Elektron kommersiyanın təhlükəsizliyinin təmin edilməsi problemləri

Aybəniz Əliyeva, Leyla Əkbərova

AMEA İnformasiya Texnologiyaları İnstitutu

[1]aybeniz63@rambler.ru, [2]akberovaleyla@ramblerl.ru

***Xülasə*— Məqalədə elektron kommersiyanın təhlükəsizliyi məsələsi nəzərdən keçirilmişdir. Elektron kommersiyanın informasiya təhlükəsizliyi ilə bağlı təhdidləri, onların növləri və aradan qaldırılması yolları göstərilmişdir.**

Açar sözlər—elektron kommersiya; elektron biznes; informasiya təhlükəsizliyi; elektron mağaza

I. GİRİŞ

Son zamanlar İnternet şəbəkəsi vasitəsilə həyata keçirilən elektron kommersiya və ya elektron ticarət dünyada sürətlə inkişaf edir. Müəssisələrin və əhalinin əhəmiyyətli hissəsinin istifadə etdiyi yeni elektron bazarlar daha böyük əhəmiyyət daşımağa başlayır. Elektron şəbəkələrdə həyata keçirilən kommersiya fəaliyyəti bir çox fiziki məhdudiyyətləri aradan qaldırır. Biznesin bu sektoru xidmətləri və malları İnternet şəbəkə vasitəsilə istənilən yerdən, istənilən zaman anında istehlakçıya təqdim etmək imkanına malik olur.

Cəmiyyətin globallaşması və İnternetin açıqlığı, zaman və məkanın qeyri-məhdudluğu elektron kommersiya (e-kommersiya) texnologiyaları vasitəsilə həyata keçirilən tranzaksiya prosesləri üçün bir sıra təhlükələrin yaranmasına səbəb olur. İnformasiya təhlükəsizliyi e- kommersiyanın inkişafi üçün əsas faktordur. Ona görə də açıq şəbəkə mühitində həyata keçirilən e-kommersiyanın təhlükəsizliyinin tədqiqi məsələsi çox aktual və vacib məsələdir.

II. E-KOMMERSİYANIN TƏHLÜKƏSİZLİYİ

E-kommersiyanın iqtisadi təhlükəsizliyinin təmini probleminin həlli ilk növbədə istifadə olunan informasiya texnologiyalarının təhlükəsizliyinin təmini ilə bağlıdır.

Kommersiya əməliyyatlarının həyata keçirilməsinə qoyulan əsas tələblər konfidensiallıq, tamlıq, autentifikasiya, avtorizasiya, zəmanət və sirrin qorunmasından ibarətdir.

İnformasiyanın təhlükəsizliyinə nail olmaqda onun əlyetərliliyinin, məxfiliyinin, tamlığının və hüquqi əhəmiyyətinin təmini əsas məsələlərdir. İnformasiyanın məxfiliyi onun yalnız nəzərdə tutulmuş fərdlər (obyektlər) üçün əlyetərli olması, informasiyanın tamlığı dedikdə isə onun təhrif olunmamış şəkli başa düşülür. İnformasiyanın əlyetərliyi sistemin həmin informasiyaya səlahiyyəti çatan subyektlərin maneəsiz girişinin vaxtında təmini etməsi qabiliyyəti ilə müəyyən olunur. İnformasiyanın hüquqi əhəmiyyəti informasiyanın təhlükəsizliyinin hüquqi-normativ bazasının yaradılması ilə müəyyən olunur.

Əgər ilk dörd tələb texniki vasitələrlə təmin olunursa, son iki tələbin yerinə yetirilməsi texniki vasitələrdən və ayrı-ayrı şəxslərin və təşkilatların məsuliyyəti, həmçinin istehlakçını satıcıların mümkün fırıldaqlarından müdafiə edən qanunların yerinə yetirilməsindən asılıdır.

İnformasiya təhlükəsizliyinin kompleks şəkildə təmini çərçivəsində ilk öncə e-biznesin təhlükəsizliyi sahəsindəki əsas problemlər kimi aşağıdakıları ayırmaq olar:

- informasiyanın rabitə kanalı ilə ötürülməsinin mühafizəsi;
- kompüter sistemlərinin, verilənlər bazasının və elektron sənəd dövriyyəsinin mühafizəsi; informasiyanın uzunmüddətli elektron şəkildə saxlanılmasının təmini;
- tranzaksiyaların təhlükəsizliyinin, kommersiya informasiyasının məxfiliyinin, autentifikasiyasının, intellektual mülkiyyətin qorunmasının təmini və s. [1].

İnternet texnologiyalarının açıq xarakteri, şəbəkə vasitəsilə ötürülən informasiyanın əlyetərliliyi göstərir ki, e-kommersiyanın informasiya təhlükəsizliyinin təmini e-kommersiyanın subyektlərinin ümumi mənafeyinə xidmət edir. İnformasiya təhlükəsizliyi partnyorların qarşılıqlı əlaqə üzrə autentifikasiyasının, şəbəkə vasitəsilə ötürülən informasiyanın tamlığının və məxfiliyinin, servislərin əlyetərliliyinin və infrastrukturun idarə oluna bilməsinin təminini özündə birləşdirir.

İnformasiya təhlükəsizliyi e-kommersiyanın inteqral təhlükəsizliyinin əsas elementlərindən biridir.

Bütün dünya üzrə informasiya sistemlərinə olan hücumların sayı hər il iki dəfədən çox artır. Belə bir şəraitdə elektron kommersiyanın təhlükəsizlik sistemləri müxtəlif və çoxsaylı daxili və xarici təhdidlərə müqavimət göstərməli olur.

E-kommersiyanın informasiya təhlükəsizliyinin əsas təhdidləri aşağıdakılarla bağlıdır [2]:

- e-kommersiyanın subyektlərinin mənafeyinin əksinə yönəlmiş qərəzli xarakter daşıyan ziyanlar (kompüter cinayətləri və kompüter virusları);
- xidmətçi personalın düşünülməmiş hərəkətləri (səhvi, diqqətsizliyi və s.);
- informasiyanın təhrif olunmasına və pozulmasına (məhv olmasına) səbəb olan texniki faktorların təsiri (elektrik enerjisinin kəsilməsi, proqramın dayanması);
- texnogen faktorların təsirləri (təbii fəlakətlər, yanğınlar, irimiqyaslı qəzalar və s.).

Təhlükəsizlik təhdidləri praktiki olaraq əhəmiyyəti və təsirləri məlum olmayan faktorlarla bağlı ola bilərlər.

E-kommersiya ilə məşğul olan müəssisədə informasya təhlükəsizliyinin pozulması ilə bağlı baş verən ziyanı birbaşa və dolayı yolla baş verən ziyana (itkilərə) bölmək olar.

Birbaşa ziyanlar dəyərlə ifadə oluna bilərlər [3]:

- yanğın, təbii fəlakət, oğurluq, soyğunçuluq, istismardakı (işə salmadakı) xətalar, xidmət edən heyətin ehtiyatsızlığı, kompüter sistemlərinin qırılması və virusların təsiri nəticəsində korlanmış və ya fiziki olaraq itmiş informasiyanın bərpası;
- elektron şəkildə həyata keçirilən pul vəsaitlərinin və qiymətli kağızlarla qeyri-qanuni əməliyyatlar, həmçinin pis niyyətlə verilənlərin dəyişdirilməsi, elektron daşıyıcılarında informasiyanın saxlanılması, nəqli və ya köçürülməsi zamanı verilənlərin qəsdən korlanması, verilənlərin elektron ötürülməsi şəbəkələrində saxtalaşdırılmış sifarişlərin ötürülməsi və alınması və s.;
- el-kommersiyanın subyektlərinə vurulan fiziki və ya madii ziyanın ödənilməsi.

Dolayı yolla dəyən ziyan əmək haqqının ödənilməsi, kreditlər üzrə faizlər, icarə haqqının ödənilməsi, müəssisənin təhlükəsizliyinin pozulması üzündən müəssisənin kommersiya fəaliyyətinin məcburi dayandırılması zamanı meydana çıxan amortizasiya və itirilmiş gəlirlərin cari xərclərində ifadə oluna bilərlər.

III. E-KOMMERSİYAYA OLAN TƏHDİDLƏRİN NÖVLƏRİ

E-kommersiyaya olan təhlükələrin aşağıdakı növləri vardır [4]:

- Sistemə kənardan müdaxilə
- Şirkətin içərisinə icazəsiz daxil olma
- Qərəzli şəkildə informasiyanı ələ keçirmək və oxumaq
- Qəsdən verilənlərin və ya şəbəkənin pozulması
- Istifadəçinin fırıldaqçılıq məqsədilə yanlış identifikasiyası
- Proqram-aparat mühafizəsinin qırılması
- Istifadəçinin bir şəbəkədən digərinə icazəsiz girişi
- Virus hücumları
- Xidmətdən imtina
- Maliyyə fırıldaqları

Bu təhdidlərin qarşısının alınması üçün müxtəlif texnologiyalara əsaslanan bir sıra üsullardan istifadə olunur: şifrələmə - verilənlərin oxunmasına, təhrif olunmasına maneə yaratmaq məqsədilə verilənlərin kodlaşdırılması, göndərənin və alanın şəxsiyyətinin həqiqiliyini yoxlayan rəqəmsal imzalar; elektron açarların istifadəsilə stealth-texnologiyaları; brandmauerlər; virtual və xüsusi şəbəkələr.

Bu metodlardan heç biri universal xarakter daşımır. Avtomatik mühafizənin sındırılmasına qarşı tamamilə etibarlı üsul yoxdur.

Elektron kommersiyanı həyata keçirən şirkət aşağıdakı təhdidlərlə qarşılaşır [5]:

- Elektron mağazanın serverinin veb-səhifəsinin qəsdən dəyişdirilməsi, sorğuların başqa serverə göndərilməsi, müştəri haqqında məlumatın, xüsusilə də onun kredit kartı ilə bağlı informasiyanın kənar şəxslər üçün əlyetərli edilməsi;
- elektron mağazanın əməkdaşları tərəfindən yalan sifarişlərin və müxtəlif fırıldaq növlərinin yaradılması (statistika göstərir ki, kompüter münaqişələrinin yarısından çoxu əməkdaşların şəxsi fəaliyyəti ilə bağlıdır);
- e-kommersiya şəbəkəsi ilə göndərilən verilənlərin ələ keçirilməsi;
- cinayətkarların şirkətin daxili şəbəkəsinə soxulması və e-kommersiya komponentlərinin gözdən salınması;
- "xidmətdən imtina" kimi hücumların həyata keçirilməsi və elektron kommersiyanın fəaliyyətinin pozulması və ya e-kommersiya qovşağının sıradan çıxması.

Belə təhdidlərin nəticəsində şirkət müştərilərin inamını, potensial və yarımçıq qalmış sövdələşmələrdən gələn pul vəsaitini itirir, e-mağazanın fəaliyyəti pozulur, onun işinin bərpası üçün vaxt, pul və insan resursları sərf olunur.

IV. E-KOMMERSİYANIN TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİ

Təhlükəsizliyin təmini elektron biznesin uğurla aparılması üçün zəruri şərt olmaqla yanaşı, həm də kontragentlər arasında etibarlı münasibətin qurulması üçün fundamentdir. Ona görə də veb serverə, veb proqramlara giriş, istifadəçilərin autentifikasiya və avtorizasiyası, verilənlərin tamlığının və məxfiliyinin təmini, rəqəmsal imzanın həyata keçirilməsi və s. kimi məsələlər də daxil olmaqla təhlükəsizliyin təmini kompleks xarakter daşıyır.

Hazırda dünyada İnternet vasitəsilə həyata keçirilən elektron kommersiyanin inkişafında şəbəkə vasitəsilə ötürülən informasiyanın mühafizəsinə böyük diqqət yetirilir. Bununla əlaqədar olaraq müxtəlif ixtisaslaşmış protokollar geniş yayılmışdır.

Bir çox ölkələrdə elektron biznesin İnformasiya təhlükəsizliyinin problemlərinin həlli ilə bağlı müstəqil konsorsium (İnternet Security Task Force (İSTF)) məşğul olur. Bu təşkilat informasiya təhlükəsizliyinin ilk növbədə elektron biznes təşkilatçılarının diqqət yetirməli olduqları on iki sahəni ayırır [6]:

- İdentifikasiya olunan informasiyanın obyektiv təsdiq mexanizminin olması.
- Fərdi, özəl informasiyaya uyğun qaydanın olması
- Təhlükəsizlik hadisəsinin təyini
- Korporativ perimetrin mühafizəsi
- Hücumun təyini
- Potensial və təhlükəli hallara nəzarət
- Girişə nəzarət
- İnzibatçılıq etmə
- Hadisəyə reaksiya.

Bir çox təhlükələrin qarşısını almaq məqsədilə *rəqəmsal imza (Rİ)* alqoritmlərindən istifadə olunur. Rİ nəinki informasiya göndərənin əsilliyinin müəyyən olmasına, həm də məlumatın tamlığının qorunmasına xidmət edir.

İnformasiya göndərənin əsilliyinin müəyyən olması üçün, Rİ-dən istifadə zamanı gizli və açıq açarlar tətbiq olunur. Proses asimmetrik şifrlənməyə oxşayır, amma bu halda gizli

açar şifrləmək üçün, açıq açar isə şifri açmaq üçün istifadə olunur [6].

Şübhəsiz ki, informasiya təhlükəsizliyinin təminin ilə mütəxəssislər məşğul olmalıdırlar. Lakin bu məsələ mülkiyyət formasından asılı olmayaraq bu və ya digər təsərrüfat subyektlərinin iqtisadi təhlükəsizliyinə məsul olan rəhbər işçilərin diqqət mərkəzində olmalıdır. Onlar üçün informasiya təhlükəsizliyinin kompleks sisteminin təşkili üçün zəruri olan əsas funksional komponentlər aşağıda verilmişdir [7]:

- Kommunikasiya protokolları;
- Kriptoqrafiya vasitələri;
- Avtorizasiya və autentifikasiya mexanizmləri;
- Ümumi istifadə şəbəkəsindən işçi yerə girişə nəzarət vasitələr;i
- Antivirus kompleksləri;
- Audit proqramları;
- Istifadəçilərin girişinə, həmçinin verilənlər paketinin təhlükəsiz mübadiləsinə, açıq şəbəkələr üzrə istənilən məlumatlara nəzarətin mərkəzləşdirilmiş vasitələri.

E-kommersiyada həyata keçirilən tranzaksiyalarda təhlükəsizliyinin təminatında protokolların xüsusi yeri və rolu vardır. E- kommersiyada protokol adı altında tranzaksiya iştirakçılarının 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.

İnternetdə verilənlərin təhlükəsiz ötürülməsinin təmini məqsədilə SSLl, SET, IPSEC kimi protokollar geniş istifadə olunur.

Elektron kommersiya sistemlərinin quruluşu zamanı istifadə olunan ən geniş yayılmış protokol *Secure Sockets Layer (SSL) protokoludur*. Verilənlərin ötürülməsində SSL protokolunun istifadə etdikdə verilənlər şifrələnir, serverin autentifikasiyası aktivləşir [5, 6, 8].

SSL texnologiyası TCP/IP protokolu ilə fəaliyyət göstərən, web-server və web-brauzer arasındakı bütün məlumat axınını mühafizə edən etibarlı bir protokoldur. SSL protokolu iki tərəf arasında etibarlı və məxfi əlaqənin təmin edilməsində çox mühüm funksiyanı həyata keçirir. SSL bağlantısı vasitəsilə göndərilən verilənlər üçüncü şəxslər tərəfindən modifikasiya edildikdə və ya oğurlandıqda tranzaksiyanın bütün iştirakçıları bundan xəbərdar olur [2].

SSL sxemlərində müştərinin autentifikasiyasının yoxluğu bu protokolun ən böyük çatışmamazlığıdır. Belə ki, SSL protokolundan istifadə zamanı kartın rekvizitləri ilə əlaqədar informasiyanın məxfiliyi təmin olunmur. Bu nöqteyi nəzərdən SET protokolundan istifadə etmək daha məqsədyönlüdür.

SET (Security Electronics Transaction) – elektron ticarətin təhlükəsizliyini təmin edən daha perspektivli təhlükəsizlik protokoludur. SET protokolu az 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 da rəqəmsal imzalardan istifadə olunur. Açıq protokollar yığımından müxtəlif istehsalçıların realizasiyaları arasındakı qarşılıqlı əlaqənin təmin olunmasında istifadə olunur [2,8].

Kənardan icazəsiz girişin aşkarlanması sistemləri (İntrusion Detection Systems, İDS) hücumların sxemlərini və ya əlamətlərini identifikasiya edə bilir və qanunsuz giriş mənbələri ilə əlaqənin kəsilməsi ilə bağlı qəza siqnalları göndərmək imkanına malikdirlər. Bu sistemlər həmçinin xidmətdən imtina hallarının qarşısını ala bilərlər [6].

NƏTİCƏ

İnternet mühitdə biznes prosseslərin inteqrasiyası təhlükəsizliyin təmini ilə bağlı mühüm dəyişiklərə gətirib çıxarır. Elektron sənədə əsasən yaranan qanun və məsuliyyət sənəd göndərənlə yanaşı onu alanın da bütün təhlükələrdən hərtərəfli mühafizəsini tələb edir. Ona görə də elektron kommersiya müəssisələrinin rəhbərləri informasiya təhlükəsizliyinin, öz serverlərinin mühafizəsinin ciddiliyini nəzərə almalıdırlar.

E-kommersiyanın təhlükəsizliyinin təmini məqsədilə tədbirlərin keçirilməsi məqsədəuyğundur. Həyata keçirilən təhlükəsizlik tədbirlərinin həcmi mövcud təhlükələrə uyğun olmalıdır. Əks təqdirdə təhlükəsizlik sistemləri iqtisadi cəhətdən səmərəli olmayacaq. Bununla əlaqədar olaraq e-kommersiyanın təhlükəsizliyinin təmini üzrə aparılan tədbirlərin səmərəliliyi üçün bir sıra kriteriyalar qəbul edilir. Bu kriteriyalar təhlükəsizliyin pozulması zamanı baş verən itkilərin müqayisəsinə və e-kommersiyanın təhlükəsizliyinin təmini üzrə aparılan tədbirlərin dəyərinə əsaslanır.

ƏDƏBİYYAT

[1] Е.В.Сибирская, О.А Старцева. Э-коммерция. М.: Форум, 2010.

[2] З. Р. Абдеева “ Проблемы безопасности электронной коммерции в сети Интернет”, Проблемы современной экономики, N 1(41), 2012.

[3] Безопасность электронной коммерции. http://studopedia.info/Ekonomika/

[4] M Niranjanamurthy, C. Dharmendra “The study of e-commerce security issues and solutions,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, No. 7, 2013, pp. 2885-2895.

[5] В.Н. Ясенев, “Информационная безопасность в экономических системах: Учебное пособие.” Н. Новгород: Изд-во ННГУ, 2006.

[6] Информационная безопасность в электронной коммерции - http://stud24.ru/information/informacionnaya-bezopasnost-v-jelektronnoj-kommercii/143095-420091-page1.html

[7] Li Fu-Guo, Dong Yu-Jie, “Realization of information security in electronic commerce,” Proceedings of the Third International Symposium on Computer Science and Computational Technology(ISCSCT ’10), 2010, pp. 014-016.

[8] Безопасность в электронной коммерции – center-yf..ru