Elektron dövlətin informasiya təhlükəsizliyi üçün diffuziya indeksi modeli

Yadigar İmamverdiyev
AMEA İnformasiya Texnologiyaları İnstitutu
yadigar@lan.ab.az

***Xülasə*— E-dövlətin informasiya təhlükəsizliyinin təmin edilməsi üçün böyük resurslar sərf edilir və nəticədə əldə edilmiş təhlükəsizlik səviyyəsinin ölçülməsi e-dövlətin informasiya təhlükəsizliyində maraqlı olan bütün tərəfləri düşündürən aktual məsələdir. Bu məqalədə e-dövlətin informasiya təhlükəsizliyinin ölçülməsi problemi analiz edilir və informasiya təhlükəsizliyinin qiymətləndirilməsi üçün müxtəlif informasiya təhlükəsizliyi metrikaları əsasında kompozit diffuziya indeksi təklif edilir.**

Açar sözlər - e-dövlət, informasiya təhlükəsizliyi, diffuziya indeksi, metrika, informasiya təhlükəsizliyi metrikası

I. GİRİŞ

E-dövlətin informasiya təhlükəsizliyi sürətlə dəyişən sahədir, dinamik bazar yeni texnologiyaların meydana çıxmasına və təhdidlər mühitinin inkişafına təkan verir. Təşkilatlar informasiya təhlükəsizliyinin təmin edilməsinə ayrılan resursları artırmağa məcbur olurlar. Lakin "nəticədə nə dərəcədə təhlükəsizik?" sualına cavab tapmaq olduqca çətindir. Buna görə də, e-dövlətin informasiya təhlükəsizliyinin ölçülməsi aktual məsələdir.

İnformasiya təhlükəsizliyinin ölçülməsi özlüyündə təcrid olunmuş məqsəd deyildir, informasiya təhlükəsizliyinin effektiv idarə edilməsinə xidmət edir. İnformasiya təhlükəsizliyinin ölçülməsi informasiya təhlükəsizliyinin cari vəziyyətinə, müəyyən period ərzində onun dəyişməsinə nəzarət etmək, təhlükəsizlik vasitələrinin fəaliyyətində problemli yerləri müəyyən etmək, səbəbləri aşkarlamaq və onların aradan qaldırılması üsullarını seçmək, informasiya təhlükəsizliyinin təmin edilməsi proseslərini təkmilləşdirmək üçün əsaslandırılmış qərarlar qəbul etmək üçün lazımdır. İnformasiya təhlükəsizliyi üzrə bu və ya digər tədbirin həyata keçirilməsindən gözlənilən nəticələri, o cümlədən, təhlükəsizliyin səviyyəsinin artması və vəsaitlərin xərclənməsi baxımından kəmiyyətcə və keyfiyyətcə qiymətləndirmək çox vacibdir.

Bu işdə e-dövlətin informasiya təhlükəsizliyi üzrə metrikaların seçilməsi və onların işlənməsi sahəsində mövcud problemlər analiz edilir. Məqalədə informasiya təhlükəsizliyi metrikalarına tələblər formalaşdırılır və müvafiq metrika qruplarının siyahısı verilir. Daha sonra e-dövlətin informasiya təhlükəsizliyi üzrə mövcud indekslər müqayisəli analiz edilir və e-dövlətin informasiya təhlükəsizliyi üçün kompozit diffuziya indeksi təklif edilir.

II. METRIKA ANLAYIŞI VƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİ ÖLÇMƏ MODELİ

Adətən, informasiya təhlükəsizliyinin ölçülməsini riskin qiymətləndirilməsi ilə əlaqələndirirlər, lakin informasiya təhlükəsizliyi risklərini dəqiq müəyyən etmək çətindir. Bundan başqa, informasiya təhlükəsizliyinin təmin edilməsi üzrə fəaliyyət geniş məsələləri əhatə edir və onun ölçülməsini təkcə risklərin qiymətləndirilməsi ilə məhdudlaşdırmaq düzgün deyil.

İnformasiya təhlükəsizliyinin ölçülməsi üzrə elmi tədqiqatlar və praktiki təşəbbüslər 2000-ci illərdən intensivləşir. Müvafiq elmi-tədqiqat və praktiki fəaliyyət istiqaməti *informasiya təhlükəsizliyi metrikaları* adlandırılır (ing. security metrics). Bu istiqamətə diqqətin göstəricisi kimi 2006-cı ildən başlayaraq hər il Usenix konfransı çərçivəsində informasiya təhlükəsizliyi metrikaları üzrə təşkil olunan Metricon seminarlarını (www.securitymetrics.org) göstərmək olar. Eyni zamanda, ABŞ Müdafiə Nazirliyinin informasiya təhlükəsizliyinə zəmanət metrikaları proqramı (layihəsi), US-CERT-in idarəetmə sistemləri üçün kiber-təhlükəsizlik metrikaları, OWASP konsorsiumunun tətbiqi proqramların təhlükəsizlik metrikaları layihəsini və s. göstərmək olar.

Metrika, ölçü və indikator terminləri çox zaman sinonim kimi işlədilir. Bir çox halda bu üç termin arasında semantik fərq çox kiçik olsa da, onların məna müxtəlifliyini başa düşmək bəzi kontekstlərdə faydalı ola bilər. Bu anlayışların məzmununa qısa nəzər salaq. Ədəbiyyatda metrika anlayışının müxtəlif tərifərinə rast gəlmək mümkündür. Bu məqalədə aşağıdakı tərif əsas götürülür.

Metrika (ing. metrics) – faəliyyətin məhsuldarlığı ilə əlaqəli relevant verilənlərin toplanması, analizi və hesabat verilməsi yolu ilə qərar qəbul edilməsini asanlaşdırmaq, faəliyyətin məhsuldarlığını və hesabatlılığı yaxşılaşdırmaq üçün nəzərdə tutulmuş alətlərdir. Sadə yanaşmada metrika ölçmə standartı və ya sistemidir. Baxılan halda, metrikalar təhlükəsizliyi ölçmək, xüsusilə təşkilatın təhlükəsizlik səviyyəsini ölçmək üçün standartdır [1].

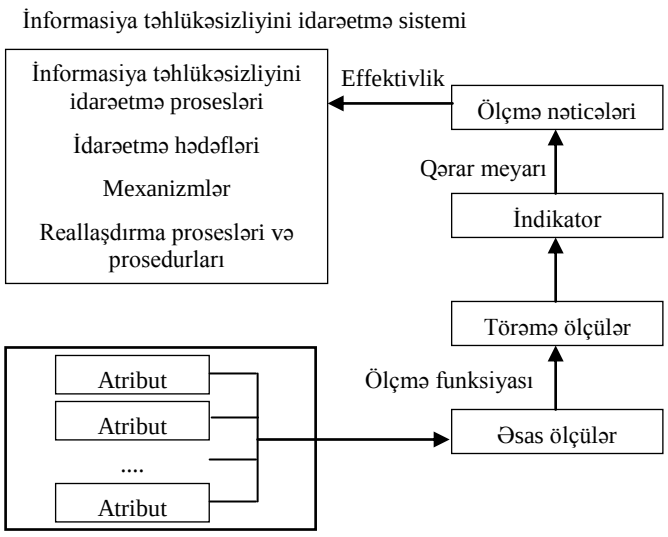
ISO/IEC 27004 standartında informasiya təhlükəsizliyini idarəetmə sisteminin effektivliyini qiymətləndirmək üçün müvafiq metrikaların yaradılması və istifadəsi üzrə tövsiyələr verilir [2]. ISO/IEC 27004-də irəli sürülən ölçmə modelinin sxemi şəkil 1-də göstərilib. Standartda aşağıdakı terminlər istifadə edilir.

Atribut – ölçmə obyektinin insan tərəfindən və ya avtomatlaşdırılmış vasitələrlə kəmiyyətcə və ya keyfiyyətcə müəyyən edilə bilən xassəsi və ya xarakteristikasıdır.

Şkala – əsas ölçüdə istifadə edilən qiymətlərin və kateqoriyaların nizamlanmış çoxluğudur.

Ölçmə metodu uyğun şkalanı tətbiq etməklə atributu kəmiyyətcə ölçür.

Əsas ölçü - atributun təyin edilmiş ölçmə metodu vasitəsilə ölçülən qiymətidir (məsələn, təlim görmüş əməkdaşların sayı). Verilənlər toplanan zaman qiymət əsas ölçüyə mənimsədilir (ölçü – qiymət mənimsədilən dəyişəndir). Əsas ölçü digər ölçülərdən funksional asılı olmur.



Şək. 1. ISO 27004 - informasiya təhlükəsizliyinin ölçülməsi modeli

Ölçmə funksiyası əsas ölçülərin törəmə ölçüdə necə birləşdirilməsini müəyyən edir.

Törəmə ölçü – iki və ya daha artıq əsas ölçünün funksiyası kimi hesablanan ölçüdür.

Analitik model hər bir ölçü üçün bir və ya daha artıq törəmə ölçünün indikatora çevrilməsini müəyyən edir.

İndikator – analitik modelin bir və ya bir neçə ölçüyə qərar qəbuletmə kriteriyalarına və informasiya ehtiyaclarına nəzərən tətbiqinin nəticəsidir. İndikatorlar törəmə ölçülərin birləşməsi və onların qərar qəbulu kriteriyaları əsasında interpretasiyası yolu ilə formalaşdırılır.

İndeks – xüsusi yaradılmış göstəricidir, indikatorların əlaqəsini, kombinasiyasını ifadə edir, müəyyən xüsusi hipotezin əsaslandırılmasına və yoxlanılmasına xidmət edir.

III. METRİKALARA TƏLƏBLƏR

Metrikalar aşağıdakı atributları ilə tam müəyyən olunurlar:

- Metrikanın adı;
- Nəyin ölçüldüyünün təsviri;
- Metrikanın ölçülməsi necə aparılır;
- Ölçmə hansı tezliklə aparılır;
- Sərhəd qiymətləri necə hesablanır;
- Metrika üçün normal hesab edilən qiymətlərin diapazonu;
- Metrikanın ən yaxşı mümkün qiymətləri;
- Ölçmə vahidi.

Adətən, yaxşı metrikaların yaradılması üçün SMART (Specific, Measurable, Achievable, Relevant, Timely) metodikası istifadə edilir [3]. Bu metodikaya görə metrika aşağıdakı tələbləri ödəməlidir:

- **Konkret (**ing. **Specific)**: metrika konkret, aydın olmalı və ölçülən prosesə bilavasitə aidiyyatı (münasibəti) olmalıdır.
- **Ölçülə bilən (**ing. **Measurable)**: metrika ölçülə bilən olmalıdır, yəni onu kəmiyyətcə birqiymətli ölçmək imkanı mövcud olmalıdır.
- **Tətbiq edilə bilən (**ing. **Actionable)**: metrikanın qiymətinin yaxşılaşması üçün prosesə təsir etmək imkanı mövcud olmalıdır.
- **Relevant (**ing. **Relevant)**: metrikanın qiymətinin yaxşılaşması təhlükəsizlik məqsədlərinə nail olunmasında baxılan prosesin təsirinin (payının) artmasını bildirməlidir.
- **Ölçmə vaxtı (**ing. **Timely)**: effektiv istifadə olunması üçün metrikanı kifayət qədər tez ölçmək mümkün olmalıdır.

Yaxşı metrikaların yaradılması üçün digər yanaşmalar da mövcuddur [4]:

- PRAGMATIC (**P**redictive, **R**elevant, **A**ctionable, **G**enuine, **M**eaningful, **A**ccurate, **T**imely, **I**ndependent);
- PURE (**P**ositively Stated, **U**nderstood, **R**ealistic, **E**thical);
- CLEAR (**C**hallenging, **L**egal, **E**nvironmentally Sound, **A**greed, **R**ecorded).

İnformasiya təhlükəsizliyinin təmin edilməsi proseslərinin və tədbirlərinin nəticəliliyini və effektivliyini izləmək üçün başlanğıcda hiss edilən nəticəsi olmayan və qiymətləndirilməsinə əhəmiyyətli zəhmət tələb edilən çox sayda metrika fikirləşmək lazım deyil. Əsas proseslər və tədbirlər üçün bir neçə metrika müəyyən etmək lazımdır ki, kənarlaşma və potensial kənarlaşma haqqında vaxtında siqnal verə bilsin. Beləliklə, müəyyən kənarlaşma müşahidə etdikdə diaqnostika məqsədləri üçün operativ olaraq əlavə metrikalar daxil etmək olar ki, onlar da qiymətləndirilən prosesdə problemi daha diqqətlə diaqnostika etməyə imkan verir. Eyni zamanda, bu metrikaların qiymətləndirilməsi periodunu və bu metrikalardan istifadəyə lüzum olmadığını müəyyən edən meyarları da müəyyən etmək zəruridir.

IV. İNFORMASİYA TƏHLÜKƏSİZLİYİ ÜZRƏ METRİKALAR

Məlumdur ki, başqa fəaliyyət sahələrində fəaliyyətin məhsuldarlığını və qarşıya qoyulmuş məqsədlərə nail olunmasını ölçmək üçün bir sıra indikatorlar mövcuddur, məsələn, fəaliyyət məhsuldarlığının əsas indikatorları (Key Performance Indicators, KPI), uğurun kritik faktorları (Critical Success Factors, CSF), əsas məqsəd indikatorları (Key Goal Indicators, KGI), balanslaşdırılmış indikatorlar sistemi

(Balanced Scorecard, BSC), təhlükəsizlik üzrə yetkinlik modelləri (COBiT, CERT/CSO, ISM3) və s.

Bu modellərin informasiya təhlükəsizliyi üçün modifikasiyaları üzərində işlər aparılır, lakin burada informasiya təhlükəsizliyinin xarakterindən irəli gələn bir sıra kritik problemlər mövcuddur.

Ümumiyyətlə, metrikaların işlənməsi üçün ən effektiv yol – biznes-məqsədin altməqsədlərə ayrılması, uyğun hərəkətlərin müəyyən edilməsi və onların hər biri üçün metrikanın seçilməsidir. Metrikaların biznes-məqsədlərə bağlı olmasını təmin edən ən sadə yanaşma isə GQM (Goal Question Metric) adlanan modeldir. Bu modeldə məqsədi aydınlaşdıran suallar verilir və hər suala uyğun metrika seçilir.

İnformasiya təhlükəsizliyi metrikaları təhlükəsizliyin məqsədləri ilə əlaqəlidir. Təhlükəsizliyin məqsədləri arzu edilən nəticəni, metrikalar isə ona nail olunmasında irəliləyişi əks etdirir. Lakin informasiya təhlükəsizliyi məqsədləri ilə informasiya təhlükəsizliyi üzrə fəaliyyət arasında birbaşa əlaqə yoxdur. Təhlükəsizlik proseslərinə müəyyən təsir edərək, siz heç zaman deyə bilməzsiniz ki, təhlükəsizlik məqsədlərinə həqiqətən də yaxınlaşmısınız. Daha bir problem ölçmələrin fəaliyyətlə əlaqələndirilməməsidir, ölçmələr çox zaman nəticələrə fokuslanır. Nəticədə, informasiya təhlükəsizliyi məqsədləri üçün metrikaları tapmaq çətindir və onlar informasiya təhlükəsizliyinin idarə edilməsi üçün o qədər də faydalı olmurlar.

Elmi-tədqiqat işlərinin və praktiki işlər haqqında hesabatların analizi e-dövlətin informasiya təhlükəsizliyi üzrə metrikaların aşağıdakı siyahısını tərtib etməyə imkan verir:

- kiber-təhdidlərin cari vəziyyətini xarakterizə edən metrikalar;
- zərərli proqramlarla əlaqədar metrikalar;
- boşluqların idarə edilməsi üzrə metrikalar;
- risk və/və ya uyğunluq metrikaları;
- informasiya təhlükəsizliyi texnologiyalarının istehsalını xarakterizə edən metrikalar;
- e-dövlət xidmətlərini xarakterizə edən metrikalar;
- informasiya təhlükəsizliyi insidentlərinin idarə edilməsi üzrə metrikalar;
- kibercinayətkarlıqla mübarizə üzrə metrikalar;
- kadr hazırlığını xarakterizə edən metrikalar;
- əhalinin və təşkilatların informasiya təhlükəsizliyi mədəniyyəti üzrə metrikalar;
- əhalinin maarifləndirilməsini xarakterizə edən metrikalar;
- informasiya təhlükəsizliyinin iqtisadiyyatı üzrə metrikalar;
- milli və beynəlxalq əməkdaşlıq üzrə metrikalar.

V. İNFORMASİYA TƏHLÜKƏSİZLİYİ METRİKALARI ÜZRƏ GÖRÜLMÜŞ İŞLƏRİN İCMALI

Son illər informasiya təhlükəsizliyi metrikaları və ölçmə modelləri mövzusunda bir sıra tədqiqat məqalələri yazılmışdır. R. Savola təhlükəsizlik metrikaları üçün taksonomiya təklif etdir [5]. T. Heyman və həmmüəllifləri təhlükəsizlik metrikalarını müəyyən etmək və onların nəticələrini interpretasiya etmək üçün təhlükəsizlik şablonları anlayışından istifadə etməyi təklif edir [6]. Andrew Jaquith yaxşı tanınan kitabında [7] fəaliyyətin məhsuldarlığı haqqında maraqlı ideyalar təqdim edir. Müəlliflər [8]-də riskin təhlükəsizlik metrikası kimi keyfiyyətlərini analiz edirlər, alternativ metrikalar kimi meyarlara uyğunluq, müdaxilələrin aşkarlanması, siyasət və insident əsasında metrikalar təklif edirlər. Nəhayət, yaxşı təhlükəsizlik metrikalarının xarakteristikalar çoxluğu sadalanır: onlar doğru şeyi ölçməlidirlər (məqsədəyönəlik olmalıdırlar), kəmiyyətcə ölçməlidirlər, dəqiqliklə ölçülə bilməlidirlər, etalon testlə müqayisə edilə bilməlidirlər, yerinə yetirilməsi ucuz olmalıdır, müstəqil olaraq yoxlanıla bilməlidirlər, təkrarlanan və miqyaslanan olmalıdırlar. A.J.A. Wang təhlükəsizlik metrikaları haqqında bəzi məsələləri xülasə edir [9]: keyfiyyət və kəmiyyət metrikalarının müqayisəsi, subyektivlik və obyektivlik, modelləşdirmə, zaman keçdikcə doğruluq, məntiqi qiymətlərin (True və False) təhlükəsizlik metrikaları üçün zəifliyi və s. Müəllif üç abstraksiya səviyyəsinə: istifadəçilər, servislər və infrastruktur səviyyəsinə baxaraq informasiya təhlükəsizliyinin formal modelini də təqdim edir. Yaxşı metrikanın arzu edilən xassələrini təsvir edən bir neçə aksiom da təqdim edilir. Müəlliflər [10]-da təhlükəsizlik metrikaları müəyyən etmək üçün sistematik metodologiya təqdim edirlər. Metodologiya metrika tələblərinin müəyyən edilməsi ilə başlayır, boşluqlar və proqram təminatının xarakteristikaları identifikasiya edilir, təhlükəsizlik modelləri analiz edilir, təhlükəsizlik metrikaları kateqoriyalaşdırılır və işlənilir.

İnformasiya təhlükəsizliyi metrikaları üzrə bir neçə milli və beynəlxalq standartlar da işlənmişdir. Onlardan NIST SP 800-55 – informasiya sistemləri üçün təhlükəsizlik metrikaları üzrə qaydaları, NIST SP 800-80 – informasiya təhlükəsizliyi üçün fəaliyyət məhsuldarlığı metrikalarının işlənməsi üçün qaydaları, ISO/IEC 21827 – sistemlərin təhlükəsizlik mühəndisliyi üçün potensialın yetkinlik modelini və yuxarıda haqqında danışılan ISO 27004 standartını qeyd etmək olar.

VI. İNFORMASİYA TƏHLÜKƏSİZLİYİ ÜZRƏ İNDEKSLƏR

İnternetdə axtarışlar nəticəsində Beynəlxalq Telekommunikasiya İttifaqının *qlobal kiber-təhlükəsizlik indeksi* (Global Cybersecurity Index, GCI) [11], Koreya İnternet və Təhlükəsizlik Agentliyinin təklif etdiyi *milli informasiya təhlükəsizliyi indeksi* (National Information Security Index, NISI) [12], *kiber-təhlükəsizlik indeksi* [13] və *milli kibertəhlükəsizliyin idarə edilməsi sisteminin yetkinlik modeli* (National Cybersecurity Management System Maturity Model, NCSecMS) [14] kimi indekslər haqqında məlumat toplamaq mümkün olmuşdur. Bu indekslərdən yalnız qlobal kiber-təhlükəsizlik indeksi üçün ölkələr üzrə qiymətləndirmələrin aparılması məlumdur.

Qlobal kiber-təhlükəsizlik indeksi dövlətlərin kibertəhlükəsizlik səviyyəsini beş əsas sahədə ölçməyi və ranqlaşdırmağı məqsəd qoyur:

1) qanunvericilik tədbirləri (kiber-cinayətkarlıq üzrə qanunvericilik, tənzimləmə və nəzarət);

2) texniki tədbirlər (CERT, standartlar, sertifikatlaşdırma);

3) təşkilati tədbirlər (siyasət, idarəçilik üzrə yol xəritəsi – strategiya, cavabdeh təşkilat, milli etalon qiymətləndirmə);

4) potensial qurulması tədbirləri (standartların işlənməsi, insan resurslarının inkişafı, peşəkarların sertifikatlaşdırılması, təşkilatların sertifikatlaşdırılması);

5) əməkdaşlıq (idarələrarası, idarədaxili, dövlət-özəl sektor, beynəlxalq).

Ölkələrin qlobal kiber-təhlükəsizlik indeksinin müəyyən edilməsi üçün ölkələrdən məlumatların toplanması 2014-cü ildə həyata keçirilirdi.

NCSecMS modeli metodologiya baxımından ISO 27001 və Cobit yanaşmasına əsaslanır. Bu modelə görə milli kiber-təhlükəsizliyin maraqlı tərəfləri dövlət, özəl sektor, vətəndaş cəmiyyəti, akademiya (universitetlər, elmi tədqiqat təşkilatları və s.) və kritik infrastrukturdur. NCSec idarəetmə platforması 5 domendən ibarətdir: 1) strategiya və siyasət; 2) reallaşdırma və təşkiletmə; 3) maarifləndirmə və kommunikasiya; 4) uyğunluq və koordinasiya; 5) qiymətləndirmə və monitorinq.

Kiber-təhlükəsizlik indeksi informasiya təhlükəsizliyi və risk menecmenti üzrə iki mütəxəssis (D. Geer və M. Pareek) tərəfindən təklif edilib. Bu indeks 2011-ci ilin aprelindən başlayaraq hər ay veb-saytda dərc olunur. İndeks 300-ə yaxın respondentin rəy sorğusu əsasında hesablanır. Sorğuya hücum aktorları (5 sual), hücum silahları (5 sual), hücum edənlərin motivasiyaları (3 sual), hücum hədəfləri (6 sual), müdafiə (2 sual), ümumi fikirlər (3 sual) daxildir. Respondent beş cavab variantından birini seçir: "sürətlə azalır", "azalır", "dəyişmir", "yüksəlir", "sürətlə yüksəlir".

VII. E-DÖVLƏTİN İNFORMASİYA TƏHLÜKƏSİZLİYİ ÜZRƏ DİFFUZİYA İNDEKSİ

Diffuziya indeksi (dinamik faktor kimi də tanınır) ekonometrikada bir neçə zaman sırasının birgə dəyişməsini müəyyən edir. Diffuziya indeksi indeksə müsbət təsir edən komponentlərin nisbətini ölçür. Onu bəzi makroiqtisadi modellərdə istifadə edirlər [15, 16]. Diffuziya indeksi ilk dəfə biznes tsiklində dönmə nöqtəsini tapmaq üçün təklif edilmişdi [17].

Diffuziya indeksi bir neçə zaman sırasındakı ümumi tendensiyanı müəyyən edir. Əgər sıraların çoxunda enmə yox, qalxma varsa, indeks 50-dən böyük olur. Əgər enmələr qalxmalardan çoxdursa, onda diffuziya indeksi 50-dən kiçikdir.

Diffuziya indeksinin hesablanmasında ilk addımda komponentlərin artdığı, azaldığı və ya dəyişmədiyi müəyyən edilir. Əgər komponentin artımı 0.05 faizdən çoxdursa, ona 1, dəyişmə 0.05 faizdən azdırsa, həmin komponentə 0.5 və 0.05 faizdən çox azalan komponentə isə 0 mənimsədilir. Sonrakı addımlarda komponentlərə mənimsədilən qiymətlər toplanır və komponentlərin sayına bölünür. Nəhayət, alınan nəticə 100-ə bölünür.

Fərz edək ki, bölmə 4-də göstərilən informasiya təhlükəsizliyi metrikalarının hər biri üçün diffuziya indeksi (DI_i) hesablanıb. Diffuziya indeksləri ölçüsüz kəmiyyətlərdir və onları toplamaq olar. Təklif edilən kompozit diffuziya indeksini $CDI = \sum_{i=1}^{n} w_i DI_i$ düsturu ilə hesablamaq olar,

burada w_i müvafiq çəkilər, n metrikaların sayıdır.

VIII. NƏTICƏ

Bu məqalədə e-dövlətin informasiya təhlükəsizliyini qiymətləndirmək üçün kompozit diffuziya indeksi təklif edilir. Təklif edilən kompozit diffuziya indeksi informasiya təhlükəsizliyi üzrə müxtəlif indikatorların aqreqasiyası əsasında formalaşır, aqreqasiya zamanı məlumat mənbələrinin əhəmiyyətlilik (relevantlıq) dərəcələri nəzərə alınır.

Gələcək tədqiqat məsələləri kimi informasiya təhlükəsizliyi metrikaları üzrə məlumatların toplanması və analizi (rəy sorğusu), indikatorların həssaslıq analizi, informasiya təhlükəsizliyi indikatorları ilə e-dövləti xarakterizə edən digər indikatorların əlaqələrinin analizi qarşıya qoyulur.

ƏDƏBIYYAT

[1] W. Jansen "NISTIR 7564: Directions in Security Metrics Research." 2009, 26 p.

[2] ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement.

[3] G. T. Doran "There's a S.M.A.R.T. way to write management's goals and objectives," Management Review (AMA FORUM), vol. 70, no. 11, pp. 35–36, 1981.

[4] W. K. Brotby, G. Hinson "PRAGMATIC security metrics: Applying metametrics to information security." Auerbach Publications. 2013.

[5] R. M. Savola "Towards a taxonomy for information security metrics," Proc. of the 2007 ACM workshop on Quality of protection (QoP'07), pp-28-30, 2007.

[6] T. Heyman, R. Scandariato, C. Huygens, W. Joosen "Using security patterns to combine security metrics," Proc. of the 3rd International Conference on Availability, Reliability and Security (ARES'08), pp.1156-1163, 2008.

[7] A. Jaquith "Security metrics: replacing fear, uncertainty, and doubt." Addison-Wesley, 2007.

[8] O. S. Saydjari "Is Risk a good security metric?," Proc. of the 2nd ACM workshop on Quality of Protection, pp. 59-60, 2006.

[9] A. J. A. Wang "Information security models and metrics," Proc. of the 43rd Annual Southeast regional conference (ACM-SE 43), vol. 2, pp. 178-184, 2005.

[10] S. Chandra, R. A. Khan "Software security metric identification framework (SSM)," Proc. of the International Conference on Advances in Computing, Communication and Control (ICAC3'09), pp.725-731, 2009.

[11] ITU Global Cybersecurity Index. www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI.pdf

[12] S.-W. Hwang "Development of the National Cyber Safety Index," ITU Regional Cybersecurity Forum (Brisbane, AU), July 15, 2008. http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/weon-national-information-security-index-brisbane-july-08.pdf

[13] M. D. El Kettani, T. Debbagh, NCSecMM: "A National Cyber Security Maturity Model for an Interoperable "National Cyber Security" Framework," Proc. of the 9th European Conference on e-Government, pp. 236-247, 2009.

[14] Index of Cyber Security http://www.cybersecurityindex.org/

[15] P. M.Getz, M. G. Ulmer "Diffusion indexes: an economic barometer," Monthly Labor Review, vol. 113, no. 4, pp. 13-22, 1990.

[16] J. H. Stock, M. W. Watson "Macroeconomic forecasting using diffusion indexes," Journal of Business & Economic Statistics, vol. 20, no. 2, pp. 147-62, 2002.

[17] M. Forni, M. Lippi, "The generalized dynamic factor model: representation theory", Econometric Theory, vol. 17, no. 6, pp. 1113-41, 2001.