

**Elektron hujjat
aylanishlar tizimi va
raqamli imzo.**

- Elektron hujjat aylanishalar tizimi haqida tushuncha.
- Elektron hujjat aylanishalar tizimlarining asosiy hususiyatlari
- Elektron hujjat aylanishalar tizimlarida ma'lumotlarni himoyalash
- Elektron raqamli imzo haqida tushuncha

- Elektron hujjat aylanishalar tizimi haqida tushuncha.

Elektron hujjat aylanishalar tizimining asosi sifatida hujjat xizmat qiladi. Hujjat – bu aniq bir ko’rinishda tartibga solingan ma’lumotdir. O’z navbatida sistema bir biri bilan o’zaro aloqda bo’lgan elementlar majmuasi bo’lib, alohida funksiyalarning bajarilishi uchun mo’ljallangan va u o’zining tashkil etuvchi elementlari xossalardan kelib chiqqan holda qandaydir xossalarga ega bo’ladi.

Elektron hujjat aylanishlar tizimida huddi shunday elementlar bo'lib hujjatlar xizmat qiladi.haqiqtdan ham xayotimizni hukkatlarsiz tasavvur etish juda qiyin: fuqaro pasportisiz bo'la olmaydi, haydovchi guvohnomasiz mashina boshqara olmaydi, turist vizasiz mamlakatda yura olmaydi, talaba zachyotkasiz imtihon topshira olmaydi va hokazo.

Hujjatlar iqtisodiyotning barcha sohalarida mavjud va ularsiz biror bir faoliyatni amalga oshirish mumkin emas. Masalan, savdo, boshqaruv, bank ishi, ishlab chiqarish, fan, texnika, moliya, soliq sohalari va boshqalar. Biror bir firma, biror bir korporatsiya hujjatlarsiz va hujjatlar aylanish tizimisiz ishlay olmaydi. Hujjat aylanish tizimi har qanday tashkilot va iqtisodiyot sohasining ajralmas qismi bo'lib hisoblanadi.

Informatsion texnologiyalarning paydo bo'lishi va rivojlanishi bilan hujjatlar aylanish tizimining rivojlanishi uvhun juda keng imkoniyatlar paydo bo'ldi. Ayniqsa internet paydo bo'lishi va rivojlanishi bilan, elektron pochtaning keng miqyosda qo'llanilish hujjatlar uzatish va qabyl qilishda masofa muammosini deyarli yo'qqa chiqaradi. Ma'lumotlar ham elektron pochta orqali jo'natilganda oluvchiga bir necha minutlar ichida yetib boradi. Ammo bu muammolarni hal qilish boshqa juda ham muhim bo'lgan muammoni keltirib chiqaradi – bu elektron hujjat jo'natilayotgan ma'lumotlarni himoya qilish bilan bog'liqdir.

Chunki ma'lumotlar va hujjatlar elektron usulda uzatilganda uni boshqalar ham olishi va o'z g'arazli maqsadlarida foydalanishlari mumkin.

Elektron hujjatga, ularning xaqiqiyligini tasdiqlash uchun oddiy qog'oz hujjatlardan farqli o'laroq, pechat va imzo qo'yish mumki emas. Shuning uchun bu vazifani elektron hujjatlarda elektron raqamli imzo bajardi. Uning nima ekanligini ham keyingi bo'limlarda ko'rib chiqamiz.

Elektron hujjat aylanishalar tizimlarining asosiy hususiyatlari

Ilm-fanda , texnikada, ishlab chiqarishda va biznesda informatsion oqimlarning juda tezlik bilan ko'payib ketishi informatsion texnologiyalar tomonidan ham kerakli chora tadbirlar ko'rishni talab qiladi. Jamiyat uchun juda ko'p miqdorda qog'ozning ishlatalishi juda ham qimmatga tushadi, undan tashqari bu qog'ozlarni saqlash, ulardan kerakli ma'lumotlarni qidirish yoki o'zlashtirsh murakkab masaladir. Shuning uchun ham hujjatlarni elektron ko'rinishda yozish, saqlash hamda kerak bo'lganda o'zgartirsih qulay, arzon va mobil desa ham bo'ladi.

Qog'ozsiz texnologiya konsepsiysi bir necha o'n yillarda buyon mavjud bo'lib, hozirgacha u to'la xayotdaga tadbiq etilmagan. Buning asosiy sabablari quyidagilardir:

- **Ma'lumotlarni elektron ko'rinishda qabul qilish va undan foydalanish o'ziga xos ko'nikishni talab qiladi, hozircha insonlar buncha insonlar bunga unchalik ko'nikmagandir;**
- **Qog'ozsiz texnologiyalar asosli va qimmat bo'lgan texnik vositalarni talab qiladi ya'ni tezkor ishlaydigan hisoblash texnikasi, ma'lumotlarni tezlik bilan uzata oladigan kommunikatsion aloqa liniyalari, texnologik fazifalarni amalga oshira oladigan samarali algoritmlar va dasturlar;**

- Ma'lumotlar xafsizligini ta'minlay oladigan dasturiy va texnik vositalar;
- Asosli huquqiy (yuridik) ta'minot – qonunlar, ko'rsatmalar, instruksiyalarva boshqalar;
- Elektron raqamli imzo va hujjatlar uchun kerakli bo'lgan boshqa rekvizitsiyalar.

Har qanday tashkilot uchun hujjatlarning 3 asosiy oqimini ko'rsatish mumkin:

Kirish hujjatlari

Ichki hujjatlar

Chiqish hujjatlari

Korxona ish yuritishning funksiyalari kirish ma'lumotlarini qabul qilish va qayta ishlashdan, ularni korxona ichida kerakli bo'lim yoki insonlarga jo'natishdan, chiqish hujjatlarini jo'natishdan, hujjatlarni hisobga olishdan, qayd qilishdan, ijroni nazorat qilishdan, hujjalarni saqlashdan va boshqarishdan iborat.

- **Elektron hujjatlar aylanishni boshqarish tizimi yuqoridagi quyidagi ishlarni avtomatlashtirishuchun mo'ljallagan:**
- **Korxonadagi turli xil hujjatlarni tayyorlash, kiritish, saqlash,qidirish va chiqarish jarayonlari – “Elektron arxiv” tizimi.**
- **Hujjatlarning standart formalarini tayyorlash, kiritish, saqlash, qidirish va chiqarsh jarayonlari – “hujjatlarning standart formalarini kiritish” tizimi.**
- **Ish yuritishni boshqarish, ya’ni hujjatlarni hosil qilish, ularga ishlov berish vahujjatlarni arxivda saqlashni tashkil qilish – “Ish yuritish” tizimi.**



Bunda quyidagi jarayonlar
avtomatizatsiya obyekti bo'ladi:

- Hujjatlarni tayyorlash;
- Tashkiliy, xisobotli, statistik, hisob, reja, iformatsion – so'rovli va baoshqa boshqaruv hujjatlarni tayyorlash, hisobga olish, tsrtibga keltirish, saqlash va qidirish;
- Hujjatlar bilan ishlash – hisobga olsi, nazorat, boshqalarga uzatish vahokazolar.

Elektron hujjatlar aylanishi boshqarish tizimini tshil qilish uchun quyidagi dasturiy va texnik vositalar zarur bo'ladi:

Qog'oz hujjatlarni kiritadigan va obrazlarni taniy olladigan vositalar;

Elektron hujjatlar hosil qiladigan vositalar;

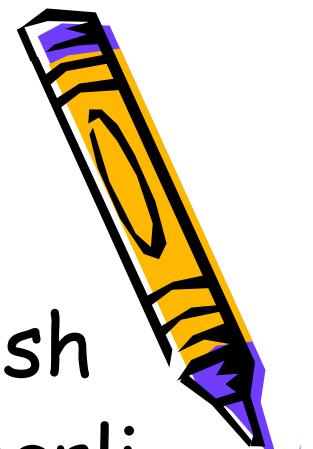
Elektron arxiv tashkil qiladigan va u bilan ishlay oladigan vositalar;

Hujjatlar aylanishini boshqarish uchun mo'ljallangan texnologik vositalar;

Hujjatlar bilan ishlashning maxsus funksiyalarini amalga oshirib beruvchi dasturlarni ishlab chiqarishga mo'ljallangan instrumental vositalar

Quyida misol tariqasida “Intellektual texnologiyalar” firmasi tomonidan ishlab chiqilgan “Elektron arxiv” tizimining asosiy ko’rsatgichlarini ko’rib chiqamiz. Bu tizim hujjatlar formatiga hech qanday jiddiy talablar qo’ymaydi hamda turli xil va ko’rinishdagi hujjatlarga ishlov berishni nazarda tutadi, bir arxivda har xil ko’rinishdagi ma’lumotlarning saqlanishiga imkon beradi. Taklif etilayotgan tizimning asosiy afzalliklari quyidagi operatsiyalarni to’liq avtomatizatsiyasini amalga oshirishdir:

- Hujjatni elektron obrazini olish
- Hujjatdagi matnni tanib olish
- Hujjat matnini morfologik analiz qilish
- Hujjatdagi matnli ma'lumotni tushunarli holatga keltirish
- Hujjatni klassifikatsiya qilish, unga annotatsiya yozish va hujjatning registratsion kartochkasini hosil qilish
- Hujjatning elektron obraziniuning registratsion atributlari yoki matn ma'nosiga qarab qidirib topsih.



Elektron hujjat aylanishalar tizimlarida ma'lumotlarni himoyalash

Elektron pochta orqali ma'lumot
uzatilayotganda quyidagi nohush hollar
ro'y berishi mumkin:

- Ma'lumot uzatuvchining manzili no'to'g'ri ko'rsatilgan - ma'lumot uzatuvchi o'z adresini no'to'gri ko'rsatishi mumkin yoki ma'lumot sarlavhasi u uzatilayotgan paytda o'zgartirilishi mumkin yoki ma'lumot jo'natuvchining o'zi kompyuter SMTP portinomidan xat jo'natishi mumkin.
- Xatlarni ruxsat so'ramasdan o'qib olish.
- Poshta bombalari - bu elektron pochta orgali hujum uyushtirishdir. Bunda hujumqilinayotgan tizimga u ma'lumotlarga to'lib, ishdan shigaunga qadar xatlar jo'natilaveradi.



Elektron pochtaga hujumlarni tahlil qilgan holda ularning quyidagi turlari ancha ko'p uchrashini qayd qilishimiz mumkin:

Elektron pochta ma'lumotlarini ruxsat so'ramasdan turib o'qib olish va boshqalarga ma'lum qilishdirmaning faoliyatini ishdan chiqarishi mumkin

Pochta serverini band qilib qo'yish xizmat ko'rsatish sifatiniancha kamaytirishi mumkin.

Pochta orqali viruslarni jo'natish ham juda xafli hujum turlaridan biridir.

Elektron pochtani himoya qilish uchun quyidagi usullardan foydalanish mumkin:

- No'to'g'ri ko'rsatilgan manzillardan himoyalanish uchun shifrlanish usuludan foydalanish mumkin. Eng yaxshi usullardan biri - ochiq kalitli shifrlashni ishlatishdir. AQSH hukumatibuning uchun Secure Hash Algorithm (SHA) va Digital Singnature Stanfart deb nomlangan Xesh-funksiyali algoritmlarni ishlatishni talab qiladi. lekin eng ko'p ishlatiladigan tijorat dasturlari RSA firmasining RC2, RC4, RC5 algoritmlaridan foydalanadi.

- Ma'lumotlarni birovlar tomonidan o'qib olishidan himoyalanish uchun na'lumotni shifrlashdan yoki ma'lumot o'tkazish kanalini shifrlashdan foydalanish mumkin.elektron pochtani shifrlashni bir necha usullari taklif etilgan, ammo ularning ichida eng keng tarqalganiPGP usulidir. PGP usulining tijorat versiyasibir necha xizmatlari uchun moslashtiriladigan vositalrga ega. Bu esa u yordamida elektron maktubga elektron imzo qo'yishni osonlashtiradi vamijoz tomonidan xatnishifrlash imkonini beradi.PGP usulining eng oxirgi variatlarishifrlash algoritmining litsenziyalı versiyasini ishlatib, RSA ochiq kalitdan foydalanadi.

- SPAM dan ximoyalanish – SPAM jo'natuvchilarni aniqlash uchun tarmoq darajasida filtratsiya qilish usulidan foydalanish mumkin

Elektron ma'lumot almashinuv (EDI) ni himoyalash informatsion xafsizlikni ta'minlashda asosiy faktorlardan biri bo'lib hisoblanadi. Bu masalani hal qilish bilan, masalan, Premenos Corp firmasi shug'ullanadi. ushbu firma himoyalangan holda ma'lumot uzatishni ta'minlab beruvchi Templar deb nomlangan dasturiy vositalar to'plamini ishlab chiqdi.

Elektron raqamli imzo haqida tushuncha

Kompyuterda saqlanayotgan har qanday fayl baytlar ketma-ketligiko'rnishida bo'ladi va shuning uchun ham biror bir uzun son orqali yoki bir necha sonlar ketma-ketligiorqali aniq ifodalanishi mumkin.

Ushbu ketma-ketlikni uning unikalligini yo'qotmasdan "qisqartirish" uchun maxsus matematik.algoritmlardan foydalanish mumkin. Masalan, nazorat yig'indisi (control total) yoki xash-funksiya (Hash function). Agarda faylning har bir baytini uning raqamiga ko'paytirsak hamda olingan natijalarning yigindisini olsak, u holda asosiy faylning uzunligidan kichikroq bo'lgan son hosil bo'ladi.

Agarda asosiy istalgan baytni o'zgartirsak, ushbu son qiymati o'zgarib qoladi. Amaliyotda bundan ko'ra murakkabroq bo'lган algoritmlar ishlataladi. Bunday algoritmlarda natijaviy sonning har qanday o'zgartirishlar kiritilganda ham o'zgarmay qolishi ta'minlanadi. Xesh-funksiya shunday unikal son sifatda aniqlanadiki, u turli xil boshlang'ich fayllardan hisoblab chiqilganda, turli xil fayllar uchun bir xil kattalikda bo'lib chiqadi. Uning algoritmi esa barcha uchun ma'lum – ochiq algoritm bo'ladi. Bunday algoritmlarning biri "Informatsion texnologiya.

Ma'lumotlarning kriptografik himoyasi. Xeshlashtirish funksiyalari" deb nomlangan davlat standartida

Endi elektron mzo qanday qlib olinishini ko'rib chiqamiz. Buning uchun kriptografiya usuli nima ekanligini tushunib chiqishimiz kerak bo'ladi. Ushbu usulni qo'llaganda ma'lumotlarni shifrlash va unio'qish uchunbir xil kalitk ishlatiladi. Bunday simmetrik shifrlash usulida eng asosiy muammo kalitni ma'lumot jo'natuvchidan uni qabul qiluvchiga uzatganda maxfiylikni saqlash hisoblanadi. Ma'lumot uzatish vaqtida kalitni oshkor qilish boshqalar tomonidan hujjatni o'qish imkonini yaratish va firibgarlarga uni o'zgartirishga imkon berish bo'ladi.



1970 yillarda ma'lumotlarni asimmetrik fshifrlash usuli kashf etildi. Uning mohiyati chundan iboratki, bunda shifr bir algoritm bilan shifrlansa, u boshqa shifr bilan o'qiladi. Bir algoritmnini bilgan holda ikkinchisini bilish yoki aniqlash mumki emas. Shuning uchun agar ma'lumot uzatuvchi hujjatni maxfiy kalit bilan shifrlasa va hujjatni o'qish imkonini yaratadigan algoritmnini ma'lumotni qabul qiluvchilarga bersa, u holda ular faqatgina konkret ma'lumot uzatuvchining hujjatlarinigina o'qiy o'qiy oladilar xolos. Ma'lumot uzatuvchining maxfiy kalitiga ega bo'lgan kimsalar hech qanday usulda ham hujjatni o'qiy olmaydilar.

ma'lumot uzatuvchi hujjatning xesh-funksiyasi hisoblab, uning kattaligini o'z maxfiy kaliti bilan shifrlaydi va natijani hujjat matni bilanbirgalikda ma'lumot qabul qiluvchiga jo'natadi. Hujjatni olgan kimsa ham xuddi o'sha algoritmyordamida hujjatning xesh-funksiyasi hisoblaydi va so'ngra ma'lumot uzatuvchi tomonidan jo'natilgan ochiq kalit yordamida xesh-funksiyaning jo'natilgan kattaligini rasshifrovka qiladi va hisoblangan hamda jo'natilgan xesh-funksiya kattaliklarini bir-biriga solishtiradi.

**Agar ushbu kattaliklar bir xil chiqsa,
demak bu ma'lumot konkret adresat
tomonidan jo'natilgan bo'lib chiqadi.
Boshqa, sun'iy yoki noto'g'ri kalitlar
ma'lumotlarni rasshifrovka qila
olmaydi. Demak, agar xesh-
funksiyaning hisoblangan va
rasshifrovka qilingan kattaliklari bir
biriga mos kelsa, u holda hujjat
o'zlashtitilmagan degan xulosa
chiqariladi. Ma'lumot uzatish
jarayonida hujjatning har qanday
o'zlashtirilishi hujjat qabul qiluvchi
tomonidan hisoblanadigan xesh-
funksiyaning yangi qiymatiniberadi va
ma'lumot uzatish jarayonini tekshirish
programmasi "hujjatning elektron
imzosi qalbaki ekan" degan ma'lumot
beradi.**

Shunday qilib qo'l bilan qo'yiladigan imzodan farqli-o'laroq, elektron raqamli inzo to'g'ridan to'g'ri biror bir shaxsga bog'liq emas, balki u konkretujat bilan va uning maxfiy kaliti bilan uzviy bog'liq bo'ladi. Agar sizning maxfiy kalitingiz bo'lgan disketani kindir eslab qolsa, u holda u siz uchun elektron imzo qo'yishi mumkin albatta. Lekin sizning elektron raqamli imzoingizni bir hujjatdan boshqa bir hujjatga ko'chirish mumkin emas, uni nusxalash, qalbakilashtirishni ham imkoni yo'q. elektron raqamli imzo har bir hujjat uchun unikal bo'ladi. Elektron raqamli imzolarni saqlash, undan foydalanish, yangilash va uniyo'qotish qoidalari bir qancha uslubiy materiallarda batafsil ko'rsatilgan va tushuntirilgan.

Shifrlash haqidagi ma'lumotlar

Endi ma'lumotlarni asimetrik kalitlar bilan shifrlash usulini ko'rib chiqamiz. Agar yuqorida ko'rsatilgan farqli ravishda kalitlarning o'rnnini almashtirib qo'ysak yani, rasshifrvka kalitini maxfiy qilib, shifrlash kalitini ochiq holda qoldirsak, u holda ma'lumot uzatuvchi hujjatni ma'lumot qabul qiluchiningochiq kaliti bilan shifrlaydi va bu holda xatni faqatgina juft maxfiy kaliti bor kimsaginao'qiy oladi, yani faqatgina hujjatni qabul qiluvchi uni o'qiydi, xolos. Bunday usulning ajoyib jihat chundaki, bunda kalitlarni konfidensial tarzda uzatishga zarurat qolmaydi. Ochiq kalitni Veb-saytda o'qib olinadiganqilish mumkin yokiuni elektron pochta orqalijo,natish mumkin.boshqalar uni bilib olsalar ham, buning uchun hech qanday hoydasi bo'lmaydi, chunki ularda juft maxfiy kalit yo'q va bolmaydi ham.

Kalitlar tizimini boshqarish

Elektron hujjat aylanish tizimida sistma adminitratsiyasi katta rol o'ynaydi. U barcha abonentlar tomonidan bir ishlash qoidalari garioya qilinishini amalga oshiradi, konfliklar bo'lib qolganda ularni hal qiladi, kalitlar sistemasini boshqaradi, barcha abonentlardagi ochiq kalitlar ma'lumotnomalarini tarribga keltirib va yangilab turadi. Agarda biror bir nohush hol yuz bersa, kalitlarni almashtirish kerak bo'lib qoladi – masalan, kalitlar disketasini yo'qotish, ularning o'g'irlanishi, disketlarning ishdan chiqishi, kalitlar bilan shug'ullanuvchi yoki u haqda ma'lumotga ega hodimning ishdan ketishi, ma'lumotlarni saqlash va ularni muddati o'tishidan so'ng yo'q qilish qoidalaring buzilishi va boshqalar.

Bunday hodisotlar ro'y began taqdirda mas'ul xodimlar tizimining administrarsiyasini bundan boxabar qilishi kerak bo'ladi. Administrarsiya esa zudlik bilan kerakli bo'lgan chora-tadbirlarni ko'rishi zarur.