O`ZBEKISTON RESPUBLIKASI
OLIY VA O`RTA MAXSUS TA'LIM VAZIRLIGI

ANDIJON MASHINASOZLIK INSTITUTI

“MASHINASOZLIK ISHLAB CHIQARISHINI AVTOMATLASHTIRISH”
kafedrasi

“INFORMATIKA VA AXBOROT TEXNOLOGIYALARI”
fanidan

KURS ISHI

Mavzu: ***Internetda axborotlar xavfsizligini ta’minlash asoslari***

Bajardi: ***“Avtomatika va elektrotexnologiya” fakulteti “TJIChAB” yo’nalishi 1-kurs 2-guruh talabasi Qobiljonov A.***

Tekshirdi: ***Jamoldinov S.***

Andijon- 2012 й.

R E J A

I. Nazariy qism.

1.1. Kirish.

1.2. Internetda ruxsatsiz kirish usullarining tasnifi .

II. Asosiy qism.

2.1. Elektron pochtada axborotlarga nisbatan mavjud xavf- xatarlar va ulardan himoyalanish asoslari

2.2. Elektron tulovlar tizimida axborotlarni himoyalash

III. Amaliy qism

3.1. $P = \prod_{i=1}^{5} \sum_{j=1}^{6} \frac{i+j}{2a}$ **кko'paytmani hisoblash dasturini tuzing, bu yerda** $a = 5$**.**

Xulosa.

Foydalanilgan adabiyotlar.

1.1. Kirish.

Axborotning muhimlik darajasi qadim zamonlardan ma’lum. Shuning uchun ham qadimda axborotni himoyalash uchun turli xil usullar qo‘llanilgan. Ulardan biri – sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o‘qiy olmagan. Asrlar davomida bu san’at – sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o‘n yil oldin hamma narsa tubdan o‘zgardi, ya’ni axborot o‘z qiymatiga ega bo‘ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o‘g‘irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday qilib, axborotni himoyalash zaruriyati tug‘iladi. Axborotni qayta ishlash sanoatining paydo bo‘lishi axborotni himoyalash sanoatining paydo bo‘lishiga olib keladi.

1.2 Internetda ruhsatsiz kirish usullarining tasnifi

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

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

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

• tashkilotning kompyuter tizimini xakerlar tomonidan buzilishi:

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

• tashkilot faoliyatiga zarar etkazilishi.

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

• ma’lumotlarni engillik bilan kulga kiritish;

• tarmoqdagi kompyuterlar manzilini soxtalashtirish;

• TCP/IP vositalarining zaifligi;

• ko‘pchilik saytlarning notugri konfiguratsiyalanishi;

• konfiguratsiyalashning murakkabligi.

Global tarmoqlarning chegarasiz keng rivojlanishi undan foydalanuvchilar sonining oshib borishiga sabab bulmokda, bu esa uz navbatida axborotlar xavfsizligiga taxdid solish extimolining oshishiga olib kelmokda. Uzok, masofalar bilan axborot almashish zaruriyati axborotlarni olishning kat'iy chegaralanishini talab etadi. SHu maqsadda tarmoqlarning segmentlarini xap xil darajadagi himoyalash usullari taklif etilgan:

• erkin kirish (masalan: WWW-server);

• chegaralangan kirishlar segmenti (uzok masofada joylashgan ish joyiga xizmatchilarning kirishi);

• ixtiyoriy kirishlarni man etish (masalan, tashkilotlarning moliyaviy lokal tarmoqlari).

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

Lokal tarmoqlarning global tarmoqarga kushilishi uchun tarmoqlar himoyasi administratori quyidagi masalalarni xal qilishi lozim:

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

— global tarmoq fondalanuvchisi uchun axborotlarni yashirish imkoniyatining yaratilishi;

Bunda quyidagi usullar mavjud:

— kirish mumkin bulmagan tarmoq manzili orqali;

— Ping dasturi yordamida tarmoq paketlarini tuldirish;

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

— ta’kiklangan tarmoq protakoli buyicha birlashtirish;

— tarmoq buyicha foydalanuvchiga parol tanlash;

— REDIREST turidagi ICMP paketi yordamida marshrutlar jadvalini modifikatsiyalash;

— RIR standart bulmagan paketi yordamida marshrutlar jadvalini uzgartirish;

— DNS spoofingdan foydalangan holda ulanish.

Ruxsat etilgan manzillarning ruxsat etilmagan vaktda ulanishi

Ushbu xavf global tarmoqlarning bir kancha soxalarini kamrab oladi,

jumladan:

• lokal soha;

• lokal-global tarmoqlarning birlashuvi;

• muhim axborotlarni global tarmoqlarda junatish;

• global tarmoqning boshqarilmaydigan qismi.

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

Global tarmoq maydonlaridagi taxdid

Taxdid	LokalMaydon	LT/GTBirlashuvi	GTAdministratorMaydoni	GTBoshqarilmaydiganMaydoni
Tarmoqlarning notugri manzili			+	+
Paketlar bilan tuldirish	+			+
Mumkin bulmagan ulanish		+		+
Mumkin bo‘lgan ulanish	+	+		+
Parolni tanlash	+	+		+
ICMP hujumi	+	+	+	
RIP hujumi		+	+	
Ruxsatsiz uzokdan boshqarish		+	+	+
Parolni uzgartirish	+			+
DNS hujumi		+	+	
Mumkin bulmagan vaktda	+	+	+	+

Serverlarning asosiy vazifasi axorotlarni saqlash va takdim qilishdan iborat.

YOvuz niyatli shaxslarni quyidagicha tasniflash mumkin:

• axborot olishga imkoniyat olish;

• xizmatlarga ruxsat etilmagan imkoniyat olish;

• ma’lum sinfdagi xizmatlarning ish rejimini ishdan chikarishga urinish;

• axborotlarni uzgartirishga harakat yoki boshqa turdagi hujumlar.

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

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

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

Tarmoqlararo ekran va uning vazifalari

Tarmoqlararo ekran — himoyalash vositasi bo‘lib, ishonchli tarmoq, va ishonchsiz tarmoq orasida ma’lumotlarga kirishni boshqarishda kullaniladi.

Tarmoqlararo ekran ko‘p komponentli bo‘lib, u Internetdan tashkilotning axborot zaxiralarini himoyalash strategiyasi sanaladi. YA’ni tashkilot tarmogi va Internet orasida kuriklash vazifasini bajaradi.

Tarmoqlararo ekranning asosiy funktsiyasi — ma’lumotlarga egalik qilishni markazlashtirilgan boshqaruvini ta’minlashdan iborat.

Tarmoqlararo ekran quyidagi himoyalarni amalga oshiradi:

• urinsiz trafiklar, ya’ni tarmoqda uzatiladigan xabarlar okimini takiklash;

• kabul kilingan trafikni ichki tizimlarga yunaltirish;

• ichki tizimning zaif qismlarini yashirish bilan Internet tomonidan

uyushtiriladigan hujumlardan himoyalash;

• barcha trafiklarni bayonlashtirish;

• ichki ma’lumotlarni, masalan tarmoq topologiyasini, tizim nomlarini, tarmoq uskunalarini va foydalanuvchilarning identifikatorlarini Internetdan yashirish;

• ishonchli autentifikatsiyani ta’minlash.

Ko‘pgina adabiyotlarda **tarmoqlararo ekran** tushunchasi **brandmauer** yoki **Fire Wall** deb yuritilgan. Umuman bularning hammasi yagona tushunchadir.

Tarmoqlararo ekran — bu tizim, umumiy tarmoqni ikki qismga ajratib, tarmoqlararo himoya vazifasini utaydi va ma’lumotlar paketining chegaradan utish shartlarini amalga oshiradigan koidalar tuplami hisoblanadi.

Odatda tarmoqlararo ekran ichki tarmoqlarni global tarmoqlardan, ya’ni Internetdan himoya kiladi. SHuni aytish kerakki, tarmoqlararo ekran nafaqat Internetdan, balki korporativ tarmoqlardan ham himoya qilish kobiliyatiga egadir. Har qanday tarmoqlararo ekran ichki tarmoqlarni tulik himoya kila oladi deb bulmaydi.

Internet xizmati va hamma protokollarning amaliy jixatdan axborotlarga nisbatan himoyasining tulik bulmaganligi muammosi bor. Bu muammolar kelib chikishining asosiy sababi Internetning UNIX operatsion tizim bilan borlikligida.

TCR/IR (Transtnission Control Protokol/lnternet Protocol) Internetning global tarmogida kommunikatsiyani ta’minlaydi va tarmoqlarda ommaviy ravishda kullaniladi, lekin ular ham himoyani etarlicha ta’minlay olmaydi, chunki TCP/IP paketining boshida xaker hujumi uchun kulay ma’lumot kursatiladi.

Internetda elektron pochtani junatishni oddiy protokol pochta transport xizmati amalga oshiradi (SMTP - Simple Mail Transfer Protocol). Bu protokolda mavjud bo‘lgan himoyalashning muhim muammolaridan biri - foydalanuvchi junatuvchining maizilini kura olmasligidir. Bundan foydalanib xaker katta mikdorda pochta xabarlarini junatishi mumkin, bu esa ishchi pochta serverni xaddan tashkari band bo‘lishiga olib keladi.

Internetda ommaviy tus olgan dastur bu Sendmail elektron pochtasidir. Sendmail tomonidan junatilgan xabarlar boskinchi xaker axborot shaklida foydalanishi mumkin.

Tarmoq nomlari xizmati (Domain Name System — DNS) foydalanuvchilar nomi va xost-kompyuterini - manzilini kursatadi. DNS kompaniyaning tarmoq tuzilishi haqida ma'lumotlarni saklaydi. DNSning muammolaridan biri shundaki, bundagi ma'lumotlar bazasini mualliflashtirilmagan foylalanuvchilardan yashirish ancha qiyin. Buning natijasida, xakerlar DNS ni ko'pincha xost-kompyuterlarning ishonchli nomlari haqida ma'lumotlar manbasidan foydalanish uchun ishlatishi mumkin.

Uzok, terminallar emulyatsiyasi ximati uzok, tizimlarni bir-biriga ulash uchun xizmat kiladi. Bu serverdan foydalanuvchilar TELNET serveridan ruyxatdan utish va uz nomi va parolini olishi lozim. TELNET serveriga ulangan xaker dasturni shunday urnatishi mumkinki, buning natijasida u foydalanuvchining nomi va parolini yozib olish imkoniga ega buladi.

World Wide Web — WWW bu tizim Internet yoki intratarmoqlardagi har xil serverlar ichidagi ma'lumotlarni kurish uchun xizmat kiladi. WWW ning acosiy xossalaridan biri — Tarmoqlararo ekran orqali anik protokol va manzillarni fil'trlash zarurligini tarmoqning himoyalash siyosati karori bilan xal etilishidir.

Har qanday tashkilotning **tarmoq xavsizligi siyosati** ikki qismdan iborat buladi: tarmoq servislaridan foydalanish; tarmoqlararo ekranni qo'llash.

Tarmoq servislaridan foydalanish siyosatiga mos ravishda Internetda servislar ruyxati aniklanadi. Bu servislapga foydalanuvchilar cheklangan kirish bilan ta'minlanadi.

Kirish usullarining cheklanilishi — foydalanuvchilar tomonidan Internet servislariga chet yullar orqali ruxsatsiz kirishni takiklash ma'nosini bildiradi.

Tarmoq servislariga kirish siyosati, odatda, quyidagi printsiplarga moyil buladi:

- Internetdan ichki tarmoqka kirishni takiklash, lekin ichki tarmoqdan Inlernetga kirishga ruxsat berish;

- vakolatlangan tizimlarga Internetdan ichki tarmoqka cheklanilgan kirishga ruxsat berish.

Tarmoqlararo ekranlarga kuyiladigan vazifaviy talablar quyidagilardan iborat.

• tarmoq darajasida fil’trlashga talab;

• amaliy darajada fil’trlashga talab;

• administratsiyalash va fil’trlash koidalarini urnatish buyicha talab;

• tarmoqli autentifikatsiyalash vositalariga talab;

• ishlarni kayd qilish va hisobni olib borish buyicha talab.

Tarmoqlararo ekranning asosiy komponentlari

Tarmoqlararo ekranlarning komponentlari sifatida quyidagilarni keltirish mumkin: fil’trlovchi -yullovchi; tarmoq, darajasidagi shlyuzlar; amaliy darajadagi shlyuzlar.

Fil’trlovchi-yullovchi — yullovchi, ya’ni kompyuter tarmogida ma’lumotlarni manzilga etkazuvchi dasturlar paketi yoki serverdagi dastur bo‘lib, u kiradigan va chikadigan paketlarni fil’trlaydi. Paketlarni fil’trlash, ya’ni ularni anik tuplamga tegishliligini tekshirish, TCP/IP sarlavxasidagi ma’lumotlar buyicha amalga oshiriladi.

Fil’trlashni anik xost-kompyuter, ya’ni tarmoqdagi fayl va kompyuter zaxiralariga kirishni amalga oshiruvchi kompyuter yoki port, ya’ni xabarlarni junatish yoki kabul qilish maqsadida mijoz va server tomonidan ishlatiladigan va odatda 16 bitli son bilan nomlanadigan dastur bilan ulanishda amalga oshirish mumkin. Masalan, foydalanuvchiga keraksiz yoki ishonchsiz xost-kompyuter va tarmoqlar bilan ulanishda takiklash.

Fil’trlash koidalarini ifodalash qiyin jarayon bo‘lib, ularni testlash vositalari mavjud emas.

Birinchi koida buyicha, Internetdan keladigan TCP paketi junatuvchining porti 1023 dan katta bulsa, 123.4.5.6 manzilli kabul qiluvchiga 23-portga utkaziladi (23-port TELNET serveri bilan boglangan).

Ikkinchi koida ham xuddi shunday bo‘lib, faqatgina 25-port SMTP bilan boglangan.

Tarmoq darajasidagi shlyuzlar ishonchli mijozlardan anik xizmatlarga surovnomasini kabul kiladi va ushbu aloqaning qonuniyligini tekshirgandan sung ularni tashki xost-kompyuter bilan ulaydi. SHundan sung shlyuz ikkala tomonga ham paketlarni fil’trlamay junatadi.

Bundan tashkari, tarmoq darajasida shlyuzlar bevosiga **server-dallol** vazifasini bajaradi. YA’ni, ichki tarmoqdan keladigan IP manzillar uzgartirilib, tashkiriga faqatgina bitta IP manzil uzatiladi. Natijada, ichki tarmoqdan tashki tarmoq bilan tugridan-tugri boglamaydi va shu yul bilan ichki tarmoqni himoyalash vazifasini utaydi.

Amaliy darajadagi shlyuzlar fil’trlovchi-yullovchilarga mansub bo‘lgan kamchiliklarni bartaraf etish maqsadida ishlab chikilgan. Ushbu dasturiy vosita **vakolatlangan server,** deb nomlanadi va u bajarilayotgan xost-kompyuter esa amaliy darajadagi shlyuz deb ataladi.

Amaliy darajadagi shlyuzlar mijoz va tashki xost-kompyuter bilan tugridan-tugri aloqa urnatishga yul kuymaydi. SHlyuz keladigan va junatiladigan paketlarni amaliy darajada fil’trlaydi. Server-dallollap shlyuz orqali anik server tomonidan ishlab chikilgan ma’lumotlarni kaytadan yunaltiradi.

Amaliy darajadagi shlyuzlar nafaqat paketlarni fil’trlash, balki serverning barcha ishlarini kayd qilish va tarmoq adminstratorini noxush ishlardan xabar qilish imkoniyatiga ham ega.

Amaliy darajadagi shlyuzlarning afzalliklari quyidagilardan iborat:

• global tarmoq tomonidan ichki tarmoq tarkibi kurinmaydi;

• ishonchli autentifikatsiya va kayd qilish;

• fil’trlash koidalarining engilligi;

• ko‘p tamoyilli nazoratlarni amalga oshirish mumkinligi.

Fil’trlovchi-yullovchilarga nisbatan amaliy darajadagi shlyuzlarning kamchiliklari quyidagilardan iborat samaradorligining pastligi; narxining kimmat bo‘lishi.

Amaliy darajadagi shlyuzlar sifatida quyidagilarni misol kilib keltirish mumkin:

• Border Ware Fire Wall Server — junatuvchining va kabul qiluvchining manzillarini, vaktini va foydalanilgan protokollarni kayd kiladi;

• Black Hole — serverning barcha ishlarini kayd kiladi va tarmoq administratoriga kutilayotgan buzilish haqida xabar junatadi.

Bulardan tashkari quyidagi shlyuzlar ham kullaniladi:

Gauntlet Internel FirewaU, Alta Visla FireWali, ANS Interlock va boshqalar.

2.1. Elektron pochtada axborotlarga nisbatan mavjud xavf-xatarlar va ulardan himoyalanish asoslari

Elektron pochtadan foydalanish

Elektron pochta yoki E-mail hozirgi kunda Internetdan foydalanish jarayonining eng mashxur kasmi hisoblanadi. E-mail orqali dunyo buyicha istalgan joyga bir zumning uzida xat yuborish yoki kabul qilish hamda yozilgan xatlarni faqatgina bir kishiga emas, balki manzillar ruyxati buyicha junatish imkoniyati mavjud. E-mail orqali munozaralar o‘tkazish imkoniyati mavjud va bu yunalishda USENET serveri kul keladi.

Ko‘pgina korxonalar uz faoliyatida bevosita E-mail tizimidan foydalanishadi. Demak, korxona va tashkilotlar raxbarlari ma’lum bir chora-tadbirlar orqali uz xodimlarini E-mail bilan ishlash, undan okilona foydalanishga urgatishi lozim. Ushbu jarayonning asosiy maqsadi muhim hujjatlar bilan ishlashni tugri yulga kuyish hisoblanadi.

Bu erda quyidagi yunalishlar buyicha takliflarni e’tiborga olish zarur:

- E-mail tizimidan tashkilot faoliyati maqsadlarida foydalanish;
- shaxsiy maqsadda foydalanish;
- maxfiy axborotlarni saqlash va ularga kirish:
- elektron xatlarni saqlash va ularni boshqarish.

E-mail asoslari

Internetda asosiy pochta protokollariga quyidagilar kiradi:

- SMTP (Simple Mail Transfer Protocol);
- POP (Post Office Protocol);
- IMAP (Internet Mail Access Protocol);
- MIME (Multi purpose Internet Mail Extensions).

Bular bilan birma-bir tanishib chikamiz:

SMTP — ushbu protokol asosida server boshqa tizimlardan xatlarni kabul kiladi va ularni foydalanuvchining pochta kutisida saklaydi. Pochta serveriga interaktiv kirish huquqiga ega bo‘lgan foydalanuvchilar uz kompyuterlaridan bevosita xatlarni ukiy oladilar. Boshqa tizimdagi foydalanuvchilar esa uz xatlarini ROR-3 va IMAP protokollari orqali o‘qib olishlari mumkin;

POP — eng keng tarkalgan protokol bo‘lib, serverdagi xatlarni, boshqa serverlardan kabul kilingan bulsa-da, bevosita foydalanuvchi tomonidan o‘qib olinishiga imkoniyat yaratadi. Foydalanuvchilar barcha xatlarni yoki hozirgacha ukilmagan xatlarni kurishi mumkin. Hozirgi kunda POP ning 3-versiyasi ishlab chikilgan bo‘lib va autentifikatsiyalash usullari bilan boyitilgan;

IMAP — yangi va shu bois ham keng tarkalmagan protokol sanaladi.

Ushbu protokol quyidagi imkoniyatlarga ega:

- pochta kutilarini yaratish, uchirish va nomini uzgartirish;
- yangi xatlarning kelishi;
- xatlarni tezkor uchirish;
- xatlarni kidirish;
- xatlarni tanlab olish.

IMAR sayoxatda bo‘lgan foydalanuvchilar uchun RORga nisbatan kulay bo‘lib hisoblanadi;

MIME — Internet pochtasining ko‘p maqsadli kengaytmasi suzlari kiskartmasi bo‘lib, u xatlarning formatini aniqlash imkonini beradi, ya’ni:

- matnlarni har xil kodlashtirishda junatish;
- har xil formatdagi nomatn axborotlarni junatish;

• xabarning bir necha qismdan iborat bo‘lishi;

• xat sarlavxasida har xil kodlashtirishdagi ma’lumotni joylashtirish.

Ushbu protokol rakamli elektron imzo va ma’lumotlarni shifrlash vositalaridan iborat bo‘lib, bundan tashkari uning yordamida pochta orqali bajariluvchi fayllarni ham junatish mumkin. Natijada, fayllar bilan birga viruslarni ham tarkatish imkoniyati tugiladi.

E-taildagi mavjud muammolar

Elektron pochta bilan ishlash jarayonida quyidagi xatolarga yul kuyish mumkin:

- xatni tasodifan junatish;
- xatning notugri manzil buyicha junatilishi;
- xatlar arxivining keskin oshib ketishi okibatida tizimning ishdan chikishi;
- yangiliklarga notugri obuna bo‘lish;
- xatni tarkatish ruyxatida xatoga yul kuyish.

Agar tashkilotning pochta tizimi bevosita Internetga ulangan bulsa, yul kuyilgan xatolar okibati keskin oshib ketadi.

Ushbu xatolarning oldini olish usullarining ba’zi birlari quyidagilar:

- foydalanuvchilarni ukitish;
- elektron pochta dasturlarini tugri konfiguratsiyalash;
- Internetdagi protokollarga tulik amal qiluvchi dasturlarni qo‘llash.

Bundan tashkari elektron pochtaning shaxsiy maqsadda ishlatilishi tashkilot raxbariyati uchun ba’zi bir muammolarni keltirib chikarishi mumkin, chunki E-mail manzilida tashkilot nomlari aks ettirilgan bo‘lishi extimoldan holi emas. Natijada, shaxs junatayotgan xat tashkilot nomidan deb kabul kilinishi mumkin. SHu bois, telefonlar kabi E-maildan shaxsiy ishlar uchun foydalanishni cheklab kuyish zarur buladi. Albatta, buni joriy qilish qiyin masala.

Elektron pochtada mavjud xavflar

Elektron pochta bilan ishlash jarayonida quyidagi xavflar mavjud:

1. Junatuvchining kalbaki manzili. Kabul kilingan xatni E-mail manzili

anikligiga tulik ishonch xosil qilish qiyin, chunki xat junatuvchi uz manzilini kalbakilashtirishi mumkin.

2. Xatni kulga kiritish. Elektron xat va uning sarlavxasi uzgartirilmasdan, shifrlanmasdan junatiladi. SHu bois, uni yulda kulga kiritish va mazmunini uzgartirishi mumkin.

3. Pochta «bomba»si. Pochga tizimiga ko‘plab elektron xatlar junatiladi, natijada tizim ishdan chikadi. Pochta serverining ishdan chikish holatlari quyidagilardir:

• disk tulib koladi va keyingi xatlar kabul kilinmaydi. Agar disk tizimli bulsa, u holda tizim tamomila ishdan chikishi mumkin;

• kirishdagi navbatda turgan xatlar sonining oshib ketishi natijasida keyingi xatlar umuman navbatga kuyilmaydi;

• olinadigan xatlarning maksimal sonini uzgartirish natijasida keyingi xatlar kabul kilinmaydi yoki uchiriladi;

• foydalanuvchiga ajratilgan diskning tuldirilishi natijasida keyingi xatlar kabul kilinmaydi va diskni tozalab bulmaydi.

4. «Kurkinchli» (noxush) xat. Internet orqali olinadigan elektron xatlarning umuman noma’lum shaxslar tomonidan junatilishi va bu xatda foydalanuvchilarning shaxsiyatiga teguvchi suzlar bo‘lishi mumkin.

Elektron pochtani himoyalash

YUkorida keltirilgan xavflarga nisbatan quyidagi himoyalanish usullari ishlab chikilgan:

- kalbaki manzildan himoyalanish, bu holda shifrlangan elektron imzolarni qo‘llash taklif kilinadi;

- xatni kulga kiritishdan himoyalanish, bu holda xabarni yoki junatish kanalini shifrlash taklif kilinadi.

Ushbu himoyalash usullari bevosita kolgan xavflarning ulushini kamaytiradi.

2.2. Elektron tulovlar tizimida axborotlarni himoyalash

Elektron tulovlar tizimi asoslari

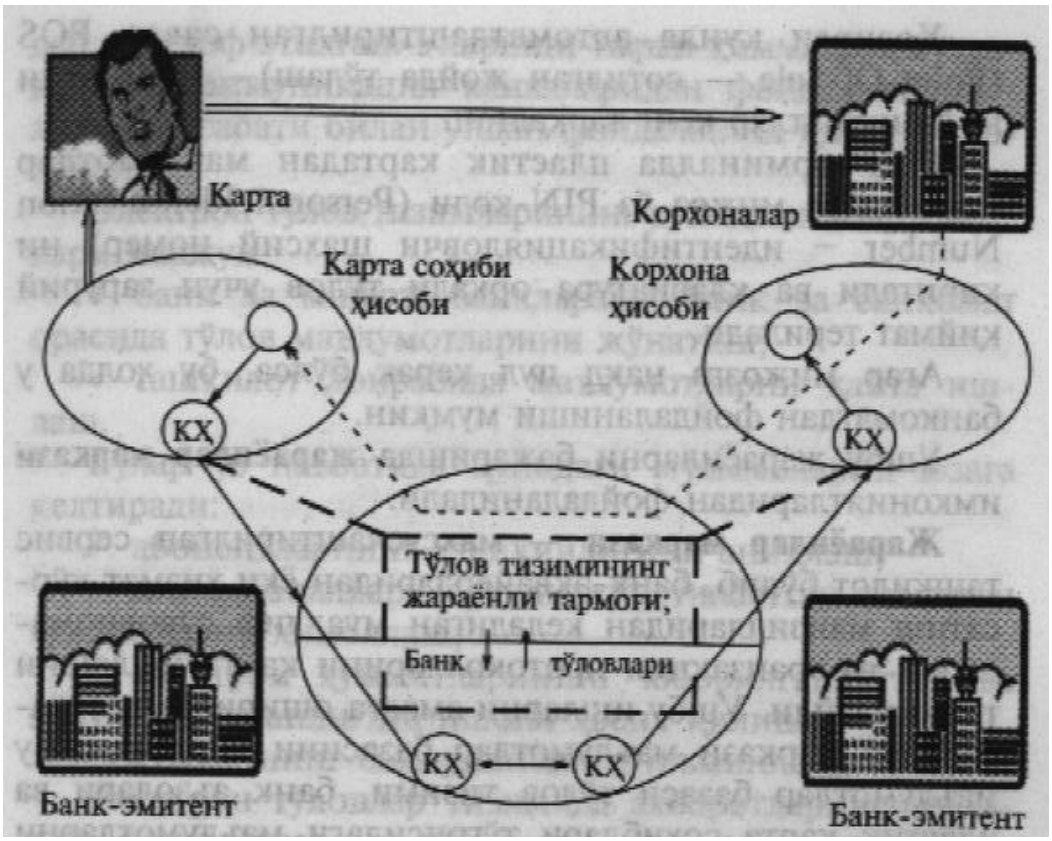
Elektron tulovlar tizimi deb bank plastik kartalarini tulov vositasi sifatada kullanilishidagi usullar va ularni amalga oshiruvchi sub’ektlar majmuasiga aytiladi.

Plastik karta — shaxsiy tulov vositasi bo‘lib, u mazkur vositadan foydalanadigan shaxsga tovar va xizmatlarni nakdsiz pulini tulash, bundan tashkari bank muassasalari va bankomatlardan nakd pulni olishga imkon beradi.

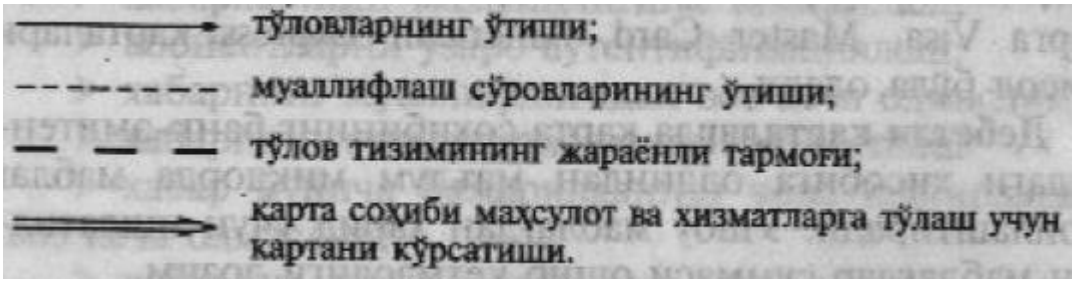
Plastik kartani tulov vositasi sifatida kabul qiluvchilar, savdo va xizmat kursatuvchi korxonalar, bank bulimlari hamda boshqalar shu plastik kartalarga xizmat kursatuvchi kabul qiluvchilar tarmogini tashkil etadi.

Elektron tulovlar tizimini yaratiщda plastik kartalarga xizmat kursatish qonun-koidalarini ishlab chikish va ularga rioya qilish asosiy masalalardan biri bo‘lib hisoblanadi. Ushbu koidalar nafaqat texnikaviy (ma’lumotlarni standartlash, uskunalar va boshqalar), balki moliyaviy masalalar (korxonalar bilan hisoblarni bajarish tartibi)ni ham kamrab oladi.

Elektron tulovlar tizimining faoliyatini quyidagidek tasavvur qilish mumkin:



Bu erda:



Elektron tulovlar tizimi bilan birgalikda faoliyat kursatadigan bank ikki, ya’ni **bank-emitent va bank-ekvayer** toifasida xizmat kursatadi:

Bank-emitent plastik kartalarni ishlab chikaradi va ularning tulov vositasi sifatida kullanilishiga kafolat beradi.

Bank-ekvayer savdo va xizmat kursatuvchi tashkilotlar tomonidan kabul kilingan tulovlarni bank bulimlari yoki bankomatlar orqali amalga oshiradi.

Hozirgi kunda avtomatlashtirilgan savdo POS (Point-Of-Sale — sotilgan joyda tulash)— terminali va bankomatlar keng tarkalgan.

PQS-terminalda plastik kartadan ma’lumotlar ukiladi va mijoz uz PIN-kodi (Personal Identification Number • identifikatsiyalovchi shaxsiy nomer)ni kiritadi va klaviatura orqali tulov uchun zaruriy kiymat teriladi.

Agar mijozga nakd pul kerak bulsa, bu holda u bankomatdan foydalanishi mumkin.

Ushbu jarayonlarni bajarishda **jarayonlar markazi** imkoniyatlaridan foydalaniladi.

Jarayonlar markazi – maxsuslashtirilgan servis tashkilot bo‘lib, bank-ekvayerlaridan yoki xizmat kursatish manzillaridan keladigan muallif surovnomalarni va tranzaktsiya protokollarini kayta ishlashni ta’minlaydi. Ushbu ishlarni amalga oshirish uchun jarayonlar markazi ma’lumotlar bazasini kiritadi. Bu ma’lumotlar bazasi tulov tizimi, bank a’zolari va plastik karta soxiblari tugrisidagi ma’lumotlarni uz tarkibiga oladi.

Plastik kartalar tulov buyicha **kreditli yoki debetli** bo‘lishi mumkin.

Kreditli kartalar buyicha karta soxibiga ko‘pincha muxlati 25 kungacha bo‘lgan vakgancha karz beriladi. Bularga Visa, Master Card, American Express kartalari misol bula oladi.

Debetli kartalarda karta soxibining bank-emitentidagi hisobiga oldindan ma’lum mikdorda mablag joylashtiradi. Ushbu mablagdan harid uchun ishlatilgan mablaglar summasi oshib ketmasligi lozim.

Ushbu kartalar faqatgina shaxsiy emas, balki korporativ ham bo‘lishi mumkin.

Hozirgi kunda **mikroprotsessorli kartalar** ishlab chikilmokda. Ushbu kartalarning oldingilaridan asosiy farki bu mijozning barcha ma’lumotlari unda aks ettirilgan bo‘lib, barcha **tranzaktsiyalar,** ya’ni ma’lumotlar bazasini bir holatdan ikkinchi holatga utkazuvchi surovnomalar, off-line rejimda amalga oshiriladi, shu bois, ular yukori darajada himoyalangan deb e’tirof etilgan. Ularning narxi kimmatrok bulsa-da, telekommunikatsiya kanallaridan foydalanilmaslik munosabati bilan undan foydalanish kiymati arzondir.

Elektron tulov tizimlarining quyidagi zaif qismlari mavjud:

• bank va mijoz, banklararo, bank va bankomat orasida tulov ma’lumotlarini junatish;

• tashkilot doirasida ma’lumotlarni kayta ishlash.

Bular uz navbatida quyidagi muammolarni yuzaga keltiradi:

• abonentlarning xakikiyligini aniqlash;

• aloqa kanallari orqali junatilayotgan elektron hujjatlarni himoyalash;

• elektron hujjatlarining yuborilganligiga va kabul kilinganligiga ishonch xosil qilish;

• hujjatning bajarilishini ta’minlash.

Elektron tulovlar tizimida axborotlarni himoyalash funktsiyalarini ta’minlash maqsadida quyidagilar amalga oshirilishi kerak:

- tizimning chetki buginlariga kirishni boshqarish;
- axborotlarning yaxlitligini nazorat qilish;
- xabarlarning maxfiyligini ta’minlash;
- abonentlarni uzaro autentifikatsiyalash;
- xabarning muallifligidan voz kecha olmaslik;
- xabarning etkazilganligini kafolatlash;

- xabar buyicha bajariladigan chora-tadbirlardan voz kecha olmaslik;
- xabarlar ketma-ketligini kayd qilish;
- ketma-ket xabarlar yaxlitligini ta’minlash.

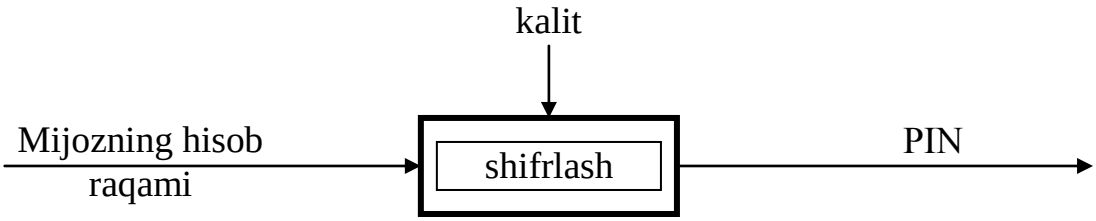
Identifikatsiyalovchn shaxsiy nomerni himoyalash

PIN-kodlarini himoyalash tulov tizimi xavfsizligini ta’minlashda asosiy omildir. SHu bois u faqatgina karta soxibiga ma’lum bo‘lib, elektron tulovlar tizimida saklanmaydi va bu tizim buyicha yuborilmaydi.

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

1) mijoz hisob rakami buyicha kriptografiya usuli bilan tashkillashtiriladi;

Ushbu jarayonni quyidagicha tasvirlash mumkin:



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

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

Mijoz tomonidan tanlaniladigan PIN kod quyidagi imkoniyatlarga ega:

- barcha maqsadlar uchun yagona PIN kodni qo‘llash;

• harflar va rakamlardan tashkil etilgan PIN kodni xotirada saqlashning engilligi.

PIN kodi buyicha mijozni identifikatsiyalashtirishning ikki usuli bilan bajarish mumkin: **algoritmlashgan va algoritmlashmagan.**

Algoritmlashmagan tekshirish usulida element kiritgan PIN kod ma'lumotlar bazasidagi shifrlangan kod bilan takkoslaniladi.

Algoritmlashgan tekshirish usulida esa mijoz kiritgan PIN kod, maxfiy kalitdan foydalangan holda, maxsus algoritm buyicha uzgartiriladi va kartadagi yozuv bilan takkoslaniladi.

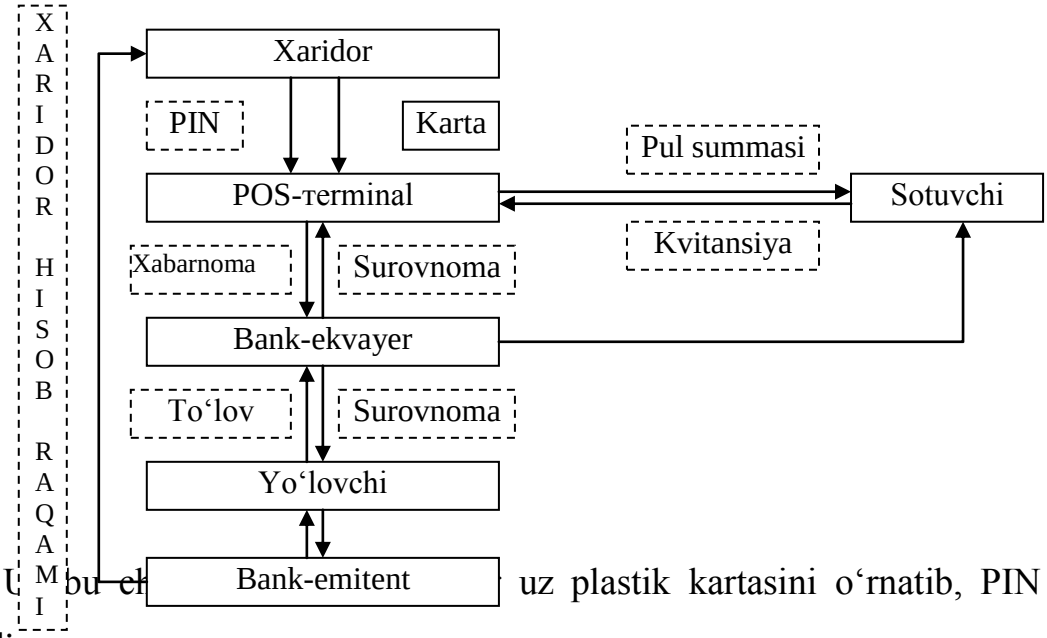
Ushbu usulning afzalliklari:

• asosiy kompyuterda PIN saklanmaydi va natijada personal tomonidan ugirlanmaydi;

• PIN kod telekommunikatsiya orqali junatilmaydi.

POS tizimi xavfsizligini ta'minlash

POS tizimini anik tasavvur qilish uchun quyidagi chizmani keltiramiz:



Ushbu el[illegible] uz plastik kartasini o‘rnatib, PIN kodini kiritadi.

Sotuvchi uz navbatida pul summasini kiritadi. SHundan sung, bank-ekvayerga (sotuvchi banki) pulni kuchirish uchun surovnoma yuboriladi.

Bank-ekvayer, uz navbatida, kartaning xakikiyligini aniqlash uchun surovnomani bank-emitentga junatadi. Natijada, bank-emitent pulni bank-

ekvayerga sotuvchi hisobiga kuchiradi. Pul kuchirilgandan sung, bank-ekvayer tomonidai POS-terminalga xabarnoma junatiladi. Ushbu xabarda tranzaktsiya bajarilganligi haqida ma’lumot buladi.

SHundan sung, sotuvchi haridorga maxsulot va kvitantsiyasini takdim etadi.

Uz-uzidan kurinib turibdiki, ushbu jarayonda har xil vokealar sodir bo‘lishi mumkin.

POS tizimining eng zaif qismi bu POS-terminaldir. Bundagi asosiy xavf bo‘lib terminaldagi maxfiy kalitning ugirlanishi hisoblanadi.

Buning okibatlari quyidagilar bo‘lishi mumkin:

• oldingi tranzaktsiyalarda ishlatilgan PIN kodni tiklash;

• keyingi tranzaktsiyalarda kullaniladigan PIN kodni tiklash.

Ushbu xavflardan himoyalanishning 3 ta usuli taklif etiladi:

- har bir tranzaktsiyasidan sung kalitni uzgartirish;
- POS-terminal va bank-ekvayer orasidagi ma’lumotlarni maxsus kalit bilan shifrlash hamda kalitni har bir tranzaktsiyadan sung uzgartirish;
- ochik kalitlar usuli yordamida uzatiladigan ma’lumotlarni shifrlash.

Bankomatlar xavfsizligini ta’minlash

Bankomatlar nakd pul olish, hisob rakamning holati va pul kuchirish imkoniyatlariga ega.

Bankomat ikki rejimda ishlaydi, off-line va online.

Off-line rejimda bankomat bank kompyuterlaridan mustakil ishlaydi va bajariladigan tranzaktsiyalar haqidagi yozuvlarni uz xotirasida saklaydi hamda printerga uzatib, ularni chop kiladi.

On-line rejimda bankomat bevosita bank kompyuterlari bilan telekommunikatsiya orqali ulangan buladi. Tranzaktsiyasini amalga oshirish maqsadida bankomat bankdagi kompyuter bilan quyidagi xabaplap bilan almashadi:

- bankomat surovnomasi;

- bankning javob xabari;
- bankomatning tulovni bajarganligi haqidagi xabarni berish.

Hozirgi kunda bankomatlar tarmoqlaridan bir necha banklargina foydalanadi. Bu erda mavjud bo‘lgan asosiy muammo bu banklarning maxfiy axborotlarini (masalan, maxfiy kalit) bir-biridan himoyalashdir.

Ushbu muammoning echimi sifatida PIN kodni, markazlashtirilgan holda, har bir bank tomonidan tekshirish taklif kilinadi.

Bundan tashkari bankomatlar tarmogi zonalarga taksimlanadi va har bir zonada ZCMK (Zone Control Master Key) kalitlari, uz navbatida, kompyuter tarmogidagi kalitlarni shifrlashda kullaniladi. Ma’lumotlarni shifrlashda esa IWK (Issuer Working Key) kalitlar ishlatiladi.

Internetda mavjud elektron tulovlar xavfsizligini ta’minlash

Hozirgi kunda Internetda ko‘pgina axborot markazlari mavjud, masalan, kutubxonalar, ko‘p soxali ma’lumotlar bazalari, davlat va tijorat tashkilotlari, birjalar, banklar va boshqalar.

Internetda bajariladigan elektron savdo katta ahamiyat kasb etmokda. Buyurtmalar tizimining ko‘payishi bilan ushbu faoliyat yana keskin rivojlanadi. Natijada, haridorlar bevosita uydan yoki ofisdan turib, buyurtmalar berish imkoniga ega bo‘lishadi. SHu bois ham, dasturiy ta’minotlar va apparat vositalar ishlab chikaruvchilar, savdo va moliyaviy tashkilotlar ushbu yunalishni rivojlantirishga faol kirishishgan.

Elektron savdo — global axborot tarmoqlari orqali maxsulotlarni sotish va pulli xizmatlar kursatish demakdir.

Elektron savdoning asosiy turlari quyidagilardir:

• axborotlar sotuvi;

• elektron dukonlar;

• elektron banklar.

Axborotlar sotuvi asosan ma’lumotlar bazasidan On-line rejimda foydalanish uchun takdim etilishi mumkin.

Elektron dukonlar Internetda Web-site orqali tashkillashtiriladi. Bunda tovarlar ruyxati, tulov vositalari va boshqalar keltiriladi. Harid kilingan maxsulotlar oddiy pochta orqali junatilishi yoki agar ular elektron maxsulot bulsa, bevosita Internetdan manzilga etkazilishi mumkin.

Elektron banklarni tashkil etishdan asosiy maqsad bankning doimiy harajatlarini kamaytirish va keng ommani kamrab olishdir. SHu bois, elektron banklar uz mijozlariga yukori foiz stavkalarini taklif qilishlari mumkin.

Axborotlarni himoyalashning asosiy vosatalari

Haridor, kredit kartasi soxibi, bevosita tarmoq orqali tulovlarni bajarish uchun ishonchli va himoyalangan vositalarga ega bo‘lishi lozim.

Hozirgi kunda SSL (Secure Socket Layer) va SET (Secure Electronic Transactions) protokollari ishlab chikilgan:

• SSL protokoli ma’lumotlarni kanal darajasida shifrlashda kullaniladi;

• SET xavfsiz elektron tranzaktsiyalari protokoli yakinda ishlab chikilgan bo‘lib, faqatgina moliyaviy ma’lumotlarni shifrlashda kullaniladi.

SET protokolining joriy etilishi bevosita Internetda kredit kartalar bilan tulovlar sonining keskin oshishiga olib keladi.

SET protokoli quyidagilarni ta’minlashga kafolat beradi:

• axborotlarning tulik maxfiyligi, chunki foydalanuvchi tulov ma’lumotlarining himoyalanganligiga tulik ishonch xosil qilishi kerak;

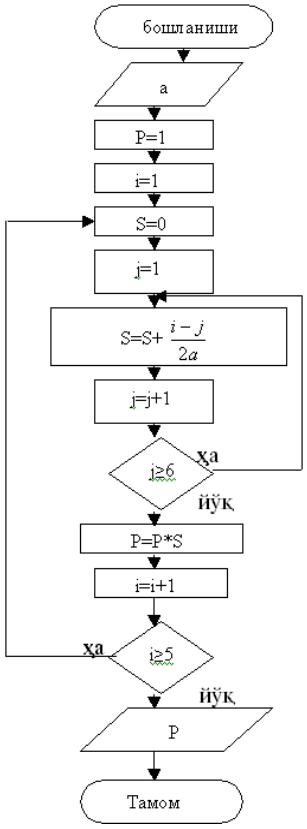
• ma’lumotlarning tulik saklanishi, ya’ni ma’lumotlarni uzatish jarayonida buzilmasligini kafolatlash. Buni bajarish omillaridan biri rakamli imzoni qo‘llashdir;

• kredit karta soxibining hisob rakamini audentifikatsiyalash, ya’ni elektron (rakamli) imzo va sertifikatlar hisob rakamini audentifikatsiyalash va kredit karta soxibi ushbu hisob rakamining xakikiy egasi ekanligini tasdiklash;

• tijoratchini uz faoliyati bilan shugullanishini kafolatlash, chunki kredit karta soxibi tijoratchining xakikiyligini, ya’ni moliyaviy operatsiyalar bajarishini bilishi shart. Bunda tijoratchining rakamli imzosini va sertifikatini qo‘llash elektron tulovlarning amalga oshirilishini kafolatlaydi.

3.1. $P=\prod_{i=1}^{5}\sum_{j=1}^{6}\frac{i+j}{2a}$ **кko'paytmani hisoblash dasturini tuzing, bu yerda** $a=5$**.**

1. Blok-sxemasini tuzamiz:



2. Paskal tilida dasturini tuzamiz:

```
Program misol;
var i, j:integer;
    a,S,P:real;
begin
read(a);
   P:=1;
for i:=1 to 5 do
begin
S:=0;
for j:=1 to 6 do
S:=S+(i+j)/ (2*a);
P:=P*S;
end;
write('P=',P);
end.
```

Xulosa.

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

Bundan tashqari kurs ishi yozish davomida axborotlarni himoyalash nechog’lik zarur ekanligini mazmun va mohiyatini tushunib yetdik.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. R.X. Alimov, B.YU. Xodiev, K.A. Alimov, S.U. Usmonov, B.A. Begalov, N.R. Zaynalov, A.A. Musaliev, F. Fayzieva, «Milliy iqtisodda axborot tizimlari va texnologiyalari», O‘quv qo‘llanma, T. Sharq, 2004 yil.
2. M.T. Gafurova, D.CH. Dursunov, V.I. Rapoport, B.YU. Xodiev. Proektirovanie sovremennых informatsionnых texnologiy. Uchebnoe posobie.-Toshkent, TDIU, 1994.-96 s.
3. Informatsionnые sistemы v ekonomike: Uchebnik/Pod red. prof. V.V. Dika.-M.:Finansы i statistika,1996.-272 s.
4. Informatika: Uchebnik/Pod red. N.V. Makarovoy. -M.: Finansы i statistika, 1997.-768s.
5. G‘ulomov S.S. va boshq. Iqtisodiy informatika: Oliy o‘quv yurtlarining iqtisodiy mutaxassisliklari uchun darslik.
6. G‘ulomov S.S., SHermuhammedov A.T., Begalov B.A.; S.S. G‘ulomovning umumiy tahriri ostida. —T.: «O‘zbekiston», 1999. —528 b.
7. Kozыrev A.A. Informatsionnые texnologii v ekonomike i upravlenii: Uchebnik, 2-e izd. .—SPb.: Izd-vo Mixaylova V.A., 2001. —360 s.
8. Xodiev B.YU., Musaliev A.A., Begalov B.A. Vvedenie v informatsionnые sistemы i texnologii. Uchebnoe posobie /Pod red. akad. S.S. Gulyamova. —T.:TGEU, 2002. —156 s.
9. Shafrin YU.A. Informatsionnые texnologii. —M.: Laboratoriya Bazovых Znaniy, 1998. —704 s.
10. Petrov B.N. Informatsionnые sistemы. – SPb.: Piter, 2003. – 688s.:il.
11. www.intuit.ru
12. www.it-study.ru
13. www.informatika.ru
14. www.ziyonet.uz
15. www.ref.uz

AndMI 1-kurs “TJIChAB” yo’nalishi talabasi A.Qobiljonovning «Informatika va axborot texnologiyalari» fanidan “Internetda axborotlar xavfsizligini ta’minlash asoslari” mavzusida bajargan kurs ishiga

T A Q R I Z

Andijon mashinasozlik institutining 1-kurs “TJICHAB” yo’nalishi talabasi A.Qobiljonovning «Informatika va axborot texnologiyalari» fanidan “Internetda axborotlar xavfsizligini ta’minlash asoslari” mavzusida bajargan kurs ishida uch bobdan iborat reja tuzilgan.

Reja bo’yica asosan elektron pochtada ishlash bilan bog’liq barcha savollarga javob berilgan.

Kurs ishida avvalo talaba tomonidan mustaqil mavzularni o’zlashtirishga harakat qilgan. Shuningdek amaliy topshiriqni ham blok sxemasi va dasturi tuzilgan.

Talabaning bajarigan ishini o’rganib chiqdim va uning himoya vaqtida berilgan savollarga javobini etiborga olib yahshi baholandi.

Rahbar: **S.Jamoldinov**