UOT 004.056 DOI: 10.25045/jpis.v09.i2.02

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

MİLLİ KİBERTƏHLÜKƏSİZLİK ÜÇÜN ENTROPİYA ÇƏKİLƏRİ VƏ DİNAMİK İNDEKS

Hazırda kibertəhlükəsizlik milli təhlükəsizliyin vacib komponentlərindən birinə çevrilmişdir və onun effektiv təmin edilməsi üçün milli kibertəhlükəsizlik səviyyəsinin qiymətləndirilməsi vacib məsələdir. Bu məsələnin həlli üçün bir sıra təşkilatlar tərəfindən milli kibertəhlükəsizlik indeksləri təklif edilmişdir. Lakin milli kibertəhlükəsizlik indeksinin işlənməsi sahəsində elmi tədqiqatlar və praktiki işlər erkən mərhələdədir,onların metodoloji əsaslandırılması qənaətbəxş və tam deyil. Bu işdə mövcud milli kibertəhlükəsizlik indeksləri müqayisəli analiz edilir, onların üstün və nöqsanlı cəhətləri göstərilir, onların təkmilləşdirilməsi üçün təkliflər irəli sürülür. Kompozit milli kibertəhlükəsizlik indekslərinə daxil olan indikatorların çəkilərinin entropiya əsasında qiymətləndirilməsi metodu təklif edilir. Nəhayət, statik və dinamik kibertəhlükəsizlik indeksləri daxil edilir və təklif edilən yanaşmaların real verilənlər əsasında qiymətləndirilməsi aparılır.

Açar sözlər: *kibertəhlükəsizlik, indikator, entropiya, kompozit indeks, dinamik indeks, statik kibertəhlükəsizlik indeksi, dinamik kibertəhlükəsizlik indeksi, milli kibertəhlükəsizlik indeksi.*

Giriş

Hazırda kibertəhlükəsizlik milli təhlükəsizliyin vacib komponentlərindən birinə çevrilmişdir [1]. Kibertəhlükəsizlik sürətlə dəyişən sahədir, dinamik bazar yeni texnologiyaların meydana çıxmasına və kibertəhdidlər mühitinin inkişafına güclü təkan verir. Dövlətlər kibertəhlükəsizliyin təmin edilməsinə ayrılan resursları artırmağa məcbur olurlar. Lakin "Nəticədə nə dərəcədə təhlükəsizik?" sualına cavab tapmaq olduqca çətindir. Buna görə də, dövlətin kibertəhlükəsizliyinin ölçülməsi aktual məsələdir.

Kibertəhlükəsizliyin ölçülməsi özlüyündə təcrid olunmuş məqsəd deyildir, kibertəhlükəsizliyin effektiv idarə edilməsinə xidmət edir. Mövcud və yeni yaranan kibertəhlükəsizlik təhdidlərinə qarşı effektiv əks-tədbirlər haqqında optimal qərarlar qəbul etmək üçün milli kibertəhlükəsizliyin cari vəziyyətini müəyyən etmək – ölçmək tələb edilir. Lakin kibertəhlükəsizliyin səviyyəsinin ölçülməsi məsələsi kifayət qədər mürəkkəb məsələdir [2]. Kibertəhlükəsizlik səviyyəsinə təsir edən faktorlar kifayət qədər çoxdur, onlar dinamik dəyişirlər və bir-biri ilə mürəkkəb qarşılıqlı əlaqələri vardır. Seçilmiş indikatorlar çoxluğu əsasında formalaşdırılan indeks kibertəhlükəsizlik vəziyyətini ayrılıqda götürülmüş bir indikatordan daha yaxşı əks etdirir. Bu baxımdan milli kibertəhlükəsizlik indeksinin işlənməsi vacibdir.

Qeyd etmək lazımdır ki, milli kibertəhlükəsizlik indeksinin işlənməsi sahəsində elmi tədqiqatlar və praktiki işlər erkən mərhələdədir, onların metodoloji əsaslandırılması hələlik qənaətbəxş deyil [2, 3]. Milli kibertəhlükəsizlik səviyyəsini necə ölçmək, hansı ölçmə indikatorlarını əsas götürmək, mümkün ölçmələrin nə dərəcədə adekvat olması kimi məsələlərə aydınlıq gətirilməlidir. Milli kibertəhlükəsizlik indeksi kiber-təhlükəsizliyin cari səviyyəsini də əks etdirməlidir.

Bu işdə mövcud milli kibertəhlükəsizlik indeksləri analiz edilir, onların qurulmasında istifadə edilən indikatorlar təhlil edilir, indekslərin üstün cəhətləri və çatışmazlıqları göstərilir, onların təkmilləşdirilməsi üçün təkliflər irəli sürülür. Kompozit milli kibertəhlükəsizlik indekslərinə daxil olan indikatorların çəkilərinin entropiya əsasında qiymətləndirilməsi təklif edilir. Nəhayət, statik və dinamik kibertəhlükəsizlik indeksləri daxil edilir və təklif edilən yanaşmaların real verilənlər əsasında qiymətləndirilməsi aparılır.

Mövcud milli kibertəhlükəsizlik indekslərinin analizi

Ölkələrin kibertəhlükəsizlik səviyyələrini qiymətləndirmək üçün bir sıra indekslər təklif edilmişdir, məsələn: Beynəlxalq Telekommunikasiya İttifaqının qlobal kiber-təhlükəsizlik indeksi (Global Cybersecurity Index, GCI) [4, 5], Koreya İnternet və Təhlükəsizlik Agentliyinin təklif etdiyi *milli informasiya təhlükəsizliyi indeksi* (National Information Security Index, NISI) [6], milli kibertəhlükəsizlik indeksi (***National Cyber Security Index, NCSI***) [7], *kiber-təhlükəsizlik indeksi* [8] və *milli kibertəhlükəsizliyin idarə edilməsi sisteminin yetkinlik modeli* (National Cybersecurity Management System Maturity Model, NCSecMS) [9]. Bu indekslərdən yalnız qlobal kiber-təhlükəsizlik indeksi (GCI) və milli kibertəhlükəsizlik indeksi **(NCSI)** üçün ölkələr üzrə qiymətləndirmələrin aparılması məlumdur. [10]-da texnoloji, hüquqi, iqtisadi, mədəni və beynəlxalq faktorları nəzərə almaqla kibertəhlükəsizlik indeksinin formalaşdırılması üçün ümumi konseptual model irəli sürülür. Aşağıda bəzi kibertəhlükəsizlik indekslərinin qısa icmalı verilir.

Qlobal kibertəhlükəsizlik indeksi (*Global CyberSecurity Index, GSI*) dövlətlərin kibertəhlükəsizlik səviyyəsinin beş əsas sahədə ölçməsi və ranqlaşdırması məqsədini daşıyır:

1) Hüquqi tədbirlər (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).

GCI bu beş istiqaməti xarakterizə edən 25 indikatoru bir indeksdə birləşdirən kompozit indeksdir. Ölkələrin GCI indeksinin müəyyən edilməsi üçün ölkələrdən məlumatların toplanması 2014-cü ildən həyata keçirilir.

Cədvəl 1. Bəzi ölkələrin Qlobal kibertəhlükəsizlik indeksləri (2015) [5]

Ölkə	Hüquqi	Texniki	Təşkilati	Potensial	Əməkdaşlıq	İndeks	Ranq
Avstraliya	0.7500	0.6667	0.8750	0.8750	0.6250	0.7647	3
Rusiya	1.0000	0.3333	0.5000	0.3750	0.5000	0.5000	12
Polşa	1.0000	0.3333	0.6250	0.6250	0.2500	0.5294	11
Pakistan	0.2500	0.1667	0.0000	0.3750	0.1250	0.1765	23
Gürcüstan	0.7500	0.6667	0.7500	0.2500	0.2500	0.5000	12
Ukrayna	0.7500	0.3333	0.2500	0.1250	0.5000	0.3529	17
Albaniya	0.7500	0.3333	0.1250	0.1250	0.0000	0.2059	22
Keniya	1.0000	0.3333	0.2500	0.2500	0.5000	0.4118	15
Nepal	0.5000	0.0000	0.1250	0.0000	0.1250	0.1176	25

Bir çox ölkələr eyni reytinqə malikdirlər, bu onların eyni hazırlıq səviyyəsinə malik olduğunu göstərir. Beləliklə, indeksin qranulyarlıq səviyyəsi aşağıdır, indeks ölkənin detallı potensialını və ya mümkün zəifliklərini xarakterizə etməyə deyil, kibertəhlükəsizlik hazırlığının səviyyəsini əks etdirməyə yönəlib.

***Milli kibertəhlükəsizlik indeksi* (*National Cyber Security Index, NCSI*)** – bu indeks Estoniyada e-Governance Academy (Estonia) tərəfindən işlənmişdir [7].

Müəlliflərə görə, NCSI indeksinin məqsədi milli kiber-təhlükəsizlik barədə dəqiq, aktual və əlyetər informasiya təmin edən kompleks ölçmə aləti təqdim etməkdir. Milli kibertəhlükəsizlik indeksi ölkənin əsas kiber-təhdidlərin baş verməsinin qarşısının alınmasına hazırlığını və kiber-insidentlərin, kibercinayətlərin, böyük miqyaslı kiberkrizislərin idarə edilməsinə hazırlığını ölçür. NCSI milli kibertəhlükəsizlik potensialının qurulmasında bir alət kimi istifadə edilə bilər.

İndeks ölkənin e-servislərdə imtinalar, verilənlərin tamlığının pozulması, verilənlərin konfidensiallığının pozulması kimi əsas kiber-təhdidlərə qarşı nə dərəcədə yaxşı hazırlandığını ölçür. NCSI metodologiyası aşağıdakı istiqamətlər üzrə 12 indikatoru əhatə edir:

- Ümumi indikatorlar (1. Siyasətin işlənməsi; 2. Təhdidlərin qiymətləndirilməsi; 3. Kibertəhlükəsizlik təhsili);
- Baza indikatorları (4. Baza təhlükəsizliyi; 5. E-servislərin təhlükəsizliyi; 6. E-identifikasiya və e-imza; 7. Kritik informasiya infrastrukturunun təhlükəsizliyi);
- İnsidentlərin idarə edilməsi indikatorları (8. Kiber-insidentləri 24/7 rejimində cavablandırma mərkəzi; 9. Krizislərin idarə edilməsi; 10. Kibercinayətlərlə mübarizə; 11. Hərbi potensial);
- Beynəlxalq əməkdaşlıq indikatorları (12. Beynəlxalq təsir).

Bu 12 indikator bir neçə sub-indikatora və ölçülən aspektlərə malikdir.

Hər bir indikator qiymətə malikdir ki, bu onun indeksdəki nisbi vacibliyini göstərir. Qiymətlər aşağıdakılar nəzərə alınmaqla ekspertlər qrupu tərəfindən verilir:

- 1 bal – müəyyən sahəni tənzimləyən hüquqi sənəd.
- 2-4 bal – kibertəhlükəsizlik üzrə müəyyən cavabdehliyi olan bölmə.
- 2 bal – əməkdaşlıq formatı (şura, komitə və s.)
- 1-3 bal – nəticə (sənəd, təlimlər, texnologiyalar və s.)

NCSI version 1.0-da maksimal qiymət 99 baldır. İndeks cədvəlində ölkənin NCSI faizi indeksin maksimal qiymətinə nisbətən hesablanır. İndikatorların əlavə edilməsindən və ya çıxarılmasından asılı olmayaraq, NCSI maksimal qiyməti həmişə 100 (100%) olur.

İndeksin ideyası milli səviyyədə əlyetər mənbələrdən verilənlərin toplanması və onu faktiki materiallar əsasında hesablamaqdır. Bu o deməkdir ki, indeks yalnız əlyetər veb-saytlarla və ya rəsmi sənədlərlə təsdiqlənə bilən məlumatlardan istifadə edir.

Bəzi ölkələrin NCSI indeksləri cədvəl 2-də göstərilib. NCSI metodologiyasında NCSI indeksinə əlavə olaraq, informasiya cəmiyyətinin inkişafı indeksi də (ISD Score) daxil edilir. ISD indeksi "ICT Development" [11] və "Networked Readiness" [12] indekslərinin ədədi ortası kimi hesablanır.

Ratio = NCSI Score – ISD Score fərqi NCSI və ISD indeksləri arasındakı asılılığı göstərir. Müsbət nisbət ölkədə milli kibertəhlükəsizliyin səviyyəsinin informasiya cəmiyyətinin inkişafına uyğun olduğunu və ya onu qabaqladığını göstərir. Mənfi nisbət göstərir ki, ölkənin elektron cəmiyyəti milli kibertəhlükəsizlik sahəsi ilə müqayisədə daha çox inkişaf edib.

NCSI v 1.0 indeksinin nöqsanı kimi qeyd etmək olar ki, bu indeks mərkəzi hökumət tərəfindən milli səviyyədə həyata keçirilən kibertəhlükəsizlik tədbirlərinin mövcudluğunu qiymətləndirir. NCSI v 1.0 bu tədbirlərin keyfiyyətini və əməliyyat effektivliyini qiymətləndirmir.

Cədvəl 2. Bəzi ölkələrin NCSI indeksləri [7]

Ranq	**Ölkə**	**NCSI indeksi**	**ISD indeksi**	**Nisbət (Ratio)**
1	Avstraliya	58.59	80.74	-22.15
2	Rusiya Federasiyası	58.24	66.69	-8.45
3	Polşa	35.36	65.98	-30.62
4	Pakistan	34.60	34.77	-0.17
5	Gürcüstan	33.30	56.25	-22.92
6	Ukrayna	31.98	54.72	-22.74
7	Albaniya	24.25	50.08	-25.83
8	Keniya	18.60	42.24	-23.64
9	Nepal	16.82	35.81	-18.99

Kibertəhlükəsizlik indeksi [8] 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".

NCSecMS modeli [9] 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.

Kiberhazırlıq indeksi (*Cyber Readiness Index, CRI****)*** [13] – beş sahədə: milli strategiya, insidentlərin cavablandırılması, e-cinayətlərlə mübarizə, informasiyanın paylaşılması və elmi-praktiki tədqiqatlar üzrə ilkin qiymətləndirmələr əsasında 35 ölkənin özlərinin İKT investisiyalarını və İnterneti qorumaqda yetkinliyini və öhdəliklərini müqayisə edir.

Kibergüc indeksi *(Cyber Power Index, CPI)* [13] – bu indeksin məqsədi G20 ölkələrinin "kiber-hücumlara qarşı durmaq və produktiv və təhlükəsiz iqtisadiyyat üçün zəruri olan rəqəmsal infrastruktur qurmaq" qabiliyyətlərini ölçməkdir. İndeksdə 4 kateqoriyada təşkil edilmiş 39 kəmiyyət və keyfiyyət indikatoru istifadə edilir. Bu kateqoriyalar və onların çəkiləri Cədvəl 3-də göstərilib.

Cədvəl 3. *CPI* kateqoriyaları və onların çəkiləri

CPI kateqoriyaları	**Çəki**
Hüquqi və tənzimləmə bazası	26.3 %
İqtisadi və sosial kontekst	25.0 %
Texnoloji infrastruktur	26.3 %
Sənaye tətbiqləri	22.5 %

"Security and Defence Agenda" tərəfindən aparılmış tədqiqatda 23 ölkənin kibertəhlükəsizlik hazırlığı qiymətləndirilmişdir [13]. Tədqiqatın nəticəsində alınmış ranqlaşdırma baxılmış digər indekslərdən fərqli olaraq subyektiv ekspert qiymətləndirməsindən istifadə edir. O, dövlət, özəl sektor, beynəlxalq təşkilatlar və akademiyadan olan 80-dən çox kiber-təhlükəsizlik eksperti arasında keçirilmiş sorğuya əsaslanır. Hesabatda kiber-hücumlara qarşı dayanıqlığı qiymətləndirmək üçün Robert Lentz tərəfindən işlənmiş ***kibertəhlükəsizlik yetkinlik modeli***ndən istifadə edilir. Bu model kiber-təhlükəsizlik hazırlığını və dayanıqlığını yaxşılaşdırmaq üçün beş-mərhələli yol xəritəsi təqdim edir. Bu mərhələlər kompüter təhlükəsizliyi gigiyenasının baza qaydalarının tətbiqindən başlayır, standartların istifadəsinə, prediktiv kiber hazırlığa və təchizat zəncirində risk menecmentinə keçir. Bu model ölkələrin kibertəhlükəsizlik hazırlığının qiymətləndirilməsi üçün ölçmə aləti kimi də istifadə edilir.

Kibertəhlükəsizliyin ölçülməsi üçün indikatorlar

Kibertəhlükəsizliyin ölçülməsinin bir sıra nəzəri və metodoloji problemləri mövcuddur. Birinci problem kibertəhlükəsizlik indikatorlarının seçilməsi ilə əlaqəlidir: hansı ölçülər relevantdır və neçə ölçü götürülməlidir? Amartya Sen bunu müvafiq "informasiya bazası" problemi adlandırır [14], yəni qiymətləndirmə prosesində hansı informasiya istifadə edilməlidir. Bu seçim çox zaman statistikanın mövcudluğu ilə şərtlənir, lakin onun dərin nəzəri nəticələri vardır və qiymətləndirmənin nəticələrinə böyük təsir göstərir.

Bununla əlaqəli texniki problem seçilmiş hər bir ölçünü adekvat əks etdirən indikatorların seçilməsi ilə bağlıdır.

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

Kibertəhlükəsizliyin 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) [15].

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 tərifl ərinə rast gəlmək mümkündür. Bu məqalədə aşağıdakı tərif əsas götürülür.

Metrika (ing. metrics) – fəaliyyətin 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 [2].

İnformasiya təhlükəsizliyi metrikaları üzrə bir neçə milli və beynəlxalq standart işlənmişdir. Onlardan NIST SP 800-55 – informasiya sistemləri üçün təhlükəsizlik metrikaları üzrə qaydaları [16], NIST SP 800-80 – informasiya təhlükəsizliyi üçün fəaliyyət məhsuldarlığı metrikalarının işlənməsi üçün qaydaları, ISO/IEC 21827 – sistemlərin təhlükəsizlik mühəndisliyi üçün potensialın yetkinlik modelini və ISO/IEC 27004 standartını qeyd etmək olar. ISO/IEC 27004 standartında informasiya təhlükəsizliyini idarəetmə sisteminin effektivliyini qiymətləndirmək üçün müvafiq metrikaların yaradılması və istifadəsi üzrə tövsiyələr verilir [17].

Məlumdur ki, başqa fəaliyyət sahələrində fəaliyyətin məhsuldarlığını və qarşıya qoyulmuş məqsədlərə nail olunmasını ölçmək üçün bir sıra indikatorlar mövcuddur [2], 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.

Ümumiyyətlə, metrikaların işlənməsi üçün ən effektiv yol biznes məqsədinin 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.

Kibertəhlükəsizlik 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, kibertəhlükəsizlik məqsədləri üçün metrikaları tapmaq çətinləşir və onlar informasiya təhlükəsizliyinin idarə edilməsi üçün o qədər də faydalı olmurlar.

Adətən, yaxşı metrikaların yaradılması üçün SMART (Specific, Measurable, Achievable, Relevant, Timely) metodikası istifadə edilir [18]. Yaxşı metrikaların yaradılması üçün digər yanaşmalar da mövcuddur [19, 2]: PRAGMATIC, PURE, CLEAR.

Kibertəhlükəsizliyin 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.

İkinci problem toplanmış informasiyanın istifadəsi ilə bağlıdır. Sonrakı bölmələr bu problemə həsr olunacaq. Müvafiq ölçülər və indikatorlar seçildikdən (və normallaşdırıldıqdan) sonra dəyərləndirmə aparmaq üçün onları zaman və ya fəzada müqayisə etmək lazım gəlir. Bir neçə indikatorla müqayisə aparmaq üçün ən azı iki alternativ üsul var: 1) "inkişaf profilləri"ndən istifadə etmək; 2) müxtəlif indikatorları kompozit indeksdə birləşdirmək.

Kompozit indekslərin qurulması problemləri

Kompozit indekslərin qurulmasında bir-biri ilə sıx əlaqəli olan addımların "ideal ardıcıllığı" [20]-də geniş izah edilir. Kompozit indekslərin qurulmasında əsas problem informasiyanın necə aqreqasiya edilməsidir. Aqreqasiya probleminin qarşılıqlı əlaqəli iki aspekti var: 1) aqreqasiya zamanı komponentlərə çəkilərin təyin edilməsi və 2) aqreqasiya funksiyasının seçilməsi.

Çəkilərin təyin edilməsi metodları çoxdur: bərabər çəkilər, əsas komponentlər metodu/faktor analizi, iyerarxiyaların analizi metodu, birgə analiz (ing. conjoint analysis), "büdcənin paylanması" və s. İdealda, çəki hər bir indikatorun kompozit (inteqral) indeksə töhfəsini əks etdirməlidir. Bir çox kompozit indeks bərabər çəkilərə əsaslanır. Bu bütün indikatorların eyni dəyərə malik olması halına uyğun gələ bilər. Alternativ kimi, bu səbəb nəticə əlaqələri haqqında yetərli biliyin olmaması və ya digər həllər haqqında konsensusun olmamasından da qaynaqlana bilər. Həmçinin, yüksək dərəcədə korrelyasiya edən dəyişənlərin kombinasiyası nəticəsində indeksə ikiqat hesablama elementi də daxil edilə bilər. Çəki verilənlərin keyfiyyətini də əks etdirə bilər, statistik etibarlı verilənlərə daha yüksək çəki verilə bilər.

İlk baxışda çəkilərin faktor analizi (əsas komponentlərin analizi) təyin edilməsi metodu daha obyektiv görünür, çünki çəkilər ekspertlər tərəfindən müəyyən edilmir, statistika metodu ilə verilənlərdən alınır. Lakin bu yanaşmanın bir neçə ciddi nöqsanı vardır. Birincisi, çəkilər verilənlərdən alındıqda onlar məkan və zamana görə sabit olmurlar, bu isə müqayisəni olduqca çətinləşdirir. İkincisi, faktor analizi çəkiləri ilkin verilənlərin dispersiyası (variasiyası) və kovariasiyası əsasında təyin edir. Bu kriteriya müxtəlif dəyişənlərin nisbi sosial-iqtisadi vacibliyini həmişə əks etdirmir. Buna görə də, statistik yanaşma ilə çəkilər obyektiv görünsələr də, onların yaxşı nəzəri bazası yoxdur.

İndikatorlar normallaşdırıldıqdan sonra onları birləşdirmək üçün bir neçə aqreqasiya strategiyası vardır [20]: xətti aqreqasiya, həndəsi aqreqasiya və çoxkriteriyalı aqreqasiya.

Xətti aqreqasiya metodunda alternativlər indikatorların hər birinə görə qiymətləndirilir və indikatorların çəkilərinə vurulur. Konkret alternativ üçün bu hasillərin bütün indikatorlar üzrə cəmi həmin alternativin indeksini (ranqını) verir:

$$R_i = \sum_{j=1}^{n} w_i a_{ij} \qquad (1)$$

Burada R_i – i-ci alternativin indeksi, n – indikatorların sayı, a_{ij} – i-ci alternativin j-cu indikatora görə qiyməti (dəyəri), w_j – j-cu indikatorun çəkisidir, $0 \le w_i \le 1, \sum_{i=1}^{m} w_i = 1$.

Xətti aqreqasiya çox sadə olduğundan və tətbiqinin və interpretasiyasının asanlığı səbəbindən geniş istifadə edilir. Xətti aqreqasiya metodunda fərz olunur ki, konkret indikatorun yekun indeksə payı digər indikatorların qiymətindən asılı deyil. Xətti aqreqasiya fərdi indikatorlar eyni ölçü vahidinə malik olduqda və miqyas effekti sayəsində sonrakı çoxqiymətlilik aradan qaldırıldıqda faydalıdır.

Həndəsi aqreqasiya metodunda alternativin hər bir indikator üzrə qiyməti həmin indikatorun çəkisinə qüvvətə yüksəldilir və bütün indikatorlar üzrə hasil hesablanır. i-ci alternativin R_i indeksi belə hesablanır:

$$R_i = \prod_{j=1}^{n} (a_{ij})^{w_j} \quad (2)$$

burada n – indikatorların sayı, a_{ij} – i-ci alternativin j-cu indikatora görə qiyməti, w_j – j-cu indikatorun çəkisidir, $0 \leq w_i \leq 1, \sum_{i=1}^{m} w_i = 1$.

Qeyd edək ki, yuxarıdakı funksiyadan fərqli olan digər həndəsi aqreqasiya operatorları da vardır [21]. Həndəsi aqreqasiya xətti aqreqasiya ilə müqayisədə daha çox dəyişkənlik yarada bilər. İndikator qiymətləri vurulduğundan, bir indikatorda kiçik ölçmə səhvi indeksdə əhəmiyyətli dəyişiklik yarada bilər. Bu cəhət onu indikator qiymətləri böyük variasiya mümkün olan subyektiv qiymətləndirmə nəticəsində alınması halı üçün daha az münasib edir.

Kompozit indekslərdə son dövrlər fundamental məsələyə – indeksin komponentləri arasında kompensasiya edilməmə məsələsinə xüsusi fikir verilir (bir ölçüdəki defisit digər ölçüdəki izafiliklə kompensasiya edilir). Kompensasiya etməyən yanaşma getdikcə daha çox tətbiq edilir. Məsələn, 2010-cu ildə BMT İnkişaf Proqramı tərəfindən hesablanan Human Development Index-də həndəsi orta istifadə edilir [22].

Kompensasiya edilməmə və verilənlərin zamana görə müqayisə edilə bilməsi kompozit indekslərin qurulmasında əsas məsələdir [23]. Kompensasiya edilməyən kompozit indekslər qeyri-additiv yanaşmalarla əldə edilə bilər. Müqayisə edilmə məsələsi isə əsasən normallaşdırma metodundan asılıdır.

Xətti aqreqasiyada kompensasiya edilmə sabitdir. Həndəsi aqreqasiyada isə kompozit indeksdə kiçik qiymətləri olan indikator olduqda kompensasiya edilmə aşağı olur. Əgər kompensasiya yolverilən dirsə və həndəsi aqreqasiya istifadə edilirsə, onda bir indikator üzrə kiçik qiymətləri olan ölkə vəziyyəti düzəltmək üçün digər indikatorlar üzrə daha böyük qiymətlər almağa çalışmalıdır.

Müxtəlif məqsədlər eyni hüquqa və vacibliyə malikdirsə, onda kompensasiya edilməmə tələbi zəruri ola bilər. Bu kompozit indeksdə müxtəlif ölçülərin cəlb edildiyi hala uyğundur, məsələn, ekologiya indeksində fiziki, sosial və iqtisadi verilənlər aqreqasiya edilə bilər. Əgər bir indikatordakı artımın digər indikatordakı azalmanı kompensasiya edə bilmədiyi qəbul edilirsə, onda nə xətti, nə də həndəsi aqreqasiya yararlı olmur. Bu halda aqreqasiya məsələsini multi-kriteriyalı yanaşma həll edə bilər. Bu yanaşmada iki və ya daha çox məqsəd arasında kompromisin tapılması məsələsi formallaşdırılır. Məsələn, [24]-də aqreqasiya məsələsi çoxkriteriyalı optimallaşdırma məsələsi kimi həll edilir.

İndikator çəkilərinin hesablanması üçün entropiya metodu

İndikatorların çəkisini müəyyən etmək üçün bir çox metod təklif edilmişdir. Lakin heç bir metod daha dəqiq nəticəyə zəmanət verə bilmir. Qərar verən eyni şəxs müxtəlif çəkilər ala bilər. Hansı çəkinin doğru olmasını müəyyənləşdirmək üçün isə kriteriya mövcud deyil [25].

Bu tədqiqatda çəkiləri hesablamaq üçün entropiyadan istifadə edilir. İndikatorlara çəki təyin etmək üçün entropiya metodu aşağıdakı faktlara görə xüsusilə faydalıdır [26, 27]: (1) bu metod hər hansı qərar qəbul edənin indikatoru ranqlaşdırmasını tələb etmir; (2) hər bir indikatorun nisbi çəkisini asan hesablamalarla əldə etmək olar. Başqa sözlə, qərar qəbul edənlər çəkilərin hesablanması üçün ölkələrin real göstəricilərindən istifadə edə bilərlər. Buna görə entropiya metodunun obyektiv çəki üsulu olduğunu iddia etmək olar. Beləliklə, çəkilərin hesablanmasına xas subyektivlik aradan qaldırılır.

Entropiya konsepsiyasına görə, əgər bir indikator üçün alternativlərin qiymətləri eyni olarsa, onda bu indikatoru irəlidə nəzərə almamaq olar. Oxşar olaraq, əgər bir indikator üçün bütün alternativlərin qiymətləri yaxın olarsa, bu indikatora təyin olunmuş çəki daha kiçik ola bilər. Digər tərəfdən, müəyyən alternativlər üzrə indikatorun qiymətləri arasında fərqlər böyük olduqda indikator daha vacib hesab edilir.

Tutaq ki, *m* alternativin *n* indikatora görə qiymətləndirilməsi matrisi *D* verilib:

$$D = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_i \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccccc} X_1 & X_2 & \cdots & X_j & \cdots & X_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1j} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2j} & \cdots & x_{2n} \\ \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ x_{i1} & x_{i2} & \cdots & x_{ij} & \cdots & x_{in} \\ \vdots & \vdots & \ldots & \vdots & \cdots & \vdots \\ x_{m1} & x_{m2} & \ldots & x_{mj} & \cdots & x_{mn} \end{bmatrix} \end{array} \quad (3)$$

burada A_i – baxılan *i*-ci alternativ (ölkə); x_{ij} – *i*-ci alternativin *j*-cu indikatora görə qiymətidir.

İndikatorların çəkilərini müəyyən etmək üçün entropiya alqoritmi aşağıdakı kimidir:

Addım 1. Qiymətləndirmə matrisinin normallaşdırılması

Normallaşdırma nəticəsində $R = (r_{ij})_{mxn}$ matrisi alınır, burada r_{ij} – *j*-cu ölkənin *i*-ci indikator üzrə qiymətləndirməsidir və $r_{ij} \in [0,1]$. Baxılan məsələdə indikatorun qiymətinin böyük olması yaxşı hesab edildiyindən, aşağıdakı normallaşdırma düsturundan istifadə edilir:

$$r_{ij} = \frac{x_{ij} - \min_i\{x_{ij}\}}{\max_i\{x_{ij}\} - \min_i\{x_{ij}\}} \quad (4)$$

Addım 2. Entropiyanın hesablanması

n obyektin *m* indikatora görə qiymətləndirilməsi məsələsində *i*-ci indikatorun entropiyası aşağıdakı kimi müəyyən edilir:

$$H_j = -k \sum_{i=1}^{n} f_{ij} \ln f_{ij}, \quad j = 1,2, \ldots, m, \quad (5)$$

burada $f_{ij} = r_{ij} / \sum_{i=1}^{n} r_{ij}$, $k = 1/\ln n$. Fərz olunur ki, $f_{ij} = 0$ olduqda, $f_{ij} \ln f_{ij} = 0$.

Addım 3. Entropiya çəkisinin müəyyən edilməsi

j-cu indikatorun entropiya çəkisini belə təyin etmək olar:

$$w_j = \frac{1 - H_j}{m - \sum_{j=1}^{m} H_j} \quad (6)$$

burada $0 \le w_j \le 1, \sum_{j=1}^{m} w_j = 1$.

Cədvəl 4-də (3)-(6) düsturları əsasında MDB ölkələri üçün 2017-ci il qlobal kibertəhlükəsizlik indeksi verilənləri [28] ilə hesablanmış indikatorların entropiya və çəki qiymətləri verilmişdir. Göründüyü kimi, entropiyaya əsaslanan yanaşmada "Texniki" və "Potensial quruculuğu" indikatorlarına daha yüksək çəkilər verilir.

Cədvəl 4. İndikatorların entropiyaları və çəkiləri

İndikator	**Entropiya**	**Entropiya əsasında çəki**	**Çəki (GSI metodologiyası) [4]**
Hüquqi	0.929	0.108	0.200
Texniki	0.821	0.273	0.200
Təşkilati	0.903	0.147	0.200
Potensial quruculuğu	0.805	0.296	0.200
Əməkdaşlıq	0.884	0.176	0.200

Statik və dinamik kibertəhlükəsizlik indeksləri

Aşağıda təklif edilən statik və dinamik kibertəhlükəsizlik indekslərinin işlənməsi zamanı [29]-da irəli sürülən yanaşma əsas götürülmüşdür.

Tutaq ki, x^t_{ij} – j-cu indikatorun i-ci ölkə üçün t zamanında qiymətidir ($j = 1, \ldots, m$; $i = 1,\ldots n$; $t = t_0,t_1$). Statik kibertəhlükəsizlik indeksini (Static Cybersecurity Index, SCI) aşağıdakı kimi təyin etmək olar:

$$SCI_i^t = \prod_{j=1}^{m} \left(\frac{x_{ij}^t}{x_{rj}^t} c \right)^{\frac{1}{m}} \quad (7)$$

burada x^t_{rj} – j-cu indikatorun t zamanında istinad və ya baza qiymətidir, məsələn, indikatorun dünya üzrə orta qiymətidir, c – miqyaslama əmsalıdır, adətən $c = 100$ götürülür. Deməli, SCI-nin c-dən böyük (kiçik) qiymətləri ortadan yuxarı (aşağı) indikatorlara malik ölkələri göstərir.

Cədvəl 5-də (7) düsturu ilə MDB ölkələri üçün 2017-ci il qlobal kibertəhlükəsizlik indeksi verilənləri [28] əsasında hesablanmış statik kibertəhlükəsizlik indeksi qiymətləri verilmişdir. Hesablamalarda indikatorların baza qiymətləri kimi MDB ölkələri üçün həmin indikatorların orta qiymətləri götürülmüşdür, həmçinin $c = 100$.

Cədvəl 5. Bəzi ölkələrin statik kibertəhlükəsizlik indeksləri

Ölkə	**GCI**	**SCI**
Azərbaycan	0.559	123.83
Belarus	0.592	132.95
Ermənistan	0.196	4.06
Gürcüstan	0.819	192.50
Qazaxıstan	0.352	69.86
Qırğızıstan	0.270	46.61
Moldova	0.418	88.32
Özbəkistan	0.277	57.72
Rusiya	0.788	184.98
Tacikistan	0.292	16.88
Türkmənistan	0.133	4.77
Ukrayna	0.501	101.20

Hər bir ölkə üçün t_0 zamanından t_1-ə verilənləri analiz etmək üçün aşağıdakı düsturla verilən "dinamik" kibertəhlükəsizlik indeksi (Dynamic Cybersecurity Index, DCI) qurmaq olar:

$$DCI_i^t = \prod_{j=1}^{m} \left(\frac{x_{ij}^{t_1}}{x_{ij}^{t_0}} c \right)^{\frac{1}{m}} \quad (8)$$

İndeks qiymətlərinin tranzitivlik xassəsinə görə SCI və DCI aşağıdakı şəkildə əlaqəlidir:

$$DCI_i^{t_1/t_0} = \left(SCI_i^{t_1} / SCI_i^{t_0} \right) DCI_r^{t_1/t_0}. \quad (9)$$

Cədvəl 6-da (8) düsturu ilə MDB ölkələri üzrə $t_1 = 2017$ və $t_0 = 2015$-ci illər üçün qlobal kibertəhlükəsizlik indeksi verilənləri əsasında hesablanmış dinamik kibertəhlükəsizlik indeksləri verilmişdir.

Çəkili qüvvətə əsaslanan SCI və DCI indeksləri ən böyük dəyişkənlik göstərən komponentlərə daha böyük çəki verir. DCI həm də mütləq zamana görə müqayisə etməyə imkan verir. Qeyd edək ki, DCI aqreqasiya funksiyası istisna olmaqla, Kanada rifah indeksinə oxşardır [30].

Cədvəl 6. Bəzi ölkələrin dinamik kibertəhlükəsizlik indeksləri

Ölkə	DCI
Azərbaycan	200.32
Belarus	13.96
Ermənistan	5.05
Gürcüstan	174.39
Qazaxıstan	13.96
Qırğızıstan	6.29
Moldova	143.32
Özbəkistan	12.16
Rusiya	184.71
Tacikistan	6.29
Türkmənistan	2.50
Ukrayna	121.86

Nəticə

Kibertəhlükəsizlik indeksi ölkələrin kibertəhlükəsizlik təşəbbüsləri baxımından vəziyyətlərini müqayisə etmək, effektiv kibertəhlükəsizlik siyasətləri və strategiyaları işləmək üçün zəruri alətlərdən biridir. Bu məqalədə mövcud kibertəhlükəsizlik indeksləri analiz edilmiş, kompozit kibertəhlükəsizlik indeksində indikatorların entropiya çəkilərinin hesablanması alqoritmi təklif edilmiş, statik və dinamik kibertəhlükəsizlik indeksləri daxil edilmişdir. Statik indeks kompensasiya edilməmə xassəsinə malikdir, dinamik indeks isə indikatorları zamana görə müqayisə etməyə imkan verir. Bu xassələr kompozit indekslər üçün olduqca vacibdir.

Gələcək tədqiqatlarda milli kibertəhlükəsizlik üçün digər indikatorları da əhatə edən yeni indeksin işlənməsinə ehtiyac vardır. Bu indeks kibertəhlükəsizliyə milli hazırlıq səviyyəsi ilə yanaşı, kiber-təhlükəsizliyin cari səviyyəsini də əks etdirməlidir, o cümlədən, ölkənin informasiya infrastrukturunun inkişaf səviyyəsini və kiberhücumlar üçün cəlbediciliyini də nəzərə almalıdır.

Bu işdə indikatorların çəkilərinin hesablanmasında istifadə edilmiş entropiya yanaşmasını inkişaf etdirərək sistemin vəziyyətinin indikatoru kimi bütövlükdə milli kibertəhlükəsizlik sisteminin vəziyyətini xarakterizə etmək üçün istifadə etmək olar. Başqa sözlə, gələcək tədqiqatlarda entropiya yanaşması əsasında milli kibertəhlükəsizlik indeksinin işlənilməsi də planlaşdırılır.

Ədəbiyyat

1. Štitilis D., Pakutinskas P., Malinauskaitė I. EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis // Security Journal, vol. 30, no. 4, pp. 1151-1168.
2. İmamverdiyev Y., Elektron dövlətin informasiya təhlükəsizliyi üçün diffuziya indeksi modeli / "Elektron dövlət quruculuğu problemləri" I Respublika elmi-praktiki konfransı, 2014, s.75-78.
3. Pironti J. P. Developing metrics for effective information security governance // Information Systems Control Journal, 2007, vol.2, pp. 33-38.
4. Global Cybersecurity Index 2017, ITU. Geneva, 2017. 78 p, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.
5. Global Cybersecurity Index & Cyberwellness Profiles, Geneva, 2015. 528 p, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
6. Hwang S.-W. Development of the National Cyber Safety Index. ITU Regional Cybersecurity Forum (Brisbane, AU), 2008. http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/weon-national-information-security-index-brisbane-july-08.pdf
7. National Cyber Security Index (NCSI) Methodology. e-Governance Academy, 2015. http://ncsi.ega.ee/methodology-description/
8. Index of Cyber Security http://www.cybersecurityindex.org

9. El Kettani M. D., Debbagh T. NCSecMM: A National Cyber Security Maturity Model for an Interoperable National Cyber Security Framework / Proc. of the 9th European Conference on e-Government, 2009, pp. 236-247.
10. Yunis M. M., Koong K. S. A conceptual model for the development of a national cybersecurity index: An integrated framework / Proc. of the 21st Americas Conference on Information Systems (AMCIS), 2015, pp. 1-13.
11. Measuring the Information Society Report 2017, Geneva, Switzerland: International Telecommunication Union (ITU), 2017, 31 p. http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf
12. Global Information Technology Report 2016, Geneva, Switzerland: World Economic Forum, 2016, 307 p, http://www.reports.weforum.org/global-information-technology-report-2016/
13. Gehem M., Usanov A., Frinking E., Rademaker M. Assessing Cyber Security: a Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks. The Hague Centre for Strategic Studies (HCSS), 2015, 102 p.
14. Sen A. Development as freedom. Oxford: Oxford University Press, 1999, 366 p.
15. Jansen W. NISTIR 7564: Directions in security metrics research, 2009, 26 p.
16. Chew E., Swanson M., Stine K. M., Bartol N., Brown A. Robinson W., SP 800-55 Rev. Performance measurement guide for information security. National Institute of Standards & Technology, 2008, 80 p.
17. ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Measurement, 2009, 58 p.
18. Doran G. T., There's a S.M.A.R.T. way to write management's goals and objectives // Management Review (AMA FORUM), 1981 vol. 70, no. 11, pp. 35–36.
19. Brotby W. K., Hinson G. PRAGMATIC security metrics: Applying metametrics to information security, Auerbach Publications 1st Edition, 2013, 512 p.
20. OECD: Handbook on constructing composite indicators. Methodology and user guide. Paris: OECD Publications, 2008, 162 p.
21. Calvo T., Kolesárová A., Komorníková M., Mesiar R. Aggregation operators: properties, classes and construction methods // Aggregation operators, 2002, pp. 3-104.
22. De Muro P., Mazziotta M., Pareto A. Composite indices of development and poverty: An application to MDGs // Social indicators research, 2011, vol. 104, no. 1, pp. 1-18.
23. Munda G., Nardo M. Noncompensatory/nonlinear composite indicators for ranking countries: a defensible setting // Applied Economics, 2009, vol. 41, no. 12, pp. 1513-1523.
24. Zhou P., Ang B.W., Zhou D.Q. Weighting and aggregation in composite indicator construction: a multiplicative optimization approach // Social Indicators Research, 2010, vol. 96, no. 1, pp. 169-181.
25. Chang Y.H., Yeh C.H. Evaluating airline competitiveness using multi-attribute decision-making // Omega, 2000, vol. 29, pp. 405–415.
26. Zou Z., Yun Y., Sun J. Entropy method for determination of weight of evaluating indicators in fuzzy synthetic evaluation for water quality assessment // Journal of Environmental Sciences, 2006, vol. 18, no. 5, pp. 1020–1023.
27. Sopadang A., Cho B.R., Leonard M. Development of the hybrid weight assessment system for multiple quality attributes // Quality Engineering, 2002, vol. 15, no. 1, pp. 75–89.
28. GCI 2017 Regional Report: CIS Region Report, 2017, 36 p. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIS_GCIv2_report.pdf
29. Mazziotta M., Pareto A. A well-being index based on the weighted product method // Topics in Theoretical and Applied Statistics, 2016, pp. 253-259.
30. Muhajarine N., Labonte R., Winquist B. D. The Canadian Index of wellbeing: Key findings from the healthy populations domain // Canadian Journal of Public Health, vol. 103, no. 5, pp. 342-347.

УДК 004.056
Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@lan.ab.az
Энтропийные веса и динамический индекс для национальной кибербезопасности
В настоящее время кибербезопасность стала одним из важнейших компонентов национальной безопасности, и для ее эффективного обеспечения необходимо оценить уровень национальной кибербезопасности. Для решения этой задачи некоторыми организациями был предложен ряд национальных индексов кибербезопасности. Однако исследования и практические работы по разработке национальных индексов кибербезопасности находятся на ранней стадии, их методологическое обоснование является неудовлетворительным и неполным. В этом исследовании существующие индексы национальной кибербезопасности анализируются сравнительно, указываются их преимущества и недостатки, выдвигаются предложения по их улучшению. Для весов показателей, включенных в композитные национальные индексы кибербезопасности, предложен метод оценки на основе энтропии. Также предложены статические и динамические индексы кибербезопасности и проведена экспериментальная проверка предлагаемых подходов на основе реальных данных.
Ключевые слова: *кибербезопасность, индикатор, энтропия, композитный индекс, динамический индекс, статический индекс кибербезопасности, динамический индекс кибербезопасности, национальный индекс кибербезопасности.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az
Entropy weights and dynamic index for national cybersecurity
At present, cybersecurity has become one of the most important components of national security, and for its effective provision, it is necessary to assess the level of national cybersecurity. To solve this problem, some organizations proposed a number of national cybersecurity indices. However, research and practical work on the development of national cybersecurity indices are at an early stage, their methodological justification is unsatisfactory and incomplete. In this study, existing indices of national cybersecurity are comparatively analyzed, their advantages and disadvantages are indicated, and proposals are put forward for their improvement. For weights of indicators included in composite national cybersecurity indices, a method based on entropy is proposed. Static and dynamic cybersecurity indices are also proposed and an experimental verification of the proposed approaches is made on the basis of real data.
Keywords: *cybersecurity, indicator, entropy, composite index, dynamic index, static cybersecurity index, dynamic cybersecurity index, national cybersecurity index.*