UOT 004.9:351

İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@lan.ab.az

E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİNƏ ETİMADIN QİYMƏTLƏNDİRİLMƏSİ MODELİ

Vətəndaşların e-dövlətin informasiya təhlükəsizliyinə etimadının təmin edilməsi e-dövlətin həqiqi potensialından tam istifadə edilməsi üçün xüsusi əhəmiyyət daşıyır. Bu məqalədə e-dövlətin informasiya təhlükəsizliyinə etimadın qurulması mexanizmləri analiz edilir və etimadın qiymətləndirilməsi üçün model təklif edilir. Model müxtəlif mənbələrdən alınmış etimad məlumatları əsasında hesablanmış reputasiya qiymətlərinin mənbələrin çəki əmsalları nəzərə alınmaqla inteqrasiyasına əsaslanır.

Açar sözlər: *e-dövlət, informasiya təhlükəsizliyi, etimad, reputasiya, informasiya təhlükəsizliyinə etimad.*

Giriş

E-dövlət informasiya və kommunikasiya texnologiyalarından istifadə etməklə, dövlət orqanlarının və vətəndaşların qarşılıqlı əlaqələrini həyata keçirməyə imkan verən müəyyən kommunikativ infrastrukturun qurulmasını nəzərdə tutur. E-dövlətin əsas məqsədi dövlət orqanları arasında koordinasiyanın yaxşılaşdırılmasını (ing. government to government, G2G), dövlət orqanları tərəfindən vətəndaşlara yüksək keyfiyyətli xidmətlərin göstərilməsini (ing. government to citizens, G2C), dövlət orqanları ilə biznes sektoru arasında qarşılıqlı əlaqənin effektivliyinin yüksəldilməsini (ing. government to business, G2B), qərarların qəbulunda dövlətlə vətandaşlar arasında qarşılıqlı əlaqənin tənzimlənməsini (ing. government to non-government organizations, G2N), dövlət və elm, texnologiya, innovasiya sektoru arasında qarşılıqlı əlaqəni (ing. government to knowledge, G2K) təmin etməkdir [1].

Lakin vətəndaşların e-dövlət xidmətlərindən istifadə səviyyəsi bir sıra səbəblərdən arzu olunan səviyyədən geri qalır [2]. E-dövlət sistemlərinə etimadın olmaması e-dövlət xidmətlərinin yayılmasına əsas maneələrdən biridir [2, 3]. Onlayn mühitdə etimad üçün maneələr identifikatorların və şəxsi xarakteristikaların olmamasından, qeyri-müəyyənlik şəraitindən qaynaqlanır. Bu faktorlar e-dövlət xidmətlərindən istifadə zamanı informasiya təhlükəsizliyi risklərini artırır.

Etimad risklə birbaşa bağlıdır və qərar qəbul etdikdə nəzərə alınır. Istifadəçilərin e-dövlət xidmətlərindən istifadə etmək qərarı onların e-dövlətin informasiya təhlükəsizliyinə olan etimadının səviyyəsindən asılıdır. Beləliklə, e-dövlət xidmətlərinin istifadəsi zamanı informasiya təhlükəsizliyinə etimad məsələsi ön plana çıxır.

Bu işdə e-dövlətin informasiya təhlükəsizliyinə etimadın formalaşdırılması və qiymətləndirilməsi sahəsində mövcud problemlər analiz edilir. Məqalədə informasiya təhlükəsizliyinə etimad anlayışının məzmununa müxtəlif yanaşmalar analiz edilir və informasiya təhlükəsizliyi ilə etimadın qarşılıqlı əlaqəsi aydınlaşdırılır. Daha sonra e-dövlətin informasiya təhlükəsizliyinə etimadın komponentləri müəyyən edilir və e-dövlətin informasiya təhlükəsizliyinə etimadın ölçülməsi modeli təklif edilir.

Etimad anlayışı

Etimad fundamental insan davranışıdır. Etimad subyektlərin bir-birindən qarşılıqlı asılılığı nəticəsində meydana çıxır. Cəmiyyətin həyatı onun üzvləri arasındakı etimaddan çox asılıdır, etimadı çox zaman cəmiyyətin "yapışqanı" adlandırırlar. Etimad bütün növ sosial institutların

əsası hesab olunur. Etimad şəxsiyyətin sosial qruplarla və təşkilatlarla qarşılıqlı əlaqəsinin vacib amilidir.

Etimad humanitar (sosiologiya, psixologiya, iqtisadiyyat, politologiya) və texniki elmlərin müxtəlif sahələrində mühüm rol oynayır [4]. Etimada tərif vermək çətindir, çünki etimadın müxtəlif növləri var və onlar konkret kontekstdən asılı olurlar.

Psixoloqlar etimadı mental münasibətlər kimi öyrənir və insan etimad etdikdə və ya etimad etmədikdə, onun şüurunda nə baş verdiyini araşdırırlar [5]. Etimadın psixoloji konsepsiyası koqnitiv, emosional və davranış aspektlərini əhatə edir. Koqnitiv etimad modellərində etimad agentin inamı əsasında formalaşır və inamın dərəcəsinin funksiyası kimi müəyyən edilir [6]. Koqnitiv yanaşmada digər agentə etimad etməyə gətirib çıxaran psixi vəziyyətlər, eləcə də, qərarın və digər agentə etibar etmək hərəkətinin psixi nəticələri modelin mühüm hissələridir. Sosioloqlar etimadı insanlar arasındakı sosial münasibətlər kimi öyrənirlər [7]. Etimadın sosial konteksti multi-agent sistemlərdə geniş istifadə edilir [8, 9]. İqtisadçılar etimadı faydalılıq anlayışı baxımından araşdırırlar [10]. Oyunlar nəzəriyyəsi istifadəçilərin müxtəlif strategiyalar tətbiq etməklə, etimadı necə qurduğunu öyrənmək üçün populyar üsullardan biridir [11].

Kompüter elmləri sahəsindəki tədqiqatçılar bütün bu tədqiqatların nəticələrindən faydalanaraq e-kommersiya, p2p şəbəkələri, qrid kompyutinq, semantik veb, veb servislər və mobil şəbəkələr sahəsində etimadın rolunu öyrənirlər [12].

Bu məqalədə etimad termini aşağıdakı kimi başa düşülür.

Etimad münasibətlərinin qurulması zamanı əsasən iki aktor çıxış edir – *etibar edən aktor* (inamın subyekti, ing. truster) və *etibar edilən aktor* (inamın obyekti, ing. trustee).

Etimad – A subyekti tərəfindən irəli sürülən subyektiv ehtimaldır, ehtimal edilməsində məqsəd B subyektinin hər hansı bir əməliyyatı icra edib-etmədiyini proqnozlaşdırmaqdır.

Bu yanaşmada etimad dedikdə, etibarlılıq başa düşülür, etimadın subyektivliyi vurğulanır, asılılıq (hərəkətlərə kənar təsirin göstərilməsi) və mənfəət faktorları (aktor öz qazancını maksimumlaşdırmağa cəhd edir) göstərilir. Eyni zamanda, agentlər arasında qarşılıqlı əlaqənin təkrarlanan olduğu güman edilir.

Etimad müxtəlif elm sahələrində və müxtəlif tədqiqatçılar tərəfindən müxtəlif bucaqlardan öyrənilsə də, ümumi olan bəzi əsas cəhətləri müəyyən etmək olar:

- Etimad yalnız ətraf mühit qeyri-müəyyən və riskli olduqda rol oynayır.
- Etimad əsasında müəyyən qərarlar qəbul edilir.
- Etimad əvvəlki bilik və təcrübə əsasında qurulur.
- Etimad fərdi rəy və dəyərlərə əsaslanan subyektiv anlayışdır.
- Etimad yeni biliklə və zamanla dəyişir, lakin təcrübənin köhnə etimad üzərində üstün təsiri var.
- Etimad kontekstdən asılıdır.
- Etimad çoxşaxəlidir (“çoxsifətlidir”).

Etimad *statik* və *dinamik* ola bilər. Statik etimadın qiyməti zamanla dəyişmir. Dinamik etimadın qiyməti isə zamana görə dəyişir. Etimad situasiyadan asılıdır. Məsələn, subyekt etimada əsaslanan qərarında situasiyadan asılı olaraq sərhəd qiymətinə dəyişiklik edə bilər.

A agenti B-nin etibarlılığı (ing. trustworthiness) haqqında inama malik olduqda, A və B arasında *etimad münasibəti* mövcud olur. Lakin əks istiqamətdə inam (B agenti A-nın etibarlılığı haqqında) olmaya bilər, başqa sözlə, etimad münasibəti biristiqamətlidir (qeyri-simmetrikdir). Əgər iki agent arasında qarşılıqlı etimad münasibəti varsa, onu iki ayrı etimad münasibəti kimi təsvir etmək onları asılı olmadan emal etmək baxımından əlverişlidir.

Etimad münasibətlərinin *birbaşa etimad*, *tövsiyə olunan etimad* [13], *reputasiya əsasında qurulan etimad* [14] kimi növləri vardır. Əgər A B-yə etimad edirsə, bu münasibət birbaşa etimad münasibəti adlanır. Əgər A B-nin digər agentin etibarlılığı haqqında verdiyi tövsiyəyə etimad edirsə, onda A və B arasında tövsiyə olunan etimad münasibəti vardır. Reputasiya əsasında qurulan etimad münasibəti, paylanmış şəbəkə mühitində hamının etimad etdiyi etibarlı

üçüncü tərəf mümkün olmadıqda, daha geniş istifadə edilir. Agentin reputasiyası onun keçmiş davranışları haqqında onunla qarşılıqlı təsirdə olan digər agentlərin verdiyi reytinq qiymətlər əsasında hesablanır.

İnformasiya təhlükəsizliyi və etimad

Etimad məsələsi informasiya texnologiyaları üçün yeni deyil. Paylanmış və multi-agent sistemlərdə etibarlılığın qiymətləndirilməsi və qeyri-müəyyənlik şəraitində qərar qəbulu üçün bu və ya digər dərəcədə etimad modellərindən istifadə edilir. Paylanmış sistemlərdə informasiya təhlükəsizliyinin təmin olunması funksiyalarından autentifikasiyanın, elektron imzanın, avtorizasiyanın reallaşdırılması etimad münasibətlərinə əsaslanır.

İnformasiya təhlükəsizliyi ilə etimad arasında mürəkkəb münasibət mövcuddur. Onlayn mühitdə informasiya təhlükəsizliyinin təmin edilməsi mexanizmlərindən (məsələn, kriptoqrafik metodlardan) istifadə edilməsi etimadın yaranmasına və yüksəlməsinə şərait yaradır, eyni zamanda, informasiya təhlükəsizliyinin pozulması halları da etimadı zədələyə bilər. Qanunvericilik bazasının, sertifikatlaşdırma, monitorinq və nəzarət sisteminin mövcudluğu kiberfəzada etimadın möhkəmləndirilməsinə kömək edir. Bundan başqa, qeyd edildiyi kimi, bir sıra informasiya təhlükəsizliyi mexanizmlərinin (autentifikasiya, şifrləmə, e-imza və kriptoqrafik protokollar) paylanmış sistemlərdə reallaşdırılması, tərəflər arasındakı etimad münasibətlərinə əsaslanır [15].

Onlayn mühitdə informasiya təhlükəsizliyinin təmin edilməsi mərkəzləşdirilmiş etimad – üçüncü tərəf vasitəsilə qurulmuş etimad infrastrukturu və ya etimad şəbəkəsi (web of trust) vasitəsilə həyata keçirilir. Mərkəzləşdirilmiş etimad infrastrukturu e-dövlət mühitində açıq açarlar infrastrukturu (Public Key Infrastructure, PKI) əsasında sertifikat xidmətləri mərkəzləri şəbəkəsinin yaradılması ilə qurula bilər. Bu şəbəkə e-imza sertifikatlarının vahid dövlət reyestrinin qurulmasına, dövlət informasiya sistemlərinin istifadəçiləri üçün e-imza sertifikatlarının hazırlanmasına və sertifikatların həyat tsiklinin təmin edilməsinə və vahid etimad fəzasının fəaliyyətinin təmin edilməsinə xidmət edir.

İnformasiya təhlükəsizliyi ilə etimad arasındakı münasibətlər baxımından informasiya təhlükəsizliyi mexanizmlərinin reallaşdırılmasına zəmanət (ing. information security assurance) anlayışına da toxunmaq zəruridir [16].

Etimad modelləri

Paylanmış sistemlərdə praktiki etimad sistemlərinin qurulması üçün bir sıra etimad modelləri təklif edilmişdir. Bu bölmədə bəzi etimad modellərinə qısa nəzər salınır.

Etimad binar (etimad/etimadsızlıq), diskret və kəsilməz qiymətlər ala bilər. Etimadın kəsilməz qiymətlər oblastı 0 – qeyri-müəyyənlik və 1 – tam etimad olmaqla [0, 1] parçası və ya 0 – tam etimadsızlıq, 0.5 – qeyri-müəyyənlik və 1 tam etimad olmaqla [0, 1] parçası ola bilər.

Bir sıra modellərdə etimad bir qiymətlə deyil, bir neçə qiymətlə (məsələn, etimadın qiyməti, etimadsızlığın qiyməti və qeyri-müəyyənliyin qiyməti) və ya intervalla göstərilə bilər. Bəzi modellərdə isə etimad reytinqlə, ranqla, ehtimalla, inamla (ing. belief), qeyri-səlis qiymətlərlə ifadə olunur.

Subyektiv məntiqə əsaslanan rəy modeli qeyri-müəyyənlik şəraitində etimad qiymətlərini hesablamaq üçün maraqlı yanaşmadır [17]. Rəy qənaəti təsvir edir və triplet kimi göstərilir: *b* (inamın ölçüsü), *d* (inamsızlığın ölçüsü) və *i* (məlumatsızlığın ölçüsü), burada b + d + i = 1. Fərz olunur ki, b, d və i kəmiyyətləri [0, 1] parçasında kəsilməz qiymətlər alır. Modelin imkanları onun rəylər barəsində fikir yürütmə qabiliyyəti (ciddi riyazi əsasda) və konsensus, tövsiyə və nizamlama operatorları ilə təyin edilir. Zəif cəhəti ondadır ki, istifadəçilərin uyğun kəmiyyətləri dəqiq təyin edəcəklərinə zəmanət vermək mümkün deyil.

Stiven Marş geniş istinad edilən dissertasiyasında *etimadın formal modeli*ni təklif edir [18]. Modeldə [-1; 1] parçasında tam etimadsızlıqdan tam etimada kimi etimadın qiymətini almaq

üçün subyektiv dəyişənlər çoxluğu və onların kombinasiyası üsulu təklif edilir (Marş qeyd edir ki, bu ekstremal vəziyyətlər mümkün deyil). Dəyişənlərin hər biri zamandan və kontekstdən asılıdır. Təsvir olunan sistemdə insan əvəzinə daha ümumi anlayış – agent anlayışı istifadə edilir. Marş etimadın üç növünü müəyyən edir: *baza etimadı* – istənilən kontekst üçün; *ümumi etimad* – iki agent arasında və onların qarşılıqlı əlaqəsinin istənilən konteksti üçün; *situasiya etimadı* – iki agent arasında konkret kontekst üçün.

Bayes yanaşmasına əsaslanan etimad modelləri reputasiyanın hesablanması üçün Bayes qaydasına və beta ehtimal paylanması funksiyasına əsaslanırlar [19]. Reputasiyanın aposterior qiyməti yeni qiymətlərin (reytinqlərin) aprior qiymətlərinin kombinasiyası kimi hesablanır. Reputasiyanın qiyməti α və β parametrləri ilə verilmiş beta funksiyanın riyazi gözləməsi kimi göstərilə bilər, burada α – iştirakçının müsbət qiymətlərinin, β – mənfi qiymətlərinin sayıdır.

Etimadın hesablanması üçün *reputasiya modelləri* daha geniş yayılıb [20]. Reputasiya – bu və ya digər subyektin keyfiyyətləri, üstünlükləri və çatışmazlıqları əsasında formalaşmış ictimai fikirdir. Reputasiyanın qiyməti müsbət və mənfi rəylərin cəmi kimi hesablanır (məsələn, eBay). Belə metod primitiv və reputasiyanın qiyməti qeyri-dəqiq olsa da, şəffaflıq və istifadəçiyə anlaşıqlı olması onun vacib üstünlüyüdür. Reputasiyadan, qiymətləndirmə zamanından, məsafədən və s. asılı olaraq qiymətlər üçün çəkilər hesablayan daha mürəkkəb sxemlər Epinions və Amazonda istifadə edilir.

CuboidTrust – pirinq şəbəkələri üçün reputasiya əsasında qlobal etimad modelidir [21]. Üç faktor: perin sistemə töhfəsi, əks-əlaqə zamanı perin etibarlılığı və resursların keyfiyyəti istifadə edilir və koordinatları (x, y, z) olan kiçik kublardan ibarət kuboidlər qurulur, burada z – resursun keyfiyyəti, y – qiyməti saxlayan per və x – resursa reytinq verən perdir. Reytinq binardır, 1 autentik və (–1) qeyri-autentik və ya reytinqin olmamasını bildirir. Hər bir per üçün qlobal etimad perlərin saxladıqları bütün qiymətlərin əsasında məxsusi qiymət alqoritmi ilə hesablanır.

EigenTrust – perlərin keçmiş yükləmə məlumatları əsasında p2p fayl paylaşımı şəbəkəsində hər bir per üçün unikal qlobal etimad qiyməti hesablayır [22]. Lokal etimad qiyməti $S_{ij} = sat(i, j) - unsat(i, j)$ kimi hesablanır, burada $sat(i, j)$ ilə i-nin j-dan qənaətbəxş yükləmələri və $unsat(i, j)$ ilə i-nin j-dan qeyri-qənaətbəxş yükləmələri hesablanır. Hər bir per üçün qlobal etimad qiyməti məxsusi qiymət alqoritmi ilə hesablanır.

AntRep – sürü intellektinə əsaslan bu alqoritmdə hər bir per məsafə vektorlarının marşrutlama cədvəlinə oxşar reputasiya cədvəlləri saxlayır [23]. Reputasiya cədvəlində: (i) hər bir per bir reputasiya kontentinə uyğundur; (ii) növbəti keçid üçün metrika hər bir qonşunun seçilməsi ehtimalıdır. Reputasiya qiymətlərini tapmaq və onları yaymaq üçün irəli- və geriyönlü qarışqalar istifadə edilir. Əgər reputasiya cədvəlində ən yüksək reputasiyalı qonşu varsa, bu istiqamətdə bir qarışqa göndərilir. Heç bir üstünlük olmadıqda, bütün istiqamətlərə bir çox qarışqa göndərilir. Tələb olunan reputasiya məlumatı tapıldıqdan sonra, geri yöndə hərəkət edən qarışqa yaradılır və bu qarışqa yolundakı hər bir reputasiya cədvəlini yeniləyir.

SemanticWeb – bu etimad modelində iki agent arasında etimadı hesablamaq üçün onları birləşdirən bütün yollar hesablanır [19]. Hər bir yoldakı tilə aid edilən reytinq qiymətləri vurulur yekun etimad qiymətinin hesablanması üçün bütün yollar üzrə qiymətlər toplanır.

TACS (*Trust Ant Colony System*) – qarışqa sürülərinin davranış modelinə əsaslanır [24]. Bu modeldə feromon izləri konkret servisi təqdim etdikdə, perin qonşularına etimadının miqdarına görə müəyyən edilir. Alqoritm qarşılıqlı təsir üçün ən etibarlı qovşağı və həmin qovşağa aparan ən etibarlı yolu hesablayır və seçir. Qarışqalar hər bir til üzrə hərəkət edərək reputasiyası ən yüksək serverə aparan ən etibarlı yolu tapmağa çalışırlar. Müştərinin tələb etdiyi servisi təqdim edən qovşaq tapılıbsa və qovşağa aparan yolda feromon izi müəyyən edilən həddən böyükdürsə, axtarış dayandırılır, əks halda hələ baş çəkilməmiş qovşaqları axtarmaqda davam edirlər.

TRUMMAR (*TRUst Model for Mobile Agent systems based on Reputation*) – etimad qiymətləri üç növ agentdən – qonşular, dostlar və kənar hostlardan alınır [19]. Qonşular eyni inzibati idarəetmə altında olan öz şəbəkələrindəki hostlara etibar edirlər, dostlar etimad edilən

inzibati nəzarət altında olan digər şəbəkələrin hostlarıdır, kənar hostlar qonşu və ya dost olmayan, lakin könüllü informasiya verən hostlardır. Etimadın yeni qiyməti əvvəlki etimad qiymət, qonşuların, dostların və kənar hostların reputasiyadan asılı çəkilər nəzərə alınmaqla hesablanmış toplu etimad qiymətlərinin çəkili cəmi kimi hesablanır

FIRE (latınca "**fi**des" ("etimad") və "**re**putasiya" hecalarından yaranıb) etimad və reputasiyanın dörd müxtəlif növünü inteqrasiya edir [25]:

Qarşılıqlı əlaqə etimadı keçmişdəki birbaşa qarşılıqlı əlaqə təcrübəsindən alınır. Qiymətləndirici hədəf agentin etibarlılığını müəyyən etmək üçün onunla əvvəlki qarşılıqlı əlaqə təcrübəsindən istifadə edir.

Şahid reputasiyası agentin davranışı haqqında şahid məlumatlarından hesablanır. Agentlərin öz təcrübələrini bölüşəcəklərinə ümid edərək, qiymətləndirici hədəf agent ilə qarşılıqlı əlaqədə olan digər agentlərin rəylərini toplaya bilər. Bu məlumatlar şahid fikirləri əsasında hədəf agentin etibarlılığını qiymətləndirmək üçün istifadə oluna bilər.

Rola əsaslanan etimad agentlər arasında rola əsaslanan müxtəlif münasibətlərlə müəyyən olunur. Agentin keçmiş davranışı ilə (əvvəlki iki halda istifadə edilir) yanaşı, etimadı müəyyən etmək üçün digər məlumatlar da istifadə edilə bilər. Bunlar qiymətləndirici və hədəf agent arasında olan müxtəlif münasibətlər və ya sahə bilikləri ola bilər (məsələn, normalar və ya qanunvericilik sistemi). Məsələn, agentin sahibi onun etibarlı olmasını təsdiq edə bilər və ya etibarlı qrupun üzvü olan digər agentə etimad göstərə bilər.

Təsdiqlənmiş reputasiya agentin özü tərəfindən təqdim olunmuş üçüncü tərəf arayışlarından qurulur. Əvvəlki hallarda qiymətləndirici tələb olunan informasiyanı özü toplamalıdır. Lakin qiymətləndirən agent də öz etibarlılığı haqqında arqumentlər təqdim etməklə, qiymətləndiricinin etimadını qazanmağa çalışa bilər.

E-dövlətin informasiya təhlükəsizliyinə etimadın faktorları

E-dövlətin informasiya təhlükəsizliyinə etimad aşağıdakı faktorlar əsasında qurulur: fərdi məlumatların təhlükəsizliyi; informasiya təhlükəsizliyinin təmin edilməsi mexanizmləri; e-dövlətlə vətəndaşlar arasında əks-əlaqə; informasiya təhlükəsizliyindən istifadənin rahatlığı.

Fərdi məlumatların və özəl yazışmaların təhlükəsizliyi (ing. privacy) informasiya sistemlərinə etimadın qurulmasında mühüm rol oynayır. Hazırda informasiya sistemləri fərdi məlumatları asanlıqla toplayır və onlara asan girişi təmin edir. Buna görə, fərdi məlumatların konfidensiallığının qəsdən və ya bilməyərəkdən pozulması riskləri artır və nəticədə, istifadəçilərin informasiya sistemlərinin təhlükəsizliyinə etimadını azaldır.

İnformasiyanın konfidensiallığının, tamlığının və əlyetərliyinin pozulması da istifadəçilərin informasiya sistemlərinin təhlükəsizliyinə etimadını azaldır. Həyat tsiklinin bütün mərhələlərində müvafiq informasiya təhlükəsizliyi mexanizmlərinin reallaşdırılması etimadın təmin edilməsi üçün vacib məsələdir.

Etimadın möhkəmləndirilməsinin əhəmiyyətli elementlərindən biri də e-dövlət və vətəndaşlar arasında əks-əlaqədir. Vətəndaşların e-dövlətin fəaliyyəti barədə məlumatlandırılması, informasiya təhlükəsizliyi sahəsində görülən tədbirlər barədə məlumatlılıq səviyyəsinin artırılması, informasiya texnologiyaları və informasiya təhlükəsizliyi sahəsində əhalinin maarifləndirilməsi etimadın qurulmasında vacib rol oynayır.

Etimada təsir edən digər atribut informasiya təhlükəsizliyindən istifadənin rahatlığıdır (ing. usability). İstifadənin rahatlığını aşağıdakı kimi xarakterizə etmək olar:

- istifadəçilərin interfeysi öyrənməsi nə qədər asandır;
- interfeysin səmərəliliyi;
- istifadəçilər nə dərəcədə asan yadda saxlaya bilərlər;
- səhvlərin azaldılması;
- interfeysdən ümumi məmnunluq.

Tədqiqatlar göstərir ki, istifadənin rahatlığı faktorları istifadəçilərin informasiya sistemlərinə, xüsusilə də veb-saytlara etimadına təsir edir, çünki onların qavranılan imkanlarını artırır. Bundan başqa, istifadənin rahatlığı etimadın zəruri şərtidir, çünki insanların proqram təminatı sistemlərini düzgün istifadə etdiklərinə inanmaları zəruridir.

E-dövlətin informasiya təhlükəsizliyinə etimadın qiymətləndirilməsi modeli

E-dövlətin informasiya təhlükəsizliyinə *etimad indeksi* anlayışını daxil etmək olar. Bu indeksin rəy sorğusu əsasında hesablanması nisbətən sadədir. "Siz elektron dövlətin informasiya təhlükəsizliyinə etimad edirsinizmi?" tipli sual və "Etimad edirəm", "Etimad etmirəm" və "Cavab verməkdə çətinlik çəkirəm" tipli cavablar olan rəy sorğusunun keçirilməsi nəzərdə tutulur. Etimad indeksi etimad edənlər və etimad etməyənlərin say fərqinin bütün respondentlərin sayına nisbəti kimi müəyyən edilir. Lakin bu yanaşma etimadın necə formalaşması sualına cavab verə bilmir.

Bu işdə etimadı müxtəlif informasiya mənbələri nəzərə alınmaqla qiymətləndirməyə imkan verən model təklif edilir. Vətəndaşlar e-dövlətin informasiya təhlükəsizliyi barəsində informasiyanı öz şəxsi təcrübələri, qonşuların və dost-tanışların rəyləri və KİV-lərdə ifadə olunan rəylər əsasında toplayırlar. Dövlət orqanları da müəyyən sübutlar təqdim edə və ya informasiya təhlükəsizliyinin təmin edilməsi üzrə müəyyən öhdəliklər götürə bilərlər (məsələn, informasiya sistemlərinin və ya istifadə edilən məhsulların informasiya təhlükəsizliyi standartlarına uyğunluq sertifikatları). Bu mənbələri modelin komponentləri adlandıraq və onları uyğun olaraq *I, W, M* və *S* simvolları ilə işarə edək.

Etimad qiymətini hesablamaq üçün e-dövlətin keçmiş davranışı haqqında modelin komponentləri üzrə relevant reytinqlər toplanmalıdır. Toplanmış reytinqlər çoxluğu e-dövlətin gələcək davranışını – gələcək qarşılıqlı təsirdə gözlənilən reytinq qiymətini qiymətləndirmək üçün istifadə edilir. Bu qiyməti hesablamaq üçün ümumi üsul çoxluqdakı bütün reytinqlərin ədədi ortasını hesablamaqdır. Lakin bu reytinqlər gözlənilən reytinq qiymətini hesablayarkən eyni dərəcədə relevant deyillər. Məsələn, bəzi reytinqlər digərlərindən köhnə ola bilər və daha az əhəmiyyətli görünə bilərlər. Bəzi reytinqlər daha etibarlı mənbələrdən gələ bilər ki, digərləri ilə müqayisədə ona daha yüksək etimad göstərilməlidir. Buna görə də modelin hər bir komponenti üçün reytinq çəkisi funksiyası daxil edilir, *K* indeksi *I, W, M* və *S* ola bilər, onlar uyğun olaraq bilavasitə təcrübə, şahid məlumatları, kütləvi media vasitələri və sertifikatlar əsasında etimadı bildirir. Etimad qiyməti bütün əlyetər reytinqlərin çəkili ortası kimi hesablanır:

$$T_K(a,c) = \frac{\sum_{r_i \in R_K(a,c)} w_K(r_i) \cdot v_i}{\sum_{r_i \in R_K(a,c)} w_K(r_i)},$$

burada $T_K(a, c)$ – a agentinin e-dövlətin informasiya təhlükəsizliyinə etimadın c faktoruna nəzərən K komponenti üzrə hesablanmış etimad qiymətidir. $R_K(a, c)$ – K komponenti tərəfindən etimadı hesablamaq üçün toplanmış reytinqlər çoxluğudur. $w_K(r_i)$ – r_i reytinqinin relevantlıq (etibarlılıq) dərəcəsini hesablamaq üçün reytinq çəki funksiyasıdır ($w_K(r_i) \geq 0$). v_i – r_i reytinqinin qiymətidir. Çəkilərin cəminə bölməklə etimad qiyməti [-1, 1] diapazonuna normallaşdırılır. Reytinq çəki funksiyaları $w_K(r_i)$ hər bir komponent üçün ayrıca müəyyən olunur.

Ümumi etimad qiyməti

$$T(a,c) = \frac{\sum_{K \in \{I,W,M,S\}} W_K \cdot T_K(a,c)}{\sum_{K \in \{I,W,M,S\}} W_K},$$

kimi hesablanır, burada W_K uyğun olaraq komponentlərin çəki əmsallarıdır. Bu əmsallar baxılan məsələ üçün hər komponentin vacibliyinə uyğun olaraq seçilir.

Nəticə

E-dövlət kontekstində etimadın və onun müxtəlif növlərinin araşdırılması həm elmi tədqiqatlar, həm də praktiki tətbiqlər üçün olduqca əhəmiyyətlidir. Bu məqalədə e-dövlətin informasiya təhlükəsizliyinə vətəndaşların etimadını qiymətləndirmək üçün model təklif edilmişdir. Təklif edilən model etimadın qiymətləndirilməsi üçün müxtəlif informasiya mənbələrindən toplanmış məlumatların aqreqasiyasına əsaslanır, aqreqasiya zamanı məlumat mənbələrinin əhəmiyyətlilik (relevantlıq) dərəcələri nəzərə alınır.

Gələcək tədqiqatlarda e-dövlətin informasiya təhlükəsizliyinə etimadın tərkib hissələrinin və onların qarşılıqlı münasibətlərinin, etimad domenlərinin (obyektlərinin) xarakteristikalarının və etimadın qurulması mexanizmlərinin modelləşdirilməsi, e-dövlət kimi multi-agent sistemlərində etimad münasibətlərinin dəstəklənməsi üçün vahid infrastrukturun arxitektur modelinin işlənməsi nəzərdə tutulur.

Ədəbiyyat

1. Alguliev R., Imamverdiyev Y., Yusifov F. Some conceptual views on information security of the society // Journal of Communication and Computer, 2012, vol.9, pp.644–648.
2. Schwester R. Examining the barriers to e-government adoption // Electronic Journal of e-Government, 2009, vol.7, no.1, pp.113–122.
3. Colesca S.E. Increasing e-trust: A solution to minimize risk in e-government adoption // Journal of Applied Quantitative Methods, 2009, vol.4, no.1, pp.31–44.
4. Rousseau D., Sitkin S., Burt R., Camerer C. Not so different after all: a cross-discipline view of trust // Academy of Management Review, 1998, vol.23, no.3, pp.393–404.
5. Simpson J. A. Psychological Foundations of Trust // Current Directions in Psychological Science, 2007, vol.16, no.5, pp.264–268.
6. Castelfranchi C., Falcone R. Trust theory: A Socio-cognitive and computational model. Wiley. 2010.
7. Sztompka P. Trust: A sociological theory. Cambridge University Press, 1999.
8. Ramchurn S. D., Huynh T. D., Jennings N. R. Trust in multi-agent systems // The Knowledge Engineering Review, 2004, vol.19, no.1, pp.1–25.
9. Pinyol I., Sabater-Mir J. Computational trust and reputation models for open multi-agent systems: a review // Artificial Intelligence Review, 2013, vol.40, no.1, pp.1–25.
10. Arai K. Trust and trustworthiness in the economy: How they function and how they should be promoted // Hitotsubashi Journal of Economics, vol.48, no.2, pp.225–240.
11. van Witteloostuijn A. A Game-theoretic framework of trust // International Studies of Management & Organization, 2003, vol.33, no.3, pp.53–71.
12. Grandison T., Sloman M. A survey of trust in internet applications // IEEE Communications Surveys & Tutorials, 2000, vol.3, no.4, pp.2–16.
13. Abdul-Rahman A., Hailes S. Using Recommendations for managing trust in distributed systems / Proc. of IEEE Malaysia International Conference on Communication, 1997.
14. Mui L., Mohtashemi M., Halberstadt A. A Computational model of trust and reputation / Proc. of the 35th Hawaii International Conference on System Sciences, 2002, pp. 2431–2439.
15. Elçi A. et al. (editors). Theory and practice of cryptography solutions for secure information systems (CRYPSIS). IGI Global, 2013.
16. ISO/IEC TR 15443-1:2012 Information technology - Security techniques - Security assurance framework - Part 1: Introduction and concepts. 2012, 52 p.
17. Jøsang A. Artificial reasoning with subjective logic / Proc. of the 2nd Australian Workshop on Commonsense Reasoning, 1997, vol.48, pp.34–50.
18. Marsh S. Formalizing trust as a computational concept. PhD thesis. University of Stirling, Department of Computer Science and Mathematics. 1994.

19. Firdhous M., Ghazali O., Hassan S. Trust management in Cloud Computing: A critical review // International Journal on Advances in ICT for Emerging Regions, 2011, vol.4, no.2, pp.24–36.
20. Sabater J., Sierra C. Review on computational trust and reputation models // Artificial intelligence review, 2005, vol.24, no.1, pp.33–60.
21. Chen R., Zhao X., Tang L., Hu J., Chen Z. CuboidTrust: A global reputation-based trust model in peer-to-peer networks / Proc. 4th International Conference Autonomic and Trusted Computing, 2007, Lecture Notes in Comp. Science, vol.4610, pp.203–215.
22. Kamvar S.D., Schlosser M.T., Garcia-Molina H. The EigenTrust algorithm for reputation management in p2p networks / Proc. of the 12th international conference on World Wide Web (WWW '03), 2003, pp.640–651.
23. Wang W., Zeng G., Yuan L. Ant-based reputation evidence distribution in p2p networks // Proc. of the 5th International Conference Grid and Cooperative Computing, 2006, pp.129–132.
24. Marmol F. G., Perez G. M., Skarmeta A. F. G. TACS, a trust model for p2p networks // Wireless Personal Communications, 2009, vol.51, no.1, pp.153–164.
25. Huynh T.D., Jennings N.R., Shadbolt N.R. An integrated trust and reputation model for open multi-agent systems // Autonomous Agents and Multi-Agent Systems, 2006, vol.13, no.2, pp.119–154.

УДК 004.9:351

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az

Модель оценки доверия к информационной безопасности э-государства

Обеспечение доверия граждан к информационной безопасности э-государства имеет важное значение для наиболее полного использования потенциала э-государства. В этой работе анализируются механизмы укрепления доверия к информационной безопасности э-государства и предлагается модель для оценки доверия. Модель основывается на интеграции значений репутаций, рассчитанных на основе данных доверия из различных источников, с учетом весов источников.

Ключевые слова: *э-государство, информационная безопасность, доверие, репутация, доверие к информационной безопасности.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az

An assessment model for e-government information security trust

Ensuring public trust in the e-government information security is essential for full use of the potential of e-government. In this paper, we analyze the mechanisms for building trust in the e-government information security, and propose a model for assessment of this trust. The model is based on the integration of the values of reputation, calculated on the basis of trust from various sources, taking into account the importance weights of sources.

Keywords: *e-government, information security, trust; reputation, information security trust.*