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

BUXORO MUHANDISLIK TEXNOLOGIYA INSTITUTI

«Informatika va axborot texnologiyalari» kafedrasi

5140900 – Kasb ta’limi («Informatika va axborotlar texnologiyalasi») ta’lim yo’nalishi bo’yicha

Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturini yaratish mavzusidagi

BITIRUV MALAKAVIY ISH

Bajardi: **16-09 MIIT guruhi talabasi**
Rustamov Karim Qahhorovich

Rahbar: **Sohibov T.F.**

Himoyaga ruxsat etildi

“____”_____2013y.

Kafedra mudiri: _____ dots. Razzoqov Sh.I.

BUXORO - 2013

BUXORO YUQORI TEXNOLOGIYALAR MUHANDISLIK TEXNIKA INSTITUTI
«TEXNOLOGIK JARAYONLARNI AVTOMATLASHTIRISH» fakulteti

«Informatika va axborot texnologiyalari» kafedrasi

5140900 – Kasb ta'limi («Informatika va axborotlar texnologiyasi») ta'lim yo'nalishi
14-09 MIIT guruhi

«Tasdiqlayman»_____
Kafedra mudiri dots.Razzoqov Sh.I.
12.11.2012 y.

BITIRUV MALAKAVIY ISHI BO'YICHA TOPSHIRIQ

Talabasi *Rustamov Karim Qahhorovich*

1. Bitiruv malakaviy ish mavzusi *Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturini yaratish.*

Kafedra majlisida 08.11.2012 yil tasdiqlangan.

2. Bitiruv malakaviy ishini topshirish muddati: 5.06.2013yil

3. Bitiruv malakaviy ishni bajarish uchun kerakli ma'lumotlar:

Adabiyotlar, BMI mavzusi bo'yicha nazariy ma'lumotlar, dastur interfeysini yaratishda Turbo Pascal dasturi.

4. Hisoblash-tushuntirish yozuvlarining tarkibi (ishlab chiqilgan masalalar ro'yxati):

Kirish; Mavzu bo'yicha nazariy ma'lumotlar; Asosiy qism; Mavzu mazmunining qisqacha bayoni; BMI dasturiy mahsulotini yaratish tartibi va uni yaratishda qo'llaniladigan dastur tizimlari; Hayot faoliyati xavfsizligi; Xulosa; Foydalanilgan adabiyotlar ro'yxati; Ilova.

5. Chizma ishlab chiqarish ro'yxati (chizmalar nomi aniq ko'rsatiladi): *Yo'q*

6. Bitiruv ishi bo'yicha maslahatchilar:

№	Bo'lim mavzusi	Maslahatchi o'qituvchi	Imzo	
			Topshiriq Berildi	Topshiriq Bajarildi
1	Nazariy qism	Sohibov T.F.		
2	Asosiy qism	Sohibov T.F.		
3	Hayot faoliyati xavfsizligi qismi	Beshimov Yu.		

7. Bitiruv ishini bajarish rejasi:

№	Bitiuv ishi bosqichlari nomi	Bajarish muddati, sana	Tekshiruvdan o'tganlik belgisi
1	Mavzu bilan tanishish, adabiyotlar ustida ishlash	Sentabr-Oktabr	
2	Bitiruv malakaviy ishining I bobi ustida ishlash	Noyabr-Dekabr	
3	Bitiruv malakaviy ishi mavzusining dasturi ustida ishlash	Yanvar-Fevral	
4	Bitiruv malakaviy ishining II bobi ustida ishlash	Aprel	
5	«Hayot faoliyati xavfsizligi» bobi ustida ishlash	May	
6	Bitiruv malakaviy ishini rasmiylashtirish	Iyun	
7	Bitiruv malakaviy ishi himoyasiga tayyorlanish	__iyun __ iyun	
8	Bitiruv malakaviy ishini himoya qilish	_____iyun	

Bitiruv malakaviy ishi rahbari: _____ Sohibov T.F.

Topshiriqni bajarishga oldim: _____ Rustamov K.Q.

Topshiriq berilgan sana: 15.11.2012 yil

16-09 MIIT guruhi talabasi Rustamov Karim Qahhorovichning “Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturini yaratish” mavzuidagi bitiruv malakaviy ishiga

ANNOTATSIYA

Zamonaviy axborot kommunikatsiya texnologiyalarining hayotimizning barcha jabhalariga shiddat bilan kirib kelishi, internetning keng ko’lamda qo’llanilishi axborot ayirboshlashni osonlashtirdi va tezlashtirdi. O’z navbatida bu imkoniyatlar axborotni ug’irlashni osonlashtirdi. Shuning uchun bugungi kunda axborot himoyasini ta’minlash yanada dolzarb muammoga aylandi. Shu sababli axborotni himoylash uchun turli xil usullardan foydalanilmoqda. Bu usullardan biri kriptografik usullardir. Kriptografik usullar qadimiy va turli-tumandir. Axborotni himoylashda kriptografik usullarni qo’llash uchun ular haqida tushunchaga ega bo’lish lozim. Ushbu BMI da aynan shu haqda tafsif berilgan va ta’limiy xarakterga ega bo’lgan dastur yaratilgan.

Ushbu BMI ning tarkibi: Kirish, Nazariy qism, Asosiy qism, Hayot faoliyati xavfsizligi qismi, Ilova, Xulosa, Adabiyotlar ro`yxati.

Kirish. Axborotlarni himoyalashning dolzarbligi, ishning maqsad va vazifalari hamda uning amaliy ahamiyati haqidagi ma’lumotlar keltirilgan.

Mavzuga doir tayanch ma`lumotlar nazariy qismda kiritilgan. Bu qismda axborotlashgan jamiyatda elektron hujjatlar, axborot xavfsizligi va axborot urushlari, axborotlar xavfsizligi tushunchalari va himoya tizimlari hamda kriptografiya – maxfiy xabarning ma`nosini yashirish haqida qisqacha ma’lumotlar keltirilgan.

Asosiy qismda Tsezar usuli va kalit so`zli Tsezar tizimi, Affin tizimidagi Tsezar usuli, Affin tizimidagi Tsezar usulida matnlarni shifrlash dasturini hamda Affin tizimidagi Tsezar usulida matnlarni deshifrlash dasturini yaratish tahlillari berilgan.

Hayot faoliyati xavfsizligi qismida inson organizmining tashqi muhitga moslashuvi, iIshlab chiqarish mikroiqlimining gigienik me`yorlari, atmosfera tarkibidagi changlar va ish joyidagi havo muhiti ma’lumotlar berilgan.

Xulosa qismida axborotlarni himoyalashda kriptografiyaning va uni o’rganishda ta’limiy xarakterdagi dasturlarning ahamiyati hamda Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturi haqida fikrlar keltirilgan.

Ilova qismida Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlashni o`rgatish metodikasi visual materiallari, dasturlar algoritmlari blok-sxemalari hamda Affin kriptotizimi dasturlari ekran ko’rinishlari berilgan.

Adabiyotlar ro`yxatida BMI ni tayyorlashda kerak bo`lgan barcha adabiyotlar ro`yxati kiritilgan.

Buxoro muhandislik texnologiya instituti 16-09 MIIT guruhi talabasi Rustamov Karim Qahhorovichning “Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturini yaratish” mavzusidagi bitiruv malakaviy ishiga

TAQRIZ

Axborotlar xavfsizligini ta’minlash hozirgi kunda eng dolzarb muammolardan biri hisoblanadi. Bu muammoni hal qilishda turli xil usullar qo’llaniladi. Bo usullardan biri kriptografiyadir. Ushbu ta’limiy xarakterdagi “Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturini yaratish” mavzusidagi ish orqali kriptografiya va uning usullari haqida tushunchaga ega bo’lish mumkin.

Bitiruv malakaviy ish kirish, nazariy qism, asosiy qism, hayot faoliyati xavfsizligi qismi, xulosa, adabiyotlar ro`yxati va ilova qismlaridan tashkil topgan.

Bitiruv malakaviy ishining asosiy qismida Tsezar usuli va kalit so`zli Tsezar tizimi, Affin tizimidagi Tsezar usuli, Affin tizimidagi Tsezar usulida matnlarni shifrlash dasturini hamda Affin tizimidagi Tsezar usulida matnlarni deshifrlash dasturini yaratish tahlillari misollar orqali keng yoritib berilgan.

Bitiruv malakaviy ishning dolzarbligini, talaba uni aniq tavsiflay olganligini, u davlat standartlari nizomi talablarga to`liq javob berishni hisobga olib, talaba Rustamov Karimga «Muallim informatika va axborotlar texnologiyasi» mutaxassisligi bakalavri ilmiy darajasi berishga va ishni a’lo (86 foiz) bahoga loyiq deb hisoblayman.

Rahbar: Sohibov T.F.

MUNDARIJA

KIRISH

Axborot asrida, axborotlashgan jamiyatda dunyoni harakatlantiruvchi asosiy kuch axborot ekani hech kimga sir emas. Agar qorayib 9 asr davom etgan agrar davrda er, 300 yilga yaqin davom etgan sanoat (industrial) zamonida asosiy boylik texnika sanalgan bo`lsa, XX asr oxiriga kelib insoniyat tarixida ilk bor sanoat rivojlangan mamlakatlar ijtimoiy ishlab chiqarishda axborotlar mehnatining asosiy predmeti bo`lib qoldi. XX asrning ikkinchi yarmida paydo bo`lgan turli axborotlar oqimi global tizimda hal qiluvchi ahamiyat kasb etadigan bo`ldi. Hozirgi mehnat resurslarini moddiy ishlab chiqarish sohasidan axborot sohasiga bevosita jalb etish tendentsiyasi yuzaga kelgan-ki, bu endilikda axborot inqolobi nomini olgan eng sezilarli belgiga aylangan. Axborot, energiya, vazn, bo`shliq va vaqtni bir butun holda batafsil o`rganish hozirgi vaqtda inson hayotining barcha jabhalarida muhim ahamiyatga ega bo`lib kelmoqda. Shu bois oliy o`quv yurtlarining XXI asr bitiruvchilari bundan keyingi axborotlashtirilgan jamiyatda ishlashni yangi sharoitlarga ijodiy va kasbiy yondoshishga tayyorlangan bo`lishlari kerak.

Mavzuning dolzarbligi. Sir emas, internet va yuqori texnologiyalardan foydalanish bugungi kun odamining odatiy ehtiyojlaridan biriga aylangan. Hozir dunyo bo`ylab aylanayotgan axborot miqdorining oshib, borayotgani hisobiga uning foydali va zararli tomonlari ham ko`rinib qolmoqda. Ayni paytda bunda xavfsizlikka ega bo`lish, uni ta`minlash chora – tadbirlarini ham e`tibordan chetda qoldirmaslik zarur. Negaki, so`nggi o`n yillikda dunyodagi kiberxavfsizlik tushunchasi batomom o`zgardi, qachonlardir bir xakerning nojuya hatti – harakatlari sifatida e`tirof etilgan kiberxurujlar bugungi kunga kelib kompleks shaklga ega bo`ldi va chinakam tahdid ko`rinishini oldi. Shu bois o`z muhim axborotlarini kiberxurujlardan himoya qilishni istagan davlatda bu boradagi dasturlar keng ko`lamda tadbiq etilmoqdaki, buning natijasi o`laroq, kibermakon xavflariga ongli ravishda qarshi ko`rashishga erishish maqsad qilinmoqda. Tabiiyki, bunday sharoitda axborot xavfsizligi masalasi dolzarb ahamiyatga ega. Shuning uchun, axborot xavfsizligi masalasiga jiddiy qarashimiz, uning tarixi, qo`llanilgan usullari va erishgan yutuqlari bilan tanishib borishimiz muhim hisoblanar ekan. Bundan, axborot xavfsizligini ta`minlashning usullaridan biri bo`lgan ushbu ‘Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash

dasturini yaratish’ mavzusidagi bitiruv malakaviy ishining dolzarb va muhim ekanligi ravshan bo`ladi.

Ishning maqsadi. Ushbu bitiruv malakaviy ishi mavzusi orqali axborotlar xavfsizligi muammolari, axborotlashgan jamiyatda elektron axborotlardan foydalanish va uni himoya qilish qanchalik muhim va ahamiyatga ekanligini yoritish, kriptografiyaning axborotlarni himoyalashning usullaridan biri ‘Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturini yaratish’ mavzusini tahlil qilgan holda, ushbu himoyalash usulini batafsil bayon etish va ta`limiy xarakterdagi dasturiy mahsulotni yaratish asosiy maqsadimizdir.

Ishning vazifasi. Mavzu doirasida axborotlashgan jamiyatda elektron axborotlar xavfsizligini ta`minlash muhimligi va uning asosiy tushunchalarini tavsiflagach, matnlarni Affin usuli orqali shifrlash va deshifrlash tizimi hamda u orqali matnlarni himoyalashga doir tahlillarimizni hamda dasturiy ta`minotni yaratishga doir tadqiqotlarimizni bayon qilamiz.

Ishning amaliy ahamiyati. Biz o`z bitiruv malakaviy ishimizda axborotlarni Affin usuli orqali shifrlash va deshifrlashni tahlil qilib, ta`limiy xarakterdagi dasturiy mahsulotni yaratishga e`tiborni qaratishni maqsad qilib oldik. Bu orqali, axborot xavfsizligini ta`minlash bo`yicha ta`limiy xarakterdagi ma`lumot va dasturiy mahsulot yuzaga keladi. Chunki, har qanday kriptotizim uslubi bayoni va matnlarni kompyuter texnikasidan foydalangan holda shifrlash va deshifrlash dasturi, kriptografiyani rivojlanishi uchun amaliy ahamiyatga ega hisoblanadi.

Ishning ilmiy yangiligi. Axborot xavfsizlini ta`minlash bo`yicha ta`limiy xarakterdagi har qanday kriptotizim uslubining batafsil tavsifi va dasturiy tadbigi ilmiy ahamiyatga ega hisoblanadi.

Tadqiqot ob`ekti va predmeti. Kompyuter muhitida saqlanayotgan axborotlar va ularning xavfsizligini ta`minlashning kriptografik usullari.

I. Elektron axborotlar va ular xavfsizligi

1.1. Axborotlashgan jamiyatda elektron hujjatlar

So`nggi paytlarda ‘elektron’ so`zi bilan boshlanuvchi iboralarga tez-tez ko`zimiz tushadi yoki eshitamiz. Ularga ko`p eshitadigan va ko`radigan ‘elektron hukumat’, ‘elektron ta`lim’, ‘elektron to`lov’, ‘elektron tijorat’, elektron raqamli imzo’, ‘elektron hujjat aylanishi’, ‘elektron axborot resurslari’, ‘elektron kitob’, ‘elektron pocha’ singari so`zlar misol bo`la oladi. Hattoki, oddiy kishilarimiz tilida ham ‘elektron versiya’ iborasi ko`p ishlatiladi. Qaysi bir idoraga kirmang, hujjatning ham qog’ozdagi matni, ham elektron versiyasi so`raladi. Bu bejiz emas, albatta. Zero, rivojlanish, taraqqiyot, xalqaro integratsiya, tovarlar, xizmatlar va sarmoyalarning butun dunyo bo`ylab erkin harakatlanishi va nihoyat, kuchli davlatdan kuchli fuqarolik jamiyati sari boshlangan harakatlarimizning o`zi shunga etaklamoqda.

Bizga, asosan, fizika ilmi orqali tanish bo`lgan ‘elektron’ so`zi ijtimoiy-iqtisodiy, siyosiy munosobatlarga ham ko`chdi. Aynan shu yo`nalishdagi qonunlarning qabul qilinishi mamlakatimiz ijtimoiy-siyosiy hayotida muhim ahamiyatga egadir.

O`zbekiston Respublikasining 2003 yil 11 dekabrda qabul qilingan ‘Elektron raqamli imzo to`g’risida’gi qonuni elektron raqamli imzodan foydalanish sohasidagi munosobatlarni tartibga solishga qaratilgan. Tabiiy savol tug’iladi: imzo ham elektron raqamli bo`ladimi? Ishga kirayotganimizda, bankdan kredit olayotganimizda, xorijga chiqish uchun viza olayotganimizda, nikohdan o`tayotganimizda, oylik maosh olayotganimizda va boshqa rasmiy hujjatlarda ‘jonli’ imzo qo`yib, tasdig’imizni bildiramiz. Endilikda ko`rib - eshitib turganimizdek, ‘elektron raqamli imzo’ iborasi iste`molga kirib keldi.

Qonunga ko`ra, bunday imzo elektron hujjatdagi axborotni raqamli imzoning yopiq kalitidan foydalangan holda maxsus o`zgartirish natijasida hosil qilinadi. Ushbu kalit yordamida elektron hujjatdagi axborotda xatolik yo`qligi aniqlanadi va imzo yopiq kalitining egasini identifikatsiya qilish imkoniyati tug’iladi. Yopiq kalit elektron raqamli imzo vositalaridan foydalangan holda hosil qilinib, faqat imzo qo`yuvchi shaxsning o`ziga ma`lum bo`ladi. Elektron hujjatda imzoni yaratish uchun muljallangan belgilar ketma - ketligi ta`minlanadi.

Elektron raqamli imzo bilan elektron hujjatlar tasdiqlanadi. Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan hamda hujjatni identifikatsiya qilish

imkonini beradigan, boshqa rekvizitlarga ega bo`lgan axborot ko`pchilik uchun qulay hisoblanadi.

Elektron raqamli imzo kaliti vakolatli organda davlat ro`yxatidan o`tgan, yuridik shaxs maqomiga ega bo`lgan Ro`yxatga olish markazlari tomonidan yaratiladi, muhofaza qilinishi ta`minlanadi. Elektron raqamli imzo kalitlari sertifikatlarning reestri yuritiladi, vaqti-vaqti bilan yangilanadi hamda undan yuridik va jismoniy shaxslarning erkin foydalana olish imkoniyati ta`minlanadi. Yuridik va jismoniy shaxslarga elektron raqamli imzo kaliti elektron shaklda va qog'oz ko`rinishida beriladi, ular o`z elektron raqamli imzolari haqiqiyligini tasdiqlagandagina u haqiqiy kuchga egadir.

Elektron raqamli imzoni yaratgan (elektron hujjatga imzo qo`ygan) va Ro`yxatga olish markazi tomonidan rasmiylashtirilib, sertifikat berilgan jismoniy shaxs uning haqiqiy egasidir va u qonunga ko`ra, o`z imzosining foydalanishi ustidan nazoratni ta`minlaydi. Elektron raqamli imzo elektron raqamli imzoning yopiq kalitidan foydalanish rejimi buzilganda jismoniy va yuridik shaxs o`zi ro`yxatga olingan markazga xabar qilishi va uning amal qilishini to`xtatib to`rishi mumkin. Keyinchalik qonunga muvofiq elektron raqamli imzo qaytadan tiklanadi.

2004 yil 29 aprelda 'Elektron hujjat aylanishi to`g'risida', 'Elektron tijorat to`g'risida'gi qonunlar qabul qilindi.

Elektron hujjat aylanishi nima? Elektron hujjat aylanishi shunday hujjatlarni axborot tizimi orqali jo`natish va qabul qilib olishdan iborat. Bitimlar va shartnomalar tuzishda, hisob-kitoblarni, rasmiy va norasmiy yozishmalarni amalga oshirishda va boshqa axborotlarni o`zatishda elektron hujjat aylanishi qo`l keladi.

Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va hujjatni identifikatsiya qilish imkoniyatini beradigan boshqa majburiy rekvizitlarga ega bo`lgan axborot bugungi kunda qulay va tezkor hisoblanadi.

Elektron hujjat texnika vositalaridan va axborot tizimlari xizmatlaridan foydalanilgan holda yaratiladi, ishlov beriladi va saqlanadi. Eng muhimi, bunday hujjat elektron hujjat aylanishi ishtirokchilari (elektron hujjatni jo`natuvchi, uni qabul qilib oluvchi, shuningdek, axborot vositachilari)ning mazkur hujjatni idora etish imkoniyatini inobatga olgan holda yaratilishi kerak. Elektron hujjat qog'oz hujjatga tenglashtiriladi va u bilan bir xil yuridik kuchga egadir.

So`nggi paytlarda internet tarmog'i orqali samolyotda uchish uchun aviachipta, sport musoboqalariga, teatr, kontsert zallariga chipta sotib olish imkoniyati tug'ildi. Ha, elektron tijoratga ham qadam qo`ydik. Axborot tizimlaridan foydalangan holda amalga oshiriladigan, tovarlarni sotish, ishlarni bajarish va xizmatlar ko`rsatishga doir tadbirkorlik faoliyati elektron tijoratdir. Elektron tijoratni amalga oshiruvchi yuridik va jismoniy shaxslar, shuningdek, tegishli tovarlarning (ishlarning, xizmatlarning) xaridori bo`lgan yuridik va jismoniy shaxslaruchun buning ahamiyati katta. Elektron tijoratda axborot vositachilari ham ishtirok etishi mumkin. Qonunga ko`ra, elektron tijoratni amalga oshiruvchi yuridik va jismoniy shaxslar tovarlar (ishlar, xizmatlar) xaridoriga uning tashkiliy-huquqiy shakli ko`rsatilgan holdagi to`liq nomini va boshqa ma`lumotlarni taqdim etadi yoxud uning bunday axborotdan foydalanish erkinligini ta`minlaydi.

Elektron tijoratdagi shartnoma bandlari qonun hujjatlrining talablariga muvofiq bo`lishi kerak. Ya`ni, shartnoma taraflari fuqarolik-huquqiy muomala layoqatiga ega bo`lishlari, tuzilayotgan shartnoma umuminsoniy qadriyatlarga mos bo`lishi, shunchaki ko`zbuyamachilik uchun emas, balki haqiqiy qonun doirasidagi ishni amalga oshirishlari lozim.

2005 yil 16 dekabrda 'Elektron to`lovlar to`g'risida' qonun qabul qilindi. Pulning vazifalaridan biri bu uning to`lov vazifasi ekanligidir. Bir paytlar pul-to`lov vazifasini nimalar bajarmadi, ha, taraqqiyot tufayli elektron to`lov davriga ham etib keldik.

Qonunga ko`ra, texnika vositalaridan, axborot texnologiyalaridan va axborot tizimlari xizmatlaridan foydalangan holda naqd pulsiz hisob-kitoblarni amalga oshirish elektron to`lov hisoblanadi. Mamlakatimizda to`lov tizimining banklararo jarayoni amalga oshiriladi, bankning ichki to`lov tizimi, chakana to`lovlar tizimi turlari ham mavjud.

Banklararo to`lov tizimi banklar o`rtasidagi elektron to`lovlarni O`zbekiston Respulikasi Markaziy bankida ochilgan vakillik hisobvaraqlari orqali amalga oshiriladi. Muassasa filiallari va mijozlar o`rtasida elektron to`lovlar o`zaro harakatda bo`lishi uchun chakana to`lovlar tizimi bank kartalari va boshqa vositalardan foydalaniladi. Bunda elektron to`lovlar vositasi uning mazkur chakana to`lovlar tizimiga mansubligini identifikatsiyalash imkoniyatini beradigan farqlovchi belgilarga (tovar va xizmat ko`rsatish belgilariga) ega bo`lishi kerak.

Muhimi, elektron to`lovlar hujjati pul hisob-kitoblari aks etgan varaqalarga tenglashtiriladi va u bilan bir xil yuridik kuchga egadir. To`lov tizimida ishtirok etayotgan shaxslar bunga tegishli barcha ma`lumotlarning maxfiyligini ta`minlashlari kerak. Qonunda belgilangan hollardan tashqari, elektron to`lovlar to`g'risidagi ma`lumotlar uchinchi bir shaxsga taqdim etilmaydi. Bir so`z bilan aytganda, bugungi kunga qadar elektron vositalar bilan bog'liq operatsiyalar, harakatlar ko`paymoqda. Dunyoning rivojlangan mamlakatlarida qo`llanilayotgan bu tajribaning mamlakatimiz bank tizimiga kirib kelishi nafaqat sarf xarajatlarni qisqartiradi, balki fuqarolarimizning ham imkoniyatlarini kengaytiradi. Prezidentimizning 2010 yilda mamlakatimizni ijtimoiy-iqtisodiy rivojlantirish yakunlari va 2011 yilga mo`ljallangan eng muhim ustivor yo`nalishlarga bag'ishlangan Vazirlar Mahkamasining majlisidagi ma`ruzasida o`quv jarayoniga keng formatli kommunikatsiya tarmoqlari va internet texnologiyalarini joriy qilish maqsadida 'Elektron ta`lim' milliy tarmog'ini barpo etishni nihoyasiga etkazish vazifasini muhim msalalaridan biri sifatida alohida ta`kidlab o`tganlar. Butun dunyoda 'elektron hukumat' haqida so`z yuritilayotgan bir paytda O`zbekiston Respublikasida ham zamon bilan hamnafaslik muhiti yaratilmoqda. Normativ-huquqiy bazaning haddan ziyod katta hajmda ekanligi, davlat (davlatlar) hududining bepoyonligi va nihoyat, bugungi globallashuv davri va shart-sharoitlar elektron hukumat mavjud bo`lishini talab etadi. Bularning barchasi yangilikka, ezgulikka, taraqqiyotga intilib yashash va ishlashga undaydi.

1.2. Axborot xavfsizligi va axborot urushlari

Xavfsizlik, bu har kuni biz to`qnashadigan va rioya qiladigan ehtiyot choralari bo`lib, u hayotimizning ajralmas qismiga aylanib ulgurgan jihatidir. eshikni qulflaymiz, qimmatbaho narsalarni begona ko`zlardan berkitamiz va hamyonni duch kelgan joyda qoldirmaymiz, sirlarimizni har kimga ham aytavermaymiz, muhim xabarlar yozilgan maktublarni konvertga solib, uni elimlab uzatamiz. Muassasa va tashkilotlarda, hatto kichik muassasalarda ham binosining kirish yo`lida sizni qorovul, yoki kirishni chegaralovchi va nazoratlovchi tizimi qarshi oladi. Ammo, muassasaga tegishli muhim axborotni himoyalash esa hali ko`ngildagidek emas. Axborotni qanday yo`qotish mumkinligini va bu qanday oqibatlarga olib kelishini barcha ham tushunavermaydi. Ayniqsa, hozirgi kunda axborot kommunikatsiya

texnologiyalari rivojlangan va barcha axborotlar kompyuterda yaratilayotganligi hamda kompyuter tarmog'i orqali uzatilayotganligi va qabul qilinayotganligi hamda davlatlar 'Elektron hukumat' ni tadbiq etayotganligi sababli axborot xavfsizligini ta`minlash yanada murakkablashib bormoqda. Chunki axborotlar xavfsizligini ta`minlashning yangi usullari va vositalari ishlab chiqilsa, o`z navbatida uni buzishning yangi usullari va vositalari ham parallel ravishda ishlab chiqilmoqda. Axborotga nisbatan tahdidlar kun sayin oshib bormoqda.

Odatda insonlardan yoki vositalardan chiqadigan va zarar etkazadigan tahdidlar quyidagi sinflarga bo`linadi: ichki yoki tashqi va tuzilmalangan (ma`lum ob`ektga qarshi) yoki tuzilmalanmagan ('kimga Xudo beradi' qabilida adreslanuvchi). Masalan, kompyuter viruslari 'tashqi tuzilmalanmagan tahdidlar' sifatida turkumlanadi va tamomila oddiy hisoblanadi. Ko`pchilik foydalanuvchilar o`zlarining kompyuterini muayyan nishon deb hisoblamaydilar va o`zlarini yaxshigina himoyalangandek sezadilar. Ammo, ularga ham hujumlar uyushtirilishini va kerakli axborotlari o`g'irlanishini sezmaydilar. Agar ularda arzigulik axborotlar mavjud bo`lmasa hamda kompyuter tarmog'iga ulanmagan bo`lishsada, ko`pchilik hollarda axborotlari o`chiriladi va dasturiy ta`minotlari ishdan chiqariladi. Sizga uyushtirilayotgan hujum darajasi aksariyat hollarda ishingizning holatiga bog'liq. Agar tashkilotingiz yoki kompaniyangiz qandaydir tazyiq nishoni bo`lsa, agar siz muhim davlat infratuzilmasi tarkibida bo`lsangiz, oddiy terroristlar bombalarini va pistoletlarini chetga qo`yib, turli - tuman dasturiy vositalar yordamida tashkilotingiz kompyuterlariga, shaxsiy kompyuterlaringizga elektron hujumni amalga oshirish masalasini ko`radilar. Shu sababli bu hujumlarni oldini olish hamda muhim axborotlarning xavfsizligini ta`minlash masalalariga jiddiy yondoshishingizga to`g'ri keladi. Savdo - sotiq va marketing bo`yicha xizmat ko`rsatuvchi oddiy tashkilot xususida so`z borsa, faqat mijozlar ro`yxatini o`g'irlovchi xizmatchilaringiz to`g'risida, qalbaki kredit kartochkalari bo`yicha tovar oluvchi firibgarlar, tarmog'ingizga preyskurantlardan foydalanish maqsadida kiruvchi raqiblar, Web-saytingizni ta`magirlik maqsadida buzuvchilar va shunga o`xshashlar to`g'risida qayg'urishingizga to`g'ri keladi. Ammo, vahimaga o`rin yo`q. Birinchi navbatda kundalik ehtiyot choralari ko`rilishi lozim. Axborotga ega bo`lishning eng ommabop usuli oddiy o`g'rilik. Ish stolimizda mo`maygina pulni qoldirib ketmaymiz-ku. Nima

uchun muhim axborotlar saqlanayotgan-shaxsiy kompyuter xavfsizligini ta`minlashga ozgina vaqt sarf qilmaymiz? Bu nafaqat apparat vositalariga, balki ma`lumotlarga ham taalluqli. Ma`lumotlarni o`g'irlatish yoki yo`qotish katta, ba`zida, tuzatib bo`lmaydigan zarar keltiradi. Ma`lumki, tizim ma`murlari barcha maxfiy materiallardan foydalanish imkoniga ega va odatda, kompaniya foydasidan o`z ulushlariga ega emaslar. Shu sababli ular tashkilot xavfsizligiga tahdid sola oluvchilar sarasiga kiradilar. Shu sababli xavfsizlik xizmatini ta`minlovchilarga, ayniqsa maslahat berish, rejalashtirish va ma`murlashni tavsiya etuvchilarni jiddiy qarash lozim.

Tamaddun rivojining zamonaviy bosqichida axborot nafaqat jamoat va davlat institutlari faoliyatida, balki har bir inson hayotida hal qiluvchi rolni o`ynaydi. Ko`z oldimizda jamiyatning axborotlashishi shiddat bilan va ko`pincha oldindan bilib bo`lmaydigan tarzda rivojlanmoqda. Biz esa uning ijtimoiy, siyosiy, iqtisodiy va boshqa oqibatlarini tushunib etishga harakat qilamiz, xolos. Jamiyatimizning axborotlashishi yagona dunyo axborot makonining yaratilishiga olib keladiki, bu makon doirasida axborotni yig'ish, ishlash, saqlash va sub`ektlar - insonlar, tashkilotlar, davlatlar o`rtasida almashish amalga oshiriladi. Ravshanki, siyosiy, iqtisodiy, ilmiy-texnikaviy va boshqa axborotlarni tezlikda almashish imkoniyati jamiyat hayotining barcha sohalarida va ayniqsa ishlab chiqarishda va boshqarishda yangi texnologiyalarning qo`llanilishi bilan bog'liqdir. Ammo, sanoatning tez rivojlanishi ekologiyaga tahdid sola boshladi, yadro fizikasi sohasidagi yutuqlar yadro urushi xavfini tug'dirdi. Axborotlashtirish ham jiddiy muammolar manbaiga aylandi, axborotlarga egalik qilish, uni o`zlashtirishga harakat qilish axborot urushini vujudga keltirdi.

Urushlar doimo bo`lgan. Vaqt o`tishi bilan urushni olib borish butun bir fanga aylandi. Har qanday fandagidek urushda o`zining tarixi, o`zining qoidasi, mashhur namoyondalari, o`zining metodologiyasi paydo bo`ldi. Zamonaviy axborot urushi g'oyasi juda ildamlab ketdi. endi uning makoni - butun er shari. Urush lokal qaroqchi hujumidan bir necha davlatlarga jiddiy xavf tug'diruvchi global muammoga aylandi. Turli mamlakatlarning harbiy doktrinalarida elektron qurol rivoji rejalari va maxsus vazifalarga mo`ljallangan dasturiy ta`minot to`g'risida eslatishlar ko`zga tashlanmoqda. Turli razvedka manbalaridan kelayotgan axborotning tahlili natijasida

xulosa qilish mumkinki, ba`zi bir davlatlarning rahbarlari hujumkor kiber-dasturlarni yaratishni moliyalamoqdalar. Axborot urushiga oddiy vositalar yordamida harbiy xarakatlar samara bermaydigan hollarga nisbatan strategik al'ternativa sifatida qaralmoqda.

Harbiylar tomonidan kiritilgan axborot urushi atamasi real, qirg'inli va emiruvchi harbiy harakatlar bilan bog'liq shafqatsiz va xavfli faoliyatni anglatadi. Ma`lumotlarni uzatish tarmoqlarining kelajak janglari maydoniga aylanishi esa allaqachon e`tirof etilgan.

Har qanday urush, shu jumladan axborot urushi ham zamonaviy qurol yordamida olib boriladi. Axborot yordamida urush olib boruvchilar e`lon qilinmagan va ko`pincha dunyoga ko`rinmaydigan qurollar yordamida urushlarni olib borishi mumkin (olib borilmoqda ham). Bu qurolning ta`sir ob`ektlari – jamiyat, davlat va davlatning iqtisodiy, siyosiy, ijtimoiy va h-zo sohalaridir. Axborot quroli hujumda va mudofaada 'elektron tezlik' bilan ishlatilishi mumkin. Axborot quroli deganda axborot massivlarini yo`qotish, buzish yoki o`g'irlash vositalari, himoyalash tizimini yo`qotish, qonuniy foydalanuvchilar faoliyatini chegaralash asbob-uskunalar va butun kompyuter tizimi ishlashi tartibini buzish vositalari tushuniladi. Bu qurol ilg'or texnologiyalarga asoslangan bo`lib, har bir yaratilgan yangi texnologiyalardan unumli foydalanishga asoslangandir. Axborot quroli qo`llanishining strategiyasi hujumkor xarakterga ega. Shu sababli bunday quroldan va axborot terrorizmidan himoyalanish muammosi hozirda kunda dunyo miqyosida birinchi o`ringa chiqqan.

Hozirda hujumkor axborot quroli sifatida quyidagilarni ko`rsatish mumkin:

o kompyuter viruslari - ko`payish, dasturlarda o`rnashish, ma`lumotlarni uzatish tarmoqlari bo`yicha uzatilish, boshqarish tizimlarni ishdan chiqarish va shunga o`xshash qobiliyatlarga ega;

o mantiqiy bombalar - signal bo`yicha yoki o`rnatilgan vaqtda harakatga keltirish maqsadida harbiy yoki fuqaro infratuzilmalariga o`rnatiluvchi dasturiy mahsulot tarkibidagi ulangan qurilmalar;

o telekommunikatsiya tarmoqlarida axborot almashinuvini bostirish vositalari, davlat va harbiy boshqaruv kanallarida axborotni soxtalashtirish;

o ob`ekt dasturiy ta`minotiga ayg'oqchilar tomonidan atayin kiritiluvchi turli xil xatoliklar;

o testli dasturlarni betaraflashtirish vositalari;

Universallik, maxfiylik, amalga oshirilishining har xilligi, ta`sirining keskinligi, qo`llanilishining vaqti va joyini tanlash imkoniyati axborot qurolini haddan tashqari xavfli qiladi. Bu qurolni, masalan, intellektual mulkni himoyalash vositasiga o`xshatib niqoblash mumkin. Undan tashqari, u hatto urush e`lon qilmasdan hujum harakatlarini avtonom tarzda olib borish imkonini beradi. Zamonaviy jamiyatda axborot qurolini ishlatish harbiy strategiyasi fuqaro sektori bilan uzviy bog'langan. Axborot qurolining ta`siri shakli va usullarining paydo bo`lishi va qo`llanishi xususiyatlarining turli-tumanliligi undan himoyalanishning murakkab masalalarini vujudga keltirdi.

Axborot quroli qo`llanilishini oldini olish yoki qo`llanishi oqibatlarini bartaraf qilish uchun quyidagi choralarni ko`rish lozim:

o axborot resurslarining fizik asosini tashkil etuvchi moddiy - texnik ob`ektlarni himoyalash;

o ma`lumotlar bazalari va banklarining me`yoriy va muttasil ishlashini ta`minlash;

o axborotdan ruxsatsiz foydalanishdan, uni buzilishidan yoki yo`q qilinishidan himoyalash;

o axborot sifatini saqlash (o`z vaqtidaligi, aniqligi, to`laligi va foydalanuvchanligi);

o muhim axborotlarni kriptografik usullar orqali himoyalash.

Davlatning dunyo ochiq tarmog'iga ulanishining iqtisodiy va ilmiy - texnik siyosatini axborot xavfsizligi orqali qurish lozim. Bu ochiq, fuqarolarning axborotga va intellektual mulkga ega bo`lish qonuniy huquqini saqlashga mo`ljallangan siyosat mamlakat hududida tarmoq asbob - uskunalariga axborot quroli elementlarining kirishidan saqlashni ko`zda tutish lozim. Bu muammo hozirda chet el axborot texnologiyalari va dasturlarini ommaviy sotib olinayotgan paytda o`ta muhimdir.

Ma`lumki, dunyo axborot makoniga ulanmasdan mamlakat iqtisodini rivojlantirib, elektron hukumat, elektron hujjat aylanishi va elektron tijoratni amalga oshirib bo`lmaydi. Internet tarmog'i tomonidan ta`minlangan axborot va hisoblash resurslaridan operativ foydalanishni davlatchilikni, fuqarolik jamiyati institutlarini mustahkamlash, ijtimoiy infratuzilmalarining rivojlanish shartlari sifatida talqin etish mumkin. Mamlakatning xalqaro kommunikatsiya tizimida va axborot almashinuvida

ishtirokini, axborot xavfsizligi muammosini kompleks hal qilmasdan mumkin emasligini aniq tasavvur etish lozim. Ayniqsa xususiy axborot resurslarini himoyalash muammosi, axborot kommunikatsiya texnologiyalar sohasida rivojlangan mamlakatlardan texnologik orqada qolayotgan mamlakatlar uchun jiddiy hisoblanadi. Axborot qurolini ishlab chiqishni va uni ishlatishni ximiyaviy va bakteriologik qurol kabi taqiqlashning imkoni yo`q. Xuddi shu kabi ko`pgina mamlakatlarning yagona global axborot makonini shakllantirish bo`yicha urinishlarini chegaralab bo`lmaydi.

Bu singari tahdidlarni oldini olishning yo`llaridan biri, arzon, tadbiq qilish imkoni mavjud bo`lgan kriptotizimlarni tadbiq qilish hisoblanadi degan fikrdamiz. Buning uchun kriptografiya va kriptologik tizimlar haqida etarlicha tushunchaga ega bo`lishimiz lozim.

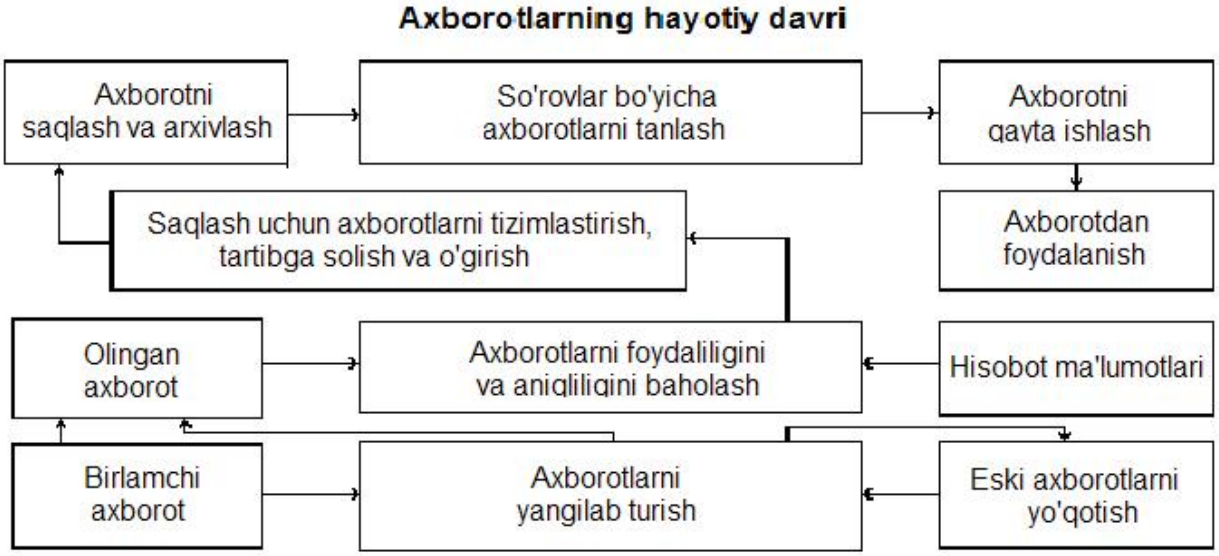
1.3. Axborotlar xavfsizligi tushunchalari va himoya tizimlari

Axborotning muhimlik darajasi qadim zamonlardan ma`lum. Shuning uchun ham qadimda axborotni himoyalash uchun turli xil usullar qo`llanilgan. Agar ma`lumot ishonchli himoyalansa va bu himoya to`sig'ini engib o`tish qiyin bo`lsa u bardoshli deyish qabul qilingan. Himoya usullaridan biri - sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o`qiy olmagan. Asrlar davomida bu san`at - sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentlari va razvedka missiyalaridan tashqariga chiqmagan. Hozirgi kunga kelib hamma narsa tubdan o`zgardi, ya`ni axborot o`z qiymatiga ega bo`ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatadilar, sotadilar va sotib oladilar. Bulardan tashqari uni o`g'irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shuning uchun axborotni himoyalash ehtiyoji yanada kuchaydi. Axborotni qayta ishlash sanoatining paydo bo`lishi axborotni himoyalash sanoatining paydo bo`lishiga olib keldi.

Avtomatlashtirilgan axborot tizimlarida axborot o`zining hayotiy davriga ega bo`ladi. Bu davr uni yaratish, undan foydalanish va kerak bo`lmaganda yo`qotishdan iboratdir. Axborotlar hayotiy davrining har bir bosqichida ularning himoyalanganlik darajasi turlicha baholanadi.

Maxfiy va qimmatbaho axborotlarga ruxsatsiz kirishdan himoyalash eng muhim vazifalardan biri sanaladi. Kompyuter egalari va foydalanuvchilarning mulkiy himoyalash - bu ishlab chiqarilayotgan axborotlarni jiddiy iqtisodiy va boshqa moddiy

hamda nomoddiy zararlar keltirishi mumkin bo`lgan turli kirishlar va o`g'irlashlardan himoyalashdir. Himoyalashning bir necha usullari mavjud va ulardan o`z o`rnida foydalanish yaxshi natijalarni beradi.



1.3.1-rasm. Axborotlarning hayotiylik davri

Hozirgi kunda axborotga nisbatan uning xavfsizligi va himoyalanganligi tushunchalari bor. Ular bir-biridan farq qiladi.

Axborot xavfsizligi deb ma`lumotlarni yo`qotish va o`zgartirishga yo`naltirilgan tabiiy yoki sun`iy xossali tasodifiy va qasddan ta`sirlardan har qanday tashuvchilarda axborotning himoyalanganligiga aytiladi.

Ilgarigi xavf faqatgina konfidentsial (maxfiy) xabarlar va hujjatlarni o`g'irlash yoki nusxa olishdan iborat bo`lsa, hozirgi paytdagi xavf esa kompyuter ma`lumotlari to`plami, elektron ma`lumotlar, elektron massivlardan ularning egasidan ruxsat so`ramasdan foydalanishdir. Bulardan tashqari, bu harakatlardan moddiy foyda olishga intilish ham rivojlanadi.

Axborotning himoyasi deb boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta`minlovchi va tashkilot axborot axborot zahiralarining yaxlitliligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta`minlovchi qat`iy reglamentlangan dinamik texnologik jarayonga aytiladi.

Axborotning egasiga, foydalanuvchisiga va boshqa shaxsga zarar etkazmoqchi bo`lgan noqonuniy muomaladan har qanday hujjatlashtirilgan, ya`ni identifikatsiya qilish imkonini beruvchi rekvizitlari qo`yilgan holda moddiy jismda qayd etilgan axborot himoyalanishi kerak.

Axborot xavfsizligi nuqtai nazaridan axborotni quyidagicha turkumlash mumkin:

- maxfiylik - aniq bir axborotga faqat tegishli shaxslar doirasigina kirishi mumkinligi, ya`ni foydalanilishi qonuniy hujjatlarga muvofiq cheklab qo`yilib, hujjatlashtirilganligi kafolati. Bu bandning buzilishi o`g'irlik yoki axborotni oshkor qilish, deyiladi;
- konfidentsiallik - ishonchliligini, tarqatilishi mumkin emasligi, maxfiyligi kafolati;
- yaxlitlik - axborot boshlang'ich ko`rinishida ekanligi, ya`ni uni saqlash va uzatishda ruxsat etilmagan o`zgarishlar qilinmaganligi kafolati. Bu bandning buzilishi axborotni soxtalashtirish deyiladi;
- autentifikatsiya - axborot zahirasi egasi deb e`lon qilingan shaxs haqiqatan ham axborotning egasi ekanligiga beriladigan kafolat. Bu bandning buzilishi xabar muallifini soxtalashtirish deyiladi;
- appelyatsiya qilishlik - etarlicha murakkab kategoriya, lekin elektron
- biznesda kent qo`llaniladi. Kerak bo`lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati.

Yuqoridagidek, axborot bilan ishlovchi tizimga nisbatan quyidagicha tasnifni keltirish mumkin:

- ishonchlilik - tizim me`yoriy va g'ayri tabiiy hollarda rejalashtirilganidek o`zini tutishlik kafolati;
- aniqlilik - hamma buyruqlarni aniq va to`liq bajarish kafolati;
- tizimga kirishni nazorat qilish - turli shaxs guruhlari axborot manbalariga har xil kirishga egaligi va bunday kirishga cheklanishlar doim bajarilishlik kafolati;
- nazorat qilinishi - istalgan paytda dastur majmuasining hohlagan qismini to`liq tekshirish mumkinligi kafolati;
- identifikatsiyalashni nazorat qilish - hozir tizimga ulangan mijoz aniq o`zini kim deb atagan bo`lsa, aniq o`sha ekanligining kafolati;
- qasddan buzilishlarga to`sqinlik - oldindan kelishilgan me`yorlar chegarasida qasddan xato kiritilgan ma`lumotlarga nisbatan tizimning oldindan kelishilgan holda o`zini tutishi.

Axborotni himoyalashning maqsadlari quyidagilardan iborat:

- axborotning kelishuvsiz chiqib ketishi, o`g'irlanishi, yo`qotilishi, o`zgartirilishi, soxtalashtirishlarning oldini olish;

- shaxs, jamiyat, davlat xavfisizligiga bo`lgan xavf 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 shaxsiy ma`lumotlarning shaxsiy maxfiyligini va konfidentsialligini saqlovchi fuqarolarning konstitutsion huquqlarini himoyalash;
- davlat sirini, qonunchilikka mos hujjatlashtirilgan axborotning konfidentsialligini saqlash;
- axborot tizimlari, texnologiyalari va ularni ta`minlovchi vositalarini yaratish, ishlab chiqish va qo`llashda sub`ektlarning huquqlarini ta`minlash.

Axborot – kommunikatsiyalar texnologiyalarining ommaviy ravishda qog’ozsiz avtomatlashtirilgan asosda boshqarilishi sababli axborot xavfsizligini ta`minlash murakkablashib va muhimlashib bormoqda. Shuning uchun, axborotni himoyalash tizimi bo`yicha turli-tuman usullar ishlab chiqilmoqda.

Axborotning zaif tomonlarini kamaytiruvchi va axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo`qolishiga to`sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi – axborotni himoyalash tizimi deyiladi.

Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo`qotilishidan keladigan zarar va himoyalash mexanizmining narxidan kelib chiqqan holda axborotni himoyalashning zaruriy darajasi hamda tizimning turini, himoyalash usullar va vositalarini aniqlashlari zarur. Axborotning qimmatliligi va talab qilinadigan himoyaning ishonchliligi bir-biri bilan bevosita bog’liq.

Himoyalash tizimi uzluksiz, rejali, markazlashtirilgan, maqsadli, aniq, ishonchli, kompleksli, oson mukammalashtiriladigan va ko`rinishi tez o`zgartiriladigan bo`lishi kerak. U odatda barcha ekstremal sharoitlarda samarali bo`lishi zarur. Himoyalash tizimi turli muassasalarda, ularda qimmatli ma`lumotlarning mavjudligiga muvofiq o`ziga xos himoya usullari qo`llaniladi.

Axborot hajmi kichik bo`lgan tashkilotlarda axborotlarni himoyalashda oddiy usullarni qo`llash maqsadga muvofiq va samaralidir. Masalan, o`qiladigan qimmatbaho

qog’ozlarni va elektron hujjatlarni alohida guruhlarga ajratish va niqoblash, ushbu hujjatlar bilan ishlaydigan xodimni tayinlash va o`rgatish, binoni qo`riqlashni tashkil etish, xizmatchilarga qimmatli axborotlarni tarqatmaslik majburiyatlarini yuklash, tashqaridan keluvchilar ustidan nazorat qilish, kompyuterni himoyalashning eng oddiy usullarini qo`llash va hokazo. Odatda, himoyalashning eng oddiy usullarni qo`llash sezilarli samara beradi.

Murakkab tarkibli, ko`p sonli avtomatlashtirilgan axborot tizimi va axborot hajmi katta bo`lgan tashkilotlarda axborotni himoyalash uchun himoyalashning majmuali tizimi tashkil qilinadi. Lekin ushbu usul hamda himoyalashning oddiy usullari xizmatchilarning ishiga haddan tashqari halaqit bermasligi kerak.

1.4. Kriptografiya – maxfiy xabarning ma`nosini yashirish

‘Kriptografiya’ atamasi dastlab ‘yashirish, yozuvni berkitib qo`ymoq’ ma`nosini bildirgan. Birinchi marta u yozuv paydo bo`lgan davrlardayoq aytib o`tilgan. Hozirgi vaqtda kriptografiya deganda har qanday shakldagi, ya`ni diskda saqlanadigan sonlar ko`rinishida yoki kompyuter tarmoqlarida uzatiladigan xabarlar ko`rinishidagi axborotni yashirish tushuniladi. Kriptografiyani raqamlar bilan kodlanishi mumkin bo`lgan har qanday axborotga nisbatan qo`llash mumkin. Maxfiylikni ta`minlashga qaratilgan kriptografiya kengroq qo`llanilish doirasiga ega. Aniqroq aytganda, kriptografiyada qo`llaniladigan usullarning o`zi axborotni himoyalash bilan bog’liq bo`lgan ko`p jarayonlarda ishlatilishi mumkin. Kriptografiya axborotni ruxsatsiz kirishdan himoyalab, uning maxfiyligini ta`minlaydi. Masalan, to`lov varaqlarini elektron pochta orqali uzatganda, u o`zgartirilishi yoki soxta yozuvlar qo`shilishi mumkin. Bunday hollarda axborotning yaxlitligini ta`minlash zaruriyati paydo bo`ladi. Umuman olganda kompyuter tarmog’iga ruxsatsiz kirishning mutlaqo oldini olish mumkin emas, lekin ularni aniqlash mumkin. Axborotning yaxlitligini tekshirishning bunday jarayoni, ko`p hollarda, axborotning haqiqiyligini ta`minlash deyiladi. Kriptografiya yordamida axborotlarning haqiqiyligini ta`minlashi mumkin. Nafaqat axborotning kompyuter tarmog’idan ma`nosi buzilmasdan kelganligini bilish, balki uning muallifdan kelganligiga ishonch hosil qilish juda muhim. Axborotni uzatuvchi shaxslarning haqiqiyligini tasdiqlovchi turli usullar ma`lum. eng universal protsedura parollar bilan himoyalashdir, lekin bu juda samarali bo`lmagan protsedura. Chunki parolni qo`liga kiritgan har qanday shaxs axborotdan foydalanishi

mumkin bo`ladi. Agar ehtiyotkorlik choralariga rioya qilinsa, u holda parollarning samaradorligini oshirish mumkin. Lekin kriptografiya bundan kuchliroq, u parolni uzluksiz o`zgartirish imkonini beradigan protseduralarni ham ta`minlaydi. Kriptografiya sohasidagi oxirgi yutuqlardan biri — raqamli signatura — maxsus xossa bilan axborotni to`ldirish yordamida yaxlitlikni ta`minlovchi usuldir. Bunda axborot uning muallifi bergan ochiq kalit ma`lum bo`lgandagina tekshirilishi mumkin. Ushbu usul maxfiy kalit yordamida yaxlitlik tekshiriladigan ma`lum usullardan ko`proq afzalliklarga ega.

Kriptografiyada uzatiladigan axborotning ma`nosini yashirish uchun ikki xil o`zgartirishlar qo`llaniladi: kodlashtirish va shifrlash.

Kodlashtirish uchun tez-tez ishlatiladigan iboralar to`plamini o`z ichiga oluvchi kitob yoki jadvallardan foydalaniladi. Bu iboralardan har biriga, ko`p hollarda, raqamlar to`plami bilan beriladigan ixtiyoriy tanlangan kodli so`z to`g’ri keladi. Axborotni kodlash uchun xuddi shunday kitob yoki jadval talab qilinadi. Kodlashtiruvchi kitob yoki jadval ixtiyoriy kriptografik o`zgartirishga misol bo`ladi. Kodlashtirishning axborot texnologiyasiga mos talablar — qatorli ma`lumotlarni sonli ma`lumotlarga aylantirish va aksincha o`zgartirishlarni bajara bilish. Kodlashtirish kitobini tezkor hamda tashqi xotira qurilmalarida amalga oshirish mumkin, lekin bunday tez va ishonchli kriptografik tizimni muvaffaqiyatli deb bo`lmaydi. Agar bu kitobdan biror marta ruxsatsiz foydalanilsa, kodlarning yangi kitobini yaratish va uni hamma foydalanuvchilarga tarqatish zaruriyati paydo bo`ladi.

Kriptografik o`zgartirishning ikkinchi turi shifrlash. U o`z ichiga - boshlang’ich matn belgilarini anglab olish mumkin bo`lmagan shaklga o`zgartirish algoritmlarini qamrab oladi. O`zgartirishlarning bu turi axborot-kommunikatsiyalar texnologiyalariga mos keladi. Bu erda algoritmni himoyalash muhim ahamiyat kasb etadi. Kriptografik kalitni qo`llab, shifrlash algoritmining o`zida himoyalashga bo`lgan talablarni kamaytirish mumkin. endi himoyalash ob`ekti sifatida faqat kalit xizmat qiladi. Agar kalitdan nusxa olingan bo`lsa, uni almashtirish mumkin va bu kodlashtiruvchi kitob yoki jadvalni almashtirishdan engildir. Shuning uchun ham kodlashtirish emas, balki shifrlash axborot-kommunikatsiyalar texnologiyalarida keng ko`lamda qo`llanilmoqda.

Sirli (mahfiy) aloqalar sohasi kriptologaya deb aytiladi. Ushbu so`z yunoncha ‘kripto’ — sirli va ‘1ogus’ — xabar ma`nosini bildiruvchi so`zlardan iborat. Kriptologiya ikki yo`nalish, ya`ni kriptografiya va kriptotahlildan iborat.

Kriptografiyaning vazifasi xabarlarning maxfiyligini va haqiqiyligini ta`minlashdir.

Kriptotahlilning vazifasi esa kriptograflar tomonidan ishlab chiqilgan himoya tizimini ochishdan borat.

Kriptografiya - axborotlarni aslidan o`zgartirilgan holatga etkazishlarning matematik uslublarini topish va takomillashtirish bilan shug’ullanadi. U ma`lumotlarni o`zgartirish usullarining to`plami bo`lib, ma`lumotlarni himoyalash bo`yicha quyidagi ikkita asosiy muammolarni hal qilishga yo`naltirilgan: maxfiylik; yaxlitlilik. Maxfiylik orqali yovuz niyatli shaxslardan axborotni yashirish tushunilsa, yaxlitlilik esa yovuz niyatli shaxslar tomonidan axborotni o`zgartira olmaslik haqida dalolat beradi.

Shunday qilib, kriptografik uslublar axborotlar matnini asli holidan o`zgartirib, faqat kalitni bilgan holdagina uni asli holatini olish imkoniyatini beradi.

Shifrlangan va deshifrlangan masalalariga tegishli bo`lgan, ma`lum bir alfavitda tuzilgan ma`lumotlar matnlarni tashkil etadi.

Alfavit – axborotlarni kodlashtirish uchun foydalaniladigan chekli sondagi belgilar to`plamidir. Misol sifatida:

- o`ttiz oltita belgidan (harfdan) iborat o`zbek tili kirill alfaviti;
- o`ttiz ikkita belgidan (harfdan) iborat rus tili kirill alfaviti;
- yigirma sakkizta belgidan (harfdan) iborat lotin alfaviti;
- ikki yuz ellik oltita belgidan iborat ASSII va KOI-8 standart kompyuter kodlarining alfaviti;
- binar alfavit, ya`ni 0 va 1 belgilardan iborat bo`lgan alfavit;
- sakkizlik va o`n oltilik sanoq tizimlari belgilaridan iborat bo`lgan alfavitlarni keltirish mumkin.

Matn – alfavitning elementlaridan (belgilaridan) tashkil topgan tartiblangan tuzilma.

Shifrlash – ochiq matn deb ataluvchi dastlabki matnni shifrlangan matn holatiga etkazish jarayoni.

Deshifrlash – shifrlashga teskari bo`lgan jarayon, ya`ni kalit yordamida shifrlangan matnni dastlabki matn holatiga etkazish.

Kalit – bevosita dastlabki matnni shifrlash va deshifrlash uchun zarur bo`lgan ma`lumot.

Kriptografiya nuqtai - nazarida shifr — bu kalit demakdir va u ochiq ma`lumotlar to`plamini yopiq (shifrlangan) ma`lumotlarga o`zgartirish algoritmlari majmuasi hisoblanadi.

Kalit kriptografiya o`zgartirishlar algoritmining ba`zi-bir parametrlarining maxfiy holati bo`lib, barcha algoritmlardan yagona variantini tanlaydi.

Kriptografiya himoyasida shifrlarga nisbatan quyidagi talablar qo`yiladi:

• etarli darajada kriptomustahkamlik;

• shifrlash va qaytarysh jarayonining oddiyligi;

• axborotlarni shifrlash oqibatida ular hajmining ortib ketmasligi;

• shifrlashdagi kichik xatolarga ta`sirchan bo`lmasligi.

Kriptografik tizim yoki kriptotizim – ochiq matnni shifrlash (deshifrlash) jarayonini tashkil etuvchi amallar majmui bo`lib, u alfavitlar belgilarini almashtirishlar ketma-ketligidan iborat.

Kriptotizimlarga nisbatan ishlatiladigan asosiy ko`rsatkich bo`lib kriptomustahkamlik hisoblanadi.

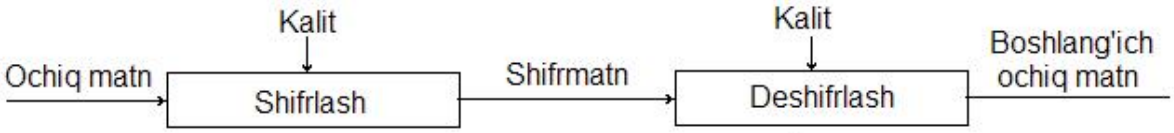
Yovuz niyatli shaxslar o`z maqsadlariga erisha olmasa va kriptotahlilchilar kalitni bilmasdan turib, shifrlangan axborotni tiklay olmasa, u holda kriptotizim kriptomustahkam tizim deb aytiladi. Kriptotizimning mustahkamligi uning kaliti bilan aniqlanadi va bu kriptotahlilning asosiy qoidalaridan biri bo`lib hisoblanadi. Ushbu ta`rifning asosiy ma`nosi shundan iboratki, kriptotizim barchaga ma`lum tizim hisoblanib, uning yaratilishi vaqt va mablag’ talab qiladi. Kriptotizim yaratilgach, faqatgina kalitni o`zgartirib turish bilan axborotni himoyalash talab qilinadi.

Hozirgi kunda kriptotizimlarni ikki sinfga ajratish mumkin:

• simmetriyali bir kalitlilik (maxfiy kalitli);

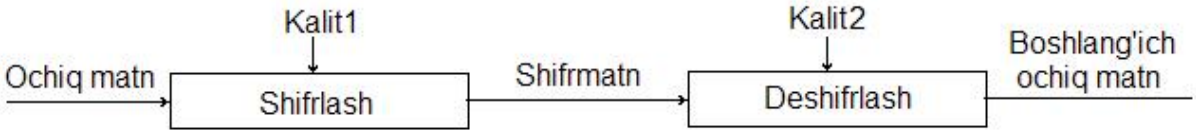
• asimmetriyali ikki kalitlilik (ochiq kalitli).

Simmetriyali (bir kalitlilik - kalit maxfiy) tizimlar quyidagi sxema asosida ishlaydi.



1.4.1-rasm.

Asimmetriyali (ikki kalitlilik - kalit1 maxfiy, kalit2 esa ochiq) tizimlar quyidagi sxema asosida ishlaydi.



1.4.2-rasm.

Simmetriyali tizimlarda quyidagi ikkita muammo mavjud:

1) Axborot almashuvida ishtirok etuvchilar qanday yo`l bilan maxfiy kalitni bir-birlariga uzatishlari mumkin?

2) Jo`natilgan xabarning haqiqiyligini qanday aniqlasa bo`ladi?

Ushbu muammolarning echimi ochiq kalitli tizimlarda o`z aksini topdi.

Ochiq kalitli asimmetriyali tizimda ikkita kalit qo`llaniladi. Hisoblash usullari bilan biridan ikkinchisini aniqlab bo`lmaydi. Birinchi kalit axborot jo`natuvchi tomonidan shifrlashda ishlatilsa, ikkinchisi axborotni qabul qiluvchi tomonidan axborotni tiklashda qo`llaniladi va u sir saqlanishi lozim. Ushbu usul bilan axborotning maxfiyligini ta`minlash mumkin. Agar birinchi kalit sirli bo`lsa, u holda uni elektron imzo sifatida qo`llash mumkin va axborotni autentifikatsiyalash, ya`ni axborotning yaxlitligini ta`minlash imkoni paydo bo`ladi. Shuningdek, axborotni autentifikatsiyalashdan tashqari quyidagi masalalarni ham echish mumkin:

• foydalanuvchini autentifikatsiyalash, ya`ni kompyuter tizimi zahiralariga kirmoqchi bo`lgan foydalanuvchini aniqlash:

• tarmoq abonentlari aloqasini o`rnatish jarayonida ularni o`zaro autentifikatsiyalash.

Hozirgi kunda kompyuterda saqlanayotgan va tarmoq orqali uzatiladigan barcha muhim hujjatlar, elektron to`lov tizimlari hamda internet yordamida amalga oshiriladigan elektron savdo singarilar himoyalanishi lozim.

II. Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturi

2.1. Tsezar usuli va kalit so`zli Tsezar tizimi

Hozirgi kunda kriptografik uslublarning axborotlar muhofazasi masalalarida qo`llanishi beqiyosdir. Haqiqatan ham, bir tomondan kompyuter tizimlarining internet tarmoqlari bilan bog'liq ravishda katta hajmdagi davlat va harbiy ahamiyatga ega bo`lgan axborotlarni hamda shu kabi iqtisodiy, shaxsiy va boshqa turdagi axborotlarni tez va sifatli uzatish va qabul qilishdagi roli ortib bormoqda. Ikkinchi tomondan esa bunday axborotlarning keng ma`nodagi muhofazasini ta`minlash masalalari muhimlashib bormoqda. Shu sababli axborotlarni himoyalash bo`yicha kriptografiya uzil-kesil asosiy fan sifatida shakllandi. Unda mavjud bo`lgan usullar takomillashtirildi va yangi – yangi usullar kashf qilindi. Bundan tashqari axborotlar xavfsizligini ta`minlash uchun xizmat qilgan muhim usullar o`rganila boshlandi. Kriptografiyada axborotlarni himoyalash uchun juda ko`plab uslublar qo`llanilgan. Ulardan biri almashtirish usullari guruhi hisoblanadi.

O`rin almashtirish shifrlari. O`rin almashtirish shifrlarida shifrlanadigan matn ramzlari shu matn qismi chegarasida aniq qoida asosida almashtiriladi. O`rin almashtirish shifrlari eng sodda hisoblanadi va eng qadimiy shifrlardir.

O`rin almashtirish usullarining mohiyati bir alfavitda yozilgan axborot simvollarini boshqa alfavit simvollari bilan ma`lum qoida bo`yicha almashtirishdan iboratdir. eng sodda usul sifatida to`g'ridan to`g'ri o`rin almashtirishni ko`rsatish mumkin. Dastlabki axborot yoziluvchi $A_0$ alfavitning $s_{0i}$ simvollariga shifrlovchi $A_1$ alfavitning $s_{1i}$ simvollari mos qo`yiladi. Oddiy holda ikkala alfavit ham bir xil simvollar to`plamiga ega bo`lishi mumkin.

Ikkala alfavitdagi simvollar o`rtasidagi moslik ma`lum algoritm bo`yicha K simvollar uzunligiga ega bo`lgan dastlabki matn T_0 simvollarining raqamli ekvivalentlarini o`zgartirish orqali amalga oshiriladi.

Eng qadimgi o`rin almashtirish usullari sifatida quyidagi usullarni keltirish mumkin: Tsezar usuli, tayanch so`zli Tsezar usuli, Affin tizimidagi Tsezar usuli va boshqalar.

Tsezar usuli. Dastlabki tizimlashgan kriptografik uslublar eramizdan oldingi 50 yillarda, rimlik imperator Gay Yuliy Tsezarning ish yuritish yozishmalarida uchraydi. U biror ma`lumotni maxfiy holda biror kishiga etkazmoqchi bo`lsa, alfavitning

birinchi harfini alfavitning to`rtinchi harfi bilan, ikkinchisi beshinchisi bilan va hokazo shu tartibda almashtirib matnning asli holatidan shifrlangan matn holatiga o`tkazgan. Keyinchalik Tsezar usulida almashtiruvchi harflar to`rtinchisiga emas, balki kelishilgan k siljish bilan aniqlangan. Shifrlashda matnning har bir harfi boshqa harf bilan quyidagi qoida asosida almashtiriladi. Bu erda K–butun son hisoblanib uni quyidagicha ifodalash mumkin:

K=Kmod(m), m -alfavit soni.

Aniqroq qilib aytganda:

Tsezar usuli orqali shifrlashnin matematik ifodasi quyidagicha:

$C_k(j)=(j+k)(\text{mod } n)$

Bu erda j – almashtirilayotgan belgini alfavitdagi o`rni,

k – siljish qadami,

n – alfavitdagi harflar soni.

Tsezar usuli orqali deshifrlashnin matematik ifodasi quyidagicha:

$C_k^{-1}(j)=S_{n-k}=(j+n-k)(\text{mod } n)$

Bu erda j – almashtirilayotgan belgini alfavitdagi o`rni,

k – siljish qadami,

n – alfavitdagi harflar soni.

Yuliy Tsezar bevosita k = 3 bo`lganda ushbu usuldan foydalangan.

K=3 bo`lganda va alifbodagi harflar 26 ta bo`lganda quyidagi jadval hosil qilinadi:

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

Misol. Matn sifatida KRIPTOGRAFIY so`zini oladigan bo`lsak, Tsezar usuli natijasida quyidagi shifrlangan yozuv hosil bo`ladi:

NULSWRJUDILB

Endi matn sifatida KOMPUTER so`zini oladigan bo`lsak, Tsezar usuli natijasida quyidagi shifrlangan yozuv hosil bo`ladi:

NRPSBXHU.

Ilmiy adabiyotlarda K=3 uchun Tsezar usulida shifrlashga Tsezarning ‘VENI VIDI VICI’ xabari (o`zbekcha tarjima qilganda ‘keldi, ko`rdi, yutdi’) misol qilib olinadi. Shifr ‘YHQL YLGL YLFL’ ko`rinishni oladi.

Tsezarning shifrlash tizimining yutug’i shifrlash va qayta ochishning soddaligi hisoblanadi.

Tsezar tizimining kamchiliklariga quyidagilarni aytib o`tish lozim.

- Tsezar tizimini ishlatganda berilgan ochiq matn harflari takrorlanish chastotasini maksimal holatga keltirmaydi;
- Almashtiruvchi harflar ketma-ketligida alfavitli tartib saqlanadi; K qiymati o`zgartirilganda faqat bu ketma-ketlikning boshlang’ich pozitsiyalari o`zgaradi;
- K ning mumkin bo`lgan qiymatlari kam;
- Tsezar’ tizimini shifr usulida harflarni paydo bo`lish chastotasini tahlili natijasida osongina ochish mumkin.

Keyinchalik Tsezar usulida shifrlash takomillashtirilib o`rinlarni almashtirish usullaridan foydalanilgan.

Kalit so`zli Tsezar tizimi. Tsezarning kalit so`zli shifrlash tizimi bitta alfavitli almashtirish tizimi hisoblanadi. Bu usulda kalit so`zi orqali harflarning surishda va tartibini o`zgartirishda foydalanadi.

Lotin alifbosi bo`yicha Tsezarning kalit so`zli shifrlash tizimi uchun k ($0<k<25$) son va so`z yoki jumladan iborat kalit so`z tanlab olamiz. Kalit so`z tarkibida harflar takrorlanmasligi maqsadga muvofiq hisoblanadi. Shuning uchun kalit so`z KASBIY va k=6 bo`lsin.

Lotin alifbosi bo`yicha Tsezarning kalit so`zli shifrlash tizimi uchun k=6 va KASBIY kalit so`z uchun o`rin almashtirish jadvalini tuzamiz. Jadvalning birinchi satriga 26 ta lotin alfaviti harflarini ketma – ket tartibda yozib chiqamiz. Jadvalning ikkinchi satriga birinchi satrdagi oxirgi k=6 ta harfni ketma ket yozamiz. Agar oxirgi olingan 6 ta harf ichida tanlab olingan KASBIY kalit harflari bo`lsa, ular olinmaydi va undan oldingi harf olinadi. Shunday qilib jadvalning birinchi satrining oxiridan

boshlab KASBIY kalit harflari bilan ustma ust tushmaydigan oltita harf olinadi. Ushbu harflarni kelish tartibi bo`yicha jadvalning ikkinchi satriga ketma – ket yozib bo`lgach KASBIY kalit harflarini ketma – ket yozamiz. Keyin esa jadvalning birinchi satri boshidan boshlab joylashgan harflarini navbat bilan ketma – ket yozishni boshlaymiz. Agar navbatdagi harf KASBIY kalit so`zda mavjud bo`lsa, uni qoldirib navbatdagi harfga o`tamiz. Natijada quyidagi o`rin almashtirish jadvali hosil bo`ladi:

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

Ushbu, k=6 va KASBIY kalit so`z uchun lotin alifbosi bo`yicha Tsezarning kalit so`zli shifrlash tizimi orqali ixtiyoriy xabarni shifrlash va deshifrlashni amalga oshirish mumkin.

1. Xabarni shifrlash uchun xabar harflari almashtirish jadvalining birinchi satridan izlab topiladi va u shu harf ostidagi almashtirish jadvalining ikkinchi satridagi harf bilan almashtiriladi.

Masalan:

INFORMATIKA VA AXBOROT TEXNOLOGIYALARI MUTAXASSISLIGI

so`zni shifrlasak, quyidagi shifr so`zni olamiz:

SDZEJCUMSIU OU UQVEJEM MYQDEYEKSRUYUJS CNMUQULLSLYSKS

2. Shifrlangan xabarni deshifrlash uchun shifrlangan xabar harflari almashtirish jadvalining ikkinchi satridan izlab topiladi va u shu harf ustidagi almashtirish jadvalining birinchi satridagi harf bilan almashtiriladi..

Masalan:

SDZEJCUMSIU OU UQVEJEM MYQDEYEKSRUYUJS CNMUQULLSLYSKS

shifrlangan so`zni deshifrlasak, quyidagi so`zni olamiz:

INFORMATIKA VA AXBOROT TEXNOLOGIYALARI MUTAXASSISLIGI

Tsezarning kalit so`zli shifrlash tizimi uchun kalit so`z sifatida tarkibida takrorlanuvchi harflari bo`lgan ixtiyoriy so`zni ham olish mumkin. Masalan kalit so`z BUGUNGI KUN TALABI va k=4 bo`lsin. eng avvalo kalit so`zni tahlil qilamiz va undagi navbatdagi takrorlanuvchi harfni hamda probelni tushirib qoldiramiz. Takrorlanuvchi harfni hamda probelni tushirib qoldirsak BUGNIKTAL harflardan

tashkil topgan kalit so`zga ega bo`lamiz. endi kalit so`z BUGNIKTAL va k=4 bo`lgan holda almashtirish jadvalini tuzamiz:

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

Ushbu almashtirish jadvali bo`yicha

INFORMATIKA VA AXBOROT TEXNOLOGIYALARI MUTAXASSISLIGI

so`zni shifrlasak, quyidagi shifr so`zni olamiz:

ICUVRDTS'SHETS PW WRXDHDM MBRCDADGISWAWHI AOMWRWJJAIGI

Bir so`zni turli siljish soni va kalit so`z bilan shifrlasak turli xildagi shifrmatn hosil bo`ldi, ya`ni:

SDZEJCUMSIU OU UQVEJEM MYQDEYEKSRUYUJS CNMUQULLSLYSKS

va

ICUVRDTS'SHETS PW WRXDHDM MBRCDADGISWAWHI AOMWRWJJAIGI

Tsezarning kalit so`zli shifrlash tizimining Tsezarning oddiy shifrlash tizimidan shak shubhasiz yutug'i, unda cheksiz kalit so`zlardan foydalanish mumkinligidadir. Ammo bu usullar hozirgi kunda amaliyotda qo`llanilmaydi.Chunki Tsezar shifrini va kalit so`zli Tsezar shifrini kiriptotahlil asosida ochish mumkin. Bu usullar faqat tarix sifatida o`qitiladi.

2.2. Affin tizimidagi Tsezar usuli

Bir alfavitli tizimlarga kriptoanalitik hujum ramzlarni paydo bo`lish chastotasini hisoblashdan boshlanadi: shifrmatnda har bir harfning paydo bo`lishi aniqlanadi. So`ngra shifrmatndagi harfrlarni paydo bo`lish chastotasining tarqaluvchanligi birlamchi xabar alfavitidagi harflar takrorlanish chastotasi bilan taqqoslanadi, masalan ingliz alfaviti. Shifrmatndagi eng ko`p paydo bo`lishlarga ega chastotali harf ingliz tili alfavitidagi eng ko`p takrorlanish chastotasiga ega bo`lgan harf bilan almashtiriladi va hokazo. Shifrlash tizimini omadli ochish ehtimolligi shifrmatnning uzunligi bilan oshaveradi. Shu sababli kriptografiyada axborotlarni aslidan o`zgartirilgan holatga etkazishlarning matematik uslublarini topish va takomillashtirish bilan doimiy ravishda shug'ullanishgan. Ayniqsa Tsezar' shifrlash

tizimiga qo`yilgan kontseptsiyalar juda hosildor bo`lib chiqdi. Natijada Tsezar' shifrlash tizimining birqancha modifikatsiyalari yaratildi. Biz ushbu modifikatsiyalardan birini ko`rib o`tamiz.

Tsezar usuli uchun ham o`rin almashtirishda matematik usul qo`llanilgani bois yangi tizim vujudga kelgan. Bu tizim Tsezar usulidagi Affin tizimi deyiladi.

Tsezar' shifrlash tizimida Z_m butun to`plamlarda faqat addaptiv xususiyatlari ishlatilgan edi. Ammo $Z_m$ ramzlar to`plamini m moduli bo`yicha ko`paytirish mumkin. Qo`shish va m moduli bo`yicha ko`paytirish operatsiyalarini birgalikda qo`llab Tsezar' joylashtirishning Afina tizimini olish mumkin. Bunday tizimni o`zgartirishlarini aniqlaymiz.

$$E_{a,b} : \overline{Z}_m \to \overline{Z}_m \qquad E_{a,b} : t \to E_{a,b}(t)$$

Affin tizimidagi Tsezar usulida har bir harfga almashtiriluvchi harflar maxsus formula bo`yicha aniqlanadi. Bu formula:

at+b (modm)

bu erda a, b - o`zaro bog'liq holda keluvchi butun sonlar, 0≤a, b<m va EKUB (a, m)=1. t – harfning alfavitdagi tartib raqami. Tartib 0 dan boshlanadi.

Demak Affin kriptotizimi TSezar usulining takomillashtirilgan varianti hisoblanadi. U ikkita a va b sonlarga bog'liq. 0<=a,b<=n-1. n - alfavitdagi harflar soni.

Shifrlash uchun:

$$Aa,b(j)=(a*j+b)(\text{mod } n)$$

Deshifrlash uchun:

$$A\text{-}1a,b(j)=(j-b)*a\text{-}1(\text{mod } n)$$

Endi, Affin tizimini qo`llashni misol orqali izohlaymiz.

Masalan, m = 26, a = 3, b = 5 bo`lsin. U holda haqiqatan ham EKUB(3,26)=1 bo`ladi.

Lotin alifbosi bo`yicha Affin tizimi uchun lotin alifbosi harflarini 0 dan 25 gacha nomerlab chiqamiz.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Bu sonlar uchun

3t+5 (mod26)

formula qo`llanilsa, quyidagi moslik sonlarini olamiz.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2

Endi sonlar o`rnigi lotin alifbosi harflarini qo`ysak, natijada quyidagi o`rin almashtirish jadvali hosil bo`ladi:

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

Ushbu, Affin tizimidagi Tsezar usuli bo`yicha m = 26, a = 3, b = 5 bo`lgan holda hosil qilingan o`rin almashtirish jadvali orqali ixtiyoriy xabarni shifrlashimiz va deshifrlashimiz mumkin.

1. Xabarni shifrlash uchun xabar harflari almashtirish jadvalining birinchi satridan izlab topiladi va u shu harf ostidagi almashtirish jadvalining ikkinchi satridagi harf bilan almashtiriladi.

Masalan:

INFORMATIKA VA AXBOROT TEXNOLOGIYALARI MUTAXASSISLIGI

so`zni shifrlasak, quyidagi shifr so`zni olamiz:

DSUVEPFKDJF QF FWIVEVK KRWSVMVXDZFMFED PNKFWFHHDHMDXD

2. Shifrlangan xabarni deshifrlash uchun shifrlangan xabar harflari almashtirish jadvalining ikkinchi satridan izlab topiladi va u shu harf ustidagi almashtirish jadvalining birinchi satridagi harf bilan almashtiriladi.

Masalan:

DSUVEPFKDJF QF FWIVEVK KRWSVMVXDZFMFED PNKFWFHHDHMDXD

shifrlangan so`zni deshifrlasak, quyidagi so`zni olamiz:

INFORMATIKA VA AXBOROT TEXNOLOGIYALARI MUTAXASSISLIGI

Affin tizimi yutug’i kalitlarni boshqarish qulayligi hisoblanadi - shifrlash va qayta ochish kalitlari (a,b) sonlar juftligi ko`rinishida ifodalanadi. Affin tizimi kamchiligi Tsezar tizimidagi kamchiliklarga xosdir.

Affina tizimi hayotda oldingi asrlarda qo`llanilgan, hozirda esa bu tizim asosiy illyustratsiyalar uchun qo`llaniladi.

2.3. Affin tizimidagi Tsezar usulida matnlarni shifrlash dasturi

Himoya tizimining ko`p qirraligiga undan huquqiy, tashkiliy, muhandis-texnik va dasturiy – matematik elementlarining mavjudligi bilan erishiladi. Elementlar nisbati va ularning mazmuni tashkilotlarning axborotni himoyalash tizimining o`ziga xosligini va uning takrorlanmasligini hamda buzish qiyinligini ta`minlaydi.

Hozirgi kunda axborot – kommunikatsiya texnologiyalarining hayotimizning barchasiga kirib kelganligi va axborotlarni asosan elektron shaklda yaratayotganligimiz sababli axborotlar xavfsizligini ta`minlashda axborotni himoyalashning dasturiy – matematik elementi muhim omil hisoblanadi. Axborotni himoyalashning dasturiy – matematik elementi kompyuter, lokal tarmoq va turli axborot tizimlarida qayta ishlanadigan va saqlanadigan qimmatli axborotlarni himoyalash uchun mo`ljallangan. Bu himoya vositasini yaratish lozim. Zamonaviy kriptotizim dasturiy ta`minotini yaratish uchun oddiy bo`lsada, uzoq ishlatib kelingan kriptotizimlarni dasturiy ta`minotini yaratish printsiplari haqida to`liq tushunchaga ega bo`lishimiz talab qilinadi. Shu sababli, quyida ulardan birini yaratish tavsifini keltirib o`tamiz va kriptotizim talab va shartlarini bevosita dasturiy mahsulotga ko`chiramiz.

Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturi uchun eng avvalo *at+b (modm)* formula uchun ikkita a va b sonlarni aniqlab olish lozim.

a, b - o`zaro bog’liq holda keluvchi butun sonlar, 0≤a, b<m va EKUB (a, m)=1 bo`lishi lozim.

Affin tizimidagi TSezar usulida matnlarni shifrlash va deshifrlash dasturi uchun tanlab olinadigan a va b sonlarni aniqlab olish algoritmlari 4-ilovada keltirilgan. Ushbu algoritmlarga asoslangan holda uning dasturini yaratamiz.

Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturi uchun tanlab olinadigan a va b sonlarni aniqlab olish dasturi:

```
{Affin kriptotizimi kalitlarini aniqlash dasturi}
uses crt;
 var p,q: integer;
    k:integer;
    h:char;
```

```
{===============sonning tub ekanligini aniqlash}
function tub(x: integer):boolean;
  var i: longInt;
  begin
   if x>1 then
     begin
       tub:=false;
       for i:=2 to trunc(sqrt(x)) do
           if x mod i = 0 then exit;
         tub:=true;
         end else tub:=false;
   end;
{===============Sonlarning eng katta umumiy buluvchini topish}
Function HOD(a,b:Integer):Integer;
begin
    while (a<>0)and(b<>0) do
      if a>b then a :=a mod b
      else b:=b mod a;
     if a=0 then HOD:=b
     else HOD:=a;
end;
{==================Affin kriptotizimi kalitlarini aniqlash dasturi=====}
BEGIN
  clrscr;
  k:=0;
 repeat
  repeat
       write('0 va 25 sonlar oraligidan birinchi tub sonni kiriting ='); readln(p);
       if (p>=0) and (p<25) then
         begin
          if tub(p)=true then begin writeln('p=',p,' tub son'); k:=1;end
          else writeln(p,' tub son emas, qaytadan:');
```

```
            end
          else writeln(' Tub son 0 va 25 sonlar oraligidan olinsin, qaytadan:');
      until k=1;
      k:=0;
      repeat
          write('0 va 25 sonlar oraligidan ikkinchi tub sonni kiriting ='); readln(q);
          if (q>=0) and (q<25) then
            begin
             if tub(q)=true then begin writeln('q=',q,' tub son'); k:=1;end
             else writeln(q,' tub son emas, qaytadan:');
            end
          else writeln(' Tub son 0 va 25 sonlar oraligidan olinsin, qaytadan:');
      until k=1;
      clrscr;
      writeln('Ixtiyoriy p=',p,' va q=',q, ' tub sonlar tanlandi');
        k:=HOD(p,26);
      writeln('Tanlangan birinchi son va alfavit harflari sonining eng katta umumiy
buluvchsi=',k);
     until k=1;
        h:=readkey;
   END.
```

Endi Affin tizimidagi Tsezar usulida matnlarni shifrlash dasturi matnini keltiramiz. Dasturda lotin alfavitini bosh harflaridan foydalanamiz. Xuddi shunday, qo`shimcha ravishda lotin alfavitining kichik harflarini kiritish ham mumkin. Bu erda kichik harflardan foydalanmaganligimiz uchun kichik harflarni ham bosh harflarga o`tkazdik. Agar shifrlanadigan matnda tinish belgilari va sonlar uchrasa, ular o`zgarishsiz qoldiriladi. Dasturda sonlar o`zaro bog'liq va tub ekanligi tekshirilmaydi. Chunki matnni shifrlash uchun kalit sonlar tekshirib, tanlab olingan bo`lishi kerak. Ularni yuqoridagi dastur yordamida tekshirib olinadi. Dasturga shifrlanadigan matn belgisi sifatida katta va kichik lotin harflarini hamda tinish belgilari va sonlarni kiritish mumkin. Shifrlangan matn bosh harflarda taqdim

qilinadi. Xuddi shu shaklda kirill harflarini ham konstanta sifatida kiritish mumkin. Natijada shifrlanadigan matnda kirill va lotin alfaviti harflari ishtirok etadi.

```
{Affin kriptotizimi orqali shifrlash}
uses crt;
Const  d=25;
      S:array[0..d] of char=('A','B','C','D','E','F','G','H','I','J','K',
           'L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z');
var
     a,b:integer;
     strok,s2,shifr:string[100];
     s1:string[1];
     kol,i:integer;
     id:byte;
     j: integer;
{=== Matnni bosh harflar bilan yozish ======}
function Boshharf(Matn: string): string;
 var
   i: integer;
   tmps:string;
   xarf:char;
begin
  tmps:='';
  for i:=1 to length(Matn) do
    begin
      xarf:=chr(ord(Matn[i]));
      tmps:=tmps+upcase(xarf);
    end;
  Boshharf:= tmps;
end;
{======= Matn harfga mos alfavit harfi raqamini topish}
  function LotCharToInt(ch: string):byte;
   var i:integer;
```

```
  begin
    for i:=0 to d do
      if ch=S[i] then begin LotCharToInt:=i;break; end
      else LotCharToInt:=d+1;
  end;
{================Affin kriptotizimi orqali shifrlash======}
BEGIN
 CLRSCR;
 write('Birinchi tub sonni kiriting ='); readln(a);
 write('Ikkinchi tub sonni kiriting ='); readln(b);
 write('Shifrlanadigan matnni kiriting='); readln(strok);
 TextColor(4);
 writeln; writeln('SHIFRLASH');writeln;
 writeln('Shifrlanadigan soz:');writeln;
 TextColor(1);
 writeln(strok);writeln;
 {strok suzidagi harflarni bosh harflarga almashtirish}
  shifr:='';
  s2:=Boshharf(strok);
  kol:=length(strok);
  for i:=1 to kol do
   begin
    s1:=copy(s2,i,1);
    id:=LotCharToInt(s1);   {sonning alfavitdagi ornini aniqlash}
    if id=d+1 then shifr:=shifr+s1
    else
      begin
        j:=(a*id+b) mod(d+1); {Affin tizimi shifrlashi}
        shifr:=shifr+S[j];
      end;
    end;
 TextColor(4);
```

```
  writeln('Shifrlangan soz:');writeln;
  TextColor(1);
  writeln(shifr);
  readln;
end.
```

2.4. Affin tizimidagi Tsezar usulida matnlarni deshifrlash dasturi

Endi Affin tizimidagi Tsezar usulida shifrlangan matnlarni deshifrlash dasturi matnini keltiramiz. Dasturda lotin alfavitinini bosh harflaridan foydalanamiz. Xuddi shunday, qo`shimcha ravishda lotin alfavitining kichik harflarini kiritish ham mumkin. Bu erda kichik harflardan foydalanmaganligimiz uchun kichik harflarni ham bosh harflarga o`tkazdik. Agar shifrlangan matnda tinish belgilari va sonlar uchrasa, ular o`zgarishsiz qoldiriladi. Dasturda sonlar o`zaro bog'liq va tub ekanligi tekshirilmaydi. Chunki matnni shifrlash uchun kalit sonlar tekshirib, tanlab olingan bo`lishi kerak. Ularni yuqoridagi dastur yordamida tekshirib olinadi. Shifrlangan matnni deshifrlash uchun shifrlashda ishlatilgan kalit so`zlar ishlatilishi shart, aks holda deshifrlash natijasi noto`g'ri bo`ladi, ya`ni shifrlangan matn o`zgartirib yuboriladi. Dasturga shifrlangan matn qanday berilgan bo`lsa, shundayligicha kiritilishi lozim. Deshifrlangan matn bosh harflarda taqdim qilinadi.

Endi Affin tizimidagi Tsezar usulida matnlarni deshifrlash dasturi matnini keltiramiz:

```
{Affin kriptotizimi orqali shifrlash}
uses crt;
Const  d=25;
      S:array[0..d] of char=('A','B','C','D','E','F','G','H','I','J','K',
           'L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z');
var
     a,b:integer;
     strok,s2,dshifr:string[100];
     s1:string[1];
     kol,i:integer;
     id:byte;
     j: integer;
```

```
{=== Matnni bosh harflar bilan yozish ======}
function Boshharf(Matn: string): string;
 var
  i: integer;
  tmps:string;
  xarf:char;
begin
 tmps:='';
 for i:=1 to length(Matn) do
  begin
   xarf:=chr(ord(Matn[i]));
   tmps:=tmps+upcase(xarf);
  end;
 Boshharf:= tmps;
end;
{======================Shifrlangan harfga mos alfavit harfi raqamini topish}
 function Deshifr(n: byte):byte;
  var i,j:integer;
  begin
    for i:=0 to d do
     begin
      j:=(a*i+b) mod(d+1);
      if n=j then begin Deshifr:=i;break; end
      else Deshifr:=d+1;
     end;
  end;
{======================Matn harfga mos alfavit harfi raqamini topish}
 function LotCharToInt(ch: string):byte;
  var i:integer;
  begin
    for i:=0 to d do
```

```
      if ch=S[i] then begin LotCharToInt:=i;break; end
      else LotCharToInt:=d+1;
   end;
{=======================Affin kriptotizimi orqali shifrlash======}
BEGIN
 CLRSCR;
 write('Birinchi tub sonni kiriting ='); readln(a);
 write('Ikkinchi tub sonni kiriting ='); readln(b);
 write('Shifrlangan matnni kiriting='); readln(strok);
 TextColor(4);
 writeln; writeln('DESHIFRLASH');writeln;
 writeln('Shifrlanadigan soz:');writeln;
 TextColor(1);
 writeln(strok);writeln;
 {strok suzidagi harflarni bosh harflarga almashtirish}
  dshifr:='';
  s2:=Boshharf(strok);
  kol:=length(strok);
  for i:=1 to kol do
   begin
    s1:=copy(s2,i,1);
    id:=LotCharToInt(s1);   {harfning alfavitdagi ornini aniqlash}
    j:=Deshifr(id);         {shifr raqamiga mos matn raqamini aniqlash}
    if j=d+1 then dshifr:=dshifr+s1
    else dshifr:=dshifr+S[j];
   end;
 TextColor(4);
 writeln('Deshifrlangan soz:');writeln;
 TextColor(1);
 writeln(dshifr);
{  readln;}
end.
```

2.5. Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlashni o`rgatish metodikasi

Mavzu	**Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash**

Axborotli ma`ruzada o`qitish texnologiyasi.

Vaqt – 2 soat	Talabalar soni: 70-80 nafar
O`quv mashg'ulotining shakli	Axborotli ma`ruza
*Ma`ruza mashg'ulotining rejasi* (O`quv jarayonining mazmuni)	• Axborotlar xavfsizligi va himoya tizimlari. • Kriptografiya. • TSezar usuli va kalit so`zli Tsezar tizimi. • Affin tizimidagi Tsezar usuli.
O`quv mashg'ulotining maqsadi: Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash xususidagi bilimlarni shakllantirish.	
Pedagogik vazifalar: - Axborotlar xavfsizligi tushunchasini ochib berish; - Axborotlar himoya tizimlari tushuntirib beriladi; - Kriptografiya haqida tushuncha berish; - Tsezar usuli va kalit so`zli Tsezar tizimini tavsiflash; - Affin tizimidagi Tsezar usulini ochib berish.	*O`quv faoliyati natijalari:* *Talaba:* - Axborotlar xavfsizligi tushunchasini tushunadi; - Axborotlar himoya tizimlari nima ekanligini anglaydi; - Kriptografiya haqida tushunchaga ega bo`ladi; - Tsezar usuli va kalit so`zli Tsezar tizimini o`rganadi; - Affin tizimidagi Tsezar usulini anglaydi.
O`qitish uslubi va texnikasi	Sxemalar orqali ko`rgazmali ma`ruza, grafik organayzerlar texnikasi (kontseptual jadval)
O`qitish vositalari	Texnik jihozlangan auditoriya, guruhda ishlash bo`yicha shart-sharoitlar.
O`qitish shakli	Frontal jamoaviy ishlash, guruhlarda ishlash
O`qitish shart-sharoiti	Ma`ruza va vizual materiallar, kompyuter texnologiyalari
Monitoring va baholash	Og'zaki nazorat: blits-so`rov

Ishning bosqichlari	Faoliyat mazmuni	
	O`qituvchining	Talabalarning
1-bosqich O`quv mashg'ulotiga kirish (5 minut)	1.1. Ma`ruza mashg'ulotining nomini e`lon qiladi. Asosiy masalalarni va terminlarni izohlaydi, o`quv mashg'ulotining maqsadi va rejalashtirilgan o`quv natijalar bilan tanishtiradi.	Eshitadilar O`UM – ni ko`radilar
2-bosqich Asosiy (65 - minut)	2.1. Ushbu mashg'ulotda nimalar haqida fikr boradi - degan savolga javob topishni taklif etadi. 2.2. O`quv mavzuning mazmunini reja asosida yoritib beradi. Organayzerlarni ekranga chiqarib tushuntiradi. 2.3. Guruhni 3 ta kichik guruhlarga bo`ladi. Kontseptual jadvalni to`ldirish qoidasini tushuntiradi (3-ilova). Dastavval mustaqil alohida va keyinchalik guruhda me`yorlashtirishga tegishli kontseptual jadvalni to`ldirish bo`yicha topshiriq beradi. Guruhlarda ishni tashkil etadi. 2.4. Olingan natijalarni prezentatsiyasini boshlashni e`lon qiladi. Prezentatsiya jarayonida har bir guruh bajargan ishni talabalar bilan muhokama qiladi, uni baholab beradi va to`ldirib boradi. 2.5. Kontseptual jadvalning to`ldirilgan yakuniy variantini daftarga ko`chirishni taklif etadi.	Ma`ruza matnida belgilar qo`yadilar. Avval yakka tartibda keyin-chalik guruhda tah-lil asosida umu-miy kontseptual jadvalni tuzadi-lar. Guruh sardorlari prezentatsiyani na-moyish qiladilar, qolgan talabalar muhokamada qatna-shadilar. Tayyor kontseptual jadvalni daftarga ko`chiradilar.
3-bosqich Yakuniy (10-minut)	3.1. Mavzu bo`yicha yakuniy xulosalar chiqaradi, uni umumlashtiradi, tayanch iboralarga e`tiborni qaratadi. 3.2.Ishni baholaydi: Guruhlardagi faollarni va passiv talabalarni ta`kidlaydi. Guruhda ishlash bo`yicha tavsiyalarni beradi. 3.3. Mustaqil ish bo`yicha topshiriqlar beradi: o`z-o`zini tekshirish bo`yicha savollarga javob tayyorlash (4-ilova), keyingi mavzuni o`qib kelish.	Topshiriqlarni yozib oladilar

III. Ish joyi muhitining ob-havo sharoiti

3.1. Inson organizmining tashqi muhitga moslashuvi

Ish joyi muhitining ob-havo sharoiti insonning mehnat qilish qobiliyatiga, uning sog'lig'iga juda katta ta`sir ko`rsatadi. Insonning hayot faoliyatida ob-havo omillarining deyarli salbiy yoki ijobiy holatlarda ta`sirini bilish va uni mo``tadillashtirishga qaratilgan chora-tadbirlarni qo`llash mehnat qilish jarayonida mehnat samaradorligini oshirishga ijobiy ta`sir ko`rsatadi. Qo`llanilgan chora-tadbirlar ba`zi sharoitlarda foydali bo`lishi yoki zararli bo`lishi mumkin. Ish bajarilayotgan joylarda havo harorati yuqori bo`lgan vaqtda ijobiy va harorat past bo`lgan vaqtda esa salbiy natija berishi kuzatiladi.

Ob-havo sharoitining doimo o`zgarib turishida tana haroratining o`zgarmasligini saqlashni inobatga olib organizmdagi biokimyoviy jarayonlar faoliyatiga yaxshi imkoniyat yaratadi. Tana harorat darajasining ortib ketishi issiqlash, tushib ketishi esa sovish deb ataladi. Issiqlash va sovish hayot faoliyatini buzuvchi halokatli holatni vujudga keltiradi. Shuning uchun ham inson organizmida tashqi muhit bilan moslashuvchi fiziologik mexanizm mavjud bo`lib, u markaziy asab tizimining nazorati ostida bo`ladi. Bu fiziologik mexanizmning asosiy vazifasi organizmda modda almashinuvi natijasida ajralib chiqayotgan issiqlikning ortiqchasini tashqi muhitga chiqarib, issiqlik nisbatini saqlab turadi.

Ish joylaridagi ob-havo sharoitini havoning quyidagi ko`rsatkichlari belgilaydi:

- havoning harorati, 'C' bilan o`lchanadi;
- havoning nisbiy namligi, % bilan aniqlanadi;
- havo bosimi, R/mm simob ustuni yoki Pa bilan o`lchanadi;
- ish joyidagi havo harakati tezligi, m/s bilan o`lchanadi.

Bulardan tashqari ob-havo sharoitiga ta`sir qiluvchi ishlab chiqarish omillari ham mavjud. Bular har xil mashina-mexanizmlar materiallari yuzalaridan tarqaladigan issiqlik nurlari bo`lib, havo haroratini oshirishga olib keladi. Yoz paytlarida korxona hovlisida to`xtab turgan mashinalar va boshqa temir beton hamda asfal't qoplamasi materiallaridan tarqalayotgan issiqligi xuddi alangadan tarqalgan haroratga o`xshaydi. Bular, albatta, korxona hududida havo haroratini oshiruvchi asosiy omillar bo`lib hisoblanadi.

Bu omillar ta`siridan hosil bo`ladigan harorat korxona havo muhitining mikroiqlimi deb yuritiladi.

Ob-havo omillari mehnat qilish qobiliyatiga va insonning sog'lig'iga juda katta ta`sir ko`rsatadi. Ishlab chiqarish sharoitida ob-havo omillarining deyarli hammasi bir vaqtda ta`sir qiladi. Ba`zi sharoitlarda bunday ta`sir ko`rsatishi foydali bo`lishi mumkin. Masalan, sovuq sharoitda tananing qurishi natijasida darmonsizlanish ko`proq uchraydi, ba`zi vaqtlarda esa, bir-biriga qo`shilishi natijasida zararli ta`sir darajasi ortib ketishi mumkin. Ana shunday, nisbiy namlik va haroratning ortib ketishi inson uchun og'ir sharoitni vujudga keltiradi. Bundan tashqari, ish joylaridagi havo harakatini oshirish harorat yuqori bo`lgan vaqtda ijobiy va harorat past bo`lgan vaqtda esa salbiy natija beradi.

Bundan ko`rinib turibdiki, ob-havo omillari ba`zi hollarda kishiga ijobiy va ba`zan esa salbiy ta`sir ko`rsatib, inson organizmining tashqi muhitga moslashuvini buzib yuborishi mumkin. Tanada muhitga moslashuv - bu inson organizmining fiziologik va kimyoviy jarayonlar asosida tana haroratining bir xil chegarada (36—37°S) saqlab turish qobiliyati, demakdir.

Tashqi muhitga moslashuv ikki xil: fizik va kimyoviy bo`lishi mumkin. Tashqi muhitga kimyoviy moslashuv organizmning issiqlash davrida modda almashinuvini kamaytirishi va sovishi natijasida modda almashinuvini oshirishi, ammo tashqi muhitga kimyoviy moslashuv uning keskin o`zgarishi borasida tashqi muhitga fizik moslashuvga nisbatan ahamiyati katta emas. Organizmning tashqi muhitga issiqlik chiqarishi uch yo`l bilan o`tishi mumkin:

- odam tanasining umumiy yuzasida infraqizil nurlanish orqali (radiatsiya orqali havo almashinuvi);

- tanani o`rab turgan havo muhitini isitish (konvektsiya);

-terining terlab bug'lanishi va nafas olish yo`llari orqali suyuqliklarning bug'lanishi natijasida.

Me`yoriy sharoitda, kuchsiz havo harakati bo`lgan holatlarda harakatsiz odam tanasi radiatsiya yo`li bilan organizm ishlab chiqarayotgan issiqlikning 45 foizini, konvektsiya natijasida 30 foiz va terlash orqali 25 foizini yo`qotishi aniqlangan. Bunda teri orqali umumiy issiqlikning 80 foizidan ortig'i, nafas olish a`zolari orqali 13 foiz va taxminan 5 foiz issiqlik ovqat, suv va havoni isitishga sarflanadi.

Radiatsiya va konvektsiya orqali issiqlikni yo`qotish faqat tashqi muhit harorati tana haroratidan kam bo`lgan hollarda bo`lishi mumkin. Shuni aytib o`tish kerakki, tashqi muhit harorati qancha past bo`lsa, issiqlik yo`qotish shuncha kuchli bo`ladi.

Tashqi muhit harorati tana haroratidan yuqori yoki teng bo`lsa, u holda issiqlik ajratish terlab bug'lanish hisobidan bo`ladi. 1 gramm terni bug'latish uchun 2,5 kJ (0.6 kkal) issiqlik yo`qotiladi.

Organizmdan chiqadigan terning miqdori tashqi muhit haroratiga va bajariladigan ish kategoriyasiga bog'liq. Harakatsiz organizmda, tashqi muhit harorati 15°S ni tashkil qilsa, terlash juda kam miqdorni (soatiga 30 ml) tashkil qiladi. Yuqori haroratlarda esa (30 °S va undan yuqori), ayniqsa og'ir ishlarni bajarganda organizmning terlashi juda ortib ketadi.

Masalan, issiq paytlarda, og'ir ishlarni bajarish natijasida terlash miqdori soatiga 1 - 1,5 litrga etadi va bu miqdor terning bug'lanishi uchun 2500-3800 kJ (600-900 kkal) issiqlik sarflanadi.

Shuni aytib o`tish kerakki, terlash yo`li bilan issiqlik sarflash faqatgina tana yuzasida ter bug'langandagina amalga oshadi. Terning bug'lanishi esa havoning harakatiga va nisbiy namligiga, kiygan kiyimining matosiga bog'liq.

Faqat terlash yo`li bilan issiqlik yo`qotilganda havoning nisbiy namligi 75—80 foiz ortiq bo`lsa, terning bug'lanishi qiyinlashadi va organizmning tashqi muhitga moslashuvi buzilishi natijasida issiqlash yuz berishi mumkin. Issiqlashning birinchi belgisi tana haroratining ko`tarilishidir. Kuchsiz issiqlash tana haroratining engil ko`tarilishi, haddan tashqari ter chiqishi, kuchli chanqoq, nafas olish va qon tomirlar urishining tezlashishi bilan chegaralanishi mumkin. Agar kuchli issiqlash yuz bersa, unda nafas olish qiyinlashadi, bosh qattiq og'riydi va aylanadi, nutqi qiyinlashadi.

Tashqi muhitga moslashishning bu xildagi buzilishi va tana haroratining keskin ko`tarilishi issiqlik gepatermiyasi deb ataladi.

Issiqlashning ikkinchi belgisi terlash natijasida inson organizmining ko`p miqdorda tuz yo`qotishi natijasida kelib chiqadi. Bu holat teri hujayralarida tuzning kamayishi tufayli, terining suvni ushlab qolish qobiliyati susayganligidan kelib chiqadi. Ichilayotgan suv tinmay ter bo`lib chiqib ketganligi sababli, organizm kuchli chanqoqlik sezadi, ichilgan suvning tezda chiqib ketishi chanqoqni yana kuchaytiradi va bu suv bilan zaharlanish holatini vujudga keltirishi mumkin. Bunda organizmning

paylarida qaltirash paydo bo`ladi, kuchli terlash va qonning quyuqlashishi kuzatiladi. Bu holat qaltirash kasalligi deb yuritiladi. Keyin issiq urish vujudga keladi, tana qarorati 40—41°S ga ko`tarilib, odam hushini yo`qotadi va qon tomirlarining urishi kuchsizlashadi. Bu vaqtda organizmdan ter chiqish butunlay to`xtaydi. Qaltirash kasali va issiq urish o`lim bilan tugashi mumkin.

Tashqi asab tizimlarining sovuq urishi natijasida suyaklarda radikulit, oyoq-qo`l va bel bo`g'inlarida hamda paylarda revmatizm kasalligi, shuningdek plevrit, bronxit va boshqa shamollash bilan bog'liq bo`lgan yuqumli kasalliklar kelib chiqishi mumkin.

Odam organizmiga sovuqning, ayniqsa, havo harakatining ta`siri kuchli bo`lib, havoning nisbiy namligi yuqori bo`lgan vaqtda bu yaqqol namoyon bo`ladi.

Chunki sovuq haroratdagi nam havo issiqlikni yaxshi o`tkazadi va havo almashish (konvektsiya) orqali issiqlik yo`qotishni kuchaytiradi.

3.2. Ishlab chiqarish mikroiqlimining gigienik me`yorlari

Ishlab chikarish mikroiqlimi me`yorlari mehnat havfsizligi standartlari tizimi 'Ish zonasi mikroiqlimi' (GOST 12.1- 005-76) ga asosan belgilangan. Ular gigienik, texnik va iqtisodiy negizlarga asoslangan. Korxonalardagi xonalar, yil fasllari va ish toifasiga qarab, ulardagi harorat, nisbiy namlik va havo harakatining ish joylari uchun ruxsat etilgan me`yorlari belgilangan.

Ish toifalari quyidagicha belgilanadi: engil jismoniy ishlar (I toifa) o`tirib, tik turib yoki yurib bajariladigan, biroq muntazam jismoniy zo`riqish yoki yuklarni ko`tarishni talab qilmaydigan ishlar, energiya sarfi soatiga 150 kkal (172 J.s)ni tashkil etadi(3.2.1.- jadval).

O`rtacha og'irlikdagi jismoniy ishlarga (II toifa)— soatiga 150—250 kkal (172-293 J.s) energiya sarflanadigan faoliyat turlari kiradi. Bunga doimiy yurish va og'ir bo`lmagan (10 kg gacha) yuklarni tashish bilan bog'liq bo`lgan ishlar kiradi(3.2.1.-jadval).

3.2.1-jadval

Ishlab chiqarish xonalari, ish joylaridagi havoning harorati, nisbiy namligi va harakat tezligining risoladagi me`yorlari

Yil fasli	Ish toifalari	Havoning harorati, °S	Nisbiy namligi,%	Harakat tezlig/s
Sovuq	Engil — I	20-23	60-30	0,2
	O`rtacha og'irlikdagi— I a	18-20	60-40	0,2

	O`rtacha og'irliqdagi— I b	17-19	60-40	0,3
	Og'ir—SH	16-18	60-40	0,3
Iliq	Engil—I	20-25	60-40	0,2
	O`rtacha og'irliqdagi— I a	21-23	60-40	0,3
	O`rtacha og'irlikdagi— I b	20-22	60-40	0,4
	Og'ir —II	18-21	60-40	0,5
Issiq	Engil— 1	20-30	60-30	0,3
	O`rtacha og'irliqdagi — I a	20-30	60-30	0,4-0,5
	O`rtacha og'irliqdagi —16	20-30	60-30	0,5-0,7
	Og'ir —SH	20-30	60-30	0,5-1,0

Og'ir jismoniy ishlar (III toifa) — muntazam jismoniy zo`riqish, xususan og'ir yuklarni (10 kg dan ortiq) muttasil bir joydan ikkinchi joyga ko`chirish va ko`tarish bilan bog'liq ishlar kiradi. Bunda energiya sarfi soatiga 250 kkal (293 J. s) dan yuqori bo`ladi (3.2.2-jadval).

Yilning sovuq va iliq davrida ishlab chiqarish xonalari harorati, nisbiy namligi va havo harakati tezligining yo`l qo`yiladigan me`yorlari.

3.2.2-jadval

Havo harorati, °S	Nisbiy namligi, %	Harakat tezligi, m/s	Tashqaridagi havo harorati, °S
19-25	75	0,2	15-30
17-25	75	0,2	15-30
13-25	75	0,4	15-30
13-25	75	0,5	15-30

Harorat, nisbiy namlik va havo harakatining tezligi risoladagi va yo`l qo`yilishi mumkin bo`lgan miqdorlar ko`rinishida belgilanadi. Risoladagi miqdorlar deganda odamga uzoq muddat va muntazam ta`sir qilganda tashqi muhitga moslashuv reaktsiyalarini kuchaytirmasdan organizmning me`yoriy faoliyatini va issiqliq holatini saqlashni ta`minlaydigan mikroiqlim ko`rsatkichlarining yig'indisi tushunilib, ular issiqlik sezish mo``tadilligini vujudga keltiradi va ish qobiliyatini oshirish uchun shart-sharoit hisoblanadi.

Yo`l qo`yilishi mumkin bo`lgan mikroiqlim sharoitlari organizmning faoliyatini va issiqlik holatdagi o`zgarishlarni, fiziologik moslanish imkoniyatlaridan chetga chiqmaydigan tashqi muhitga moslashish reaktsiyalarining kuchayishini bartaraf etadigan va tez me`yorga soladigan mikroiqlim ko`rsatkichlarining yig'indisidir. Bunda sog'liq uchun xatarli holatlar vujudga kelmaydi, biroq nomo``tadil issiqlik sezgilari, kayfiyatning yomonlashuvi va ish qobiliyatning pasayishi kuzatilishi mumkin. 3.2.1, 3.2.2, 3.2.3-jadvallarda mikroiqlimning risoladagi va yo`l qo`yilishi mumkin bo`lgan me`yorlari keltirilgan. Doimiy ishlarda 3.2.1 jadvalda keltirilgan

miqdorlar ta`minlanishi lozim, ular havoni mo``tadillashtirishda ham majburiydir. Qator hollarda, masalan, issiqlik ko`p ajralib chiqadigan yoki isitiladigan xonalarning hajmi katta bo`lgan metallurgiya, mashinasozlik va boshqa zavodlarda yo`l qo`yiladigan me`yorlarga (3.2.1, 3.2.2-jadval) asoslanish mumkin, biroq mehnat va dam olish holatlariga qo`yiladigan gigienik talablarga, organizmning issiqlab ketishi va sovuq qotishini oldini olishga qaratilgan barcha vositalaridan foydalanishga ham amal qilish zarur.

Yo`l qo`yilishi mumkin bo`lgan me`yorlar yilning sovuq va bir mavsumdan ikkinchisiga o`tish davrlarida (tashqi havoning) o`rtacha kundalik harorati +10 °S dan yuqori (yoki muvofiq holda past) doimiy ish joylaridan tashqarida (3.2.1-jadval) birmuncha katta raqamlarda o`zgarib turishi, yilning issiq paytida esa (3.2.2-jadval) ish joylari havosining oshgan harorati (ayniqsa, Markaziy Osiyo sharoitida va issiqlik ajralib chiqishi mumkin bo`lgan ish joylarida) issiqlikning ancha ortiqcha bo`lishini ko`zda tutadi. Bu tashqi muhitning issiq bo`lishi bilan birga katta miqdordagi issiqlikni yo`qotishning qiyinligi bilan bog'liq.

Biroq bu holda ham me`yorlar yo`l qo`ysa bo`ladigan maksimumni chegaralaydi. Issiqlik ajralishi yuqori bo`lgan ish joylarida havoning harakat tezligi ham birmuncha ortiqcha belgilanadi.

3.2.3 - jadval

Yilning issiq davridagi ishlab chiqarish xonalari harorati, nisbiy namligi va havo harakati tezligining yo`l qo`yiladigan me`yorlari

Ish toifalari	Harorati, °S	Nisbiy namlik, %	Havo harakati tezligi, m/s
engil -1	eng issiq oyning soat 13 da tashqi havo o`rtacha haroratidan yuqori bo`lmasligi biroq 28°S dan oshmasligi kerak	28 °Sda 55-27° Sda 26 °Sda 65 25 °Sda 70 24 °Sda 75 dan ortiqbo`l-masligi kerak	0,2-0 50,8-0,7 0,3-0,7 0,3-0,7 0,3-0,7
o`rtacha og'ir-likdagi -1a			
o`rtacha og'ir-likdagi—116		26°Sda65 25 °Sda 70	0,5 - 1,0 0,5-0,1
og'ir - 111	eng issiq oyning soat 13da tashqi havo haroratidan 5 °S dan yuqori bo`lmasligi, biroq 26 °S dan oshmasligi kerak	24 °Sda va bundan past bo`lganda75dan ortiq bo`lmas-ligi kerak	0,5-0,1

Xonalarning katta-kichikligi, bir vaqtning o`zida ham issiqlik, ham namlikning ajralishi, doimiy harorat va namlik kabilarni sun`iy usulda tutib turish sharoitlarini

hisobga oladigan koeffitsientlarni ishlab chiqish lozim bo`ladi. Ish nechog'liq og'ir bo`lsa, harorat shunchalik past va havo harakati shuncha yuqori bo`ladi.

3.3. Atmosfera tarkibidagi changlar

Sanoatda, transport vositalarini ishlatishda va qishlok xo`jaligida bajariladigan ishlarning deyarli hammasida chang hosil bo`lishi va ajralishi kuzatiladi. Umuman changlar, ularning kelib chiqish manbalarini hisobga olgan holda tabiiy va sun`iy changlarga bo`lib o`rganiladi. Ma`lumki, changlangan havo muhiti insoniyatni qadim zamonlardan beri ta`qib qilib kelgan. Tabiiy changlar sirasiga tabiatda inson ta`sirisiz hosil bo`ladigan changlar kiritiladi. Bunday changlarga shamol va qattiq bo`ronlar ta`sirida tuproqning erroziyalangan qatlamlarining uchishi, o`simlik va hayvonot olamida paydo bo`ladigan changlar, vulqonlar otilishi, kosmosdan er atmosferasi ta`siriga tushib qolgan meteoritlar, kosmik jismlarning yonib ketishidan hosil bo`ladigan changlar va boshqa hollarda hosil bo`ladigan changlarni kiritish mumkin.

Tabiiy changlarning atmosfera muhitidagi miqdori tabiiy sharoitga, havoning holatiga, yilning fasllariga va aniqlanayotgan joyning qaysi mintaqada joylashganligiga bog'liq. Masalan, atmosferadagi chang miqdori shimoliy hududlarga nisbatan janubiy hududlarda, o`rmon mintaqalariga qaraganda cho`l mintaqalarida, shuningdek qish oylariga nisbatan yoz oylarida ko`proq bo`lishi ma`lum. Aniqlanishicha, har bir kubometr havo tarkibida katta shaharlar hududlarida 6000 atrofida (ba`zi bir manbalarda avtomobil vositalaridan ajralgan tutunlarni ham kiritib 30000) har xil kattalikdagi chang zarralari bo`lishi aniqlangan. Dalalar va bog'larda bu miqdor o`n marta kamayadi, tog'li hududlarda esa undan ham kamroq chang zarralari bo`ladi.

Sun`iy changlar sanoat korxonalarida va qurilishlarda insonning bevosita yoki bilvosita ta`siri natijasida hosil bo`ladi. Masalan, mashinasozlik sanoatida cho`yan ishlab chiqaruvchi domna va marten pechlarida va hamda tosh tsexlarida, issiqlik elektrostantsiyalarida yoqilgan ko`mirning ma`lum qismi kul va tutun sifatida atmosferaga chiqarib yuboriladi. Qurilish ishlarida er qazish, portlatish, tsement ishlab chiqarish, shuningdek tog'lardan ma`danlarni qazib olish va boshqa juda ko`p ishlarda ko`plab miqdorda chang ajraladiki, bu changlarni atrof-muhitga chiqarib yuborish tabiatga halokatli ta`sir ko`rsatishi mumkin.

Sanoatning ba`zi bir tarmoqlarida, masalan, kimyo sanoatida shunday havfli sanoat changlari ajraladiki, ularni tozalamasdan chiqarib yuborish fojiali holatlarni vujudga keltiradi. Kelib chiqishi bo`yicha organik, mineral va aralashma changlar mavjud. Changning zararli ta`sirining tavsifi asosan uning kimyoviy tarkibiga bog'liq. Changning kattaligi (ya`ni dispers tarkibi) bo`yicha uch guruhga bo`lib qaraladi:

a) kattaligi 10 mkm dan katga bo`lgan changlar yirik changlar deb ataladi. Odatda bunday changlar o`z og'irligi ta`sirida erga qo`nadi;

b) katgaligi 10 mkm dan 0,25 mkm gacha bo`lgan changlar. Bu changlarni mayda changlar yoki mikroskopik changlar deb yuritiladi. Ular erga ma`lum ijobiy sharoitlar bo`lganda, masalan, yomg'ir, qor va shabnam kabi erga yog'ilayotgan og'ir zarralarga ilashib qo`nishi mumkin;

v) kattaligi 0,25 mkm dan kichik bo`lgan changlar ul'tra mikroskopik changlar deb yuritiladi va bu changlar hech qachon erga qo`nmay, betartib harakat qilib, uchib yuradi.

3.4. Ish joyidagi havo muhiti

Havoning kimyoviy tarkibi va xossalari - inson hayotida havoning ahamiyati juda katta ekanligi ma`lum. Uning kimyoviy tarkibi, fizik xususiyatlari va tarkibida har xil moddalarning bo`lishi, havodan nafas olib, mehnat qilayotgan kishilar uchun juda muhim. Chunki, havoning tozaligi inson salomatligiini saqlovchi muhim omil hisoblanadi.

Er atmosferasi quruq havo bilan ma`lum miqdorda suv bug'larining aralashmasidan tashkil topgan. Quruq atmosfera havosining tarkibida 78 foiz azot, 20,9 foiz kislorod, 0,3 foiz karbonat angidridi va uncha ko`p bo`lmagan miqdorda geliy, neon, kripton va boshqa gazlar bor.

Ma`lumki, inson uchun eng mudhishi havo tarkibida kislorodning kam miqdorda bo`lishidir.

Havo holati uning bosimi, zichligi, harorati, absolyut namligi, namlik sig'imi, nisbiy namligi, issiqlik sig'imi va boshqalar bilan belgilanadi.

Ish joyidagi havo muhitini mo``tadillashtirishda shamollatishning ahamiyati kattadir. SHu sababdan quyida shamollatishning usullari keltirilgan.

Umumiy shamollatish. Ishlab chiqarish binolarida ajralib chiqayotgan har xil zararli moddalarni shamol yo`naltirish vositasi bilan birgalikda chiqarib yuborishning imkoniyati bo`lmasa yoki ajralib chiqayotgan moddalar, texnologik jarayonning maydonlaridan ajralib chiqayotgan bo`lsa, unda yakka tartibda shamollatish vositalarini qo`llash imkoniyati yo`qoladi. Bunday hollarda umumiy shamollatish usulidan foydalaniladi. Umumiy shamollatish vositasini zararli moddalar yoki issiqlik eng ko`p ajralib chiqayotan joyga o`rnatish kerak.

Ishlab chiqarish joylarida yig'ilgan havodagi zararli moddalarni havo almashtirish maqsadida o`rnatilgan havo qabul qilish vositalari orqali chiqarib yuborish mumkin. Sof havoni esa yuqorida ko`rsatib o`tilgan vositalarning biri yordamida hosil qilish mumkin. Qanday yo`l bilan xonaga sof havo berish va zararli moddalar yig'ilgan havoni chiqarib yuborish usullari zararli moddaning xona bo`ylab tarqalish xususiyatiga bog'liq bo`ladi. Masalan, agar ish joyida ko`plab issiqlik ajralib chiqishi mumkin bo`lgan mashina va mexanizmlar o`rnatilgan bo`lsa, ularni ish joyida joylashish holatiga qarab shamollatish usullari qo`llaniladi.

Bundan tashqari har xil zararli omillarga ega bo`lgan jihozlarni ish joylari bo`ylab joylashtirishning ham ahamiyati katta. Shuning uchun ham korxona binolar loyihalanayotgan vaqtda iqlim sharoitini, quyosh nurlarining tushish holatlari va ish joyidagi jihozlarni to`g'ri joylashtirish masalalari qoniqarli hal qilingan bo`lsa, shamollatish vositalarini o`rnatish ham shunchalik osonlashadi.

Tabiiy shamollatish. Tashqaridan bino ichiga kirgan sovuq havo bino ichidagi issiqlik hisobiga issiqlik qabul qilib, isigandan keyin hajmi kengayganligi sababli binoning yuqori tomoniga qarab harakatlanadi va agar binoning yuqori qismida havoning chiqib ketishi uchun quvur yoki tirqishlar hosil qilinsa, unda havoni tashqariga chiqarib yuborish imkoniyatiga ega bo`lamiz. Bu jarayon korxona binolarida, shuningdek, har qanday binoda, ayniqsa, sovuq faslda davom etadi va mazkur hodisa aeratsiya deb yuritiladi.

Ushbu usuldan foydalanishda asosiy e`tiborni havoni kirish yo`nalishlari va chiqish joylarini ta`minlashga qaratish lozim. Ma`lumki, issiq havo yuqoriga qarab ko`tariladi, sovuq havo esa pastga yo`naladi. Shuning uchun ko`p miqdorda issiqlik ajralib chiquvchi ish joylarida sovuq havoni poldan 4 m balandlikdan berish maqsadga muvofiq hisoblaniladi. Sovuq havo pastga qarab yo`nalishi borasida issiq

havo bilan aralashadi, isiydi va vajudga kelgan tabiiy oqimlar harakatiga qo`shilib uzluksiz harakat hosil qiladi. Bu uzluksiz harakat davomida oqimlarga yangidan yangi miqdorlar qo`yilishi natijasida yuqori to`siqlar tomon yo`naladi va bir qismi tabiiy shamollatish tirqishlaridan tashqariga chiqib ketadi. Bir qismi esa sovub yana pastga qarab yo`naladi va bu bilan havoning xona ichidagi aylanma harakatini kuchaytirishga o`z hissasini qo`shadi. Shunday qilib binolarning ichida havo harakatining tutash oqimlari vujudga keladi. Buni 3.4.1 -rasmda ko`rsatilgan shaklda ifodalash mumkin. Agar tashqarida havo nihoyatda issiq bo`lsa (30 - 40°S atrofida), tabiiy shamollatishga ehtiyoj oshadi.

Tabiiy shamollatishni hisoblashda, asosan, ma'lum darajadagi isish hisobiga engillashib, binoning yuqori qismlarida yig'ilgan ortiqcha bosimni, biron-bir havo chiqarib yuborish joyidan tashqariga yo`naltirish mo`ljallanadi. Faraz qilaylik: 3.4.1-rasmda ko`rsatilgan ko`ndalang kesimga ega bo`lgan ish joylarida umumiy havo bosimi asosida ma`lum balandlikka ko`tarilgan havo isib, xona haroratiga tenglashgan chizig'ini belgilab olsak, shu 0 chiziqdan yuqori tomonda bosim ortiqcha bo`lib, past tomonda bir muncha kam bo`lishi shakldan ko`rinib turibdi.

Ortiqcha bosim balandlik hisobiga hosil bo`lganligidan uni quyidagicha ifodalash mumkin:

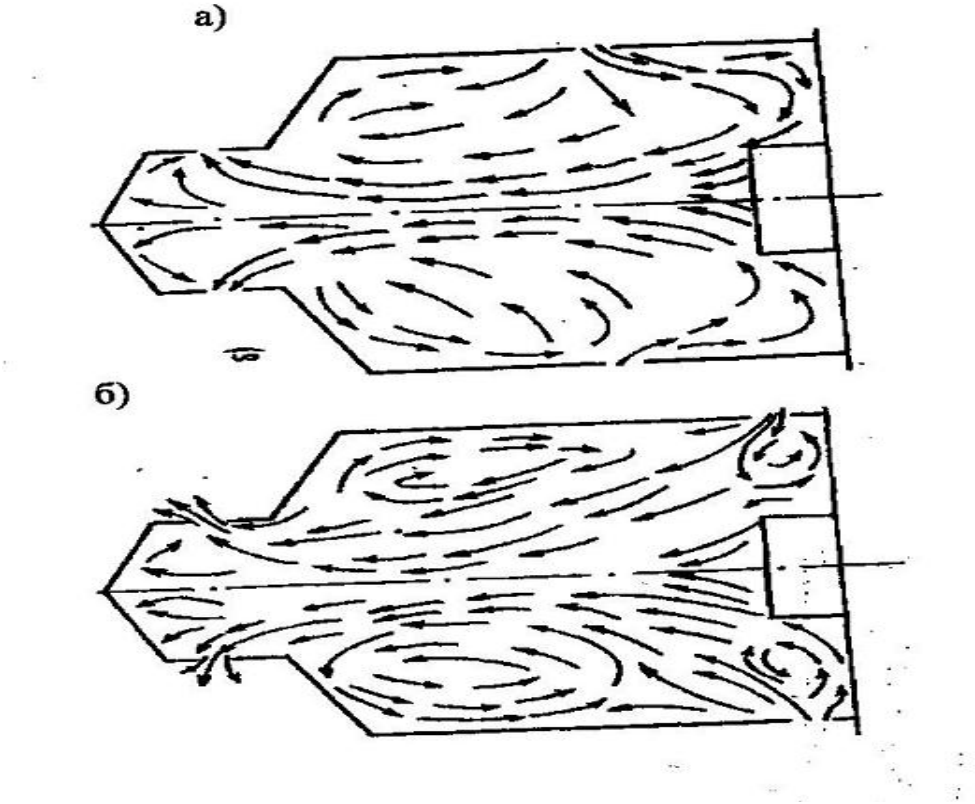
$$\Delta R = N(\gamma_m - \gamma_i)$$

bunda N— quyi havo kirish joyi bilan yuqoridagi havo chiqish joyi orasidagi balandlik, m; γ_m -.tashqaridagi havoning zichligi, kg/m^3; γ_i — ichkaridagi havoning zichligi, kg/m^3.

Bundan tashqari tabiiy havo almashishi shamol ta`sirida ham bo`lishi mumkin. Agar binoga shamol urilayotgan tamondagi bosim shamol hisobiga bir muncha ijobiy bo`lsa, shamol urmayotgan tomonda bosim salbiy yo`nalishda bo`ladi va buni quyidagicha ifodalash mumkin:

$$R = R_1 – R_2$$

bunda R_1 - shamol urilayotgan tomondagi bosim; R_2 - shamol urilmayotgan tomondagi bosim.



3.4.1- rasm. Tabiiy shamollatish harakatining ko`rinishi:

a) havo iliq bo`lgan vaqtda;

b) havo sovuq bo`lgan vaqtlarda.

Agar binoga har ikkala bosim kuchi tabiiy shamollatish vazifasini bajarayapti deb hisoblasak:

$$\Delta R = (\gamma_m - \gamma_i)\, N + (R_1 - R_2)$$

Ortiqcha bosim miqdorini aniqlagandan keyin chiqarib yuborilayotgan havo miqdorini ham aniqlash mumkin:

$$Q = \mu f \sqrt{\Delta R}$$

ko`rinishga ega bo`ladi.

Agar chiqarib yuborilayotgan havo miqdorini kirib kelayotgan havo miqdoriga teng desak, unda biz kirib kelayotgan va chiqib ketayotgan havo harakat tezligini topishimiz mumkin:

$$V = Q / F$$

Bu erda F -havo chiqib ketayotgan tirqish kesim yuzasi.

XULOSA

Zamonaviy axborot kommunikatsiya texnologiyalarining, ayniqsa internetning keng joriy qilinishi insoniyatga ko`plab imkoniyatlarni tuhfa qilmoqda. Ma`lumotlarga qaraganda ayni kunda dunyo bo`yicha internet xizmatidan muntazam foydalanuvchilar soni 300 milliondan oshib ketdi. e`tiborlisi shuki bu ko`rsatkich soniyalar ichida o`zgarib boryapti. Har ikki-uch daqiqada bir kishi ro`yxatdan o`tayotgani fikrimiz dalilidir. Yana bir hayratlinarli raqam, bir kunda 7 milliondan ortiq veb-sahifalar yaratilyapti. Internetning bu qadar ommalashuviga uning axborotni tez va arzon narxda etkazib berishi asosiy sabab bo`lmoqda. Pochta xizmati bilan taqqoslaganda ‘o`rgimchak to`ri’ning xizmati 720 barobar tez va 355 barobar arzondir.

Internetda axborotlarni matnli, audio, video, grafik ob`ektlar, baza ma`lumotlari, dasturlar va boshqa ko`rinishda kuzatish mumkin. Mazkur xizmatga ulangan har qanday kishi istalgan vaqtda-kechasimi yo kunduzi, bir turdagi materiallar bilan bir necha marta tanishishi, tarmoqqa ma`lumotlar joylashtirishi, ularni ko`paytirishi mumkin.

Afsuski, zamonaviy axborot kommunikatsiya texnologiyalarining keng joriy qilinishi insoniyatga ko`plab imkoniyatlarni tuhfa etish barobarida, jamiyatga bir qator muammolar, xususan, kompyuter jinoyatchiligi va kiberterrorizm xavfini ham paydo qilmoqda. So`nggi kunlarda ommaviy axborot vositalarida kiberjinoyatchilik, kiberterrorizm singari yangi atamalarning tez – tez tilga olinayotgani bu borada insoniyat oldida jiddiy xavf paydo bo`layotganini anglatadi. Bu kabi jinoyatlar, eng avvalo kompyuterlar, kompyuter tarmoqlari va tizimlari ishiga noqonuniy aralashuv orqali ma`lumotlarni o`g’irlash, o`zlashtirish, o`zgartirish kabi harakatlarda namoyon bo`lmoqda. Shu sababli axborot xavfsizligini ta`minlashga e`tiborsizlik bilan qarashga haqqimiz yo`q. Axborot xavfsizligini ta`minlash kechiktirib bo`lmaydigan va barcha bilishi hamda o`rganishi bo`lgan muammo hisoblanadi. Bu muammoni echish uchun qadim davrlardan boshlab insonlar turli xil usul va uslublardan foydalanishgan. Ushbu usul va uslublarni o`rganishgan, ularni takomillashtirishgan hamda yangilarini yaratishgan. O`z vaqtida unumli qo`llanilgan usul va uslublarni unutmasligimiz hamda ularni o`rganish orqali yangilarini yaratishimizni davr taqoza qiladi.

Axborot xavfsizligini ta`minlashning usullaridan biri kriptografiyadir. Shu sababli, yuqorida keltirilgan fikrga tayangan holda ushbu bitiruv malakaviy ishi, ‘Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturini yaratish’ mavzusi bo`yicha biz axborot, axborotning jamiyatdagi o`rni, hozirgi axborot kommunikatsiya texnologiyalari davrida elektron axborotlar, axborotlashgan jamiyatda elektron hujjatlar hamda ularning harakati va ular xavfsizligini ta`minlash haqida fikrlarimizni keltirib o`tdik.

Biz ushbu bitiruv malakaviy ishida ‘Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash dasturini yaratish’ mavzusi bo`yicha axborot asrida eng muhim masalalar hisoblangan ‘Axborotlashgan jamiyatda elektron hujjatlar’ ga tavsif bergach ‘Axborot xavfsizligi va axborot urushlari’, ‘Axborotlar xavfsizligi tushunchalari va himoya tizimlari’ hamda ‘Kriptografiya – maxfiy xabarning ma`nosini yashirish’ masalalariga to`xtalib o`tdik. Keyin esa kriptografiya haqida qisqacha ma`lumot berilgandan so`ng bevosita Affin tizimidagi Tsezar usulida matnlarni shifrlash va deshifrlash haqidagi tavsiflarimizni keltirdik hamda mutanosib dasturlarni tuzdik. Dastur Paskal tilida yaratildi.

FOYDALANILGAN ADABIYOTLAR

1. I.Karimov O`zbekiston XXI – asr bo`sag'asida: xavfsizlikka tahdid, barqarorlik shartlari va taraqiyot kafolatlari. Toshkent. 1997 y.
2. Брюс Шнайер. Секреты и ложь. Безопасность данных в цифровом мире. Триумф-2002.
3. Майкл Ховард, Девид Лебланк. Защищенный код. Москва 2004.
4. Д. Скляров. Искусство, защиты и взлома информации. Санкт-Петербург. БХВ-Петербург. 2004.
5. Роберт Чёрчхаус. Коды и шифры. Москва 2006.
6. В. В. Ященко. Введения в криптография. Москва 2006.
7. Ж. Брассар. Современная криптология. Москва 2006.
8. В. Громов, Г.А. Васильев Энциклопедия компютерной безопасносты. Москва 2007.
9. Баричев С., Гончаров В.В., Серов Р.Е. Основы современной криптологии. Москва. Горячая линия. Телесом 2001 г/
10. Ғаниев С.К., Каримов М.М. Ҳисоблаш тизимлари ва тармоқларида информация ҳимояси: Олий ўқув юрт. талаб. учун ўқув қўлланма. - Тошкент давлат техника университети, 2003. 77б.
11. Шеннон К. Работы по теории информации и кибернетики / Пер. с англ. – М.: Иностранная литература, 1963. – 829с.
12. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии.–М.: Гелиус АРВ, 2001.– 480 с.
13. Бабаш А. В., Шанкин Г. П. История криптографии. Часть 1. М., «Гелиос», 2002.
14. Завгородний В.И. Комплексная защита информации в компютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
15. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
16. Фролов Г. Тайны тайнописи. М., 1992.
17. Жельников В.А. Криптография от папируса до компьютера. М., BF, 1997.
18. Масленников А. Практическая криптография BHV – СПб 2003й.

19. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.

20. A. Ismoilov, Q. Usmonov. Hayot faoliyati xavfsizligi. O`quv qo`llanma. Samarqand – 2010

21. O.Qudratov, T. G'aniev. Hayotiy faoliyat xavfsizligi. Toshkent, 2004 y.

22. X.Rahimova va boshqalar. Mehnatni muhofaza qilish. Toshkent, 2004 y.

23. M.A.Qudratov va boshqalar. Hayotiy faoliyat xavfsizligi (ma'ruza kursi). Toshkent, 2005y.

24. ftp://ftp.kiae.su/msdos/crypto/pgp

25. http://drago.centerline.com:8080/franl/pgp/…

26. Yahoo - Computers, Security-and-Encryption

27. http://gov.uz

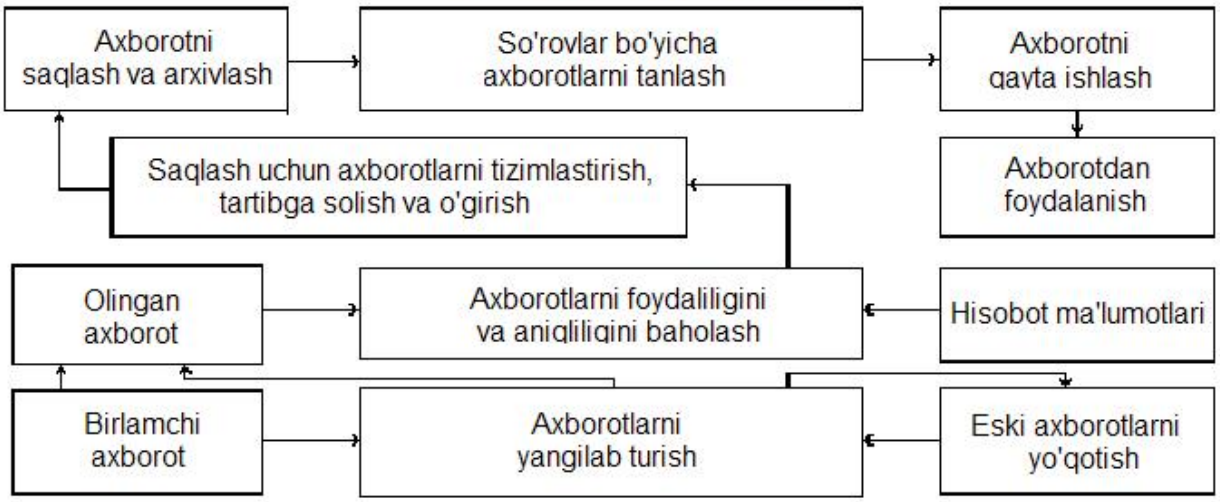
ILOVA

1-ilova.

MA`RUZANING O`QUV-VIZUAL MATERIALLARI

Axborotni ishlab chiqaradilar, saqlaydilar, uzatadilar, sotadilar va sotib oladilar. Bulardan tashqari uni o`g'irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shuning uchun axborotni himoyalash extiyoji yanada kuchaydi.

Axborotlarning hayotiy davri



Axborot xavfsizligi deb ma`lumotlarni yo`qotish va o`zgartirishga yo`naltirilgan tabiiy yoki sun`iy xossali tasodifiy va qasddan ta`sirlardan har qanday tashuvchilarda axborotning himoyalanganligiga aytiladi.

Axborotning himoyasi deb boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta`minlovchi va tashkilot axborot axborot zahiralarining yaxlitliligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta`minlovchi qat`iy reglamentlangan dinamik texnologik jarayonga aytiladi.

Axborotning zaif tomonlarini kamaytiruvchi va axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo`qolishiga to`sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi – axborotni himoyalash tizimi deyiladi.

Kriptografiya deganda har qanday shakldagi, ya`ni diskda saqlanadigan sonlar ko`rinishida yoki kompyuter tarmoqlarida uzatiladigan xabarlar ko`rinishidagi axborotni yashirish tushuniladi.

Kriptografiya - axborotlarni aslidan o`zgartirilgan holatga etkazishlarning matematik uslublarini topish va takomillashtirish bilan shug'ullanadi.

Kriptografiya ikkita asosiy muammolarni hal qilishga yo`naltirilgan: maxfiylik; yaxlitlilik. Maxfiylik orqali yovuz niyatli shaxslardan axborotni yashirish tushunilsa, yaxlitlilik esa yovuz niyatli shaxslar tomonidan axborotni o`zgartira olmaslik haqida dalolat beradi.

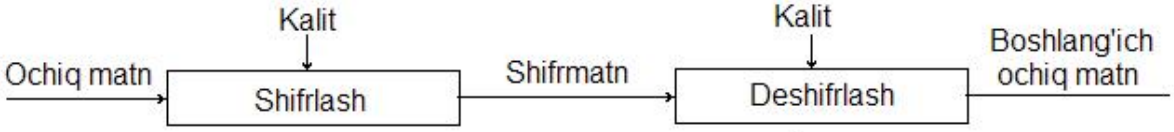
Kriptografik o`zgartirishning shifrlash turi o`z ichiga boshlang'ich matn belgilarini anglab olish mumkin bo`lmagan shaklga o`zgartirishni amalga oshiruvchi algoritmlarni qamrab oladi. Bu erda himoyalash ob`ekti sifatida faqat kalit xizmat qiladi. Uni tez-tez almashtirish mumkin.

Kriptografiya nuqtai - nazarida shifr — bu kalit demakdir va u ochiq ma`lumotlar to`plamini yopiq (shifrlangan) ma`lumotlarga o`zgartirish algoritmlari majmuasi hisoblanadi.

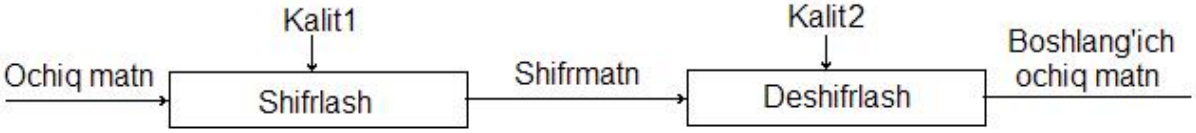
Kriptografik tizim yoki kriptotizim – ochiq matnni shifrlash (deshifrlash) jarayonini tashkil etuvchi amallar majmui bo`lib, u alfavitlar belgilarini almashtirishlar ketma-ketligidan iborat.

Hozirgi kunda kriptotizimlarni ikki sinfga ajratish mumkin:
- simmetriyali bir kalitlilik (maxfiy kalitli);
- asimmetriyali ikki kalitlilik (ochiq kalitli).

Simmetriyali (bir kalitlilik - kalit maxfiy) tizimlar quyidagi sxema asosida ishlaydi.



Asimmetriyali (ikki kalitlilik - kalit1 maxfiy, kalit2 esa ochiq) tizimlar quyidagi sxema asosida ishlaydi.



O`rin almashtirish shifrlarida shifrlanadigan matn ramzlari shu matn qismi chegarasida aniq qoida asosida almashtiriladi. O`rin almashtirish shifrlari eng sodda hisoblanadi va eng qadimiy shifrlardir.

Eramizdan oldingi 50 yillarda, rimlik imperator Gay Yuliy Tsezarning ish yuritish yozishmalarida biror ma`lumotni maxfiy holda biror kishiga etkazmoqchi bo`lsa, alfavitning birinchi harfini alfavitning to`rtinchi harfi bilan, ikkinchisi beshinchisi bilan va hokazo shu tartibda almashtirib matnning asli holatidan shifrlangan matn holatiga o`tkazgan.

Affin kriptotizimi Tsezar usulining takomillashtirilgan varianti hisoblanadi. Affin tizimidagi Tsezar usulida har bir harfga almashtiriluvchi harflar maxsus formula bo`yicha aniqlanadi.

Bu formula:

at+b (modm)

bu erda a, b - o`zaro bog’liq holda keluvchi butun sonlar, 0≤a, b<m va EKUB (a, m)=1. t – harfning alfavitdagi tartib raqami. Tartib 0 dan boshlanadi.

Affin kriptotizimi ikkita a va b sonlarga bog’liq. 0<=a,b<=n-1. n - alfavitdagi harflar soni.

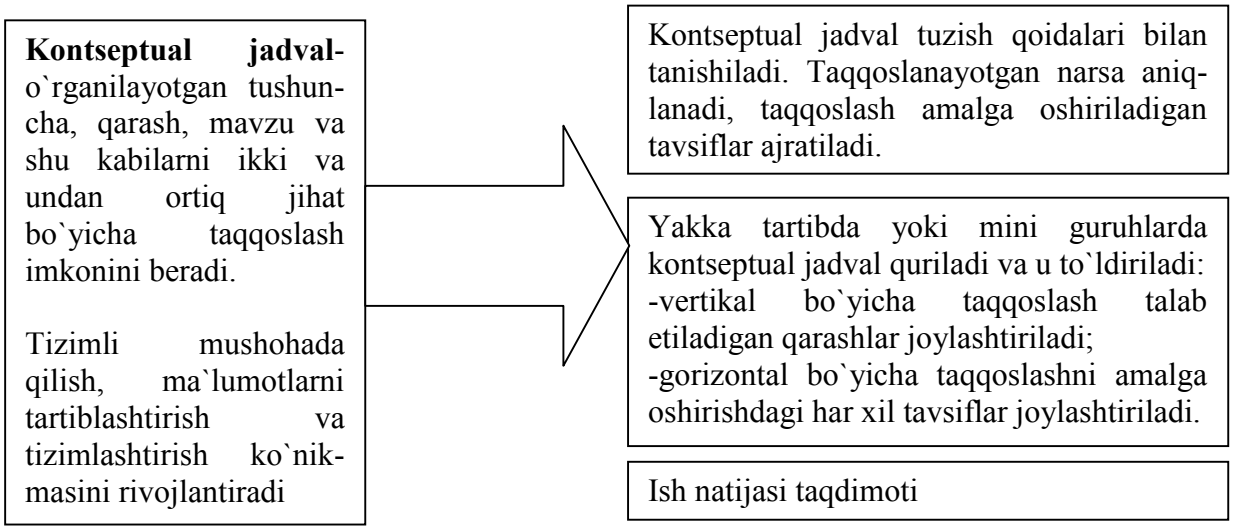
Shifrlash uchun:

$$Aa,b(j)=(a*j+b)(\text{mod } n)$$

Deshifrlash uchun:

$$A\text{-}1a,b(j)=(j-b)*a\text{-}1(\text{mod } n)$$

2-ilova.



3-ilova

Me`yoriy shakllar kontseptual jadvalni to`ldiring

Me`yoriy shakllar	**XARAKTERISTIKALARI**			
	Tarkibiga me`yoriy shakllarni oladi	Vazifasi	Kaysi me`yoriy shakldan keyin tuziladi	Nimalardan tuzilganligi

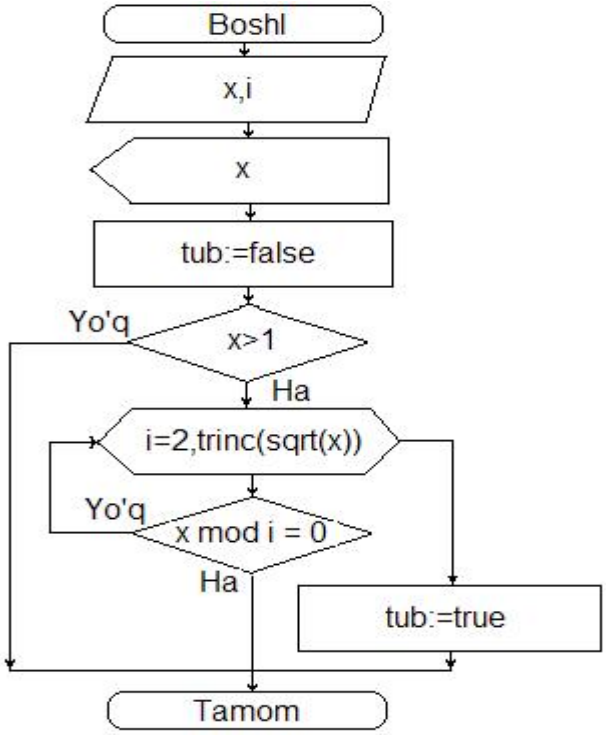
4-ilova.

Nazorat savollari

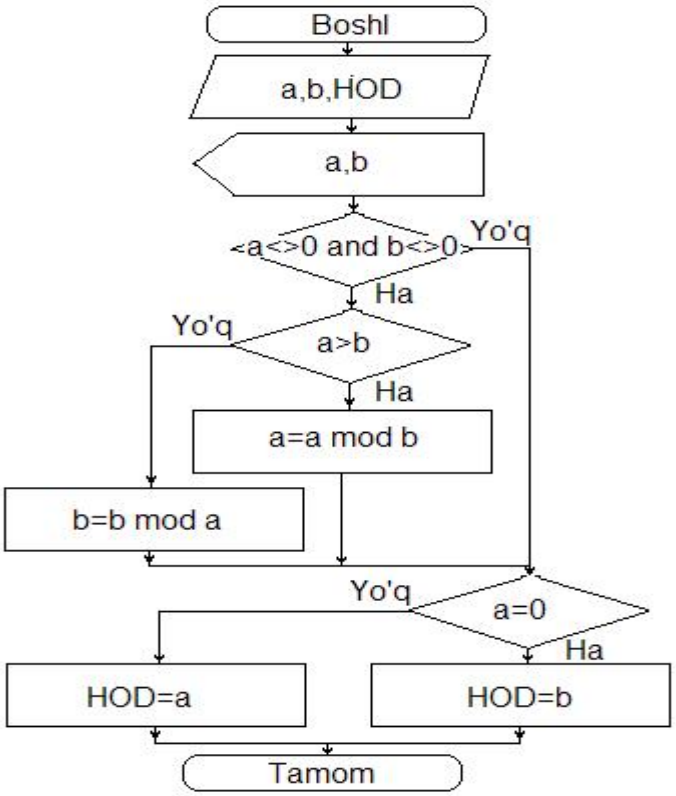
1. Nima uchun axborot himoyalanadi?
2. Axborotning hayotiylik davrini tavsiflang.
3. Axborot xavfsizligi deganda nimani tushunasiz?
4. Axborotning himoyasi deganda nimani tushunasiz?
5. Axborotni himoyalash tizimi nima?
6. Kriptografiya deganda nimani tushunasiz?
7. Kriptografiya qaysi muammolarni hal qiladi.
8. Kriptografik o`zgartirishni tavsiflang.
9. Shifr nima?
10. Kriptografik tizim yoki kriptotizim nima?
11. Kriptotizimlarni necha sinfga ajratish mumkin?
12. Simmetriyali tizimlarni ishlash sxemasini tavsiflang.
13. Simmetriyali tizimlarni ishlash sxemasini tavsiflang.
14. O`rin almashtirish shifrlari haqida tushuncha bering.
15. Tsezar usuli haqida tushuncha bering.
16. Affin kriptotizimini tavsiflang.

5-ilova.

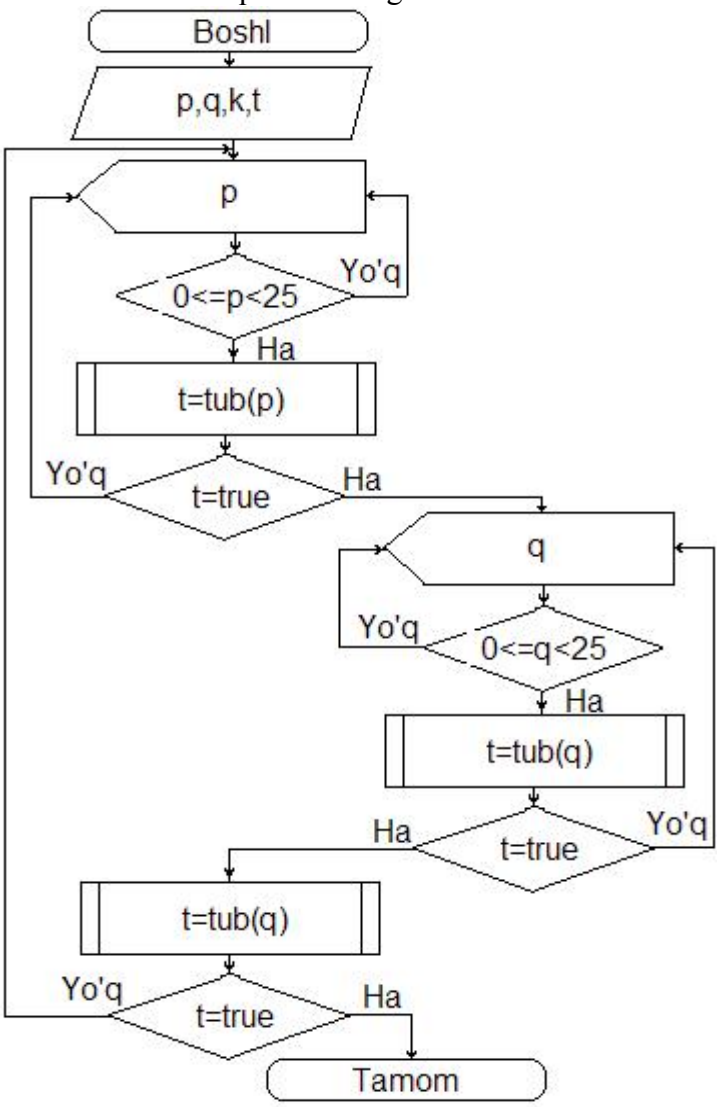
1. Sonning tub ekanligini aniqlash algoritmi:



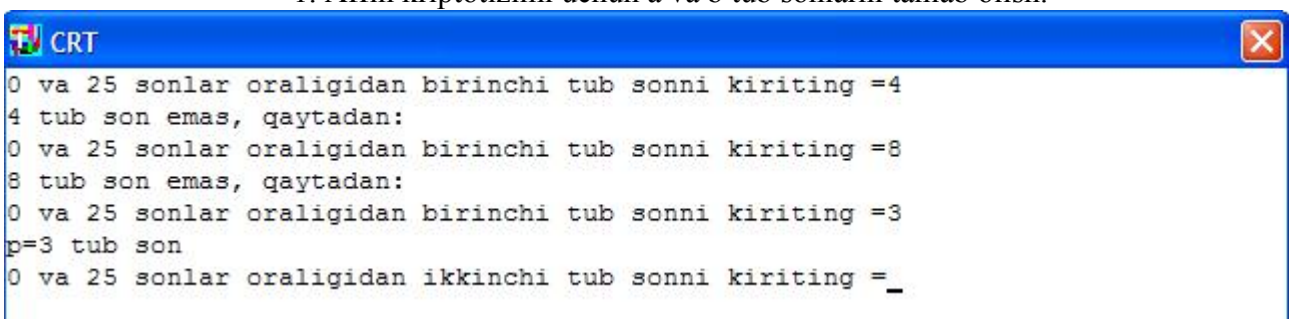
2. Sonlar eng katta bo`luvchisi 1 ekanligini aniqlash algoritmi:

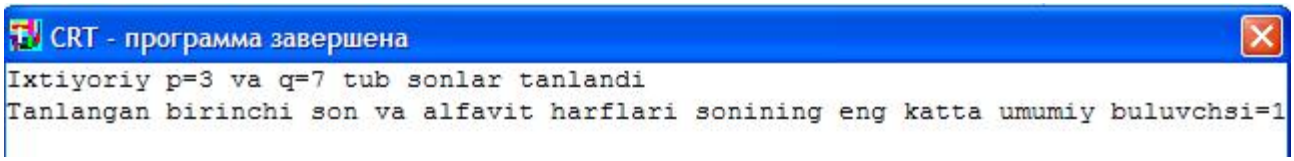


Kalit sonlarni, ya`ni a va b sonlarni aniqlab olish algoritmi:

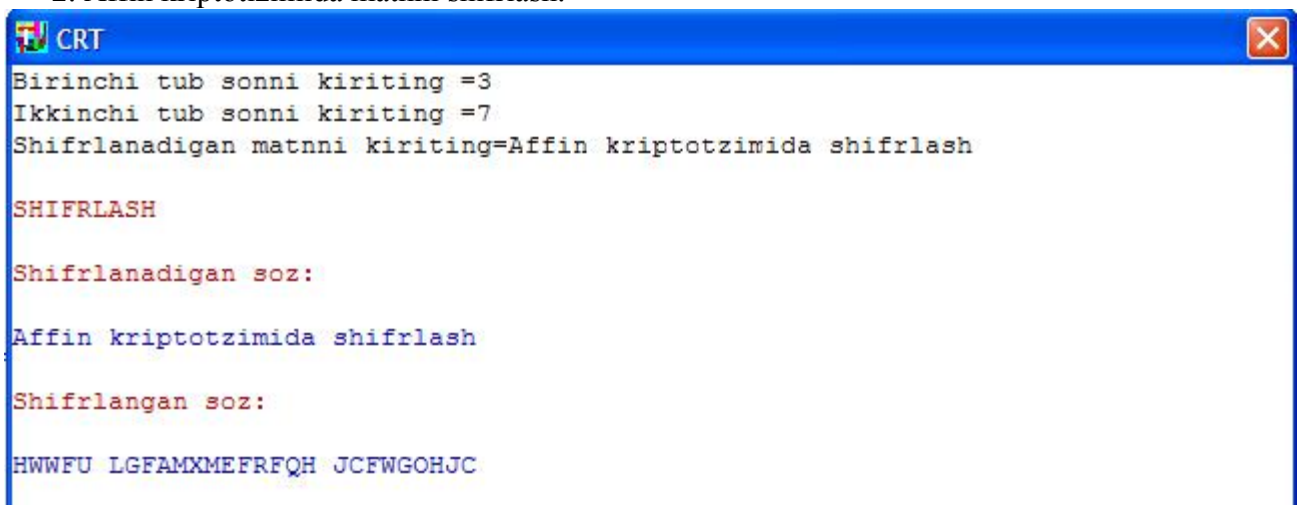


1. Affin kriptotizimi uchun a va b tub sonlarni tanlab olish.





2. Affin kriptotizimida matnni shifrlash.



3. Affin kriptotizimida shifrmatnni deshifrlash.