

**WO`ZBEKSTAN RESPUBLIKASI` BAYLANI`S,
INFORMACIYALASTI`RI`W HA`M TELEKOMMUNIKACIYA
TEXNOLOGIYALARI` MA`MLEKETLIK KOMITETI**

**TASHKENT INFORMACIYALI`Q TEXNOLOGIYALARI`
UNIVERSITETI NO`KIS FILIALI`**

Informaciyali`q texnologiyalar kafedrası`

**Komp`yuter injiniringi fakultetinin`
Informatika ha`m informaciyali`q texnologiyalar bag`dari`
studenti Nurjanov Dawran Perdebaevichtin`**

PITKERIW QA`NIGELIK JUM I`SI`

**Temasi`: Elektron hu`jjet almasi`w sistemasi` imkaniyatlari`nan toli`q tu`rde
paydalani`w usi`llari`.**

**İlimiy basshi`** \_\_\_\_\_ Rambergenov Q., «O`zbekiston pochtasi» AAJ
QQ filiali` bas esapshi`si`, ass. Begilov B.

**Kafedra basli`g`i`** \_\_\_\_\_ t.i.k. Arzi`mbetov T.Z.

No`kis-2014 j.

MAZMUNI’:

Kirisiw.	3
I-BAP. ELEKTRON HU`JJETLERİN ALİ’P BARI’WDİ’ BASQARI’W	6
1.1 Da`stu`riy metodlar	6
1.2 Logikali’q modellerge qoyi’latug`i’n geypara funkcional talaplardi’n` ani’qlamasi’	10
1.3 Standartlar ha`m spesifikaciyalar	12
1.4 Arxitekturali’q funkciyalar	14
1.5 Sistemani’n` ekspluctaciya’q xarakteristikasi’	17
1.6 Jazi’wlardi’ funkcional` basqari’w	19
1.7 Tan`lap ali’wdi’n` funkciyanalli’g`i’	21
II-BAP. ELEKTRON HU`JJET AYLANI’Sİ’NDA ELEKTRON CİFRLİ’	
İMZA ALGORİTMLERİNİN` SALİ’Sİ’RMALİ’ ANALİZİ.....	22
2.1 ECİ ni payda etiw processı.	24
2.2 ECİ ni` tekseriw processı.....	26
2.3 ESIGN algoritmi.....	28
III-BAP. ELEKTRON HU`JJET AYLANI’Sİ’N AVTOMATLASTİ’Rİ’WDİ’	
TA’MIYNLEWSHİ SİSTEMANİ’ JARATİ’WDA QOLLANI’LATUG`İ’N	
DRUPAL PROGRAMMASI’	32
3.1 Drupal programması’n Ubuntu operacion sistemasi’nda ornati’w.....	32
3.2 Drupal programması’n Windows operacion sistemasi’nda ornati’w	38
VI-BAP MİLLİY ELEKTRON HU`JJET ALMASI’W SİSTEMASI’	43
4.1 E-XAT qorg`algan elektron pochtasi’	43
4.2 Programmani’ installyaciya qi’li’w	44
4.3 E-HUJJAT sistemani’n` qollani’li’wi’.	56
JUWMAQLAW.....	61
PAYDALANI’LG`AN A`DEBİYATLAR:	62

Kirisiw.

Wo'tken a'sirdin` 90-ji'llari'nan baslap firmalar o`z informaciyali'q resurslari' ha'm dereklerin basqari'wg'a ma'selesine u'lken itibar qarata basladi'. Lekin, seziwge bolatug'i'n basqa derekler menen sali'sti'rg'anda informaciya bazali'q o'lshe'm birligine iye emes. İnsanni'n` miynet ku'shi o'nimdarlig'i' insanni'n` jumsag'an waqti' yaki toli'q ba'ntlighi menen o'lsHENEDI. Materialli'q dereklerdi basqari'wda o'lshe'm, salmaq yaki san kriteriyalari' qollani'ladi'. Finansli'q tarawda bolsa esaplawlar Amerika dollari', yapon yenasi' yaki nemis markasi' menen o'lsHENEDI. U'skenenin` ku'shi kilovatt saat, kubometr, futo-svecha, mil`, kilometr menen o'lsHENEDI. Informaciyali'q dereklerdi qalay o'lsheymiz? Informaciyani'n` quni'n qalayi'nsha buxgalteriyali'q esabat penen o'lsheymiz? Dereklerdin` bazasi'n o'lshegende qanday terminlerden paydalanasi'z, mag'li'ymatlardi' bir bazag'a qoyasi'z, ketekshelerdi bir tablicag'a, fayllardi' serverge, betti hu`jjetlerge, hu`jjetlerdi adamg'a ju`kleysiz be?

(UIR) informaciya resurslari'n basqari'w jan'alani'w bosag'asi'nda tur. U'lken o`zgerisler ju`z berip ati'r. Firmalar mag'li'wmat ha'm sistemalardi' rawajalandi'ri'wg'a u'lken g'a'rejet jumsawdi'n` orni'na hu`jjetlerdi birinshi da'rejege shi'g'armaqta. Bunday o`zgeris hu`jjetin` birlēmshi tu'sinigin payda etiw yag'ni'y hu`jjetli-bag'darlang'an processtin` bazali'q birligin payda etiw. Ko'pshilik basshi'lar ha'm basqari'wshi'lar ani'q joba tayar bolmag'ang'a shekem yag'ni'y kishkene o`zgerisler menen risklerdi ani'qlap almag'ang'a shekem o`zgerislerdi qabi'l etiwdi keyinge su`rip kelmekte. Bunday keshigiw firmani'n` jumi's o'nimdarli'g'i'n kemeytip jiberiwi mu'mkin. Bul haqqi'nda Samuel` Djonson bi'lay degen edi: «Ha'r qanday tosqi'nli'qti' aldi'n ala baqlawg'a almay turi'p jetiskenlikke erisiw qi'yi'n».

Keyingi 25 ji'l ishinde firmalardi'n` byudjetinin` informaciyali'q resurslardi' qollap turatug'i'n bo`limi mag'li'wmat ha'm sistemalardan ibarat bolg'an. Bunday qosi'mshada firmani'n` uli'wma mag'li'wmatlari'ni'n` 15% tan Kemi jayg'asadi'. Lekin son'g'i' tuti'ni'wshi' informaciyalardi'n` 75 ten 85 procentke shekem o`zinde ja'mleytug'i'n hu`jjet aylani'si'n isleytug'i'n qosi'mshalarg'a mu'ta'j

esaplanadi'. Ko'p g'ana firmalar hu'jjetlerdi basqari'w ha'm qag'az jumi'si' ko'lemin kemeytiwge qarati'lg'an halda byudjetin artti'ri'p baradi'. Bunday ha'reket en' son'g'i' ma'rtebe informaciyalardi' basqari'w sistemasi' qa'nigeleri ta'repinen sekseninshi ji'llari' islengedi. Bul waqi'tta firmalardi'n' aylani'si'na mag'li'wmatlar bazasi'n basqari'w sistemasi' kirip kelgen edi.

O'zgerislerdin' kerekligi tek g'ana firma jumi'sshi'lari'ni'n' qag'azg'a ko'milip qalmawi'nan shorshi'wi'nan payda bolmag'an. Firmalardan o'z jumi'sshi'lari'nan o'z jumi'si'na nemquraydi'li'q penen qaramastan, toli'q iskerligin ko'rsetiwin talap etiw ju'klenbekte. Bosqa jumi'slatug'i'n tapsi'rmalar menen ko'p waqi'tti' alatug'i'n ha'm hesh kim ushi'n a'hmiyeti joq jumi'slardi' joqqa shi'g'ari'w ha'm qalg'an ma'selelerdi az sandag'i' adamlar ku'shi menen sheshiwdi biykar etiw boli'p tabi'ladi'. Ba'sekiliktin' en jayi'wi' bizden shtat kestesinen kishkene basshi'lardi' ali'p taslap ha'm olardi'n' minnetlemelerin buri'n hu'jjetlerdi izlew ha'm saqlaw menen shug'i'llanbag'an jumi'sshi'larg'a tapsi'ri'wdi' talap etpekte.

A'piwayi' etip aytqanda qag'az benen islesiw jumi'si' mayda kleklerden wazi'ypasi'na kiredi degen pikir shi'nli'qqa tuwra kelmeytug'i'n boldi'. Hu'jjetlerdi saqlaw ha'm izlew en' a'hmiyetli iskerliktin' birine aylandi' olardan firmani'n' erten'gi g'a'rezli boli'p qaldi'.

Hu'jjetti siz qalay tu'sinesiz? Mine usi' jerde biz u'lken tosqi'nli'qqa dus kelemiz. A'piwayi' hu'jjetti ko'z aldi'mi'zg'a keltiriw, oni'n' xarakteristikasi'n, og'an tu'sinik beriwden an'sat boli'p esaplanadi'.

En' aldi' menen hu'jjettin' qurami'na kiretug'i'ni' haqqi'nda gu'man tuwdi'rmaytug'i'n islenbelerdi ko'rip o'teyik. Amerikani'n' g'a'rezsizligi haqqi'nda Deklaraciya, Kanadan'i'n' erkinlik ha'm huqi'q haqqi'ndag'i' xartiyasi', arqa amerikada Erkin sawda-sati'q islew kelisimi ha'm a'sirese insaniyat ushi'n en' a'xmiyetli bolg'an on muqaddes wazi'ypa, bul insan ushi'n insan ushi'n inam etilgen standart emes hu'jjetler birikpesi. Barli'q mi'sallarda hu'jjetlilikke gu'man joq. Eger sizden usi' ha'r qi'yli' mi'sallar tiykari'nda hu'jjet haqqi'nda uli'wma tu'sinik Ber dese, sizde u'lken qi'yi'nshi'li'q payda boladi'. Sog'an qarastan,

olardi'n` engiziliwi, turmi's cikli, quram bo`legi ha`m firma hu`jjetlerin islep shi'g`i'wdi'n` sistemali' modelin yadta tuti'n`, bul o`z gezeginde sizin` firma ushi'n qaysi' na`rse hu`jjet boli'p esaplanatug`i'ni'n ani'qaw ushi'n ja`rdemin tiygizedi.

Eger hu`jjetlerdi basqari'w haqqi'nda so`z bolg`anda o`zin`iz ushi'n oylawdi'n` ha`m jumi's islewdin` jan`a gorizonti'n ashi'w ushi'n tayar boli'wi'n`i'z kerek. Birinshi bo`lim tayarlani'w ushi'n ja`rdem beredi.

Bunda siz ushi'n hu`jjetlerdi talqi'law, olardi' basqari'w ha`m isleniw sistemasi' haqqi'ndag`i' tiykarg`i' terminologiya keltiriledi. A`sirese, hu`jjetlerdi basqari'wdi'n` arxitekturali'q sistemali' komponenti ha`m qollani'li'w maqseti ayri'qsha atap ko`rsetilgen, yag`ni'y koncepciya, logika ha`m predmetlik iske tu`siriw. Soni'n` menen birge hu`jjetlerdi basqari'w procesine baylani'sli' bolg`an standartlasti'ri'w ha`m specifikaciya da usi'larg`a kiredi.

I-BAP. ELEKTRON HU`JJETLERIN ALI'P BARI'WDI' BASQARI'W

1.1 Da`stu`riy metodlar

Zamanago`y firmalarda hu`jjetlerdi basqari'w ha`m bildiriw jazi'p qaldi'ri'w metodi' hesh qanday na`tiyje bermeydi. Bildiriwlerdi saqlaw ha`m sho`lkemlestiriw sistemasi'ni'n` buri'ng`i' tu`ri na`tiyje bermeytug`i'ni' ani'q boli'p qaldi'. Aktualli'g`i'n jog`altqan hu`jjetlerdi arxivlerde saqlaw sistemasi' o`z na`tiyjeliligini jog`altti'. Hu`jjet penen islesetug`i'n ko`pshilik xi'zmetkerler hu`jjetlerdi arxivte saqlaw ta`rtibin sho`lkemlestiriw ma`selelerin joqqa shi'g`aradi', eger buni'n` arti'nda keskin administrativlik juwapkershilik ko`rilmese.

O`z jumi'si'na baylani'sli' hu`jjetlerdi qolg`a kirgizgen adam oni' jasi'ri'p qali'wg`a meyilli boli'p keledi. Ja`ne bir jag`dayda hu`jjetler menen islesip bolg`annan son` barli'q hu`jjetlerdi bir papkag`a tigip qoyadi'.

Soni'n` menen birge islengen hu`jjetlerdin` sani', jari'q ko`riwi ha`m informaciyalardi'n` firmalar ta`repinen lokal tarmaq yaki elektorn pochta arqali' jiberiliwi hu`jjetlerdi baqlap bari'w, qorg`aw, olardi'n` ha`reketin bilip oti'ri'w boyi'nsha mashqalalardi'n` birinshi plang`a shi'g`i'wi'na ali'p keldi. Buri'n` a`xmiyetli hu`jjetegi informaciyani' qorg`a ha`m og`an kiriwdi qorg`aw ushi'n fayl jaylasqan papkalardag`i' en` a`hmiyetligi jag`i'nan sereletug`i'n edi. Bu`gingi ku`ni hu`jjetti baqlap bari'w huqi'qi'na iye sistema administratori' o`zi juwap bere alatug`i'n tarmaq ishindegi elektron pochtaga`i' qa`legen xati' oqi'y aladi'.

Hu`jjetlerdin` da`stu`riy ha`reket etiwinde fayl protokollari'nda ko`rinetug`i'n edi. Onda hu`jjetti ko`re alatug`i'nlardi'n` dizimi bar edi ha`m sistemag`a Kire alatug`i'n ha`m onnan shi'g`a alatug`i'nlar dizimnen o`tetug`i'n edi. Elektron pochta xi'zmeti adresatlar dizimen qa`legen adamdi' kirgiziw mu`mkinshiligin beredi (xatti'n` haqqi'nda nusqasi'nda bul na`rse ko`rsetilmese de) yaki ali'ng`an xati' qa`legen xi'zmetkerge jiberiw mu`mkinshiligin beredi.

Ha`zirgi waqi'tta ha`reket etip turg`an hu`jjetlerdi izlew sistemasi' fayllardan ibarat papkalarg`a zagalovka qoyi'w yaki fayldi'n` mazmuni'n ko`rsetetug`i'n gilt

soʻzler dizimin beredi. Lekin bul fayldagʻiʻ huʻjjetti izlep tabiʻwgʻa kepillik bermeydi. MS Windows operaciyaliʻq sistemasiʻnda fayldiʻnʻ atamasiʻniʻnʻ haʻm direktoriyasiʻniʻnʻ uziʻn-shubay boliʻwiʻn sheklew ornatiʻlgʻan. Simvol 8 den artpawiʻ kerek, bul naʻrse uʻlken mashqalaniʻ keltirip shiʻgʻardiʻ. Elektron pochta xiʻzmeti oʻzininʻ jeke maʻlimlemeler bazasiʻ strukturasiʻniʻnʻ koʻlemindegi bildiriwlerdi saqlap qaladiʻ. Bul naʻrse oʻz gezeginde tekst huʻjjetlerin izlew mexaniziminde tabiʻwdiʻ sheklep qoyadiʻ.

Is (informaciyaliʻq sistemalar) qaʻnigeleri tek gʻana keyingi waqiʻtlariʻ sistemaniʻ basqariʻwdiʻ, magʻliʻwmatlardiʻ basqariʻw texnologiyasiʻn haʻm informaciyaniʻ modellestiriw metodikasiʻn shoʻlkem boyiʻnsha islep turgʻan barliʻq sistema haʻm magʻliʻwmatlardiʻ basqariʻw ushiʻn jetilistirdi. Usiʻ qaʻnigelerdinʻ koʻpshiligi huʻjjetlerdi basqariʻw teoriyasiʻn bilmeydi, usiʻ jumiʻsta qollaniʻliʻp atiʻrgʻan qurallar, texnologiyalar, islenbeler, metodikalar menen qiʻziʻqsiʻnbaydiʻ. Jumiʻstiʻ toliʻq tuʻsinip ketiwi ushiʻn olargʻa bir yaki eki jiʻl kerek boladiʻ. Lekin (firma huʻjjetlerin basqariʻw sistemasiʻ) FHBS niʻnʻ haʻreketlerine koʻp naʻrse baylaniʻsliʻ ekenin esapqa alatugʻiʻn bolsaq, bul waqiʻt koʻp boliʻp tabiʻladiʻ. FHBS termini haʻm programmaliʻ taʻminleniw olar ushiʻn tuʻsinikli boliʻp tabiʻladiʻ.

Kompʻyuter haʻm kompʻyuter sistemalariʻniʻnʻ rawajlaniʻp oʻzin bekkem tutiʻwiʻ ushiʻn 25 jiʻldan artiʻq waqiʻt talap etildi. Endi olardiʻnʻ aldiʻnda janʻa tapsiʻrma tur. Buriʻnnan sarqiʻt boliʻp qalgʻan qagʻaz haʻm elektron nusqadagʻiʻ huʻjjetler sistemasiʻn firmada huʻjjetlerdi basqariʻwdiʻnʻ birlesken avtomatlasqan jumiʻsshiʻ sistemasiʻna oʻtkeriw.

Texnologiyalardiʻnʻ rawajlaniʻwiʻna qoyiʻlgʻan investiciyalardiʻnʻ firmalar ushiʻn daʻramat keltiriwi ushiʻn jumiʻstiʻnʻ metodiʻna haʻm basqariʻwiʻnda janʻa qatnas kerek boladiʻ. Adam aʻsirese, informaciyaliʻq sistemalar menen islesip atiʻrgʻanlar basqalargʻa qaragʻanda janʻashiʻliʻqqa tapban tirewi muʻmkin. Baqlap bariʻw masshtabiʻ oʻsip barmaqta. Firmalardanʻ daʻramatlariʻniʻnʻ basiʻp koʻpshiligininʻ informaciyaliʻq sistemalardiʻ haʻm texnologiyalardiʻ rawajlandiʻriʻwgʻa qaratiʻliʻp atiʻrgʻaniʻn esapqa alatugʻiʻn bolsaq oʻzgeristinʻ

boli'p ati'rg`ani'n sezemiz. O`zgerislerdin` tez pa't penen boli'p ati'rg`anli'g`i' jumi'sti' isleytug`i'n adamlardi'n` uli'wma adamlardi'n` kewil keypiyati' menen bir ekenligin ko`rsetpekte. Yag`ni'y alg`a qoyi'lg`an ma`selenin` kolemi ha`reket etiwden taysaldi'ri'p taslamaqta.

Jumi'sti'n` masshtabi'n ko`z aldi'mi'zg`a keltiriw ushi'n 1000 adam jumi's isleytug`i'n firmani' ali'p qarayi'q. Olardi'n` ha`r biri ji'li'na ortasha 500 hu`jjet isleydi. Uli'wmalasti'rg`anda bul ji'li'na 500000 jan`a cifrli' hu`jjetti keltirip shi'g`aradi'. Olardi' bir tegis baqlawda uslap turi'w mu`mkin bolmag`an tapsi'rma. Ko`pshilik firmalar qanday jan`a texnologiyani' qollanbasi'n jan`a ma`selelerdi sheshiwge ma`jbu'r boldi'. Olar hu`jjetlerdi islep shi'g`i'w ha`m tarqati'w.

Djonatan Svift shi'g`armalari'ni'n` birinde, u`yin sati'w ushi'n bir gerbishte «u`lgi retinde qari'ydarg`a ta`sir etiw maqsetinde ali'p ju`rgen bir adam haqqi'nda so`z etiledi. Buni'n` na`tiyjesinde jaydi' sati'wda qanday da kelisimgе kelindi me, yadi'mda joq, biraq bul jigit 6yinin` konceptual` ha`m fizikali'q modeline qatti' isenip, logikali'q modelin yadtan shi'g`arg`an.

Logikali'q sxema–SUDFni'n` en` a`hmiyetli buwi'ni'. o`ytkeni, bunda qanday islewine qaray emes, al konkret jag`dayda islegenin ju`zege shi'g`adi'. Kelesi bo`limde predmetlerdin` ju`zege shi'g`i'wi' tuwrali' so`z boldi', bull bolsa ko`p jag`dayda «gerbish» penen baylani'sli'. Bul jerde sistema konkret jag`dayda ko`rinedi ha`m sistema qalay isleytug`i'ni', qanday apparatlar menen ta`miyinleniwi za`ru'rliги ha`m qanday operaciyali'q sistema, qanday fayllar ha`reketke keletug`i'n ha`m tag`i' basqalar tuwrali' ayti'ladi'.

Logikali'q model` tiykari'nan texnikali'q boli'p, eki o`zine ta`n ayi'rmashi'li'qqa iye, xarakterli, buni' men o`ner dep atag`an bolar edin`, bull negizinde do`retiw ushi'n kerek. Oni'n` tabi'sli' islewi, islewshinin` sheberligi, oylawi'nan baslap oni' tayarlawshi'g`a da baylani'sli': ha`m ol arti'qsha detalizaciyag`a aralasi'p ketedi, bull bolsa koncepcual` procesti shekleydi.

Bul bo`limde SUDFni'n` logikali'q modeline qoyi'latug`i'n geypara funkcional` talaplar ko`rip shi'g`i'ladi'. Bunday qanday ta`miyinleniwdi ha`m qanday islep shi'g`ari'wshi'lardi' izlew kerekligi, sonday-aq arxitekturani'n` basli'

xarakteristikasi', sistemani'n` islewi, jazi'wlardi' basqari'w, izlew ha`m hu`jjetlerdi ali'w, funksional` informaciyalardi' qorg`aw, bunnanti'sqari', logikali'q model`di sho`lkemlestiriw ha`m sistemali'q saqlawlar ha`m basqa da spECIfikali'q o`zgeshelikleri ko`rip shi'g'i'ladi'.

1.2 Logikali'q modellerge qoyi'latug'i'n geypara funkcionall talaplardi'n`ani'qlamasi'

SUDFni' sati'p ali'w ko'p ta'repinen zat ali'wg'a uqsas. Jan'a mashina kerek da'ldalshi' jaqi'n avtostoyankag'a kelip tosattan avtomobil` sati'p ali'wi' mu'mkin. Bul adam erten`ine de mashina buzi'lmaytug'i'ni'na u'mit etedi, ja'rdem sorasa kim bolsa da trubkani' ko'teretug'i'ni'na isenedi. Al, qari'yardar bolsa basqasha ha'reket etedi. Ol en` da'slep biraz izertlew ju'rgizedi ha'm sati'p alg'an na'rzeni juwap beriwi tiyis: bul mashinada siz ne tasi'maqshi'si'z? Mashinag'a bahali' ju'kti iseniwge bola ma? Paydalani'wshi'ni'n` basqari'w paneli ha'm qollanbasi' duri's islengen be? Buri'ng'i' qari'yardarlar sati'p alg'an zati'na kewli tolg'an ba?-spekli funkcionall talaplardi' analizleydi.

Bull bo'limde SUDFni'n` sati'p ali'w menen baylani'sli' geypara ta'wekelshilik ha'm sistemag'a qoyflatug'i'n talaplar ko'rip shi'g'i'ladi', bularsi'z di'qqat qarati'wi'n'i'z ha'm tu'sinip ali'wi'n'i'z za'ru'r bolg'an barli'q faktorlar tuwrali' pikir ali'sami'z. En` basli'si', Siz turmi'sqa logikali'q model`di engiziwdi u'yrenesiz. Sizge, avtomobil`di sati'p ali'wshi' si'pati'nda erten` sizin` qon'i'rawi'n'i'zg'a juwap beretug'i'n, sonday-aq Sizin` jag`dayi'n'i'zda programmali'q ta'miyinlew siz biypa'rwa emessiz. Konkret jag`dayda bul sistemani'n` standart emes sheshimleri basqalari'nan ayri'li'p turatug'i'nli'g'i' haqqi'nda bilgin`iz keledi.

Funkcionalli'q ha'm ta'wekelshilik boyi'nsha bizler to'mendegi tematikali'q bag`dardi' ko'rip shi'g`ami'z.

Arxitekturali'q funkcionalli'q.

Sistemani'n` ekspluatatsiyali'q xarakteristikasi'.

Jazi'wda basqari'wdi'n` funkcionalli'g'i'.

Tan`lawdi'n` funkcionalli'g'i'.

Izlewdin` funkcionalli'g'i'.

Sistemani'n` qa'wipsizligi, qadag'alaw ha'm administrirofaniyani'n` funkcionalli'g'i'.

Barli'q SUDF da birdey boli'p islenbeydi. Sistema anaw yamasa mi'naw funkcionallardi' atqara ala ma, buni' biliw ko'plik etpeydi. Klientke funkciyalardi'n` jumi's islewinin` ku'shli ha'm ha'lsiz ta'replerin sali'sti'rmali' tu'rde biliw kerek. Bul jerde arxitekturali'q funkcionalli'qti'n` eki aspektine-belgili standartlarga ha'm spECIfikaciya'g'a juwap beriwi, sonday-aq, arxitekturali'q funkciyalar kompleksi jumi's isley ali'wi'na basli' di'qqat qarati'w kerek.

SUDF spECIfikaciya ha'm standartqa juwap beriwi kerek. Bunnan sonni' tu'siniw kerek, birinshiden ol ani'q islewi, ekinshiden, buri'nnan bar prilojeniyag'a u'ylesiwi kerek.

Qari'ydar en` basli' u'sh elementke di'qqat awdari'wi' kerek:

1.Cortur Sroure tasti'yi'qlag`an klient/server ortalig`i'ni'n` u'shinshi basqi'shi' ha'm onnan joqari' bahalawi' o'lshe mine tuwri' keliwi.

2.Belgilengen DMA spECIfikaciya's na tuwri' keliwi.

3.Belgilengen ODMA spECIfikaciya's versiyasi'na mass keliwi.

1.3 Standartlar ha'm specifikacyalar

Klient-server ortali'q programmali'q ta'miyinlew Carther Crop tasti'yi'qlag'an klient/server ortali'g'i'ni'n` u'shinshi ha'm onnan joqari' basqi'shi'n bahalaw o'lshe mine tuwri' keliwi. Duri's, uli'wma qabi'llang'an klient/server ortali'g'i'ni'n` o'zi joq bolsa da, Cortur Sroure ko'pshilikke jayi'lg'an modellerdin` bul ortali'qtag'i' bahalawin` islep shi'qqan.

Bul model'ge iyisli bir neshe sawallardi' berip, qari'ydare effektli islemeytug'i'n jumi'slardi' bile di, sonday-aq, bul programmali'q ta'miyinlew klient/server ortali'g'i'ni'n` juqa yaki qalin` tu'rine kiretug'i'ni'n` ani'qlap aladi'. Klient/server ortali'g'i'ni'n` juqa varianti' degenimiz bul-jumi'stin` azg`ana bo'legi klienttin` moyni'na t6sedi: sietama serverdi toli'g'i' qadag`alaydi'. Klient server ortali'g'i'ni'n` qalin` varinati'n engiziw degenimiz. Jumi'stin` ko'pshilik bo'legin paydalani'wshi' isleydi.

En` tiyimlisi, sete jui'sti' paydalani'wshi' ha'm server ortasi'nda bo'listirip, settin` tiyimli jumi's islewin ta'miyinlew kerek. Klassifikacyani'n` u'shinshi basqi'shi' Carther Croupqa tuwri' keletug'i'n sistemada usi'nday ten'salmaqli'li'q ko'zde tuti'lg'an. Jumi'stin` ju'ginin` ortasha awi'rli'g'i' paydalani'wshi' ha'm serverge ten` tu'siwi ko'zde tuti'lg'an.

Saqlawda turg'an tu'rli hu'jjetlerdin` o'z-ara ha'reketinin` joqarg'i' basqi'shi'n ta'miyinlew ushi'n SUDF programmali'q ta'miyinlew DMA specifikacyasi'na juwap beriwi tiyis. Mi'sali', paydalani'wshi' komp'yuterde DOCS OPEN programmali'q ta'miyinlewi menen islegende, saqlawdag'i' hu'jjetlerdi programmali'q ta'miyinlew arqali' izleydi, ol sonday-aq, o'z komp'yuterinde Soros Mezzanine yamasa Soft Solutions tiykari'nda kerekli qosi'mshani' qospay-aq, saqlawda turg'an hu'jjetler arasi'nan izlew ju'rgiziw mu'mkinshiligine iye.

SUDF programmali'q ta'miyinlew ODMA specifikacyasi'na juwap eriw tiyi. Bul specifikalardi'n` talaplari'n ori'nlaw sistemasi'ni'n` (AR1) progarramalli'q ta'miyinlew ha'm uli'wma basqa prikladnoy programmali'q interfeys arqali' birge ha'reket etiwge mu'mkinshilik beredi. Mi'sali', personal` basqari'w bo'limindegi prilojeniyada islegende paydalani'wshi'g'a saqlawja turg'an hu'jjet kerek boli'p

qaldi'. AR1 interfays solay silengen, paydalani'wi'nda SUDF da personaldi' basqari'w bo`limi prilojeniyasi'nan intergirovat` etiw mu`mkinshiligin aladi'. Na`tiyjede klaviaturani' terip komanda beriw za`r6rligi qalmaydi', tuwri'dan-tuwri' saqlawg`a shi'g`adi'.

1.4 Arxitekturali'q funkciyalar

Arxitektura sistemasi' standartqa juwap berip qoymastan, al ja'rdemlesiwın funkciyalardi' da qollap-quwatlaw arqali' hu'jjetleri basqari'w processin jen'illestirip, kereklihu'jjetlerdi tan'lawg'a ja'rdemlesiwı kerek.

Sistema saqlawdi' logikali'q jaqtan bo'liwi ha'm olardi'n` ha'r birin izlewdi na'zerde tuti'wi' kerek. Bo'liw komp'yuterdi si'rtqi' qa'wipten qrg'awdi' ku'sheytiwi ha'm jabi'q xabarlarqa sankiciyasi'z kiriwdi qi'sqartadi'. Mi'sali', ka'rxana hu'jjetlerdi personaldi' basqari'w, resurs-materiallar ha'm operativ jazi'wlardi' bo'listirgende bir serverge jaylasti'ri'li'wi'n, biraq barli'g'i' u'sh saqlag'i'shqa tiyisli boli'wi'n na'zerde tutadi'. Bul sistemada paydadani'wshi'lar topari' ju'da` kerek bolmasa, olardi'n` hu'jjetlerine kiriw basqalarg'a berilmeytug'i'ni'na isenedi.

Parallel` izertlewi-bul klient/server ortali'g'i' programmali'q ta'miyinlewdi'n` ka'rxana ko'leminde paydalani'latug'i'n komp'yuterlerdin` sorawlari' menen isleydi. Mi'sali', ka'rxanada 3 lokal set quri'lg'an, ha'r biri o'zinin` serserine iye. Ka'rxanani'n` yuris-ken'esgo'yinde barli'q saqlag'i'shlardi' tekseriw za'ru'rligi payda boldi'. Kerekli sawalg'a tiyisli informaciyani' tabi'w (mi'sal, jetkerip beriw buyi'rtpasi', xi'zmet jazi'wlari' ha'm belgili bir kelisimge tiyisli esabatlar). Buni' qa'legen programmali'q ta'miyinlew an`sat isley almaydi'.

Sistemag'a quri'lg'an hu'jjetlerdin` arxitekturali'q qkrami' (HAK) tu'rli hu'jjetlerdi qollap-quwatlawshi' funkciyag'a iye boli'wi' kerek. Sonnan tu'rli tasi'wshi'larda berilgen. SCML, HTML ha'M ob'ektlerdi SUDFni'n` ko'plegen prilojeniyalari' hu'jjetlerdi bir neshe bo'leklerge bo'ledi. Mi'sali', siz tekst redaktori'nda hu'jjetti ashsan'i'z ol buni' sete o'z aldi'na faylda jazi'p aladi'. Al, HAK ta hu'jjet ob'ektlari bo'lek-bo'lek saqlanadi', olar bir-biri menen tek paydalani'wshi' barli'q hu'jjetti ko'rgisi kirgende kesisedi. Tikkeley hu'jjettin` o'zi joq, ol tek virtual tu'rde bar. Barli'q qaramli' bo'lekler saqlawda o'z aldi'na fayli' jaylasti'ri'lg'an. Bunday fayllardi'n` ha'r birin izlew joli'n ko'rip shi'g'i'w kerek. (Hu'jjet ob'ektlarinde), ha'r bir fayl o'zleri tiyisli bolg'an uli'wma hu'jjetke yaki hu'jjetlerdin` bir neshe bo'legine su'yeniwi lazi'm.

Sistema o`zi basqaratug`i`n si`rtqi` ob`ektlardi de qadag`alawi` tiyis. Mi`sali`, bir hu`jjetke tiyisi sistemali`q informaciya polyasi`ndag`i` hu`jjetke tiyisli ob`ekt fizikali`q ta`repi`nen saqlawda turg`an boli`p, SUDFni`n` qadag`alawi`nda emes ha`m oni`n` sistemali`q qorg`awi`nda bolmaydi`. Bunday ob`ekterge audio ha`m video plenalar, mikroinformaciya tasi`wshi`lar ha`m qag`az papkalari` boladi`. Sistemada eski hu`jjetlardi jan`a formatqa konvertaciyalawdi`n` an`sat usi`li` bar. Ha`r bir sistema eski hu`jjetlardi o`zinshe jan`a formatqa o`tkeredi. Geyde bul jazi`wlardi` bir waqi`tta ju`klep ali`w arqali` islenedi. Sistemali`q mag`li`wmatlari` qoldan kirgiziw u`lken ku`sh talap etedi. Sstemani`n` ja`ne bir o`zgesheligi, paydalani`wshi` papkani` ko`rsetedi, bunda buri`ng`i` sistemadag`i` hu`jjet da`slep SUDF ramkasi`na jaylasti`ri`ladi`. SUDFni`n` sistemali`q jumi`s processii menen birigiwin na`zerde tuti`w kerek. SUDF basqari`w sistemasi`ni`n` jumi`s process penen ilesiwine barli`q mu`mkinshilikti jaratadi`. Mi`sali` elektron ob`ektlardi bir paydalani`wshi`dan ekinshisine o`tkeredi. Za`ru`r bolg`anda jumi`sti` sessiyasi`n tamamlawi`n qadag`alaydi`. Ko`plegen ka`rxanalar jumi`sshi` korporaciya jumi`s processin SUDFni` engiziw arqali` elektron tiykarg`a o`tkergen. Jumi`s processin basqari`w sistemasi`n SUDFg`a tuwri`lawdi` an`latadi` yaki AR1 interfays arqali` SUDF prilojeniyasi`na biriktiriledi.

Sistemani` mag`li`wmatlardi`n` so`zlik terminologiyasi` menen ta`miyinlew kerek. Ka`rxana boyi`nsha polya ha`m atributlar, sistemani`n` mag`li`wmatlari` haqqi`ndag`i` terminologiyani`n` bir sistemasi` boli`wi` kerek. Bul jerde en` qi`yi`ni` sol, bunday so`zliklerdin` ko`pshiligi qaytalanbaytug`i`n identifikatorlar (mi`sali`, hu`jjet tu`ri so`z dizbegi-TD 0006 kodi`na tuwri` keliwi kerek) menen sali`sti`ri`ladi`. Ko`plegen SUDFlarda ha`r bir polyag`a ishki paydalani`w ushi`n basqa, al (bunday hu`jjetler tu`rinde) kom`yuterdin` ekrani`na shi`g`i`w ushi`n basqa atama beriledi.

Sistema islenip ati`rg`an hu`jjetli toli`q qadag`alawi` yaki oni`n` ko`lemi haqqi`nda uli`wma mag`li`wmatqa iye boli`wi` kerek. Sistema onda jarati`li`p ati`rg`an ha`m og`an tu`sip ati`rg`an na`rselerdi qadag`alawi` kerek. Ka`rxanada ha`r ku`ni ha`r bir xi`zmetkerge ortasha esapta u`shten beske shekem elektron xat

keledi, og`an tekst redaktorlari`ni`n` hu`jjetleri, elektron keste, komp`yuter vyorstkasi`ni`n` ob`ektlari, sonday-aq, hu`jjetli papkalardag`i` qag`azlar ha`m si`rtqi` pochtadan kelgenlerdi qosami`z. Barli`g`i`n qamti`g`an statistikali`q mag`li`wmatlar planlasti`ri`ladi`, komp`yuterler seti shen`berinde jazi`p ali`p saqlawdi`n` jan`a quwatli`li`g`i`n jetilistirige mu`mkinshilik beredi.

1.5 Sistemani'n` ekspluatsiyali'q xarakteristikasi'

Ekspluatsiyali'q xarakteristika degenimiz bul sistema islewi yamasa model'din` jumi's islewi. Solay da, bizin` jag`dayi'mi'zda bul logikali'q sawal boli'p tabi'ladi'. O`ytkeni, siz sistemani' sati'p alg`ani'n`i'zda sistema islewi tiyis hu`jjetlerdin` ha`mmesin isley ala ma, degen sawalg`a ani'qli'q kirgiziwin`iz kerek. Basqasha aytkanda sistema bul organizaciya isleytug`i'n ha`m si'rttan qabi'llaytug`i'n hu`jjetlerdi islewge ku'shi jeteme eken. Bi'lay qarag`anda, bul a`piwayi'day ko`rinedi, mine a`ne usi' jerde yag`ni'y tu`rli sistemalardi' sali'sti'rg`anda qa`tege jol qoyadi'. Qari'yardar ta'miyinlewdi jetkerip beriwshi eskertpesin ko`rgende, konkret aspektlerdi (Sizin` ka`rxana qansha waqi'ttan berli bul sistemadan paydalanadi'? Sistemada qanday konfiguraciyalar bar? Sistemani' qansha adam paydalanadi'? sistemag`a qansha server jalg`ang`an? Siz qashan son`g`i' ma`rte texnikali'q qollap-kuwatlaw xi'zmetinen ja`rdem soradi'n`i'z?! degen sawallardi' qoyi'w orni'na, bul sistemag`a sizin` kewlin`iz toldi' ma? Sizge bul unadi' ma? Si'yali' sawallardi' beredi.

Sonni' este tuti', jetkerip beriwshi geyde kompaniyani'n` rekomendaciyasi'n beredi, ol bolsa sizin` qoli'n`i'zdag`i' menen tuwri' kelmeydi.

Ji'li'na 250 mi'n` hu`jjet penen isleytug`i'n kishkene firma SUDFni'n` programmali'q ta'miyinlewine kewli toli'wi' mu'mkin. Solay da bul programmali'q ta'miyinlew ji'li'na million jan`a hu`jjetlerdi islewge ku'shi jetpewi mu'mkin ja`ne mi'na sawaldi' beriwdi uni'tpan`, SUDF sete bir waqi'tti'n` o`zinde bir neshe paydalani'wshi'ni'n` talaplari'n qandi'ra alama yaki gezek penen qandi'ra ma? Programmali'q ta'miyilew sistemasi'na paydalani'wshi'lardi'n` bir neshewi kirse, quwatli'li'g`i' jete me? Mag`an tani's bir firma bir waqi'tti'n` o`zinde 300 den 400 ge shekem paydalani'wshi'larg`a xi'zmet ko`rsetiwshi sistemani' izlep ju`redi. Jetkerip beriwshi kompaniyani'n` 50 den 75 ke shekem paydalani'wshi'g`a xi'zmet ko`rsete alatugi'n rekomendaciyasi'n ko`rsetti. Negizinde bul SUDF Sizge kerekli paydalani'wshi'g`a xi'zmet ko`rsete aladi', dedi jetkerip beriwshi. Obrazli' aytqanda, eger adam ju`k mashinasi'n algi'si' kelse, og`an kishi gaboritli eki esikli avtomobil` ali'wdi' usi'ni'p, bul mashinag`a

adam ha'm Siz ma'sla'ha't sorag'anlarg'a mi'naday sawal beriwiniz kerek, olar jan'a SUDF kerek bolsa, eskisin sati'p ala ma eken? Bul sawalg'a juwap ali'p, Siz sistemani'n ku'shli ha'm ha'lsiz ta'repleri haqqi'nda ani'q bahani' bilip alasi'z. Jetkerip beriwshi geyde klientlerdi ma'sla'ha'tke kim jiberip ati'rg'ani'n da oylamaydi'. Men bir waqi'yani' bilemen, sonda SUDFni' jetkerip beriwshi sistema si'nawdan o'tkerilip ati'rg'anda qanday da bir kompaniyani'n rekonstruksiyasi'n ali'p keldi. Bizler kompaniyag'a qon'i'raw etkenimizde, olar basqa sistema izlen', dedi, sebebi bul kompaniya jetkeriw beriwshi menen baylani'sqa kewli tolmaydi' eken. Sog'an hayran qalasan', geypara sistema islep shi'g'ari'wshi'lar haqi'yqi'y klientlerine kim ma'sla'ha't berip ati'rg'ani'n bilmeydi eken.

1.6 Jazi'wlardi' funksional' basqari'w

Paydalani'wshi'lar sistemada an'sat islewi ha'm administratori' hu'jjetler toplami'n basqari'wi' ha'm qadag'alawi' ushi'n bir neshe funkciyalardi'n baylani'sli' biliw kerek. Paydalani'wshi' en`da`slep, bul boyi'nsha o`zine kerekli na`rseni ani'qlap ali'wi' ha'm buni' qanaatlandi'ra alatugi'n sistemani' tabi'wi' tyiis. Solay da, bir neshe uli'wmali'q talaplardi' aji'rati'p ali'wi' kerek.

En`da`slep sistema o`z aldi'na hu'jjetke eki bir topar hu'jjetke sa`ne qoyi'w VR (ko`rip shi'g'i'w ushi'n) funkciyasi'n qollap-quwatlawi' kerek. Mi'sali', firma yuristti sudqa jiberiliwi tiyis hu'jjetlerdin`barli'g'i'na. VR belgisin qoyi'wi' kerek.

Onnan ti'sqari', sistema hu'jjetlerinin`saqlani'w ha'm aylalani'stan shi'g'ari'li'w waqti'na ja`rdem beriwi, sonday-aq, jazi'wlardi'n`aylani'stan shi'g'ari'li'w waqti'n belgilewi kerek. Administrator u'jjetlerdin`o`z aldi'na hu'jjet esabi'nda yaki ob`ekt esabi'nda (mi'sali', papka yaki yashik) saqlani'w waqti'n ani'qlawi' tiyis, jazi'w ni'zamg'a sa'ykes yaki za`ru'rlikke qaray 7 ji'l saqlani'wi' kerek. 7 ji'ldan son`arxiv bo`limine ji`eriledi, bul jerde qanday hu'jjetlerdi saqlap qoyi'w kerek, qaysi'si'n joq etiw kerekligi ani'qlanadi'. Jazi'wlardi' basqari'w funkciyasi'ni'n`buri'ng'i'si' menen baylani'sli' sol-bul mu`mkinshilik jazi'wlardi' ko`riw grafigi belgilenedi yamasa arxivke taslaydi', yaki aylanasi'tan shi'g`aradi'.

Bunnan ti'sqari', sistemada belgilengen jazi'wdi' birewinen ekinshisine saqlaw funkciyasi' da bar. Mi'sali', jazi'p ali'w adminstratori' bes ji'ld aldi'n`g'i' jumi'slar haqqi'nda mag'li'wamlardi' tan`lap aladi', bular bolsa, kerek boli'wi' shamali', olardi' bolsa basqa setler arali'q yamasa avtonom saqlag'i'shqa o`tkeredi. Onnan ti'sqari' sistema hu'jjetlerdi bir topar jazi'wlardan ekinshi toparg'a o`tkerip ali'wi' kerek. Eger shtatlar qi'sqari'wi' menen kompaniyani'n`bir strukturali'q bo`legi joq bolsa, barli'q qalg'an fayllardi' basqa strukturali'q bo`limge o`tkeriw adminisratorg'a ju`klenedi. Sistemada fayllardi'n`daslepki nomerin baqlap baylani'si'n baqlawi' kerek. Eger paydalani'wshi' birinshi fayllardi' tan`lasa, onda konceptual`model`de ani'q ekinshi ha'm u`shinshi basqi'shtagi' israrxiyali'q fayllar menen baylani'si'n yadlap qali'w kerek.

Sistemag`a qoyi`latug`i`n tag`i` bir talap-hu`jjetlerdi sistemag`a tu`siriw processii funkciyasi`n qadag`alaw. Mi`sali`, eger paydalani`wshi` informaciyani` basqa jaqqa qoysa, yamasa qayda qoyi`wdi` bilmese, onda mi`na procedurani` islewi kerek. Onda jazi`p ali`w adminstratori` bul processti qadag`alaydi` ha`m hu`jjetti sistemag`a tuwri` jaylasti`radi`.

Sistemada esap beriw matricasi`n qoyi`w kerek, ol paydalani`wshi` isleytug`i`n sho`lkemnin` strukturali`q bo`leginde boladi` yaki jazi`wlar sessiyasi`nda, og`an bolsa hu`jjetler yaki eki parametрге kiredi. ka`rxanada hu`jjetke kim juwap беретуги`ni`n bioiw kerek. Mi`sali`, jumi`sti`n` bahasi`n беретуги`n mag`li`wmatti` islegen xi`zmetkerler informaciyani`n` tuwri`li`g`i`na juwap berem e yaki bul jag`dayda juwapkershilik menedjerge yamasa personallar menen islesiw bo`limi xi`zmetkerine ju`klene me.

1.7 Tan`lap ali`wdi`n` funkciyanalli`g`i`

Ízlew tamanlang`annan son` (qaran`, kelesi bo`limde) paydalani`wshi` basqa etap-tan`lap ali`wg`a o`tedi. Eger izlew dawami`nda bir qansha hu`jjet tabi`lg`an bolsa, oni`n` ani`qli`g`i` shamali` boladi`. Bunda paydalani`wshi` birinshi ali`ng`an jduwmaqi` fil`trdan o`tkeredi, bunda ol izlew paarametrlerin ani`qlaydi` ha`m og`an tiyisli emes terminlerdi ali`p taslaydi`. Bunnan ti`sqari`, paydalani`wshi` tabi`lgan hu`jjetlerdin` qi`sqasha rezyumesin yaki uli`wma sxemasi` bolmasa sistemali`q informaciyani` hu`jjetni ashpay turi`p ko`rgisi keledi. Mi`sali`, izlew dawami`nda hu`jjetlerdin` zavolovkasi` tabi`ladi`. Zagolovkalardi` oqi`p paydalani`wshi` olar menen jaqsi`lap tani`si`w ushi`n onnan bir yamasa yaki konkret hu`jjetni tan`lap aladi`.

Bul funkciya klient /server sistemasi`nda sorawlardi` ki`sqarti`wg`a mu`mkinshilik jaratadi`. Eger izlewdi taraycaq, yag`ni`y izlekwde hu`jjetlerdi 10 g`a qi`sqarcaq, olardi` da bir ma`rtede bir neshewin g`ana ko`rsek, setke (paydalani`wshi`g`a da) tu`setug`i`n ju`k qi`sqaradi`. Onnan ti`sqari`, rezyume hu`jjetin` bar-joqli`g`i`n biliw mu`mkinshiligin jaratadi`. Bunda xi`zmetkerge hu`jjetni ko`riw za`ru`rligi qalmaydi`. Hu`jjetni tawi`p, paydalani`wshi` oni` oqi`w ushi`n ko`riwi mu`mkin.

Ízlewdin` funkcionalli`g`i`

Endi izlew processin toli`g`i`raq ko`rip shi`g`ami`z. A`lbette, izlewdin` barli`q funkciyasi` da paydalani`wshi`g`a za`ru`r emes, biraq qanday mu`mkinshilikler bar ekenligin biliw ko`plik etpeydi. Sizin` ka`rxanan`i`z talabi`nan kelip shi`g`i`p, funkciya fakul`tativ, kerek eki kerek boli`wi` mu`mkin. Ízlew funkciyasi` diopazoni` ju`da` ken` boli`wi` mu`mkin.

II-BAP. ELEKTRON HU`JJET AYLANI'SI'NDA ELEKTRON CİFRLİ' İMZA ALGORİTMLERİNİN SALİ'STİ'RMALİ' ANALİZİ.

Ha`zirgi ku`nde ja`miyetimizdin` barlı'q tarawları'nda zamanago`y informaciyalı' texnologiyalardı', komp`yuter texnikası' həm telekommunikaciya quralları'n hər bir tarawg`a engiziw olardan paydalani'w, puxaralardı'n` informaciyag`a bolg`an talaptı'n` arti'wi', jəhan informaciyalı'q jamiyetge aylanı'p baratı'rg`an talap həm zəru`rlıklar di ja`nede qandı'ri'w, informaciyalı'q resurslardan paydalani'wdi' ken`eytiw ushi'n qolay sharayat jaratı'p beriw ushi'n «Elektron cıfrlı' imza» tusinigi jəmiyetimizge kirip keldi.

Elektron hu`jjet texnika quralları'nan həm informaciyalı'q sistemalardan həm informaciyalı'q texnologiyalardan paydalang`an halda jaratı'ladi', qayta islenedi həm saqlanadi', Elektron ko`riniste jazı'lg`an ECİ quralları'nan paydalani'p, ECİ menen tasta'yi'qlang`an həm elektron hu`jjetin` oni' identifikaciya qı'li'w imkaniyatı'n beretug`i'n basqa rekvezitlerge iye bolg`an informaciya elektron hu`jjet bolı'p esaplanadi'.

ECİ — elektron hu`jjetge usi' elektron hu`jjet informaciyani' ECİ jabi'q gıltın paydalang`an halda arnawlı' o`zgerisler kiritiw nətiyjesinde payda qı'li'ng`an həmde ECİ ashi'q gıltlı jərdeminde elektron hu`jjetdegi informaciyada qa`telik joqlı'g`i'n ani'qlaw həm ECİ jabi'q gıltının` iyesin identifikaciya qı'li'w imkaniyatı'n beretug`i'n imza. Bul informaciya - kommunikaciya sistemaları' arqalı' uzatı'latug`i'n hu`jjetlerdi həm informaciyalardı'n` durı'slı'g`i'n tekseriwde qollanı'ladi'.

Mag`li'wmat jiberiwshinin` qabi'l qı'li'wshi'g`a qandayda bir mag`li'wmatı'n əpiwayı' usi'lda jiberiw ko`p jag`daylarda tu`rlishe mashqalalardı' keltirip shı'g`aradı'. Bunday jag`daylarda tu`rlishe mashqalalardı'n` elip shı'g`i'wi'na alı'p keledi. Bunda process qatnası'wshi'lar tiykari'nan to`mendegi jag`daylarg`a duslası'wi' mu`mkin:

- biykarlaw – xabar jibergen o`zi jibergen xabardi' biykarlaw;
- o`zgertiw – qabi'l qı'li'wshi' xabardi' o`zgertedi;

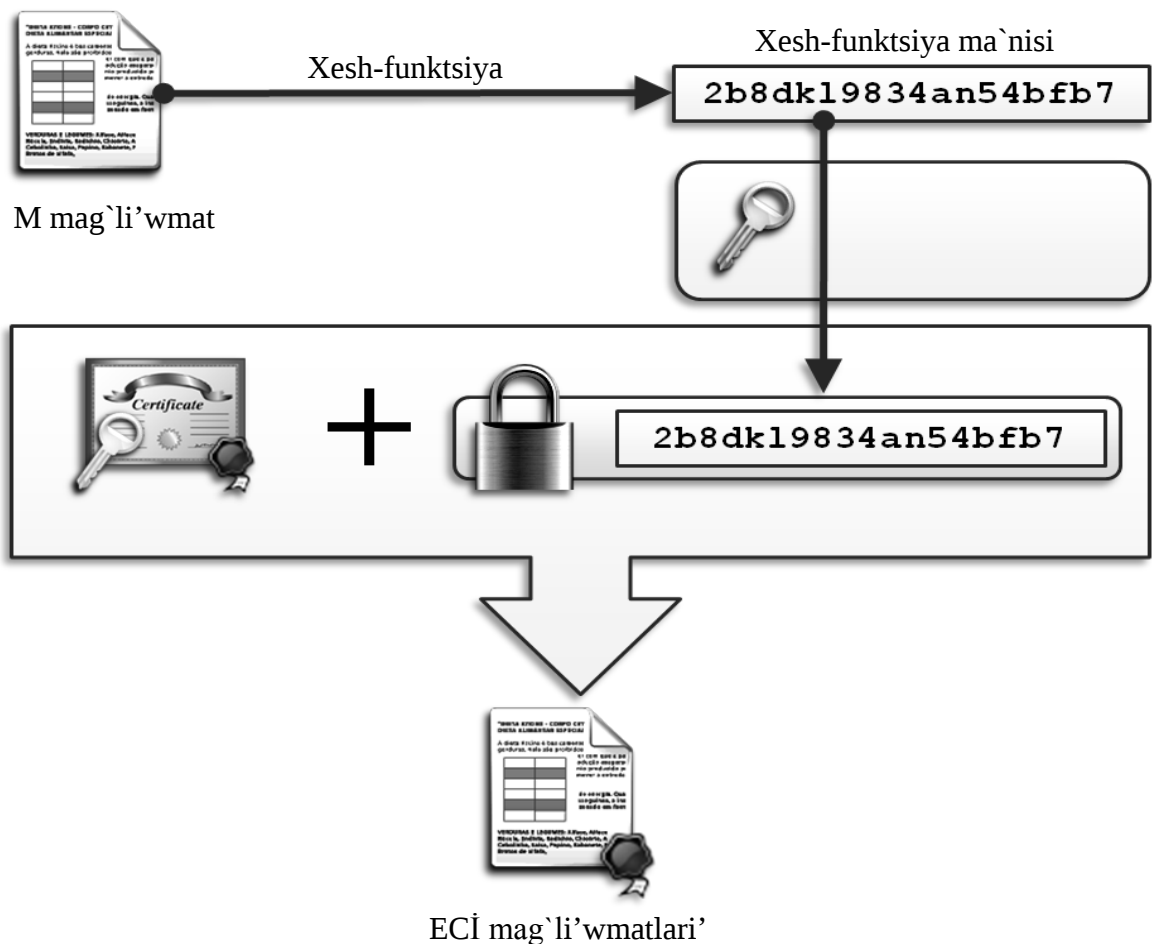
- maskalaw – ta`rtip buzard xabardi' basqa shaxsqa rasmiylestiredi.

Usi'nday jag`daylarda ECI baylani's sistemalari'nda joqari'da sanap o`tilgen buzg`i'nshi'li'qlar bolmawi' tamiynlenedi, yag`ni'y:

- Jasi'ri'n gilt tek g`ana jiberiwshinin` o`zine belgili bolsa, bunday jag`dayda qabi'l qi'li'wshi' terepinen qabi'l qi'li'p ali'ng`an mag`li'wmat tek g`ana jiberiwshi terepinen jiberilgenligin d`lilleydi

- Qarama-qarsi' terep jasi'ri'n gilti bilmegen halda o`zgertiw, qalbekilestiriw, maskalaw h`m basqa usi' qusag`an baylani's sistemasi' qag`i'ydalari'n buzi'li'wi'na imkaniyat bermeydi. Hu`jjetti o`zgertiwte xesh ma`nis o`zgeredi h`m imza ni'zamli' ku`shke iye bolmay qaladi'.

Sunday-aq, ECI ka`rxana h`m sawda-sati'qqa tiyisli sho`lkemlerde esabatlardi' elektron ko`rinside tapsi'ri'wda, elektron hu`jjetke yuridik ku`sh beriw u`lken `hmiyetke iye.



2.1 ECI ni payda etiw processi.

ECI ni'n` uli'wma tən ali'ng`an sxemasi' (modeli) u`sh processti o`z ishine aladi':

- ECI giltlerin generaciyalaw;
- ECI ni' payda etiw;
- ECI ni' tekseriw.

Elektron hu`jjetti ECI menen payda etiw processi 1-surette keltirilgen boli'p, jiberiliwshi mag`li'wmatti'n` xesh-funkciya ma`nisi esaplanadi'. Sonnan elektron cifrli' imza algoritmine qarap jiberiwshi tərep jabi'q gilti arqali' mag`li'wmat imzalanadi'.

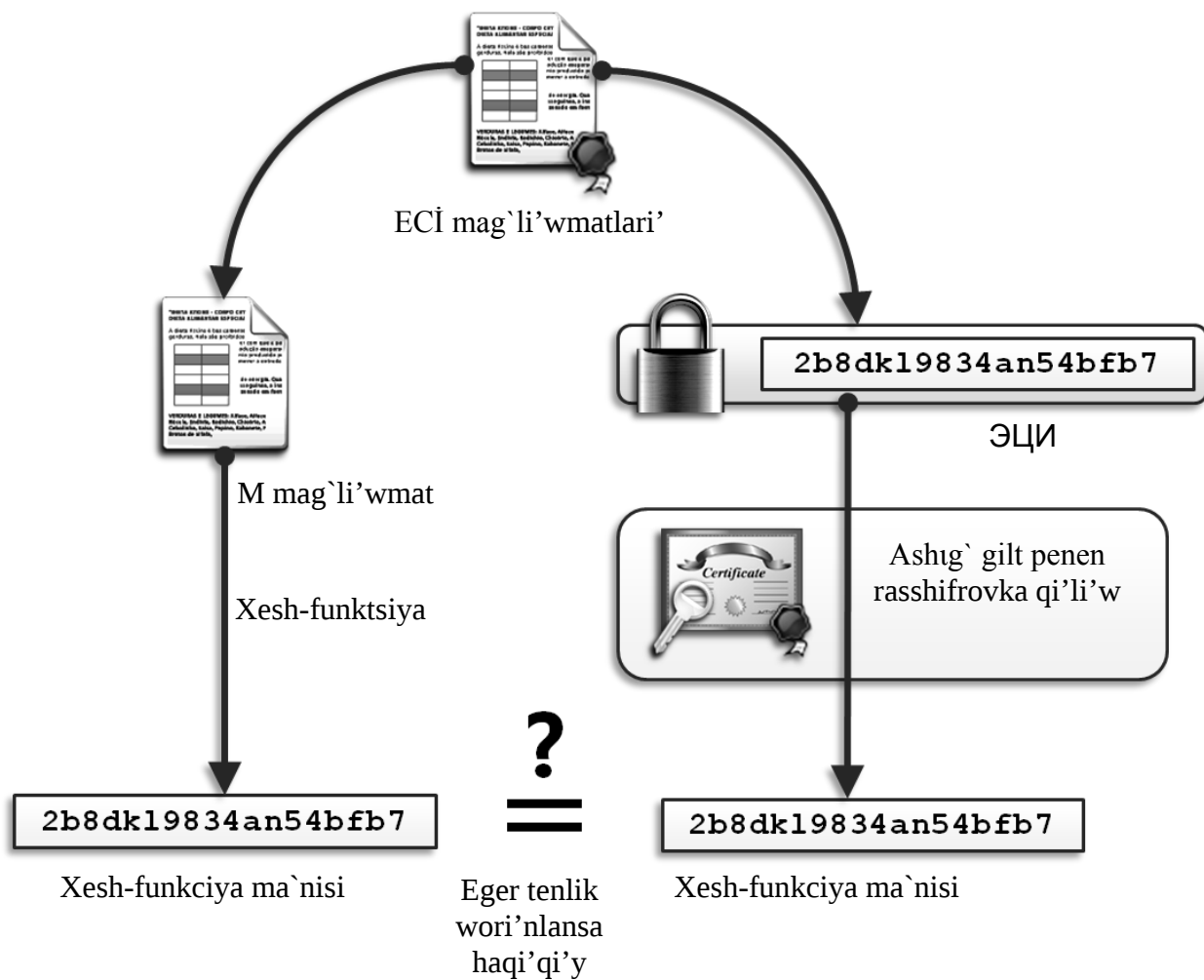
ECI ni' tekseriwde jiberiwshi ta`repien ashi'q giltli gilti arqali' esaplang`an xesh-funkciya ma`nisi həm mag`li'wmat xesh-funkciya ma`nisleri sali'sti'ri'ladi'. To`mendegi 2-su`wrette. ECI ni tekseriw processi keltirilgen.

Tu`rli ECI algoritmlerin payda etiw həm oni'n` haqi'yqi'yli'g`i'n tekseriw a`melleri olardi'n` matematikali'q funkciyalarii' arqali' parqlanadi'.

ECI algoritmlerinin` matematikali'q funkciyalari' mashqalalari' quramali'li'g`ana qarap klasslarga bo`lingen (1-keste):

- Faktorlaw mashqalasi'ni'n` quramali'li'g`i'na tiykarlang`an ECI algoritmleri.
- Diskret logarifm mashqalasi'ni'n` quramali'li'g`i'na tiykarlang`an ECI algoritmleri.
- Elliptik si'zi'qli' diskret logarifm mashqalasi'na tiykarlang`an ECI algoritmleri.
- Parametrler algebrasi'na tiykarlang`an ECI algoritmleri.
- Turli mashqalalarga (masalen. Kvadratik sheklew, n moduli' boyi'nsha kvadratkorengə) tiykarlang`an ECI algoritmleri.

To`mendegi 1-tablicada ECI algoritmleri mashqalalar quramali'li'g`i' boyi'nsha klasslarga bo`lingen.



2.2 ECI ni' tekseriw processi

1-keste

ECI algoritmlerinin` mashqalalar quramali'li'g'i' boyi'nsha klasslaw

ECI algoritmleri				
Faktorlaw mashqalasi'-na tiykarlang'an ECI	Diskret logarifmlaw mashqalasi'na tiykarlang'an ECI	Elliptik iymek si'zi'qli' diskret logarifmlash mashqalasi'na tiykarlang'an ECI	Parametrler algebrasi' mashqalasi'na tiykarlang'an ECI	Turli mashqalasi'na tiykarlang'an ECI
RSA, ESIGN, Ong-Schnorr-Shamir, PGP, RPK	EGSA, DSA, Shnorr, GOST 34.10-94	ECDSA, GOST 34.10-2001, EC-KCDSA, EC-GDSA , DSTU 4145-2002	O'zDSt 1092:2009	Kvadratik sheklew, n moduli boyi'nsha kvadrat korennen shi'gari'wg'a tiykarlang'an ECI algoritmleri a'meliyatda kem qollani'ladi'

Faktorlash mashqalasi'na tiykarlang'an algoritmler topari'na kiriwshi RSA h m ESIGN qusag'an ECI algoritmleri ko'p qollani'ladi'. RSA algoritminin` q wipsizlik da'rejesi u'lken sanlardi' ko'beytiwshilerge ajrati'w quramali'li'g'i'na tiykarlanadi'. Usi' algoritm ashi'q modul  $n$  eki tu'p sanni'n` ko'beymesi boli'p, ko'beytiwshiler si'r tuti'ladi'. Bul tu'p faktor (kobeytiwshi)lerdi n boyi'nsha tabi'w, yag'ni'y faktorlasti'ri'w mashqalasi'n sheshiw qi'yi'n quramali' mashqalalar tu'rine kiriwi kriptosistemani'n` joqari' shi'damli'li'g'i'n t miynleydi.

ESIGN sxemasi' 1985 ji'l Yaponiya ali'mlari' t repinen usi'ni's ki'li'ng'an. Bul elektron cifrli' imzani'n tiykarli' xarakteri oni'n` tezliginde. RSA yamasa El-Gamal algoritmleri sali'sti'ri'lg'anda, ESIGN algoritmi ja'rdeminde hu'jjetti

imzalar ham imzani tekseriw processi bir neshshe ret tezlik penen amalge asiri'ladi'.

Imza parametrlariga to'mendegiler kiredi: ESIGN algoritminde si'rli' gilt si'pati'nda u'lken tu'p p ham q sanlar jupli'g'i'nan paydalani'ladi' ham ular boyi'nsha $n = p^2 * q$ ten'lik penen ani'qlanadi'. Ashi'q gilt si'pati'nda (n, k) jupli'g'i' ali'nadi'. Bul jerde k – qawipsizlik parametri.

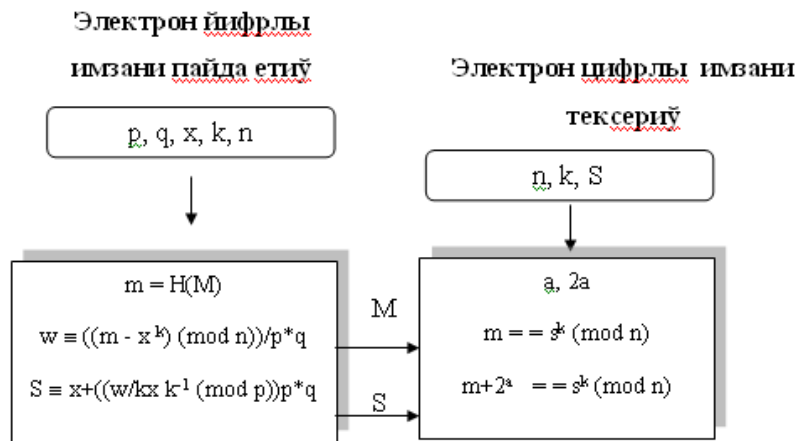
ESIGN algoritmi boyi'nsha ECI payda etiw ham oni' uzati'w to'mendegi adi'mlarda izbe-izligin o'z ishine aladi' (3-su'wret):

1. M informatsiya ushi'n $m = H(M)$ xesh-funktsiya esaplanadi', $0 < m < n-1$.
2. x son generatsiyalanadi', $p * q < x$.
3. $w \equiv ((m - x^k) \pmod{n}) / p * q$.
4. S elektron cifrli' imza payda etiledi:
$$S \equiv x + ((w / k x^{k-1} \pmod{p})) p * q$$

Qabi'l qili'wshi' ta'rep ali'ng'an informatsiya M ham elektron cifrli' imza S ten paydalani'p to'mendegi adi'mlar izbe-izligin o'z ishine aladi':

1. xesh-funktsiya $m = H(M)$ esaplanadi';
2. ashi'q gilt (n, k) nan paydalani'p S ushi'n $S^k \pmod{n}$ esaplanadi';
3. n bitler sani'ni'n' eki eselengenin 3 ga bo'lgenge ten' yamasa u'lken bolg'an, pu'tinnen bir qancha kishi a sani' ham 2^a esaplanadi';
4. m ham $m + 2^a$ menen $S^k \pmod{n}$ sali'stiri'ladi':
$$m = S^k \pmod{n};$$
$$m + 2^a = S^k \pmod{n}.$$

Eger $S^k \pmod{n}$ m ga ten' yamasa onnan u'lken bolsa ham $S^k \pmod{n}$ $m + 2^a$ dan kishi bolsa, ECI haqi'qi'y, keru jag'dayda haqi'qi'y emas dep tabi'ladi'. Bul algoritmda x ham k menen baylani'sli' esaplawlardi' aldi'nnan ori'nlap qoyi'w imkoniyati' barli'g'i' ECI payda etiw processin tezlestiriwge imkoniyat jaratadi'.



2.3 ESIGN algoritmi

ESIGN algoritmin payda etiw h m tekseriw processleri

Diskret logarifmlaw mashqalasi'na tiykarlang'an Shnorr elektron cifrli' imzasi'n payda etiw tiykarǵı' modul tiykari'nda esaplanatug'ı'n h m onnan bir qansha kishi ekinshi tu'p moduldan paydalani'ladi'. Shnorr elektron cifrli' imzasi' giltlerdi generaciya qı'li'w ushi'n birinshi eki tu'p p h m q san sonday tan'lanadi', q sani', $p-1$ di'n  ko'beytiwshisi bolǵ'an. Keyin $a^q \equiv 1 \pmod{p}$ bolǵ'anda 1 den u'lken a tan'lanadi'. r, q h m a erkin halda boli'wi' ha'mde paydalani'wshi'lar topari' ushi'n qollani'li'wi' mu'mkin [5].

Giltler jupli'g'ı'n generaciya qı'li'w ushi'n q dan kishi qa'legen san tan'lanadi'. Ol jasi'ri'n gilt s boli'p, oni'n  ja'rdeminde ashkara gilt $v \equiv a^{-s} \pmod{p}$ esaplanadi'.

Shnorr elektron cifrli' imza sxemasi'ni'n  tiykarǵı' kemshiligi, qarama-qarsi' t rep kriptosistema tiykari'nda ali'ng'an diskret logarifm mashqalasi'n jeterli ani'q qoya alg'anda h m oni'n  bul mashqalani' sheshiwde resursleri' jeterli bolǵ'anda qabi'l qı'li'wshi' kelip tu'sken elektron cifrli' imza jalǵ'anli'g'ı', imzalawshi' shaxsda imzani' jalǵ'anli'g'ı'n d lillewshi d liyller h m mag'li'wmatlardi'n  joqli'g'ı'.

Q wipsizlik bag'anasi' bir qı'yli' bolǵ'anda Shnorr sxemasi' ushi'n elektron cifrli' imza uzi'nli'g'ı' RSA h m El-Gamal elektron cifrli' imza sxemalari'n

ekiden bir qansha ki'sqa. Milliy standartdag'i' O'zDSt 1092:2009 standarti'nda ha'm Shnorrr algoritmine tiykarlang'an r h m q modullerinen paydalani'ladi'.

H zirgi waqi'tta en' quramali' esaplang'an elliptik iymek si'zi'qli' diskret logarifm mashqalasi'na tiyarlang'an ECİ algoritmlerinen ken' paydalani'lmaqta. Elliptik kriptografiyani'n' abzalli'q ta'repi sonda, usi' waqi'tta elliptik iymek si'zi'qlar tochkalari' topari'na diskret logarifmlew ma'seleleri sheshimlari ushi'n subeksponencial algoritmler jarati'lmag'an.

Bu mashqalag'a tiykarlang'an algoritmlerdin' en' belgililari GOST 34.10-2001, ECDSA ECİ algoritmleri esaplanadi'. ECDSA algoritminde gilt o'lshe-min o'shiriw menen imza payda etiw sezilerli d rejede tez a'melge asi'ri'ladi', imza haqi'yqi'yli'g'i'n tasti'yi'qlaw bolsa bir qansha a'ste boladi'.

To'mendegi 2-estede elliptik iymek si'zi'qli' diskret logarifm mashqalasi'na tiykarlang'an ECDSA algoritminin' faktorlaw mashqalasi'na tiykarlang'an RSA algoritmine sali'sti'rg'anda qi'sqa giltler tezligi ko'rsetilgen.

2-keste

RSA h m ECDSA algoritmleri tiykari'nda ECİ jarati'w h m oni' tekseriw

Algoritmler	İmza jarati'w	İmzani' tekseriw
RSA (2048 bit)	120 ms	5ms
ECDSA (216 bit)	68 ms	70 ms

Kesteden ko'rinip turg'ani'nday, 216 bit uzi'nli'qta ECDSA algoritmi menen ECİ jarati'w ushi'n ketken 2048 bit uzi'nli'qta RSA algoritmi menen ECİ jarati'w ushi'n ketken waqi'ttan shama menen 2 ese kem sari'planadi'.

H zirgi kundegi quramali'li'q d rejesi joqari' bolg'an kriptografik mashqalalardan biri bul parametrlar algebrasi'. O'zbekstanli' ali'mlar t repinen islep shi'g'i'lg'an O'zDSt 1092:2009 standarti' usi' mashqalag'a tiykarlang'an. Onda modul arifmetikasi'ni'n' jasi'ri'n joli' jan'a bir ta'repleme funkciyasi' qollani'ladi'. O'zDSt 1092:2009da elektron cifrli' imzani' payda etiw processine elektron cifrli' imzani'n haqi'qi'yli'g'i'n tasti'yi'qlaw processinde

qollani'latug'i'n seans gildi ta'rtibin kiritiw menen elektron cifrli' imzani'n`
jalg'anli'g'i'n ani'qlaw na`zerde tuti'ladi'.

Bul algoritmda to'mendegi matematik tiykarlardan paydalani'ladi':

Tiykar X ti' p modul boyi'nsha R koefficient menen e da'rejege ko'teriw
a'meli to'mendegishe belgilenedi: $X^e \pmod{p}$ [4, 6].

$$X \otimes Y \pmod{p} \equiv X + (1 + X \times R) \times Y \pmod{p} .$$

X o'zgeriwshinin p modul boyi'nsha R koefficient menen kerilew a'meli X^{-1}
¹ ko'riniste belgilenedi:

$$X^{-1} \equiv (p - X) \times (1 + X \times R)^{-1} \pmod{p}.$$

To'mendegi 3-kestede. O'zDSt 1092:2009 ECİ algoritminin` ECDSA
algoritmi menen sali'sti'rmali' analiz keltirilgen.

**O'zDSt 1092:2009 algoritmin ECDSA algoritmi menen
sali'sti'rmali' analizi**

Ko`rsetkishler	O'zDSt 1092:2009	ECDSA
Modul`	$p > 2^{255}$	$n > 2^{255}$
Faktor	$2^{254} < q < 2^{256}$	-
Tiykar	Yopiq - g	Ashi'q tochka R
Tiykarg`i' ameller	Koefficient penen darejge ko`teriw	Qosi'w
	Koefficient menen ko`beytiw	Biykarlaw
	Koefficient menen kerilew	Konkatenaciya
	-	Ko`p martelik qosi'w
Jabi'q gilt	U`shlik (x,u,g)	x
Ashi'q gilt	Jupli'q (y,z)	Q
Jalg`andi' ani'qlaw gilti	Jupli'q (R_1, y_1)	-
ECİ	Jupli'q (r, s)	Jupli'q (r, s)

Usi' tablicadan ko`rinip turg`ani'nday, ECDSA algoritminin kemshiligi amellerdi quramali'li'g'i' h m jalg`anli'g'i'n ani'qlaw giltinin joqli'g'i'. Joqari'dag'i'larg`a tiykarlani'p, O'zDSt 1092:2009 da imza o`zgeratilgen yamasa jalg`anlasti'ri'lg`an bolsa, buni' bilip ali'w imkaniyati' bar boli'p, buni'n ushi'n seans gilti maromdan paydalanish kerek boladi.

III-BAP. ELEKTRON HU`JJET AYLANI'SI'N AVTOMATLASTI'RI'WDI' TA'MIYNLEWSHI SISTEMANI' JARATI'WDA QOLLANI'LATUG'I'N DRUPAL PROGRAMMASI'



Drupal—PHP tilinde jazi'lgan ha'm relyacion mag'li'wmatlar bazasi'nda saqlawshi' si'pati'nda isleytugi'n MySQL, PostgreSQL, Java ha'm basqa da'stu'rler menen birgelikte isleydi. Drupal ashi'q kodli' erkin programmali'q ta'miynat, GPL licenziyasi' menen qorg'alg'an, ham du'n'yadag'i' entuziastlerdin' ha'reketleri menen rawajlanbaqta.

Dastu'rdi Intel mashinada ha'm Makentosh te ha'm birdey ko`riniste boladi'.

3.1 Drupal programmasi'n Ubuntu operacion sistemasi'nda ornati'w



Repozitordi' ornati'w

Drupal 6 ornati'w ushi'n to'mendegi buyri'qlardi' ori'nlaw jeterli.

```
sudo apt-get install drupal6
```

Ubuntu 12.04 operacion sistema repozitori'nda Drupal 7 ni ornati'wdi'n baslang'i'sh ko`rinishi.

```
sudo apt-get install drupal7
```

Drupal di' Apache ta dizimnen o'tkeriw

- Drupal 6 ushi'n:

```
sudo ln -s /etc/drupal/6/apache.conf /etc/apache2/conf.d/drupal6.conf
```

- Drupal 7 ushi'n:

```
sudo ln -s /etc/drupal/7/apache2.conf /etc/apache2/conf.d/drupal7.conf
```

Apache ti' qayta ju'klew

```
sudo /etc/init.d/apache2 restart
```

Repozitoriyada ornati'lg'an versiyani' ko'rip shi'g'ami'z.

Ornati'wdan aldi'n sizde LAMP ha'm php5-gd paketi ornati'lg'anli'g'i'n tekserip ko'rin` Drupal di'n` arnawli' dastu'ri arxivinen ju'klep ali'n`:

```
wget http://ftp.drupal.org/files/projecc/drupal-7.14.tar.gz
```

1. Ju'klep ali'ng'an mag'li'wmatti' arxivten ashi'w:

```
tar -xvzf drupal-7.14.tar.gz
```

2. Katolog jarati'w ha'm og'an arxiv fayllari'n jaylasti'ri'n`.
/var/www/drupal:

3. **sudo mkdir /var/www/drupal**

```
sudo mv drupal-7.14/* drupal-7.14/.htaccess /var/www/drupal
```

4. Dastu'r ushi'n direktoriya jarati'n` ha'm oni' www-data iyesine ornati'n`:

5. **sudo mkdir /var/www/drupal/sites/default/files**

```
sudo chown www-data:www-data /var/www/drupal/sites/default/files
```

6. Sazlaw fayllari'n ko'shirin`:

7. **sudo cp /var/www/drupal/sites/default/default.settings.php
/var/www/drupal/sites/default/settings.php**

```
sudo chown www-data:www-data  
/var/www/drupal/sites/default/settings.php
```

8. To`mendegishe konfiguraciya fayli`n jarati`n`
Apache */etc/apache2/sites-available/drupal* :

9. Alias */drupal /usr/share/drupal*
10.
11. <Directory */usr/share/drupal/*>
12. Options +**FollowSymLinks**

AllowOverride All

13. order allow,deny
14. allow from **all**

</Directory>

15. Aldi`ng`i` dastu`rdin` punkti`n qosi`n` ha`m Apache ti` qayta ju`klen`:

16. **sudo** a2ensite drupal

```
sudo /etc/init.d/apache2 restart
```

Sazlaw

Paydalani`wdan aldi`n Drupal mag`li`wmatlar bazasi`n mysql klienti ja`rdeminde jarati`n`:

```
CREATE DATABASE название_базы;
```

Tek jarati`lg`an bazag`a ruxsat beriwshi bo`lek MySQL paydalani`wshi`si`n belgilew:

```
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX,  
ALTER, CREATE TEMPORARY TABLES, LOCK TABLES ON  
название_базы.* TO 'drupaluser'@'localhost' IDENTIFIED BY 'drupalpass';
```

Bul operaciyalardi' phpMyAdmin ja'rdeminde a'melge asi'ri'wg'ada boladi'. <http://localhost/drupal7/install.php> betine o'tin` (ornati'li'p ati'rg'an versiyag'a qarap jol o'zgeriwi mu'mkin) ha'm ornati'w procedurasi'na o'tin`:

1. Kerekli tildi tan'lan`.
2. Jarati'lg'an mag'li'wmatlar bazasi' xaqqi'nda mag'li'wmatlardi' tolti'ri'n` ha'mde paydalani'wshi' ha'm paroldi de.

Eger clean URLs opciyasi'n qosi'w talap etilse to'mendegi buyi'ri'qti' ori'nlan`:

```
sudo a2enmod rewrite
```

```
sudo sed -i "s/^.*# RewriteBase \/drupal/ RewriteBase \/drupal/"  
/etc/drupal/7/htaccess
```

Tekstli fayldi' o'shiriw:

Katalog tiykari'nda

```
cd ~/public_html  
rm -f CHANGELOG.txt COPYRIGHT.txt INSTALL.mysql.txt  
INSTALL.pgsql.txt INSTALL.txt LICENSE.txt MAINTAINERS.txt  
UPGRADE.txt
```

modul kataloglari'nda aldi'n nelerdi o'shiriw kerekligin ko'rip shi'g'ami'z .

```
find ~/public_html/sites/all -name "*.txt" -type f | xargs ls
```

keyin o'shiremiz

```
find ~/public_html/sites/all -name "*.txt" -type f | xargs /bin/rm -f
```

Moduldi ornati'w

dh-make-drupal– An`satraq basqari'w ushi'n Drupal modulinen dh-make-drupal skript jarati'wg'a imkan beredi. Buni' ju'klew ushi'n ori'nlan`:

```
sudo apt-get install dh-make-drupal
```

Paydalani'w mi'sallari':

```
dh-make-drupal views
```

```
sudo dpkg -i ./drupal6-mod-views_2.16-1_all.deb
```

Drush

Drush – buyri'qlar qatari'nan Drupal di' basqari'wda ruxsat beretug'i'n instrument. Keshti tazalaw, moduldi ornati'w, bekaplardi' jarati'w, statusqa iye boli'w si'yaqli' bir qansha ha'reketlerdi a'melge asi'ri'w. Toli'q ha'reketler diziminin` dizimin to'mendegi dastu'rde ko'riwin`iz mu'mkin <http://www.drush.org/>.

Drush Ubuntu repozitori'nda saqlanadi' oni' ornati'w ushi'n to'mendegi buyi'ri'qti' ori'nlan`.

```
sudo apt-get install drush
```

Bekap bazalari'

Bekap mag'li'wmatlar bazasi'n jarati'w

```
drush -r /usr/share/drupal6 sql-dump --result-file=~db_backup.sql
```

Janalaw

Drupaldi'n` jan`alang`ani'nan keyin mende modullerim joyti'ldi' ha'm o`ship ketti clean urls bekap fayllari'

~/drush-backups/drupal6/20120709210216/drupal papkasi'nda saqlanadi'. Eger /usr/share/drupal6/.htaccess. fayli' orni'na /etc/drupal/6/htaccess ssi'lkasi'n jaracaq clean urls ti' qayta tiklewge boladi', joyti'lg`an modullerdi qaytadan ornati'wg`a boladi'.

```
sudo drush -r /usr/share/drupal6 up
```

Moduldi ornati'w

Moduldi ju`klew

```
sudo drush -r /usr/share/drupal6 dl cck ckeditor admin bueditor i18n captcha  
contact_field views
```

ornati'w

```
sudo drush -r /usr/share/drupal6 en content text ckeditor admin bueditor i18n  
captcha image_captcha contact_field views views_ui
```

Dəstu'r bekapi'

Dəstu'r bekapi' to'rt etaptan ibarat:

1. Dəstu'r xi'zmet ko'rsetiw jag'dayi'na o'tkeriw
2. phpmyadmin programmasi' ja'rdeminde MB nusqasi'n saqlaw
3. Ba'rshe fayllardi' ko'shiriw
4. Dəstu'r izlew jag'dayi'na o'tkeriw

ssh, rsync i drush ja'rdeminde bekap dəstu'rin yari'mavtomat isletiw mu'mkin:

1. Ani'q waqi'tqa baylani'sli' papka jarati'w

```
mkdir ~/work/backup/$( date +%H.%M_%d.%m.%Y )
```

2. ssh ja'rdeminde programmag'a kiriw

```
ssh user@hostingserver.ru
```

3. Programmani' offlayng'a o'tkeriw

```
~/drush/drush -y -r ~/public_html vset site_offline 1
```

4. bekap MB jarati'w

```
~/drush/drush -r ~/public_html sql-dump --result-file=~baza_drup1.sql
```

5. Basqa konsoldag'i' ba'rshe fayllardi' ssh ha'm rsync ja'rdeminde nusqalaw.

```
rsync -v -a -r -t -e ssh user@hostingserver.ru:/home/siteaccount/  
~/work/backup/31.01.2012
```

6. MB dag`i` birinshi konsoldi` o`shiriw

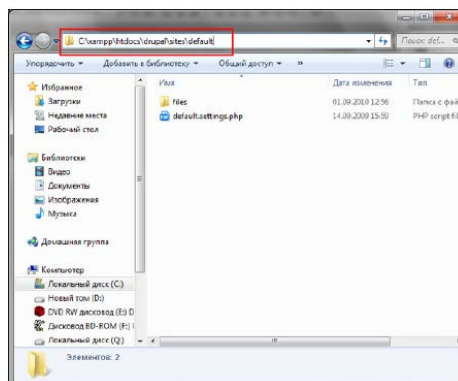
```
rm ~/baza_drup1.sql
```

7. Programmani` aktivlestiriw

```
~/drush/drush -y -r ~/public_html vset site_offline 0
```

3.2 Drupal programmasi`n Windows operacion sistemasi`nda ornati`w

Drupal programmasi`n ornati`w bir qansha qa`demlerden ibarat. Birinshi Drupal programmasi` qatti` disktn` qaysi` bo`limine ornati`li`wi` ko`rsetiliwi kerek yaki o`zi tuwri`dan-tuwri` Windows jaylasqan diskten ori`n iyeleydi

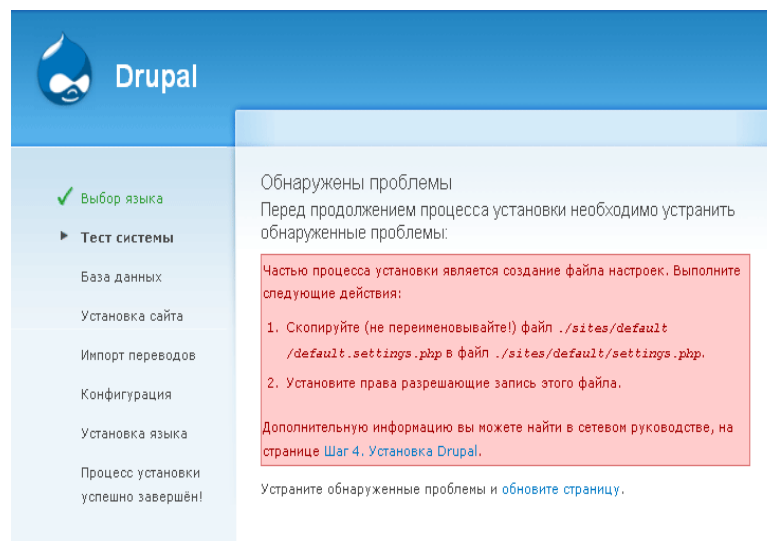


drupal.site

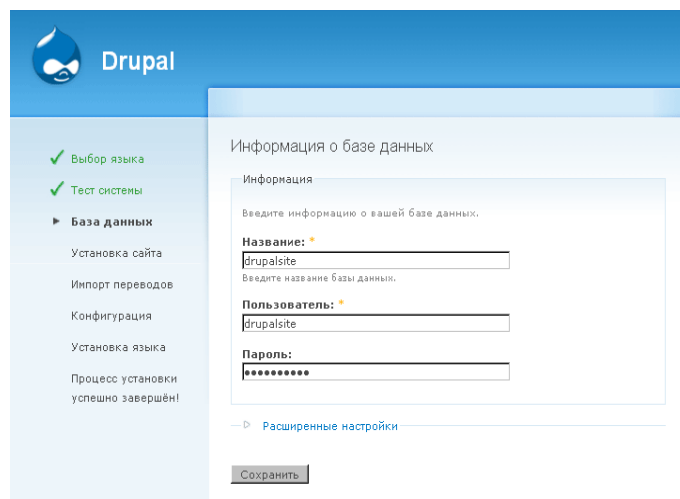
Kerekli tildi tan`law ma`selen «Russian (Русский)» ha`m kelesi etapqa «Select language» tuymesi ja`rdeminde o`tiw.



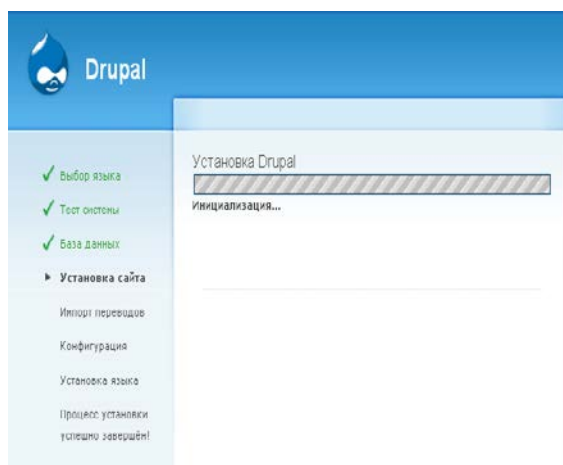
Kelesi bette Drupal *sites/default* papkasi'nda *settings.php* fayli'n jarati'wg'a ruxsat etedi. Bul fayl *default.settings.php* fayli' ishinde jaylasadi'. Jarati'lg'an jan'a fayldi' o'zgertpew u'lken a'hmiyetke iye. Solay etip *sites/default* papkasi'nda eki fayl: *default.settings.php* ha'm *settings.php* jaylasadi'. «обновите страницу» ssi'lkasi'n basi'w menen aqi'rg'i' qatarg'a o'tiledi.



Kelesi bet mag'li'wmatlar bazasi'n ornati'w (ismi, paydalani'wshi' ha'm parol') kiritiledi «Сохранить» tu'ymesı basi'ladi'



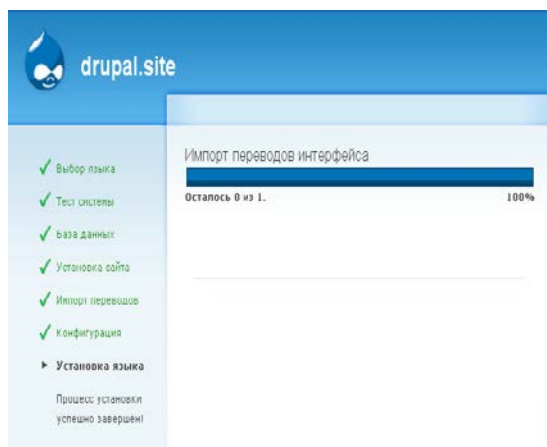
«Установка Drupal» aynasi' tezlik penen jawi'ladi', ha'm sol waqi'tta Drupal *settings.php* fayli'na o'zgerisler kiritedi.



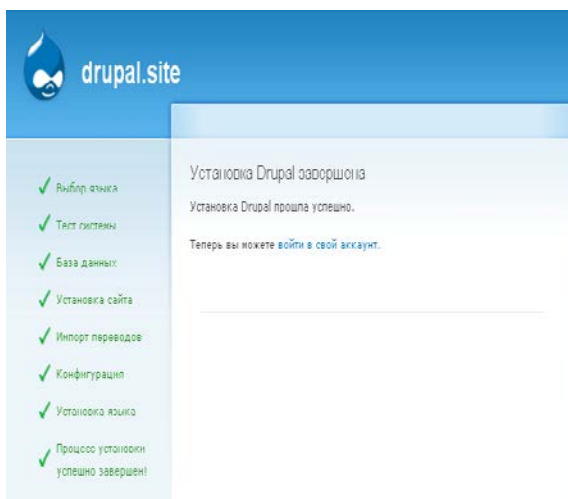
Keyingi bette “Импорта переводов интерфейса” procedurasi' dawam etedi ha'm toli'q ekrandi' iyeleydi. Uli'wma xostingte u'lken ko'lemdegi mag'li'wmatlardi' jaylasti'ri'w ha'm sheklengen waqi't dawami'nda soralg'an buyi'ri'qlar ha'm mag'li'wmatlardi' tuwri' jetkerip beriw imkani'n jarati'p beredi.

Usi' procedura na'tiyjeli tamamlansa dastu'rge ba'rshe kerekli mag'li'wmatlar kiritiledi (ati', pochta adresi, qosi'msha kerekli ssi'lkalar, waqi't ko'rsetkishleri) ha'm basqa.

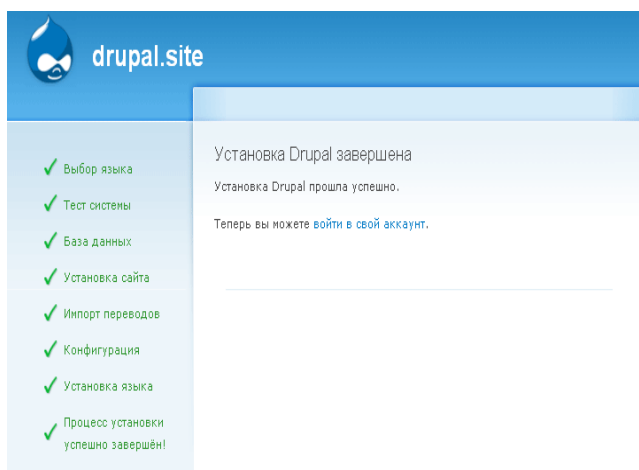
Kelesi bette tan'lang'an til qaytadan tekseriledi.



Programmani' ornati'wdi'n` aqi'rg`i' beti, Drupal akkauntqa procedura juwmaqlang`anli'g`i' xaqqi'nda xabar beredi ha`m «войти в свой аккаунт» ssi'lkasi' basi'ladi'.



Paydalani'wshi'g`a Drupal dan qanday paydalani'w kerekligi haqqi'nda ko`rsetpeler beriledi. Kelesi bette paydalani'wshi' o`zine kerekli bo`limdi



tan`laydi', ma`selen programmani'n` qosi'msha abzalli'qlari'nan paydalani'w, ornati'wg`a qosi'mshalar kiritiw, programmani' sazlaw ha'm basqa. Bettin` qaptal ta`repindegi tu`ymeden paydalani'p jan`a hu`jjet jarati'w, jarati'lg`an hu`jjetti basqari'w, jarati'lg`an hu`jjetten shi'g`i'w si'yaqli' processler a`melge asi'ri'ladi'. Paydalani'wshi' jumi'sti' baslamastan da`slep usi' bette keltirilgen barli'q mag`li'wmatlardi' di'qqat penen oqi'p shi'g`i'wdi' usi'nadi'.



VI-BAP MILLIY ELEKTRON HU`JJET ALMASI'W SISTEMASI'.

4.1 E-XAT qorg`algan elektron pochta

E-XAT qorg`alg`an elektron pochta sistemasi' E-XAT sistemasi' paydalani'wshi'lar ortasi'nda elektron xabarlar menen qorg`alg`an almasi'wdi' sho'lkemlestiriw ushi'n arnalg`an. Qorg`alg`an elektron pochta sistemasi' mag`li'wmatti' kriptografikali'q qorg`aw tarawi'ndag`i' ma'mleketlik standartlari' tiykari'ndag`i' mag`li'wmatti' kriptografikali'q qorg`aw qurallari' h m elektron cifrli' imza qurallari' (milliy kriptovayder)dan paydalani'ladi'.

Qorg`aw qurallari'nan paydalani'w esabi'nan E-XAT sistemasi' mag`li'wmat q wipsizligi maselesinde to`mendegi talaplarg`a juwap beredi:

- identifikaciya qi'li'w – E-XAT sistemasi' paydalani'wshi'si' elektron cifrli' imzag`a tiykarlani'p oni'n` haqi'yqi'yli'g`i' ornati'ladi';
- konfidencialli'g`i' – elektron xabarlardi' shifrlaw joli' menen olardi' qorg`aw qi'li'w;
- har bir elektron xabarda elektron cifrli' imzani'n` tekseriw tiykari'nda elektron xabar jiberiwshini autentifikaciya qi'li'w;
- elektron xabarlardi'n` pu`tinligi – elektron xabardag`i' mag`li'wmatti'n` buzi'lmag`anli'g`i'n tekseriw.

E-XAT sistemasi'nda izlew ushi'n u`sh tilden paydalani'ladi': o`zbek (lati'n h m kirill jazi'wlari' tiykari'nda), rus (kirill jazi'wi' tiykari'ndag`i') h m inglis (lotin jazi'wi' tiykari'ndag`i') tiller.

E-XAT sistemasi'da islew ushi'n ha`r bir paydalani'wshi' elektron cifrli' imza giltlerin dizimge ali'w orayi'n t repinen berilgen jabi'q h m ashi'q klyuch sertifikati'na iye boli'wi' kerek.

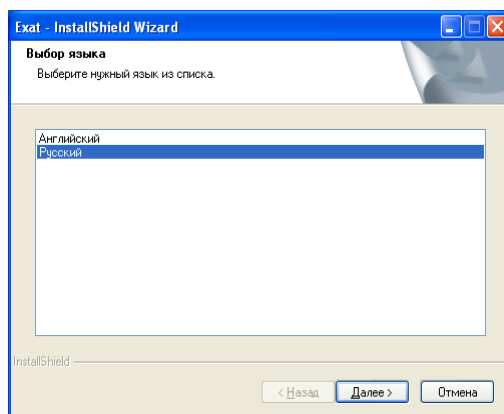
EXAT qorg`alg`an elektron pochta (bunnan keyin – EXAT KEP) diziminen o`keriw ha`m onnan paydalani'w ta`rtibi to`mendegishe.

Dizimge ali'w paydalani'wshi'ni'n` arzasi' tiykari'nda ERI giltlerin dizimge ali'w orayi' ta`repinen tayarlanadi', aldi'n ali'ng`an elektron cifrlı' imza (ERI) gilti ha`m ECI ashi'q giltinin` sertifikati' tiykari'nda o`tkeriledi.

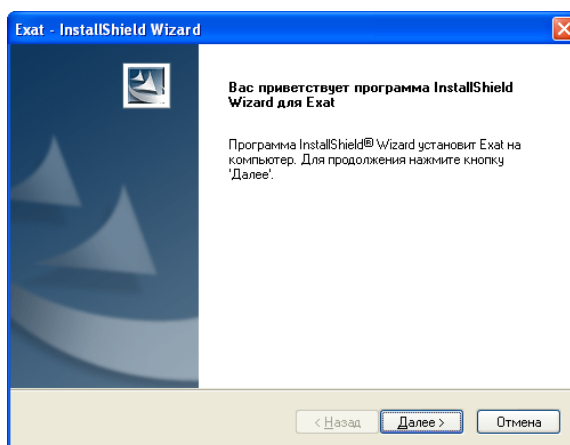
4.2 Programmani' installyaciya qi'li'w

Jumi'sti' baslaw ushi'n klient EXAT KEP programmali'q ta`miynati'n ornati'w za`ru`r. Programmani' komp'yuterde iske tu`siriw programmani'n` ornati'latug'i'n fayl u`stine basi'w (mishka menen eki ret basi'w) menen a`melge asi'ri'ladi'.

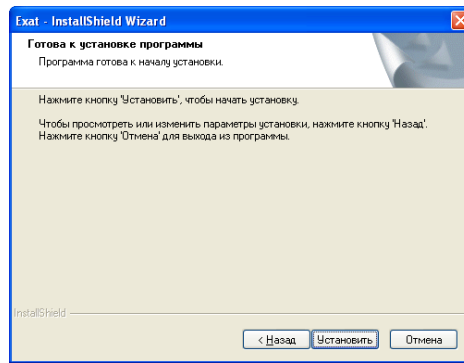
Payda bolg`an aynada paydalani'wshi' isleytug'i'n til tan`lanadi' (rus tili yaki inglis tili).



«Bunnan keyin» («Далее») tuymesı basi'lg`anda programmani' ornati'w ushi'n ayna payda boladi'.



Onan keyin «Licenziya kelisiwi» («Лицензионное соглашение») payda boladi', «Licenziya kelisiwi» «Лицензионного соглашение» sha`rtleri qabi'l qi'li'ng`annan son` to`mendegi ayna payda boladi'.

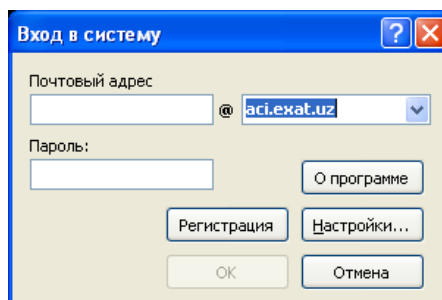


Ornati'w «Установить» tuymesi basi'lg`ani'nda dastur C:\Program Files\Incoft-Service Ltd\Exat da ornati'ladi'.

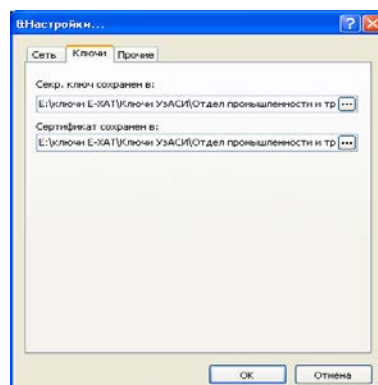
Programmani' iske tu`siriw – Incoft-Service Ltd – Exat - Exat Secured Mail Programmasi'ni'n` Puski arqali' a`melge asi'ri'ladi'.

Programmani' sazlaw

Programmani' iske tu`siriwden aldi'n **Dizimge kiriw («Вход в систему»)** aynasi' ashi'ladi', og`an sazlawdi'n` kerek bolatug`i'n mag`li'wmatlari' kiritiliwi kerek boladi'.

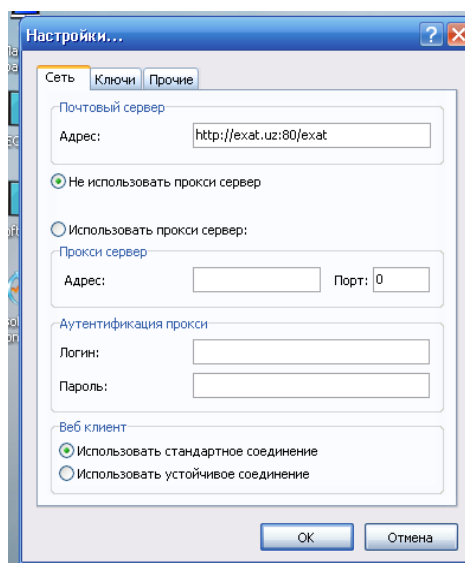


Programmani' sazlaw **Dizimge kiriw («Вход в систему»)** aynasi'ndag`i' **Sazlaw («Настройка»)** tu`ymesin basi'w a`melge asi'ri'ladi'. **Giltler («Ключи»)** vkladkasi'nda paydalani'wshi'ni'n` ECI jabi'q gilti ha`m ashi'q giltinin` sertifikati' saqlanatug`i'n ori'n ko`rsetiledi.



Si'qli' giltke jol («Путь к секретному ключу») maydani'nda jabi'q gilt saqlanatug'i'n orni'n ko'rsetiledi, **Sertifikatka jol** («Путь к сертификату») maydani'nda bolsa ashi'q gilt sertifikati' saqlanatug'i'n orni'n ko'rsetiledi. Jabi'q gilt ha'm sertifikati' jumi's orni'ni'n` komp'yuterinde yaki sheship ali'wshi' tasi'wshi'da saqlani'wi' mu'mkin.

EXAT serverinen paydalani'wdi'n` tarmaq sazlawlari'n ornati'w ushi'n «**Adres**» maydani'ndag'i' **Tarmaq** («Сеть») vkladkasi'nda <http://exat.uz:80/exat/> pochta serverinin` adresi ko'rsetiliwi kerek.



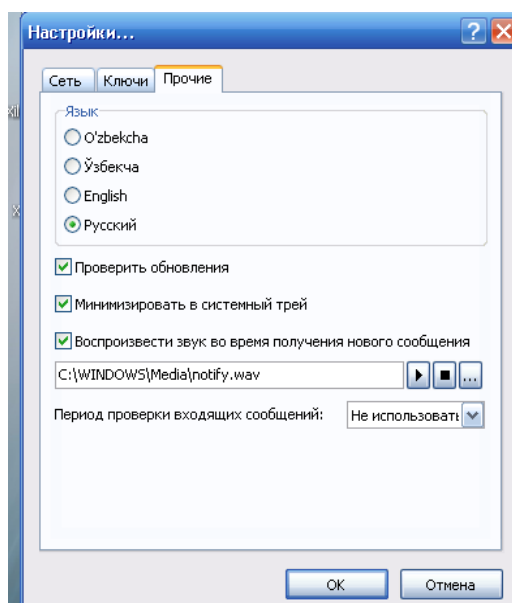
Eger komp'yuterdin` Internet tarmag'i'na kiriwi proksi-server arqali' a'melge asi'ri'lsa, sazlawda «**Internet Explorer sazlawlari'nan paydalani'w**» («Использовать настройки Internet Explorer») (Internet Explorer de ko'rsetilgen sazlawlardan paydalani'ladi') ko'rsetiliwi kerek yaki **Proksi-serverden paydalani'w** («Использовать прокси-сервер») ko'rsetiledi ha'm to'mendegi maydanlarda proksi-server adresin ha'm porti'n, paydalani'w login ha'm paroli ko'rsetiledi.

Eger EXAT KEP serverine kiriwde qa'te payda bolsa, onda sazlawlarda server adresinin`, jabi'q gilt ha'm sertifikati'na joldi'n` tuwri' ko'rsetilgenligi, soni'nday, proksi-server arqali' kiriw sazlang'anli'g'i'ni'n` tuwri'li'g'i' tekseriliwi kerek.

Basqalar («Прочие») vkladkasi'nda paydalani'wshi' programmani'n` qosi'msha opsiyalari'n sazlawi' mu'mkin: **Til** («Язык»), **jan'alani'wlardi'**

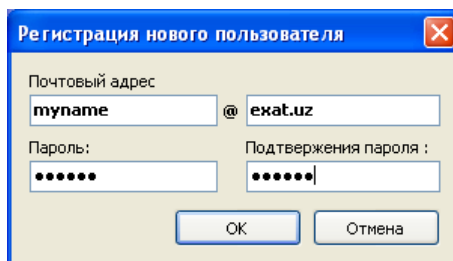
tekseriw («Проверка обновлений»), jana xabardi' ali'wda dawi'sti' qayta esittiriw («Воспроизведение звука при получении нового сообщения»), kiriwshi xabarlaridi' tekseriw da'wiri («Период проверки входящих сообщений») ha'm usi'g'an uqsag'anlar.

3.7 EXAT KEP sistemasi' 4 tilge tiyisli interfeys (o'zbekshe-kirill, o'zbekshe-lati'n, russha -inglisshe)ti saqlaydi'



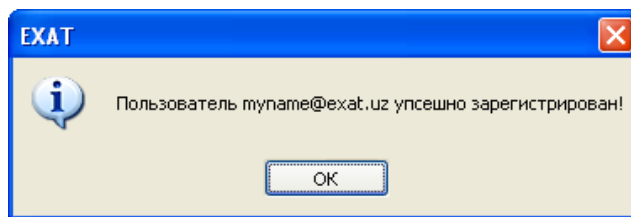
Paydalani'ushi'ni' dizimge ali'w

Jumi'sti' baslawdan aldi'n paydalani'wshi' EXAT KEP sistemasi'nda dizimnen o'tiwi kerek. Buni'n` ushi'n **Dizimge kiriw** («Вход в систему») aynasi'nda **Dizimge ali'w** («Регистрация») tu`ymesin basi'w kerek. Jan`a paydalani'wshi'ni' dizimge ali'w («Регистрация нового пользователя») aynasi'nda kerek maydanlar tolti'ri'ladi'.

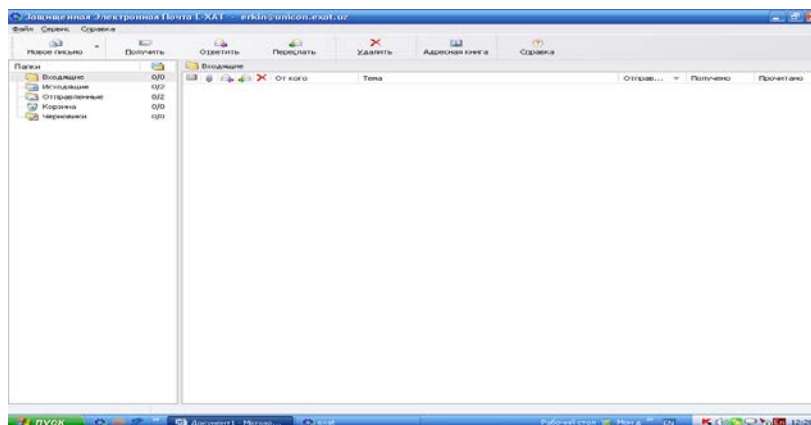


«OK» tu`ymesini basi'lg`anda paydalani'wshi' EXAT KEP sistemasi'nda dizimge ali'ng`an boladi'. Eger dizimge ali'w a`melge aspasa, pochta serverinin`

adresini, giti ha'm sertifikatini saqlaw jolida, shunday pochta adresidagi atini tuwri ko'rsatilganligini ko'zdan o'tkeriw kerek.



Sistemadan na'tiyjeli dizimnen o'tkennan son paydalani'wshi' sistemaga kiriwi mumkin. Buni'n ushi'n paydalani'wshi' **Sistemaga kiriw («Вход в систему»)** aynasinda o'zini'n logini, pochta adresi ha'm parolin ko'rsetiwi ha'm **«OK» tu'ymesin basi'w kerek**, onnan keyin to'mendegi ayna payda boladi'.

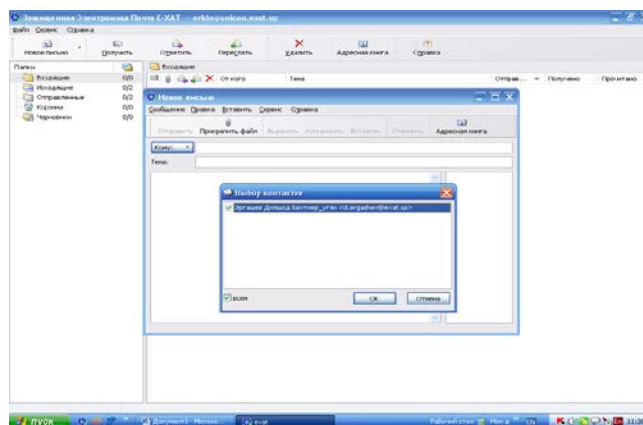


Ushu interfeys EXAT KEP penen islegende paydalani'wshi'ni'n jumi's orni' boli'p esaplanadi'. **«Servis» tu'ymesin basi'lg'anda** interfeystin joqari maydani'ndagi paydalani'wshi'ni'n sol waqittagi sazlavlari'n o'zgertiwi mumkin.

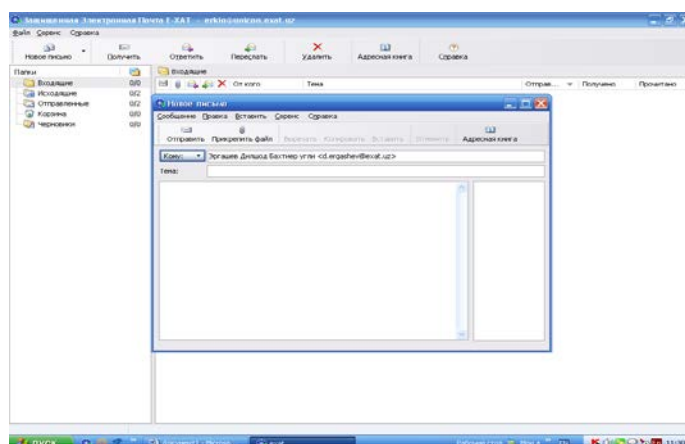
EXAT sistemasi'nda islew

5.1 Pochta mag'li'wmatti'n jiberiw ushi'n **«Fayl» - «Jan'a xat» («Fayl» - «Новое письмо»)**di tan'law, yaki **Jan'a xat («Новое письмо»g'a basi'w kerek**. **«Taza xat» («Новое письмо»)** aynasi' payda boladi'.

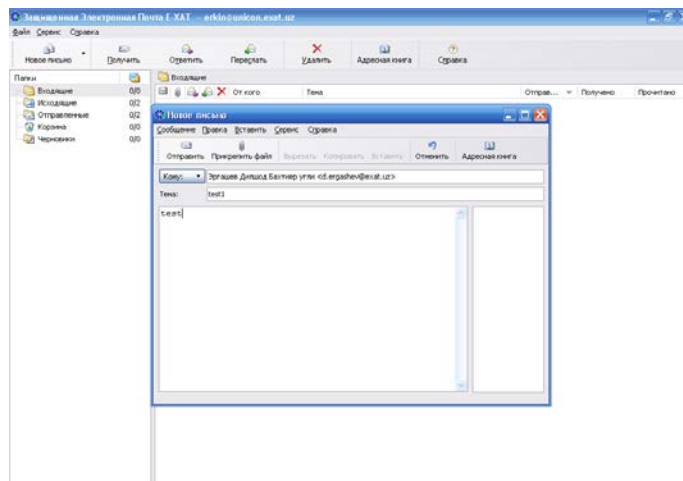
«Taza xat» («Новое письмо») aynasinda **Kimge («Кому»)** tu'ymesin basi'p, ushi' mag'li'wmatti' qabi'l etip ali'wshi'ni tan'law kerek. Keyin **Kontaktlardi' tan'law («Би'бор контактов»)** aynasinda kerek kontakti' yaki ba'rshe paydalani'ushi'lardi' tan'law (tiyisli maydang'a belgi qoyi'p) kerek.



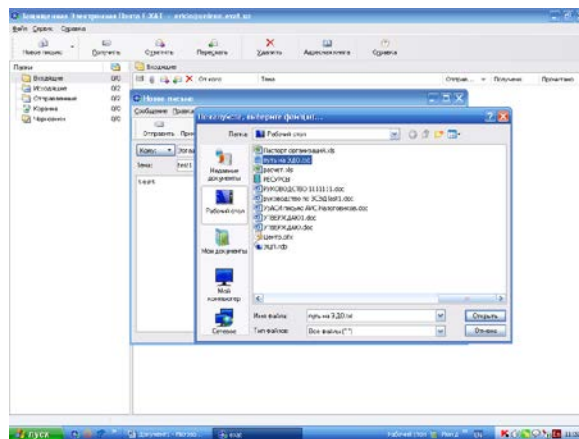
Mag`li`wmatti` qabi`l etip ali`wshi` tiyisli maydanda payda boladi`.



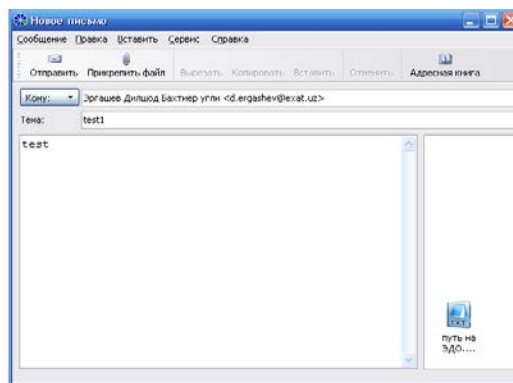
«Taza xabar» («**Новое сообщение**»)di` payda etiwde sonday, «Тема» («**Тема**») maydani`n tolti`ri`w ha`m tiyisli maydang`a xabar tekstin kiritiw kerek.



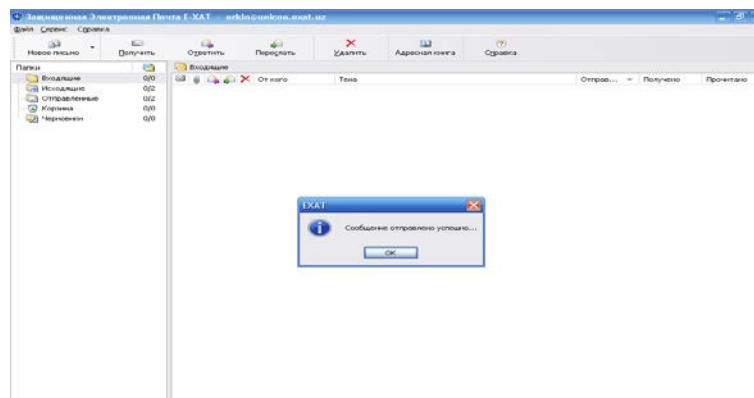
Kerek bolg`anda **Fayldi` biriktiriw** («**Прикрепить файл**») tu`ymesine basi`p xabarg`a ka`legen fomattag`i` fayldi` jaylasti`ri`w mu`mkin.



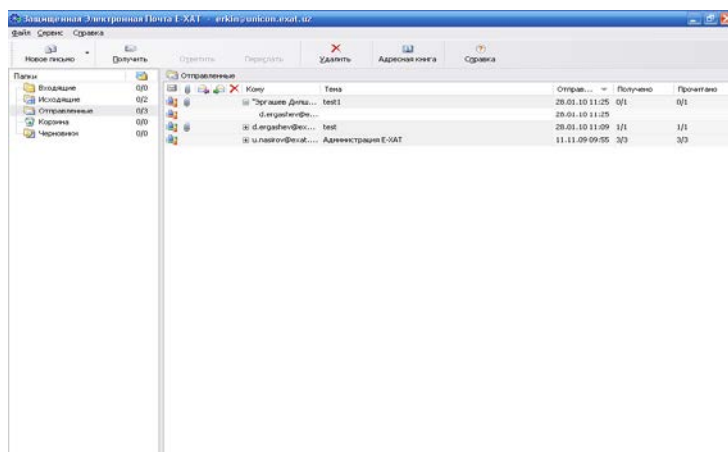
Fayl sali'ng'an mag'li'wmat to'mendegi ko'rinishe iye boladi'.



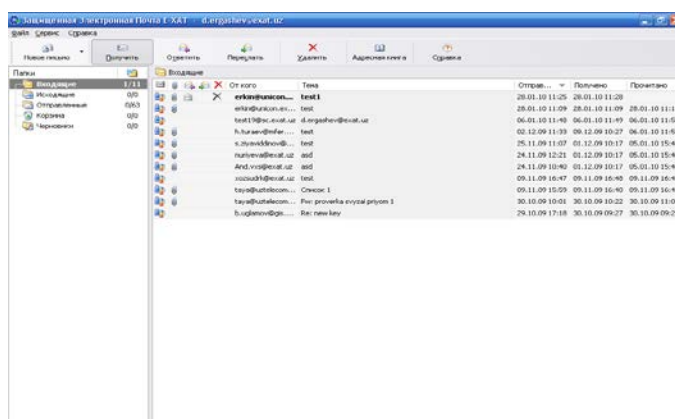
Jiberiw («Отправить») tu'ymesin basi'wda xabar na'tiyjeli jiberilgenligi xaqqi'nda bildiriw payda boladi'.



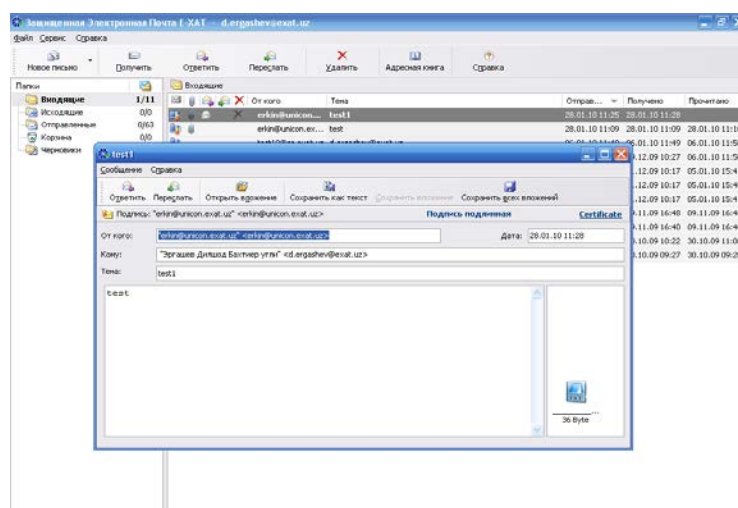
Jiberilgen mag'li'wmat Jiberilgenler («Отправленные») papkasi'nda saqlanadi'.



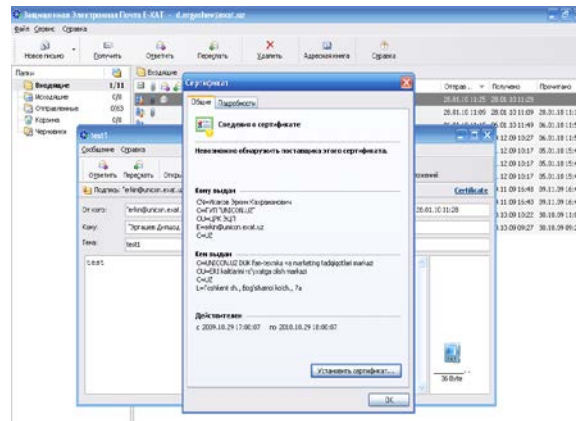
Kiriwshi xabarlardi' qabi'l qi'li'p ali'w ushi'n Ali'w («Получить») tu`ymesin basi'w yaki sazlawda kiriwshi xabarlardi' tekseriw periodli'li'g'i' ornati'li'wi' kerek.



Kiriwshi xabardi' ashi'w ushi'n og'an basami'z, bunda to'mendegi ayna ashi'ladi':

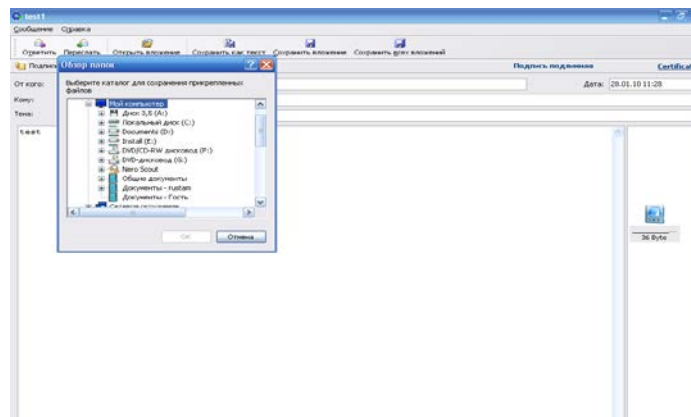


«Certificate» usi'ni'si'n basi'p, jiberiwshinin` sertifikati'n ko`rip shi'g'i'w mu`mkin.

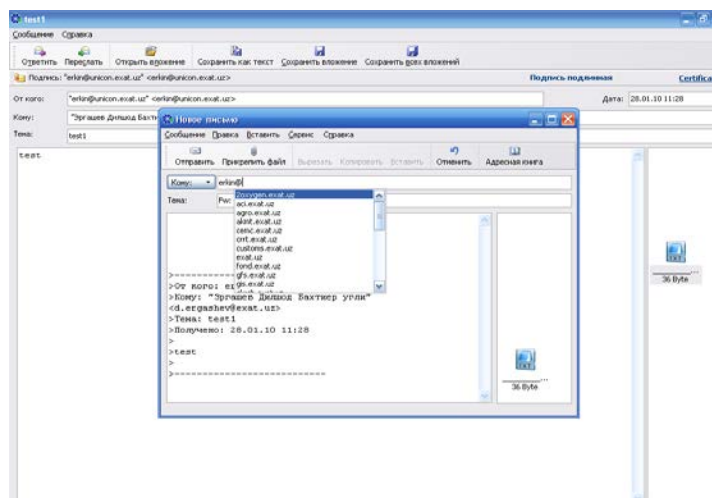


Xatka joylasqan fayldi' saqlaw ushi'n Jaylasqan zatti' saqlaw («Сохранить вложение») basi'li'wi' kerek.

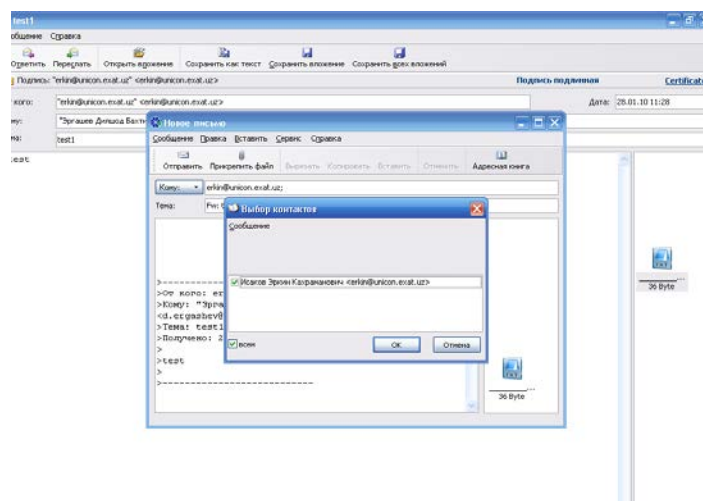
Biz fayldi' saqlamaqshi' bolg'an papkani' tanlaw usi'ni's etiledi.



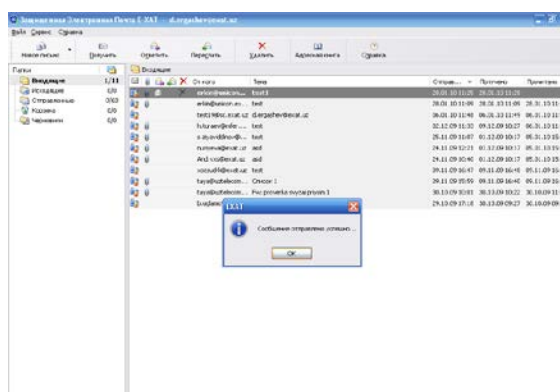
Xabardi' «Qayta jiberiw» («Переслать») tu`ymesin basi'p, sistemani'n` basqa paydalani'wshi'si'na qayta jiberiw mu`mkin. @ tu`yimesi basi'lg`ani'nan keyin ma`nzildi kiritiwde, sistema dizimindegi domendi tanlawdi' usi'ni's etedi.



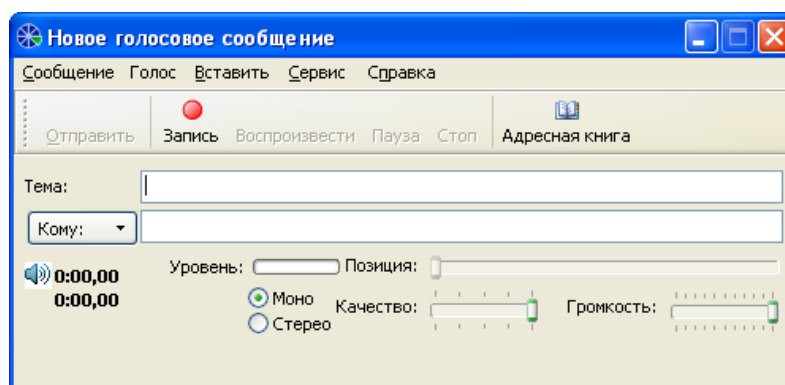
Sunday «Kinge» («**Кому**») tu`ymesin yaki «Ma`nzil kitabi» («**Адресная книга**») tu`ymesin basi'p, dizimdegı ali'wshi'ni' tan'law mu'mkin:

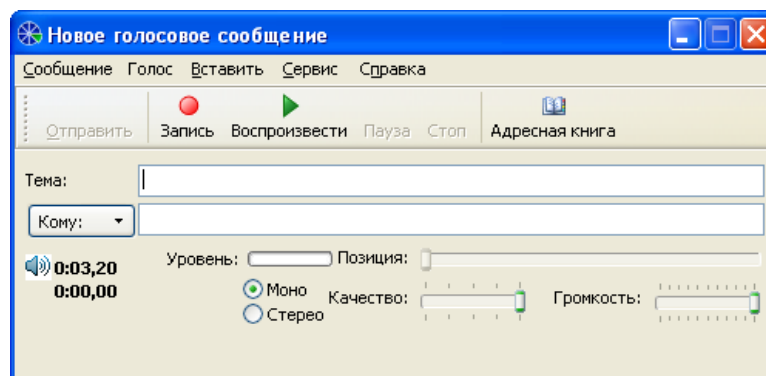


Xabar na'tiyjeli jiberilgenligin, ekranda to'mendegi ayna shi'g'ari'ladi':



«Ctrl-w» klavishalari'n birgelikte basi'p, jiberiwshi dawı'sli' jazi'lg'an (mikrofonnan paydalang'an halda) yaki dawı'sli' fayldı' salı'w quralı'nda dawı'sli' xabardı' payda etiwı mu'mkin.





«Qayta esittiriw» («**Воспроизвести**») tu`ymesin basi`p, jiberiletug`i`n yaki kiriwshi dawı'sli' xabardi' yaki qoyi'lg`an dawı'sli' fayldi' esitip ko`riw mu`mkin.

Dawı'sli' xabar aynasi`ndag`i' menyu ha`m tu`ymelerdin` wazi`ypasi' to`mendegishe:

«Jazi`w» («**Запись**») - mikrofon ja`rdeminde dawı'sli' xabardi' jazi`u;

«Qayta esittiriw» («**Воспроизвести**») - jazi'lg`an dawı'sli' xabardi' yaki qoyi'lg`an dawı'sli' fayldi' qayta esittiriw;

«Dawı's» («**Голос**») – dawı'sli' xabar menen islew (jazi`w, qayta esittiriw, pawza, toqtati`w);

«Qoyi`w» («**Вставить**») - dawı'sli' fayi`ldi' koyi`w.

EXAT KEP interfeystin` menyu ha`m papkalari`ni`n` wazi`ypasi' to`mendegishe:

«Fayl» menyusi:

«Taza xat» («**Новое письмо**»)– taza pochta xabari`n jarati`w;

«Taza dawı'sli' xabar» («**Новое голосовое сообщение**») – taza dawı'sli' xabardi' payda etiw;

«Qosi`w» («**Добавить**») – taza kiriwshi xabarlardi`n` kelip tu`siwin tekseriu;

«Ali`p taslaw» («**Удалить**») – ajrati'lg`an xabarlardi' ali`p taslaw;

«Juwap beriw» («**Ответить**») – kiriwshi xabarg`a juwap xabari`n payda etiw.

«Qayta jiberiw» («**Переслать**») – kiriwshi xabardi' taza adresatqa qayta jiberiw;

«Shi`g`i`w» («**Выход**») – EXAT KEP programmadan shi`g`i`w.

«Сервис» menyusi;

«Til» («Язык») – interfeys tilin tan`law;

«Ma`nzil kitabi» («Адресная книга») – paydalani`wshi`lar kontaktlerinin` dizimin shi`g`i`ri`w;

«Paydalani`wshi` parolin o`zgertiw» («Изменить пароль пользователя») – EXAT KEPdan paydalani`w ushi`n paydalani`wshi`ni`n` usi` parolin almasti`ri`w;

«Sazlaw» («Настройка») – paydalani`wshi`ni`n` usi` sazlawlari`n o`zgertiw.

«Mag`li`wmatnama» («Справка») – programma xaqqi`ndag`i` mag`li`wmatlardi` shaqi`ri`w;

«Programma xaqqi`nda» («О программе») – programma islep shi`g`ari`wshi` ha`m versiyalari` xaqqi`ndag`i` xabar.

«Kiriwshi» («Входящие») papkasi` – kiriwshi xabarlardi` saqlaw;

«Shi`g`i`wshi`» («Исходящие») papkasi` – shi`g`i`wshi` xabarlardi` saqlaw (jiberiw waqti`na shekem);

«Jiberilgen» («Отправление») – jiberilgen xabarlardi` saklaw;

«Корзина» – ali`p taslang`an xatlardi` arali`q saqlaw;

«Черновики» – jarati`lg`an, biraq jiberilmegen xabarlardi` saqlaw.

Jiberilip ati`rg`anda ha`r bir pochta xabari` ECI menen imzalanadi` ha`m paydalani`wshi` giltinen paydalangan halda shifrlanadi`.

Ba`rshe kiriwshi xabarlar E-XAT klient programmasi`nda shifrlang`an ko`riniste saqlanadi`. Xabarlardi` rasshifrovka qi`li`w olar ashi`lg`anda a`melge asi`ri`ladi`.

4.3 E-HUJJAT sistemani'n`qollani'li'wi'.

E-Hujjet sistemasi', sonday Ministrler Ken`esi t`repiinen 1999-j`i'ldi'n` 29-marti'nda 140-sanli' qarari' menen tasti'yi'qlang`an normativ hujjetlerge muwapi'q is ju`ritiliwi h`em hujjetler ori'nlani'wi'n qadag`alaw talaplari'na juwap beredi.

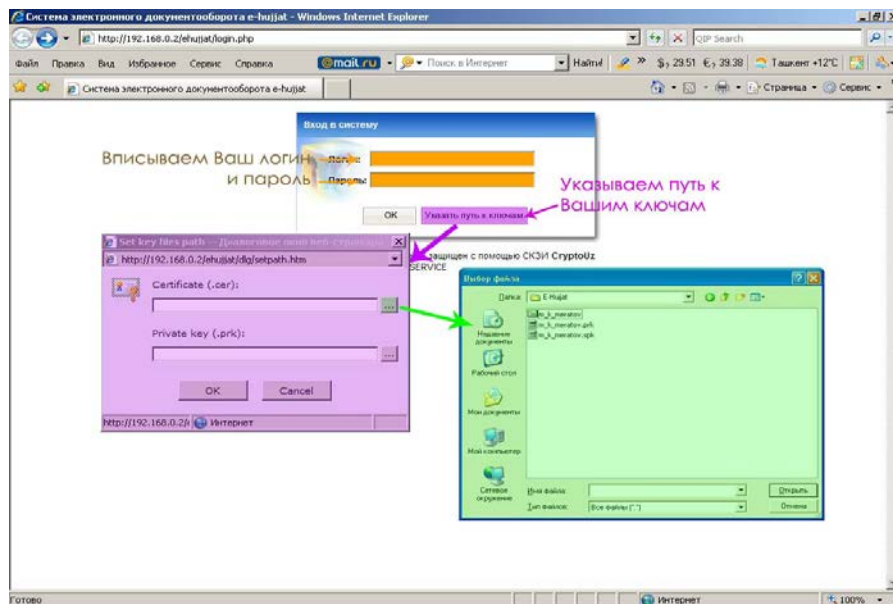
E-Hujjet elektron hu`jjet aylani'w sistemasi'ni'n` tiykarg`i' funkciyalari' boli'p to`mendegiler esaplanadi':

- elektron hu`jjetin` jarati'li'wi';
- elektron hu`jjet ushi'n wazi'ypalardi' payda etiw;
- hu`jjetti dizimge ali'w h`em qadag`alawshi'lar imzasi'n qoyi'w;
- elektron hu`jjetlerdin` ori'nlani'wi';
- elektron hu`jjetlerdi kelisiw h`em imzalaw;
- elektron hu`jjetler ori'nlani'wi'n oraylasti'ri'lg`an h`em oraylasti'ri'lmag`an ko`riniste qadag`alaw.

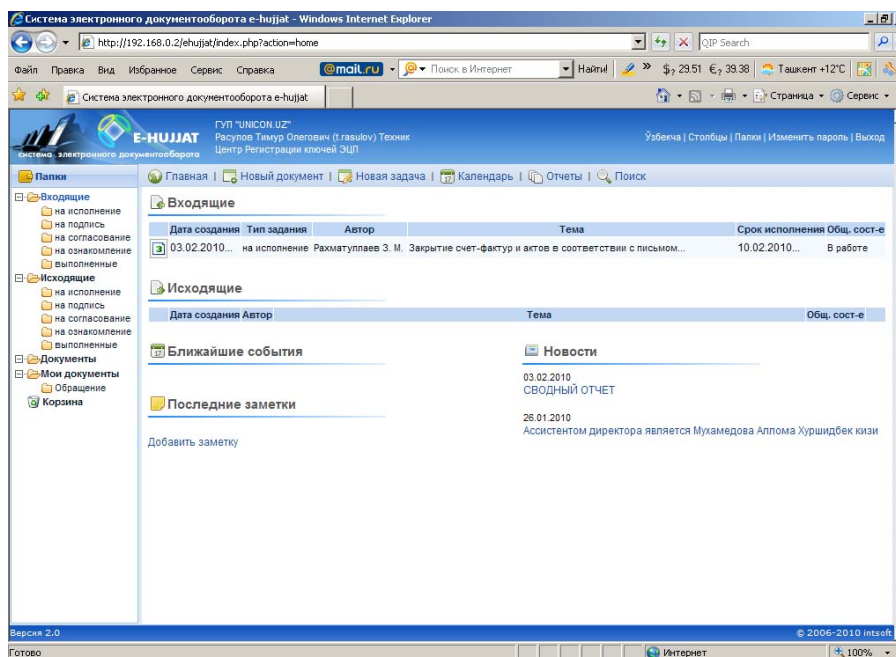
Sistema to`mendegi imkaniyatlardi' jarati'p beredi:

- arxiv is ju`ritiliwine baylani'sli' hu`jjetlerdin` elektron arxivin ju`ritiw;
- elektron hu`jjetlerdi saqlaw h`em izlew;
- ijra intizami' boyi'nsha esabatlardi' sa`wlelendiriw h.t.b.
- Mag`li'wmat almasi'wda n`otiyjeli sistemani' jarati'w;
- qag`azsi'z elektron hu`jjet aylani'wi'na basqi'shpa-basqi'sh o`tiw;
- elektron hu`jjetlerdin` saqlani'wi' h`em n`otiyjeli izlewdi t`emiynlew

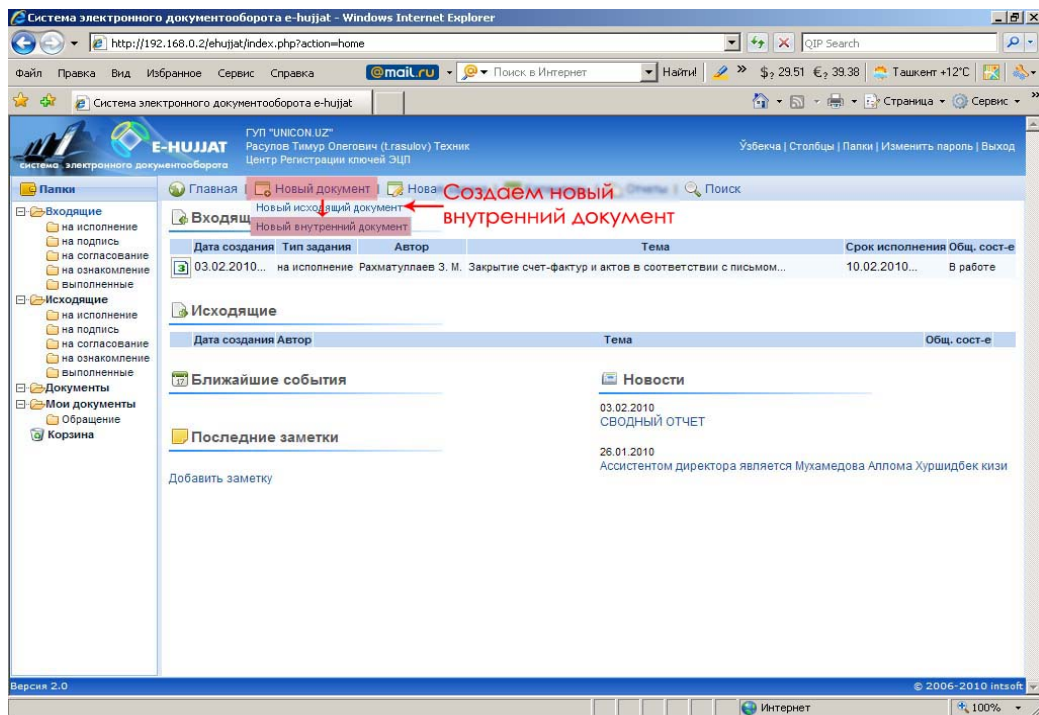
Jeke paydalani'wshi' jumi'si'ni'n` sho`lkemletiriw izbe izligi to`mendegishe



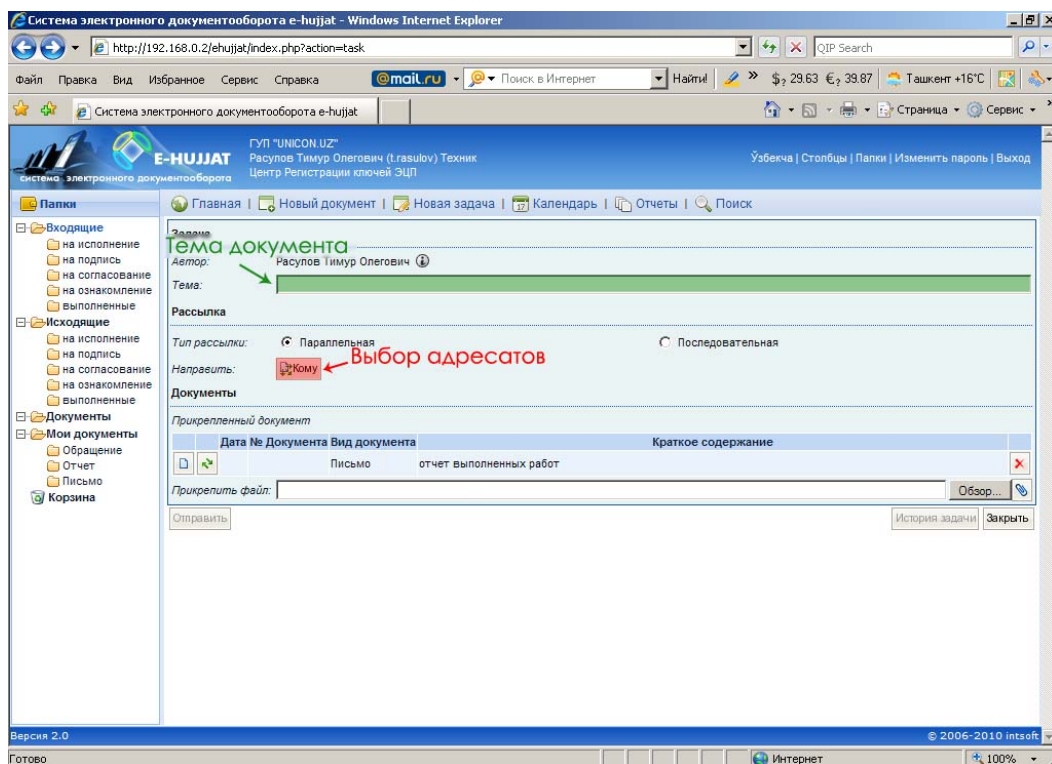
Sistemag`a kiriw



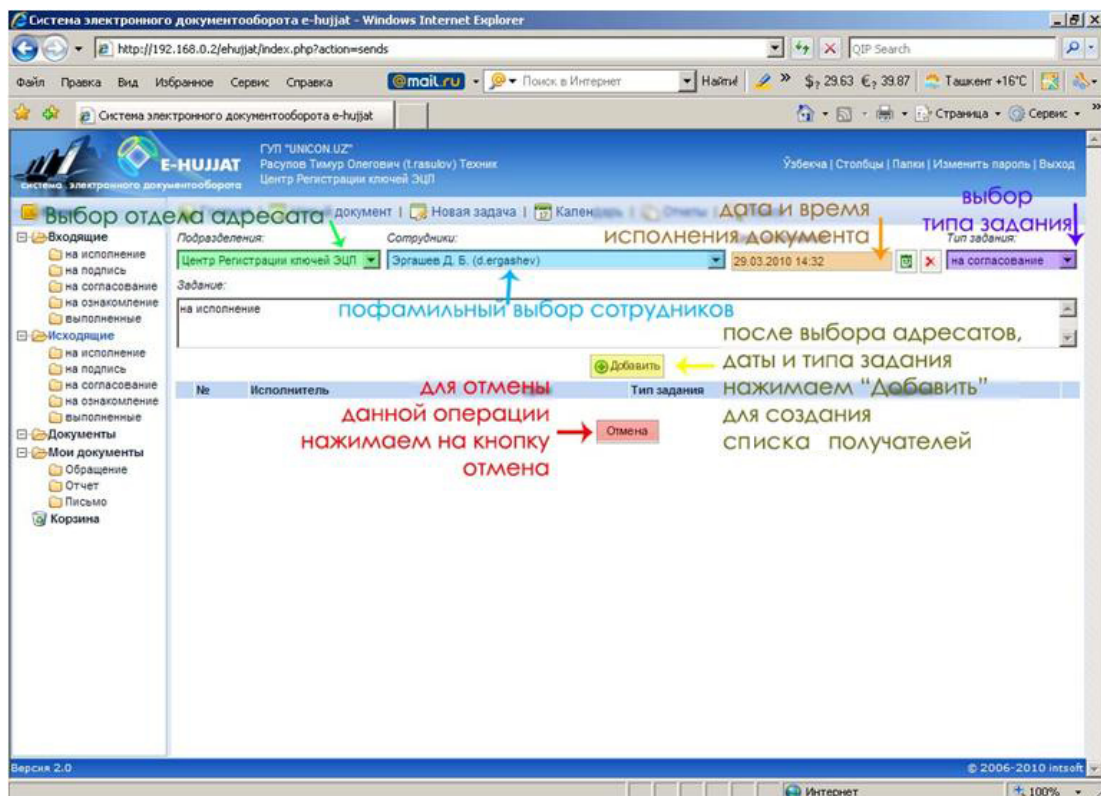
Bas bet



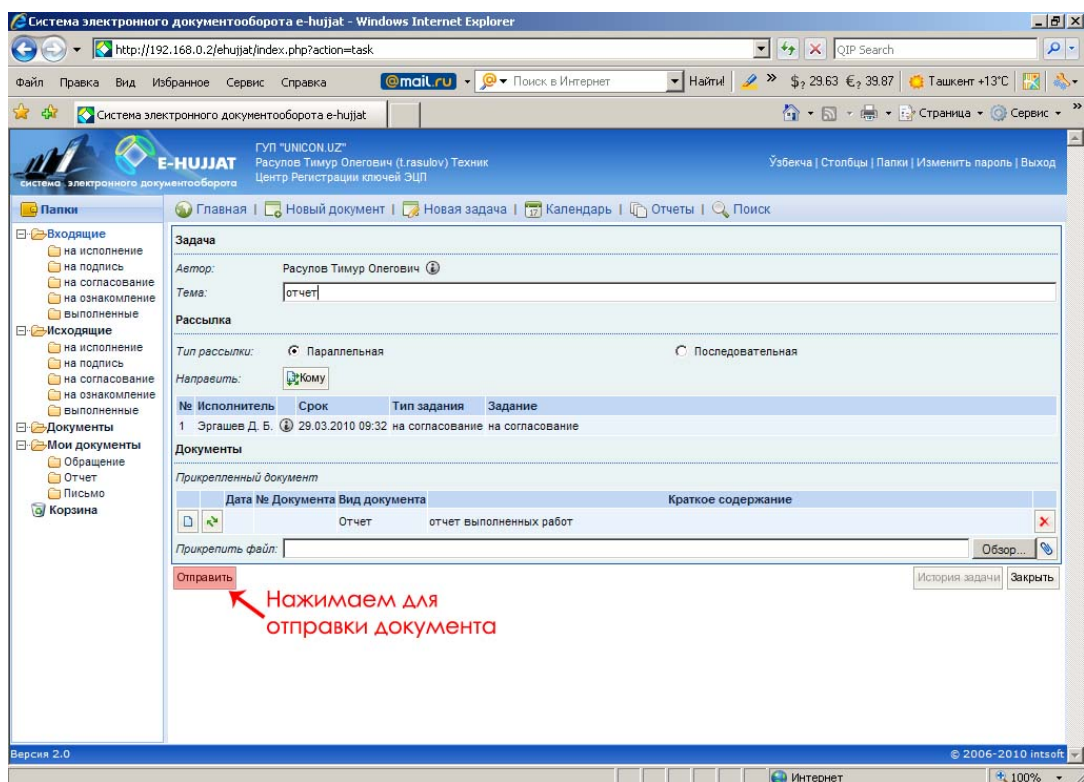
Taza hu`jjet jarati`w



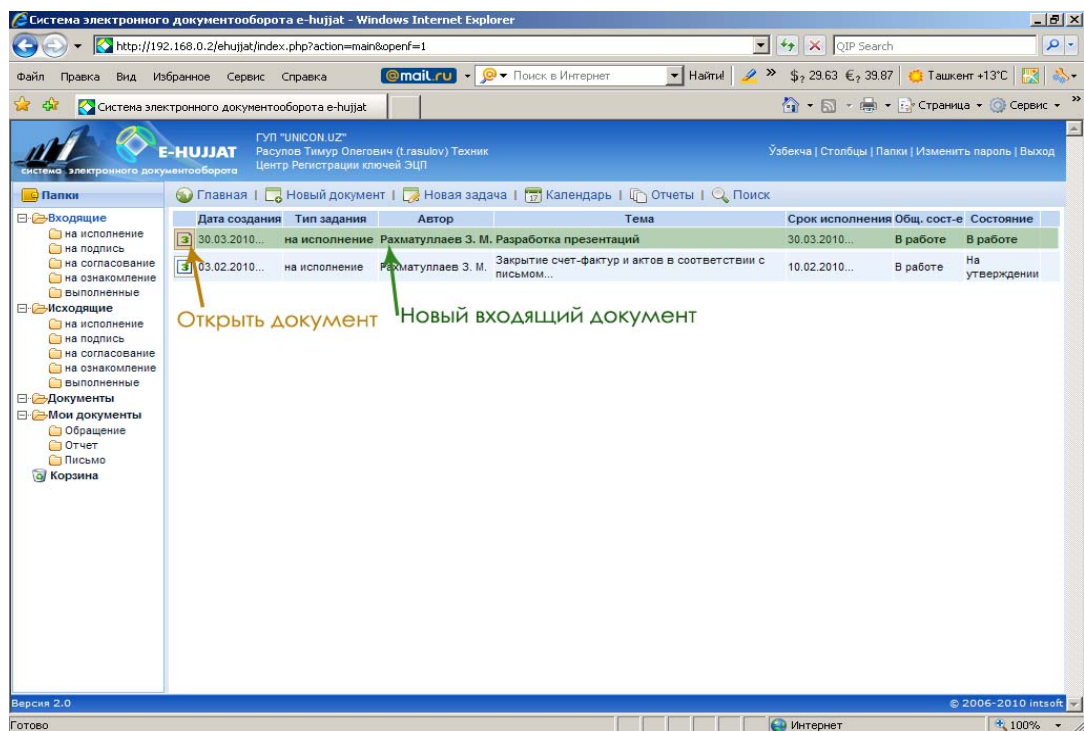
Hu`jjet ushi`n wazi`ypa jarati`w



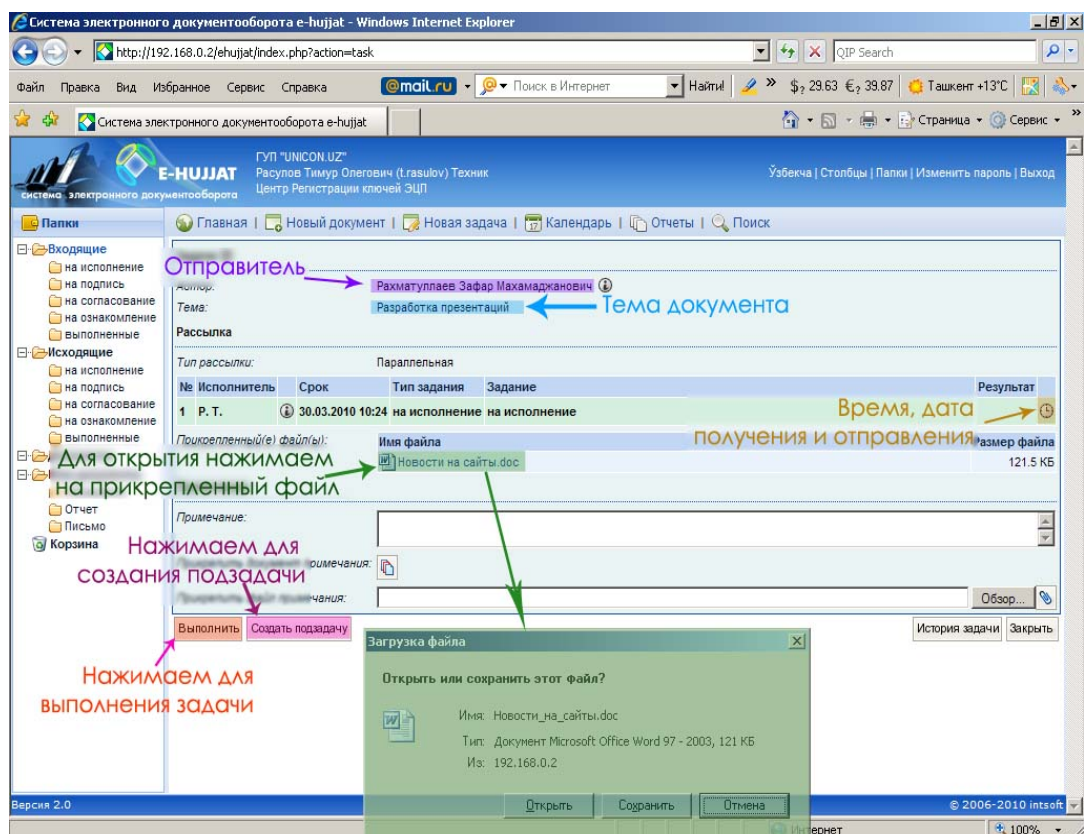
Adresatlardi' tan'law



Xu jjet ushi'n tayar wazi'upa



Kiriwshi hu`jjetti dizimge ali'w



JUWMAQLAW.

Elektron hu`jjet aylani'si'n paydalani'wda to`mendegishe imkaniyatlar jaratadi'.

- identifikaciya qi'li'w cifrli' imzag`a tiykarlani'p oni'n` haqi'yqi'yli'g'i' ornatladi';

- konfidencialli'g'i' – elektron xabarlardi' shifrlaw joli' menen wolar qorg`aladi';

- har bir elektron xabarda elektron cifrli' imzani'n` tekseriw tiykari'nda elektron xabar jiberiwshi autentifikaciya qi'li'nadi';

- elektron xabarlardi'n` pu`tinligi – elektron xabardag`i' mag`li'wmatti'n` buzi'lmag`anli'g'i' tekseriledi.

- sistemada izlew ushi'n kerekli tillerden paydalani'ladi'.

PAYDALANI'LG'AN A'DEBIYATLAR:

1. “Elektron hujjat aylanishi to'g'risida”gi O'zbekiston Respublikasi Qonuni. 11.12.2003 y.
2. “Elektron tsifrlı imza to'g'risida”gi O'zbekiston Respublikasi Qonuni. 29.04.2003y.
3. Akbarov D.e. Informatsiya xavfsizligini ta'minlashning kriptografik usullari ham ularning qo'llanishlari. Toshkent. "O'zbekiston markasi ", 2009. – 432 b.
4. O'z DSt 1092:2009 «Informatsiya texnologiyasi. Informatsiyaning kriptografik muhofazasi. Elektron tsifrlı imzani shakllantirish ham tekshirish protsesslari».
5. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ – Москҳам: ТРИУМФ, 2002.
6. Xasanov X.P. Takomillashgan diamatritsalar algebralari ham parametrlı algebra asosida kriptosistemalar yaratish usullari ham algoritmlari. – Toshkent, 2008. 208 b.
7. Смирнова Г. Н. Электронные системы управления документооборотом
8. Майкл Дж. Д. Саттон. Корпоративный документооборот. Принципы, технологии, методология внедрения.
9. Независимый портал о СЭД - www.doc-online.ru
- 10.Официальный сайт разработчика СЭД iTs-Office - www.its.dn.ua
- 11.Алеев В. А. Оптимизация работы с документами: опыт создания электронного архива в компании // Современные технологии делопроизводства и документооборота. № 0. 2010. С. 51 = 54.
- 12.Андреев В. Создание системы автоматизации документооборота. Часть 5. Что превращает приложения корпоративной СЭД в единую систему // [Информационный ресурс]. Режим доступа: <http://www.pcweek.ru/ecm/article/detail.php?ID=135396>

13. Артизов А. Н. Передача государственных полномочий в сфере архивного дела. // Отечественные архивы. 2008. № 6. С. 23 - 28.
14. Артизов А. Н. Об организации доступа пользователей к документам Архивного фонда Российской Федерации в федеральных государственных архивах. // Вестник архивиста. 2009. № 3. С. 3 - 8.
15. Арутюнов Ю. С., Бобылева М. П. Проблемы совершенствования технологии управления. // М.: Институт повышения квалификации информационных работников. 1991.
16. Балакин М. М. Разработка механизмов корпоративного управления строительным холдингом на основе имитационного моделирования // Автореф. дисс.... Канд. экон. наук. Москва. 2008.
17. Баласанян В. Э. Применение автоматизированных систем документационного обеспечения управления (АС ДОУ) для повышения эффективности управления // Делопроизводство. 2002. № 2. С. 5.