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

TOSHKENT MOLIYA INSTITUTI

O.T. KENJABOYEV, A.SH. ALLANAZAROV

AXBOROT TIZIMI XAVFSIZLIGI

O‘quv qo‘llanma

Toshkent
«IQTISOD-MOLIYA»
2013

UO'K 004.056(075)
KBK 32.973-018.2
K-33

Дастурлаш тамойиллари

Taqrizchilar:
TDIU «Axborot texnologiyalari» kafedrasi dotsenti **O.Azamatov;**
TMI «Informatsion-kommunikatsion-texnologiyalar» kafedrasi professori **Z.Sh.Afzalov**

Kenjaboyev O.T.

Axborot tizimlari xavfsizligi: o'quv qo'llanma. O.T. Kenjaboyev, A.Sh. Allanazarov. O'zbekiston Respublikasi Oliy va o'rta maxsus ta'lim vazirligi; Toshkent Moliya instituti. –T.: «MOLIYA-IQTISOD», 2013. 100 bet.

Ushbu qo'llanma tadqiqotchilar va ushbu sohada ta'lim oluvchilar uchun zarur manba bo'lib xizmat qildi. Mualliflar uni yaratishda nazariy va amaliy ma'lumotlar olish imkonini bergan ilmiy manbalarlarning mualliflariga. xususan, birinchi va ikkinchi boblarni yoritishdagi qimmatli maslahatlari bilan yaqindan yordam berganliklari uchun G.O.Ernazarovaga o'zlarining minnatdorchiligini izhor etadilar.

UO'K 004.056(075)
KBK 32.973-018.2

ISBN 978-9943-13-412-6

KIRISH

Jamiyatning axborotlashtirish hozirgi zamonning davr talabiga aylanib bormoqda. Inson faoliyatining barcha jabhalari axborotni qabul qilish va o'zlashtirish jarayonlari bilan chambarchas bog'liqdir. Rivojlanishning zamonaviy bosqichida axborot texnologiyalari jamiyatni mo'tadil taraqqiy etishga bevosita ta'sir etuvchi ilmiy-texnikaviy taraqqiyotining ustuvor yo'nalishlaridan hisoblanadi.

O'zbekistonning XXI asrga qadam qo'yishi axborot va telekommunikatsiya texnologiyalari sohasidagi inqilobiy o'zgarishlar bilan kuzatiladi. Shu sharoitda respublikamiz oldida xalqaro maydonga integratsiyalashuv va jamiyatning turli sohalariga zamonaviy axborot texnologiyalarini joriy etish masalalari turadi. Shu sababdan ham hukumatimiz axborot telekommunikatsiya texnologiyalarini keng joriy etish va omma o'rtasida undan samarali foydalanishi borasidagi strategik maqsadlarni ko'zlagan holda tegishli choralarni ko'rishga alohida e'tibor qaratmoqda. Xususan, milliy axborot telekommunikatsiya tizimini shakllantirish borasida qator qonun va hujjatlar: «Aloqa to'g'risida», «Axborotlashtirish to'g'risida», «Elektron raqamli imzo to'g'risida», «Elektron hujjat almashinuvi to'g'risida», «Ommaviy axborot vositalari to'g'risida» kabi qabul qilingan qonunlarda mamlakatda axborot xavfsizligini ta'milashning maqsad va vazifalari o'z ifodasini topgan. Mazkur yaratilgan qonunchilik bazasi mamlakatimizda axborot texnologiyalari industriyasining rivojlanshiga asos yaratmoqda.

1-bob. AXBOROT XAVFSIZLIGI VA UNI TA'MINLASH USLUBIYOTI

1.1. Axborotlar xavfsizligini ta'minlashning eng oddiy usuli

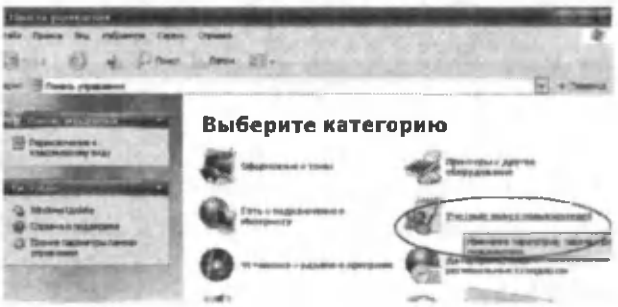
Axborot texnologiyalarining keng tarqalganligi va axborotga kirish imkoniyatining mavjudligi xavf soluvchi ta'sirlarga ko'proq mubtalo bo'ladi. Amaliyotda bunday holatlarga ko'plab misollar keltirsa bo'ladi. Masalan, axborot tizimlari taraqqiy etgan AQShda har 20 soniyada dasturiy tizimlardan foydalanish orqali sodir etiladigan ko'plab jinoyatlar kuzatiladi. Kompyuter tarmoqlarini buzish va bu yo'nalishdagi nojo'ya xatti-harakatlari oqibatida ko'riladigan zararlar miqdori yiliga 100 mln AQSh dollardan ko'proq mablag'ni tashkil etmoqda. Hozirgi kunda xo'jalik subyektining raqobatbardoshlik darajasi ham ma'lum ma'noda maxfiy ma'lumotlarni saqlash, ularni o'zgarishi yoki yo'qolishi oldini ola bilishga bog'liq bo'lib qolgan. Bu, o'z navbatida, moliyaviy hamda iqtisodiyotning boshqa sektorlarida faoliyat yuritayotgan muassasalarning axborot bazalariga kirish, turli maxfiy ma'lumotlarni ko'chirish, o'g'irlash, elektron to'lov tizimlarini buzish hollarida o'z aksini topmoqda.

Hozirgi kunda mutaxassislar, ishlab chiqarish korxonalari yoki muassasalarning faoliyati ko'p jihatdan ularning qay darajada zaruriy ma'lumot va axborotlar bilan to'la ta'minlanganligiga hamda ushbu ma'lumotlardan qay darajada samarali foydalanganligiga bog'liq bo'lib qolmoqda. Ma'lumotlar to'plami shu qadar ko'payib ketadiki, ularni qayta ishlash va tahlil qilish maxsus texnik tizimlar yordamila amalga oshirib bo'lmay qoladi. Bundan tashqari, kundalik hayotda qabul qilish va qayta ishlash zarur bo'lgan axborotlar hajmi nihoyatda ortib borayotganligi sababli ba'zan ularni tahlil qilishga ulgurish qiyin.

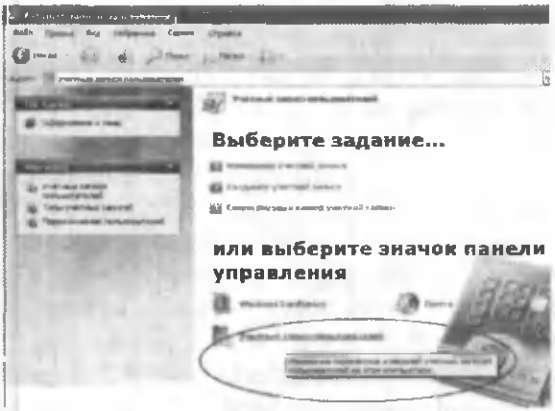
Ma'lumki, axborot hajmining o'zgarishi, ya'ni bu qadar ko'payib ketishi, oqimining tezlashib borishiga asosiy sabablardan biri informa-

tsion texnika va texnologiyalarning rivojlanishi-zamonaviy eng yangi texnologiyalarni qo'llash, ikkilamchi xomashyolardan oqilona foydalanish, energetik resurslarni tejamkorlik bilan ishlatish, inson mehnatini yengillashtirish hisobiga oshirish bosqichiga kirganligidir. Bu esa, o'z navbatida, jamiyatni yuqori darajada informatsiyalashgan bo'lishini talab etadi. Jamiyatning informatsiyalashuvi ijtimoiy taraqqiyotning asosiy qonunlaridan biri bo'lib hisoblanadi. Aynan shuning uchun inson faoliyatining barcha sohalariga intellektual mehnat quroli sifatida axborotlarni tezkorlik bilan yig'ish, qayta ishlash, jarayon va hodisalarni modellashtirish, ularni tahlil qilish imkonini beruvchi kompyuterlashtirilgan tizimlar va informatsion texnologiyalar kirib kelishini bildiradi. Tabiiyki, axborot texnologiyalari jamiyat informatsion resurslaridan oqilona foydalanishning eng muhim usullaridan biri bo'lib qolmoqda. Har qanday korxona va tashkilotda zaruriy va maxfiy axborotlar asosan elektron shaklda kompyuter xotirasida saqlanadi. Mana shunday maxsus va kerakli axbotorlarni xavfsizligini ta'minlashning birinchi usuli sistemaga parol qo'yish va har bir foydalanuvchi uchun maxsus joy va chegara o'rnatib qo'yish. Masalan: bitta kompyuterdagi ma'lumotlardan bitta bo'limdagi bir necha xodimlar ishlash, ma'lumot olish huquqiga ega bo'lsa, u holda usbu kompyuterdagi axborotlar xavfsizligini ta'minlash uchun, unda uskunalar paneli bandiga kirib foydalanuvchilarni hisobga olish bandi orqali boshqa foydalanuvchilar uchun joy ajratiladi. Gap shundaki bu yangi foydalanuvchi kompyuterdagi axborotlarni hammasini o'qiy olmaydi, ularga o'zgartirish kirita olmaydi, ya'ni axborotlarning yaxlitligi va maxfiyligi saqlanadi. Quyida ushbu vazifa amaliy jihatdan qanday amalga oshirilishini ko'rib chiqamiz:

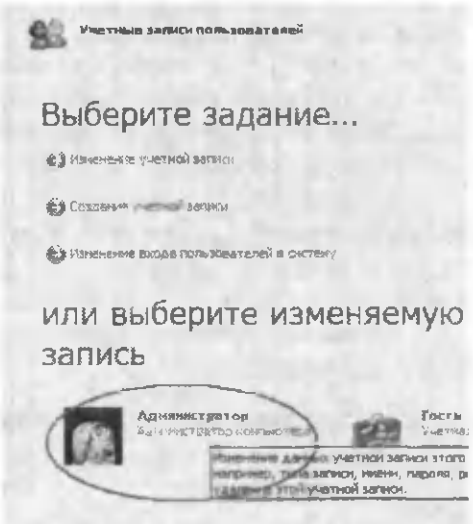
Adminstrator uchun «Панель управления» bandi orqali parol o'rnatish mumkin. Buning uchun «Панель управления» bandi faollashtiriladi va ekranda quyidagi oyna hosil bo'ladi.



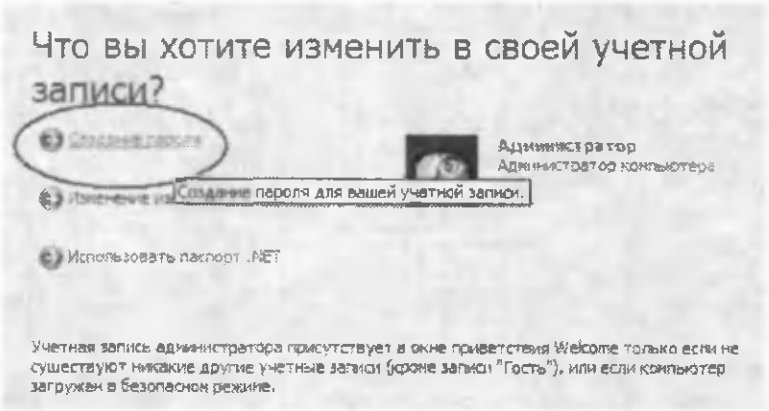
«Учетные записи пользователей» tanlanganda, ekranda shu nomdagi oyna hosil bo'ladi:



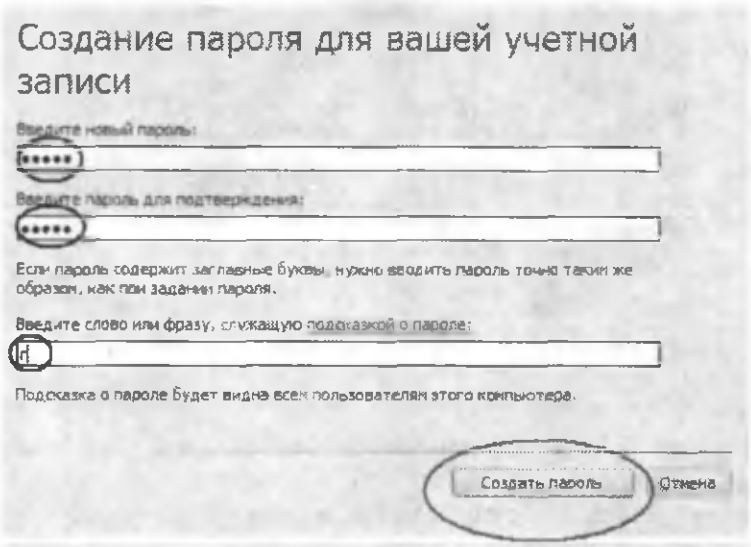
«Учетные записи пользователей» bandini faollashtiramiz. Ekranda quyidagi oyna hosil bo'ladi:



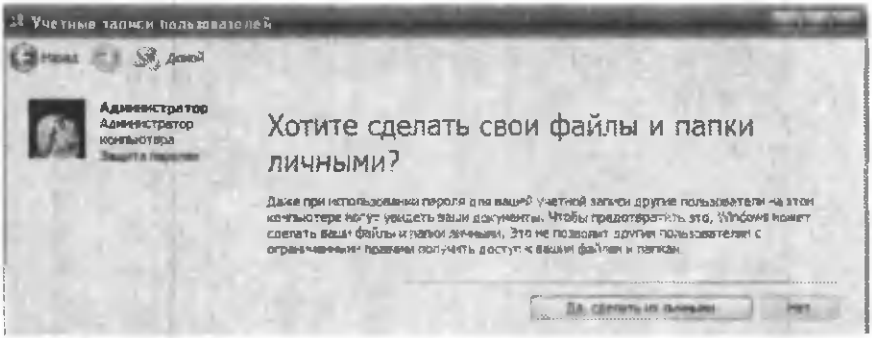
Oynada topshiriqlardan keraklisini tanlaymiz. Ekranda yangi so'rov oynasi hosil bo'ladi. U yerda hisobga olish yozuvini o'zgartirish haqidagi so'rovning javob bandlari keltirilgan bo'lib, ulardan «Создание пароля» bandini tanlab ENTER tugmasi bosilganda, ekranda parol o'rnatish oynasi hosil bo'ladi.



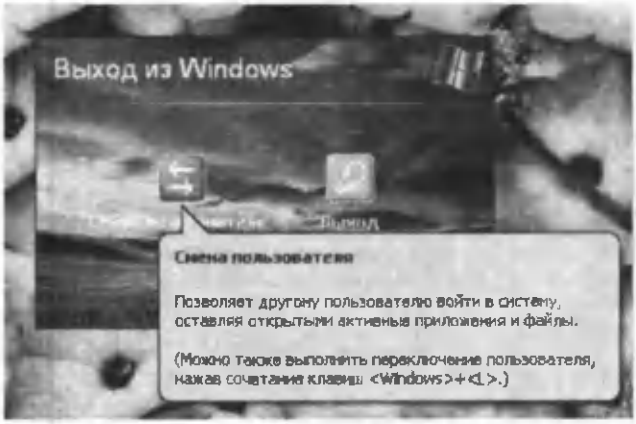
Ushbu oynaning yangi parol kiritish bandiga parol yoziladi. U harflar, sonlar yoki belgilardan iborat bo'lishi mumkin. Ikkinchi parolni tasdiqlash darchasida ham parolning nomi qayta takror yoziladi. Uchinchi parol yoddan chiqib qolgan holda yordamchi so'z vazifasini beruvchi darchaga esa, parolning nomiga yaqin harf, son yoki belgi qo'yish mumkin. Shundan so'ng «Создать пароль» bandi faollashtiriladi.



Ekranda yana yangi oyna ochiladi, unda «Fayl va papkalarni shaxsiylashtirish» to'g'risida so'rov bo'lib, agar oynada yozilgan takliflar sizga ma'qul bo'lsa, «Да», aks holda «Нет» tugmasi bosiladi.

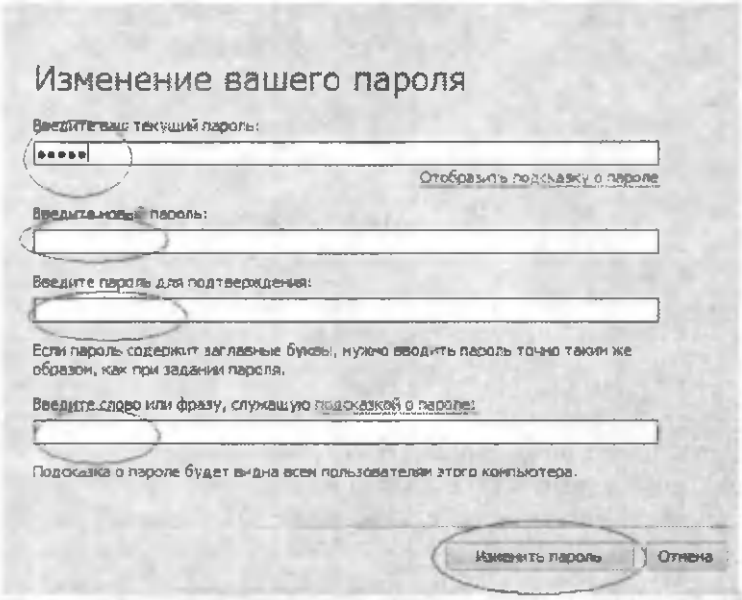


Oynadagi «Да, сделать их личными» tugmasini bosamiz va barcha ochilgan oynalarni yopib chiqamiz. Bu bilan administrator – ya'ni kompyuterdan foydalanuvchi asosiy mas`ul shaxsga parol o'rnatildi. Kompyuterni ishga tushirgan vaqtda foydalanuvchi darchasida «Administrator»ning ushbu ornatilgan yangi paroli parol darchasiga yozilsa kompyuter ishga tushadi, aks holda, uni ochish mushkul. Bu bilan kompyuterga begona shaxslar o'tirgan yoki ma'lumotlarni olishga harakat bo'lgan holda ham uni parolsiz ocha olmaydi.

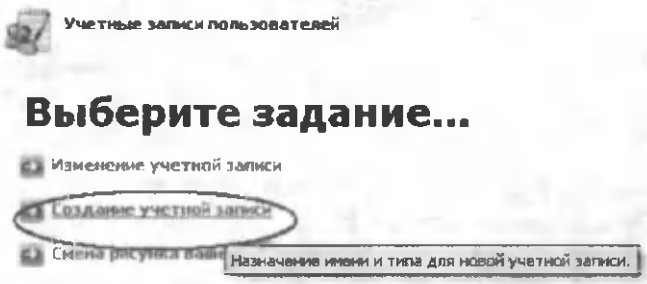


Bu parolni faqat «Administrator» biladi va u shu parol bilan kompyuter ma'lumotlari va dasturlariga kirishi mumkin. Agar parolni yangilamoqchi yoki bekor qilmoqchi bo'lsa, u holda uskunalar paneli bandiga kirib yuqoridagi operatsiyalar ketma-ketligi bajarilishi lozim. Parolni bekor qilish uchun parolni o'zgartirish bandiga kirib avvalgi, ya'ni bekor qilmoqchi bolgan parol nomi kiritiladi. Shunda yangi parol darchalari ochiladi. Ular ochiq qoldirilib, «Изменить пароль» bandi faollshtiriladi.

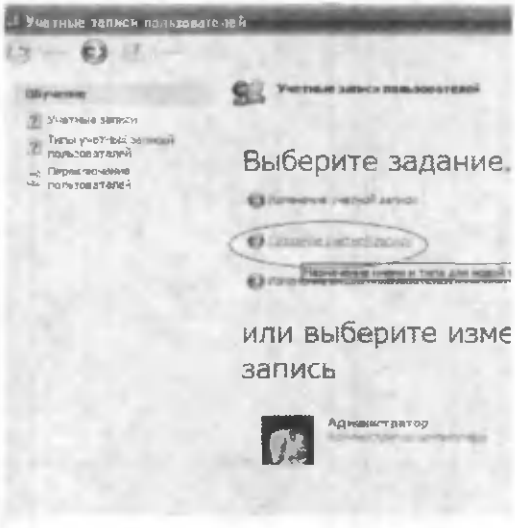
Lekin kompyuterdagi muhim va maxfiy ma'lumotlardan administratordan boshqa foydalanmasligini ta'minlash uchun yangi foydalanuvchiga alohida joy ajratib qo'yish yaxshi samara beradi.



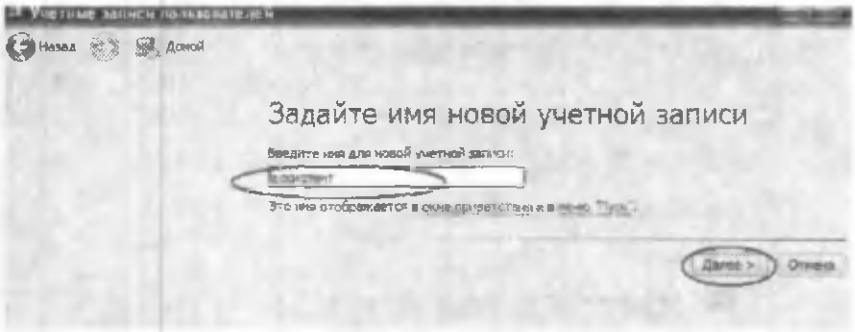
Buning uchun «пуск-панель управления» – ketma-ketligida «Учетные записи пользователей» bandi faollashtiriladi. Ekranda maxsus «Учетные записи пользователей» oynasi hosil bo'ladi, undan «Создание учетной записи» bandi faollshtiriladi.



Ekranda navbatdagi foydalanuvchilami hisobga olish oynasi hosil bo'ladi. Ushbu oynada topshiriqlar qatoridan «Создание учетной записи» bandini tanlaymiz.

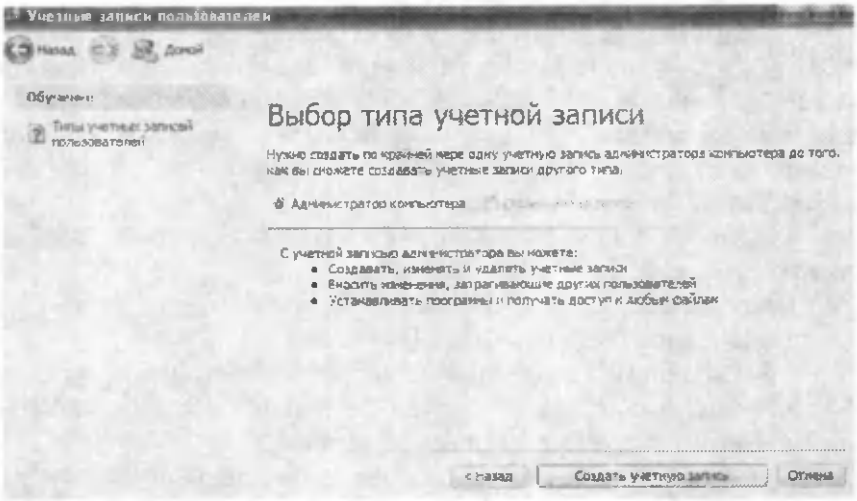


Ekranda hosil bo'lgan navbatdagi oynada yangi foydalanuvchining nomini kiritish so'ralgan bo'lib, yangi hisobga olish nomini kiritish darchasiga yangi foydalanuvchi nomi kiritiladi (M: assistent) va «Далее» tugmasi bosiladi.



Ekranda hisobga olish turini tanlash uchun oyna hosil bo'ladi. U yerdan «Ограниченная запись» bandi faollshtirilib, «Создать учетую запись» tugmasi bosiladi.

Yangi foydalanuvchiga kompyuterdagi ma`lumotlarni muhimlik darajasiga ko'ra kerakli fayllarga kirish, o'zgartirish yoki qo'shimcha kiritish kabilar ta`qiqlab qo'yiladi, ya`ni ularga «Доступ» – ruxsat berilmaydi va faoliyat chegaralab qo'yiladi.



Bu bilan axborotlarni ishonchli qo'llarda uzoq vaqt sifatli saqlashga erishish mumkin. Axborotlarni himoyalash va ishonchli saqlash asosan moliya muassasalarida, xususan, bank tizimida juda muhimdir. Quyida shu masala haqida fikr yuritamiz.

1.2. Axborotlarni himoyalash tadbirlari

Moliya muassasalarida biznes sohasida deyarli barcha ishlar ma'lum miqdordagi axborotni qayta ishlash va jo'natish bilan bog'liqdir. Hozirda biznesga doir axborot bilan ishlash jarayonini avtomatlashtirmagan birorta bank bo'lmasa kerak. Internetdan foydalanadigan va masofada turib, o'z tizimlariga kirish imkonini beradigan banklar soni to'xtovsiz ko'payib bormoqda. Bank faoliyatining turli sohalari bilan bog'laydigan kompleks axborot tizimigina moliya muassasining biznes yuritish jarayonlarini batamom avtomatlashtirishga va ularni birlashtib, bir butun holga keltirishga qodir. Mijozlar bilan ishlash, foizlar yozish, xilma-xil bank xizmatlarini ko'rsatish bankning ichki xo'jalik faoliyati, buxgalteriyasi bilan bog'langan bo'lishi kerak. Axborot bir markazda qayta ishlanishini, asosiy moliyaviy operatsiyalar xilma-xil valutada olib borilishini va avtomatlashtirilishini ta'minlaydigan kompleks tizim bankning barcha filiallarini samarali boshqarish, nazorat qilish va ulardan kundalik faoliyat haqida hisobot olib turish imkonini beradi.

Bank industriyasining axborot xavfsizligini ta'minlash muammosi kompleks muammodir. Axborot xavfsizligiga qilinayotgan xarajatlar

g'arb mamlakatlarida 2003-yilda 20 foizni, 2007-yilda 37 foizni, 2012-yilda esa 45 foizni, Rossiyada 2003-yilda 2–3 foizni, 2007-yilda 4,2 foizni, 2012-yilda esa 15 foizni tashkil qildi. Bundan tashqaru xavfsizlik bilan bog'liq bo'lgan murakkab masalalarda, chunonchi axborotni muhofaza qilish, kompleks tizimlarni qo'llash masalalarida ko'pgina mutaxassislarning bilimi yetishmaydi.

Axbortlarni himoyalash tadbirlari va usullarini qo'llash quyidagi mustaqil yo'nalishlarni o'z ichiga oladi:

- axborotlarga ruxsatsiz kirishdan himoyalash;
- axborotlarni aloqa tizimlarida himoyalash;
- elektron hujjatlarning yuridik ahamiyatini himoyalash;
- maxfiy axborotlarni qo'shimcha elektron magnitli nurlanishlar va uzatish kanallaridan chiqib ketishdan himoyalash;
- axborotlarni kompyuter viruslari va dasturlarini tarqatish kanallari bo'yicha boshqa xavfli ta'sirlardan himoyalash;
- dastur va qimmatli kompyuter axborotlarini ruxsatsiz nusxa ko'chirish va tarqatilishidan himoyalash.

Har bir yo'nalish bo'yicha asosiy maqsad va vazifalar aniqlanadi.

Ruxsatsiz kirish ostida foydalanuvchilar va cheklanish avtomatlashtirilgan axborot tizimlarining boshqa subyektlarini tasodifan yoki qasddan harakati natijasida axborotlarni himoyalashning asosiy qismi bo'lgan kirishni cheklashning belgilangan kodlari buzilishi tushuniladi.

Axborotlarga ruxsatsiz kirishni amalga oshirgan subyektlar qoida buzuvchilar deb ataladi. Axborotlarni himoyalash nuqtayi nazaridan ruxsatsiz kirish quyidagi oqibatlarga olib kelishi mumkin:

- ishlab chiqilayotgan maxfiy axborotning chetga chiqib ketishi;
- avtomatlashtirilgan axborot tizimlarini ish qobiliyatini qasddan buzish natijasida uning buzilishi;
- muhim axborotlar yo'qotilishi va hokazo.

Quyidagilardan har biri tartib buzuvchi bo'lishi mumkin:

- avtomatlashtirilgan axborot tizimlaridan shtatli foydalanuvchilar;
- avtomatlashtirilgan axborot tizimlarining tizimili, umumiy va amaliy dasturlar bilan ta'minlanishini kuzatib boruvchi dasturlovchi xodimlar;
- xizmat ko'rsatuvchi xodimlar (muhandislar);
- avtomatlashtirilgan axborot tizimlariga ruxsatli kirishga ega boshqa xodimlar (shu jumladan, yordamchi ishchilar, farroshlar va h.k.)

Avtomatlashtirilgan axborot tizimlariga boshqa begona shaxslarning

(ko'rsatilgan kategoriyalarga kirmaydiganlarni) kirishi tashkiliy usulni tadbirlar asosida istesno qiladi.

Axborotlarga ruxsatsiz kirish kanali ostida shaxslar tomonidan bajarilayotgan texnologik tadbirlar harakatining izchilligi tushuniladi. Ular yoki ruxsatsiz bajariladi yoki xodimlarning xatolari yoki uskunalarning buzilishi natijasida noto'g'ri ishlab chiqiladi. Ruxsatsiz kirishning butun kanallarini aniqlashni loyihalashtirish axborotlarni saqlash, kuzatish va ishlab chiqish texnologiyalarini, axborotlarni himoyalash tizimini va tartib buzuvchisining tanlangan modelini tahlil qilish yo'li bilan o'tkaziladi.

Maxfiy va qimmatli axborotlarga ruxsatsiz kirish va ularni himoyalash eng muhim vazifalardandir. Kompyuter egalari va foydalanuvchilarning mulkiy huquqlarini himoyalash ishlab chiqarilayotgan axborotlarni gavdalanayotgan mulkni jiddiy iqtisodiy va boshqa moddiy va nomoddiy zararlar keltirishi mumkin bo'lgan turli kirishlar va o'g'irlashlardan himoyalashdir.

Nafaqat ehtimol bo'lgan tartib buzuvchini kompyuterda saqlanayotgan axborotlarni o'qish imkoniyatlarini, balki shtatli va shtatsiz vositalari bilan tartib buzuvchi imkoniyatini ham bartaraf etishga qaratilgan. Vazifaviy kafolatlarni va axborotlarga kirishni cheklash vazifasi axborotlarga ruxsatsiz kirishdan himoyalash muammosining asosiy mezoni hisoblanadi.

Axborotlarga ruxsatsiz kirishni himoyalash bo'yicha talablar himoyalanayotgan axborotlarning uchta asosiy xususiyatlariga erishishiga yo'naltirilgan:

1) **maxfiylik** (maxfiy axborotlarga faqat unga tegishli bo'lgan kishilar kirishi kerak);

2) **yaxlitlilik** (muhim qarorlar qabul qilishda foydalanayotgan axborotlar ishonchli va aniq bo'lishi va qasddan hamda g'araz maqsadlari bilan buzilish imkoniyatlaridan himoyalangan bo'lishi kerak);

3) **tayyorlilik** (axborotlar va tegishli axborot xizmatlari ularga zarurat tug'ilgan paytda, hamma vaqt xizmat ko'rsatishga tayyor bo'lishlari kerak) ma'lumotlarga kirishning nazorati ostida avtomatlashtirilgan axborot tizimlaridan foydalanuvchilar va tizim tomonidan ishlab chiqiliyotgan axborotlar o'rtasida kirishga cheklash tizimi bo'lishi kerak.

Bank axborotlariga kirishni cheklashning har qanday tizimini muvaffaqiyatli faoliyat yuritishi uchun ikkita vazifani yechish zarur:

1. Tanlangan model doirasida bo'lgan harakatlar bilan axborotlarga kirishni cheklash tizimini chetlab o'tishni mumkin bo'lmaydigan qilish;

2. Ma'lumotlarga kirishni amalga oshirayotgan foydavlanuvchining identifikatsiyasini belgilash, kafolatlash.

Ro'yxatga olish avtomatlashtirilgan axborot tizimlarining (AAT) xavfsizligini samarali ta'minlash usullaridan biri bo'ladi. Ro'yxatga olish qayd daftari asosida javobgar bo'lganni ro'yxatga va hisobga olish tizimi qo'llanilib, uning asosida o'tmishda nima sodir bo'lganligini kuzatishga va shunga ko'ra axborotlarni chiqib ketish kanalini bilishga imkon beradi. Ro'yxatga olish qayd daftarida ma'lumotlar va dasturlarga kirishning barcha amalga oshirilgan va amalga oshirilmagan harakatlar qayd etiladi. Ro'yxatga olish daftarining mazmuni davriy va uzluksiz tahlil qilinishi mumkin.

Ro'yxatga olish qayd daftarida bank avtomatlashtirilgan axborot tizimlarining foydalanuvchilari tomonidan amalga oshirilayotgan barcha nazorat qilinayotgan so'rovlarining ro'yxati olib boriladi.

Ro'yxatga va hisobga olish tizimi quyidagilarni amalga oshiradi:

1. Kirish subyektlarini tizimga (tizimdan) kirishi (chiqish)ni ro'yxatga olishni yoki operatsion tizimni ish bilan to'la ta'minlash va initsiallashtirish va uning dasturiy to'xtashini ro'yxatga olish (AATni apparat uzilish paytida tizimdan chiqish va to'xtashni ro'yxatga olish o'tkazilmaydi).

2. Nusxadagi bosma (grafik) hujjatlarni berishni ro'yxatga va hisobga olish.

3. Himoyalangan fayllarni ishlab chiqish uchun mo'ljallangan dasturlar va jarayonlar (vazifalar, masalalar)ni ishga tushirish (to'xtatish)ni ro'yxatga olish.

4. Dasturiy vositalar, dasturlar, jarayonlar, vazifalar, masalalar himoyalanayotgan fayllarga kirishga qilinayotgan harakatlarini ro'yxatga olish.

5. Axborotlarning himoyalanadigan manbalarni har qanday belgilash (markazlash) yordamida hisobga olish (himoyalanadigan manbalarini hisobga olish qayd daftarida, kartotekada ularni berish) qabul qilishni ro'yxatga olish bilan o'tkaziladi.

6. Aloqa tizimlarida axborotlarni himoyalash har xil turdagi aloqa kanallarda aylanib yuruvchi maxfiy va qimmatli axborotlarga ruxsatsiz kirishning imkoniyatini bartaraf etishga qaratilgan.

Uning asosida himoyaning bu turi quyidagi maqsadlarga qaratiladi: axborotlar maxfiyligi va yaxlitligini ta'minlashga erishilishni ko'zda tutadi. Kriptografiya va maxsus axborot bayonnomalarini qo'llash

aloqali nazorat qilinmaydigan kanallardagi axborotlarni himoyalashning eng samarali vositasi bo'ladi.

Elektron hujjatlarning yuridik ahamiyatini himoyalash buyruqlar, to'lov topshiriqnomalari, kontraktlar va boshqa farmoyish, shartnoma va moliyaviy hujjatlarni saqlovchi axborot obyektlarini ishlab chiqish, saqlash va uzatish uchun tizimlar va tarmoqlardan foydalanishda zarur bo'ladi. Ushbu muammoni yechish uchun raqamli imzolarni qo'llash bilan bog'liq axborot obyektlarining haqiqiyligini tekshirishning zamonaviy kriptografik usulidan foydalaniladi. Amalda elektron hujjatlar ahamiyatini himoyalash masalasi bilan birgalikda hal qilinadi.

Qo'shimcha elektron magnit nurlanishlar va uzatish kanallari bo'yicha axborotlarni chiqib ketishdan himoyalash, kompyuterdagi maxfiy va sirli axborotlarga begona shaxslar tomonidan ruxsatsiz kirishdan himoyalashning muhim jihati bo'ladi. Himoyaning ushbu turi axborotli elektromagnit signallarini qo'riqlayotgan hudud tashqarisiga chiqib ketish imkoniyatini bartaraf qilishga qaratilgan. Bunda shu narsa ko'zda tutiladiki, qo'riqlayotgan hudud ichida elektron magnitli signallarni tutib olish, ro'yxatga olish va tasvirlashning maxsus apparatlaridan nazoratsiz foydalanish imkoniyatlarini yo'qqa chiqaruvchi samarali choralar qo'llaniladi. Qo'shimcha elektron magnitli nurlanishlar va uzatish kanallardan himoyalash uchun hisoblash texnikasini joylashtirish uchun mo'ljallangan xonalarni ekranlapshtirish hamda uskunaning o'zini (kompyuter va aloqa vositalarini) axborot nurlanishining intensivligini pasaytirishga imkon beruvchi texnik tadbirlar qo'llaniladi.

Ba'zi bir mas'uliyatli hollarda hisoblash uskunalarini kompyuterning axborot nurlanishlari hamda nutqli va muhim bo'lmagan kuchsiz axborotli signallarni ro'yxatga olish yoki yozish maqsadida tatbiq etishi mumkin bo'lgan moliyaviy josuslikning maxsus qo'yiluvchi qurilmalarini aniqlash uchun qo'shimcha tekshiruvlar zarur.

Axborotlarni kompyuter viruslari va dasturlarini tarqatish kanallari bo'yicha boshqa xavfli tavsiflardan himoyalash keyingi vaqtda alohida muhim ahamiyat kasb etadi. Virusli kasalliklarni haqiqiy aniqlanish ko'lamlari kompyuterlarni kasallanishining yuz minglab holatlari bilan baholanadi. Ba'zi bir virus dasturlari butunlay zararsiz bo'lsalar ham, ulardan ko'pchiligi xarob qiluvchi xususiyatga ega. Ayniqsa, turli mahalliy hisoblash tarmoqlar tarkibiga kiruvchi kompyuterlar uchun viruslar xavflidir. Zamonaviy axborot tizimlarining ba'zi bir xususiyatlari viruslarni tarqalishi uchun qulay sharoitlar yaratadi.

Ularga xususan, quyidagilar kiradi:

► ko'pgina foydalanuvchilarning dasturiy ta'minotdan birgalikda fodlanishlarining zaruriyati;

► dasturdan foydalanishni cheklashning qiyinchiligi;

► himoyalashning mavjud tizimlarining ishonchsizligi;

► virusga qarshi harakatga nisbatan axborotlarga kirishning cheklanganligi.

Virusdan himoyalanish usullarida ikkita yo'nalish mavjud:

1. Ruxsatsiz o'zgartirish kiritish imkoniyatlaridan himoyalangan «Immuno bardoshli» dasturiy vositalarni (kirishni cheklash, o'z-o'zini nazorat qilih va o'z-o'zini tiklash usullarini) qo'llash

2. ADPlar faoliyatida chetga chiqishlarning vujudga kelishining doimiy nazoratini, virusli faollikning ehtimol bo'lgan boshqa izlari mavjudligini davriy tekshirishni (masalan, davriy ta'minlanishni buzilishini topishni) hamda yangi dasturni ulardan foydalanish oldidan kirishning nazoratini (ularning tanasida virusli tuzilmalarining mavjudligini o'ziga xos alomatlari bo'yicha) amalga oshiruvchi maxsus tahlilchi dasturlarni qo'llash

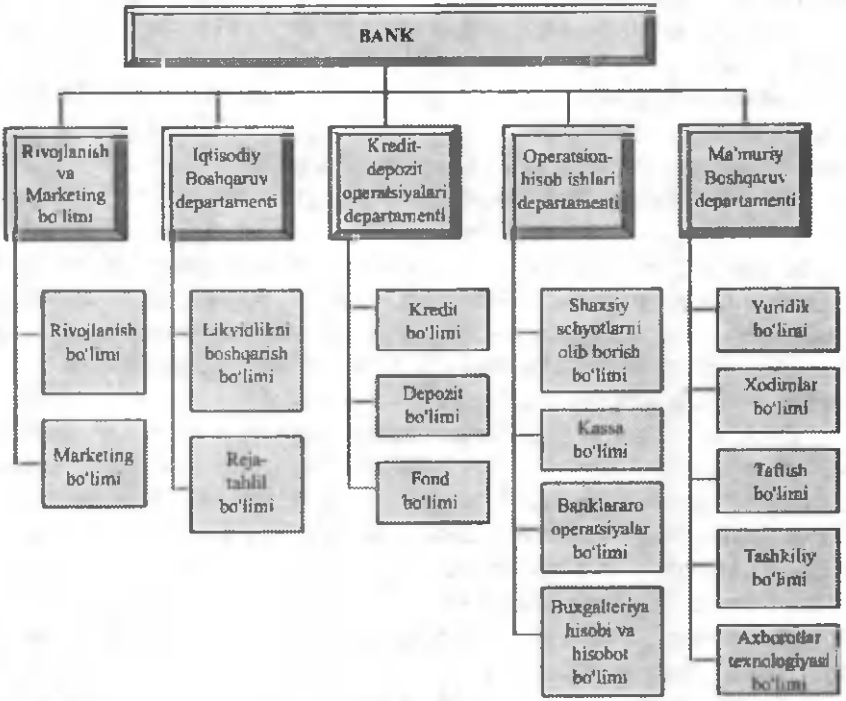
3. Dasturlar va qimmatli bank axborotlaridan ruxsatsiz nusxa ko'chirish va tarqatilishdan himoyalash kompyuterlar dasturlari va ma'lumotlarining qimmatli bazalar ko'rinishida gavdalangan aqliy mulkini saqlash muammosiga mo'ljallangan mulkiy huquqlarni himoyalashning mustaqil turidan iborat bo'ladi.

Ushbu himoyalash, odatda, himoyalanayotgan dasturlar va ma'lumotlar bazasini avvaldan ishlab chiquvchi (parolli himoya, kalit va kalitli disketlarni saqlash bo'yicha qurilmalarga murojaat qilish bo'yicha tekshirish, ishchi kompyuterning noyob ta'riflari bo'yicha tekshirish) maxsus dasturiy vositalar yordamida amalga oshiriladi. Bu ishlab chiqish himoyalanayotgan dastur va ma'lumotlar bazasining bajarilayotgan kodini, begona mashinalar bajarishiga to'siq qo'yuvchi holatga keltiriladi.

Himoyalanishni oshirish uchun printerning uzuvchisi yoki kompyuterning tizimli shinasiga ulanuvchi qo'shimcha apparat bloklari hamda dasturning foydalanilayotgan kodiga ega shriftli fayllar qo'llaniladi.

Dasturlarni ruxsatsiz nusxa ko'chirishdan himoyalanishning umumiy xususiyatlari bunday himoyalashning barqarorligining cheklanishidir, yakuniy holda dasturdan foydalaniladigan kodni bajarilishda markaziy protsessorga ochiq holda kelib tushadi va apparatli sozlovchilar yordamida kuzatish mumkin.

Ammo bu holl himoyalash vositalarining iste'mol xususiyatlarini nolgacha tushirmaydi, chunki ulardan foydalanishdan asosiy maqsad qimmatli, vaqtincha bo'lsa ham, eng yuqori darajagacha qiyinlashtiradi. Shuning uchun bank avtomatlashtirilgan axborot tizimlari (BAAT)ni ishlab chiqish va ulardan samarali foydalanishi zarur.



1-rasm **Bank boshqaruv tuzilmasi**

1. BAATini ishlab chiqish muammolari.

Bank avtomatlashtirilgan axborot tizimlari dastlab AQSH, Yaponiya va Germaniya davlatlari tajribasida qo'llanilgan. Bu tizimning afzalligi banklarda turli xil murakkab operatsiyalarni osongina hal bo'lishi va mijoz bilan bo'ladigan munosabatlarning samaraliligini ta'minlardi. 1994-yilda O'zbekiston Respublikasi Markaziy Bankida mamlakat bank tizimini kompyuterlashtirish bo'yicha Muvofiqlashtiruvchi Kengash tuzildi. Bu kengashni tuzishdan maqsad umumdavlat miqyosda elektron to'lovlarni tizimini qurish, tijorat banklari axborot infratuzilmasini yaratish va bank axborot tizimi texnologiyalarini rivojlantirish konsepsiya-

sini ishlab chiqishdan iborat edi. Bank axborot tizimi texnologiyasi uning boshqaruv tuzilmasi bilan bevosita bog'liqdir (1-rasm). Bankning boshqaruv tuzilmasi turli xil tashkil qilingan bo'lishi mumkin. Bu ko'proq bankning kattaligi, xizmatlar turining sonlari, mijozlarning va bank tomonidan bajarilayotgan operatsiyalarning soniga bog'liq. Boshqaruv tuzilishlari **to'g'ri chiziqli, shtabli** va **to'g'ri chiziqli shtabli** bo'ladi.

To'gri chiziqli boshqaruvda bank boshqaruviga bo'limlar bevosita bo'ysunadi.

Shtabli boshqaruv murakkabroq bo'lib, bunda boshqaruvda bajarilayotgan boshqaruv vazifalarining bir turligi tamoili bo'yicha bo'limlarni birlashtiruvchi departamentlarga bo'ysunadilar.

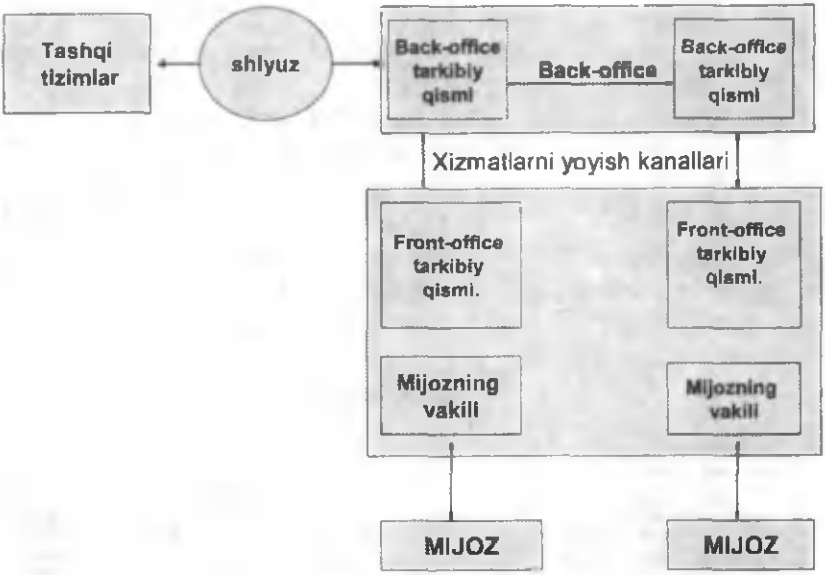
To'g'ri chiziqli shtabli boshqaruv yanada murakkab bo'lib, bunda depozit, kredit, investitsion va boshqa operatsiyalarning bajarilishini ta'minlovchi bo'limlar yuridik va jismoniy shaxslarning har xil guruhlariga xizmat qiluvchi oraliq bosqichdagi boshqaruvga bo'ysunadilar. Bu tizim boshqaruvni murakkablashtiradi va qimmatlashtiradi, ammo uning sifat darajasini oshiradi. Mamlakatimizda turli tijorat banklari faoliyat ko'rsatadi va turli boshqaruv tuzilmasidan foydalanadi.

BAATni texnik ta'minlash jarayonida bank texnologiyalari apparat vositalari arxitekturasi zamonaviy talablar asosida qurilishlari kerak. Ularga: aloqaning turli-tuman telekommunikatsion vositalari, ko'p mashinali majmualar, «mijoz-server»ning arxitekturasidan foydalanish, mahalliy, mintaqaviy va global tezkor tarmoqlarni qo'llash, apparatli yechimlarni unifikatsiyalash kiradi.

«Mijoz-server» arxitekturasi banklarning axborot texnologiyalarini qurilishdagi texnik yechimlarga zamonaviy yondashishning asosi bo'ladi. Bu texnik ta'minlanishni tashkil qilish va axborotlarni ishlab chiqishni mijoz (ishchi stansiya) va server deb nomlangan ikkita tarkibiy qism o'rtasida taqsimlanishini ko'zda tutadi. Ikkala qism birlashtirilgan kompyuterlarda bajariladi. Bunda mijoz serverga so'rovlar yuboradi, server esa ularga xizmat ko'rsatadi. 2-rasmda bankning telekommunikatsion arxitekturasini tuzilmasi ifodalangan.

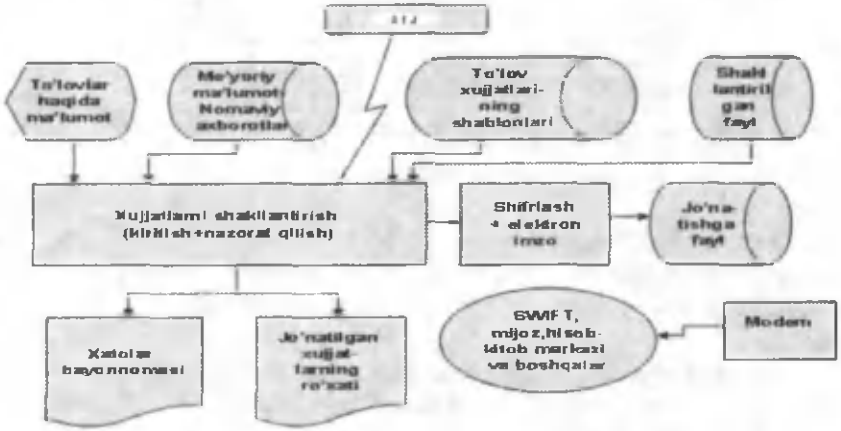
Bank biznes jarayonlarning telekommunikatsion ta'minlanishi o'zining korporativ tarmog'iga xizmat ko'rsatish va har qanday boshqa mahalliy va global tarmoqlarga kirishni hisobga olish bilan quriladi.

Telekommunikatsion tizimlar bankka avtomatlashtirishning eng muhim masalalari bisnes jarayonlarning o'zaro hamkorliklarining eng muvofiq unumdorligi va taniqligini ta'minlash kabi sof texnikadan tortib bank xizmatini ko'rsatishning eng yuqori darajasidagi vazifagacha hal



2-rasm. **Bankning telekommunikatsion arxitekturasi tuzilmasi**

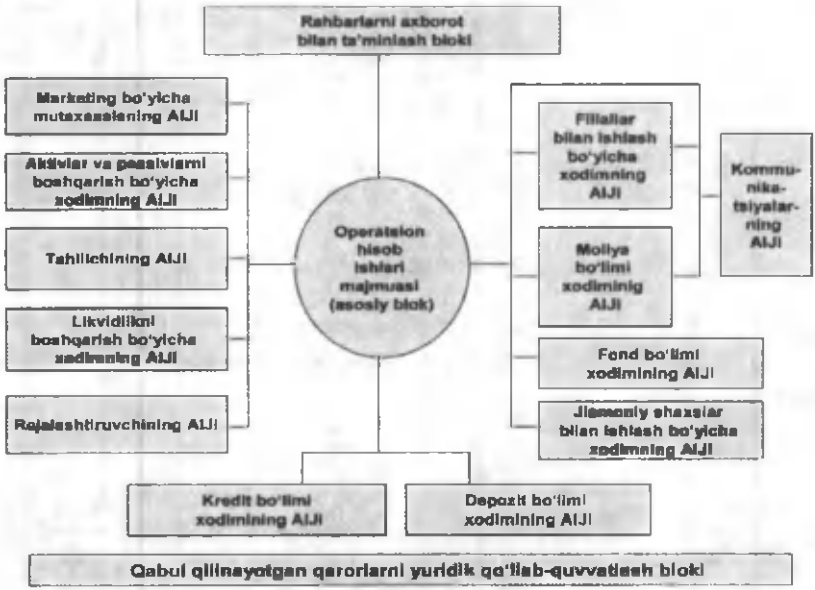
qilishga imkon beradi. Quyida ma'lumotlarning eksporti bo'yicha avtomatlashtirilgan ish joylari kommunikatsiyalarini ishlash chizmasini keltiramiz (3-rasm).



3-rasm. **Ma'lumotlarning eksporti bo'yicha avtomatlashtirilgan ish joylari kommunikatsiyalarini ishlash chizmasi**

Banklararo o'zaro hamkorlikning kichik protokolini tarmoqlarda tatbiq etish g'oyatda muhim, ular axborotlarning eng samarali almashuvini tashkil qilishga imkon beradi.

Tajriba shuni ko'rsatmoqdaki, serverlar banklarning hisoblash majmualarida eng kuchsiz bo'g'in hisoblanadi. Ulardan eng istiqbollisi UNIX server. Pastroq darajadagi serverlar, masalan, IBM PC serverlar diskli tizimchani kengaytirish, uzilishli vaziyatlarni oldindan aytib berish bo'yicha yechimlarni talab qiladilar. Quyidagi 4-rasmda mujassamlashgan BAATning tarkibiy tuzilishi keltirilgan. Unda bankning barcha faoliyatlarini qamrab olish ko'zda tutilgan.



4-rasm. **BAATning tarkibiy tuzilishi**

Avtomatlashtirilgan bank tizimlari o'z xizmatlarining keng, turli-tumanligi bo'yicha mijozlarga tez va sifatli xizmat ko'rsatishga imkon beradi. Tizimning asosiy xizmat modullari quyidagilarni amalga oshiradi:

– yuridik shaxslarga hisoblash-kassa xizmatini ko'rsatish;

– bank-korrespondentlari schyotlari bo'yicha xizmat ko'rsatish;

– kredit, depozit, valuta operatsiyalari;

– xususiy shaxslar kiritmalarining har qanday turlari va ular bo'yicha operatsiyalar;

– fond operatsiyalari;
– plastik kartochkalar yordamida hisob-kitoblar;
– bug'galteriya vazifalari;
– tahlil, qarorlar qabul qilish, menejment, marketing va boshqalar.

Banklarning amaliy faoliyatida axborotlarni himoyalash tadbirlari va usullarini qo'llash quyidagi mustaqil yo'nalishlarni o'z ichiga oladi:

1. Axborotga ruxsatsiz kirishdan himoyalash;
2. Axborotlarni aloqa tizimlarda himoyalash;
3. Elektron hujjatlarning yuridik ahamiyatini himoyalash;
4. Maxfiy axborotlarni qo'shimcha elektron magnitli nurlanishlar va uzatish kanallaridan chiqib ketishini himoyalash;
5. Axborotlarni kompyuter viruslari va dasturlarini tarqatish kanallari bo'yicha boshqa xavfli ta'sirlardan himoyalash;
6. Dastur va qimmatli kompyuter axborotlarini ruxsatsiz nusxa ko'chirish va tarqatilishidan himoyalash.

Har bir yo'nalish uchun asosiy maqsad va vazifalar aniqlanadi. Ruxsatsiz kirish ostida foydalanuvchining va cheklanish AATning boshqa subyektlarini tasodifan yoki qasddan harakati natijasida axborotlarni himoyalashning asosiy qismi bo'lgan kirishni cheklashning belgilangan qoidalari buzilishi tushuniladi.

Aloqa tizimlarida axborotlarni himoyalash har xil turdagi aloqa kanallarda aylanib yuruvchi maxfiy va qimmatli axborotlarga ruxsatsiz kirishning imkoniyatini bartaraf etishga qaratilgan.

Ma'lumotlar himoyasi (konfidensial) deganda, axborotlarning himoyalanish darajasi tushuniladi. Subyekt – axborot tizimining faol ishtirokchisi bo'lib, axborotlar oqimini obyektdan subyektga o'tib ketishiga sabab bo'ladi, yoki tizimning holatini o'zgartiradi. Obyekt axborot tizimining passiv ishtirokchisi bo'lib, axborotlarni qabul qiladi, saqlaydi, uzatadi.

Xavfsizlik yoki himoya tizimi – himoya vositalariga ega tizim bo'lib, xavfsizlikni ifodalaydi. Himoya vositalari kompleksi texnik va dasturiy bo'ladi. Xavfsizlik siyosati – xavfsizlikni ifodalaydigan me'yor, qoidalar va amaliy ko'rsatmalardan iborat. Elektron hujjatlarning yuridik ahamiyatini himoyalash buyruqlari, to'lov topshiriqnomalari, kontraktlar va boshqa farmoyish, shartnoma va moliyaviy hujjatlarni saqlovchi axborot obyektlarini ishlab chiqish, saqlash va uzatish uchun tizimlar va tarmoqlardan foydalanishda zarur bo'ladi.

Qo'shimcha elektron magnit nurlanishlar va uzatish kanallari bo'yicha axborotlarning chiqib ketishdan himoyalashda axborotli elektro-

magnit signallarini qo'riqlayotgan hudud tashqarisiga chiqib ketish imkoniyatini bartaraf qilishga qaratilgan. Ba'zi bir mas'uliyatli hollarda hisoblash uskunalarini kompyuterning axborot nurlanishlari hamda nutqli va muhim bo'lmagah kuchsiz axborotli signallarni ro'yxatga olish yoki yozish maqsadida tatbiq etishi mumkin bo'lgan moliyaviy josuslikning maxsus qo'yiluvchi qurilmalarini aniqlash uchun qo'shimcha tekshiruv zarur.

Ekstranet – Web serverga begonalar kirishidan himoyalangan holda korxona, keltirib beruvchi, iste'molchilar va axborotlardan birgalikda foydalanuvchi hamkorlar bilan aloqa o'rnatadi. Internetda elektron tijoratni amalga oishirishda iqtisodiy axborotlarni xavfsizligini ta'minlash maqsadida:

A. Shifrlash.

B. Raqamli qo'l qo'yish.

D. Raqamli sertifikat amalga oshiriladi.

Shifrlash – bu matnni shunday o'zgartirishki, undan keyin matnni faqat qayta o'zgartirish yoki shifr kalitini bilsagina ochib bo'ladi. Shifrlashning simmetrik va nosimmetrik usullari bor. Birinchi bo'lib, an'anaviy va tayyorlanmagan foydalanuvchiga tushunarli bo'lgan yagona kalit ishlatiladi. Bunda kalit ham, yuboruvchi ham ma'lumot manzilida bo'ladi. Bugungi kunda internetda shifrlashning asosiy usuli ochiq kalitli nosimmetrik shifrlash hisoblanadi. Bu usulda har bir foydalanuvchining 2 ta kaliti bo'ladi – ochiq (ommaviy) va yopiq (shaxsiy).

Ommaviy kalit bilan shifrlangan axborotni, faqat shaxsiy kalit bilan shifrni ochish mumkin yoki aksincha, ommaviy kalit axborot almashinuvchi hamma korrespondentlarga aytiladi, shaxsiy kod esa sir saqlanadi. Yopiq kalit bilan shifrlash texnologiyasi yuqori darajali himoyani ta'minlab bersa ham, u ko'p qirrali qidiruv resurslarini talab qiladi, uzun axborotlarni uzatishda ancha sekin ishlaydi. Shuning uchun ma'lumotlarning operativ almashinuvi zarur bo'lsa, shunday usul qo'llaniladiki, unda simmetrik va nosimmetrik shifrlashlarning birgalikda ishlatish imkoniyatlaridan foydalaniladi.

Mijoz va server o'rtasida himoyalangan aloqa bo'lgan tashkilotda, ko'pincha, seansli kalit usuliga asoslangan SSL – Secure Socket Layer – protokolidan foydalaniladi. Bunda server tomonidan tasodifan shifrlanishning simmetrik kaliti generatsiya qiladi. U mijozga simmetrik bo'lmagan ochiq kalit yordamida uzatiladi. Shifrlash internetdan uzatilayotgan ma'lumotlarni begonalardan himoyalashga yordam beradi. Lekin transaksiyada 2-tomon ishtirok etayotgan shaxs aynan o'sha ekanligiga

amin bo'lishi kerak. Biznesda buyurtmachi shaxsining asosiy identifikatori bo'lib uni qo'li hisoblanadi. Elektron tijoratda an'anaviy qo'lning elektron ekvivalentiga raqamli qo'l ishlatiladi. Uning yordamida oldi-sotdi shartnomasi o'sha muayyan yuridik yoki jismoniy shaxs bilan tuzilganligini isbotlash mumkin. Masalan: 2 hamkor internet orqali shartnoma tuzishmoqchi, deb tasavvur qilaylik. Oldin ular ochiq kalitlar bilan almashinadi. Kevin tomonlardan biri shartnoma tuzadi, uni hamkorning ochiq kaliti bilan shifrlaydi va o'zining yopiq kaliti bilan shifrlangan shaxsiy imzosini qo'yadi. Ikki tomon shartnoma matnini o'zining shaxsiy kaliti bilan shifrlab ochadi. Imzoni esa o'zining yopiq kaliti bilan shifrlangan qo'lini qo'yib hamkoriga qaytarib yuboradi.

Raqamli imzo deganda faqat familiyasi yoki tashkilot nomini tushunish mumkin emas. Elektron imzo – ketma-ket yozilgan raqamlardan iborat bo'ladi. Raqamli imzoda maxsus shifrlash algoritmlari yordamida va ochiq yoki maxfiy kalitlar texnologiyasi qo'llaniladi.

Elektron sertifikatlar – bu Internetda ma'lumot saqlashni himoyalashni amalga oshirish usullaridan biri. Elektron sertifikatlashning ma'nosi shuki, ochiq kalit yoki elektorn imzolar maxsus mas'ul shunga mo'ljallangan sertifikatlash markazi tomonidan tasdiqlanishi kerak. Istalgan tijorat shartnomalarining oxirgi bosqichi davlatda yuritilayotgan to'lov tizimlaridan biri asosida hisob-kitob qilish bilan yakunlanadi.

Elektron sretifikat rivojlanishi va keng tarqalishi, iste'molchiga global tarmoqda sotib olish uchun tovarlar va xizmatlar to'lovi oddiy, qulay va ishonchli amalga oshiradigan zamonaviy elektron to'lov tizimini tashkil qilish va mukammallashtirishga undaydi. Kriptografiya – konfidensial axborotlarni o'zgartirish haqidagi fan. Kriptografiya – bu axborotni himoyalanmagan kanal orqali maxfiy uzatish maqsadida uni kod-

lash (axbortlarni o'zgartiruvchi) to'grisidagi fan bo'lib. axborotlar xavfsizligini ta'minlash haqida bilim va ko'nikmalar beradi.

Axborotni maxsus himoyalash – shunday algoritm bo'ladiki, har qanday axborot shifrlanib uzatiladi va qabul qilinadi. Ma'lumki, **www** – odatda, **http** protokoli bilan ishlaydi. Agar internetda ma'lumotlarni himoyasini ta'minlash talab etilsa, u holda **https** – himoyalangan kanalga muhim ma'lumotlarni kiritish maqsadga muvofiq bo'ladi. **https** – Internetda himoyalangan kanal bo'lib, unda sistemaga parolsiz kirish mumkin emas. Himoyalangan kanalda shifrlash kalit orqali amalga oshiriladi. Avval bu faqat harbiy maqsadlarda foydalanilgan. Agar undan foydalanilsa, bu axborotni hech kim o'qiy olmaydi.

Shifrlash algoritmi masalan, matn qatorlarini vertikal qilib qo'yish mumkin. Bu **shifrator** bo'ladi.

Deshifrator esa uni qayta ochadigan algoritm. Uni ikkalasini birdan berib bo'lmaydi. Avval shifratorni ma'lum vaqtdan so'ng deshifratorni yuboramiz, EHM uni ocha olmaydi.

Bugungi kungacha muhim axborotlar xavfsizligini saqlash uchun turli-tuman shifrlash usullari ishlab chiqilgan. Shularning ba'zilari bilan yaqindan tanishib chiqaylik. Hozirgi paytda kriptosistemalarning ikki xili mavjud. Bular:

– **simmetrik kriptosistemalar,** bunda shifrovka va deshifrovka uchun bitta kalit bo'ladi.

– **asimmetrik (ochiq kalit qo'llash) kriptosistemalar.** bunda shifrovka, deshifrovka uchun alohida kalit bo'ladi. Ya'ni bir kalit bilan shifrlanadi, bir kalit bilan deshifrlanadi.

Simmetrik kriptosistemalarda axborotni uzatuvchi ham, uni qabul etuvchi shaxs ham bir xil turdagi simmetrik kalitlarga ega bo'ladilar. **Asimmetrik** kriptosistemalarda esa ochiq kalit axborot uzatuvchi uchun va shaxsiy kalit uni ochish uchun mavjud bo'ladi. Endi, kriptosistemalarning asosiy terminlarini konkretlashtiramiz.

Kalit shifrlangan ma'lumotni, ya'ni axborotni ochish va undan foydalanishni ta'minlaydigan vosita. Kalitlarning turli xillari mavjud:

Maxfiy kalit (asosiy kod) shifrlashda va uni ochishda qo'llaniladi. Simmetrik algoritmlarda axborot yuboruvchi ham qabul qiluvchi ham ushbu kodga ega bo'lishi shart.

Ochiq kalit. Axborot qabul qiluvchi shaxs uchun mo'ljallangan bo'lib, shifrlangan axborotni ochish uchun qo'llaniladi. Bunday tizim faol ishlashi uchun kod keng tarqalgan bo'lishi shart.

Shaxsiy kalit. Bunday kalit faqat konkret shaxsga ma'lum bo'lishi

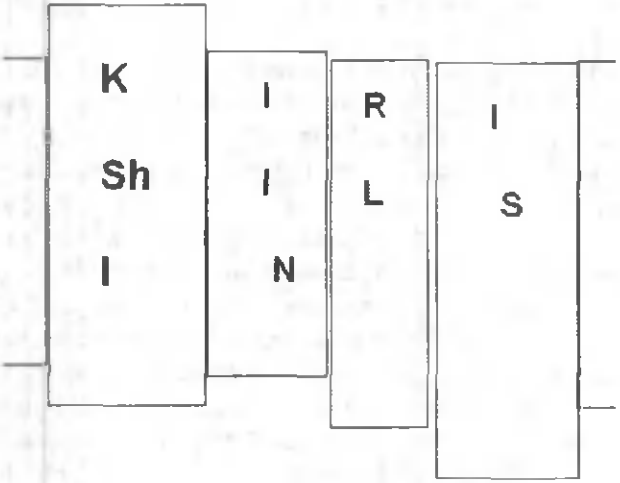
kerak. U ochiq kalit yordamida shifrlangan ma'lumotni ochish uchun ishlatiladi.

Shifrlashning eng oddiy usullaridan biri-bu **kod kitoblaridan** foydalanishdir. Ushbu kitobda har bir harf boshqa harf bilan almashtiriladi. Masalan, **URF** guruhida alfavit 13 ta harfga surilgan bo'lib, **A** harfi **N**, **V** esa **D** harfiga almashtiriladi va hokazo. Bunday shifrlangan informatsiyani kalit yordamida ochish uchun 13 pozitsiyaga surilgan harflarni o'zaro almashtirish kifoyadir. Odatda, kriptosistemalarda boshlang'ich uzatilayotgan axborot ochiq matn deb, kalit yordamida o'zgartirilgan ma'lumot shifrlangan matn deb ataladi. Ammo bunday usul har doim yaxshi samara bermaydi. Shifrlangan matnning noqonuniy kanal orqali qo'lga kiritgan shaxs harflarni har xil variantda almashtirish yo'li bilan ochiq matnni ajratib olishi mumkin. Masalan, ikkinchi jahon urushi davrida simmetrik kriptosistemalardan keng foydalanilgan. Ularning naqadar murakkabligiga qaramasdan dushman taraf bir necha bor urinishlardan so'ng shifrlangan matnga kalit topishga qodirligi ayon bo'lgan edi. Bu usulning yana bir kamchiligi shunda ediki, shifrni ochishda bitta kalit mavjudligidir. Agar bu kalit dushman qo'liga tushsa, hamma ishni boshidan boshlashga to'g'ri kelar edi. Kompyuterlardan keng sohada foydalanish esa bu usulda axborotdan foydalanish va uzatishda himoyalanishni yanada yomonlashtirdi, chunki endi shifrlangan kalitni qo'lga kiritish kun yoki oylarni emas, bir necha minutlarni tashkil etadigan bo'ldi.

Axborot xavfsizligini ta'minlab kelgan shifrlash va autentifikatsiya usullari haqida qisqacha ma'lumotga ega bo'lamiz.

1.3. Oddiy shifrlash usuli yordamida axborot xavfsizligini ta'minlash

O'zaro almashtirish usuli. Bu usulda shifrlanayotgan matn harflari ma'lum qoida bo'yicha o'zaro almashtiriladi. O'zaro almashtirish usuli shifrlashning eng sodda va qadim zamonlarda joriy qilingan usullariga kiradi. Masalan, eramizdan avvalgi V asrdayoq Sparta hukmdorligi davrida urush paytida o'ziga xos shifrlangan matnlardan foydalanishda, skitala degan kriptografik qurilmani yaratishgan. Bunda harflarni o'zaro almashtirishning eng sodda usullaridan foydalanganlar. Masalan, «KIRISHILSIN» degan ma'lumotni yuborishda harflarni (2, 3, ...) pozitsiyada so'z tugaguncha yozilsa, shifrlangan va harflari xaotik joylashgan matnni olish mumkin bo'lgan (5-rasm).



5-rasm. **Oddiy shifrlash usuli**

Bunday shifrlangan matnning asl nusxasini olish uchun shifrlash qoidasini bilishdan tashqari shifrlash kalitini ham bilish zarurdir. Shifrlash jadvallari. Uyg'onish davriga kelib (XV asr oxiri) kriptografiya yo'nalishi paydo bo'ldi. Endi, kriptografiya usullari nafaqat siyosatda, diplomatiyada va harbiy mudofaa ishlarida, balki yuksak intellektual potensialga ega bo'lgan shaxslarni inkvizitsiyadan himoya qilishda ham ishlatilgan.

Ishlab chiqilgan usullardan shifrlash jarayonini shifrlash jadvallari orqali hal qilish ko'proq ishlatilgan. Matnlarni himoyalangan holda bu usul bilan uzatishda nafaqat uning harflarini almashtirishni, balki uni tasodifiy shaxslardan himoyalash ham mumkin bo'lgan. Ishlab chiqilgan shifrlar o'rin almashuvida shifrlash jadvallaridan foydalanilgan. Shifrlovchi jadvallarda kalit sifatida quyidagi ko'rsatkichlarga asoslangan:

– jadval o'lchovi,
– o'zaro almashtirishni ifodalovchi so'z,
– jadval strukturasining xususiyatlari.

Eng sodda jadvalli shifrlashda asosan uzatiladigan ma'lumotning harflari juda sodda holda o'rin almashgan. Bu usulning kaliti jadval o'lchovi bilan aniqlangan. Bu usul skitala usuliga juda o'xshash. Masalan, **konkurs yettinchida o'n ikki yarimda bo'ladi**, degan ma'lumot jadvalga ustun bo'yicha yoziladi. Beshta qator va yettita ustundan iborat jadvalga ma'lumot quyidagicha yoziladi (6-rasm).

K	R	I	A	K	M	L
O	S	N	O‘	I	D	A
N	E	CH	N	YA	A	D
K	T	I	I	R	B	I
U	T	D	K	I	O‘	

6-rasm. **Jadvalli shifrlash usuli**

Bu yerda 5 qatorga guruhlab yozilgan matn quyidagicha shifr ko‘rinishiga ega bo‘ladi: **KRIAKML OSNO‘IDA NECHNYAAD KTIIRBI UTDKIO‘**

Albatta, besh qatorga bo‘linib yozilgan shifrlangan matn shifr kalitini tashkil etmaydi va u asosan, shifrlangan matnni yozishni osonlashtirish uchun foydalaniladi.

Shifr kalitini esa jadval o‘lchovi tashkil etadi va uni uzatuvchi va qabul qilib oluvchi shaxs bilishi matnni himoyalanishini tashkil etadi. Uzatilayotgan matnni yanada muhofazalash uchun o‘zaro almashtirish usulining boshqa variantlari ham mavjud bo‘lib, ularning ishlash jarayoni ham yuqorida keltirilgan usulga o‘xshash, farqi shifrlashda matnli kalitdan foydalanganligidadir. Undan tashqari, magik kvadratlash hamda polibian kvadratlash variantlari ham diqqatga sazovordir. Magik kvadratlash usulida kvadrat jadvallar shifrlanib, matn shu shifrlar bilan niqoblangan bo‘ladi. Bunda kvadrat jadval katakchalariga natural sonlar raqamlari 1 dan boshlab shunday yoziladiki, har bir qator, har bir ustun va *diagonal bo‘yicha yozilgan raqamlar yig‘indisi bir xil natija berishi* shart. Shifrlanadigan matn magik kvadrat ichiga kataklar nomerlariga qarab yoziladi. Masalan, **Sizni kutmoqdaman** iborasini shifrlash quyidagi magik kvadratda o‘z aksini topadi:

16	3	2	13		N	Z	I	A
5	10	11	8		I	O	Q	T
9	6	7	12		M	K	U	D
4	15	14	1		N	A	M	S

O‘ng tomondagi jadvalda satr bo‘yicha yozilgan matn shifri quyidagicha ifodalangan: **nzia ioqt mkud nams.**

Shuni aytish joizki, bu usulni qo‘llaganda kvadrat o‘lchami oshgan sari magik kvadratlar soni tez o‘sib ketadi. Bu esa, o‘z navbatida, shifrlangan matnni tez tahlil qilish jarayonini qiyinlashtirib yuboradi. Shuning uchun ham eng ko‘p qo‘llaniladigan magik jadval o‘lchovi 3×3 dir. Bordi-yu, magik jadval o‘lchovi 4×4 bo‘lsa, u holda 880 ta, 5×5

o'lchamlisida esa magik kvadratlar soni 250 000 ga yetadi. Bu holda matnni tahlil qilish mushkul bo'ladi.

Oddiy almashtirish shifrlari. Bu usulning asosini shifrlanishi kerak bo'lgan matn harflarini biror alfavitdagisini boshqa alfavit harflari bilan almashtirish tashkil etadi. Agarda faqat bitta alfavit harflari bilan oldindan kelishib olingan holda o'zaro almashtirib ishlatilsa, u holda polibian kvadrat usuli, deb yuritiladigan himoya vositasi vujudga keladi. Polibian kvadrat usuli matn harflarini almashtirishda oddiy shifrlashning eng sodda usulini eramizdan avval ikkinchi asrda grek yozuvchisi va tarixchisi Polibiy yaratgan bo'lib, unda asosan 5×5 o'lchovdagi grek harflari bilan to'ldirilgan jadval tuzishda foydalanilgan.

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

7-rasm. **Shifrlashning Polibian usuli**

Polibian kvadratida matn harflari tasodifiy usulda shifrlangan. Bunday jadval bilan shifrlashda almashtirlayotgan navbatdagi harf polibian kvadratida shu ustunni pastida joylashgan harf bilan, agar ochiq matndagi harf pastda joylashgan bo'lsa, shu ustunning eng yuqori harfi bilan almashtirilgan. Shifrlashning polibian usuli ko'pgina kriptosistemalarda o'z samarasini berdi. Bir alfavitli sodda almashtiruvning xususiy holini Rim imperatori **Gay Yuliy Sezar** amalga tatbiq etib, o'ziga xos yangicha shifrlash usulini yaratdi. Sezarning shifrlash sistemasi **Sezar Siseron** bilan axborot almashuv jarayonida vujudga kelgan bo'lib, bunda harflarni almashtirish quyidagi qoida bo'yicha amalga oshirilgan.

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	

8-rasm. **Harflarni almashtirib shifrlash**

Almashtirish alfavitdagi harfni biron K pozitsiyaga surish yo'li bilan amalga oshirilgan. Alfavit oxiriga yetganda takroriy ravishda alfavit boshiga o'tish davom ettiriladi.

Sezar harflarni o'zaro almashtirishda K q 3 bo'lgan holni olgan. Bunday shifr almashuvini ochiq matn tarkibida va shifrmatnlarda ikkitadan harfli jadvalli o'zgartirishlar asosida hal qilish mumkin. Quyida K q 3 bo'lgan holda o'zaro almashtirish mumkin bo'lgan variantlar keltirilgan. Masalan, yuqoridagi jadval bo'yicha Sezarning quyidagi maktubi **VENI YLGL YLPL** (o'zbekchaga tarjima qilinsa, **«Keldim, ko'rdim, yutdim»**) shifrlangan holdagi ko'rinishi quyidagi holda bo'ladi: **YHQL YLGL YLPL.**

Xuddi yuqorida keltirilgan usullardek ishlash prinsipiga ega bo'lgan oddiy shifrlashning boshqa variantlari ham mavjud bo'lib, ulardan eng ko'p tarqalganlari Trisemusning shifrlash jadvallari hamda Pleyfeyrning biogramm shifrlaridir. 1508-yilda germaniyalik Iogani Trisemus kriptologiya sohasiga bag'ishlangan **«Poligrafiya»** asarini yozdi. Ushbu kitobda birinchi bor kriptografiyada alvafit bilan tasodifiy to'ldirilgan shifrlovchi jadvaldan foydalanishni sistemali tarzda bayon etgan. Bu jadvallarga avvalo satrlarga kalitli so'zlar to'ldirilgan (takrorlanadigan harflardan tashqari). Keyinchalik jadval hali uchramagan alfavitdagi harflar bilan ketma-ket to'ldirilgan. Kalitli so'z yoki so'z birikmasini xotirada saqlash qiyin bo'lmagani uchun bunday usul shifrlash va antishifrlash uchun ham qiyin kechmagan. Misol tariqasida rus alifbosidagi harflar bilan ish yuritamiz. Rus alifbosi uchun shifrlash jadvali 4×8 o'lchamli bo'ladi. Kalit vazifasini boringki, **BANDEROL** degan so'z bajarsin. Bu holda shifrlash jadvali quyidagi ko'rinishda bo'ladi (9-rasm):

B A n d E r o l

v g j z i y ĸ

M P c t U f h ch

Ch sh e yu ya

9-rasm. **Tresimus usulida shifrlash**

Bunda ham xuddi Polibian kvadratida bo'lganidek, shifrlash jarayonida ochiq matnning navbatdagi harfini shifrmatnga shu ustunning pastki qismidagisini yozadi. Agar matn harfi jadvalning pastki satrida bo'lsa, u holda shifrmatnga ustunning eng yuqorisidagi harfni yozadi. Bunday usulda tuzilgan jadvalli shifrlar monogramma deb ataladi, chun-

ki ular faqat birgina harfdan tuzilgan. Ammo ikkitadan harf bilan shifrlovchi jadvallarni yaratish mumkinligini ham Trisemus isbotlashga harakat qildi. Bunday shifrlarni bigrammlar deb atadi.

Pleyfeyrning bigramm shifrlari. 1854-yili Pleyfeyr tomonidan shifrlashning bigramm usuli yaratilib, u birinchi jahon urushida Buyuk Britaniya tomonidan keng qo'llanilgan. Pleyfeyr shifri asosini yuborilgan matnning mazmuni tasodifiy joylashgan harflar shifrmatni tashkil etadi. Shifrlovchi jadvalni esda saqlash uchun matnni jo'natuvchi va qabul qiluvchi jadvalning dastlabki satrlarini to'ldirishda kalitli so'zni bilsa kifoya. Umuman olganda, Trisemus shifrlovchi jadvali xuddi Pleyfeyr sistemasiga o'xshashu, ammo shifrlash jarayonida quyidagi shartlar ketma-ket bajarilishi zarur.

1. Yuboriladigan matn toq harfli bo'lishi kerak. Ma'lumotning ochiq matni ikkitadan harflar bilan ifodalanishi zarur va unda ikkita bir xil harf (bigramm) bo'lmasligi kerak.

2. Ochiq matnning bigrammasi shifrlovchi jadval yordamida shifrmatnning bigrammasiga quyidagi qoida bo'yicha aylantiriladi:

– agar ochiq matn bigrammasining ikkita harfi bir satrga yoki ustunga tushmasa, u holda harflarni to'g'ri to'rtburchak burchaklaridan qidirish lozim. Shunda bigramma shifr matnidagi harflar ochiq matnning harflariga oynadek akslanishi kerak.

– agar biogrammaning ikkala harfi ham jadvalning bir ustuniga joylashsa, u holda shifrmatnning harflari uning ostidagi harflar ekan, deyish mumkin. Bordi-yu, ochiq matn harflari pastki satrda bo'lsa, u holda shifrmatn uchun shu ustunning ustki satrdagi harflari olinadi.

– agar ochiq matn bigrammasining ikkala harfi ham bir satrga tegishli bo'lsa, u holda shifrmatn harflari uchun o'ng tomondagi harflar olinadi. Bordi-yu, ochiq matn harflari o'ng tomondagi oxirgi ustunda bo'lsa, u holda shu satrning chap tomonidagi ustun harflari olinadi.

1.4. Murakkab almashtirish shifrlari usuli yordamida axborot xavfsizligini ta'minlash

Shifrlashning murakkab almashtirish usuli – ko'p alfavitli deb ataladi, chunki oddiy shifrlash usuli bilan almashtirilgan har bir harf keyinchalik ketma-ket va takroriy bosqichda alfavitlarni almashtirish usuli bilan amalga oshiriladi. **K** – alfavitli almashtirishda **X0** simvoli, **V0** alfavitining **U0** simvoli bilan almashtiriladi, aksincha, **X1** simvoli esa V1 alfavitining **U1** simvoli bilan va hokazo, **X(k-1)** simvoli **V(k-1)**

alfavitining **U(k-1)** simvoli bilan almashtiriladi. Nihoyat Xk simvoli yana **V0** alfavitining **U1** simvoli bilan almashtirilib, butun yuqorida keltirilgan jarayon qaytariladi. Bunday ko'palfavitli o'zaro almashtirishning samarasi shundaki, shifrlanayotgan **A** alfavitli ochiq matn boshqa **V(r)** alfavitlari bilan yashirin holga keltiriladi. Bunda himoyalanish darajasi **K** uzunligi davriga proporsional bo'ladi. Quyida rq4 uchun ko'palfavitli almashtirishning umumiy sxemasi keltirilgan:

Asl nusxa simvoli	**Xo**	**X1**	**X2**	**X3**	**X4**	**X5**	**X6**	**X7**	**X8**	**X9**
Almashtirish alfaviti	**V0**	**V1**	**V2**	**V3**	**V0**	**V1**	**V2**	**V3**	**V0**	**V1**

10-rasm. **Shifrlashning murakkab usuli**

Shuni qayd etish joizki, kriptografiyada ko'palfavitli shifr almashtirish jarayonini ixtiro qilgan va uni amaliyotga tatbiq etgan nazariyotchi olim va taniqli arxitektor **Leon Batist Alberti** edi. Uning 1566-yili yozgan «**Shifr haqida traktat**» kitobi Yevropada yozilgan kriptologiya to'g'risidagi birinchi ilmiy asar hisoblanadi. Shuning uchun ham **L.Albertini** butun jahon kriptologlari ushbu yo'nalishning asoschisi deb hisoblaydilar.

Uitstonning «ikkilamchi kvadrat» shifrlash usuli. 1854-yili ingliz **Charlz Uitston** bigramm usuli bilan shifrlashning yangi bir usulini kashf qildi va uni «**ikkili kvadrat**» deb atadi. Ushbu shifrlash usuli kriptografiya tarixida yangi bir etapni vujudga keltirdi, deyish mumkin. Polibian usulidan farqli ravishda bu usulda birdaniga gorizontal joylashgan ikkita jadvaldan foydalanib, shifrlash bigramm ko'rinishida bo'ladi. Bu shifrlash usulini qo'lda ham yaratish mumkin bo'lganligi uchun nemislar II jahon urushida shu usuldan unumli va ishonchli foydalanishgan. Masalan, ushbu usulni rus alifbosi harflari tasodifiy joylashgan ikkita jadvaldan iborat deylik (11-rasm):

J	**sh**	**N**	**Yu**	**R**		**I**	**Ch**	**G**	**Ya**	**T**
I	**T**		**Ts**	**B**		**,**	**J**		**M**	**O**
Ya	**M**	**Ye**	**.**	**S**		**Z**	**Yu**	**R**	**V**	
V		**P**	**Ch**					**:**	**P**	**Ye**	**L**
:	**D**	**U**	**O**	**K**		**'**	**A**	**N**	**.**	**X**
Z	**E**	**F**	**G**	**Sh**		**E**	**K**	**S**	**Sh**	**D**
X	**A**	**;**	**L**			**B**	**F**	**U**		

11-rasm. **Bigramm usuli bilan shifrlash**

Shifrlashdan oldin yuboriladigan ma'lumot matni bigrammlarga ajratiladi. Har bir bigramm alohida shifrlanadi. Bigrammning birinchi harfini chap tomondagi jadvaldan topiladi, ikkinchi harfini esa o'ng tomondagi jadvaldan qidiriladi. Keyin tafakkurda fikran to'g'ri to'rtburchak tuzilib, uning qarama-qarshi uchlarida bigramm harflari yotibdi, deb faraz qilinadi. Boshqa qarama-qarshi uchlarida esa shifr–matnning bigramm harflari joylashadi.

1.5. DES algoritmi bilan shifrlash orqali axborotni himoyalash

1975-yili **IBM, NSA** va **NBS** yoki qisqacha NIST firmalari ochiq kalitli algoritm qo'llashni tavsiya etishdi. Bu algoritm «**Data Encruption Standart**» – shifrlangan ma'lumotlar standarti yoki qisqacha **DES** nomi bilan mashhurdir. **DES** faqat bitta shifrlash algoritmi bilan emas, balki yagona oilani ichiga kiruvchi bir qancha algoritmlardan tashkil topgan.

Masalaning bunday qo'yilishi algoritmni har qanday shaxs bilishi mumkinligini taqozo etadi, lekin bu bilan shifrlangan axborot o'z maxfiyligini yo'qotmaydi, deb ayta olmaymiz. Bundan tashqari, ushbu algoritm maxfiy kalitni murakkabligini (kodlar soni) anchaga kamaytirishga imkon beradi. Bu holda axborot tarqatuvchi har bir shaxsga algoritm nusxasi bilan birga maxfiy kalitni yuborishi kifoya. Odatda, maxfiy kalit 256 sonidan kichik bo'lib, u shu qadar katta sonki, uni har xil variantlarini bilib qo'yish bilan maxfiy kalitni aniqlash ancha murakkab masaladir.

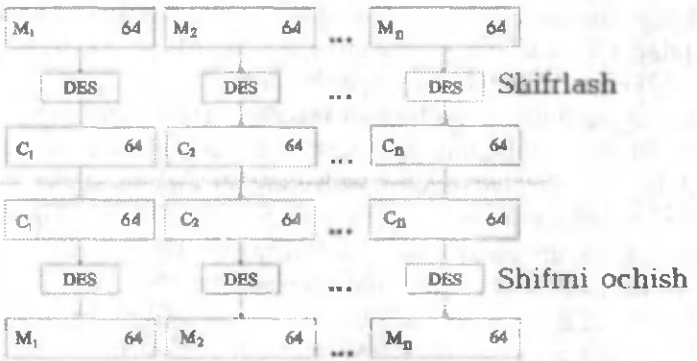
Hozirgi paytda **DES** o'z samarasini berdi. **DES** algoritmlari keng ommaga yetarli darajada tarqanganligiga qaramay, maxfiy kalitni juda quvvatli hisoblash texnikasisiz amalda aniqlab bo'lmaydi. Agar **DES**da bitta ma'lumot uch marta har xil maxfiy kalitlar yordamida shifrlansa, uni bor algoritmlar yordamida ochish umuman mumkin emas.

Oxirigi paytda har xil yangi simmetrik kriptosistemalar yaratilishiga qaramay, **DES** eng ko'p tarqalganligi bilan ajralib turadi. **DES** algoritmi ma'lumotlarni shifrlashda ham, ularni autentifikatsiya qilishda ham juda qulaylik yaratadi. U 64 bitli ochiq matnni 64 bitli shifrlangan matnga aylantirishga imkon beradi. Lekin ma'lumot 64 raz ryad bilan cheklanib qolmaydi. Kriptografik masalalarni **DES** algoritmidan foydalanib yechishda 4 xil ish tartibi tashkil etilgan:

YeCB elektron kod kitobi (Electronic Code Book),
CBC blok shifrlarini ulash (Cipher Block Chaining),
CFB shifr matnlar bo'yicha teskari aloqa (Cipher Feed Back),
OFB chiqish signali bo'yicha teskari aloqa (Output Feed Back).

Shularning har biri bilan alohida-alohida tanishib chiqamiz. Elektron kod kitobi rejimida 64 bitli blok 8 baytli bo'laklarga bo'linadi. Har bir blok bitta kalitdan foydadalanishidan qat'i nazar shifrlash imkoniga ega.

Uning asosiy qulayligi – qo'llanishining oson tatbiq qilinishadir. Kamchiligi esa uning turg'unsizligidadir. Blok shifrlarini ulash rejimida ochiq ma'lumotli fayl 64 bitli bloklarga bo'linadi (12-rasm).



12-rasm. **Shifrlash va uni ochish usuli**

«Shifr bloklarining birlashuv» rejimi. Bu rejimda boshlang'ich fayl **M**(64ta bitli bloklarga (bo'laklarga ma'nosida) bo'linadi:

Mq M1 M2 M3„„Mn.

Birinchi blok **M1** 2 modulli 64 bitli boshlang'ich vektor bilan yig'iladi. Bu vektor o'zgarib turadi va maxfiy saqlanadi. Bunda kriptotahlil lug'at orqali amalga oshiriladi. Xatolar ko'payishiga yo'l qo'ymaslik, ushbu usulning afzalligini belgilaydi. Hosil bo'lgan yig'indi keyinchalik ma'lumot yuboruvchi va oluvchi uchun ma'lum bo'lgan **DES** kaliti bilan shifrlanadi.

Olingan 64 bitli shifr **S1** ikkili modul bilan matnning ikkinchi blok bilan yig'iladi. Natija shifrlanib, ikkinchi 64 bitli **S2** shifr hosil bo'ladi. Bunday holat to matnning barcha bloklari qayta ishlanguncha davom etadi. Shunday qilib, barcha iq1...n (bunda n bloklar soni) uchun shifr-

lash natijasi **Siq DES (Mi (Ci–1)**, C_0 – boshlang'ich vektorga teng boshlang'ich shifrning qiymati). Aynan shifrmatnning oxirgi 64 bitli bloki kalit maxfiyligining, boshlang'ich vektorning va ochiq matnning (uzunligi qanchalik bo'lishidan qat'i nazar) har bir bit funksiyasi bo'lib qoladi. Shifrmatnning bu bloki ma'lumotning autentifikatsiya kodi (**MAK**) deb ataladi. Bu kod maxfiy kalitda (11-rasm), boshlang'ich vektorga ega bo'lgan ma'lumot oluvchi tomonidan ma'lumot yuboruvchining takroriy operatsiyalari asosida osongina tekshirilishi mumkin. **M** bloki **Si–1** va **Ci** ning funksiyasi hisoblanadi. Shuning uchun ham ma'lumot yuborilganda boshlang'ich matnning faqatgina ikkita bloki yo'qolishi mumkin.

«Shifr bilan teskari bog'lanish» rejimi. Bu rejimda blok o'lchami 64 bitdan farq qilishi mumkin. Shifrlanishi kerak bo'lgan fayl **K** bit uzunlikdagi ketma-ket bloklar deb qabul qilinadi **(K q 1...64)**. U holda har qanday i_g1...n uchun shifrmatn bloki **Si_g Mi & Pi–1**(bunda **Pi–1** avval shifrlangan) blokning **K** yuqori bitlaridir.

DES algoritmining qo'llanish sohalari. **DES** algoritmining sanab o'tilgan barcha rejimlarining o'ziga xos yutuqlari va kamchiliklari mavjud bo'lib, ular tatbiq etish sohalariga juda bog'liqdir. Masalan, **YeSV** rejimi kalitlarni shifrlashda yaxshi natijalar bersa, **CFB** rejimi esa alohida olingan simvollarni shifrlashda asqotadi. **OFB** rejimi qo'llanilsa, sun'iy yo'ldosh orqali bog'lanishlar oson shifrlanadi.

SVS va **CFB** rejimlari ma'lumotlarni autentifikatsiya qilishda juda qulay hisoblanadi, ya'ni bosh **EHM** bilan terminal o'rtasida ma'lumotlar almashinuvida interaktiv shifrlashni amalga oshirishda qo'l keladi, amaliyotda kalitlarni avtomatik tarqatish jarayonida kalitlarni kriptografik shifrlashda qo'llaniladi, fayllarni shifrlashda, pochta orqali jo'natishda, sun'iy yo'ldosh bog'lanishlari va turli amaliy masalalarni jo'natishda juda qulaydir.

OEZ standarti **EHM** berilganlarni shifrlash va antishifrlashda ishlatilardi. Lekin uning qo'llanishi autentifikatsiya uchun ham umumlashtirilgan edi. Ma'lumotlarni avtomatik qayta ishlash jarayonida inson har bir ma'lumotga biror o'zgarish kiritilganmi, yo'qmi buni kuzata olmaydi. Shuning uchun oldindan ma'lumotlarning o'zgarishi to'g'risida biror xabar beradigan avtomatik vositaga ega bo'lishi kerak. Bunda xatoliklarni aniqlaydigan oddiy kodlar biror natija bermaydi.

Ammo **DES** algoritmi yordamida kriptografik yig'indi (summa)ni tashkil etish mumkin. Bu summa ma'lumotlarni tasodifiy va notasodifiy o'zgarishlardan saqlashi mumkin. Bu jarayon EHMdan olingan natijalar-

ni autentifikatsiya standartini ifodalaydi. Standartning mohiyati shundaki, berilgan ma'lumotlar **CFB** rejimi bilan shifrmatn ko'rinishga yoki **SVS** rejimi bilan blokli shifrlar bog'lanishiga ega ko'rinishdagi natijaviy shifr blokidan iborat bo'lgan ochiq matnning barcha razryadlari funksiyasiga ega bo'ladi.

Shundan keyin yuboriladigan ochiq matnli ma'lumot (soobshenie) hisoblab chiqilgan blokli shifrlar asosida jo'natiladi. Bir xil ma'lumotlarni *himoya qilishda ham shifrlash usulidan foydalanish, ham autentifikatsiya* usulini qo'llash mumkin. Autentifikatsiya algoritmini ham ochiq matnga, ham shifrlangan matnga tatbiq etish mumkin. Shifrlash va autentifikatsiyani kompyuter xotirasidagi axborot uchun ham qo'llash mumkin.

Ko'pgina kompyuterlarda parollarni qaytmas ko'rinishda xotirada saqlaydilar. Foydalanuvchi kompyuterga murojaat qilganda parolni kiritib uni shifrlaydi. Shifrlangan parol avvalgisi bilan taqqoslanadi. Bordi-yu ikkala shifrlangan parol bir xil bo'lib chiqsa, u holda foydalanuvchi kompyuter xizmatidan foydalana oladi, aks holda – yo'q!

Ba'zan shifrlangan parolni DES algoritmi bilan ochish imkoni paydo bo'ladi. Bunda algoritm kaliti parolga o'xshash bo'lib, ochiq matn esa foydalanuvchining aynan matni bo'ladi. **DES** algoritmining eng ko'p qo'llanadigan sohasi – bu bank va moliya yo'nalishi bo'lib, elektron to'lovlar tizimida ma'lumotlarni himoya qilishdir. Shuning uchun ham bank avtomatlarida, savdo tarmoqlarida, avtomatlashtirilgan moliya tarmoqlaridagi asosiy kompyuterlarda **DES** algoritmi juda keng qo'llanadi.

1.6. Axborotni himoyalashda shifrlashning blokli kombinatsiya usulini qo'llash

Shifrlash algoritmlari ichida blokli **DES** algoritmi bir qadar ishonchli hisoblanadi. Ushbu algoritmni 20 yil davomida kripto tahlil qilinib, turli kalitli variantlari ishlab chiqildi. **DES** kaliti 56 bit uzunlikka ega, shuning uchun uning 2 ning 56 darajasi qadar kalitlar tanlash im-

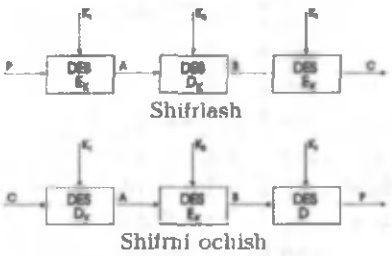
koniyati mavjud. Faraz qilsak, superkompyuter bir sekundda kalit tanlashning million variantini bajarish imkoniyatiga ega. U holda to'g'ri kalitni topish uchun 2285 yil kerak bo'lardi. Agar kalit uzunligi 128 bit bo'lsa bormi, u holda 10 ning 25 darajasidagi yil kerak bo'lardi. Savol tug'iladi: **DES algoritmi asosida uzunligi kattaroq algoritm yaratish mumkin emasmi?**

Yangi algoritm olish uchun blokli algoritmlar kombinatsiyasi asosida ish yuritish maqsadga muvofiq ekan. Shunday algoritmdan biri ochiq matn bloklarini ikkita kalit bilan ikki karra shifrlash usuli. Bunda avval ochiq matnning **R** blokini K1 kaliti bilan shifrlash (shifrmatn Yek1 **(R))**, keyinchalik uni **K2** kaliti bilan shifrlab, quyidagi kriptogrammani hosil qilamiz:

Sq Yek2 (Ek1 (R)).

Shifrdan chiqarish (расшифрование) teskari jarayon:

Rq Dk1 (Dk2 (C)).



13-rasm. **DES** algoritmi bilan shifrlash.

Shunday qilib, kalit qidirishning 2 ning n darajasi o'rniga 2 ning **2n** darajasida kalit qidirish imkoniyati paydo bo'ldi. **U.Tachmen** taklif etgan usulda esa ochiq matnning **R** blokini **K1** va **K2** kalitlar bilan 3 marta shifrlash hamda shifrni ochish jarayonlarini sodir etish mumkinligi qayd etilgan (13-rasm).

Shifrlash jarayoni: **Sq Yek1 (Dk2 (Ek1 (P)).** Bunda ochiq matnning **R** bloki avvalo **K1** kaliti bilan shifrlanadi, keyin **K2** kaliti bilan teskari amal, ya'ni shifrdan ozod qilinadi, so'ngra yana **K1** kalit bilan boshqatdan shifrlanadi. Bu rejim ba'zan **EDE** (encrypt-decrypt-encrypt) rejimi deb atashadi. Bu holda ***n*-bitli kalitli algoritm 2*n*-bitli kalitga ega** algoritmga aylanadi. Umuman olganda, algoritmlarni blok holida kombinatsiyalash usuli bilan yangi algoritmlarni yaratish mumkin yoki buni ko'psonli har xil kalitlar asosida shifrlash yo'li bilan ham amalga oshirsa bo'ladi.

Bundan tashqari, ikkita turli xil kalit yordamida uch karra shifrlash yo'li bilan ham yangi va yanada mukammal kombinatsiyalashgan **DES** algoritmlarini ham yaratish mumkin. Bu usul o'zining mustahkamligi va turg'unligi bilan ajralib turadi. Ushbu algoritm foydalanuvchilar uchun juda katta imkoniyatlar yaratib berdi va boshqa kriptosxemalarni jalb qilishga hojat qoldirmadi.

1.7. Axborotni RSA algoritmi bilan shifrlash

1978-yili **RSA** algoritmini uch avtor **R. Reyvest, A. Shamir**, va **A.Adleman**lar ishlab chiqishdi. **RSA** algoritmi o'zining mohiyati jihatidan birinchi takomillashgan algoritm bo'lib, u ochiq kalit bilan ishlab, bir vaqtning o'zida ikki rejimda, ya'ni ma'lumotlarni shifrlash va elek tron raqamli muhrlash masalalarini hal qila oladi. **RSA** kriptosistemada – K_o ochiq kalit, **Kc** – maxfiy kalit va kriptogramma **Sn**lar ko'psonli butun sonlarga tegishlidir:

$$Zn = (0, 1, 2, ..., N-1).$$

Bu yerda: **N** – modul, **Nq = P*Q** deb faraz qilinsa, **P** va **Q** tasodifiy oddiy katta sonlar bo'lib, muhofazalashni mukamallashtirish uchun P va **Q** larni bir xil uzunlikda olinadi va ular maxfiylashtiriladi. **Zn** to'plamida qo'shish va ayirish amallarini **N** moduli bilan bajarganda **N** – modulli arifmetikani tashkil etadi. Kv ochiq kalitni tasodifiy tarzda tanlab olganda quyidagi shartlarga rioya etish kerak bo'ladi:

$$1<K_v <= \varphi(N), NOD(K_v,\varphi(N)) = 1$$

$$\varphi(P,Q) = (P-1)(Q-1),$$

bu yerda: **N** – **Eyler funksiyasi** bo'lib, **1** va **N** intervalda bo'ladigan musbat va manfiy sonlarni ifodalaydi. **Kv** ochiq kaliti va **Eyler** algoritmi o'zaro sodda bog'lanishni ifodalaydi. **Evklid**ning kengaytirilgan algoritmidan foydalanib maxfiy kalitni ochish imkoniyati mavjud:

$$k_b * K_b \equiv 1(\mathrm{mod}_{\varphi}(N)),$$

yoki

$$k_b = K^{-1}{}_b(\mathrm{mod}(P-1)(Q-1)).$$

Demak, ochiq kalit **Kv** ni shifrlash uchun, K_i ni esa, aksincha shifrni ochish (расшифровка) uchun ishlatiladi. Shifrlashni o'zgartirish jarayonida **S** kriptogrammani olish uchun ochiq kalit **Kv** bilan **M** ma'lumot asosida quyidagi formulani hisoblash lozim:

$$C=E_{Kв}(M)=E_B(M)=M^{K}{}_B(\mathrm{mod}\ N).$$

Shifrni ochish texnologiyasi esa quyidagi formula bilan aniqlanadi:

$$D_в(E_в(M))=M.$$

Shunday qilib, biror ma'lumot jo'natuvchi shaxs kriptogramma

yaratsa, u holda 2 ta parametr bo'yicha himoya vositasini tashkil qila oladi:

♦ maxfiy kalit **Kv,**

♦ juft sonlar **(R,Q)** bo'lib, ularning ko'paytmasi **N** ning modulini aniqlaydi.

Faraz qilaylik, dushman tomonga **Kv, N** qiymatlari ma'lum bo'lsin. Agar dushman **N** sonini **P, Q** ko'paytuvchilarga ajrata olsa, u holda **(Q** uchlikning «yashirin yo'lini» topar edi. Buning uchun **Eyler** funksiyasini quyidagi formula bilan hisoblab, maxfiy kalit kb qiymatini topar edi, ammo bunday hisoblash jarayoni juda ko'p vaqtni oladi, chunki N sonini ko'paytuvchilarga ajratish ancha mushkul masala. Endi, **RSA** kriptosistemada shifrlash va shifrni ochish jarayoni bilan yaqindan tanishib chihamiz.

Faraz qilaylik, foydalanuvchi **A** ma'lumotni foydalanuvchi **V** ga **RSA** sistemasida shifrlangan holatda yubormoqchi. Yuqorida aytilganidek, **RSA** kriptosistemani tashkil etgan va uni oluvchi o'rtasida bo'ladigan jarayonni ko'rib chihamiz:

1. **V** foydalanuvchi 2 ta ixtiyoriy katta oddiy sonlar **R** va **Q** ni tanlab **N = P · Q** ni hisoblaydi. So'ngra **Eyler** funksiyasini topib:

$$\varphi=(P-1)(Q-1).$$

Kv ochiq kalitning tasodifiy qiymatini quyidagi shartlar bajarilgan holda aniqlaydi:

$$1<K_B<=\varphi(P, Q), NOD(K_B, \varphi(P, Q))=1.$$

So'ngra maxfiy kalit K_b ning qiymatini **Evklid**ning kengaytirilgan algoritmi bilan hisoblaydi:

$$k_b \equiv K^{-1}{}_B (\text{mod } \varphi(P,Q).$$

V foydalanuvchi himoya qilinmagan kanal orqali **A** foydalanuvchiga 2 ta son **(N, Kb)**ni yuboradi. Agar **A** foydalanuvchi **V** foydalanuvchiga **M** ma'lumot yubormoqchi bo'lsa, u holda quyidagicha ish yuritadi:

♦ **A** foydalanuvchi o'zining **M** ochiq matnli axborotini bloklarga **(M=0,1,2,.....N–1)** bo'ladi va keyin shifrlaydi:

$$S_i=M_i^K{}_b \text{ (mod N)}$$

so'ng kriptogrammalarni **V** foydalanuvchiga jo'natadi:

S1, S2, S3, ..., Si ...

V foydalanuvchi maxfiy k_b kalitini quyidagi formula bilan hisoblab topadi:

$$M_i = S_i^{k}{}_b \text{ (mod N)}.$$

Natijada **Mi** ketma-ketlikdagi sonlar qatori ko'rinishida M ma'lumot kelib chiqadi.

Xullas, **RSA** algoritmi bilan ish yuritganda oddiy sonlar to'plamidan foydalanish maqsadga muvofiq ekan. Hozirgi kunda **RSA** algoritmi bilan shifrlash va uni ochish uchun maxsus protsessorlar ishlab chiqilgan. Bunday protsessorlar juda yuqori integral sxemalarda yaratilgan. Lekin **DES** simmetrik kriptoalgoritmlari ushbu **RSA** kriptoalgoritmlaridan 1000 karra tezroq ishlaydi. Shuning uchun ham **RSA** algoritmlari amaliyotda kam qo'llanadi.

Yuqorida ta'kidlaganimizdek, simmetrik kriptotarmoqlarda boshqa shaxs bilan aloqa o'rnatishdan oldin unga shaxsan maxfiy kalitni tutqazish kerak. 1976-yildan qo'llanilayotgan nosimmetrik kriptotarmoqlarda ochiq kalitlarni qo'llanilishi bu muammoni ham yechib berdi va biznes faoliyatida ishlatilishi mumkin bo'lgan elektron tarmoqlarning shakllanishiga olib keldi.

Ochiq kalitlar bilan ishlaydigan kriptotarmoqlar ortga qaytmas bir taraflama funksiyalardan foydalanadi. Bunda oldindan berilgan **X** qiymatidan osonlik bilan **f(X)**ni hisoblash mumkin, ammo **f(X)**ning teskari funksiyasini hisoblab topish mumkin emas. Ortga qaytmas funksiyalarning tahlili asosan uch yo'nalishda olib boriladi:

1) diskret darajaga ko'tarish,
2) oddiy sonlarni ko'paytirish,
3) kombinatsiya usullari.

Rivest, Shamir, Adelman – ortga qaytmas funksiyalarda ochiq kalitlarni qo'llash usulini yaratdilar, u qisqacha **RSA**-nosimmetrik kriptosistema deb yuritila boshlandi. Yuqorida ta'kidlaganimizdek, bu usul oddiy muhrlarni elektron muhri bilan almashtirishga omil yaratdi. Quyida simmetrik (**DES**) va asimmmetrik (**RSA**) kriptotarmoqlarda mazkur algoritmning ish yuritish jarayonining tasnifi keltirilgan:

Kriptotarmoqlar algoritmlarining tasnifi

Tasnifi:	DES	RSA
Ishlash tezligi	tez	sekin
Qo'llaniladigan funksiya	o'zaro almashtirib joylash	darajaga ko'tarish
Eng oson amalga oshiriladigan kripto tahlil	butun kalit fazo maydonida almashtirish	modulni bo'lib o'rganish
Kripto tahlil uchun ketgan vaqt	yuz yillar	kalit murakkabligiga bog'liq
Kalit xili	simmetrik	asimmetrik

1.8. Axborotni shifrlashning gibrid usulini qo'llash

Ma'lumki, ochiq kalitli kriptosistemalarda yuqori darajada muhofaza qilish imkoniyati mavjud, ammo axborot uzatish jarayoni sekin kechadi. Simmetrik kriptosistemalarda esa maxfiy kalitning axborot uzatilayotgan davrda ochilib qolish ehtimoli bor. Shularni nazarda tutib, yangi bir gibrid usuli ishlab chiqilib, unda maxfiy kalit bilan shifrlaydigan simmetrik kriptosistema va ochiq kalit bilan shifrlaydigan asimmetrik kriptosistemalar yutuqlari mujassamlashgan. Masalan, **A** foydalanuvchi **M** axborotni gibrid (комбинированный) usuli bilan jo'natmoqchi bo'lsa, u holda quyidagicha ish yuritadi:

1. Simmetrik xususiyatga ega bo'lgan seansli kalit **Ks** yaratiladi.
2. Axborotni seansli kalit Ks bilan shifrlanadi.
3. Seansli kalit **Ksni** ochiq kalit **Kv** va o'zining maxfiy kaliti **Ka** bilan shifrlanadi.
4. Ochiq kanal orqali shifrlangan **M** axborotni **V** foydalanuvchiga shifrlangan seansli kalit bilan uzatish. **U** holda **V** foydalanuvchining ish yuritishi quyidagicha bo'ladi:

□ O'zining maxfiy kaliti **Kv** va **A** foydalanuvchining ochiq kaliti Ka bilan seansli kalit K_s ni shifrdan ochadi.

□ Seansli kalit **Ks** bilan **M** axborotning shifrini ochadi. Demak, ushbu gibrid (комбинированный) hisoblanmish usulda ham simmetrik, ham asimmetrik kriptosistemalar kalitlari ishtirok etadi. Quyidagi jadvalda simmetrik va asimmetrik kriptosistemalar kalitlari uzunligi berilgan:

Simmetrik kriptosistema kalitlari uzunligi, bit	Asimmetrik kriptosistema kalitlari uzunligi, bit
56	384
64	512
80	768
112	1792
128	2304

Gibrid usuli autentifikatsiya (yuborilgan axborotning haqiqiyligi) masalasini ham hal qiladi. Buning uchun **A** foydalanuvchi tomonidan yuborilgan ma'lumotni xeshlash funksiyasiga asoslangan holda va o'zining maxfiy **Ka** kaliti yordamida elektron muhr imzosi algoritmiga binoan jo'natiladigan ma'lumoti fayli oxiriga imzoni qo'yadi. **V** foydalanuvchi yuborilgan ma'lumotni o'qib, haqiqiyligiga raqamli imzosi tufayli ishonch hosil qiladi. Xullas, ushbu usul o'zining

racionalligi bilan va ochiq kalitli shifrlash kriptosistemasi kafolati asosida amaliyotda keng qo'llanilmoqda.

Nazorat uchun savollar

1. Axborot xavfsizligi haqida fikr bildiring.
2. Axborot xavfsizligi asosiy tushunchalari to'g'risida o'z fikrlaringizni bayon qiling.
3. Axborot xavfsizligini ta'minlovchi vositalar nima?
4. Ochiq va maxfiy kalit deganda nimani tushunasiz?
5. Axborot uzatishda shifrlash va shifrni ochish nima?
6. Shifrlashning qanday usullarini bilasiz, sanab ko'rsating va ularning o'ziga xos tomonlarini aytib bering.
7. An'anaviy va zamonaviy shifrlash usullarini qiyoslang.
8. Matnlarni oddiy shifrlash usullari haqida gapiring.
9. Murakkab almashtirish usulida shifrlash nima?
10. Axborot xavfsizligini ta'minlashning texnik vositalarini ifodalang.
11. Axborotlarni himoya qiluvchi dasturiy vositalarni aytib bering.
12. DES algoritmi haqida fikr bildiring.
13. RSA algoritmi haqida nimani bilasiz?
14. Kriptografiya, kriptotahlil deganda nimani tushunasiz?
15. Simmetrik va asimmetrik usullar umumiyligi va farqi nimada, misol ustida tushuntiring.
16. Shifrlashning gibrid usuli haqida gapiring.
17. Blokli (segmentlash yo'li bilan) algoritm bilan shifrlash qanday amalga oshiriladi?
18. DES algoritmining qo'llanish sohalari.
19. Shifrlash va autentifikatsiya masalalari haqida nima bilasiz?
20. Ochiq kalitli kriptosistema konsepsiyasi nima?
21. DES algoritmi strukturasini ifodalang.
22. Axborot xavfsizligida «kalit» vazifasini gapirib bering.
23. Shifr nima va uning qanday turlarini bilasiz?
24. Shifrni ochish deganda qanday ish yuritiladi?
25. Ochiq va maxfiy kalitlar nechun va ular qayerlarda, qachon ishlatiladi?

Testlar

1. Quyidagi qaysi qatorda axborotlarga ruxsatsiz kirishni himoyalash bo'yicha talablar himoyalanayotgan axborotlarning uchta asosiy xususiyatlariga erishishiga yo'naltirilganlik to'g'ri ko'rsatilgan?

A. maxfiylik, yaxlitlilik, tayyorlilik
B. muhimlik, tayyorlilik, maxfiylik
C. tegishlilik, aniqlik, yaxlitlik
D. ishonchlilik, tayyorlilik, muhimlik

2. Bankning boshqaruv tuzilmasi turli xil tashkil qilingan bo'lishi mumkin. Bu ko'proq nimaga bog'liq?

A. bankninmg kattaligiga

B. xizmatlar turining sonlari

C. mijozlarning va bank tomonidan bajarilayotgan operatsiyalarning soniga

D. A, B, C hammasi

3. BAATni texnik ta'minlash jarayonida bank texnologiyalari apparat vositalari arxitekturasi zamonaviy talablar asosida qurilishlari kerak. Ularga nimalar kiradi?

A. aloqaning turli-tuman telekomunikatsion vositalari kiradi

B. ko'p mashinali majmualar kiradi

C. «mijoz-server»ning arxitekturasidan foydalanish kiradi

D. A, B, C va mahalliy, mintaqaviy, global tezkor tarmoqlarni qo'llash, apparatli yechimlarni unifikatsiyalash kiradi.

4. Telekommunikatsion tizimlar bankka nima uchun kerak?

A. bankka avtomatlashtirishning eng muhim masalalarini bajarish uchun kerak

B. bisnes jarayonlarning o'zaro hamkorliklarining eng muvofiq unumdorligi u orqali amalga oshiriladi

C. sof texnikadan tortib bank xizmatini ko'rsatishning eng yuqori darajasidagi vazifagacha hal qilishga imkon beradi.

D. A, B, C barchasi

5. Banklarning amaliy faoliyatida axborotlarni himoyalash tadbirlari va usullarini qo'llash quyidagi mustaqil yo'nalishlarni o'z ichiga oladi. To'g'ri qatorni ko'rsating.

A. Axborotga ruxsatsiz kirishdan himoyalash

B. Axborotlarni aloqa tizimlarda himoyalash

C. A, B, D va maxfiy axborotlarni qo'shimcha elektron magnitli nurlanishlar va uzatish kanallaridan chiqib ketishini himoyalash.

D. Elektron hujjatlarning yuridik ahamiyatini himoyalash

6. Deshifrator nima?

A. sihratorni qayta ochadigan algoritm

B. yopiq kalit

C. ochiq kalit

D. kriptosistema

7. Simmetrik kriptosistemalarda axborotni uzatush qanday bo'ladi?

A. shifrovka, deshifrovka uchun alohida kalit

B. kriptosistemalarda *axborotni uzatuvchi ham, uni qabul etuvchi shaxs ham* bir xil turdagi simmetrik kalitlarga ega bo`ladilar

C. maxfiy kalitga ega bo'ladilar

D. A, B, C to'g'ri

8. Bunday kalit faqat konkret shaxsga ma'lum bo'lishi kerak. U ochiq kalit yordamida shifrlangan ma'lumotni ochish uchun ishlatiladi. Bu qaysi kalitga xos ta'rif?

A. ochiq kalit

B. maxfiy kalit

C. shaxsiy kalit

D. barcha variantlar to'g'ri

9. Bu *usulning asosini shifrlanishi kerak bo'lgan matn harflarini biror* alfavitdagisini boshqa alfavit harflari bilan almashtirish tashkil etadi. Agarda faqat bitta alfavit harflari bilan oldindan kelishib olingan holda o'zaro almashtirish ishlatilsa, u holda polibian kvadrat usuli deb yuritiladigan himoya vositasi vujudga keladi.

A. Oddiy almashtirish shifrlari

B. O'zaro almashtirish usuli

C. murakkab almashtirish usuli

D. shifrlashning Polibian usuli

10. Quyidagilarning qaysi biri shifrlashning murakkab usuliga kiradi

A. Gronsfeld usuli

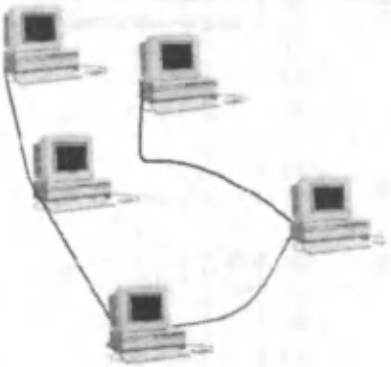
B. Bigramm usuli bilan shifrlash.

C. DES algoritmi bilan shifrlash

D. barchasi

2-bob. TARMOQLARDA TO‘LOVLARNI AMALGA OSHIRISHDA AXBOROT XAVFSIZLIGINI TA‘MINLASH

2.1. Kompyuter tizimlarida axborot xavfsizligi



Tabiiyki, hozirgi paytda jamiyatning axborotga bo‘lgan talabining keskin ortib borishi, jamlangan har turdagi axborotlarni himoyalash masalasini dolzarb qilib qo‘ymoqda. Darhaqiqat, axborot – bu inson ongida tashqi dunyoda kechayotgan jarayonlarning qayta ishlash natijalaridir. Ikki inson o`rtasidagi ma`lumotlar o‘zaro almashinuvi (yoki inson bilan mashina) jarayonida axborotni muhofaza qilish muammosi kelib chiqadi. Bu jarayonda shuni inobatga olish zarurki, har qanday axborot ham himoyalanishga muhtojlik tug‘dirmaydi, balki ma`lum qiymatga ega bo‘lgan axborotgina himoyalanishni talab etadi. Har qanday axborot faqat uning qiymatiga qarab emas, balki muhimligiga qarab bir necha turlarga bo`linadi:

– tashkilotning faoliyati uchun muhim va boshqa ma`lumotlar bilan almashtirib bo‘lmaydigan axborot, birinchi darajada himoyalanadigan axborot turidir,

– boshqa ma`lumotlar bilan almashtirib bo`ladigan, lekin bu jarayon katta pul mablag‘i va vaqt talab qiladigan axborotlar ikkinchi darajali axborotlardir,

– ba`zi turdagi ma`lumotlar tashkilot kelgusi faoliyatiga ta`siri yo`q deb topilgan bo`lsa, bunday turdagi axborotlar uchinchi darajali deb yuritiladi.

Axborotlarni qayta ishlaydigan avtomatlashtirilgan tizim (sistema)larda axborotlar himoyasi uchun asosan ikki xavf mavjuddir:

–tasodifiy xavflar,

– notasodifiy (aniq reja ostida axborot himoyasiga putur yetkazish) xavflar.

Notasodifiy xavf tug'dirish, asosan ruxsatsiz axborot bazasiga kirish va viruslardan foydalanish oqibatida amalga oshiriladi. Bunday xavf tug'dirish axborot yo'qolishiga yoki uni soxta axborotlar bilan o'zgartirishga olib keladi. Buning uchun axborot yo'qolishiga yoki uni o'zgartirilishiga olib keluvchi xavflar tabiatini, ularning kelib chiqish omillarini aniqlash va konkretlashtirish zarur.

Tasodifiy xavflar. Tajriba shuni ko'rsatadiki, har turdagi axborotlarni kompyuterga kiritish, saqlash, qayta ishlash va uzatish jarayonlarida jamlangan axborotlar turli tasodifiy ta'sirlarga uchraydi. Buning natijasida axborotni belgilovchi sonli kodlarda o'zgarishlar sodir bo'ladi. Masalan, 1 raqam bilan belgilangan kod 0 raqami bilan yoki aksincha, **0** raqami bilan belgilangan kod 1 raqami bilan almashinib qolishi mumkin. Bunday holatlarda kompyuter xotirasida mavjud maxsus nazorat tizimi o'zgarishlarni vaqtida aniqlab, o'zgartirishlar kiritmasa, katta hajmdagi axborot tubdan o'zgarishi yoki qisman o'zgarishi mumkin. Ayniqsa, axborotlarni avtomat qayta ishlash tizimi **(AAQIT)**larida saqlanayotgan axborotlarga tasodifiy xavf tug'diruvchi quyidagi sabablar mavjud:

– apparatdagi nosozliklar;

– tashqi muhitning aloqa tarmoqlariga ta'siri;

– tizimning bir bo'lagi bo'lmish foydalanuvchi mutaxassisning xatolari;

– mutaxassislarning tizim yaratishidagi sxematik va texnik xatolari;

– avariya holatlari va boshqa tasodifiy ta'sirlar.

Notasodifiy xavflar. Notasodifiy yoki biron-bir reja ostida hosil qilingan xavflar, asosan **AAQIT** tizimining bir qismi bo'lgan inson tomonidan amalga oshiriladi. Bunday xavflarni asosan ikki guruhga bo'lish mumkin:

□ ijtimoiy (sotsial);

□ texnik xarakterga xos bo'lgan xavflar.

Bizni ko'proq notasodifiy xavflar kelib chiqishi mumkin bo'lgan texnik xarakterga xos bo'lgan xavflar va ularni bartaraf etish usullari qiziqtiradi. Sotsial xarakterga xos bo'lgan xavflar ko'pchilik hollarda tashkiliy usullar bilan bartaraf etiladi. Demak, notasodifiy texnik xavflarni bartaraf etishda obyekt sifatida **AAQIT** tizimining eng muhim elementi bo'lmish kompyuter tanlab olinadi. Masalaning bunday qo'yilishi, jamlangan axborot bilan bevosita aloqador qonuniy shtat kanallarini konkretlashtiradi. Bunday qonuniy shtat kanallari quyidagilar:

– terminallar;
– tizim adminstratorining terminali;
– funksional nazorat operatorining terminali;
– axborotlarni qayd etish qurilmalari;
– axborotlarni hujjatlashtirish qurilmalari;
– programmalarni kompyuterga kiritish qurilmalari;
– axborotlarnini saqlash qurilmalari **(OZU, DZU)**;
– tashqi aloqa tarmoqlari.

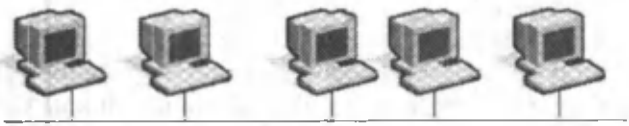
Notasodifiy xavf keltirib chiqaruvchi shaxs, yuqorida qayd etilgan qonuniy kanallardan tashqari, noqonuniy kanallardan ham foydalanishi mumkin. Bular asosan quyidagi holatlarda yuz beradi:

– foydalanuvchi shaxs qonuniy kanallardan maqsadga zid va o'ziga berilgan vakolatni buzgan hollar,
– shtat kanallaridan begona shaxs foydalanishi,
– apparaturada ichki montaj yoki tashqi kommunikatsiya ishlari olib borilishi.

2.2. Axborotlarni avtomatik qayta ishlash tizimi (AAQIT)ning axborot xavfsizligi

Yuqorida ta'kidlab o'tilgandek, **AAQIT** tizimida axborotlardan soxta yo'l bilan foydalanuvchi shaxslar tug'diradigan xavfni bartaraf etuvchi eng oddiy usullar quyidagilardir:

– foydalanuvchi shaxslar doirasini cheklash,
– axborotdan foydalanish doirasini cheklash,
– axborotni kriptografik o'zgartirish,
– foydalanuvchi shaxslar nazorati va hisobotini o'rnatish,
– axborot xavfsizligini ta'minlovchi har turdagi qonuniy choralarni qo'llash.



AAQIT tizimini texnik jihatdan murakkablashib borishi, albatta, foydalanuvchi shaxslarning ko'payishiga, turli noqonuniy aloqa tarmoqlarining paydo bo'lishiga olib kelishi mumkin. Bu esa, o'z navbatida, yuqorida aytib o'tilgan usullarni takomillashuviga va yangi usullarni joriy etilishiga olib keladi. Bularga birinchi o'rinda quyidagi usullar kiradi:

– apparaturada ro'y berayotgan noaniqliklarni hamda foydalanuvchi shaxs tomonidan qilingan xatolarni nazorat qiluvchi usullar;

– axborotning ishonchliligini oshirish usullari;

– avariya holatlarida axborotlarni muhofaza qilish;

– apparatning ichki, tashqi tarmoqlarini hamda texnologik boshqaruv organlarini nazorat qilish usullari;

– axborotdan foydalanishni chegaralash usullari;

– texnik va axborot saqlovchi qurilmalarni identifikatsiya qilish usullari.

AAQIT xavfsizligini saqlashda 2 ta usul bor:

• «fragmentar» yondoshuv ma'lum sharoitda aniq bo'lgan xavflarga qarshi kurash. Masalan, shifrlashning avtonom vosita va usullari, maxsus antivirus programmalar va boshqalar. Bunday usulning qulayligi shundaki, konkret xavfga yo'naltirilgan kurash usullari mavjud.

• kompleks usulda xavfga qarshi bir qator vosita va usullar birlashib ta'sir etadi. Bunda himoya muhitining yaratilishi **AAQIT** muhofazasini ma'lum darajada kafolatlaydi. Odatda, kompleks usulni tatbiq etish o'ta muhim muammolar yechimini hal qiladigan tashkilot va banklarda yoki katta hajmdagi axborotlarni qayta ishlash texnologyasini amalga oshirayotgan muassasalarda asqotadi.

AAQIT ni har qanday kutilmagan xavflardan himoya qilish tizimi quyidagi etaplardan iborat:

AAQIT uchun kutilishi mumkin bo'lgan xavflar tahlili ;

• himoya tizimini rejalashtirish;

• himoya tizimini ishga tushirish;

• himoya tiziminin kuzatish.

AAQIT uchun kutilgan xavflarni tahlil etish bosqichida asosan apparat va programma vositalari konfiguratsiyasida, yoki axborotlarni qayta ishlash jarayonida sodir bo'ladigan xavflarni oldindan ko'ra bilish zarur, buning uchun esa profilaktika jarayoni to'g'ri yo'lga qo'yilishi kerak. Himoya tizimini rejalashtirish bosqichida **AAQIT**ni muhofaza qiladigan umumlashgan xavfsizlik tizimini tashkil etish nazarda turadi.

Xullas, kompyuter tizimlari va tarmoqlari uchun xavfsizlikni ta'minlash usullari quyidagilarni o'z ichiga oladi:

• huquqiy (qonuniy),

• insonlarning imonli va e'tiqodli sog'lom muhiti,

• ma'muriy(tashkiliy usullar va vositalar),

• fizik (mexanik, elektronnomexanik qurilmalar, vositalar va moslamalar),

• apparat, programma vositalari (turli elektron qurilmalar va maxsus programmalar).

Sanab o'tilgan himoya omillarining ko'pchiligi xavfsizlikni ta'minlovchi kriptografik usullardan foydalanadilar.

Tarmoqlararo ekranlarda axborotni himoyalash uchun maxsus tizimni yaratishni davr taqozo qiladi. Bu tarmoq bir tarafdan foydalanuvchi shaxsni aniqlash tarmog'iga ega bo'lsa, ikkinchi tarafdan axborotdan foydalanish hajmini chegaralashi kerak. Albatta, gap Internet yoki lokal hisoblash tarmog'i ustida ketayotgani uchun yuqorida aytib o'tilgan tizim fayl-server yoki tarmoqdagi boshqa shaxsiy kompyuterlarda jamlangan axborotlarga chegaralangan holda yondashishni amalga oshiradi. Asosan, fayl-serverdagi axborot himoyasi quyidagi usullar bilan bajariladi:

– kirish paroli yordamida;

– yuqori bosqich jami ma'lumotlarni himoyalash;

– katalogda va fayl atributlari yordamida himoyalash.

Kirish paroli asosan hamma foydalanuvchilarda qo'llanilib, ular fayl-serverdan foydalanishlari uchun «ismlarini» va 6–8 simvoldan iborat parollarini bilishlari shart. Internet dan foydalanuvchi tashkilot tomonidan tarmoqqa kirishi uchun qo'shimcha talablar qo'yilishi mumkin. Masalan:

– tarmoqdan foydalanish vaqtini cheklash,

– tarmoqqa kirish maxsus adreslarni belgilash,

– tarmoqqa kiruvchi ishchi stansiyalar sonini cheklash,

– bir necha bor noto'g'ri parol bilan tarmoqqa kiruvchi shaxsga tarmoqqa kirish man etilishi.

Demak, mahalliy tarmoqning global tarmoqqa kirishi uchun tarmoq xavfsizligi administratori quyidagi masalalarni yechishi kerak:

– mahalliy tarmoq xavfsizligini himoya qilgan holda global tarmoq tomonidan mahalliy tarmoq bilan noqonuniy bog'lamasin;

– global tarmoqdan foydalanuvchilar uchun mahalliy tarmoq strukturasini va uning komponentalarini yashirin saqlash,

– muhofaza qilinayotgan tarmoqqa global tarmoqdan kirish va global tarmoqqa ushbu tarmoqdan kirish chegaralansin.

Xavfsizligi saqlanayotgan tarmoq axborot resurslariga global tarmoqdan foydalanuvchilarga kirish jiddiy chegaralanishi kerak. Jiddiy himoyaviy chegaralanish bir qator segmentlarda o'z ifodasini topadi:

– erkin kirish segmenti (masalan, **WWW** reklama serveri uchun mumkin);

– chegaralangan segmentli kirish(masalan, uzoq masofadan kirishni ta'minlaydigan sistema xodimlari uchun);

– yopiq segmentlar (masalan, mahalliy moliya tashkilotlari tarmoqlari uchun).

Mahalliy yoki korporativ tarmoqlarda xavfsizlikni ta'minlash uchun quyidagi tarmoqlararo ekranlar himoya sxemalari mavjud:

– tarmoqlararo ekran-filtrli marshrutizator;

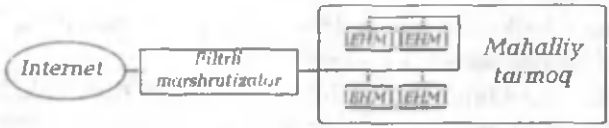
– ikki portli shlyuz asosidagi tarmoqlararo ekran;

– ekranlashgan shlyuz aosidagi tarmoqlararo ekran;

– ekranlangan tarmoqli tarmoqlararo ekran.

Endi, sanab o'tilgan ushbu himoya sxemalari bilan yaqindan tanishamiz.

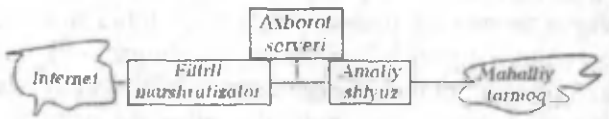
Filtrli marshrutizator. Filtrlangan paketlar asosida tuzilgan bunday tarmoqlararo ekran eng ko'p tarqalgan, u himoyadagi tarmoq bilan Internet tarmog'i orasiga joylashgan filtrli marshrutizatordan iborat (14-rasm):



14-rasm. **Filtrli marshrutizator asosidagi tarmoqlararo ekran**

Bunda himoyaga olingan tarmoqdagi kompyuterlar global tarmoqqa to'g'ridan to'g'ri kirish imkoniyatiga ega, ammo Internetdan kirish esa chegaralangan. Ko'pincha, eng xavfli bo'lgan xizmatlar – **X Windows, NIS, NFS** chegaralanadi.

Ikki portli shlyuz asosidagi tarmoqlararo ekran. Bunday ekran ikki o'ylli 2 tadan tarmoq interfeysiga ega xost-kompyuterdan iborat bo'ladi (15-rasm):



15-rasm. **Ikki portli shlyuz asosidagi tarmoqlararo ekran**

Amaliy shlyuzli bunday ekran himoyadagi tarmoq bilan Internet o'rtasidagi IP grafikni to'liq chegaralaydi. Amaliy shlyuzdagi server yordamchilargina faqat o'z vazifasini bajarishga mas'ul. Bu usulning himoya darajasi ancha yuksak, chunki muhofazadagi tarmoqqa marsh-

rutlar faqatgina tarmoqlararo ekranga ma'lum va tashqi sistemalardan yashiringan.

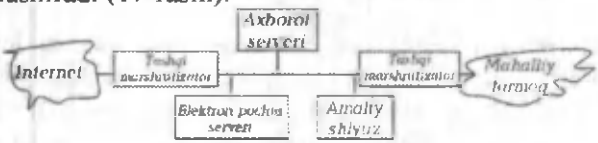
Ekranlashtirilgan shlyuz asosidagi tarmoqlararo ekran. Bu sxema bo'yicha ish tashkil etilganda, xavfsizlik muammosi yanada oydinlashadi. Chunki tarmoqlararo ekran filtrli marshrutizator bilan amaliy shlyuzni bog'laydi. Amaliy shlyuz xost-kompyuterda tashkil etiladi va faqat birgina tarmoq interfeysiga ega, ya'ni u ham bo'lsa, filtrli marshrutizatordir. Bu sxemada birinchi xavfsizlikni filtrli marshrutizator ta'minlaydi. Paketli filtrlash esa quyidagi usullarning biri orqali sodir bo'ladi (16-rasm):

16-rasm. **Paketli filtrlash**

1) ichki xost-kompyuterlar Internet tarmog'i tarkibidagi xost-kompyuterlar bilan bog'lanish uchun yo'l qidiradi.

2) ichki xost-kompyuterlar bilan bog'lanish man etiladi. Bu usullardan turli kombinatsiya uyushtirib har xil servislarga ish yuritish ruxsat etiladi. Bularning barchasi ichki tarmoqlar xavfsizligini ta'minlash siyosati bilan bog'liqdir. Masalan, **TELNET, FTR, SMTR** servislari uchun shunday imkoniyat mavjud. Ushbu xavfsizlikni ta'minlash sxemasining kamchiligi shundaki, agar hujum qiluvchi shaxs xost-kompyuterga kirib olsa, u holda ichki tarmoqdagi axborotlar himoyasi xavf ostida qoladi.

Tarmoqosti tarmoqlararo ekran aslida ekranlashgan shlyuzli tarmoqlararo ekran sxemasiga asoslanib, uning imkoniyatlari kengaytirilgan varianti, deb hisoblanadi. Bunda 2 ta marshrutizator xizmatidan foydalanish ko'zda tutilgan. Tashqi marshrutizator Internet tarmog'i bilan ekranlanadigan tarmoqosti orasiga joylashgan. Ichki marshrutizator esa ekranlanadigan tarmoqosti uchun himoyaga olingan ichki tarmoq o'rtasida aloqa o'rnatadi. Ekranlanadigan tarmoqosti amaliy shlyuzga ega bo'lib, axborot resurslari va nazorat talab qiladigan boshqa sistemalarni ham ishga tushiradi (17-rasm):



17-rasm. **Tashqi marshrutizatorli ekran**

Tashqi marshrutizator Internet tarmog'idan ichki tarmoq bilan ekranlanadigan tarmoqostini muhofaza qiladi. Trafiklarni yuborishni quyidagicha hal etadi:

– Internet obyektlaridan amaliy shlyuzga trafik yuborishni ta'minlaydi;

– amaliy shlyuzdan Internet tarmog'iga trafik yuborishni bajaradi.

– elektron pochta trafigini Internetdan elektron pochta serveriga yuboradi.

– elektron pochta trafigini elektron pochta serveridan Internet tarmog'iga yuboradi.

FTR, Gopher trafiklarini Internetdan axborot serveriga yuboradi.

Qolgan trafiklarga ruxsat etilmaydi.

Tashqi marshrutizator Internetdan ichki tarmoqlar sistemasiga kirishni man etadi va barcha trafiklar yo'lini to'sadi. Bu marshrutizator boshqa qaydnomalar yo'lini ham to'sib qo'yadi (ichki tarmoq xost-kompyuterlariga yo'l yo'q hisobi va aksincha).

Ichki marshrutizator ichki tarmoqni Internetdan va ekranlanadigan tarmoqostidan himoya qiladi. Ichki marshrutizator asosan paketli filtratsiyani amalga oshiradi. Bu marshrutizator ichki tarmoqlar sistemasiga va undan trafik jo'natishni quyidagi qoidalarga asoslanib boshqaradi:

□ amaliy shlyuzdan tarmoq sistemalariga trafik yuboradi;

□ tarmoq sistemalaridan amaliy shlyuzga trafikni uzatadi;

□ elektron pochta serveridan elektron pochta trafigini tarmoq sistemalariga jo'natadi;

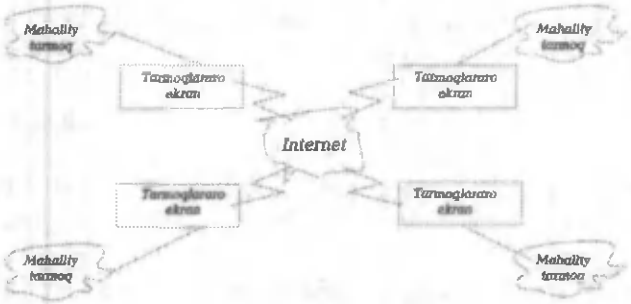
□ elektron pochta trafigini tarmoq sistemalaridan elektron pochta serveriga yuboradi;

□ **FTR, Gopher** trafiklarini tarmoq sistemasidan axborot serveriga jo'natadi.

Boshqa trafiklarni jo'natish man etiladi.

Demak, ichki tarmoqqa kirish uchun 2 ta marshrutizatordan o'tish talab etiladi. Buzg'unchi birinchi filtrdan o'tib, xavf tug'dirsa ham, ikkinchi marshrutizatordan o'tish yo'li kesiladi, hech bo'lmaganda chegaralanadi. Shunday qilib, ichki tarmoq sistemalari Internetdan keladigan xavfdan xolis bo'ladi va aksincha. Amaliy shlyuz kuchli autentifikatsiya programmasiga egadir va shuni ishga soladi.

Virtual korporativ tarmoqlarga tarmoqlararo ekran tatbiqi. Bir qator tarmoqlararo ekranlar vertual korporativ tarmoqlar tashkil etishda ishtirok etadi. Global tarmoqqa ulangan birnecha mahalliy tarmoqlar bitta virtual tarmoqqa birlashishi mumkin (18-rasm).



18-rasm. **Virtual tarmoq ekrani**

Bunda mahalliy tarmoqlar o'rtasida foydalanuvchilar uchun axborot almashuv shaffof holatda vujudga keladi. Uzatilayotgan axborot ishonchliligi va butunliligi saqlangan holda shifrlash va shifrdan ochish texnologiyasi buzilmagan bo'lishi shart. Shifrlash jarayonida nafaqat paket tarkibidagi ma`lumotlar, hattoki katta va kichik sarlavhalarigacha shifrlanadi.

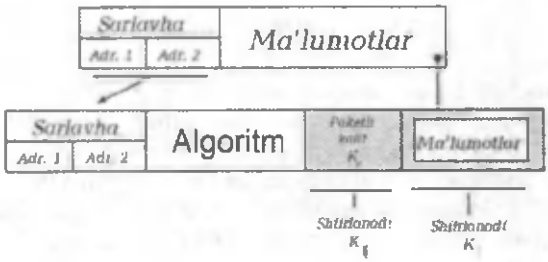
2.3. Axborotlarni dasturiy muhofaza qilish usuli

Internet tarmoqlarida axborotlarni muhofaza qilish uchun programmalash usullaridan keng foydalaniladi. Internet tarmog'ini taraqqiy ettirish chog'ida ko'plab himoyalangan tarmoq qaydnomalari tashkil etildi. Internet tarmog'ida axborotni himoyalashni programmalashtilgan usullariga kripto qaydnomalarni kiritish mumkin. Muhofazalangan tarmoq qaydnomalariga maxfiy kalitli simmetrik kriptografiyani yoki ochiq kalitli asimmetrik kriptografiyani kiritganlar. Hozir eng qulay va samarali muhofaza qiladigan **kriptoqaydnoma**larga **SKIP** texnologiyasini va tarmoq bog'lanishini himoya qiladigan **SSL qaydnoma**ni keltirish mumkin. **SKIP** (Secure Key Internet Protocol) texnologiyasi **IP** paket grafikasini standart muhofaza qiladigan jarayon bo'lib, tarmoq orqali yuboriladigan ma'lumotlarni himoya qilishni amalga oshiradi. Shu texnologiya bo'yicha muhofaza qilishning 2 ta usuli mavjud:

– **IP** paket bloklaridagi axborotlarni shifrlaydi.

– **SKIP** paketga **IP** paketni joylashtirish(inkapsulyatsiya).

IP paket bloklaridagi axborotlarni shifrlash quyidagi rasmda keltirilgan bo'lib, bunda simmetrik kriptografiya usuli bilan shifrlashni faqat IP paket ma'lumotlariga tatbiq etiladi. Uning sarlavhasi ochiq qoladi va paket marshruti haqiqiy adreslar bo'yicha bo'ladi (19-rasm):

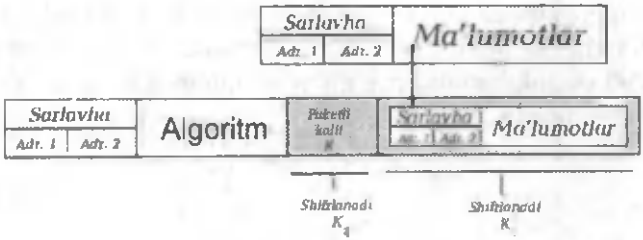


19-rasm. **Diffi-Xelman usuli**

Yopiq kalit **Kij** tarmoqning **I** va **J** tugunlarida bo'lib, ularni hisoblash **Diffi-Xelman** usullari orqali amalga oshadi.

IP paketini **SKIP paketiga** joylashtirish quyidagicha (20-rasm).

SKIP paketi tashqi ko'rinishi jihatdan xuddi IP paketiga o'xshash. **SKIP** paketi ma'lumotlari maydonida **IP** paketi shifrlangan holda joylashadi. Bu holda avvalgi sarlavhasi o'rnida boshqa adreslar bo'lishi mumkin. **SKIP** paketining bunday strukturasi Internet tarmoqlaridagi ixtiyoriy xost-kompyuterga ma'lumotlarni hech qanday qarshiliksiz jo'natishi mumkin. Ushbu holda tarmoqlararo adreslash jarayoni odatdagi **IP** sarlavhasi bo'yicha amalga oshiriladi.



20-rasm. **Inkapsulyatsiya usuli**

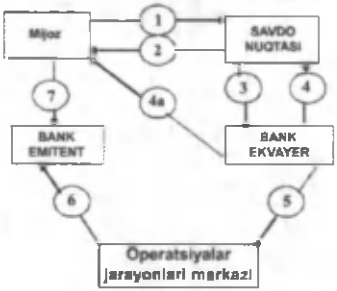
SSL (Secure Socket Layer) bog'lanishli himoyaning universal **qaydnoma OSI** etalon modelining seansi darajasida ish yuritadi. **SSL qaydnoma** Netscape kompaniyasi tomonidan yaratilgan bo'lib, ochiq kalitli kriptografiya bilan ishlaydi. Haqiqatan ham bu **qaydnoma** universal bo'lib, amaliyotda ishlatilayotgan turli **qaydnoma**lar (FTP, **TELNET, SMTP, DNS)** bilan ishlay oladi. Shuning uchun ham undan turli taniqli kompaniyalar **(IBM, Digital Eguipment Corporation, Microsoft Corporation, Motorola, Novell Inc., Sun MicroSystems, MasterCard International Inc.)** o'z ish faoliyatida foydalanadilar.

Nazorat uchun savollar

1. Kompyuter tizimlarida axborot xavfsizligi nima?
2. Tasodifiy va notasodifiy xavflarni sanab bering.
3. Kompyuter tizimlarida mavjud xavflarni ifodalang.
4. **AAQIT**da axborot muhofazasi qanday amalga oshiriladi?
5. Kompyuter tarmoqlarida axborotlarni qanday muhofaza qilinadi?
6. Tarmoqlararo axborot almashuvida xavfsizlik qaysi usullar bilan amalga oshiriladi?
7. Filtrli marshrutizator nima?
8. Amaliy shlyuz texnologiyasi haqida fikr bildiring.
9. Virtual korporativ tarmoq deganda nimani tushunasiz va unda axborot muhofazasi qanday amalga oshiriladi?
10. Dasturiy muhofaza usullaridan qay birini bilasiz?
10. **SKIP** texnologiyasi qanday ish yuritadi?
12. **SSL** qaydnomasi bilan qayerda va qachon foydalanish afzalroq?

2.4. Elektron to'lov tizimlarida xavfsizlikni ta'minlash

Hozirgi zamon bank tizimlarini, savdo-to'lov vositalarini kompyuter xizmatidan foydalanmay hal etish mushkul bo'lib qoldi. Ayniqsa, banklararo ma'lumotlar ayirboshlash jarayonida kerakli axborotlarni muhofaza qilgan holda jo'natish davr talabi bo'lib qolmoqda. To'lov vositalari sifatida esa plastik kartalardan foydalanish kun tartibiga qo'yilgan. Chunki plastik kartalar eng qulay va himoyalangan to'lov vositasiga aylanib bormoqda.



21-rasm. **Elektron to'lovni amalga oshirish jarayoni**

Plastik karta – bu shaxsiylashtirilgan to'lov vositasi bo'lib, undan foydalanuvchiga pulsiz tovar-xaridor muomulasini vujudga keltiradigan va banklar tizimidan avtomatik ravishda foydalanish imkoniyatini beradigan juda ixcham va qulay bir yangi axborot texnologiyasining ijobiy

natijasidir. To'lov tizimining asosini shartnomaga binoan tuzilgan banklar assotsiatsiyasi tashkil etadi. Bundan tashqari, elektron to'lov tizimiga savdo va servis korxonalari ham kiradi. To'lov tizimining normal ish yuritishi uchun maxsus tashkilotlar ham tuzilgan bo'lib, bular kartalarning texnik xizmatini o'taydi. Hozirgi kunda eng katta ahamiyatga molik to'lov tizimining avtomatlashgan savdo sistemasi **POS terminallar** va bankomat hisoblanadi.

Shuni qayd etish lozimki, yaqin-yaqingacha Internet tizimi asosan pochta buyurtmalari bilan ish yuritish va fayllarni jo'natish bilan shug'ullanardi. Internet infrastrukturasi ham o'zgarib bormoqda, ya'ni axborotlarning barcha turlari bo'yicha kerakli ma'lumot berishga qodir. Masalan, dunyo kutubxonalariga o'tirgan joyingizda kirish, ilmiy va huquqiy sohadagi ma'lumotlar bazasidan unumli foydalanish, davlat va kommersiya tashkilotlari axborotlaridan tez va soz foydalana bilish, birja va bank tizimlari o'rtasida axborot almashuv jarayonlari va hokazo. Ixtiyoriy tashkilot o'z axborotlarini butun dunyo bo'ylab tarqatishi sir emas.

Ayniqsa, savdo sohasidagi ish yuritishlar juda dolzarb. Internetning tezkor – operativ rejimida savdo qilish butun dunyo bozorlarini o'ziga jalb etmoqda. Endi an'anaviy bozorlar o'rnini ofis va uy egallashi mumkin.

Buning uchun axborot xavfsizligini saqlash asosiy hal qilinishi kerak bo'lgan masalalardan hisoblanadi. Shuning uchun ushbu xizmatni o'taydigan texnik va dasturiy vositalar hamda ish yuritish vositasi bo'lgan kartalarni shaxsiylashtirish, elektron imzolar qo'yish texnologiyasi bilan yaqindan tanishishimiz lozim.

Darhaqiqat, elektron to'lov vositalaridan foydalanganda elektron imzoni yaratish shart. Chunki shifrlash texnologiyasi bilan shug'ullangan vaqtimizda, albatta, uni kafolatlash uchun imzo qo'yiladi. Xo'sh, elektron imzo nima va u qanday yaratiladi, degan savolga javob berishga harakat qilaylik.

Ma'lumki, elektron imzo algoritmlarida va asimmetrik shifrlash jarayonida maxfiy va ochiq kalitlar ishlatiladi. Maxfiy kalit tasodifiy usulda olinishi ham mumkin, ochiq kalit esa maxfiy kalit algoritmidan shunday hisoblab olinadiki, ikkinchisidan birinchisini topish mumkin bo'lmasin. Faraz qilaylik, siz o'z do'stingizga biror ma'lumot yubormoqchisiz. Buning uchun quyidagi nazariy jarayonni o'tash lozim:

• Avval elektron imzo kalitlarini yarating. Xuddi shifrlash jarayonida bo'lganidek, bu kalitlar fayllarda saqlanadi. Har biringiz o'z maxfiy va ochiq kalitingizga ega bo'lishingiz lozim.

• Maxfiy kalitlarni o'zingizda qoldirib, ochiq kalitlarni almashtiring.

• Maxfiy kalitingiz bilan do'stingizga xat yozing va uni o'z imzo-yingiz bilan jo'nating.

Elektron imzo ketma-ket yozilgan raqamlardan iborat bo'ladi. Tashqaridan qaraganda ular tartibsiz yozilgandek, ammo ular quyidagi formula yordamida hisoblanadi:

$$f(M, k_S),$$

bu yerda **M** – xat matni, k_s – maxfiy kalit.

• Elektron imzo bilan jo'natilgan xatni olgach, do'stingiz sizning ochiq kalitingiz bilan xatning haqiqiyligini tekshiradi. Bordi-yu xatni jo'natish arafasida biron-bir kichik o'zgarishlar kiritgan bo'lsangiz, u holda, uni darrov aniqlash mumkin bo'ladi. Maxfiy kalitni o'ta maxfiy-lashtirish kerak, aks holda uni tezda bilib olib, sizning imzoyingiz o'z-lashtirilishi mumkin. Elektron imzoning yanada muhim xususiyati jo'-natiladigan ma'lumot muallifligini saqlashdir. Odatda, kalitlar fayliga shaxsiy kalitingizdan tashqari qo'shimcha ma'lumotlar: familiyangiz, ismingiz, nasabingiz, ish joyingiz, imzoyingiz qo'yilgan vaqt va boshqa ma'lumotlar ham yoziladi. Elektron imzo tekshirilganda kompyuter ek-raniga quyidagi ma'lumotlar chiqadi:

Fayl imzosi **compromat.bmp verna** (Muallif:Azizov F.M.)

Har qanday ochiq kalitli kriptografik algoritm kabi elektron imzoni turli adresatlarga Internet orqali ochiq kalit vositasida yuborish mumkin. Ammo bu jarayonga xaker aralashib qolsa bormi, ishlar butunlay o'z-gacha tus oladi. Bu holda xuddi asimmetrik kalitli shifrlashda bo'l-ganidek, ochiq kalitni o'zlashtirish hollari ro'y berishi mumkin. Natijada butunlay o'zgacha holat sodir bo'ladi, ya'ni faraz qiling, siz o'z do's-tingiz bilan ochiq kalit orqali axborot almashmoqchi bo'ldingiz. Axbo-rotni jo'natish jarayonida qandaydir xaker paydo bo'lib, u siz yuborgan to'g'ri ochiq kalitni ushlab oladi. Do'stingiz siz yuborgan ushbu ochiq kalitni olib ham ulgurmaydi. Xaker to'g'ri ochiq kalitdan Sizning ismi-nasabingizni bilib olib, yangitdan ikki juft kalit yaratib (ochiq va maxfiy kalitlar), u yerga sizning adresingiz bilan ma'lumot jo'natadi (maxfiy kalitini o'zida qoldiradida, so'ng ochiq kalit bilan sizning nomingizdan jo'natadi). Toki yolg'on ochilmaguncha, xaker shu yo'l bilan do'stingiz-ga xatlar jo'nataveradi. Agarda ochiq kalitlar sertifikatsiya qilingan bo'l-sa, u holda ochiq kalitni bunday o'zlashtirishlardan saqlash mumkin. Hozirgi kunda elektron imzolarni tashkil etishning turli usullari mavjud, jumladan:

1. Elektron imzo standarti **GOST R34.10-94** mavjud bo'lib, u sim-

metrik shifrlash standarti **GOST 28147-89** kabi Rossiyaning kommersiya ishlarida keng ishlatiladi.

2. 2002-yil 1-iyulidan boshlab harakatga tushgan yangi standart **GOST Z34.10-2001** ham eng ko'p ishlatiladi.

Eng ko'p tarqalgan elektron imzo algoritmlari:

1. RSA (Rivest Shamir Adleman).
2. El-Gamalya
3. DSA (Digital Signature Algorithm).

Ushbu sanab o'tilgan algoritmlarda xesh funksiyasi ishlatiladi. *Uning matematik ifodalanishi bilan tanishib chihamiz.*

Xesh funksiya. Yuqorida keltirilgan elektron imzo formulasi to'liq holda quyidagicha ifodalanadi:

$$S = f(h(M), k_S),$$

bunda h(M) – xesh funksiya.

Ma'lumki, matnli axborot turlicha bo'ladi – oddiy to'ldirilmagan sahifadan tortib, turli jadvallarga, rasmlarga ega sahifalarni o'z ichiga olishi mumkin. Bu holda xesh funksiya imkoniyatidan foydalanishga to'g'ri keladi. Xesh funksiya ixtiyoriy hajmdagi ma'lumotni standart o'lchovdagi raqamlar ketma-ketligi shaklida hisoblab beradi. Odatda, xesh funksiya quyidagi xususiyatlarga ega:

□ Xesh funksiya bir yo'nalishga ega. Shuning uchun ham **h(M)**ni aniqlagan holda yuborilgan ma'lumot Mni hisoblab bo'lmaydi, yoki har bir **M** ma'lumot uchun shunday M' ni tanlab quyidagi shart bajariladi deb bo'lmaydi, ya'ni **h(M)qh(M*).**

□ h(M) ma'lumoti o'ziga aynan bo'lishi shart va bu funksiya o'zgargandagina uning yuboradigan ma'lumoti ham o'zgaradi. **h(M)** nafaqat ma'lumot jo'natish jarayonida, balki autentifikatsiya (ma'lumotning haqiqiyligini aniqlash) jarayonida ham ishlatiladi. **h(M)** standartlari – MD (Message Digest) va **GOST Z34.11-94.**

Odatda, shifrlash jarayoni ma'lumotlarni bilib qolishdan saqlasa, elektron imzo uni o'zlashtirishdan himoya qiladi. Modomiki shunday ekan, axborotlarni *muhofaza qilish jarayonida ularning ikkalasidan* foydalansak, maqsadga muvofiq ish bo'lardi. Buning uchun quyidagilar bajarilishi shart:

1. Ma'lumotlarni jo'natish jarayoni arafasida asimmetrik tarzda shifrlash va elektron imzo uchun ikki xil kalit (ochiq, maxfiy) yaratilishi lozim. Ochiq kalitlari bilan foydalanuvchilar o'zaro muloqotga kirishsa, keyinchalik biri ikkinchisiga o'z ma'lumotlarini elektron imzosi (maxfiy kalit orqali) bilan yuborish uchun tayyorgarlik ko'radilar.

2. Foydalanuvchilardan biri simmetrik shifrlashni amalga oshirishda ixtiyoriy **K** kalitlar generatsiyasini hosil qilib, ma'lumotlarni jo'natadi.

3. Yuborilgan ma'lumotning shifrini ochish uchun **K** kalit asimmetrik shifrlash jarayoni ochiq kaliti bilan shifrlanadi va uni ham ma'lumotga qo'shib jo'natadi.

4. Ikkinchi foydalanuvchi shifrlangan ma'lumotni olgach, uni o'zining maxfiy asimmetrik shifrlash kaliti bilan **K** kalit shifrini ochadi. Undan keyingina yuborilgan xatning shifrini ochishga muyassar bo'ladi.

5. Oxirida birinchi foydalanuvchining ochiq kaliti bilan uning elektron imzosi haqqoniyligini tekshirib ko'radi.

Simmetrik shifrlash jarayoni va o'zining elektron imzosini ham bir varakayiga tekshirib ko'rish imkoniyatini beradigan **Diffi-Xellman** algoritmi bilan elektron imzoning ham ochiq, ham maxfiy kalitini yaratish mumkin. Bu algoritmning mohiyati quyidagicha: **GOST R34.10**-94 standartdagi elektron imzo ochiq kaliti maxfiy kalitdan quyidagi formula bilan hisoblanadi:

$$K_p = a^k \text{ s mod p},$$

bunda: **a, p** – oldindan ma'lum bo'lgan juda katta sonlar (masalan, 21024).

Faraz qilaylik, **A** va **B** foydalanuvchilar mavjud bo'lib, ular o'zlarining maxfiy kalitlarini generatsiya qilib, ochiq kalitni quyidagicha aniqlaydilar:

$$K_{p1} = a^k S1 \text{ mod p},$$
$$K_{p2} = a^k S2 \text{ mod p}.$$

Ochiq kalitlar bilan almashishgandan keyin har ikkalasida ham ikkitadan kalit hosil bo'ldi: o'zining maxfiy kaliti va o'zganing ochiq kaliti, ya'ni K_sA va K_pA hamda K_sB va K_pA Bu holda umumiy kalit quyidagi formula bilan ifodalanadi:

$$Kc = (K_{p1})^k S2 = (a^k S1)^k S2 \text{ modp} = (a^k S2)^k S1 \text{ mod p} = (K_{p2})^k S1$$

Demak, juft bog'lanish kaliti **Ks** ni faqat foydalanuvchilar hisoblay oladi. Bordi-yu, ushbu axborot xaker qo'liga tushib qolsa, u bu jumboqni darrovgina yecha olmaydi. **Ks** kalit orqali esa **GOST 28147-89** standart orqali yuborilgan ma`lumotni tezgina simmetrik shifrlash mumkin bo'ladi.

Elektron imzo algoritmi. Bugungi kunda elektron raqamli imzo tushunchasi odatiy bo'lib qoldi, chunki turli bank xodimlari ushbu tushunchadan keng foydalana boshladilar. Sababi: bank tizimidagi hujjatlar qog'ozli ko'rinishdan elektron hujjat ko'rinishida samarali ishlatila boshlandi.

Bankning elektron to'lov hujjatlarida imzoning haqiqiyligini aniqlash juda zarur bo'lib qoladi. Ana shu vaqtlarda kriptografiya imkoniyatlariga asoslangan elektron raqamli imzoni yaratishga keng yo'l ochildi.

Imzoning haqiqiyligi (autentifikatsiya)ni aniqlash deganda, nimani tushunamiz? Avvalo, ma'lumot haqiqiy egasi tomonidan biror o'zgarishsiz yuborilganmi yoki yo'qmi shuni aniqlash. so'ngra imzo o'z egasinikimi yoki yo'qmi?

Odatda, autentifikatsiya jarayoni kriptografiya usullari zaminida maxsus algoritm va programmalar yaratilib, ular orqali aniqlanadi. Avvalo, elektron hujjatlarda sodir bo'ladigan xavf masalasini aniqlash kerak. Elektron hujjatlar ayirboshlash jarayonida quyidagi ko'rinishdagi xavfli vaziyatlar bo'lishi mumkin:

□ **Inkor qilish**: **A** abonent **B** abonentga yuborgan hujjatini yo'q deb, inkor etadi (aslida hujjatni yuborgan bo'ladi).

□ **Modifikatsiya**: **B** abonent hujjatni o'zgartirib, shu holatda **A** abonentdan qabul qilganini tasdiqlamoqchi bo'ladi.

□ **Podmena (almashtirib qo'yish)**: B abonent o'zi hujjat tayyorlab uni A abonentdan olganligini qayd etadi.

□ **Faol ushlab olish(perexvat)**: tarmoqqa ulangan buzg'unchi hujjatlarni faol ravishda ushlab olib, ularni yoki fayllarni o'zgartirib yuboradi.

□ **«Maskarad»**: **C** abonent **A** abonent nomidan hujjatlarni jo'natadi.

□ **Takror: C** abonent **A** abonent tomonidan **B** abonentga jo'natilgan hujjatni qayta **A** abonentga jo'natadi.

Yuqorida sanab o'tilgan ushbu xavfli xatti-harakatlar bank ishlarini ancha tashvishli vaziyatga olib keladi. Bundan tashqari, bunday nojo'ya xavflar bank xodimlarida kompyuter texnologiyasiga nisbatan ishonchni yo'qotadi. Shuning uchun ham sodir bo'ladigan bunday xavflarni yo'qotish uchun kriptografiya usullaridan foydalanib ish yuritishga to'g'ri keladi. Ayniqsa, 2 ta kalitli kriptografik usullar bu holatlarda juda samarali ish beradi.

Bu holda har bir abonent hujjatni uzatish jarayonida o'z imzosining maxfiy kalitiga ega bo'ladi, ochiq kaliti esa boshqa abonentlarga ma'lum. Ochiq kalitlar maxfiy kalitni ochish mumkin bo'ladigan holatlar ifodasidan iborat bo'lib, hechqachon maxfiy kalitni aynan ocha olmaydi. Hujjatni uzatuvchi abonent shaxsan o'zi maxfiy kalitga javobgar hisoblanadi va undan boshqa hech kim uning imzosini tiklay olmaydi. Elektron raqamli imzo algoritmlarining matematik sxemasi bir yo'nali-

shli funksiyalar xossalariga asoslangan bo'lib, quyidagicha ish yuritadi: hujjat jo'natuvchi har bir abonent qabul qiluvchi abonentga elektron imzo E(o)ni tekshirishni yuklaydi. O'zining original imzosini maxfiy holda saqlaydi. Bunday amallar bajarilishi uchun quyidagi xususiyatlarga ega bo'lishi lozim:

1) **D |E(o)| q X** har qanday mavjud **X** uchun. **Ye** va **D** lar oson hisoblanadi. **Ye** ni ma'lum **D** orqali aniqlash mushkul jarayon. Amalda elektron raqamli imzoni aniqlash sxemasida x ni hisoblash o'rnida uning xesh funksiyasi **h(o)**ni aniqlanadi.

Elektron raqamli imzoni hisoblash algoritmlaridan eng ko'p tarqalgan sxemasi quyidagilardan iborat:

□ **RSA** – (R.L.Rivest, A. Shamir, L. Adleman) avtorlar familiyasining birinchi harflari olingan.

□ **OSS** – (H.Ong, C.P. Schnorr, A. Shamir) avtorlar familiyasi birinchi harflaridan tashkil topgan.

□ **El-Gamalya** (T. El-Gamal).

□ **Rabina (M.Rabin)**.

□ **Okamoto Siraisi (T.Okamoto, A. Shiraishi)**.

□ **Macumoto Imai (T. Matsumoto, H.Imai)** va elliptik egri chiziqlardan iborat sxemalar.

RSA, Rabina, El-Gamalya sxemalarida imzolarni o'zgartirganligini topish faktorlash va diskret logarifmlash usullari bilan amalga oshiriladi. Ammo bu jarayonni hisoblash vaqtida ancha qiyinchiliklarga duchor bo'lish mumkin. Hisoblash jarayoni eng oson kechadigan usullarga **A.A.Grushon**ing original sxemasini keltirish mumkin. Bunda hisoblash algoritmi chiziqli bo'lmagan Bul algebrasi asosidagi tenglamalar sistemasini o'z ichiga oladi. Shunga qaramasdan, eng ko'p qo'llaniladigan algoritm sifatida **El-Gamalya** va **Shhorra** sxemasi qabul qilinib, uning standarti tashkil etilgan **(GOST R34.10-94** va **R 34.11-94)**. Algoritmlarni tatbiq qilish texnologiyasi. Keltirilgan algoritmlarni ishlatish texnologiyasi asosan bir-biriga turli hujjatlar yuboradigan abonentlar tarmog'i uchun yaratilgan Abonent sifatida bank klienti yoki bankning o'zi ham (banklararo axborot almashuv jarayonida) bo'lishi mumkin. Abonentlardan biri jo'natilgan hujjatlarni faqat tekshirishi, ba'zilari esa unga elektron imzo qo'yishi, boshqa biri ham imzo chekishi, ham qo'yilgan imzoni tekshirishi mumkin. Ushbu jarayonda 2 ta situatsiya bo'lishi mumkin:

1. Tarmoqda markaz mavjud bo'lib, unda ayrim ko'rsatilgan shaxs rahbar sifatida imzo chekishi mumkin.

2. Barcha abonenntlar teng huquqli ravishda imzo chekish imkoniyatiga ega.

Markazlashgan tarmoqlarda «**ishonch**» darajasi mavjud bo'lib, u orqali kim va qachon, qanday hujjatlarga imzo chekishi oldindan belgilab qo'yilgan bo'ladi.

Elektron imzo algoritmi arxitekturasi. Harqanday hujjatga imzo chekishda ehtiyotkorlik choralarini ko'rish lozim.

Programmalash yo'li bilan elektron imzo qo'yish va uni shifrlashda maxfiy kalit imzo chekuvchining shaxsiy disketida bo'lib, undan nusxa olish himoyalangan bo'lishi kerak. Bunda himoyaning eng oddiy usuli bu parol qo'yishdir. Bundan tashqari, himoyalanishning programma usulida «**kriptovirus**»lardan ehtiyot bo'lish lozim. Chunki bunday viruslar imzo chekish jarayonida maxfiy kalitni qo'lga kiritishi ehtimoldan uzoq emas, ya'ni nusxasini olib qo'yadi. Imzoni tekshirish jarayonida sistemani imzo to'g'ri deb aytishga ham majbur qilishi mumkin.

Masalan, kalitlar tasodifiy sonlar majmuyi asosida generatsiya qilinadigan bo'lsa, u holda virus taymerning ko'rsatkichini o'zgartirib, keyin qayta tiklash imkoniyatiga ham ega bo'ladi. Keyinchalik bu kalitlar xavfli abonent qo'liga tushib qolishi mumkin. Bu holda viruslar o'z ishini bajarib bo'lgan hisoblanadi. Shuning uchun ham «**kriptovirus**»larga qarshi qaratilgan asosiy qurol bu toza sistemali disketdan foydalanishdir.

Imzo chekish. Aniq bir hujjatga imzo chekish uchun kattagina hisoblash ishlarini bajarishga to'g'ri keladi. Bunday hisoblashlar ikki bosqichga bo'linadi:

1. Kalitlar generatsiyasi. Bunda har bir abonent uchun 2 tadan maxfiy va ochiq kalit generatsiya qilinadi. Maxfiy kalit abonent tomonidan sir saqlanadi. Bu kalit imzo uchun ishlatiladi. Ochiq kalit maxfiy kalit bilan alohida matematik bog'lanish bilan bog'langan. Odatda, ochiq kalit barcha abonentlar uchun ma'lum va elektron imzoni tekshirish uchun ishlatiladi.

Shuning uchun ham uni elektron imzo muallifini tekshiruvchi va uning haqiqiyligini aniqlovchi (ammo maxfiy kalitni hisoblab topuvchi vosita emas) vosita sifatida ishlatishadi. Bu vazifalarni bajarishda 2 ta variant mavjud: birinchisi – kalitlar generatsiyasini abonent mustaqil hal etishi mumkin. Ba'zi bir hollarda bu vazifani bajarishni tarmoq markaziga yuklatiladi. Ikkinchi variant administrativ xarakterga ega bo'lib, bunda har bir abonentning kalitlari yagona ekanligiga kafolat yo'q. Chunki markaz har bir abonent imzosini o'zgartira olish (подделка) imkoniyatiga ega.

2. Hujjatni imzolash. Dastlab hujjat hajmini iloji boricha birnecha o'n yoki yuz baytlar atrofida «**siqiladi**». Bu jarayon **xesh funksiyasi** yordamida amalga oshiriladi. Keyinchalik xesh funksiya qiymatini topish uchun matematik bog'lanishlar bilan ish yuritib, hujjatning xususiy imzosi aniqlanadi. Bu imzo o'qiladigan simvollardan tashkil topadi, ba'zan o'qiy olish qiyin bo'lgan simvollar ketma-ketligidan ham iborat bo'lishi mumkin. Elektron imzo hujjat bilan birgalikda saqlanadi (hujjat boshida, oxirida yoki alohida olingan faylda).

3. Imzoni tekshirish. Elektron imzoni tekshirish imzo chekkan shaxsning ochiq kaliti orqali amalga oshiriladi. Ushbu kalit autentifikatsiya shartini bajarishi shart, ya'ni tekshiruvchi ochiq kalit haqiqatan ham egasiniki ekanligiga to'la ishonch hosil qilishi kerak. Bordi-yu abonentlar mustaqil ravishda kalit almashuvni amalga oshirishmoqchi bo'lishsa, u holda telefon orqali yoki shaxsiy kontakt vositasida bog'lanishi lozim. Agarda abonentlar ajratilgan markaz orqali harakat qilishsa, u holda ochiq kalitlar markaz orqali sertifikatsiya qilinadi. Imzoni tekshirish ikki bosqishdan iborat:

- □ Hujjatning **xesh funksiya**sini hisoblash.
- □ Imzo algoritmining matematik hisobotini aniqlash.

Hujjatning xesh funksiyasi bilan imzo algoritmi matematik bog'lanishi va ochiq kalit o'rtasidagi munosabatni aniqlash vositasida elektron imzo haqiqiyligi tekshiriladi. Agar ular o'rtasidagi munosabat bajarilgan bo'lsa, u holda chekilgan imzo haqiqiy deb topiladi, aks holda, teskari aniqlanadi, ya'ni imzo qalbaki deb hisoblanadi.

Amaliyotda bank xodimlarini elektron imzoni tekshirishning matematik sxemalari emas, balki ishlatiladigan programma yoki apparat mahsulotlari ko'proq qiziqtiradi. Elektron imzo yaratish algoritmlarining quyidagi tasnifi (xarakteristikasi) katta ahamiyatga ega:

- □ Kripto turg'unligi,
- □ Ish yuritish tezkorligi,
- □ Funksional imkoniyatlari,
- □ Foydalanuvchiga qulayligi.

Elektron imzoning kriptoturg'unligi ochiq kalit uchun tanlab olingan kriptoalgoritmga bog'liq. Bundan tashqari, xesh funksiyani to'g'ri tanlab olishimizga va programma kompleksini himoyalanish darajasiga ham bog'liq. Ish yuritish tezkorligi esa kripto algoritmning tezkorlik sifati va kompyuter turi bilan baholanadi.

Kompyuter tarmoqlari uchun eng qulay parametr-bu imzoning uzunligi. Bordi-yu uzatiladigan fayl kichik, ammo ular soni (miqdori)

katta bo'lsa, u holda imzo uzunligi axborot almashuv jarayoni tezkorligiga ta'sir etadi. Ba'zan axborotlar (bank yoki kommersiya ma'lumotlarini maxfiy uzatish)ni jo'natish jarayonida imzolash bilan bir qatorda ularning shifrini ochish kerak bo'ladi. Bu holatda programma kompleksida shular bormi yoki yo'qligini aniqlash kerak bo'ladi.

2.5. Elektron kredit kartalari

Kredit kartochkalarini to'lov vositasida ishlatiladigan tizimlar hozirgi vaqtda dunyo miqyosidagi to'lov tizimlari orasida eng yuqori o'rinda turadi. Internetda hisob-kitobga plastikli kartochkalar ishlatishning yutug'i, ularning ko'p jihatdan an'anaviy to'lov tizimlariga o'xshashligidandir. Bunday holatda, Internet ma'lumot uzatishning axborot xavfsizligini ta'minlash texnologiyalari bilan amalga oshiriladi ishlatiladi. Bu tizimlarga **Cyber Plat. Open market, First Virtual** va boshqa bir qator to'lov tizimlari kiradi. **SSL – Secure Socket Layer** – protokoli bilan bir qatorda shu kabi tizimlarda axborot almashinuvida ma'lumot uzatishning SET – Secure Electronic Transaction – protokoli ishlatiladi va u kredit kartochkalari raqamlarini ishonchli himoyalashni ta'minlaydi.

SET spesifikatsiyasi **Master Card** va **Viza. NetsCape. IBM. VerisignD** yordami bilan ishlab chiqarilgan – kreditli karta ishlatishda tovarlarning narxini to'lashning eng xavfsiz yo'llaridan biri. **SET** spesifikatsiyasi asosida ommaviy kalit va raqamli sertifikatlar bilan ishlash kriptografiyasi yotadi. SET protokoli iste'molchining o'g'irlangan yoki soxta kartochkalar bilan bo'ladigan bezoriliklaridan himoya qiladi. U haqida toliq ma'lumotni http:Fwww.emoney.ru.Fpublish – manzilidan olish mumkin.

Kredit tizimining kamchiligi:

– transaksiyalarni o'tkazishda mijozning to'lov qobiliyatini tekshirish va kartochkaning avtorizatsiyasini tekshirish zaruriyati;

– har bir transaksiyag kartochka emitenti transaksiya summasidan 1,5–3 % oladi, lekin u 20 %dan oshmaydi;

– anonimning yo'qligi, savdo tizimlari tomonidan majburiy servis;

– kredit kartochkada ishlovchi elektron magazinlar soni chegaralanganligi;

– kredit hisobi ochish kerakligi;

– kartochka ma'lumotlarini tarmoqda uzatish kompleksi.

Lekin shunga qaramasdan, qalbaki to'lovlarning oldini olish jarayonida elektron kredit kartalari ancha yaxshi samara bermoqda. Bunday ish yuritish jarayonida har qanday mijoz va har bir sotuvchi ochiq va maxfiy

kalitlardan foydalanadi. Ochiq kalit kredit kompaniyasining ochiq kalitlar serveriga yuboriladi, maxfiy kalit esa parol yordamida qayta shifrlanadi va uning oldingi versiyasi o'chiriladi. Endi har bir shaxs bankdagi puldan foydalanishi uchun ham maxfiy kalitni, ham parolni bilishi kerak.

Faraz qilaylik, mijoz biron bir narsani **X** sotuvchidan sotib olmoqchi bo'lsa, u quyidagicha ma'lumot yuboradi: «Hozir vaqt T, men **Y** dollar **Z** tovari uchun to'layman». Shundan so'ng, u o'z parolidan foydalangan holda ochiq kalit yordamida muhr qo'yadi. Sotuvchi esa, o'z navbatida, maxfiy kalit yordamida muhr qo'yadi va uni kredit kompaniyasida mijoz uchun «**Y**» dollar X sotuvchiga o'tkazadi. Ko'rinib turibdiki, mijoz tovarni olishdan bosh tortmaydi, chunki u muhr qo'ygan, sotuvchi xohlagancha qaytadan pul talab qila olmaydi, chunki u mijozning kalitini bilmaydi. Bunday muhofazalangan elektron kartochkalar hozirgi paytda keng tarqalgan. Bunday kartochkalardan eng ko'p tarqalgani elektron plastik kartadir.

Plastik karta standart (**85,6×53,9×0,76 mm**) o'lchamga ega bo'lgan plastinkadan iborat mexanik, issiqlik ta'sirlariga o'ta chidamli plastmassadan ishlangan. Plastik karta bank to'lov sistemasining abonenti bo'lgan shaxsning elektron timsoli bo'lib, uning asosiy vazifasi talab qilingan vaqtda shu abonentning ishonchini oqlab uni qanoatlantirish. Shuning uchun ham plastik kartada bank logotipi, shu shaxsga xizmat qiladigan emitenti va to'lov sistemasi, karta egasining ismi, uning schyot raqami, kartaning xizmat muddati ko'rsatilgan bo'ladi. Bundan tashqari, plast kartada shaxsning fotosurati va shaxsiy imzosi ham bo'lishi mumkin. Alfavit raqamli ma'lumotlar relyefli shrift bilan yoziladi.

Sababi: hisobot jarayoni qo'lda bajarilganda ma'lumotlarni chekka o'tkazishda yoki imprinterdan o'tkazishda qulaylik tug'diradi. Ishlash prinsipiga asosan plast kartalar ikki turga bo'linadi:

- Passiv plast kartalar.
- Faol (aktiv) plast kartalar.

Passiv plast kartalar magnitli yo'lkalarda axborotlarni faqatgina saqlash uchun xizmat qiladi. Bugungi kunda bunday plast kartalar juda keng tarqalgan (>2 milliardan). Magnit yo'lkasi kartaning teskari tomoniga ishlangan bo'lib, 3 ta yo'lkadan iborat (**standarti SO 7811**). Uning 2 ta yo'lkasida asosiy ma'lumotlar saqlanadi, uchinchi yo'lkasiga esa joriy ma'lumotlar yoziladi. Ammo bunday plast kartalarda axborotlar muhofazasi juda past.

Shuning uchun ham mazkur prinsipda ish yuritadigan kartalarda hi-

moyani kuchaytirish uchun qo'shimcha grafik muhofaza vositalari kiritiladi. Masalan, gologrаfiya va nostandart shriftlardan foydalanish kabi. Savdo shoxobchalarida esa to'lov sistemalarida **on-line** mualliflik tizimlari ishlatiladi. Aloqa vositalari (telefon kommunikatsiyasi yomon ishlaydigan) yetarli bo'lmagan mamlakatlar bilan bunday prinsipda ish yuritish mumkin bo'lmaydi.

Faol plast kartalar elektron sxemaga ega bo'lib, uning standarti **ISO 7816** 1974-yili fransuz **Rolan Moreno** tomonidan yaratilgan. Elektron mikrosxemali bunday plast kartalarni bir qator belgilari asosida tasniflash mumkin:

1. **Birinchi belgisi** – funksional imkoniyatlari bo'lib, shu asosda quyidagilarga bo'linadi:
– sanash vazifasini o'taydigan schyotchik-kartalar;
– xotiraga ega kartalar;
– *mikroprotsessorli kartalar.*

2. **Ikkinchi belgisi** – o'qish qurilmasi bilan bog'lanish turi:
– kontakt bo'yicha o'qiladigan kartalar;
– induksiya usulida o'qiladigan kartalar.

Schyotchikli kartalar, asosan, karta egasining to'lov tizimi (sistemasi)dagi ishlatilgan va qolgan qoldiq o'rtasidagi ayirmalarni hisoblashda qo'llaniladi. Shuning uchun ham bunday kartalar keng qo'llanish imkoniyatiga ega emas.

Xotirali kartalar xotirasining hajmi 32 baytdan 16 kilobaytgacha bo'lib, ular schyotchikli kartalar bilan protsessorli kartalar oralig'idagi ishlarni bajarish imkoniyatiga ega. Bunday kartalarning xotirasi doimiy saqlash qurilmasini programmalashga asoslanib, bir karra yozish va ko'p karra o'qish imkoniyatini beradi.

Xotirali kartalarni ikki turga bo'lish mumkin: himoya qilinmagan xotirali va himoyalangan xotirali. Birinchi tur kartalar uchun ma'lumotlarni o'qish va yozish chegaralanmagan. Ularni to'lov vositasi sifatida ishlatish mumkin emas, chunki o'rta malakali mutaxassis ham uni buzib qo'yishi ehtimoldan xoli emas. Ikkinchi turdagi kartalarni to'lov sistemasida bemalol ishlatish mumkin, chunki ularda asosiy ma'lumotlar yoziladigan va bir yoki birnecha amaliy ish yuritadigan joylarga ega. Asosiy ma'lumot yoziladigan o'rni (joyi) shaxsiylashtirilganda faqat bir karra yozish va keyinchalik faqat o'qish uchun mo'ljallangan. Shaxsiylashtirish va mualliflikni belgilash jarayoni kartalarni tayyorlashda va *ishlatilishida asosiy bosqishdan hisoblanadi.* Shaxsiylashtirish jarayoni kartalarni mijozlarga tarqatishda amalga oshiriladi.

Bunda kartaga har bir shaxsning kerakli ma'lumotlari kiritiladi va pul to'lovi jarayonida kartaning ish bajarish «**qobiliyati**» tekshiriladi. Mualliflgini belgilash jarayonida to'lov sistemasida bo'ladigan sotuv va to'lovni tasdiqlash masalalari hal qilinadi. Mualliflikni hal qilish karta turiga, to'lov tizimi sxemasiga va xizmat doirasining moddiy-texnik ta'minotiga bog'liq. Kartalarni shaxsiylashtirish I bosqichida kartalar embossirovanie qilinadi (ma'lumotlarni relyefli kiritish jarayoni mavjud):

* karta tartib raqami (nomeri);
* kartaning boshlanish va tugash muddati;
* shaxsning ismi-sharifi.

Kartalarni shaxsiylashtirishda magnit yo'lkalarini kodlash va yoki mikrosxemalarni programmalash jarayoni ham mavjud.

Magnit yo'lkalarini kodlash jarayoni xuddi embrossirovanie jarayoni kabi bo'lib, faqat qo'shimcha qurilma yordamida hal qilinadigan «**o'qish-yozish**» funksiyasi kiritilishi bilan farqlanadi (bunda: **PIN-kod** mijoz xohishi bo'yicha tanlanadi). Mikrosxemani programmalash esa hech qanday qurilmasiz, faqat tashkiliy xususiyatlarga egadir, ya'ni mustahkam muhofazali bo'lish uchun har bir xodimning huquqiy himoyasini saqlash imkoniyatini programmalash jarayonini ko'zda tutadi.

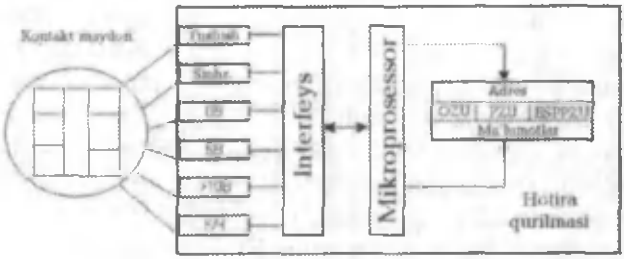
Odatda, mualliflik jarayoni yoki «**qo'lda**» (qachonki sotuvchi yoxud hisobchi so'rovni telefon orqali so'ralganda) yoki avtomatik ravishda (karta **POS terminal**ga joylashtirilib, ma'lumotlar sanaladi, hisobchi to'lovning yig'indisini muallif maxsus klaviaturadagi maxfiy **PIN-kod**ni aniqlab oladi). Shundan keyingina terminal mualliflikni o'rnatadi. Bordi-yu, naqd pul olmoqchi bo'linsa, u holda ham xuddi shunday ish yuritiladi, faqat pul maxsus qurilmadan avtomatik tarzda to'lanadi (muallifni aniqlaydigan bankomat orqali). Kartani har qanday xavfdan himoya qilish uchun turli usullar mavjud. Masalan, kartani shaxsiylashtirish uchun kartaning plastik asosiga muallifning qora yoki rangli fondagi fotosuvrati termobosma vositasida yopishtiriladi. Ixtiyoriy kartani olsak, uning maxsus yo'lkasida muallif imzosining namunasi bo'ladi. Kartani muhofaza qilish maqsadida uning chap va o'ng tomonida gologramma usulida hajmiy tasvir bo'ladi.

Odatda, mikroprotsessorli kartalarni intellektual karta yoki **smart-karta** (smart cards) deb ataladi. Mikroprotsessorli kartani mikrokompyuterga qiyoslasak bo'ladi, chunki unda ham markaziy protsessor, operativ va doimiy xotiralar va elektron o'chiradigan qurilma **PZU (ESPPZU)** mavjud (22-rasm).

Hozirgi kunda smart-kartalar quyidagi ko'rsatkichlarga ega:

* matnli chastotasi 5 MHz bo'lgan mikroprotsessor;
* operativ xotirasi 256 bayt;
* doimiy xotirasi 10 Kbayt;
* energiyaga bog'liq xotirasi 8 Kbayt.

Doimiy xotirasida **COS** (Card Operation System) kartasining tezkor xotirasini tashkil etadigan programmalar joylashgan. Tezkor xotira faylli tizimga ega bo'lib, **ESPPZU**ning ishlash prinsipiga asoslangan (xotirasi 1...8 Kbaytdan to 64 Kbaytgacha o'zgara oladi).



22-rasm. **Smart-karta arxitekturasi**

Smart-karta bir qator funksiyalarni bajarish imkoniyatiga ega:

* ichki resurslarga kirish chegaralangan (himoyalangan faylli tizimda ish yuritadi);
* ma'lumotlarni turli algoritmlar bilan shifrlaydi;
* elektron imzoni tashkil qiladi;
* kalitlar tizimini kiritish;
* karta egasi bilan bank va sotuvchi o'rtasida bo'ladigan barcha operatsiyalarni bajarish.

Smart-kartalar bilan ishlaganda **PIN-kod**ni tekshirish uchun – mikroprotsessorda maxsus algoritm mavjud bo'lib, u PIN ni real vaqtda va markaziy tekshirish jarayonida bankomat va **POS terminal**ni ishdan to'xtatadi. Ushbu xususiyatlari bilan smart-kartalar yuqori darajada himoya qilingan deb faraz qilinadi va moliya sohalarida juda keng ishlatiladi. O'qish qurilmasi bilan bog'langan holda ishlash prinsipiga binoan smart-kartalar 2 turga bo'linadi:

* kontaktli o'qish imkoniga ega kartalar;
* kontaktsiz o'qiladigan kartalar.

Kontaktli o'qish xususiyatiga ega kartalar sirtida 8...10 kontaktli plastinkalar bo'ladi. Ularning joylashuvi turli tashkilotlarda turlicha bo'lishi bilan farq qiladi. Bugungi kunga kelib kontaktsiz o'qiladigan kartalar ko'proq qo'llanila boshlandi. Bularda ma'lumotlar almashuvi (karta

bilan o'qish qurilmasi o'rtasida) induksion usul bilan amalga oshiriladi. Shuning uchun ham bunday kartalar ishonchli va uzoq muddatli hisoblanadi.

PIN tartib raqamini shaxsiylashtirish. Tabiiyki, **PIN** qiymati faqat o'z egasiga ma'lum bo'lishi kerak. **PIN** uzunligi iloji boricha katta bo'lishi lozim, chunki shundagina uning himoyalash imkoniyati yuqori bo'ladi. Ikkinchi tomondan, **PIN** qiymati bank atributlari bilan ham bog'liq. Shuning uchn ham uni karta egasining imzosi deb atash mumkin va **PIN** qiymatini kartaning muddati tugaguncha maxfiy saqlash maqsadga muvofiqdir. Elektron to'lov tizimini himoya qilish maqsadida **PIN** qiymatini generatsiya qilish usulidan foydalaniladi. Kartalarni shaxsiylashtirish 2 usulda amalga oshiriladi:

* kartani bergan bank tomonidan ajratilagn **PIN;**
* karta egasi tomonidan tanlangan **PIN.**

PIN bank tomonidan ajratilganda quyidagi ikki variantdan biri bilan generatsiya qilinadi. Birinchi variantda **PIN** kriptografik usulda generatsiya qilinadi (23-rasm):

23-rasm. **PIN ni mijoz raqamidan chiqarish**

Bunda mijoz kartasining raqamlari 16 razryadga to'lgunga qadar 0 bilan yoki boshqa biror konstanta bilan to'ldiriladi, ya'ni 8 baytgacha, keyin **DES** algoritmi bilan maxfiy kalitdan foydalanib shifrlanadi. 8 bayt uzunlikdagi shifrmatndan 4 bitli bloklar ajratiladi. Ushbu bitlardan tashkil topgan son <10 bo'lsa, u holda olingan raqam **PIN** ga qo'yiladi, aks holda olingan qiymat ishlatilmaydi. Ushbu usulning yuksakligi, **PIN** qiymatini to'lov tizimining ichida saqlash kerak emas.

Ikkinchi variantda bank **PIN** qiymatini tasodifiy usulda kriptogrammadan tanlab oladi va muhofaza qilingan kanaldan mijozga tarqatiladi. Ammo bu usulda mijoz olgan kartaning **PIN** qiymati juda uzun raqamlardan iborat bo'lsa ham noqulay. Chunki mijoz har vaqt ham uni esda saqlab qola olmaydi. Shuning uchun mijoz tomonidan tanlab olingan **PIN** qiymati durust hisoblanadi. Chunki mijoz o'zi tanlagan **PIN** qiymatini turli maqsadlar uchun ishlatish mumkin, ikkinchidan, ushbu qiymat esda qolish oson bo'lgan raqamlar va harflar majmuyidan iborat bo'lishi mumkin. Mijoz o'zi tanlagan **PIN** qiymatini, albatta, bankka

xabar etishi lozim. Bankka xabar qilish himoyalangan terminal yoki buyurtmali pochta orqali jo'natiladi.

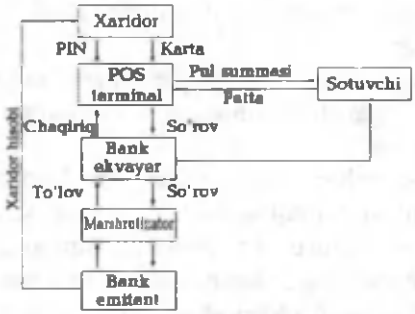
Xullas, mijoz kartasini **PIN** qiymati bilan shaxsiylashtirish 2 usulda amalga oshiriladi:

1) algoritmik usul;

2) noalgoritmik usul.

Noalgoritmik usul bilan tekshirilganda **PIN** qiymati ma'lumotlar bazasidagi mavjud qiymatlarga solishtiriladi. Odatda, **PIN** qiymatlaridan tuzilgan ma'lumotlar bazasi akslanish (прозрачного шифрования) usuli bilan shifrlanadi. Algoritmik usulda **PIN** qiymatini tekshirish uchun mijoz kiritgan qiymatni biror aniq algoritm bilan maxfiy kalitdan foydalangan holda o'zgartirilib, so'ng kartadagi qiymati bilan solishtiriladi.

POS tizimini muhofaza qilish. Rivojlangan mamlakatlarning savdo-sotiq sistemasida allaqachonlar **POS** tizimi bilan sotuvchi va xaridor o'rtasidagi muloqot o'rnatilgan. **POS** tizimi «elektron» bozorlarda (masalan, avtozapravkalarda, supermarketlarda) xaridorning debet va kredit kartalarini nazoratdan o'tkazish masalalari bilan shug'ullanadi. Moliya hisob-kitoblarida magnit yo'lkali plast kartalardan va smart-kartalardan foydalanganda transaksiyalarni qayta ishlash jarayonida **POS** tizimi ish yuritadi (24-rasm).



24-rasm. **POS sistemasining ish yuritishi**

POS terminaldan foydalanish natijasida ushbu kartalar bilan ish yuritish avtomatik tarzda amalga oshiriladi va bunda vaqtdan yutiladi. **POS** terminal kompleksiyasi va imkoniyatlari juda keng bo'lib, hozirgi namunaviy **POS** terminal ham magnit yo'lkali kartalarni, ham smart-kartalarni o'qiy oladigan o'qish qurilmasi, energiyaga bog'liq xotira, **PIN** klaviaturani ishga tushiradigan port, printer, shaxsiy kompyuter yoki elektron kassa apparati bilan bog'lanish imkoniyatiga ega.

Odatda, **POS** terminal modemga ham ega bo'ladi. U holda **POS** terminal «**intellektual**» imkoniyatga ega bo'lib, programmalash jarayonini ham assembler tilida yoki **SI** va Basic algoritmik tillarida amalga oshiradi.

Xaridor kerakli molni xarid qilishda o'z shaxsini tasdiqlash uchun debet yoki kredit kartasini ko'rsatib, **PIN** qiymatini **POS** terminalga kiritadi. Sotuvchi o'z navbatida mol (tovar) va xizmat haqqi uchun kerakli pul mig'dorini sistemaga kiritadi. Keyin **bank ekvayer** (sotuvchi banki)ga pul jo'natishga so'rov tushadi. Bank ekvayer esa bu so'rovni **bank emitent**ga kartaning shaxsini tasdiqlash uchun jo'natadi. Karta haqiqiy bo'lsa, xaridor tovar va xizmat haqlari uchun kerakli pul miqdorini to'lashga qodir. Demak, bank emitent bank ekvayerga sotuvchi hisobidan pul to'lashga ruxsat beradi. Shundan keyingina bank ekvayer **POS** terminalga xabar yuborib **transaksiya** tugaganini bildiradi. So'ngra sotuvchi xaridorga tovar va chaqiriqnomani beradi. Bunday qaralganda ancha murakkab jarayon va bu jarayonda ma'lumotlar yo'qolishi va o'zgartirilib yuborilgan ham bo'lishi mumkin. Shuning uchun ham **POS sistema**ni himoya qilish uchun quyidagi shartlar bajarilishi lozim:

* **PIN** qiymatini tekshirish bank emitent tomonidan bajarilishi kerak. Biror aloqa vositasi orqali jo'natilganda esa, **PIN** qiymati shifrlangan bo'lishi zarur.

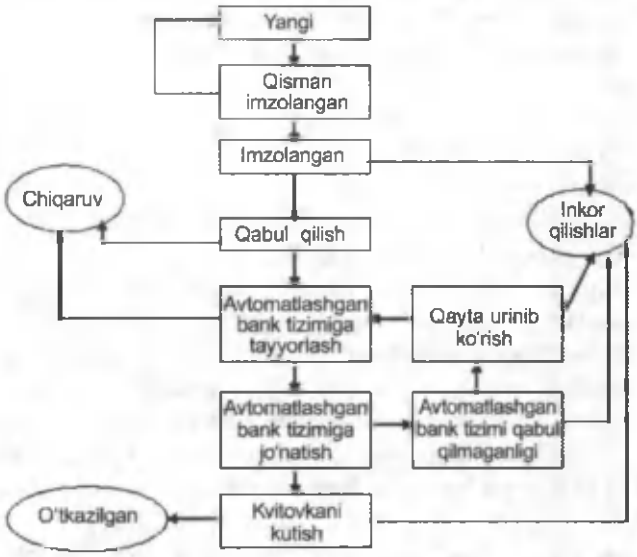
* Pulni o'tkazish uchun yuborilgan so'rov haqiqiyligi tekshirilishi ham kerak (biror o'zgarish bo'lmadimi yoki aloqa tizimida o'rin almashuv sodir bo'lmadimi).

POS sistemasi uchun eng xavflisi, shifrlashda ishtirok etadigan maxfiy kalitni ochib qo'ymaslik. Maxfiy kalitni ocha oladigan ikki xil xavf eng katta qiron keltiruvchi sanaladi, ular to'g'ri va teskari trassirlash (прямое и обратное трассирование) deb ataladi. To'g'ri trassirlashda maxfiy kalitni bilib olgan shaxs **PIN** qiymati kelgusida qanday bo'lishini tiklashga intiladi. Teskari trassirlashda esa PIN qiymati avval qanday bo'lganligini tiklashga intiladi. Bunday xavflardan qutulish uchun quyidagi usullar yaratilgan:

* Olib tashlangan kalit.
* Transaksiya kaliti.
* Ochiq kalitlar.

Ikkinchi va uchinchi usulning mohiyati kalitlarni har bir transaksiyada almashtirishni talab etadi. Kalitni olib tashlash usulida esa har bir transaksiya natijasida ma'lumot qanday mazmunda bo'lishidan qat'i na-

zar. kalit olib tashlanadi. Kalitlarni shifrlash generatsiyasi uchun kalitning qiymani ifodalovchi biryoqlama funksiyalardan va tasodifiy miqdorlardan foydalaniladi. Navbatdagi transaksiyani shifrlash uchun 25-rasmda ifodalangan algoritm bo'yicha ish yuritiladi.



25-rasm. **Bankomatda avtomatik tekshiruv jarayoni chizmasi**

Bunda maxfiy kalitning dastlabki qiymati algoritm boshlanishi hisoblanadi. S nomerli kalitni olish uchun uni ikkilik sistemasida ifodalaymiz (0,1). Keyinchalik kalit qiymatini hisoblashda ikkilik sistemasidagi **S** ning strukturasiga e'tibor beramiz (katta razryadidan boshlab). Agarda **S** ning **L** – razryadidagi qiymati **1 ga teng bo'lsa**, u holda joriy holatdagi **K** qiymatini bir tomonlama funksiya **FL(R)** bilan ifodalaymiz (bunda: **L** ko'rilayotgan ikkilik razryadining nomeri). Aks holda, S ning navbatdagi razryadini ko'rishni taqozo etadi. Bu esa **DES** algoritmi bilan bajariladi. Bu usul asosan, teskari trassirlashdan muhofaza qilish uchun asqotadi. Bank to'lov sistemasining abonenti plastik kartalar bilan ishlashda asosan bankomatlar qo'llaniladi. Zamonaviy bankomatlar bank kassiri bajaradigan hamma vazifalarni bajaradi. Masalan: naqd pul berish, kartochkada qolgan pul haqida ma'lumot berish, kartochka egasining kartochkadagi mablag'idan kerakli summani naqd pulsiz boshqa hisob raqamiga ko'chirish va hokazolar. Bu vazifalarni to'liq funksiyali **Automated Teller Machine**lar bajarish imkoniyatiga ega. **Cash Dis-**

panser oddiy bankomatlar faqat naqd pul berish vazifasini bajaradi. Bankomatlarni tashqi ko'rinishida displey–oyna bilan metall shkaf ko'rinishida bo'lib, ma'lumotlar va buyruqlarni kiritish uchun klaviatura o'rnatilgan. Old panelida kartochkalarni qabul qilish tuynugi, kvitansiyalarni berish, pullarni berish uchun maxsus darchalari bor.

Bankomatlar hajmi va o'rnatiladigan joyiga qarab quyidagi turlarga ajratiladi:

1) stolga qo'yiladigan bankomat;

2) polga qo'yiladigan bankomat.

O'rnatiladagan o'rniga qarab

1) binoning ichiga, xonaga qo'yiladigan bankomat;

2) ko'chaga qo'yiladigan bankomat;

3) devorga qo'uiladigan bankomatlar turlariga bo'linadi.

Bankomtlarga bank xodimlarining xizmat ko'rsatilishini o'rnatilishi oddiy holda banknot **zagruzkasi** – bankomatning old tomonidan yoki binoning ichida devorning orqa tomonildan amalga oshiriladi. Bankomat ichi – elektronika bo'yicha ma'lumotlarni kartadan o'qish, banknotlarni saqlash va ularni uzatish qurilmasi, pullarni qabul qilish qurilmasi va depozitlar hujjatlarga va buzilgan kartochkalarni va buzilgan brak bo'lgan ***kupyuralar***ni saqlash kassetasi, kvitansiyalarni bosmaga chiqaruvchi printerlardan iborat. Bankomatlarni yaratuvchi yirik firmalar bugungi kunda aniq maqsadlarga yo'naltirilgan bankomtalarni taklif qilmoqda. Masalan: Siemens Nixdorf 4**: seriyadagi bankomatlarni chiqaradi. 4**, Cash Compact, Procash 400, CSC/430, CSC/450, CSC/456 va boshqalar.

Siemens Nixdorf ning asosiy funksional modullari quyidagicha:

– sistemalar bloki;

– foydalanuvchi bilan muloqot vositasi;

– plastik kartochkalar bilan qayta ishlash qurilmasi;

– pul berish va banknotlarni saqlash qurilmasi;

– pul vkladlarini qabul qilish qurilmasi;

– xavfsizlikni ta'minlovchi qurilma.

Sistemalar bloki –shaxsiy kompyuterdagi singari bo'lib, u Siemens Nixdorfda ishlab chiqariladi. Protsessor Intel 80486 'rb Pentium, OZU 32 MB gacha, vinchester qattiq disk 850 MB. Ba'zan korpusning ichiga odatdagi klaviatura o'rnatiladi. Foydalanuvchi bilan muloqot vositalari mijoz tomonidan bankomatni boshqarish uchun zarur.

Siemens Nixdorf bankomatida monoxromli displeydan foydalaniladi. Shuningdek, 9 yoki 10 dyuymli displeylar ruxsat etiladi. Ko'chaga

o'rnatiladigan bankomatlarga esa LCD displey o'rnatiladi. Uning konstruksiyasi insonning tashqi ko'rinishi yuzini hatto quyosh nuri tushib turgan bo'lsa ham qabul qiladi. Klaviatura esa bankomatni boshqarish va PINni kiritish uchun foydalaniladi. Klaviatura 10ta sondan iborat bo'lib. Unda 4 ta boshqaruvchi va 2 ta dasturlash qo'shimcha klavishi bo'ladi.

Invalidlarning tizimdan yaxshi foydalanishlari uchun 3 darajali kattalashtirish mumkin bo'lgan klaviatura, ya'ni nuqtalar bilan ta'minlangan bo'lib, sezish orqali hatto ko'zi ojizlar ham boshqarishi mumkin.

Printerlar – bankomatdagi moliyaviy operatsiyalar qog'ozda protokollashtiriladi. Siemens Nixdorf 2 ta printerni komplektlashgan holda joylashtirgan bo'lib, ulardan biri summa ko'rsatilgan chekni pechat qilish uchun – plastik kartochka bo'yicha mini vipiska schyot, ya'ni kichik mablag' haqida ma'lumotni pechatga berish uchun ishlatiladi.

Ikkinchisi esa ma'lumotlar bazasi jurnalida bajarilgan operatsiyalarni belgilash va dasturiy xizmatga oid hodisalarini pechatga chiqaradi. Jurnalli bosmaga chiqarish printeri oddiy kassa apparati singari analogli nazorat lentalari ko'rinishida bo'ladi.

Bundan tashqari, to'liq funksiyali, CSC/430, CSC/450, bankomatlari qo'shimcha maxsus keng printerlarni mablag' schyot holati haqida ma'lumotlarni pechatga chiqarish uchun o'rnatilgan bo'ladi.

Kartochkalarni qayta ishlash yoki kartrider – Siemens Nixdorfning barcha bankomatlarida magnit lentali kartochkani va smart-kartani qayta ishlashga ixtisoslashgan kartrider o'rnatilgan. To'lov tizimiga magnitli plastik kartochka murojaat qilganda bankomatda doimiy telekommunikatsiya aloqasi mavjud bo'lib, u avtorizatsiya markazi bilan bog'lanishi kerak, buning uchun bankomatga tarmoq kartasi o'rnatilgan bo'ladi.

Avtorizatsiya va transaksiya on-line rejimida avtorizatsiya markazida kompyuter orqali amalga oshiriladi (kompyuterda mablag' ko'rsatkichlari stop-listda xuddi kartochkadagi ma'lumotlar singari saqlanadi. Agar karta kompyuterda identifikatsiyalangan bo'lsa, avtorizatsiya markazida, stop-listdagi kabi **kartrider** shunday kartalar ushlab qolganligi haqida komanda oladi.)

Bankomatning o'zining programmasi kartochkalar to'xtab qolishi 2 holatda qarab chiqadi:

1) agar 3 marta uringanda ham PIN noto'g'ri kiritilgan bo'lsa;

2) aniq belgailangan vaqtda berilgan tizimda karta davolanmagan bo'lsa, kartani ishlovga bergan vaqtda kartrider magnit polosasini shunday to'g'ri tutadiki, unga boshqa predmetlar kirib qolishidan himoya qiladi.

Banknotni saqlash kassetalari – bankomat seyfining ichida 1 dan 4 gacha bo'lgan kupyuralar bilan ishlashga 4 ta nominalda ishlashi mumkin bo'lgan banknot kassetalar joylashgan.

Pul berish qurilmasi yoki dispenser – Dispenser banknot kupyuralari joylashgan kassetalar bilan yonma-yon seyf maydoniga o'rnatilgan bo'ladi. U kassetalardan kupyuralarni uzatish darchasigacha uzatish uchun xizmat qiladi. Kassetadagi har bir kupyura o'z yo'liga ega bo'lib, uzatish darchasiga maxsus analizator orqali o'tadi. Analizator uni optik qalinligi, pishiqligini tekshiradi, o'lchaydi. Agar o'lchangan qiymat zichligi kupyuranikidan etaloni bo'yicha farq qilsa, u holda «отказная» bekor qilish – inkor qilish kassetasiga pulni jo'natadi. Dispenser xotirasida valutalarning 10 xil optik zichligi haqidagi ma'lumot saqlanadi. Ular valuta kodlari parametrlari bo'yicha farq qiladi, nominallar va chiqargan yili bo'yicha ham farq qiladi.

Shuning uchun bir vaqtning o'zida bir-biridan valuta bo'yicha farq qiluvchi 4 ta kasseta qo'yish mumkin. Masalan: 1 kasseta 1994-yilda chiqarilgan 1000 so'mlik, 2 kassetaga 1997-yilda chiqarilgan 1000 so'mlik, 3 kassetaga 100 dollarlik banknotlar, 4 kassetaga esa 50 yevrolik bo'lishi mumkin.

Xavfsizlikni ta'minlovchi vositalar – Siemens Nixdorf bankomatlarida ko'p darajali himoya operatsiyalari – mexanik, optik, elektrik, dasturiy himoya va signalizatsiyalar va videokameralar o'rnatilgan. Banknot kassetalari UL 291 yoki S lar seyfida joylashgan bo'lib, seyfning eshigi maxsus qulf bilan berkitiladi va u sonli qurilmalar bilan blokirovka qilingan bo'ladi. Seyf bilan birgalikda 3 ta kalit beriladi, ulardan birortasi saqlanib qolgan taqdirda ham yangi seyf buyurtma berishga hojat qolmaydi.

Bankomatni buzishga urinishga qarshi har xil turdagi datchiklar o'rnatilgan bo'lib, ular signalizatsiya tizimi bilan bog'langan.

Komplekt himoyaga videomagnitafon va videokameralar kiradi. Ular mijozning bankomat bilan barcha harakatlarini kuzatib boradi.

Pulli vkladlarni qabul qilish qurilmasi yoki depozitor – bankomat depozitori 500 konvertni hujjatlari bilan, banknotlari, tanga va boshqa qiymatlarda qabul qilish imkoniyatiga ega. Konvertda schyot mablag'lari haqidagi axborot bosmaga chiqadi va operatsiya bajariladi. Maxsus printer depozitorniki, to'ldirilgan konvertni pechatlashi mumkin.

Konvertlar qabul kassetasida saqlanadi. Bankomatlar haqida gapirilganda, uning ish prinsiplari elektron kassirlar, avtomatik elektron pul almashtirish va bank axborotlari uchun printerlarni ham o'rganish joizdir.

Elektron kassir

Elektron kassir – naqd pullarni berish uchun ishlatiladi. Elektron kassir plastik kartochkaga xizmat qilmaydi. Shuning uchun u arzon. Bankomatdagi singari kupyuralar uchun kassetalar ishlatiladi, otkaznaya kassetasi bo'ladi. Bundan tashqari 1 yoki 2 ta depozit kassetalari bo'ladi. Naqd pullarni qabul qilish uchun, ularning barchasi seyfning ichida joylashgan bo'ladi. Elektron kassirlar bankning xavfsizligini ta'minlash uchun zarur. Pul doimiy seyfda turadi. Uni hatto operator ham xavfsizlik xizmati xodimlari ishtirokisiz ochishga haqqi yo'q.

Avtomatik valuta almashtirish

Avtomatik valuta almashtirish-bu qurilmaning tashqi ko'rinishi bankomatni eslatadi. Uning asosiy moduli valutalar detektori ya'ni kiruvchi kupyuralarning haqiqiy va nominal ekanligini aniqlash xususiyatiga ega. U odatdagi valuta almashtirish shaxobchasidan biroz qimmat bo'lsada uning ishlash darajasi va ishonchliligi yuqori.

Bank axborot printeri

Bank axborot printeri – bu qurilma ham bank mijozlariga xizmat *qilish uchun mo'ljallangan. Kartrider* – PIN klaviatura displeydan iborat. Printer quyidagi vazifalarni bajaradi:

– har xil schyotlar holati haqida ma'lumotlar berish, masalan, kartochka yoki kommunal to'lov haqidagi;

– shaxsiy formulyarlar berish mumkin. Pul o'tkazish perevodlar bo'yicha.

Bunday printerlar bank imijini yaxsxilashga xizmat qiladi. Mijozlar bilan ishlash madaniyatini oshiradi.

Imprinter

Imprinter – to'lov kvitansiyalarini amalga oshirish uchun ishlatiladi. Maxsus va universal imprinterlar do'konlar, bank va benzokolonkalarda foydalanish uchun qulay. Imprinterlar AQShning Roki Maunt shahrida maxsus ishlab chiqariladi. Uning New Bold 916 modeli jahonda eng ko'p tarqalgan, savdo nuqtalarida magazin va aptekalar kafe bar restoran va boshqa ommaviy nuqtalarda ishlatiladi. Avtomatik yig'uv qurilmasi mavjud va u 2 kartali bo'lib, turizmdan aviabiletlar sotishda ishlatiladi.

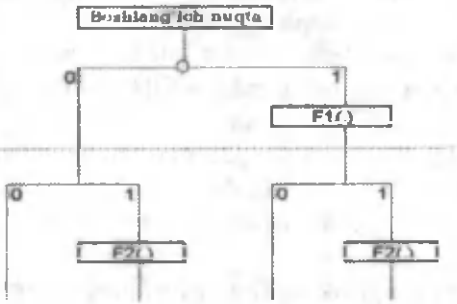
2.6. Bankomatlarni muhofaza qilish

Plastik kartalar vositasida naqd pul to'lash va inkassatsiya qiladigan avtomatik qurilmalarni bankomat deb ataladi. Bankomat kartalarni o'qiydigan qurilma, displey va klaviatura bilan jihozlangan bo'lib, elek-

tron kartalarni avtomatik tarzda o'qishga mo'ljallangan va shaxsiy **EHM** tomonidan boshqariladi.

Kommunikatsiya funksiyalarini bajarish uchun **X.25** platalari va ba'zan modemlar bilan ham jihozlangan. Oxirgi paytlarda bankomat naqd pullarni saqlaydigan omborga aylanib qolmoqda desak, mubolag'a bo'lmaydi. Pul kupyurlari maxsus seyflarga ega bankomat kassetalarida saqlanadi.

Bankomat ma'lum og'irlikka va gabaritga ega statsionar qurilma bo'lib, ba'zan uning og'irligi tonnada, balandligi 1,5–1,8 m; eni va bo'yi 1 m atrofida tayyorlanadi. Ko'pgina bankomatlar bugungi kunda real vaqt **(on-line)** rejimida ishlaydi. Ba'zan avtonom rejim **(off-line)**da smart-kartalar bilan ishlaydi va bunda bank kompyuterisiz ham ish yuritiladi. Transaksiya haqidagi axborotni ichki magnit diskiga yoziladi va natija o'rnatilgan printerga chiqariladi.



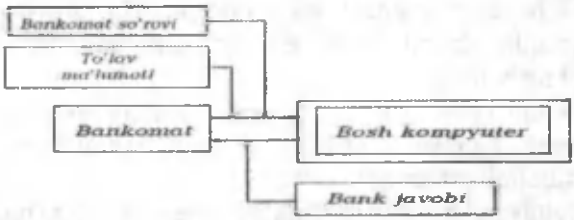
26-rasm. **Kalitni chiqarish algoritmi**

Avtonom rejim **(off-line)**da ish yuritish mohiyati shundaki, bunda bankomat bank kompyuteriga bog'liq bo'lmaydi. Bundan tashqari, kommunikatsiya aloqalari bilan ham bog'liq emas, shuning uchun bu usulda ish yuritish ancha arzonga tushadi. Kommunikatsiya aloqalari past darajada bo'lgan mamlakatlar uchun juda asqotadi.

Ammo mijozlarni autentifikatsiya qilishda biroz qiyinchiliklar tug'iladi. Chunki magnit yo'lkali kartalarda axborotlarni himoya qilishda shifrlash usullaridan foydalaniladi va bunda joriy bank uchun faqatgina bitta kalit bilan shifrlash jarayoni amalga oshiriladi. Agar bu borada xatoga yo'l qo'yilsa, u holda barcha bankomatlarda axborot xavfsizligi xatoligi sodir bo'lishi mumkin.

Real vaqt **(on-line)** rejimida ish yuritilganda bankomat to'g'ri yoki PIN tarmog'i **(PIN Block Network)** bloki telefon tarmog'i vositasida

bankning bosh kompyuteri bilan bog'lanadi. Bu holda transaksiyani registratsiya qilish bosh kompyuterda amalga oshiriladi. Shunda bankomat bosh kompyuter bilan 3 xil xabar (ma'lumot) orqali almashuv sodir etadi.



27-rasm. **Bankomat va bosh kompyuter bilan axborot almashuv**

1) bankomat so'rovi;
2) bankning javob xabari;
3) bankomatning to'lov haqidagi xabari.

Bankomat so'rovi quyidagi ma'lumotlardan iborat:

- bankomat identifikatori;
- mijozning hisob raqami va qayd qilinadigan ma'lumotlar;
- kartaning seriya raqami;
- himoya simvoli;
- mijozning shifrlangan **PIN** qiymati;
- talab qilingan pul miqdori;
- transaksiya raqami;
- xabarning barcha ma'lumotlarini tekshiradigan kod.

Bankning javob xabari quyidagilardan iborat:

* bankomat identifikatori,
* to'lovni amalga oshiradigan operatsiya kodi,
* transaksiya kodi,
* xabarning barcha turlariga mos tekshirish kodi.

Bunday axborot almashuv jarayonida ma'lumotlarning to'liqligini nazorat qilish uchun autentifikatsiya kodi **MAS** (Message Authentication Code) ishlatiladi. Real vaqt rejimi avtonom rejimga nisbatan bir qator qulayliklarga ega. Bunda mijoz nafaqat pul olish, balki o'z hisobkitobini ham to'g'rilab qo'yish imkoniyatiga egadir.

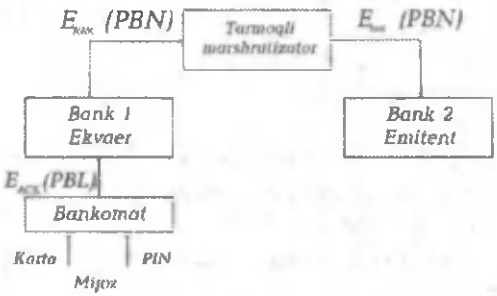
Biroq, bu tizimning turg'un ishlashi va har tomonlama himoyalangan bo'lishi ishonchli aloqa tarmog'ining ishlash jarayoniga bog'liqdir. Bu jihatdan qaraganda bankomatning ushbu rejimda ish yuritishi biroz qimmatroq bo'ladi. Boz ustiga, kommunikatsiya vositalarida turg'un

aloqaning bo'lishi ham shart hisoblanadi. Ayniqsa, bosh kompyuter bilan bankomat o'rtasida sodir bo'lishi mumkin trafika tahlili buni yaqqol isbotlaydi.

Bankomatlar tarmog'i. Bankomatlarni ekspluatatsiya qilishning tarmoq usuli bugungi kunda keng tarqalgan. Bu jarayonda bir qator banklar tarmoqda ishtirok etadi. Bunday tarmoqda shtirok etayotgan banklarning asosiy maqsadi:

- ishtirok etuvchilar bajaradigan operatsiyalar narxining kamayishi,
- ishtirokchi banklar o'rtasida xizmatning yangi turlari uchun sarf qilinadigan xarajatlar taqsimoti,
- foydalanuvchilar uchun geografik chegaralanish xizmatlarini yo'lga qo'yish.

Bankomatning bank tarmoqlaridan foydalanishida muammo yuzaga keladi. Bu – banklarning konfidensial ma'lumotlarini himoya qilish masalasi (shifrlash kalitlari va b.m.). Bu muammoni hal qilish uchun **PIN** qiymatini markaziy nazorat qilish masalasi o'rtaga qo'yildi. Bunda har bir bank o'z markazida bankomat bilan hamkorlikda ushbu masalani hal qiladi. Unda tarmoq ishtirokchilari o'rtasida kalitlarni taqsimlash masalasi qiyinlashadi (28-rasm):



28-rasm. **Mijozning PIN qiymati to'g'risidagi ma'lumotning bankomat va banklar o'rtasida o'tishi**

Mijoz kartasining **PIN** qiymati bilan bankomat va **bank-ekvayer** (bankomatga qarashli bank) va **bank emitent** (mijoz kartasini chiqargan bank) o'rtasida ish yuritish sxemasi bilan tanishib chihamiz. Faraz qilaylik, bank emitent mijozi bank ekvayerga murojaat qilsin. Bank tizimida quyidagicha harakat vujudga keladi:

1. Bankomatning o'qish qurilmasi mijoz kartasini o'qib, uning ushbu bankda hisob raqami bor yoki yo'qligini aniqlaydi.

2. Agar mijoz bank ekvayerda hisob raqamiga ega bo'lmasa, u holda, transaksiya tarmoq marshrutizatori (bank emitent identifikatoriga ega)ga jo'natiladi. Bu yerdan transaksiya bank 2 ning bosh kompyuteriga jo'natiladi, yoki shu bank 2 uchun **PIN**ni nazoratdan o'tkazadi.

3. Agar PINni bosh kompyuter nazoratdan o'tkazsa, u holda transaksiya to'g'risida to'liq ma'lumotga ega bo'linadi va PINning aniqligi tekshiriladi.

4. Tekshirish natijasidan qat'i nazar, bank 2 olingan natijani tarmoq marshrutizatori orqali bank 1 kompyuteriga jo'natadi.

Keltirilgan misoldan xulosa shuki, *bank emitent* quyidagi shartlarga rioya qilishi lozim:

* bank yaratgan kartalar bankomat tarmog'idagi barcha banklar uchun foydalana oladigan bo'lsin,

* bank emitent o'z mijozlari PIN qiymatini tekshirish texnologiyasiga ega bo'lsin,

*Bank ekvayer*ga esa boshqa shartlar qo'yilgan:

* bankomatda yoki bosh kompyuterda transaksiyaning tegishli ekanini nazoratdan o'tkazish mumkin bo'lsin,

* begona **PIN** qiymatini tekshirish imkoni yo'q bo'lsa, u holda bank ekvayer transaksiya ma'lumotlarini tarmoq marshrutizatoriga yuborishi lozim.

Bankomat va kompyuterlarda muhofaza vositasini ta'minlash uchun aloqa tarmoqlarida abonentli shifrlash masalasini hal etish kerak. Odatda, quyidagi uslub qo'llaniladi:

– bankomatlar tarmog'i zonalarga bo'linadi va ularning har birida zonal shifrlash kalitlari bo'ladi – **ZCMK (Zone Control Master Key)** Ushbu kalit tasodifiy yo'l bilan marshrutizator vositasida generatsiya qilinadi va noelektrik usulda bankka jo'natiladi. **ZCMK** kalitni ochish butun **PIN** larni aniqlash bilan baravar.

Bank emitentning bosh kompyuteridan marshrutizatorga kelgan axborotni shifrlash uchun shu bankning ishchi kaliti – **IWK (Issuer Working Key)** ish yuritadi. Ishchi kalit foydalanuvchi so'roviga muvofiq ish yuritish jarayonida o'zgarishi mumkin. **IWK**ni emitent bankining bosh kompyuteriga marshrutizator **ZCMK** unikal ko'rinishida shifrlangan holatda uzatadi. Xuddi shunga o'xshash bank ekvayerning ham ishchi kaliti – **AWK (Acquirer Working Key)** mavjud. Bankomatdan bank ekvayerning bosh kompyuteriga jo'natilgan axborotni shifrlashda ekvayerning aloqa kaliti – **ACK (Acquirer Communication Key)** ish yuritadi. Sistema ish jarayonini muhofaza qilishda quyidagi belgilashlar kiritilgan:

Ey (X) – **X** xabarni **DES** algoritmi bilan **Y** kalit vositasida shifrlash, **Dy (X)** – **Y** kalit yordamida **DES** algoritmi bilan **X** xabarni shifrdan chiqarish, **PBL(PIN Block Local)** – **PIN**ning mahalliy (lokal) bloki bo'lib, mijoz tomonidan kiritilgan PIN (8 simvolga to'ldirilgan)ning bankomat ichki formatida ifodalanishi.

PBN (PIN Block Network) – **PIN**ning tarmoq bloki bo'lib, tarmoqqa uzatishga tayyor.

Endi, rasmda ifodalangan sxema bo'yicha ish yuritish jarayonini o'zlashtirishga harakat qilamiz. Faraz qilaylik:

1. Mijoz bank 1 ning bankomatiga murojaat qilib, klaviaturadan o'ziga qarashli PIN qiymatini kiritdi. Bankomat **PBL**ni tashkil etib, uni **ACK** kaliti bilan shifrlaydi, ya'ni **EACK (PBL)** kriptogrammani hisoblaydi va natijani bank 1 ning bosh kompyuteriga yuboradi.

2. Bank 1 ning bosh kompyuterida PBL blok shifrdan ozod bo'ladi va **PBN** blokka aylanadi, keyin bu blok **AWK** kaliti bilan shifrlanadi hamda tarmoq marshrutizatoriga yuboriladi. Demak, **YEASK,** $E_{ACK}(PBL) < E_{AWK}$ **(PBN)** jarayon **PIN** blokining translyatsiyasi deyiladi. Bu jarayonning asosiy vazifasi shifrlash kalitini almashtirishdan iborat.

3. Agar **PIN** tarmoq marshrutizatorida tekshirilsa, u holda **EAWK (PBN)** kriptogramma olingach, uni shifrdan chiqarib keyin **PIN**ni qu-yidagi o'zgartirishdan so'ng ajratamiz:

$$D_{AWK}(E_{AWK}(PBN))=PBN \prod PIN$$

Agar **PIN** bank 2 da tekshirilsa, u holda olingan kriptogramma **AWK** kalitdan **IWK** kalitga translyatsiya etiladi.

$$E_{AWK}(PBN) \prod E_{IWK}(PBN).$$

Endi shu kriptogramma bank 2 ga yuboriladi.

4. 2-bankka tushgan kriptogramma E_{IWK}**(PBN)** foydalanilgan uslubiga qarab yoki ochiq **PIN:**

$$D_{IWK}(E_{IWK}(PBN))= PBN \prod PIN,$$

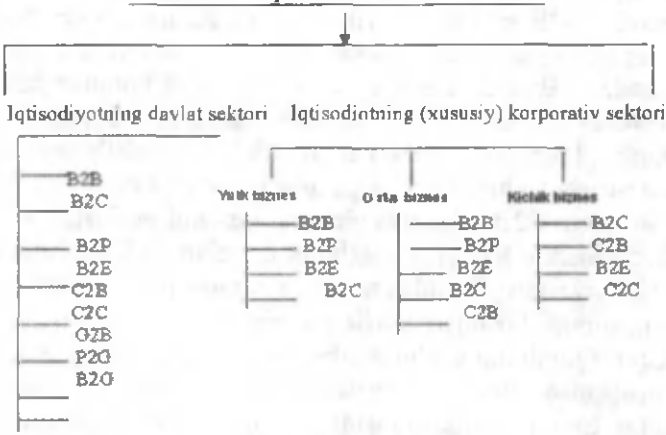
yoki **DBK** ma'lumotlar bazasi kaliti bilan shifrlangan **PBL** blok formasidagi **PIN**:

$$E_{IWK}(PBN) \prod E_{DBK}(PBL) \text{ ga aylanadi.}$$

5. Shunday o'zgartirishlardan so'ng **PIN** ma'lumotlar bazasidagi haqiqiy **PIN** topiladi.

6. Mijoz tomonidan kiritilgan **PIN** tekshirishlar natijasida yoki qabul qilinadi, yoki qabul etilmaydi. Tekshirish natijasidan qat'i nazar, 2-bankning bosh kompyuteri olingan natijani tarmoq marshrutizatori orqali 1-bank kompyuteriga jo'natadi, ushbu kompyuter esa yechim natijasini bankomatga yetkazadi.

Kompyuterlar o'rtasidagi himoya vositasini ta'minlash simmetrik **DES** algoritmi asosida amalga oshirilgan. Shuning uchun ham **ZCMK** kalitiga jiddiy talablar qo'yilgan. Shifrlashda ochiq kalit uchun asimmetrik kalitdan foydalanish anchagina osonlik tug'diradi, ayniqsa, bankomat bilan bosh kompyuter o'rtasida ish yuritish birmuncha yengillashadi. Bunday yopiq sikIli texnologiya elektron tijoratni amalga oshirishda ham qo'llaniladi, lekin u boshqacharoq yo'nalishda bo'ladi.



29-rasm. **Elektron tijorat andozalari**

Elektron tijorat tushunchasi ostida tovar buyurtmasini qabul qilish, to'lovni amalga oshirish, tovar (xizmat bajarilishi) yetkazib beriilshidagi boshqaruvda qatnashuvni o'z ichiga oluvchi operatsiyalar (amallar)ning yopiq sikIli texnologiyasi tushuniladi. Ushbu amallar (operatsiyalar) axborot texnologiyalari va elektron vositalar yordamida o'tkazilib, egalik etish yoki ishlatish huquqini bir yuridik (jismoniy) shaxsdan ikkinchisiga o'tishini ta'minlaydi. **Electronic Data Interchange** – EDI – ma'lumotlarning elektron almashinuvi, EFT – **Electronic Funds Transfer** – fondlarning elektron almashinuvi, **E-mail Electronic Mail** – elektron pochta kabilarda elektron tijorat tizimlarining ma'lumotlarni almashishini tashkiliy usulidan foydalaniladi.

Elektron tijorat kundan kunga tovar va xizmatlar assortimentini oshira boshlagan sari alohida shaxslarni, korxonalarni, sohalarni, davlat muassasalarini va nihoyat davlatlarni bir jamjamiyatga birlashtirib, hamkorlarning o'zaro ta'siri axborot va telekommunikasion texnologiya yordamida samarali va to'siqsiz ro'y berishiga imkon beradi.

Hozirgi vaqtda iqtisodiy rivojlangan mamlaktalarda turli darajada yuqorida ko'rsatilgan B2B, B2C, B2P, B2E,C2B, C2C, G2B, C2C,P2G, B2G kabi iqtisodiyotning davlat sektori andozalaridan foydalaniladi.

Bu yerda: G – (Government) – davlat; B – (Business) – biznes-korxona; C – (Consumer) – mijoz, iste'molchi; P – (Partner) – hamkor; E – (Executive, Employee) – korxona xodimini anglatadi (29-rasm). B2B modeli bo'yicha elektron tijoratni yuritish o'zaro aloqalarda, ish jarayonda to'liq avtomatlashtirilgan tizimlardan foydalanish samarali natijalarni beradi. B2B modeli 30 yil avval yaratilgan bo'lib, hozirda jahonda keng tarqalgan model hisoblanadi. B2B modeli ikki xil maqsadlarda ishlatiladi. Birinchidan, ikki va undan ortiq kompaniyalar o'zaro savdo jarayonlarida ishtirok etishsa, B2B modeli qo'llaniladi.

Masalan, kompaniya internet orqali o'z takliflarini yuborishi, shartnoma tuzishi va hisobni amalga oshirishi mumkin.

Ikkinichidan, B2B sektorida elektron tijoratni yuritishni rivojlangan tizimlarining muhim hususiyati, axborot tizimlari va korporativ tizimlari bilan integratsiyasidir. Bu bilan xarid va xarajatlar jarayoninigina emas, butun kompaniyani boshqarish tizimini ishlab chiqish ta'minlanadi.

Elektron tijoratning ushbu modeli elektron tijoratning eng samarali sohasi hisoblanadi. Ichki bozorda elektron biznes ishlarini yuritish, davlat ishlab chiqaruvchilari orasidagi yangi tijorat aloqalarini o'rnatish imkonini beradi, shu bilan birga, bir davlat miqiyosidagi ishlab chiqaruvchilar xomashyolar va qurilmalar bilan ta'minlanish jarayoni chet davlatlardan import qilish bilan taqqoslaganda ancha yengillashadi.

B2B modelining halqaro miqiyosdagi o'rni, davlatni jahon bozoriga olib chiqish imkonini beradi. B2B modelini qurish va uning samarali ishlashini ta'minlash uchun, bu model qo'llaniladigan bozor segmenti buni qabul qilishga va joriy etish masalasi yechimlarini talab qiladi. Bu bozor segmenti ma'lum hajm, struktura va umumiylikka (массовость) ega bo'lishi kerak. Albatta, shimoliy Amerika, Sharqiy Yevropa va boshqa mamlakatlar hajm bo'yicha bozor ko'rsatkichlari turlicha bo'ladi. Agar Amerika kompaniyalari B2B modeli bo'yicha elektron tijoratni yuritish, bozorning yillik daromadi milliardlab dollar bo'lgan segmentlariga yo'naltirilgan bo'lsa, boshqa davlatlar bu ko'rsatkichga hali ega emas.

Bozor o'z strukturasiga ega bo'lishi kerak, ya'ni (meva, metall, avtosanoat va shu kabi strukturalar) bir-biridan bozori, ishtirokchilari bilan farq qiladigan va bunda ularga qo'yilgan aniq qoidalar bo'yicha ish yuritiladi.

Bozor yana umumiylikka ega bo'lishi kerak, agar bozorni kompaniyalar guruhi boshqarsa yoki bozor monopoliyasiga ega bo'lsa, bu bozor segmentida elektron tijorat yuritishning B2B modeli kutilgan natijalarni bermaydi. Bozor segmentidagi turli xil kompaniyalar va ishtirokchilar o'z maqsadlari yo'lida ish yuritishadi, lekin B2B modelini qo'llash va unda ishlash barcha uchun samarali natijalarni beradi. B2B modeli joriy etilgan ishlab chiqaruvchi kompaniyalar – o'z mahsulotlarini, texnologiyalarini sotishdan keyinchalik shu model bo'yicha elektron tijorat ishlarini olib borishdan katta yutiqlarga erishish imkoni yuqori bo'ladi.

Bu kompaniyalar axborot resurslariga ega bo'lishlari yoki bunga to'la huquqli hamkori bo'lib qoladi va bu jarayondan daromad olishda ishtirok etish imkoniga ega bo'ladi. Haridor – kompaniyalar yetkazib beruvchi va mahsulotlarini bir joydan olish, sifatli mahsulotlarning, narhlarini kamaytirish imkoniyatlariga Internetning paydo bo'lishi bilan birga biz bir lahzada so'nggi birja ma'lumotlari, on-line magazin, mobil aloqa kompaniyalarinig doyimo yangilanib va kengayib borayotgan xizmatlari, Internet provayderlari, IP-aloqa va boshqa turdagi minglab saytlaridan fiydalanish imkoniyatiga egamiz. Bunday qulaylik tovar va xizmatlar uchun tunu kun to'lovlarni amalga oshirish uchun zamin yaratadi.

Internet millionlab foydalanuvchilarining har biriga yirik auditoriyani yaratdi. Internet bugungi kunda butun jahon erkin bozoriga aylandi, elektron to'lov tizimlari esa sotuvchi va haridorlarning bir lahzada hisob-kitobi uchun imkoniyat yaratadi. 1998-yil 24-noyabrda Internet tizimida tovar va xizmatlar bozori ishtirokchilari o'rtasida hisob-kitoblarni xavfsiz real vaqt oralig'ida amalga oshirish, shuningdek, xususiy pul o'tkazmalarini amalga oshirish imkoniyatini beruvchi Web Money Transfer elektron to'lov tizimi o'z faoliyatini boshladi. Web Money Transfer – bu elektron hisob tizimi bo'lib, unda barcha foydalanuvchilar universal hisob birliklari bilan ayira boshlashlari mumkin: Web Money (WM) titul belgilari bilan.

WM titul belgilari bilan Internet tizimida tovar va xizmatlar uchun to'lov sifatida qabul qilinishi mumkin, undan tashqari WM titul belgilarini keng tarqalgan WM ayira boshlash shohobchalari orqali bank yoki pochta o'tkazmalariga, boshqa titul belgilariga ayira boshlash mumkin. O'z kompyuterida WM Keeper mijozlik dasturiy ta'minot tizimini ornatish bilan Web Money Transfer tizimi foydalanuvchisi maqomini oladi. Har bir Web Money Transfer tizimi foydalanuvchisi o'z

shahsiy WM – hamyonni ochadi (yoki turli xildagi WM titul belgilari uchun bir necha hamyonlarni), bu hamyondan boshqa bir istalgan hamyonga tovar va xizmatlar to'lov sifatida mablag'larni bir zumda o'tkazishi mumkin yoki xususiy o'tkazmani amalga oshirishni taqozo qiladi. Bunda o'tkazma uchun foyiz – o'tkazma miqdoridan 0,8 %, biroq mutanosib ravishda 50 dollardan oshmagan holda. Titul belgilarining hisobi, saqlanishi va bir zumda bir foydalanuvchining hisobidan boshqa foydalanuvchi hisobiga o'tkazilishi WM Keeper mijozlik dasturiy ta'minot tizimi tomonidan olib boriladi.

Web Money Transfer tizimida moliyaviy va huquqiy kafolatni tizim garantlari ta'minlaydi. Xavfsizlik tadbirlari majmuasi foydalanuvchilarning mablag'laridan noqonuniy foydalanish holatlarinig oldini oladi va ma'lumotlarning sir saqlanishini ta'minlaydi. Mahfiy habarlar orqali boshqa foydalanuvchilar bilan yopiq muloqot olib borish, shartnoma qismlarini muhokama qilish, to'lovlarni sharhlab borish mumkin. Amalda ko'rsatilganidek, Web Money Transfer tizimining himoyalanganlik darajasi boshqa to'lov tizimlarinikidan ko'ra ancha yuqori.

Web Money Transfer tizimida foydalanuvchilar o'rtasidagi bahsli holatlarni hal etish uchun hakamlik xizmati va foydalanuvchining xohish-istagiga qarab uning shaxsini tasdiqlovchi elektron raqamli attestatlar beruvchi WM – attestatlash xizmatlari mavjud Web Money Transfer quyidagi titul belgilari bilan muomala qiladi:

► WMY – O'zbekiston zonasida operatsiyalarni amalga oshirish uchun UZSning Y – hamyonlardagi ekvivalenti, WMY operatsiyalarining kafili bo'lib, «TILLO GARANT» MChJ O'zbek Kafolat Agentligi xizmat qiladi.

► WMR – rubl zonasida operatsiyalarni amalga oshirish uchun RURning R – hamyonlardagi ekvivalenti, WMR operatsiyalarining kafili bo'lib, Web Money Transgerning Rossiya hududidagi vakili «BMP» MChJ xizmat qiladi.

► WMZ – AQSh dollarida transfert operatsiyalarni amalga oshirish uchun USDning Z – hamyonlardagi ekvivalenti.

► WME – YEVROda operatsiyalarni amalga oshirish uchun EUR ning E-hamyonlardagi ekvivalenti, WMZ va WME operatsiyalarining kafili bo'lib, Amstar Holdings Limited. S.A. xizmat qiladi.

► WMU – Ukraina zonasida operatsiyalarni amalga oshirish uchun UAHning U – hamyonlardagi ekvivalenti, WMU operatsiyalarining kafili bo'lib, «Украинское Гарантийное Агентство» MChJ xizmat qiladi.

2005-yilning 20-sentabr kuni 24 ta tashkilot (kompaniya) axborot

texnologiyalari tashkilotlari assotsiatsiyasini tuzishga o'z xohishlarini bildirgan holda hujjatni imzolashdi. Internet yildan yilga kompaniyalar faoliyotiga chuqur kirib bormoqda. Internetda olib boriluvchi biznes, an'anadagidan tubdan farq qiladi. Bu internetga kiruvchilar sonining ortishi va biznes sohasining savdodagi asosiy kanalga aylanishi bilan bog'liq.

Tabiiyki, Internet, birinchi navbatda, elektron sayt va pochtaga asoslanadi. Bu ikkalasi 1971-yil «Eskisi» va ikkinchisi «Yosh» 1993-yil, virtual olamda biznesni yuritish imkoniyatini beradi. Elektron pochtaning kam chiqimli, tezkor himoyalanganligi, ma'lumotlarni arxivlash imkoniyati va boshqa, saytda esa mahsulotlar va xizmatlar reklamasining to'liq o'rnatilishi internetda biznesni yuritishga yaxshi imkondir. Internetda biznesni yo'lga qo'yishning turlaridan misollar keltiramiz:

► kompaniya internetga ulangach, zaruriy axborotlarni yig'ishda xarajatlarni kamaytiradi. Ertami yoki kechmi sizning kompaniyangiz marketing bo'yicha axborotlar yetishmasligini sezadi, ya'ni mijozlarni qayerdan izlash, ularni nima qiziqtiradi, bozorning talabi qanday va uning rivojlanish istiqboli qanaqa kabi ko'plab savollarga internetdan javob topish mumkin. Doimiy ravishda gazetalar o'qish, qirqib olish, qimmat konsultant yollash shart emas. Internetning **Rauber**, **List, Yahoo** kabi qidiruv sistemalaridan ma'lumotlarni topish mumkin. Asta - sekin siz doimiy qiziq axborotlarni chop etuvchi saytlarni topib olasiz. Ular tez va bepul. Agar sizda saytlardagi yangiliklarni o'qishga vaqt bo'lmasa, siz u holda bepul ma'lumotlarni uzatish xizmati kursidan foydalanishingiz mumkin. Masalan: **subscribe.ru** 2000 ta yangiliklarni uzatish imkoniyatiga ega. Siz o'zingizni qiziqtirgan har qanday mavzudagi yangilikni topishingiz mumkin. Bunga obuna bo'lish 3 minutdan ortiq vaqtni egallamaydi. So'ng sizning pochtangizga doimiy ravishda axborotlar tushib turadi.

► Adres, telefon, mahsulotlar haqida ma'lumotlarni operativ olish. An'anadagi usullar o'zini oqlamaydi. Spravochniklar pechatdan chiqquncha eskirib ulguradi. 09 ga telefon qilib, tushish oson emas, bundan tashqari har doim ham kerakli ma'lumotlarni olishga erisha olmaysiz. Shu kabi muammolarni yechishda tarmoq yordam beradi. Yuzlab spravochniklar, telefon raqamlari, banklar, buxgalteriya, qonun chiqaruvchi organlar va boshqalar sizning xizmatingizda. Ko'plab xizmat ko'rsatishlar bepul, ular reklamalar hisobiga foyda ko'rishadi. Masalan: **List.ru** – katalogida 775 ta oziq-ovqat mahsulotlari savdosi bo'yicha, shuningdek, elektron do'konlar bo'yicha 388, spravochniklar, adreslar

va telefonlar bo'yicha 165 ta, 348 ta transport jadvallari bo'yicha ma'lumotlar katalogi registratsiyadan o'tgan (http://list.ru/catalog/)

► Bepul va tez adreslarni tanlash – **Cyberatlas** manbasidan foydalangan holda g'arbda 67 % korxonalar xodimlarni tanlash va ishga o'rnatishda tarmoqdan foydalanadi. Yangi ishchi-xodimlarni ham maxsus saytlar orqali qidirib topish mumkin. Yoki o'zining xususiy sayti orqali topish mumkin. Har ikkala variant ham qlay. Birinchi o'rinda siz vakant joy uchun odam topasiz va unga vakant taklif etasiz.

► Mahsulot va xizmatlar uchun xarajatlarning kamayishi. Ko'plab kompaniyalar mahsulotlar va xizmatlar uchun to'lov narxlarini xususiy saytlariga joylashtirishadi. Ular **prays-listlar** deyiladi. Amaliyotchilarning 90 % zarur axborotni zarur axborotni tarmoq orqali Internetdan topib, tahlil qilib, so'ng savdoni amalga oshiradi. Bir xil mahsulotni 100 xil narxda ko'rish mumkin. Ularning narxlari va **postavka**-mahsulotni yetkazib berish usullarini taqqoslash mumkin.

Mijozlarni qidirish, ularni nima qiziqtirishi, bozorning ahvoli va uning rivojlanishi, raqobatchi kimligi kabi zarur axborotlarni internetdan olish vaqtni tejaydi.

► Tashqi kommunikatsiya uchun xarajatlarni kamaytirish Faks xabarlari va oddiy pochtani biznes korrespondnesiya elektorn pochta siqib bormoqda. Shu yil amerika kompaniyalaridan birining *izlanishlari* kommunikatsiyaning yangi turlari bo'yicha istiqbolli afzalliklarini aniqladi. Minglab xizmatchilar so'rovnomadan o'tkazildi. Ularning 80 foizi oddiy pochtadan ko'ra elektron pochtadan foydalanishni, 73 foizi esa E-mail faksli aloqani ma'qul deb topgan. Bir kompyuterdan boshqa kompyuterga uzatilayotgan elektron xabar 1 minut ichida amalga oshiriladi. Faksli aloqada aniq muammolarga duch kelish mumkin:

1) telefon stansiyalari va podstansiyalarning katta territoriyada ekanligi, qurilmalarning eskirganligi, kunduzgi vaqtda nagruzkaning to'g'rilay olmaslik. Abonentlarning tarmoqda bir-biriga tushishi qiyinligi, natijada vaqtning yo'qotilishi;

2) faks orqali uzatiluvchi xabar hamma vaqt ham yaxshi sifatli bo'lavermaydi. Ko'pincha, xabarlarni o'qib bo'lmaydi. Ko'pgina kompaniyalar *avtomatik rejimli faks apparatidan* foydalanadi. Shuning uchun yana bir marta faks qanday o'tganligini aniqlash uchun qayta telefon qilish kerak bo'ladi. Aloqa xarajatlari o'sib boradi.

Agar elektorn pochtadan foydalanilsa, bunday muammolarga duch kelinmaydi. Internetda shaxsiy sayt osish mumkin. Lekin 200–1000 dollar buyurtma uchun to'lanishi lozim. Bu biroz qimmatga tushadi. Buning bir necha variantlari mavjud.

1-sayt-vizitka. Xuddi amaldagi vizitkalar kabi, zarur va kerakli, unda kompaniya nomi, kontakt informatsiya, logotip, faoliyat ko'rsatish sohasi bo'yicha umumiy ma'lumotlar bo'lishi kerak. Ba'zan prays-listlar publikatsiya qilinadi. Rahbarlar haqida ma'lumotlar bo'lishi mumkin. Masalan: http://www.chat.ru/qsamis/, http://www.sura.ru/molkom/.

2-sayt-buklet. Bunda kompaniyaning yillik hisoboti, mahsulotlar katalogi va boshqalarning qog'ozdagi hujjatlarning internetdagi elektron versiyasi yaratiladi. Masalan:http://www.redoct.msk.ru.

3-sayt vitrina. Katalogdan tashqari navbatdagi ma'lumotlar, xizmatlar, kompaniya yangiliklari, ishlab chiqarish bo'yicha qo'shimcha ma'lumotlar, maslahatlar, analitika va boshqalarning elektron versiyai yaratiladi. Masalan: http://www.nestle.ru.

4-elektron magazin -elektron vitrinani tashkil etadi. Ya'ni unga kiruvchilar bilan interaktiv rejimda ishlaydi. Undagi materiallar doimiy ravishda yangilanib turadi. Foydalanuvchi nafaqat bu mahsulotlar haqida zarur axborot olishi, balki, mahsulotlar va xizmatlarga buyurtma berishi, mos hujjatlarni rasmiylashtirishi, sohaga tegishli mutaxassisdan maslahatlar olishi mumkin. Masalan:http://www.grdart.ru/index.htm.

2.7. Universal elektron to'lov sistemasi (UEPS)

UEPS elektron to'lov sistemasi konsepsiyasi va ishlatish texnologiyasi fransuz kompaniyasi **NET 1** International tomonidan ishlab chiqilgan. Uning asosiy texnologik prinsipi barcha moliyaviy transaksiyalarni **off-line** rejimida ish yuritib bajarish. Axborotni shifrlashda asosiy algoritm **DES** hisoblanadi. Yuqori kriptoturg'unlikka erishish uchun uzunligi 8 bayt bo'lgan kalit orqali ikki karrali shifrlashni amalga oshiradi. To'lov sistemalarida ish yuritish jarayonini nazorat qilish mikroprotsessorli kartaga tushadi, chunki bunday karta **UEPS**ning asosiy elementi hisoblanadi. **UEPS**da uch xil mikroprotsessorli kartadan foydalaniladi:

* bank xodimining xizmat kartasi;
* sotuv kartalari;
* mijoz kartasi.

Barcha kartalar 8 bitli protsessordan tashkil topgan. UEPS sistemasida mijoz kartasining texnik xarakteristikasini tahlil qilamiz:

* Protsessor: **SGS-Thompson**, 8 bit, buyruqlar tizimi **Motorola 6805.**

* Operatsion sistema: Ko'pmasalali OS chip **MCOS** (Multi Tasking Chip Operation System).

* Tezkor (operativ) xotira: 160 bayt.
* Doimiy xotira: 6 Kbayt.
* **ESPPZU**: 2 Kbayt (16 Kbit).

Mikroprotsessor arxitekturasi axborotlarni mexanik tarzda o'qishga yo'l qo'ymaydi. Bordi-yu, o'qish qurilmasi elektron mikroskop vositasida skanerlasa, yoki ultrafioletli ta'sir ostida ishlasa, yoki kristalni qatlamlar bo'yicha arralash yo'li bilan ish yuritsa, mikroprotsessor butunlay ishdan chiqadi. Microprotsessorli kartaning arxitekturasi shunday yaratilganki, protsessor xotiraning himoya qilingan joylariga murojaat bo'lganda, uni maxsus yaratilgan amaliy programma asosida nazoratga oladi. Kartaga axborot tashqaridan faqat shifrlangan holda keladi va kartaning ichki imkoniyatlari orqali mavjud kalitlar bilan shifrdan chiqariladi. Kartadan chiqib ketayotgan axborot ham xuddi shunday yo'l bilan shifrlangan holatda bo'ladi. Bank kalitlari hech qachon kartalarni ochiq holatda bayon etmaydi.

To'lov sistemasining arxitekturasi va tarkibi. To'lov sistemasining asosiy tizim tashkil etuvchi qismi-emissiya markazi hisoblanib, u quyidagi vazifalarni bajaradi:

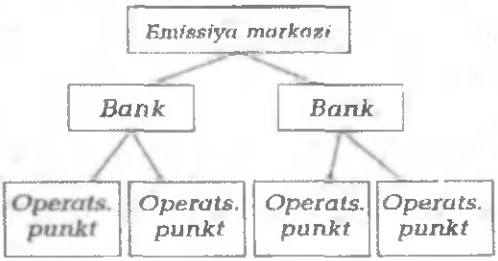
♦ To'lov sistemasining bosh kalitini generatsiya qilish.

♦ Mikroprotsessorli kartalarning boshlang'ich emissiyasini tashkil etish, ya'ni kartalarga unikal seriyali raqamlar(USN)ni berish, kartaga umumtizimli, nazorat qilinadigan axborotlarni kiritish, kartaga sistemaning bosh kalitini kiritish mumkin.

♦ Sistemaga yangi kiritilayotgan bank ekvayer va bank emitentlarning hisobotlari ma'lumotnomalarini kiritish

♦ Sistemaga kartalar turi va valuta kodlari haqidagi ma'lumotnomalarni kiritish

♦ Sistemaga zavod raqamlari to'qrisida va **USM**dagi kartalar tartib raqami bilan tuzilgan ma'lumotni kiritish.



30-rasm. **To'lov sistemasi arxitekturasi**

To'lov sistemasining ikkinchi bosqichida ishtirokchi banklar turadi. To'lov sistemasining ishtirokchi banki – bu moliya instituti bo'lib, u mikroprotsessorli kartalardagi hisobotlarni va transaksiya masalalarini hal etishga ko'maklashadi. Har bir ishtirokchi bank o'z kartalarini chiqarishdan oldin emitent va ekvayer uchun kalitlar majmuyini yaratadi. Bu kalitlar emissiya paytida va moliyaviy transaksiyani tashkil etishda asqotadi. Ishtirokchi banklar texnik vositalari qatorida **AIJ** (avtomatlashtirilgan ish joylari) ham mavjud.

To'lov sistemasi ierarxiyasining uchinchi bosqichida Operatsion punktlar joylashgan bo'lib, ular ishtirokchi bankning struktura tarkibini tashkil etadi, ya'ni mijozlarga xizmat ko'rsatish operatsiyalarini bajaradi.

Kalitlar va parollar taqsimoti. **UERS** tizimining xavfsizligini saqlash maqsadida kalit va parollarni juda ehtiyotkorlik bilan taqsimlash sxemasini avvaldan rejali tuzish lozim. Masalan, **R0** – kalitlar kartaga kirishning bog'ichi bo'ladi va u faqat emissiya markaziga ma'lum hamda shu markaz tomonidan tayinlanadi. **R1** – parollar guruhi uchun **PIN B** – bank operatori paroli, **PIN M** – magazin hisobchisi paroli, **PIN 1** – kartaga ma'lumotlarni kiritish paroli bo'lib u faqat karta egasigagina ma'lum. Mijoz tomonidan faqat of-line terminalida o'zgartiriladi. **PIN 2** – guruhi parollarida **RFU** – zaxiradagi parol, PIN 2 – kartadan ma'lumotlarni olib tashlash paroli. **R3** va **R4** ham zaxira parollari hisoblanadi. **R5** va **R7** session kalitlar ishlatilgandagi parollar. **R6**-kalitlar **(KIx, KAx)** ga yozish uchun ishlatiladi. Bu parol ishtirokchi bank tomonidan tayinlanadi. **R6–RFU** zaxiradagi parol.

Savdo terminallari. Savdo va bank tarmoqlari **EFT-10** terminallari va **UEPS** programma ta`minoti bilan ta`minlangan. Terminalda kartalarni o'qish uchun 2 ta qurilmasi mavjud bo'lib, birinchi qurilmaga sotuvchi kartasi, ikkinchisiga esa xaridor kartasi o`rnatiladi. Savdo terminali doimo bank tashqarisida bo'lgani uchun xavfsizlik jihatidan juda himoyaga muhtoj bo'ladi. Shuning uchun ham unga biror parol yoki bank kalitini, shifrlash algoritmini va moliyaviy transaksiyani berish mumkin emas. **UEPS** to'lov sistemasida savdo terminali hech qanday maxfiy ma`lumotni saqlamaydi va faqat sotuvchi bilan xaridor o'rtasidagi interfeys vazifasini bajaradi. Barcha to'lov operatsiyalari ikki karta o'rtasidagi muloqot bilan belgilanadi. Bu holatda barcha axborot session kalitlar vositasida shifrlanadi.

Session kalitlarni tashkil etish. Mijoz kartasi tasodifiy sonlar to'plamidan tasodifiy bir sonni tanlab oladida, uni **R5, R7** kalitlar bilan

shifrlab sotuvchi kartasiga bildiradi. Sotuvchi kartasi esa shifrlangan sonni shifrdan chiqarib berilgan ma'lumotga ega bo'ladi. Berilgan shu sonni turli kalitlar kombinatsiyasi bilan taqqoslab, mijoz va sotuvchi kartasi uchun umumiy session kalitni yaratadi. Bu kalit faqat ikkala karta xotirasida saqlanadi. Shu session kalit asosida barcha axbortlar shifrlanadi.

Kartalar emissiyasi. Emissiya protsedurasi quyidagi uch bosqishdan iborat:

* emissiya markazi tomonidan tizim kalitlarini tasdiqlash;
* ishtirokchi banklar tomonidan bank kalitlari va parollarini tasdiqlash;
* ishtirokchi bank tomonidan mijoz kartasini shaxsiylashtirish.

Bulardan ikkita birinchi bosqichi o'ta maxfiy bo'lib, maxsus bo'limlarda xavfsizlikni saqlagan holda bajariladi. Uchinchi bosqichi esa bank operatori tomonidan maxfiy bo'lmagan holda mijoz ishtirokida bajariladi.

Emissiya jarayoni quyidagicha bajariladi: emissiya markazi uch turli kartalar (bank, mijoz va savdo kartalari) tirajini oladi. Barcha kartalar formatlangan va **UERS** programma ta'minoti bilan ta'minlangan. Barcha kartalarga kirish $\mathbf{R_0}$ – transport kaliti bilan berkitilgan.

Emissiyaning birinchi bosqichi (maxfiy faza) emissiya markazida bajariladi, ya'ni kartalarga $\mathbf{R_0}$ kaliti bilan kirib, ularga kalitlar ustasi (masteri) orqali emissiya markazining xususiy $\mathbf{R_0}$ – kaliti beriladi, $\mathbf{R_7}$ va $\mathbf{R_8}$ sistema kalitlari vositasida har bir kartaga unikal tartib raqami – **USN** o'rnatiladi.

Emissiyaning ikkinchi bosqichi(maxfiy faza) ishtirokchi bank tomonidan har bir olingan kartalar tiraji uchun xavfsizlik choralari ko'riladi, ya'ni bank va savdo kartalariga $\mathbf{R_1}$ va $\mathbf{R_6}$ – parollari o'rnatiladi. Bank va savdo kartalariga $\mathbf{R_6}$ – paroli taqdimotida $\mathbf{KI_1}$ va $\mathbf{KI_2}$ parollari bank kartalariga, $\mathbf{KA_1}$ va $\mathbf{KA_2}$ – savdo kartalariga beriladi. Bundan tashqari, bank kartalarga qo'shimcha ma'lumot (valutalar kodi, do'konlar haqida ma'lumot va h.k.)lar ham kiritiladi.

Emissiya uchinchi bosqichi (kartalarni shaxsiylashtirish)da ochiq operatsiyalar o'tkaziladi, ya'ni bank operatori tomonidan mijoz ishtirokida kartalar kerakli ma'lumotlar bilan to'ldiriladi. Bunda mijoz kartaga **PIN 1** va **PIN 2** parollarini o'zining alohida klaviaturasidan joylashtiradi. Bank operatori kartasi o'zining shaxsiy **PIN B** paroli bilan operatorning sistemaga kirishini nazorat qiladi. Bundan tashqari, bankning kartasi ham mikroprotsessorga kiritiladi. Shuning uchun ham kar-

tani shaxsiylashtirishda qaysi bankning qaysi operatori ish yuritgani ham rasmiylashtirilgan bo'ladi. Shuni ta'kidlash lozimki, bank operatori mijozning **PIN 1** va **PIN 2** parollari haqida ma'lumotga ega emas. Bu parollar sistemada saqlanmaydi. Ular mijoz tomonidan belgilanadi, shuning uchun ularni faqat mijoz va karta aniqlay oladi. Mijoz ruxsatisiz uning kartalari bilan ish yuritish mumkin bo'lmaydi.

2.8. Internetda elektron savdo va uning xavfsizligini ta'minlash

Bugungi kunda Internet orqali xalqaro elektron bozor vujudga kelmoqda. Elektron savdo deganda tovarlarni va pullik xizmat vositalarini global tarmoq orqali amalga oshirish tushuniladi. Hozirgi paytda eng ko'p tarqalgan elektron bozorlar turi bilan yaqindan tanishamiz.

1. Elektron savdoning an'anaviy ko'rinishlaridan biri – bu axborotlar savdosi hisoblanadi. Masalan, on-line rejimida ma'lumotlar bazasini sotib olishga obuna bo'lish (Rossiyada «Rossiya on-line», «Garant-Park» savdo markazlari ishlab turibdi).

2. Xorijda faoliyat ko'rsatayotgan «elektron magazinlar» o'z **Web-site**ga ega bo'lib, unda tovarlarning tezkor katalogi mavjud bo'lib, ushbu magazinlar xaridorlarning virtual aravachalari» (telejka)da kerakli tovarlarni jamlab kredit kartochkalari asosida sotuvni amalga oshiradi. Tovarlarni xaridorlarga jo'natish pochta orqali yoki elektron pochta kanallari vositasida yoki to'g'ridan to'g'ri Internet **Web-site** orqali amalga oshiriladi.

31-rasm. **Internetda elektron banklarning axborot almashuvi**

3. Elektron savdoning yangi turi – elektron banklar paydo bo'lishi bilan belgilanadi. Elektron banklarning asosiy yutug'i – bunday banklar tashkil etishning arzonga tushishi (katta imoratlarni arendaga olishning va qimmatbaho qog'ozlarni saqlashning ham keragi yo'q) va mijozlarni ko'plab yig'ib olish mumkinligidadir (Internet tizimining ixtiyoriy foydalanuvchisi elektron bankning potensial mijozi bo'la oladi).

Shuning uchun ham elektron bank mavjud banklarga nisbatan mijozlarga yuqori darajada foiz to'lash va tovarlar spektri xilma-xilligi hamda arzon narxda ekanligi bilan ajralib turadi. Tabiiyki, elektron bank o'zining xususiy xavfsizlik tizimida maxsus kartalarga ega bo'lib (bank serveridagi parollarga to'g'ri keladigan tasodifiy parollar generatoriga ega), mijozlarining har bir murojaatida unikal parol bilan ish yuritadi. Bundan tashqari, ancha arzon bo'lgan smart-kartalariga ham ega. Smart-kartalar esa session (seansli) kalitlarni generatsiya qilib ish yuritishadi.

Ma'lumki, Internet ish yuritish jarayonida 3 ta funksional xizmatni o'taydi:

1.Kommunikatsion.

2. Axborot (informatsion).

3.Boshqaruv.

Turli xizmatlar turlicha funkesiyani ta'minlaydi. Masalan, kommunikatsion va boshqaruv xizmatini ta'minlovchi serverlar bo'lgani uchun uning asosiy vazifasi – axborot qidiruvdan iborat bo'ladi. Mabodo bizga biror ma'lumot kerak bo'lib qolsa, darrov WWW axborot fazosiga murojaat qilamiz. Bu axborot fazosida 2 milliarddan ko'p hujjat joylashgan. Uning ichidan biz uchun kerak bo'lgan ma'lumotni topish – bu oson ish emas. Buning uchun maxsus axborot qidiruv servislari bo'lishi kerak (bunday servislar bepul xizmat qiladi). Qidiruv servislari maxsus Web tugunlaridan iborat bo'lib, mijoz so'roviga giperuzatishlar ro'yxatini topib beradi. Ushbu vazifani bajarish uchun bir qator modellar yaratilgan. Ular ichidan eng ommabop bo'lganlari bu:

- ► qidiruv kataloglari,
- ► qidiruv ko'rsatkichlari,
- ► portallar.

Qidiruv kataloglari. Qidiruv kataloglari katta kutubxonalarning tematik katalogi kabi ish yuritadi. Qidiruv kataloglariga murojaat qilinsa, uning asosiy sahifalarida qisqartirilgan ulkan tematik kategoriyalar ro'yxatiga duch kelamiz. Masalan, iqtisod va tadbirkorlik kategoriya ro'yxatidagi har bir yozuv – bu giperuzatishdir. Shulardan biror mavzu ustida «sichqoncha» tugmasi bosilsa, bo'limlar ro'yxati kelib chiqadi. Masalan, elektron to'lov tizimi, yoki Internet do'konlari. Shular ichidan keraklisi Web hujjat sifatida tanlab olinadi.

Qidiruv kataloglari bilan ish yuritish oson, ammo uni tashkil etish juda murakkab masala, chunki qidiruv kataloglari qo'l meqnati bilan amalga oshiriladi. Jahonda eng yirik qidiruv katalogi – Yahoo (WWW.yahoo.com) bo'lib, unda 150 dan ortiq redaktor (muharrir) xiz-

mat qiladi. Undagi Web resurslar milliondan ortiq bo'lib, Internet xizmatining atigi 10 %ni tashkil etadi.

Rossiyada shunday qidiruv kataloglaridan 100 dan ortiq muharrirga ega Atrus (WWW.atrus.ru) katalogi mavjud. Umuman olganda, dunyoda qidiruv kataloglari ko'p emas. Sababi: xizmat qilishning ancha mushkulligi, yaxshi malakaga ega redaktorlar va kadrlar etishmasligi hamda WWW resurslardan foydalana bilish past darajada. Shuni e'tiborga olib, qidiruv ishlarini kataloglardagidek qo'lda bajarmay, avtomatlashtirish uchun qidiruv ko'rsatkichlari modellari ishlab chiqilgan. Qidiruv ko'rsatkichlarini asosiy ish yuritish prinsipi – Web resurslari kalitli so'zlar bilan qidirish jarayonini tashkil etish hisoblanadi. Bunda qidiruv tizimi so'rov asosida Web-sahifalar ro'yxatini berib, u giperuzatishlar bilan bir vaqtda topilgan resurslar to'g'risida qisqacha xabar beradi. Bugungi kunda Jahonda 10 000 dan ortiq qidiruv ko'rsatkichlari ishlab chiqilgan. Masalan, **Alta Vista, GoTo, Google, Excite, Aport, Yandex, Rambler**.

Qidiruv ko'rsatkichlari bilan ish yuritish 3 bosqichda amalga oshiriladi. Ulardan 1- va 2-bosqichi tayyorlov bo'lib, mijoz uchun bilinmaydi. 3-bosqichida esa qidiruv ko'rsatkichi foydalanuvchi bilan birgalikda ish yuritadi. 1-bosqichida qidiruv tizimi WWW informatsion fazoni skanerlaydi. Buning uchun maxsus «chuvolchang» degan dastur bilan ish yuritiladi, ya'ni avtomatik ravishda tarmoqda kichik o'lchovli «chuvolchang» Web resurslarni giperuzatish asosida qidira boshlaydi. Bordiyu, bu resurs qidiruv tizimiga noma'lum bo'lsa, undan o'zining MBsiga nusxa olib qo'yadi.

Qidiruv «chuvolchangi» samarali ish yuritsa, qidiruv ko'rsatkichining mazmun-mohiyati o'zgara boradi. Shu usulda tashkil etilgan MB indeksatsiyalanadi, chunki foydalanuvchi oniy sekund davomida o'z so'roviga javob olishi kerak. So'ngra filtrdan o'tkazilib alfavit bo'yicha saralanadi. 3-bosqichida esa uzatishlar ro'yxati tuziladi. Natijaviy ro'yxatni rafinlash qidiruv natijasini filtrdan o'tkazish va baholash (ранжировка)dan iborat.

Shuni qayd etish lozimki, Web-sahifalari ortgan sari qidiruv ko'rsatkichlari krizisi vujudga keladi. Sababi: Web-sahifalari hajmi ortishi bilan qidiruv ko'rsatkichlari dinamikasida mutanosiblik paydo bo'ladi. Masalan:

1. Web resurslarni qidiruv ko'rsatkichi tushib keta boshladi.

2. Qidiruv ko'rsatkichlaridagi indeksatsiyalash jarayoni eng zamonaviy elektron qurilmalar (moddiy-texnik ta'minot), malakali kadrlar va dasturiy resurslar yetishmay qolmoqda.

3. Yirik-yirik investorlar soni ko'payib, ularning Internet xizmatiga murojaati ortib bormoqda. Natijada bir qator qidiruv ko'rsatkichlari uchun aksionerlash jarayoni boshlanib ketdi. Aksionerlar so'rovini bajarish uchun qidiruv tizimlari endi Web resurslarni indeksatsiyalash emas, balki aksionerlarni qanoatlantirishga o'tib ketmoqda, ya'ni savdo jarayoni boshlanmoqda.

4. Web-sahifalari hajmi ortishi bilan mijoz uchun juda ko'p giperuzatishlarni qidiruv tizimi chiqarib bermoqda. Ular ichidan keraklisini tanlash mijozning ko'p vaqtini olmoqda yoki bir qidiruv tizimi o'zidan xoli qilish uchun mijozni ikkinchi bir qidiruv tizimiga jo'natib yuborishga intilmoqda. Masalan, (www.inrtomi.com) boshqa qidiruv tizimi topshirig'ini bajaradi.

Demak, yangi qidiruv texnologiyalarini ishlab chiqish kerak bo'lib qolmoqda, SMART-texnologiyasi yordamila avtomatik ravishda kataloglar yaratish yoki Aloqa (www.abxa.com) markaziy serverga murojaat qilib mijoz dasturini Internet Explorer vositasida hal etish mimkin.

Internetdan yangiliklarni muntazam ravishda olish imkoniyati bor. Bu imkoniyatni server ta'minlaydi. Serverga yangi ma'lumot kelib tushganda, ma'lumot avtomatik tarzda shu ro'yxatda yozilgan foydalanuvchilar adreslariga jo'natiladi. Har bir ro'yxat biror mavzuga bag'ishlangan bo'ladi. Shu ro'yxatdagi ma'lumotlarni muntazam ravishda olish uchun unga foydalanuvchi ismi yozilishi shart. Ro'yxatlar odatda ikki turli bo'ladi: ***munozara va informatsion***.

Munozara ro'yxatidan foydalanuvchi boshqalar fikrini bilish imkoniyatiga ega. Bunda barcha foydalanuvchilar muhokamada qatnasha oladi.

Informatsion ro'yxatlar yangiliklarni keng foydalanuvchilar ommasiga tarqatadi, ya'ni foydalanuvchilar ma'lumotni qidirishga vaqt sarf qilmaydilar.

Ro'yxatlarga yozilish tartibi quyidagicha: biror ommabop sahifaga kirish yoki yozilish jarayonida ro'yxatlar imkoniyati taklif etiladi. U yerda ro'yxatga yozilish taklif etiladi. Masalan, **Yandex** yangiliklaridan foydalanish kerak bo'lsa, **Yandex.ru** da ism (login) qayd etilishi lozim. Buning uchun login va parolni kiritib, **Зарегистрироваться** tugmasi bosiladi. Shunda ekranda muayyan shakl paydo bo'ladi, uning maydonlariga foydalanuvchi o'zi haqida kerakli ma'lumotlarni kiritib OK tugmasi bosiladi. Yangiliklarni muntazam ravishda olish kerak bo'lsa, u holda **Подписка** tugmachasini ishga tushirish shart.

Nazorat uchun savollar

1. Elektron to'lov tizimi haqida qanday fikr yuritasiz?
2. Plastik karta deganda nimani tushundingiz?
3. Elektron savdo tizimi nima?
4. Elektron bozor qanday amalga oshiriladi?
5. Elektron imzo nima uchun kerak?
6. Elektron banklar an'anaviy banklardan nimasi bilan farq qiladi?
7. Elektron bozor strukturasini ifodalang.
8. Elektron bank strukturasi nimalardan tashkil topgan?
9. Savdo terminallari haqida fikr bildiring.
10. Session kalitlar qanday yaratiladi?
11. Bankomatlar xavfsizligini ta'minlashda qanday usullar mavjud. Ularning umumiyligi va farqi nimada?
12. Bank ekvayerning ish yuritish texnologiyasi qanday?
13. Bank emitent qanday vazifalarni bajaradi?
14. Universal UEPS sistemasi haqida fikr bildiring.
15. Tarmoqlararo himoya vositalari haqida gapiring.
16. Kompyuter tarmoqlarida xavfsizlik sxemasi.
17. Xavfsizlikni ta'minlashning dasturiy vositalari.
18. Smart-kartalar bilan plastik kartalar o'rtasidagi o'xshashlik, umumiylik va farq nimada?
19. Elektron savdoning asosiy turlari haqida gapiring.
20. PIN parollarining vazifalari nimadan iborat?
21. Kartalar emissiyasi nimadan iborat?
22. Bankomatning xavfsizligi qanday ta'minlanadi?

Testlar

1. AAQIT tizimida axborotlardan soxta yo'l bilan foydalanuvchi shaxslar tug'diradigan xavfni bartaraf etuvchi eng oddiy usullarni ko'rsating.

A. foydalanuvchilar doirasini cheklash

B. axborotdan foydalanish doirasini cheklash, axborotni kriptografik o'zgartirish, foydalanuvchi shaxslar nazorati va hisobotini o'rnatish

C. axborot xavfsizligini ta'minlovchi har turdagi qonuniy choralarni qo'llash

D. A, B, C to'g'ri

2. Mahalliy yoki korporativ tarmoqlarda xavfsizlikni ta'minlash uchun qanday tarmoqlararo ekranlar himoya sxemalari mavjud?

A. tarmoqlararo ekran – filtrli marshrutizator

B. ikki portli shlyuz asosidagi tarmoqlararo ekran

C. ekranlashgan shlyuz asosidagi tarmoqlararo ekran

D. ekranlangan tarmoqli tarmoqlararo ekran va A, B, C barchasi.

3. Hozirgi kunda eng katta ahamiyatga molik to'lov tizimining avtomatlashgan savdo sistemasi POS terminallar va bankomat hisoblanadi.

A. B, C

B. POS terminallar

C. bankomatlar

D. elektron kredit kartalari

4. SKIP (Secure Key Internet Protocol) texnologiyasi IP paket grafikasini standart muhofaza qiladigan jarayon bo'lib, tarmoq orqali yuboriladigan ma'lumotlarni himoya qilishni amalga oshiradi. Shu texnologiya bo'yicha muhofaza qilishning 2 ta usuli mavjud. To'gri javobni ko'rsating.

A. IP paket bloklaridagi axborotlarni shifrlaydi, SKIP paketga IP paketni joylashtirish (inkapsulyatsiya).

B. Diffi-Xelman usuli, inkapsulyatsiya usuli

C. tarmoqdan foydalanish vaqtini cheklash, tarmoqqa kirish maxsus adreslarni belgilash,

D. tarmoqqa kiruvchi ishchi stansiyalar sonini cheklash, bir necha bor noto'g'ri parol bilan tarmoqqa kiruvchi shaxsga tarmoqqa kirish man etilishi.

5. Hujjatni imzolashda dastlab hujjat hajmini iloji boricha birnecha o'n yoki yuz baytlar atrofida «siqiladi». Bu jarayon qanday amalga oshiriladi?

A. simmetrik shifrlash jarayoni

B. kalitlar generatsiyasi yordamida amalga oshiriladi

C. xesh funksiyasi yordamida amalga oshiriladi.

D. to'g'ri javob yo'q

6. ishlash prinsipiga asosan plast kartalar ikki turga bo'linadi:

A. passiv plast kartalar va faol (aktiv) plast kartalar.

B. sanash vazifasini o'taydigan schyotchik-kartalar, mikroprotsessorli kartalar

C. xotiraga ega kartalar, passiv kartalar

D. mikroprotsessorli kartalar, faol kartalar

7. PIN qiymatini tekshirish kim tomonidan bajarilishi kerak.

A. bank ekvayyr tomonidan bajarilishi kerak

B. operator tomonidan PIN qiymati shifrlangan bo'lishi tekshirilishi kerak

C. pulni o'tkazish uchun yuborilgan so'rov haqiqiyligi mijoz tomonidan tekshirilishi kerak

D. bank emitent tomonidan bajarilishi kerak

8. Imprinter nima uchun ishlatiladi?

A. har xil schyotlar holati haqida ma'lumotlar berish uchun

B. plastik kartalar vositasida naqd pul to'lash va inkassatsiya uchun

C. imprinter – to'lov kvitansiyalarini amalga oshirish uchun ishlatiladi.

D. naqd pullarni berish uchun ishlatiladi

9. Ikki firma o'rtasidagi elektron tijorat nima deb ataladi?

A. firma–firma

B. biznes–biznes

C. biznes–mijoz

D. firma–mijoz

10. O'zbekistonda Web Money tizimi bo'yicha qaysi tashkilot mijozlarga xizmat qiladi?

A. TILLO GARANT MChJ

B. Web Money Uzbek MChJ

C. UzTransfer MChJ
D. TIF Milliy banki

11. O'zbekiston uchun qaysi Web Money Transfer titul belgisi qabul qilingan?

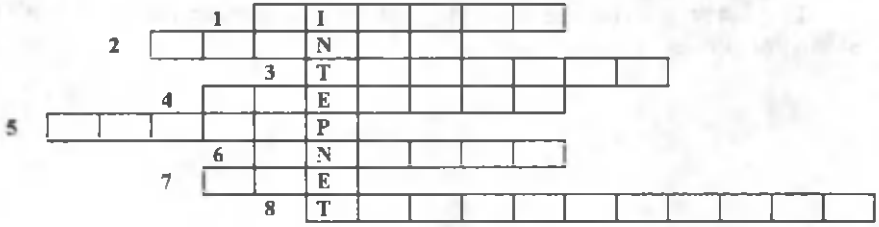
A. WMY
B. WMR
C. WMZ
D. WME

12. AQSh dollarida transfert operatsiyalarni amalga oshirish uchun USD ning ekvivalenti ayting

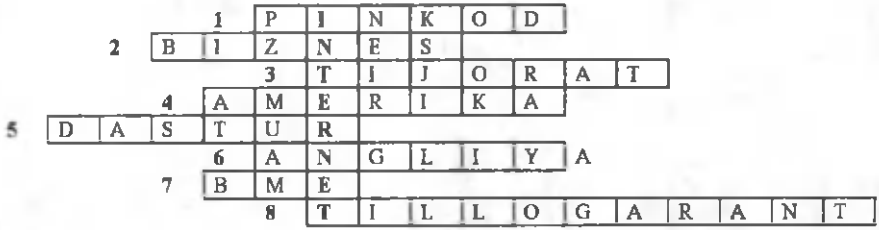
A. Y
B. R
C. Z
D. E

Krossvord

1. Elektron tijorat xavfsizlik choralaridan biri...
2. Elektron tijorat turi ... ... – *Mijoz.*
3. Zamonaviy elektron .....
4. Elektron tijorat eng ko'p tarqalgan davlat
5. Elektron tijoratni amalga oshirish uchun zarur narsa
6. Internet-bank qayerda paydo bo'lgan?
7. YEVRO uchun Web Money Transfer titul belgisi.
8. O'zbekistonda Web Money Transfer xizmatini ko'rsatuvchi tashkilot.



Krossvord javoblari:



Foydalanilgan adabiyotlar

1. Анин Б. О шифровании и дешифровании. Конфидент, 1997.

2. Балакирский Б.В. Безопасность электронного платежа. Конфидент, 1996.

3. Гедеев А.А. Электронное государство. Елит, 2008.

4. Гайкович В. Компьютерная безопасность. Банковская технология, 1997.

5. Желников В. Криптография от папируса до компьютер. АБФ, 1997.

6. Завалеев В. Пластиковая карточка как платежный инструмент (основные понятия) http://citforum.ru/marketing/articles/art_8.shtml

7. Ikromova X.Z. Internet asoslari / (o'quv qo'llanma). –T.: TAQI, 2001.

8. Ikromova X.Z. Zamonaviy kompyuter texnologiyalari / (o'quv qo'llanma). –T.: TAQI, 2001.

9. Ikromova X.Z. Informatika / (o'quv qo'llanma). –T.: TAQI, 2000.

10. Ikromova X.Z. va boshqalar. Informatika, axborot texnologiyalari / (o'quv qo'llanma). –T.: TDTU, 2003.

11. Ikromova X.Z. Axborot va kommunikatsiya texnologiyalari / (o'quv qo'llanma). – T.: TIU, YUNESCO, 2004.

12. Abdullayev R. A., Ibragimov. Iqtisodiy axborotni ishlashning avtomatlashtirilgan tizimlari. Toshkent. 1995.

13. Мельников В.В. Защита информации в компьютерных системах. –М.: Финансы и статистика, Электроинформ. 1997.

14. Романцев Ю. Зашита информации в компьютерных системах и сетях. –М.: «Радио и связь», 1999, №3.

15. Тайли Е. «Безопасность персоналного компьютера». –М.: ООО «Попури», 1997.

MUNDARIJA

O.T. KENJABOYEV, A.SH. ALLANAZAROV

AXBOROT TIZIMI XAVFSIZLIGI

O‘quv qo‘llanma

Muharrir E. Bozorov
Badiiy muharrir M. Odilov
Kompyuterda sahifalovchi A. Tillaxo‘jayev

Nashr lits. AI № 174, 11.06.2010.
Bosishga ruxsat 19.03.2013da berildi. Bichimi 60×84 1/16.
Ofset qog‘ozi №2. «Times New Roman» garniturasi. Shartli b.t. 5,81.
Nashr-hisob t. 6,25. Adadi 100 dona.
10-buyurtma.

«IQTISOD-MOLIYA» nashriyotida tayyorlandi.
100084. Toshkent. Kichik halqa yo‘li ko‘chasi, 7-uy.

«HUMOYUNBEK-ISTIQLOL MO‘JIZASI» bosmaxonasida
ofset usulida chop etildi.
100003. Toshkent. Olmazor ko‘chasi, 171-uy.