезонлар орқали (калит сўзлар, саналар, фан йўналишлари, мавзулар, муаллифнинг исми ва шарифи ва ҳ.к.) тезда излаб топиб беришга хизмат қилувчи воситалардир.

Маълумотлар модели - ахборотларни ифодаловчи воситалар мажмуи.

Маълумотлар омбори - компютернинг узоқ муддатли хотирасида сақланаётган берилганлар ва улар устида аниқ амалларни бажаришга имкон берадиган маълумотлар йиғиндиси.

Маълумотлар омборидаги доимий маълумотлар - маълумотлар омборининг узоқ муддат ўзгармай қоладиган элементлари.

Маълумотлар омборидаги ўзгарувчан маълумотлар - маълумотлар омборининг қиймати тез-тез ўзгартириб турадиган элементлари.

Маълумотлар омборини бошқариш тизими - маълумотлар омборидан фойдаланиш учун махсус яратилган дастур.

Маълумотлар омборини бошқаришнинг иерархик тизими - маълумотларнинг иерархик тизимини яратиш ва ундан фойдаланиш учун мўлжалланган маълумотлар омборини яратиш тизими.

Маълумотлар омборини бошқаришнинг реляцион тизими - маълумотларнинг реляцион тизимини яратиш ва ундан фойдаланиш учун мўлжалланган маълумотлар омборини яратиш тизими.

Маълумотлар омборини бошқаришнинг тармоқли тизими - маълумотларнинг тармоқли тизимини яратиш ва ундан фойдаланиш учун мўлжалланган маълумотлар омборини яратиш тизими.

Маълумотларни чегириш - ахборотлар тизимида кўрсатилган шартни қаноатлантирмаган элементларнинг маълумотлар омборига киритмай қолдириш ҳолати.

Маълумотларни тартиблаш - маълумотлар қиймати ва форматини фойдаланиш учун қулай ҳолатга келтириш жараёни.

Маъмурият тизимлари - тармоқни бошқарадиган тизимлар.

Математик модел - ўрганилаётган объектнинг математик формула ёки алгоритм кўринишида ифодаланган характеристикалари орасидаги функционал боғланиш.

Модел - бирор объект ёки объектлар тизимининг образи ёки намунаси.

Моделлаштириш - билиш объектларини уларнинг моделлари ёрдамида тадқиқ қилиш, мавжуд предмет ва ҳодисаларнинг моделларини яшаш ва ўрганиш.

Объект - ўзига ўхшашларидан ажралиб турадиган алоҳида олинган предмет.

Қимматлилиқ хоссаси. Бир мақсадга хизмат қилувчи бир нечта информация ичидан энг мақсадга мувофиқлари, яъни қимматлилари танлаб олиниши керак.

Қисқалиқ хоссаси. Информация қисқа ва мазмундор бўлиши, яъни унда ортиқча маълумотлар ёки такрорланишлар бўлмаслиги керак. Бу еса бошқаришни тез ва обектив кечишини таъминлайди.

Сонли маълумот - ихтиёрий сондан иборат маълумот тури.

Тўлалик хоссаси. Информациалар шароитга қараб, жаҳон фан ва техникасининг сўнги ютуқлари ҳамда бошқариш жараёнида тўпланган тажрибаларни ҳисобга олиб, узлуксиз равишда ўзгартирилиб, янгиланиб, тўлдирилиб борилиши керак. Бу еса бошқаришда замонавий усуллардан кенг фойдаланиш имконини беради ва объектнинг ҳар қандай ўзгаришларига бардошлиги, мослашиши даражасини оширади.

Тушунарлилик хоссаси. Информация - бошқариш органи (яъни ЕХМ) тушуна оладиган ҳолатда (сараланган, кодлаштирилган, информация ташувчи воситаларга ёзилган) бўлиши, яъни дастлабки қайта ишлашдан ўтган бўлиши керак.

Ахборот манбаларига стратегик хужумлар - кўпинча, бир-бири билан уруш ҳолатида бўлган давлатларнинг бир-бирига нисбатан амалга оширилувчи ахборотий хужумларидир. Бундай ҳаракатларнинг асосий мақсади, рақиб давлатнинг ҳарбий аҳамиятга ега бўлган ахборот тизимларига кириб бориб, уларни ишдан чиқариш ёки уларда сақланаётган стратегик маълумотларни ўғирлаш ва йўқотишдир.

Бош калит - маълумотлар омборида саралаш ишларининг тез ва аниқ бажарилишига имкон берадиган жадвалнинг бир устуни.

Бошқариш мосламаси - енг мураккаб мослама бўлиб, барча қурилмалардан келувчи сигналларни қайта ишлайди ва бошқарувчи буйруқларни ишлаб чиқади, уларни керакли қурилмаларга узатади ҳамда шу буйруқларнинг бажарилишини назорат қилиб боради.

Бошқариш органи - системани қўйилган мақсадга мувофиқ бошқариш учун зарур тадбирлар, буйруқлар ишлаб чиқувчи ҳамда уларнинг бажарилишини назорат қилиб турувчи бўлимдир.

Бошқариш тизими - бошқариш субъектлари - бошқарувчи тизимлар ва бошқариш объектлари - турли табиатли мураккаб динамик тизимлар мажмуи.

Чувалчанг («Черви») - бошқа дастурий воситаларни зарарламовчи, фақат ўзидан нусха олиб кўпаювчи вируслардир. Бундай вирусларнинг таъсири натижасида компьютер хотираси бегона файллар билан (вирус-дастурларнинг нусхалари билан) тўлиб қолиб, унинг самарадорлиги кескин пасаяди.

Диагностика воситалари. Компютер қурилмаларининг ва магнит дискларининг ишлаш қобилятларини ва ҳолатларини текширувчи ҳамда улардаги нуқсонли жойларни аниқлаб, иложи борича тузатувчи воситалардир.

Доктор ревизорлар - файл ва дискнинг тизимли соҳасидаги ўзгаришларни аниқлаш билан бирга, ўзгарган файлларни дастлабки ҳолатига қайтара оладиган вирусга қарши дастурлар.

Электрон котиблар. Бундай компютерлар - манзилгоҳлар, телефон рақамлари, жорий ишлар рўйхати, кун тартиби каби иш фаолиятида тез-тез зарур бўлиб турадиган электрон маълумотларни ташкил қилиш ва сақлашга хизмат қилувчи компютерлардир.

Электрон ёзув дафтарчалари. Электрон хотира дафтарчалари деб ҳам аталади. Электрон котиблар каби вазифаларни бажаради. Лекин улардан фарқи шундаки, бундай компютерларда айрим амалларни бажариш учун фойдаланувчи тамонидан дастур тузилмайди. Улар фақат хотирасига ёзилган стандарт амалларнигина бажариши мумкин.

Факс-серверлар - фойдаланувчиларга кўп адресли электрон факсимил алоқа хизматидан фойдаланишга имкон берувчи серверлар.

Фактографик тизим - содда ва қўйилган масалаларга ягона ҳамда аниқ ечимни кўрсата оладиган тизим.

ФАТ вируслари - ФАТ жадвалини ишдан чиқарувчи, яъни файлларнинг дискда жойлашувини кўрсатувчи жадвални ўзгартирувчи ёки йўқотувчи вируслар.

Файлли дискеталар - фойдаланувчининг файлларини сақловчи дискеталар.

Файл-менеджерлар - фойдаланувчининг МСДОС бошқарувида компютер билан

кулай ва кўргазмали равишда мулоқот олиб боришини таъминловчи дастурий воситалардир. Кўпинча «қобиқ» *дастурлар* деб ҳам айтилади.

Файл-серверлар - фойдаланувчиларга турли ахборот тизимларидаги файллар билан ишлашга имкон берувчи серверлар.

Филтр дастурлар ёки резидент дастурлар - вируслар томонидан зарарни кўпайтириш ва зиён етказиш мақсадида операцион тизимга қилинаётган мурожаатларни ушлаб қолиш ва улар ҳақида фойдаланувчига маълум қилиш вазифасини бажарувчи вирусга қарши дастурлар.

Гибрид вируслар - резидент файлли вирусларнинг ҳамда кўринмас вирусларнинг барча хусусиятларини ўзида мужассамлаштирган вируслар.

Ҳимоя филтрлари - фойдаланувчини мониторларнинг электрон-нурли трубкасидан тарқалаётган нурланишлардан (электромагнит, рентген, инфрақизил, ултрабинафша, радиочастотали) ҳимоя қилувчи воситалар.

Интернет - минглаб локал ва минтақавий компьютер тармоқларини бир бутун қилиб бирлаштирувчи бутун дунё компьютер армоғи.

Интернетнинг ахборотли қисми - Интернет тармоғида мавжуд бўлган турли электрон ҳужжат, график расм, аудиоёзув, ведеотасвир ва ҳоказо кўринишидаги ахборотлар мажмуи.

Интернетнинг дастурий таъминоти - тармоққа уланган компьютерлар ва тармоқ воситаларини ягона стандарт асосида мулоқот қилиш, маълумотларни ихтиёрий алоқа канали ёрдамида узатиш даражасида қайта ишлаш, ахборотларни қидириб топиш ва сақлаш ҳамда тармоқда ахборот хавфсизлигини таъминлаш каби муҳим вазифаларни амалга оширувчи дастурлар мажмуи.

Интернетнинг техник таркибий қисми - турли русумдаги компьютерлар, алоқа каналлари, тармоқ техник воситалари мажмуи.

Интранет - Интернет технологияси, дастур таъминоти ва баённомалари асосида ташкил етилган, маълумотлар омбори ва электрон жадваллар билан жамоа бўлиб ишлаш имконини беърувчи корхона ёки ташкилот миқёсидаги компьютер тармоғи.

Кўринмас вируслар - резидент вирусларга ўхшайди, лекин улар ўзларининг борлигини сездирмасликка ҳаракат қилади яъни ўзларининг борлигини турли усуллар билан никобловчи вируслар.

Компютер вируслари - компютерда турли нохуш амалларни бажаришга мўлжаллаб ёзилган, ўлчами катта бўлмаган дастурлар.

Мантикий «бомба» - махсус ўрнатилган санада ёки белгиланган шарт бажарилмаганда (масалан, вирус-дастур муаллифининг маоши оширилмаганда) ишга тушувчи вируслар.

Парол билан архивлаш - бегона фойдаланувчилар очмасликлари учун файлга парол қўйиб архивлаш.

Ревизор дастурлар - дастлаб дастур ва дискнинг тизимли соҳаси ҳақидаги маълумотларни хотирага олиб, сўнгра уларни дастлабкиси билан солиштирадиган ва мос келмаган ҳолларда фойдаланувчига маълум қиладиган вирусга қарши дастурлар.

Шифрланган вируслар - ҳар бир таъсир қилиш сиклидан кейин ўзининг кодланишини ҳам, жойлашишини ҳам ўзгартириб турувчи вируслар.

Шлюз - баённомани бир турдаги муҳитдан иккинчи турдаги муҳитга ўтказувчи тармоқ қурилмаси.

Тўлиқ ҳимоя филтрлари - енг юқори сифатли филтрлардан бўлиб, махсус қопламали ойнадан тайёрланган. Барча нурланишларнинг таъсирини 70-80% гача камайтиради. Тўрли филтрлар - нурланишлардан яхши ҳимоя қила олмайди. Лекин улар кўзни ташқи ёритиш шуълаларидан ва экраннинг милтиллашидан ҳимоя қилиши мумкин.

Тозаловчи дискета - оддий дискетага ўхшаш бўлиб, фақат дискининг сатҳи махсус жилвир қоғоз билан қопланган дискета. Бундай дискета дисководнинг ўқувчи ва ёзувчи магнит каллакчасини турли ифлосликлардан, дисковод кўп ишлатилганда пайдо бўладиган оксидловчи қатламдан тозалашга хизмат қилади. Бунинг учун дискета дисководга ўрнатилиб, сунгра дисковод ишга туширилади.

Троя оти - ўзини оддий дастурлардек тутувчи, бузғунчилик фаолиятини еса фақат маълум амал бажарилгандагина (масалан, нусха олиш амали, файлни босмага чиқариш амали ва ҳ.к.) бошловчи вируслар.

Тузилган архив файлни текшириб кўриш - архив файлнинг зарарланган ёки зарарланмаганлигини ҳамда зарарланиш даражасини махсус буйруқ ёрдамида текшириш.

УнЕrase Визард - тасодифан ўчириб юборилган файлларни қайта тиклашга имкон берувчи восита.

Утилитлар - тизим дастурлар сафига кирувчи дастурий воситаларлар. Компютернинг ҳамда унинг қурилмаларининг самарали ишлашини таъминлашга хизмат қилади.

Юкловчи сектор вируслари - дисклар ёки дискеталарнинг юкловчи секторини ишдан чиқаришга мўлжалланган, яъни шу секторларда жойлашган тизимли дастурларни зарарловчи вируслар.

Адабиётлар

1. Леонтьев В.. Новейшая энциклопедия персонального компьютера. -М.: Олма пресс образование, Москва. -2005.
2. Қобулов В.Қ. Ақл мўжизаси. - Т.: Фан, Тошкент. - 1984.
3. Жуманов И.И., Мингбоев Н.С.. Информатика. Услубий қўлланма. – Самарқанд: СамДУ. - 2002.
4. Нурмухаммедов Т.А. ИБМ ПС ва МС ДОС билан ишлаш. - Т.: Фан, Тошкент – 1995.
5. Ғуломов С.С., Шермухаммедов А.Т., Бегалов Б.А. Иқтисодий информатика. – Т.: “Ўзбекистон”, Тошкент. – 1999.
6. Бройдо В.Л. Офис техникаси (бошқариш ва иш юритиш учун). – Т.: Меҳнат, Тошкент. - 2001.
7. Қобилов С.С., Жуманов И.И. СУБД и информაციонные системы. – Самарқанд: СамДУ. - 1997.
8. Арипов М. Интернет ва электрон почта алоқаси. - Т.: «Университет».- 2000.
9. Жуманов И.И., Мингбоев Н.С. Ҳисоблаш системаларининг информაციон асослари. – Самарқанд: СамДУ. – 2002.
10. Ғуломов С.С. ва бошқалар. «Иқтисодий информатика». - Т.: Фан - 1999.
11. Рахмонқулова С.И. ИБМ ПС шахсий компютерида ишлаш. - Т.: Фан, Тошкент – 1999.
12. Насретдинова Ш. Windows учун Excel саҳифаларида. - Т.: Фан. – 1999.
13. Фигурнов В.Э. ИБМ ПС для пользователя. - М.: Инфра, 1996.
14. Шафрин Ю. Основы компьютерной технологии. - Б.: Туркистон, Бишкек. – 1998.

13. МАЪРУЗА МАШҒУЛОТЛАРИ ДАРС ИШЛАНМАСИ

Самарқанд Давлат университети

“Ахборотлаштириш технологиялари” кафедраси

Туракулов И.Н.
Химматов И.Қ.

Ахборотларни ҳимоялаш фанидан

маъруза машғулотлари ишланмаси

САМАРҚАНД — 2017

**1 - МАЪРУЗА: ЗАМОНАВИЙ АХБОРОТЛАШГАН ЖАМИЯТ ВА
АХБОРОТ ХАВФСИЗЛИГИ. АСОСИЙ ТУШУНЧАЛАР ВА ТАЪРИФЛАР**

РЕЖА

- 1. Ахборот хавфсизлигига кириш;*
- 2. Предметнинг асосий тушунчалари ва мақсади;*
- 3. Ахборотларга нисбатан хавф-хатарлар таснифи;*
- 4. Тармок хавфсизлигини назорат қилиш воситалари*

Дарснинг ўқув ва тарбиявий мақсади: Талабаларга ахборот хавфсизлигининг асосий тушунчалари билан таништириш; предметнинг мақсад ва вазифалари ҳақида маълумот бериш, ахборот хавфсизлигига хавф-хатарларни таснифлаш, хавфсизликни назорат қилиш воситалари бўйича маълумот бериш.

Таянч иборалар: ахборот хавфсизлиги, ахборот ҳимояси, ахборотларга нисбатан хавф хатарлар; ёвуз ниятли шахс, ахборотларга рухсатсиз кириш, бузгунчи.

Дарс ўтиш воситалари: синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва компютердан самарали фойдаланилади.

Дарс ўтиш усуллари: такрорлаш, суҳбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулоҳазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут.

Ташкилий қисми: Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давомати – 2 минут.

Билимларни баҳолаш: янги мавзуни ўрганиш учун зарур бўлган материал бўйича суҳбат – 10 минут.

Янги мавзуни баён этиш – 55 минут.

Мавзу ўзлаштирилган даражасини аниқлаш – 10 минут.

Уйга вазифа – 3 минут.

Ахборот хавфсизлигига кириш

Мамлакатимиз миллий иқтисодининг ҳеч бир тармоғи самарали ва мўътадил ташкил қилинган ахборот инфратузилмасисиз фаолият кўрсатиши мумкин эмас. Ҳозирги кунда миллий ахборот ресурслари ҳар бир давлатнинг иқтисодий ва ҳарбий салоҳиятини ташкил қилувчи омилларидан бири бўлиб хизмат қилмоқда. Ушбу ресурсдан самарали фойдаланиш мамлакат хавфсизлигини ва демократик ахборотлашган жамиятни муваффақиятли шакллантиришни таъминлайди. Бундай жамиятда ахборот алмашуви тезлиги юксалади, ахборотларни йиғиш, сақлаш, қайта ишлаш ва улардан фойдаланиш бўйича илғор ахборот – коммуникациялар технологияларини қўллаш кенгайди. Турли хилдаги ахборотлар ҳудудий жойлашишидан қатъий назар бизнинг кундалик ҳаётимизга Интернет ҳалқаро компьютер тармоғи

орқали кириб келди. Ахборотлашган жамият шу компьютер тармоғи орқали тезлик билан шаклланиб бормокда. Ахборотлар дунёсига саёхат қилишда давлат чегаралари деган тушунча йўқолиб бормокда. Жаҳон компьютер тармоғи давлат бошқарувини тубдан ўзгартирмокда, яъни давлат ахборотларнинг тарқалиши механизмини бошқара олмай қолмокда. Шунинг учун ҳам мавжуд ахборотларга ноқонуний кириш, улардан фойдаланиш ва йўқотиш каби муаммолар долзарб бўлиб қолди. Буларнинг бари шахс, жамият ва давлатнинг ахборот хавфсизлиги даражасининг пасайишига олиб келмокда. Давлатнинг ахборот хавфсизлигини таъминлаш муаммоси миллий хавфсизликни таъминлашнинг асосий ва ажралмас қисми бўлиб, ахборот ҳимояси эса давлатнинг бирламчи масалаларига айланмокда.

Ҳозирги кунда хавфсизликнинг бир қанча йўналишларини қайд этиш мумкин.

Предметнинг асосий тушунчалари ва мақсади

Ахборотнинг муҳимлик даражаси қадим замонлардан маълум. Шунинг учун ҳам қадимда ахборотни ҳимоялаш учун турли хил усуллар қўлланилган. Улардан бири – сирли ёзувдир. Ундаги хабарни хабар юборилган манзил эгасидан бошқа шахс ўқий олмаган. Асрлар давомида бу санъат – сирли ёзув жамиятнинг юқори табақалари, давлатнинг элчихона резиденциялари ва разведка миссияларидан ташқарига чиқмаган. Фақат бир неча ўн йил олдин ҳамма нарса тубдан ўзгарди, яъни ахборот ўз қийматига эга бўлди ва кенг тарқаладиган маҳсулотга айланди. Уни эндиликда ишлаб чиқарадилар, сақлайдилар, узатишади, сотадилар ва сотиб оладилар. Булардан ташқари уни ўғирлайдилар, бузиб талқин этадилар ва сохталаштирадилар. Шундай қилиб, ахборотни ҳимоялаш зарурияти туғилади. Ахборотни қайта ишлаш саноатининг пайдо бўлиши ахборотни ҳимоялаш саноатининг пайдо бўлишига олиб келади.

Автоматлаштирилган ахборот тизимларида ахборотлар ўзининг ҳаётий даврига эга бўлади. Бу давр уни яратиш, ундан фойдаланиш ва керак бўлмаганда йўқотишдан иборатдир.

Ахборотлар ҳаётий даврининг ҳар бир босқичида уларнинг ҳимояланганлик даражаси турлича баҳоланади.

Махфий ва қимматбаҳо ахборотларга рухсатсиз киришдан ҳимоялаш энг муҳим вазифалардан бири саналади. Компьютер эгалари ва фойдаланувчиларнинг мулки ҳуқуқларини ҳимоялаш - бу ишлаб чиқарилаётган ахборотларни жиддий иқтисодий ва бошқа моддий ҳамда номоддий зарарлар келтириши мумкин бўлган турли киришлар ва ўғирлашлардан ҳимоялашдир.

Ахборот хавфсизлиги деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодиқий ва қасддан таъсирлардан ҳар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади.

Илгариги хавф фақатгина конфиденциал (махфий) хабарлар ва ҳужжатларни ўғирлаш ёки нусха олишдан иборат бўлса, ҳозирги пайтдаги хавф эса компьютер маълумотлари тўплами, электрон маълумотлар, электрон массивлардан уларнинг эгасидан рухсат сўрамасдан фойдаланишдир.

Булардан ташқари, бу ҳаракатлардан моддий фойда олишга интилиш ҳам ривожланиди.

Ахборотнинг ҳимояси деб, бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлиги, ишончлиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатъий регламентланган динамик технологик жараёнга айтилади.

Ахборотнинг эгасига, фойдаланувчисига ва бошқа шахсга зарар етказмокчи бўлган ноҳуқуқий муомаладан ҳар қандай ҳужжатлаштирилган, яъни идентификация қилиш имконини берувчи реквизитлари қўйилган ҳолда моддий жисмда қайд этилган ахборот ҳимояланиши керак.

Ахборот хавфсизлиги нуктаи назаридан ахборотни қуйидагича туркумлаш мумкин:

- махфийлик — аниқ бир ахборотга фақат тегишли шахслар доирасигина кириши мумкинлиги, яъни фойдаланилиши қонуний ҳужжатларга мувофиқ чеклаб қўйилиб, ҳужжатлаштирилганлиги қафолати. Бу банднинг бузилиши ўғирлик ёки ахборотни ошкор қилиш, дейилади;

- конфиденциаллик — ишончлиги, тарқатилиши мумкин эмаслиги, махфийлиги қафолати;

- яхлитлик — ахборот бошланғич кўринишда эканлиги, яъни уни сақлаш ва узатишда рухсат этилмаган ўзгаришлар қилинмаганлиги қафолати; бу банднинг бузилиши ахборотни сохталаштириш дейилади;

- аутентификация — ахборот захираси эгаси деб эълон қилинган шахс ҳақиқатан ҳам ахборотнинг эгаси эканлигига бериладиган қафолат; бу банднинг бузилиши хабар муаллифини сохталаштириш дейилади;

- апелляция қилишлик — етарлича мураккаб категория, лекин электрон бизнесда кенг қўлланилади. Керак бўлганда хабарнинг муаллифи кимлигини исботлаш мумкинлиги қафолати.

Юқоридагидек, ахборот тизимига нисбатан қуйидагича таснифни келтириш мумкин:

- ишончлилик — тизим меъёрий ва ғайри табиий ҳолларда режалаштирилганидек ўзини тутишлик қафолати;

- аниқлилик — ҳамма буйруқларни аниқ ва тўлиқ бажариш қафолати;

- тизимга киришни назорат қилиш — турли шахс гуруҳлари ахборот манбаларига ҳар хил киришга эгалиги ва бундай киришга чеклашлар доим бажарилишлик қафолати;

- назорат қилиниши — исталган пайтда дастур мажмуасининг хоҳлаган қисмини тулик текшириш мумкинлиги қафолати;

- идентификациялашни назорат қилиш — ҳозир тизимга уланган мижоз аниқ ўзини ким деб атаган бўлса, аниқ ўша эканлигининг қафолати;

- қасддан бузилишларга тўсқинлик — олдиндан қелишилган меъёрлар чегарасида қасддан хато қиритилган маълумотларга нисбатан тизимнинг олдиндан қелишилган ҳолда ўзини тутиши.

Ахборотни ҳимоялашнинг мақсадлари қуйидагилардан иборат:

- ахборотнинг қелишувсиз чиқиб кетиши, угирланиши, йукотилиши, узгартирилиши, сохталаштирилишларнинг олдини олиш;

- шахс, жамият, давлат хавфсизлигига булган хавф – хатарнинг олдини олиш;

- ахборотни йук килиш, узгартириш, сохталаштириш, нусха кучириш, тусиклаш буйича рухсат этилмаган ҳаракатларнинг олдини олиш;

- ҳужжатлаштирилган ахборотнинг миқдори сифатида ҳукукий тартибини таъминловчи, ахборот захираси ва ахборот тизимида ҳар қандай ноқонуний аралашувларнинг қуринишларининг олдини олиш;

- ахборот тизимида мавжуд булган шахсий маълумотларнинг шахсий махфийлигини ва конфиденциаллигини сақловчи фуқароларнинг конституцион ҳуқуқларини ҳимоялаш;

- давлат сирини, қонунчиликка мос ҳужжатлаштирилган ахборотнинг конфиденциаллигини сақлаш;

- ахборот тизимлари, технологиялари ва уларни таъминловчи воситаларни яратиш, ишлаб чиқиш ва қўллашда субъектларнинг ҳуқуқларини таъминлаш.

Тармок хавфсизлигини назорат қилиш воситалари

Замонавий ахборот - коммуникациялар технологияларининг ютуқлари ҳимоя услубларининг бир қатор зарурий инструментал воситаларини яратиш имконини бери.

Ахборотларни ҳимояловчи инструментал воситалар деганда дастурлаш, дастурий - аппаратли ва аппаратли воситалар тушунилади. Уларнинг функционал тулдирилиши хавфсизлик хизматлари олдига қўйилган ахборотларни ҳимоялаш масалаларини ечишда самаралидир. Ҳозирги кунда тармок хавфсизлигини назорат қилиш техник воситаларининг жуда кенг спектри ишлаб чиқарилган.

Такрорлаш учун саволлар

1. Ахборот хавфсизлиги мақсад ва вазифалари нимадан иборат?
2. Предметнинг асосий тушунчаларини таърифлаб беринг.
3. Ахборотларга нисбатан хавф-хатарларни таснифлаб беринг.
4. Қайси тармок хавфсизлигини назорат қилиш воситаларини биласиз?

Мустақил иш топшириқлари:

1. Ахборот хавфсизлигининг асосий тушунчалари луғатини тузинг.
2. Ахборотларга нисбатан хавф-хатарларга мисоллар кўрсатинг?
3. Ташкилот ва муассасаларда ахборотларга нисбатан хавф-хатарлардан кўрилган зарарга мисоллар кўрсатинг?
4. Маълумотларга рухсатсиз қиришда вирусдан қандай фойдаланиш мумкин?
5. Ахборот хавфсизлигини назорат қилиб турувчи воситаларга мисол кўрсатинг.

Мавзуга доир тестлар:

1. Ахборот ҳимояси деганда қуйидагилар тушунилади:
*а) Бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг

яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик жараён

б) Бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик процедураси

с) Бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик услуги

д) Барча жавоблар тугри

2. Тармок даражасида химояланишнинг техник усуллари қуйидагиларга бўлинадилар:

*а) аппаратли, дастурли, аппарат-дастурли

б) ташкиллаштирилган, тизимли, аппаратли

с) аппарат-дастурли, тизимли, дастурли

д) тугри жавоб йук

3. Қайси тизимлар мақсад ёмон ниятли кишиларни алдаш учун псевдо-сервислар билан ишлайди.

*а) алмаштириш тизими

б) регистрацион тизим

с) хужумларни ушлаш тизими

д) бутунлигини назорат қилиш тизимлари

Адабиётлар:

1. Абдувоҳидов А. М., Позилов Б. К. Замонавий ахборот технологияси. - Т.: 1999.
2. Ғуломов С.С. ва бошқалар. Иқтисодий информатика: Олий ўқув юртларининг иқтисодий мутахассисликлари учун дарслик.
3. Галатенко В.А., Под ред. Бетелина В.Б. Информационная безопасность: практический подход. Наука, 1998

2 – МАЪРУЗА: АХБОРОТ ХАВФСИЗЛИГИНИНГ АСОСИЙ ХАВФЛАРИ

РЕЖА

1. Автоматлаштирилган ахборот тизимларида химоялаш зарурияти;
2. Ахборотни химоялаш тизими;
3. Ташкилотлардаги ахборотларни химоялаш;
4. Химоялаш тизимининг комплекслиги;
5. Ахборотларни ташкилий химоялаш элементлари;
6. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар.

Дарснинг ўқув ва тарбиявий мақсади: Талабаларга ахборот химоялаш тизими, ташкилотлардаги ахборотларни химоялаш тизимининг комплекслиги; ахборотларни ташкилий химоялаш элементлари; ахборот тизимларида маълумотларга нисбатан хавф-хатарлар бўйича маълумот бериш.

Таянч иборалар: ахборотларга нисбатан хавф хатарлар; химоя тизими, ҳуқуқий, техник-муҳандис, дастурий-математик, ташкилий, чоралар мажмуаси.

Дарс ўтиш воситалари: синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва компютердан самарали фойдаланилади.

Дарс ўтиш усуллари: такрорлаш, суҳбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулоҳазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар яқун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут.

Ташкилий қисми: Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давомати – 2 минут.

Билимларни баҳолаш: янги мавзуни ўрганиш учун зарур бўлган материал бўйича суҳбат – 10 минут.

Янги мавзуни баён этиш – 55 минут.

Мавзу ўзлаштирилган даражасини аниқлаш – 10 минут.

Уйга вазифа – 3 минут.

Автоматлаштирилган ахборот тизимларида химоялаш зарурияти

Ахборот - коммуникациялар технологияларининг оммавий равишда коғозсиз автоматлаштирилган асосда бошқарилиши сабабли ахборот хавфсизлигини таъминлаш мураккаблашиб ва муҳимлашиб бормокда. Шунинг учун ҳам автоматлаштирилган ахборот тизимларида ахборотни химоялашнинг янги замонавий технологияси пайдо бўлмокда. ДатаҚуест компаниясининг маълумотига кура, 1996—2000 йилларда ахборот химояси воситаларининг сотувдаги ҳажми 13 млрд. АКШ долларига тенг бўлган.

Ахборотни химоялаш тизими

Ахборотнинг заиф томонларини камайтирувчи ахборотга рухсат этилмаган киришга, унинг чиқиб кетишига ва йукатилишига тускинлик килувчи ташкилий, техник, дастурий, технологик ва бошқа восита, усул ва чораларнинг комплекси — ахборотни химоялаш тизими дейилади.

Ахборот эгалари ҳамда ваколатли давлат органлари шахсан ахборотнинг қимматлилиги, унинг йукотилишидан келадиган зарар ва химоялаш механизмининг нархидан келиб чиққан ҳолда ахборотни химоялашнинг зарурий даражаси ҳамда тизимнинг турини, химоялаш усуллари ва воситаларини аниқлашлари зарур. Ахборотнинг қимматлилиги ва

талаб килинадиган химоянинг ишончилиги бир-бири билан бевосита боғлиқ.

Химоялаш тизими узлуксиз, режали, марказлаштирилган, мақсадли, аниқ, ишончли, комплексли, осон мукамаллаштириладиган ва қуриниши тез узгартириладиган бўлиши керак. У одатда барча экстремал шароитларда самарали бўлиши зарур.

Ташкилотлардаги ахборотларни химоялаш

Ахборот ҳажми кичик бўлган ташкилотларда ахборотларни химоялашда оддий усулларни куллаш мақсадга мувофиқ ва самаралидир. Масалан, уқиладиган қимматбоҳо қозғаларни ва электрон ҳужжатларни алоҳида гуруҳларга ажратиш ва ниқоблаш, ушбу ҳужжатлар билан ишлайдиган ходимни тайинлаш ва ургатиш, бинони қуриқлашни ташкил этиш, хизматчиларга қимматли ахборотларни тарқатмаслик мажбуриятини юқлаш, ташқаридан келувчилар устидан назорат қилиш, компьютерни химоялашнинг энг оддий усуллари қуллаш ва ҳоказо. Одатда, химоялашнинг энг оддий усуллари қуллаш сезиларли самара беради.

Мураккаб тарқибли, қўп сонли автоматлаштирилган ахборот тизими ва ахборот ҳажми катга бўлган ташкилотларда ахборотни химоялаш учун химоялашнинг мажмуали тизими ташкил қилинади. Лекин ушбу усул ҳамда химоялашнинг оддий усуллари хизматчиларнинг ишига ҳаддан ташқари ҳалакит бермаслиги керак.

Химоялаш тизимининг комплекслилиги

Химоя тизимининг комплекслилигига унда ҳуқуқий, ташкилий, муҳандис – техник ва дастурий – математик элементларнинг мавжудлиги билан эришилади. Элементлар нисбати ва уларнинг мазмуни ташкилотларнинг ахборотни химоялаш тизимининг ўзига ҳослигини ва унинг тақдорланмаслигини ҳамда бузиш қийинлигини таъминлайди.

Аниқ тизимни қўп турли элементлардан иборат, деб тасаввур қилиш мумкин. Тизим элементларининг мазмуни нафақат унинг ўзига ҳослигини, балки ахборотнинг қимматлилигини ва тизимнинг қийматини ҳисобга олган ҳолда белгиланган химоя даражасини аниқлайди.

Ахборотни ҳуқуқий химоялаш элементи химоялаш чораларининг ҳақли эканлиги маъносида ташкилот ва давлатларнинг узаро муносабатларини юридик мустаҳкамлаш ҳамда персоналнинг ташкилот қимматли ахборотини химоялаш тартибига риоя қилиши ва ушбу тартибни бузилишида жавобгарлиги тасаввур қилинади.

Ахборотларни ташкилий химоялаш элементлари

Химоялаш технологияси персонални ташкилотнинг қимматли ахборотларини химоялаш қоидаларига риоя қилишга ундовчи бошқариш ва чеклаш характерига эга бўлган чора-тадбирларни ўз ичига олади.

Ташкилий химоялаш элементи бошқа барча элементларни ягона тизимга боғловчи омил бўлиб ҳисобланади. Қўпчилиқ мутахассисларнинг фикрича, ахборотларни химоялаш тизимлари таркибида ташкилий химоялаш 50—60 % ни ташкил қилади. Бу ҳол қўп омилларга боғлиқ, жумладан, ахборотларни ташкилий химоялашнинг асосий томони амалда химоялашнинг принципи ва усуллари бажарувчи персонални танлаш, жойлаштириш ва ургатиш ҳисобланади.

Ахборотларни ҳимоялашнинг ташкилий чора – тадбирлари ташкилот хавфсизлиги хизматининг меъёрий услубий ҳужжатларида уз аксини топади. Шу муносабат билан кўп ҳолларда юқорида кўрилган тизим элементларининг ягана номи — ахборотни ташкилий - ҳуқуқий ҳимоялаш элементини ишлатадилар.

Ахборотларни муҳандис – техник ҳимоялаш элементи — техник воситалар комплекси ёрдамида ҳудуд, бино ва қурилмаларни қуриқлашни ташкил қилиш ҳамда техник текшириш воситаларига қарши суғуст ва фаол кураш учун мулжалланган. Техник ҳимоялаш воситаларининг нархи баланд бўлсада, ахборот тизимини ҳимоялашда бу элемент муҳим аҳамиятга эга.

Ахборотни ҳимоялашнинг дастурий – математик элементи компьютер, локал тармоқ ва турли ахборот тизимларида қайта ишланадиган ва сақланадиган қимматли ахборотларни ҳимоялаш учун мўлжалланган.

Ахборот тизимларида маълумотларга нисбатан хавф-хатарлар

Маълумки, компьютер тизим (тармоғ)ининг асосий компонентлари — техник воситалари, дастурий - математик таъминот ва маълумотлардир.

Назарий томондан бу компонентларга нисбатан тўрт турдаги хавфлар мавжуд, яъни узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш:

— узилиш — қандайдир ташқи ҳаракатлар (ишлар, жараёнлар)ни бажариш учун ҳозирги ишларни вақтинча марказий процессор қурилмаси ёрдамида тўхтатишдир, уларни бажаргандан сўнг процессор олдинги ҳолатга қайтади ва тўхтатиб қўйилган ишни давом эттиради. Ҳар бир узилиш тартиб рақамига эга, унга асосан марказий процессор қурилмаси қайта ишлаш учун қисм – дастурни қидириб топади. Процессорлар икки турдаги узилишлар билан ишлашни вужудга келтириши мумкин: дастурий ва техник. Бирор қурилма фавқулодда хизмат кўрсатилишига муҳтож бўлса, унда техник узилишлар пайдо бўлади. Одатда бундай узилиш марказий процессор учун қутилмаган ҳодисадир. Дастурий узилишлар асосий дастурлар ичида процессорнинг махсус буйруқлари ёрдамида бажарилади. Дастурий узилишда дастур ўз – ўзини вақтинча тўхтатиб, узилишга тааллуқли жараённи бажаради.

— тутиб олиш — жараёни оқибатида ғаразли шахслар дастурий воситалар ва ахборотларнинг турли магнитли ташувчиларига киришни қулга киритади. Дастур ва маълумотлардан ноқонуний нусха олиш, компьютер тармоқлари алоқа каналларидан номуаллифлик ўқишлар ва ҳоказо ҳаракатлар тутиб олиш жараёнларига мисол бўла олади.

— ўзгартириш — ушбу жараён ёвуз ниятли шахс нафақат компьютер тизими компонентларига (маълумотлар тўпламлари, дастурлар, техник элементлари) киришни қулга киритади, балки улар билан манипуляция (ўзгартириш, кўринишини ўзгартириш) ҳам қилади. Масалан, ўзгартириш сифатида ғаразли шахснинг маълумотлар тўпламидаги маълумотларни ўзгартириши, ёки умуман компьютер тизими файлларини ўзгартириши, ёки қандайдир қўшимча ноқонуний қайта ишлашни амалга ошириш мақсадида фойдаланилаётган дастурнинг кодини ўзгартириши тушунилади;

— сохталаштириш — ҳам жараён саналиб, унинг ёрдамида ғаразли шахслар тизимда ҳисобга олинмаган вазиятларни ўрганиб, ундаги камчиликларни аниқлаб, кейинчалик ўзига керакли ҳаракатларни бажариш

мақсадида тизимга қандайдир сохта жараённи ёки тизим ва бошқа фойдаланувчиларга сохта ёзувларни юборади.

Такрорлаш учун саволлар

1. *Автоматлаштирилган ахборот тизимларида химоялаш зарурияти.*
2. *Ахборотни химоялаш тизими элементларини айтиб утинг.*
3. *Ташкilotлардаги ахборотларни химоялаш муҳимлигини тушунтириб беринг.*
4. *Химоялаш тизимининг комплекслигига андай эришилади.*
5. *Ахборотларни ташкилий химоялаш элементлари вазифаси.*
6. *Ахборот тизимларида маълумотларга насбатан хавф-хатарлар*

Мустақил иш топшириқлари:

1. Ташкilot ва муассасаларда ахборот алмашуви хажмига нисбатан қандай ахборот химояси чоралари қўрилиши мақсадли?
2. Ахборотларни химоялаш тизимининг ҳуқуқий чора-тадбирларга мисоллар кўрсатинг.
3. Ахборотларни химоялаш тизимининг техник-муҳандис чора-тадбирларга мисоллар кўрсатинг.
4. Ахборотларни химоялаш тизимининг ташкилий чора-тадбирларга мисоллар кўрсатинг.
4. Ахборотларни химоялаш тизимининг дастурий чора-тадбирларга мисоллар кўрсатинг.

Мавзуга доир тестлар:

1. Фойдаланувчиларни идентификация қилиш қуйидагиларни аниқлайди
 - *а) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш шкаласини
 - б) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш графигини
 - с) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш паролени
 - д) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш кодини

2. Маълумотларни физик химоялаш кўпроқ
 - а) ташкилий ва ноташкилий чораларга қарашлидир
 - *б) ташкилий чораларга қарашлидир
 - с) ноташкилий чораларга қарашлидир
 - д) туғри жавоб йўқ

3. Ахборотга кириш ҳуқуқини узатиш ва химоя қилиш воситалари қуйидаги
 - а) Файллар мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди

- б) Браузерлар мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди
- с) Дифференциаллашган мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди
- *д) Маълумотлар билан дифференциаллашган мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди

4. Ҳимоя қилишнинг асосий муаммолари қуйидагилардан иборат

- *а) Ахборотга киришга йўл қўймаслик
- б) Файлга киришга йўл қўймаслик
- с) Шифрга киришга йўл қўймаслик
- д) Кодга киришга йўл қўймаслик

Адабиётлар

1. Абдувоҳидов А. М., Позилов Б. К. Замонавий ахборот технологияси. - Т.: 1999.
2. А.Ортиқов, А. Маматқулов. «ИБМ РС компьютерларидан фойдаланиш». Т.: 1992 й.
3. Ғуломов С.С. ва бошқалар. Иқтисодий информатика: Олий ўқув юртларининг иқтисодий мутахассисликлари учун дарслик.
4. Галатенко В.А., Под ред. Бетелина В.Б. Информационная безопасность: практический подход. Наука, 1998
5. Трубачев А.П. и др. Оценка безопасности информационных технологий СИП РИА, 2001
6. Допильченко И.А. И др. Автоматизированные системы управления предприятиями. М. Машиностроение 1984.
7. Карминский А. М., Нестеров П.В. «Автоматизация бизнеса». Москва «Финансы и статистика». 1997 год
8. «Информатика» / Под ред. Проф. Н. В. Макаровой./ Москва: Финансы и статистика. 1997 й.
9. Руссел Д., Гангеми Г.Т. Ср.Сомпутер Сесуритй Басисс ЎРеиллй, 1992
10. Гайкович В., Першин А. Безопасность электронных банковских систем Единая Европа, 1994.

3 – МАЪРУЗА: ВИРУС ВА АНТИВИРУСЛАР ТАСНИФИ

РЕЖА

1. Вирус ва унинг турлари;
2. Компьютер вирусларидан ахборотларга рухсатсиз кириш ва улардан фойдаланишни таъқиқ этиши;

3. *Антивирус дастурлари;*
4. *Вирусларга қарши чора-тадбирлар.*

Дарснинг ўқув ва тарбиявий мақсади: Талабаларга ахборот хавфизлигининг асосий тушунчаларидан бўлган вирус, уларнинг пайдо бўлиш йўллари ва турлари ҳақида маълумот бериш; эркин фикрлаб, вирусга қарши қўлланадиган воситалар бўйича маълумотга эга бўлиб, асосий антивирус дастурлар турларини таҳлил қилишни ўргатиш, хусусий ҳолларга мос дастурларни танлаб билиш ва уларни аниқ ҳолатларда қўллаб билиш кўникмаларни ҳосил қилиш.

Таянч иборалар: ахборотларга нисбатан хавф хатарлар; вирус, файлли, юкловчи, зарарли, ахборотларни ҳимоялаш, рухсат этилган кириш, маълумотларни ўқиш олиш, антивирус, диск, фаг, доктор, ревизор.

Дарс ўтиш воситалари: синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва компютердан самарали фойдаланилади.

Дарс ўтиш усуллари: такрорлаш, суҳбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулоҳазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар яқин қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут.

Ташкилий қисми: Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давомати – 2 минут.

Билимларни баҳолаш: янги мавзуни ўрганиш учун зарур бўлган материал бўйича суҳбат – 10 минут.

Янги мавзуни баён этиш – 55 минут.

Мавзу ўзлаштирилган даражасини аниқлаш – 10 минут.

Уйга вазифа – 3 минут.

Вирус ва унинг турлари

Ҳозирги кунда компютер вируслари ғаразли мақсадларда ишлатилувчи турли хил дастурларни олиб келиб татбиқ этишда энг самарали воситалардан бири ҳисобланади. Компютер вирусларини дастурли вируслар деб аташ тугрироқ бўлади.

Дастурли вирус деб автоном равишда ишлаш, бошқа дастур таркибига ўз – ўзидан қушилувчи, ишга кодир ва компютер тармоқлари ва алоҳида компютерларда уз – узидан тарқалиш хусусиятига эга булган дастурга айтилади.

Вируслар билан зарарланган дастурлар вирус ташувчи ёки зарарланган дастурлар дейилади.

Зарарланган диск – бу ишга тушириш секторида вирус дастур жойлашиб олган дискдир.

Хозирги пайтда компьютерлар учун купгина нокулайликлар тугдираётган хар хил турлардаги компьютер вируслари кенг таркалган. Шунинг учун хам улардан сакланиш усулларини ишлаб чикиш мухим масалалардан бири хисобланади. Хозирги вақтда 65000 дан куп булган вирус дастурлари борлиги аникланган. Бу вирусларнинг катта гуруҳини компьютернинг иш бажариш тартибини бузмайдиган, яъни «таъсирчан булмаган» вируслар гуруҳи ташкил этади.

Вирусларнинг бошка гуруҳига компьютернинг иш тартибини бузувчи вируслар киради. Бу вирусларни куйидаги турларга булиш мумкин: хавфсиз вируслар (файллар таркибини бузмайдиган), хавфли вируслар (файллар таркибини бузувчи) хамда жуда хавфли вируслар (компьютер курилмаларини бузувчи ва оператор соғлигига таъсир этувчи). Бу каби вируслар одатда профессионал дастурчилар томонидан тузилади.

Компьютер вируси – бу махсус ёзилган дастур булиб, бошка дастурлар таркибига ёзилади, яъни зарарлайди ва компьютерларда узининг гаразли максадларини амалга оширади. Компьютер вируси оркали зарарланиш оқибатида компьютерларда куйидаги узгаришлар пайдо булади:

- айрим дастурлар ишламайди ёки хато ишлай бошлайди;
- бажарилувчи файлнинг хажми ва унинг яратилган вақти узгаради;
- экранда англаб булмайдиган белгилар, тасвир ва товушлар пайдо булади;
- компьютернинг ишлаши секинлашади ва тезкор хотирадаги хажми камаяди;
- диск ёки дискдаги бир неча файллар зарарланади (баъзи холларда диск ва файлларни тиклаб булмайди);
- винчестер оркали компьютернинг ишга тушиши йуқолади.

Хозирги пайтда хазил шаклидаги вируслардан тортиб то компьютер курилмаларини ишдан чиқарувчи вирусларнинг турлари мавжуд.

Масалан. Win 95.СІХ вируси доимий саклаш курилмаси (Флаш БІОС) микросхемасини бузади. Афсуски, бу каби вирусларни йуқ қилиш учун, факат улар уз гаразли ишини бажариб булгандан сунггина, қарши чоралар ишлаб чиқилади. Win 95.СІХ вирусига қарши чораларни қуриш имқонияти Др.Веб дастурида мавжуд.

Компьютер вирусларидан ахборотларга рухсатсиз қириш ва улардан фойдаланишини ташкил этиш

Шуни айтиб утиш лозимки, хозирги пайтда хар-хил турдаги ахборот ва дастурларни угирлаб олиш ниятида компьютер вирусларидан фойдаланиш энг самарали усуллардан бири хисобланади.

Троян дастурлари фойдаланувчига зарар келтирувчи булиб, улар буйруқлар (модулар) кетма – кетлигидан ташкил топган, омма орасида жуда кенг таркалган дастурлар (тахрирловчилар, ўйинлар, трансляторлар) ичига ўрнатилган бўлиб, бир қанча ҳодисалар бажарилиши билан ишга тушадиган «мантикий бомба» деб аталадиган дастурдир. Ўз навбатида, «мантикий бомба»нинг турли кўринишларидан бири «соат механизмли бомба» хисобланади.

Шуни таъкидлаб ўтиш керакки, троян дастурлари ўз-ўзидан кўпаймасдан, компьютер тизими бўйича дастурловчилар томонидан тарқатилади.

Троян дастурлардан вирусларнинг фарқи шундаки, вируслар компьютер тизимлари бўйлаб тарқатилганда, улар мустақил равишда ҳосил бўлиб, ўз иш фаолиятида дастурларга ўз матнларини ёзган ҳолда уларга зарар кўрсатади.

Вирус ҳаёти одатда қуйидаги даврларни ўз ичига олади: кулланилиш, инкубация, репликация (ўз-ўзидан кўпайиш) ва ҳосил бўлиш. Инкубация даврида вирус пассив бўлиб, уни излаб топиш ва йукотиш қийин. Ҳосил булиш даврида у ўз функциясини бажаради ва қўйилган мақсадига эришади.

Таркиби жиҳатидан вирус жуда оддий бўлиб, бош қисм ва баъзи ҳолларда думдан иборат. Вируснинг бош қисми деб бошқарилишини биринчи бўлиб таъминловчи имкониятга эга бўлган дастурга айтилади. Вируснинг дум қисми зарарланган дастурда бўлиб, у бош қисмидан алоҳида жойда жойлашади.

Компьютер вируслари характерларига нисбатан норезидент, резидент, бутли, гибридли ва пакетли вирусларга ажратилади.

Файлли норезидент вируслар тўлиқлигича бажарилаётган файлда жойлашади, шунинг учун ҳам у фақат вирус ташувчи дастур фаоллашгандан сўнг ишга тушади ва бажарилгандан сўнг тезкор хотирада сақланмайди.

Резидент вирус норезидент вирусдан фарқлироқ тезкор хотирада сақланади.

Резидент вирусларнинг яна бир кўриниши бут вируслар бўлиб, бу вируснинг вазифаси винчестер ва эгилувчан магнитли дискларнинг юқловчи секторини ишдан чиқаришдан иборат. Бут вирусларнинг боши дискнинг юқловчи бут секторида ва думи дискларнинг ихтиёрий бошка секторларида жойлашган бўлади.

Пакетли вируснинг бош қисми пакетли файлда жойлашган бўлиб, у операцион тизим топшириқларидан иборат.

Гибридли вирусларнинг боши пакетли файлда жойлашади. Бу вирус ҳам файлли, ҳам бут секторли бўлади.

Тармоқли вируслар компьютер тармоқларида тарқалишга мослаштирилган, яъни тармоқли вируслар деб ахборот алмашишда тарқаладиган вирусларга айтилади.

Вирусларнинг турлари:

1) файл вируслари. Бу вируслар *com*, *exe* каби турли файлларни зарарлайди;

2) юқловчи вируслар. Компьютерни юқловчи дастурларни зарарлайди;

3) драйверларни зарарловчи вируслар. Операцион тизимдаги *config.sys* файлини зарарлайди. Бу компьютернинг ишламаслигига сабаб бўлади;

4) ДИР вируслари. ФАТ таркибини зарарлайди;

5) стелс-вируслари. Бу вируслар ўзининг таркибини узгартириб, тасодифий код ўзгариши бўйича тарқалади. Уни аниклаш жуда қийин, чунки файлларнинг ўзлари ўзгармайди;

6) Windows вируслари. Windows операцион тизимидаги дастурларни зарарлайди.

Асосланган алгоритмлар бўйича дастурли вирусларни қуйидагича таснифланади.

Паразитли вирус — файлларнинг таркибини ва дискнинг секторини ўзгартирувчи вирус. Бу вирус оддий вируслар туркумидан бўлиб, осонлик билан аниқланади ва ўчириб ташланади.

Репликаторли вирус — «чувалчанг» деб номланади, компьютер тармоқлари бўйича тарқалиб, компьютерларнинг тармоқдаги манзилни аниқлайди ва у ерда ўзининг нусхасини қолдиради.

Куринмас вирус — стелс-вирус деб ном олиб, зарарланган файлларга ва секторларга операцион тизим томонидан мурожаат қилинса, автоматик равишда зарарланган қисмлар ўрнига дискнинг тоза қисмини тақдим этади. Натижада ушбу вирусларни аниқлаш ва тозалаш жуда катта қийинчиликларга олиб келади.

Мутант вирус — шифрлаш ва дешифрлаш алгоритмларидан иборат бўлиб, натижада вирус нусхалари умуман бир-бирига ўхшамайди. Ушбу вирусларни аниқлаш жуда қийин муаммо.

Квазивирус вирус — «Троян» дастурлари, деб ном олган бўлиб, ушбу вируслар кўпайиш хусусиятига эга бўлмаса-да, «фойдали» қисм-дастур хисобида бўлиб, антивирус дастурлар томонидан аниқланмайди. Шу боис ҳам улар ўзларида мукаммаллаштирилган алгоритмларни тўсиқсиз бажариб, қўйилган мақсадларига эришишлари мумкин.

Антивирус дастурлари

Ҳозирги вақтда вирусларни йўқотиш учун кўпгина усуллар ишлаб чиқилган ва бу усуллар билан ишлайдиган дастурларни антивируслар деб аташади. Антивирусларни, кулланиш усулига кўра, қуйидагиларга ажратишимиз мумкин: *детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар.*

Детекторлар — вируснинг сигнатураси (вирусга тааллуқли байтлар кетма-кетлиги) бўйича тезкор хотира ва файлларни кўриш натижасида маълум вирусларни топади ва хабар беради. Янги вирусларни аниқлаб олмаслиги детекторларнинг камчилиги ҳисобланади.

Фаглар — детекторларга хос бўлган ишни бажарган ҳолда зарарланган файлдан вирусларни чиқариб ташлайди ва файлни олдинги ҳолатига қайтаради.

Вакциналар — юқоридагилардан фарқли равишда ҳимояланаётган дастурга урнатилади. Натижада дастур зарарланган деб ҳисобланиб, вирус томонидан ўзгартирилмайди. Фақатгина маълум вирусларга нисбатан вакцина қилиниши унинг камчилиги ҳисобланади. Шу боис ҳам, ушбу антивирус дастурлари кенг тарқалмаган.

Прививка — файлларда худди вирус зарарлагандек из қолдиради. Бунинг натижасида вируслар «прививка қилинган» файлга ёпишмайди.

Фильтрлар — куриқловчи дастурлар курунишида бўлиб, резидент ҳолатда ишлаб туради ва вирусларга хос жараёнлар бажарилганда, бу ҳақда фойдаланувчига хабар беради.

Ревизорлар — энг ишончли ҳимояловчи восита бўлиб, дискнинг биринчи ҳолатини хотирасида сақлаб, ундаги кейинги ўзгаришларни доимий равишда назорат қилиб боради.

Детектор дастурлар компьютер хотирасидан, файллардан вирусларни қидиради ва аниқланган вируслар ҳақида хабар беради.

Доктор дастурлари нафақат вирус билан касалланган файлларни топади, балки уларни даволаб, дастлабки ҳолатига қайтаради. Бундай дастурларга Аидтест, Достор Веб дастурларини мисол қилиб келтириш мумкин. Янги вирусларнинг тўхтовсиз пайдо бўлиб туришини ҳисобга олиб, доктор дастурларини ҳам янги версиялари билан алмаштириб туриш лозим.

Фильтр дастурлар компьютер ишлаш жараёнида вирусларга хос бўлган шубҳали ҳаракатларни топиш учун ишлатилади.

Текширувчи (ревизор) дастурлари вирусдан химояланишнинг энг ишончли воситаси бўлиб, компьютер зарарланмаган ҳолатидаги дастурлар, каталоглар ва дискнинг тизим майдони ҳолатини хотирада сақлаб, доимий равишда ёки фойдаланувчи ихтиёри билан компьютернинг жорий ва бошлангач ҳолатларини бир-бири билан солиштиради. Бунга АДИНФ дастурини мисол қилиб келтириш мумкин.

Вирусларга қарши чора-тадбирлар

Компьютерни вируслар билан зарарланишидан сақлаш ва ахборотларни ишончли сақлаш учун қуйидаги қоидаларга амал қилиш лозим:

- компьютерни замонавий антивирус дастурлар билан таъминлаш;
- дискеталарни ишлатишдан олдин ҳар доим вирусга қарши текшириш;
- қимматли ахборотларнинг нусхасини ҳар доим архив файл кўринишида сақлаш.

Компьютер вирусларига қарши курашнинг қуйидаги турлари мавжуд:

- вируслар компьютерга кириб бузган файлларни ўз ҳолига қайтарувчи дастурларнинг мавжудлиги;
- компьютерга пароль билан кириш, диск юритувчиларнинг ёпиқ туриши;
- дискларни ёзишдан химоялаш;
- лицензион дастурий таъминотлардан фойдаланиш ва ўғирланган дастурларни қўлламаслик;
- компьютерга кириталаётган дастурларнинг вирусларнинг мавжудлигини текшириш;
- антивирус дастурларидан кенг фойдаланиш;
- даврий равишда компьютерларни антивирус дастурлари ёрдамида вирусларга қарши текшириш.

Антивирус дастурларидан ДрВеб, Адинф, АВП, ВоотСХК ва Нортон Антивирус, Касперский Сесуритй кабилар кенг фойдаланилади.

Такрорлаш учун назорат саволлари

1.Вирус тушунчасини таърифлаб беринг.

2. Компьютернинг вируслар билан зарарланиш йулларини айтиб утинг.
3. Компьютер вирусларидан ахборотларга рухсатсиз кириш қандай ташкил қилинади?
4. Антивирус дастурларини таснифлаб беринг.
5. Вирусларга қарши қандай чора-тадбирлар самарали ҳисбланади.

Мустақил иш топшириқлари:

1. Вируслар билан зарарланиш натижасидаги оқибатларга мисоллар кўрсатинг.
2. Охириги 5 йилда кенг тарқалган вирус дастурлар номлари ва уларнинг зарарли функцияларига мисоллар кўрсатинг?
3. Маълумотларга рухсатсиз киришда вирусдан қандай фойдаланиш мумкин?
4. Ҳозирги кунда оммавийлашган антивирус дастурларидан бирига мисол кўрсатинг ва унинг имкониятларини таҳлил қилиб беринг.
5. Вирусни шахсий компьютерга туширмаслик учун энг самарали чора-тадбирлар кетма-кетлигини кўрсатиб беринг.

Мавзуга доир тестлар:

1. Антивирус дастурларини синовдан ўтказиш билан қандай ташкилот шуғулланади?
 - а) Интел, Селерон
 - б) Селерон, ИБМ
 - в) Компьютер хавфсизлиги миллий ассоциацияси НССА (Национал Компьютер Сесурити Ассоциатсион)
 - д) ИБМ, ИНТЕЛ
2. Бутликни назорат қилиш тизими
 - а) Команда файлларини, қачонки ёвуз ниятли уларга узгартиришлар киритилганини аниклаш учун текширади
 - б) Тизим файлларини, қачонки ёвуз ниятли уларга узгартиришлар киритилганини аниклаш учун текширади
 - в) Модул файлларини, қачонки ёвуз ниятли уларга узгартиришлар киритилганини аниклаш учун текширади
 - д) тугри жавоб тугри
3. Руйхатга олинган файллар монитори
 - а) Тармоқдаги серверлар ва ишчи станцияларда яратиладиган руйхатга олинган файлларни назорат қилади
 - б) Тармоқдаги серверлар ва ишчи станцияларда яратиладиган руйхатга олинган тизимли файлларини назорат қилади
 - в) Тармоқдаги серверлар ва ишчи станцияларда яратиладиган руйхатга олинган буйруқ файлларини назорат қилади
 - д) Автоматик юклаш файлларини

Адабиётлар:

1. Абдувоҳидов А. М., Позиллов Б. К. Замонавий ахборот технологияси. - Т.: 1999.
2. Гуломов С.С. ва бошқалар. Иқтисодий информатика: Олий ўқув юртларининг иқтисодий мутахассисликлари учун дарслик.
3. Галатенко В.А., Под ред. Бетелина В.Б. Информационная безопасность: практический подход. Наука, 1998

4 – МАЪРУЗА: АХБОРОТЛАРНИ СТЕГАНОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ ВА КРИПТОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ

РЕЖА

1. *Замонавий компьютер стенографияси;*
2. *Конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш.*
3. *Стенографик дастурлар тўғрисида қисқача маълумот*
4. *Криптография ҳақида асосий тушунчалар.*
5. *Симметрияли криптотизим асослари.*

Дарснинг ўқув ва тарбиявий мақсади: Талабаларга ахборот хавфизлигининг асосий қисмларидан бўлган замонавий компьютер стеганографияси, конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш, стенографик дастурлар тўғрисида қисқача маълумот, криптография ҳақида асосий тушунчалар, симметрияли криптотизим асослари ҳақида маълумот бериш.

Таянч иборалар: стеганографик усуллар, сув ҳимоя белгиси, инверслаш, маълумотни қуриш, криптографик ҳимоялаш, очиқ калит, махфий калит.

Дарс ўтиш воситалари: синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва компьютардан самарали фойдаланилади.

Дарс ўтиш усуллари: такрорлаш, суҳбат, ва савол-жавоб ҳамда, мунозара (мавзунинг ўзлаштиришни мустақамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларининг баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрининг баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар яқун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут.

Ташкилий қисми: Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давомати – 2 минут.

Билимларни баҳолаш: янги мавзуни ўрганиш учун зарур бўлган материал бўйича суҳбат – 10 минут.

Янги мавзуни баён этиш – 55 минут.

Мавзу ўзлаштирилган даражасини аниқлаш – 10 минут.

Уйга вазифа – 3 минут.

Замонавий компьютер стеганографияси

Рухсат этилмаган киришдан ахборотни ишончли ҳимоялаш муаммоси энг илгаритдан мавжуд ва ҳозирги вақтгача ҳал қилинмаган. Махфий хабарларни яшириш усуллари қадимдан маълум, инсон фаолиятининг бу соҳаси стеганография деган ном олган. Бу сўз грекча Стеганос (махфий, сир) ва Грапхй (ёзув) сўзларидан келиб чиққан ва «сирли ёзув» деган маънони билдиради. Стенография усуллари, эҳтимол, ёзув пайдо бўлишидан олдин пайдо бўлган (дастлаб шартли белги ва белгилашлар қулланилган) бўлиши мумкин.

Ахборотни ҳимоялаш учун кодлаштириш ва криптография усуллари қўлланилади. Кодлаштириш деб ахборотни бир тизимдан бошқа тизимга маълум бир белгилар ёрдамида белгиланган тартиб бўйича ўтказиш жараёнига айтилади. Криптография деб махфий хабар мазмунини шифрлаш, яъни маълумотларни махсус алгоритм бўйича ўзгартириб, шифрланган матнни яратиш йўли билан ахборотга рухсат этилмаган киришга тусиқ қуйиш усулига айтилади.

Стеганографиянинг кринтографиядан бошқа ўзгача фарқи ҳам бор. Яъни унинг мақсади — махфий хабарнинг мавжудлигини яширишдир. Бу иккала усул бирлаштирилиши мумкин ва натижада ахборотни ҳимоялаш самарадорлигини ошириш учун ишлатилиши имкони пайдо бўлади (масалан, криптографик калитларни узатиш учун).

Глобал компьютер тармоқлари ва мультимедиа соҳасидаги замонавий прогресс телекоммуникация каналларида маълумотларни узатиш хавфсизлигини таъминлаш учун мўлжалланган янги усулларни яратишга олиб келди. Бу усуллар шифрлаш қурилмаларининг табиий ноаниқлигидан ва аналогли видео ёки аудиосигналларнинг сероблигидан фойдаланиб хабарларни компьютер файллари (контейнерлар)да яшириш имконини беради. Шу билан бирга криптографиядан фарқли равишда бу усуллар ахборотни узатиш фактининг ўзини ҳам яширади.

К.Шеннон сирли ёзувнинг умумий назариясини яратдики, у фан сифатида стеганографиянинг базаси ҳисобланади. Замонавий компьютер стеганографиясида иккита асосий файл турлари мавжуд: яшириш учун мўлжалланган хабар-файл, ва контейнер-файл, у хабарни яшириш учун ишлатилиши мумкин. Бунда контейнерлар икки турда бўлади: контейнер-оригинал (ёки «бўш» контейнер) - бу контейнер яширин ахборотни сақламайди; контейнер-натижа (ёки «тулдирилган» контейнер) — бу контейнер яширин ахборотни сақлайди. Калит сифатида хабарни контейнерга киритиб қуйиш тартибини аниқлайдиган махфий элемент тушунилади.

Компьютер стеганографияси ҳозирги кунда ахборот хавфсизлиги бўйича асосий технологиялардан бири бўлиб ҳисобланади.

Замонавий компьютер стеганографиясининг асосий ҳолатлари қуйидагилардан иборат:

- яшириш усуллари файлнинг аутентификацияланишлигини ва яхлитлигини таъминлаши керак;
- ёвуз ниятли шахсларга қўлланилувчи стеганография усуллари тўлиқ маълум деб фараз қилинади;
- усулларнинг ахборотга нисбатан хавфсизликни таъминлаши очик узаталадиган файлнинг асосий хоссаларини стенографик алмаштиришлар билан сақлашга ва бошқа шахсларга номаълум бўлган қандайдир ахборот — калитга асосланади;
- агар ёвуз ниятли шахсларга хабарни очиш вақти маълум бўлиб қолган бўлса, махфий хабарнинг ўзини чиқариб олиш жараёни мураккаб ҳисоблаш масаласи сифатида тасаввур қилиниши лозим.

Интернет компьютер тармоғининг ахборот манбаларини таҳлили қуйидаги ҳулосага келишга имкон берди, яъни ҳозирги вақтда стенографик тизимлар қуйидаги асосий масалаларни ечишда фаол ишлатиляпти:

- конфиденциал ахборотни рухсат этилмаган киришдан ҳимоялаш;
- мониторинг ва тармоқ захираларини бошқариш тизимларини енгил;
- дастурий таъминотни никоблаш;
- интеллектуал эгаликнинг баъзи бир турларида муаллифлик ҳуқуқларини ҳимоялаш.

Стеганографик дастурлар тўғрисида қисқача маълумот

Windows операцион муҳитида ишловчи дастурлар:

- Стеганос фор Вин95 дастури ишлатишда жуда енгил бўлиб, айти пайтда файлларни шифрлаш ва уларни BMP, ДИВ, ВОС, WAB, АССИИ, HTML кен-гайтмали файллар ичига жойлаштириб яширишда жуда қудратли ҳисобланади;

- Сонтрабанд дастури 24-битли BMP форматдаги график файллар ичида ҳар қандай файлни яшира олиш имкониятига эга.

ДОС муҳитида ишловчи дастурлар:

- Жстег дастури маълумотни ЖРГ форматли файллар ичига яшириш учун мўлжалланган;

- ФФЕнкоде дастури маълумотларни матнли файллар ичида яшириш имкониятига эга;

- СтегоДОС дастурлар пакетининг ахборотни тасвирда яшириш имконияти мавжуд;

- Винсторм дастурлар пакети РСХ форматли файллар ичига хабарни шифрлаб яширади.

ОС/2 операцион муҳитида ишловчи дастурлар:

- Техто дастури маълумотларни инглиз тилидаги матнга айлантиради;

- Ҳиде4ПП в1.1 дастури BMP, WAB, ВОС форматли файллар ичига маълумотларни яшириш имкониятига эга.

Масинтош компьютерлари учун мўлжалланган дастурлар:

- Рараноид дастури маълумотларни шифрлаб, товушли форматли файл ичига яширади:

- Стего дастурининг РИСТ кенгайтмали файл ичига маълумотларни яшириш имконияти мавжуд.

Криптография ҳақида асосий тушунчалар

«Криптография» атамаси дастлаб «яшириш, ёзувни беркитиб қуймоқ» маъносини билдирган. Криптография ахборотни рухсатсиз киришдан ҳимоялаб, унинг махфийлигини таъминлайди. Криптография соҳасидаги охирги ютуқлардан бири — рақамли сигнатура — махсус хосса билан ахборотни тўлдириш ёрдамида яхлитликни таъминловчи усул, бунда ахборот унинг муаллифи берган очиқ калит маълум бўлгандагина текширилиши мумкин. Ушбу усул махфий калит ёрдамида яхлитлик текшириладиган маълум усулларан кўпроқ афзалликларга эга.

Сирли (махфий) алоқалар соҳаси криптология деб айтилади. Ушбу сўз юнонча «крипто» — сирли ва «логус» — хабар маъносини билдирувчи сўзлардан иборат. Криптология икки йўналиш, яъни криптография ва криптотаҳлилдан иборат.

Криптографиянинг вазифаси хабарларнинг махфийлигини ва ҳақиқийлигини таъминлашдан иборат.

Криптотаҳлилнинг вазифаси эса криптографлар томонидан ишлаб чиқилган ҳимоя тизимини очишдан иборат.

Симметрияли криптотизим асослари.

Ҳозирги кунда криптотизимни икки синфга ажратиш мумкин:

- симметрияли бир калитлилик (махфий калитли);
- асимметрияли икки калитлилик (очиқ калитли).

Симметрияли тизимларда қуйидаги иккита муаммо мавжуд:

1) Ахборот алмашувида иштирок этувчилар қандай йўл билан махфий калитни бир-бирларига узатишлари мумкин?

2) Жўнатилган хабарнинг ҳақиқийлигини қандай аниқласа бўлади?

Ушбу муаммоларнинг ечими очиқ калитли тизимларда ўз аксини топди.

Очиқ калитли асимметрияли тизимда иккита калит қўлланилади. Биридан иккинчисини ҳисоблаш усуллари билан аниқлаб бўлмайди.

Биринчи калит ахборот жўнатувчи томонидан шифрлашда ишлатилса, иккинчиси ахборотни қабул қилувчи томонидан ахборотни тиклашда қўлланилади ва у сир сақланиши лозим.

Ушбу усул билан ахборотнинг махфийлигини таъминлаш мумкин. Агар биринчи калит сирли бўлса, у ҳолда уни электрон имзо сифатида қўллаш мумкин ва бу усул билан ахборотни аутентификациялаш, яъни ахборотнинг яхлитлигини таъминлаш имкони пайдо бўлади.

Ахборотни аутентификациялашдан ташқари қуйидаги масалаларни ечиш мумкин:

- фойдаланувчини аутентификациялаш, яъни компьютер тизими захираларига кирмоқчи бўлган фойдаланувчини аниқлаш;
- тармок абонентлари алоқасини урнатиш жараёнида уларни ўзаро аутентификациялаш.

Ҳозирги кунда ҳимояланиши зарур бўлган йўналишлардан бири бу электрон тўлов тизимлари ва Интернет ёрдамида амалга ошириладиган электрон савдолардир.

Криптография — маълумотларни ўзгартириш усуллари туплами бўлиб, маълумотларни ҳимоялаш бўйича қуйидаги иккита асосий муаммоларни ҳал қилишга йуналтирилган: махфийлик; яхлитлилик.

Махфийлик орқали ёвуз ниятли шахслардан ахборотни яшириш тушунилса, яхлитлилик эса ёвуз ниятли шахслар томонидан ахборотни ўзгартира олмаслик ҳақида далолат беради.

Криптография тизимини схематик равишда тасвирлаганда, калит қандайдир ҳимояланган канал орқали жунатилади (чизмада пунктир чизиклар билан тасвирланган). Умуман олганда, ушбу механизм симметрияли бир калитлик тизимига тааллуқлидир.

Ассимметрияли икки калитлик криптография тизимида ҳимояланган канал бўйича очик калит жўнатилиб, махфий калит жўнатилмайд.

Ёвуз ниятли шахслар уз мақсадларига эриша олмаса ва криптоахлилчилар калитни билмасдан туриб, шифрланган ахборотни тиклай олмаса, у ҳолда криптотизим криптомустаҳкам тизим деб айтилади. Криптотизимнинг мустаҳкамлиги унинг калити билан аникланади ва бу криптоахлилнинг асосий қоидаларидан бири бўлиб ҳисобланади.

Ушбу таърифнинг асосий маъноси шундан иборатки, криптотизим барчаларга маълум тизим ҳисобланиб, унинг ўзгартирилиши кўп вақт ва маблағ талаб қилади, шу боис ҳам фақатгина калитни ўзгартириб туриш билан ахборотни ҳимоялаш талаб қилинади.

Криптография нуктаи – назаридан шифр — бу калит демакдир ва очик маълумотлар тупламини ёпик (шифрланган) маълумотларга ўзгартириш криптография ўзгартиришлар алгоритмлари мажмуаси ҳисобланади. Калит — криптография ўзгартиришлар алгоритмининг баъзи-бир параметрларининг махфий ҳолати бўлиб, барча алгоритмлардан ягона варианты танлайди. Калитларга нисбатан ишлатиладиган асосий курсаткич бўлиб криптомустаҳкамлик ҳисобланади.

Криптография ҳимоясида шифрларга нисбатан қуйидаги талаблар қўйилади:

- етарли даражада криптомустаҳкамлик;
- шифрлаш ва кайтариш жараёнининг оддийлиги;
- ахборотларни шифрлаш оқибатида улар ҳажмининг ортиб кетмаслиги;

- шифрлашдаги кичик хатоларга таъсирчан бўлмаслиги.

Ушбу талабларга қуйидаги тизимлар жавоб беради:

- уринларини алмаштириш;
- алмаштириш;
- гаммалаштириш;
- аналитик ўзгартириш.

Уринларини алмаштириш шифрлаш усули бўйича бошлангич матн белгиларининг матннинг маълум бир қисми доирасида махсус қоидалар ёрдамида уринлари алмаштирилади.

Алмаштириш шифрлаш усули буйича бошлангич матн белгилари фойдаланилаётган ёки бошқа бир алифбо белгиларига алмаштирилди.

Гаммалаштириш усули буйича бошлангич матн белгилари шифрлаш гаммаси белгилари, яъни тасодикий белгилар кетма-кетлиги билан бирлаштирилади.

Тахлилий узгартириш усули буйича бошлангич матн белгилари аналитик формулалар ёрдамида узгартирилади, масалан, векторни матрицага кўпайтириш ёрдамида. Бу ерда вектор матндаги белгилар кетма-кетлиги бўлса, матрица эса калит сифатида хизмат килади.

Такрорлаш учун саволлар

1. *Замонавий компьютер стенографияси истикболлари.*
2. *Компьютер стенографиясининг асосий вазифалари.*
3. *Конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш учун андай йўналишлар мавжуд?*
4. *Криптографиянинг асосий тушунчаларини таърифлаб беринг.*
5. *Ахборотларни криптографияли ҳимоялаш тамойиллари.*
6. *Уринларни алмаштириш ва алмаштириш усуллари қандай криптолизиларга тегишли?*

Мустақил иш топшириқлари:

1. Дастурий таъминотни ниқоблаш алгоритмларини ўрганиб, энг самаралисини танлаш усулини таклиф қилинг?
2. Муаллифлик ҳуқуқларни ҳимоялашда стеганографиядан қандай фойдаланилади?
3. Windows операцион муҳитида ишловчи стеганография дастурларининг ишлаш принципларини, модуллари таркибини тавсифлаб беринг?
4. Симметрияли криптографик тизимдаги ўринларни алмаштириш усулларига мисоллар кўрсатинг.
5. Симметрияли криптографик тизимдаги алмаштириш усулларига мисоллар кўрсатинг.
6. Симметрияли криптографик тизимдаги гаммалаш усулларига мисоллар кўрсатинг.
7. Симметрияли криптографик тизимдаги тахлилий ўзгартириш усулларига мисоллар кўрсатинг.

Мавзуга доир тестлар:

1. Криптомустаҳкамлик – бу
 - *А. Шифрнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир
 - Б.Идентификаторнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир
 - С. Коднинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир

Д. Код ва идентификаторнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир

2. Калитларни тақсимлаш ва калит билан бошқариш терминлари қайси жараёнда таалуқли?

А. Ахборотни чиқаришнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

Б. Ахборотни киритишнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

*С. Ахборотни қайта ишлашнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

Д. Ахборотни ёзишнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

3. Очиқ калитли тизимда шифрлаш ва дешифрлаш учун қандай калит ишлатилади?

А. очиқ

*Б. очиқ ва ёпиқ

С. ёпиқ

Д. барча жавоблар нотўғри

4. Криптомустаҳкамликнинг қанақа кўрсаткичлари мавжуд

А. –мумкин бўлган калитлар сони; –крипто таҳлил учун керакли бошланғич вақт;

*Б. –мумкин бўлган калитлар сони; –крипто таҳлил учун керакли ўртача вақт;

С. –мумкин бўлган калитлар сони; –крипто таҳлил учун керакли охириги вақт;

Д. барча жавоблар тўғри

5. Ахборотни ҳимоялаш мақсадида шифрлашнинг эффективлиги қуйдагилардан боғлиқ

А. Тўғри жавоблар йўқ

Б. Шифрни криптомустаҳкамлиги ва идентификаторларнинг сирини сақлашдан

*С. Шифрни криптомустаҳкамлиги ва калитнинг сирини сақлашдан

Д. Шифрни криптомустаҳкамлиги ва коднинг сирини сақлашдан

6. Шифрланган маълумот ўқилиши мумкин фақат

*А. Калити берилган бўлса

Б. Коди берилган бўлса

С. Идентификатори берилган бўлса

Д. Шифри берилган бўлса

7. Шифрланган ахборотни шарҳлаб беришда мумкин бўлган калитларни танлаш йўли учун зарур жараёнлар сони қуйдагиларни ўз ичига олади

А. Юқоридан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқади

Б. Қуйидан баҳолаш қаттиқ талаб қилинмайди; замонавий компьютерлар имконият чегарасидан чиқади

*С. Қуйидан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқади

Д. Қуйидан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқмайди

8. Калитларни сезиларсиз ўзгартириш қуйдагиларга олиб келиши мумкин

А. Хато бир хил калитни ишлатганда шифрланган маълумот кўриниши сезиларли ўзгариш олади

Б. Хато бир хил калитни ишлатганда шифрланган маълумот кўриниши сезиларли ва сезиларсиз ўзгариш олади

С. Хато бир хил калитни ишлатганда шифрланган маълумот кўриниши сезиларсиз ўзгариш олади

*Д. битта ва бир хил калитдан фойдаланганда ҳам шифрланган хабарлар сезиларли даражада ўзгаришга эга бўлади

Адабиётлар

1. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.:СИНТЕГ, 2000, 248 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.- М.: Издательство ТРИУМФ, 2003 – 816 с.

3. Коблиц. Н. Курс теории чисел и криптографии - М., Научное издательство ТВП, 2001 г., 260 стр. (перевод с английского).

5 – МАЪРУЗА: МАЪЛУМОТЛАРНИНГ ТАРКАЛИБ КЕТИШИ ВА МАЪЛУМОТЛАРГА РУХСАТСИЗ КИРИШ

РЕЖА

1. *Ахбопом химоя тизимларини ташкил қилиш долзарблиги*
2. *Ахбопом тизимларнинг таъсирчан қисмлари;*
3. *Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари.*

Дарснинг ўқув ва тарбиявий мақсади: Талабаларга маълумотларнинг таркалиб кетиши ва маълумотларга рухсатсиз киришдан химоя қилиш чоратadbирлари ва воситалари ҳақида маълумот бериш. Ахбопот химоя тизимларини ташкил қилиш долзарблиги, ахбопот тизимларнинг таъсирчан қисмлари, маълумотларга рухсатсиз киришнинг дастурий ва техник воситаларини ўргатиш.

Таянч иборалар: маълумот тарқалиши, рухсатсиз кириш, таъсирчан кисм, протокол, дастурий ва техник воситалар.

Дарс ўтиш воситалари: синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва компьютардан самарали фойдаланилади.

Дарс ўтиш усуллари: такрорлаш, сухбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут.

Ташкилий қисми: Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давомати – 2 минут.

Билимларни баҳолаш: янги мавзуни ўрганиш учун зарур бўлган материал бўйича сухбат – 10 минут.

Янги мавзуни баён этиш – 55 минут.

Мавзу ўзлаштирилган даражасини аниқлаш – 10 минут.

Уйга вазифа – 3 минут.

Ахборот химоя тизимларини ташкил қилиш долзарблиги

Хозирги вақтларда мавжуд ахборот тизимларида жуда катта ҳажмда махфий ахборотлар сақланади ва уларни химоялаш энг долзарб муаммолардан ҳисобланади.

Масалан, биргина АКШ мудофза вазирлигида айни чоғда 10000 компьютер тармоклари ва 1,5 млн компьютерларга қарашли ахборотларнинг аксарият қисми махфий эканлиги ҳаммага аён. Бу компьютерларга 1999 йили 22144 марта турлича ҳужумлар уюштирилган, уларнинг 600 тасида Пентагон тизимларининг вақтинчалик ишдан чиқишига олиб келган, 200 тасида эса махфий бўлмаган маълумотлар базаларига рухсатсиз кирилган ва натижада Пентагон 25 миллиард АКШ доллари миқдорида иқтисодий зарар кўпган. Бунақа ҳужумлар 2000 йили 25000 марта амалга оширилган. Уларга қарши курашиш учун Пентагон томонидан янги технологиялар яратишга 2002 йили Сарнегье Меллон университетига 35,5 млн. АКШ доллари миқдорида грант ажратилган.

Маълумотларга қараганда, ҳар йили АКШ ҳукумати компьютерларига уртача ҳисобда 250—300 минг ҳужум уюштирилади ва улардан 65 % и муваффақиятли амалга оширилади.

Замонавий автоматлаштирилган ахборот тизимлари — бу тараккиёт дастурий-техник мажмуасидир ва улар ахборот алмашувини талаб этадиган масалаларни ечишни таъминлайди. Кейинги йилларда фойдаланувчиларнинг ишини енгиллаштириш мақсадида янгиликларни тарқатиш хизмати УСЕНЕТ-ННТП, мультимедиа маълумотларини ИНТЕРНЕТ-ЎТТП тармоғи орқати узатиш каби протоколлар кенг тарқалди.

Бу протоколлар бир канча ижобий имкониятлари билан бирга анчагина камчиликларга ҳам эга ва бу камчиликлар тизимнинг захираларига рухсатсиз киришга йул куйиб бермокда.

Ахборот тизимларнинг таъсирчан кисмлари

Ахборот тизимларининг асосий таъсирчан кисмлари куйидагилар:

- ИНТЕРНЕТ тармогидаги серверлар. Бу серверлар: дастурлар ёки маълумотлар файлларини йук, килиш оркали, серверларни хаддан ташкари куп тугалланмаган жараёнлар билан юклаш оркали: тизим журналининг кескин тулдириб юборилиши оркали; броузер — дастурларини ишламай колишига олиб келувчи файлларни нусхалаш оркали ишдан чикарилади;
- маълумотларни узатиш каналлари — бирор-бир порт оркали ахборот олиш максатида яширин канални ташкил этувчи дастурлар юборилади;
- маълумотларни тезкор узатиш каналлари — бу каналлар жуда куп микдорда хеч кимга керак булмаган файллар билан юкланади ва уларнинг маълумот узатиш тезлиги сусайиб кетади;
- янгиликларни узатиш каналлари — бу каналлар эскирган ахборот билан тулдириб ташланади ёки бу каналлар умуман йук килиб ташланади;
- ахборотларни узатиш йули — УСЕНЕТ тармогида янгиликлар пакетининг маршрути бузилади;
- ЖАВА броузерлари — СУН фирмаси яратган ЖАВА тили имкониятларидан фойдаланиб, апплетлар (апплец) ташкил этиш оркали маълумотларга рухсатсиз кириш мумкин булади. ЖАВА — апплетлари тармокда автоматик равишда ишга тушиб кетади ва бунинг натижасида фойдаланувчи бирор-бир хужжатни ишлатаётган пайтда хакикатда нима содир этилишини хеч қачон кура билмайди, масалан, тармок вирусларини ташкил этиш на ЖАВА-апплетлари оркали вирусларни жунатиш мумкин булади ёки фойдаланувчининг кредит карталари ракамларига эгалик килиш имконияти вужудга келади.

АҚШ саноат шпionaжига қарши кураш ассоциациясининг текширишларига асосан компьютер тармоклари ва ахборот тизимларига хужумлар куйидагича таснифланади: 20% — аралаш хужумлар; 40% — ички хужумлар ва 40% — ташки хужумлар.

Жуда куп холларда бунақа хужумлар муваффақиятли ташкил этилади. Масалан, Буюк Британия саноати, компьютер жиноятлари сабабли, ҳар йили 1 млрд фунт стерлинг зарар куради.

Демак, юкорида олиб борилган тахлилдан шу нарса куринадики, ҳозирги пайтда компьютер тармоклари жуда куп таъсирчан кисмларга эга булиб, улар оркали ахборотларга рухсатсиз киришлар амалга оширилмокда ёки маълумотлар базалари йук килиб юборилмокда ва бунинг натижасида инсоният млрд-млрд АҚШ доллари микдорида иктисодий зарар курмокда.

Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари

Маълумки, ҳисоблаш техникаси воситалари иши электромагнит нурланиши оркали бажарилади, бу эса, уз навбатида, маълумотларни таркатиш учун зарур булган сигналларнинг захирасидир. Бундай кисмларга компьютерларнинг платалари, электрон таъминот манбалари, принтерлар, плоттерлар, алоқа аппаратлари ва х.к. киради. Лекин, статистик

маълумотлардан асосий юкори частотали электромагнит нурланиш манбаи сифатида дисплейнинг рол уйнаши маълум булди. Бу дисплейларда электрон нурли трубкалар урнатилган булади. Дисплей экранда тасвир худди телевизордагидек ташкил этилади. Бу эса видеосигналларга эгалик килиш ва уз навбатида, ахборотларга эгалик килиш имкониятини яратади. Дисплей экрандаги курсатув нухаси телевизорда хосил булади.

Юкорида келтирилган компьютер кисмларидан бошка ахборотларга эгалик килиш мақсадида тармок кабеллари ҳамда серверлардан ҳам фойдаланилмокда.

Компьютер тизимлари захираларига рухсатсиз кириш сифатида мазкур тизим маълумотларидан фойдаланиш, уларни узгартириш ва учуриб ташлаш харакатлари тушунилади.

Агар компьютер тизимлари рухсатсиз киришдан химояланиш механизмларига эга булса, у холда рухсатсиз кириш харакатлари куйидагича ташкил этилади:

- химоялаш механизмини олиб ташлаш ёки куринишини узгартириш;
- тизимга бирор-бир фойдаланувчининг номи ва пароли билан кириш.

Агар биринчи холда дастурнинг узгартирилиши ёки тизим суровларининг узтартирилиши талаб этилса, иккинчи холда эса мавжуд фойдаланувчининг паролени клавиатура оркали киритаётган пайтда куриб олиш ва ундан фойдаланиш оркали рухсатсиз кириш амалга оширилади.

Маълумотларга рухсатсиз эгалик килиш учун зарур булган дастурларни татбик этиш усуллари куйидагилардир:

- компьютер тизимлари захираларига рухсатсиз эгалик килиш;
- компьютер тармоги алока каналларидаги хабар алмашуви жараёнига рухсатсиз аралашув;
- вирус куринишидаги дастурий камчиликлар (дефектлар)ни киритиш.

Купинча компьютер тизимида мавжуд заиф кисмларни «тешик»лар, «люк»лар деб аташади. Баъзан дастурчиларнинг узи дастур тузиш пайтида бу «тушик»ларни колдиришади, масалан:

- натижавий дастурий махсулотни енгил йигиш мақсадида;
- дастур тайёр булгандан кейин яширинча дастурга кириш воситасига эга булиш мақсадида.

Мавжуд «тешик»ка зарурий буйруклап куйилади ва бу буруклар керакли пайтда уз ишини бажариб боради. Вирус куринишидаги дастурлар эса маълумотларни йукотиш ёки кисман узгартириш, иш сеансларини бузиш учун ишлатилади.

Юкорида келтирилганлардан хулоса килиб, маълумотларга рухсатсиз эгалик килиш учун дастурий мосламалар энг кучли ва самарали инструмент булиб, компьютер ахборот захираларига катта хавф тугдириши ва буларга карши кураш энг долзарб муаммолардан бири эканлигини таъкидлаш мумкин.

Такрорлаш учун саволлар

1. Протоколлар ижобий имкониятлари билан бирга кандай камчиликларга ҳам эга?
2. Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари.

3. Маълумотларга рухсатсиз эгалик қилиш учун зарур бўлган дастурларни татбиқ этиш усуллари айтиб ўтинг.

Мустақил иш топшириқлари:

1. Ахборот химояси тизимини ташкил қилиш долзарблигини Ўзбекистон Республикасидаги корхоналар мисолида кўрсатинг.
2. Ахборот тизимларининг асосий таъсирчан қисмлари рўйхатини кенгайтиринг.
3. Windows операцион муҳитида маълумотга рухсатсиз киришдан қанчалик даражада химоялангани ҳақида маълумот беринг.
4. Маълумотларга рухсатсиз киришнинг дастурий воситаларига мисоллар келтиринг

Мавзуга доир тестлар:

1. Шифрлаштириш сузининг маъноси нима ?
 - *А. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн шифрланган матн билан алмаштирилади.
 - Б. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн жадвал билан алмаштирилади.
 - С. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн латинча матн билан алмаштирилади.
 - Д. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн инглизча матн билан алмаштирилади.
2. Дешифрлаштириш сўзининг маъноси нима?
 - А. Дешифрлаштириш – бу матн маълумотларини ўзгартириш учун иккилик коди.
 - *Б. Дешифрлаштириш – шифрлаштиришга тескари жараён. Калит асосида шифрланган матн ўз ҳолатига ўзгартирилади.
 - С. Шифрлаштириш – бу график маълумотларни ўзгартириш учун саккизлик коди.
 - Д. Шифрлаштириш – бу график ва матнли маълумотларни ўзгартириш учун саккизлик коди
3. Калитларни тақсимлаш ва калит билан бошқариш терминлари қайси жараёнда тааллуқли?
 - А. Ахборотни чиқаришнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади
 - Б. Ахборотни киритишнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади
 - *С. Ахборотни қайта ишлашнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади
 - Д. Ахборотни ёзишнинг шундай жараёни, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

4. Мумкин бўлган тўпламлардан олинган ҳар қандай калитрлар куйидагини таъминлайди

- *а) ахборотни ишончли ҳимоялаш
- б) компьютерни ишончли ҳимоялаш
- с) файлни ишончли ҳимоялаш
- д) ахборот ва файлни ишончли ҳимоялаш

Адабиётлар

1. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.:СИНТЕГ, 2000, 248 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.- М.: Издательство ТРИУМФ, 2003 – 816 с.
3. Коблиц. Н. Курс теории чисел и криптографии - М., Научное издательство ТВП, 2001 г., 260 стр. (перевод с английского).

6 – МАЪРУЗА: КОМПЬЮТЕР ТАРМОҚЛАРИДА ЗАМОНАВИЙ ҲИМОЯЛАШ УСУЛЛАРИ ВА ВОСИТАЛАРИ

РЕЖА

1. *Компьютер тармоқларида ахборот ҳимоясини ташкил қилиш асослари.*
2. *Компьютер телефониясидаги ҳимоялаш усуллари.*
3. *Компьютер тармоқларида ҳимояни таъминлаш усуллари.*
4. *Компьютер тармоқларида маълумотларни ҳимоялашнинг асосий йуналишлари.*

Дарснинг ўқув ва тарбиявий мақсади: Талабаларга компьютер тармоқларининг заиф қисмлари, тармоқ ҳимоясини ташкил қилиш асослари ва таъминлаш усуллари, компьютер телефониясидаги ҳимоялаш усуллари ҳақида тушунча бериш.

Таянч иборалар: компьютер тармоғи, тармоқ ҳимояси, операцион тизим, маълумот тарқалиши, рухсатсиз кириш, протокол, дастурий ва техник воситалар.

Дарс ўтиш воситалари: синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва компьютердан самарали фойдаланилади.

Дарс ўтиш усуллари: такрорлаш, суҳбат, ва савол-жавоб ҳамда, мунозара (мавзунини ўзлаштиришни мустақамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага

ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут.

Ташкилий қисми: Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давомати – 2 минут.

Билимларни баҳолаш: янги мавзунини ўрганиш учун зарур бўлган материал бўйича суҳбат – 10 минут.

Янги мавзунини баён этиш – 55 минут.

Мавзу ўзлаштирилган даражасини аниқлаш – 10 минут.

Уйга вазифа – 3 минут.

Компьютер тармоқларида ахборот химоясини таъкил қилиш асослари.

Хозирги вақтда локал ҳисоблаш тармоқари (ЛАН) ва глобал ҳисоблаш тармоқлари (WAN) орасидаги фарқлар йўқолиб бормокда. Масалан, Netware 4x ёки Винес 4.11. операцион тизимлари ЛАНнинг фаолиятини ҳудудий даражасига чиқармокда. Бу эса, яъни ЛАН имкониятларининг ортиши, маълумотларни химоялаш усуллари янада такомиллаштиришни талаб қилмокда.

Тармоқни химоялаш зарурлиги қуйидаги ҳоллардан келиб чиқади:

- бошқа фойдаланувчилар массивларини ўқиш;
- компьютер хотирасида қолиб кетган маълумотларни ўқиш;
- химоя чораларини айланиб ўтиб, маълумот ташувчиларни нусхалаш;
- фойдаланувчи сифатида яширинча ишлаш;
- дастурий тутгичларни ишлатиш;
- дастурлаш тилларининг камчиликларидан фойдаланиш;
- химоя воситаларини билиб туриб ишдан чиқариш;
- компьютер вирусларини киритиш ва ишлатиш.

Тармоқ, муҳофазасини таъкил этишда қуйидагиларни эътиборга олиш лозим:

- муҳофаза тизимининг назорати;
- файлларга киришнинг назорати;
- тармоқда маълумот узатишнинг назорати;
- ахборот захираларига киришнинг назорати;
- тармоқ билан уланган бошқа тапмоқлапга маълумот тарқалишининг назорати.

Тармоқ, элементлари уртасида утқазилаётган маълумотларни муҳофаза этиш учун қуйидаги чораларни куриш керак:

- маълумотларни аниқлаб олишга йўл қўймаслик;
- ахборот алмашишни таҳлил қилишга йўл қўймаслик;
- хабарларни узгартиришга йўл қўймаслик;
- яширинча уланишга йўл қўймаслик ва бу ҳолларни тезда аниқлаш.

Хозирги вақтга мувофиқлаш дастурий таъминоти хилма-хил бўлса ҳам, операцион тизимлар зарурий муҳофазанинг керакли даражасини таъминламас эди. Netware 4.1, Windows NT операцион тизимлари етарли даражада муҳофазани таъминлай олиши мумкин.

Компьютер телефониясидаги химоялаш усуллари

Электрон коммуникацияларнинг замонавий технологиялари кейинги пайтларда ишбилармонларга алоқа каналлари бўйича ахборотнинг турлича қуринишлари (масалан: факс, видео, компьютерли, нуткли ахборотлар)ни узатишда купгина имкониятлар яратиб бермоқда.

Замонавий офис бугунги кунда алоқа воситалари ва ташкилий техника билан ҳаддан ташқари тулдириб юборилган ва уларга телефон, факс, автожавоб апарати, модем, сканер, шахсий компьютер ва х.к. қиради. Замонавий техника учун ахборот-коммуникациялар технологияси — компьютерлар телефонияси ривожланиши билан катта тўртки берилди.

Компьютер телефониясида қулланилаётган нутқини аниқловчи технология телефон қилувчининг овозидан таниб олиш учун аҳамиятга эгадир. Компьютер телефониясининг химоясини етарли даражада таъминлаш учун Преттй Гоод Привасй Инс. фирмасининг ПС Пҳоне 1.0 дастурий пакет ишлаб чиқарилган. У компьютер телефонияси орқали узатилаётган ахборотларни химоялаш учун ахборотларни рақамли қуринишга ўтказди ва қабул пайтида эса дастурий-техник воситалар ёрдамида қайта ишлайди. Замонавий компьютер телефонияси воситаларининг шифрлаш тезлиги ҳам жуда юқоридир, ҳато қилиш эҳтимоли эса жуда кичикдир (тахминан $10^{-8} - 10^{-12}$).

Компьютер тармоқларида химояни таъминлаш усуллари

Компьютер тармоқларида ахборотни химоялаш деб фойдаланувчиларни руҳсатсиз тармоқ, элементлари ва захираларига эғалик қилишни ман этишдаги техник, дастурий ва криптографик усул ва воситалар, ҳамда ташкилий тадбирларга айтилади.

Бевосита телекоммуникация каналларида ахборот ҳавфсизлигини таъминлаш усул ва воситаларини қуйидагича таснифлаш мумкин:

Тўсқинлик апаратларга, маълумот ташувчиларга ва бошқаларга қиринишга физикавий усуллар билан қаршилиқ қўришиш деб айтилади.

Эғаликни бошқариш — тизим захиралари билан ишлашни тартибга солиш усулидир.

Никоблаш — маълумотларни ўқиб олишни қийинлаштириш мақсадида уларни криптография орқали кодлаш.

Тартиблаш — маълумотлар билан ишлашда шундай шарт-шароитлар яратиладики, руҳсатсиз тизимга қириб олиш эҳтимоли қамайтирилади.

Мажбурлаш — қабул қилинган қоидаларга асосан маълумотларни қайта ишлаш, ақс ҳолда фойдаланувчилар моддий, маъмурий ва жиноий жазоланадилар.

Ўндамок — ахлокий ва одобий қоидаларга биноан қабул қилинган тартибларни бажаришга йўналтирилган.

Ўшбу тадбирларни амалга оширишда асосан криптографик усуллар қулланилади.

Компьютер оркали содир этидадиган жиноятлар окибатида факатгина АКШ хар йили 100 млрд. доллар зарар куради. Уртача хар бир жиноятда 430 минг доллар угирланади ва жиноятчини кидириб топиш эхтимоли 0,004% ни ташкил этади.

Мутахассисларнинг фикрича ушбу жиноятларни 80%и бевосита корхонада ишлайдиган ходимлар томонидан амалга оширилади.

Ушбу камчиликларни бартараф килишда ва компьютер жиноятларини камайтиришда куйидаги чора-тадбирларни утказиш керак булади:

- персонал масъулиятини ошириш;
- ишга кабул килинадиган ходимларни текширувдан утказиш;
- мухим вазифани бажарувчи ходимларни алмаштириб туриш;
- пароль ва фойдаланувчиларни кайд килишни яхши йулга куйиш;
- маълумотларга эгалик килишни чеклаш;
- маълумотларни шифрлаш.

Ахборот-коммуникациялар технологияларининг ривожланиши окибатида купгина ахборотни химоялаш инструментал воситалари ишлаб чикилган. Улар дастурий, дастурий-техник ва техник воситалардир.

Компьютер тармокларида маълумотларни химоялашнинг асосий йуналишлари

Ахборотларни химоялашнинг мавжуд усул ва воситалари хамда компьютер тармоклари каналларидаги алоканинг хавфсизлигини таъминлаш технологияси эволюциясини солиштириш шуни курсатмокдаки, бу технология ривожланишининг биринчи боскичида дастурий воситалар афзал топилди ва ривожланишга эга булди, иккинчи боскичида химоянинг хамма асосий усуллари ва воситалари интенсив ривожланиши билан характерланди, учинчи боскичида эса куйидаги тенденциялар равшан булмокда:

- ахборотларни химоялаш асосий функцияларининг техник жихатдан амалга оширилиши;
- бир нечта хавфсизлик функцияларини бажарувчи химоялашнинг биргаликдаги воситаларини яратиш;
- алгоритм ва техник воситаларни унификация килиш ва стандартлаштириш.

Компьютер тармокларида хавфсизликни таъминлашда хужумлар юкори даражада малакага эга булган мутахассислар томонидан амалга оширилишини доим эсда тутиш лозим. Бунда уларнинг харакат моделларидан доимо устун турувчи моделлар яратиш талаб этилади. Бундан ташкари, автоматлаштирилган ахборот тизимларида персонал энг таъсирчан кисмлардан биридир. Шунинг учун, ёвуз ниятли шахсга ахборот тизими персоналидан фойдалана олмаслик чора-тадбирларини утказиб туриш хам катта ахамиятга эга.

Такрорлаш учун саволлар

1. *Компьютер тармокларининг заиф кисмлари нимадан иборат?*
2. *Тармок химоясини ташикл килишда нималарга эътибор бериш зарур?*

3. *Компьютер телефониясида қандай хавсизлик муаммолари мавжуд?*
4. *Компьютер тармоқларида маълумотларни химоялашнинг асосий йуналишларини айтиб утинг.*

Мустақил иш топшириқлари:

1. Компьютер тармоқларининг заиф қисмлари руйхатини тузинг.
2. Компьютер телефониясидаги химоялаш усуллариға мисоллар кўрсатинг.
3. Компьютер тармоқларида химояни таъминлаш учун қуланадиган усуллар руйхатини келтиринг.
4. ЭХМ химоясини таъминлашнинг техник воситаларини таснифлаб беринг.
5. Компьютер жинойтларини камайтиришда қандай чора-тадбирларни утказиш керак?

Мавзуга доир тестлар:

1. Автоматик қайта қакирув усули гоёси қуйдагидан иборат
 - а) марказий базадан узоклашган фойдаланувчи базаға бевосита муружаат қилолмайди – шифр талаб этилади
 - *б) марказий базадан узоклашган фойдаланувчи базаға бевосита муружаат қилолмайди – идентификацион код талаб этилади
 - с) марказий базадан узоклашган фойдаланувчи базаға бевосита муружаат қилолмайди – шифр талаб этилмайди
 - д) марказий базадан узоклашган фойдаланувчи базаға бевосита муружаат қилолмайди – парол ва шифр талаб этилади
2. Узок (олис)лаштирилган масофадан бузиш нима?
 - а) Хаваскорлик фаолияти
 - б) Абонентлик фаолияти
 - *с) Хакерлик фаолияти
 - д) Фойдаланувчи фаолияти
3. Хакер (ҳаскер) нима?
 - *а) хакер – бу булаётган ходисаларға қушилишни истайдиган одам учун умумий таъриф
 - б) хакер – ШК фойдаланувчиси
 - с) хакер – бу Интернет абоненти
 - д) хакер – бу булаётган ходисаларға қушилишни истамайдиган одам учун асосий таъриф.
4. Бузувчи (взломщик) нима?
 - а) сраскер - хакер
 - *б) сраскер – интродер (қоида бузувчи)

- с) сраскер - Пинг
- д) сраскер - домаин

Адабиётлар

1. Гуломов С.С. ва бошқ. Иктисодий информатика: Олий уқув юртларининг иктисодий мутахассисликлари учун дарслик.
2. Галатенко В.А., Под ред. Бетелина В.Б. Информационная безопасность: практический подход. Наука, 1998
3. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.:СИНТЕГ, 2000, 248 с.

7 – МАЪРУЗА: ИНТЕРНЕТДА АХБОРОТЛАР ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ АСОСЛАРИ

РЕЖА

1. *Интернетда пйхсамсиз кириш усулларининг таснифи;*
2. *Рухсат этилган манзилларнинг рухсат этилмаган вақтда уланиши;*
3. *Тармоқлараро экран ва унинг вазифалари;*
4. *Тармоқлараро экраннинг асосий компонентлари.*

Дарснинг ўқув ва тарбиявий мақсади: Талабаларга Интернетда пйхсатсиз кириш усуллари, рухсат этилган манзилларнинг рухсат этилмаган вақтда уланиши, тармоқлараро экран, унинг вазифалари ва асосий компонентлари ҳақида тушунча бериш.

Таянч иборалар: глобал тармоқ, манзил, рухсат этилган, рухсатсиз кириш, тармоқ ҳимояси, тармоқлараро экран, шлюз, амалий даража, тармоқ даражаси.

Дарс ўтиш воситалари: синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва компьютердан самарали фойдаланилади.

Дарс ўтиш усуллари: такрорлаш, суҳбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут.

Ташкилий қисми: Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давомати – 2 минут.

Билимларни баҳолаш: янги мавзуни ўрганиш учун зарур бўлган материал бўйича суҳбат – 10 минут.

Янги мавзуни баён этиш – 55 минут.

Мавзу ўзлаштирилган даражасини аниқлаш – 10 минут.

Уйга вазифа – 3 минут.

Интернетда пўхсамсиз кириш усулларининг таснифи

Хар кандай ташкилот Интернетга уланганидан сунг, хосил буладиган куйидаги муаммоларни хал этишлари шарт:

- ташкилотнинг компьютер тизимини хакерлар томонидан бузилиши;
- Интернет оркали жунатилган маълумотларнинг ёвуз ниятли шахслар томонидан укиб олиниси;
- ташкилот фаолиятига зарар етказилиши.

Интернет лойихалаш даврида бевосита химояланган тармок сифатида ишлаб чикилмаган. Бу сохада хозирги кунда мавжуд булган куйидаги муаммоларни келтириш мумкин:

- маълумотларни енгиллик билан кулга киритиш;
- тармокдаги компьютерлар манзилини сохталаштириш;
- ТСП/ИП воситаларининг заифлиги;
- купчилик сайтларнинг нотугри конфигурацияланиши;
- конфигурациялашнинг мураккаблиги.

Глобал тармокларнинг чегарасиз кенг ривожланиши ундан фойдаланувчилар сонининг ошиб боришига сабаб булмокда, бу эса уз навбатида ахборотлар хавфсизлигига тахдид солиш эхтимолининг ошишига олиб келмокда. Узок, масофалар билан ахборот алмашиш зарурияти ахборотларни олишнинг катъий чегараланишини талаб этади. Шу максадда тармокларнинг сегментларини хап хил даражадаги химоялаш усуллари таклиф этилган:

- эркин кириш (масалан: WWW-сервер);
- чегараланган киришлар сегменти (узок масофада жойлашган иш жойига хизматчиларнинг кириши);
- ихтиёрий киришларни ман этиш (масалан, ташкилотларнинг молиявий локал тармоклари).

Рухсат этилган манзилларнинг рухсат этилмаган вақта уланиши

Ушбу хавф глобал тармокларнинг бир канча сохаларини камраб олади, жумладан:

- локал соха;
- локал-глобал тармокларнинг бирлашуви;
- мухим ахборотларни глобал тармокларда жунатиш;
- глобал тармокнинг бошкарилмайдиган кисми.

Ихтиёрий ахборот тармокларининг асосий компонентлари бу серверлар ва ишчи станциялар хисобланади. Серверда ахборотлар ёки хисоблаш ресурслари ва ишчи станцияларда хизматчилар ишлайди. Умуман ихтиёрий компьютер хам, сервер хам ишчи станция булиши мумкин — бу холда уларга нисбатан хавфли хужумлар булиши эхтимоли бор.

Серверларнинг асосий вазифаси ахборотларни саклаш ва такдим килишдан иборат.

Ёвуз ниятли шахсларни куйидагича таснифлаш мумкин:

- ахборот олишга имконият олиш;
- хизматларга рухсат этилмаган имконият олиш;
- маълум синфдаги хизматларнинг иш режимини ишдан чиқаришга уриниш;
- ахборотларни узгартиришга ҳаракат ёки бошқа турдаги ҳужумлар.

Ишчи станцияларга ҳужумнинг асосий мақсади, асосан, қайта ишланаётган маълумотларни ёки локал сақланаётган ахборотларни олишдир. Бундай ҳужумларнинг асосий воситаси «Троян» дастурлар саналади. Бу дастур уз тузилиши бўйича компьютер вирусларидан фарқ қилмайди ва компьютерга тушиши билан узини билинтирмасдан туради. Бошқача айтганда, бу дастурнинг асосий мақсади — тармок, станциясидаги химоя тизимини ички томондан бузишдан иборат.

Бу ҳолатда масалани ҳал қилиш маълум кийинчиликка олиб келади, яъни махсус тайёрланган мутахассис лозим ёки бошқа чоралар қабул қилиш керак бўлади. Бошқа бир оддий химоя усулларида бири ҳар қайси ишчи станциядаги тизимли файллар ва хизмат соҳасидаги маълумотларнинг узгаришини текшириб турувчи ревизор (ингл. *адвизер*— қиравчи) урнатиш саналади.

Тармоқлараро экран ва унинг вазифалари

Тармоқлараро экран — химоялаш воситаси бўлиб, ишончли тармок, ва ишончсиз тармок орасида маълумотларга қиришни бошқаришда қулланилади.

Тармоқлараро экран қуп компонентли бўлиб, у Интернетдан ташкилотнинг ахборот захираларини химоялаш стратегияси саналади. Яъни ташкилот тармоғи ва Интернет орасида қуриклаш вазифасини бажаради.

Тармоқлараро экраннинг асосий функцияси — маълумотларга эғалик қилишни марказлаштирилган бошқарувини таъминлашдан иборат.

Тармоқлараро экран қуйидаги химояларни амалга оширади:

- уринсиз трафиклар, яъни тармокда узатиладиган ҳабарлар оқимини тақиклаш;
- қабул қилинган трафикни ички тизимларга йуналтириш;
- ички тизимнинг заиф қисмларини яшириш билан Интернет томонидан уюштириладиган ҳужумлардан химоялаш;
- барча трафикларни баёнлаштириш;
- ички маълумотларни, масалан тармок топологиясини, тизим номларини, тармок усқуналарини ва фойдаланувчиларнинг идентификаторларини Интернетдан яшириш;
- ишончли аутентификацияни таъминлаш.

Тармоқлараро экраннинг асосий компонентлари

Тармоқлараро экранларнинг компонентлари сифатида қуйидагиларни қелтириш мумкин: филътрловчи -йуллоовчи; тармок, даражасидаги шлюзлар; амалий даражадаги шлюзлар.

Филътрловчи-йуллоовчи — йуллоовчи, яъни компьютер тармоғида маълумотларни манзилга етказувчи дастурлар пакети ёки сервердаги дастур бўлиб, у қирадиган ва қикадиган пакетларни филътрлайди. Пакетларни

филтрлаш, яъни уларни аник тупламга тегишлилигини текшириш, ТСП/ИП сарлавхасидаги маълумотлар буйича амалга оширилади.

Тармок даражасидаги шлюзлар ишончли мижозлардан аник хизматларга суровномасини кабул килади ва ушбу алоканинг конунийлигини текширгандан сунг уларни ташки хост-компьютер билан улайди. Шундан сунг шлюз иккала томонга хам пакетларни филтрламай жунатади.

Бундан ташкари, тармок даражасида шлюзлар бевосига сервер-даллол вазифасини бажаради. Яъни, ички тармокдан келадиган ИП манзиллар узгартирилиб, ташкирига факатгина битта ИП манзил узатилади. Натижада, ички тармокдан ташки тармок билан тугридан-тугри богламайди ва шу йул билан ички тармокни химоялаш вазифасини утайди.

Амалий даражадаги шлюзлар филтрловчи-йулловчиларга мансуб булган камчиликларни бартараф этиш максидида ишлаб чикилган. Ушбу дастурий восита ваколатланган сервер, деб номланади ва у бажарилаётган хост-компьютер эса амалий даражадаги шлюз деб аталади.

Амалий даражадаги шлюзлар мижоз ва ташки хост-компьютер билан тугридан-тугри алока урнатишга йул куймайди. Шлюз келадиган ва жунатиладиган пакетларни амалий даражада филтрлайди. Сервер-даллоллап шлюз оркали аник сервер томонидан ишлаб чикилган маълумотларни кайтадан йуналтиради.

Амалий даражадаги шлюзлар нафакат пакетларни филтрлаш, балки сервернинг барча ишларини кайд килиш ва тармок администраторини нохуш ишлардан хабар килиш имкониятига хам эга.

Амалий даражадаги шлюзларнинг афзалликлари куйидагилардан иборат:

- глобал тармок томонидан ички тармок таркиби курунмайди;
- ишончли аутентификация ва кайд килиш;
- филтрлаш коидаларининг енгиллиги;
- куп тамойилли назоратларни амалга ошириш мумкинлиги.

Филтрловчи-йулловчиларга нисбатан амалий даражадаги шлюзларнинг камчиликлари куйидагилардан иборат самарадорлигининг пастлиги; нархининг киммат булиши.

Амалий даражадаги шлюзлар сифатида куйидагиларни мисол килиб келтириш мумкин:

- Бордер Варе Фире Валл Сервер — жунатувчининг ва кабул килувчининг манзилларини, вақтини ва фойдаланилган протоколларни кайд килади;

- Бласк Холе — сервернинг барча ишларини кайд килади ва тармок администраторига кутилаётган бузилиш хакида хабар жунатади.

Булардан ташкари куйидаги шлюзлар хам кулланилади:

Гаунтлет Интернетел ФиреуаУ, Алта Висла ФиреВали, АНС Интернетоск ва бошқалар.

Такрорлаш учун саволлар

1. Хар кандай ташкилот Интернетга уланганидан сунг андай муаммоларни хал этиши шарт?

2. Рухсат этилган манзилларнинг рухсат этилмаган вақтда уланишни тушунтириб беринг.

3. Қайси хавф глобал тармоқларнинг бир канча соҳаларини камраб олади?

4. Тармоқлараро экран ва унинг вазифалари

5. Тармоқлараро экраннинг асосий компонентлари

Мустақил иш топшириқлари:

1. Интернетда ахборот хавфсизлиги нуктаи назаридан мавжуд булган муаммоларни кўрсатинг.

2. Локал тармоқларнинг глобал тармоқарга кушилиши учун тармоқлар химояси администратори қандай масалаларни ҳал қилиши лозим:

3. Рухсат этилган манзилларнинг рухсат этилмаган вақтда уланиши хавфи глобал тармоқларнинг қайси соҳаларини камраб олади?

4. Тармоқлараро экраннинг вазифаларини таърифлаб беринг.

5. Амалий ва тармоқ даражадаги шлюзларнинг ишлаш принципларини кўрсатиб беринг.

Мавзуга доир тестлар:

1. “Инструстион Детестион Сйстем” нима?

а) Хужумни аниклаш дастури

б) Хужумни аниклаш модули

*с) Хужумни аниклаш тизими

д) Хужумни аниклаш пакети

2. Тармоқ даражасидаги аниклаш тизими қуйидагиларни текширади?

*а) Тармоқ доирасидаги пакетлар ва ёвуз ниятлининг химояланадиган тизим ичига кириш ҳолатини аниқлайди

б) Тармоқ доирасидаги дастур ва ёвуз ниятлининг химояланадиган тизим ичига кириш ҳолатини аниқлайди

с) Тармоқ доирасидаги модул ва ёвуз ниятлининг химояланадиган тизим ичига кириш ҳолатини аниқлайди

д) барча жавоблар тугри

3. Тармоқ даражасида химояланишнинг техник усуллари қуйидагиларга бўлинадилар:

*а) аппаратли, дастурли, аппарат-дастурли

б) ташкиллаштирилган, тизимли, аппаратли

с) аппарат-дастурли, тизимли, дастурли

д) тугри жавоб йук

Адабиётлар

1. Гуломов С.С. ва бошқ. Иктисодий информатика: Олий укув юртларининг иктисодий мутахассисликлари учун дарслик.

2. Галатенко В.А., Под ред. Бетелина В.Б. Информационная безопасность: практический подход. Наука, 1998

3. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.:СИНТЕГ, 2000, 248 с.

8 – МАЪРУЗА: ЭЛЕКТРОН ПОЧТАДА АХБОРОТЛАРГА НИСБАТАН МАВЖУД ХАВФ-ХАТАРЛАР ВА УЛАРДАН ХИМОЯЛАНИШ АСОСЛАРИ

РЕЖА

1. *Электрон почтадан фойдаланиш.*
2. *Электрон почтада мавжуд хавфлар.*
3. *Электрон почтани химоялаш.*

Дарснинг ўқув ва тарбиявий мақсади: Талабаларга электрон почтадан фойдаланишда ахборот хавфсизлигига нисбатан мавжуд бўлган хавфлар ва уларни бартараф этиш усуллари, чора-тадбирлари воситалари ҳақида тушунча бериш.

Таянч иборалар: глобал тармоқ, электрон почта, протокол, шахсий маълумот, спам, рухсат этилган манзил, апплет, динамик дастур тармоқ химояси.

Дарс ўтиш воситалари: синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва копмьютердан самарали фойдаланилади.

Дарс ўтиш усуллари: такрорлаш, суҳбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут.

Ташкилий қисми: Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давомати – 2 минут.

Билимларни баҳолаш: янги мавзуни ўрганиш учун зарур бўлган материал бўйича суҳбат – 10 минут.

Янги мавзуни баён этиш – 55 минут.

Мавзу ўзлаштирилган даражасини аниқлаш – 10 минут.

Уйга вазифа – 3 минут.

Электрон почтадан фойдаланиш

Электрон почта ёки Е-маил ҳозирги кунда Интернетдан фойдаланиш жараёнининг энг машхур касми ҳисобланади. Е-маил оркали дунё бўйича исталган жойга бир зумнинг узида хат юбориш ёки қабул қилиш ҳамда ёзилган хатларни факатгина бир кишига эмас, балки манзиллар руйхати бўйича жунатиш имконияти мавжуд. Е-маил оркали мунозаралар утказиш имконияти мавжуд ва бу йуналишда УСЕНЕТ сервери кул келади.

Купгина корхоналар уз фаолиятида бевосита Е-маил тизимидан фойдаланишади. Демак, корхона ва ташкилотлар рахбарлари маълум бир чора-тадбирлар оркали уз ходимларини Е-маил билан ишлаш, ундан оқилона фойдаланишга ургатиши лозим. Ушбу жараённинг асосий мақсади муҳим ҳужжатлар билан ишлашни тугри йулга қуйиш ҳисобланади.

Бу ерда қуйидаги йуналишлар бўйича тақлифларни эътиборга олиш зарур:

- Е-маил тизимидан ташкилот фаолияти мақсадларида фойдаланиш;
- шахсий мақсадда фойдаланиш;
- махфий ахборотларни сақлаш ва уларга кириш;
- электрон хатларни сақлаш ва уларни бошқариш.

Интернетда асосий почта протоколларига қуйидагилар қиради:

- СМТП (Симпле Маил Трансфер Протосол);
- ПОП (Пост Оффисе Протосол);
- ИМАП (Интернет Маил Ассесс Протосол);
- МИМЕ (Мульти пурпосе Интернет Маил Ехтенсионс).

Электрон почта билан ишлаш жараёнида қуйидаги хатоларга йул қуйиш мумкин: хатни тасодифан жунатиш; хатнинг нотугри манзил бўйича жунатилиши; хатлар архивининг кескин ошиб кетиши оқибатида тизимнинг ишдан чиқиши; янгиликларга нотугри обуна бўлиш; хатни тарқатиш руйхатида хатога йул қуйиш.

Агар ташкилотнинг почта тизими бевосита Интернетга уланган бўлса, йул қуйилган хатолар оқибати кескин ошиб кетади.

Ушбу хатоларнинг олдини олиш усулларининг баъзи бирлари қуйидагилар:

- фойдаланувчиларни уқитиш;
- электрон почта дастурларини тугри конфигурациялаш;
- Интернетдаги протоколларга тулик амал қилувчи дастурларни қуллаш.

Бундан ташқари электрон почтанинг шахсий мақсадда ишлатилиши ташкилот раҳбарияти учун баъзи бир муаммоларни келтириб чиқариши мумкин, чунки Е-маил манзилида ташкилот номлари акс эттирилган бўлиши эҳтимолдан холи эмас. Натижада, шахс жунатаётган хат ташкилот номидан деб қабул қилиниши мумкин. Шу боис, телефонлар қаби Е-маилдан шахсий ишлар учун фойдаланишни чеклаб қуйиш зарур бўлади. Албатта, буни жорий қилиш қийин масала.

Интернет тизимидаги электрон почта жуда қуп ишлатилаётган ахборот алмашиш каналларидан бири ҳисобланади. Электрон почта ёрдамида ахборот алмашуви тармокдаги ахборот алмашувининг 30%ини ташкил этади. Бунда ахборот алмашуви бор-йуги иккита протокол: СМТП (Симпле Маил Трансфер Протосол) ва POP-3 (Пост Оффисе Рголосол)ларни ишлатиш ёрдамида амалга оширилади. POP-3 мультимедиа технологияларининг ривожини акс эттиради, СМТП эса Аппранет проекти даражасида ташкил этилган эди. Шунинг учун ҳам бу протоколларнинг ҳаммага очиклиги сабабли, электрон почта ресурсларига руҳсатсиз киришга имкониятлар яратилиб берилмокда:

- СМТП сервер — дастурларининг ноқоррект урнатилиши туфайли бу серверлардан рухсатсиз фойдаланилмоқда ва бу технология «спама» технологияси номи билан маълум;

- электрон почта хабарларига рухсатсиз эгалик қилиш учун оддийгина ва самарали усуллардан фойдаланилмоқда, яъни қуйи катламларда винчестердаги маълумотларни ўқиш, почта ресурсларига қириш паролини ўқиб олиш ва ҳоказолар.

Электрон почтада мавжуд хавфлар

Электрон почта хизмати ва ҳамма протоколларнинг амалий жихатдан ахборотларга нисбатан ҳимоясининг тулик бўлмаганлиги муаммоси бор. Бу муаммолар қелиб чиқишининг асосий сабаби Интернетнинг УНИХ операцион тизим билан борликларида.

ТСР/ИР (Транснессион Сонтрол Протокол/Интернет Протосол) Интернетнинг глобал тармоғида коммуникацияни таъминлайди ва тармоқларда оммавий равишда қулланилади, лекин улар ҳам ҳимояни етарлича таъминлай олмайди, чунки ТСП/ИП пакетининг бошида ҳакер хужуми учун қулай маълумот қурсатилади.

Интернетда электрон почтани жунатишни оддий протокол почта транспорт хизмати амалга оширади (СМТП - Симпле Маил Трансфер Протосол). Бу протоколда мавжуд бўлган ҳимоялашнинг муҳим муаммоларидан бири - фойдаланувчи жунатувчининг мазилини қура олмаслиғидир. Бундан фойдаланиб ҳакер катта миқдорда почта хабарларини жунатиши мумкин, бу эса ишчи почта серверни қаддан ташқари банд бўлишига олиб қелади.

Интернетда оммавий тус олган дастур бу Сендмаил электрон почтасидир. Сендмаил томонидан жунатилган хабарлар босқинчи ҳакер ахборот шаклида фойдаланиши мумкин.

Тармоқ номлари хизмати (Домаин Наме Систем — ДНС) фойдаланувчилар номи ва хост-компьютерини - манзилини қурсатади. ДНС компаниянинг тармоқ тузилиши ҳақида маълумотларни сақлайди. ДНСнинг муаммоларидан бири шундаки, бундаги маълумотлар базасини муаллифлаштирилмаган фойдаланувчилардан яшириш анча қийин. Бунинг натижасида, ҳакерлар ДНС ни қупинча хост-компьютерларнинг ишончли номлари ҳақида маълумотлар манбасидан фойдаланиш учун ишлатиши мумкин.

Ўзқ, терминаллар эмуляцияси ҳимати ўзқ, тизимларни бир-бирига ўлаш учун хизмат қилади. Бу сервердан фойдаланувчилар ТЕЛНЕТ серверидан қуйхатдан ўтиш ва ўз номи ва паролини олиши лозим. ТЕЛНЕТ серверига ўланган ҳакер дастурни шундай ўрнатиши мумкинки, бунинг натижасида у фойдаланувчининг номи ва паролини ёзиб олиш имқонига эга бўлади.

Ўорлд Виде Веб — WWW бу тизим Интернет ёки интратармоқлардаги ҳар хил серверлар ичидаги маълумотларни қуриш учун хизмат қилади. WWW нинг асосий хоссаларидан бири — Тармоқлараро экран орқали аниқ протокол ва манзилларни фильтрлаш зарурлигини тармоқнинг ҳимоялаш сиёсати қарори билан ҳал этилишидир.

Электрон почта билан ишлаш қараёнида қуйидаги хавфлар мавжуд:

1. Жунатувчининг калбаки манзили. Кабул килинган хатни Е-маил манзили аниклигига тулик ишонч хосил килиш кийин, чунки хат жунатувчи уз манзилини калбакилаштириши мумкин.

2. Хатни кулга киритиш. Электрон хат ва унинг сарлавхаси узгартирилмасдан, шифрланмасдан жунатилади. Шу боис, уни йулда кулга киритиш ва мазмунини узгартириши мумкин.

3. Почта «бомба»си. Почта тизимига кўплаб электрон хатлар жунатилади, натижада тизим ишдан чиқади. Почта серверининг ишдан чиқиш ҳолатлари куйидагилардир:

- диск тулиб қолади ва кейинги хатлар кабул килинмайди. Агар диск тизимли бўлса, у ҳолда тизим тамомила ишдан чиқиши мумкин;

- киришдаги навбатда турган хатлар сонининг ошиб кетиши натижасида кейинги хатлар умуман навбатга куйилмайди;

- олинadиган хатларнинг максимал сонини узгартириш натижасида кейинги хатлар кабул килинмайди ёки учиради;

- фойдаланувчига ажратилган дискнинг тулдирилиши натижасида кейинги хатлар кабул килинмайди ва дискни тозалаб бўлмайди.

4. «Куркинчли» (нохуш) хат. Интернет оркали олинadиган электрон хатларнинг умуман номаълум шахслар томонидан жунатилиши ва бу хатда фойдаланувчиларнинг шахсиятига тегувчи сузлар бўлиши мумкин.

Электрон почтани химоялаш

Юкорида келтирилган хавфларга нисбатан куйидаги химояланиш усуллари ишлаб чиқилган:

- калбаки манзилдан химояланиш, бу ҳолда шифрланган электрон имзоларни куллаш таклиф килинади;

- хатни кулга киритишдан химояланиш, бу ҳолда хабарни ёки жунатиш каналини шифрлаш таклиф килинади.

Ушбу химоялаш усуллари бевосита қолган хавфларнинг улушини камайтиради.

Такрорлаш учун саволлар

1. *Электрон почтадан фойдаланиш хусусиятларини кўрсатинг.*

2. *Е-маил адресларидан фойдаланишда қандай ахборот хавфсизлиги муаммолари мавжуд.*

3. *Электрон почтада мавжуд хавфлар.*

4. *Электрон почтага рухсатсиз киришнинг қандай усуллари мавжуд.*

5. *Электрон почтани химоялаш усуллари ҳақида гапириб беринг.*

Мустақил иш топшириқлари:

1. Интернетда ахборот хавфсизлиги нуқтаи назаридан мавжуд бўлган муаммоларни кўрсатинг.

2. Электрон почта ишини таъминладиган протоколлар руйхатини келтиринг.

3. Бирон-бир электрон почта протоколининг ишлаш принципини тавсифлаб беринг.

4. Электрон почта билан ишлаш жараёнида мавжуд хавфлар руйхатини келтиринг.

5. Электрон почтада ахборот хавфсизлигига нисбатан хавфларга қандай химояланиш усуллари ишлаб чиқилган:

Мавзуга доир тестлар:

1. Ахборот химояси деганда қуйидагилар тушунилади:

*а) Бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик жараён

б) Бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик процедураси

с) Бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик услуги

д) Барча жавоблар тугри

2. Ахборотлар тарқалиш канали – бу:

а) Манбаларнинг ёпиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар ҳисобланадилар

*б) Манбаларнинг очиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар ҳисобланадилар

с) Манбаларнинг ёпиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар ҳисобланадилар

д) Тугри жавоблар йук

3. Ахборотлар тарқалиш техник каналлари – бу:

а) Акустик ва вироакустик, электрик, телеканаллар, оптик

б) Акустик ва вироакустик, электрик, серверлар, оптик

*с) Акустик ва вироакустик, электрик, радио каналлар, оптик

д) Акустик ва вироакустик, электрик, теле каналлар, провайдерлар

Адабиётлар

1. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.:СИНТЕГ, 2000, 248 с.

2. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация химояси: Олий ўқув юрт. талаб. учун ўқув ўқланма.- Тошкент давлат техника университети, 2003. 77 б.

3. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.

14. АМАЛИЁТ МАШҒУЛОТЛАРИ ДАРС ИШЛАНМАСИ

Самарқанд Давлат университети

“Ахборотлаштириш технологиялари” кафедраси

Химматов И.Қ

Ахборотларни ҳимоялаш фанидан

амалиёт машғулотлари ишланмаси

18 соат

САМАРҚАНД — 2019

1 амалиёт машғулоти

Мавзу: Бевосита ўрин алмаштириш бўйича шифрлаш

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади:

Симметриқ криптотизимни асосий усуллари ўрганиш ва тадқиқ етиш.

Таянч иборалар: шифр ва шифрлаш, ўрин алмаштириш, блок, криптотурғунлик, ахборот, блок, калит.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компьютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намоёниш, амалий ишлаш.

Дарснинг технологик харитаси: -80 минут.

Ташкилий қисм: хонанинг тозаллиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.

Талабалар билимини баҳолаш: ўтилган мавзунини қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.

Янги мавзу баёни: -30 минут.

Мавзунини ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-20 минут.

Синов саволлари – 5 минут.

Уйга вазифалар бериш - 3 минут.

Мавзу баёни

Қисқача назарий маълумот:

Ўрин алмаштиришга мисол тариқасида дастлабки ахборот блокинини матрицага қатор бўйича ёзишни, ўқишни еса устун бўйича амалга оширишни кўрсатиш мумкин. Матрица қаторларини тўлдириш ва шифрланган ахборотни устун бўйича ўқиш кетма-кетлиги калит ёрдамида берилиши мумкин. Усулнинг криптотурғунлиги блок узунлигига (матрица ўлчамига) боғлиқ. Масалан узунлиги 64 символга тенг бўлган блок (матрица ўлчами 8x8) учун калитнинг $1,6 \cdot 10^9$ комбинацияси бўлиши мумкин. Узунлиги 256 символга тенг бўлган блок (матрица ўлчами 16x16) калитнинг мумкин бўлган комбинацияси $1,4 \cdot 10^{26}$ га етиши мумкин. Бу ҳолда калитни саралаш масаласи замонавий ЕХМлар учун ҳам мураккаб ҳисобланади.

Ўрин алмаштириш шифри оддий шифрлаш ҳисобланиб, бу усулда қатор ва устундан фойдаланилади. Чунки шифрлаш жадвал асосида амалга оширилади. Бу ерда калит (К) сифатида жадвалнинг устун ва қатори хизмат

килади. Матн (T_0) символларининг ўлчамига қараб $N \times M$ жадвали тузилади ва очиқ матнни (T_0) устун бўйича жойлаштирилиб чиқилади, қатор бўйича ўқилиб шифрланган матнга (T_1) ега бўлинади ва блокларга бўлинади.

Масалан, «Ахборот хавфсизлиги жадвали» матни шифрлансин.

T_0 =Ахборот хавфсизлиги жадвали;

$K = 5 \times 5$; $B=5$;

А	О	Ф	И	Д
Х	Т	С	Г	В
Б	Х	И	И	А
О	А	З	Ж	Л
Р	В	Л	А	И

T_1 =АОФИД_ХТСГВ_БХИИА_ОАЗЖЛ_РВЛАИ

Биринчи бўлиб, шифрлаш жадвалидан (ХИВ асрнинг охирларида) дипломатик муносабатларда, харбий соҳаларда ахборотни муҳофазалашда фойдаланилган.

Оддий ўрин алмаштириш усулидан ташқари калит ёрдамида ўрин алмаштириш усули ҳам мавжуд. Шифрлаш жадвалидан калит орқали фойдаланилади.

Бу ерда калит символларига мос ҳолда жадвалнинг ўлчамига қараб $N \times M$ жадвали тузилади ва очиқ матнни (T_0) устун бўйича жойлаштирилиб чиқилади. Сўнгра калит символлари алфавит тартибида тартибланиб, устун бўйича ўрин алмаштирилади, қатор бўйича ўқилиб шифрланган матнга (T_1) ега бўлинади ва блокларга бўлинади.

T_0 = Ўзбекистон келажаги буюк давлат;

K = Тошкент;

$B=4$;

Матнда 28-та ва калитда 7-та ҳарфлар борлиги учун 7×7 жадвал тузамиз.

Ў	К	О	Л	Г	Ю	В
З	И	Н	А	И	К	Л
Б	С	К	Ж	Б	Д	А
Е	Т	Е	А	У	А	Т

Енди калит орқали 7×6 жадвал тузиб калитдаги ҳарфларни алфавит бўйича рақамлаб чиқамиз.

Т	о	Ш	к	Е	н	Т
5	4	7	2	1	3	6
Ў	К	О	Л	Г	Ю	В
З	И	Н	А	И	К	Л
Б	С	К	Ж	Б	Д	А
Е	Т	Е	А	У	А	Т

Рақам бўйича устунларни ўзгартириб чиқамиз .

е	к	н	о	Т	т	ш
1	2	3	4	5	6	7
Г	Л	Ю	К	Ў	В	О
И	А	К	И	З	Л	Н
Б	Ж	Д	С	Б	А	К
У	А	А	Т	Е	Т	Е

Қатор бўйича 4 тадан блокларга бўлиб, символлар кетма-кетлигидаги шифрланган матнни оламиз. Шунинг учун керакки, агар қаторда кетма-кет иккита бир хил ҳарф келса, чап тарафдан келадиган ҳарф биринчи рақамланади, кейин эса иккинчиси рақамланади ва шифрланган матн ҳосил қилинади.

$T_1 = \text{ГЛЮК УВОИ АК ИЗ ЛНБЖ ДСБА КУУА ТЕТЕ}''$;

Шифрни очишда тескари жараён амалга оширилади. Шифрланиш жараёни қадамма – қадам амалга оширилса мақсадга мувофиқ бўлади.

Икки томонлама ўрин алмаштириш усули. Бу усулда калит сифатида устун ва қатордаги ҳарфлар тартибидagi сонлардан фойдаланилади. Аввал бор калит символларига қараб жадвал тузилади, ва очиқ T_0 матн жойлаштирилиб чиқилади, сўнгра эса рақамлар навбатма – навбат тартибланиб, аввал устун, сўнгра эса қаторлар ўрни алмаштирилади ва жадвалдаги маълумот қатор бўйича ўқилиб T_1 га ега бўлинади. Масалан: «Интилганга толе ёр» очиқ матни шифрлаш талаб этилсин. Бу ерда калит бўлиб 1342 ва 2314 хизмат қилади. Яхшироқ изоҳланиши учун $K_1=1342$ ва $K_2=2314$, $B=4$ деб белгилаб оламиз.

4x4 жадвал яратиб T_0 қатор бўйича ёзамиз:

	2	3	1	4	
1	И	Н	Т	И	
3	Л	Г	А	Н	
4	Г	А	Т	О	
2	Л	Е	Ё	Р	

K_2

Энди қатор ва устул K_1 бўйича ўринлари алмаштирилади.

	2	3	4	1	
1	И	Н	Т	И	
2	Л	Е	Ё	Р	
3	Л	Г	А	Н	
4	Г	А	Т	О	

	2	3	4	1	
--	---	---	---	---	--

1	И	И	Н	Т
2	Р	Л	Е	Ё
3	Н	Л	Г	А
4	О	Г	А	Т

Охирги жадвалга асосан шифрланган матнни ёзамиз ва блокларга бўлиб чиқамиз.

$T_1 = \text{ИИНТ_РЛЕЁ_НЛГА_ОГАТ}$

Икки томонлама алмаштиришда жадвал катталигига қараб вариантлар ҳам ортиб боради. Жадвал ўлчамининг катталиги шифр чидамлилигини оширади: 3x3 жадвалда 36 та вариант, 4x4 жадвалда 576 та вариант, 5x5 жадвалда 14400 вариант;

Мураккаб алмаштиришли шифр. Мураккаб алмаштиришли шифр кўп алфавитли бўлиб, шифрлашда келувчи матннинг ҳар бир ҳарфи ўзининг оддий алмаштириш шифри каби шифрланади. Кўп алфавитли алмаштиришда алфавит кетма-кетлиги ва сиклидан фойдаланилади.

А-алфавитли алмаштиришда кирувчи ахборотнинг X_0 -ҳарфи B_0 -алфавитнинг Y_0 -ҳарфи билан алмаштирилади, X_1 -ҳарфи еса B_1 -алфавитнинг Y_1 -ҳарфи билан алмаштирилади, X_{p-1} -ҳарфи B_{p-1} -алфавитнинг Y_{p-1} -ҳарфи билан алмаштирилади ва ҳоказо.

Кўп алфавитли алмаштиришнинг $p=4$ бўлган ҳол учун умумий кўриниши қуйидаги жадвалда келтирилган.

Кирувчи ҳарфлар	X0	X1	X2	X3	X4	X5	X6	X7	X8	X9
Алфавит алмаштириш	B0	B1	B2	B3	B0	B1	B2	B3	B0	B1

Бу усул билан шифрланган матнни очишда етарли қийинчиликлар туғдиради, энди к-калит бир-неча маротаба ўзгаради. Бунда душман ҳар бир матн бўлагини қандай қилиб очишни бундай шифрлашда химояланганлик даражаси фойдаланиётган B_j -алфавит кетма-кетлигига боғлиқдир. Кўп алфавитли алмаштириш шифрини Леон Батист Альберт криптографияга киритди. 1566-йилда унинг “Трактат о шифре” китоби чиққан. Бутун дунёда кириптология (криптотахлил) асосини Л. Альберт назарияси ташкил қилади.

Ишни бажарилиш тартиби ва қўйилган вазифа:

Асосий матн шифрлаш усулларида бирида шифрлансин ва кадамма – кадам изоҳлансин. Шунингдек Делпи, ВБА, C++ ва C# дастурлаш тизимларидан бирида дастурий таъминот яратилсин.

Ҳисобот мазмуни:

Иш мавзуси.

Ишдан мақсад.

Шифрлаш алгоритмини блок-схемаси.

Дастур матни.

Топшириқ вариантлари

- **ВАРИАНТ №1.** «Самарқанд давлат университети» сўзи оддий ўрин алмаштириш усули билан шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №2.** «Самарқанд давлат университети» сўзи Сезар усули билан шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №3.** «Самарқанд давлат университети» сўзи силжитиш ва кўпайтиришга асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №4.** «Самарқанд давлат университети» сўзи кўпайтириш ва силжитишга асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №5.** «Самарқанд давлат университети» матни 6*6 жадвалга жойлаштирилсин. Жадвал устунлари ўринларини алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №6.** «Самарқанд давлат университети» матни 6*6 жадвалга жойлаштирилсин. Жадвал сатрлари ўринларини алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №7.** «Самарқанд давлат университети» матни блокларга ажратилсин. Ҳар бир блок номери силжитиш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №8.** «Самарқанд давлат университети» матни блокларга ажратилсин. Ҳар бир блок номери кўпайтириш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №9.** «Самарқанд давлат университети» матни блокларга ажратилсин. Ҳар бир блок номери айириш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №10.** «Самарқанд давлат университети» матни каррали силжитишга (силжитишлар символнинг жойлашган ўринлари номерига боғлиқда, масалан, калит $k=3$ да «Фан» сўзидаги «Ф» симболи 3+1 га, «а» симболи 3+2 га, «н» симболи еса 3+3 га силжийди) асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №11.** «Самарқанд давлат университети» матни тескари ўқиш ҳамда силжитиш алгоритми асосида шифрлансин ва шифр очилсин;
- **ВАРИАНТ №12.** «Самарқанд давлат университети» матни тескари ўқиш ҳамда кўпайтириш алгоритми асосида шифрлансин ва шифр очилсин;
- **ВАРИАНТ №13.** «Самарқанд давлат университети» матни тескари ўқиш ҳамда кўпайтириш ва силжитиш алгоритми асосида шифрлансин ва шифр очилсин;
- **ВАРИАНТ №14.** «Самарқанд давлат университети» матни 6*6 жадвалга жойлаштирилсин. Сатрлар ўрнига устунларни ёзиш орқали янги жадвал ҳосил қилинсин. Кейин еса сатрлари ўринларини алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №15.** «Самарқанд давлат университети» матни «сеҳирли квадрат» жадвали асосида шифрлансин ва шифр очилсин;

Назорат саволлари

1. Криптография мақсади ва вазифаси.
2. Оддий ўрин алмаштириш усули ва калит сўзли ўрин алмаштириш усули.
3. Икки марталик қайта куйиш усули ва сеҳрли квадрат усули.
4. Сезар усули ва калит сўзли Сезар тизими.

Фойдаланилган адабиётлар

9. Желников В. Криптография от папируса до компьютера. М.: АБФ, 1997. – 336с.
10. Нилс Фергюсон, Брюс Шнаер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
11. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
12. Коблис Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001й.
13. Масленников А. Практическая криптография БХВ – СПб 2003й.
14. Шнаер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
15. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002й.
16. Ганиев С.К.,Каримов М.М. Ҳисоблаш системалари ва тармоқларида информасия химояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.

2-амалиёт машғулоти

№2-Лаборатория иши

Мавзу: Полиалфавитли вижинер жадвалини (матрисасини) қўллаган ҳолда шифрлаш

Режа:

1. Қисқача назарий маълумот

2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади:

Симметрик криптоанизимни асосий усуллари, жумладан, полиалфавитли вижинер жадвалини, ўрганиш ва дастурини ишлаб чиқиш.

Таянч иборалар: Вижинер, Сезар, жадвал, матрица, шифр ва шифрлаш, ўрин алмаштириш, блок, криптографик, ахборот, блок. калит.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компьютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мукаамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси:-80 минут.

Ташкилий қисм: хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.

Талабалар билимини баҳолаш: ўтилган мавзунини қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.

Янги мавзу баёни: -30 минут.

Мавзунини ўзлаштириш даражасини аниқлаш ва мукаамлаш-20 минут.

Синов саволлари – 5 минут.

Уйга вазифалар бериш - 3 минут.

Мавзу баёни

Қисқача назарий маълумот

Вижинернинг шифрлаш тизими. Биринчи бўлиб Вижинер тизими 1586-йилда чоп этилган ва у кўп алфавитли тизимга нисбатан юқориқ ўринда туради. Блеза Вижинера ўзининг ХВИ асрнинг франсуз дипломати деб ҳисоблайди. У криптография тизимига, яъни унинг ривожланишига ўз ҳиссасини қўшган. Вижинер тизими Сезар шифрлаш тизимига қараганда мукаамалроқ ҳисобланиб, унда калит ҳарфидан ҳарфга алмаштирилади. Бундай кўп алфавитли алмаштириш шифрининг шифрлаш жадвали орқали ифодалаш мумкин. Қуйидаги биринчи жадвалда Вижинернинг инглиз алфавити учун мос келувчи жадвал кўрсатилган. Бу жадвалдан матнни шифрлаш ва уни очиш учун ишлатилади. Жадвалнинг иккита қисми бўлиб:

- Юқори қатордаги ҳарфлардан қиравчи очик ёзув учун фойдаланилади.
- Чап устундан еса калит ҳарфларидан фойдаланилади.

Мисол учун калит кетма-кетлигини р-деб олайлик, у ҳолда калит р-алфавитли р-сатрдан иборат бўлади.

$$\pi=(\pi_0, \pi_1, \dots, \pi_{p-1});$$

Вижинернинг шифрлаш тизимида очик матн $x=(x_0, x_1, \dots, x_{n-1})$ ва шифрланган матн $y=(y_0, y_1, \dots, y_{n-1})$ кўринишга ега. $\pi=(\pi_0, \pi_1, \dots, \pi_{p-1})$ калит ёрдамида қуйидагича муносабатда бўлади.

$$x=(x_0, x_1, \dots, x_{n-1}) \quad y=(y_0, y_1, \dots, y_{n-1});$$

$$(y_0, y_1, \dots, y_{n-1})=(\pi_0(x_0), \pi_1(x_1), \dots, \pi_{n-1}(x_{n-1}));$$

Юқоридаги ифодадан маълумки Вижинер жадвали орқали шифрлашда матннинг (ахборотнинг) ҳар бир ҳарфига мос келувчи калитнинг ҳар бир ҳарфи орқали уларнинг устун ва сатрлари кесишмасига мос келувчи ҳарфлар олинади.

Агар ўзбек алфавити ишлатилса, Вижинер матричаси [36x36] ўлчамга ега бўлади (2.1. -расм).

АБВГД.....	ЎҚҒҲ_
БВГДЕ.....	ҚҒҲ_А
ВГДЕЖ.....	ҒҲ_АБ
.....	_АБ
ВГ.....	ЯЎҚҒҲ

2.1.- расм. Вижинер матричаси.

Вижинер жадвали ёрдамида шифрлаш алгоритми қуйидаги қадамлар кетма-кетлигидан иборат.

1-қадам. Узунлиги M символли калит K ни танлаш.

2-қадам. Танланган калит K учун $[(M+1), P]$ ўлчамли шифрлаш матричаси $\Pi_x=(b_{иж})$ ни қуриш.

3- қадам. Дастлабки матннинг ҳар бир символи $c_{ор}$ тагига калит символи k_m жойлаштирилади. Калит кераклича такрорланади.

4-қадам. Дастлабки матн символлари шифрлаш матричаси Π_x дан қуйидаги қоида бўйича танланган символлар билан кетма-кет алмаштирилади.

5) K калитнинг алмаштирилувчи $c_{ор}$ символга мос k_m символи аниқланади;

6) шифрлаш матричаси Π_x даги $k_m = b_{ж1}$ шарт бажарилувчи и қатор топилади.

7) $c_{ор} = b_{и1}$ шарт бажарилувчи ж устун аниқланади....

8) $c_{ор}$ символи $b_{иж}$ символи билан алмаштирилади.

5-қадам. Шифрланган кетма-кетлик маълум узунликдаги (масалан 4 символли) блоklarга ажратилади. Охирги блокнинг бўш жойлари махсус символ-тўлдирувчилар билан тўлдирилади.

Расшифровка қилиш қуйидаги кетма-кетликда амалга оширилади.

1-қадам. Шифрлаш алгоритмининг 3-қадамидагидек шифрматн тагига калит символлари кетма-кетлиги ёзилади.

2-қадам. Шифрматндан $c_{1р}$ символлари ва мос калит символлари k_m кетма-кет танланади. Π_x матрисада $k_m = b_{иж}$ шартни қаноатлантирувчи и қатор аниқланади. и-қаторда $b_{иж} = c_{1р}$ элемент аниқланади. Расшифровка қилинган матнда p - ўрнига $b_{иж}$ символи жойлаштирилади.

3-кадам. Расшифровка қилинган матн ажратилмасдан ёзилади. Хизматчи символлар олиб ташланади.

Агар калит сифатида <ВАЗА> сўзи танланган бўлса, шифрлаш матрисаси бешта қатордан иборат бўлади. (2.2. - расм)

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	С	Ш	Ъ	Е	Ю	Я	Ў	Қ	Ғ	Х	_
В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	С	Ш	Ъ	Е	Ю	Я	Ў	Қ	Ғ	Х	_	А	Б
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	С	Ш	Ъ	Е	Ю	Я	Ў	Қ	Ғ	Х	_
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	С	Ш	Ъ	Е	Ю	Я	Ў	Қ	Ғ	Х	_	А	Б	В	Г	Д	Е	Ё	Ж
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	С	Ш	Ъ	Е	Ю	Я	Ў	Қ	Ғ	Х	_

2.2. - расм. «Ваза» калити учун шифрлаш матрисаси.

Мисол. К = <ВАЗА> калити ёрдамида Т = <БАЙРАМ КУНИ> дастлабки матни шифрлансин.

Шифрматн Т₁ қуйидагича бўлади: ГАСРВМЖКХНП

Сезарнинг шифрлаш тизими. Алмаштириш усуллари сифатида қуйидаги усулларни келтириш мумкин: Сезар усули, Аффин тизимидаги Сезар усули, таянч сўзли Сезар усули ва бошқалар.

Сезар шифри оддий силжитиш шифрининг бир қисми ҳисобланади. Бу шифрни римлик олим Голе Юлий Сезар ўйлаб топган. Шифрлашда матннинг ҳар бир ҳарфи бошқа ҳарф билан қуйидаги қоида асосида алмаштирилади. Ҳарфларни алмаштиришда келаётган ёзув ҳарфларини К-га силжитиб алмаштирилади. Бу ерда К – бутун сон ҳисобланиб уни қуйидагича ифодалаш мумкин. $K = K_{\text{мод}}(m)$, m - алфавит сони. Сезар усулида алмаштирувчи ҳарфлар к ва силжиш билан аниқланади. Юлий Сезар бевосита $k = 3$ бўлганда ушбу усулдан фойланган.

$k = 3$ бўлганда ва алифбодаги ҳарфлар $m = 26$ та бўлганда қуйидаги жалвал ҳосил қилинади:

Силжимаган алфавит	Силжиган алфавит	Силжимаган алфавит	Силжиган алфавит	Силжимаган алфавит	Силжиган алфавит
А	Д	Ж	М	С	В
В	Е	К	Н	Т	W
С	Ф	Л	О	У	Х
Д	Г	М	П	В	Й
Е	Х	Н	Қ	W	З
Ф	И	О	Р	Х	А
Г	Ж	П	С	Й	Б
Х	К	Қ	Т	З	С
И	Л	Р	У		

Масалан, матн сифатида КОМПЬУТЕР сўзини оладиган бўлсак, Сезар усули натижасида қуйидаги шифрланган ёзув ҳосил бўлади:

Т₁ = НРПСХWХУ.

Сезар усулининг камчилиги бу бир хил ҳарфларнинг ўз навбатида, бир хил ҳарфларга алмашишидир.

Аффин тизимидаги Сезар усулида ҳар бир ҳарфга алмаштирилувчи ҳарфлар махсус формула бўйича аниқланади: $at+b \pmod m$, бу ерда а, б - бутун сонлар, $0 \leq a, b < m$.

м=26, а=3, б=5 бўлганда
куйидаги жадвал ҳосил қилинади:

T	3T+5
0	5
1	8
2	11
3	14
4	17
5	20
6	23
7	26
8	29
9	32
10	35
11	38
12	41
13	44
14	47
15	50
16	53
17	56
18	59
19	62
20	65
21	68
22	71
23	74
24	77
25	80
26	83

Шунга мос равишда ҳарфлар
куйидагича алмашади:

А	Ф
Б	Ъ
В	Ь
Г	Э
Д	Ю
Е	Я
Ж	З
З	Қ
И	Ғ
Й	Ҳ
К	П
Л	Т
М	Х
Н	Б
О	Ф
П	Ж
Р	Н
С	Р
Т	В
У	З
Ф	Д
Х	Қ
Ц	Л
Ч	П
Ш	Т
Ў	Х

Натижада юқорида келтирилган матн куйидагича шифрланади:

$T_1 = \text{ПФХЖДЗСР}$

Калит сўзли Сезар тизими. Сезарнинг калит сўзли шифрлаш тизими битта алфавитли алмаштириш тизими ҳисобланади. Бу усулда калит сўзи орқали ҳарфларнинг суришда ва тартибини ўзгартиришда фойдаланади. Калит сўзини танлашда такрорланмайдиган ҳар хил ҳарфлардан иборат бўлган сўзни танлаш мақсадга мувофиқдир. Бу усул амалётда қўлланилмайди. Чунки калит сўзли Сезар шифрини кириптоатаҳлил асосида очиш мумкин.

Ишни бажарилиш тартиби ва қўйилган вазифа:
Асосий матн шифрлаш усулларида бирида шифрлансин ва кадамма – кадам изоҳлансин. Шунингдек ВБА ёки C++ дастурлаш тизимида дастурий таъминот яратилсин.

Ҳисобот мазмуни:

1. Иш мавзуси.
2. Ишдан мақсад.
3. Шифрлаш алгоритмини блок-схемаси.
4. Дастур матни.

4. Назорат саволлари

1. Ўрин алмаштириш методлари аппарат амалга оширилиши.
2. Шифрлашнинг аналитик методларининг моҳияти.
3. Шифрлашнинг гаммалаш (аддитив) методларининг моҳияти.
4. Шифрлашнинг комбинацияланган методларининг моҳияти.

Фойдаланилган адабиётлар

1. Желников В. Криптография от папируса до компьютера. М.: АБФ, 1997. – 336с.
2. Нилс Фергюсон, Брюс Шнаер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблис Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001й.
5. Масленников А. Практическая криптография БХВ – СПб 2003й.
6. Шнаер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002й.
8. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информасия химояси: Олий ўқув юрт. талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.

Қўшимча адабиётлар

9. <ftp://ftp.kiae.ru/msdos/crypt/pgp>
10. [хтtp://драго.сентерлине.сом:8080/франл/pgp/...](http://драго.сентерлине.сом:8080/франл/pgp/...)
11. Яхоо - Сомпутерс, Сесуритй-анд-Енсрйптион

3-4 АМАЛИЁТ МАШҒУЛОТЛАРИ

№3-Лаборатория иши

Мавзу: Гамилтон маршрутларига асосланган шифрлаш

Режа:

1. Қисқача назарий маълумот

2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади:

Компютердаги маълумотлар ҳимояси ва уларни қайта тиклаш.

Таянч иборалар: маршрутлар, символнинг тартиб рақами, шифр ва шифрлаш, ўрин алмаштириш, блок, криптотурғунлик, ахборот, блок. Калит, дешифрлаш.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компьютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намоёниш, амалий ишлаш.

Дарснинг технологик харитаси: -80+80 минут.

Ташкилий қисм: *хонанинг тозаллиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати -2+2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзунини қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш - 20+20 минут.*

Янги мавзу баёни: *-30+30 минут.*

Мавзунини ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш - *20+20 минут.*

Синов саволлари – *5+5 минут.*

Уйга вазифалар бериш – *3+3 минут.*

Мавзу баёни

Қисқача назарий маълумот:

Гамилтон маршрутларига асосланган усулда ҳам ўрин алмаштиришлардан фойдаланилади. Ушбу усул қуйидаги қадамларни бажариш орқали амалга оширилади.

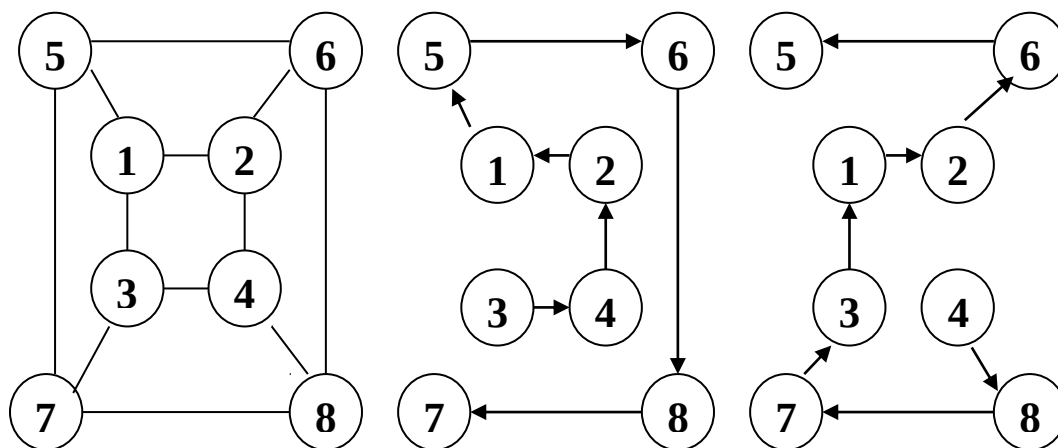
1-қадам. Дастлабки ахборот блоklarга ажратилади. Агар шифрланувчи ахборот узунлиги блок узунлигига қаррали бўлмаса, охириги блокдаги бўш ўринларга махсус хизматчи символлар-тўлдирувчилар жойлаштирилади (масалан, *).

2-қадам. Блок символлари ёрдамида жадвал тўлдирилади ва бу жадвалда символнинг тартиб рақами учун маълум жой ажратилади. (1 - расм)

3-қадам. Жадвалдаги символларни ўқиш маршрутларнинг бири бўйича амалга оширилади. Маршрутлар сонининг ошиши шифр криптотурғунлигини оширади. Маршрутлар кетма-кет танланади ёки уларнинг навбатланиши калит ёрдамида берилади.

4-қадам. Символларнинг шифрланган кетма-кетлиги белгиланган Л узунликдаги блоklarга ажратилади. Л катталиқ 1-қадамда дастлабки ахборот бўлинадиган блоklar узунлигидан фарқланиши мумкин.

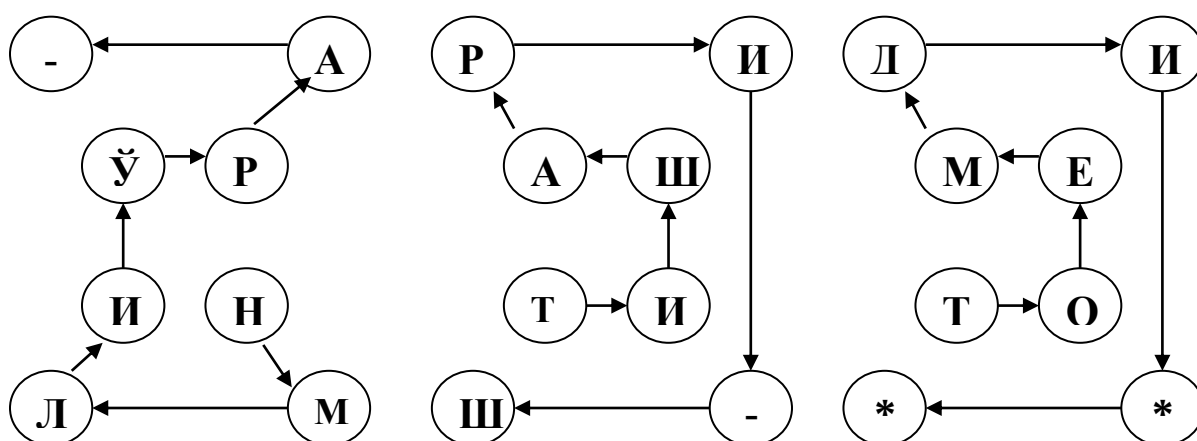
Дешифрлаш қилиш тескари тартибда амалга оширилади. Калитга мос ҳолда маршрут танланади ва бу маршрутга биноан жадвал тўлдирилади.



1-расм. 8-элементли жадвал ва Гамилтон маршрутлари вариантлари.

Жадвалдан символлар элемент номерлари келиши тартибида ўқилади.

Мисол. Дастлабки матн T_0 «Ўрин алмаштириш усули»ни шифрлаш талаб этилсин. Калит ва шифрланган блоklar узунлиги мос ҳолда қуйидагиларга тенг: $K=\langle 2,1,1 \rangle$, $L=4$. Шифрлаш учун 2.5-расмда келтирилган жадвал ва иккита маршрутдан фойдаланилади. Берилган шартлар учун матрисалари тўлдирилган маршрутлар 2.6-расмда келтирилган кўринишга ега.



2 - расм. Гамилтон маршрути ёрдамида шифрлаш мисоли.

1-қадам. Дастлабки матн учта блокка ажратилади. $B_1=\langle \text{Ўрин_алм} \rangle$, $B_2=\langle \text{аштириш-} \rangle$, $B_3=\langle \text{усули}^{**} \rangle$;

2-қадам. 2,1,1 маршрутли учта матриса тўлдирилади;

3-қадам. Маршрутларга биноан символларни жой-жойига қўйиш орқали шифрматнни ҳосил қилиш.

$T_1=\langle \text{НМЛИЎРА_ТИШАРИ_ШТОЕМДИ}^{**} \rangle$

4-қадам. Шифрматнни блоklarга ажратиш.

$T_1=\langle \text{НМЛИ ЎРА_ТИША РИ_Ш ТОЕМ ДИ}^{**} \rangle$

3.Қўйилган вазифа:

Назарий келтирилган маълумот учун дастур ишлаб чиқилсин. Дастур ВБА, С++ ёки С# дастурлаш тизимидан фойдаланган ҳолатда яратилсин.

Ҳисобот мазмуни:

1. Иш мавзуси.

2. Ишдан мақсад.
3. Шифрлаш алгоритмини блок-схемаси.
4. Дастур матни.

4. Назорат саволлари

1. Шифрлашнинг полиалфавитли алмаштириш усулининг моҳияти.
2. Вижинер матрисаси (жадвали) қаерда қўлланилади?
3. Гамильтон маршрутларига асосланган ўрин алмаштириш усулининг моҳияти.
4. Ўрин алмаштириш усуллари аппарат амалга оширилиши.

Фойдаланилган адабиётлар

1. Желников В. Криптография от папируса до компьютера. М.: АБФ, 1997. – 336с.
2. Нилс Фергюсон, Брюс Шнаер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблис Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001й.
5. Масленников А. Практическая криптография БХВ – СПб 2003й.
6. Шнаер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002й.

№4-Лаборатория иши

Мавзу: Очик калитли шифрлаш тизимлари

РСА, Эл-Гамал, Мак-Элис тизимлари

Режа:

1. Қисқача назарий маълумот

2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади: Ассимметрик криптотизимлар дастурини ишлаб чиқиш.

Таянч иборалар: Очик калит, қайтарилмас ёки бир томонли функциялар, маршрутлар, символнинг тартиб рақами, шифр ва шифрлаш, ўрин алмаштириш, блок, криптотурғунлик, ахборот, блок, калит, дешифрлаш, РСА, Эл-Гамал, Мак-Элис.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компьютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намоёниш, амалий ишлаш.

Дарснинг технологик харитаси: -80 минут.

Ташкилий қисм: хонанинг тозаллиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.

Талабалар билимини баҳолаш: ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.

Янги мавзу баёни: -30 минут.

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-20 минут.

Синов саволлари – 5 минут.

Уйга вазифалар бериш – 3 минут.

Мавзу баёни

Қисқача назарий маълумот: Очик калитли шифрлаш тизимларида иккита калит ишлатилади. Ахборот очик калит ёрдамида шифрланса, махфий калит ёрдамида дешифрлаш қилинади.

Очик калитли тизимларини қўллаш асосида қайтарилмас ёки бир томонли функциялардан фойдаланиш ётади. Бундай функциялар қуйидаги хусусиятларга эга. Маълумки x маълум бўлса $y=f(x)$ функцияни аниқлаш осон. Аммо унинг маълум қиймати бўйича x ни аниқлаш амалий жихатдан мумкин эмас. Криптографияда яширин деб аталувчи йўлга эга бўлган бир томонли функциялар ишлатилади. z параметрли бундай функциялар қуйидаги хусусиятларга эга. Маълум z учун E_z ва D_z алгоритмларини аниқлаш мумкин. E_z алгоритми ёрдамида аниқлик соҳасидаги барча x учун $f_z(x)$ функцияни осонгина олиш мумкин. Худди шу тариқа D_z алгоритми ёрдамида жоиз қийматлар соҳасидаги барча y учун тескари функция $x=f_z^{-1}(y)$

$^1(y)$ ҳам осонгина аниқланади. Айни вақтда жоиз қийматлар соҳасидаги барча z ва деярли барча, y учун хатто E_3 маълум бўлганида ҳам $\phi^{-1}(y)$ ни ҳисоблашлар ёрдамида топиб бўлмайди. Очiq калит сифатида y ишлатилса, махфий калит сифатида x ишлатилади.

Очiq калитни ишлатиб шифрлаш амалга оширилганда ўзаро мулоқатда бўлган субъектлар ўртасида махфий калитни алмашиш зарурияти йўқолади. Бу еса ўз навбатида узатилувчи ахборотнинг криптоҳимоясини соддалаштиради.

Очiq калитли криптотизимлари бир томонли функциялар кўриниши бўйича фарқлаш мумкин. Буларнинг ичида RSA, Эл-Гамал ва Мак-Элис тизимларини алоҳида тилга олиш ўринли. Ҳозирда енг самарали ва кенг тарқалган очiq калитли шифрлаш алгоритми сифатида RSA алгоритмини кўрсатиш мумкин. RSA номи алгоритмни яратувчилари фамилияларининг биринчи харфидан олинган (Ривест, Шамир ва Адлеман).

Алгоритм модул арифметикасининг даражага кўтариш амалидан фойдаланишга асосланган. Алгоритмни қуйидаги қадамлар кетма-кетлиги кўринишида ифодалаш мумкин.

1-қадам. Иккита 200дан катта бўлган туб сон p ва q танланади.

2-қадам. Калитнинг очiq ташкил етувчиси n ҳосил қилинади
$$n = p \cdot q.$$

3-қадам. Қуйидаги формула бўйича Ейлер функцияси ҳисобланади:
$$\phi(p, q) = (p-1)(q-1).$$

Ейлер функцияси n билан ўзаро туб, 1 дан n гача бўлган бутун мусбат сонлар сонини кўрсатади. Ўзаро туб сонлар деганда 1 дан бошқа бирорта умумий бўлувчисига ега бўлмаган сонлар тушунилади.

4-қадам. $\phi(p, q)$ киймати билан ўзаро туб бўлган катта туб сон d танлаб олинади.

5-қадам. Қуйидаги шартни қаноатлантирувчи e сони аниқланади
$$e \cdot d = 1 \pmod{\phi(p, q)}.$$

Бу шартга биноан $e \cdot d$ кўпайтманинг $\phi(p, q)$ функцияга бўлишдан қолган қолдиқ 1га тенг. e сони очiq калитнинг иккинчи ташкил етувчиси сифатида қабул қилинади. Махфий калит сифатида d ва n сонлари ишлатилади.

6-қадам. Дастлабки ахборот унинг физик табиатидан қатъий назар рақамли иккили кўринишда ифодаланади. Битлар кетма-кетлиги L бит узунликдаги блокларга ажратилади, бу ерда $L - L \geq \log_2(n+1)$ шартини қаноатлантирувчи енг кичик бутун сон. Ҳар бир блок $[0, n-1]$ ораликқа тааллуқли бутун мусбат сон каби кўрилади. Шундай қилиб, дастлабки ахборот $X(i)$, $i = \overline{1, L}$ сонларнинг кетма-кетлиги орқали ифодаланади. И нинг қиймати шифрланувчи кетма-кетликнинг узунлиги орқали аниқланади.

7-қадам. Шифрланган ахборот қуйидаги формула бўйича аниқланувчи $Y(i)$ сонларнинг кетма-кетлиги кўринишида олинади:

$$Y(i) = (X(i))^e \pmod{n}.$$

Ахборотни дешифрлаш қилишда қуйидаги муносабатдан фойдаланилади:

$$X(i) = (Y(i))^d \pmod{n}.$$

Мисол. <ГАЗ> сўзини шифрлаш ва дешифрлаш қилиш талаб этилсин. Дастлабки сўзни шифрлаш учун қуйидаги қадамларни бажариш лозим.

1-қадам. $p=3$ ва $q=11$ танлаб олинади.

2-қадам. $n = 3 \cdot 11 = 33$ ҳисобланади.

3-қадам. Ейлер функцияси аниқланади.

$$f(p, q) = (3-1) \cdot (11-1) = 20$$

4-қадам. Ўзаро тўб сон сифатида $d=3$ сони танлаб олинади.

5-қадам. $(e \cdot 3) \cdot (\text{mod } 20) = 1$ шартини қаноатлантирувчи e сони танланади.

Айтайлик, $e=7$.

6-қадам. Дастлабки сўзнинг алфавитдаги харфлар тартиб рақами кетма-кетлигига мос сон эквиваленти аниқланади. А харфига –1, Г харфига –4, З харфига –9. Ўзбек алфавитида 36та харф ишлатилиши сабабли иккили кодда ифодалаш учун 6 та иккили хона керак бўлади. Дастлабки ахборот иккили кодда қуйидаги кўринишга ега бўлади:

000100 000001 001001.

Блок узунлиги L бутун сонлар ичидан $L \geq \log_2(33+1)$ шартини қаноатлантирувчи минимал сон сифатида аниқланади. $n=33$ бўлганлиги сабабли $L=6$.

Демак, дастлабки матн $X(i) \leq \langle 4,1,9 \rangle$ кетма-кетлик кўринишида ифодаланади.

7-қадам. $X(i)$ кетма-кетлиги очиқ калит $\{7,33\}$ ёрдамида шифрланади:

$$Y(1)=(4^7)(\text{mod } 33)=16384(\text{mod } 33)=16$$

$$Y(2)=(1^7)(\text{mod } 33)=1(\text{mod } 33)=1$$

$$Y(3)=(9^7)(\text{mod } 33)=4782969(\text{mod } 33)=15$$

Шифрланган сўз $Y(i)=\langle 16,1,15 \rangle$

Шифрланган сўзни дешифрлаш қилиш махфий калит $\{3,33\}$ ёрдамида бажарилади.:

$$Y(1)=(16^3)(\text{mod } 33)=4096(\text{mod } 33)=4$$

$$Y(2)=(1^3)(\text{mod } 33)=1(\text{mod } 33)=1$$

$$Y(3)=(15^3)(\text{mod } 33)=3375(\text{mod } 33)=9$$

Дастлабки сон кетма-кетлиги дешифрлаш қилинган $X(i)=\langle 4,1,9 \rangle$ кўринишида дастлабки матн <ГАЗ> билан алмаштирилади.

Эл-Гамал тизими чекли майдонларда дискрет логарифмларнинг ҳисобланиш мураккаблигига асосланган. RSA ва Эл-Гамал тизимларининг асосий камчилиги сифатида модул арифметикасидаги мураккаб амалларнинг бажарилиши заруриятини кўрсатиш мумкин. Бу ўз навбатида айтарлича ҳисоблаш ресурсларини талаб қилади.

Мак-Элис криптолизимида хатоликларни тузатувчи кодлар ишлатилади. Бу тизим RSA тизимига нисбатан тезроқ амалга оширилсада, жиддий камчиликка ега. Мак-Элис криптолизимида катта узунликдаги калит ишлатилади ва олинган шифрматн узунлиги дастлабки матн узунлигидан икки марта катта бўлади.

Барча очиқ калитли шифрлаш методлари учун НП-тўлиқ масалани (тўлиқ саралаш масаласи) ечишга асосланган криптотахлил методидан бошқа методларининг йўқлиги қатъий исботланмаган. Агар бундай

масалаларни ечувчи самарали методлар пайдо бўлса, бундай хилдаги криптоанизим обрўсизлантирилади.

Юқорида кўрилган шифрлаш методларининг криптотурғунлиги калит узунлигига боғлиқ бўлиб, бу узунлик замонавий тизимлар учун, лоақал, 90 битдан катта бўлиши шарт.

Айрим муҳим кулланишларда нафақат калит, балки шифрлаш алгоритми ҳам махфий бўлади. Шифрларнинг криптотурғунлигини ошириш учун бир неча калит (одатда учта) ишлатилиши мумкин. Биринчи калит ёрдамида шифрланган ахборот иккинчи калит ёрдамида шифрланади ва ҳ.

Шифрлашнинг ўзгарувчан алгоритмларини қўллаш тавсия қилинади. Бунда шифрлаш калити шифрлашнинг муайян алгоритмини танлаш учун ҳам ишлатилади.

Очиқ калитлардан фойдаланувчи шифрлаш методларининг афзаллиги, аввало, махфий калитларни тарқатиш заруриятининг йўқлигидир. Катта масофаларда тарқалган компьютер тизимлари учун махфий калитларни тарқатиш айтарлича мураккаб масала ҳисобланади. Очиқ калитли тизимларнинг оммалашувига махфий калитларнинг фақат уларни тўлиқ саралаш орқали олинишидан бошқа йўл билан олиб бўлмаслиги исботининг йўқлиги тўсқинлик қилади.

Стеганография ахборотни криптоҳимоялашнинг истиқболли йўналишларидан ҳисобланади. Стеганография билан шифрлашни биргаликда (комплекс) ишлатилиши махфий ахборот криптотурғунлигини айтарлича оширади.

3. Ишни бажарилиш тартиби ва қўйилган вазифа:

Асосий матн шифрлаш усулларида бирида шифрлансин ва кадамма – кадам изохлансин. Шунингдек ВБА ёки С++ дастурлаш тизимида дастурий таъминот яратилсин.

Ҳисобот мазмуни:

1. Иш мавзуси.
2. Ишдан мақсад.
3. Шифрлаш алгоритмини блок-схемаси.
4. Дастур матни.

Назорат саволлари

1. Очиқ калитли шифрлаш тизимлари.
2. RSA криптоанизимининг моҳияти.
3. Ел-Гамал ва МакЕлис криптоанизимининг моҳияти.
4. **Шифрлаш стандартлари.**

Фойдаланилган адабиётлар

1. Желников В. Криптография от папируса до компьютера. М.: АБФ, 1997. – 336с.
2. Зубанов Ф. WINDOWS NT-выбор “профи”. – М.: Издателский отдел “Русская Редакция” ТОО “Чанел Традинг Лтд.”, 1996.
3. Баричев С. Криптография без секретов. М.: "ДИАЛОГ-МИФИ", - 1995.

№5-Лаборатория иши

Мавзу: Компютер тизимларининг вируслар билан заҳарланиш профликаси

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади: Компютер тизимларида вируслар ва уларнинг химояси.

Таянч иборалар: тармоқ, вирус, махсус дастур, анитвируслар, детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар, Аидтест, Достор Веб, НОД, КАВ.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси: -80 минут.

Ташкилий қисм: хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.

Талабалар билимини баҳолаш: ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.

Янги мавзу баёни: -30 минут.

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-20 минут.

Синов саволлари – 5 минут.

Уйга вазифалар бериш - 3 минут.

Мавзу баёни

Компютер вируси – бу махсус ёзилган дастур бўлиб, бошқа дастурлар таркибига ёзилади, яъни зарарлайди ва компютерларда ўзининг ғаразли мақсадларини амалга оширади.

Компютер вируси орқали зарарланиш оқибатида компютерларда қуйидаги узгаришлар пайдо бўлади:

- айрим дастурлар ишламайди ёки хато ишлай бошлайди;
- бажарилувчи файлнинг хажми ва унинг яратилган вақти узгаради;
- экранда англаб бўлмайдиган белгилар, турли хил тасвир ва товушлар пайдо бўлади;
- компютернинг ишлаши секинлашади ва тезкор хотирадаги буш жой хажми камаяди;
- диск ёки дискдаги бир неча файллар зарарланади (баъзи холларда диск ва файлларни тиклаб бўлмайди);
- винчестер орқали компютернинг ишга тушиши йўқолади.

Ҳозирги вақтда вирусларни йўқотиш учун кўпгина усуллар ишлаб чиқилган ва бу усуллар билан ишлайдиган дастурларни антивируслар деб аташади. Антивирусларни, кўлланиш усулига кўра, қуйидагиларга ажратишимиз мумкин: *детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар.*

Детекторлар — вируснинг сигнатураси (вирусга тааллуқли байтлар кетма-кетлиги) бўйича тезкор хотира ва файлларни кўриш натижасида маълум вирусларни топади ва хабар беради. Янги вирусларни аниқлаб олмаслиги детекторларнинг камчилиги ҳисобланади.

Фаглар — ёки докторлар, детекторларга хос бўлган ишни бажарган ҳолда зарарланган файлдан вирусларни чиқариб ташлайди ва файлни олдинги ҳолатига қайтаради.

Вакциналар — юқоридагилардан фарқли равишда ҳимояланаётган дастурга урнатилади. Натижада дастур зарарланган деб ҳисобланиб, вирус томонидан ўзгартирилмайди. Фақатгина маълум вирусларга нисбатан вакцина қилиниши унинг камчилиги ҳисобланади. Шу боис ҳам, ушбу антивирус дастурлари кенг тарқалмаган.

Прививка — файлларда худди вирус зарарлагандек из қолдиради. Бунинг натижасида вируслар «прививка қилинган» файлга ёпишмайди.

Филтрлар — куриқловчи дастурлар курилишида бўлиб, резидент ҳолатда ишлаб туради ва вирусларга хос жараёнлар бажарилганда, бу ҳақда фойдаланувчига хабар беради.

Ревизорлар — энг ишончли ҳимояловчи восита бўлиб, дискнинг биринчи ҳолатини хотирасида сақлаб, ундаги кейинги ўзгаришларни доимий равишда назорат қилиб боради.

Детектор дастурлар компьютер хотирасидан, файллардан вирусларни кидиради ва аниқланган вируслар ҳақида хабар беради.

Доктор дастурлари нафақат вирус билан касалланган файлларни топади, балки уларни даволаб, дастлабки ҳолатига қайтаради. Бундай дастурларга Аидтест, Достор Веб дастурларини мисол қилиб келтириш мумкин. Янги вирусларнинг тўхтовсиз пайдо бўлиб туришини ҳисобга олиб, доктор дастурларини ҳам янги версиялари билан алмаштириб туриш лозим.

Филтр дастурлар компьютер ишлаш жараёнида вирусларга хос бўлган шубҳали ҳаракатларни топиш учун ишлатилади.

Бу ҳаракатлар қуйидагича бўлиши мумкин:

- файллар атрибутларининг ўзгариши;
- дискларга доимий манзилларда маълумотларни ёзиш;
- дискнинг ишга юкловчи секторларига маълумотларни ёзиб юбориш.

Текширувчи (ревизор) дастурлари вирусдан ҳимояланишнинг энг ишончли воситаси бўлиб, компьютер зарарланмаган ҳолатидаги дастурлар, каталоглар ва дискнинг тизим майдони ҳолатини хотирада сақлаб, доимий равишда ёки фойдаланувчи ихтиёри билан компьютернинг жорий ва бошлангач ҳолатларини бир-бири билан солиштиради. Бунга АДИНФ дастурини мисол қилиб келтириш мумкин.

Компютер тизимларида хавф-хатарсиз ишлашнинг амалда синаб кўрилган ва юқори самара берган асосий қоидалари қуйидагилар.

Биринчи қоида. Қонуний расмий йўл билан олинган программ маҳсулотлардан фойдаланиш.

Иккинчи қоида. Ахборотни иккилаш. Аввало программ таъминотнинг дистрибутив елтувчиларини сақлаш лозим. Ишчи ахборотнинг сақланишига катта еътибор бериш лозим.

Учинчи қоида. Вирусга қарши воситалардан мунтазам равишда фойдаланиш лозим. Ишни бошламасдан аввал программа-сканерлар ва программа-тафтишлар ишлатилиши керак. Вирусларга қарши воситаларнинг мунтазам равишда янгиланиб турилиши шарт.

Тўртинчи қоида. Айниқса ахборотнинг янги елтувчиларидан ва янги файллардан фойдаланишда еҳтиёт бўлиш лозим. Янги дискеталар уларда юклама файлли вирусларнинг йўқлиги нуқтаи назаридан сўзсиз текширилиши шарт.

Бешинчи қоида. Таксимланган тизимлар ёки жамоа фойдаланувчи тизимлар билан ишлаганда янги алмаштириладиган ахборот елтувчилар ва тизимга киритилувчи файллар махсус ҳисоблаш машинасида текширилиши лозим.

Вирусга қарши ҳар томонлама текшириш амалга оширилганидан кейингина дисклар ва файллар тизимдан фойдаланувчиларга узатилиши мумкин.

Олтинчи қоида. Елтувчига ахборот ёзиш кўзда тутилмаган бўлса, бу амални бажарилишига йўл қўйиш керак емас. Бунинг учун 3,5 дюмли дискетларда квадрат тешик очиш кифоя.

Юқорида келтирилган тавсияларга риоя қилиш программ вируслар билан захарланиш еҳтимолини айтарлича камайтиради ва фойдаланувчини ахборотни йўқотишдан сақлайди.

Компютер вирусларига қарши курашнинг қуйидаги турлари мавжуд:

- вируслар компьютерга кириб бузган файлларни ўз ҳолига қайтарувчи дастурларнинг мавжудлиги;
- компьютерга парол билан кириш, диск юритувчиларнинг ёпик туриши;
- дискларни ёзишдан ҳимоялаш;
- лисензион дастурий таъминотлардан фойдаланиш ва ўғирланган дастурларни қўлламаслик;
- компьютерга кириталаётган дастурларнинг вирусларнинг мавжудлигини текшириш;
- антивирус дастурларидан кенг фойдаланиш;
- даврий равишда компьютерларни антивирус дастурлари ёрдамида вирусларга қарши текшириш.

Антивирус дастурларидан DrWeb, Адинф, АВП, ВоотСХК ва Нортон Антивирус, Касперский Сесуритй кабилар кенг фойдаланилади.

НАЗОРАТ САВОЛЛАРИ

1. Компютер вируслари қандай аломатлари бўйича классификацияланади?
2. «Стелс»-вируслар ва полиморф вирусларнинг таъсири принципини тушунтиринг.
3. Файл вируси ва унинг таъсири алгоритмини тушунтиринг.
4. Макровирус ва юклама вируслар таъсири алгоритми қандай?
5. Вирусларни аниқлаш методлари.
6. Вируслар таъсири оқибатларини йўқотиш методлари.
7. Компютер системаларининг вируслар билан захарланишининг олдини оловчи профилактик чоралар кетма-кетлигини санаб ўтинг.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
2. Столинс, Вилем. Основы защиты сетей. Приложения и стандарты: Пер. С англ.- М.: Издательский дом «Вильямс», 2002. 432 с.
3. Ғаниев С.К.,Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация химояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.

№6 - Лаборатория иши

Мавзу: Тармоқни бошқариш қисм тизимида ахборотни ҳимоялаш

Режа:

1. Қисқача назарий маълумот

2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади:

Тармоқни бошқариш қисм тизимида ахборотни ҳимоялашнинг асосий усуллари ўрганиш ва тадқиқ етиш.

Таянч иборалар: тармоқ, халқаро стандарт-ТСП/ИП ва Х.25 протоколлар, протоколларнинг сатҳ моделлари.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компьютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси: -80 минут.

Ташкилий қисм: хонанинг тозаллиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.

Талабалар билимини баҳолаш: ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.

Янги мавзу баёни: -30 минут.

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-20 минут.

Синов саволлари – 5 минут.

Уйга вазифалар бериш - 3 минут.

Мавзу баёни

1.Ишдан мақсад: Компютердаги маълумотлар ҳимояси ва уларни қайта тиклаш.

2.Қисқача назарий маълумот:

Ахборотларни узатиш бошқариш протоколлари деб аталувчи маълум қоидалар бўйича амалга оширилади. Ҳозирда компютер тармоқларида тармоқнинг узоклаштирилган элементлари ўртасидаги алоқа иккита халқаро стандарт-ТСП/ИП ва Х.25 протоколлари ёрдамида амалга оширилади.

ТСП/ИП протоколи асосида Интернет тармоғи қурилган. Х.25 протокоliga пакетларни коммутасиялаш асосида қурилган маълумотларни узатиш технологиясининг ривож сифатида қараш мумкин. Х.25 протоколи очиқ тизимларнинг ўзаро алоқаси модели ОСИ га мувофиқ халқаро стандартлаш ташкилоти ИСО томонидан яратилган. Х.25 моделида тармоқнинг барча вазифалари 7 сатҳга ажратилса, ТСП/ИП моделида 5 сатҳ мавжуд.

Х.25 протоколи узоклаштирилган жараёнлар ўртасида юқори ишончли алоқани таъминлай олади. ТСП/ИП протоколининг афзаллиги сифатида

тармоққа уланишнинг соддалигини ва нархининг пастлигини кўрсатиш мумкин.

ОСИ модели	ТСП/ИП модели
Татбиқий	Татбиқий
Тақдимий	
Сеанс	Транспорт
Транспорт	
Тармоқ	Тармоқ
Каналли	Каналли
Физикавий	Физикавий

1 - расм. Протоколларнинг сатҳ моделлари.

Тармоқда ахборотни ҳимоялашни таъминлаш масаласи барча сатҳларда амалга оширилади. Протоколларнинг бажарилиши бошқариш қисм тизими томонидан ташкил етилади.

3.Қўйилган вазифа:

1. Ахборот хавфсизлиги масалалари ҳам ечиладиган тармоқни бошқарувчи ягона бошқариш марказини яратиш.
2. Тармоқнинг барча объектларини рўйхатга олиш ва уларнинг ҳимоясини таъминлаш. Идентификаторларни тақдим етиш ва барча тармоқдан фойдаланувчиларни ҳисобга олиш.
3. Тармоқ ресурсларидан фойдаланишни бошқариш.
4. Калитларни шакллантириш ва уларни компютер тармоқ абонентларига тарқатиш.
5. Трафикни (тармоқдаги ахборотлар оқимини) мониторинглаш, абонентларнинг ишлаш қоидаларига риоя қилишларини назоратлаш, бузилишларга тездан ўз муносабатини билдириш.
6. Тармоқ элементларининг ишлаши бузилганида уларнинг ишлаш қобилиятини тиклашни ташкил етиш.

Ҳисобот мазмуни:

1. Иш мавзуси.
2. Ишдан мақсад.
3. Назарий қисм.

4. Назорат саволлари

1. Тармоқ қандай қисм тизимларига ажратилади.?
2. Коммуникасион қисм тизимининг таркиби.

3. Тармоқда информасияни ҳимоялаш тизимини яратишда нималарни ҳисобга олиш зарур?
4. Фойдаланувчи қисм тизимида информасия ҳимоясини таъминлаш қандай амалга оширилади?
5. Ихтисослаштирилган коммуникацион компьютер тизимларида информасия ҳимояси қандай таъминланади.
6. Тармоқни бошқариш қисм тизимида информасияни ҳимоялаш.
7. Тармоқлараро экранлашнинг моҳиятини тушунтиринг.
8. Ўзаро алоқада бўлган жараёнларнинг ҳақиқийлигига қандай ишонч ҳосил қилинади?
9. Коммуникацион қисм тармоқ орқали олинувчи информасиянинг сохта емаслигининг тасдиғига қандай еришилади?

Фойдаланилган адабиётлар

1. Гук М. Аппаратные средства ИБМ ПС. Енсиклопедия. - СПб.: Питер, 2002, - 928 с.
2. Мииаси М. Модернизасия и обслуживание персонального компьютера. Базовый курс. - М.; Век, 2000. - 592 с.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
4. Столинс, Виям. Основы защиты сетей. Приложения и стандарты: Пер. С англ.-М.: Издателский дом «Виямс», 2002. 432 с.
5. Ғаниев С.К.,Каримов М.М. Ҳисоблаш системалари ва тармоқларида информасия ҳимояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77

8-9 амалий машғулот
№7 Лаборатория иши
Мавзу: Компютер вирусларининг таснифланиши

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади:

Компютер вируслари ва улардан ҳимояланиш тизимларини таҳлил етиш ва ўрганиш.

Таянч иборалар: вирус, тармоқли, файлли, юкланадиган ва файлли-юкланадиган, чувалчанг, резидентли ва резидентли бўлмаган.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси:-80+80 минут.

Ташкилий қисм: *хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2+2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзунини қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20+20 минут.*

Янги мавзу баёни: *-30+30 минут.*

Мавзунини ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-*20+20 минут.*

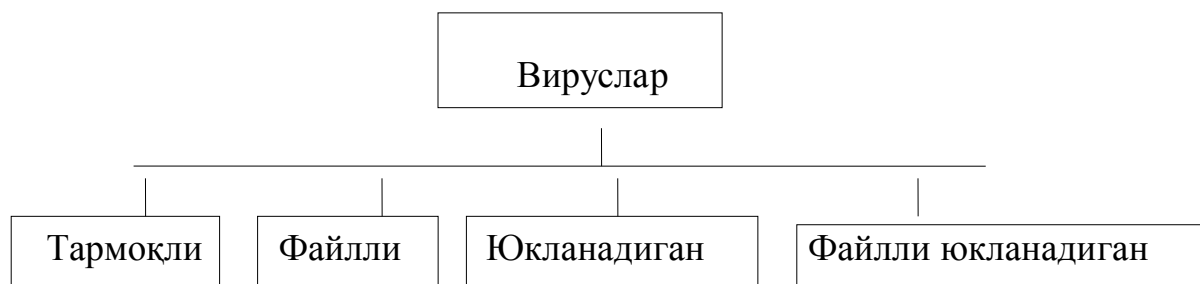
Синов саволлари – *5+5 минут.*

Уйга вазифалар бериш – *3+3 минут.*

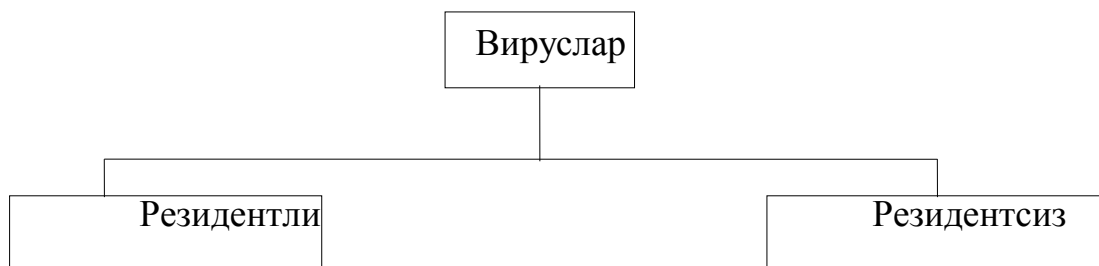
Мавзу баёни

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

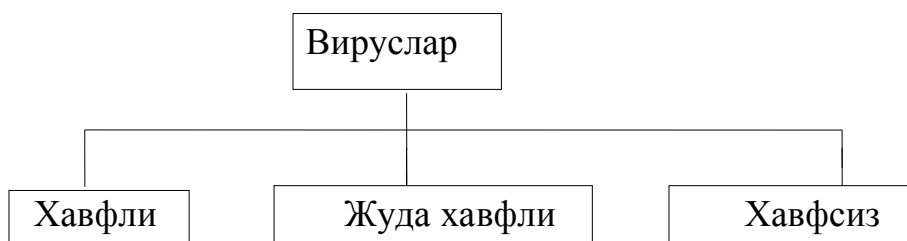
- а) яшаш муҳити бўйича;
- б) зарарлантириш усули бўйича;
- в) таъсир етиши бўйича;
- г) алгоритмнинг хусусиятлари бўйича;
- А) Яшаш муҳити бўйича вирусларнинг таснифлаши



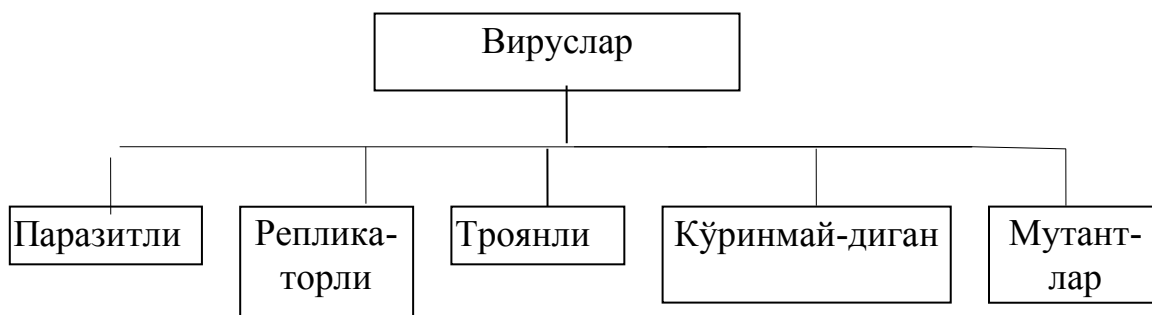
Б) Зарарлантириш усули бўйича вирусларнинг таснифланиши



В) Таъсир етиш даражаси бўйича вирусларнинг таснифланиши



Г) Алгоритмларнинг хусусиятлари бўйича вирусларнинг таснифланиши



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

Тармоқли вируслар турли компьютер тармоқлари бўйича тарқаладилар. Дискетадан емас, балки локал ёки глобал тармоқдан тарқатиладиган бу вируслар бажарадиган дастурларни зарарлантирмайдилар. Улар ҳимоя қилишнинг тармоқ воситалари орқали кириб олиш учун мослашганлар ва тармоқда юқори тарқалиш тезлигига егадир.

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

Компютер “чувалчанглари” тизимнинг жиддий бузилишларига олиб келмайди. Вирус “чувалчанг” сифатида Worm дастурини келтириш мумкин, у ўзининг нусхаларини тарқатиш учун ўзининг дастурли кодини Интернет

тармоғи бўйича электрон хабарларга иловалар кўринишида жўнатади. Бу вирус бажариладиган HARRY99.EXE файлида жойлашади.

Файлли вируслар асосан бажариладиган модулларга, яъни .COM ва .EXE кенгайтмаларга ега бўлган файлларга, татбиқ қилинади. Файлли вируслар бошқа турдаги файлларга ҳам татбиқ қилиниши мумкин, лекин бунда улар бошқаришни узатадилар, ва, демак, кўпайиш қобилятини йўқотадилар. Файлли вируслар компютердан компютерга файлларда кўчиб ўтадилар ва юқори зарарлантириш хоссасига ега.

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

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

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

Зарарлантириш усули бўйича вируслар резидентли ва резидентли бўлмаган бўлади.

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

Резидентли бўлмаган вируслар компютер хотирасини зарарлантирмайдилар ва чегараланган вақт ичида фаол ҳисобланади.

Таъсир етиш даражаси бўйича вирусларни қуйидаги кўринишларга бўлиш мумкин

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

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

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

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

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

Чувалчанглар деб аталадиган вирус репликаторларни таъкидлаш керакки, улар компютер тармоқлари бўйича тарқаладилар, тармоқ

компютерларининг манзилларини ҳисоблайдилар ва бу манзиллар бўйича ўзларининг нусхаларини ёзадилар.

Стелс-вируслар деб аталадиган кўринмайдиган вируслар мавжуд бўлиб, уларни пайқаш ва зарарлантириш жуда мушкулдир, чунки улар операцион тизимни зарарланган файлларга ва дискларнинг секторларига мурожаат қилишни ушлаб оладилар ва ўзининг танасини ўрнига дискнинг зарарланмаган қисмларини қўяди.

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

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

Компютер вирусларидан ҳимоя қилиш усуллари

Компютер вирусларидан ҳимоя қилишнинг учта чегараси мавжуддир:

- вирусларни кириб келишини бартараф етиш;
- агар вирус барибир компютерга кирган бўлса, вирус ҳужумини бартараф етиш;
- агар ҳужум барибир амалга ошган бўлса, бузувчи оқибатларни бартараф етиш.
- ҳимоя қилишни амалга оширишни учта усули мавжуддир:
- ҳимоя қилишнинг дастурли усуллари;
- ҳимоя қилишнинг аппаратли усуллари;
- ҳимоя қилишнинг ташкилий усуллари.

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

Маълумотлар билан ишончли ва хавфсиз ишлашга фақат шундагина еришиладики, агар исталган кутилмаган ҳодиса, шу жумладан компютерни

тўлиқ физик ишдан чиқариш ҳам, халоқатли оқибатларга олиб келмаслиги керак.

Вирусга қарши ҳимоя қилиш воситалари

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

Маълумотларни захиралашда яна шуни инобатга олиш керакки, барча рўйхатдан ўтган ва паролли маълумотларни, Интернетнинг тармоқли хизматларига мурожаат қилиш учун, алоҳида сақлаш керак. Уларни компютерда сақламаслик керак. Одатдаги сақлаш жойи - бўлим раҳбарининг сейфидаги хизмат кундалигидир. Ахборотни захирали нусхалаш бўйича тадбирлар режасини тузиб олиб захирали нусхалар компютерда алоҳида сақланиш кераклигини инобатга олиш керак. Яъни масалан, ўша компютернинг алоҳида қаттиқ дискида ахборотни захиралаш фақатгина хавфсизлик иллюзиясини яратади.

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

Ахборотни ҳимоя қилишнинг ёрдамчи воситалари вирусга қарши дастурлар ва аппаратли ҳимоя қилиш воситалари ҳисобланади. Масалан, бош платада уланиш жойини оддийгина ўчириб қўйиш ДЕҚҚ сини қайта дастурланadиган (флеш - БИОС) микросхемасини ўчиришни амалга ошириш имконини бермайди, бунда бу ишни ким амалга оширишига: компютер вирусими, ёмон ниятли кишими ёки тартибсиз фойдаланувчими бунга боғлиқ емасдир.

Вирусга қарши ҳимоя қилишнинг етарлича кўп дастур воситалари мавжуддир.

Вирусдан ҳимоя қилиш учун ишлатиш мумкин:

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

О вирус билан зарарланиш еҳтимолини камайтириш имконини берадиган профилактик чоралар;

О вируслардан ҳимоя қилиш учун махсус дастурлар.

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

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

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

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

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

Вируслардан компютерларни ва маълумотларни хавфсизлигига ҳисса қўшиш бўйича биринчи ўринда, шубҳасиз, маълумотларни нусхалаш, ҳисобланади. Вирус билан компютер зарарланганда ҳали ҳам ҳеч бўлмаганда маълумотларнинг бир қисмини тиклаш мумкин, лекин агар компютерда каттиқ диск бузилса, унда нима қилмоқ керак? Бундан ташқари, нусхалари архивда мавжуд бўлган дастурлар ва маълумотлар исталганча бузилганда, қўшимча уларни турли “докторлар” билан даволашни амалга оширишга интилмасдан, архивдан тўғри нусхаларни нусхалаш мақсадга мувофиқдир.

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

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

Филтрлар дастури тўртинчи ўринда туради. Бу дастурлар кўплаб вирусларни (ҳаммасини бўлмаса ҳам), улар ҳали кўп нарсаларни бузишга ёки зарарлантиришга улгурмасдан олдин, енг бошланғич босқичда пайқаш имконини беради. Антивирус ва Флу Шот Плус туридаги дастурлар филтрлар дастурига тегишлидир.

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

Докторлар дастури- (фаглар) олтинчи ўринда (умуман биринчида эмас) жойлашган. Уларни, бузилган дастурни нусхаси архивда бўлмаганда, ва уни бошқа усул билан олиш қийин бўлган ҳоллардагина қўллаган маъқулроқ. Бундан ташқари, агар дастур-фаг ишлатилаётган бўлса, унда кейин тикланган файлни дастур-тафтишчи билан албатта текшириш керак бўлади

(тушунарлики, агар бу файл тўғрисидаги ахборот олдиндан сақланган бўлса), лекин ҳар доим ҳам дастур-доктор тўғри даволайвермайди.

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

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

Вирус билан зарарланишга қарши профилактика

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

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

2. Вирусдан ҳимоя қилиш учун резидентли филтрлар дастурини доимо, мумкин бўлган ҳамма вақтда ишлатиш мақсадга мувофиқдир.

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

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

5. ДОС бошланғич юкланганда бажариладиган AUTOEXEC.BAT буйрукли файлига, параметр сифатида файлларнинг унча катта бўлмаган рўйхатини кўрсатган ҳолда, файлларда ўзгаришларни текшириш учун тафтишчи-дастурни чақиришни қўйиш мақсадга мувофиқдир.

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

жойлашишидан халос бўлиши учун, вирус борлигини аввалроқ диагностика қилиш учун дастурни бажариш мақсадга мувофиқдир.

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

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

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

10. Компютерда ишлашга бегона шахсларни, айниқса агар улар ўзларининг дискеталарига ега бўлмасалар, қаровсиз қолдирмасдан рухсат бермаслик керак. Жуда кўп ҳолларда компютерни вирус билан зарарланиш сабаби дискетада олиб келинган, кимдир уни компютерда 10-15 минут ўйнаган компютер ўйини ҳисобланади. Агар компютерга тасодикий шахсларни мурожаат қилишдан халос бўлишнинг имкони бўлмаса (масалан, ўқув марказида), компютернинг қаттиқ дискида жойлашган барча ёки деярли барча дастурларни ёзишдан ҳимоя қилинган дискда жойлаштирилган мақсадга мувофиқдир.

11. Агар компютер қаттиқ дискка ега бўлса, ҳар доим ишончли жойда “тизимли” дискетага, яъни ДОС операцион тизимини юклаш мумкин бўлган дискетага ега бўлиш керак.

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

- ўзига яхши тавсиянома берган;
- вирусларнинг кенг диапозонига ёки бошқа дастурлар билан “ушлаб олинмайдиган” вирусларга мўлжалланган;
- ўзларида вируслар йўқлигига текширилган дастурларни йиғиш керак

Вирусларни пайқаш ва улардан ҳимоя қилиш дастурлари ва уларнинг тавсифлари

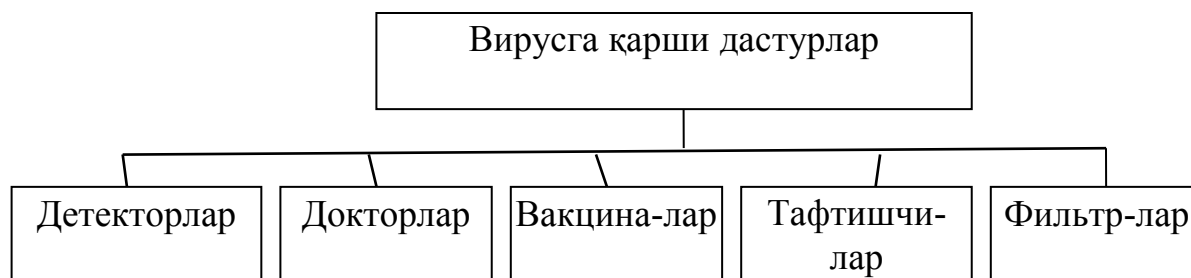
Компютер вирусларини пайқаш, ўчириш ва улардан ҳимоя қилиш учун махсус дастурларнинг бир нечта турлари ишлаб чиқилган, улар вирусларни пайқаш ва йўқотиш имконини беради. Бундай дастурлар вирусга қарши дастурлар деб аталади.

Вирусга қарши дастурларнинг қуйидаги турлари мавжуд:

- 1) детекторлар дастури;
- 2) докторлар дастури ёки фаглар;
- 3) тафтишчилар дастури;

- 4) филтрлар дастури;
- 5) вакциналар дастури ёки иммунизаторлар.

Вирусга қарши дастурларнинг турлари



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

Докторлар дастури ёки фаглар, ҳамда вакциналар дастури нафақатгина вируслар билан зарарланган файлларни топмасдан, балки уларни “даволайди” ҳам, яъни файдан вирус-дастур танасини ўчирадилар, файлларни бошланғич ҳолатга қайтарадилар. Фаглар ўзининг ишини бошида тезкор хотирада вирусларни киди-ради, уларни йўқотади ва фақат кейингина файлларни “даволашга” ўтади. Фаглар орасида ярим фагларни ажратиш мумкин, улар катта миқдордаги вирусларни кидириш ва йўқотиш учун мўлжалланган докторлар дастуридир. Аидтест, Ссан, Нортон Антивирус ва Достор Web энг машҳур полифаглар ҳисобланадилар. Янги вируслар доимо пайдо бўлиб боришини инобатга олиб, детекторлар дастури ва докторлар дастури тезда ескирадилар, ва уларнинг версияларини доимо янгилаб бориш талаб этилади.

Тафтишчилар дастури вируслардан ҳимоя қилишнинг энг ишончли усуллариغا тегишлидир. Тафтишчилар, компьютер вирус билан зарарланмаганда, каталогларнинг дастурларини ва дискнинг тизимли соҳаларини бошланғич қийматини еслаб қоладилар, кейин еса даврий равишда ёки фойдаланувчининг хохиши бўйича жорий ҳолатни бошланғич ҳолат билан таққослайди. Пайқалган ўзгаришлар видеомонитор экранига чиқарилади. Қоидага кўра, ҳолатларни тақ-қослаш опкрасион тизим юклангандан кейин бирданига амалга оширилади. Таққослашда файл узунлиги, сиклик назорат қилиш коди (файлнинг назорат йиғиндиси), ўзгартириш санаси ва вақти, бошқа параметрлар текширилади. Тафтишчилар дастури етарлича ривожланган алгоритмларга ега, стелс-вирусларни пайқайдилар, ва хаттоки текширилаётган дастурдаги версияларини ўзгаришларини вирус томонидан киритилган ўзгаришлардан фарқини пайқайдилар.

Россияда кенг тарқалган “Диалог-Наука” фирмасининг Адинф дастури тафтишчилар дастури қаторига киради.

Филтрлар дастури ёки “қоровуллар”- компьютер ишлашида вируслар учун тегишли бўлган шубҳали ҳаракатларни пайқаш учун мўлжалланган, унча катта бўлмаган резидентли дастурлардир. Бундай ҳаракатлар бўлиши мумкин:

- 1) .COM ва .EXE кенгайтмали файлларни тўғрилашга интилишлар;
- 2) файллар атрибутларини ўзгартириш;
- 3) абсолют манзил бўйича дискка тўғридан-тўғри ёзиш;
- 4) дискнинг юкланадиган секторларига ёзиш;
- 5) резидент дастурни юклаш.

Бирор дастур томонидан кўрсатилган амалларни бажаришга интилиш бўлганда “қоровул” фойдаланувчига хабар юборилади ва мос амалларни таъқиқлашни ёки рухсат беришни таклиф этади. Филтрлар дастури жуда фойдалидир, чунки улар вирусни уни пайдо бўлишини бошланғич босқичларида, кўпайгунга қадар пайқаш қобилиятига егадир. Аммо улар файлларни ва дискларни “даво-ламайдилар”. Вирусларни йўқотиш учун бошқа дастурларни, масалан фағларни, қўллаш талаб етилади. Дастур-қоровулларнинг камчиликларига уларнинг жонга тегишини “(масалан, улар бажарилаётган файлни нусхалашга ихтиёрий интилиш тўғрисида доимо огоҳлантириб турадилар), ҳамда бошқа дастур таъминоти билан мумкин бўлган келишмовчиликларни келтириш мумкин. Дастур-филтрга мисол тариқасида MS DOS операцион тизимининг утилитларини тўпламини таркибига кирувчи Vsafe дастурини келтириш мумкин. [25; 112-119]

Вакциналар ёки иммунизаторлар - файлларни зарарланишини бартараф етувчи резидентли дастур ҳисобланади. Вакциналарни вирусни “даволайдиган” дастур докторлар йўқ бўлганда қўлланилади. Ваксиналаш фақатгина маълум бўлган вируслардан мумкиндир. Ваксина дастурни ёки дискни шундай ўзгартирадики, бу уларнинг ишлашида акс еттирилмайди, вирус еса уларни зарарланган деб қабул қилади ва шунинг учун татбиқ етилмайди. Ҳозирги вақтда вакциналар дастури чекланилган қўлланишга ега.

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

Компютер вирусларидан ҳимоя қилиш учун асосий чоралар

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

- компьютерни замонавий вирусга қарши дастурлар, масалан Аидтест ёки Достор Web, билан таъминланг ва уларнинг версияларини доимо янгилаб бординг;

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

- ўзингизни компютерингизга архивланган кўринишдаги файлларни кўчириб ўтишда, текшириш соҳасини ҳозиргина ёзилган файллар билан

чеклаган ҳолда, уларни қайта архивлангандан кейин тезда қаттиқ дискда текширинг;

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

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

- Сиз учун муҳим бўлган ахборотларни архивли нусхаларини дискеталарда албатта ишлаб чиқинг;

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

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

- Аидтест ва Достор Web дастурларини қўллашни юқори хавфсизлигини таъминлаш учун Адинф диск текширувчисини ҳар куни ишлатиб бориш керак.

Ишни бажарилиш тартиби ва қўйилган вазифа:

Компютер вирусларидан ҳимоя қилиш учун асосий чоралар, Ваксиналар ёки иммунизаторлар, Филтрлар дастури ёки “қоровуллар”, Тафтишчилар дастури, Докторлар дастури, Детекторлар дастури, Вирус билан зарарланишга қарши профилактика мавзуларини ўрганиш ва улар ҳақида маълумотлар тўпланг.

Ҳисобот мазмуни:

1. Иш мавзуси.
2. Ишдан мақсад.
3. Асосий маълумотлар.
4. Умумий хулосалар.

Назорат саволлари

1. Компютер вируси нима ва унинг табиати қандай?
2. Вирусларни компютерга кириб боришини асосий йўллари қандай?
3. Компютер вирусларини зарарлари нималарда намоён бўлади?
4. Сизларга компютер вирусларини қандай асосий кўринишлари маълум?
5. Вирусларни пайқаш ва улардан ҳимоя қилиш учун дастурларнинг қандай турлари мавжуд?
6. Детекторлар дастури ва докторлар дастурининг фарқлари ва ўхшаш жойлари нимада?
7. Тафтишчилар дастурининг ва филтрлар дастурининг афзалликлари нималарда намоён бўлади?
8. Компютер вирусларидан ҳимоя қилиш бўйича асосий чораларни айтиб беринг.
9. Дастур маҳсулотларини ҳимоя қилиш нима учун керак?

10 амалий машғулот
№8 Лаборатория иши
Мавзу: Антивирус дастурлари ва уларнинг вазифалари

Режа:

- 1. Қисқача назарий маълумот**
- 2. Ишни бажарилиш тартиби ва қўйилган вазифа:**

Дарснинг мақсади:

Антивирус дастурлари, уларнинг вазифалари билан танишин ва уилардан фойдаланиш.

Таянч иборалар: Аидстест, Достор Веб полифаг дастури, мураккаб вируслар мутантлар, Евристик таҳлил, Адинф, Адинф Суре Модуле даволовчи блоки

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компьютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намоиш, амалий ишлаш.

Дарснинг технологик харитаси:-80 минут.

Ташкилий қисм: *хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзунини қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.*

Янги мавзу баёни: *-30 минут.*

Мавзунини ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-*20 минут.*

Синов саволлари – *5 минут.*

Уйга вазифалар бериш - *3 минут.*

Мавзу баёни

А. Аидстест дастури - полифаг

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

Аидстест ни ишга тушириш учун қуйидаги буйруқни бериш керак:

Аидстест <патҳ>[<оптионс>]

бу ерда: патҳ - диск номи, тўлиқ ном, файл спецификасияси, файллар гуруҳининг ноқоби:

*- каттиқ дискнинг барча бўлимлари

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

Опционс - қуйидаги калитларнинг исталган комбинацияси:
F- зарарланган дастурларни тўғрилаш ва бузилганларини ўчириш;
G- барча файлларни кетма-кет текшириш (фақатгина .COM, .EXE ва СЙС ларни емас);
H- бузилган вирусларни қидириш учун секин ишлаш;
X- вирус таркибида бузилишлар бўлган барча файлларни ўчириш;
Q- бузилган файлларни ўчиришга рухсат сўраш;
R- кейинги дискектани қайта ишлашни таклиф етмаслик.

Мисол 1. АИСТЕСТ В: /Ф/Г/Қ

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

Достор Web полифаг дастури

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

Др.Web дастури Аидтест кучи етмайдиган мураккаб вируслар мутантлар билан самарали курашиши мумкин. Аидтест дан фарқли равишда Др.Web дастури хусусий дастурли коддаги ўзгаришларни пайқаш, ҳамда “вакцинали беркитишни” енгиб ўтган ҳолда шифрланган ва ихчамлаштирилган файлларга кириб янги, нўмалум вируслар билан зарарланган файлларни самарали аниқ-лаш қобилиятига егадир. Бу кучли евристик таҳлилчи мавжудлиги ҳисобига еришилади.

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

Евристик таҳлилни учта даражаси кўзда тутилган. Евристик таҳлил режимида ёлғон ишлашлар, яъни зарарланмаган ҳисобланмаган файлларни детекторлаш мумкиндир. “Евристика” даражаси ёлғон ишлаш мавжуд бўлмаган кодни таҳлил қилиш даражаси кўринишига егадир. Евристик таҳлилчининг ишлашини биринчи иккита даражаси тавсия етилади.

Евристик таҳлилни учинчи даражаси файлларни яратилишини “шубхали” вақтига уларни қўшимча текширишни кўзда тутди. Файллар зарарланишида баъзи бир вируслар ушбу файлларнинг зарарганлик белгиси каби яратилишининг нотўғри вақтини ўрнатади. Масалан, зарарланган

файллар учун секундлар 62 қийматга ега бўлиши мумкин, яратилиш йили еса 100 йилга кўпайтирилиши мумкин.

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

Др.Веб дастури билан икки режимда ишлаш мумкин:

- меню ва мулоқот ойнасини ишлатиб тўлиқ экранли интерфейс режимида;

- буйруқ қатори орқали бошқариш режимида.

Доимий бўлмаган бир марталик қўллаш учун биринчи режим кулайроқдир, лекин дискеталарнинг доимий киришини назорат қилиш мақсадида доимий қўллаш учун яхшиси иккинчи режимини қўллаган маъқулдир.

Иккинчи режимни ишлатганда Др.Веб нинг мос ишга тушириш буйруғи Нортон Коммандер операцион қобиғини фойдаланувчисини менюсига ёки махсус буйруқли файлга киритилган бўлиши мумкин.

Др.Веб ни ишга тушириш учун буйруқ қатори қуйидаги кўринишга ега:

Др.Веб [диск:] [йўл] [калитлар]

бу ерда диск: - қаттиқ дискни мантикий қурилмаси ёки егилувчан дискни физик қурилмаси, масалан, Ф: ёки А:

*- қаттиқ дискдаги барча мантикий қурилмалар;

йўл - бу талаб етилаётган файлларнинг йўли ёки ниқоби.

Енг муҳим калитлар:

/ АЛ-берилган қурилмадаги барча файлларнинг диагностикаси;

/ СУ [П] - дискларни ва файлларни “даволаш”, топилган вирусларни ўчи-риш;

Р- фойдаланувчининг тасдиқлаши билан вирусларни ўчириш;

/ ДЛ-тўғрилаб даволашни имкони бўлмаган файлларни ўчириш;

/ НА [даража]- файлларни евристик таҳлил қилиш ва уларда номаълум вирусларни кидириш, бу ерда [даража] 0,1,2 қийматларни қабул қилиш мумкин;

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

/ ҚУ- тестлашдан кейин тезда ДОС га чиқиш.

Агар Др.Веб нинг буйруқли қаторида бирорта ҳам калит кўрсатилмаган бўлса, унда жорий сўров учун барча ахборот ДРВЕБ. ЕХЕ жойлашган каталогда жойлашган ДРВЕБ.ИНИ конфигурация файлидан ўқилади. Конфигурация файли тестлаш учун зарур бўлган параметрларни сақлаш буйруғи ёрдамида Др.Веб дастури билан ишлаш жараёнида ишлатилади. Мисол-2: ДрВеб Б: / АЛ/ СУП/ ХА1/ҚУ/СЛ

В: дискни текшириш ва даволаш учун Др.Веб вирусга қарши дастурини ишга тушириш.

Тўлиқ экранли интерфейс режимида Др. Веб дастури билан
ишлаш технологияси

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

Др.Веб ТЕСТ НАСТРОЙКИ ДОПОЛНЕНИЯ

Исталган режимни танлашда мос қисмменю очилади.

Др.Веб қисмининг менюси ДОС га вақтинчалик кириш, Др.Веб дастури ва унинг муаллифи тўғрисида қисқача ахборотни олиш ёки дастурдан чиқиб кетиш имконини беради.

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

Настройки қисмининг менюси мулоқот ойналари ёрдамида дастурни созлаш параметрларини ўрнатиш, қидиришни йўллари ва ниқобларини ўрнатиш ва параметрларни ДРВЕБ.ИНИ конфигурация файлида сақлаш учун хизмат қилади.

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

Дискнинг вирусга қарши тафтишчиси Адинф

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

Адинф дастури еслаб қолади:

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

Компютерни бутун ишлаши давомида Адинф дастури бу тавсифларни сақланганлигини кузатиб боради. Ҳар кунги назорат қилиш режимида Адинф дастури компьютер биринчи марта уланганда автоматик равишда ишга туширилади. Айниқса вирусга ўхшаш ўзгаришлар кузатиб борилади, улар тўғрисида тезда огоҳлантириш берилади. Файлларнинг бутунлиги назорат қилишдан ташқари Адинф дастури қисм каталогларни яратишни ва ўчиришни, файлларни яратишни, силжитишни ва қайта номлашни, янги бузуқ кластерларни пайдо бўлишини, юкланадиган секторларини сақлаганлигини ва кўплаб бошқа нарсаларни кузатади. Вирусни тизимга татбиқ қилиш учун мумкин бўлган барча жойлар ёпиб қўйилади. Адинф

дастури, ДОС ни ишлатмасдан БИОС га тўғридан-тўғри мурожаат қилиб дискни секторлари бўйича ўқиган ҳолда текширади.

Адинф Ссйпе Модуле даволовчи блоки

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

Дастур маҳсулотларини ҳимоя қилиш

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

Биринчидан, улар юқори малакали мутахассисларнинг, баъзида ўнлаб хаттоки юзлаб кишиларнинг интеллектуал меҳнати маҳсулоти ҳисобланади.

Иккинчидан, бу маҳсулотларни лойиҳалаш жараёни моддий ва меҳнат ресурсларини сезиларли ҳаракатлари билан боғлангандир, қимматбаҳо компьютер жиҳозларини ва илмий-техникавий технологияларни ишлатишга асосланган.

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

Дастур маҳсулотларини ҳимоя қилиш қуйидаги мақсадларни кўзда тутаяди:

- фойдаланувчиларнинг алоҳида тоифаларини дастур маҳсулотлари билан ишлаш учун тақиқланган мурожаат қилишни чеклаш;
- маълумотларни қайта ишлашни меъёрида олиб бориш мақсадида дастурларни олдиндан режалаштирилган бузилишини инкор қилиш;
- дастур маҳсулотини ишлаб чиқарувчиларни нуфузини бузиш мақсадида дастурларни олдиндан режалаштирилган ўзгартирилишни инкор қилиш;
- дастурларни тақиқланган ададлашни (нусхалашни) инкор қилиш;
- дастурларни мазмунини, таркибини ва ишлаш механизмини тақиқланган ўрганишни инкор қилиш.

Дастур маҳсулотлари турлича объектларнинг кишини, техник воситаларни, махсус дастурларни, атроф муҳитни ва бошқаларни тақиқланган таъсирларидан ҳимоя қилиниши керак.

Кишилар дастур маҳсулотига шу дастур маҳсулотини ҳужжатларини ёки машина ташувчисининг ўзини ўғрилаш ёки физик йўқотиш, дастур воситаларини ишлаш қобилиятини бузиш йўли билан таъсир етиши мумкин.

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

Махсус дастурлар ёрдамида дастур маҳсулотини вирус билан зарарлантириш, уни тақиқланган нусхалаш, унинг маъносини рухсациз ўрганиш ва амалга ошириши мумкин.

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

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

- О дастурлар ишга тушганда уларни пароль билан ҳимоя қилиш;

- О калит дискетани ишлатиш;

- О компьютернинг киритиш - чиқариш портига уланадиган махсус техник қурилмани (электрон калитни) ишлатиш.

- О дастурларни тақиқланган нусхалашдан сақлаш мақсадида ҳимоя қилишнинг махсус дастурли воситалари:

- О дастур ишга тушириладиган муҳитни идентификациялаш;

- О рухсат етилган инсталляцияларни ва нусхалашларни бажарилишини миқдорини ҳисобини олиб бориш;

- О тизимларнинг ишлаш алгоритмларини ва дастурларини ўрганишга қарши туриш (хаттоки ўз-ўзини бузишгача) керак.

- О дастур маҳсулотлари учун самарали ҳимоя қилиш чоралари қуйидагилар ҳисобланадилар:

- О ишга туширадиган дискетани ностандарт шакллантириш;

- О қаттиқ дискда дастурларни жойлашган жойини қатъий белгилаш;

- О киритиш-чиқариш портига қўйиладиган электрон калитга боғланиш;

- О БИОС номерига боғланиш ва бошқалар.

- О Дастур маҳсулотларини ҳимоя қилиш ҳуқуқий усуллар билан ҳам албатта амалга оширилиши керак, уларнинг қаторига келишувлар ва шартномаларни, патентли ҳимоя қилишни, муаллифлик ҳуқуқини, технологик ва ишлаб чиқариш махфийлигини ва бошқаларни киритиш мумкин.

Компютер тизимларини ривожланиши билан янада янги компютер вируслари пайдо бўлмоқда, шунга мос равишда турли хил антивирусли тизимлар ва воситалар ҳам пайдо бўлмоқда. Одатда вируслар компютер тизимида сақлаётган дастур таъминотини маълумотларни ўзгартиради ёки йўқ қилади. Зарар келтирадиган дастурларга биологик вирусларнинг хоссалари киради.

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

Шак-шубҳасиз, махсус антивирусли воситаларни ишлаб чиқиш ва ишлатиш долзарбдир. Антивирусли воситалар вирусдан зарарланиш оқибатларини аниқлаш (сканерлаш, ўзгаришларни пайқаш усули, евриетик таҳлил етиш, аппарат - дастурли антивирусли воситалар ва ҳакозо) ва юк килиш масалаларини ечади, шу билан бир каторда файлларни ва хотира сохаларини, юкланиш секторларини тиклайди.

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

Компютер вирусларидан ҳимоя қилишнинг асосий чораларидан дастур маҳсулотларини расмий йўл билан ишлатишни келтириш мумкин. Алоҳида таъкидлаш керакки, антивирусли воситалар доимо янгилашиб бориши керак, бунда ташқаридан келадиган янги дастурларга ва файлларга алоҳида еътиборни қаратиш керак.

Таъкидлаб ўтамизки, дастур маҳсулотларини вируслардан ҳимоя қилишнинг аҳамияти жуда каттадир. Бундай ҳимоя, оддий вируслардан ташқари, албатта ҳуқуқий усуллар билан амалга оширилиши керакдир.

Асосий атамалар

Вирусга қарши дастур, юкланадиган вирус, компютер вируси, вирус-мутант, кўринмайдиган вирус (стелс-вирус), хавфсиз вирус, резидент бўлмаган вирус, хавфли вирус, жуда хавфли вирус, паразит (текинхур) вирус, резидент вирус, вирус-репликатор (чувалчанг), тармоқли вирус, троян вируси, файл вируси, зарарланган дастур, зарарланган диск, дастур-ваксина, дастур-доктор (фаг), дастур-детектор, дастур-тафтишчи, дастур-филтр (қоровул), Аидстест ва Достор Веб полифаг дастурилари.

Ишни бажарилиш тартиби ва қўйилган вазифа:

Компютер вирусларга қарши курашадиган антивирус дастурлари, жумладан, Аидстест, Достор Веб, НОД 32, КАВ, Адинф, Адинф Суре Модуле ларни компютерга ўрнатиш, уларнинг параметрларини созлаш, ишлатиш, натижаларини таҳлил етиш.

Ҳисобот мазмуни:

1. Иш мавзуси.
2. Ишдан мақсад.
3. Дастурий воситани ўрнатиш алгоритми.
4. Дастур параметрларини созлаш.
5. Базаларини ўрнатиш.
6. Дастурни ишга тушириш ва унинг натижасини таҳлил қилиш.

Назорат саволлари

1. Компютер вируси нима ва унинг табиати қандай?

2. Вирусларни компьютерга кириб боришини асосий йўллари қандай?
3. Компьютер вирусларини зарарлари нималарда намоён бўлади?
4. Сизларга компьютер вирусларини қандай асосий кўринишлари маълум?
5. Вирусларни пайқаш ва улардан ҳимоя қилиш учун дастурларнинг қандай турлари мавжуд?
6. Детекторлар дастури ва докторлар дастурининг фарқлари ва ўхшаш жойлари нимада?
7. Тафтишчилар дастурининг ва филтрлар дастурининг афзалликлари нималарда намоён бўлади?
8. Компьютер вирусларидан ҳимоя қилиш бўйича асосий чораларни айтиб беринг.
9. “Диалог-Наука” ХЖ нинг вирусга қарши дастурлар тўпламини таркибини ва вазифасини айтиб беринг.
10. Вирусларни пайқаш ва йўқ қилиш учун Аидстест дастурини қандай қўллаш керак?
11. Др.Веб вирусга қарши дастурини Аидстест дастуридан фарқи нимада?
12. Др.Веб дастурини қандай режимларда ишлатиш мумкин?
13. Қаттиқ дискни вируслар мавжудлигига даврий равишда текшириш технологиясини айтиб беринг.
14. Дастур маҳсулотларини ҳимоя қилиш нима учун керак?

