Elektron səsvermə sistemlərində təhlükəsizlik təhdidlərinin qiymətləndirilməsi

Fərhad Yusifov

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

farhadyusifov@gmail.com

Xülasə– **E-səsvermə e-demokratiyanın ən mühüm komponentlərindən biri hesab edilir. E-səsvermə sistemlərinin tətbiqində və inkişaf etdirilməsində təhlükəsizlik məsələləri həlledici rola malikdir. Məqalədə e-səsvermə sisteminə dair yanaşmalar və sistemin təhlükəsizliyinə olan təhdidlər araşdırılır. Çoxmeyarlı qərar qəbul etmə modeli əsasında e-səsvermə sisteminin təhlükəsizliyinə olan təhdidlərin empirik qiymətləndirilməsi məsələsinə baxılır.**

Açar sözlər – e-səsvermə; İnternet səsvermə; e-demokratiya; təhlükəsizlik, təhlükəsizlik təhdidləri.

I. GİRİŞ

Elektron səsvermə (e-səsvermə) sistemi səsvermənin gizliliyi, fərdi məlumatların qorunması və şəffaflığın təmin olunması baxımından e-demokratiyanın ən mühüm tətbiqlərindən biridir [1,2]. E-səsvermə e-demokratiyanın ən vacib komponentlərindən biri olmaqla özündə seçkilərdə iştirak mexanizmləri, təhlükəsizliyin və leqitimliyin təmin olunması, e-səsvermə üçün texnoloji həllər və onların e-səsvermədə səmərəli tətbiqi kimi maraqlı tədqiqat mövzularını əhatə edir. Kompleks yanaşmada e-səsvermə e-seçkilərin ən əhəmiyyətli tərkib hissəsi hesab olunur.

Elmi mənbələrdə İKT-nin tətbiqi ilə səsvermə formalarına dair müxtəlif yanaşmalar vardır və istifadə olunan terminlərin unifikasiyasına ehtiyac duyulur. Əsasən onlayn olaraq keçirilən səsverməni ifadə etmək üçün 2 termindən, e-səsvermə və İnternet səsvermə terminlərindən istifadə olunur [2-4]. E-səsvermə termini daha geniş mənada istifadə olunsa da, İnternet səsvermə onun formalarından yalnız biri kimi göstərilir.

İnformasiya texnologiyalarının sürətli inkişafı və kriptoqrafiya üsüllarının təkmilləşdirilməsi hesabına e-səsvermə artıq hökümətlər tərəfindən tətbiq olunmağa başlamışdır. Bununla belə, demokratik prinsiplər nəzərə alınaraq e-səsvermənin keçirilmə prosedurları və onun təhlükəsizliyənə dair məsələlər hələ də müzakirə olunmaqdadır. Siyasi arenada səsvermə prosesində şəffaflığın təmin olunması, səslərin demokratik prinsiplərə uyğun hesablanması, namizədlərin və seçicilərin konstitusyon hüquqlarının qorunması ən mühüm məsələlər kimi ön plana çıxır.

E-səsvermə sisteminin tətbiqi ölkələrdə mövcud siyasi proseslərə təsir gücünə malikdir və kritik təhlükəsizlik sistemlərinə aid edilir [5]. Bu baxımdan, vətəndaşların demokratik proseslərdə yaxından iştirakının və şəffaflığın təmin olunması üçün e-səsvermənin təhlükəsizliyinə olan təhdidlərin müəyyənləşdirilməsi və qiymətləndirilməsi aktual məsələlərdən biri hesab olunur. Tədqiqat işində e-səsvermə sistemindəki boşluqlar araşdırılır və sistemin təhlükəsizliyinə olan təhdidlərin qiymətləndirilməsi məsələsinə baxılır.

II. E-DEMOKRATİYA ÜÇÜN E-SƏSVERMƏ

E-dövlətin inkişafının son mərhələsi hesab olunan e-demokratiyanın formalaşdırılmasının əsası kimi e-səsvermə, ictimai forumlar, açıq dövlət, ictimai rəyin analizi və əks əlaqə mexanizmlərinin işlənilməsi göstərilir [6]. E-demokratiya, xüsusən də e-səsvermə təcrübədə və ədəbiyyatda geniş müzakirələrə səbəb olmuşdur [4-7]. Əsas müzakirə mövzuları kimi e-səsvermənin təhlükəsizlik problemləri və sosial-siyasi proseslərə təsiri ön plana çəkilir. Bu səbəbdən, e-səsvermə sistemlərinin tətbiqində təhlükəsizlik məsələləri həlledici rol oynayır. Səsvermə vətəndaşlarının demokratik proseslərdə iştirakı ilə xarakterizə olunan və ümümi rəyin formalaşmasına imkan verən bir sistem kimi baxılır. Lakin, mütəxəssislərin əksəriyyəti e-səsvermənin daha kompleks və həssas bir sistem olduğunu qeyd edirlər. Seçki prosesinin təhlükəsizliyinə milli təhlükəsizlik səviyyəsində baxılmalıdır. Çünki demokratiyanın leqitimliyi seçkilərin ədalətli, açıq və etibarlı olması səviyyəsindən asılıdır. Bu baxımdan, e-səsvermə sisteminin cəmiyyət qarışısında öhdəlikləri var və onun uğursuzluğu siyasi proseslərə vətəndaşların inamı ilə bağlı çox ciddi problemlərə səbəb ola bilər [7].

Ümumilikdə, seçki prosesində iştirak edənlərin sayının azalması tendensiyası İnternetdən istifadənin sürətlə genişlənməsi ilə dəstəklənən e-səsvermə üçün yeni imkanlar yaratmaqdadır. Hazırda nə elmi ədəbiyatda, nə də seçki təcrübəsində e-səsvermə ilə bağlı yekdil bir yanaşma, anlayış yoxdur [7]. Bəzi tədqiqatçılar e-demokratiyanın inkişaf etdirilməsi baxımından e-səsverməni seçicilərin rahatlığının nəzərə alınması nəticəsində yaranan texnoloji həlli hesab edir. Digər tərəfdən, bir qrup mütəxəssis hesab edir ki, seçicilərin səsvermədə aktivliyini xüsusən, gənc seçicilərin e-səsvermə prosesinə cəlb edilməsi hesabına təmin etmək olar.

Seçki prosesini asanlaşdırmaq, daha səmərəli və daha ucuz etmək üçün elektron vasitələrdən istifadə etməklə e-səsvermə iki formada həyata keçirilə bilər: müşahidə olunan e-səsvermə - hökumətin və ya seçki orqanı nümayəndəsinin olmasını tələb

DOI: 10.25045/NCInfoSec.2017.03

edir və ya uzaqdan e-səsvermə - nümayəndə tərəfindən müşahidəçinin olmasını tələb etmir və İnternet səsvermə və ya mobil qurğular vasitəsilə həyata keçirilə bilər [2,5,7]. İnternet vasitəsilə uzaq e-səsvermə ilə əlaqədar olaraq, ədəbiyyatda e-səsvermə həlləri üç əsas sinfə ayrılır: köşk səsvermə, səsvermə mərkəzində internet səsvermə və uzaqdan internet səsvermə [7]. E-səsvermə ilə bağlı müxtəlif yanaşmalar olsa da, e-səsvermənin həyata keçirilməsini zəruri edən amillər nəzərə alınaraq yaxın perspektivdə mobil səsvermə həllərinin inkişaf etdiriləcəyi güman edilir.

III. E-SƏSVERMƏ SİSTEMİ

E-səsvermə sisteminin tətbiqi seçki prosesində yaranan səhvlərin azaldılmasına, ümumilkdə seçki prosesinin tamlığının, şəffaflığının və rahatlığının təmin olunmasına imkan verir. E-səsvermə siseminin tətbiqinin üstünlüklərinə baxmayaraq, bu proses çox sayda sosial, hüquqi və texniki problemlərlə müşayət olunur. Onların sırasında seçici mərkəzlərinə bərabər çıxış imkanı, məxfiliyin təmin oluması, müdaxilələrə qarşı mübarizə, təhdidlərin qiymətləndirilməsi məlumatın yoxlama, dəyişdirmə və digər proseduraların təsdiqlənməsi, universal təsdiqləmə, səsvermə hüququ, bir seçici və bir səs prinsipinin qorunması, xətalara qarşı dayanıqlılıq və s. göstərmək olar. Onların sırasında, xüsusilə hüquqi məhdudiyyətlərin texniki və təhlükəsizlik həllərinə çevrilməsinin zəruriliyini qeyd etmək olar. E-səsvermənin həyata keçirilməsini zəruri edən amillər aşağıdakılardır:

Təhlükəsizlik: Səsvermə sisteminin tətbiqində ən çox müzakirə olunan məsələlərdən biri də təhlükəsizlikdir [8-11]. Ənənəvi seçki sistemində hər kəsə aydındır ki, səslərə görə seçicilərin müəyyənləşdirilməsi mümkünsüz idi. Çünki seçki prosesi gizli səsvermə yolu ilə həyata keçirilirdi və hər bir seçici bağlı zərfini seçki qutusuna atırdı. Hər bir seçici gizlilik prinsipinə riayət edirdi. Lakin bu seçki prosesinin heç də şəffaf olmasına dəlalət etmir. Məsələn, seçicinin onun səsinin sonrada dəyişdirilməyəcəyinə dair heç bir zəmanəti yoxdur və s. E-səsvermə sisteminin təhlükəsizliyinin təmin olunması istiqamətində səylərə baxmayaraq, e-səsvermə fərdi məlumatların konfidensiallığına real təhdid hesab olunur.

Şəffaflığın lazımi səviyyədə olmaması: Şübhəsiz ki, informasiya texnologiyalarının köməyilə təhlükəsizlik tələblərinin təmin edilməsi, hətta kriptoqrafiyanın metod və alətlərindən istifadə olunması seçki prosesində şəffaflığının artırılmasına xidmət edirsə də, seçicilərin təhlükəsizliklə bağlı tələbləri qəbul etməsində və yerinə yetirməsində çətinliklərin olacağı inkar edilmir [4,5,8,9].

E-demokratiyanın inkişaf etdirilməsi: E-demokratiyanın formalaşdırılması və inkişaf etdirilməsi üçün səmərəli e-səsvermə mexanizmlərinin işlənilməsi olduqca vacibdir. E-səsvermə dövlət orqanlarının, siyasi partiyaların və siyasətçilərin diqqətini çəkir və demokratik prinsiplərin təmin olunmasında güclü vasitə hesab olunur. Demokratiya təşəbbüsü ilə çıxış edən inkişaf etməkdə olan ölkələrdə rəqəmsal fərqliliyin aradan qaldırılması, əyalətlərlə mərkəzlər arasında sıx əlaqənin yaradılması, demokratik dəyərlərin qorunması və ədalətli seçkilərin keçirilməsi baxımından e-səsvermə böyük əhəmiyyət kəsb edir.

Seçki saxtakarlığı: Qeyd edək ki, ənənəvi seçkilərin təhlükəsizliyi insanlara inama və seçki komitələrinin müstəqiliyinə əsaslanır. Təcrübə göstərir ki, demokratiya təşəbbüsü ilə çıxış edən inkişaf etməkdə olan ölkələrdə bu mexanizmlərə inam çox az olduğuna görə təşkilati təhlükəsizlikdən çox texniki təhlükəsizliyə yəni, kriptoqrafik kodlaşdırma və s. keçid səmərəli hesab oluna bilər. Qeyd etmək lazımıdır ki, təşkilati və texniki təhlükəsizlik tədbirlərinin birgə istifadəsi mərhələli xarakterə malikdir. Yəni əgər təşkilat strukturları korrupsiyalaşıbsa, hətta ən etibarlı texnologiyanın istifadəsindən belə imtina oluna bilər. Bununla yanaşı, təşkilati və texniki təhlükəsizlik tədbirlərinin birgə istifadəsinin tədricən bir xarakterə malik olduğunu qeyd etmək lazımdır [9,12-14].

Seçicilərin aktivliyi: E-səsvermə seçicilərin fəallığına təsiri böyük ehtimalla yalnız səsvermə formasına görə yox eyni zamanda, müvafiq mədəni, siyasi və coğrafi şəraitlə də səciyyəvi olacaqdır. Məsələn, Avstraliya əhalisinin sıxlığının aşağı olması, Estoniyada əhalinin çox hissəsinin əmək fəaliyyəti ilə əlaqədar digər avropa ölkələrinə miqrasiya etməsi, siyasi münaqişə və ya müharibə vəziyyətində olan ölkələrdə seçicilərin mühacir həyatı yaşaması və s.

Etibarsız səslərin azaldılması: Etibarsız səslər bilərəkdən və hər hansı texniki səbəbdən asılı olaraq bilməyərəkdən yarana bilər. Səslərin saxtalaşdırılması demokratik prinsiplərə zidd bir addım kimi qiymətləndirilir və etibarsız səslərin sayının artması seçki nəticələrini şübhə altında qoyur.

E-səsvermə prosesində etibarsız səslərin yaranması yoxlanış zamanı aşkarlana bilər və proqram təminatında edilən dəyişiliklər etibarsız səslərin sayının minimuma endirilməsinə imkan verir. Bu baxımdan demokratik “bərabərlik prinsipinə” məhdudiyyətlər gətirən bu tip əngəllərin hüquqi cəhətdən qəbul edilib edilməməsi qanuni olaraq araşdırılmalıdır [1-4,13,15].

Xərclərin minimuma endirilməsi: Səsvermədə fiziki iştirakın çox olmaması və səslərin hesablanmasına az sayda əməkdaşın cəlb olunması və ya səfərlərə xərclənən vəsaitin azaldılması hesabına xərcləri minimallaşdırmaq olar. Digər tərəfdən, səsvermə sisteminin yaradılması, seçicilərin lazımı texniki avadanlıqla təmin olunması maliyyə vəsaiti tələb edir. Bundan əlavə, yaxın gələcəkdə siyasi seçkilərdə seçki məntəqələri öz əhəmiyyətini itirmiş olacaq. Bütün bunlar nəzərə alınaraq, e-səsvermənin tətbiqinin seçkinin keçirilməsinə xərclənən vəsaitə qənaət etməyə imkan verəcəyi hələlik müzakirə mövzusu olaraq qalmaqdadır.

Elmi ədəbiyyatda seçkilərin keçirilməsinə dair hüquqi müstəvidə geniş müzakirələr aparılır və nəticə etibarı ilə hesab edilir ki, hüquqi məsələlərin həlli qanundan texnologiyaya keçiddə körpü rolunu oynamaqdadır.

IV. E-SƏSVERMƏ SISTEMINDƏKI BOŞLUQLAR

Müasir demokratik ölkələrdə seçki e-səsvermə sistemi vasitəsilə həyata keçirilir. İKT-nin istifadəsi səslərin verilməsi və seçicilərin sayının artırılması baxımından seçki prosesini daha effektiv edir. Bu onunla izah olunur ki, e-səsvermə prinsipal olaraq prosesin asanlaşdırılmasına və dəstəklənməsinə xidmət edir. E-səsvermənin və xüsusilə

İnternet əsaslı səsvermə sistemlərinin əsas töhvəsi seçicilərin mobilliyinin təmin olunmasının dəstəklənməsi hesab olunur və bu da öz növbəsində seçicilərə İnternetə çıxış təmin olunan istənilən yerdən seçkidə iştirak etməyə imkan verir. E-səsvermə ilə bağlı əsas boşluqlar seçicilərin autentifikasiyası və xüsusilə, İnternet səsvermədə proqram təminatlarına olan təhdidlər, məsələn, viruslar, “troyan atları” kimi ziyanlı proqram vasitələri göstərilir [5]. İnternet səsvermənin problemləri kimi seçici məlumatlarının tamlığı, səslərin etibarlı ötürülməsi və saxlanması, səsin təkrarlanmasının qarşısının alınması və s. göstərilir [5,7-13].

Müxtəlif e-səsvermə sistemləri ilə əlaqəli çox sayda boşluqlar mövcuddur [2-5,8,11-14]. Hazırda mövcud olan e-səsvermə sistemlərinin əksəriyyəti etibarlı seçkilərin keçirilməsi üçün yetərli deyil, çünki mövcud təcrübə onların dürüstlüyünü sübut edə biləcək hər hansı dəlillərin təqdim olunmamasını göstərir. Məhz inamın olmaması e-səsvermənin geniş yayılmamasnın əsas səbəbi hesab olunur, lakin yaxın gələcəkdə səmərəli mexanizmlərin işlənməsilə e-səsvermə sisteminin daha effektli olacağı güman edilir.

E-səsvermə sistemi 3 əsas kateqoriyaya ayrıla bilər: texniki təminat, proqram təminatı və insan faktoru. Aparat vasitələrinin təhlükəsizliyi elementlərinə elektromexaniki və elektrik hissələri aiddir [2]. Proqram təminatı üçün təhlükəsizlik elementləri əməliyyat sistemi, kompilyatorlar, verilənlər bazası, proqramda istifadə olunan qaydalar və s. göstərilir. İnsan faktorunun təhlükəsizlik elementlərinə istifadə rahatlığı, qaydalar, strategiyalar, şəffaflıq, inam, qəbul edilmə və s. aiddir. Ədəbiyyat analizində və təcrübədə təhlükəsizlik riskləri baxımından hər 3 kateqoriyanın eyni dərəcədə əhəmiyyətli olduğu qeyd olunur [2].

Dövlət tərəfindən funksional və konstitusional öhdəliklərin tənzimlənməsi e-səsvermə sisteminin çox sayda problemlərlə qarşılaşmasına səbəb olur. Bu baxımdan e-səsvermə sistemi konsitutsiyon seçki prinsiplərinə tam cavab verməlidir. Texnoloji həll üçün bu yanaşma təhlükəsizlik tələblərinə çevrilir və səsvermənin keçirildiyi mühitdə həyata keçirilməlidir. Effektiv e-səsvermə sisteminin texniki və təhlükəsizlik xarakteristikaları kimi dəqiqlik, yoxlanıla bilmə, demokratik, çeviklik, mobillik, etibarlılıq, dəyişməzlik, ictimayyət tərəfindən qəbul edilmə və s. göstərilir. Digər arzu olunan tələblər kimi rahatlıq, şəffaflıq, qiymətləndirilə bilmə və iqtisadi cəhətdən səmərəli olması göstərilir. Elmi ədəbiyyatda e-səsvermə sisteminin təhlükəsiliyinin təmin olunmasına dair müxtəlif yanaşmalar olsa da göstərilən tələblərin əksəriyyəti tədqiqatçılar tərəfindən birmənalı qəbul edilir [1,13-17]

Buna baxmayaraq, bəzi tələblər arasında mübahisə doğuran münaqişə vəziyyətləri vardır. Məsələn, autentifikasiya və konfidensiallıq arasında konflikt yaradan məqam seçicinin səsvermədə iştirak hüququnun olub olmamasının yoxlanması tələbi ilə yanaşı, eyni zamanda seçicinin səsinin konfidensiallığının təmin edilməsi tələbinin olmasıdır.

V. E-SƏSVERMƏ SİSTEMİNİN TƏHLÜKƏSİZLİYİNƏ TƏHDİDLƏR

E-səsvermə sahəsində tədqiqatların aparılması e-demokratiya mexanizmlərinin inkişaf etdirilməsi baxımından mühüm istiqamətlərdən biri hesab olunur. Rahat və təhlükəsiz e-səsvermə sisteminin yaradılması kiberfəzadan insanların fikirlərinin, rəylərinin toplanması üçün güclü vasitəyə çevrilə bilər. E-səsvermə sisteminə hücumlar müxtəlif üsullarla həyata keçirilə bilər. Təhdidlər təhlükəsizliyin müxtəlif sahələrinə təsir etməklə sistemin etibarsız hesab olunmasına gətirib çıxara bilər. E-səsvermə sisteminə potensial təhdidlər kimi aşağıdakıları göstərmək olar [5,8,9-11,15]:

Texniki boşluqlar. Proqram təminatının yaradıcıları və ya sistem inzibatçıları operatorlar üçün əlyetərli olmayan inzibatçı hesabı *(administrator account*) yaradırlar. İnzibatçı hesabı problemlər, sistemdə baş verə biləcək xətaların aradan qaldırılması və ya şəxsi məqsədlər üçün istifadə olunur. Bu hesablar hakerlər tərəfindən ələ keçirilərək bədniyyətli məqsədlər üçün istifadə oluna bilər və bu xarakterli boşluqlar texniki təhdidlərə aid edilir.

Xidmətdən imtina (*Denial of Service*) hücumu. Xidmətdən imtina *DoS* hücumlar dağıdıcı nəticələrə səbəb olur və çox hallarda sistemin dayanıqlığına təsir göstərərək sistemə çıxışı təmin etməyi mümkünsüz edir. Hakerlər müxtəlif üsullardan, o cümlədən, “ölüm paketi” (*Ping of Death*) və “Paket seli” (*Packet Flooding*) üsullardan istifadə edərək e-səsvermə sisteminə çıxışı təhlükə altında qoya bilər. Bu tip hücumlar bütün sistemlərə eyni formada təsir göstərmir, bəzi sistemlərin fəaliyyəti dayandırılıdığı halda bəzilərinə təsir göstərməyə də bilər.

Viruslar. Kompüter virusu – öz özünü bərpa edə bilən və aktiv olduğu kompüterlərdə istənməyən təsirlərə səbəb olan kompüter proqramıdır. Viruslar e-səsvermə sistemini məhv edə bilər. Virus hücumu seçki dövründə sistemə çıxışı təhlükə altında qoyaraq, hökuməti və qurumları təkrar seçkilərin keçirilməsinə məcbur edə bilər. Belə hücmlardan ən geniş yayılmışı e-poçtlara olan hücumlardır və texniki təhdidlərə aid edilir.

Soğulcanlar. Bu tip viruslar mövcud proqramlarda və faylarda dəyişiklik etmədən yayılırlar. Virusa yoluxmuş kompüterdə özünün nüsxələrini yaradaraq digər sistemlərdə aktiv olmaq üçün yayılırlar. Virus məqsədli şəkildə proqramlaşdırılıbsa fayllar və səsvermə nəticələrin dəyişdirilərək, səsvermənin etibarsız hesab olunmasına səbəb ola bilər.

Troya atı. Troya atı virusu kompüterin İnternetə qoşulduğunda yüklənən zərərli proqram kodudur. İlk baxışda zərərsiz olan bu virus kompüterdən mühüm bir faylı silə, dəyişdirə, zərərli bir virus yarada və hətta istifadəçi parollarını ələ keçirə bilər. Bu virus e-səsvermə sistemindəki informasiyanın tamlığına və konfidensiallığına çox ciddi təhdid hesab olunur.

Fişinq. Bəzi fişinq-dələduzları leqal veb-səhifələrə bənzəyən saxta veb-səhifələr hazırlayır və qeyri-qanuni olaraq seçicilərin məlumatlarını əldə edir, onların hüquqlarından istifadə edərək seçki nəticələrini saxtalaşdırırlar. Bu təhdid

hücumun növündən asılı olaraq həm texniki, həm də, sosial kateqoriyaya aid edilə bilər.

Fiziki hücumlar. Seçki prosesini pozmaq üçün e-səsvermə sisteminə çoxsaylı fiziki hücumlar edilə bilər. Bədniyyətli şəxs tərəfindən İnternetə çıxış və enerji mənbəyinə müdaxilə son nəticədə səslərin itirilməsinə səbəb ola bilər. Sərt diskin və ya smart-kartın sıradan çıxarılması və ya onların saxta verilənlərlə əvəzlənməsi, seçicilərin fərdi məlumatlarının ələ keçirilməsi və s. e-səsvermə prosesinə ciddi təhdid hesab olunur.

Hesablama altsistemi və sistemin tamlığına təhdidlər. Hesablama altsisteminə hücum klyent proqram təminatından və ya server tərəfindən bəniyyətli şəxsin istəyinə uyğun saxtalaşdırıla və dəyişdirilə bilər. Bu təhdid həm texniki və həm də, sosial kateqoriyaya aid edilə bilər.

İstifadəçi kompüterinə təhdidlər. Elmi ədəbiyyatda digər əməliyyat sistemləri ilə müqayisədə Windows sistemində boşluqların daha çox müşahidə olunduğu göstərilir. Windows mühitində hər hansı populyar proqramın yenilənməsi prosesində Troya atı, *backdoor* kimi viruslar nəzərə çarpmadan kompüterə yüklənə bilər və bu halda istifadəçi kompüteri müxtəlif məqsədlər üçün istifadə olunur. İnsanların bu əməliyyat sistemindən daha çox istifadə etməsi və boşluqların daha çox olması, eləcə də, bu boşluqların hakerlər tərəfindən asan müəyyənləşdirilməsi e-səsvermə üçün ciddi təhdid hesab olunur.

VI. EMPİRİK HESABLAMA

Fərz edək ki, yerli seçkilərdə e-səsvermə sisteminin tətbiq olunmasına qərar verilmişdir. Çoxmeyarlı qərar qəbul etmə modelindən istifadə edərək e-səsvermə sisteminə olan tədidlərin ranqlaşdırılması məsələsinə baxaq. E-səsvermə sisteminə aşağıdakı 4 təhdidin $A=\{A_1,A_2,A_3,A_4\}$ olması ehtimal olunur. Burada, A_1 - *DoS* xidmətdən imtina hücumları, A_2 - Virus hücumları, A_3 - Fişinq təhdidi, A_4 - Fiziki hücumlar.

Təhdidlərin qiymətləndirilməsi üçün istifadə olunan meyarlar $C=\{C_1,C_2,C_3\}$ aşağıdakılardır:

C_1 - Sistemin fəaliyyətinin dayandırılması, C_2 - İnformasiyanın tamlığının və konfidensiallığının pozulması, C_3 - Seçki nəticələrinin saxtalaşdırılması.

Addım 1. Əgər *Saaty* yanaşmasından [18,19] istifadə etsək, onda hər bir meyar $c_j \in C$ üzrə alternativlərin ranq münasibətlərini $\frac{R_i}{R_l}$ aşağıdakı kimi göstərə bilərik.

$$\frac{R_i}{R_l}=\begin{cases} 1, \text{əgər } A_i \ A_l \text{ ilə eynidir,} \\ 5, \text{əgər } A_i \ A_l - \text{dən üstündür,} \\ 7, \text{əgər } A_i \ A_l - \text{dən daha üstündür,} \\ 2,4,6 - \text{aralıq qiymətlər.} \end{cases}$$

Burada, $A_l - A_i$ ($i=1,4$) alternativləri arasında $l-ci$ ən pis alternativdir. Hər bir təhdidin meyarlar üzrə qiymətləndirilməsi Cədvəl 1-də göstərilmişdir.

CƏDVƏL 1. TƏHDİDLƏRİN MEYARLAR ÜZRƏ QİYMƏTLƏNDİRİLMƏSİ

	C_1	C_2	C_3
A_1	7	5	2
A_2	5	1	3
A_3	3	6	1
A_4	1	4	7

Addım 2. Tutaq ki, A_l alternativi w_l çəkisi və R_l ranqı ilə ən pis alternativdir. Ən pis hal metodundan istifadə edərək bütün alternativin çəkilərini hesablaya bilərik [19,20]. Meyarlar üzrə alternativlərin hesablanmış çəkiləri meyarları qeyri-səlis universal çoxluqlar kimi ifadə etməyə imkan verir [19].

Addım 3. Belman-Zadə prinsipinə əsasən ən yaxşı alternativ (A_{opt}) bu meyarların qeyri-səlis çoxluqlarının kəsişməsi daxilində tapıla bilər [19]. Onda, $A_{opt} \in D = C_1 \cap C_2 \cap C_3$ kəsişməsi qeyri-səlis çoxluq yaradır.

CƏDVƏL 2. ƏN PİS HAL METODU İLƏ HESABLANAN ALTERNATİVLƏRİN ÇƏKİLƏRİ

	C_1	C_2	C_3
A_1	0,438	0,333	0,154
A_2	0,313	0,067	0,231
A_3	0,188	0,400	0,077
A_4	0,063	0,200	0,538

Qeyri-səlis çoxluqlar nəzəriyyəsinə əsasən kəsişmə əməlini $\cap \to \min$ əməli ilə əvəzləyərək ən yaxşı alternativ kimi (A_{opt}) maksimum çəkili alternativ $A_{opt} \in D$ seçilir. Cədvəl 3-dən göründüyü kimi, alternativlər A_1, A_3, A_2 və A_4 ardıcıllığı ilə ranqlaşdırılır.

CƏDVƏL 3. TƏHDİDLƏRİN RANQLAŞDIRILMASI

	D	Ranq
A_1	0,154	1
A_2	0,067	3
A_3	0,077	2
A_4	0,063	4

Addım 4. Zadə yanaşmasına [21] əsasən meyarların əhəmiyyətinə görə çəki əmsallarını $\alpha_1=0.6$ (çox əhəmiyyətli), $\alpha_2=0.3$ (əhəmiyyətli) və $\alpha_3=0.1$ (az əhəmiyyətli) götürərək alternativləri ranqlaşdırmaq olar və alternativlərin çəkiləri aşağıdakı formulada göstərilmişdir.

$$D^{\alpha}=\left\{\frac{0,015}{A_1},\frac{0.02}{A_2},\frac{0.008}{A_3},\frac{0.038}{A_4}\right\}$$

Göründüyü kimi, təhdidlər meyarların əhəmiyyətinə görə A_4, A_2, A_1 və A_3 ardıcıllığı ilə ranqlaşdırılır.

NƏTİCƏ

E-səsvermə istənilən digər elektron tranzaksiyalardan öz əhəmiyyətliliyinə görə fərqləndirilir. E-səsvermədə gizli səsvermə hüququnun pozulması siyasi qalmaqala və sosial iğtişaşların baş verməsinə səbəb ola bilər. Bu baxımdan e-səsvermə fərdi məlumatların konfidensiallığına real təhdid hesab olunur. Fişinq problemi, viruslar, casus proqramları seçicilər və e-səsvermə sisteminə ciddi təhdid olaraq qalmaqdadır. Məqalədə e-səsvermə sisteminə dair yanaşmalar, tətbiqini zəruri edən amillər və sistemin təhlükəsizliyinə olan təhdidlər araşdırılır. Çoxmeyarlı qərar qəbul etmə modeli əsasında e-səsvermə sisteminin təhlükəsizliyinə olan təhdidlərin empirik qiymətləndirilməsi məsələsinə baxılır. Ən pis hal metodundan istifadə edərək bütün alternativlərin çəkiləri hesablanılır və Belman-Zadə prinsipinə əsasən təhdidlər ranqlaşdırılır.

E-səsvermə sahəsində mövcud təcrübə analiz edilərək belə nəticəyə gəlmək olar ki, lokal səviyyədə e-səsvermə sisteminin təhlükəsizliyinə olan təhdidlər qiymətləndirilməli və empirik tədqiqatlara üstünlük verilməlidir. Xüsusilə, bu məsələ inkişaf etməkdə olan ölkələr üçün aktualldır və böyük əhəmiyyət kəsb edir. E-səsvermə sisteminin təhlükəsizlik səviyyəsinə görə xüsusiyyətləri nəzərə alınmaqla yaradılacaq effektli e-səsvermə mexanizmləri bir sıra problemləri aradan qaldırmağa imkan verəcəkdir.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun mailyyə yardımı ilə yerinə yetirilmişdir – **Qrant № EİF-KETPL-2-2015-1(25)-56/05/1**

ƏDƏBİYYAT

[1] E. Abu-Shanab, M. Knight, H. Refai, “E-voting systems: a tool for e-democracy management research and practice,” vol. 2, issue 3, pp. 264-274.

[2] M. Mursi, G. Assassa and et al., “On the Development of Electronic Voting: A Survey,” International Journal of Computer Applications, vol. 61, no.16, pp. 1-13.

[3] M. Musial-Karg, “The use of e-voting as a new tool of e-participation in modern democracies,” 2014, http://pressto.amu.edu.pl/index.php/pp/-article/viewFile/2101/2091

[4] G.Schryen, “Security Aspects of Internet Voting,” Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04), 2004.

[5] X.Sh. Li, H.R. Lee, M. Lee and J.-Y. Choi, “A Study of Vulnerabilities in E-Voting System, Advanced Science and Technology Letters,” vol. 95, 2015, pp.136-139.

[6] T. G.L.A. Van der Meer, D. Gelders and S. Rotthier, “E-democracy: exploring the current stage of e-government,” Journal of Information Policy, Penn State University Press, vol. 4, 2014, pp. 489-506.

[7] M. Stoica, B. Ghilic-Micu, “E-Voting Solutions for Digital Democracy in Knowledge Society,” Informatica Economică vol. 20, no. 3, 2016, pp. 55-65.

[8] A. Al-Ameen and S.Talab, “The Technical Feasibility and Security of E-Voting,” The International Arab Journal of Information Technology, vol. 10, No. 4, 2013, pp. 397-404.

[9] R. Ssekibuule, Security Analysis of Remote E-Voting, Advances in Systems Modelling and ICT Applications, 2007 http://cit.mak.ac.ug/iccir/downloads/SREC_07/Richard%20Ssekibuule_07.pdf

[10] M.A. Javaid, Electronic Voting System Security, 2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393158

[11] Thomas W. Lauer, The Risk of e-Voting, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.93.1362

[12] B. Kang, “Cryptanalysis on an e-voting scheme over computer network,” International conference on computer science and software engineering. vol. 3, 2008. pp. 826-29.

[13] O. Cetinkaya, and D. Cetinkaya, “Verification and Validation Issues in Electronic Voting,” The Electronic Journal of e-Government, vol. 5 Issue 2, 2007, pp.117 - 126, www.ejeg.com

[14] K.-H. Wang, S.K. Mondal, K. Chan and X. Xie, “A Review of Contemporary E-voting: Requirements, Technology,” Systems and Usability, Data Science and Pattern Recognition, Volume 1, Number 1, February 2017, pp. 31-47.

[15] K. Dhillon, Challenges for LargeScale Internet Voting Implementations, 2015, https://www.cs.princeton.edu/sites/default/files/uploads/kyle_-dhillon.pdf

[16] G.Z.Qadah, “Electronic voting systems: Requirements, design, and implementation,” Elsevier Standards and interfaces, vol. 29, No. 3, 2007. p. 376-86.

[17] O.O. Okediran, E.O. Omidiora, “A Framework for A Multifaceted Electronic Voting System,” International Journal of Applied Science and Technology, vol. 1, No.4, 2011, pp. 135-142.

[18] T.L. Saaty, “Decision making with the analytic hierarchy process,” International Journal of Services Sciences, 1(1), 2008, pp. 83–98.

[19] A.P. Rotshtein, “Fuzzy multicriteria choice among alternatives: Worst-case approach,” Journal of Computer and Systems Sciences International, 48(3), 2009, pp. 379–383.

[20] R.M. Alguliyev, R.M. Aliguliyev, R.M. Mahmudova, “A Fuzzy TOPSIS+Worst-Case Model for Personnel Evaluation Using Information Culture Criteria,” International Journal of Operations Research and Information Systems, vol. 7 (4), 2016, pp. 38-66.

[21] L.A. Zadeh, “A very simple formula for aggregation and multicriteria optimization,” International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 24, no. 6, pp. 961–962, 2016.

EVALUATION OF THE ELECTRONIC VOTING SYSTEM SECURITY THREATS

Farhad Yusifov
Institute of Information Technology of ANAS, Baku, Azerbaijan
farhadyusifov@gmail.com

Abstract – E-voting is considered one of the most important components of e-democracy. Security issues play a crucial role in the implementation and development of e-voting systems. The article examines the approaches to e-voting systems and the security threats of the system. An empirical evaluation of the e-voting system security threats based on the multi-criteria decision-making model is being reviewed.

Keywords – e-voting; Internet voting; e-democracy; security; security threats.