O’ZBEKISTON RESPUBLIKASI
OLIY VA O’RTA MAXSUS TA’LIM VAZIRLIGI

NIZOMIY NOMIDAGI TOSHKENT DAVLAT PEDAGOGIKA UNIVERSITETI

«Axborot- kommunikatsiya texnologiyalari» kafedrasi

L.M.Nabiulina, Sh.A.Abdurahmanova

AXBOROT XAVFSIZLIGI

Metodik qo’llanma

TOSHKENT – 2015

L.M.Nabiulina, Sh.A.Abdurahmanova «Axborot xavfsizligi» fani bo'yicha metodik qo'llanma.Toshkent, Nizomiy nomidagi TDPU, 2015 y.

Annotatsiya

Ushbu metodik qo'llanma mualliflar tomonidan informatika va axborot texnologiyalari yo'nalishidagi fanlari tarkibidan o'rin olgan "Axborot xavfsizligi" fani bo'yicha yaratilgan. Mazkur qo'llanma o'quv-uslubiy va ma'lumotli hujjatlardan iborat bo'lib, nazariy mashg'ulotlarini o'tkazish bo'yicha metodik ko'rsatmalar keltirilgan. Metodik qo'llanma yangi pedagogik texnologiyalari asosida yozilgan. Metodik qo'llanma "Axborot xavfsizligi" fani bo'yicha darslarni yuqori saviyada o'tkazish uchun oliy ta'lim, akademik litsey va kasb-hunar kollej o'qituvchilari uchun mo'ljallangan.

Taqrizchilar: Migranova E.A. — Toshkent axborot texnologiyalar universiteti, "Ta'limda axborot texnologiyalari" kafedrasi dotsenti, texnika fanlari nomzodi, dotsent

Alibekov S.A. — Nizomiy nomidagi TDPU, "Axborot-kommunikatsiya texnologiyalari" kafedrasi katta o'qituvchisi, fizika-matematika fanlari nomzodi

Mundarija

MAVZU № 1 (2 soat)

AXBOROTNI HIMOYALASH VA AXBOROT XAVFSIZLIGI
MA'RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	____ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1. Axborotni muhofaza qilish, axborot xavfsizligi va uning zamonaviy konsepsiyasi 2. Axborot xavfsizligiga tahdid va uning turlari 3. Axborot xavfsizligi va ma'lumotlarni himoyalash bo'yicha me'yoriy-huquqiy hujjatlar.
Dars maqsadi: Talabalarda axborotlarni himoyalash va axborot xavfsizligi haqida tushunchalar hosil qilish	
Pedagog vazifalari:	***O'quv natijalari:***
- Axborotni muxofoza qilish, axborot xavfsizligi va uning zamonaviy kontseptsiyasi bilan tanishtiriish; - Axborot xavfsizligiga tahdid va uning turlarini tushuntirib berish; - Axborot xavfsizligi va ma'lumotlarni himoyalash bo'yicha me'yoriy-huquqiy hujjatlar bilan tanishtirish.	- Axborotni muhofaza qilish, axborot xavfsizligi va uning zamonaviy konsepsiyasi haqida tushunchalarni o'zlashtiradilar va yozib oladilar; - Axborot xavfsizligiga tahdid va uning turlarini o'rganadilar va yozib oladilar; - Axborot xavfsizligi va ma'lumotlarni himoyalash bo'yicha me'yoriy-huquqiy hujjatlar bilan tanishib chiqadilar va yozib oladilar.
O'qitish usullari	Klaster metodi, "Aqliy hujum" metodi
Ta'limni tashkil etish shakli:	Frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali jihozlar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

AXBOROTNI HIMOYALASH VA AXBOROT XAVFSIZLIGI
MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	**Faoliyatning mazmuni**	
	O'qituvchi	**Talaba**
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1.Talabalarga axborotni muxofoza qilish, axborot xavfsizligi va uning zamonaviy kontseptsiyasini klaster metodi asosida tushuntirib beriladi. (3-ilova) 2.2. Axborot xavfsizligiga tahdid va uning turlari haqida tushuntirib beradi. (4-ilova) 2.3 Axborot xavfsizligi va ma'lumotlarni	Yozib oladilar E'tibor beradilar va yozib oladilar Keltirilgan me'yoriy-huquqiy

	himoyalash bo’yicha me’yoriy-huquqiy hujjatlar bilan tanishtirib chiqiladi. (5-ilova)	hujjatlar bilan tanishib chiqadilar va yozib oladilar
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo’yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi va buni aniqlash maqsadida “Aqliy hujum” metodi qo’llaniladi. (6-ilova)	Savollar beradi. Savollarga javob berishadi.

1-ilova

Mavzu: AXBOROTNI HIMOYALASH VA AXBOROT XAVFSIZLIGI

Mavzu rejasi::	1. Axborotni muhofaza qilish, axborot xavfsizligi av uning zamonaviy konsepsiyasi 2. Axborot xavfsizligiga tahdid va uning turlari 3. Axborot xavfsizligi va ma’lumotlarni himoyalash bo’yicha me’yoriy-huquqiy hujjatlar.
Darsning maqsadi: Talabalarda axborotlarni himoyalash va axborot xavfsizligi haqida tushunchalar hosil qilish	

2-ilova

Адабиётлар:

1. Муҳаммадиев Ж.Ў. Ахборот хавфсизлиги: муаммо ва уечимлар:
Монография. – Т., 2011.
2. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: Учебное пособие. – Брянск, 2007.
3. Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги.
Ахборот-коммуникацион тизимлари хавфсизлиги. – Т.. 2008.

3-ilova

Axborot xavfsizligi - fuqarolar, tashkilotlar va davlat manfaati yo’lida jamiyat axborot muhitini shakllantirish, takomillashtirish hamda undan foydalanish jarayonlarida uning ichki va tashqi tahdidlardan himoyalanganligini ta’minlovchi holat.

Avvallari axborotga tajovuz qilish deganda, muhim va konfidentsial xarakterga ega bo’lgan hujjat va ma’lumotlarni o’g’irlash yoki ulardan nusxa ko’chirish tushunilsa, hozirga kelib, moddiy manfaat va o’z foydasini ko’zlagan holda kompьyuter ma’lumot bazalariga

noqonuniy kirib ishlar bajarish, elektron ma’lumotlar massivlariga egasining roziligisiz kirib, undan ma’lumotlar olish kabi harakatlar ko’payib bormoqda.

Axborot xavfsizligi to’g’risida gap yuritilar ekan, birinchi navbatda, xavfsizlikka bo’ladigan tahdidlarning manbalari, ularni amalga oshirish usullari, maqsadlari va shunga o’xshash xavfsizlikni buzishga undovchi boshqa shartlar aniqlanishi lozim. Tabiiyki, bu tahdidlar yetkazadigan zarardan himoya qilish choralarini ham ko’rib chiqish kerak.

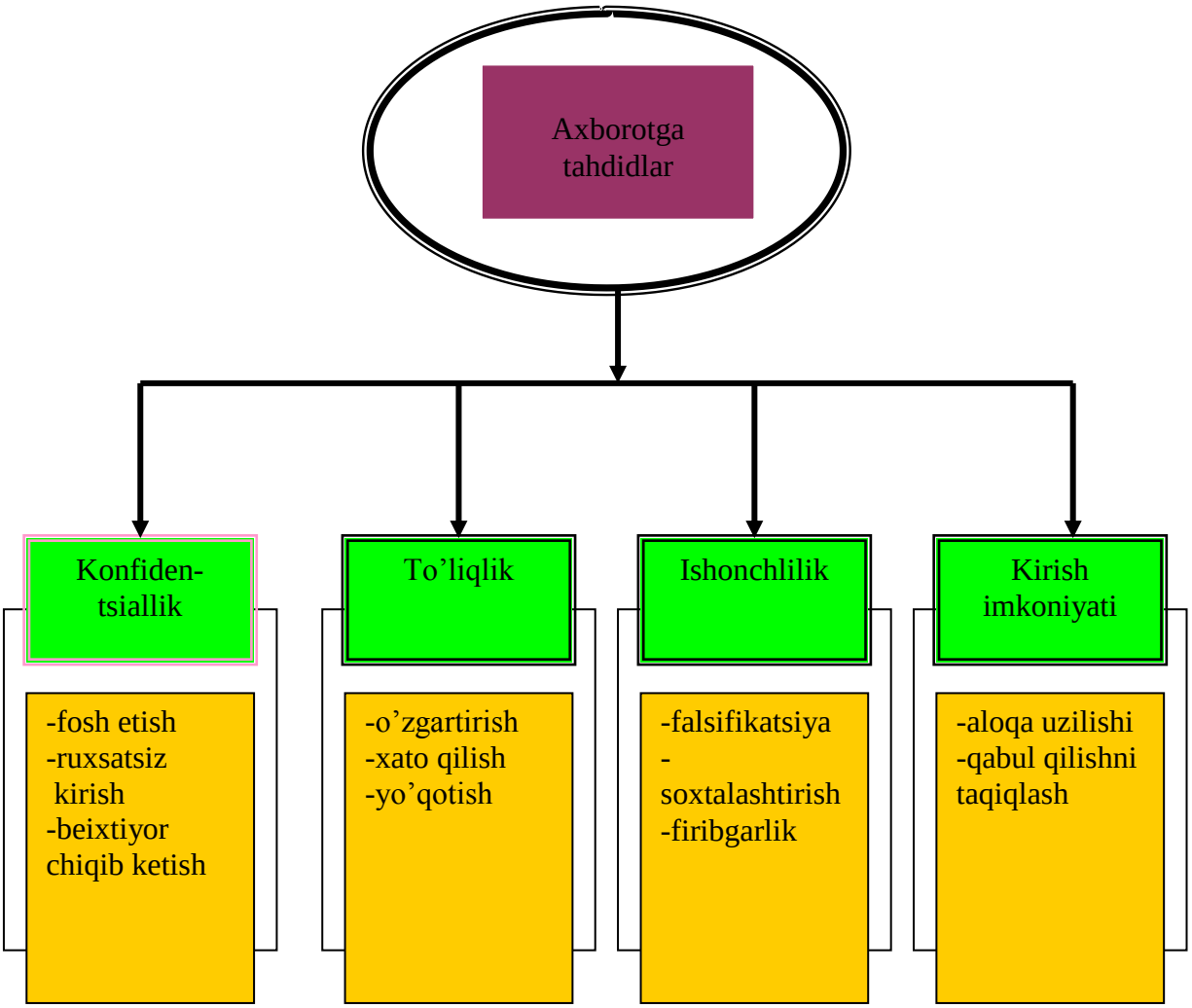
Axborot xavfsizligining kontseptual modeli keltirilgan.

Axborot xavfsizligiga tahdid ob’ektlariga himoya qilinishi lozim bo’lgan ob’ektning tarkibi, holati va faoliyati haqidagi ma’lumotlar kiradi.

Axborotga tahdid deganda, uning konfidentsialligi, butunligi, to’laligi va u bilan tanishish qoidasi buzilishi tushuniladi.

Axborot xavfsizligiga tahdid manbalariga raqiblar, jinoyatchilar, korruptsiyachilar hamda boshqa buzg’unchilar kiradi.

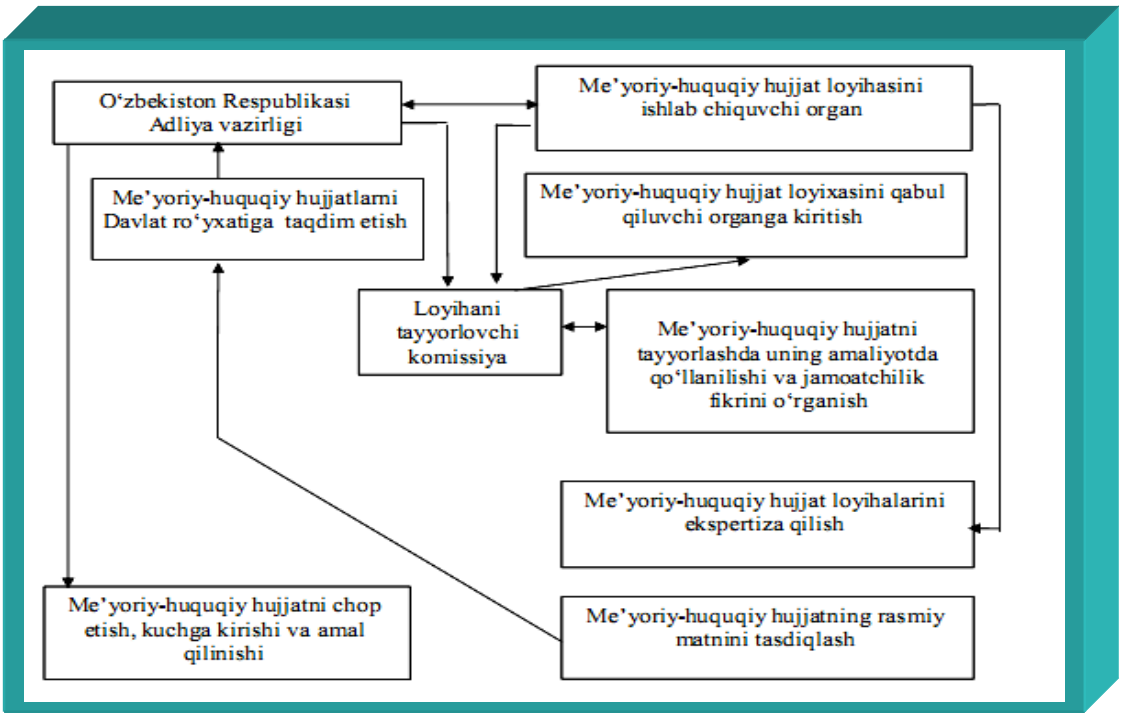
4-ilova



Axborot jarayonida qiziqishlari qarama-qarshi bo’lgan ob’ekt (firma, tashkilot) va sub’ekt (raqib, buzg’unchi) orasidagi munosabatlar-ni konfidentsial ma’lumotlarga ega bo’lishga qaratilgan faol harakatlar nuqtai nazaridan ko’rib chiqilganda quyidagi holatlar ro’y berishi mumkin:

- axborot egasi (manba) konfidentsial axborotni saqlashga hech qanday chora ko’rmaganligi sababli raqib o’zi qiziqqan ma’lumotni oson olishi mumkin;
- axborot manbai axborot xavfsizligi choralarini qattiq saqlaydi va raqib saqlanayotgan axborotga kirishi yoki uni olishi uchun unga sanktsiyasiz kirishning barcha usullarini qo’llaydi;
- axborot egasi (manba) bilmagan holda texnik kanallardan axborotni beixtiyor chiqib ketishi va undan raqib o’z maqsadida hech qanday qiyinchiliksiz foydalanishi mumkin.

5-ilova



Bu borada mustaqil diyorimiz O’zbekiston Respublikasida ahamiyatga molik bo’lgan ulkan ishlar olib borilmoqda. Bunga misol tariqasida O’zbekiston aloqa va axborotlashtirish agentligining ilmiy-texnik va marketing tadqiqotlari markazi tomonidan ishlab chiqilgan O’z DSt 1092:2005 "Axborot texnologiyasi. Ma’lumotlarni kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari", O’z DSt 1105:2006 "Axborot texnologiyasi. Ma’lumotlarni kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi", O’z DSt 1106:2006 "Axborot texnologiyasi. Ma’lumotlarni kriptografik muhofazasi. Xeshlash funktsiyasi" va O’z DSt 1108:2006 "Axborot texnologiyasi. Ochiq tizimlar o’zaro boliqligi. Elektron raqamli imzo ochiq kaliti sertifikati va atribut sertifikatining tuzilmasi" standartlarini va

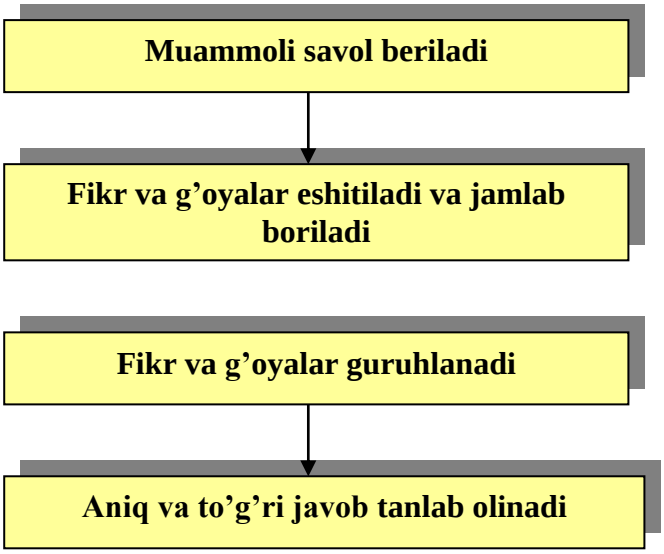
RH 45-187:2006 «Xavfsizlik talablari» boshqaruv xujjatini ko’rsatib o’tish mumkin. Ushbu markaz tomonidan ishlab chiqilgan standartlar № 05-11 12.04.2006 yilda O’zbekiston standartlashtirish, metrologiya va sertifikatsiyalash agentligi tomonidan tasdiqlangan.
Bundan tashqari yurtimizda axborot xavfsizligi sohasida faoliyat yuritayotgan O’zbekiston aloqa va axborotlashtirish agentligi qoshidagi “Ilmiy-texnik va marketing tadqiqotlari markazi”, «UzInfocom» va boshqa tashkilotlarni aytib o’tish maqsadga muvofiq. Chunki bu tashkilotlarning yurtimiz ravnaqi uchun ko’shayotgan xissasi katta ahamiyatga ega.

6-ilova

“Aqliy hujum” metodini qo’llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g’oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g’oyalar, ular hatto to’g’ri bo’lmasa ham inobatga olinadi.
3. Har bir ta’lim oluvchi qatnashishi shart.

Quyida (1-chizma) “Aqliy hujum” metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. Axborot xavsizligi tushunchasi nimani anglatadi?
2. Axborot xavsizligiga tahdid deganda siz nimani tushunasiz?
3. Axborot xavsizligiga tahdid turlarini gapirib bering?
4. Axborot xavfsizligi va ma’lumotlarni himoyalash bo’yicha qanday me’yoriy-huquqiy hujjatlarni bilasiz?

MAVZU № 2 (4 soat)

AVTOMATLASHTIRILGAN AXBOROT TIZIMLARIDA AXBOROTLARNI HIMOYALASH

MA’RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	____ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo’yicha ma’ruza
Mavzu rejasi:	1.Texnik vositalar bilan himoyalanadigan axborotlarning turlari; 2.Axborot chiqib ketish texnik kanallarining tasnifi va tarkibi.
Dars maqsadi: Talabalarda axborotlarni avtomatlashgan texnik vositalar bilan himoyalash tushunchasini hosil qilish	
Pedagog vazifalari:	***O’quv natijalari:***
- Texnik vositalar bilan himoyalanadigan axborotlarning turlari bilan tanishtiriish va ma’ruzani bayon qilish; - Axborot chiqib ketish texnik kanallarining tasnifi va tarkibini tushuntirib berish;	- Texnik vositalar bilan himoyalanadigan axborotlarning turlari haqida tushunchaga ega bo’ladilar va daftarga yozib oladilar; - Axborot chiqib ketish texnik kanallarining tasnifi va tarkibini ıцrganadilar .
O’qitish usullari	Ma’ruza, klaster metodi, aqliy hujum
Ta’limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko’rgazmali qurollar.
Ta’limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta’minlangan xona.
Nazorat	O’zini-o’zi nazorat qilish

AVTOMATLASHTIRILGAN AXBOROT TIZIMLARIDA AXBOROTLARNI HIMOYALASH

MAVZUSIDAGI MA’RUZA DARSIGA

TEXNOLOGIK XARITA

Faoliyat bosqichlari	**Faoliyatning mazmuni**	
	O’qituvchi	**Talaba**
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo’yicha kerakli adabiyotlarni e’lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1.Talabalarga texnik vositalar bilan himoyalanadigan axborotlarning turlari haqida tushuncha beriladi (3-ilova) 2.2. Axborot chiqib ketish texnik kanallarining tasnifi va tarkibi haqida batafsil ma’lumot beriladi. Klaster metodi qo’llagan holda tushuntiriladi. (4-ilova)	Yozib oladilar E’tibor beradilar, savollar beradilar va yozib oladilar.
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo’yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B. jadvalini to’ldirish beriladi (5 ilova). 3.3. Talabalar bilimini faollashtirish uchun	Savollar beradi. Jadvalni to’ldiradilar Savollarga javob beradilar

	“Aqliy xujum” metodi qo’llaniladi (3-ilova)	

1-ilova

Mavzu: AVTOMATLASHTIRILGAN AXBOROT TIZIMLARIDA AXBOROTLARNI HIMOYALASH

Mavzu rejasi::	1. Texnik vositalar bilan himoyalanadigan axborotlarning turlari; 2. Axborot chiqib ketish texnik kanallarining tasnifi va tarkibi.
Darsning maqsadi: Talabalarda axborotlarni avtomatlashgan texnik vositalar bilan himoyalash tushunchasini hosil qilish	

2-ilova

Адабиётлар:

1. Муҳаммадиев Ж.Ў. Ахборот хавфсизлиги: муаммо ва ечимлар:
Монография. – Т., 2011.
2. Миродова Ш. Проблемы обеспечения информационной безо пасности Республике Узбекистан в условиях глоболизации. – Т., 2008.
3. Қосимов С.С. Ахборот технологиялари. – Т., 2006.
4. Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги.

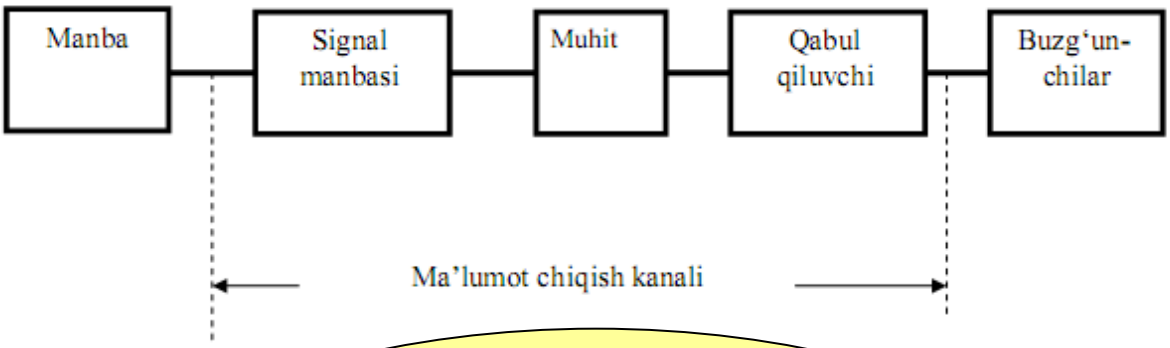
3-ilova

Axborotlarni muhofaza qilishning texnik vositalari – obyektning niqoblovchi (maskirovkalovchi) belgilari ochilishini bartaraf etish yoki kamaytirish, yolg‘on alomatlarni yaratish hamda texnik vositalar orqali axborotga ruxsatsiz kirishga to‘sqinlik qilishga mo‘ljallangan texnik vositalardir.

Himoyaning texnik vositalari – bu texnik qurilmalar, komplekslar yoki tizimlar yordamida obyektni himoyalashdir. Texnik vositalarning afzalligi keng ko‘lamdagi masalalarni hal etilishda, yuqori ishonchlilikda, kompleks rivojlangan himoya tizimini yaratish imkoniyatida, ruxsatsiz foydalanishga urinishlarga mos munosabat bildirishda va himoyalash amallarini bajarish usullaridan foydalanishning an’anaviyligida namoyon

Texnik vositalar bilan himoyalanadigan ma’lumotlarning manbasi va tashuvchilari:
– obyekt tarkibining fizik xususiyatlarini tavsiflovchi belgilar (issiqlik va elektr o‘tkazuvchanligi, tarkibi, qattiqligi va hokazo);
– obyekt tomonidan hosil bo‘ladigan fizik maydonni tavsiflovchi belgilar (eletromagnit, radiatsion, akustik, gravitatsion va hokazo);
– obyektning shakli, rangi, o‘lchami va elementlarini tavsiflovchi belgilar;
– obyektning fazoviy koordinatalarini (harakatlanadigan obyektlarning tezligini) tavsiflovchi belgilar;
– obyektlar va ularning elementlari o‘rtasidagi ma’lum bir aloqalar mavjudligini tavsiflovchi belgilar;
– obyekt faoliyati natijasini (tutun chiqarish, changitish, obyektning tuproqdagi izi, suv va havoni ifloslantirish va shu kabi) tavsiflovchi belgilar.

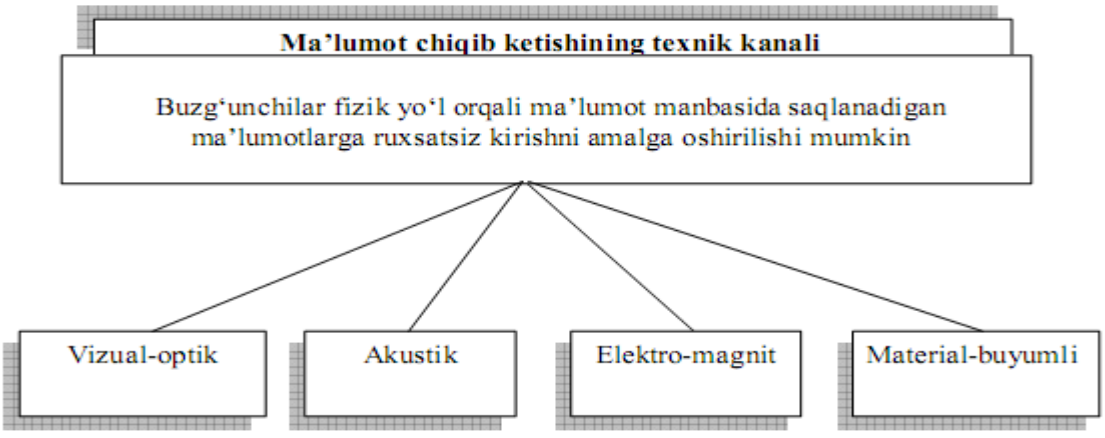
4-ilova

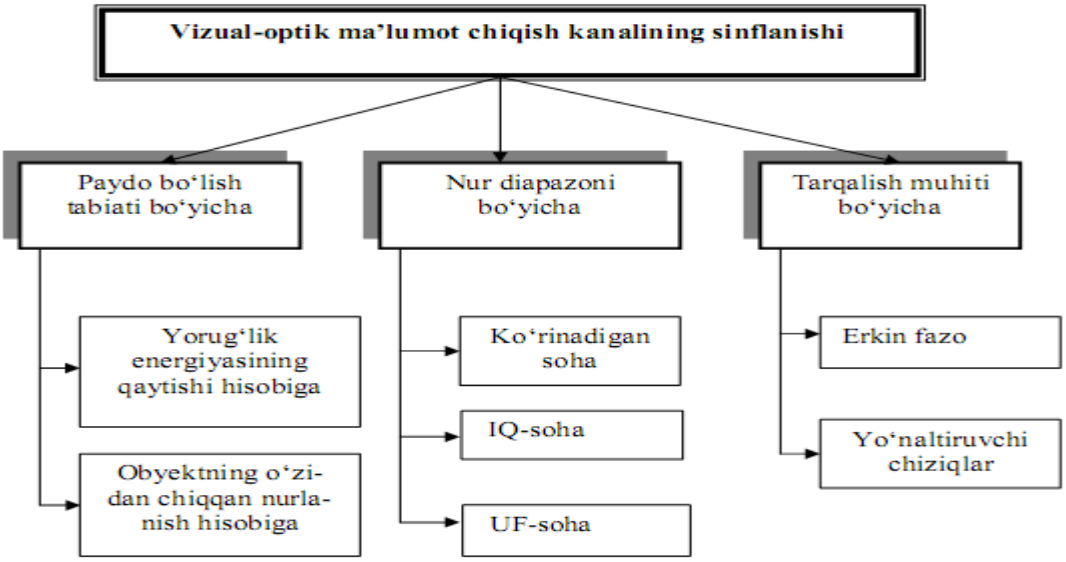


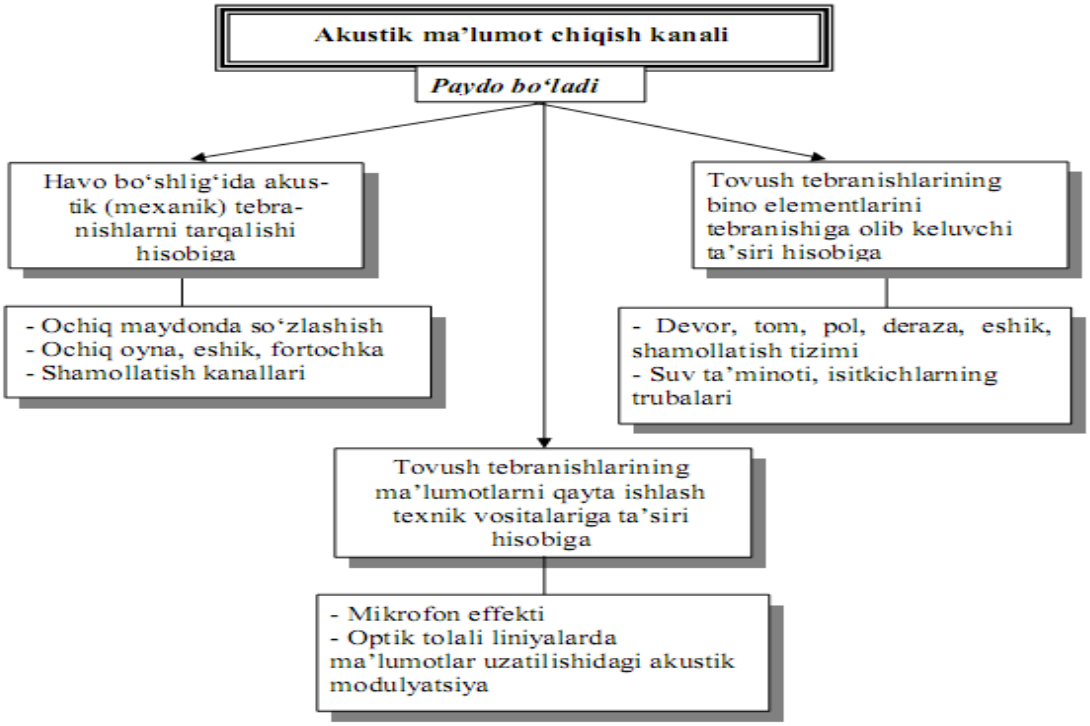
Ma’lumotlar chiqib ketish kanali deb konfedensial ma’lumotlar manbasidan yovuz niyatli shaxsgacha bo‘lgan fizik yo‘l tushuniladi. Bu yo‘l orqali ma’lumot chiqib ketishi yoki saqlanayotgan ma’lumotga ruxsatsiz kirish mumkin. Ma’lumotlar chiqib ketish kanalining vujudga kelishi (paydo bo‘lishi, o‘rnatish) uchun ma’lum fazoviy, energetik va vaqtdagi sharoit hamda yovuz niyatli shaxsda ularga mos ma’lumotlarni qabul qilish va qayd qilish vositalari mavjud bo‘lishi kerak.

Fizik xususiyatlarini inobatga olgan holda ma’lumotlar chiqib ketish kanalining paydo bo‘lishini quyidagi guruhlarga ajratish mumkin:

– visual-optik;
– akustik;
– elektromagnit (magnit va elektrik maydonni o‘z ichiga oladi);
– material+buyumli (qog‘oz, foto, magnitli tashuvchilar, turli ko‘rinishdagi qattiq, suyuq, gaz holatidagi sanoat chiqindilari).




Vizual-optik ma'lumot chiqish kanalining sinflanishi
Paydo bo'lish tabiati bo'yicha
Nur diapazoni bo'yicha
Tarqalish muhiti bo'yicha
Yorug'lik energiyasining qaytishi hisobiga
Obyektning o'zidan chiqqan nurlanish hisobiga
Ko'rinadigan soha
IQ-soha
UF-soha
Erkin fazo
Yo'naltiruvchi chiziqlar


Akustik ma'lumot chiqish kanali
Paydo bo'ladi
Havo bo'shlig'ida akustik (mexanik) tebranishlarni tarqalishi hisobiga
- Ochiq maydonda so'zlashish
- Ochiq oyna, eshik, fortochka
- Shamollatish kanallari
Tovush tebranishlarining bino elementlarini tebranishiga olib keluvchi ta'siri hisobiga
- Devor, tom, pol, deraza, eshik, shamollatish tizimi
- Suv ta'minoti, isitkichlarning trubalari
Tovush tebranishlarining ma'lumotlarni qayta ishlash texnik vositalariga ta'siri hisobiga
- Mikrofon effekti
- Optik tolali liniyalarda ma'lumotlar uzatilishidagi akustik modulyatsiya

5-ilova

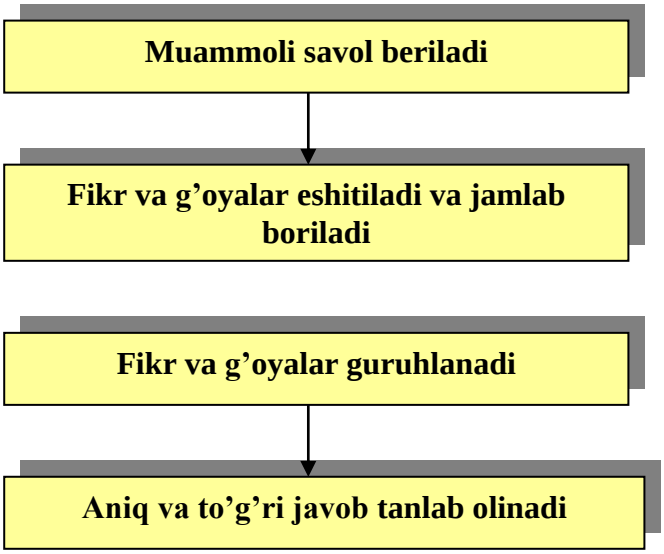
B	BX	B
.....	.....	.....

6-ilova

“Aqliy hujum” metodini qo’llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g’oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g’oyalar, ular hatto to’g’ri bo’lmasa ham inobatga olinadi.
3. Har bir ta’lim oluvchi qatnashishi shart.

Quyida (1-chizma) “Aqliy hujum” metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. Ma’lumotlarni chiqib ketish kanali deb nimaga aytiladi?
2. Ma’lumotlarni chiqib ketishning texnik kanaliga nimalar kiradi?
3. Ximoyalashning texnik vositalariga qanday qurilmalar kiradi?

AVTOMATLASHTIRILGAN AXBOROT TIZIMLARIDA AXBOROTLARNI HIMOYALASH

MA’RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	____ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo’yicha ma’ruza
Mavzu rejasi:	1. Ob’ektlarni kuzatish, signallarni eshitish va tutib olishning asosiy usul va tamoyillari; 2.Axborotlarni injener-texnik himoyalash.
Dars maqsadi: Talabalarda axborotlarni avtomatlashgan texnik vositalar bilan himoyalash tushunchasini hosil qilish	
Pedagog vazifalari:	***O’quv natijalari:***
- Ob’ektlarni kuzatish, signallarni eshitish va tutib olishning asosiy usul va tamoyillari bilan tanishtiriish va ma’ruzani bayon qьilish; - Axborotlarni injener-texnik himoyalash usulini tushuntirib berish;	- Ob’ektlarni kuzatish, signallarni eshitish va tutib olishning asosiy usul va tamoyillari haqida tushunchaga ega bo’ladilarva daftarga yozib oladilar; - Axborotlarni injener-texnik himoyalash usulini o’rganadilar.
O’qitish usullari	Ma’ruza, klaster metodi, “Aqliy hujum” metodi
Ta’limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko’rgazmali qurollar.
Ta’limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta’minlangan xona.
Nazorat	O’zini-o’zi nazorat qilish

AVTOMATLASHTIRILGAN AXBOROT TIZIMLARIDA AXBOROTLARNI HIMOYALASH

MAVZUSIDAGI MA’RUZA DARSIGA

TEXNOLOGIK XARITA

Faoliyat bosqichlari	**Faoliyatning mazmuni**	
	O’qituvchi	**Talaba**
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo’yicha kerakli adabiyotlarni e’lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1. Ob’ektlarni kuzatish, signallarni eshitish va tutib olishning asosiy usul va tamoyillari haqida tushuncha beriladi va ma’ruza bayon qilinadi. Ma’lumotlarning daraxtsimon metodi orqali taqdim etiladi. (3-ilova) 2.2. Axborotlarni injener-texnik himoyalash usuli haqida batafsil ma’lumot beriladi. (4-ilova)	Yozib oladilar E’tibor beradilar, savollar beradilar va yozib oladilar.

3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B. jadvalini to'ldirish beriladi (5 ilova) 3.3. Talabalar bilimini nazorat qilish uchun "Aqliy xujum" metodi qo'llaniladi (6-ilova)	Savollar beradi. Jadvalni to'ldiradilar Savollarga javob berishadi

1-ilova

Mavzu: AVTOMATLASHTIRILGAN AXBOROT TIZIMLARIDA AXBOROTLARNI HIMOYALASH

Mavzu rejasi::	1. Ob'ektlarni kuzatish, signallarni eshitish va tutib olishning asosiy usul va tamoyillari; 2. Axborotlarni injener-texnik himoyalash.
Darsning maqsadi: Talabalarda axborotlarni avtomatlashgan texnik vositalar bilan himoyalash tushunchasini hosil qilish	

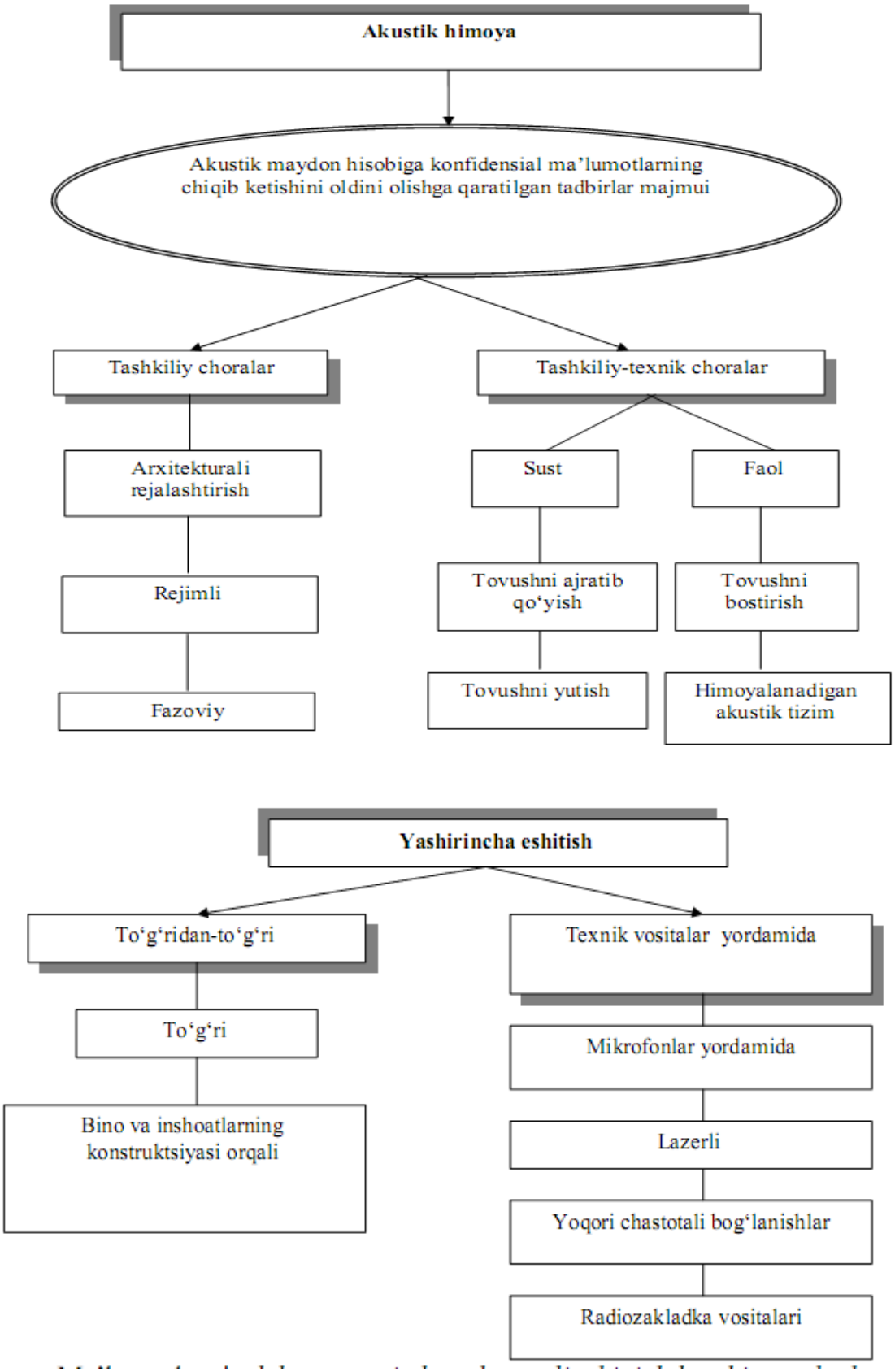
2-ilova

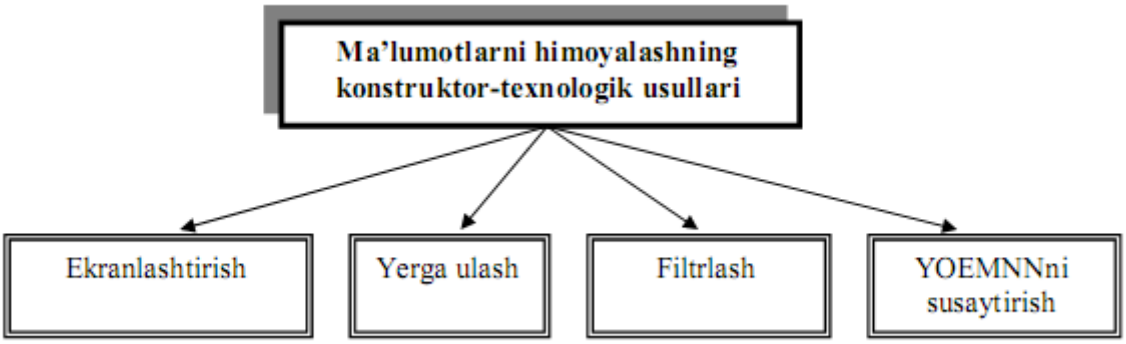
Адабиётлар:

1. Муҳаммадиев Ж.Ў. Ахборот хавфсизлиги: муаммо ва ечимлар:
Монография. – Т., 2011.
2. Миродова Ш. Проблемы обеспечения информационной безо пасности Республике Узбекистан в условиях глоболизации. – Т., 2008.
3. Қосимов С.С. Ахборот технологиялари. – Т., 2006.
4. Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги.

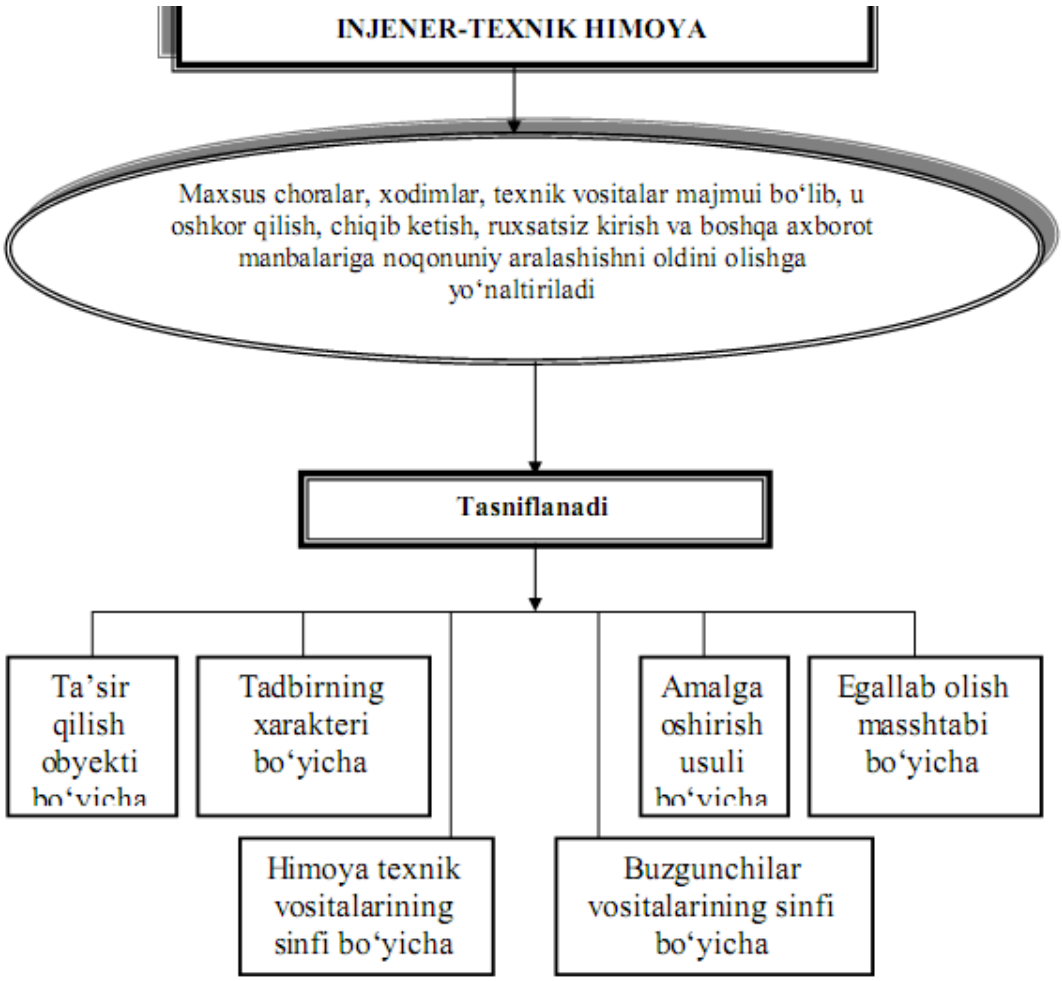
3-ilova

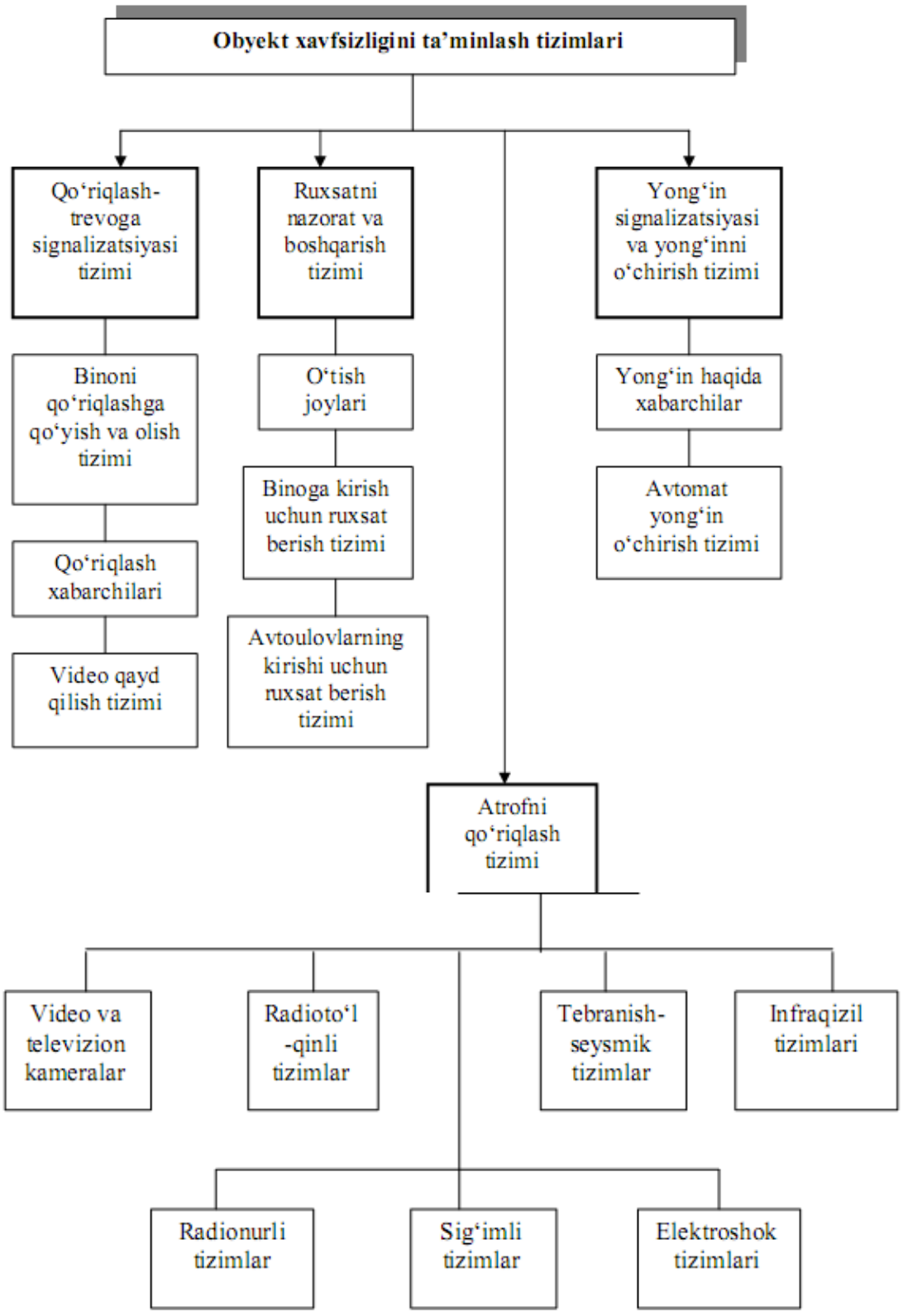
Ma’lumotlarning taqdim etishning daraxtsimon metodi:




Ma’lumotlarni himoyalashning konstruktor-texnologik usullari
Ekranlashtirish
Yerga ulash
Filtrlash
YOEMNNni susaytirish

4-ilova


INJENER-TEXNIK HIMOYA
Maxsus choralar, xodimlar, texnik vositalar majmui bo‘lib, u oshkor qilish, chiqib ketish, ruxsatsiz kirish va boshqa axborot manbalariga noqonuniy aralashishni oldini olishga yo‘naltiriladi
Tasniflanadi
Ta’sir qilish obyekti bo‘yicha
Tadbirning xarakteri bo‘yicha
Himoya texnik vositalarining sinfi bo‘yicha
Buzgunchilar vositalarining sinfi bo‘yicha
Amalga oshirish usuli bo‘yicha
Egallab olish masshtabi bo‘yicha


Obyekt xavfsizligini ta’minlash tizimlari
Qo‘riqlash-trevoga signalizatsiyasi tizimi
Ruxsatni nazorat va boshqarish tizimi
Yong‘in signalizatsiyasi va yong‘inni o‘chirish tizimi
Binoni qo‘riqlashga qo‘yish va olish tizimi
O‘tish joylari
Yong‘in haqida xabarchilar
Qo‘riqlash xabarchilari
Binoga kirish uchun ruxsat berish tizimi
Avtomat yong‘in o‘chirish tizimi
Video qayd qilish tizimi
Avtoulovlarning kirishi uchun ruxsat berish tizimi
Atrofni qo‘riqlash tizimi
Video va televizion kameralar
Radioto‘l-qinli tizimlar
Tebranish-seysmik tizimlar
Infraqizil tizimlari
Radionurli tizimlar
Sig‘imli tizimlar
Elektroshok tizimlari

5-ilova

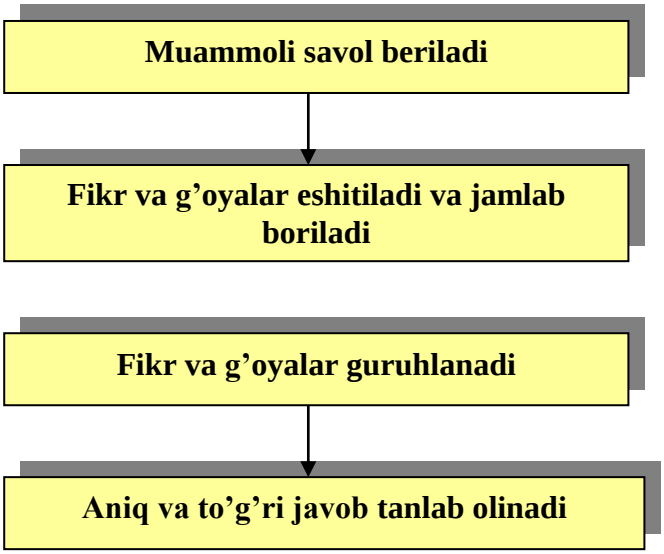
B	BX	B
.....	.....	.....

6-ilova

“Aqliy hujum” metodini qo’llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g’oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g’oyalar, ular hatto to’g’ri bo’lmasa ham inobatga olinadi.
3. Har bir ta’lim oluvchi qatnashishi shart.

Quyida (1-chizma) “Aqliy hujum” metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. Axborotlarni injener-texnik himoyalash deganda nimani tushunasiz?
2. Ob’ekt xavfsizligini ta’minlash tizimlariga nimalar kiradi?
3. Injener-texnik ximoyalash usullariga nimalar kiradi?
4. Ma’lumotlarni himoyalashni konstruktor-texnologik usullari?

MAVZU № 3 (4 soat)

AXBOROTLARNI STENOGRAFIK HIMOYALASH MA'RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	___ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1.Zamonaviy kompyuter stenografiyasi 2. Kompyuter stenografiyasi istikbollari
Dars maqsadi: Talabalarda axborotlarni stenografik ximoyalash tushunchasini hosil qilish	
Pedagog vazifalari:	***O'quv natijalari:***
- Zamonaviy kompyuter stenografiyasi tushunchasi bilan tanishtiriish va ma'ruzani bayon qilish; - Kompyuter stenografiyasi istikbollari yoritib berish.	- Zamonaviy kompyuter stenografiyasi haqida tushunchaga ega bo'ladilar va ma'ruzani daftarga yozib oladilar; - Kompyuter stenografiyasi istikbollarini o'rganadilar
O'qitish usullari	Ma'ruza, B.BX.B metodi, aqliy hujum
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

AXBOROTLARNI STENOGRAFIK HIMOYALASH MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1. Zamonaviy kompyuter stenografiyasining asosiy usullari haqidagi tushunchasi bilan tanishtiriish va ma'ruzani bayon qilish. (3-ilova) 2.2. Komp'yuter stenografiyasi istikbollari haqida batafsil ma'lumot beriladi. (4-ilova)	Yozib oladilar E'tibor beradilar, savollar beradilar va yozib oladilar.
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B. jadvalini to'ldirish beriladi (5 ilova) 3.3. Talabalar bilimini nazorat qilish uchun "Aqliy xujum" metodi qo'llaniladi (6-ilova)	Savollar beradi. Jadvalni to'ldiradilar Savollarga javob beradilar

1-ilova

Mavzu: **AXBOROTLARNI STENOGRAFIK HIMOYALASH**

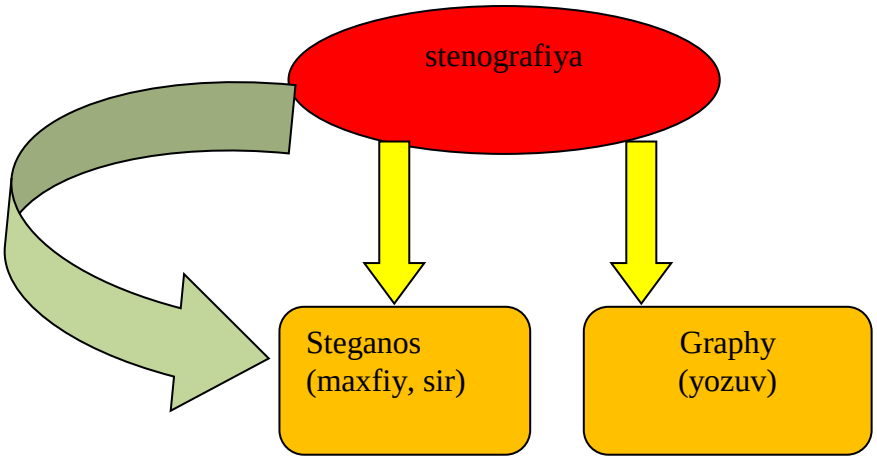
Mavzu rejasi::	1.Zamonaviy kompyuter stenografiyasi 2. Komp'yuter stenografiyasi istikbollari.
Darsning maqsadi: Talabalarda axborotlarni stenografik ximoyalash tushunchasini hosil qilish	

2-ilova

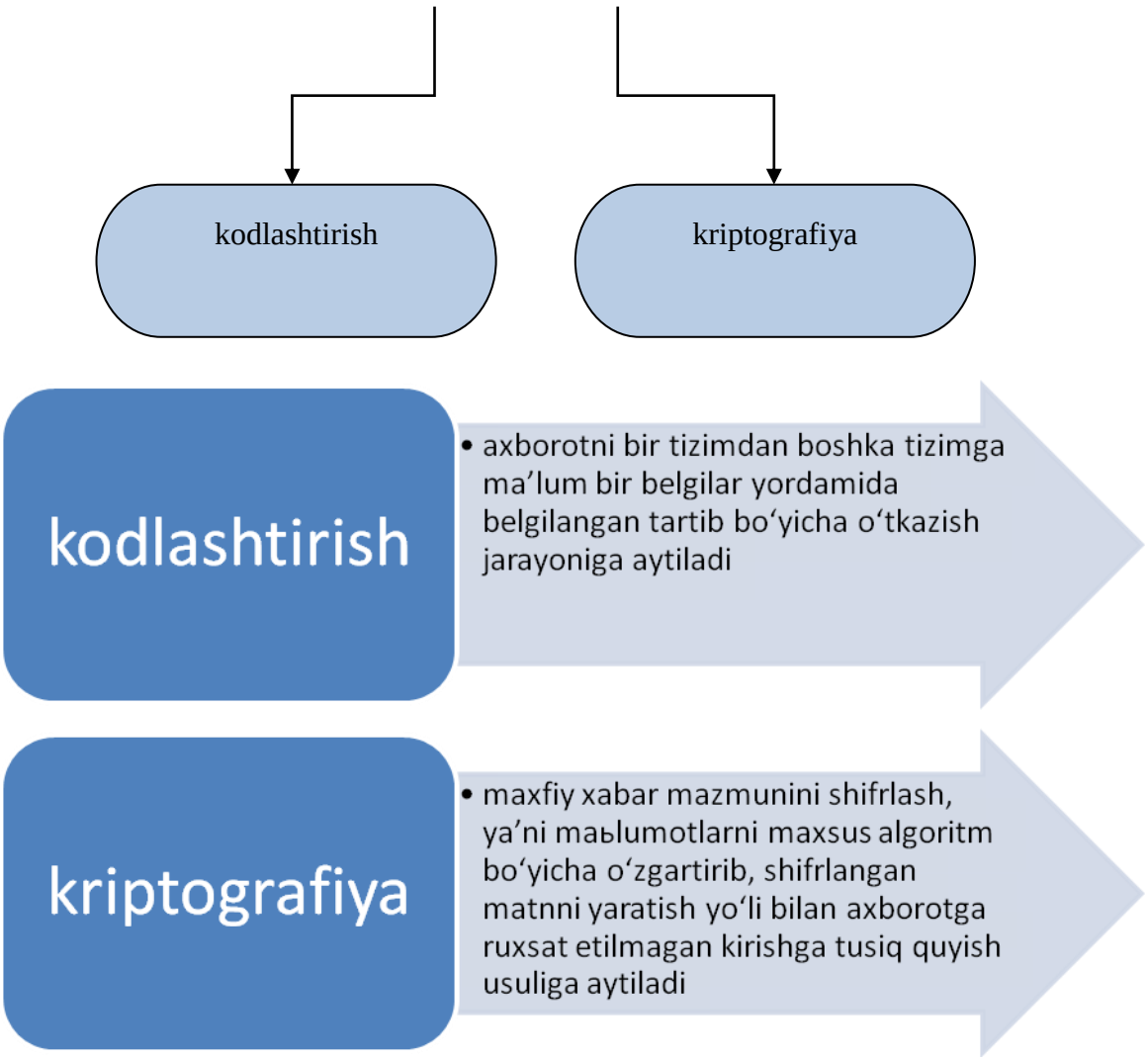
Адабиётлар:
1. Муҳаммадиев Ж.Ў. Ахборот хавфсизлиги: муаммо ва ечимлар:
Монография. – Т., 2011.
2. Миродова Ш. Проблемы обеспечения информационной безо
пасности Республике Узбекистан в условиях глоболизации.
– Т., 2008.

3-ilova

Ruxsat etilmagan kirishdan axborotni ishonchli himoyalash muammosi eng ilgaritdan mavjud va hozirgi vaqtgacha hal qilinmagan.



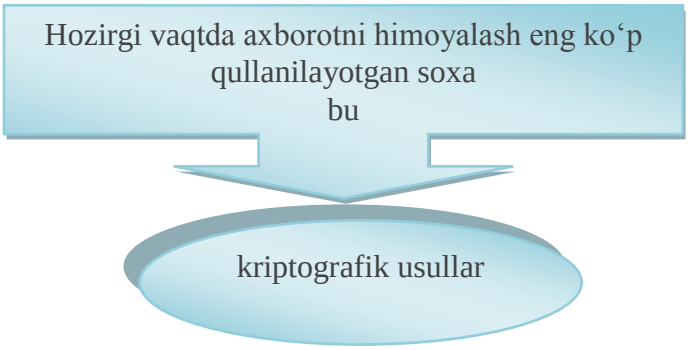
Axborotni ximoyalash uchun qo’llaniladigan usullar



Kompyuter texnologiyalari stenografiyaning rivojlanishi va mukammallashuviga yangi turtki berdi. Natijada axborotni himoyalash sohasida yangi yo‘nalish — **kompyuter stenogryafiya**si paydo bo‘ldi. Global tarmoqlari va mulьtimedia soxasidagi zamonaviy progress telekommunikatsiya kanallarida ma’lumotlarni uzatish xavfsizligini ta’minlash uchun mo‘ljallangan yangi usullarni yaratishga olib keldi. Bu usullar shifrlash qurilmalarining tabiiy noaniqligidan va analogli video yoki audiosignallarning serobligidan foydalanib xabarlarni komp'yuter fayllari (konteynerlar)da yashirish imkonini beradi. Shu bilan birga kriptografiyadan farqli ravishda bu usullar axborotni uzatish faktining o‘zini ham yashiradi. K.Shennon sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi. Zamonaviy steganografiyasida ikkita asosiy fayl turlari mavjud: yashirish uchun mo‘ljallangan **xabar-fayl**, va **konteyner-fayl**, u xabarni yashirish uchun ishlatilishi mumkin. Bunda konteynerlar ikki turda bo‘ladi: **konteyner-original** (yoki «bo‘sh» konteyner) - bu konteyner yashirin axborotni saqlamaydi; **konteyner-natija** (yoki «tuldirilgan» konteyner) — bu konteyner yashirin axborotni saqlaydi. **Kalit** sifatida xabarni konteynerga kiritib kuyish tartibini aniklaydigan maxfiy element tushuniladi.

4-ilova

Komp'yuter stenografiyasi rivojlanishi tendensiyasining tahlili shuni ko‘rsatadiki, keyingi yillarda komp'yuter stenografiyasi usullarini rivojlantirishga qiziqish kuchayib bormoqda. Jumladan, ma’lumki, axborot xavfsizligi muammosining dolzarbligi doim kuchayib bormoqda va axborotni himoyalashning yangi usullarini qidirishga rag‘batlantirilayapti. Boshka tomondan, axborot-kommunikatsiyalar texnologiyalarining jadal rivojlanishi ushbu axborotni ximoyalashning yangi usullarini joriy qilish imkoniyatlari bilan ta’minlayapti va albatta, bu jarayonning kuchli katalizatori bo‘lib umumfoydalaniladigan Internet komp'yuter tarmogining juda kuchli rivojlanishi hisoblanadi.



Lekin, bu yo‘lda komp'yuter viruslari, «mantiqiy bomba»lar kabi axborotiy qurollarning kriptovositalarni buzadigan ta’siriga bog‘liq ko‘p echilmagan muammolar mavjud. Boshka tomondan, kriptografik usullarni ishlatishda kalitlarni taqsimlash muammosi ham bugungi kunda oxirigacha echilmay turibdi. Komp'yuter steganografiyasi va kriptografiyalarining birlashtirilishi paydo bo‘lgan sharoitdan qutulishning yaxshi bir yo‘li bular edi, chunki, bu holda axborotni himoyalash usullarining zaif tomonlarini yo‘qotish mumkin. Shunday qilib, komp'yuter stenografiyasi hozirgi kunda axborot xavfsizligi bo‘yicha asosiy texnologiyalardan biri bo‘lib hisoblanadi.

5-ilova

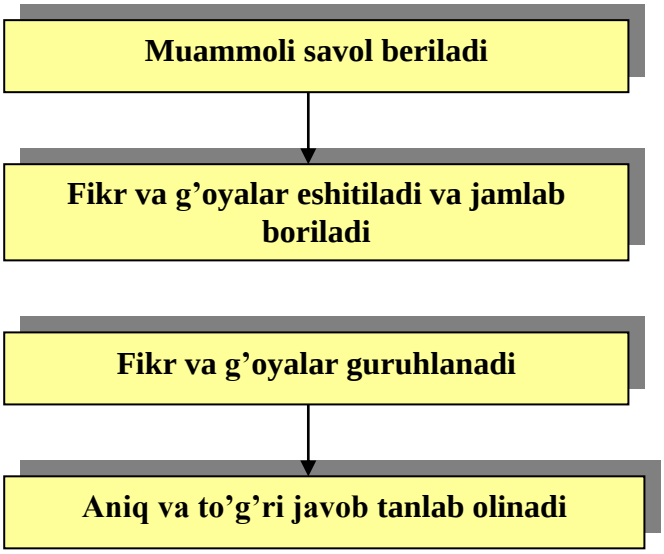
B	BX	B
.....	.....	.....

6-ilova

“Aqliy hujum” metodini qo’llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g’oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g’oyalar, ular hatto to’g’ri bo’lmasa ham inobatga olinadi.
3. Har bir ta’lim oluvchi qatnashishi shart.

Quyida (1-chizma) “Aqliy hujum” metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. Stenografiya deb nimaga aytiladi?
2. Kodlashtirish va shifrlashni orasidagi farqni tushuntirib bering?
3. Kriptografiya nima?
4. Axborotlarni ximoyalash usullariga qaysilarni kiritish mumkin?

AXBOROTLARNI STENOGRAFIK HIMOYALASH
MA'RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	___ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1. Komp'yuter stenografiyasining asosiy vazifalari 2. Stenografik dasturlar to'grisida qisqacha ma'lumot
Dars maqsadi: Talabalarda axborotlarni stenografik ximoyalash tushunchasini hosil qilish	
Pedagog vazifalari:	***O'quv natijalari:***
-Komp'yuter stenografiyasining asosiy vazifalari bilan tanishtiriish va ma'ruzani talabalarga yozdirish; - Stenografik dasturlar to'grisida qisqacha ma'lumot berish.	- Kompyuter stenografiyasining asosiy vazifalari bilan tanishib chiqadilar va ma'ruzani yozib oladilar; - Stenografik dasturlar to'grisida ma'lumotga ega bo'ladilar.
O'qitish usullari	Ma'ruza, klaster metodi, insert metodi, "Aqliy xujum" metodi.
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

AXBOROTLARNI STENOGRAFIK HIMOYALASH
MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1. Kompyuter stenografiyasining asosiy vazifalari bilan tanishtiriish va ma'ruzani bayon qilish. (3-ilova) 2.2. Stenografik dasturlar to'grisida qisqacha ma'lumot berish. (4-ilova)	Yozib oladilar E'tibor beradilar, savollar beradilar va yozib oladilar.
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B. jadvalini to'ldirish beriladi (5 ilova) 3.3. Talabalar bilimini nazorat qilish uchun "Aqliy xujum" metodi qo'llaniladi (6-ilova)	Savollar beradi. Jadvalni to'ldiradilar Savollarga javob berishadi

1-ilova

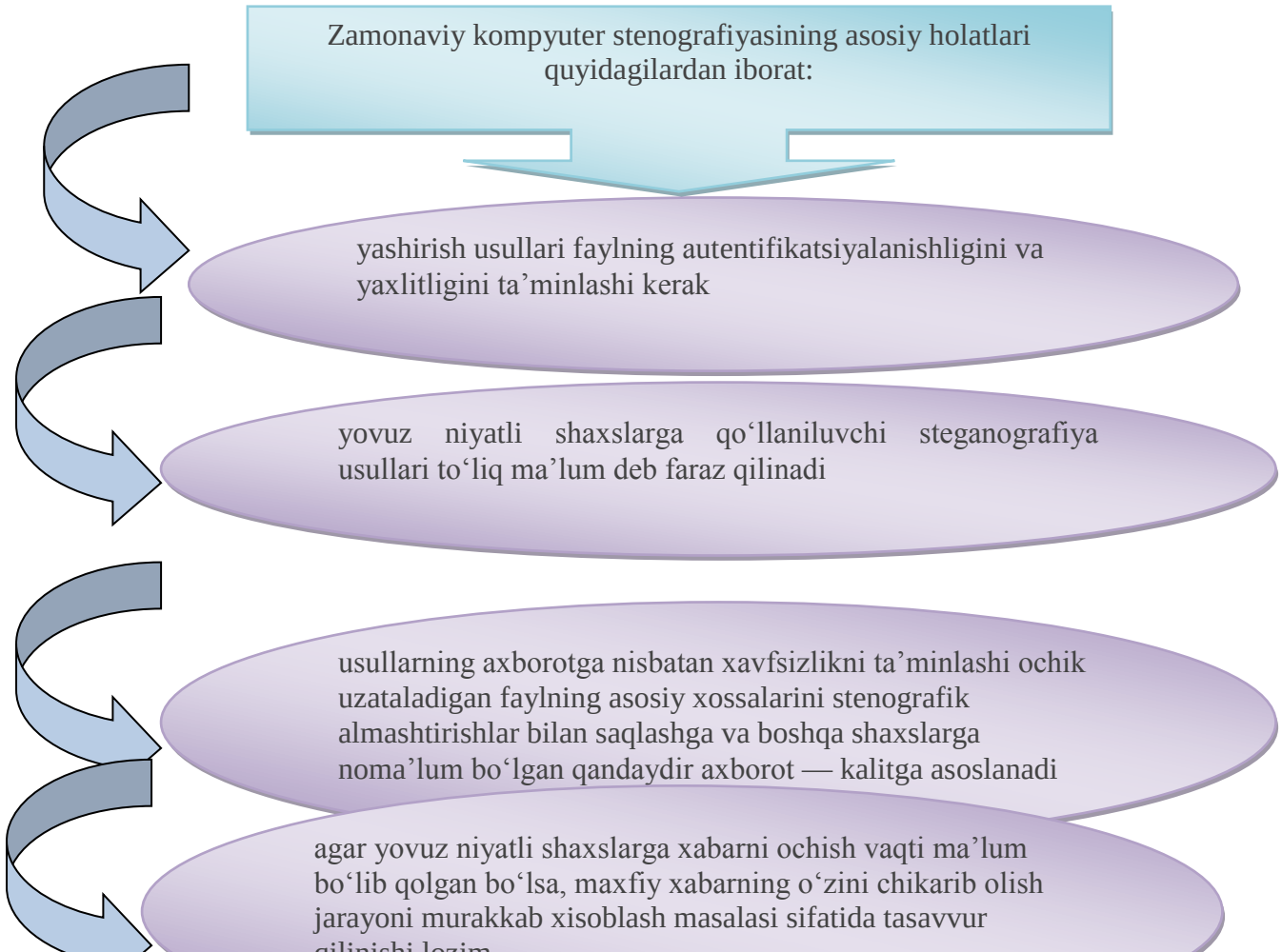
Mavzu: **AXBOROTLARNI STENOGRAFIK HIMOYALASH**

Mavzu rejasi::	1. Kompyuter stenografiyasining asosiy vazifalari 2. Stenografik dasturlar to‘grisida qisqacha ma'lumot
Darsning maqsadi: Talabalarda axborotlarni stenografik ximoyalash tushunchasini hosil qilish	

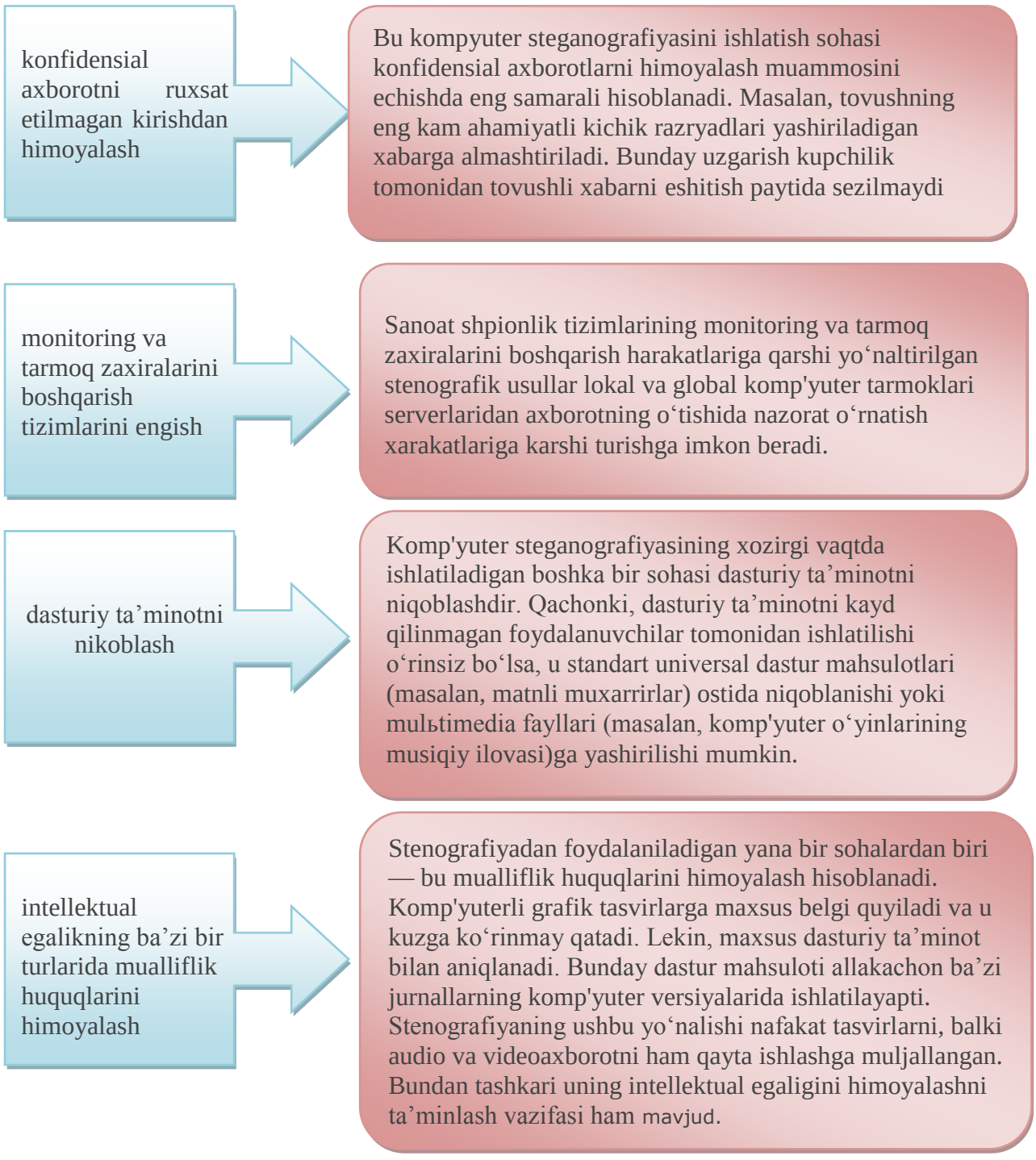
2-ilova

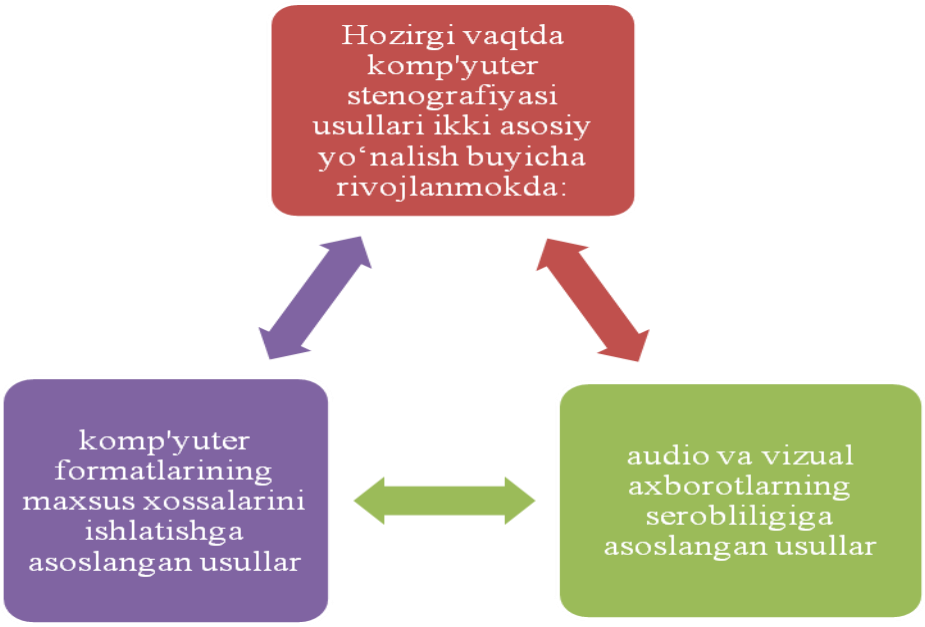
Адабиётлар:
1. Муҳаммадиев Ж.Ў. Ахборот хавфсизлиги: муаммо ва ечимлар:
Монография. – Т., 2011.
2. Миродова Ш. Проблемы обеспечения информационной безо пасности Республике Узбекистан в условиях глоболизации. – Т., 2008.
3. Қосимов С.С. Ахборот технологиялари. – Т., 2006.
4. Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги.

3-ilova

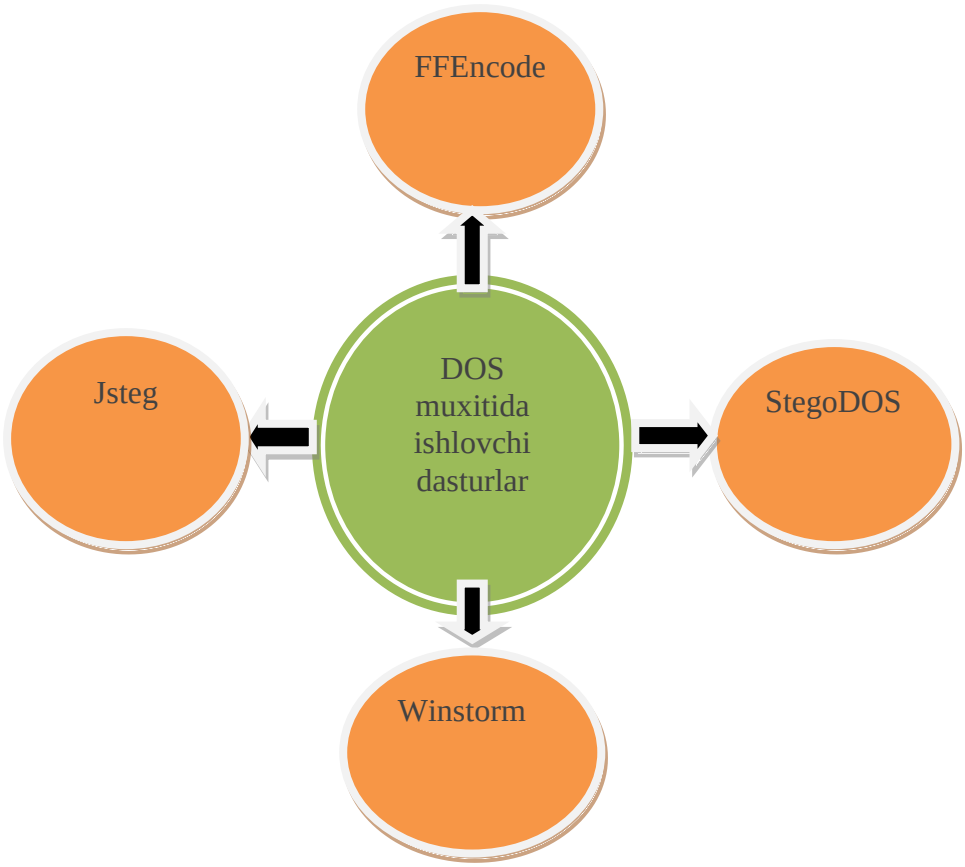


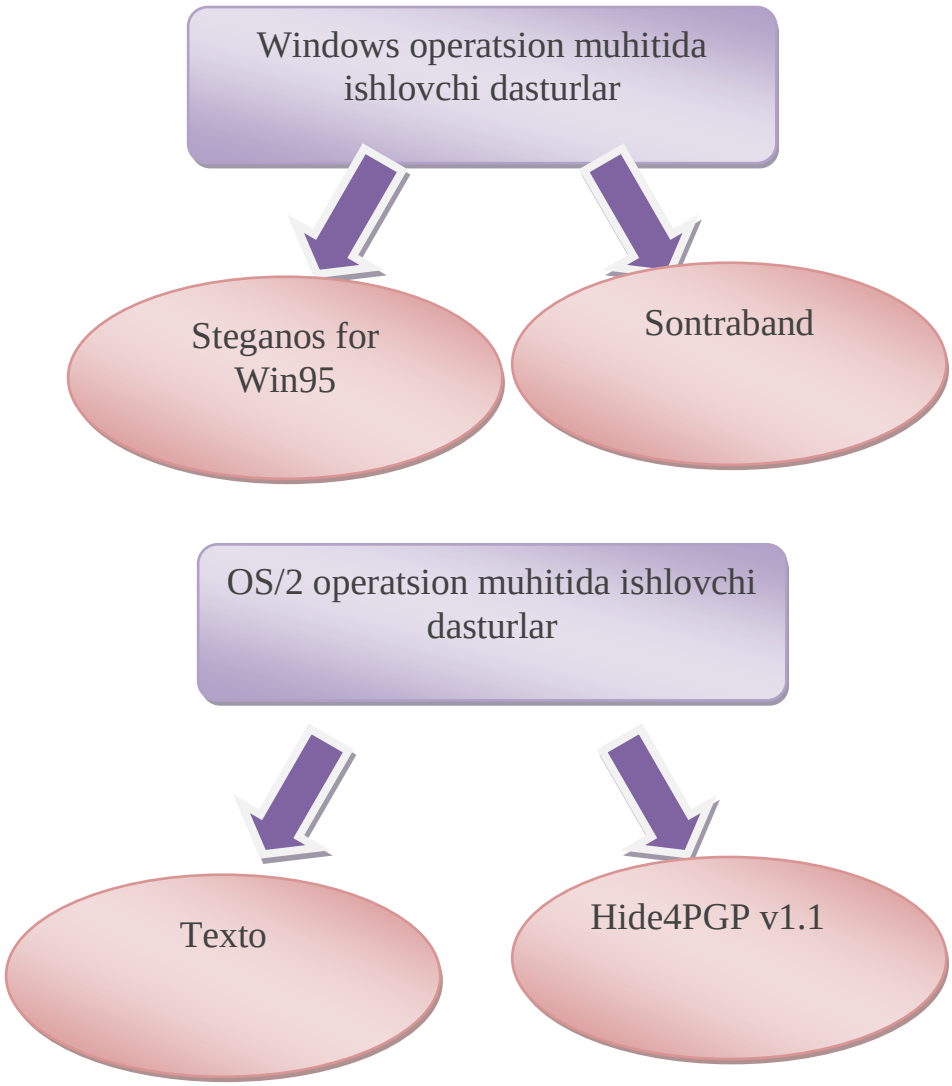
Internet komp'yuter tarmog‘ining axborot manbalarini tahlili quyidagi xulosaga kelishga imkon berdi, ya’ni hozirgi vaqtda stenografik tizimlar quyidagi asosiy masalalarni echishda faol ishlatilayapti:




Hozirgi vaqtda komp'yuter stenografiyasi usullari ikki asosiy yo‘nalish buyicha rivojlanmokda:
komp'yuter formatlarining maxsus xossalarini ishlatishga asoslangan usullar
audio va vizual axborotlarning serobliligiga asoslangan usullar

4-ilova


FFEncode
Jsteg
DOS muxitida ishlovchi dasturlar
StegoDOS
Winstorm



Windows operatsion muhitida ishlovchi dasturlar:

• Steganos for Win95 dasturi ishlatishda juda engil bo‘lib, ayni paytda fayllarni shifrlash va ularni VMR, DIV, VOS, WAV, ASCII, NTML ken-gaytmali fayllar ichiga joylashtirib yashirishda juda kudratli xisoblanadi;
• Sontraband dasturi 24-bitli VMR formatdagi grafik fayllar ichida har qanday faylni yashira olish imkoniyatiga ega.
DOS muxitida ishlovchi dasturlar:
• Jsteg dasturi ma’lumotni JRG formatli fayllar ichiga yashirish uchun mo‘ljallangan;
• FFEncode dasturi ma’lumotlarni matnli fayllar ichida yashirish imkoniyatiga ega;
• StegoDOS dasturlar paketining axborotni tasvirda yashirish imkoniyati mavjud;
• Winstorm dasturlar paketi RSX formatli fayllar ichiga xabarni shifrlab yashiradi.
OS/2 operatsion muhitida ishlovchi dasturlar:
- Texto dasturi ma’lumotlarni ingliz tilidagi matnga aylantiradi;
- Hide4PGP v1.1 dasturi VMR, WAV, VOS formatli fayllar ichiga maьlumotlarni yashirish imkoniyatiga ega.
Macintosh komp'yuterlari uchun mo‘ljallangan dasturlar:
- Raranoid dasturi ma’lumotlarni shifrlab, tovushli formatli fayl ichiga yashiradi:
- Stego dasturining RIST kengaytmali fayl ichiga ma’lumotlarni yashirish imkoniyati mavjud.

5-ilova

V	+	–	?

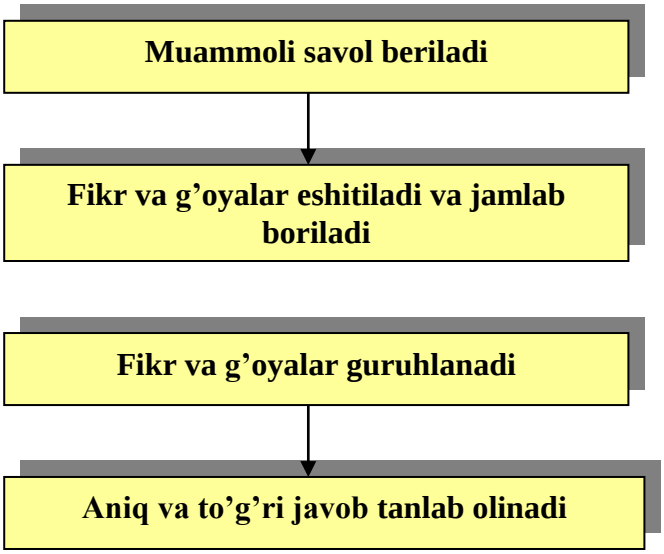
“V”- men bilgan ma’lumotlarga mos;
“-“ - men bilgan ma’lumotlarga zid;
“+” - men uchun yangi ma’lumot;
“?” - men uchun tushunarsiz yoki ma’lumotni

6-ilova

“Aqliy hujum” metodini qo’llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g’oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g’oyalar, ular hatto to’g’ri bo’lmasa ham inobatga olinadi.
3. Har bir ta’lim oluvchi qatnashishi shart.

Quyida (1-chizma) “Aqliy hujum” metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. Stenografiyaning asosiy vazifalariga nimalar kiradi?
2. Kompyuter stenografiyasining asosiy xolatlarini keltirib o’ting?
3. Kompyuter stenografiyasining asosiy yo’nalishlarini sanab o’ting?

AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH
MA'RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	____ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1. Kriptografiya asosi va asosiy terminlari; 2. Zamonaviy kriptografiya.
Dars maqsadi: Talabalarda axborotlarni kriptografik ximoyalash tushunchasini hosil qilish	
Pedagog vazifalari:	***O'quv natijalari:***
- Kriptografiya asosi va asosiy terminlari bilan tanishtirish va ma'ruzani bayon qilish; - Zamonaviy kriptografiya tushunchasini yoritib berish.	- Kriptografiya asosi va asosiy terminlari bilan tanishib chiqadilar va daftarlariga yozib oladilar; - Zamonaviy kriptografiya tushunchasini tushunadilar va yozib oladilar
O'qitish usullari	Ma'ruza, insert metodi, "Aqliy xujum" metodi
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH
MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1 Kriptografiya asosi va asosiy terminlari bilan tanishtiradi va ma'ruzani bayon qiladi. (3-ilova) 2.2. Zamonaviy kriptografiya haqida batafsil ma'lumot beriladi. (4-ilova)	Yozib oladilar E'tibor beradilar, savollar beradilar va yozib oladilar.
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B. jadvalini to'ldirish beriladi (5 ilova) 3.3. Talabalar bilimini nazorat qilish uchun "Aqliy xujum" metodi qo'llaniladi (6-ilova)	Savollar beradi. Jadvalni to'ldiradilar Savollarga javob beradilar

1-ilova

Mavzu: **AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH**

Mavzu rejasi::	1. Kriptografiya asosi va asosiy terminlari; 2. Zamonaviy kriptografiya.
Darsning maqsadi: Talabalarda axborotlarni kriptografik ximoyalash tushunchasini hosil qilish	

2-ilova

Адабиётлар:

1. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
2. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
3. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001й.
4. Ященко В.В. Введение в криптографию. МЦМО, 2003й.
5. Масленников А. Практическая криптография BHV – 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. . С.К. Ғаниев, М.М. Каримов, К.А. Ташев «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.

3-ilova

Kriptografiyaning masalasi va asosiy terminlari

Kriptografiya – so'zi grek tilidan olingan bo'lib, "maxfiy yozish" degan ma'noni anglatadi. Umumiy qo'lanilishiga ko'ra mazkur tushuncha biror ma'lumotni maxfiy saqlash va himoyalash demakdir.

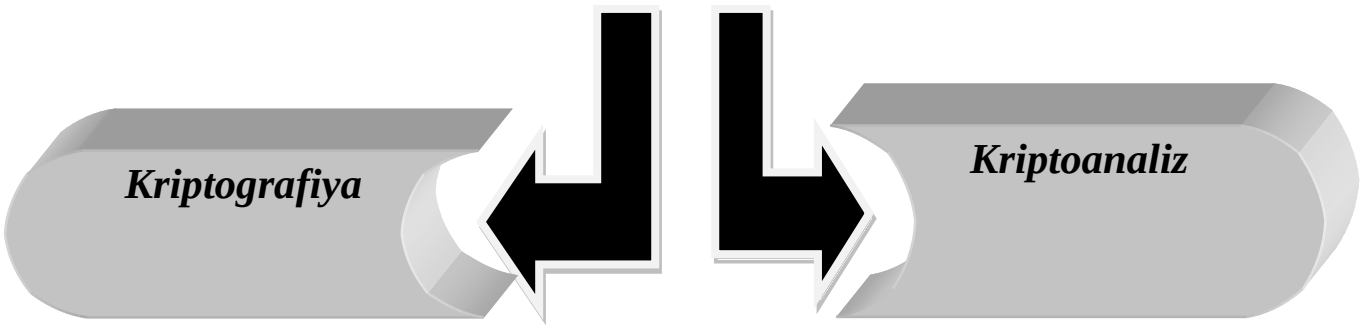
Shifrlarning kriptografik xossalarini tashkil etuvchi: kriptohujumlarga bardoshliligi, axborot-kommunikatsiya tarmoqlarida qo'llanishi samaradorligi, elektron qurilmalarining yaratilishini qulayligi kabi masalalarni tahlil qilish bilan shug'ullanuvchi fan turiga **kriptotahlil** deb yuritiladi. Ushbu termin fanga 1920 yilda buyuk matematik U. Fridman tomonidan kiritilgan.

Kriptografiya va kriptotahlil birlashtiruvchi(fan) bilim sohasiga **kriptologiya** deyiladi.

Shunday qilib, kriptografiya va kriptotahlil bir-birlari bilan uzviy ravishda bog'liq bo'lgan fan yo'nalishlaridir, ya'ni har qanday himoyalanishni chuqur kriptotahlil qilmasdan amalga oshirish mumkin emas.

Kriptologiya – axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi (*kryptos* – maxfiy, sirli, *logos* - fan). Kriptologiya ikki yo'nalishga bo'linadi *kriptografiya* va *kriptoanaliz*. Bu ikki yo'nalishning maqsadlari qarama-qarshi.

Kriptologiya



Kriptografik usullardan foydalanishning asosiy yo'nalishi – maxfiy axborotning aloqa kanalidan uzatish (masalan, elektron pochta), uzatiladigan xabarning uzunligini o'rnatish, axborotni (hujjatlarni, ma'lumotlar bazasini) shifrlangan holda raqamli vositalarda saqlash.

Shunday qilib, kriptografiya axborotni shunday qayta ishlash imkonini beradiki, bunda uni qayta tiklash faqat kalitni bilgandagina mumkin.

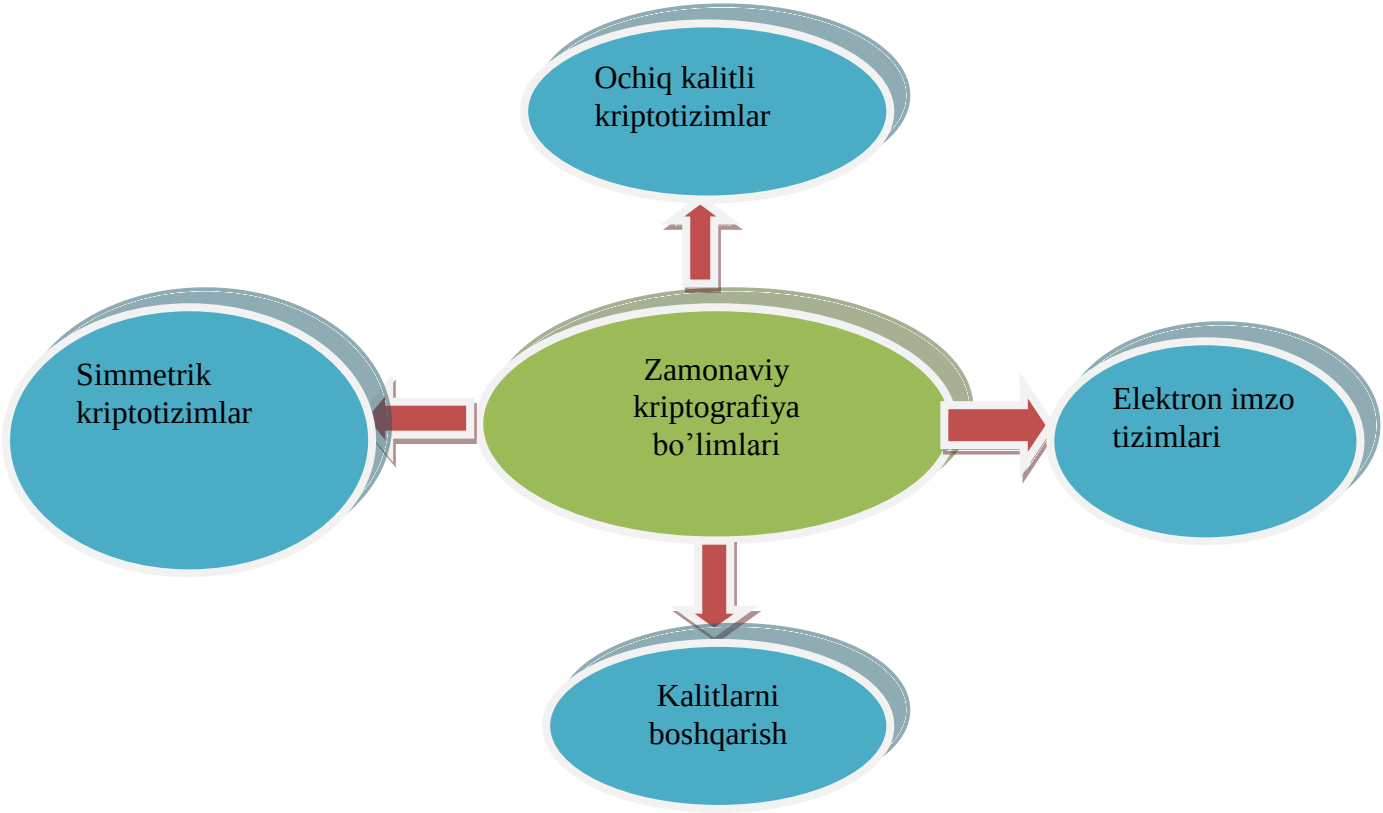
Shifrlash va deshifrlashda qatnashadigan axborot sifatida biror alifbo asosida yozilgan matnlar qaraladi. Bu terminlar ostida quyidagilar tushuniladi.

Alifbo	axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam.
Matn	alifbo elementlarining tartiblangan to'plami
Shifrlash	akslantirish jarayoni: ***ochiq matn*** deb ham nomlanadigan matn ***shifrmatnga*** almashtiriladi
Deshifrlash	shifrlashga teskari jarayon. Kalit asosida shifrmatn ochiq matnga akslantiriladi
Kalit	matnni shifrlash va shifrini ochish uchun kerakli axborot.

4-ilova

Zamonaviy kriptografiya

Kriptografik tizim – ochiq matnni akslantirishning *T* oilasini o'zida mujassamlashtiradi. Bu oila a'zolari *k* bilan indekslanadi yoki belgilanadi. *k* parametr kalit hisoblanadi. *K* kalitlar fazosi – bu kalitning mumkin bo'lgan qiymatlari to'plami. Odatda kalit alifbo harflari ketma-ketligidan iborat bo'ladi.



- ***Simmetrik kriptotizimlarda*** shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi.
- ***Ochiq kalitli kriptotizimlar***da bir-biriga matematik usullar bilan bog'langan *ochiq* va *yopiq* kalitlardan foydalaniladi. Axborot ochiq kalit yordamida shifrlanadi, ochiq kalit barchaga oshkor qilingan

Kriptobardoshlilik deb kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifiga aytiladi.
Kriptobardoshlilikning bir necha ko'rsatkichlari bo'lib, ular:

- barcha mumkin bo'lgan kalitlar soni;
- kriptoanaliz uchun zarur bo'lgan o'rtacha vaqt.

T_k akslantirish unga mos keluvchi algoritm va ***K*** kalit qiymati bilan aniqlanadi. Axborotni himoyalash maqsadida samarali shifrlash kalitni yashirin saqlashga va shifrning kriptobardoshliligiga bog'liq.

5-ilova

V	+	–	?

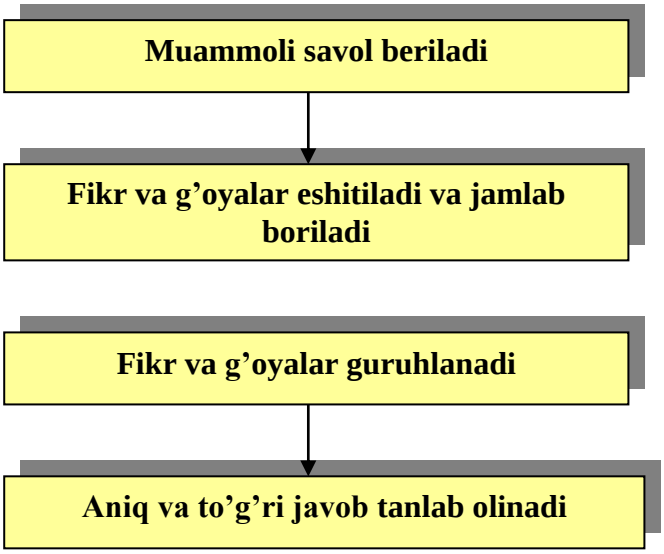
"V"- men bilgan ma'lumotlarga mos;
"-" - men bilgan ma'lumotlarga zid;
"+" - men uchun yangi ma'lumot;
"?" - men uchun tushunarsiz yoki ma'lumotni

6-ilova

"Aqliy hujum" metodini qo'llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g’oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g’oyalar, ular hatto to’g’ri bo’lmasa ham inobatga olinadi.
3. Har bir ta’lim oluvchi qatnashishi shart.

Quyida (1-chizma) “Aqliy hujum” metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. Kriptografiya tushunchasiga ta’rif bering?
2. Kriptografik tizim deb nimaga aytiladi?
3. Kriptobardoshlik deganda nimani tushunasiz?
4. Zamonaviy kriptografiya bo’limlarini sanab o’ting?

Talabalar soni:	____ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1. Kriptotizimlarga qo'yiladigan talablar 2. Kriptografik tizimlarning mutlaqo maxfiyligi.
Dars maqsadi: Talabalarda axborotlarni kriptografik tizimlari tushunchasini hosil qilish	
Pedagog vazifalari:	***O'quv natijalari:***
- Kriptotizimlarga qo'yiladigan talablar bilan tanishtirish va ma'ruzani bayon qilish; - Kriptografik tizimlarning mutlaqo maxfiyligi tushunchasini yoritib berish.	- Kriptotizimlarga qo'yiladigan talablar bilan tanishib chiqadilar va ma'ruzani daftarga yozib oladilar; - Kriptografik tizimlarning mutlaqo maxfiyligi tushunchasini o'zlashtiradilar.
O'qitish usullari	Ma'ruza, blits-so'rov, aqliy xujum
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH
MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1 Kriptotizimlarga qo'yiladigan talablar bilan tanishtiradi va ma'ruzani bayon qiladi. (3-ilova) 2.2. Kriptografik tizimlarning mutlaqo maxfiyligi haqida batafsil ma'lumot beriladi. (4-ilova)	Yozib oladilar E'tibor beradilar, savollar beradilar.
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B. jadvalini to'ldirish beriladi (5 ilova) 3.3. Talabalar bilimini nazorat qilish uchun "Aqliy xujum" metodi qo'llaniladi (6-ilova)	Savollar beradi. Jadvalni to'ldiradilar Savollarga javob berishadi

1-ilova

Mavzu: **AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH**

Mavzu rejasi::	1. Kriptotizimlarga qo’yiladigan talablar 2. Kriptografik tizimlarning mutlaqo maxfiyligi.
Darsning maqsadi: Talabalarda axborotlarni kriptografik tizimlari tushunchasini hosil qilish	

2-ilova

Адабиётлар:

1. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
2. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
3. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001й.
4. Ященко В.В. Введение в криптографию. МЦМО, 2003й.
5. Масленников А. Практическая криптография BHV – 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. . С.К. Ғаниев, М.М. Каримов, К.А. Ташев «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.

3-ilova

Kriptotizimlarga qo’yiladigan talablar

Kriptografik tizimning nazariy bardoshliligi tushunchasi kriptografik tizimlarni baholashga aniqlik kiritadi, lekin bardoshliligi yuqori bo'lgan kriptotizimlarning yaratilishi nuqtai nazardan tushkunlikka olib keladi. Amalda ko'plab hollarda nazariy bardoshli kriptotizimlarning yaratilishi mahfiy kalit hajmining cheksiz katta bo'lib ketishi masalasi bilan bog'liq.

Uzatilayotgan ochiq ma'lumot ko'rinishini almashtirish muammosi aloqa tarmog'ida foydalanuvchilari o'rtasida yechilishi kerak bo'lgan masalaning bir tomoni bo'lsa, ikkinchi tomoni - ma'lumotlar almashuvi amalga oshirilganda uzatilayotgan va qabul qilib olinayotgan ma'lumotlarning hamda foydalanuvchilarning haqiqiyligiga ishonch hosil qilish.

Yuqorida keltirilgan muammolarni yechish uchun quyidagilarni amalga oshirish kerak:

1

-foydalanuvchilar va ma'lumotlarning haqiqiyligini tasdiqlash, tekshirish;

2

-o'zaro muomalaga kirishib ma'lumot almashinuvchi tomonlarning bir-birlariga zarar keltirish yoki aldash maqsadida qasddan qiladigan har-qanday hatti harakatlarini qayd qilishni va oldini olishni ta'minlash zarur.

Mazkur muammolarni yechishda kriptografik usullar oldin bajarilgan har qanday hatti-harakatlarning inkor etilmasligini, yolg'on ma'lumot uzatilganda esa uni aniqlash kabi imkoniyatlarni bera oladi.

Demak, zamonaviy kritpografiya – axborotlarning aloqa tarmog'ida almashinuvi jarayonlarida ularning:

-maxfiyligini (konfidentsialligi ta'minlash);
-to'liqligini (o'zgartirilmagaligini aniqlash);
-autentifikatsiyasi (foydalanuvchilarning haqiqiyligini aniqlash);
-tomonlarning avtorlikni tan olmasligi kabi xolatlarning oldini olishni ta'minlash;
-kalitlarni yaratish, tarqatish va boshqarishni ta'minlash;
kabi masalalarni yechish bilan shug'ullanuvchi bilim sohasi hisoblanadi.

Amalga oshirish usullariga bog'liq bo'lmagan holda axborotni himoyalashning zamonaviy kriptografik tizimlariga quyidagi umumiy talablar qo'yiladi:

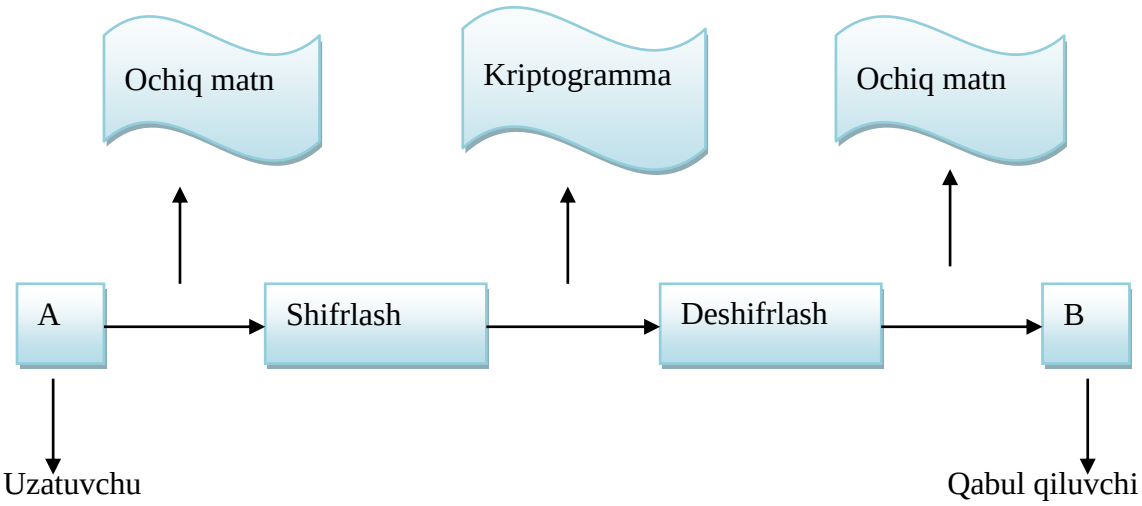
- *shifrlash algoritmini bilish shifrmatn kriptobardoshliligini tushirib yubormasligi lozim. Barcha kriptotizimlar bu talabga javob berishi kerak;*
- *shifrlangan xabarning biror qismi va unga mos ochiq matn asosida kalitni aniqlash uchun zarur bo'lgan amallar soni mumkin bo'lgan umumiy kalitlarga sarflanadigan amallar sonidan kam bo'lmasligi kerak;*
- *shifrlangan matndan ochiq matnni hosil qilish uchun mumkin bo'lgan kalitlar to'plamini to'la ko'rib chiqish amallari soni qat'iy past ko'rsatkichga ega bo'lishi va zamonaviy kompьyuterlar imkoniyatlari chegarasidan chiqib ketishi kerak;*
- *shifrlash algoritmini bilish himoyaga ta'sir qilmasligi kerak;*
- *kalitdagi yoki boshlang'ich ochiq matndagi kichik o'zgarishlar shifrlangan matnni tubdan o'zgartirib yuborishi kerak;*
- *shifrlash algoritmining tarkibiy elementlari o'zgarmas bo'lishi lozim;*
- *shifrlash jarayonida qo'shilgan qo'shimcha bitlar shifrmatnda bir butunligini saqlashi va yetarlicha yashirilgan bo'lishi talab etiladi;*
- *shifrmatn uzunligi ochiq matn uzunligiga teng bo'lishi kerak;*
- *shifrlash jarayonida ketma-ket qo'llaniladigan kalitlar o'rtasida o'zaro oddiy va oson bog'liqlik bo'lmasligi kerak;*
- *mumkin bo'lgan kalitlar to'plamidagi ixtiyoriy kalit, shifrmatnning kriptobardoshliligini ta'minlashi kerak;*
- *algoritm ham dasturiy, ham apparatli realizatsiyaga qulay, va kalit uzunligining o'zgarishi, shifrlash algoritmining sifatini pasaytirmasligi kerak.*

ova

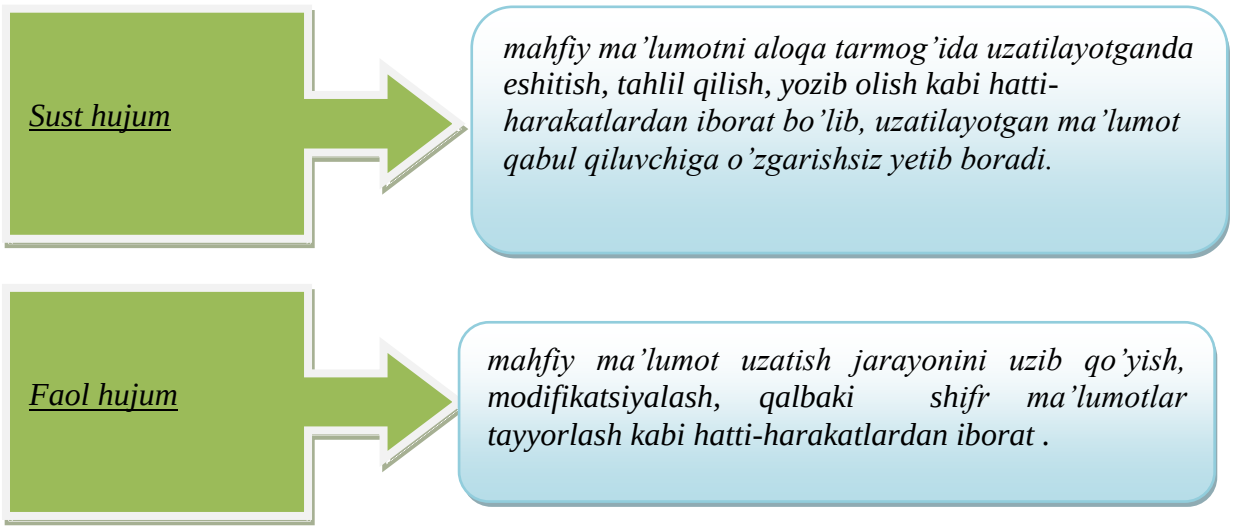
Kriptografik tizimlarning mutlaqo maxfiyligi

Shennon mutlaqo mahfiylik tushunchasining ta'rifini: X - ochiq ma'lumot va Y –shifr ma'lumot statistik bog'liq emas, ya'ni ixtiyoriy ochiq ma'lumot va shifr

Kriptografiyaning ananaviy masalalaridan biri: ochiq aloqa tarmog'i kriptoanalitik tomonidan nazorat qilinganda uzatilayotgan ma'lumotning maxfiyligini ta'minlash hisoblanadi. Eng sodda holda ushbu masala uchta tomonning birgalikdagi ma'lumotlar almashinuvi jaryonidagi hati-harakatlarida namoyon bo'ladi. Ushbu xolatni ifodalovchi umumiy sxema quyidagicha:



Shifrlangan ma'lumotni uzatish jarayonida kriptoanalitik: sust yoki faol hujum turlarini amalga oshiradi.



Faol hujum turlari ***imitatsiyalash*** *deyiladi.*

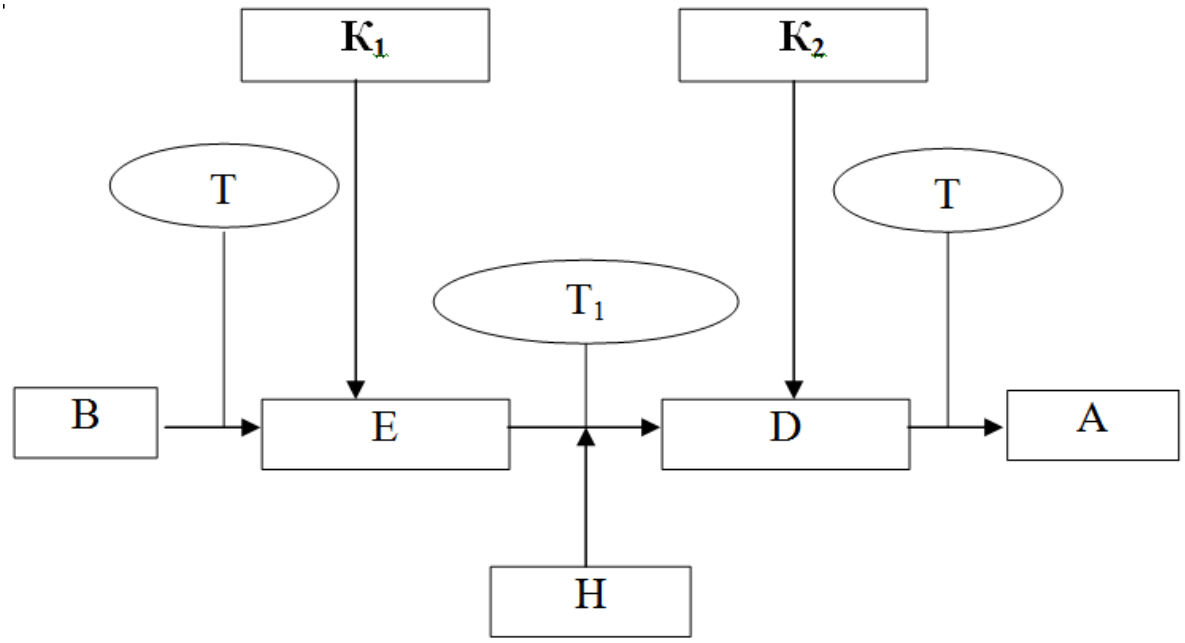
Shifrlash va deshifrlash algoritmlari juftligi kriptotizim yoki shifrtizim deyiladi. Quyidagicha belgilashlar kiritib olamiz:
T - ochiq matn;
T_1- shifr matn (kriptogramma);
E - shifrlash algoritmi;
D - deshifrlash algoritmi;
K_1 – shifrlash kaliti;
K_2 – deshifrlash kaliti.

Ushbu belgilashlarga nisbatan shifrlash va deshifrlash jarayonini quyidagicha tengliklar bilan ifodalash mumkin:
$E_K(T) = T_1$,
$D_K(T_1) = T$,
Bu yerda
$D_K(E_K(T)) = T$
sharti bajarilishi zarur.
Simmetrik kriptotizimlar uchun $k_1 = k_2$ tenglik o'rinli bo'ladi, ya'ni shifrlash va deshifrlash kalitlari bir xilda.
Asimmetrik kriptotizimlarda esa k_1 k_2 bo'lib, k_1 -kalit, k_2 -kalit bilan bog'liq bo'lsada, k_1 -kalitni bilish, k_2 -kalitni topish imkonini bermaydi. Shuningdek, k_1 - ochiq kalit, k_2 - esa yopiq kalit deb ham yuritiladi.

simmetrik kriptotizimlar

Uzlukli tizimda ochiq matnning har bir harf yoki simvoli alohida shifrlanadi.

Blokli tizimda esa ochiq matnni biror fiksirlangan uzunliklarga teng bo'linib chiqib, ushbu uzunliklar bo'yicha shifrlash amalga oshiriladi.



Bu yerda,

K_1– ochiq kalit;

K_2- yopiq kalit;

T – ochik matn(shifrlanishi kerak bo'lgan maьlumot);

E - shifrlash algoritmi;

D- deshifrlash algoritmi;

T_1 – shifrmatn;

H – yovuz niyatli shaxs;

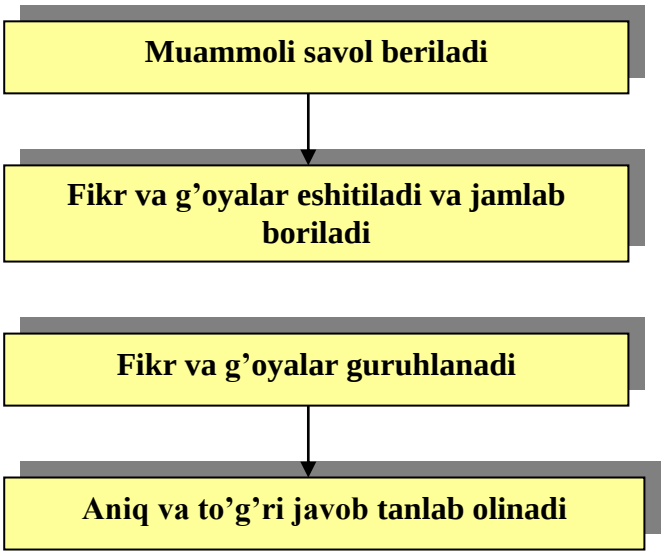
5-ilova

"Aqliy hujum" metodini qo'llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g'oyalar muhokama qilinmaydi va baholanmaydi.

2. Bildirilgan har qanday fikr-g’oyalar, ular hatto to’g’ri bo’lmasa ham inobatga olinadi.
3. Har bir ta’lim oluvchi qatnashishi shart.

Quyida (1-chizma) “Aqliy hujum” metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. *Kriptografiya nima?*
2. *Kriptografiya rivojlanishining qanday bosqichlari mavjud?*
3. *Zamonaviy kriptografiya qanaqa muammolarni hal etuvchi bilim sohasi hisoblanadi?*
4. *Axborotlarni sodda shifrlashni qanday usullari bor?*
5. *Sezarning shifrlash usuli qanday amalga oshiriladi?*

Talabalar soni:	___ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1. Shifrlash algoritmlarining klassifikatsiyasi; 2. O'rniga qo'yish shifrlash algoritmlari; 3. Bir qiymatli va ko'p qiymatli o'rniga qo'yish shifrlash algoritmlari;
Dars maqsadi: Talabalarda simmetrik (maxfiy) kalitli shifrlash sistemasi tushunchasini hosil qilish	
Pedagog vazifalari:	***O'quv natijalari:***
- Shifrlash algoritmlarining klassifikatsiyasi bilan tanishtirish va ma'ruzani bayon qilish; - O'rniga qo'yish shifrlash algoritmlari tushunchasini yoritib berish; - Bir qiymatli va ko'p qiymatli o'rniga qo'yish shifrlash algoritmlarini tushuntirib berish;	- Shifrlash algoritmlarining klassifikatsiyasi bilan tanishib chiqadilar va daftarga yozib oladilar; - O'rniga qo'yish shifrlash algoritmlari tushunchasini o'zlashtiradilar va yozib oladilar; - Bir qiymatli va ko'p qiymatli o'rniga qo'yish shifrlash algoritmlarini o'rganadilar;
O'qitish usullari	Ma'ruza, B.BX.B metodi,"Aqliy xujum" metodi
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH
MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1 Shifrlash algoritmlarining klassifikatsiyasi bilan tanishtiradi va ma'ruzani bayon qiladi. (3-ilova) 2.2. O'rniga qo'yish shifrlash algoritmlari haqida batafsil ma'lumot beriladi. (4-ilova) 2.3. Bir qiymatli va ko'p qiymatli o'rniga qo'yish shifrlash algoritmlari ko'rsatiladi. (5-ilova)	Yozib oladilar Tinglaydilar va yozib oladilar E'tibor beradilar, savollar beradilar va yozib oladilar.
3-bosqich. Yakunlovchi qism.	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi.	Savollar beradi.

(10 min)	3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B. jadvalini to'ldirish beriladi (6- ilova) 3.3. Talabalar bilimini nazorat qilish uchun "Aqliy xujum" metodi qo'llaniladi (7-ilova)	Jadvalni to'ldiradilar Savollarga javob berishadi

1-ilova

Mavzu: **AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH**

Mavzu rejasi::	1. Shifrlash algoritmlarining klassifikatsiyasi; 2. O'rniga qo'yish shifrlash algoritmlari; 3. Bir qiymatli va ko'p qiymatli o'rniga qo'yish shifrlash algoritmlari;
Darsning maqsadi: Talabalarda simmetrik (maxfiy) kalitli shifrlash sistemasi tushunchasini hosil qilish	

2-ilova

Адабиётлар:

1. С.К. Ғаниев, М.М. Каримов, К.А. Ташев «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.
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. Ященко В.В. Введение в криптографию. МЦМО, 2003й.
6. Масленников А. Практическая криптография BHV – СПб 2003й.

3-ilova

Shifrlash jarayonida ochiq ma'lumot alfaviti belgilari shifr ma'lumot alfaviti belgilariga almashtirilsa, bunday akslantirishga asoslangan shifrlash algoritmi **o'rniga qo'yish shifrlash** sinfiga kiradi.

Agar shifrlash jarayonida ochiq ma'lumot alfaviti belgilarining o'rinlari almashtirilsa, bunday shifrlash algoritmi **o'rin almashtirish shifrlash** sinfiga kiradi.

O’rniga qo’yish shifrlash algoritmlarida shifrma’lumotni tashkil etuvchi alfavit belgilari ma’nosi ochiq ma’lumotni tashkil etuvchi alfavit belgilarining ma’nosi bilan bir xil bo’lmaydi. SHifrlash jarayonida o’rniga qo’yish va o’rin almashtirish akslantirishlarining kombinatsiyalaridan birgalikda foydalanilsa, bunday shifrlash algoritmi kompozitsion shifrlash turkumiga kiradi. Demak, shifrlash algoritmlari akslantirish turlariga qarab o’rniga qo’yish, o’rin almashtirish va kompozitsion shifrlash sinfiga bo’linadi.

Tabiiy ravishda, o’rniga qo’yish shifrlash algoritmlari bir qiymatli va ko’p qiymatli shifrlash sinfiga bo’linadi. Bir qiymatli shifrlash algoritmlarida ochiq ma’lumot alfaviti belgilarining har biriga shifr ma’lumot alfavitining bitta belgisi mos qo’yiladi. Ko’p qiymatli shifrlash algoritmlarida ochiq ma’lumot alfaviti belgilarining har biriga shifr ma’lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo’yiladi, ya’ni ochiq ma’lumot alfavitining biror x_i belgisiga shifr ma’lumot alfavitining chekli $\{y_{i1}, y_{i2}, \ldots, y_{it}\}$ to’plamdan olingan biror y_{it}, $(1 \le j \le t)$, belgisi mos qo’yiladi.

Shifrlash algoritmlari, kalitlardan foydalanish turlariga ko’ra, simmetrik va asimmetrik sinflarga bo’linadi. Agar shifrlash va deshifrlash jarayonlari bir xil kalit bilan amalga oshirilsa, bunday shifrlash algoritmi simmetrik shifrlash algoritmi sinfiga kiradi. Agar shifrlash jarayoni biror k_1 kalit bilan amalga oshirilib, deshifrlash jarayoni $k_2 \neq k_1$ bo’lgan k_2 kalit bilan amalga oshirilib, k_1 kalitni bilgan holda k_2 kalitni topish yechilishi murakkab bo’lgan masala bilan bog’liq bo’lsa, bunday shifrlash algoritmi asimmetrik shifrlash algoritmi sinfiga taaluqli bo’ladi

Shifrlash jarayoni ochiq ma’lumotni ifodalovchi elementar (masalan: bit, yarim bayt, besh bit, bayt) belgilarni shifrma’lumotni ifodalovchi elementar belgilarga akslantirish asosida amalga oshirilsa, bunday shifrlash algoritmi uzluksiz(oqimli) shifrlash sinf turkumiga kiradi.
Shifrlash jarayoni ochiq ma’lumot alfaviti belgilarining ikki va undan ortiq chekli sondagi birikmalarini shifrma’lumot alfaviti belgilarining birikmalariga akslantirishga asoslangan bo’lsa, bunday shifrlash algoritmi blokli shifrlash sinfiga kiradi.

Shifrlash jarayonida ochiq ma’lumot alfavitining biror alohida olingan a_i belgisi har doim shifr ma’lumot alfavitining biror fiksirlangan b_j belgisiga almashtirilsa, bunday shifrlash algoritmi bir alfavitli shifrlash sinfiga kiradi. Agar shifrlash jarayoning har xil bosqichlarida ochiq ma’lumot alfavitining biror alohida olingan a_i belgisi shifrma’lumot alfavitining har xil b_j, b_l, ..., b_t belgilariga almashtirilsa, bunday shifrlash algoritmi ko’p alfavitli shifrlash sinfiga kiradi.

Shifrlash jaryonida ochiq ma’lumot alfaviti belgilari yoki alfavit belgilari birikmalari biror amal bajarish bilan shifr ma’lumot alfaviti belgilari yoki ularning birikmalariga almashtirilsa, bunday shifrlash algoritmi gammalashtirilgan shifrlash sinfiga kiradi.

4-ilova

Shifrlash algoritmlari ochiq ma’lumot alfaviti belgilarini shifr ma’lumot belgilariga akslantirishdan iborat ekanligi takidlandi. Akslantirishlar funktsiyalari (kalit deb ataluvchi noma’lum) parametrga bog’liq holda: jadval va analitik ifoda ko’rinishlarida berilishi mumkin. O’rniga qo’yish shifrlash algoritmlarining dastlabki namunalari bo’lgan tarixiy shifrlash algoritmlarining deyarli hammasi jadval ko’rinishida ifodalanadi**.**

Kirilcha alfavit belgilari soni 32 ta, shu 32 ta har xil belgilarni bitlar bilan ifodalash uchun besh bit kifoya, ya’ni $2^5=32$. Keltirilgan jadvaldan foydalanib, kirillcha alfavitda ifodalangan ochiq ma’lumot belgilarni ularga mos keluvchi ikkilik sanoq sistemasidagi besh bitlik belgilarga almashtirib shifr ma’lumot hosil qilinadi, ya’ni $x_i^j \in \{0,1\}$. Agarda, keltirilgan jadvalda ochiq ma’lumot alfaviti belgilariga shifr ma’lumot alfavitining besh bitlik belgitlari mos qo’yilganligi noma’lum bo’lsa, bu jadval kalit bo’lib, shifr ma’lumotdan ochiq ma’lumotni tiklash masalasi murakkablashadi. Bunday shifrlash jarayonini ifodalovchi algoritmning kalitlarining umumiy soni 32! bo’lib, ushbu $n!\approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ - Stirling formulasiga ko’ra quyidagicha $32!= \left(\frac{32}{2,7}\right)^{32} \sqrt{2\cdot 3,14\cdot 32} > \left(\frac{32}{4}\right)^{32} \sqrt{2\cdot 2\cdot 32} > \left(\frac{32}{4}\right)^{32} \sqrt{2\cdot 2\cdot 32} = 2^{96}\cdot 2^3\cdot\sqrt{2} > 2^{99}$ hisoblanadi. Bunday xolat esa kalitni bilmagan holda deshifrlash jarayonini amalga oshirishni jiddiy murakkablashtiradi.

Agarda ochiq ma’lumot kompyuterdan foydalanilgan holda tuzilib, standart ASCII kodi alfaviti belgilarini birini boshqasi bilan almashtirishdan iborat bo’lgan o’rniga qo’yish shifrlash algoritmini qo’llash natijasida hosil qilingan bo’lsa, u xolda shifrlash jarayoni asosini quyidagi o’rniga qo’yish almashtirish jadvali tashkil etadi:

Ochiq ma’lumot alfaviti (standart ASCII kodi belgilari)	ASCII	ASCII	....	....	ASCII
Shifr ma’lumot alfaviti (ikkilik sanoq sistemasi belgilari)	$x_0^0, x_1^0, ..., x_7^0$	$x_0^1, x_1^1, ..., x_7^1$			$x_0^{255}, x_1^{255}, ..., x_7^{255}$

bu yerda $x_i^j \in \{0,1\}$ bo’lib, standart ASCII kodi alfaviti belgilarini 256 ta har xil belgilarini bitlar bilan ifodalash uchun 8 bit kifoya, ya’ni $2^8=256$.

Bu shifrlash jarayonini ifodalovchi algoritm kalitlarning umumiy soni 256! bo’lib, ushbu $n!\approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ - Stirling formulasiga ko’ra quyidagicha $256!= \left(\frac{256}{2,7}\right)^{256} \sqrt{2\cdot 3,14\cdot 256} > \left(\frac{256}{4}\right)^{256} \sqrt{2\cdot 2\cdot 256} > \left(\frac{4\cdot 2^6}{4}\right)^{256} \sqrt{2\cdot 2\cdot 256} >$

Shifr ma’lumot alfaviti belgilarini: $y_1,y_2,\ldots,y_M$ deb belgilansa, u holda bir qiymatli o’rniga qo’yish shifrlash algoritmining umumiy holdagi modeli jadval ko’rinishda quyidagicha ifodalanadi:

Ochiq ma’lumot alfaviti belgilari		x_2	...	...	x_N
Shifr ma’lumot alfaviti		y_{i2}	...	...	y_{iN}

bu yerda $y_{ij} \in \{y_1,y_2,\ldots,y_M\}$.

Misol sifatida quyidagi (2x26)-o’lchamli jadvalni keltirish mumkin:

Ochiq ma’lumot alfaviti (lotincha belgilar)	A	B	...	...	Z
Shifr ma’lumot alfaviti (kirilcha belgilar)	И	Л	...	...	У

5-ilova

O’rniga qo’ E’tibor beradilar, savollar beradilar va yozib oladilar.*yish shifrlash algoritmlari, ularning asosini tashkil etuvchi akslantirishning bir qiymatli yoki ko’p qiymatliligiga ko’ra, bir qiymatli va ko’p qiymatli sinflarga bo’linadi.*

Agar o’rniga qo’yish shifrlash algoritmida ochiq ma’lumot alfaviti belgilarining har biriga shifr ma’lumot alfavitining bitta belgisi mos qo’yilsa, bunday algoritm bir qiymatli o’rniga qo’yish shifrlash algoritmi sinfiga kiradi. Ochiq ma’lumot alfaviti belgilari $x_1,x_2,\ldots,x_N$ deb belgilansa, masalan lotin alfaviti belgilari uchun N=26, kirill alfaviti belgilari uchun N=32, standart ASCII kodi alfaviti belgilari

Ko’p qiymatli shifrlash algoritmlarida ochiq ma’lumot alfaviti belgilarning har biriga shifr ma’lumot alfavitining ikki yoki undan ortiq chekli sondagi belgilari mos qo’yiladi, ya’ni ochiq ma’lumot alfavitining biror x_i belgisiga shifr ma’lumot alfavitining chekli $\{y_{i1}, y_{i2}, \ldots, y_{it}\} \grave{I} \{y_1, y_2, \ldots, y_M\}$to’plamdan olingan biror y_{ij} $(1 \le j \le t)$, belgisi mos qo’yiladi. Ko’p qiymatli o’rniga qo’yish shifrlash algoritmining umumiy holdagi modeli ko’rinishida quyidagicha ifodalanadi:

Ochiq ma’lumot alfaviti belgilari	x_1	x_2	…	x_N
Shifr ma’lumot alfaviti	$y_{i11}, y_{i21,\ldots}, y_{it1}$	$y_{i12}, y_{i22,\ldots}, y_{ir2}$	…	$y_{i12}, y_{i22,\ldots}, y_{ipN}$

bu yerda $y_{ild} \in \{y_1, y_2, \ldots, y_M\}$

Shunday qilib, ko’p alfavitli o’rniga qo’yish shifrlash algoritmining umumiy holdagi modeli jadval ko’rinishida quyidagicha ifodalanadi:

Ochiq ma’lumot alfaviti belgilari	x_1	x_2	…	…	x_N
Shifr ma’lumot alfaviti	y_{i1}^1	y_{i2}^1	…	…	y_{iN}^1
Shifr ma’lumot alfaviti	y_{i1}^2	y_{i2}^2	…	…	y_{iN}^2
…..	…	…	…	…	…
Shifr ma’lumot alfaviti	y_{i1}^w	y^w_{i2}	…	…	y_{iN}^w

bu yerda $y_i^d \in \{y_1, y_2, \ldots, y_M\}$

6-ilova

B	BX	B
…….	……..	……..

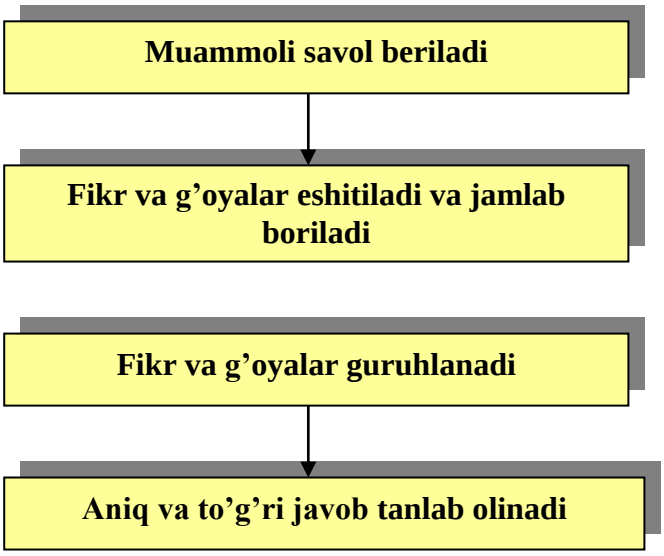
7-ilova

“Aqliy hujum” metodini qo’llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g’oyalar muhokama qilinmaydi va baholanmaydi.

2. Bildirilgan har qanday fikr-g’oyalar, ular hatto to’g’ri bo’lmasa ham inobatga olinadi.
3. Har bir ta’lim oluvchi qatnashishi shart.

Quyida (1-chizma) “Aqliy hujum” metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. *Vijinerning shifrlash tizimi nima?*
2. *Kalit deganda nima tushuniladi?*
3. *Simmetrik shifrlash qanday amalga oshiriladi?*
4. *Asimmetrik shifrlash nima?*
5. *Simmetrik va asimmetrik kalit yordamida shifrlash qanday amalga oshiriladi?*

MAVZU № 5 (4 soat)

VIRUS VA ANTIVIRUSLAR
MA'RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	___ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1.Kompyuter virusi tushunchasi; 2. Kompyuter viruslarining klassifikatsiyasi.
Dars maqsadi: Talabalarda kompyuter viruslari haqida tushunchasini hosil qilish	
Pedagog vazifalari:	***O'quv natijalari:***
- Kompyuter virusi tushunchasi bilan tanishtirish va ma'ruzani bayon qilish; - Kompyuter viruslarining klassifikatsiyasi tushunchasini yoritib berish.	- Kompyuter virusi tushunchasi bilan tanishib chiqadilar va ma'ruzani daftarga yozib oladilar; - Kompyuter viruslarining klassifikatsiyasi haqida ma'lumot olishadi.
O'qitish usullari	Ma'ruza, "Aqliy xujum" metodi
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

VIRUS VA ANTIVIRUSLAR
MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1 Komputer virusi tushunchasi bilan tanishtiradi va ma'ruzani bayon qiladilar. (3-ilova) 2.2. Komputer viruslarining klassifikatsiyasi haqida batafsil ma'lumot beriladi. (4-ilova)	Yo zib oladilar Tinglaydilar va yozib oladilar
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. "Aqliy xujum" metodi (6- ilova)	Savollar beradi. Savollarga javob beradilar

1-ilova

Mavzu: **VIRUS VA ANTIVIRUSLAR**

Mavzu rejasi::	1.Kompyuter virusi tushunchasi; 2. Kompyuter viruslarining klassifikatsiyasi.
Darsning maqsadi: Talabalarda kompyuter viruslari haqida tushunchasini hosil qilish	

2-ilova

Адабиётлар:

1. Karimov I.M. va boshqalar. Axborot texnologiyalari: Darslik. – T.,2011.
2. Муҳаммадиев Ж.Ў. Ахборот хавфсизлиги: муаммо ва ечимлар: Монография. – Т., 2011.
3. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
5. С.К. Ғаниев, М.М. Каримов, К.А. Ташев «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет
6. Мельников В.П. и др. Информационная безопасность и защита информации: Учебое пособие. – М., 2008.

3-ilova

Zararkunanda dasturlar va avvalo, viruslar komputer tizimsi uchun jiddiy xavf xisoblanadi. Bu xavfni nazar pisand kilmaslik foydalanuvchilar axborotsi uchun jiddiy okibatlarga sabab bulishi mumkin. Viruslarning xavfini xaddan tashkari oshirib yuborish xam kompyuter tizimlarining barcha imkoniyatlaridan foydalanishga salbiy ta’sir kursatadi. Viruslar ta’siri mexanizmini, ular bilan kurashish metodlarini bilish viruslarga karshi samarali kurashishni tashkil etishga, ular ta’siri natijasida zararlanish extimolini va yukotishlarni minimumga keltirishga imkon beradi.

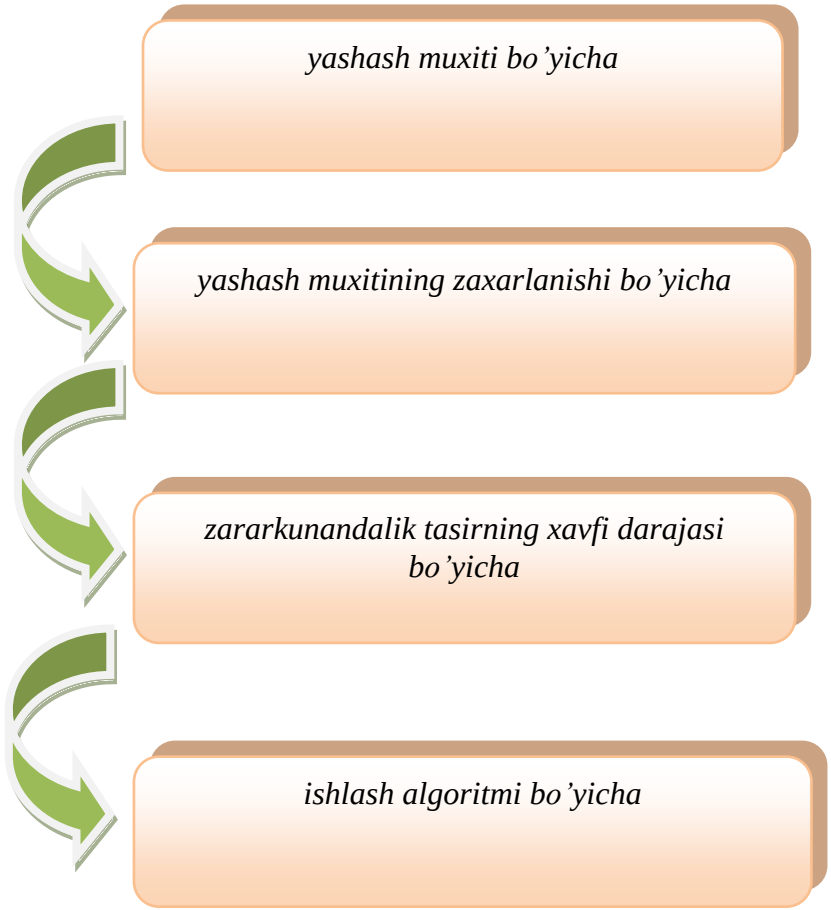
«Kompyuter virusi» atamasi 80-yillarning o’rtalarida kiritilgan. Biologik viruslarga tegishli ulchamlarining kichikligi, uz-uzidan kupayib va obьektlarga singib (ularni zaxarlab) tez tarqalish qobiliyati, tizimga salbiy taьsiri kabi alomatlar zararkunanda programmalarga xam taallualidir.

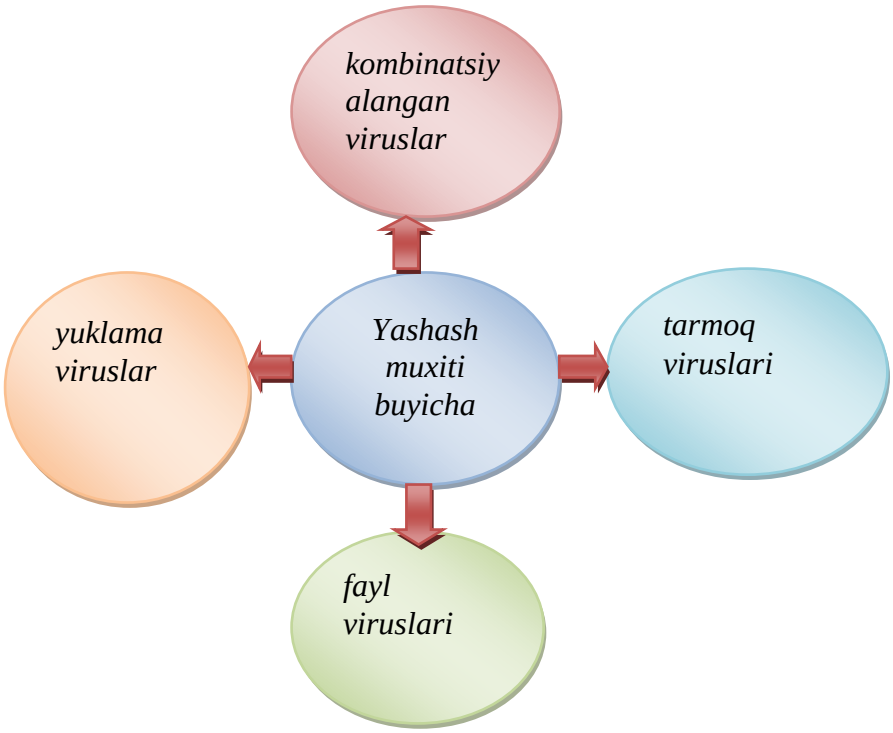
Kompyuter viruslari bilan ish kurilganda «virus» atamasi bilan bir qatorda «zaxarlanish», «yashash muxiti», «profilaktika» kabi tibbiyot atamalaridan xam foydalaniladi.

Xozirda dunyoda faqat ruyxatga olingan 65 mingdan ortiq komputer viruslari mavjud. Zamonaviy zarakunanda programmalarining aksariyati uz-uzidan kupayish qobiliyatiga ega bulganliklari sababli ularni xam komputer viruslariga taalluqli deb xisoblaydilar.

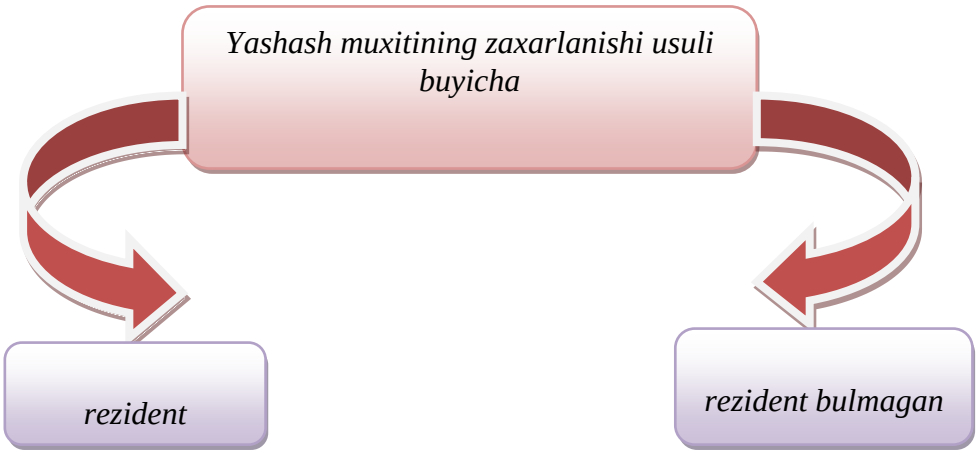
4-ilova

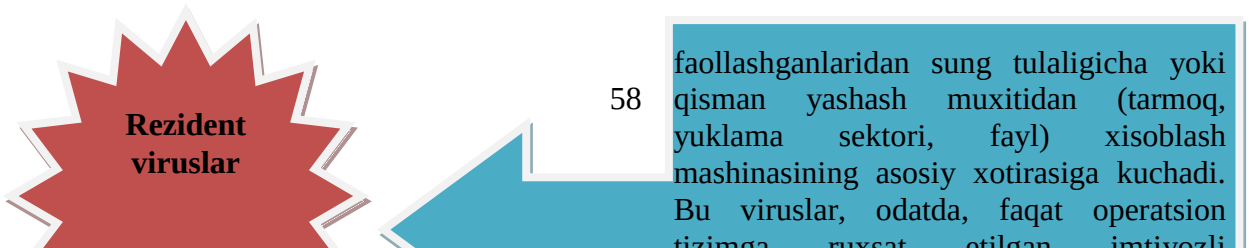
Barcha komputer viruslari quyidagi alomatlari buyicha klassifikatsiyalanishi mumkin:





Tarmoq viruslarning yashash muxiti komputer tarmoqlarining elementlaridir. Fayl viruslar bajariluvchi fayllarda joylashadi. Fayl viruslar ichida makroviruslar aloxida urin tutadi. Makroviruslar-makrotillarda yozilgan zararkunanda prgrammalar, elektron jadvallar va x. Yuklama viruslar tashqi xotira qurilmalarining yuklama sektorlarida (boot-sektorlarda) buladi. Kombinatsiyalangan viruslar bir necha yashash muxitida joylashgan buladi. Misol tariqasida yuklama fayl viruslarni kursatish mumkin.





Virusning zararkunandalik imkoniyatlari ularni yaratuvchisining maqsadi va malakasiga xamda komputer tizimlarining xususiyatlariga bogliq.

Foydalanuvchining informatsion resurslari uchun xavf darajasi buyicha komputer viruslarini quyidagilarga ajratish mumkin: beziyon viruslar; xavfli viruslar; juda xavfli viruslar;

Beziyon *kompyuter viruslari kompьyuter tizimsi resurslariga qandaydir shikast yetkazishni uziga maqsad qilmagan mualliflar tomonidan yaratiladi. Ularning maqsadi, odatda, uzlarini programmist imkoniyatlarini kuz-kuz qilishdir. Bunday viruslarning zararkunandaligi monotoringda aybsiz matnlarni va rasmlarni, musiqiy parchalarning ijro etilishiga olib keladi va x.*

Ammo bezarar bulib kuringan bunday viruslar kompyuter tizimlariga malum shikast yetkazadi. Birinchidan bunday viruslar kompyuter tizimlarini resurslarini sarflaydi, natijada uning ishlash samaradorligi pasayadi. Ikkinchidan, kompyuter viruslarida kompyuter tizimlarining informatsion resurslariga shikast keltiruvchi xatoliklar bo'lishi mumkin.

Xavfli *viruslarga kompyuter tizimlarining samaradorligini jiddiy pasayishiga olib keluvchi, ammo xotirlovchi qurilmalarda saqlanuvchi axborotning yaxlitligini va maxfiyligini buzmaydigan viruslar kiradi. Bunday viruslar ta'siri*

Juda xavfli *viruslarga axborotning maxfiyligini buzilishiga, yuq qilinishiga, qaytarilmaydigan turlanishga (shifrlash xam shu qatorda) xamda axborotdan foydalanishga tusqinlik tsiluvchi va natijada apparat vositalarning ishdan chiqishiga va foydalanuvchilar sogligiga shikast yetishiga sabab buluvchi viruslar kiradi.*

Ishlash algoritmining xususiyatlari buyicha viruslarni ikkita sinfga ajratish mumkin.

tarqalishida yashash makonini uzgartirmaydigan tarqalishida

yashash makonini uzgartiradigan.

Yashash makonini uzgartirmaydigan viruslar uz navbatida ikkita guruxga ajratilishi mumkin.

- viruslar-«yuldoshlar» (companion),
- viruslar-«qurtlar» (worm).

Viruslar-«yuldoshlar» fayllarni uzgartirmaydi. Uning taьsir mexanizmi bajariluvchi fayllarning nusxalarini yaratishdan iboratdir.

Viruslar-«qurtlar» tarmoq orqali ishchi stantsiyaga tushadi, tarmoqning boshqa abonentlari buyicha virusni junatish adreslarini xisoblaydi va virusni uzatishni bajaradi. Virus fayllarni uzgartirmaydi va disklarning yuklama sektorlariga yozilmaydi. Baьzi bir viruslar-«qurtlar» diskda virusning ishchi nusxasini yaratadi, boshqalari faqat xisoblash mashinasining asosiy xotirasida joylashadi.

Algoritmlarning murakkabligi, mukammalik darajasi va yashirinish xususiyatlari buyicha yashash makonini uzgartiradigan viruslar quyidagilarga bulinadi:

1. talaba viruslar;

2. «stels» viruslar (kurinmaydigan viruslar);

3. polimorf viruslar.

Talaba-viruslar malakasi past yaratuvchilar tomonidan yaratiladi. Bunday viruslar, odatda, rezident bulmagan viruslar qatoriga kiradi, ularda kupincha xatoliklar mavjud buladi, osongina taniladi va yuqotiladi.

«Stels» viruslar malakali mutaxasislar tomonidan yaryatiladi. «Stels»-viruslar operatsion tizimning shikastlangan fayllarga murojaatlarini ushlab qolish yuli bilan uzini yashash makonidagiligini yashiradi va operatsion tizimni axborotning shikastlanmagan qismiga yunaltiradi. Virus rezident xisoblanadi, operatsion tizim programmalari ostida yashirinadi, xotirada joyini uzgartirishi mumkin. «Stels» -viruslar rezident antivirus vositalariga qarshi taьsir kursata olish qobiliyatiga ega.

Polimorf viruslar xam malakali mutaxasislar tomonidan yaratiladi, va doimiy tanituvchi guruxlar-signaturalarga ega bulmaydi. Oddiy viruslar yashash makonining zaxarlanganligini aniqlash uchun zaxarlangan obьektga maxsus tanituvchi ikkili ketma-ketlikni yoki simvollar ketma-ketligini (signaturani) joylashtiradi. Bu ketma-ketlik fayl yoki sektorning zaxarlanganligini aniqlaydi. Polimorf viruslar virus tanasini shifrlashdan va shifrlash programmasini turlantirishdan foydalanadi. Bunday uzgartirish evaziga polimorf viruslarda kodlarning muvofiqligi bulmaydi.

Ma’lum viruslar bilan ishlashda kulaylikni ta’minlash maksadida viruslar katalogidan foydalaniladi. Katalogda viruslarning kuyidagi standart xususiyatlari tugrisidagi ma’lumot joylashtiriladi: nomi, uzunligi, zaxarlanuvchi fayllar, fayldagi urni, zaxarlash usuli, rezident viruslar uchun asosiy xotiraga joylashtirish usuli, kelib chikaradigan natijalari, zarakunandalik vazifalarining borligi (yuk-ligi) va xatoliklar. Kataloglarning mavjudligi viruslarni tavsiflashda ularning standart xususiyatlari va ta’sirlarini tushirib koldirib, fakat uziga xos xususiyatlarini kursatishga imkon beradi.

5-ilova

Aqliy xujum savollari:

1. Komputer viruslari kanday alomatlari buyicha klassifikatsiyalanadi?
2. Fayl virusi va uning ta’siri algoritmini tushuntiring.
3. Makrovirus va yuklama viruslar ta’siri algoritmi qanday?
4. Viruslarni aniqlash metodlari.
5. Viruslar ta’siri oqibatlarini yo’qotish metodlari.

VIRUS VA ANTIVIRUSLAR
MA'RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	___ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1.Komputer viruslari bilan kurashish metodlari; 2. Viruslar bilan kurashish vositalari. Antivirus dasturlar
Dars maqsadi: Talabalarda komputer viruslari bilan kurashish metodlari hamda antivirus dasturlar haqida tushunchani hosil qilish	
Pedagog vazifalari:	***O'quv natijalari:***
- Komputer viruslari bilan kurashish metodlarini keltirish va ma'ruzani bayon qilish; - Viruslar bilan kurashish vositalari. Antivirus dasturlar bilan tanishtirish.	- Komputer viruslari bilan kurashish metodlarini o'rganadilar va daftarga yozib oladilar; - Viruslar bilan kurashish vositalari. Antivirus dasturlar haqida ma'lumot olishadi va yozib olishadi.
O'qitish usullari	Ma'ruza, klaster metodi, "Aqliy xujum" metodi
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

VIRUS VA ANTIVIRUSLAR
MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1 Komputer viruslari bilan kurashish metodlarini batafsil bayon etadi va ma'ruzani bayon qiladi. (3-ilova) 2.2. Viruslar bilan kurashish vositalari. Antivirus dasturlar haqida batafsil ma'lumot beriladi. (4-ilova)	Yozib oladilar Tinglaydilar va yozib oladilar
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. "Aqliy xujum" metodi (6- ilova)	Savollar beradi. Savollarga javob beradilar

1-ilova

Mavzu: **VIRUS VA ANTIVIRUSLAR**

Mavzu rejasi::	1.Komputer viruslari bilan kurashish metodlari; 2. Viruslar bilan kurashish vositalari. Antivirus dasturlar
Darsning maqsadi: Talabalarda komputer viruslari bilan kurashish metodlari hamda antivirus dasturlar haqida tushunchani hosil qilish	

2-ilova

Адабиётлар:

1. Безбогов А.А. Методы и средства защиты компьютерной информации. Учебное пособие. – Тамбов, 2006.
2. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
3. С.К. Ғаниев, М.М. Каримов, К.А. Ташев «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет
4. Мельников В.П. и др. Информационная безопасность и защита информации: Учебое пособие. – М., 2008.
5. Karimov I.M. va boshqalar. Axborot texnologiyalari: Darslik. – T.,2011.
6. Муҳаммадиев Ж.Ў. Ахборот хавфсизлиги: муаммо ва ечимлар: Монография. – Т., 2011.

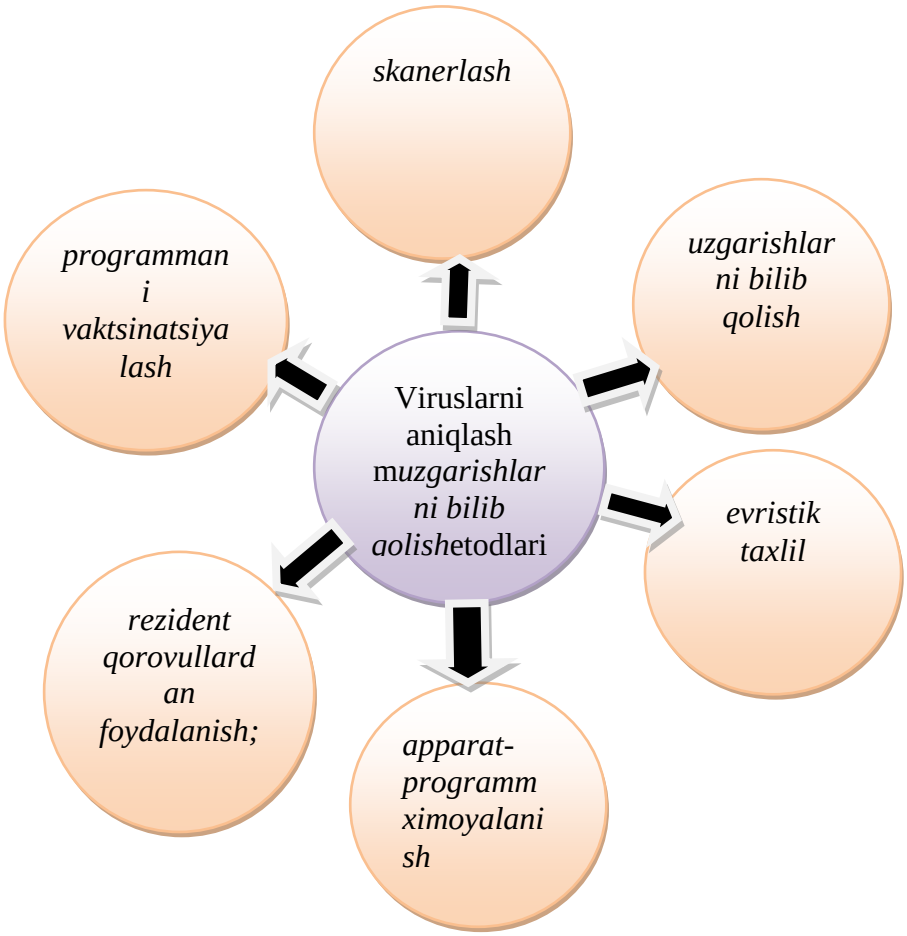
3-ilova

Viruslar tarqalishining ommalashuvi, ular ta’siri oqibatlarining jiddiyligi virusga qarshi maxsus vositalarni va ularni qullash metodlarini yaratish zaruriyatini tugdirdi. Virusga qarshi vositalar yordamida quyidagi masalalar yechiladi:

1. komputer tizimlarida viruslarni aniqlash;

2. viruslar ta’siri oqibatlarini yuqotish.

Viruslarni aniqlashni ularning ta’siri boshlanishi bilanoq yoki, loaqal, zararkunandalik vazifalari boshlanmasdanoq amalga oshirish maqsadga muvofiq xisoblanadi. Ta’kidlash lozimki, barcha xil viruslarning aniqlanishini kafolatlovchi virusga qarshi vositalar mavjud emas.



Skanerlash - viruslarni aniqlashning eng oddiy metodlaridan xisoblanadi. Skanerlash programma-skaner tomonidan amalga oshiriladi. Bu programma-skaner viruslarning tanituvchi qismini-signaturani qidirish maqsadida fayllarni kurib chiqadi. Kupincha programma-skanerlar aniqlangan viruslarni yuqotishi mumkin. Bunday programmalar polifaglar deb ataladi. Skanerlash usuli signaturalari ajratilgan va doimiy bulgan viruslarni aniqlashda qullaniladi.

Uzgarishlarni bilib qolish usuli programm-taf-tishchidan foydalanishga asoslangan. Bunday programmalar odatda virus joylashadigan diskning barcha qismlari xarakteristikalarini aniqlaydi va eslab qoladi. Programma-taf-tishchining davriy bajarilishi jarayonida saqlanuvchi xarakteristikalari bilan disk qismlarini nazoratlash natijasidagi xarakteristikalar taqqoslanadi. Taftish natijasida programma viruslar borligi xususida taxminga asoslangan axborotni beradi.

Metodning eng asosiy afzalligi- viruslarning barcha xilini xamda noma’lum viruslarni aniqlashi imkoniyatidir.

Evristik taxlil usuli xam uzgarishlarni bilib olish metodlari kabi noma’lum viruslarni aniqlash imkonini beradi. Ammo bu metod fayl tizimsi xususidagi axborotni oldindan yizish, ishlash va saqlashni talab etmaydi. Evristik taxlilning moxiyati-viruslarning mumkin bulgan yashash makonlarini tekshirish va ulardagi viruslarga xarakterli komandalarni (komandalar guruxini) aniqlashdan iboratdir.

Rezident qorovullaridan foydalanuvchi usuli xisoblash mashinasining asosiy xotirasida doimo saqlanuvchi va boshqa programmalar xarakatini kuzatuvchi programmalarga asoslangan. Bu metodning, jiddiy kamchiligi sifatida yolgon-dakam trevogalar foizining kupligidir.

Programmani vakqinatsiyalash deganda uning yaxlitligini nazorat qilish maqsadida maxsus modulning yaratilishi tushuniladi. Fayl yaxlitligining xarakteristikasi sifatida odatda nazorat yigindisidan foydalaniladi. Vaktsinatsiyalangan faylning zaxarlanishi sodir bulsa nazorat moduli nazorat yigindisining uzgarishini aniqlaydi va bu xususida foydalanuvchini ogoxlantiradi.

Viruslarga qarshi apparat-programm vositalardan foydalanish usuli viruslardan ximoyalanishning eng ishonchli usuli xisoblanadi. X,ozirda shaxsiy komputerlarni ximoyalashda maxsus kontrollerlar va ularning programm ta'minotidan foydalaniladi. Kontroller umumiy shinadan foydalana oladi va shu sababli disk tizimsiga bulgan barcha murojaatlarni nazorat qiloladi. Kontrollerning programm ta'minotida ishlashning oddiy rejimida diskning uzgartiri-lishi mumkin bulmagan qismlari xotirlanadi.

Viruslarga qarshi apparat-programm vositalar quyidagi afzalliklarga ega: doimo ishlaydi;

ta'sir mexanizmidan qat'iy nazar barcha viruslarni aniqlaydi; virus ta'siri yoki malakasiz foydalanuvchi ishi natijasidagi ruxsatsiz xarakatlarni tuxtadi. Bu vositalarning kamchiligi sifatida ularning shaxsiy komputer apparat vositalariga bogliqligini kursatish mumkin.

Viruslar ta'siri oqibatlarini yuqotish jarayonida viruslarni yuqotish, xamda virus bulgan fayllar va xotira qismlarini tiklash amalga oshiriladi. Viruslarga qarshi programmlar yordamida viruslar ta'siri oqibatlarini yuqotishning ikki usuli mavjud.

Birinchi metodga binoan tizim ma'lum viruslar ta'siridan sung tiklanadi. Virusni yuqotuvchi programmani yaratuvchi virusning stukturasini va uning yashash makonida joylashish xarakteristkalarini bilishi shart.

Ikkinchi metod noma'lum viruslar bilan zaxarlangan fayllarni va yuklama sektorini tiklashga imkon beradi. Fayllarni tiklash uchun tiklovchi programma fayllar xususidagi viruslar yuqligidagi axborotni oldindan saqlashi lozim. Zaxarlanmagan fayl xususidagi axborot va viruslar ishlashining umumiy prinqiplari xususidagi axborotlar fayllarni tiklashga imkon beradi.

4-ilova

Viruslarga qarshi kurashish usullari

Hozirgi kunda kompyuter viruslarini aniqlash va ulardan himoyalanish uchun maxsus dasturlarning bir necha xillari ishlab chiqilgan bo'lib, bu dasturlar kompyuter viruslarini aniqlash va yo'qotishga imkon beradi.

Bunday dasturlar virusga qarshi dasturlar yoki ***antiviruslar*** deb yuritiladi. Antivirus dasturlariga **AVP, Dr.Web, Nod32** dasturlarini kiritish mumkin.

Viruslarga qarshi kurashishning asosan quyidagi usullari mavjud:

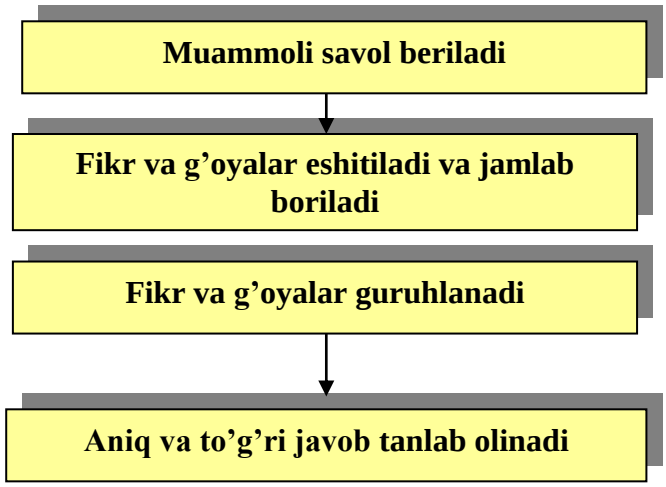
1. Muntazam profilaktika ishlarini, ya'ni virusga tekshiruv ishlarini olib borish.
2. Taniqli virusni zararsizlantirish.
3. Taniqli bo'lmagan virusni zarasizlantirish.

5-ilova

"Aqliy hujum" metodini qo'llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g'oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g'oyalar, ular hatto to'g'ri bo'lmasa ham inobatga olinadi.
3. Har bir ta'lim oluvchi qatnashishi shart.

Quyida (1-chizma) "Aqliy hujum" metodining tuzilmasi keltirilgan.



1-chizma. "Aqliy hujum" metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. Komputer viruslari kanday alomatlari buyicha klassifikatsiyalanadi?
2. Fayl virusi va uning ta'siri algoritmini tushuntiring.
3. Makrovirus va yuklama viruslar ta'siri algoritmi kanday?
4. Viruslarni aniklash metodlari.
5. Viruslar ta'siri okibatlarini yukotish metodlari.
6. Komputer tizimlarining viruslar bilan zaxarlanishining oldini oluvchi profilaktik choralar ketma-ketligini sanab uting

MAVZU № 6 (6 soat)

TARMOQDA AXBOROT XAVFSIZLIGI VA HIMOYALANISH USULLARI MA’RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	____ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo’yicha ma’ruza
Mavzu rejasi:	1.Komputer tarmog’idan foydalanishning imkoniyatlari; 2. Tarmoqda axborot himoyalashning maqsadlari
Dars maqsadi: Talabalarda komputer tarmog’idan foydalanish imkoniyatlari hamda himoyalanish maqsadlari haqida tushunchani hosil qilish qilish	
Pedagog vazifalari:	***O’quv natijalari:***
- Komputer tarmog’idan foydalanishning imkoniyatlarini keltirib o’tiladi va daftarga yozdiriladi; - Tarmoqda axborot himoyalashning maqsadlari bilan tanishtirish.	- Komputer tarmog’idan foydalanishning imkoniyatlarini o’rganadilar va daftarga yozib oladilar; - Tarmoqda axborot himoyalashning maqsadlari bilan tanishib chiqadilar va yozib oladilar.
O’qitish usullari	Ma’ruza, “Aqliy xujum” metodi
Ta’limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko’rgazmali qurollar.
Ta’limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta’minlangan xona.
Nazorat	O’zini-o’zi nazorat qilish

TARMOQDA AXBOROT XAVFSIZLIGI VA HIMOYALANISH USULLARI MAVZUSIDAGI MA’RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O’qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo’yicha kerakli adabiyotlarni e’lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1 Komputer tarmog’idan foydalanishning imkoniyatlarini batafsil bayon etadi va daftarga ma’ruza yozdiriladi. (3-ilova) 2.2. Tarmoqda axborot himoyalashning maqsadlari bilan tanishtiradi. (4-ilova)	Yozib oladilar Tinglaydilar va yozib oladilar
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo’yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. Mavzu bo’yicha “Aqliy xujum” o’tkazitladi (6-ilova)	Savollar beradi. Savollarga javob beradilar

1-ilova

Mavzu: **TARMOQDA AXBOROT XAVFSIZLIGI VA HIMOYALANISH USULLARI**

Mavzu rejasi::	1.Komputer tarmog'idan foydalanishning imkoniyatlari; 2. Tarmoqda axborot himoyalashning maqsadlari
Darsning maqsadi: Talabalarda komputer tarmog'idan foydalanish imkoniyatlari hamda himoyalanish maqsadlari haqida tushunchani hosil qilish	

2-ilova

Адабиётлар:

1. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
2. Столинс, Вильям. Основы защиты сетей. Приложения и стандарты: Пер. С англ.-М.: Издательский дом «Вильямс», 2002. 432 с.
3. Ғаниев С.К.,Каримов М.М. Ҳисоблаш тизимлари ва тармоқларида ахборот ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.-Тошкент давлат техника университети, 2003. 77 б.
4. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия - Телеком, 2000. 452с.
5. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «безопасность». – М.:СИНТЕГ, 2000, 248 с.

3-ilova

Tarmoqlardan foydalanish nima beradi

- **Integral ustunlik (yutuq) – ya'ni korxonalarini ishlab chikarish samaradorligini keskin oshirish.**
- **Har kanday masalalarni parallel yechish va shuning hisobidan ishlab chiqarishni hamda mustahkamligini oshirish.**
- **Keng qamrovli amaliy masalalarni aniqligini ta'minlash.**
- **Ma'lumotlarni va qurilmalarni xamkorlikda ishlashini ta'minlash.**
- **Umumiy tizim bo'yicha ishlarni teng va oson taqsimlash.**
- **Korporativ ma'lumotlarga operativ ravishda ega bo'lish.**
- **Kommunikatsiya tarmoqlarini takomillashtirish.**

Ikki kompyuterni bir-biri bilan boglanishi

Kompyuter tarmoqlari

Apparat qurilmalari va tarmoq dastur ta’minoti orqali o’zaro bir-birlari bilan xamoxang ishlay oladigan kompyuterlar majmuiga tarmoq deyiladi.

Tarmoqlarni turli me’yorlarga ko’ra sinflarga ajratish mumkin.

Bular:

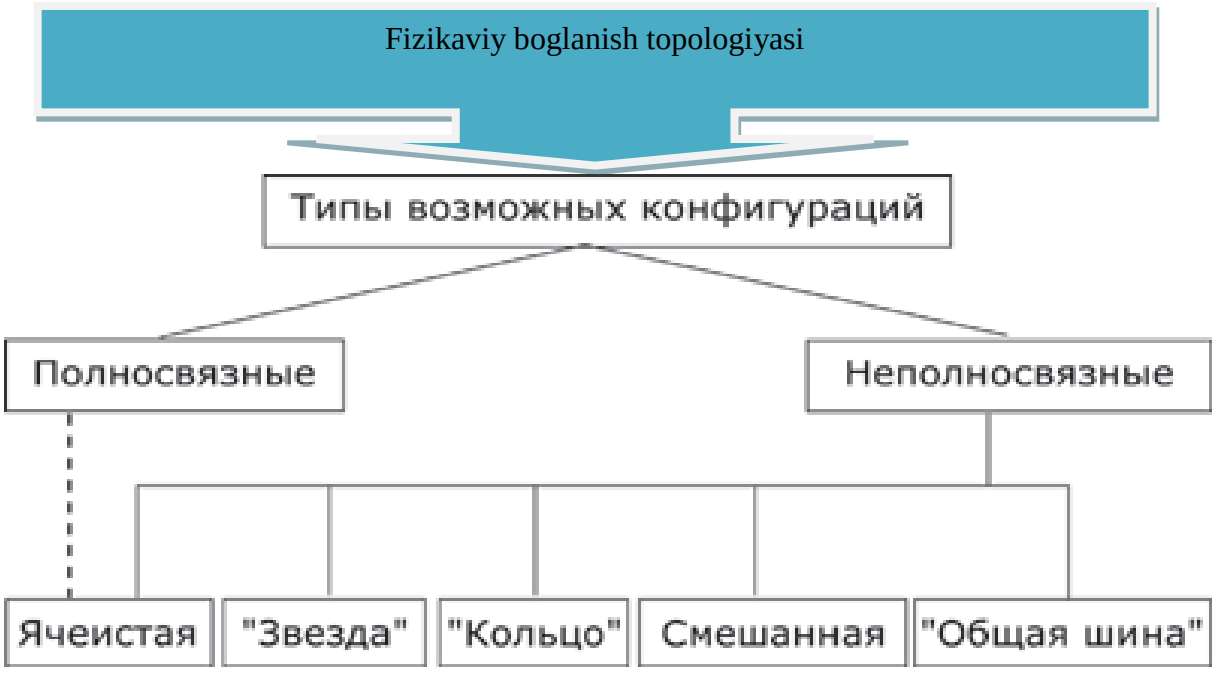
- 1) **o’tkazish qobiliyati**, ya’ni ma’lumotlarni tarmoqqa uzatish tezligiga muvofiq:
- - past 100 Kbit/s gacha;
- - o’rta 0,5-10 Mbit/s gacha;
- - yuqori 10 Mbit/s dan ortiq

2) uzoq kommunikatsiya tarmoqlari bilan ishlash tezligi, ularning **fizik o’lchoviga** muvofiq:

- **LAN** (Local - Area - Network) lokal tarmoq (LXT bir ofis, bino ichidagi aloqa);
- **CAN** (Campus – Area - Network) - kampus tarmoq, bir-biri bilan telefon yoki modemlar bilan ulanishi shart bo’lmagan, ammo yetarlicha bir-birlaridan uzoqda joylashgan kompьyuter lokal tarmog’i;
- **MAN** (Metropoliten - Area - Network) katta tezlik bilan aloqa uzatish (100 Mbit/s) imkoniyatiga, katta radiusga (bir necha o’n km) axborot uzatuvchi kengaytirilgan tarmoq;
- **WAN** (Wide – Area - Network) keng masshtabli (mintaqaviy) maxsus qurilma va dasturlar bilan ta'minlangan alohida tarmoqlarni birlashtiruvchi yirik tarmoq;
- **GAN** (Global - Area - Network) global (xalqaro, qit'alararo) tarmoq;

3) **tugunlar munosabatiga** ko’ra:
- **bir xil rangli** (peer-to-peer), uncha katta bo’lmagan, bir xil mavqega ega bo’lgan kompьyuterlar (bu yerda hamma kompyuterlar ham "mijoz", ya’ni tarmoqning oddiy foydalanuvchisi, ham "server", ya’ni tarmoq foydalanuvchilariga xizmat ko’rsatishni ta'minlovchi bo’lishi mumkin). Masalan, WINDOWS OS tarmog’i;
-**tarqatilgan** (Distributed) tarmoqlar. Bunda serverlar tarmoq foydalanuvchilariga xizmat ko’rsatadi, biroq tarmoqni boshqarmaydi;
-**server** (Server based) yoki markazlashgan boshqarishga ega tarmoqlar. Bu erda tarmoqning bosh elementi serverdir, qolgan tugunlar serverning resurslaridan foydalanishi mumkin (masalan, Nowell Net Ware, Microsoft LAN va boshqalar).

4) tarmoq **operatsion sistemalarini** ishlatish bo’yicha (tarmoq OS):
- gomogenli - hamma tugunlarda bir xil yoki yaqin operatsion sistemalardan foydalaniladi (masalan, WINDOWS OS tarmog’i);
- geterogenli - bir vaqtning o’zida bir nechta tarmoq operatsion sistemalari ishlatiladi (masalan, Nowell Net Ware va WINDOWS OC).



Internetga ulanish usullari

1. Oxirgi mil ulanish usuli.
2. Telefon aloka kanallari orqali oddiy modemlar bilan bog'lanish.
3. DSL-texnologiyasi orqali bog'lanish.
4. Asimmetrik DSL (A DSL) modemlari orqali ulanish.
5. Keng polosali kanallar orqali bog'lanish.
6. Ajratilgan aloka liniyalari orqali bog'lanish.
7. Kabel televideniesi orqali:
8. Simsiz radiokanal aloka liniyalari orqali:

8.1. Wi Fi.
8.2. Wi Max.
8.3. Mobil telefonlar yordamida.
8.4. Bluetooth orqali bog'lanish.
8.5. Flesh modemlari yordamida.
8.6. Yerning sun'iy yuldoshlari orqali ulanish.

9. Elektr tarmoqlarining simlari orqali bog'lanish.

4-ilova

Axborotni himoyalashning maqsadlari

- **axborotning kelishuvsiz chiqib ketishi, o'g'irlanishi, yo'qotilishi, o'zgartirilishi, soxtalashtirilishlarning oldini olish;**
- **shaxc, jamiyat, davlat xavfsizliligiga bo'lgan havf-xatarning oldini olish;**
- **axborotni yo'q qilish, o'zgartirish, soxtalashtirish, nusxa ko'chirish, to'siqlash bo'yicha ruxsat etilmagan harakatlarning oldini olish;**
- **hujjatlashtirilgan axborotning miqdori sifatida huquqiy tartibini ta'minlovchi, axborot zahirasi va axborot tizimiga har qanday noqonuniy aralashuvlarning ko'rinishlarining oldini olish;**
- **axborot tizimida mavjud bo'lgan shahsiy ma'lumotlarning shahsiy maxfiyligini va konfidentsialligini saqlovchi fuqarolarning konstitutsion huquqlarini ximoyalash;**
- **davlat sirini, qonunchilikka mos hujjatlashtirilgan axborotning konfidentsialligini saklash;**
- **axborot tizimlari, texnologiyalari va ularni ta'minlovchi vositalarni yaratish, ishlab chiqish va qo'llashda sub'ektlarning huquqlarini ta'minlash.**

Kompyuter tizimlari va tarmoklaridagi havf-xatar va xujum turlari

Kompyuter tizimi (tarmogi)ga ziyon yetkazishi mumkin bo'lgan sharoit, harakat va jarayonlar kompьyuter tizimi (tarmogi) uchun havf-xatarlar, deb hisoblanadi.

Avtomatlashtirilgan axborot tizimlariga tasodifiy ta'sir ko'rsatish sabablari:

- 1. Apparaturadagi to'xtab qolishliklar
- 2. Ishlab chiquvchining sxemalik, texnik va tizimli xatolari
- 3. Tashqi muhit ta'sirida aloqa kanallaridagi tusqinliklar
- 4. Tarkibiy, algoritmik va dasturiy xatoliklar
- 5. Tizimning bir qismi sanaluvchi insonning xatosi
- 6. Halokatli holatlar va boshqa ta'sirlar

Kompyuter tarmoklarida uzatilayotgan axborotni ximoyalash

Apparat-texnik vositalari deb telekommunikatsiya qurilmalariga kiritilgan yoki u bilan interfeys orqali ulangan qurilmalarga aytiladi. Masalan, ma'lumotlarni nazorat qilishning juftlik chizmasi, ya'ni jo'natiladigan ma'lumot yo'lda buzib talqin etilishini aniqpashda qo'llaniladigan nazorat bo'lib, avtomatik raviщda ish sonining juftligini (nazorat razryadi bilan birgalikda) tekshiradi.

5-ilova

Aqliy xujum savollari:

1. Kompyuter tarmog'i deb nimaga aytiladi?
2. Tarmoqning necha turi mavjud?
3. Tarmoqda axborotlarni himoyalash usullari?
4. Axborotlarni himoyalashning maqsadlari nimalardan iborat?
5. Internet nima?
6. Internetga ulanish usullarini sanab o'ting?
7. Kompyuter tizimlari va tarmoklaridagi havf-xatar va xujum turlari?
8. Internet va intranetning farqi nimada?
9. Axborotlarni muhofaza qilishning texnik vositalari tushunchasi nimani anglatadi?
10. Ma'lumotlarni ruxsatsiz olishning obyektlari, usullari va vositalari nimalardan iborat?

TARMOQDA AXBOROT XAVFSIZLIGI VA HIMOYALANISH USULLARI MA'RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	___ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1. Komputer tarmoqlarida zamonaviy himoyalash usullari va vositalari 2. Tarmoq xavfsizligini ta'minlash
Dars maqsadi: Talabalarda komputer tarmoqlarida zamonaviy himoyalash usullari va vositalari haqidagi tushunchani hosil qilish qilish	
Pedagog vazifalari:	***O'quv natijalari:***
- Komputer tarmoqlarida zamonaviy himoyalash usullari va vositalari bilan tanishtirish va ma'ruzani bayon qilish; - Tarmoq xavfsizligini ta'minlash usullarini keltirib o'tish.	- Komputer tarmoqlarida zamonaviy himoyalash usullari va vositalari bilan tanishadilar va ma'ruzani daftarga yozadilar; - Tarmoq xavfsizligini ta'minlash usullarini o'rganadilar va yozib oladilar.
O'qitish usullari	Ma'ruza, "Aqliy xujum" metodi
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

TARMOQDA AXBOROT XAVFSIZLIGI VA HIMOYALANISH USULLARI MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1 Komputer tarmog'idan foydalanishning imkoniyatlarini batafsil bayon etadi. (3-ilova) 2.2. Tarmoqda axborot himoyalashning maqsadlari bilan tanishtiradi. (4-ilova)	Yozib oladilar Tinglaydilar va yozib oladilar
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. "Aqliy xujum" metodini qo'llagan holda tezkor savol-javoblar o'tkaziladi (5- ilova)	Savollar beradi. Savollarga javob beradilar

1-ilova

Mavzu: **TARMOQDA AXBOROT XAVFSIZLIGI VA HIMOYALANISH USULLARI**

Mavzu rejasi::	1. Komputer tarmoqlarida zamonaviy himoyalash usullari va vositalari 2. Tarmoq xavfsizligini ta'minlash
Darsning maqsadi: Talabalarda komputer tarmoqlarida zamonaviy himoyalash usullari va vositalari haqidagi tushunchani hosil qilish qilish	

2-ilova

Адабиётлар:

1. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
2. Столинс, Вильям. Основы защиты сетей. Приложения и стандарты: Пер. С англ.-М.: Издательский дом «Вильямс», 2002. 432 с.
3. Ғаниев С.К.,Каримов М.М. Ҳисоблаш тизимлари ва тармоқларида ахборот ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.- Тошкент давлат техника университети, 2003. 77 б.
4. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия - Телеком, 2000. 452с.
5. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «безопасность». – М.:СИНТЕГ, 2000, 248 с.

3-ilova

Kompyuter tarmoqlarida zamonaviy himoyalash usullari va vositalari

- *Rasmiy vositalar* — shaxslarni ishtirokisiz axborotlarni ximoyalash funktsiyalarini bajaradigan vositalardir.
- *Norasmiy vositalar* — bevosita shaxslarni faoliyati yoki uning faoliyatini aniklab beruvchi reglamentlardir.
- *Texnikaviy vositalar* sifatida elektr, elektromexanik va elektron kurilmalar tushuniladi. Texnikaviy vositalar uz navbatida, fizikaviy va apparatli bo'lishi mumkin.

Fizikaviy texnik vositalar

Bu avtonom holda ishlaydigan qurilma va tizimlardir. Masalan, oddiy eshik qulflari, derazada o'rnatilgan temir panjaralar, qo'riqlash elektr uskunalari fizikaviy texnik vositalarga kiradi.

Dasturiy vositalar

- Bu axborotlarni ximoyalash funktsiyalarini bajarish uchun mo'ljallangan maxsus dasturiy ta'minotdir. Axborotlarni ximoyalashda birinchi navbatda eng keng qo'llanilgan dasturiy vositalar hozirgi kunda ikkinchi darajali himoya vositasi hisoblanadi. Bunga misol sifatida parolь tizimini keltirish mumkin.
- Bu axborotlarni ximoyalash funktsiyalarini bajarish uchun mo'ljallangan maxsus dasturiy ta'minotdir. Axborotlarni ximoyalashda birinchi navbatda eng keng qo'llanilgan dasturiy vositalar hozirgi kunda ikkinchi darajali himoya vositasi hisoblanadi. Bunga misol sifatida parolь tizimini keltirish mumkin.

Tashkiliy ximoyalash vositalari

Bu telekommunikatsiya uskunalarining yaratilishi va qo'llanishi jarayonida qabul kilingan tashkiliy-texnikaviy va tashkiliy-huquqiy tadbirlardir. Bunga bevosita misol sifatida kuyidagi jarayonlarni keltirish mumkin: binolarning qurilishi, tizimni loyihalash, qurilmalarni o'rnatish, tekshirish va ishga tushirish.

Ahloqiy va odobiy ximoyalash vositalari

Bu hisoblash texnikasini rivojlanishi oqibatida paydo bo'ladigan tartib va kelishuvlardir. Ushbu tartiblar qonun darajasida bo'lmasada, uni tan olmaslik foydalanuvchilarni obro'siga ziyon yetkazishi mumkin.

Qonuniy himoyalash vositalari

Bu davlat tomonidan ishlab chiqilgan hukukiy hujjatlar sanaladi. Ular bevosita axborotlardan foydalanish, qayta ishlash va uzatishni tartiblashtiradi va ushbu qoidalarni buzuv-chilarning mas'uliyatlarini aniqlab beradi.

4-ilova

Hozirgi kunda ma’lumotlarni ruxsatsiz chetga chiqib ketish yo’llari kuyidagilardan iborat:

• elektron nurlarni chetdan turib o’qib olish;
• aloqa kabellarini elektromagnit tulkinlar bilan nurlatish;
• yashirin tinglash qurilmalarini qo’llash;
• masofadan rasmga tushirish;
• printerdan chiqadigan akustik to’lqinlarni o’qib olish;
• ma’lumot tashuvchilarni va ishlab chiqarish chikindilarini o’g’irlash;
• tizim xotirasida saklanib kolgan ma’lumotlarni o’qib olish;
• ximoyani yengib ma’lumotlarni nusxalash;
• qayd qilingan foydalanuvchi niqobida tizimgakirish;
• dasturiy tuzoklarni qo’llash;
• dasturlash tillari va operatsion tizimlarning kamchiliklarida foydalanish;
• dasturlarda maxsus belgilangan sharoitlarda ishga tushishi mumkin bo’lgan qism dasturlarning mavjud bo’lishi;
• aloqa va apparatlarga noqonuniy ulanish;
• ximoyalash vositalarini qasddan ishdan chiqarish;
• kompyuter viruslarini tizimga kiritish va undan foydalanish.

Bevosita tarmoq bo’yicha uzatiladigan ma’lumotlarni himoyalash maqsadida quyidagi tadbirlarni bajarish lozim bo’ladi:

— uzatiladigan ma’lumotlarni ochib o’kishdan saqlash;
— uzatiladigan ma’lumotlarni taxlil qilishdan saqlanish;
—uzatiladigan ma’lumotlarni o’zgartirishga yo’l qo’ymaslik va o’zgartirishga urinishlarni aniklash;
ma’lumotlarni uzatish maqsadida qo’llaniladigan dasturiy uzilishlarni aniqlashga yo’l qo’ymaslik;
—firibgar ulanishlarning oldini olish. Ushbu tadbirlarni amalga oshirishda asosan kriptografik usullar qo’llaniladi.

Jinoyatlarni kamaytirish uchun

• personal mas’uliyatini oshirish;
• ishga qabul qilinadigan xodimlarni tekshiruvdan o’tkazish;
• muhim vazifani bajaruvchi xodimlarni almashtirib turish;
• parolь va foydalanuvchilarni qayd qilishni yaxshi yo’lga qo’yish;
• ma’lumotlarga egalik qilishni cheklash;
• ma’lumotlarni shifrlash.

Tarmoq xavfsizligini ta’minlash maqsadida

Fizikaviy himoyalash vositalari **— maxsus elektron qurilmalar yordamida ma’lumotlarga egalik qilishni taqiqlash vositalaridir.**

Mantiqiy himoyalash **-- dasturiy vositalar bilan ma’lumotlarga egalik qilishni taqiqlash uchun qo’llaniladi.**

Tarmoqlararo ekranlar va shlyuzlar **— tizimga keladigan hamda undan chiqadigan ma’lumotlarni ma’lum hujumlar bilan tekshirib boradi va protokollashtiradi.**

Xavfsizlikni auditlash tizimlari **-- joriy etilgan operatsiyalarni tizimdan o’rnatilgan parametrlarni zaifligini qidirishda qo’llaniladigan tizimdir.**

Real vaqtda ishlaydigan xavfsizlik tizimi **— doimiy ravishda tarmoqning xavfsizligini taxlillash va auditlashni ta’minlaydi.**

5-ilova

Aqliy xujum savollari:

1. Maskirovkalovchi belgilarning ochilishi tushunchasini nimani bildiradi?

2. Demaskirovka belgilari nimalar bilan farq qiladi?

3. Himoya obyektlarining demaskirovka belgilariga nimalar kiradi?

4. Texnik vositalar bilan himoyalanadigan ma’lumotlarning manbalari va tashuvchilari nimalardan iborat?

5. Obyektning demaskirovka belgilari qanday guruhlarga bo‘linadi?

6. Obyektning ko‘rinadigan va infraqizil elektromagnit spektr diapazonlaridagi emaskirovka belgilari nimalardan iborat?

7. Radioelektron vositalarning qanday demaskirovka belgilari mavjud?

8. Nimalar ma’lumot tashuvchi vositalar hisoblanadi?

9. Ma’lumotlar chiqish kanali deb nimaga aytiladi?

10. Ma’lumotlar chiqib ketish kanali qanday guruhlarga ajratiladi?

11. Ma’lumotlar chiqib ketish kanalining paydo bo‘lish sabablari va sharoitlari nimalardan iborat?

12. Texnik kanal bo‘yicha ma’lumotlar chiqib ketishidan himoyalashda qanday amallar bajarilishi talab etiladi?

TARMOQDA AXBOROT XAVFSIZLIGI VA HIMOYALANISH USULLARI MA'RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	___ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1. Tarmoqlararo ekranlarning ishlash xususiyatlari. 2. Tarmoqlararo ekranlarning turkumlanishi.
Dars maqsadi: Talabalarda tarmoqlararo ekranlarning ishlash xususiyatlari haqidagi tushunchani hosil qilish qilish	
Pedagog vazifalari:	***O'quv natijalari:***
- Tarmoqlararo ekranlarning ishlash xususiyatlari bilan tanishtirish va ma'ruzani bayon qilish; - Tarmoqlararo ekranlarning turkumlanishi batafsil yoritib berish.	- Tarmoqlararo ekranlarning ishlash xususiyatlari bilan tanishadilar va ma'ruzani yozib oladilar; - Tarmoqlararo ekranlarning turkumlanishini o'rganadilar va yozib oladilar.
O'qitish usullari	Ma'ruza, "Aqliy xujum" metodi
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

TARMOQDA AXBOROT XAVFSIZLIGI VA HIMOYALANISH USULLARI MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1 Tarmoqlararo ekranlarning ishlash xususiyatlarini ma'ruza sifatida batafsil bayon etadi. (3-ilova) 2.2. Tarmoqlararo ekranlarning turkumlanishi bilan tanishtiradi. (4-ilova)	Yozib oladilar Tinglaydilar va yozib oladilar
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. "Aqliy xujum" metodini qo'llagan holda tezkor savol-javoblar o'tkaziladi (5- ilova)	Savollar beradi. Savollarga javob beradilar

1-ilova

Mavzu: **TARMOQDA AXBOROT XAVFSIZLIGI VA HIMOYALANISH USULLARI**

Mavzu rejasi::	1. Tarmoqlararo ekranlarning ishlash xususiyatlari. 2. Tarmoqlararo ekranlarning turkumlanishi.
Darsning maqsadi: Talabalarda tarmoqlararo ekranlarning ishlash xususiyatlari haqidagi tushunchani hosil qilish qilish	

2-ilova

Адабиётлар:

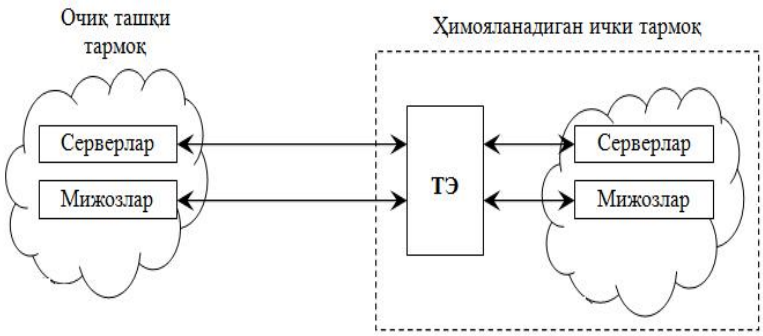
1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги» «Алоқачи» - 2008 й.
2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
3. Филин С. А. «Информационная безопсность», М.: Альфа – Пресс, 2006 г.
4. Ғаниев С.К., Каримов М.М. Ҳисоблаш тизимлари ва тармоқларида ахборот ҳимояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.
5. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия - Телеком, 2000. 452с.
6. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «безопасность». – М.:СИНТЕГ, 2000, 248 с.

3-ilova

Tarmoqlararo ekran (TE) - *brandmauer* yoki *firewall sistemasi* deb ham ataluvchi tarmoqlararo himoyaning ixtisoslashtirilgan kompleksi. Tarmoqlararo ekran umumiy tarmoqni ikki yoki undan ko’p qismlarga ajratish va ma’lumot paketlarini chegara orqali umumiy tarmoqning bir qismidan ikkinchisiga o’tish shartlarini belgilovchi qoidalar naborini amalga oshirish imkonini beradi.

Ruxsat etilmagan tarmoqlararo foydalanishga qarshi ta’sir ko’rsatish uchun tarmoqlararo ekran ichki tarmoq hisoblanuvchi tashkilotning himoyalanuvchi tarmog’i va tashqi g’anim tarmoq orasida joylanishi lozim Bunda bu tarmoqlar orasidagi barcha aloqa faqat tarmoqlararo ekran orqali amalga oshirilishi lozim. Tashkiliy nuqtai nazaridan tarmoqlararo ekran himoyalanuvchi tarmoq tarkibiga kiradi.

Tarmoqlararo ekranni ulash sxemasi



Ichki tarmoqning ko’pgina uzellarini birdaniga himoyalovchi tarmoqlararo ekran quyidagi ikkita vazifani bajarishi kerak:

- tashqi (himoyalanuvchi tarmoqqa nisbatan) foydalanuvchilarning korporativ tarmoqning ichki resurslaridan foydalanishini chegaralash. Bunday foydalanuvchilar qatoriga tarmoqlararo ekran himoyalovchi ma’lumotlar bazasining serveridan foydalanishga urinuvchi sheriklar, masofadagi foydalanuvchilar, xakerlar, hatto kompaniyaning xodimlari kiritilishi mumkin;
- himoyalanuvchi tarmoqdan foydalanuvchilarning tashqi resurslardan foydalanishlarini chegaralash. Bu masalaning yechilishi, masalan, serverdan xizmat vazifalari talab etmaydigan foydalanishni tartibga solishga imkon beradi.

4-ilova

Tarmoqlararo ekranlarning tavsiflariga asoslangan holda, ularni quyidagi asosiy alomatlari bo'yicha turkumlash mumkin:

OSI modeli sathlarida ishlashi bo'yicha:

- paketli filtr (ekranlovchi marshrutizator – screening router);
- seans sathi shlyuzi (ekranlovchi transport);
- tatbiqiy shlyuz (application gateway);
- ekspert sathi shlyuzi (stateful inspection firewall).

Ishlatiladigan texnologiya bo'yicha:

- protokol holatini nazoratlash (Stateful inspection);
- vositachilar modullari asosida (proxy);

Bajarilishi bo'yicha:

- apparat-dasturiy;
- dasturiy;

lanish sxemasi bo'yicha:

- tarmoqni umumiy himoyalash sxemasi;
- tarmoq segmentlari himoyalanuvchi berk va rmoq segmentlari himoyalanmaydigan ochiq xema;
- tarmoqning berk va ochiq segmentlarini lohida himoyalovchi sxema.

5-ilova

Aqliy xujum savollari:

1. Ma'lumotlarni vizual-optik kanal bo'yicha chiqib ketishidan himoyalash qanday amalga oshiriladi?
2. Akustik kanal orqali ma'lumot chiqishidan himoyalashda qanday choralar Ko'riladi?
3. Ma'lumot chiqishining qanday elektromagnit kanallari mavjud?
4. Ma'lumotlarni himoyalashning qanday konstruktor-texnologik usullari bor?
5. Tutib olishdan himoyalashning qanday usullar mavjud?
6. Injener-texnik himoya tushunchasi nimani bildiradi?
7. Funksional vazifasi bo'yicha injener-texnik himoya vositalari qanday guruhlarga ajratiladi?
8. Himoya tizimini ishlab chiqish bosqichlari nimalardan iborat?
9. Fizik himoya vositalarining asosiy vazifalariga nimalar kiradi?
10. Obyekt xavfsizligini ta'minlash tizimlari nimalardan iborat?

MAVZU № 7 (4 soat)

INTERNET TIZIMIDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH USULLARI MA'RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	___ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1. Internetda ruxsatsiz kirish usullarining tasnifi; 2. Real Secure tizimi.
Dars maqsadi: Talabalarda internet tizimida ma'lumotlar xavfsizligini ta'minlash usullari haqidagi tushunchani hosil qilish qilish	
Pedagog vazifalari:	***O'quv natijalari:***
-Internetda ruxsatsiz kirish usullarning tasnifini tushuntirib berishva ma'ruzani yozdirish; - Real Secure tizimini batafsil yoritib berish.	- Internetda ruxsatsiz kirish usullarning tasnifi bilan tanishib chiqadilar va yozib oladilar; - Real Secure tizimini o'rganadilar va yozib oladilar.
O'qitish usullari	Ma'ruza, B.BX.B metodi metodi, "Aqliy xujum" metodi
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

INTERNET TIZIMIDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH USULLARI MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1 Internetda ruxsatsiz kirish usullarning tasnifini batafsil bayon etadi va ma'ruza yozdiriladi. (3-ilova) 2.2. Real Secure tizimi bilan tanishtiradi. (4-ilova)	Yozib oladilar Tinglaydilar va yozib oladilar
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B metodi (5- ilova) 3.3. "Aqliy xujum" metodini qo'llagan holda tezkor savol-javoblar o'tkaziladi (6-ilova)	Savollar beradi. Jadval to'ldiriladi Savollarga javob beradilar

1-ilova

Mavzu: **INTERNET TIZIMIDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH USULLARI**

Mavzu rejasi::	1. Internetda pyxcamciz kirish usullarining tasnifi; 2. Real Secure tizimi.
Darsning maqsadi Talabalarda internet tizimida ma'lumotlar xavfsizligini ta'minlash usullari haqidagi tushunchani hosil qilish qilish	

2-ilova

Адабиётлар:

1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги» «Алоқачи» - 2008 й.
2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
3. Филин С. А. «Информационная безопсность», М.: Альфа – Пресс, 2006 г.
4. Ғаниев С.К., Каримов М.М. Ҳисоблаш тизимлари ва тармоқларида ахборот ҳимояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.

3-ilova

Global tarmoqlarning rivojlanishi va axborotlarni olish, qayta ishlash va uzatishning yangi texnologiyalari paydo bo'lishi bilan Internet tarmogiga har xil shaxs va tashkilotlarning e'tibori karatildi. Ko'plab tashkilotlar uz lokal tarmoqlarini global tarmoqlarga ulashga karor qilishgan va hozirgi paytda WWW, FTP, Gophes va boshqa serverlardan foydalanishmokda. Tijorat maqsadida ishlatiluvchi yoki davlat siri bo'lgan axborotlarning global tarmoqlar buyicha joylarga uzatish imkoni paydo buldi va uz navbatida, shu axborotlarni himoyalash tizimida malakali mutaxassislarga extiyoj tugilmokda.

Global tarmoqlardan foydalanish bu faqatgina «kizikarli» axborotlarni izlash emas, balki tijorat maqsadida va boshqa ahamiyatga molik ishlarni bajarishdan iborat. Bunday faoliyat vaktida axborotlarni himoyalash vositalarining yukligi tufayli ko'plab talofotlarga duch kelish mumkin.

Har qanday tashkilot Intenetga ulanganidan sung, xosil buladigan quyidagi muammolarni xal etishlari shart:

• tashkilotning kompyuter tizimini xakerlar tomonidan buzilishi:

• Internet orqali junatilgan ma'lumotlarning yovuz niyatli shaxslar tomonidan o'qib olinishi;

• tashkilot faoliyatiga zarar etkazilishi.

Internet loyixalash davrida bevosita himoyalangan tarmoq sifatida ishlab chikilmagan. Bu soxada hozirgi kunda mavjud bo'lgan quyidagi muammolarni keltirish mumkin:

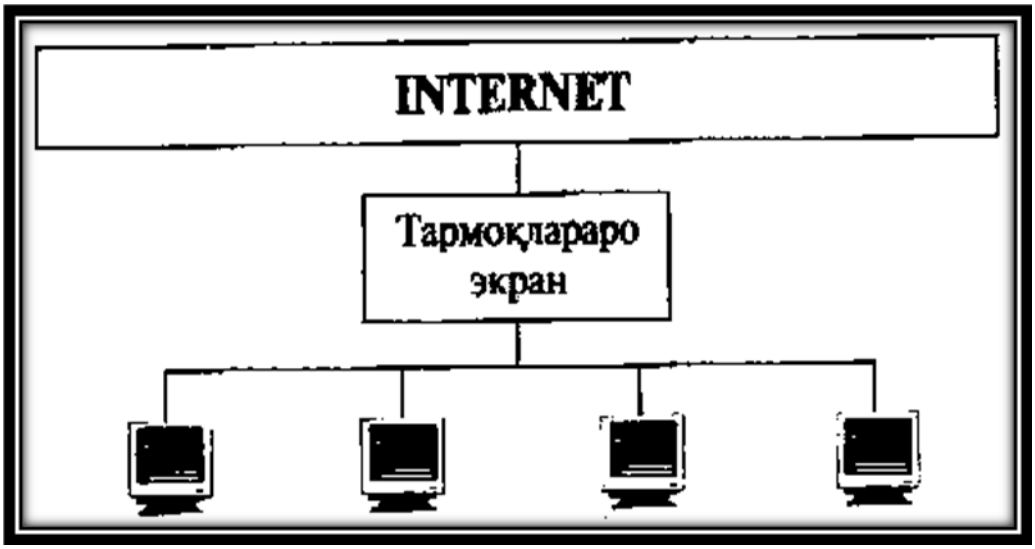
• ma'lumotlarni engillik bilan kulga kiritish;

• tarmoqdagi kompyuterlar manzilini soxtalashtirish;

• TCP/IP vositalarining zaifligi;

• ko'pchilik saytlarning notugri konfiguratsiyalanishi;

• konfiguratsiyalashning murakkabligi.



Global tarmoqlarning chegarasiz keng rivojlanishi undan foydalanuvchilar sonining oshib borishiga sabab bulmokda, bu esa uz navbatida axborotlar xavfsizligiga taxdid solish extimolining oshishiga olib kelmokda. Uzoq, masofalar bilan axborot almashish zaruriyati axborotlarni olishning kat'iy chegaralanishini talab etadi.

Shu maqsadda tarmoqlarning segmentlarini xap xil darajadagi himoyalash usullari taklif etilgan:

- erkin kirish (masalan: WWW-server);
- chegaralangan kirishlar segmenti (uzok masofada joylashgan ish joyiga xizmatchilarning kirishi);
- ixtiyoriy kirishlarni man etish (masalan, tashkilotlarning moliyaviy lokal tarmoqlari).

Internet global axborot tarmogi uzida nixoyatda katta xajmga ega bo‘lgan axborot resurslaridan milliy iktisodning turli tarmoqlarida samarali foydanishga imkoniyat tugdirishiga karamasdan axborotlarga bo‘lgan xavfsizlik darajasini oshirmoqda. Shuning uchun ham Internetga ulangan har bir korxona uzining axborot xavfsizligini ta’minlash masalalariga katta e’tibor berishi kerak. Ushbu tarmoqda axborotlar xavfsizligining yulga kuyilishi yondashuvi kuyida keltirilgan:

Lokal tarmoqlarning global tarmoqarga qo’shilishi uchun tarmoqlar himoyasi administratori quyidagi masalalarni xal qilishi lozim:

— lokal tarmoqlarga global tarmoq, tomonidan mavjud xavflarga nisbatan himoyaning yaratilishi;

— global tarmoq fondalanuvchisi uchun axborotlarni yashirish imkoniyatining yaratilishi;

Bunda quyidagi usullar mavjud:

— kirish mumkin bulmagan tarmoq manzili orqali;

— Ping dasturi yordamida tarmoq paketlarini tuldirish;

— ruxsat etilgan tarmoq manzili bilan takiklangan tarmoq manzili buyicha birlashtirish;

— ta’kiklangan tarmoq protakoli buyicha birlashtirish;

— tarmoq buyicha foydalanuvchiga parol tanlash;

— REDIREST turidagi ICMP paketi yordamida marshrutlar jadvalini modifikatsiyalash;

— RIR standart bulmagan paketi yordamida marshrutlar jadvalini uzgartirish;

— DNS spoofingdan foydalangan holda ulanish.

4-ilova

Real Secure tizimi.

Kompyuter tarmoqlarida xujum qiluvchilarni aniqlab beruvchi Real Secure tizimi amerikadagi Internet Security System kompaniyasi tomonidan 1998 yilda ishlab chiqilgan. Ushbu tizim (qurilma)-intellektual analizatordan iborat bo’lib kelayotgan ma’lumot paketlarini tahlil etib xujumlarni aniqlaydi. Bu sistema real vaqt masshtabida ishlab tarmoqdagi ma’lumot paketlarini tahlil etadi va tarmoqning bir segmentidagi ma’lumotlarni himoya qiladi.

Hujum bo’layotganligi aniqlangan holda elektron pochta yoki konsol orqali ma’muriyat boshqaruvchiga ma’lumot beriladi. Shu bilan birgalikda ma’lumotlar ba’zasiga xujum to’g’risida yozib qo’yiladi va kerak bo’lgan paytda tahlil etiladi. Agar qilinayotgan xujum sizning kompyuter tizimingizni ishdan chikarishi mumkinligi aniqlansa,u holda avtomatik ravishda xujum etuvchi bilan aloqa uziladi va marshrutizator keyingi bog’lanishlikni taqiqlaydi. Ushbu Real Secure sistemasi kompyuter tarmog’ining ichidagi hamda tashqarida kelayotgan havfni aniqlaydi va himoya qiladi.

Real Secure tizimining asosiy komponentlari

Real Secure sistemasi tarkalgan arxitektura asosida ishlaydi va 2 ta asosiy kompanentdan iboratdir, ya'ni Real Secure Detector va Real Secure Manager. Birinchi kompanent kompьyuter tarmogida xosil bulayotgan xujumlarni aniklaydi. U moduldan ya'ni tarmok va sistemali agentlardan tashkil topgan. Tarmok agenti kompьyuter ma'lumotlarining almashuvida bulayotgan xodisalar asosida xavf borligini aniklab beradi. Sistemali agent esa tekshirilaetgan tarmoq tuguniga ulanib, xujum bulaetganligi tugrisida xabar beradi. Ikkinchi komponent, ya'ni Real Secure Manager koiponenti ma'lumotlarini detektordan yigish va sozlash ishlariga javob beradi.

Real Secure sistemasining qobiliyati quyidagicha:

a) Aniqlovchi xujumlarning sonini ko'pligi;
b) Nazorat etish modullarini markazlashgan holda boshqarish;
c) Juda ko'p tarmoq protokollarini filtrlash va tahlil qilish (TEP, UDP, IEMP);
d) Xujumlarga har xil variantlar asosida ta'sir etish;
e) Xujum qilaetgan tugun bilan aloqani uzish;
f) Tarmok ekranlari va marshrutizarotlarni boshqarish;
g) Xar bir xujumni qayta ko'rib chiqish va tahlil etish uchun yezib olish;
h) Ethernet, Fast Ethernet va Token Ring tarmoq interfeyslarida ishlashni ta'minlash;
i) Maxsus uskunalar talab etmasligi;
j) Tarmok unumdorligini pasaytirmaslik;
k) Xisobot tarmoklarining har xilligi;
l) Uskunaviy va dasturiy ta'minotlarga talablarning balandmasligi va hokazo.

Xujumlarga e'tiroz etishning har xil variantlari aniqlangan va ular quyidagicha:

A) Xujum xaqida qayd etish va ro'yxatga olish;
B) Ma'muriyatni elektron pochta yoki boshqaruv konsuli orqali ogoxlantirish;
C) Xujum qilayotgan tarmoq tugunini avariya sifatida uzib quyish;
D) Qilingan xujumlarini ko'rib chiqish va tahlil etish uchun yozib olish;
E) Tarmoqlararo ekranlarni va marshrutizatorlarni tarmoq ko'rinishini o'zgartirish va hokazolar.

5-ilova

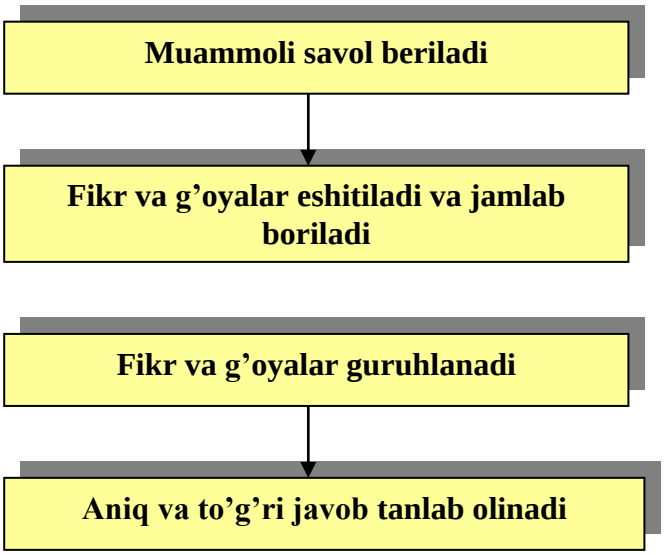
B	BX	B
.....	.....	.....

6-ilova

“Aqliy hujum” metodini qo’llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g’oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g’oyalar, ular hatto to’g’ri bo’lmasa ham inobatga olinadi.
3. Har bir ta’lim oluvchi qatnashishi shart.

Quyida (1-chizma) “Aqliy hujum” metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. Tarmoq topologiyasini izohlab bering?
2. Global va lokal tarmoq?
3. Tarmoqlarning segmentlarini xap xil darajadagi himoyalash usullari?
4. Real Secure tizimi nima?
5. Real Secure tizimining asosiy komponentlari?
6. Xujumlarni e’tiroz etish yo’llari?

INTERNET TIZIMIDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH USULLARI MA'RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	___ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1. Ruxsat etilgan manzillarning ruxsat etilmagan vaktda ulanishi; 2. Axborot xavfsizligida indentifikatsiya va autentifikatsiya.
Dars maqsadi: Talabalarda axborot xavfsizligida indentifikatsiya va autentifikatsiya haqidagi tushunchani hosil qilish qilish	
Pedagog vazifalari:	***O'quv natijalari:***
-Ruxsat etilgan manzillarning ruxsat etilmagan vaqtda ulanish tushunchasini tushuntirib berish va daftarga yozdirish; - Axborot xavfsizligida indentifikatsiya va autentifikatsiya tushunchasini talabalarga yetkazish.	- Ruxsat etilgan manzillarning ruxsat etilmagan vaqtda ulanish tushunchasini tushunib oladilar va yozib oladilar; - Axborot xavfsizligida indentifikatsiya va autentifikatsiya tushunchasini o'rganadilar va yozib oladilar.
O'qitish usullari	Ma'ruza, B.BX.B metodi metodi, "Aqliy xujum" metodi
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

INTERNET TIZIMIDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH USULLARI MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1 Ruxsat etilgan manzillarning ruxsat etilmagan vaqtda ulanish tushunchasini batafsil yoritib beradi va daftarga yozdiradi. (3-ilova) 2.2. Axborot xavfsizligida indentifikatsiya va autentifikatsiya tushunchasi bilan tanishtiradi. (4-ilova)	Yozib oladilar Tinglaydilar va yozib oladilar
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B metodi (5- ilova) 3.3. "Aqliy xujum" metodini qo'llagan holda tezkor savol-javoblar o'tkaziladi (6-ilova)	Savollar beradi. Jadvalni to'ldiradilar Savollarga javob beradilar

1-ilova

Mavzu: **INTERNET TIZIMIDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH USULLARI**

Mavzu rejasi::	1. Ruxsat etilgan manzillarning ruxsat etilmagan vaqtda ulanishi; 2. Axborot xavfsizligida indentifikatsiya va autentifikatsiya.
Darsning maqsadi Talabalarda axborot xavfsizligida indentifikatsiya va autentifikatsiya haqidagi tushunchani hosil qilish qilish	

2-ilova

Адабиётлар:

1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги» «Алоқачи» - 2008 й.
2. Ғаниев С.К., Каримов М.М. Ҳисоблаш тизимлари ва тармоқларида ахборот ҳимояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.
3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия - Телеком, 2000. 452с.
4. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «безопасность». – М.:СИНТЕГ, 2000, 248 с.

3-ilova

Ruxsat etilgan manzillarning ruxsat etilmagan vaktda ulanishi

Ushbu xavf global tarmoqlarning bir kancha soxalarini kamrab oladi, jumladan:

- lokal soha;
- lokal-global tarmoqlarning birlashuvi;
- muhim axborotlarni global tarmoqlarda junatish;
- global tarmoqning boshqarilmaydigan qismi.

Ixtiyoriy axborot tarmoqlarining asosiy komponentlari bu serverlar va ishchi stantsiyalar hisoblanadi. Serverda axborotlar yoki hisoblash resurslari va ishchi stantsiyalarda xizmatchilar ishlaydi. Umuman ixtiyoriy kompyuter ham, server ham ishchi stantsiya bo'lishi mumkin — bu holda ularga nisbatan xavfli hujumlar bo'lishi extimoli bor.

Global tarmoq maydonlaridagi taxdid

Taxdid	L okal maydon	L T/GT birla-	GT admin- strator	GT boshqa- rilmay-

		shuvi	maydoni	digan maydoni
Tarmoqlarning notugri manzili			+	+
Paketlar bilan tuldirish	+			+
Mumkin bulmagan ulanish		+		+
Mumkin bo‘lgan ulanish	+	+		+
Parolni tanlash	+	+		+
ICMP hujumi	+	+	+	
RIP hujumi		+	+	
Ruxsatsiz uzokdan boshqarish		+	+	+
Parolni uzgartirish	+			+
DNS hujumi		+	+	
Mumkin bulmagan vaktda	+	+	+	+

Serverlarning asosiy vazifasi axorotlarni saqlash va takdim qilishdan iborat.

Yovuz niyatli shaxslarni quyidagicha tasniflash mumkin:
• axborot olishga imkoniyat olish;
• xizmatlarga ruxsat etilmagan imkoniyat olish;
• ma’lum sinfdagi xizmatlarning ish rejimini ishdan chikarishga urinish;
• axborotlarni uzgartirishga harakat yoki boshqa turdagi hujumlar.

Uz navbatida, hozirgi zamonaviy rivojlanish davomida servis xizmatini izdan chikarishga qarshi kurash muammosi muhim ahamiyat kasb etadi. Bu xildagi hujumlar «servisdagi buzilish» nomini olgan.

Ishchi stantsiyalarga hujumning asosiy maqsadi, asosan, kayta ishlanayotgan ma’lumotlarni yoki lokal saklanayotgan axborotlarni olishdir. Bunday hujumlarnint asosiy vositasi «Troyan» dasturlar sanaladi. Bu dastur uz tuzilishi buyicha kompyuter viruslaridan fark kilmaydi va kompyuterga tushishi bilan uzini bilintirmasdan turadi. Boshqacha aytganda, bu dasturning asosiy maqsadi — tarmoq, stantsiyasidagi himoya tizimini ichki tomondan buzishdan iborat.

Bu holatda masalani xal qilish ma’lum qiyinchilikka olib keladi, ya’ni maxsus tayyorlangan mutaxassis lozim yoki boshqa choralar kabul qilish kerak buladi. Boshqa bir oddiy himoya usullaridan biri har kaysi ishchi stantsiyadagi tizimli fayllar va xizmat soxasidagi ma’lumotlarning uzgarishini tekshirib turuvchi revizor (ingl. ***advizer***— kiruvchi) urnatish sanaladi.

4-ilova

Identifikatsiya (*Identification*) - foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni. Bu foydalanuvchi tarmoqdan foydalanishga uringanida birinchi galda bajariladigan funktsiyadir. Foydalanuvchi tizimga uning so'rovi bo'yicha o'zining identifikatorini bildiradi, tizim esa o'zining ma'lumotlar bazasida uning borligini tekshiradi.

Autentifikatsiya (*Authentication*) – ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi. Bu tekshirish foydalanuvchi (jarayon yoki qurilma) haqiqatan aynan o'zi ekanligiga ishonch xosil qilishiga imkon beradi. Odatda foydalanuvchi tizimga o'z xususidagi noyob, boshqalarga ma'lum bo'lmagan axborotni (masalan, parol yoki sertifikat) kiritishi orqali identifikatsiyani tasdiqlaydi.

Identifikatsiya* va *autentifikatsiya sub'ektlarning (foydalanuvchilarning) haqiqiy ekanligini aniqlash va tekshirishning o'zaro bog'langan jarayonidir. Muayyan foydalanuvchi yoki jarayonning tizim resurslaridan foydalanishiga tizimning ruxsati aynan shularga bog'liq. Sub'ektni identifikatsiyalash va autentifikatsiyalashdan so'ng uni avtorizatsiyalash boshlanadi.

Avtorizatsiya (*Authorization*) – subektga tizimda ma'lum vakolat va resurslarni berish muolajasi, ya'ni avtorizatsiya sub'ekt harakati doirasini va u foydalanadigan resurslarni belgilaydi. Agar tizim avtorizatsiyalangan shaxsni avtorizatsiyalanmagan shaxsdan ishonchli ajrata olmasa bu tizimda axborotning konfidentsialligi va yaxlitligi buzilishi mumkin.

Ma'murlash (*Accounting*) – foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish. Ushbu hisobot axboroti xavfsizlik nuqtai nazaridan tarmoqdagi xavfsizlik xodisalarini oshkor qilish, taxlillash va ularga mos reaktsiya ko'rsatish uchun juda muhimdir.

5-**ilova**

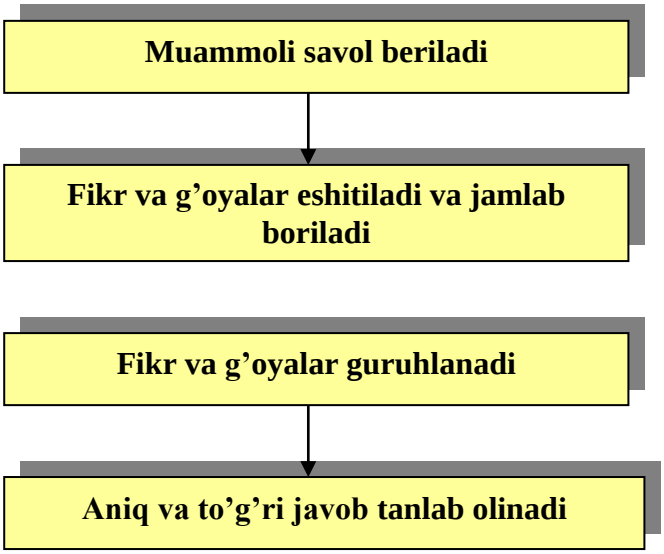
B	BX	B
.....	.....	.....

6-ilova

“Aqliy hujum” metodini qo’llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g’oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g’oyalar, ular hatto to’g’ri bo’lmasa ham inobatga olinadi.
3. Har bir ta’lim oluvchi qatnashishi shart.

Quyida (1-chizma) “Aqliy hujum” metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. Identifikatsiya nima?
2. Autentifikatsiya nima?
3. Avtorizatsiya tushunchasiga ta’rif bering?
4. Ixtisoslashtirilgan kommunikatsion kompьyuter sistemalarida informatsiya himoyasi qanday ta’minlanadi?
5. Tarmoqni boshqarish qism sistemasida informatsiyani himoyalash qanday amalga oshiriladi?
6. Tarmoqlararo ekranlashning mohiyatini tushuntiring.

MAVZU № 8 (2 soat)

ELEKTRON POCHTADA HIMOYALANISH
MA'RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	___ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo'yicha ma'ruza
Mavzu rejasi:	1. Login va parolь tushunchasi; 2. Elektron raqamli imzo
Dars maqsadi: Talabalarda elektron pochta hamda elektron raqamli imzo haqidagi tushunchani hosil qilish qilish	
Pedagog vazifalari:	***O'quv natijalari:***
- Login va parolь tushunchasini tushuntirib berish va ma'ruzani daftarga yozdirish; - Elektron raqamli imzo tushunchasini talabalarga yetkazish.	- Login va parol tushunchasi haqidagi ma'lumotga ega bo'lishadi va daftarga yozib olishadi; - Elektron raqamli imzo tushunchasini o'rganadilar va yozib oladilar.
O'qitish usullari	Ma'ruza, B.BX.B metodi metodi, "Aqliy xujum" metodi
Ta'limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko'rgazmali qurollar.
Ta'limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta'minlangan xona.
Nazorat	O'zini-o'zi nazorat qilish

ELEKTRON POCHTADA HIMOYALANISH
MAVZUSIDAGI MA'RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O'qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va geja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo'yicha kerakli adabiyotlarni e'lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1. Login va parol tushunchasini batafsil yoritib beradi va ma'ruzani bayon qiladi. (3-ilova) 2.2. Elektron raqamli imzo tushunchasi bilan tanishtiradi. (4-ilova)	Yozib oladilar Tinglaydilar va yozib oladilar
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo'yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B metodi (5- ilova) 3.3. "Aqliy xujum" metodini qo'llagan holda tezkor savol-javoblar o'tkaziladi (6-ilova)	Savollar beradi. Jadvalni to'ldirishadi Savollarga javob beradilar

1-ilova

Mavzu: **INTERNET TIZIMIDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH USULLARI**

Mavzu rejasi::	1. Login va parol tushunchasi; 2. Elektron raqamli imzo
Darsning maqsadi Talabalarda elektron pochta hamda elektron raqamli imzo haqidagi tushunchani hosil qilish qilish	

2-ilova

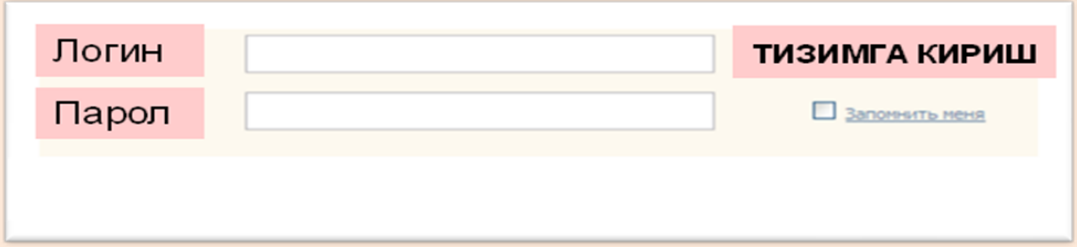
Адабиётлар:

1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги» «Алоқачи» - 2008 й.
2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
3. Филин С. А. «Информационная безопсность», М.: Альфа – Пресс, 2006 г.

3-ilova

Login va parol tushunchasi

- **Login** – shaxsning, o'zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo'llaniladigan belgilar ketma-ketligi bo'lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi hisoblanadi.
- **Parol** – uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi. U kompyuter bilan muloqot boshlashdan oldin, unga klaviatura yoki identifikatsiya kartasi yordamida kiritiladigan harfli, raqamli yoki harfli-raqamli kod shaklidagi mahfiy so'zdan iborat.
- **Avtorizatsiya** – foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni. Bunda foydalanuvchiga hisoblash tizimida ba'zi ishlarni bajarish uchun muayyan huquqlar beriladi. Avtorizatsiya shaxs harakati doirasini va u foydalanadigan resurslarni belgilaydi.



Ro’yxatdan o’tish tartibi

Ro’yxatdan o’tish – foydalanuvchilarni ro’yxatga olish va ularga dasturlar va ma’lumotlarni ishlatish-ga huquq berish jarayoni.
Ayrim veb-saytlar foydalanuvchilarga qo’shimcha xizmatlarni olish va pullik xizmatlarga obuna bo’lish uchun ro’yxatdan o’tishni hamda login va parol olishni taklif qiladilar.
Foydalanuvchi ro’yxatdan o’tgandan so’ng tizimda unga qayd yozuvi (account) yaratiladi va unda foydalanuvchiga tegishli axborotlar saqlanadi.

Login va parol masalalari

- **Login va parolga ega bo’lish shartlari.** Biror shaxs o’zining login va paroliga ega bo’lishi uchun u birinchidan axborot kommunikatsiya tizimida ruyxatdan o’tgan bo’lishi kerak va shundan so’ng u o’z logini va parolini o’zi hosil qilishi yoki tizim tomonidan berilgan login parolga ega bo’lishi mumkin.
- **Login va parolni buzish.** Login va parolni buzish – bu buzg’unchining biror bir maqsad yo’lida axborot kommunikatsiya tizimi ob’ektlaridan foydalanish uchun qonuniy tarzda foydalanuvchilarga tegishli login va parollarini buzishdir.
- **Login va parolni o’g’irlash.** Login va parolni o’g’irlash – bu foydalanuvchilarning mahfiy ma’lumotlari bo’lgan login va parollarga ega bo’lish maqsadida amalga oshiriladigan internet firibgarligining bir turidir.

Resurslardan ruxsatsiz foydalanish va uning oqibatlari

Axborot-kommunikatsiya tizimining ixtiyoriy tarkibiy qismlaridan biri bo’lgan, hamda axborot tizimi taqdim etadigan imkoniyat mavjud bo’lgan resurslardan belgilangan qoidalarga muvofiq bo’lmagan holda, foydalanishni cheklash qoidalariga rioya qilmasdan foydalanish – bu resurslardan ruxsatsiz foydalanish toifasiga kiradi.
Bunday foydalanish natijasida quyidagi oqibatlar yuzaga kelishi mumkin:

- axborotning o’g’irlanishi;
- axborotni o’zgartirish;
- axborotning yo’qotilishi;
- yolg’on axborotni kiritish;
- axborotni qalbakilashtirish va h.k.

4-ilova

ERI telekommunikatsiya kanallari orqali uzatiluvchi matnlarni autentifikatsiyalash uchun ishlatiladi. ERI ishlashi bo’yicha oddiy qo’lyozma imzoga o’xshash bo’lib, quyidagi afzalliklarga ega:

- imzo chekilgan matn imzo qo’ygan shaxsga tegishli ekanligini tasdiqlaydi;
- bu shaxsga imzo chekilgan matnga bog’liq majburiyatlaridan tonish imkoniyatini bermaydi;
- imzo chekilgan matn yaxlitligini kafolatlaydi.

Elektron raqamli imzo - imzo chekiluvchi matn bilan birga uzatiluvchi qo’shimcha raqamli xabarga nisbatan katta bo’lmagan sondir.

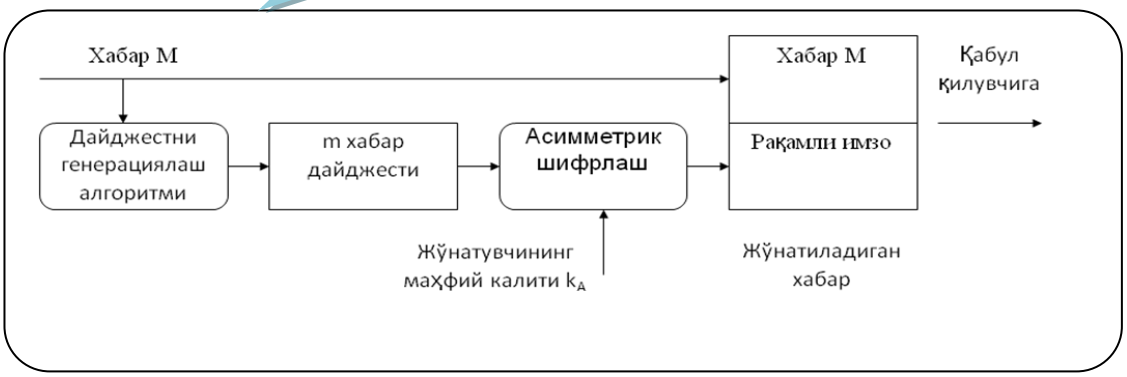
Elektron raqamli imzo asimmetrik shifrlarning qaytaruvchanligiga hamda xabar tarkibi, imzoning o’zi va kalitlar juftining o’zaro bog’liqligiga asoslanadi. Bu elementlarning xatto birining o’zgarishi raqamli imzoning haqiqiyligini tasdiqlashga imkon bermaydi. Elektron raqamli imzo shifrlashning asimmetrik algoritmlari va xesh–funktsiyalari yordamida amalga oshiriladi.

ERI tizimi ikkita asosiy muolajani amalga oshiradi:

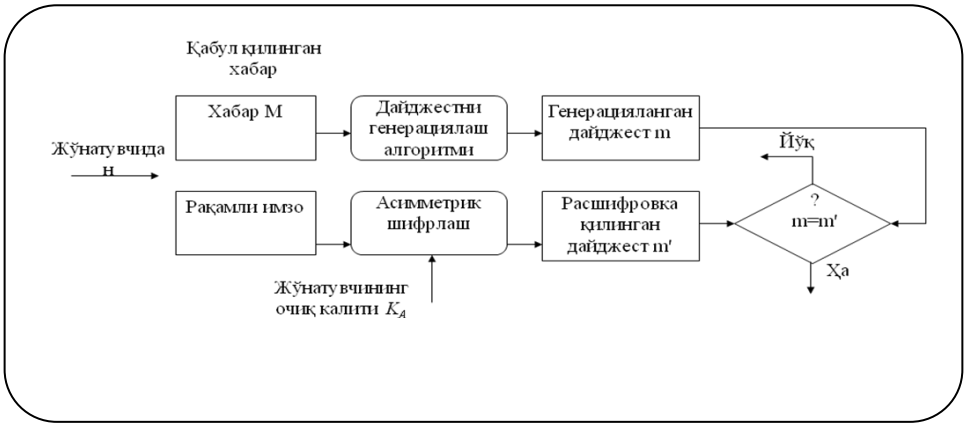
- *raqamli imzoni shakllantirish muolajasi*

-*raqamli imzoni tekshirish muolajasi*

Elektron raqamli imzoni shakllantirish sxemasi



Elektron raqamli imzoni tekshirish sxemasi.



Har bir imzo quyidagi axborotni o’z ichiga oladi:

- imzo chekilgan sana
- ushbu imzo kaliti ta’sirining tugashi muddati
- faylga imzo chekuvchi shaxs xususidagi axborot (F.I.SH., mansabi, ish joyi)
- imzo chekuvchining indentifikatori (ochiq kalit nomi)
- raqamli imzoning o’zi

Ishonchliligining yuqoriligi va shaxsiy kompьyuterlarda amalga oshirilishining qulayligi bilan ajralib turuvchi raqamli imzo algoritmli 1984 yilda El Gamal tomonidan ishlab chiqildi. El Gamalning raqamli imzo algoritmi (EGSA) RSA raqamli imzo algoritmidagi kamchiliklardan holi bo'lib, AQSH ning standartlar va texnologiyalarning Milliy universiteti tomonidan raqamli imzoning milliy standartiga asos kabi qabul qilindi.

5-ilova

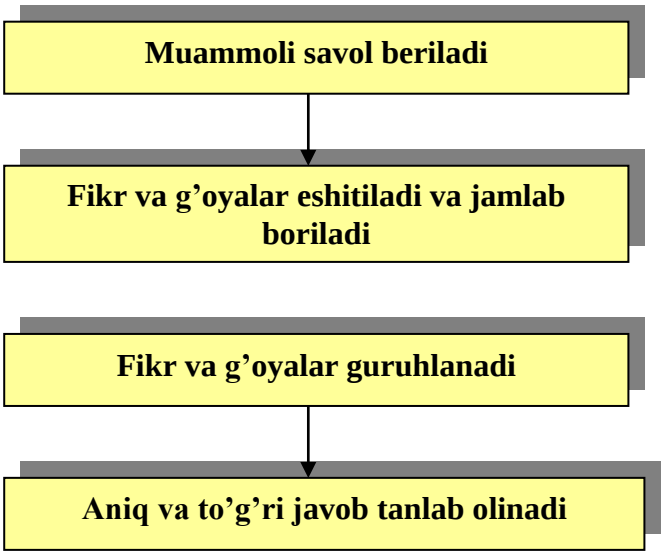
B	BX	B
.....	.....	.....

6-ilova

"Aqliy hujum" metodini qo'llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g'oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g'oyalar, ular hatto to'g'ri bo'lmasa ham inobatga olinadi.
3. Har bir ta'lim oluvchi qatnashishi shart.

Quyida (1-chizma) "Aqliy hujum" metodining tuzilmasi keltirilgan.



1-chizma. "Aqliy hujum" metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. Elektron hujjatlar autentifikatsiyasi
2. Elektron hujjat almashishdagi jinoyatkorona xarakatlar.
3. Elektron raqamli imzo afzalliklari.
4. Raqamli imzoni shakllantirish muolajasi;
5. Raqamli imzoni tekshirish muolajasi.

MAVZU № 9 (4 soat)

ELEKTRON TO‘LOV TIZIMIDA AXBOROTLARNI HIMOYALASH
MA’RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	____ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo’yicha ma’ruza
Mavzu rejasi:	1. Elektron to’lovlar tizimi asoslari. 2. Identifikatsiyalovchi shaxsiy nomerni himoyalash.
Dars maqsadi: Talabalarda elektron to’lovlar tizimi asoslari haqidagi tushunchani hosil qilish qilish	
Pedagog vazifalari:	***O’quv natijalari:***
- Elektron to’lovlar tizimi tushunchasini tushuntirib berish vua ma’ruzani bayon qilish; - Identifikatsiyalovchi shaxsiy nomerni himoyalash tushunchasini talabalarga yetkazish.	- Elektron to’lovlar tizimi tushunchasi haqidagi ma’lumotga ega bo’lishadi va daftarga yozib olishadi; - Identifikatsiyalovchi shaxsiy nomerni himoyalash tushunchasini o’rganadilar va yozib oladilar.
O’qitish usullari	Ma’ruza, B.BX.B metodi, “Aqliy xujum” metodi
Ta’limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko’rgazmali qurollar.
Ta’limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta’minlangan xona.
Nazorat	O’zini-o’zi nazorat qilish

ELEKTRON TO‘LOV TIZIMIDA AXBOROTLARNI HIMOYALASH
MAVZUSIDAGI MA’RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O’qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo’yicha kerakli adabiyotlarni e’lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1. Elektron to’lovlar tizimi asoslari tushunchasini batafsil yoritib beradi. (3-ilova) 2.2. Identifikatsiyalovchi shaxsiy nomerni himoyalash tushunchasi bilan tanishtiradi. (4-ilova)	Yozib oladilar Tinglaydilar va yozib oladilar
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo’yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B metodi (5- ilova) 3.3. “Aqliy xujum” metodini qo’llagan holda tezkor savol-javoblar o’tkaziladi (6-ilova)	Savollar beradi. Jadvalni to’ldirishadi Savollarga javob beradilar

1-ilova

Mavzu: **ELEKTRON TO‘LOV TIZIMIDA AXBOROTLARNI HIMOYALASH**

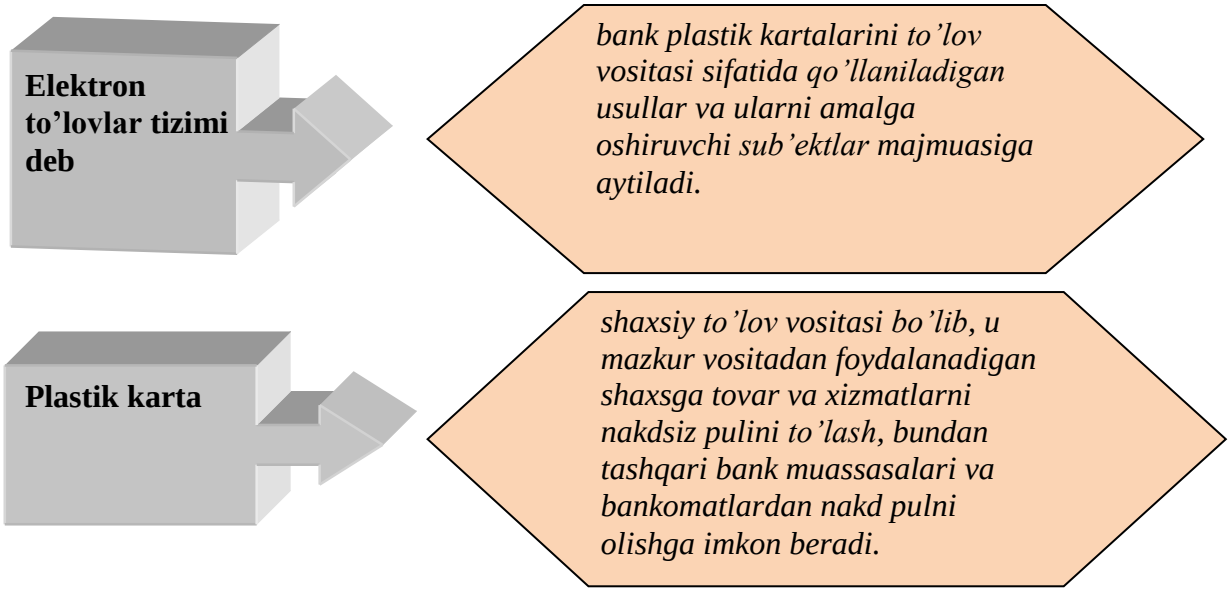
Mavzu rejasi::	1. Elektron to’lovlar tizimi asoslari. 2. Identifikatsiyalovchi shaxsiy nomerni himoyalash.
Darsning maqsadi qilish qilish	Talabalarda elektron to’lovlar tizimi asoslari haqidagi tushunchani hosil

2-ilova

Адабиётлар:

1. Завгородний В.И. Комплексная защита информации в компьютерных тизимх. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
2. Ғаниев С.К.,Каримов М.М. Ҳисоблаш тизимлари ва тармоқларида ахборот ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.-Тошкент давлат техника университети, 2003. 77 б.
3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия - Телеком, 2000. 452с.
4. С.К.Ғаниев, М.М. Каримов, К.А. Тошев «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.

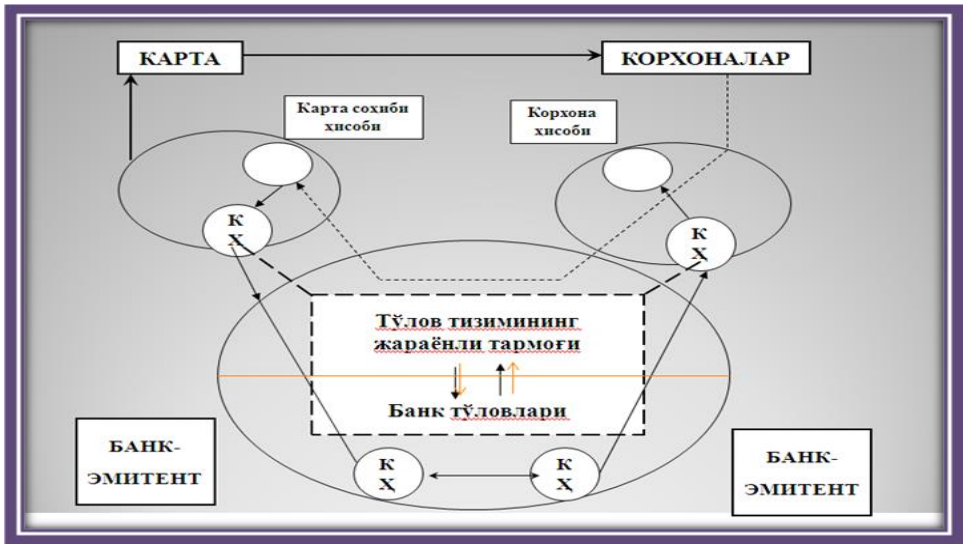
3-ilova



Elektron to’lovlar tizimi bilan birgalikda faoliyat ko’rsatadigan bank ikki, ya’ni ***bank-emitent va bank-ekvayer*** toifasida xizmat ko’rsatadi:

Bank-emitent *plastik kartalarni ishlab chiqaradi va ularning to’lov vositasi sifatida qo’llanilishiga kafolat beradi.*

Bank-ekvayer *savdo va xizmat ko’rsatuvchi tashkilotlar tomonidan qabul qilingan to’lovlarni bank bo’limlari yoki bankomatlar orqali amalga oshiradi.*



Plastik kartalar to’lov bo’yicha **kreditli yoki debetli** bo’lishi mumkin.

Kreditli kartalar bo’yicha karta sohibiga ko’pincha muhlati 25 kungacha bo’lgan vaqtgacha qarz beriladi. Bularga Visa, Master Card, American Express kartalari misol bo’la oladi.

Debetli kartalarda karta sohibining bank-emitentidagi hisobiga oldindan ma’lum miqdorda mablag’ joylashtiradi. Ushbu mablag’dan xarid uchun ishlatilgan mablag’lar summasi oshib ketmasligi lozim.

4-ilova

PIN-kodlarini ximoyalash to’lov tizimi xavfsizligini ta’minlashda asosiy omildir. SHu bois u faqatgina karta sohibiga ma’lum bo’lib, elektron to’lovlar tizimida saqlanmaydi va bu tizim bo’yicha yuborilmaydi.

Umuman olganda, PIN bank tomonidan berilishi yoki mijoz tomonidan tanlanishi mumkin. Bank tomonidan beriladigan PIN quyidagi ikki variantdan biri bo’yicha amalga oshiriladi:

1) mijoz xisob raqami bo’yicha kriptografiya usuli bilan tashkillashtiriladi;

Ushbu usulning afzalligi PIN kodi elektron to'lovlar tizimida saqlanishi shart emasligidadir, kamchiligi esa ushbu mijoz uchun boshqa PIN berilishi lozim bo'lsa, unga boshqa xisob raqami ochilishi zapypligida, chunki bank bo'yicha bitta kalit qo'llaniladi.

2) bank ixtiyoriy PIN kodni taklif qiladi va uni o'zida shifrlab saqlaydi. PIN kodni xotirada saqlash qiyinligi ushbu usulning asosiy kamchiligi bo'lib hisoblanadi.

5-ilova

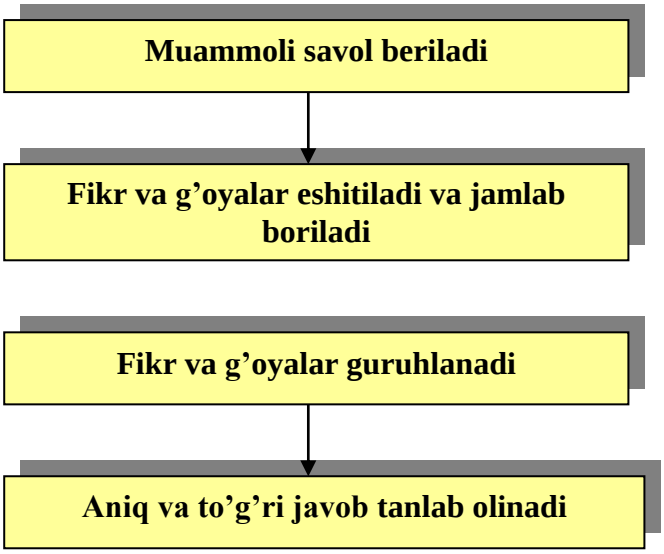
B	BX	B
.....	.....	.....

6-ilova

"Aqliy hujum" metodini qo'llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g'oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g'oyalar, ular hatto to'g'ri bo'lmasa ham inobatga olinadi.
3. Har bir ta'lim oluvchi qatnashishi shart.

Quyida (1-chizma) "Aqliy hujum" metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. Elektron to’lovlar tizimi asoslari iborat?
2. Identifikatsiyalovchi shaxsiy nomerni himoyalash qanday amalga oshiriladi?
3. PIN-kodlarini ximoyalash deganda nima tushuniladi?
4. Plastik kartalar to’lov bo’yicha **kreditli yoki debetli** bo’lishi mumkinmi?
5. Elektron to’lovlar tizimi bilan birgalikda faoliyat ko’rsatadigan bank necha toifaga xizmat ko’rsatadi?

ELEKTRON TO‘LOV TIZIMIDA AXBOROTLARNI HIMOYALASH
MA’RUZA DARSINI OLIB BORISH TEXNOLOGIYASI

Talabalar soni:	____ nafar talaba
Vaqti:	2 soat
Dars shakli:	Mavzu bo’yicha ma’ruza
Mavzu rejasi:	1. POS tizimi xavfsizligini ta’minlash. 2. Bankomatlar xavfsizligini ta’minlash. 3. Axborotlarni himoyalashning asosiy vositalari**.**
Dars maqsadi: Talabalarda axborotlarni himoyalashning asosiy vositalari haqidagi tushunchani hosil qilish qilish	
Pedagog vazifalari:	***O’quv natijalari:***
- POS tizimi xavfsizligini ta’minlash tushunchasini tushuntirib berish; - Bankomatlar xavfsizligini ta’minlash tushunchasini talabalarga yetkazish; - Axborotlarni himoyalashning asosiy vositalari haqida tushuncha kiritish.	- POS tizimi xavfsizligini ta’minlash haqidagi ma’lumotga ega bo’lishadi; - Bankomatlar xavfsizligini qanday ta’minlash mumkinligini o’rganadilar; - Axborotlarni himoyalashning asosiy vositalari haqidagi tushunchaga ega bo’ladilar.
O’qitish usullari	Ma’ruza, insert jadvali
Ta’limni tashkil etish shakli:	Suhbat, frontal
Didaktik vositalar:	Slaydlar, ko’rgazmali qurollar.
Ta’limni tashkil etish sharoiti:	Maxsus texnik jihozlar bilan ta’minlangan xona.
Nazorat	O’zini-o’zi nazorat qilish

ELEKTRON TO‘LOV TIZIMIDA AXBOROTLARNI HIMOYALASH
MAVZUSIDAGI MA’RUZA DARSIGA
TEXNOLOGIK XARITA

Faoliyat bosqichlari	***Faoliyatning mazmuni***	
	O’qituvchi	***Talaba***
1-bosqich. Mavzuga kirish. (10 min)	1.1. Mavzu, uning maqsadi va reja savollarini ekranga chiqariladi. (1-ilova) 1.2. Mavzu bo’yicha kerakli adabiyotlarni e’lon qiladi (2-ilova)	Eshitadilar, yozib oladilar Yozib oladilar.
2-bosqich. Asosiy qism. (60 min)	2.1. POS tizimi xavfsizligini ta’minlash tushunchasini batafsil yoritib beradi va ma’ruzani bayon qiladi. (3-ilova) 2.2. Bankomatlar xavfsizligini qanday ta’minlash tushunchasi bilan tanishtiradi. (4-ilova) 2.3. Axborotlarni himoyalashning asosiy vositalarini keltirib o’tadi. (5-ilova)	Yozib oladilar Tinglaydilar va yozib oladilar Yozib oladilar
3-bosqich. Yakunlovchi qism. (10 min)	3.1. Mavzu bo’yicha yakunlovchi xulosa qiladi. 3.2. Mavzu maqsadiga erishishdagi talabalar faoliyati tahlil qilinadi. B.BX.B	Savollar beradi. Jadvalni to’ldiradilar

	metodi (5- ilova) 3.3. “Aqliy xujum” metodini qo’llagan holda tezkor savol-javoblar o’tkaziladi (6-ilova)	Savollarga javob beradilar

1-ilova

Mavzu: **ELEKTRON TO‘LOV TIZIMIDA AXBOROTLARNI HIMOYALASH**

Mavzu rejasi::	1. POS tizimi xavfsizligini ta’minlash. 2. Bankomatlar xavfsizligini ta’minlash. 3. Axborotlarni himoyalashning asosiy vositalari**.**
Darsning maqsadi Talabalarda axborotlarni himoyalashning asosiy vositalari haqidagi tushunchani hosil qilish qilish	

2-ilova

Адабиётлар:

1. Завгородний В.И. Комплексная защита информации в компьютерных тизимх. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
2. Ғаниев С.К.,Каримов М.М. Ҳисоблаш тизимлари ва тармоқларида ахборот ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.- Тошкент давлат техника университети, 2003. 77 б.
3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия - Телеком, 2000. 452с.
4. С.К.Ғаниев, М.М. Каримов, К.А. Тошев «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.

3-ilova

Ushbu chizma bo'yicha xaridor o'z plastik kartasini o'rnatib, PIN kodini kiritadi.

Sotuvchi o'z navbatida pul summasini kiritadi. Shundan so'ng, bank-ekvayerga (sotuvchi banki) pulni ko'chirish uchun so'rovnoma yuboriladi.

Bank-ekvayer, o'z navbatida, kartaning xaqiqiyligini aniqlash uchun so'rovnomani bank-emitentga jo'natadi. Natijada, bank-emitent pulni bank-ekvayerga sotuvchi xisobiga ko'chiradi. Pul ko'chirilgandan sung, bank-ekvayer tomonidai POS-terminalga xabarnoma jo'natiladi. Ushbu xabarda tranzaktsiya bajarilganligi xaqida ma'lumot bo'ladi.

4-ilova

Bankomat ikki rejimda ishlaydi,
off-line va on-line.

Off-line — *rejimda bankomat bank kompьyuterlaridan mustaqil ishlaydi va bajariladigan tranzaktsiyalar xaqidagi yozuvlarni o'z xotirasida saqlaydi xamda printerga uzatib, ularni chop qiladi.*

On-line — *rejimda bankomat bevosita bank kompьyuterlari bilan telekommunikatsiya orqali ulangan bo'ladi.*

5-ilova

Xozirgi kunda SSL (Secure Socket Layer) va SET (Secure Electronic Transactions) protokollari ishlab chiqilgan:

SSL protokoli ma'lumotlarni kanal darajasida shifrlashda qo'llaniladi;

SET xavfsiz elektron tranzaktsiyalari protokoli yaqinda ishlab chiqilgan bo'lib, faqatgina moliyaviy ma'lumotlarni shifrlashda qo'llaniladi.

SET protokolining joriy etilishi bevosita Internetda kredit kartalar bilan to'lovlar sonining keskin oshishiga olib keladi.

SET protokoli quyidagilarni ta’minlashga kafolat beradi:

axborotlarning to’liq maxfiyligi, chunki foydalanuvchi to’lov ma’lumotlarining himoyalanganligiga to’liq ishonch xosil qilishi kerak;

ma’lumotlarning to’liq saqlanishi, ya’ni ma’lumotlarni uzatish jarayonida buzilmasligini kafolatlash. Buni bajarish omillaridan biri raqamli imzoni qo’llashdir;

kredit karta sohibining xisob raqamini audentifikatsiyalash, ya’ni elektron (rakamli) imzo va sertifikatlar xisob raqamini audentifikatsiyalash va kredit karta sohibi ushbu xisob raqamining xaqiqiy egasi ekanligini tasdiqlash;

tijoratchini o’z faoliyati bilan shug’ullanishini kafolatlash, chunki kredit karta soxibi tijoratchining xaqiqiyligini, ya’ni moliyaviy operatsiyalar bajarishini bilishi shart. Bunda tijoratchining raqamli imzosini va sertifikatini qo’llash elektron to’lovlarning amalga oshirilishini kafolatlaydi.

6-ilova

V	+	–	?

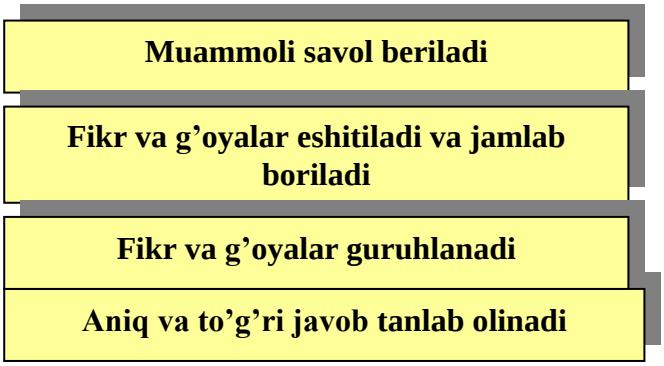
“V”- men bilgan ma’lumotlarga mos;
“-“ - men bilgan ma’lumotlarga zid;
“+” - men uchun yangi ma’lumot;
“?” - men uchun tushunarsiz yoki ma’lumotni.

7-ilova

“Aqliy hujum” metodini qo’llashdagi asosiy qoidalar:

1. Bildirilgan fikr-g’oyalar muhokama qilinmaydi va baholanmaydi.
2. Bildirilgan har qanday fikr-g’oyalar, ular hatto to’g’ri bo’lmasa ham inobatga olinadi.
3. Har bir ta’lim oluvchi qatnashishi shart.

Quyida (1-chizma) “Aqliy hujum” metodining tuzilmasi keltirilgan.



1-chizma. “Aqliy hujum” metodining tuzilmasi

AQLIY XUJUM SAVOLLARI:

1. POS tizimi xavfsizligini ta’minlash deganda nima tushunasiz?
2. Bankomatlar xavfsizligini ta’minlash usullarini sanab o’ting?
3. Axborotlarni himoyalashning asosiy vositalari nimadan iborat?
4. Elektron to’lov qanday amalga oshiriladi?
5. SET protokoli nimalarni ta’minlashga yordam beradi?