**AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ**
**AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ**

**«MAGİSTRATURA MƏRKƏZİ»**

**Hüseynova Təhminə Ramiz qızı**

# MÖVZU: «AZƏRBAYCANDA İQTİSADİ FƏALİYYƏTİN ELEKTRONLAŞDIRILMASINDA TƏHLÜKƏSİZLİK SİSTEMLƏRİNİN ROLU»

## *MAGİSTR DİSSERTASİYASI*

| | | |
|---|---|---|
| **İstiqamətin şifri və adı:** | İİM 020000 | Mühəndis iqtisadiyyatı və idarəetmə |
| **İxtisasın şifri və adı:** | İİM 020006 | İqtisadi fəaliyyətin riyazi və informasiya təminatı |

**Elmi rəhbər**
dos.Quliyeva A.A.

**Magistr proqramının rəhbəri**
prof. Quliyev R.A.

**KAFEDRA MÜDİRİ:** **akad.ABBASOV Ə.M.**

BAKI - 2015

# MÜNDƏRİCAT

**PLAN**

**REFERAT**……..... 3-5

**GİRİŞ**……..... 6-7

**FƏSİL 1. Ölkədə iqtisadi fəaliyyətin idarəedilməsində informasiya texnologiyalarının rolu**..... 8-31

**1.1. Ölkənin müxtəlif sahələrində informasiya texnologiyalarının tətbiq durumu**..... 8-20

**1.2. Ölkədə informasiya cəmiyyətinin genişləndirilməsi istiqamətləri**..... 21-31

**FƏSİL 2. İqtisadiyyatın elektronlaşdırılmasına təsir edən amillər**..... 32-63

**2.1. İqtisadiyyatın elektronlaşdırılmasında təhlükəsizlik problemi**.... 32-48

**2.2.İqtisadiyyatın elektron idarəedilməsində təhlükəsizlik məsələləri və rəqəmsal sertifikatlar**..... 49-63

**FƏSİL 3. Ölkədə iqtisadiyyatın elektronlaşdırılmasının təkmilləşdirmə istiqamətləri**..... 64-85

**3.1. İqtisadiyyatın elektronlaşdırılmasında SET və SSL protokollarının rolu**..... 64-77

**3.2. Elektron ödəmə sistemlərinin təkmilləşdirmə istiqamətləri**..... 78-85

**NƏTİCƏ VƏ TƏKLİFLƏR**……..... 86-89

**ƏDƏBİYYAT SİYAHISI**……..... 90

# REFERAT

**Mövzunun aktuallığı:** Müasir dövrdə iqtisadi fəaliyyətin informasiyalaşması və kompüterləşməsi ilə əlaqədar olaraq elektron ödəmələrdə informasiya təhlükəsizliyi məsələsinin əhəmiyyəti xeyli dərəcədə artmışdır. Hələ 30 il bundan əvvəl informasiya hücumlarının obyekti iqtisadi sahədə fəaliyyət göstərən obyektlər ilə əlaqədar olan informasiya olmuşdur. Belə hücümlar çox nadir hallarda baş verirdi, onların sifarişçilərinin əhatə dairəsi çox dar idi və vurduğu ziyan isə yalnız xüsusi hallarda çox ciddi fəsadlar törədə bilərdi. Bizim dövrdə isə elektron ödəmələr, plastik kartlar, kompüter şəbəkələrindən istifadənin geniş yayılması ilə əlaqədar olaraq informasiya hücumlarının obyekti bilavasitə həm iqtisadiyyatın müştərilərinin pul vəsaitləri olmuşdur. Oğurluq və ya qarət cəhdini hər kəs edə bilər – bunun üçün internet şəbəkəsinə qoşulmuş kompüterin mövcudluğu kifayətdir.

Məhz bu problem müasir dövrdə ən aktual olan və ən az tədqiq olunandır. İnformasiya təhlükəsizliyinin klassik və fiziki təminatına yönəldilmiş davamlı yanaşmaların artıq çoxdan işlənib hazırlandığı halda, texnologiyalarda tez-tez radikal dəyişikliklərin baş verməsi ilə əlaqədar olaraq banklarda informasiya emalının avtomatlaşdırımış sistemlərinin (BİEAS) təhlükəsizliyi metodları fasiləsiz olaraq yenilənməlidir. Təcrübə göstərir ki, səhvləri olmayan mürəkkəb kompüter sistemləri mövcud deyil.

Hesablama texnikası vasitələrinin və ilk növbədə fərdi elektron hesablama maşınlarının əlverişliliyi əhalinin geniş təbəqəsində kompüter savadlılığının yayılmasına gətirib çıxartmışdır. Bu da öz növbəsində hökümət, kommersiya və xüsusilə bank sistemlərində bir sıra məqsədli və ya sadəcə olaraq maraq naminə müdaxilələrin meydana gəlməsinə səbəb olmuşdur. Bu cəhdlərdən çoxu uğurlu olmuş və informasiya və hesablama sistemləri sahiblərinə ciddi ziyan vurmuşdur.

Qeyd etmək lazımdır ki, tamamilə mühafizə edilmiş sistemlər mövcud deyil. Tamamilə etibarlı sistem barəsində birincisi, yalnız, müəyyən ehtimallar, ikincisi, müəyyən kateqoriya cinayətkarlardan mühafizə olunmuş təqdirdə danışmaq olar. Bununla belə, kompüter sisteminə müdaxiləni qabaqcadan nəzərə almaq mümkündür. Mühafizə - bir növ müdafiə və hücum arasında yarışdır: kim daha çox biliklərə malikdirsə və daha çox aktiv tədbirlər görürsə - o bu yarışmada qalib olur.

**Tədqiqatın məqsədi:** Tədqiqatın əsas məqsədi iqtisadiyyatın elektronlaşdırılması məsələsi xüsusiyyətlərini tədqiq etmək, iqtisadiyyatın elektronlaşdırılması əsaslarını araşdırmaq və elektronlaşdırmada təhlükəsizlik sistemlərinin roluna təsir edən amillərinin öyrənilməsindən ibarətdir.

**Tədqiqatın predmeti:** Tədqiqatın predmeti kimi iqtisadiyyatın elektronlaşdırılması, elektronlaşdırlma məsələsində təhlükəsizlik sistemlərinin rolu və onların tətbiqinin tədqiqi çıxış edir.

**Tədqiqatın nəzəri əsaslarını** iqtisadiyyatın elektronlaşdırılması sahəsində elmi klassiklərinin, müasir Qərb iqtisadçılarının əsərləri ilə yanaşı rus və Azərbaycan iqtisadçı alimlərinin tədqiqatları, həmçinin tədqiqatçının fərdi yanaşması təşkil edir. Dissertasiyanın yazılmasında iqtisadiyyatın elektronlaşdırılması, təhlükəsizlik məsələləri, təhlükəsizlik sistemləri və təhlükəsizlik sistemlərinin fəaliyyətinin təkmilləşdirmə məsələləri və digər elmlərin müddəalarından geniş istifadə edilmişdir.

**Tədqiqatın metodoloji bazasını** informasiya iqtisadiyyatı, elektron iqtisadiyyat və təhlükəsizlik sistemlərin ilə əlaqədar elmlərin əsaslandığı elmi tədqiqat metodlarının geniş spektri və problemin tədqiqində elmi abstraksiya, tarixi və məntiqi əlaqə, induksiya, deduksiya, analiz və sintez metodlarından istifadə edilməklə faktlar yığılıb-ümumiləşdirilmiş, onlar arasında qanunauyğun və təsadüfi əlaqələr müəyyənləşdirilmiş xarakterik əlamətlər aşkara çıxarılmış, həmçinin müasir inkişaf xüsusiyyətlərini və təmayüllərini izah edən bir çox xarici ölkə alimlərinin elmi mülahizərələri və nəticələri təşkil edir.

**Elmi yenilik:** Magistr dissertasiyasının elmi yeniliyi iqtisadi fəaliyyətin elektronlaşdırılması, təhlükəsizlik sistemlərinin fəaliyyət mexanizmi və onların təkmilləşdirilməsi istiqamətlərinin müəyyənləşdirilməsi barəsində təklif və tövsiyələrin hazırlanmasından ibarətdir.

**Nəzəri və təcrübi əhəmiyyəti** aparılan tədqiqatın əsas nəticə və elmi müddəalarından təkliflər və tövsiyələrdən, iqtisadiyyatın elektronlaşdırılması, elektron iqtisadiyyat, elektron kommersiya, təhlükəsizlik sistemləri və onların təkmilləşdirmə məsələlərinin həllinin həyata keçirilməsidir.

**İnformasiya mənbəyi** müxtəlif beynəlxalq təşkilatların dövrü nəşrləri, Azərbaycan Respublikası Rabitə və İnformasiya Texnologiyaları Nazirliyinin, Azərbaycan Respublikası Dövlət Statistika Komitəsinin, Mərkəzi Bankın, İqtisadiyyat və Sənaye Nazirliyininin məlumatlarından ibarətdir.

**İşin strukturu və həcmi.** Aparılmış tədqiqat işi giriş, üç fəsil, nəticə və təkliflərdən ibarətdir. Girişdə işin aktuallığı, tədqiqatın istiqamətləri göstərilir və tədqiq ediləcək problemlər müəyyənləşdirilir.

Magistr dissertasiya işinin birinci fəslində ölkənin müxtəlif sahələrində informasiya texnologiyalarının tətbiq durumu və ölkədə informasiya cəmiyyətinin genişləndirilməsi istiqamətləri geniş şəkildə araşdırılmışdır.

Magistr dissertasiya işinin ikinci fəslində iqtisadiyyatın elektronlaşdırılmasında təhlükəsizlik problemi və iqtisadiyyatın elektron idarəedilməsində təhlükəsizlik məsələləri və rəqəmsal sertifikatlar öyrənilmişdir.

Magisr dissertasiya işinin üçüncü fəslində isə iqtisadiyyatın elektronlaşdırılmasında SET və SSL protokollarının rolu və elektron ödəmə sistemlərinin təkmilləşdirilməsi istiqamətləri təhlil edilmişdir.

Işin sonunda isə məntiqi yekunu olaraq nəticə və təkliflər və ədəbiyyat siyahısı verilmişdir.

# GİRİŞ

Biz informasiya axınlarının günü – gündən yüksək templə artdığı bir cəmiyyətdə yaşayırıq. Bu informasiya axınlarının öhdəsindən insanlar yalnız informasiya texnologiyalarından istifadə etməklə gələ bilirlər. Son zamanlar informasiya texnologiyalarının sürətli inkişafı göstərir ki, hesablama texnikası elmi – tədqiqat işlərinin aparılmasında, iqtisadi fəaliyyətin təşkilində, idarəetmə proseslərində və insan fəaliyyətinin digər sahələrində tətbiqi qərarların qəbul edilməsi məsələlərinin həlli zamanı asan, daha tez və düzgün nəticələrin əldə olunmasında çox böyük rol oynaya bilər.

Bir çox ölkələr üçün informasiya texnologiyaları XXI əsrin informasiya dünyasında insanları həyata və işə hazırlamaq üçün yeganə şansdır. Bununla əlaqədar müasir həyatda kompüter texnikasının tətbiqi əvəzolunmazdır. Sahələrin böyük əksəriyyəti məsələlərin həllini sürətləndirmək üçün hesablama maşınlarından istifadə edirlər. Son vaxtlara qədər bütün kompüter texnikası insan üçün ancaq köməkçi bir vasitə olmuşdur. Kompüter müxtəlif hesablamaları aparırdı, qalan işlər isə insanın öhdəsinə düşürdü.

İnformasiya cəmiyyətinin, ənənəvi sənayenin və xidmət sahələrinin hökm sürdüyü cəmiyyətdən fərqi ondadır ki, informasiya, biliklər, informasiya xidmətləri və onların istehsalı ilə əlaqədar olan bütün sahələr (telekommunikasiya, kompüter və televiziya) çox böyük sürətlə inkişaf edirlər, yeni iş yerləri mənbəyidirlər, iqtisadi inkişafda mühüm yer tuturlar. İnformasiyalı cəmiyyətə keçid dövründə ən böyük təhlükə insanların informasiyaya malik, İTT (İnformasiya Telekommunikasiya Texnologiyaları) ilə davrana bilən və bu xüsusiyyətlərə malik olmayan təbəqələrə bölünməsindən ibarətdir.

Hal-hazırda dünyanın əksər ölkələrində bütün sahələrdə olduğu kimi, iqtisadiyyatda da informasiya və kommunikasiya texnologiyalarının tətbiqi iqtisadiyyatın səmərəliliyinin artmasında və məhsuldarlığının yüksəlməsində böyük rol oynayır. Iqtisadiyyatın elektronlaşdırılması ölkələrin əksəriyyətinin

əhəmiyyət vürdiyi məsələdir. Bu sahənin formalaşması və təkmilləşdirilməsi məqsədilə lazımi qanunverici baza formalaşdırılmış və müvafiq tədbirlər həyata keçirilmişdir. Lakin iqtisadiyyatın elektronlaşdırılmasında təhlükəsizlik məsələlərinin həlli bu sahənin inkişafına təkan verən ən əsas məsələdir. Bu səbəbdən də təqdim edilən magistr dissertasiya işinin mövzusu öz aktuallığı ilə seçilir.

# FƏSİL 1. Ölkədə iqtisadi fəaliyyətin idarəedilməsində informasiya texnologiyalarının rolu

## 1.1. Ölkənin müxtəlif sahələrində informasiya texnologiyalarının tətbiq durumu

Qloballaşmaya qərar vermiş müasir dünyamızda inkişaf etmiş dövlətlərdə kompüter sisteminin müasir informasiya və təhlil texnologiyalarından bütün fəaliyyət sahələrində geniş istifadə olunur.

İnformasiya texnologiyaları əsri kimi qədəm qoyduğumuz XXI əsrdə iqtisadi inkişafın əsasını elmi-texniki tərəqqi təşkil edir. Belə ki, müasir informasiya texnologiyalarından istifadə etməklə mürəkkəb dinamik prosesləri təhlil edərək, gələcəkdə hansısa qeyri-standart vəziyyətlərin yaranacağı ehtimalını əvvəlcədən görməyə, müəyyən qabaqlayıcı tədbirlərin həyata keçirilməsinə imkan yaranır.

Dünya təcrübəsinin təhlili göstərir ki, informasiya texnologiyalarının inkişafı, tətbiqi və istifadəsi iqtisadi artım, əmək məhsuldarlığı və əhali məşğulluğunun artırılması üçün geniş potensial imkanlar yaradır. Bu da təkcə informasiya texnologiyaları sahəsinin deyil, iqtisadiyyatın digər sahələrinin də, o cümlədən sənaye sahələrinin də səmərəliliyini artırır.

Biliyə əsaslanan (intellektual) iqtisadiyyat keçən əsrin ikinci yarısında meydana gəlib, sürətlə inkişafa başlayaraq, istehsalın səviyyəsinin artması, iqtisadi səmərəlilik və maddi rifahın yaxşılaşması kimi iqtisadi faydalar gətirmişdir. Son illərdə inkişaf etmiş bazar iqtisadiyyatlı ölkələrdə maddi rifahın yaxşılaşması məhz intellektual iqtisadiyyatın artmasının nəticəsidir.

Keyfiyyət baxımından biliyə əsaslanan iqtisadiyyat, ümumiyyətlə, ictimaiyyətin həyat və fəaliyyət tərzinə vacib və əsaslı dəyişikliklər gətirmişdir. Bu, ictimai və iqtisadi agentlərin bilik və informasiyanı hansı yol və vasitə ilə əldə etməsində, yaradılmasında, paylanmasında və istifadə olunmasında, istehsalın,

əməyin, texnoloji proseslərin və ticarətin təşkil edilməsində, bir-birilə əlaqə saxlamasında, siyasi proseslərdə iştirakında və s. dəyişikliklərdə özünü göstərir.

Sərmayələrin azlığı ilə informasiya və kommunikasiya texnologiyaları (İKT) sahəsinin yüksək dərəcədə inhisarlaşması və əhalinin get-gedə artan yoxsulluğu bəzi ölkələrdə intellektual iqtisadiyyatın özülünü qoymaqda çətinliklər yaradıb. Ən inkişaf etmiş ölkələrin təcrübəsi göstərir ki, intellektual iqtisadiyyatın genişlənməsi üçün bəzi şərtlərin nəzərə alınması vacibdir:

- informasiya və kommunikasiya texnologiyaları, informasiya infrastrukturu və İKT xidmət təminatının mövcud olması və əlverişliliyi;
- bilik və informasiyanın əldə edilməsi, yaradılması və səmərəli istifadəsi üçün davranışlı əsasnamənin olması;
- cəmiyyəti bilik və informasiyanın istifadəsinə həvəsləndirməkdə, bilik və informasiyanın səmərəli istifadəsini təmin etməkdə və əhali üçün əlverişli etməkdə dövlətin fəal rolu;
- elmi bacarıq və tutumların mövcud olması, onların məqsədyönlü və səmərəli istifadəsi;
- təhsil və sahibkarlığa meyl göstərən əhali.

Birləşmiş Millətlər Təşkilatının Avropa İqtisadi Komissiyası keçid dövründə olan ölkələrdə intellektual iqtisadiyyatın yaradılması və üzə çıxarılmasında fəal rol oynayır.

İqtisadiyyatın informasiya texnologiyaları tətbiq edilən bölməsi informasiya texnologiyalarının istehsalı, yayılması və tətbiqi ilə bağlı iqtisadi fəaliyyət növlərinin məcmusu kimi müəyyən olunur. Bu və ya digər sahənin təsnifləşməsinin müəyyən olunması verilən bölmənin xarakterik xüsusiyyətləri ilə bağlı bir sıra çətinliklərlə qarşılaşır. Əvvəla, iqtisadiyyatın informasiya texnologiyaları tətbiq edilən bölməsi, iqtisadiyyatın bir sahəsi deyil, informasiya texnologiyaları ilə bu və ya digər şəkildə bağlı olan mal və xidmətlər müxtəlif fəaliyyət növləri ilə məşğul olan müəssisələr tərəfindən istehsal olunur. İkincisi, maddi və qeyri-maddi komponentləri özündə əks etdirən informasiya texnologiyalarının kompleksliyini nəzərə alsaq, bu bölmə həm müəyyən malların

istehsalını, həm də qarşılıqlı araşdırılan müvafiq xidmətləri əhatə edir. Üçüncüsü, iqtisadiyyatın informasiya texnologiyaları tətbiq edilən bölməsi olduqca intensiv şəkildə inkişaf edir, ənənəvi statistik təsnifatlarda nəzərə alınmayan yeni məhsul və xidmətlər isə köhnəlir. Ona görə də informasiya texnologiyaları sahəsində məhsul və xidmətlərin qruplaşdırılması daim yeniləşməlidir.

İqtisadiyyatın informasiya texnologiyaları tətbiq edilən bölməsinə aid edilən iqtisadi fəaliyyət nəticəsində yaranmış mal və xidmətlər informasiya texnologiyaları ilə bağlı mal və xidmətlərdir.

Müasir elm və innovasiya statistikasının informasiya texnologiyaları statistikası ilə metodoloji uyğunluğunu təmin etməklə, onun əsasında duran prinsiplərə əsaslanmaq məqsədəuyğundur.

Hazırda kompüterdən istifadə olunması qismən insanın iştirakı olmadan informasiyanı avtomatik qurğularda işləməyə şərait yaratmışdır. Bu qurğular kifayət qədər uzun müddət işləməklə bərabər öz sürəti ilə insanı milyon dəfələrlə qabaqlayır.

EHM-in tətbiqi xalq təsərrüfatının bir çox sahələrində, o cümlədən sənaye sahələrində istehsal texnologiyasının kökündən dəyişdirilməsinə, əmək məhsuldarlığının artırılmasına, insanların əmək şəraitlərinin yaxşılaşdırılmasına səbəb olur.

EHM-in köməyi ilə müxtəlif maşınqayırma, aviasiya, avtomobil, detal və konstruksiyalarının qrafikinin qurulması və hesablamalar avtomatlaşdırılmış layihələndirmə sisteminin (ALS) tərkib hissələridir. Belə sistemlər konstruktorun əmək məhsuldarlığını qat-qat artırır və iş vaxtına qənaət edir, EHM-ə qoşulmuş ekran qarşısında oturmaqla avtomobilin ayrı-ayrı hissə və birləşmələrini təsvir etməyi EHM-ə əmr edə bilər. Bu isə avtomobilin xarici görünüşünü və yığcamlığını qiymətləndirməyə imkan verir. EHM-in köməyi ilə birləşmələrin iş modelini yaratmaq və istismar zamanı onların ən çox haradan sınması ehtimalını müəyyən etmək olar.

Detalı müvəffəqiyyətlə layihələndirdikdən sonra onu hazırlamaq da lazımdır. Dəzgahlarda detalların hazırlanması prosesini də EHM-in köməyi ilə

avtomatlaşdırmaq olar. EHM-in köməyi ilə idarə edilən dəzgahları ədədi proqramla idarə edilən dəzgahlar adlandırırlar (ƏPİ). Detalı ƏPİ dəzgahlarında emal etmək üçün əvvəlcə bu dəzgahlarda əməliyyatların yerinə yetirilməsi ardıcıllığını əks etdirən proqram tərtib olunmalıdır. Hazırlanmış belə proqram yazılıb EHM-in yaddaşına daxil edildikdən sonra ƏPİ dəzgahı detalı avtomatik, insanın iştirakı olmadan emal edə bilər. Eyni bir proqramla müəyyən seriyalı detaldan istənilən qədər emal etmək olar. Başqa bir detal hazırlamaq üçün ancaq dəzgahı idarə edən EHM-in yaddaşındakı proqramı dəyişmək lazımdır.

Kompüterlərə mexaniki və yorucu işləri həvalə etməklə biz insanı yaradıcı fəaliyyət üçün azad edirik. EHM-in lazımi məsələləri həll etməsi üçün insanlar öz biliklərini müntəzəm olaraq dəqiq informasiyalar, ciddi qaydalar, səhvsiz alqoritmlər və səmərəli proqramlar şəklində kompüterlərə ötürməlidirlər.

Mərkəzləşdirilmiş iqtisadiyyat dövründə əgər müəssisə göstəriciləri, ümumiyyətlə, statistik göstəricilər yalnız planlaşdırmaya xidmət edirdisə, bazar iqtisadiyyatı şəraitində əldə edilmiş göstəricilərin yeni informasiya texnologiyaları vasitəsilə operativ və keyfiyyətli təhlili artıq intensiv inkişaf yoluna qədəm qoymuş gənc, müstəqil dövlətin daha da möhkəmlənməsi, yeni nailiyyətlər əldə etməsi üçün optimal qərarların qəbul edilməsində, iqitsadi siyasətin istiqamətləndirilməsində mühüm rol oynayır. Çünki bazar iqtisadiyyatı şəraitində göstəricilər keçmiş haqqında fundamental məlumat mənbəyi kimi cəmiyyətin vacib informasiya infrastrukturuna çevrilərək istifadəçilərin informasiyaya olan tələbatının ödənilməsi, görülmüş işləri, qazanılmış nəticələri və gələcək prosesləri təhlil etmək və proqnozlaşdırmaq üçün ilkin verilənlər toplusu kimi qəbul edilir.

Müasir dövrdə sosial və texniki infrastrukturun mürəkkəbləşdirilmə şəraitində informasiya resursları ən mühüm strateji bir resursa çevrildi. Müasir informasiya texnologiyaları, kompüterizasiya yeni əsrin atributları oldu və ən əsası informasiya texnologiyaları ictimaiyyət fəaliyyətinin hər bir sahəsinin daha da effektiv işləməsinə şərait yaratdı. İndi bütün dövlətlər həm inkişaf etmiş, həm də inkişaf etməkdə olan dövlətlər bu sahədə çox fəal iş aparır bu sahənin inkişaf

etməsinə hər cür şərait yaradırlar, sahənin inkişafı naminə dövlət strategiyaları hazırlanır və həyata keçirilir.

İnformasiya texnologiyaları sırasında ən qabaqcıl yeri dünya İnternet informasiya şəbəkə sistemi tutur. İnternet istifadəçilərinin sayına görə birinci yeri Çin tutur. Qeyd edək ki, son dövrlərə qədər bu sahədə birinci yer Amerika Birləşmiş Ştatlarına məxsus idi. Azərbaycanda da internet çox yüksək templə yayılır və istifadəçilərin sayı gündən-günə artır. Hal-hazırda internet sahəsi Azərbaycanda ən yüksək templə inkişaf etməkdə olan rabitə və informasiya sahələrindən biridir.

Dünya təcrübəsi göstərir ki, informasiya və kommunikasiya texnologiyalarından geniş istifadə olunması ölkənin hərtərəfli inkişafına xidmət edir və məhz bu texnologiyalar əhalinin sosial-iqtisadi vəziyyətində mövcud olan problemlərin həll olunması və yoxsulluğun azaldılması üçün tutarlı vasitələrdəndir.

Son illərdə Azərbaycanda informasiya və kommunikasiya texnologiyalarından istifadə sahəsində müəyyən addımlar atılmış, bir sıra sahələrdə bu texnologiyaların tətbiqində ciddi uğurlar qazanılmış və ümumiyyətlə, bu istiqamət dövlət siyasətinin prioritetlərindən birinə çevrilmişdir.

Azərbaycanın informasiya və kommunikasiya texnologiyalarının tətbiqinə istək və marağını, həmçinin bu istəyin reallığa çevrilmə imkanlarını aşağıdakılar əyani nümayiş etdirir:

- Azərbaycan hökuməti informasiya cəmiyyətinin formalaşdırılması prosesini sürətləndirməyə qərarlıdır, digər tərəfdən BMTİP və başqa beynəlxalq təşkilatlar bu sahədə ölkəyə texniki və maliyyə dəstəyi göstərməyə hazırdırlar;
- İnformasiya cəmiyyətinin hüquqi normativ bazasının yaradılması sahəsində Azərbaycan dövlətinin artıq müəyyən müsbət təcrübəsi vardır;
- Respublikanın ali və orta ixtisas məktəblərinə tələbə qəbulu prosesində yeni texnologiyalar geniş şəkildə tətbiq edilmiş, on-line rejimində biliyin yoxlanılması həyata keçirilmiş, bu sahədə informasiya resursları

formalaşdırılmışdır. Əhaliyə İnternet vasitəsilə geniş informasiya xidmətləri göstərilir;

- Respublikada məhkəmə hakimlərinin və bir sıra dövlət qulluqçularının seçilməsi prosesində informasiya və kommunikasiya texnologiyaları müvəffəqiyyətlə tətbiq edilir;
- "Seçkilər" dövlət avtomatlaşdırılmış informasiya sistemi yaradılmışdır və 2000-ci ildən başlayaraq əhalinin səs verməsi zamanı İKT-dən geniş istifadə olunur;
- Azərbaycanın bir çox elm və təhsil müəssisələrini birləşdirən telekommunikasiya şəbəkəsi yaradılmışdır;
- İnformasiya və kommunikasiya texnologiyaları üzrə sertifikatlı mütəxəssislərin hazırlanması üçün regional Akademiyanın yaradılması layihəsi həyata keçirilmişdir;
- "Azərbaycanın milli pasport sistemi" layihəsində müasir informasiya və kommunikasiya texnologiyaları geniş tətbiq edilmişdir;
- Azərbaycanın bank sistemində real vaxt rejimində banklararası milli elektron ödəniş sistemi və kiçik ödənişlər üçün avtomatlaşdırılmış klirinq sistemi layihələri həyata keçirilmişdir;
- Respublikada beynəlxalq təşkilatların dəstəyi ilə informasiya sahəsində maarifləndirmə yönümlü bir sıra regional mərkəzlər yaradılmışdır;
- Trans-Asiya-Avropa layihəsi çərçivəsində Respublikada optik rabitə xətləri şəbəkəsi qurulmuş, bunun sayəsində mövcud rabitə kanalları əsasən rəqəmli rejimə keçirilmişdir;
- TRASEKA layihəsi çərçivəsində Bakı-Tbilisi dəmiryolu xətti boyunca optik rabitə xətti istifadəyə verilmişdir;
- Gömrük sistemində idarəetmənin və prosedurların təkmilləşdirilməsi məqsədilə "Məlumatların ötürülmə şəbəkəsi və avtomatlaşdırılmış nəzarət sistemi" yaradılmışdır;

- Azərbaycan Respublikası Dövlət Neft Şirkətində "İnformasiyanın ötürülmə şəbəkəsi" və "Avtomatlaşdırılmış nəzarət sistemi" layihələri həyata keçirilmişdir;
- Bir sıra dövlət və özəl qurumlarda informasiya və kommunikasiya texnologiyaları sahəsində əhəmiyyətli layihələr həyata keçirilmişdir və s.

Bu gün İKT sektorunda regional liderliyi ölkəyə idxal olunan və ixrac edilən müəyyən məhsulların çoxluğu deyil, milli innovasiya sistemi müəyyənləşdirir. Yəni İKT sektorunda uğurların əldə olunması üçün əsas bazanı universitetlər, müəssisələr, tədqiqat mərkəzləri, texnoloji infrastruktur və digər elmi və texnoloji mərkəzlər təşkil edir. Lakin bu qurumların sadəcə varlığı kifayət etmir, qurumlar arasındakı effektli əlaqələr və müştərək öyrənmə şəraitinin yaradılması da öz növbəsində zəruridir. İnkişaf etməkdə olan ölkələr arasında, xüsusilə, Braziliya, Cənubi Koreya və Finlandiyanın təcrübələri nəzərə alınarsa, söylədiklərimiz daha yaxşı başa düşülə bilər. Məsələn, Braziliya elmi və texnoloji infrastrukturun inkişafına böyük ehtiyatlar ayırmaqla yanaşı telekommunikasiya infrastrukturunun inkişafı üçün də böyük investisiyaları həyata keçirmişdir. Lakin zaman-zaman belə ölkələr təcrübəni uzun illərin nəticəsində toplamış və qoruyub saxlamışlar.

Bu gün Azərbaycan İKT sahəsində regionda şübhəsiz liderdir və birmənalı olaraq bu liderliyini qorumağa çalışacaq. Bunun üçün isə ixtisaslı kadr arsenalını daim təkmilləşdirmək, müvafiq qanunvericiliyə paralel olaraq fəaliyyəti daha da genişləndirmək və ən başlıcası innovasiya sistemlərindən bəhrələnərək İKT infrastrukturunun iqtisadi bazasını durmadan yüksəltmək lazımdır. Çünki bu məsələ ilə bilavasitə əlaqəli olan digər proseslərin həlli və Azərbaycanın iqtisadiyyatı məntiqli olaraq günümüzün yeni texnologiyalarının mənimsənilməsi ilə bağlıdır.

Son illər Azərbaycan Respublikası ilə bir sıra xarici ölkələr arasında bir neçə beynəlxalq saziş imzalanmışdır. Onlardan bəziləri aşağıdakılardır:

- Beynəlxalq Telekommunikasiya Birliyinin Nizamnaməsi və Konvensiyası 22.12.1992-ci il tarixində qəbul edilmiş və 14.12.1994-cü il tarixində Kiotoda dəyişikliklər edilmişdir;

- Azərbaycan Respublikası Hökuməti və Ukrayna Respublikası Nazirlər Kabineti arasında 2000-ci ildə imzalanmış "Hökumətlərarası kommunikasiya sahəsində əməkdaşlıq haqqında" Saziş;
- Avropa Poçt və Telekommunikasiya Rəhbərliklərinin Konfransının yaradılmasına dəstək verilməsi 07.09.1992-ci il tarixində və bu konfransın prosedur qaydaları 06.09.1996-ci il tarixində qəbul edilmişdir;
- Azərbaycan Respublikası Milli Təhlükəsizlik Nazirliyi və Rusiya Prezidenti yanında Federal Kommunikasiya və İnformasiya Agentliyi arasında "Hökumətlərarası kommunikasiya və informasiya təhlükəsizliyinin təmin edilməsi sahəsində əməkdaşlıq haqqında" Saziş;
- "Azərbaycan Respublikası və Özbəkistan Respublikası arasında rabitə və telekommunikasiya sahəsində əməkdaşlıq haqqında" Saziş, 25 iyul 1997-ci il;
- "Azərbaycan Respublikası və Qazaxıstan Respublikası arasında rabitə sahəsində əməkdaşlıq haqqında" Saziş, 01.02.1999;
- "Şanvari Mobil Rabitə Sistemləri sahəsində əməkdaşlıq, inkişaf və onların tətbiqi haqqında" MDB Sazişi, 30.03.1999;
- Azərbaycan və Ukrayna Nazirlər Kabinetləri arasında "Hökumətlərarası rabitə sahəsində əməkdaşlıq" Sazişi, 24.03.2000;
- "Şanvari mobil rabitə sistemlərinin tətbiqi və inkişafı haqqında sazişə düzəlişlər haqqında" protokol, 24.10.2000;
- Azərbaycan Respublikası ilə Latviya Respublikasi arasında rabitə, informasiya və kommunikasiya texnologiyaları sahəsində ikitərəfli saziş. Həmin sənəd İKT-nin təhsilə tətbiqi istiqamətində də iki ölkə arasında əməkdaşlıq üçün geniş imkanlar açır.

Latviyada İKT-nin inkişafı və informasiya cəmiyyətinin formalaşdırılması istiqamətində işlər 1994-cü ildən başlanmış, 1997-ci ildən isə daha da sürətləndirilmişdir. Bu sahədə xüsusi proqramlar qəbul olunmuş, İKT-nin təhsildə tətbiqi həmin proqramlarda özünə xüsusi yer almışdır.

Öncə hər təhsil müəssisəsinə 3 dəst kompüter verilməklə təhsilin idarə edilməsi informatlaşdırılmış, məktəb rəhbərlərinin kağızla işləməsi aradan qaldırılmışdır.

Sonra kompüter texnikasının şagirdlərə öyrədilməsi hədəf götürülmüş, tədris ocaqlarının İKT ilə təchizinə başlanmışdır. İnformatika Latviyada 6-cı sinifdən öyrədilir. Hər birində orta hesabla 30 şagirdin oxuduğu siniflər 2 dəst kompüterlə təchiz olunmuşdur. Ötən ildən bütün məktəblərdə kompüter sinifləri var.

Bu məqsəd üçün ayrılmış dövlət vəsaiti ilə yanaşı, əlavə maliyyə resurslarından da istifadə olunur, kommersiya müəssisələri ilə əlaqə saxlanılır, onlardan 3-4 il istifadə olunmuş kompüterlər alınaraq məktəblərə verilir ki, uşaqlar onu ilkin formada öyrənsinlər.

Ölkədə 2007-2013-cü illəri əhatə edən keyfiyyətli təhsil üçün "İnformatika və kommunikasiya texnologiyası Proqramı" işlənib hazırlanmışdır. Proqram hazırlanarkən şagirdlərin, tələbələrin və valideynlərin rəyi öyrənilmiş, onların nə istədikləri müəyyənləşdirilmişdir. Bu Proqramın ən mühüm vəzifəsi bütün əhalidə İKT-dən istifadə vərdişləri yaratmaqdır.

Proqram bir neçə istiqamətdə layihələri özündə ehtiva edir. Onlardan birincisi "Məktəb-informatika layihə"sidir. Bu layihə İKT-dən tədris prosesində daha geniş istifadəni nəzərdə tutur. Artıq bir sıra fənlər üzrə elektron tədris vəsaitləri hazırlanmışdır.

Proqramın ikinci bir layihəsi "Müəllimlərin təhsili" adlanır. Layihə təkcə məktəb rəhbərləri, informatika müəllimlərini deyil, bütün müəllimlərin öyrədilməsini nəzərdə tutur.

Proqramın bir layihəsi də əhaliyə, valideynlərə İKT-dən istifadənin öyrədilməsini əhatə edir.

Multimedia laboratoriyaları yaratmaq, kitabxanalarda elektron oxu zallarının təşkili, bütün kitabxanaların internetə qoşulması, əhali təbəqələrinin internet vasitəsi ilə məsafədən təhsilə cəlb olunması və s. də görüləcək işlərdəndir.

Son illər telekommunikasiya liderlik uğrunda mübarizə aparılan sahəyə çevrilmişdir. ABŞ da belə ölkələr siyahısındadır. İqtisadi və ictimai həyatda

informatikanın səviyyəsinə görə ABŞ irəlidədir. Bu nailiyyət nəhəng iqtisadiyyat, onun mobil olması, investisiya qoyuluşu, biznesmen və alim axını nəticəsində əldə olunmuşdur. Əlbəttə, bu nailiyyətlər hökumətin dəstəyi ilə əldə olunmuşdur. ABŞ-da telekommunikasiya sahəsində nailiyyətlər o zamankı ölkə prezidenti Bill Klinton tərəfindən 1996-cı il 8 fevral tarixində "Telekommunikasiya haqqında" qanunun qəbul olunmasından sonra əldə olunmağa başlandı. Qanunun qəbul olunması mərasimində Bill Klinton çıxış edərək bildirmişdir ki, hazırkı informasiya inqilabı nəinki bizim iş üsulumuzda, mövqeyimizdə, hətta bizim bir-birimizə olan münasibətimizdə də dəyişikliklər aparır. Telekommunikasiya sahəsinin inkişaf səviyyəsinə görə ABŞ 80-ci illərin ortalarında Şərqi Avropa ilə eyni yeri bölüşdürürdü. 1984-cü ildə telekommunikasiya sahəsində müxtəlif uzunmüddətli layihələr həyata keçirilməyə başlandı. Bunlardan "ESPRİT" Proqramını misal göstərmək olar. Bu Proqram Avropa informasiya cəmiyyətinin yaradılması məqsədi üçün nəzərdə tutulmuşdu. Proqramın əsas hissəsi proqram təminatı və multimedia texnologiyaları sahəsində tədqiqatların aparılmasına həsr olunmuşdur.

Hazırda ölkədə informasiya texnologiyaları öndə duran məsələlərdən biridir və bu sahənin inkişafına xüsusilə diqqət yetirilir.

Rusiya kompüter parkının inkişaf sürətinə görə dünyada birinci yeri tutur. Son üç il ərzində kompüter istifadəçilərinin sayı, demək olar ki, iki dəfə artmışdır. Bununla belə, nəzərəçarpan artıma baxmayaraq, onların ümumi sayı inkişaf etmiş ölkələrlə müqayisədə çox deyil; 142 milyon rusiyalının cəmi 35 faizi kompüterdən istifadə edir. Ölkədə 23 milyon şəxsi kompüter var. Müqayisə üçün: ABŞ-da, Qərbi Avropada, Yaponiyada, demək olar ki, hamının kompüteri var, qlobal şəbəkə istifadəçilərinin sayı isə əhalinin ümumi sayının təxminən yarısını təşkil edir.

"Score Networks" şirkətinin məlumatına görə, Rusiyada qlobal şəbəkə istifadəçilərinin sayı il ərzində rekord səviyyədə - 21% artmışdır. Ancaq onların ümumi sayı 12,7 milyon nəfərdən çox deyil.

Nəticədə 2015-ci ilədək Rusiyada stasionar telefon çəkmək, şanvari rabitədən istifadə etmək, həmçinin internetə daxil olmaq üçün texniki imkanı olmayan bir dənə də yaşayış məntəqəsi qalmamalıdır. İKT sahəsində liderliyə nail olmaq üçün dövlət əqli mülkiyyətin müdafiəsinə, informasiya texnologiyaları sahəsində texniki reqlamentlərin və standartların işlənib hazırlanmasına, həmçinin müasir lisenziya və patent fəaliyyəti sistemlərinə xüsusi diqqət yetirəcək.

Təəssüf ki, Rusiyada İKT sahəsinin modernləşdirilməsi üçün nə qədər investisiya tələb olunduğunu hətta təxmini hesablamaq mümkün deyil. Təkcə məktəblərin və ucqar yaşayış məntəqələrinin rabitə vasitələri və kompüter kommunikasiyaları ilə təchizinə, hakimiyyət orqanlarının fəaliyyətində informasiya texnologiyalarının tətbiqinə milyardlarla rubl pul lazımdır. Özü də rusiyalıları müasir kommunikasiya vasitələri ilə təchiz etmək üçün böyük səylər tələb olunmaya da bilər. Belə ki, dövlətin hər hansı iştirakı olmadan cəmi bir neçə il ərzində rusiyalılar ölkə ərazisinin böyük bir hissəsində özlərini mobil rabitə ilə təmin etmişlər. Onlar özlərini internetlə də təmin etmək iqtidarındadırlar, müasir rabitə texnologiyaları hətta ən ucqar rayonlarda bu işi görməyə imkan verir.

Yüksək texnologiyalar sahəsini praktik olaraq sıfırdan başlayaraq inkişaf etdirmək Rusiya sahibkarlarının gücü çatan iş deyil. Rusiyaya SSRİ-dən miras qalmış texnologiyalar əsasən hərbi təyinatlı idi. Onlar müasir yüksək mülki texnologiyalar dünyasında az tətbiq olunur. Deməli, ölkədə mobil telefon istehsalını təşkil etmək, yaxud kompüter texnikası üçün baza yaratmaqdan ötrü milyardlarla rubl tələb oluna bilər.

Bu gün Rusiyada İKT-nin inkişafı üzrə proqramlar fəaliyyət göstərir. Onlardan biri Prezident Proqramı "İnternet məktəblərdə", digər Proqram "Elektron Rusiya" və başqalarıdır.

Pakistan isə nisbətən zəif telekommunikasiya infrastrukturuna malik ölkələrdən biridir. "Pakistan Telecommunication Company Limited" (PTCL) Pakistanın nəhəng telekommunikasiya kompaniyasıdır. Bu kompaniyanın yaranma tarixi 1947-ci ilə təsadüf edir. PTCL müxtəlif növ şəbəkəni idarə edir. Buraya mobil, sabit şəbəkələr, kabel televiziyası və s.-ni aid etmək olar. Kompaniyanın

şəbəkəsi bütün Pakistan ərazisini əhatə edir. PTCL Pakistanda CDMA450 standartlı WLL ümumi şəbəkənin genişləndirilməsi məqsədilə strateji tərəfdaş kimi Huawei Technologies kompaniyasını seçmişdir. Layihəyə əsasən 220 min abunəçiyə telekommunikasiya xidməti təqdim etmək nəzərdə tutulmuşdur. Telefonlaşmanın səviyyəsini artırmaq və universal xidmət (Universal services) problemini həll etmək məqsədilə Pakistan hökuməti "Kəndlərin telefonlaşdırılması" Dövlət Proqramını həyata keçirmək qərarına gəlmişdir. Pakistanın nəhəng telekommunikasiya operatoru kimi PTCL bu sosial proqramın həyata keçirilməsini öz üzərinə götürmüşdür. Bu məqsədlə kompaniya müxtəlif avadanlıq təchizatçılarının təklifinə baxış keçirdikdən sonra məhz Huawei Technologies kompaniyasına üstünlük verdi. CDMA450 WLL şəbəkəsi Pakistanın bütün şəhər və kəndlərini əhatə edərək səsin və verilənlərin yüksək sürətlə ötürülməsi, həmçinin əlavə xidmətlərdən PPS (əvvəlcədən ödəniş xidməti), simsiz taksofonlar, SMS və başqa xidmətləri təqdim edir.

Pakistanın ilk dəfə şəbəkəyə qoşulması 1992-ci ilə təsadüf edir. O zamanlar ilk domen "zona.pk" olmuşdur. İlk internet provayderi isə 1996-cı ildən fəaliyyət göstərməyə başlamışdır. Hazırda isə ölkədə XcessNet, GoNet, SHOA, WorldTel, Cubexs, Net21, TeleNet, Cyberlinks, FastNet internet provayderləri fəaliyyət göstərir. Ölkə ərazisində televiziya, videokonfrans və internet təhsili ilə əlaqədar virtual universitet də mövcuddur. Tələbələr universitetə internet vasitəsilə qoşulurlar. Virtual universitetin təşkilatçıları bundan sonra da tələbələrin sayının artırılmasını nəzərdə tutublar. Bununla yanaşı 60 universitet, 2500 məktəb və kolleci birləşdirən yüksək sürətli kompüter şəbəkəsinin yaradılması da planlaşdırılıb. Pakistanlıların internetə marağı getdikcə artır. Hökumət hər bir kəsin internetə qoşulması üçün bütün qüvvəsini səfərbər etmişdir.

Pakistan sosial-iqtisadi inkişaf səviyyəsinə görə bir çox ölkələrdən geridə qalmışdır. Bununla yanaşı hökumət ölkə iqtisadiyyatının inkişafına təkan verəcək İKT sahəsinə böyük ümidlər bəsləyir. Bu məqsədlə 2000-ci ildə dövlət başçısı bu sahədə öz siyasətinin istiqamətlərini elan etmişdir. Bunlara yüksək səviyyəli mütəxəssislərin hazırlanmasını, bilik və savadın əhali arasında geniş yayılmasının

təminini, müasir telekommunikasiya infrastrukturunun yaradılmasını, proqram təminatı sənayesinin yaradılmasını, internetə qoşulmanı və b. aid etmək olar. Ölkədə hərbi vəziyyət mövcud olduğu üçün qanunvericilik aktları parlament tərəfindən deyil, prezident tərəfindən qəbul olunur. Pakistanda İKT sahəsi yüksək templə inkişaf etməyə başlamışdır. İKT-nin inkişafını işgüzar və elmi sazişlər olmadan təsəvvür etmək mümkün deyil. Elə buna görə də ölkənin şəhərlərində sərgilər, seminar və konfranslar keçirilir. Buna misal olaraq, 2002-ci ildə Microsoft korporasiyası və Milli Dillər Departamentinin təşkilatçılığı ilə İslamabadda keçirilən "Pakistanda dillərin kompüterləşməsi" konfransını göstərmək olar. Bu konfransın keçirilməsi ölkədə 30 dildən istifadə edilməsi ilə bağlıdır. Bu dillərin içərisində ölkədə ən çox 6 dildən istifadə olunur. İKT sahəsinə qoyulan xarici investisiyaların sayı artmaqdadır. Hazırda ölkədə Microsoft, İntel, Mobilnik, Ericsson, Siemens, Motorolla kimi beynəlxalq kompaniyaların nümayəndəlikləri fəaliyyət göstərir. Çin firmaları İKT-nin bazarına daha çox müdaxilə edirlər. Beynəlxalq Maliyyə Təşkilatı İKT sahəsinə sponsorluq edir. BMT-nin Sənaye İnkişafı Beynəlxalq Təşkilatı ilə əməkdaşlıq çərçivəsində informasiya sənaye şəbəkəsinin yaradılması layihəsi həyata keçirilir.

Azəbaycanda İKT sferasının inkişafında Litva Respublikasının təcrübələrindən də istifadə olunur.

Litva Respublikasında İKT sferasını təşkil edən təşkilatlara Litva Respublikası hökumətinin İnformasiya Cəmiyyətinin İnkişaf Komitəsi, Litva parlamentində İnformasiya Cəmiyyətinin İnkişaf Komitəsi, rabitəni nizamlayan dövlət xidməti (rabitə və telekommunikasiya sahəsinin nizamlanması), Daxili İşlər Nazirliyinin İnformasiya Siyasəti Departamenti, Litva Respublikasının Dövlət Təhlükəsizlik Departamenti və Verilənləri Mühafizə edən Dövlət İnspeksiyası (təftiş) aiddir.

Azərbaycan Respublikasında İKT sferasınım inkişafında xarici təcrübənin özünəməxsus yeri vardır və bu təcrübələr bu sferanın gələcəkdə qabaqcıl sahələrdən birinə çevrilməsinə şarait yaradacaqdır.

## 1.2. Ölkədə informasiya cəmiyyətinin genişləndirilməsi istiqamətləri

XX əsrin sonu və XXI əsrin əvvəli İnformasiya və Kommunikasiya Texnologiyaları (İKT) cəmiyyətin inkişafına təsir göstərən vacib amillərdən birinə çevrilmişdir. Cəmiyyətin inkişaf tarixində üç qlobal sosial-texniki inqilab qeyd olunur - aqrar, sənaye və informasiya. Sonuncu müasir informasiya texnologiyalarının tətbiqi ilə ictimai həyatın informasiyalaşdırılması prosesi kimi reallaşır və günümüzün ən aktual proseslərindən biridir.

İlk fərdi kompüterlər yaranan zaman heç kim onun bütün imkanları haqqında tam təsəvvürə malik deyildi və az insanlar inanırdılar ki, informasiya inqilabı Dünyanı və onun dünənini əsaslı formada dəyişəcək. Əlbəttə ki, bu gün formalaşmaqda olan informasiya cəmiyyətini çoxlarımız təsəvvürümüzə belə gətirə bilməzdik. Son illərdə informasiya texnologiyalarının fantastik inkişafı nəticəsində biz yeni Dünyaya - İnformasiya Dünyasına keçid dövrünü yaşayırıq. Bu Dünyada bizi nələr gözlədiyini tam bilməsək də, onu bilirik ki, fərdi kompüter erasından fərqli olaraq İnformasiya Dünyası daha çox insanı əhatə edəcək və cəmiyyəti daha da inkişaf etdirəcək. İlk növbədə münasibətlərin forması və məzmunu dəyişəcək və bu dəyişiklik fərdi kompüterin yaratdığı imkanlardan daha möhtəşəm olacaq. Belə ki, fərdi kompüterlər, İnternet, elektron poçt, multimedia məhsulları, İP-telefon, virtual oyunlar, intellektual sistemlər, obrazların və nitqin tanınması - bunlar hamısı növbəti inqilabı səciyyələndirən fundamental elementlərdir.

Fərdi kompüterlərin ilk yarandığı və imkanlarının üzə çıxdığı vaxtlar cəmiyyətdə elə də geniş əhatə dairəsi yaratmamışdı. Kütləvi informasiya vasitələri bu yeni sahəni demək olar ki, çox səthi işıqlandırırdılar. Kompüterə və onun imkanlarına aludə olmuş insanlar, sanki geniş kütlədən təcrid olunaraq öz dünyalarında yaşayırdılar. Bunun bir səbəbi də, bu yeniliyin bu qədər sürətlə və əhatəli olaraq cəmiyyətin məişətinə daxil olacağına inamsızlıq idi. Fakt isə göz qarşısında, hər birimizin gündəlik fəaliyyətində və həyatındadır.

Bundan fərqli olaraq, İnformasiya Dünyası mövzusu kütləvi informasiya vasitələrinin, aparıcı televiziya kanallarının, beynəlxalq təsisatların, elmi konfransların, Sammitlərin, aparıcı dövlətlərin liderlərinin zirvə görüşlərinin əsas müzakirə predmetinə çevrilmişdir. Son illər bu məsələyə demək olar ki, cəmiyyətin bütün təbəqələri (dövlət, biznes və vətəndaş) tərəfindən çox böyük diqqət və maraq göstərilir. İnformasiya Cəmiyyəti üzrə keçirilmiş Cenevrə və Tunis Sammitləri göstərdi ki, bu diqqət və maraq təkcə inkişaf etmiş ölkələrdə deyil, həmçinin kompüter istifadəçilərinin sayına görə dünya üzrə sonuncu yerləri tutan ölkələrdə də çox böyükdür.

Mütəxəssislərin fikrincə, rabitə sahəsində inqilab hələ yenicə başlayır və onillikləri əhatə edəcəkdir. Onun nəticələri isə, yeni vasitələr olacaq, hansı ki, insanların bu gün təsəvvürümüzdə canlandırmağa çalışdığımız İnformasiya Dünyasındakı ehtiyaclarını aradan qaldırmağa imkan verəcək. Bunun üçün isə növbəti illərdə hökumətlər, şirkətlər və ayrı-ayrı insanlar çox ciddi qərarlar qəbul etməlidirlər.

Təsadüfi deyil ki, bu gün informasiya cəmiyyətinin formalaşması əksər dövlətlərdə strateji məsələ olaraq qarşıya qoyulmuşdur və müasir informasiya texnologiyalarının cəmiyyətə inteqrasiya səviyyəsi ölkənin iqtisadi inkişaf dərəcəsini əks etdirən amilə çevrilmişdir. İnkişaf etmiş ölkələrin təcrübəsi göstərir ki, informasiya cəmiyyətinin formalaşması prosesi mürəkkəb və çoxşaxəlidir. Prosesin uğurla həyata keçirilməsi isə cəmiyyətin hər bir üzvünün informasiya texnologiyalarının gündəlik həyatımızda əhəmiyyətini necə dərk etməsindən birbaşa asılıdır.

Məhz elə bu fikir 2003-cü ilin dekabrında Cenevrədə və 2005-ci ilin noyabrında Tunisdə respublikamızın da təmsil olunduğu İnformasiya Cəmiyyəti üzrə Dünya Sammitlərində müzakirə olunan mövzuların ana xəttini təşkil edirdi. Bu Sammitlər cəmiyyətin inkişafında bir də ona görə tarixi əhəmiyyət kəsb edirdi ki, ilk dəfə olaraq biznes, hökumət və ən başlıcası vətəndaş cəmiyyətinin nümayəndələri bir araya gələrək sivilizasiyanın inkişafı naminə vahid mövqedən çıxış etdilər.

Bu ideyanı daim gündəmdə saxlamaq üçün hər ilin 17 May tarixinin "Ümumdünya İnformasiya Cəmiyyəti Günü" kimi qeyd olunması qərara alındı. "Tunis Öhdəlikləri" sənədində isə iştirakçı dövlətlər bütün xalqların inkişafına xidmət edəcək Qlobal İnformasiya Cəmiyyətinin qurulması prosesində ortaya çıxa biləcək hər bir problemin vaxtında və operativ həlli üçün birgə fəaliyyət göstərəcəklərini bir daha təsdiqlədilər.

Ümumbəşəri inkişaf yolu ilə gedərək ölkəmizdə də informasiya cəmiyyətinə keçid üçün müvafiq mühitin yaradılması yolu seçilmişdir. Azərbaycanda aparılan dövlət siyasəti informasiya-kommunikasiya texnologiyalarının yeni bir prioritet sahə kimi inkişafına əlverişli şərait yaratmışdır. Informasiya-kommunikasiya texnologiyaları müasir cəmiyyətin ən vacib infrastrukturu, iqtisadiyyatın bir sektoru, məhsuldarlığın artım amili və müasir humanitar inkişafın katalizatoru olaraq, Azərbaycanda energetika sektorundan sonra ən dinamik inkişaf edən ikinci sahədir.

Xatırlatmaq lazımdır ki, ulu öndər Heydər Əliyevin siyasi qətiyyəti sayəsində 1994-ci ilin sentyabrında "Əsrin müqaviləsi"nin imzalanması ölkənin yeni sosial-iqtisadi inkişaf modelinin həyata keçirilməsi üçün zəruri əsaslar formalaşdırmaqla yanaşı, müasir rabitə və informasiya texnologiyalarının sürətlə inkişafına da böyük canlanma yaratmışdır. Neft sektoruna və iqtisadiyyatın digər sahələrinə milyardlarla investisiya yatıran Qərb şirkətləri ölkədə informasiya cəmiyyətinin bərqərar olması prosesində yaxından iştirak etməyə başlamış, bu məqsədlə Azərbaycana ən yeni və modern texnologiyalar gətirilmişdir.

Ölkədə İKT-nin inkişaf etdirilməsi məqsədilə ilk növbədə qanuni və hüquqi baza yaradılmasının vacib olduğundan Azərbaycanda da bu məqsədlə adları aşağıda qeyd edilən çoxlu sayda dövlət proqramları, strategiya və qanunlar qəbul olunmuşdur:

**"Azərbaycan Respublikasının inkişafı naminə informasiya və kommunikasiya texnologiyaları üzrə Milli Strategiya" (2003-2012-ci illər)"**

Milli Strategiyanın əsas məqsədi informasiya və kommunikasiya texnologiyalarından geniş istifadə etməklə ölkənin demokratik inkişafına kömək etmək və informasiya cəmiyyətinə keçidi təmin etməkdir.

Milli Strategiyanın əsas vəzifələrinə aşağıdakılar aiddir:

- informasiya cəmiyyətinin hüquqi əsaslarının yaradılması və inkişaf etdirilməsi;

- cəmiyyətdə insan amilinin inkişaf etdirilməsi, vətəndaşların keyfiyyətli təhsil, tibbi xidmət və sosial təminatlar alması üçün əlverişli şəraitin yaradılması;

- vətəndaşların və sosial institutların məlumat almaq, onu yaymaq və istifadə etmək kimi hüquqlarının təmin edilməsi üçün müvafiq mühitin yaradılması;

- effektiv, şəffaf və nəzarət oluna bilən dövlət idarəetməsi və yerli özünüidarəetmənin həyata keçirilməsi, elektron hökumətin yaradılması, elektron ticarətin formalaşdırılması və inkişaf etdirilməsi;

- ölkənin iqtisadi, sosial və intellektual potensialının möhkəmləndirilməsi, informasiya və biliklərə əsaslanan, rəqabətə davamlı iqtisadiyyatın qurulması, informasiya və bilik bazarının yaradılması və inkişaf etdirilməsi;

- xalqın tarixi, ədəbi və mədəni irsinin qorunub saxlanması və onun geniş təbliği;

- inkişaf etmiş informasiya və kommunikasiya infrastrukturunun yaradılması, vahid milli elektron informasiya məkanının formalaşdırılması, informasiya və kommunikasiya xidmətlərinin genişləndirilməsi;

- ölkənin informasiya təhlükəsizliyinin təmin olunması;

- ölkənin ümumdünya elektron informasiya məkanına inteqrasiyası;

- milli proqram vasitələrinin yaradılması, informasiya və kommunikasiya texnologiyaları məhsullarının istehsalının (İKT sənayesinin) inkişaf etdirilməsi;

- ölkənin «rəqəmsal geriliyinin» aradan qaldırılması.

Strategiyanın həyata keçirilməsi nəticəsində dövlət idarəetməsində şəffaflığın təmin olunması, davamlı iqtisadi dirçəlişə nail olunması, əhalinin həyat şəraiti yüksək dərəcədə yaxşılaşması, ölkədə vahid elektron informasiya məkanın formalaşması, bütün vətəndaşlar üçün informasiya əldə etmək imkanları yaranması

və milli maraqlar nəzərə alınmaqla ölkə ümumdünya elektron informasiya məkanına inteqrasiya olunması nəzərdə tutulmuşdur.

## "Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2005-2008-ci illər üçün Dövlət Proqramı" (Elektron Azərbaycan)"

Dövlət Proqramının məqsədi Azərbaycanda rabitə və informasiya texnologiyalarının inkişafını təmin etmək və bu yolla ölkənin hərtərəfli tərəqqisi üçün xidmət göstərmək, eyni zamanda İKT-nin inkişafı üzrə Milli Strategiyanın həyata keçirilməsini təmin etmək, müəyyən edilmiş məqsədlərə və fəaliyyət istiqamətlərinə uyğun olaraq layihələri planlaşdırmaq və icra etməkdir.

Bununla əlaqədar aşağıdakı məsələlərin həlli xüsusi əhəmiyyət kəsb etmişdir:

- rabitə və informasiya texnologiyaları sahəsinin gələcək inkişafı üçün islahatların aparılması və effektiv mexanizminin formalaşdırılması;

- qlobal informasiya fəzasına inteqrasiyanın genişləndirilməsi;

- cəmiyyətin, iqtisadiyyatın, dövlət orqanlarının, hüquqi və fiziki şəxslərin ümumistifadəli rabitə və informasiya texnologiyaları şəbəkələrinə qoşulma imkanlarının və onların artan tələbatının təmin edilməsi;

- ölkənin milli informasiya təhlükəsizliyi sisteminin yaradılması, informasiya fəzasının təhlükəsizliyinin və vətəndaşların informasiya hüquqlarının müdafiəsinin təmin edilməsi;

- rabitə və informasiya texnologiyalarının inkişafını təmin etmək üçün normativ-hüquqi bazanın təkmilləşdirilməsi;

- rabitə və informasiya texnologiyaları sahəsində standartlaşdırmanın, sertifikatlaşdırmanın, radiotezlik və nömrələnmə ehtiyatlarının tənzimlənməsinin beynəlxalq standartlara uyğun təşkil edilməsi;

- rabitə və informasiya texnolojiyaları sahəsinə investisiyaların cəlb edilməsinə şərait yaradılması və özəl sektorun inkişaf etdirilməsi;

- poçt şəraitinin modernləşdirilməsi və yeni xidmət növlərinin istifadəyə verilməsi;

- yeni texnika və texnologiyalar tətbiq edilməklə daha keyfiyyətli radio-televiziya yayımı və peyk rabitəsi xidmətlərinin göstərilməsi;

- innovasiya siyasətinin müəyyənləşdirilməsi və informasiya cəmiyyətinin qurulmasını təmin edən fundamental və tətbiqi elmi tədqiqatların aparılması;

- təhsil sahəsində müasir texnologiyalardan geniş istifadə olunması, yüksək ixtisaslı kadrların, o cümlədən informasiya təhlükəsizliyi üzrə mütəxəssislərin hazırlığının təmin edilməsi;

- sahə üzrə sənayenin inkişafının təmin edilməsi, yerli istehsalın stimullaşdırılması və onun ixrac potensialının dəstəklənməsi;

- rabitə və informasiya texnologiyaları bazarında sərbəst və azad rəqabət şəraitinin yaradılması;

- dövlət, ictimai və sahə informasiya resurslarının formalaşdırılması, informasiya sistemlərinin və şəbəkələrinin yaradılması.

Dövlət Proqramında qarşıya qoyulan məqsədə nail olmaq üçün aparılacaq fəaliyyət aşağıdakı istiqamətlərdə həyata keçirməsi nəzərdə tutulmuşdur:

- rabitə və informasiya texnologiyaları sahəsində iqtisadi-struktur islahatlarının aparılması;

- rabitə və informasiya texnologiyaları sahəsində modernləşmə və yeni texnologiyaların tətbiqinin həyata keçirilməsi;

- informasiya cəmiyyətinə keçid üzrə layihələrin hazırlanması və həyata keçirilməsi.

**"Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2010-2012-ci illər üçün Dövlət Proqramı"**

**(Elektron Azərbaycan)**

Dövlət Proqramının məqsədi Milli Strategiyadan irəli gələn vəzifələrin yerinə yetirilməsi, respublikanın informasiya cəmiyyətinə keçidinin təmin edilməsi, İKT-nin inkişafını və geniş tətbiqini təmin etmək yolu ilə informasiya və biliklərə əsaslanan, rəqabətə davamlı iqtisadiyyatın qurulması və inkişaf etdirilməsi üçün zəminin formalaşdırılması, dövlət idarəetmə mexanizmlərinin səmərəliliyinin artırılması və qərarların qəbulu prosesində vətəndaşların və sosial institutların

iştirakı imkanlarının genişləndirilməsi, cəmiyyətin informasiya məhsulu və xidmətlərinə olan tələbatının dolğun ödənilməsidir.

Dövlət Proqramında qoyulmuş məqsədlərə çatmaq üçün aşağıdakı məsələlərin həlli nəzərdə tutulur:

- respublikada müasir informasiya və kommunikasiya infrastrukturunun inkişaf etdirilməsi, fiziki və hüquqi şəxslərin dövlət orqanlarının fəaliyyəti haqqında məlumatlara, həmçinin dövlət, ictimai və sahə informasiya resurslarına çıxışının genişləndirilməsi, informasiya və kommunikasiya xidmətlərinin genişləndirilməsi və onların keyfiyyətinin artırılması;
- dövlət idarəçiliyinin bütün səviyyələrində İKT həllərinin tətbiqi, dövlət informasiya sistemləri və resurslarının formalaşdırılması və inkişaf etdirilməsi;
- vahid texnoloji standartlar əsasında dövlət informasiya resursları və sistemlərinin inteqrasiyasının təmin edilməsi, dövlət orqanları arasında etibarlı və təhlükəsiz informasiya mübadiləsinin həyata keçirilməsi üçün vahid konfidensial multiservis şəbəkəsinin inkişaf etdirilməsi, təşkilati-texniki, texnoloji tədbirlərin həyata keçirilməsi və müvafiq mühitin formalaşdırılması;
- dövlət orqanlarının göstərdiyi xidmətlərin operativliyinin və keyfiyyətinin, habelə dövlət idarəetmə mexanizmlərinin səmərəliliyinin artırılması üçün "E-hökumət" həllərinin geniş tətbiqi, "bir pəncərə" prinsipi əsasında elektron xidmətlərin təşkili;
- müasir inkişaf tələblərinə uyğun olaraq, sahə üzrə normativ hüquqi bazanın təkmilləşdirilməsi;
- sahə üzrə standartlaşdırma və sertifikatlaşdırmanın beynəlxalq təcrübəyə uyğun həyata keçirilməsi;
- müasir İKT ixtisasları üzrə mütəxəssis hazırlığının keyfiyyətinin artırılması;
- İKT xidmət və məhsullarının istehsalının inkişaf etdirilməsi və ixrac potensialının artırılması;

- yeni texnika və texnologiyaların tətbiqi, sahə üzrə xidmətlərin, o cümlədən poçt və telekommunikasiya (o cümlədən peyk rabitəsi) xidmətlərinin genişləndirilməsi və keyfiyyətinin yüksəldilməsi;

- poçt şəbəkəsi vasitəsilə poçt-maliyyə xidmətlərinin həyata keçirilməsinin inkişaf etdirilməsi;

- e-ticarət, e-səhiyyə kimi mütərəqqi fəaliyyət formalarının inkişaf etdirilməsi;

- "rəqəmsal geriliyin" azaldılması üçün tədbirlərin həyata keçirilməsi;

- informasiya cəmiyyətinin qurulması istiqamətində vahid elmi-texniki və innovasiya siyasətinin həyata keçirilməsi;

- informasiya cəmiyyətinin qurulması üzrə görülən işlərə ictimai nəzarətin təmin edilməsi.

## Elektron imza və elektron sənəd haqqında Azərbaycan Respublikasının Qanunu

Bu Qanun elektron imzanın və elektron sənədin istifadəsinin, onların elektron sənəd dövriyyəsində tətbiqinin təşkilati, hüquqi əsaslarını və əlaqədar subyektlərin hüquqlarını müəyyən edir, aralarında yaranan münasibətləri tənzimləyir.

## "Xalq kompüteri" Layihəsi

Azərbaycan Respublikasının Rabitə və İnformasiya Texnologiyaları Nazirliyi, Azərbaycan Respublikasının Təhsil Nazirliyi, HP, Microsoft və Bestcomp Group şirkətlərinin birgə olaraq həyata keçirdikləri "Xalq kompüteri" layihəsini ölkədə kütləvi kompüterləşmənin ilkin mərhələsi hesab etmək olar.

Layihənin əsas məqsədi əhalinin sosial təbəqələrinin müasir kompüterlə və lisenziyalı proqramlarla təchiz edilmiş güzəştli şərtlərlə əldə etməsinə şərait yaratmaq və bölgələrdə İKT-nin tətbiqini genişləndirməklə rəqəmli geriliyi azaltmaq, Azərbaycan hökumətinin informasiya cəmiyyətinin və e-hökumətin inkişaf etdirilməsi istiqamətindəki fəaliyyətini dəstəkləməkdir.

Layihənin məqsədi insanların İKT imkanlarından səmərəli istifadə edərək həyat səviyyəsini yüksəltmək və həyat tərzini yaxşılaşdırmaq, informasiya

cəmiyyətinə keçidi təmin etmək üçün aşağıdakı məsələlərin inkişafına nail olmaqdır:

- Əqli əməyin təşviqi;
- Bilik iqtisadiyyatı yönümlü kadrların hazırlanması;
- İKT yönümlü kadrların hazırlanmasını stimullaşdırmaq;
- E-hökumətin inkişaf etdirilməsi;
- Təhsil sisteminin dəstəklənməsi;
- İntellektual mülkiyyətin qorunması;
- Kompüter vərdişlərinin təşviqi;
- Aztəminatlı sosial qrupların dəstəklənməsi;
- Əhalinin kompüterlərlə təminatına şərait yaratmaq;
- Kompüter sayının dünyanın orta göstəricilərinə çatdırmaq.

İlkin olaraq 2009-cu ilin aprelində başlayan və 4 ay müddəti əhatə edən pilot layihə həyata keçirilmişdir. Bu müddət ərzində layihə çərçivəsində yalnız orta məktəb müəllimləri kompüterlər əldə etmişlər. 18 noyabrın 2009-cu il tarixindən etibarən «Xalq Kompüteri» layihəsinin növbəti mərhələsinə start verilib. Bu mərhələ də orta məktəb müəllimlərinə aid edilmişdir. 30 iyun 2010-cu il tarixindən isə «Xalq Kompüter» layihəsinin ikinci mərhələsinə start verilmişdir. İmzalanmış razılaşmanın şərtlərinə əsasən, "Xalq Kompüteri" layihəsi çərçivəsində müəllimlərdən başqa orta məktəb şagirdləri və ali təhsil müəssisələrinin müəllim və tələbələri də kompüter və lisenziyalı proqram təminatını almaq imkanı əldə etmişlər.

Yuxarıda qeyd edilənlərdən əlavə olaraq, Azərbaycan Respublikasının Konstitusiyasının 50-ci maddəsi ilə təsbit olunmuş məlumat almaq hüququnun sərbəst, maneəsiz və hamı üçün bərabər şərtlərlə, açıq cəmiyyətin və demokratik hüquqi dövlətin prinsipləri əsasında təmin edilməsinin hüquqi əsaslarının müəyyənləşdirməkdən, həmçinin, ictimai vəzifələrin yerinə yetirilməsinə vətəndaşlar tərəfindən şərait yaratmaqdan ötrü "İnformasiya əldə etmək" haqqında və ölkədə telekommunikasiya sahəsində fəaliyyətin hüquqi, iqtisadi, təşkilati əsaslarının müəyyənləşdirilməsi və telekommunikasiya resurslarının məqsədyönlü

planlaşdırılmasını və istifadə olunmasını tənzimləmək məqsədilə "Telekommunikasiya" haqqında qanunlar qəbul olunmuş, ölkədə kosmik sənayenin yaradılması və inkişafı məqsədilə Dövlət Proqramı təsdiq edilmişdir.

## Azərbaycan Respublikasında kosmik sənayenin yaradılması və inkişafı üzrə Dövlət Proqramı

Dövlət Proqramının əsas məqsədi respublikada kosmik sənayenin yaradılması və inkişaf etdirilməsi, dövlət strukturlarının peyk rabitəsinə olan tələbatının ödənilməsi, regionlarda əhalinin teleradio yayımına artan tələbatının təmin edilməsi, ölkənin beynəlxalq rabitə kanallarının artırılması və kosmik fəzadan səmərəli istifadə etməklə iqtisadi, sosial, elmi, mədəni, təhlükəsizlik və s. sahələrin inkişaf etdirilməsidir. Kosmik sənaye sahəsində beynəlxalq əməkdaşlığın genişləndirilməsi, respublikanın kosmik sənaye potensialının möhkəmləndirilməsi, kosmik sənaye texnikasının inkişafı, yeni rabitə xidmətlərinin təşkili, teleradio yayımı, yerin məsafədən zondlanması, hidrometeorologiya, ekoloji monitorinq, fövqəladə hallara nəzarət, kosmik tədqiqatlar, axtarış və xilasetmə üzrə proqramlar və s. bu sahənin inkişafına geniş perspektivlər yaradacaqdır.

Dünyada telekommunikasiya və İKT sektorunun çox böyük inkişafı peyk şəbəkələrinin rəqabət qabiliyyətinin artırılması istiqamətində əməli tədbirlərin görülməsini tələb edir. Bununla əlaqədar, kosmik sənaye kompleksinin perspektiv inkişafı üçün aşağıda qeyd edilənlər aktual hesab olunur:

- peyk rabitə və yayım xidmətlərinin daha cəlbedici olması və geniş əhali kütləsi üçün nəzərdə tutulması;

- orbitə yeni çıxarılan peyklərin rəqabət qabiliyyətinin artırılması;

- fiksasiya olunmuş peyk sistemləri peyklərinin kommersiya effektliliyinin artırılması;

- yeni peyklər vasitəsilə təqdim olunan xidmətlərin qiymətlərinin tənzimlənməsi;

- yeni peyklər vasitəsilə göstərilən xidmətlərin infrastrukturunun təkmilləşdirilməsi;

- peyk rabitə sistemlərinin yerüstü yayım xidmətləri ilə inteqrasiyasının genişləndirilməsi.

Dövlət Proqramında aşağıdakı əsas strateji məqsədlər nəzərdə tutulur:

- gələcək inkişaf üçün potensialın yaradılması;

- milli və informasiya təhlükəsizliyinin təmin olunması və gücləndirilməsi;

- qlobal informasiya məkanına inteqrasiyanın genişləndirilməsi;

- dövlət orqanlarının, hüquqi və fiziki şəxslərin peyk şəbəkələrinə qoşulma imkanlarının təmin edilməsi;

- peyk sistemləri, onların idarə edilməsi və istismarı, eyni zamanda, kosmik sənayenin yaradılması və inkişafı üzrə normativ hüquqi bazanın təkmilləşdirilməsi;

- kosmik sənaye sahəsinə investisiyaların cəlb edilməsinə şəraitin yaradılması;

- respublika ərazisinin peyk rabitəsi, radio və televiziya yayımı ilə təmin edilməsi;

- dövlət strukturlarının xüsusi rabitəyə olan tələbatının ödənilməsi;

- respublika ərazisində ətraf mühitin monitorinqi və texnogen mənşəli fövqəladə halların proqnozlaşdırılması və tədqiqi üzrə araşdırmaların aparılması, dənizdə və quruda neft dağılmalarının miqyasının qiymətləndirilməsi;

- respublikanın beynəlxalq kosmik proqramlarda iştirakına şəraitin yaradılması;

- kosmik sənayenin inkişafının təmin edilməsi, yerli istehsalın stimullaşdırılması və onun ixrac potensialının dəstəklənməsi;

- kosmik sənaye və peyk sistemləri sahəsində mütəxəssislərin hazırlanması;

- strateji əhəmiyyətli infrastruktur obyektlərin təhlükəsizliyinin təmin edilməsi məqsədi ilə monitorinqin aparılması.

- kosmik sənayenin yaradılması və inkişafı.

# FƏSİL 2. İqtisadiyyatın elektronlaşdırılmasına təsir edən amillər

## 2.1. İqtisadiyyatın elektronlaşdırılmasında təhlükəsizlik problemi

Hər gün internetdə milyonlarla istifadəçi maliyyə əməliyyatlarını həyata keçirir, lakin onlardan çoxu heç düşünmür ki, onların hesabları böyük təhlükə altına düşür.Biz internetdə plastik kartımızın rəqəmlərini daxil etmətə başladığımız andan öz pul vəsaitlərimizin hamısını risk altına atmış oluruq .Bəs nömrəni oğurlaya bilən cinayətkarlar kimlərdir? Nömrəni bir neçə üsulla əldə etmək olar.

Birincisi,siz hər hansı bir sayta daxil olan zaman administrator sizin 18 yaşına çatmağınıza əmin olmaq üçün kredit kartınızın nömrəsini daxil etməyə xahiş edə bilər.Və ya heç kəsin söğortalana bilmədiyi bir digər üsul: əgər kimsə internet-mağazaya hücum edirsə,onda oradan sizin nömrəni əldə edə bilər (əgər mağaza müdaxilədən zəif mühafizə edilmişdirsə).Həmçinin sizə kart nömrənizin yanlışlıq üzündən silindiyi barəsində yazılı məktub gələ bilər və sizin kartınızla əlaqədar verilənləri yenidən göndərməyiniz xahiş oluna bilər.Bəs bundan necə yaxa qurtarmaq olar?Bundan aşağıdakı qaydalara riayət olunan zaman qorunmaq olar:

- Nömrəni tanış olmayan insanlara vermək olmaz və heç vaxt xüsusi şifrələnmə olmadan kart barəsindəki məlumatları məktub şəklində internet vasitəsilə göndərmək olmaz.
- Yalnız yaxşı ada malik olan, yoxlanılmış internet mağazadan mühafizə edilmiş əlaqə rejimində istifadə etmək lazımdır.Bu vəziyyət üçün saytda uyğun olan təlimatlar dərc olunmalıdır.
- Ən yaxşı üsullardan biri iki kredit kartından istifadə etməkdir, onlardan birində bütün vəsaitlər,digərində isə yalnız köçürüləcək məbləğ yerləşdirilməlidir.Bununla vəsaitlərin yerləşdiyi kartdan yalnız digər kredit kartına pulların köçürülməsi zamanı istifadə ediləcəkdir.

Kartın şəxsi verilənlərini göndərməzdən əvvəl verilənlərin ötürülməsinin kodlaşdırma sisteminin qoşulduğuna əmin olmaq lazımdır.Onun qoşulması

barəsində brauzerdə bağlı qıfıl şəklinin və ya informasiya mətnində məlumatın meydana gəlməsi xəbərdarlıq edir – bu kart sahibinin göndərdiyi informasiyanın başqaları tərəfindən ələ keçirilməsindən etibarlı mühafizə edir.Məhsul və ya xidmətlərin ödənişinim həyata keçirilməsi üçün kartları qəbul edən bir çox mağazaların intenet-səhifələri qeydiyyat və ya sifariş bölümündə qeyd olunan beynəlxalq sertifikat təşkilatlarından birinin şəhadətnaməsinə malikdirlər:Belsign,Verisign,Thawte və s.Bir qayda olaraq, internet-mağaza sertifikasiya təşkilatının verilənlər bazasında serverin sertifikatının həqiqiliyinin yoxlanılması imkanını təklif edir.Hesablamaların təhlükəsiliyinin əsas şərti isə internet mağazanın etibarlılığına əminlikdir.

Virtual əməliyyatları həyata keçirməzdən öncə mağazanın qaydaları ilə diqqətlə tanış olmaq çox əhəmiyyətlidir.Kənar şəxslərə kartda çap edilmiş verilənləri – nömrə,fəaliyyət müddəti ,təhlükəsizlik kodu barəsindəki məlumatları söyləmək olmaz.Ən yaxşı üsul dostlar və ya tanışların tövsiyyə etdiyi etibarlı və yoxlanılmış internet – mağazalardan istifadə etməkdir.Virtual- mağazanın etibarlılığının əlavə sübutu təhlükəsizlik kodunun( CVV2/CVC2) yoxlanılması, həmçinin ödəniş üzrə verilənlərin ötürülməsi zamanı verilənlərin ötürülməsinin təhlükəsizlik protokolu olan SSL-dən istifadə etmək labüddür.Həmçinin şirkətin saytının diqqətlə tətqiq edilməsi də çox əhəmiyyətlidir:o, ünvan və əlaqə sxemi, bank rekvizitləri,əlaqə telefonları başda olmaqla maksimal sayda əlverişli informasiyaya malik olmalıdır.Ödənişi həyata keçirməzdən əvvəl verilən telefon nömrələrinə zəng vurmaq və dəqiqləşdirici suallar vermək məsləhətlidir.Əgər zəng düzgün şəkildə qəbul olunub emal edilərsə, onda bu şirkətə çox güman ki, şəxsi məxfi informasiyanı etibar emtək olar.Təcrübə göstərir ki, cinayətkarlar öz saytlarının arayiş-sorğu xidmətinin yaradılmasına kifayət dərəcədə az əhəmiyyət verirlər.

Kartın verilənləri barəsindəki məlumatı yalnız ödənişi həyata keçirən zaman həyata keçirmək lazımdır; daimi olaraq kart hesabı üzrə çıxarışları həyata keçirilən virtual əməliyyatların çıxarışları ilə müqayisə etmək əhəmiyyətlidir.Kartın itirilməsi, oğurlanması və ya ondan qeyri-qanuni şəkildə

istifadə edilməsindən şübhələnən zaman dərhal bankın müştərilərə yardım xidmətinə xəbərdarlıq vermək və kartı bloklaşdırmaq tələb olunur.Zəng mütləq yazılı şəkildə məktubla təsdiqlənməlidir,hansı ki, bankın istənilən şöbəsində rəsmiləşdirilə bilər.

Kart hesabı üzrə verilənlərin hərəkətinə nəzarət etmək üçün kart üzrə aparılan hər bir əməliyyat üzrə operativ informasiyanı əldə etməyə imkan verən və bütün yerli GSM – mobil operator şəbəkələri üzrə bütün mobil telefonlara SMS məlumatlar şəklində bank kartındakı vəsaitlərin qalığı barəsində informasiyanı verən "Mobil Bank" xidmətlərinə qoşulmaq məqsədəuyğun və rahatdır.Bundan başqa, müştərinin mobil telefon vasitəsilə real zaman rejimində kart üzrə əməliyyatlara nəzarət etməsiylə yanaşı , ona SMS məlumatlar göndərməklə kartını bloklaşdırmaq imkanı təqdim edilir.

Elektron verilənləri mühafizəsi (EVM) sisteminin müumi təhlükəsizlik problemlərini təyin etmək üçün elektron verilənlərin mübadiləsi zamanı sənədlərin hərəkətini nəzərdən keçirək.Burada əsas 3 mərhələni ayırmaq olar:

- Sənədin göndərilməyə hazırlığı;
- Sənədin əlaqə kanalı üzrə ötürülməsi;
- Sənədin qəbulu və onun əks şəklə salınması.

EVM sistemində təhlükəsizlik nöqteyi nəzərindən aşağıdakı zəif yerlər müşahidə olunur:

1. Banklar və ya banklar və onların müştəriləri arasında ödənişlər və ya digər məlumatların ötürülməsi;
2. Məlumatı göndərən və qəbul edən təşkilat daxilində məlumatların emalı;
3. Hesabda toplanmış vəsaitlərə müxtərinin çıxışının olması.

Elektron verilənlər mübadiləsi sitemində ən zəif yerlərdən biri – banklar, banklar və bankomatlar və ya banklar və müştərilər arasında ödənişlər və digər məlumatların ötürülməsidir.Ödəniş və ya digər məlumatların ötürülməsi zamanı aşağıdakı problemlər meydana çıxır:

- Məlumatı qəbul edən və göndərən təşkilatların daxili sistemi elektron sənədlərin qəbulu/göndərilməsinə uyğunlaşdırılmalı və onların təşkilat daxilində emalı zamanı tələb olunan təhlükəsizliyini təmin etməlidir.
- Sənədi qəbul edən və göndərənin qarşılıqlı fəaliyyəti vasitəli şəkildə-əlaqə kanalı vasitəsilə həyata keçirilir.Bu üç tip problem törədir:
    1. Abonentlərin qarşılıqlı tanınması (əlaqənin quraşdırılması zamanı autentifikasiyanın quraşdırılması problemi)
    2. Əlaqə kanalı ilə ötürülən sənədlərin mühafizəsi (sənədlərin tamlığının və məxfiliyinin təmin edilməsi).
    3. Sənədlərin mübadiləsi prosesinin özünün mühafizəsi (sənədin göndərilməsi/çatdırılmasının sübut edilməsi problemi).
- Ümumi halda sənədi göndərən və qəbul edən bir – birindən asılı olmayan müxtəlif təşkilatlara mənsub olurlar.Bu amil tərəflər arasında etibarsızlıq problemini yaradır.Texniki nöqteyi nəzərindən bu problem elektron bank sistemlərinin adekvat təhlükəsizliyinin təminatına görə cavab verən bir neçə mexanizmin köməyilə həll edilir.Bu mexanizmlərin çoxunun işi genişlənmiş xidmət yığımına malik şəbəkə xidmətləri vasitəsilə təmin edilir (Value-Added Network, VAN).EVM – ni həyata keçirən xidmətlər aşağıdakı funksiyaları həyata keçirməlidir:

— Təsadüfi və ya məqsədli səhvlərdən mühafizəsi təmin etmək;

— Topologiyalar,trafikin həcmi, giriş əldə etmə üsulu, avadanlıqların tipi, istifadəçilərin kəmiyyətindəki dəyişikliklərə adaptasiyanın təminatı;

— Müxtəlif istehsalçılar tərəfindən təchiz edilən proqram və apparat vasitələrinin müxtəlif tiplərinin dəstəklənməsi;

— Işin vasiləsizliyinin və diaqnostik pozuntuların təmin edilməsi üçün şəbəkənin dəstəklənməsi və idarəetmənin həyata keçirilməsi;

— Elektron poçt daxil olmaqla EVM – in bütöv tətbiqi məsələlər spektrini reallaşdırmaq;

— Əməkdaşların maksimal mümkün təltəblərinin sayını reallaşdırmaq;

— Ehtiyat surətçıxarma və qəzadan sonra bərpaedilmə xidmətlərinin qoşulması.

EVM sistemlərində, yüksək səviyyəli protokollar səviyyəsində bu sistemlərin ayrı – ayrı düyünlərində mühafizə funksiyalarının reallaşmasını təmin edən aşağıdakı mexanizmlər reallaşdırılmalıdır:

— Abonentlərin bərabərhüquqlu autentifikasiyası;
— Məlumatın qəbulundan/məlumatın müəllifliliyindən imtinanın mümkünsüzlüyü;
— Məlumatın tamlığına nəzarət;
— Məlumatın məxfiliyinin təminatı;
— Kənar sistemlərə çıxışın idarə edilməsi;
— Məlumatın çatdırılmasına zəmanət;
— Məlumatla əlaqədar tədbirlərin qəbul edilməsi və ya imtina edilməsinin mümkünsüzlüyü;
— Məlumatların ardıcıllığının qeydə alınması;
— Məlumatların ardıcıllığının tamlığına nəzarət;
— Məlumat axınının məxfiliyinin təmin edilməsi.

Yuxarıda nəzərdən keçirilən problemlərin həll tamlığı yüksək səviyyədə şifrələnmə sisteminin düzgün seçilməsindən asılıdır.Şifrələnmə sistemi və ya kriptosistem şifrələnmə alqoritmlərinin və açarların yayılması metodlarının məcmusunu ifadə edir.Şifrələnmə sisteminin düzgün və dəqiq seçilməsi aşağıdakılara kömək edir:

— Sənədin içindəkiləri şifrələmək yoluyla onu kənar şəxslərdən gizlətmək (sənədin məxfiliyinin təminatı);
— İnformasiyanın kriptoqrafik bölüşdürmə və uyğun bölüşdürmə açarları protokolu vasitəsilə EVM sisteminin istifadəçi qrupunun sənəddən birgə istifadəsini təmin etmək.Bununla qrupun üzvü olmayan şəxslər sənədə çıxışı əldə edə bilməzlər.

— Əlamətlərə kriptoqrafik nəzarətin daxil edilməsi yoluyla sənəddəki təhriflərin,saxtakarlıqların vaxtında aşkar edilməsi(sənədin tamlığının təmin edilməsi);
— Şəbəkə üzrə əlaqə yaradılan şəxsin həqiqətən də özünü təqdim edən şəxs olmasına əmin olmaq( abonentin/verilənlər mənbəyinin autentifikasiyası).

Qeyd etmək lazımdır ki, EVM sisteminin mühafizəsi zamanı sənədin şifrələnməsinə nisbətən, əlaqə seansının həyata keçirilməsi zamanı onun tamlığının təmin edilməsi və abonentlərin (verilənlərin mənbəyinin) autentifikasiyası daha böyük rol oynayır.Ona görə də bu cür sistemlərə şifrələnmə mexanizmləri adətən vasitəçi rolunu oynayır.Kriptosistemin etibarlılığı bütövlükdə daha çox proses iştirakçıları arasında açarların göndərilmə mexanizmlərindən asılıdır.Açarların göndərilməsi problemi müasir dövrdə ümumi həllərə malik deyil.Hər bir konkret situasiyada banklarda bütün mühafizə edilən informasiya emalının avtomatlaşdırımış sisteminin fəaliyyət xüsusiyyətlərini nəzərə alaraq həll edilməlidir.Bu problemin həllinə bir sıra müxtəlif yanaşmalar mövcuddur.Bunlardan hər birinin xırdalıqlarına daxil olmadan, bunlardan ən əsaslarını nəzərdən keçirək:

Baza/seans açarlar metodu : Bu metodun mahiyyəti ondan ibarətdir ki, burada açarların iyerarxiyası daxil edilir (əsas açar (ƏA) / açarları şifrələyən açar (AA) / verilənləri şifrələyən açar (VA)).İyerarxiya ikisəviyyəli(AA/VA) və ya üçsəviyyəli(ƏA/ AA/VA) ola bilər.Bununla əsas açar iyerarxidana prosesin iştirakçıları arasında qeyri – elektron şəkildə yayılır, bununla da onun etibardan düşməsi və ya tutulması istisna edilir.Standart açarların yayılmasının üç üsulunu təyin edir:vasitəsiz ötürülmə, bölüşdürmə kanalından istifadə edtməklə ötürmə və açarların translyasiyası mərkəzi vasitəsilə ötürmə.Standart, satış mərkəzlərindəki hesab qurğuları və bankomatlar kimi ixtisaslaşmış bank qurğuları arasında açarların bölüşdürülməsində tətbiq olunmur.

Açıq açarlar metodu:Bu metod, açarın bir hissəsinin açıq qaldığı və əlaqə kanalları üzrə açıq şəkildə ötürüldüyü birtərəfli dəyişmələrə əsaslanıb.Bu, şifrələnmə

açarlarının qeyri-elektron üsulla bölüşdürülməsinin bahalı prosedurundan azad edir.

Çıxarılmış açar metodu, satış nöqtəsində hesablama sistemi terminalı ilə bankın kompüteri arasında ötürülən informasiyanın mühafizəsi zamanı tətbiq olunur.Bu metod zamanı hər bir sonrakı tranzaksiyanın şifrələnməsi açarı öncəki açarın və tranzaksiyaların parametrlərinin şəklinin birtərəfli dəyişdirilməsi yoluyla hesablanır.

Tranzaksiya açarı metodu.Bu metod da həmçinin satış nöqtəsində hesablama sistemi terminalı ilə bankın kompüteri arasında ötürülən informasiyanın mühafizəsi zamanı tətbiq olunur.O, çıxarılmış açar metodundan onunla fərqlənir ki, sonrakı tranzaksiya üçün açarın hesablanması zamanı tranzaksiyanın parametrlərindən istifadə olunmur.

İnformasiyanın mühafizəsi üzrə tədbirlərin reallaşdırılmasına qoyulan sərt məhdudiyyətlərdən EVM – in artıq mövcud olan standartının tələbatlarının əlavə edilməsi hesab edilir.Belə ki, tamamilə müdafiə edilmiş möhkəm sistemlər mövcud deyil , hər bir təşkilat özünün EVM sisteminin mühafizə səviyyəsi barəsindəki məsələləri müstəqil şəkildə həll etməlidir: mühafizənin dəstəklənməçi üçün təşkilata əlavə vəsaitlər xərcləmək və ya daimi risk altında fəaliyyət göstərməklə qənaət etmək.

Xüsusi bank şəbəkələri və digər şəbəkələrin, həmçinin milli klirinq sistemlərinin köməyilə elektron bank xidmətlərinin dəstəklənməsi zərurəti bank və onarın müştəriləri arasındakı münasibətlərin radikal dəyişməsinə səbəb olmuşdur.Bütün bank əməliyyatlarını həyata keçirən müxtəlif klirinq sistemləri yalnız son onilliklər ərzində əlverişli olmuşdur,müasir dövrdə isə onlardan hər yerdə istifadə olunur.Onların daxilində olan verilənlər və təlimatlar real zaman rejimində daxil edilir, bölüşdürülür və emal edilir.

Nəğd pul və hesab əməliyyatlarının təhlükəsizliyi istənilən elektron maliyyə xidmətlərinin mühafizəsi üçün zəruri olan tədbirlərin görülməsinə ehtiyac duyur.Xüsusi diqqəti elektron ödəmə sistemlərinə qoşulmuş terminalların mühafizəsinə yönəltmək lazımdır.Əgər bank yüksək risk altında əməliyyatları

aparırsa, onda təhlükəsizliyin təminatı üzrə reallaşdırılan prosedurlar özünə parolla mühafizə, istifadəçilərin çoxsəviyyəli avtorizasiyasını, əməliyyatlara nəzarət və sistem jurnalının aparılması kimi tədbirləri daxil etməlidir.Həmçinin istifadəçilərin fiziki səviyyədə mühafizə edilməli olan kənar qurğu və terminallar olan çıxışına müəyyən sərhədlər qoyulmalıdır.Əlaqə kanalı ilə ötürülən verilənlərin təhlükəsizliyinin təminatı üçün kriptoqrafik metodlardan istifadə etmək zəruridir.Banklarda informasiya emalının avtomatlaşdırımış mərkəzi sistemlərinin təhlükəsizlik sistemi özünə periferiya qurğularına və mərkəzi verilənlər bazasına çıxışa çoxsəviyyəli ciddi nəzarəti də daxil etməlidir.

Fiziki şəxslərin fərdi ödəmələrində təhlükəsizlik təminatından danışmamazdan əvvəl qeyd etmək lazımdır ki,fərdi ödəmələrin həyata keçirilməsinin 3 tipi mövcuddur:

1. Ev telefonu ilə xidmət;
2. Avtomatik kassa apparatları (bankomatlar) ilə ödənişlər;
3. Satış nöqtəsində ödənişlər.

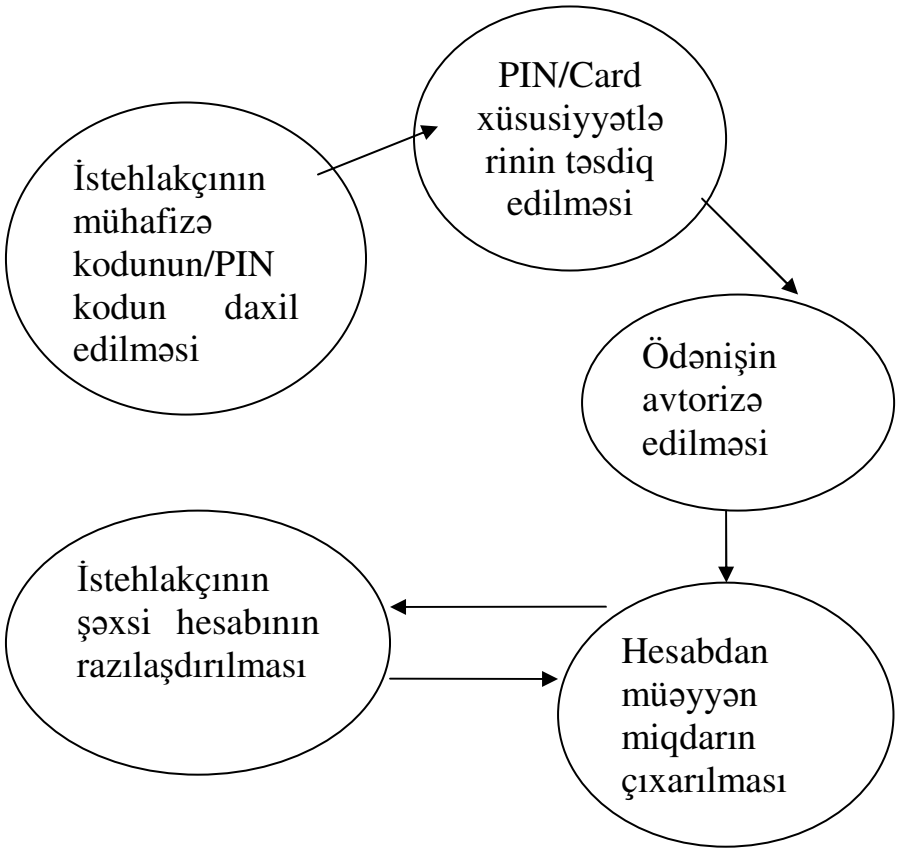
Müsair dövrdə 4-cü tip ödənişlərdən – ümumdünya şəbəkəsi olan internet vasitəsilə maliyyə xidmətindən də istifadə olunur.

Ev telefonları ilə bank xidmətləri müştərilərə evdən ayrılmadan bank və informasiya xidmətlərinə çıxışı əldə etməyə imkan verir.Səs əlaqəsi zamanı ödəniş üçün verilənlərin daxil edilməsi (identifikator, hesabın nömrəsi, ödənişin həcmi) müştəri tərəfindən ya telefonun klaviaturu vasitəsilə ya da ki şifahı şəkildə (hansı ki,həm təhlükəsizlik, həm də texniki nöqteyi nəzərindən daha əlverişsizdir) həyata keçirilə bilər.

Müştərilərə ev şəraitində telefon xidmət sistemlərinə misal olaraq First Direct sistemini göstərmək olar.O,1989-cu ildən bəri fəaliyyət göstərir.Onun əsas fərqi ondan ibarətdir ki, bu sistem hesablamaların həyata keçirilməsi üçün sintez edilmiş səsdən və ya fərdi kompüterdən istifadə etmir.First Direct sistemində əsas diqqət abonentin ilkin identifikasiyasına və yoxlanılmasına yönəldilib.İdentifikasiya üçün müştəri tərəfindən təyin edilən və yalnız ona məlum olan on simvollu paroldan istifadə olunur.Abonentin yoxlanılması operatorla qarşılıqlı əlaqə zamanı həyata

keçirilir.Əvvəlcə operator istifadəçinin parolundan bir və ya bir neçə hərfi soruşur.Əlavə olaraq müştəri bu prosedurda istifadə olunan kodlaşdırılmış sözlə təchiz olunur.Lakin bu sistemdə identifikasiya və autentifikasiya prosesinin detalları sirr olaraq saxlanılır.

Avtomatlaşdırılmış kassa aparatları(bankomatlar) (AKA)– bank heyəti iştirak etmədən müştəriyə xidmət göstərmək üçün təyin edilən ixtisaslaşmış qurğudur.Bu, bank sisteminin nəğd pulların verilməsi üçün təyin edilmiş ən əhəmiyyətli hissəsidir.Bu funksiyadan başqa AKA, müştərinin hesabının yoxlanılması,müştərinin hesabının parametrlərinin dəyişdirilməsi, müxtəlif növ ödənişlərin həyata keçirilməsi, müştərinin sığorta təminatı,fond bazarında qiymtli kağızların kotirovkası,aksiyaların alışı və satışı,valyuta kursları barəsində informasiyanın verilməsi kimi funksiyaları da həyata keçirir.AKA – ın işləmə mexanizmi aşağıdakı şəkildə təsvir edilib:



Satış nöqtəsində alıcının və satıcının hesablamalarını həyata keçirən sistemlər (point-of-sale,POS) ABŞ-da 25 il bundan əvvəl fəaliyyət göstərməyə başlamışdır.Əsasən, bu sistemlərə qoşulmuş bütün terminallar ticarət şikətlərində yerləşdirilir.Bu cür terminalların çoxu supermarketlərdə,mağazalarda və avtodoldurucu mərkəzlərdə yeləşdirilir, belə ki, məhz orada gün ərzində daha çox satış həyata keçirilir.POS sistemləri aşağıdakı xidmətləri göstərir:

— Çeklərin yoxlanılması və təsdiq edilməsi;
— Debet və kredit kartlarına xidmət göstərilməsi və onların yoxlanılması;
— Elektron hesablama sistemlərinin istifadə edilməsi.

POS terminalların iki növü movcuddur.Onların birində təxmin edilir ki,həm satici ,həm alıcı eyni bir bankda hesablara malikdirlər.Ödəniş üçün zəruri olan məlumatlar POS sisteminin terminalları vasitəsilə bank kompüterinə ötürülür,ödəniş həyata keçirilir və pul vəsaitləri alıcının hesabından satıcının hesabına köçürülür.Daha mürəkkəb sistemdə iki və ya daha çox bank iştirak edir.Ödəniş zamanı əvvəlcə alıcının bankı çağırılır,ödəniş həyata keçirilir və hesablama palatasına ötürülmək üçün maqnit lentin yaddaşına yazılır.Hesablama palatası da öz növbəsində ödəniş üçün zəruri olan məlumatları ödənişi kreditləşdirən satıcının bankına ötürür.

POS və AKA sistemlərinin istifadəsi,istifadəçini idenatifikasiya edə və müəyyən uçot məlumatlarını saxlaya biləcək informasiya daçıyıcısının yaradılmasına ehtiyac duyurdu.Bu cür daşıyıcı qismində plastik kartlar çıxış etməyə başladı.Onlardan ən məşhurları Visa və MasterCard kredit kartları, Eurocheque və Postcheque beynəlxalq çek zəmanətləri,American Exspress cə Diner Club-un səyahət və əyləncələrin ödənilməsi üçün kartlardır.

Maqnit kartın üzərində 3 cığırdan ibarət olan maqnit zolaq yerləşdirilmişdir.Onların hər biri müəyyən təyinata malikdir.Kartın ölçüləri,saxlanılan verilənlərin formatı xüsusi standart İSO 7811 tərəfindən təyin edilir.Bu cür kartların həcmi 2 – 16 kilobayt arasındadır.Kartın daxilində yerləşdrilmiş mikrosxemlər həm adi – enerjidən asılı olmayan, həm də kifayət

qədər mürəkkəb mikroprosessorlar ola bilərlər.Bu cür kartlar aşağıdakı funksiyaların yığımını həyata keçirir:

— Mühafizə edilmiş fayl sistemi ilə işləmək imkanı;
— Müxtəlif alqoritmlərin tətbiqi vasitəsilə verilənlərin şifrələnməsi;
— Açar sisteminin aparılması və s.

Bəzi kartlar qeyri-qanuni giriş cəhdləri zamanı "özünü bloklaşdırmaq" rejimini təmin edirlər.İntelektual kartların üstünlüyü ondan ibarətdir ki, onlar böyük həcmdə informasiyaya,saxtakarlığa qarşı davamlılığa və bir sıra proqramlarda istifadə edilmək imkanına malikdirlər.İntelektual kartlar müştərinin identifikasiyası prosesini əhəmiyyətli dərəcədə asanlaşdırmağa imkan verir.Bu,real zaman rejimində AKA-ın işindən və mərkəzləşdirilmiş PIN yoxlamasından imtina etməyə imkan verir.PIN yoxlaması üçün kartın mikroprosessoru tərəfindən reallaşdırılan alqoritm tətbiq olunur.Entelektual kartın fiziki mühafizəsi PIN yoxlamasının nəticəsinin dəqiqliyinə zəmanət verməyə imkan verir.

Bununla yanaşı intelektual kartlar onların yayılmasını məhdudlaşdıran əhəmiyyətli çatışmamazlıqlara malikdirlər.Bunlardan ən əsasları aşağıdakılardır:

— Kartların istehsalının bahalığı;
— Standartlara nisbətən qalınlığın böyük olması.Bunun nəticəsində kartlar adi AKA aparatında oxuna bilmirlər.Bunun üçün xüsusi hesablama qurğularının quraşdırılmasına ehtiyac duyulur.

Plastik kartlar AKA və POS qurğularının əsas informasiya daşıyıcısı kimi cinayətkarlar üçün cəlbedici obyektdir.Bunun üçün bu cür kartları buraxmamışdan əvvəl onların müxtəlif təsirlərdən mühafizə səviyyəsini çox dəqiqliklə işləyib hazırlamaq zəruridir.Bank kartlarına iki əsas tələb mövcuddur: unikallıq və bərpa edilməzlik.Birinci tələbin mahiyyəti ondadır ki, bank tərəfindən buraxılmış bütün kartların içərisində xarakteristikalarına görə 2 eyni kart mövcud olmamalıdır.Buna bənzər kartların yaradılması xüsusi olaraq cinayətkarlar üçün nəzərdə tutulmalıdır.İkinci tələbə əsasən,kartda mövcud olan ilkin informasiya bərpa edilə bilməz.Bu cür tələblərin reallaşdırılması üçün hər bir istehsalçı şirkət özünün və bütün xirdalıqlarının sirr olaraq saxlandığı mühafizə sxemlərini tərtib

etməlidir.Maqnit kartların saxtakarlıqdan mühafizəsinin iki əsas üsulunu nəzərdən keçirək: maqnit su nişanları metodu və "sendviç" metodu.Maqnit su nişanları metodu,kart üzərində yerləşdirilmiş maqnit lent üzərinə xüsusi təsvirlərin yazılmasını nəzərdə tutur.Bu təsvirlər maqnit sahəsinin köməyilə cızılır və qiymətli kağızlarda yerləşdirilən adi su nişanlarının daşıdığı funksiyaları həyata keçirir.İstehsal edilən zaman kart 45 dərəcəli bucaq altında güclü elektromaqnit sahəsinin təsirinə məruz qalır.Daha sonra ona maqnit sahəsini kartın üzərinə xüsusi istiqamətləndirən yazı qurğuları təsir göstərir.Maqnit su nişanları yerləşdirilmiş kartların yoxlanılması xüsusi qirğular tərəfindən həyata keçirilir.Bu mühafizə metodu informasiya zolaqlarında yazılmış informasiyaya təsir etmir, o ,istifadə olunmayan sıfırıncı zolağa 50 – 100 əlavə informasiya dərəcələrini əlavə edir.Bu işarələndən əlavə yoxlama üçün istifadə olunur.

"Sendviç" metodu su nişanları metoduna alternativ olaraq istifadə olunur və mahiyyəti ondan ibarətdir ki,burada bir zolaq müxtəlif səviyyəli maqnitləşmə dərəcəsinə malik sahələrə malikdir, bununla belə daha az maqnitləşməyə malik olan sahə yazma/oxuma başlığına yaxın yerləşdirilir.İnformasiyanın kart üzərinə yazılması üzün güclü maqnit sahəsindən istifadə olunur.İnformasiyanı oxuyan qurğuda kart əvvəlcə silinmə sahəsindən keçir.Bu zaman daha az maqnitləşmə dərəcəsinə malik olan sahədə informasiya silinir,daha güclü maqnitləşmə dərəcəsində esə dəyişməz olaraq qalıq.Daha sonra informasiya zolaqlardan ənənəvi şəkildə oxunur.Bu mühafizə metodunun etibarlılığı iki fərziyyəyə əsaslanıb: birincisi, əgər cinayətkar kartı saxtalaşdırmaq üçün bir qatlı zolaqdan istifadə edərsə, onun üzərində olan bütün informasiya silinmə sahəsi vasitəsilə pozulacaqdır; ikincisi, ikiqatlı zolaqın yazılması üçün, gücünə görə zəruri maqnit sahəsinin yaradılması üçün xüsusi qurğuya ehtiyac duyulacaqdır.

Müasir plastik kartlar bir neçə mühafizə səviyyəsinə malikdirlər.Məsələn, Visa sisteminin kartları 7 mühafizə səviyyəsinə malikdirlər:

1. Mühafizə simvolu ilə birgə Visa kartının tipini identifikasiya edən məhsulun ticarət adı;

2. Panel ətrafında bankın identifikasiya kodlarının çap edildiyi haşıyə yerləşdirilib;
3. Məhsulun identifikasiya nahiyəsində fine – line sahəsi:
   — Mühafizə simvolu;
   — Mühafizə simvolunun yuxarısında bankın identifikatoru;
   — Yalnız ultrabənövşəyi şüalar altında görünən göyərçin (Visa – ın emblemi) təsviri;
   — Göyərçinin üçölçülü haloqramı.

Plastik kartlarla iş zamanı təhlükəsizliyin təminatına qoyulan əsas tələbatlardan biri – bankomatların təhlükəsizliyinin təminatıdır.Maqnit xətli plastik kartlar dünyasında tranzaksiyaların fırıldaqçılıqdan ən etibarlı mühafizəsi üsulu bank emitent tərəfindən kartın sahibinin identifikasiyası üçün PIN-koddan istifadə edilməsidir.Kartın sahibinin malik olduğu məxfi informasiyası onun PIN kodudur.O, 4 – 12 rəqəmdən ibarət olan və yalnız kartın sahibinə və onun bank emitentinə məlum olan ardıcıllığı ifadə edir. PIN kod yüksək risk altında tranzaksiyaların həyata keçirilməsi zamanı tətbiq olunur,məsələn, bankomatlarda kart sahibinə pulların verilməsi zamanı.Pul vəsaitlərin bankomatlarda verilməsi bank əməkdaşlarının iştirakı olmadan həyata keçirilir.Buna görə də nəğd pulların bankomatlardan çıxarılması əməliyyatlarının mühafizəsi üçün plastik kartların adi rekvizitləri kifayət deyil və bunun üçün əlavə məxfi informasiyadan – PIN koddan istifadə olunur.

Bundan başqa, ödəmə sistemlərinin inkişafının ümumi meyli – debet kartları üzrə "alış" əməliyyatlarının aparılması üçün PIN kodlardan daha fəal istifadə olunmasıdır.Bununla hesab edilə bilər ki, bu cür identifikatorun istifadə olunması elektron kommersiyada bütün təhlükəsizlik problemlərini həll edə bilər, lakin bu belə deyil.Təəssüf ki, elektron kommersiyaya əlavə olaraq bu metod klassik şəkildə tətbiq oluna bilməz.

Həqiqətən də, PIN kodun istifadə olunması elə üsulla həyata keçirilməlidir ki, bu məxfi parametr tranzaksiyanın emalının bütün mərhələlərində şifrələnmiş olaraq qalsın.Real həyatda bu tələbat son dərəcə etibarlı üsulla müəyyən

informasiyanı saxlamağa və çevirməyə imkan verən, PIN – PAD adlandırılan və Hardware Security Module – proqram-apparat qurğularına malik olan xüsusi fiziki qurğuların tranzaksiyalarının daxil etmə qurğularında istifadə edilməsi hesabına reallaşdırılır.Bu qurğular xüsusi üsulla mühafizə edilmiş məxfi kommunikasiya açarını saxlayırlar.Kartın sahibi PIN kodu daxil etdikdə, o dərhal kommunikasiya açarı vasitəsilə bağlanır(şifrələnir) və avtorizasiya sorğusunun daxilində xidmətedici bankın hostuna göndərilir.Daha dəqiq desək, PIN kodun özü deyil, kodun yerləşdirildiyi müəyyən elektron "zərf" şifrələnir.Xidmətedici bankın hostunda şifrələnmiş identifikasiya kodu hostun Hardware Security Module'u (xidmətedici bankın kodu həmçinin özünün şifrələnmə qurğusuna malikdir) daxilində ödəmə sisteminin kommunikasiya açarına şifrələnmiş bloka yenidən kodlaşdırılır və emitentə sonrakı təqdimat üçün şəbəkəyə ötürülür.Emitentə doğru gedən yolda PIN kod bir neçə dəfə şəklini dəyişir,lakin bu o qədər də əhəmiyyətli deyil.Burada əhəmiyyətli olan odur ki, PIN kodun klassik emal sxeminə əməl etmək üçün hər bir kart sahibi bütün xidmətedici bankların kriptoqrafik kommunikasiya açarlarını saxlamalıdır, bu isə təcrübədə qeyri-mümkündür.

Klassik sxemin, kart sahibinin PIN kodunun açıq açarla şifrələnməsi ilə birgə assimetrik şifrələmə alqoritmlərinin tətbiq edilməsi vasitəsilə reallaşdırılması mümkün ola bilərdi.Lakin PIN kodun ödəmə şəbəkəsinə təqdim edilməsi üçün onu bütün ödəmə sistemlərində qəbul olunduğu kimi simmetrik açarla şıfrələmək tələb olunur.Lakin, assimetrik kriptalqoritm vasitəsilə şifrələnmiş PIN kodu simmetrik şifrələmə alqoritminə şifrələnmiş PIN koda translyasiya edə biləcək bir dənə də olsun Hardware Security Module qurğusu mövcud deyil.

PIN kodun istifadəsi üzrə digər – qeyri-klassik metod mövcuddur.Məsələn, kart sahibinin kompüterinə, yalnız emitent və onun bankına məlum olan açarda yerləşdirilən tranzaksiyadan tranzaksiyaya dəyişən bəzi dunamik məkumatları və PIN kodu şifrələmək mümkündür.Bu cür yanaşma gizli açarların bölüşdürülməsi məsələsinin həllini tələb edir.Bu məsələ son dərəcədə asan deyil (aydındır ki,hər bir kart sahibinə məxsus individual açar mövcud olmalıdır) və əgər bu məsələ həll edilirsə də, onda onun həllinin istifadə edilməsi kart sahibinin autentifikasiya

metodları vasitəsilə PIN kodun yoxlanılması ilə müqayisədə daha effektiv digər metodlar üçün əhəmiyyətli ola bilər.

Eyni zamanda PIN kodun yoxlanılması ideyasi, verilənlər bazasının STB Card prosessorunun hostunda saxlandığı kartlar üzrə həyata keçirilən tranzaksiyalarda təhlükəsizliyin yüksəldilməsi məqsədilə reallaşdırılmışdır.Ümumilikdə STB Card aşağıdakı sxemi reallaşdırır.Öz verilənlər bazası kartlarını STB Card –ın hostunda yerləşdirən emitentlər –kart sahibləri PIN2 adlandırılan əlavə PIN kod əldə edə bilərlər.Bu kod, kartın sahibinə ötürülən PIN-zərfdə (bank emitent tərəfindən,emitenləşən karta aid edilən məxfi informasiyanın saxlanması üçün istifadə edilən xüsusi kağız zərf) çap edilmiş 16 onaltıonluqlu rəqəm ardıcıllıqdan ibarətdir.O, emitent bank tərəfindən,yalnız kartın emitentinə məlum olan gizli açarı istifadə edən və kartın nömrəsinə tətbiq edilən simmetrik şifrələmə alqoritmi vasitəsilə müəyyən edilir.

Daha sonra STB Card bankının xidmət göstərdiyi ticarət müəssisələrinin birində elektron kommersiya tranzaksiyalarının həyata keçirilməsi zamanı,kartın sahibindən müştəri haqqında məlumatların əldə edilməsi prosesində PIN2 kodu üzrə informasiya tələb olunur.Müştəri PIN2 kodunu formaya daxil edir və onu ticarət müəssisəsinə göndərir.Burada vacib qeyd etmək lazımdır ki,kartın sahibi əslində mühafizə edilmiş SSL – sessiyasında ticarət müəssisəsi ilə deyil,virtual POS –serverlə dialoq aparır.Ticarət müəssisəsi məhz POS –server vasitəsilə fəaliyyət göstərir.Hazırda STB Card sistemi ASSİST serverindən istifadə edir.

STB Card sxeminə qayıtmaqla qeyd etmək istəyərdim ki, əlbəttə ki, müştəri tərəfindən doldurulmuş formada PIN2 mövcud deyil,əslində bütün proses aşağıdakı şəkildədir:Ticarət müəssisəsi,daha dəqiqliklə Assist serveri, STB Card bankının kartı ilə iş gördüyünü təyin etdikdən sonra kartın sahibinə müəyyən simmetrik şifrələmə alqoritmlərini reallaşdıran və imzalanmış Java-appletə malik olan formanı ötürür.Bununla PIN2, bu şifrələmə alqoritminin gizli açarı rolunu oynayır,şifrələnən verilənlər isə xeş funksiyasının kartın nömrəsinə,tranzaksiyaların məcmusuna və tarixinə, ticarət müəssisəsinə generasiya edilmiş təsadüfi x rəqəminə tətbiq edilməsi nəticəsində meydana gəlir.Beləliklə,

kart sahibi tərəfindən doldurulmuş formada yalnız PIN2 açarında tranzaksiyalara aid yuxarıda sadalanmış verilənlərin şifrələnmiş nəticəsi mövcud olur.

Daha sonra, ticarət müəssisəsi xidmətedici bankın hostuna ötürülən və tranzaksiyaya aid "standart" verilənlərdən başqa təsadüfi x rəqəmini və şifrələnmə nəticəsini özündə əks etdirən avtorizasiya məlumatını formalaşdırır.Kartın emitenti ticarət müəssisəsinin məlumatını əldə etdikdən sonra kartın mömrəsi üzrə PIN2-ni müəyyən edir və daha sonra kartın nömrəsi, tranzaksiyaların məcmusu və tarixi,həmçinin təsadüfi x rəqəminə görə PIN2 açarında bu verilənlərin şifrələmə nəticəsini müəyyən edir.Əgər əldə edilən kəmiyyət ticarət müəssisəsinin məlumatındakı analoji kəmiyyət ilə üst-üstə düşərsə,onda PIN kodunun verifikasiyası uğurla həyata keçirilmş hesab edilir.Əks halda tranzaksiya qəbul edilmir.

Beləliklə, STB Card sistemində qəbul edilmiş PIN kodun yoxlanılması texnologiyası əslində təkcə müştərinin dinamik autentifikasiyasını təmin edilmir, həmçinin tranzaksiyalara aid bəzi məlumatların (tranzaksiyaların məcmusu,karın nömrəsi və s.)müştəridən bank emitentə ötürülməsi zamanı onların modifikasiya olunmasından mühafizəsinə zəmanət verir.

Həyata keçirilmiş təhlil əsasında ödəmə sistemləri elektron kommersiyada tranzaksiyaların həyata keçirilməsi sxeminə qarşı zəruri təhlükəsizlik səviyyəsini təmin edəcək tələblər irəli sürmüşdür.Bu tələblər aşağıdakılara gətirilir:

- Satışın iştirakçılarının – alıcının,ticarət nümayəndəsinin və onun xodmətedici bankının autentifikasiyası.Alıcının (satıcının) autentifikasiyası dedikdə, verilən kart sahibinin həqiqətən də verilən ödəmə sisteminin hər hansı bir emitent iştirakçısının müştərisi olduğunu sübut edən prosedur başa düşülür.
- Elektron kommersiya tranzaksiyasının həyata keçirilməsi zamanı istifadə olunan ödəmə kartının rekvizitləri (kartın nömrəsi,onun fəaliyyət dövrü, CVC2/CVV2 və s.) ticarət müəssisəsindən gizli olaraq saxlanılmalıdır.
- Elektron kommersiya tranzaksiyasının bütün iştirakçıları üçün tranzaksiyadan imtinanın mümkünsüzlüyü,yəni bütün iştirakçılarda alışın

(satışın,sifarişin və ya ödənişin) həyata keçirilməsi barəsində danılmaz sübutun mövcud olması.

Elektron alışın ödənişinin həyata keçirilməsinə görə mağazaya zəmanətin verilməsi – yəni ticarət müəssisəsində sifarişin həyata keçirilməsinə aid sübutun mövcudluğu.

## 2.2.İqtisadiyyatın elektron idarəedilməsində təhlükəsizlik məsələləri və rəqəmsal sertifikatlar

İnternet vasitəsilə elektron əməliyyatları həyata keçirən zaman sahibkarlar qısa müddət ərzində yüksək rəqabət qabiliyyətini əldə edə bilərlər,çünki, onların müştərisi bütün dünyadır.Lakin Web daxilində təhlükəsizlik nöqteyi nəzərindən bəzi nyuanslar mövcuddur ki, onları da riskin qarşısını almaq üçün mütləq nəzərə almaq lazımdır.Müştəri yalnız özünün şəxsi informasiyasının (kredit kartının nömrəsi, maliyyə verilənləri və s.) mühafizə olunacağına əmin olduqdan sonra onu Web vasitəsilə göndərməyə hazır olacaqdır.

Qlobal informasiya cəmiyyəti yol ayrıcındadır.Bəzi ölkələr aqrar və ya sənaye bazasından yeni informasiya iqtisadiyaytı bazasına keçməklə informasiya texnologiyalarını öz inkişfalarının hərəkətverici qüvvəsinə çevirə bilər.Digərləri isə əsas addımları atmaqda gecikə və texnoloji yarışda geri qala bilər.

McConnell International Risk E-Business şirkəti tərəfindən işlənib hazırlanan hesabatda informasiya iqtisadiyyatına hazırlıq səviyyəsinə görə 42 ölkə göstəriciləri təhlil olunub müqayisə edilmişdir.Bu hesabatda diqqətə alınan ən əsas göstəricilərdən biri informasiya təhlükəsizliyi faktoru idi.

İnformasiya iqtisadiyyatına hazırlıq üzrə əhəmiyyətli dərəcədə hesab edilən aspekt informasiya təhlükəsizliyinin yüksək səviyyəsi ilə müəyyən edilir.İnformasiyanın yaradılması, saxlanması və yayılması proseslərinin mühafizəsi və qanunvericilik bazasının zəifliyi elektron biznesin həyata keçirilməsi üçün əlverişsiz mühiti formalaşdırır.İntelektual mülkiyyətin aşağı səviyyəli mühafizəsi proqram təminatının işlənib hazırlanması sənayesinin inkişaf tempinə mane ola bilər.Şəxsi verilənlərin qeyri – adekvat mühafizəsi informasiya mübadiləsinin həyata keçirilməsi üçün əngəl yaradır. Elektron imzaların qəbul edilməsindən imtina və ya verilənlərin şifrələnməsinə qadağaların qoyulması biznesin həyata keçirilməsinin yeni üsullarına qarşı etibarı sarsıdır.Elektron ticarət sferasında əsas informasiya elementləri özünə aşağıdakıları daxil edir:

- Hüquqi mühafizənin səviyyəsi və intelektual mülkiyyətin, xüsusilə də proqram təminatının mühafizəsi sagəsində inkişafın səviyyəsi;
- Elektron piratlılığa qarşı istiqamətlənmiş səylərin səviyyəsi;
- Kompüter cinayətkarlılığına qarşı işlərin açılmasına, elektron imzaların avtorizasiyasına və açıq açarların istifadəsi üçün infrastrukturların yaradılmasına istiqamətlənmiş hüquqi sistemin effektivliliyi və möhkəmliyi.

Kiber-cinayətkarlıq qarşısında bir sıra ölkələr, gözləndiyi kimi, müəlliflik hüququ, şəxsi mülkiyyət və istehlakçı hüquqlarının standart mühafizə qanunlarına arxayın olacaqlar.

Bu hesabatda təhlil edilən ölkələrdən bəziləri artıq elektron imzaları qəbul edən qanunlar qəbul ediblər, lakin elektronm kommersiyaya doğru addımlayan ölkələrin çoxu şifrələnmənin istifadəsini tənzimləməyə qadir deyil.Yalnız bəzi ölkələr təhlükəsizlik alətlərinin geniş miqyasda tətbiq edilməsi üçün əhəmiyyətli olan açıq açar infrastrukturunun yaradılması məqsədilə milli səviyyədə əlaqələndirilmiş səylər göstərirlər.Rusiya və Ukraynada hələ də intelektual mülkiyət sferasında qanunvericilik bazası zəif olaraq qalmaqdadır.Bu da informasiya mübadiləsinin və elektron biznesin həyata keçirilməsi üçün ciddi maneə törədir.

İntelektual mülkiyyətin lazımi səviyyədə mühafizəsinin təşkili yerli elektron biznesin inkişafına şərait yaradır.Lakin tədqiq edilən ölkələrin çoxunda kompüter piratlılığı əvvəlki kimi ciddi problem yaratmaqda olaraq qalır.

McConnell International Risk E-Business şirkəti aşağıdakı regionlarda araşdırmalar aparmışdı və aşağıdakı nəticələr əldə etmişdir:

**Latin Amerikası**: Argentina, Braziliya, Venesuella, Kosta-Rika, Meksika,Peru,Çili və Ekvador.

Bütövlükdə , Latın Amerikasında elektron kommersiyaya investisiyaların cəlb edilməsi və onun inkişaf etdirilməsi üçün əlverişli şərait mövcuddur.Buna baxmayaraq, bu ölkələrdə online biznesin aparılması üçün etibarlı bünövrə mövcud deyil.Bu da ki qismən informasiy təhlükəsizliyi təminatı sistemində müəyyən qeyri-adekvat dəyişikliklərin meydana gəlməsinə səbəb olur.İT sənayesi ldierlərinin forlamaşmasının fəal prosesi və böyük insan kapitalının mövcud

olmasına baxmayaraq, bu regionun ölkələri İnternetə giriş imkanlarının aşağı səviyyəsi və elektron komemrsiyaya maliyyə qoyuluşlarının çatışmaması məsələsinə diqqət yetirməlidirlər.

**Asiya:** Vyetnam, Hindistan, Çin, Malayziya, Pakistan, Tayland, Tayvan, Filippin və Cənubi Koreya.

Bu regionun əsas xüsusiyyəti ondan ibarətdir ki, birada 1997-1998-ci illər ərzində baş vermiş böhranın ağır nticələrini aradan qaldırmaq üçün elektron kommeriyaanın cəlb edilməsi üçün əhəmiyyətli dərəcədə səylər göstərən bəzi ölkələrin mövcud olmasıdır.Lakin, burada informasiya təhlükəsizliyi təminatı üzrə adekvat vasitələrin mövcud olmaması yeni iqtisadiyyata keçid yolunda ciddi maneə yaradır.Bundan başqa, əhalinin sayının çox və ərazinin geniş olması bu ölkələrin informasiya iqtisadiyyatında iştirakını təmin edir.

**Mərkəzi və Cənubi Avropa:** Bolqarıstan, Macarıstan, Yunanıstan, İspaniya, İtaliya, Latviya, Litva, Polşa, Portuqaliya, Rusiya, Rumıniya, Slovakiya, Sloveniya, Türkiyə, Ukrayna, Çexiya Respublikası və Estoniya.

Mərkəzi və Cənubi Avropa – informasiya iqtisadiyyatına keçid üzrə dünya ölkələri sırasında hazırlılığına görə ən qabaqcıl yerləri tutur.Xüsusilə də, əhalinin yüksək savadlılığı və informasiya təhlükəsizliyinin münasib səviyyəsi dəyişikliklərin həyata keçirilməsi riskini əhəmiyyətli dərəsədə azaldır.Bununla belə, bu regionun ölkələrində hələ də elektron kommersiyanın, xüsusilə də, adekvat hüquqi bazanın yaradılması ilə əlaqədar olan bir sıra həll edilməmiş məsələlər qalmaqdadır.

**Yaxın Şərq və Afrika:** Qana, Misir, Kenya, Nigeriya, Səudiyyə Ərəbistanı, Tanzaniya və CAR.

Bütün təhlil edilən dörd region arasında Yaxın Şərq və Afrika ölkələrinin yeni informasiya iqtisadiyyatına keçidi ən problematik olaraq sayılır.Hətta informasiya texnologiyalarından birgə istifadəyə meyilliliyin mövcud olmasına baxmayaraq, mövcud olan zəif infrastruktur digər sahələrdə islahatların həyata keçirilməsinə ciddi sədd yaradır.

Rusiya və Ukraynanın informasiya iqtisadiyyatına keçid üzrə daha hazırlıqlı olan ölkələr siyahısını daxil olmasına baxamyaraq, onların bu sahədə hələ çox işlər görməyə ehtiyacları var.Yüksək ixtisaslaşdırılmış insan kapitalının mövcudluğuna baxmayaraq Rusiyanın hakimiyyətinin əhalinin internetə çıxış imkanlarını genişləndirməsi zəruridir. Bu məsələlərin həlli hal-hazirda Ukraynanın da qarşısında durur.

Müasir dövrdə qlobal elektron kommersiyanın iki modeli inkişaf edib geniş yayılmışdır:B2B (Business-to-Business) – şirkətlər arasındakı ticarət münasibətləri və B2C (Business-to-customer) – şirkət və alıcılar arasındakı tcarət münasibətləri.

İnternet vasitəsilə elektron kommersiyanın dövriyyə həcminin nəhəngliyi elektron kommersiyanın iqtisadi təhlükəsizliyin təminatı problemi ilə müəyyən olunur.Əgər təhlükəsizlik səviyyəsi bu günkü səviyyədə qalarsa, onda elektron kommersiyanın dünya üzrə dövriyyəsi azalmağa doğru gedəcəkdir.Buradan belə nəticəyə gəlmək olar ki, məhz elektron kommersiyanın mühafizəsinin aşağı səviyyəsi onun inkişafını ləngidən əsas faktorlardan biridir.

Elektron kommersiyanın iqtisadi təhlükəsizlik təminatı probleminin həlli ilk növbədə onda istifadə olunan informasiya texnologiyalarının mühafizəsi, yəni informasiya təhlükəsizliyinin təminatı məsələlərinin həlli ilə əlaqədardır.Elektron kommersiya çoxlu sayda müxtəlif funksiyaları birləşdirir.Orada alıcılar və satıcılar arasındakı əlaqənin, təqdim etmə metodlarının, sifarişin formalaşdırılması və müzakirəsinin,sövdələşmə şərtlərinin təyin edilməsinin, məhsul və xidmətlərin satış ardıcıllığının təşkili üçün, həmçinin ödənişlərin həyata keçirilməsi prosesinin reallaşdırılması üçün yeni texnologiyalardan istifadə olunur.

Müasir dövrdə elektron biznesin təşkili üçün bir sıra proqram həlləri mövcuddur.Azərbaycanda elektron kommersiyanın inkişafını aşağıdakı amillər ləngidir:

- İnfokommunikasiya infrastrukturunun zəif inkişaf etməsi;
- Cinayətkarlar qarşısında onun yüksək zəifliyi;
- Rəqabət mübarizəsinin artan səviyyəsi.

Göründüyü kimi yuxarıda sadalanan bütün maneələr informasiya təhlükəsiliyi ilə birbaşa əlaqədardır.Təəssüflər olsun ki, elektron kommersiya müəssisələrinin rəhbərləri yalnız resurslarının informasiya hücumlarına məruz qalmasından sonra informasiya təhlükəsizliyinin ciddiliyini və mühafizənin təşkilinin əhəmiyyətliliyini lazımi dərəcədə dərk etməyə başlayırlar.

Elektron kommersiya müəssisəsinin iqtisadi mühafizəsinin təminatının bir neçə yolunu nəzərdən keçirək.Özüdə bu məsələ xüsusi olaraq iştirakçıların tranzaksiyanın təşkil olunması prosesinə qarşı etibarının təmin olunmasına istiqamətlənmir: onların təhlükəsizliyinin elektron biznesin həyata keçirilməsinin hər bir mərhələsində təmin olunması əhəmiyyətlidir.

Elektron kommersiya prosesi genişlənmiş şəkildə yeddi mərhələni əhatə edir:

- Şirkətin serverində xidmət və ya məhsulun seçilməsi və sifarişin rəsmiləşdirilməsi;
- Sifarişin mağazanın verilənlər bazasına daxil edilməsi;
- Sifariş edilən məhsulun mərkəzi verilənlər bazasından əlverişliliyinin yoxlanılması;
- Sifarişin vaxtlı vaxtında çatdırılmasının mümkünsüzlüyü və sifariş olunan məhsulun yoxluğu zamanı onun korreksiyası ilə əlaqədar xəbərdarlıq;
- Sifarişin təsdiq edilməsi və sifariş olunan məhsulun mövcud olduğu təqdirdə onun verilənlər bazasına yerləşdirilməsi;
- Real zaman rejimi daxilində müştəri tərəfindən sifarişin ödənilməsi;
- Sifariş olunan məhsulun müştəriyə çatdırılması.

Elektron kommersiyanı hər bir mərhələdə aparan şirkəti aşağıdakı təhlükələr gözləyə bilər:

- Elektron mağaza serverinin web-səhifəsinin dəyişdirilməsi, nəticədə, müştəri barəsində məlumatlar, xüsusilə də onun kredit kartlar kənar şəxslər üçün əlverişli olur;
- Saxta sifarişlərin yaradılması və elektron mağazanın işçiləri tərəfindən müxtəlif formalı cinayətkarlar, məsələn, verilənlər bazası ilə aparılan

manipulyasiyalar ( statistika göstərir ki, kompüter insidetnlərinin yarısından çoxu maöazanın öz işçilərinin fəaliyyəti ilə əlaqədardır);

- Elektron kommersiya şəbəkələri üzrə ötürülən verilənlərin tutulması;
- Cinayətkarların şirkətin daxili şəbəkəsinə daxil olması və elektron mağazanın komponentlərinin nüfuzdan salınması.
- Xidmətdən imtina tipli hücumların reallaşması və elektron kommesiyanın fəaliyyətinin pozulması.

Bu cür təhlükələrin reallaşdırılması nəticəsində şirkət müştərilərin etibarını itirir, potensial və ya həyata keçirilməmiş sövdələşmələrdən pul itirir,elektron mağazanın fəaliyyəti pozulur,funksionallaşdırılmanın bərpa olunmasına isə əlavə pul vəsaitləri, insan resursları və zaman sərf olunur.

Əlbəttə ki, İnternet vasitəsilə ötürülən informasiyanın tutulması ilə əlaqədar olan təhlükələr yalnız elektron kommersiyaya xas deyil.Xüsusilə bu cür təhlükələrin elektron kommersiyada tətbiqi bu sistemdə böyük iqtisadi əhəmiyyətə malik olan informasiyanın – kredit kart nömrələrinin, hesab nömrələrinin, müqavilələrin məzmununun və s.in dövr etməsini nümayiş etdirir.

Xaricdə elektron biznesdə informasiya təhlükəsizliyi problemi ilə müstəqil konsorsium – İnternet Security Task Force (ISTF) məşğul olur. ISTF – elektron biznes, internet–xidmət provayderləri və informasiya təhlükəsizliyi vasitələrinin təchizatı ilə məşğul olan şirkətlərin ekspertləri və nümayəndələrindən təşkil olunan ictimai təşkilatdır. ISTF konsorsiumu informasiya təhlükəsizliyinin on iki sahəsini ayırır, hansılara ki elektron biznes təşkilatçılarının hər biri ilk növbədə diqqət yetirməlidir:

- İdentifikasiya edilən informasiyanın təsdiqlənməsinin obyektiv mexanizmi;
- Özəl və şəxsi informasiyaya malik olma hüququ;
- Təhlükəsizlik hadisələrinin müəyyən edilməsi;
- Korporativ perimetrin mühafizəsi;
- Hücumlardan mühafizə;
- Potensial təhlükələrin yoxlanılması;
- Çıxış imkanına nəzarət;

- İnzibatçılıq;
- Hadisələrə qarşı reaksiya.

Biznesin bütün yarana biləcək iqtisadi nəticələrlə birgə fasiləsiz olaraq fəaliyyət göstərməsi yuxarıda sadalanan sahələrin mühafizəsindən asılıdır.Təhlükəsizlik artıq biznesin əlavə aspekti rolunda çıxış etmir: hətta əgər təhlükəsilik və etibarlılıq sistemi 97%-ə qədər təmin olunsa belə bu o demək olacaqdır ki, biznes üçün il ərzində 293 saat itiriləcəkdir.Əlbəttə, informasiya təhlükəsizliyi məsələləri ilə bu sahənin mütəxəssisləri məşğul olmalıdırlar, lakin mülkiyyət formalarından asılı olmayaraq bu və ya digər təsərrüfat subyetinin iqtisadi təhlükəsizlinə görə cavab verən müəssisə, təşkilat və ya dövlət hakimiyyət orqanlarının rəhbərləri təhlükəsizlik problemi məsələlərini daimi olaraq diqqət qarşısında saxlamalıdırlar.Onlar əsasən aşağıdakı kompleks informasiya təhlükəsizliyi sisteminin təşkilati komponentlərini diqqətə almalıdırlar:

- Kommunikasiya protokolları;
- Kriptoqrafiya vasitələri;
- Avtorizasiya və autentifikasiya mexanizmlərini;
- Ümumistifadə şəbəkələrindən işçi yerlərinə çıxışa nəzarət vasitələri;
- Antivirus kompleksləri;
- Hücumların aşkar edilməsi proqramları və audit;
- İstifadəçilərin şəbəkəyə giriş imkanının, həmçinin açıq IP–şəbəkələri üzrə məlumatların və verilənlərin təhlükəsiz mübadiləsinin mərkəzi idarə edilməsi vasitələri.

Müxtəlif istehsalçılar tərəfindən təqdim edilən elektron kommersiyanın tətbiqi həllərinin detallı təhlili nümayiş etdirir ki, bu əlavələr təhlükəsizlik və mühafizə funksiyalarının yalnız müəyyən hissəsini reallaşdırır.

Bu cür sistemlərdə bir qayda olaraq, aşağıdakılar reallaşır: xüsusi protokollardan istifadə edilməklə mühafizə olunmuş kommunikasiya funksiyaları; verilənlərin tamlığına nəzarət funksiyası; ticarət sisteminə istifadəçilərin giriş imkanının avtorizasiyası və autentifikasiyası; və daha nadir hallarda ötürülən verilənlərin məxfiliyinin təminatı funksiyası. Lakin bu tətbiqi sistemlərdən biri

şəbəkənin və bütün informasiya sisteminin tamlığına nəzarəti həyata keçirməyə, daxili şəbəkədən avtorizasiya olunmamış müdaxilədən sistemi mühafizə etməyə və həmçinin ümumistifadə şəbəkələrindən sistemi avtorizasiya olunmamış çüdaxilədən mühafizə etməyə qadir deyil.

Bir qayda olaraq, elektron kommersiyanın tətbiqi həlləri:

- İstifadəçilərin öz iş yerlərinə çıxışına nəzarət sistemləri ilə inteqrasiya edilmir;
- Onlardan heç biri "troyan proqramları"ndan və digər tip viruslardan mühafizə olunmayıb;
- Bundan başqa, icazəsiz girişin aşkar edilməsi və audit prosesləri ticarət sistemi ilə münasibətdə xarici mexanizmlər vasitəsilə reallaşdırılır.

Beləliklə, belə bir nəticəyə gəlmək olar ki, elektron kommersiya sahəsində istifadə olunan tətbiqi həllərin heç biri informasiya mühafizəsinin inteqrasiya edilmiş kompleks idarəetmə sistemini təmin etmir, həmçinin onların hamısı informasiyanın etibardan salınması, təhrifi, itkilər və s. riskinə məruz qalırlar.

ISTF tövsiyyələrinə əsasən Elektron biznes və ticarətdə informasiya təhlükəsizliyi sisteminin işlənib hazırlanmasınıın ən birinici və vacib mərhələsi ümumistifadə şəbəkələrinə və ümumistifadə şəbəkələrindən çıxışın, həmçinin şəbəkələrarası ekranlar və özəl mühafizə edilmiş virtual şəbəkələr (VPN) vasitəsilə reallaşan təhlükəsiz kommunikasiya mexanizmlərinin idarə edilməsi mexanizmləri olacaqdır.Bunları mühafizə sisteminin (PKİ – açıq açar infrastrukturu) əsas açar informasiyasının idarə edilməsi və inteqrasiyası vasitələri ilə müşayiət etməklə, nisbətən tam,mərkəzləşdirilmiş formada idarə edilən infromasiya təhlükəsizliyi sistemi əldə olunur.

Növbəti addım özünə ümumi struktura inteqrasiya edilmiş istifadəçilərin birdəfəli giriş və avtorizasiya sistemi (Single Sign On) ilə birgə çıxışa nəzarət vasitələrini daxil edir.

Antivirus mühafizəsi, audit və hücumların aşkar edilməsi vasitələri inteqrasiya edilmiş bütöv təhlükəsizlik sisteminin yaradılmasını tamamlayır, əgər söhbət məxfi verilənlər üzərində işdən getmirsə.Bu halda həmçinin paralel olaraq verilənlərin

kriptoqrafik mühafizə vasitələri və elektron – rəqəmsal imzalara da ehtiyac duyulacaqdır.

Bu mexanizmlərdən yalnız bəziləri təchizatçı tərəfindən hazır elektron biznes və kommeriya əlavələrinə quraşdırılır.Elektron kommersiya və biznesin təhlükəsizliyi və informasiya mühafizəsinin yaradılması üzrə qalan və əsas işi informasiya təhlükəsizliyi üzrə mütəxəssislər – bi sahənin sistem inteqratorları öz üzərilərinə götürməlidirlər.Onalrın iştirakı olmadan informasiya mühafizəsi sistemi həmişə müəyyən qüsurlara malik olacaqdır.

Elektron kommersiyada təhlükəsizliyin təminatı üsullarından biri VISA Address Verification System (AVS) metodudur.Bu metodunmahiyyəti ondan ibarətdir ki, burada ticarət müəssisəsi müştəridən verifikasiya məqsədilə avtorizasiya sorğularında kart sahibinin bank emitentinə istiqamətlənən Cardholder Billing Adress (müştərinin, öz emitent bankından müəyyən zaman periodu ərzində öz kartı üzrə həyata keçirdiyi tranzaksiyalarla bağlı hesabatlarla əlaqədar informasiyanı əldə etdiyi ünvan) – in parametrlərini tələb edir.AVS metodunun tətbiq edilməsi üçün Cardholder Billing Address parametrlərinin xidmətedici bank tərəfindən kartın emitentinə göndərilən avtorizasiya sorğularında dəstəklənməsi zəruridir.Son zamanlara qədər AVS, VİSA sistemində yalnız amerika bankları tərəfindən dəstəklənirdi.AVS texnologiyası artıq neçə illərdir ki, amerika bankları tərəfindən uğurla istifadə olunur və 2001-ci ilin aprelindən Böyük Britaniya banklarında da tətbiq olunmağa başlanmışdır.

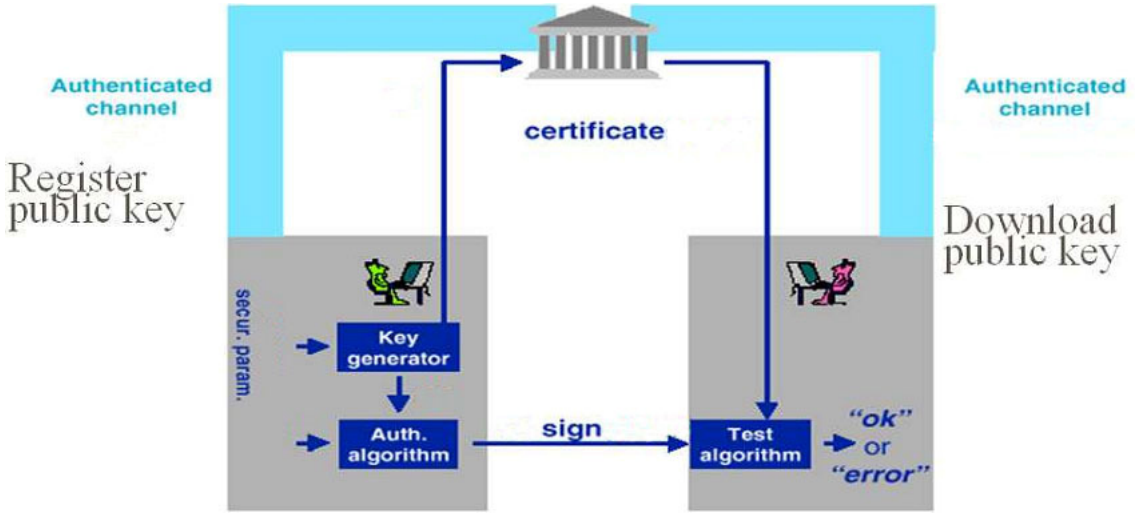
Lakin AVS metodunun iki çatışmamazlığı mövcuddur.Birincisi, o CVC2/CVV2 – in yoxlama metodu kimi statikdir və uyğun olaraq yeni parametrin cinayətkarların əlinə düşməsi sadəcə zamandan asılıdır.İkincisi bu metod yalnız Visa sistemi tərəfindən dəstəklənir və dünyada bu ödəmə sisteminin payına elektron komersiyada həyata keçirilən bütün tranzaksiyaların 50%-dən çoxunun düşməsinə baxmayaraq bu hələ İnternetdə ödəmələr bazarının hamısı demək deyil.Başqa sözlə AVS metodu bu gün üçün ən universal metod hesab edilmir.

Elektron kommersiyda təhlükəsizliyin təminatı vasitəsi kimi ən çox istifadə olunan metodlardan biri elektron rəqəmsal sertifikatlar hesab edilir.Elektron

rəqəmsal sertifikat özlüyündə müəyyən bir elektron passportu ifadə edir.Rəqəmsal sertifikat, müştəri (adı,müştərinin identifikatoru), müştərinin açıq açarı, sertifikatı hazırlamış təsdiqedici mərkəz, sertifikatın seriya nömrəsi, fəaliyyət müddəti və s. ilə bağlı informasiyanı daşıyır.Rəqəmsal sertifikat fayl şəklində disketə yazılır və istfadçinin hər dəfə sistemə daxil olduğu zaman istifadə olunur.Elektron rəqəmsal sertifikatlar Rəqəmsal Sertifikatlar Mərkəzi tərəfindən yaradılır və təsdiqlənir. Beləliklə sistemə çıxış imkanına yalnız bankda müəyyən yolxmaları keçmiş sertifikasiya edilmiş istifadəçilər malik ola bilərlər.

Açıq açar sertifikatı (rəqəmsal sertifikat) dedikdə, açıq açar, həmçinin istifadəçini birmənalı identifikasiya etməyə imkan verən açarı ilə bağlı informasiyaya malik olan elektron sənəd başa düşülür.

Serfifikatlar Təsdiqedici Mərzəkin elektron imazsıyla imzalanır, bununla da azıq açarın sertifikatda onun sahibini verilənlərinə uyğunluğu təsdiqlənir.Təsdiqedici mərkəzin açıq açarına malik olan hər kəs təsdiqedici mərkəzin imzasını yoxlaya və yoxlanılan sahibin açıq açarının həqiqiliyində əmin ola bilər, əlbəttə ki, əgər sertifikatı təqdime etmiş təsdiqedici mərkəzə etibar edirsə.Rəqəmsal sertifikatların fəaliyyət mexanizmini sxematik olaraq aşağıdakı kimi göstərmək olar:



Rəqəmsal sertifikar – bir növ sahibkarlıq fəaliyyətinə görə verilən lisenziyanın ekvivaln\enti rolunda çıxış edir.Rəqəmsal sertifikatlar etibar qazanmış və müəyyən səlahiyyətlərə malik malik olan üçüncü tərəf (Certificate Authority, CA) tərəfindən verilir.Bu cür rəqəmsal sertifikatlara misal olaraq bu sahədə dünya lideri adını qazanmış VeriSign şirkətinin təqdim etdiyi rəqəmsal sertifikatları göstərmək olar.Sertifikatı təqdim edən səlahiyyətli tərəf sahibkarların öz adlarında və URL ünvanlarından istifadə etmək hüququna zamin olur.Lakin, rəqəmsal sertifikatlar fiziki şəxslər tərəfindən də əldə edilə bilər.

VeriSign rəqəmsal sertifikatı Web-ə əsaslanmış kommunikasiyaların təhlükəsizlik standartı hesab edilən SSL texnologiyası ilə birgə fəaliyyət göstərir.Veb-server rəqəmsal sertifikatla yalnız onun Apache Freeware, C2Net, IBM, Lotus, Netscape, Microsoft və ya hər hansı bir digər istehsalçı tərəfindən hazırlandığı təqdirdə işləyə biləcəkdir.

Rəqəmsal sertifikat quraşdırıldıqdan sonra server alıcının brauzeri ilə təhlükəsiz əlaqə kanalı quraşdırmaqla SSL protokolunu avtimatik olaraq aktivləşdirir.Bunun vasitəsilə sayt artıq Netscape Navigator, Microsoft Internet Explorer və bəzi digər məşhur poçt proqramlarının istifadəçiləri ilə təhlükəsiz əlaqə yaratmaq imkanına malik olur.Bir dəfə rəqəmsal sertifikatla aktivləşdirilmiş SSL texnologiyası dərhal təhlükəsiz elektron tranzaksiyaların həyata keçirilməsi üçün zəruri olan aşağıdakı komponentləri təmin etmiş olur:

- **Autentifikasiya** – rəqəmsal setrifikatlar elektron tranzaksiyaların həyata keçirilməsi zaman şəxsin və ya təşkilatın rəqəmsal şəxsiyyətinin autentifikasiyasında istifadə olunur.Rəqəmsal sertifikatlar emaillerin göndərilməsi və ya elektron vəsitlərin ötürülməsi zaman da istifadə oluna bilər.Həmçinin şirkətin elektron sertifikatını yoxlamaqla alıcılar websaytın cinayətkarlara deyil, həqiqətən də şirkətə məxsus olduğuna əmin ola bilərlər.Bu alıcılarda məxfi informasiyanın göndəriləmsi zamanı əminlik hissi oyadır.

- **Məlumatların konfidensiallığı** – SSL seansın unikal açarından istifadə etməklə web serverin müştərilərlə mübadilə zamanı göndərdiyi bütün informasiyanı şifrələyir.Seans açarının istifadəçiyə göndərilməsinin təhlükəsizliyini təmin etmək üçün, server onu ictimai açar (public key) vasitəsilə şifrələyir.Hər bir seans açarı yalnız bir dəfə – bir yeganə müştəri ilə bir yeganə seans zamanı istifadə olunur.Konfidensiallığın bu mühafizə səviyyələri informasiyanın tutulduğu zaman oxunmasının qeyri-mümkünlüyünü təmin edir.
- **Məlumatların tamlığı –** Məlumatları göndərən zaman həm onu göndərən, həm də onu qəbul edən kompüter məlumatın məzmununa uyğun olan xüsusi açar yaradırlar.Əgər məlumat yolda olan zaman onun hər hansı bir simvolu modifikasiya edilərsə, məlumatı qəbul edən kompüter digər yeni bir kod yaradacaq və sonradan məlumatı göndərənə məlumatın etibarsız olduğunu xəbər verəcəkdir.Beləliklə, qarşılıqlı fəaliyyətdə olan hər iki tərəf digər tərəfin onlara göndərdiyi informasiyanı dəqiqliklə gördüklərinə əmin ola bilərlər.

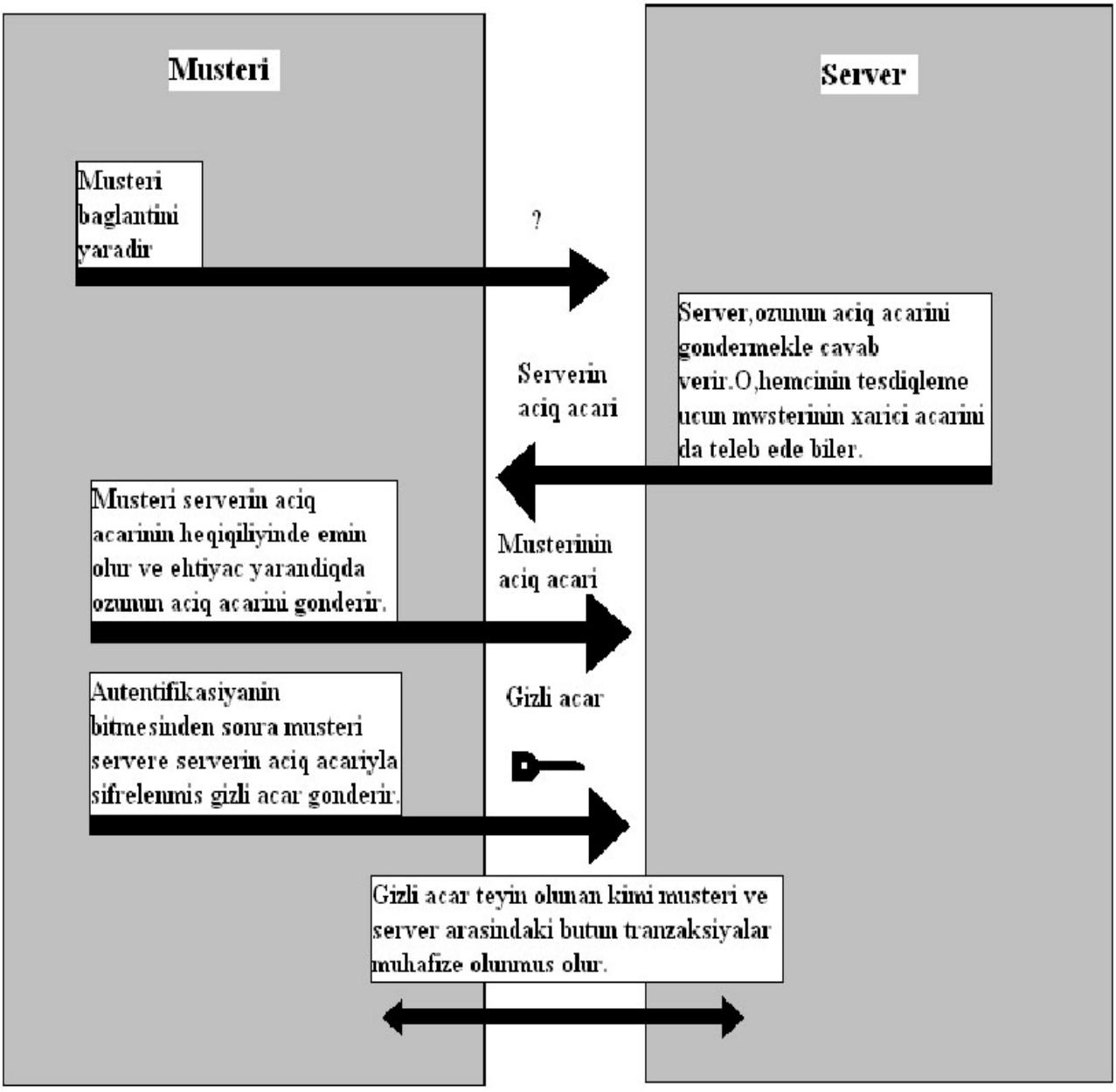
  Aşağıda göstərilmiş sxem web serverlə müştəri arasındakı tranzaksiyaların təhlükəsizliyinə zəmanət verən prosesi nümayiş etdirir.Rəqəmsal sertifikatla əlaqədar olan mübadilə müəyyən saniyələr ərzində baş verir və müştərinin müdaxiləsini tələb etmir.

VeriSign SSL rəqəmsal sertifikatların iki növünü təklif edir.Onlardan hər biri ziyarətçilərin istifadə etdiyi brauzerlərin buraxılışından asılı olan müxtəli növ şifrələmə səviyyələrini nəzərdə tutur.

**40-bitli rəqəmsal SSL sertifikatları** – Netscape və ya Microsoft Internet Explorer kimi brauzerlərin ixracat buraxılışları ilə 40 bitli SSL seansları aparmağa imkan verir.İnternet istifadəçilərinin 50%-dən çoxu ixracat buraxılışları ilə işləyir.Böyük həcmə malik olmayan web saytlar və internet şəbəkələrinin çoxu üçün 40-bitli şifrələmə kifayət edir.Lakin brauerlərin "ev" buraxılışları ilə qarşılıqlı əlaqə zamanı rəqəmsal sertifikat "yüksək davamlı" 128-bitli SSL şifrədən istifadə etməyə imkan verir.Heç bir 128-bitli SSL şifrəsi indiyə kimi sındırıla

bilməyib, hətta ən yeni texnologiyalardan istifadə edilsə belə onu sındırmaq üçün trilyonlarla il tələb oluna bilər.

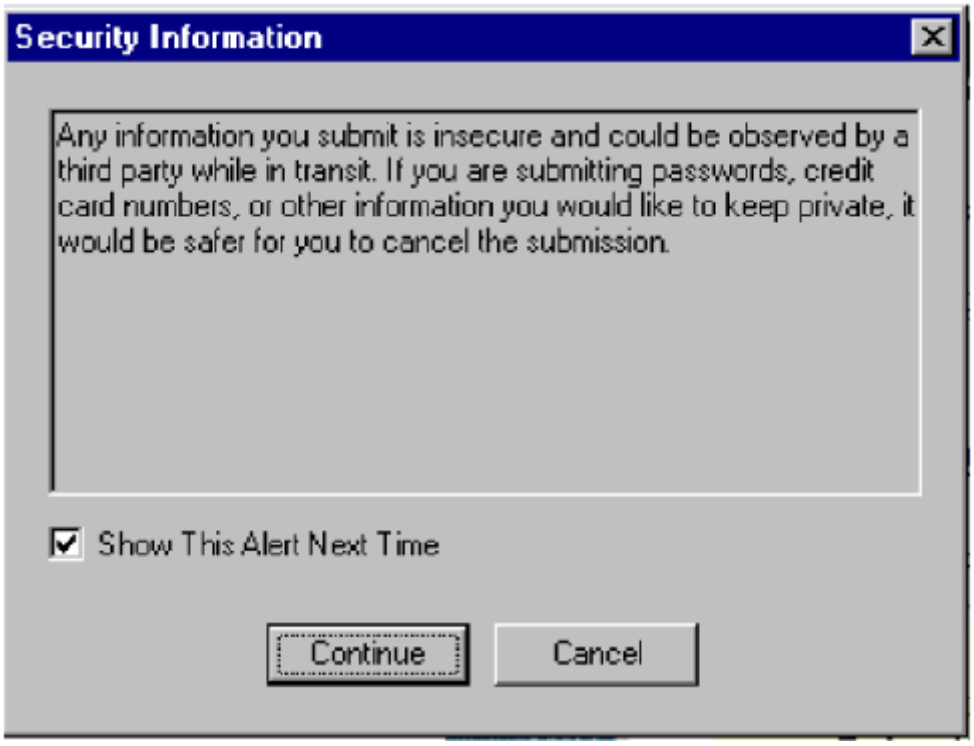
**128-bitli qlobal rəqəmsal sertifikatlar** – brauzerlərin həm "ev", həm də "ixracat" buraxılışları ilə qarşılıqlı əlaqə zamanı avtomatik olaraq SSL – in 128-bitli ən minimal şifrələmə səviyyəsini təmin edir.Qlobal rəqəmsal sertifikatların 128-bitli möhkəm şifrəsi sayəsində, onlar həssas və məxfi informasiya (kredit kartların nömrələri və s.) mübadiləsinin həyata keçirildiyi bütün saytlar üçün ideal olaraq uyğun gəlirlər.




Şəkil 1.Müştəri və server arasındakı tranzaksiyaların sxemi

Nəticədə ticarət saytında rəqəmsal sertifikatın istifadə edilməsi – on-line rejimdə sövdələşmələrin təhlükəsizliyini təmin edir.Alıcılar əmin olurlar ki, onlar özlərinin məxfi informasiyasını cinayətkarlara deyil, legitim bir sahibkara göndərirlər.Qarşılığında sahibkar da əmin olur ki, nəticədə onun şirkətinə müştəri tərəfindən təkzib edilə bilməyəcək dəqiq informasiya daxil olur.

Elektron sertifikatların quraşdırılması eletkron ticarəti daha təhlükəsiz etməklə yanaşı, İnternet vasitəsilə kredit kartların nömrələri kimi informasiyaların ötürülməsini asanlaşdırır.Microsoft və Netscape kimi brauzerlərdə mühafizə edilməmiş kanallar üzrə istifadəçi informasiyasının qeyri – iradi ötürülməsinin qarşısını alan təhlükəsizlik mexanizmləri quraşdırılmışdır.İstifadəçi mühafizə edilməmiş, yəni rəqəmsal sertifikata malik olmayan sayta hər hansı bir məlumatı göndərmək istədikdə brauzerlər pəncərədə təhlükə ilə bağlı xəbərdarlıq verən məlumatı əks etdirməlidir:




Əksinə əgər istifadəçi rəqəmsal sertifikata malik olan sayta hər hansı bir məlumat göndərdikdə bu xəbərdarlıq əks olunmayacaqdır.Təhlükəsiz bağlantı hiss olunmur, bu da nəticədə elektron formada alışın həyata keçirilməsini daha xoş

edir.Bundan əlavə, istifadəçilər əmin ola biləcək ki bu saytda həyata keçirilən büün tranzaksiyalar tam təhlükəsizldir.

Rəqəmsal sertifikatlar məlumatı göndərənin şəxsiyyətini identifikasiya etməyə və məlumatı qəbul edənə onu əldə etməyə imkan verir.Bu cür sertifikat özlüyündə sankı açıq açarın sarığı rolunu oynayır.Rəqəmsal sertifikatlar İnternetin kommersiya məqsədilə istifadə edilməsinə doğru atılan yeni bir addımdır.Lakin hələ ki, rəqəmsal sertifikatların zəruri istifadəsinə zəmanət verən kifayət dərəcəli infrastruktur mövcud deyil.Təşkilt daxilində istifadə zamanı adətən problemlər meydana çıxmır belə ki, sistem administratorları onların buraxılışlarına nəzarət edə bilirlər.

Elektron kommersiyada informasiya təhlükəsizliyi probleminin həlli elektron biznesidə iqtisadi təhlükəsizlik təminatının ən vacib komponentlərindən biri sayılır.Bundan başqa, onun bütövlükdə dövlətin iqtisadiyyatı üçün artan əhəmiyyətini nəzərə aldıqda, yadda saxlamaq lazımdır ki, elektron biznesin fəaliyyətinin etibarlılığı artıq bu gündə bilavasitə inkişaf etmiş informasiya cəmiyyətlərinin milli təhlükəsizliyinə təsir göstərə bilər, bu təsirin gələcək üçün isə daha da artıralacağı gözlənilir.

# FƏSİL 3. Ölkədə iqtisadiyyatın elektronlaşdırılmasının təkmilləşdirmə istiqamətləri

## 3.1. İqtisadiyyatın elektronlaşdırılmasında SET Və SSL Protokollarının Rolu

Planetin aparıcı səkkiz ölkəsi tərəfindən imzalanmış Qlobal İnformasiya cəmiyyətinin Okina xartiyasında deyilir ki, informasiya kommunikasiya texnologiyaları iyirmi birinci əsrin cəmiyyətinə təsir göstərən əsas faktorlardan biridir.Son zamanlar bilavasitə maliyyə–kredit institutlarının iştirakı ilə həyata keçirilən İnternet şəbəkəsi üzrə fəaliyyət göstərən ticarət və ya elektron kommersiya strukturları inkişaf etməyə başlamışdır.Bu ticarət növü xüsusilə elektron bazardan əhalinin və müəssisələrin daha çox istifadə edə biləcəyi yerlərdə daha çox məşhur olmağa başlamışdır.

Lakin, elektron kommersiyanın daha çox inkişaf etdiyi xarici ölkələrdə ticarət sövdələşmələrinin və ya mhəsullerın həcmi adətən 300–400 dollarla məhdudlaşdırılır.Bu, kompüter şəbəkələrində informasiya təhlükəsizliyi probleminin kifayət dərəcədə həllini tapmaması ilə əlaqədardır.BMT komitetinin onunla bağlı mübarizə ilə verdiyi qiymətləndirməyə əsasən, kompüter cinayətkarlığı beynəlxalq problemlərdən birinin səviyyəsinə gəlib çıxmışdır.ABŞ-da cinayətkarlığın bu növü narkotik və silah ticarətindən sonra gəlirliliyinə görə 3 – cü yeri tutur.

Elektron kommersiyada həyata keçirilən tranzaksiyalarda təhlükəsizliyinin təminatında protokolların xüsusi yeri və rolu vardır.Elektron kommersiyada protokol adı altında tranzaksiya iştirakçılarının (kart sahibi, ticarət nöqtələri, xidmətedici bank, bank-emitent, sertifikasiya mərkəzi) qarşılıqlı fəaliyyət ardıcıllığını və onların bir biri ilə avtorizasiya və hesablama proseslərini təmin etmək məqsədilə mübadilə etdikləri məlumatların formatlarını müəyyən etməyə imkan verən alqoritm başa düşülür.Hal-hazırda elektron kommersiya sistemlərinin

quruluşu zamanı istifadə olunan ən geniş yayılmış ( bəzi məlumatlara görə 99%-ə qədər) protokol SSL protokoludur.

SSL texnologiyası TCP/IP protokolu ilə fəaliyyət göstərən, web-server və web-brauzer arasındakı bütün məlumat axınını mühafizə edən etibarlı bir protokoldur.O, bütün məşhur web-server və web-brauzerdə tətbiq olunma imkanına malikdir.Müasir dövrdə internet vasitəsilə elektron ticarətdə və elektron iş fəaliyyətində çox əhəmiyyətli rola malikdir.SSL protokolu iki tərəf arasında etibarlı və məxfi əlaqənin təmin edilməsində çox mühüm finksiyanı həyata keçirir.SSL bağlantısı vasitəsilə göndərilən verilənlər üçüncü şəhslər tərəfindən modifikasiya edildikdə və ya oğurlandıqda tranzaksiyanın bütün iştirakçıları bundan xəbərdar olur.

Bu sistemdə kredit kartlarla bağlı bütün məlumatlar SSL texnologiyasıyla şifrələndikdən sonra online olaraq banka göndərilir və daha sonra alışın həyata keçirildiyi mağazada işləyənlər tərəfindən oxuna bilir.

Secure Sockets Layer (SSL) – web-brauzerlər və web-serverlər arasında ötürülən məlumatların mühafizəsini təmin edən protokoldur.SSL həmiçinin web düyündən əldə olunan məlumatların həqiqətən də həmin düyündən gəldiyinə və ötürülmə zamanı məlumatların təhrif olunmadığına əmin olmağa imkan verir.Ünvanı https – lə başlayan istənilən web düyün SSL protokolunu dəstəkləyir.

SSL protokolu 1994-cü ildə Netscape Communications şirkəti tərəfindən işlənib hazırlanmışdır.O, HTTP, NNTP, FTP və s. kimi servis protokolları ilə TCP/IP kimi nəqliyyat protokolları arasında verilənlərin mühafizəsini təmin edir.O ilk növbədə verilənlərin ötürülməsi üçün şifrələmə kanalının yaradılması məqsədilə müştəri və serverin autentifikasiyasının həyata keçirilməsindən ötrü tətbiq olunur.Autentifikasiya açıq açarlar infrastrukturunun tətbiqinə əsaslanır.Bununla belə, hər kəsin istifadə edə biləcəyi açıq açar və yalnız kartın sahibinin malik olduğu bağlı açardan da istifadə olunur.Açıq açarla şifrələnmiş informasiya qoşa bağlı açar vasitəsilə deşifrələnə bilər və əksinə.

Açıq açarların bölüşdürülməsi istifadəçiləri sertifikatlar təmin edən xüsusi sertifikasiya mərkəzləri tərəfindən həyata keçirilir.Sertifikat mərkəzin bağlı açarı

vasitəsilə imzalanır.Sertifikatların köməyilə həm serverin , həm də ki müştərinin ciddi autentifikasiyası həyata keçirilir.Bu proses kifayət dərəcədə çətindir, bununla bu zaman həmçinin sertifikatın hansı sertifikasiya mərkəzi tərəfindən verilməsi, onun zədələnməməsi və ya geri çağırılmaması yoxlanılır.

Adətən SSL-dən iki halda istifadə olunur: müştərinin qoşulduğu serverin və TCP/IP üzrə verilənlərin ötürülməsi zamanı şifrələmə kanalının təmin edilməsi üçün müştərinin özünün identifikasiyasının aparıldığı zaman.Bundan başqa, SSL protokolu vasitəsilə qurulan bağlantılar verilənlərin tamlığına zəmanət verir.Şifrələmə nadir hallarda aparılır, yəni o çoxlu resurs tələb edən bir prosesdir, buna görə də serverin gücü və imkanları kifayət dərəcədə yüksək olmalıdır. Kanalın şifrələnməsi üçün istifadə olunan seans açarları autentifikasiya prosesinin uğurla həyata keçirilməsindən sonra yaradılır.Hər sonrakı bir neçə dəqiqə onlar dəyişilir,bu da kriptodavamlılığı artırır.

1996-cı ildə SSL protokolunun 3.0 buraxılışının çıxmasıyla əlaqədar o, bütün brauzerlərin (MS Explorer,Netscape Navigarot və s.) dəstəklədiyi bir standart halına gəlmiş və çox geniş tətbiq sahəsini əldə edmişdir.SSL, göndərilən məlumatın dəqiqliklə və sadəcə doğru ünvanda deşifrə ediləbilməsini təmin edir.Məlumat göndərilmədən öncə avtomatik olaraq şifrələnir və sadəcə doğru alıcı tərəfindən deşifrələnə edilə bilər.Hər iki tərəfdə də autentifikasiya prosesi həyata keçirilərək əməliyyatın və məlumatların gizliliyi və tamlığı təmin olunur.

Kompüterlərin bir – birini “tanıma” əməliyyatı açıq-bağlı açar texnologiyasına (public-private key encryption) əsaslanan kripto sistem ilə təmin olunur.Bu sistemdə iki təşkil olunan bir açar cütü mövcuddur.Bunlardan açıq açar (public key) hər kəsə məlum olan və göndərilən məlumatın şifrələnməsində istifadə olunan rəqəmsal açardır.Ancaq, açıq açar ilə şifrələnən məlumat yalnız bu açarın digər cütü olan “bağlı açar” (private key) tərəfindən açıla,yəni deşifrələnə bilər.Bağlı açar da yalnız məlumatı göndərənə məlum olduğuna görə onun etibarlılığı təmin olunmuş olur.Məsələn, siz sizə məlumat göndərmək istəyən birinə öz açıq açarınızı göndərirsiniz.Qarşı tərəf bu açardan istifadə edərək məlumatı şifrələyir və sizə göndərir.Şifrələnən məlumat yalnız sizə məlum olan bir açar, yəni bağlı açar

tərəfindən açılıb oxuna bilər.Verilənlərin mübadiləsi zaman istifadə olunan şifrələmənin gücü açarın uzunluğundan asılıdır.

Açarın uzunluğu məlumatların mühafizəsi üçün çox önəmlidir.SSL protokolunda 40 bit və 128 bitlik şifrələnmədən istifadə olunur.128 bitlik şifrələnmədə 2128 dəyişik açar vardır və bu şifrənin açılması üçün böyük bir maliyyə vəsaitlərinə və zamana ehtiyac duyulur.Pis niyyətli bir insanın 128 bitlik şifrəni açа bilməsi üçün 1 milyon dollarlıq vəsait qoyduqdan sonra 67 ilə qədər zaman xərcləməsi tələb olunur.Bu misaldan aydın olur ki, SSL etibarlı sistemi tam və dəqiq bir mühafizəni təmin edir.

SSL protokolun geniş yayılma səbəblərindən biri də odur ki, o, bütün məşhur brauzer və web-serverlərin aparıcı tərkib hissəsidir.Bu o deməkdir ki, faktiki olaraq hər bir kart sahibi İnternetə standart çıxış vasitələrindən istifadə edir və bu zaman SSL protokolundan istifadə etməklə tranzaksiyaları həyata keçirmək imkanını əldə edir.SSL protokolunun digər üstünlüyü onun sadəliyi və yüksək əməliyyat göstəriciləridir( tranzaksiyanın reallaşma sürətliliyi).Sonuncu üstünlüyü onunla əlaqədardır ki, protokol məlumtların ötürülməsi zamanı eyni kriptodavamlılıq səviyyəsində assimetrik alqoritmlərə nisbətən 2-4 dəfə tez işləyən simmetrik şifrələmə alqoritmlərindən istifadə edir.

Eyni zamanda, SSL protokolu elektron kommersiyada bir sıra çatışmamazlıqlara malikdir.SSL protokolundan istifadəni məhdudlaşdıran əsas iki mənfi cəhət mövcuddur.Ondan istifadənin klassik variantında istifadəçilərin mobilliyinə nail olunmur və autentifikasiyanı həyata keçirməkdə əsas faktor olan istifadəçinin sertifikatından bağlı açarın oğurlanması təhlükəsi mövcud olur.

SSL-in istifadəsinə əsaslanmış elektron kommersiya protokolları İnternet mağaza tərəfindən müştərinin autentifikasiyasını dəstəkləmir, belə ki, bu cür protokollarda müştərinin sertifikatlarından demək olar ki istifadə edilmir.SSL sxemlərində müştərilər tərəfindən "klassik" sertifatlardan istifadə praktiki olaraq faydasızdır.Müştəri tərəfindən məşhur sertifikasiya mərkəzlərinin birindən əldə edilmiş bu cür sertifikat yalnız müştərinin adına və çox nadir hallarda onun şəbəkə ünvanına malik olur.Müştərilərdən çoxu dinamik İP ünvana malik olurlar.Bu

şəkildə sertifikat tranzaksiyaların keçirilməsi üçün ticarətdə az faydalıdır, çünki, asanlıqla cinayətkarla tərəfindən əldə edilə bilər.Müştərinin sertifikatının ticarət nöqtəsi üçün hər hansı bir əhəmiyyətə malik olması üçün onun müştərinin kart nömrəsi ilə onun bank emitenti arasında əlaqə yaratması zəruridir.Bununla belə, sertifikata malik olan kart sahibinin alış üçün müraciət etdiyi istənilən internet-mağaza bu əlaqəni yoxlamaq imkanına malik olamldır (özünün xidmətedici bankın köməyindən istifadə etməklə).Başqa sözlə, bü cür sertifikat müştəri tərəfindən özünün bank emitentidən əldə edilməlidir.Bu halda sertifikatın formatı, sertifikatda kartın nömrəsinin gizlədilməsi (aydındır ki, kartın nömrəsi sertifikatda açıq şəkildə görsənməməlidir), sertifikatların yayılma və geri çağırılma prosedurları və bir sıra digər hallar tranzaksiyanın bütün iştirakçıları arasında müzakirə edilməlidir.Başqa sözlə desək, sertifikasiya mərkəzlərinin iyerarxik infrastrukturunun yaradılmasına ehtiyac vardır.Bu cür infrastruktur yaradılmadan tranzaksiyanın bütün iştirakçıları arasında qarçılıqlı autentifikasiyadan söhbət gedə bilməz.

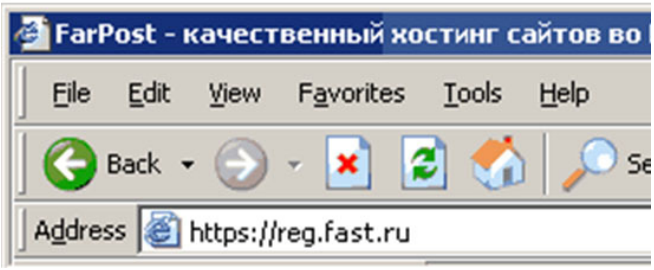
SSL sxemlərində müştərinin autentifikasiyasının yoxluğu bu protokolun ən böyük çatışmamazlığıdır, belə ki, bu çatışmamazlıq cinayətkarlara sadəcə olaraq kartın rekvizitlərindənxəbərdar olmaqla tranzaksiyanı uğurla həyata keçirməyə imkan verir.Xüsusilə də, SSL protokolunun xidmətedici bank tərəfindən müştərinin autentifikasiyasını həyata keçirməyə imkan vermədiyini nəzərə aldıqda.

Bütün bunlara baxmayaraq SSL protokolunun kifayət dərəcədə geniş tətbiq sferası mövcuddur.SSL protokolu daha çox web-brauzerlərlə web-serverlər arasında məlumatların mübadiləsinin mühafizəsi məqsədilə istifadə olunur.Bu mühafizə protokolunun əsas təyinatı aşağıdakılardna ibarətdir:

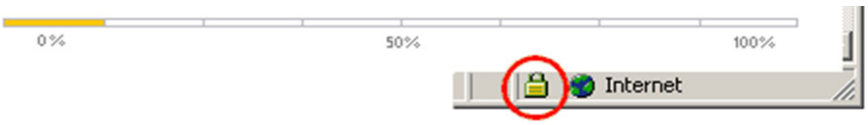
- Serverin autentifikasiyası – bu istifadəçilərə onların həqiqətən də istədikləri web-düyünü ziyarət etdiklərinə zəmanət verir;
- İnformasiyanın serverlə brauzer arasında kodlaşdırılmış şəkildə ötürülməsinə imkan verən mühafizə edilmiş kanalın yaradılması.Bu ötürülmə zamanı informasiyanın təhrif olunmasının qarşısını alır.
- Verilənlərin tamlığı.

Web istifadəçiləri web-serverin SSL protokolunu dəstəkləməsini https ünvan başlığı ilə müəyyən edə bilər.Burada məlum olan HTTP – Hypertext Transfer Protokol – una əlavə edilmiş “s” hərfi secure, yəni “mühafizə edilmiş” anlamını verir.İstifadəçinin SSL-bağlantısına qoşulmaq üçün xüsusi əməliyyatlar həyata keçirməyə ehtiyac yoxdur.SSL – in müştəri proqramı brauzerə quraşdırılıb;onlardan bir çoxu sadəcə olaraq istifadəçinin həqiqliyinə əmin olmaq üçün qeydiyyat nömrəsini və parolu tələb edə bilər.Buna misal olaraq,

Məsələn, https://reg.fast.ru/




Qeydiyyat Prosesi




*Seritifkatın həqiqiliyində əmin olmaq üçün ikonaya basın*

Şəkil 2.Brauzer tərəfindən SSL-in dəstəklənməsi

Fəaliyyəti internetlə əlaqədar olan şirkət sertifikatlara görə müvəkkil olan və şirkətin həqiqətən də özünü təqdim edən olduğunu təsdiqləyən VeriSign və ya

GeoTrust kimi müstəqil təşkilatlara müraciət etməsi zəruridir.Yoxlamanın bitməsindən sonra şirkət özünün web-serverlərində SSL bağlantılarını təşkil edə bilərlər.

| SSL-in mühafizə edlimiş bağlantını yaratması | | |
|---|---|---|
| *Mühafizə edilmiş bağlantılar, elektron kommersiya, mühafizə edilmiş interaktiv bank əməliyyatlarının təminatı, digər elektron biznes və müəyyən təhlükəsizlik səviyyəsini tələb edən bütün növ tranzaksiyalar üçün kritik əhəmiyyətə malikdir.*   | | |
| **SSL seansına sorğu**<br><br>İstifadəçi ünvanı https ilə başlayan web-düyünü ziyarət edir. “s” hərfi göstərir ki, server iş üçün SSL protokolundan istifadəni tələb edir. | **Bağlantının proqram quraşdırılması**<br>İstifadəçinin brauzeri və web-düyünün serveri handshake adını qazanmış məlumatlar mübadiləsi prosesinə başlayırlar.<br><br>**A.**Server brauzerə özünün VeriSign və ya GeoTrust kimi etibar qazanmış və səlahiyyətli şirkət tərəfindən sertifikasiya edilmiş açıq açarını göndərir.Brauzer serverin serverin serfitikatını yoxlayır.<br><br>**B.** Server brauzerə verilənlərin kodlaşdırılması və ya şifrələnməsi üçün neçə dərəcədən istifadə ediləcəyi barəsində məlumat verir.Adətən 128 dərəcədən istifadə etmək tövsiyyə olunur. | **Mühafizə edilmiş bağlantı**<br><br>Verilənlərin mübadiləsi, cinayətkarlara məlumatları öyrənməyə və təhrif etməyə imkan verməyən mühafizə edilmiş kanal üzrə həyata keçirilir.Verilənlərin tamlığının yoxlanılması onların brauzerdən serverə doğru və ya əksinə ötürülməsi prosesində modifikasiya edilməməsinə zəmanət verir.Verilənlər serverdə və ya brauzerdə görünən kimi onların mühafizəsinə artıq zəmanət verilmir. |

Şəkil 3.*SSL bağlantının təmin olunması*.

SSL protokolundan istifadə zamanı ticarət nöqtəsi yalnız özünün internetdəki ünvanı, yəni URL ünvanı üzrə autentifikasiya olunur.Bu o deməkdir ki, tranzaksiyanı həyata keçirən müştəri ticarət nöqtəsini əvvəldə qeyd edildiyi anlamda autentifikasiya etmir, yəni, ticarət nöqtəsi ilə ödəmə sisteminin iştirakçısı olan xidmətedici bankı arasındakı razılıq münasibətlərinin mövcudluq sübutunu əldə etmir.Ticarət nöqtəsinin yalnız URL üzrə autentifikasiyası cinayətkarların müxtəlif elektron kommersiya sistemlərinə çıxış əldə etməsini asanlaşdırır.

Burada qeyd etmək zəruridir ki, ticarət nöqtəsi serverinin sertifikatının yoxlanılması yalnız URL üzrə ona görə baş verir ki, bu cür quruluşa müştərilərin iş yerlərindəki bütün məşhur brauzerlər malikdir.SSL protokolu brauzerlərlə işləyən bütün əlavələrə onlar tərəfindən təhlil edilə bilən informasiyanı ötürməyə imkan verir.Məsələn, sertifikat sahibinin adı, sessiyanın quraşdırılmasının başlanma tarixi ve vaxtı və s.Əldə edilən verilənlərin təhlili əsasında əlavələr protokolun işinə müdaxilə etmək imkanını əldə edirlər (məsələn, SSL-sessiyası iştirakçılarından birinin autentifikasiyasını uğursuz qəbul etmək və sessiyanı dayandırmaq).Bu cür əlavə təhlilin mümkün olması üçün brauzerin funksionallığından istifadə edə biləcək xüsusi əlavələrə ehtiyac duyulur.Bu cür əlavə – müştəri tərəfindən elektron alışı reallaşdırmaq məqsədilə istifadə olunan xüsusi proqram təminatı olan elektron pul kisəsi çərçivəsində reallaşır.

Elektron pul kisəsindən istifadə müştəri tərəfindən bəzi çətinlikləri yaratmaqdan ( pul kisəsini yükləmək tələb olunur) və bu cür pul kisələrini bölüşdürən mərkəzin mövcudluğunu nəzərə almaqdan başqa özü özlüyündə bu problemi həll etmir.Problemin həlli üçün yuxarıda haqqında danışılan sertifikasiya mərkəzlərinin iyerarxik infrastrukturuna ehtiyac duyulur.Ticarət nöqtəsinin leqallığı, ödəmə sisteminin hər kəsə məlum olan sertifikatına malik olan xidmətedici bank tərəfindən verilən bağlı açara uyğun olan ticarət nöqtəsinin açıq açarının sertifikatı faktının yoxlanılması ilə müəyyən edilməlidir.

SSL protokolundan istifadə zamanı ticarət nöqtəsi üçün kartın rekvizitləri ilə əlaqədar informasiyanın məxfiliyi təmin olunmur.Bu nöqteyi nəzərdən digər təhlükəsizlik təminatında SET protokolundan istifadə etmək daha məqsədyönlüdür.
SET (Security Electronics Transaction) – İnternetdə şəbəkə üzrə elektron ticarətin təhlükəsizliyini təmin edən daha perspektivli təhlükəsizlik protokoludur.Mühafizə edilmiş tranzaksiyaların həyata keçirilməsi protokolu olan SET, IBM, GlobeSet və digər partnyorların iştirakı ilə Visa və MasterCard şirkətləri tərəfindən işlənib hazırlanmış standartdır.O, alıcılara İnternet vasitəsilə müasir dövrdə mövcud olan ən təhlükəsiz mexanizmlə ödənişləri həyata keçirməyə imkan verir.SET İnternetdə plastik kartlardan istifadə zamanı təhlükəsiz ödəmələrin həyata keçirilməsi üçün tətbiq olunan çoxtərəfli açıq standart protokoldur.SET protokolu qiymətli verilənlərin şifrələnməsini, məlumatların məxfiliyi və tamlığını və məhsula görə ödənişin hazırlılığını yoxlamaq məqsədilə satıcının, onun bankının və kart sahibinin hesabının kros-autentifikasiyasını təmin edir.Buna görə də SET-i İnternet vasitəsilə plastik kartlardan istifadə zamanı təhlükəsiz ödənişlərin həyata keçirilməsi üçün tətbiq olunan protokollar sistemi və ya standart texnologiya kimi də adlandırmaq olar.
SET, istehlakçılara və satıcılara kriptoqrafiyanın köməyi və həmçinin rəqəmsal sertifikatlardan istifadə etməklə İnternetdə həyata keçirilən əməliyyatların bütün iştirakçılarının həqiqiliyini təsdiq etməyə imkan verir.
Elektron kommersiya sahəsində potensial satış həcmi İnternet vasitəsilə ödəmələrin təhlükəszilik təminatı probleminə görə narahatlıq keçirən bütün maliyyə institutları, satıcı və alıcıların hamısının birlikdə təmin etdiyi zəruri informasiya təhlükəsizliyi səviyyəsinin əldə olunması ilə məhdudlaşır.Əvvəldə qeyd edildiyi kimi informasiya mühazifəsinin əsas məsələsi onun əlverişliliyinin, məxfililiyinin, tamlığının və hüquqi əhəmiyyətliliyinin təmin olunması ilə müəyyən olunur.
Müasir dövrdə bir çox şirkətlərin elektron kommersiyada fəaliyyət göstərməsi məqsədilə özlərinin proqram təminatlarını işləyib hazırlaması ilə əlaqədar olaraq bir porblem də meydana çıxır.Çünki bu cür proqram təminatından istifadə etmək

üçün əməliyyatın bütün iştirakçıları eyni bir əlavəyə malik olmalıdır, bu isə praktiki olaraq qeyri-mümkündür.Bu səbəbdən müxtəlif istehsalçıların əlavələri arasında qarşılıqlı fəaliyyət mexanizminin təmin olunması üçün digər bir üsula ehtiyac duyulur.

Yuxarıda sadalanan problemlərlə əlaqədar olaraq Visa və MasterCard şirkətləri texniki məsələlərlə məşğul olan digər şirkətlərlə birlikdə Set standartının protokollar yığımını və spesifikasiyasını işləyib hazırlamışlar. Bu açıq spesifikasiya tez bir müddət ərzində elektron kommersiya üçün de-fakto standartı adını qazanmışdır.Bu spesifikasiyada informasiyanın şifrələnməsi onun məxfiliyini təmin edir.Rəqəmsal imza və sertifikatlar tranzaksiya iştirakçılarının identifikasiyasını və autentifikasiyasını təmin edir.Verilənlərin tamlığının təmin olunmasında rəqəmsal imzalardan həmçinin istifadə olunur.Açıq protokollar yığımından müxtəlif istehsalçıların realizasiyaları arasındakı qarşılıqlı fəaliyyətin təmin olunmasında istifadə olunur.

SET elektron kommersiyada aparılan əməliyyatların mühafizəsi məqsədilə aşağıdakı xüsusi tələblərin həyata keçirilməsini təmin edir:

- Ödənişlə əlaqədar verilənlərin və bu verilənlərlə birgə göndərilmiş sifarişlə bağlı informasiyanın məxfiliyi;
- Ödənişlə əlaqədar verilənlərin tamlığının qorunub saxlanması; rəqəmsal imza vasitəsilə tamlığın təminatı;
- Autentfikasiyanın həyata keçirilməsi üçün açıq açarlı xüsusi kriptoqrafiyanın təmin olunması;
- Kredit kart sahibinin autentifikasiyası, bu kart sahibinin rəqəmsal imzası və sertifikatlarının tətbiqi nəticəsində təmin olunur;
- Satıcının rəqəmsal imzası və sertifikatı tətbiq olunmaqla satıcının və onun kredit kartlar üzrə aparılan ödənişləri qəbul etmək imkanının autentifikasiyası;
- Satıcı bankının prosessing mərkəzi ilə əlaqə vasitəsilə kredit kartlar üzrə ödənişləri qəbul edə bilən fəaliyyət göstərən təşkilat olduğunu

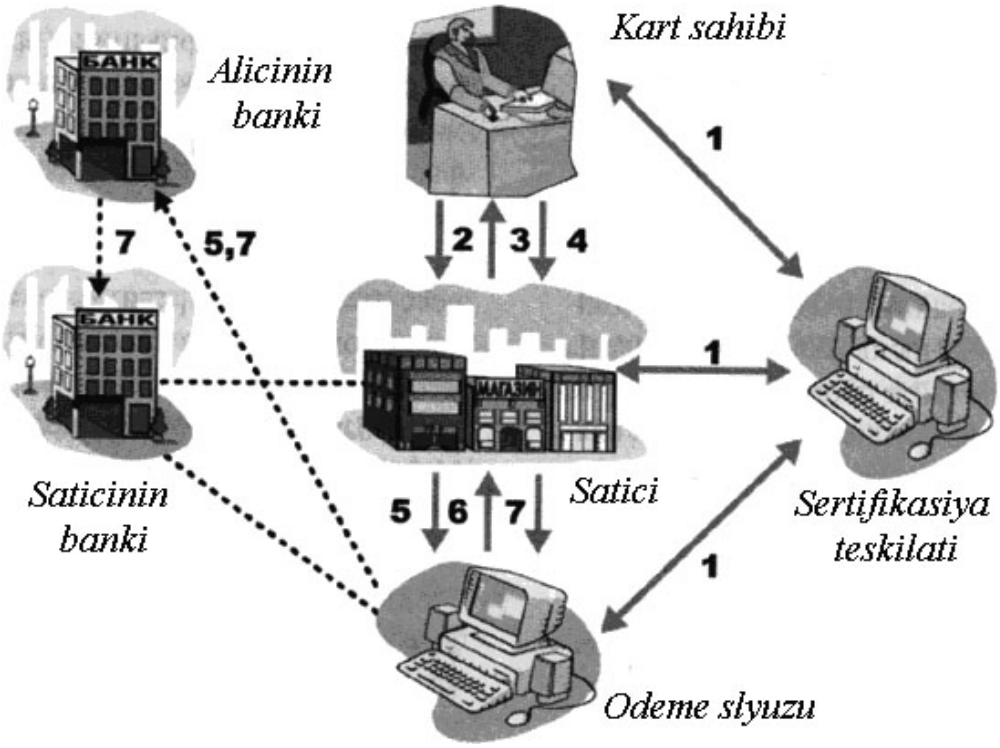
təsdiqləmək; bu təsdiqlənmə satıcı bankının rəqəmsal sertifikat və rəqəmsal imzası vasitəsilə təmin olunur;

- Kriptoqrafiyadan istifadə nəticəsində verilənlərin ötürülməsinin təhlükəsizliyi.

SET satıcılar, kart sahibləri və banklar arasında mövcud olan münasibətləri qoruyub saxlamağa imkan verir və aşağıdakı xüsusiyyətlərə əsaslanır:

- Maliyyə sənayesi üçün açıq və tamamilə sənədləşdirilmiş standart;
- Ödəmə sistemlərinin beynəlxalq standartlarına əsaslanıb;
- Maliyyə sahəsində mövcud olan texnologiyalara və hüquqi mexanizmlərə əsaslanır.

SET spesifikasiyasına uyğun olaraq ödəmə əməliyyatı iştirakçılarının qarşılıqlı fəaliyyət prosesi daha dəqiq olaraq aşağıdakı şəkildə təqdim edilir:




Şəkil 4.*SET standartı üzrə ödəmə sisteminin iştirakçılarının qarşılıqlı fəaliyyət sxemi*

Şəkildə kart sahibi sifarişi edən alıcı; alıcının bankı alıcı üçün kredit kartı buraxan maliyyə institutu; satıcı xidmət və məhsulları təklif edən elektron mağaza; satıcının bankı satıcının əmliyyatlarını həyata keçirən maliyyə strukturu; ödəmə şlyuzu satıcının sorğularını emal edən və alıcının bankı ilə qarşılıqlı fəaliyyət göstərən və adətən satıcının bakı tərəfindən nəzarətdə saxlanılan sistem; sertifikasiya təşkilatı isə sertifikatları verən və yoxlayan etibarlı strukturdur.

Şəkildə əməliyyat iştirakçılarının qarşılıqlı fəaliyyət mexanizmi kəsilməz (SET protokolu və ya standartı tərəfindən təsvir edilən qarşılıqlı fəaliyyət) və punktirli xətlərlə (bəzi mümkün əməliyyatlar) göstərilmişdir.

SET standartının spesifikasiyasına uyğun olaraq qarşılıqlı əlaqələrin və informasiya axınlarının dinamikası özünə aşağıdakı əməliyyatları daxil edir:

1. İştirakçılar sertifikasiya təşkilatına sorğu göndərir və oradan sertifikatlar əldə edirlər;
2. Plastik kartın sahibi elektron kataloqu gözdən keçirir, məhsulları seçir və sifarişi satıcıya göndərir;
3. Satıcı özünü təsdiqləmək üçün öz sertifikatını kart sahibinə təqdim edir;
4. Kart ashibi öz sertifikatını satıcıya təqdim edir;
5. Satıcı ödəmə şlyuzunun yoxlama əməliyyatını aparması üçün ona sorğu göndərir.Şlyuz təqdim edilən informasiyanı elektron kartı buraxan bankın informasiyası ilə tutuşdurur;
6. Yoxlamadan sonra ödəmə şlyuzu nəticələri satıcıya qaytarır;
7. Bir müddət sonra, satıcı ödəmə şlyuzundan bir və ya daha çox maliyyə əməliyyatlarını həyata keçirməyi tələb edir.Şlyuz müəyyən məbləğdə vəsaitlərin alıcının bankından satıcının bankına köçürülməsi üçün sorğu göndərir.

SET protokolu etibarlılıqla əlaqədar olaraq çox mühüm üstünlüklərə malikdir.Şəbəkədə verilənlərin mübadiləsi zamanı etibarlılığın bu üstünlükləri aşağıdakı üç amillə müəyyən olunur:

- Məxfilik, məlumatların şifrələnərək gizli hala salınmasıyla təmin olunur;

- Məlumatların tamlığı, rəqəmsal imzalardan istifadə etməklə məlumatın göndərildiyi şəkildə heç bir dəyişkliyə uğramadan qarşı tərəfə çatdırılmasını təmin edir”
- Autentifikasiya, rəqəmsal imzadan istifadə nəticəsində təmin olunur.Rəqəmsal imzalar vasitəsilə əməliyyat iştirakçılarının kimlikləri təsdiqlənir, göndərdikləri məlumatları inkar etmələrinin qarşısı alınmış olur.

Əməliyyatların məxfiliyi və məlumatların modifikasiyadan qorunması kriptoqrafiya ilə təmin olunur.SET protokolu RSA və DES olmaqla iki fərqli alqoritmlərdən istifadə edir.DES simmetrik bir alqoritmdir və əməliyyat zamanı mübadilə edilən verilənlərin kriptoqrafiyasını təmin edir.RSA isə assimetrik bir alqoritm olub, imzalar üçün və simmetrik açarlarla bank kartı nömrələrinin açıq açarlı kriptoqrafiyasını həyata keçirmək üçün istifadə olunur.

Bu şəkildə SET protokolu ən yaxşı iki alqoritmin birgə istifadəsiylə yüksək bir kriptodavamlılığı təmin etmiş olur.Bu sistem bu cür işləyir: İlk olaraq, verilənlər təsadüfi şəkildə yaradılmış bir simmetrik DES açarıyla şifrələnir.Daha sonra bu açar məlumat alıcısının RSA açarıyla şifrələnir.Bununla ikinci açar məlumatın içinə yerləşdirilən bir “rəqəmsal zərf” formasında olur.Alıcı bu zərfi aldığı zaman özünün xüsusi açarıyla açaraq təsadüfi şəkildə yaradılmış simmetrik açarı əldə etmiş olur və bu açar da orijinal məlumatın şifrəsini açmaq üçün istifadə olunur.

Məlumatın tamlığı dedikdə, onun alıcıya modifikasiya edilmədən çatdırılması nəzərdə tutulur və hashing alqoritmlərinin istifadə edildiyi bir istiqamətli şifrələnmə və rəqəmsal imzalarla təmin edilir.Hashing alqoritmi məlumatı dəyişərək ona bənzər olmayan bir formaya salır.Bu əməliyyat tək başına olaraq məlumatın tamlığın zəmanət verməyə kifayət deyildir.Buna görə də gizli bir kripto açarla birlikdə istifadə edilir.Bu zaman rəqəmsal imzalar əməliyyata daxil olur.

Autentifikasiya, məlumatı göndərənin kimliyini təsdiqləmək üçün istifadə edilir.SET əməliyyatının iştirakçılarının hər biri rəqəmsal sertifikatlarla təmin olunur.Bu sertifikatlar etibarlı üçüncü tərəf olan sertifikasiya mərkəzi (Certification

Authority – CA) tərəfindən yaradılır.Hər rəqəmsal sertifikat özünə aid olduğu insanın kimliyi ilə bağlı məlumatları və açıq açarlarından birini daxil edir.Bundan başqa hər bir sertifikat etibarlı olduğunun təsdiqlənməsi üçün sertifikasiya quruluşu tərəfindən rəqəmsal olaraq imzalanır.

SET protokolunun istifadə etdiyi şifrələmə alqoritmi 1024 bitlik şifrələmə ilə həyata keçirilir.Bu şifrənin sındırıla bilməsi üçün saniyədə 10.000.000 əmri həyata keçirmək qabiliyyətinə malik olan 100 kompüterin təqribən 2.800.000.000.000 il çalışmasının lazım olduğu hesablanmışdır.Bu halda belə, açılan şifrə sadəcə bir məlumatın oxunması üçün faydalı ola bilər, sonrakı məlumatın oxunması üçünsə bu əməliyyatın təkrarən həyata keçirilməsi lazımdır.

Eyni şifrələmə metodlarından istifadə etməklə yanaşı SSL və SET protokollarının bir-birindən fərqli olduğunu nümayiş etdirən nöqtələr də mövcuddur.Bunlar aşağıdakılardır:

- SSL-də kartla bağlı məlumatları göndərən insanın həqiqətən də kartın sahibi olduğuna zəmanət verilmir.Bu nöqsan SET protokolunda aradan qaldırılmış olur;
- SSL-də kartın aid olduğu və POS-un aid olduğu banklar bu modelə daxil deyillər;
- SSL-də kart sahibinin kart məlumatları internet vasitəsilə göndərilən zaman şifrələnir,lakin onları qəbul edən mağaza onları oxumaq imkanına malik olur.SET protokolunda isə kartlar bağlı məlumatlar mağazadan gizli olaraq saxlanılır və yalnız bank tərəfindən oxuna bilər.

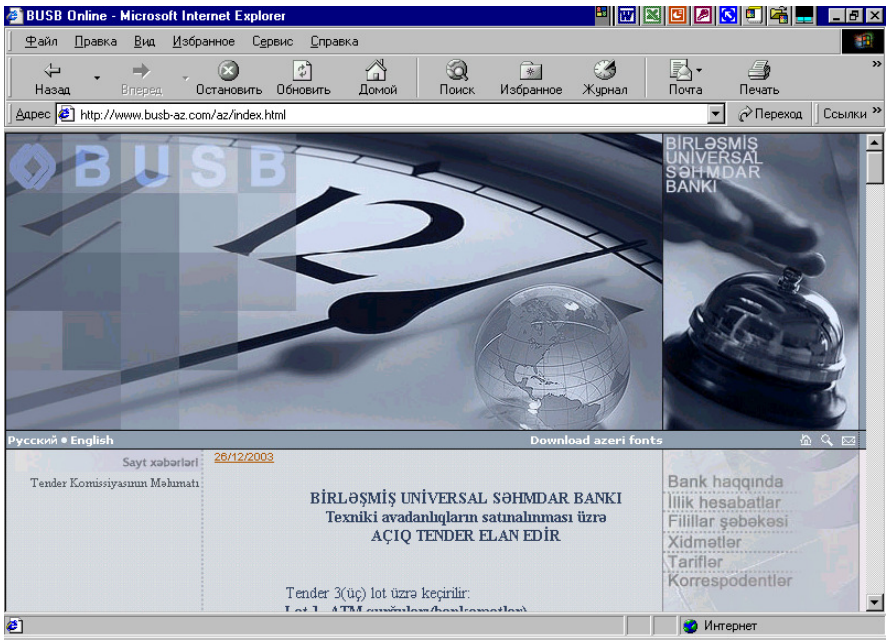
Visa və MasterCard tərəfindən yaradılaraq 1996-cı ildən bu yana həyata keçirilən işlər nəticəsində SET, günümüzdə texniki xüsusiyyətlərinə görə özünü reallaşdırmış və bazarda kifayət dərəcədə geniş yayılmışdır.Bu gün SET internet vasitəsilə tamamilə etibarlı əməliyyatların həyata keçirilməsi üçün tam hazırdır.

## 3.2. Elektron ödəmə sistemlərinin təkmilləşdirmə istiqamətləri

Dünyəvi hörümçək toru – İNTERNET-in insan fəaliyyətinin bütün sahələrinə yol tapması və gözlənilməz effekt yaratması biznes sahəsində xüsusilə hiss edilməkdədir. Bu effekt öz növbəsində yeni bir anlayışın - elektron pul məfhumunun yaranmasına səbəb olmuşdur. Beləliklə də dünyəvi şəbəkədə ümumi yeni bir valyutaya ehtiyac duyulur.

Həqiqətən də elektron kommersiyanın inkişafı ilə əlaqədar tez və rahat ödəmələr üçün elektron pul yaranması zərurəti ortaya çıxıdı. Bununla əlaqədar müxtəlif elektron ödəmə sistemləri yaranmışdır. Bu sistemlərin istifadəçilərində istifadə etdikləri xidmətin və ya aldıqları malın haqqını dünyanın başqa bir nöqtəsinə necə göndərmək haqda sual yaranmır. Çünki, onun valyuta kursu və pulun köçürülməsi forması haqda problemi olmur. Belə ki, bu cür sistemlərin hər birinin istifadəçilər arasında haqq-hesab üçün öz şərti valyuta ekvivalentləri olur. Məsələn, E-qold elektron ödəmə vasitəsi qızıl, gümüş, platin kimi qiymətli metalların çəki əmsallarından istifadə edir. İstifadəçi sistemin şərti vahidləri formasında öz hesabına daxil olmuş elektron ödənişi müxtəlif yollarla nəqd valyutaya çevirə bilər və ya olduğu kimi İNTERNET-də istifadə edə bilər.

WebMoney MDB məkanında ən geniş istifadə olunan elektron ödəmə vasitəsidir. burada elektron pul iki nəqd valyuta ilə müdafiə olunur: ABŞ dolları – WMZ və Rus rublu – WMR vasitəsilə. Respublikamızda da banklar öz xidmətlərini internet vasitəsi ilə təqdim etməyə başlamışlar. Məsələn, ABB (Azərbaycan Beynəlxalq Bnkı), Atabank, BUSBank (Birləşmiş Universal) səhmdar bankları və s.




Şəkil 5. BUSBank (Birləşmiş Universal Səhmdar Bank) Transfer saytının başlanğıc səhifəsi –www.busb-az.com

Elektron ödəniş onsuz da fiziki hesab nömrəsinə bağlıdır. Ödəniş hesaba keçirilir, müştərinin kartına isə bu ödənişin elektron ekvivalenti qeyd edilir, yəni real pul kütləsi hərəkət etmir. Real pul ya elektron dəyərə çevrilir, ya da hesabdan hesaba elektron dəyər kimi ödənilir.

Elektron formada ödənişin bir neçə növü var:

1. Müştərinin bankdakı pul vəsaiti elektron dəyər satıcının hesabına keçirilənədək onun hesabında qalır. yəni alınan mala görə müştəri nəqd pul əvəzinə elektron dəyər alır və sonra onu banka təqdim edərək nəqd pul götürür və ya müştəri tərəfindən verilən hesab-fakturaya görə vəsait satıcının hesabına köçürülür.
2. Üçüncü tərəf ödəmə kartı istehsal edərək, bankı və müştərini elektron dəyərlə təmin edir və müştəri elektron dəyərə görə öz bank hesabından və ya nəqd formada pul ödəyir.
3. Bank kartı üçüncü tərəfdən alır və müştərilərə satır.

Biznes aləmini banklarsız təsəvvür etmək əlbəttə ki, çətindir. bu baxımdan virtual məkanda da banklarsız böyük bir boşluq yaranardı. çünki ödənişlər bu qurumlar vasitəsilə həyata keçirilir.

İnternet-bank sisteminin ənənəvi bank-müştəri klassik sistemindən əsas

üstünlükləri aşağıdakılardır:

1. Operativlik. Sistem hər hansı bir coğrafi məkana və ya kompüterə bağlanmır, yəni ondan asılı olmur. Müştəri istədiyi əməliyyatı dünyanın internetə çıxış olan ixtiyari nöqtəsindən həyata keçirə bilər.
2. Elastiklik. İnternet bank tərəfindən daxil edilən ixtiyari bir dəyişiklik avtomatik olaraq bütün müştərilərə aid edilir.
3. Real zaman kəsiyində nəzarət. -dəniş zamanı avtomatik müştərinin rekvizitləri əsasında onun borclu olması yoxlanılır və borc olduqda ona məlumat göndərilir.
4. Aşağı qiymət. Müştəri hissəsində xüsusi brauzerdən istifadə edilir ki, o da ödəniş qismində yalnız müdafiə vasitəsinin dəyərini tələb edir.
5. Rahatlıq. Sistemdə çox istifadə edilən standart sənədlərin elektron formasında arxivi saxlanılır ki, bu da sənədlərin hazırlanmasına sərf olunan vaxtı azaldır, rahat iş mühiti yaradır. Bu sənədlərə misal olaraq vergi ödəmələri, kommunal ödəmələr, mobil telefona görə ödəmələr və s. aid edilir.

İnternet-Bank sisteminin funksiyaları aşağıdakılardır:

- ödəmə hesabların banka göndərilməsi;
- ödənişin istifadə edilməsi haqda məlumat;
- şəxsi hesabda olan qalıq haqda məlumat;
- olan köçürmə haqda çıxarış təqdim etmək;
- giriş-çıxış əməliyyatları haqda informasiya.

İnternet-Bank sisteminin yaradılması prinsipləri:

- İnternet-bank sistemi dünya internet şəbəkəsi texnologiyası əsasında yaradılır;
- İki hissədən ibarət olur: müştəri və bank sistemindən;
- Standart Windows 95/98/NT əməliyyat sistemləri və web səifələrə baxmaq üçün standart brauzerlər istifadə edilir;
- Əməliyyat aparmaq üçün uyğun bankın Web-saytından istifadə edilir.

Elektron ödəmə sistemlərinin əsas iki növü mövcuddur – məlumatların mübadiləsi (sifarişlər, hesablar və s.) və pul vəsaitlərinin elektron köçürmələri. Elektron köçürmələr banklar arasında həyata keçirilir və böyük həcmə malik olurlar.

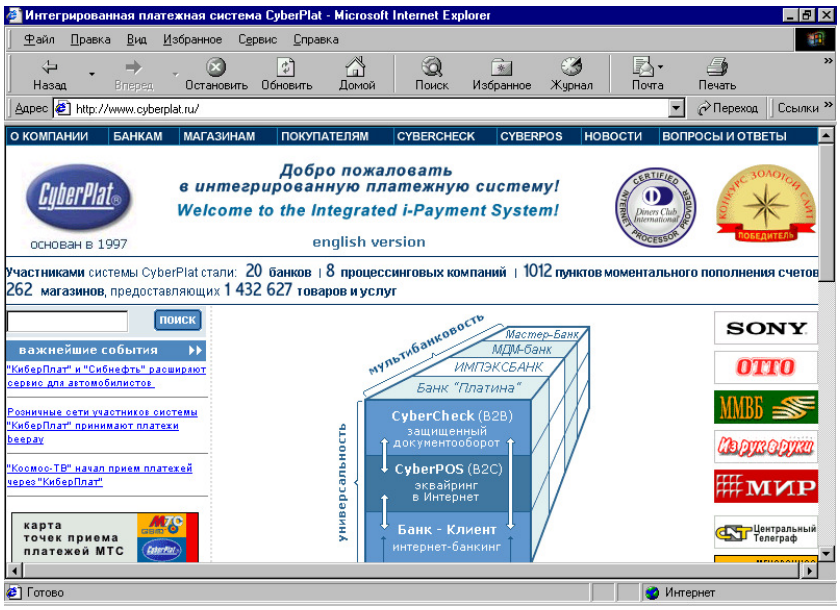
Elektron ödəmə vasitələrinin üç tipi mövcuddur. Birinci tip adi və elektron ödəmələrin kombinasiyasından ibarətdir. Məsələn, ödəniş ənənəvi qaydada həyata keçirilir, ancaq sahibinə təsdiqi elektron poçtla göndərilir və ya əksinə, ödəniş elektron qaydada yerinə yetirilir, təsdiqi adi poçtla gəlir.

İkinci tip – pul vəsaitlərinin köçürülməsinin ənənəvi qaydasının genişlənməsidir. Burada kredit kartların nömrələrinin elektron qaydada ötürülməsi və sahibi haqqında bütün məlumatları saxlayan və ötürən smart-kartlardan istifadə edilməsi daxildir. Bu halda bütün əməliyyat elektron şəkildə yerinə yetirilə bilir.

Üçüncü tipə rəqəm nəqdlərinin müxtəlif növləri və elektron pul daxildir. Birinci iki tip arasında fərq ondan ibarətdir ki, sonuncu halda təkcə məlumat deyil, həqiqətən pul köçürülür. Məsələn, əgər təkcə kredit kartın nömrəsi köçürülürsə, - bu ikinci tip ödəmədir, yox əgər məlumatın özü ilə müəyyən məbləğdə pul köçürülərsə – bu üçüncü tipdir.

Elektron pullar – bu, müəyyən kodlaşdırılmış seriyalı nömrələrdir ki, onlar real məbləğdə pul təmsil edirlər. Bu zaman onlar tamamilə adi pula dəyişdirilə bilən qiymətli pul vəsaiti olurlar.

Smart-kart – elektron kommersiya çərçivəsində tranzaksiyaların həyata keçirilməsi üçün vacib olan, informasiyanı saxlaya bilən kiçik qurğudur. Smart-kartlar elektron nəqdlərini, sahib haqqında məlumatları, elektron açarlar və s. .özündə saxlaya bilər.




Şəkil 6. İnternet vasitəsi ilə elektron ödəmə sistemi –

Mikroödəmələr – mikrotranzaksiyaları ödəmək üçün vacib olan elektron pulun xüsusi növüdür. Bir tranzaksiyanın dəyəri o qədər kiçik ola bilir ki, onları adi pul vahidləri ilə ifadə etmək çətin olur. Ona görə də mikroödəmələrin vacibliyi meydana gəldi. Onu qeyd etmək lazımdır ki, mikroödəmə elektron kommersiyaya xasdır.

İnternet-kommersiyanın inkişafı elektron formada ticarət zamanı ödəniş mexanizmləri işləyib hazırlamağı gündəmə gətirdi. İlk vaxtlar İNTERNET-də xidmət və malların ödənişi üçün kredit və debitor kartlarından istifadə edilib. 90-cı illərin ortalarından isə *Bank-Müştəri* və ya *İnternet-Müştəri* tipli sistemdən istifadə olunmağa başlanıb. Bunun da nəticəsində bank çekləri və banknotlarının elektron analoqu – *elektron pul* (*e-mony*) meydana gəldi. Qeyd edək ki, elektron-pul xüsusi olaraq yalnız İnternet vasitəsilə hesablaşma aparmaq üçün yaradılıb.

İnternetdə xüsusi hesablaşma vasitəsinin yaradılması zəruriliyi İnternet-ticarətin xüsusiyyətindən irəli gəlir. Belə ki, İnternet vasitəsilə ticarət, adətən, pərakəndə formada baş verir, müştərilərin sayı qeyri-məhdud olur, onların sayını proqnozlaşdırmaq mümkünsüzdür və onlar haqqında heç nə məlum olmur. Ona görə də, hesablaşma sistemi çoxlu sayda ödəmələri təhlil etmək

iqtidarında olmalıdır. Nəzərə almaq lazımdır ki, bu hesabların çox hissəsi kiçik həcmli olur. Çünki əksər hallrda ticarət pərakəndə formada aparılır. Ona görə də belə hallarda klassik ödəmə sistemi yararlı olmur. Çünki bankın xidmət haqqı bəzən ödəniş haqqından artıq olur. Məhz bu səbəbdən nəqd pula bənzər elektron ödəmə vastəsindən istifadə edilir.

Elektron-kommersiya sahəsində çox olmasa da qeyri-material formalı xidmət növləri də təşəkkül tapıb. Bu, əsasən, informasiya təqdimatı, məsləhət və maliyyə xidmətləridir. Ötürmə kanallarından istifadə etməklə bu xidmətlər bilavasitə sifariş verilən anda həyata keçirilir. Elektron-kommersiyanın ən geniş inkişaf etmiş sahəsi maliyyə xidmətlərinin satışı və hesablaşmanın İnternet vasitəsilə aparılmasıdır. Bu *elektron-maliyyə* (*e-finance*) adlanır. Bundan başqa, bu gün İnternet vasitəsilə məsafədən təhsil, hüquq və həkim məsləhətləri aparılır. İnternet vasitəsilə bank xidmətləri *İnernet-bankinq* (*i-banking*), qiymətli kağızlar bazarında aparılan əməliyyatlar üzrə elektron xidmətlər *İnternet-treydinq* (*i-trading*), sığorta xidmətləri *İnternet-sığorta* (*i-insurace*) adlanır. Bu terminləri işlədərkən, bəzən İnternet sözünü online sözü ilə əvəz edirlər: məsələn, *online banking internet-banking* (i-*banking*) sözünün sinonimidir.

Hal-hazırda 10 milyondan çox Web-səhifədən yalnız 31-i kommersiya yönümlü deyil. Elektron-kommersiya bazarında illik dövriyyə 30-50 milyard ABŞ doları təşkil edir.

Müasir Elektron-kommersiya bazarında aşağıdakı xidmət növləri mövcuddur:

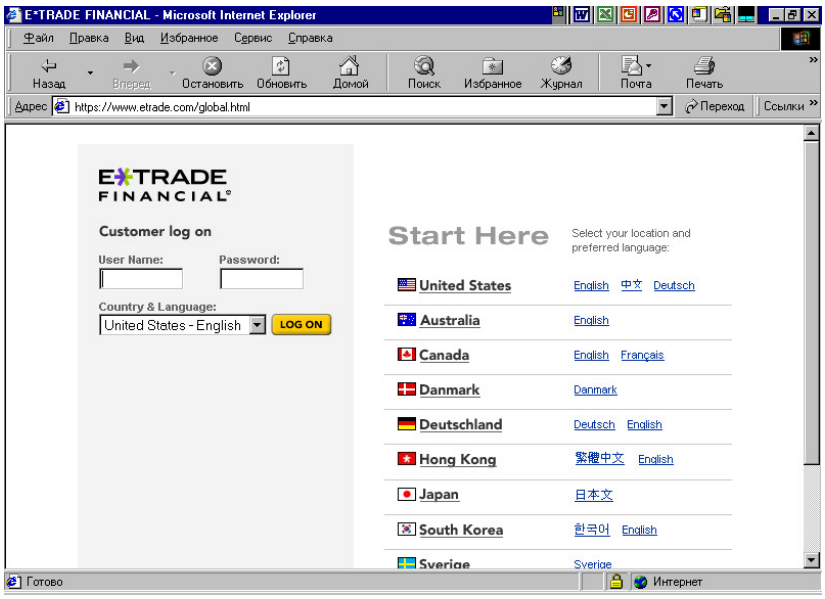
1. Texnologiya təminatçıları.
2. Elektron-kommersiya xidmətçiləri.
3. İnternet-kommersiya əlaqələndiriciləri.
4. Elektron ödəmə xidmətləri.

Texnologiya təminatçıları (*technology providers*) – bunlar kommunikasiya kompaniyaları, İnternet-provayderlər (ISP), proqram və aparat təminatı üzrə istehsal kompaniyaları – informasiya texnologiyaları (IT) sektoru kompaniya-

larıdır.

Kommersiya xidmətçiləri (*content providers*) – bunlar operativ informasiya və xidmət təminatı ilə məşğul olan kompaniyalardır. Bunların sırasına aşağıdakılar aiddir:

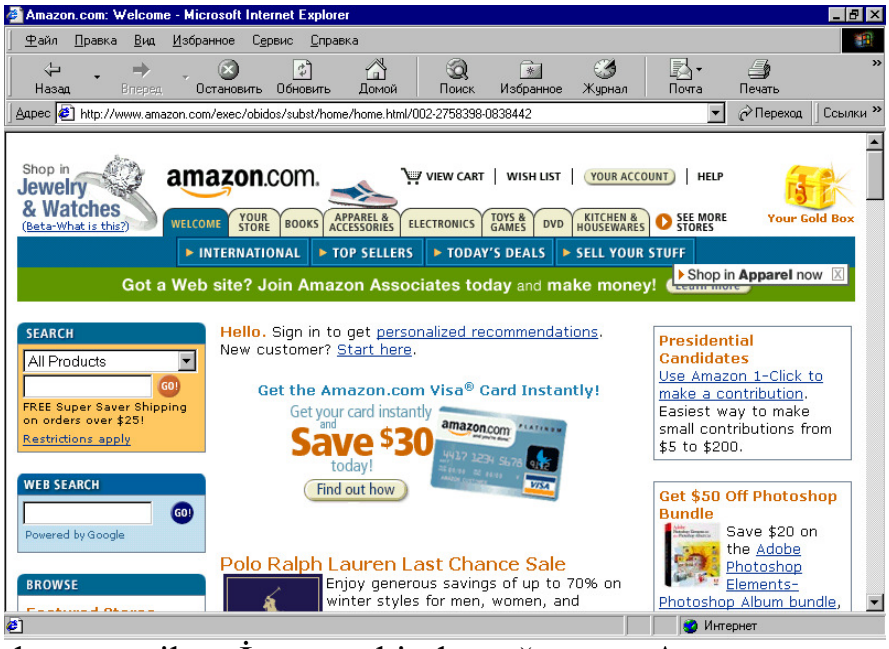
- idmət sahibləri (*owners*) – bunlar sahibkarlar, bilavasitə xidmətçilər və satıcılar ola bilər. Bankların əksər hissəsi öz İnternet-xidmətlərini Web-səhəhifələrdə kataloqlar formasında təqdim edir və elektron-kommersiya bazarı iştirakçılarının xidmət sahibləri kateqoriyasına aiddirlər.
- Elektron brokerlər (*e-brokers*) – elə bir təşkilatdır ki, son istifadəçiyə müxtəlif məhsul və xidmətlərlə tanışlıq imkanı təşkil edir. Elektron-brokerlər üçüncü firmaya aid məhsul və xidmətləri təklif edir, onları qiymətləndirir, bu və ya digər məhsulun alınıb-satılması haqda təkliflər verir və bununla da satış prosesini asanlaşdırır. Elektron-brokerin mühüm bir növü *informasiya-brokeridir*. Onlar müxtəlif informasiya bazalarına giriş imkanını təmin edirlər. Elektron-brokerlərə misal olaraq maliyyə sferasında fəaliyyət göstərərək, suda təqdim edən E-loan (www.e-loan.com) kompaniyasını və qiymətli kağızlarla ticarəti təşkil edən E-Trade (www.e-trade.com) kompaniyasını göstərmək olar. Əksər informasiya və analitik agentliklər informasiya brokerləri adlanır. Bir sıra banklar da öz Web-səhifələrində müxtəlif iqtisadi göstəriciləri, indeksləri, valyuta kurslarını nəşr edərək informasiya brokeri rolunda çıxış edirlər.




Şəkil 7. Qiymətli kağızlarla ticarəti təşkil edən E-Trade (www.e-trade.com)

kompaniyası.

- Elektron xidmət provayderi (*e-services providers*) – bu İnternetdə müəssisənin virtual ofisi deyil, fəaliyyətinin çox hissəsi bilavasitə İnternet vasitəsilə həyata keçirilən müəssisədir. Daha doğrusu, bu virtual və ya onlayn müəssisədir. Elektron-kommersiya bazarında fəaliyyət göstərən ən məhşur provayder – *Amazon.com* (www.amazon.com) virtual kitab mağazasıdır.




Şəkil 8. Məşhur amerikan İnternet kitab mağazası – Amazon.com

- digər nümunə İnternet-banklar və ya Virtual-banklar (*Virtual bank*), şəbəkə-bankları (*net-only banks*), elektron-banklar (*e-banks*) və onlayn-banklar (*online-banks*) ola bilər. İnternet-bank şöbələri və filialları olmayan və bank xidmətlərinin tam spektirini təqdim edən təşkilatdır. Aşağıdakı İnternet-bankları qeyd etmək olar: www.electonicbanker.com, www.open-vision.com, www.firstdirect.com, www.egg.co.uk, www.advance-bank.de və başqaları. Bu internet banklar öz müştərilərinə məsafədən özünəxidmət təşkil edir və onların xidmətləri klassik banklara nisbətən ucuzdur. Çünki, burada bütün proses avtomatlaşdırılmışdır və buna görə də əmək haqqı, icarə haqqı kimi ödəmələrdən azaddırlar.

# NƏTİCƏ VƏ TƏKLİFLƏR

Beləliklə, göründüyü kimi informasiya təhlükəsizliyinə nail olma zamanı ən vacib məsələlər – informasiyanın əlverişliliyinin, məxfiliyinin, tamlığının və hüquqi əhəmiyyətliliyinin təmin olunmasıdır.Burada hər bir potensial təhlükə bu dörd xüsusiyyəti və ya informasiya təhlükəsizliyinin keyfiyyətini nə dərəcədə əhatə etməsi nöqteyi nəzərindən təhlil edilməlidir.İnformasiyanın məxfiliyi dedikdə, məhdud giriş imkanı ilə xarakterizə olunan informasiyanın yalnız öz təyinatı üzrə istifadə edilməsi başa düşülür. Tamlıq anlayışı altında informasiyanın aktuallığı , ziddiyyətsizliyi, onun arzuolunmaz dəyişikliklərdən müdafiəsi başa düşülür. Tamlıq verilənlərin müxtəlif təsiri nəticəsində öz informasiya məzmunlarını və interpritasiyasının bir qiymətliliyinin saxlanmasıdır. İnformasiyanın əlverişliliyi, lazımi səlahiyyətlərə malik olan informasiya subyektlərinə maneəsiz çıxışı təmin etmək qabiliyyəti ilə müəyyən olunur. İnformasiyanın hüquqi əhəmiyyətliliyi isə bizim ölkədə informasiya təhlükəsizliyinin hüquqi-normativ bazasının yaradılması ilə əlaqədar olaraq daha vacib əhəmiyyətə malik olmağa başlamışdır.

Bu gün dünya üzrə bir sıra şirkətlər elektron ticarət sistemlərində hüquqi əhəmiyyətə malik olan elektron sənəd dövriyyəsinin təşkil olunması məqsədilə fəal işlər həyata keçirirlər.Bunun üçün Azərbaycanda da o cümlədən, elektron ticarət sferasında hüquqi əhəmiyyətə malik olan sənəd dövriyyəsinin təhlükəsiz şəkildə həyata keçirilməsi üçün bir neçə mühüm tədbirləri həyata keçirtmək lazımdır.Birincisi, "tipik işçi yeri" qismində sertifikatlaşdırılmşı proqram – apparat kompleksindən istifadə olunmalıdır.Elektron rəqəmsal açarların ümum istifadə informasiya sistemində istifadə edilməsi məqsədilə yaradılması zamanı elektron rəqəmsal sertifikatların yalnız sertifikatlaşdırılmış vasitələri tətbiq olunmalıdır. Bundan başqa, müxtəlif təsdiqedici mərkəzlər tərəfindən verilən ticarət meydançalarının istifadəçilərinin sertifikatları arasında etibar sisteminin formalaşdırılması zəruridir.

Azərbaycan Milli Elmlər Akademiyasının İnformasiya Texnologiyaları İnstitutunun verdiyi məlumata əsasən, bu yaxınlarda informasiya təhlükəsizliyinin təmin edilməsi sistemlərində kriptoqrafik mühafizə vasitələrinin tətbiqi üzrə kriptoqrafik mühafizə vasitələrinin işlənməsi və konsaltinq xidmətlərinin göstərilməsi layihəsi formalaşdırılmışdır.Bu layihə informasiya təhlükəsizliyinin konfidensiallıq, informasiyanın bütövlüyü, elektron imza, elektron ödəmələr və s. ilə əlaqədar məsələləri yüksək təhlükəsizlik səviyyəsində və iqtisadi cəhətdən daha səmərəli şəkildə həll etməyə imkan verir. Layihə yeni kriptoqrafik alqoritmlərin işlənməsi, mövcud kriptoqrafik alqoritmlərin qiymətləndirilməsində, seçilməsində, onların müxtəlif hesablama mühitlərində və platformalarında reallaşdırılmasında mütəxəssis məsləhətlərinə, müxtəlif tövsiyələrin hazırlanmasına, informasiyanın kriptoqrafik mühafizəsinin proqram vasitələrinin işlənməsinə də şərait yaradır.

Iqtisadiyyatın elektronlaşdırılmasının bariz nümunəsi ölkədə elektron kommersiyanın formalaşması və inkişafıdır. Lakin hələlik ölkəmizdə bu sahə lazımi şəkildə inkişaf etməmişdir. Bütövlükdə iqtisadiyyatın elektronlaşdırılması aşağıdakı səbəblərdən ləngiyir:

- Çeklər və bank kartları üzrə ödəniş mexanizmlərinin az inkişaf etməsi;
- «Aznet»də ticarəti həyata keçirməyə hazır olan ölkə əhalisinin informasiya savadının aşağı səviyyədə olması;
- Normativ-hüquqi təminatın qeyri-kamilliyi;
- Ticarət münasibətləri iştirakçıları tərəfindən qarşılıqlı öhdəliklərin pozulması;
- Nahid nizama salınmış çatdırılma sisteminin olmaması.

Bu gün üçün ölkədə artıq təxminən 50 virtual mağaza işləyir. Məhsulların siyahısı və qiymətləri saytlarda yerləşdirir, lakin onlayn ödənişlər sistemi olmadığından bütün hesablaşmalar məhsul əldə edilərkən həyata keçirilir. Əsasən, "Aznet"də məişət texnikası, mebel, geyim, kosmetika və parfümeriya, kompüter, mobil telefon və aksessuarlar, daşınmaz əmlak, avtomobillərin satışı üzrə virtual mağazalar populyardır. Tədqiqatlar göstərir ki, istehlakçıları daha çox saytdan və ya web-mağazadan istifadə etməyin, eləcə də şəxsi məlumatın qorunub saxlanmasına zəmanət verilməsinin rahatlığı cəlb edir. Bundan başqa, virtual

əməliyyatların təhlükəsizliyinin təmin edilməsi ilə bağlı problemlər də ortaya çıxır ki, bunun da həlli bütün dünyada çətinlik yaradır. Təcrübə göstərir ki, müştərilərin vəsaitlərinin təhlükəsizliyini təmin etmək üçün zəruri olan proqram təminatı 15-20 min ABŞ dolları civarındadır. Çox vaxt asan yolla pul qazanmaq istəyənlər alıcı vəsaitinin təhlükəsizliyinə göz yumurlar. Mütəxəssislərinin fikrincə, sözün geniş mənasında, elektron kommersiyası sahəsində başlıca çatışmayan cəhət, ilk növbədə, onun imkanlarının kifayət qədər fəal təbliğ olunmaması və xüsusilə B2B sahəsində uğurla həyata keçirilən qərarların kifayət qədər nümayiş etdirilməməsi ilə bağlıdır. Elektron kommersiyasının təşkili üçün standart proqram həlləri də lazımi qədər deyil – burada müəlliflər və distrübütorlar üçün yeni imkanlar açılır. Rəqəmli imzalar, sertifikatlar və şifrləmə vasitələri kifayət qədər inkişaf etməyib, daha dəqiq desək, ümumiyyətlə inkişaf etməyib. İnternet texnologiyalar, elektron kommersiyası sistemlərindən istifadə edilməsi yeni müştərilərin cəlb olunması üzrə daha səmərəli üsul əldə etməyə, əhatə dairəsini genişləndirməyə, mövcud müştərilər üçün əlavə servisi təmin etməyə, kommunikasiyalara, eləcə də sifarişlərin qəbulu və işlənməsinə çəkilən xərcləri azaltmağa imkan verir. Böhranlı şəraitdə bir çox şirkətlər elektron kommersiyasına biznesin səmərəli şəkildə aparılması üçün alət kimi müraciət edə bilər. Bundan başqa, xüsusilə bank sahəsində qapalı klub ödəniş sistemləri, agent-bank şəbəkələrinin yaradılması e-ticarətin inkişafında problemlər yaradır. E-ticarətin inkişafı home-banking kimi xidmətlərin yayılması da daxil olmaqla bank xidmətlərinin internetləşdirilməsini tələb edir. Elektron kommersiyanın təşkili üçün standart proqram həlləri də lazımi qədər deyil - burada müəlliflər və distribütorlar üçün yeni imkanlar açılır. Rəqəmli imzalar, sertifikatlar və şifrləmə vasitələri kifayət qədər inkişaf etməyib. İnternet texnologiyalar, elektron kommersiyası sistemlərindən istifadə edilməsi yeni müştərilərin cəlb olunması üzrə daha səmərəli üsul əldə etməyə, əhatə dairəsini genişləndirməyə, mövcud müştərilər üçün əlavə servisi təmin etməyə, kommunikasiyalara, eləcə də sifarişlərin qəbulu və işlənməsinə çəkilən xərcləri azaltmağa imkan verir. Bundan başqa, ölkəmizdə İKT-nin geniş tətbiqi və internet istifadəçilərinin sürətlə artımı e-ticarətin yaranmasına və inkişaf etməsinə zəmin

yaratmışdır. Ehtimal olunur ki, bu işlərin praktiki reallaşdırılması e-ticarətin, e-ödənişlərin geniş miqyasda istifadəsi üçün.əlverişli şərait yaradacaqdır. Hazırda dünya ölkələrində sənaye müəssisələri İKT-nin imkanlarından daha geniş şəkildə bəhrələnmək məqsədilə B2B layihələri üzərində iş aparırlar. B2B sənaye müəssisələrinin sürətli texnikanın tətbiqinə əngəl törədən əsas maneələrdən biri - ümumi avtomatlaşdırmanın aşağı səviyyədə olmasıdır. Azərbaycanda da B2B-layihələrinin Qərbdə olduğu kimi effektiv və səmərəli surətdə həyata keçirilməsi məqsədəuyğundur. Qərbdə e-ticarət meydançalarının əsasını biznes alyansları, biznesin şəffaflığı və yaxşı təşkili, ticarət meydançası iştirakçılarının texnoloji cəhətdən qarşılıqlı əlaqəyə hazır olması təşkil edir. Hazırda respublikamızda iqtisadiyyatın şəffaflığı və onun dünya iqtisadiyyatına inteqrasiyası istiqamətində böyük işlər görülür. Azərbaycanın sənaye müəssisələrində sifarişlərin qəbul edilməsi və yerinə yetirilməsi, istehsalatın planlaşdırılması, təchizat və satış üzrə avtomatlaşdırılmış sistemlər yaranır, eləcə də mallar, uçot sistemi, satışları idarəetmə sistemi üzrə hazır göstəricilər bazası və həmin bazanın internet vasitəsilə inteqrasiyası formalaşdırılır. Bundan əlavə, Azərbaycanda korporativ saytların işlənib hazırlanması sahəsində təcrübə artır, İnternetin Azərbaycan seqmentində ticarət meydançaları yaradılır. Deməli, Azərbaycanda sənaye müəssisələrinin məhsulunu istifadəçiyə həm də alternativ yolla - elektron ticarət vasitəsilə çatdırmağın real zəminləri vardır.

# ƏDƏBİYYAT SİYAHISI


1. Donal O'Mahony, Michael Pierge, Hitesh Tewari "Electronic Payment Systems for E-Commerse", second edition, London 2001;
2. Godfried B.Williams "Online Business Security Systems",UK 2007;
3. Benjamin Graham "The Evolution of Electronic Payments", Quinsland 2003.
4. А.А.Малюк "Информационная Безопасность", Москва 2004;
5. В.А.Галатенко «Основы информационной безопасности» Москва 2003;
6. Попов В.Б «Основы информационных и телекоммуникационных технологий», Москва 2005;
7. Баричев С. «Криптография без секретов» , Москва 2005;
8. Cisco Systems , Inc., "Руководство по технологии объединенных сетей", Киев 2005;
9. Алексунин В.А. Электронная коммерция и маркетинг в интернете. – М.: Дашков и К ИТК, 2005.
10. Вулкан Н.В. Электронная коммерция: Стратегическое руководство для понимания и построения торговли в режиме "он-лайн". – М.: Интернет-трейдинг ООО, 2003.
11. http://www. daily.sec.ru/
12. http://www. yury.name/crypto
13. http://www.sirius.ru
14. http://www.cryptopro.ru
15. http://www.webmoney.ru
16. http://www.ase.md
17. http://www.leo-arek.narod.ru
18. http://www.e-port.ru
19. http://www.piter.com
20. http://www.pmik.petrsu.ru

## РЕЗЮМЕ

Мы находимся на поток информации - от дня мы живем в обществе, где высокие темпы роста. Эта информация поступает с теми, кто может прийти только через использование информационных технологий.Стремительное развитие информационных технологий в последние годы показывает, что вычислительная наука - научно-исследовательские работы, и организация хозяйственной деятельности, процессы принятия управленческих решений и применение в других областях человеческой деятельности легко быстрее решать вопросы, и вы можете играть очень важную роль в достижении нужных результатов.

В настоящее время большинство стран во всех областях, а также повышение эффективности экономики и экономики в информационных и коммуникационных технологий играют важную роль в повышении производительности труда.Цифровизации из самых важных экономических вопроса.

Оцифровка и системы безопасности для решения проблем экономики, укрепление безопасности является важным вопросом.

Магистерская диссертация представляется в роли информационных технологий в управлении экономической активности в стране, экономика и страна исследованы факторы, влияющие на электронной автоматизации, тенденции развития экономики были изучены.

## ABSTRACT

We are living in the society that information flow is increasing everyday. For solving this information flow problem we have to apply information and communication technologies in this regard. At recent years development of information technologies indicates that ICT has essential role in research and development, formatting economy proses, menegment and other sectors.

Now at the every country of the world as every sectors as economy they use information and communication technologies for increasing effectiveness and efficiency.

At the direct of solving safety issues and improving activity of safety systems is important problem.

At this master dissertation role of information and communication technologies in economy activity and factors of that influence electron economy was studied and complication of electron economy has investigated.