UOT 004.056

***İmamverdiyev Y.N.*[1]*, Derakshandeh S.A.*[2]**
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*yadigar@lan.ab.az*; [2]*smdk364@yahoo.com*

İNFORMASİYA TƏHLÜKƏSİZLİYİ TƏHDİDLƏRİNİN RANQLAŞDIRILMASININ BİR METODU HAQQINDA

İnformasiya təhlükəsizliyi təhdidlərinin ranqlaşdırılması üçün qeyri-səlis TOPSIS metodu təklif edilmişdir. Təhdidlərin subyektiv kriteriyalar üzrə qiymətləri və kriteriyaların çəkiləri qeyri-səlis üçbucaqlı ədədlərlə ifadə edilmiş linqvistik dəyişənlərlə qiymətləndirilir. Obyektiv kriteriyalar üzrə alınmış qiymətlər ölçüsüz qiymətlərə çevrilir ki, subyektiv kriteriyalar üzrə qiymətlərlə uyuşanlıq təmin edilsin. Təhdidlərin ranqlaşdırılması üçün yaxınlıq əmsalları ideal pozitiv və ideal neqativ təhdidlərdən məsafə kimi müəyyən edilir. Təklif edilmiş metodun hesablama prosesi ədədi nümunə ilə nümayiş etdirilir.

Açar sözlər: *informasiya təhlükəsizliyi, informasiya təhlükəsizliyi riski, təhdid, boşluq, qeyri-səlis TOPSIS metodu, təhdidlərin ranqlaşdırılması.*

Giriş

İnformasiya və kommunikasiya texnologiyalarının (İKT) geniş istifadə edildiyi müasir şəraitdə informasiya təhlükəsizliyi (İnT) risklərinin idarə edilməsi aktual məsələyə çevrilir, çünki İKT hətta təşkilatın varlığını sual altına alan təhdidlərin mənbəyi ola bilər. İnT risklərinin idarə edilməsi əsasında təşkilatın əsas biznes-proseslərinə mənfi təsir edən əsas kritik faktorları qiymətləndirmək və onların minimallaşdırılması üçün əsaslandırılmış və səmərəli həllər təklif etmək olar [1]. Hazırda İnT risklərinin idarə edilməsi üçün bir sıra beynəlxalq, milli və sahə standartları mövcuddur [2]: ISO/IEC 27005:2007, NIST 800-30, OCTAVE, CRAMM və s.

İnT risklərinin idarə edilməsi belə bir müddəadan çıxış edir ki, "tam mükəmməl" İnT sisteminin qurulması cəhdi iqtisadi və texnoloji cəhətdən gerçəkləşdirilə bilməz, burada əsas prinsip informasiya təhlükəsizliyinin yolverilən müəyyən səviyyəsinin qəbul edilməsidir. Yetərli miqdarda vasitələr və zaman olduqda istənilən informasiya təhlükəsizliyi sistemini “sındırmaq” olar. Yüksək effektivliyə malik informasiya təhlükəsizliyi sisteminin qurulması böyük həcmdə xərclər tələb edir, buna görə də elə kafi səviyyə seçmək lazımdır ki, mümkün ziyanın ehtimalı və həcmi ilə informasiya təhlükəsizliyi sisteminə çəkilən xərc optimal şəkildə uyğunlaşdırılsın. Belə yanaşmanı gerçəkləşdirən zaman təşkilata təsiri baxımından təhdidlərin bir sıra kriteriyalara görə ranqlaşdırılmasından istifadə edilməsi zəruridir.

Bu işdə TOPSIS (Technique for Order Preferences by Similarity to Ideal Solution, ideal həll ilə oxşarlığa görə nizamlı üstünlük) metodunun [3] qeyri-səlis variantı əsasında təhdidlərin ranqlaşdırılması metodu təklif edilir. TOPSIS metodu çox sayda kriteriyalar nəzərə alınmaqla alternativlər üçün inteqral indeks hesablamağa imkan verir və bununla qərar qəbul edən şəxsin iştirakı ilə variantların seçilməsi proseduru üçün alternativlərin ranqlaşdırılmasını təmin edir. Qeyri-səlis TOPSIS metodu bir sıra tətbiqi məsələlərdə faktorların ranqlaşdırılması [4], alternativlərin seçilməsi [5 – 7], qrup qərarlarının qəbulu [8] üçün istifadə edilmişdir. Qeyd edək ki, alternativlərin çox kriteriyalı ranqlaşdırılması üçün daha çox istifadə edilən AHP (Analytical Hierarchy Prosess – iyerarxiyaların analizi) metodunun [9] bir sıra nöqsanları mövcuddur. Bura hesablama yükünün çoxluğu, ekspertlərin sayı çox olduqda ekspert qiymətlərinin ziddiyyətliliyi və s. aid edilə bilər. [10]-da iyerarxiyaların analizi metodunun əsas müddəası nəzərdən keçirilmiş və sadə misalla nümayiş etdirilmişdir ki, bu müddəa əsasında kriteriyaların üstünlük dərəcələrinin hesablanması səhv nəticələr verə bilər.

Təhdidlərin ranqlaşdırılmasına yanaşmalar

İnT risklərinin qiymətləndirilməsi metodları özlüyündə təhdidlərin ranqlaşdırılması metodları ilə səbəb və nəticələrin analizi metodlarının müxtəlif kombinasiyasından ibarətdirlər və çox vaxt keyfiyyət xarakterlidirlər. Təhdidlərin ranqlaşdırılması üçün ekspert qiymətləndirməsi metodları (məsələn, Delfi, cüt-cüt müqayisə, risk qruplarının təsnifatı) daha geniş istifadə edilir. Bu metodlar ekspert qiymətləndirməsinin təşkili ilə yanaşı, təhdidlərin qiymətləndirilən faktorlar çoxluğu ilə də fərqlənirlər. Məsələn, [11]-də təhdidlərin qiymətləndirilməsi "təhdid mənbəyi → boşluq → təhdid → nəticə (hücum)" məntiqi ardıcıllığının qarşılıqlı əlaqələri analiz edilməklə aparılır. Təhdid mənbəyinin təhlükə dərəcəsinə görə ranqlaşdırılması üçün üç dolayı göstərici seçilir və 5-ballıq şkala ilə qiymətləndirilir: mənbənin meydana çıxması imkanı; mənbənin hazırlıq səviyyəsi və hücumun labüdlüyü. İnT boşluqlarının təhlükə dərəcəsinə görə ranqlaşdırılması üçün də üç göstərici daxil edilir və onların ölçülməsi üçün də subyektiv şkala daxil edilir.

Proqram təminatına təhdidlərin modelləşdirilməsi (klassifikasiyası) üçün Microsoft şirkətinin STRIDE metodikasında [12] təhdidlərin qeyd olunmuş siniflərinə baxılır: Spoofing (verilənlərin əvəzlənməsi), Tampering (müdaxilə), Repudiation (inkaretmə), Information Disclosure (informasiyanın açılması), Denial of Service (xidmətdən imtina) və Elevation of Privilege (giriş hüququnun artırılması). STRIDE yanaşmasına görə sistem müvafiq komponentlərə bölünür, hər bir komponentin təhdidlərə həssaslığı qiymətləndirilir və təhdidlərin təsiri aradan qaldırılır. Bu prosesi risklərin yolverilən səviyyəsi əldə edilənə qədər təkrarlamaq olar. Proqram təminatına təhdidlərin qiymətləndirilməsi üçün Microsoft şirkəti əməkdaşlarının DREAD metodikasını təklif etmişlər [12]. DREAD aşağıdakı kriteriyaların ingilis dilindəki adlarının baş hərflərinə görə adlanır:

Damage potential (Potensial ziyan) – uğurlu hücum nəticəsində vurulan ziyan;

Reproducibility (Gerçəkləşdirilmə) – təhlükənin həyata keçirilməsi imkanı;

Exploitability (İstismara yararlılıq) – hücum üçün tələb edilən səylər və kvalifikasiya;

Affected users (Təsirlənən istifadəçilər) – uğurlu hücumla işi pozulan istifadəçilərin nisbi sayı;

Discoverability (aşkarlanma ehtimalı) – təhdidi aşkarlamaq nə qədər asandır?

Hər bir kriteriya 10-ballıq şkala ilə qiymətləndirilir. Yekun DREAD-qiymət kriteriyalar üzrə qiymətlərin ədədi ortası kimi hesablanır, yəni risk (təhdidin ranqı) 1 ilə 10 arasında olur.

ABŞ Milli Standartlar və Texnologiyalar İnstitutunun təklif etdiyi yanaşmada [13] çəkili xalvermə metodu istifadə edilir – təhdidlərin aktivlərə təsiri üçün üç sinif müəyyən edilir (Low, Medium, High) və hər bir təsir sinfi üçün çəkilər təyin edilir: Low sinfi üçün 10, Medium sinfi üçün 50 və High sinfi üçün 100.

OWASP (Open Web Application Security Project, veb tətbiqi proqramlarının təhlükəsizliyi üzrə açıq layihə) təşkilatının risklərin reytinqi metodologiyasında [14] risk üç komponent – təhdid, boşluq və təsir əsasında qiymətləndirilir, komponentlərin qiymətləndirilməsi üçün kriteriyalar sistemi təklif edilir. Təhdid agentinin kriteriyaları: kvalifikasiya, motiv, fürsət və say; boşluq faktorunun kriteriyaları: aşkarlanmanın asanlığı, istismarın asanlığı, məlumluq və müdaxilənin aşkarlanması kimi müəyyən edilib. Təsirlər çoxluğu texniki və biznes təsirlərinə bölünüb. Texniki təsirin kriteriyaları: konfidensiallığın itirilməsi, tamlığın itirilməsi, əlyetənliyin itirilməsi, hesabatlılığın itirilməsi, biznes təsirin kriteriyaları: maliyyə itkiləri, nüfuzun itirilməsi, normativ sənədlərlə uyğunsuzluq və fərdi məlumatlarla bağlı pozuntulardır. Kriteriyalar üzrə qiymətləndirmə 9-ballıq şkala üzrə aparılır. Hər komponent üçün kriteriyalar üzrə qiymətlərin orta qiyməti hesablanır.

Göstərilən yanaşmaların əsas nöqsanlarına onların qiymətləndirmə aparan şəxslərin informasiya texnologiyaları sahəsində peşəkarlığına yüksək tələblər irəli sürməsini, universal

olmamalarını, nəticələrin interpretasiya edilməsinin çətinliyini, bu yanaşmalar əsasında müxtəlif variantların müqayisəsinin qeyri-mümkünlüyünü aid etmək olar.

Təhdidlərin qiymətləndirilməsi kriteriyalarının seçilməsi

Əvvəlki bölmədə qeyd edildiyi kimi təhdidlərin qiymətləndirilməsi üçün müxtəlif kriteriyalar təklif edilmişdir.

Bu işdə təhdidlərin qiymətləndirilməsi üçün risklərin idarə edilməsinin ümumi modelinə [15] uyğun olaraq "Təhdidlər→İnT mexanizmləri→İT-servislər→Biznes proseslər" zəncirində qarşılıqlı əlaqələr nəzərə alınmaqla aşağıdakı kriteriyalar sistemi təklif edilir. Bu işdə təhdidi xarakterizə edən kriteriya kimi təhdidin gerçəkləşməsi ehtimalı seçilir və fərz edək ki, təhdidlərin gerçəkləşmə ehtimalı təhdid mənbəyinin motivasiyası və imkanlarından (intellektual, texniki) və istismar edilən boşluğun təbiətindən asılıdır və aşağıdakı subyektiv şkala ilə qiymətləndirilir:

Aşağı (L) – Təhdid mənbəyinin motivasiyası və ya potensialı zəifdir və ya boşluğu istismar etmək çətindir;

Orta (M) – Təhdid mənbəyinin motivasiyası və potensialı ortadır və boşluğu istismar etmək asandır;

Yüksək (H) – Təhdid mənbəyinin motivasiyası yüksəkdir və potensialı yetərlidir və ya boşluğu istismar etmək asandır.

İnT mexanizmlərinin təhdidlərə qarşı effektivliyi aşağıdakı subyektiv şkala ilə qiymətləndirilir:

- Aşağı (L) – İnT mexanizmi təhdidin təsirlərini az dərəcədə azaldır (qalıq riskin səviyyəsi yüksəkdir);
- Orta (M) – İnT mexanizmi təhdidin təsirlərini orta səviyyədə azaldır (qalıq riskin səviyyəsi ortadır);
- Yüksək (H) – İnT mexanizmi tətbiq edildikdən sonra təhdidin əksər təsirləri neytrallaşdırılır (qalıq risklərin səviyyəsi aşağıdır).

"İT-servislər→Biznes-proseslər" tandemi əsasən təhdidin reallaşması nəticəsində vurulan ziyanın qiymətləndirilməsi üçün istifadə edilir. Aşağıdakı kriteriyalar nəzərə alınır:

- İT-servisdən asılı olan biznes-proseslərin kritikliyi;
- İT-servisin bərpasına (yenidən qurulmasına, əvəzlənməsinə) çəkilən xərclər;
- Biznes-prosesin pozulması nəticəsində təşkilata vurulan maddi ziyan;
- Biznes-prosesin pozulması nəticəsində təşkilatın nüfuzuna vurulan ziyan;
- Biznes-prosesin pozulması nəticəsində təşkilata vurulan digər ziyanlar;
- Müqavilə şərtlərinin pozulmasına görə cərimələr və s.

[16]-də İnT risklərinin qiymətləndirilməsinə müxtəlif yanaşmalar (ehtimallı, qeyri-səlis və ekspert) müqayisəli analiz edilmiş və belə qənaətə gəlinmişdir ki, risklərin qiymətləndirilməsinin adekvatlığını artırmaq üçün qeyri-səlis yanaşma daha perspektivlidir. Qeyri-səlis yanaşma ekspert biliklərinin aşkarlanmasının sadəliyi ilə xarakterizə olunur. Bundan başqa, müxtəlif növ qeyri-müəyyənlikləri formal təsvir etmək və nəzərə almağa, həmçinin qeyri-bircins informasiyanı (determinə olunmuş, intervallı, statistik, linqvistik) vahid formada formallaşdırmağa və istifadə etməyə imkan verir. Bu və digər üstünlükləri nəzərə alaraq bu işdə yuxarıda sadalanan kriteriyalardan təhdidin gerçəkləşməsi ehtimalının, İnT mexanizmlərinin effektivliyinin, biznes-proseslərin kritikliyinin, təşkilatın nüfuzuna vurulan ziyanın qeyri-səlis üçbucaqlı ədədlər ilə ifadə edildiyi qəbul edilir.

TOPSIS metodu

TOPSIS – sonlu alternativlər çoxluğundan həllin müəyyən edilməsi üçün çoxkriteriyalı metoddur. TOPSIS metodunun əsas ideyası pozitiv ideal alternativlərin və neqativ ideal alternativlərin müəyyən edilməsidir. Pozitiv ideal alternativ gəlir kriteriyalarını maksimallaşdıran və xərc meyarlarını minimallaşdıran alternativdir. Neqativ ideal alternativ xərc kriteriyalarını

maksimallaşdırır və gəlir kriteriyalarını minimallaşdırır. Optimal alternativ pozitiv ideal alternativdən ən yaxın məsafədə və neqativ ideal alternativdən ən uzaq məsafədə olan alternativ(lər)dir.

TOPSIS metodunun işini aşağıdakı addımlar ardıcıllığı ilə izah etmək olar:

(1) n alternativin k kriteriya üzrə reytinqləri matrisi $X_{n\times k}$ qurulur. Reytinq qiymətləri adətən normallaşdırılır.

(2) Hər bir kriteriya üçün w_k vaciblik əmsalı müəyyən edilir.

(3) İdeal S^+ alternativini müəyyən edirlər (hər kriteriya üzrə ekstremal reytinqlər).

(4) İdeal S^- alternativini müəyyən edirlər (hər kriteriya üzrə ekstremal tərs reytinqlər).

(5) Hər bir alternativin ideal $\left(D_i^+\right)$ və neqativ ideal alternativdən $\left(D_i^-\right)$ məsafəsi hesablanır.

(6) Hər bir alternativ üçün yaxınlıq əmsalı hesablanır: $D_i^* = \dfrac{D_i^-}{D_i^- + D_i^+}$

(7) Alternativlər yaxınlıq əmsalı üzrə ranqlaşdırılır.

Qeyri-səlis ədədlər

Bu bölmədə qeyri-səlis ədədlərin bəzi anlayışları verilir [17-18].

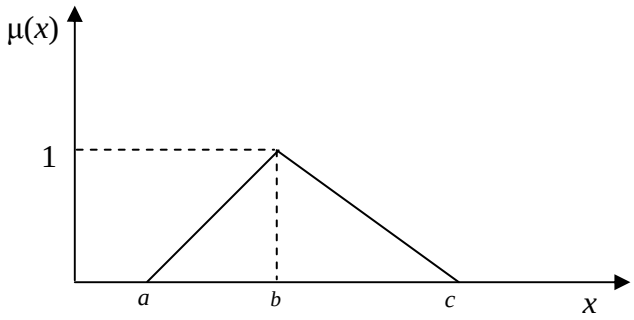
Tərif 1. Həqiqi ədədlər çoxluğunun $\mu(x)$ mənsubiyyət funksiyası aşağıdakı şərtləri ödəyən qeyri-səlis altçoxluğuna qeyri-səlis ədəd deyilir:

1. Kəsilməzlik.
2. Normallıq: $\sup\limits_{x\in R}\{\mu(x)\} = 1$.
3. Qabarıqlıq: $\mu(x_j) \geq \min\{\mu(x_i), \mu(x_k)\}, x_i \leq x_j \leq x_k$.

Tərif 2. Üçbucaqlı qeyri-səlis ədədin mənsubiyyət funksiyası aşağıdakı şəkildə olan qeyri-səlis çoxluğa deyilir (şəkil 1):

$$\mu(x) = \begin{cases} (x-a)/(b-a), & a \leq x \leq b, \\ (x-c)/(b-c), & b \leq x \leq c, \\ 0, & \textit{qalan hallarda.} \end{cases} \qquad (1)$$

burada a, b, c – həqiqi ədədlərdir. Üçbucaqlı qeyri-səlis ədədi (a, b, c) üçlüyü kimi işarə etmək olar.



Şəkil 1. Üçbucaqlı qeyri-səlis ədəd

Bu işdə üçbucaqlı qeyri-səlis ədədlərin toplanması və adi müsbət ədədə vurulması əməllərindən istifadə ediləcək. $A = (a_1, a_2, a_3)$ və $B = (b_1, b_2, b_3)$ üçbucaqlı qeyri-səlis ədədlərinin toplanmasını ($\oplus$) və adi müsbət ədədə vurulmasını ($\otimes$) aşağıdakı düsturlarla vermək olar:

$$A \oplus B = (a_1 + b_1, a_2 + b_2, a_3 + b_3), \qquad (2)$$

$$r \otimes A = (ra_1, ra_2, ra_3),\ r \in R^+. \quad (3)$$

Tutaq ki, $A = (a_1, a_2, a_3)$ və $B = (b_1, b_2, b_3)$ iki üçbucaqlı qeyri-səlis ədəddir. A və B qeyri-səlis ədədləri arasındakı $d(A,B)$ məsafəsini aşağıdakı kimi müəyyən etmək olar:

$$d(A,B) = \sqrt{\frac{1}{3}\left[(a_1 - b_1)^2 + (a_2 - b_2)^2 + (a_3 - b_3)^2\right]}. \quad (4)$$

Bu işdə $A = (a,b,c)$ üçbucaqlı qeyri-səlis ədədinin səlisləşdirilməsi üçün aşağıdakı düstur istifadə edilir.

$$D(A) = \frac{1}{3} \times (a + b + c) \quad (5)$$

Qeyri-səlis TOPSIS metodu

Fərz edək ki, $D_j, j = 1,...,n$ ekspertləri $T_i, i = 1,...,m$ təhdidlərini $C_k, k = 1,...,K$ kriteriyalarının hər biri üzrə qiymətləndirir. Ekspertlər kriteriyaların vaciblik əmsallarını (çəkilərini) də qiymətləndirirlər. Tutaq ki, $C_k, k = 1,...,K$ kriteriyaları obyektiv və subyektiv kimi təsnif olunurlar. Təhdidlərin subyektiv kriteriyalar üzrə qiymətləri, həmçinin kriteriyaların çəkiləri üçbucaqlı qeyri-səlis ədədlərlə təsvir olunan linqvistik dəyişənlər vasitəsilə qiymətləndirilir.

Addım 1. Kriteriyaların çəkilərinin aqreqasiyası. Bu işdə kriteriyaların çəkilərinin aqreqasiyası üçün ortalama metodu istifadə edilir. Tutaq ki, $W_{kj} = (a_{kj}, b_{kj}, c_{kj})$ $k = 1,...,K;\ j = 1,...,n$ – j-cu ekspert tərəfindən k-cı kriteriyaya verilmiş linqvistik çəkidir. k-cı kriteriyanın aqreqasiya edilmiş $w_k = (a_k, b_k, c_k), k = 1,...,K$ linqvistik çəkisi aşağıdakı kimi hesablana bilər:

$$w_k = \left(1/n\right) \otimes (W_{k1} \oplus W_{k2} \oplus ... \oplus W_{kn}), \quad (6)$$

burada $a_k = \dfrac{\sum_{j=1}^{n} a_{kj}}{n}$, $b_k = \dfrac{\sum_{j=1}^{n} b_{kj}}{n}$, $c_k = \dfrac{\sum_{j=1}^{n} c_{kj}}{n}$.

Addım 2. Təhdidlərin kriteriyalar üzrə reytinqlərinin aqreqasiyası. Tutaq ki, $r_{ikj} = (o_{ikj}, p_{ikj}, q_{ikj}),\quad i = 1,...,m;\ k = 1,...,K;\ j = 1,...,n$ – j-cu ekspertin k-cı kriteriya üzrə $i-$ci təhdidə uyğun gördüyü qeyri-səlis reytinqdir. T_i təhdidinin C_k kriteriyası üzrə aqreqasiya edilmiş $R_{ik} = (o_{ik}, p_{ik}, q_{ik}), i = 1,...m;\ k = 1,...,K$ reytinqi belə hesablana bilər:

$$R_{ik} = \left(1/n\right) \otimes (R_{ik1} \oplus R_{ik2} \oplus ... \oplus R_{ikn}), \quad (7)$$

burada $o_{ik} = \dfrac{\sum_{j=1}^{n} o_{ikj}}{n}$, $p_{ik} = \dfrac{\sum_{j=1}^{n} p_{ikj}}{n}$, $q_{ik} = \dfrac{\sum_{j=1}^{n} q_{ikj}}{n}$.

Addım 3. Kriteriyalar üzrə qiymətlərin normallaşdırılması. Bu addımda müxtəlif ölçülərə malik qiymətlər ölçüsüz qiymətlərə çevrilir, bu sonradan onları müqayisə etməyə imkan verir. Bu işdə çevrilmələr Hsu və Chen [19] metodu tətbiq edilməklə yerinə yetirilir, bu metod çevrilmiş üçbucaqlı qeyri-səlis ədədlərin [0,1]-ə aid olmasını təmin edir. Tutaq ki, $R_{ik} = (o_{ik}, p_{ik}, q_{ik}), i = 1,...m;\ k = 1,...,K$ – T_i təhdidinin C_k kriteriyası üzrə qiymətidir, onda normallaşdırılmış qiymət aşağıdakı düsturlarla hesablanacaq:

$$\tilde{R}_{ik} = \left(\frac{o_{ik}}{q_k^+}, \frac{p_{ik}}{q_k^+}, \frac{q_{ik}}{q_k^+}\right),\ i = 1,...m;\ k \in B, \quad (8)$$

$$\tilde{R}_{ik} = \left(\frac{o_k^-}{q_{ik}}, \frac{o_k^-}{p_{ik}}, \frac{o_k^-}{o_{ik}}\right),\ i = 1,...m;\ k \in C, \quad (9)$$

burada $q_k^+ = \max_i q_{ik}$, $o_k^- = \min_i o_{ik}$, B və C isə uyğun olaraq gəlir və xərc kriteriyalarının indeksləri çoxluğudur.

Addım 4. Çəkili matrisin hesablanması. Çəkili matris qeyri-səlis çəkilərin normallaşmış matrisin qeyri-səlis elementlərinə vurmaqla alınır. Hesablamaları sadələşdirmək üçün bu işdə üçbucaqlı qeyri-səlis ədədlərlə ifadə edilmiş çəkilərin (5) düsturu ilə səlisləşdirilməsi aparılır. Çəkili V matrisi normallaşmış matrisin hər bir sütununun uyğun w_k çəki əmsalına vurulması ilə alınır:

$$v_{ik} = w_k \otimes \tilde{R}_{ik}, \quad i = 1,...,m; k = 1,...,K. \tag{10}$$

Addım 5. Qeyri-səlis pozitiv və neqativ ideal həllərin müəyyən edilməsi. Tutaq ki, I^+ və I^- uyğun olaraq qeyri-səlis pozitiv və qeyri-səlis neqativ ideal həlləri işarə edir. I^+ və I^- aşağıdakı düsturlarla müəyyən edilir:

$$I^- = [v_1^-, v_2^-, \ldots v_n^-], \tag{11}$$

$$I^+ = [v_1^+, v_2^+, \ldots v_n^+], \tag{12}$$

burada $v_j^+ = \max_i \{v_{ij}\}$, $v_j^- = \min_i \{v_{ij}\}$, $j = 1,2,\ldots,n.$

Addım 6. İdeal həllərdən məsafələrin hesablanması. Hər bir $T_i, i = 1,...,m$ təhdidinin qeyri-səlis pozitiv və qeyri-səlis neqativ ideal həllərdən məsafələrini aşağıdakı kimi hesablamaq olar:

$$D_i^+ = \sum_{j=1}^{n} d(v_{ij}, v_j^+), \ i = 1,...,m, \tag{13}$$

$$D_i^- = \sum_{j=1}^{n} d(v_{ij}, v_j^-), \ i = 1,...,m, \tag{14}$$

burada d – üçbucaqlı qeyri-səlis ədədlər arasında (4) düsturu ilə müəyyən edilmiş məsafədir.

Addım 7. Yaxınlıq əmsallarının hesablanması. T_i təhdidinin I^+ həllinə yaxınlıq əmsalını belə müəyyən etmək olar:

$$C_i^* = \frac{D_i^-}{D_i^- + D_i^+} \tag{15}$$

Aydındır ki, $0 \le C_i^* \le 1$, $i = 1,2,\ldots,m.$ Əgər $C_i^* = 0$ olarsa, onda T_i təhdidi ideal neqativ həll olmalıdır, əksinə, əgər $C_i^* = 1$ olarsa, onda T_i ideal pozitiv həldir. Əgər T_i təhdidi neqativ ideal həllə yaxındırsa və ideal həldən uzaqdırsa, onda C_i^* qiyməti 0-a yaxınlaşır. Əgər T_i ideal həllə yaxın və neqativ ideal həldən uzaqdırsa, onda C_i^* qiyməti 1-ə yaxınlaşır. Deməli, yaxınlıq əmsalları əsasında təhdidlər çoxluğunun ranqlaşdırma sırasını müəyyən etmək olar.

Hesablama eksperimenti

Fərz edək ki, təşkilat e-kommersiya ilə məşğul olur və bunu özünün korporativ şəbəkəsində yerləşdirilmiş veb-server vasitəsilə həyata keçirir. Aşağıdakı üç təhdidə baxaq:

T_1: veb-serverə paylanmış xidmətdən imtina hücumu (Distributed Denial of Service, DDoS);

T_2: müştəri verilənlərinin konfidensiallığının pozulması;

T_3: korporativ şəbəkə resurslarından nəzarətsiz istifadə.

Təhdidlərin qiymətləndirilməsi üçün istifadə edilən kriteriyalar subyektiv və obyektiv kriteriyalar olmaqla iki sinfə bölünərək cədvəl 1-də göstərilir.

Cədvəl 1

Təhdidlərin qiymətləndirilməsi kriteriyaları

Subyektiv kriteriyalar	**Obyektiv kriteriyalar**
Təhdidin gerçəkləşməsi ehtimalı (C_1)	İT-servisin bərpası xərcləri (C_5)
İnT mexanizmlərinin effektivliyi (C_2)	Təşkilata vurulan maddi ziyan (C_6)
Biznes-proseslərin kritikliyi (C_3)	Müqavilə şərtlərinin pozulmasına görə cərimələr (C_7)
Təşkilatın nüfuzuna vurulan ziyan (C_4)	Təşkilata vurulan digər ziyanlar (C_8)

Fərz edək ki, ekspertlər kriteriyaların çəkilərini (vaciblik əmsallarını) *Vaciblik* = *W* linqvistik dəyişəni ilə qiymətləndirirlər. Tutaq ki, *Vaciblik* linqvistik dəyişəninin şkalası 5 qiymətə bölünüb: *W* = {*VI, I, F, UI, VUI*}, burada *VI = çox vacib, I = vacib, F = orta vacib, UI = az vacib, VUI = çox az vacib*. Bu dəyişənin qiymətlərini aşağıdakı kimi üçbucaqlı qeyri-səlis ədədlər şəklində göstərək: *VI* = (0.8; 1.0; 1.0), *I* = (0.5; 0.7; 0.9), *F* = (0.3; 0.5; 0.7), *UI* = (0.1; 0.3; 0.5), *VUI* = (0.0; 0.0; 0.2). Kriteriyalara ekspertlər tərəfindən verilmiş çəkilər, (6) düsturuna əsasən hesablanmış uyğun orta çəkilər və (5) düsturuna əsasən hesablanmış səlisləşdirilmiş orta çəkilər cədvəl 2-də göstərilir.

Cədvəl 2

Kriteriyaların çəkiləri və orta çəkilər

Kriteriyalar	Ekspertlər				Orta çəkilər ($w_k, k = 1,...,K$)	Səlisləşdirilmiş orta çəkilər
	E_1	E_2	E_3	E_4		
C_1	F	I	VI	I	(0.131, 0.181, 0.219)	0.177
C_2	F	VI	I	VI	(0.15, 0.20, 0.225)	0.192
C_3	VUI	F	UI	F	(0.044, 0.081, 0.131)	0.085
C_4	UI	F	F	F	(0.063, 0.113, 0.163)	0.133
C_5	VI	I	I	VI	(0.163, 0.212, 0.238)	0.204
C_6	I	VI	VI	I	(0.163, 0.212, 0.238)	0.204
C_7	VI	I	F	I	(0.131, 0.181, 0.219)	0.177
C_8	I	UI	F	I	(0.088, 0.138, 0.187)	0.138

Cədvəl 3-də təhdidlərin subyektiv kriteriyalar üzrə ekspertlər tərəfindən verilmiş reytinqləri və (7) düsturuna əsasən hesablanmış orta reytinqləri göstərilir. Təhdidin gerçəkləşməsi ehtimalının qiymətləri üçün aşağıdakı üçbucaqlı qeyri-səlis ədədlərdən istifadə edilir: L = (0.0; 0.3; 0.3), M = (0.3; 0.6; 0.8), H = (0.7; 1.0; 1.0). Biznes-proseslərin kritikliyi *Kritiklik* linqvistik dəyişəni ilə qiymətləndirilir: *C* = {*VC, C, F, LC, VLC*}, burada *VC = çox kritik, C = kritik, F = orta kritik, LC = az kritik, VLC = çox az kritik*. Bu dəyişənin qiymətlərini aşağıdakı üçbucaqlı qeyri-səlis ədədlər şəklində göstərək: *VC* = (0.7; 1.0; 1.0), *C* = (0.5; 0.7; 1.0), *F* = (0.2; 0.5; 0.8), *LC* = (0.0; 0.3; 0.5), *VLC* = (0.0; 0.0; 0.3).

Təşkilatın nüfuzuna vurulan ziyanı aşağıdakı üçbucaqlı qeyri-səlis ədədlər şəklində göstərilən linqvistik dəyişənlə ifadə edək: *VL* = çox aşağı = (0.0; 0.0; 0.3), *L* = aşağı = (0.0; 0.3; 0.5), *M* = orta = (0.2; 0.5; 0.8), *H* = yüksək = (0.5; 0.7; 1.0), *VH* = çox yüksək = (0.7; 1.0; 1.0).

Cədvəl 3

Təhdidlərin subyektiv kriteriyalar üzrə reytinqləri və orta reytinqlər

Kriteriyalar	Təhdidlər	Ekspertlər				Ortalama reytinqlər (R_{ik})
		E_1	E_2	E_3	E_4	
C_1	T_1	M	L	M	H	(0.081; 0.156; 0.181)
	T_2	H	M	L	L	(0.063; 0.138; 0.15)
	T_3	L	H	L	H	(0.088; 0.163; 0.163)
C_2	T_1	L	L	M	M	(0.038; 0.113; 0.138)
	T_2	M	M	H	L	(0.081; 0.156; 0.181)
	T_3	M	M	H	H	(0.125; 0.2; 0.225)
C_3	T_1	VC	VC	C	VC	(0.163; 0.231; 0.25)
	T_2	C	F	F	LC	(0.056; 0.125; 0.194)
	T_3	LC	F	C	LC	(0.044; 0.113; 0.175)
C_4	T_1	VH	VH	H	H	(0.15; 0.213; 0.25)
	T_2	H	M	M	L	(0.056; 0.125; 0.194)
	T_3	M	L	L	H	(0.044; 0.113; 0.175)

Təhdidlərin obyektiv kriteriyalar üzrə ekspertlər tərəfindən verilmiş qiymətləri (şərti maliyyə vahidləri ilə) cədvəl 4-də göstərilir.

Cədvəl 4

Təhdidlərin obyektiv kriteriyalar üzrə qiymətləri

Təhdidlər	C_5	C_6	C_7	C_8
T_1	(55.5; 57.0; 58.6)	(94.0; 95.0; 96.0)	(10.5; 12.5; 13.5)	(1.1; 1.2; 1.4)
T_2	(25.0; 27.0; 29.0)	(12.5; 14.0; 16.5)	(4.5; 6.0; 7.5)	(1.0; 1.5; 2.0)
T_3	(7.5; 8.5; 10.0)	(13.5; 15.0; 17.5)	(0.1; 0.5; 0.7)	(2.0; 3.0; 4.0)

Cədvəl 5-də təhdidlərin obyektiv kriteriyalar üzrə (8) və (9) düsturları ilə normallaşdırılmış qiymətləri göstərilir. Kriteriyalar xərc kriteriyaları olduğundan (9) düsturu istifadə edilir.

Cədvəl 5

Təhdidlərin obyektiv kriteriyalar üzrə normallaşdırılmış qiymətləri

Təhdid	C_5	C_6	C_7	C_8
T_1	(0.128; 0.132; 0.135)	(0.13; 0.132; 0.133)	(0.007; 0.008; 0.01)	(0.714; 0.83; 0.91)
T_2	(0.259; 0.278; 0.3)	(0.758; 0.893; 1.0)	(0.013; 0.017; 0.02)	(0.5; 0.667; 1.0)
T_3	(0.75; 0.882; 1.0)	(0.714; 0.833; 0.926)	(0.143; 0.2; 1.0)	(0.25; 0.333; 0.5)

Cədvəl 6-da təhdidlərin obyektiv kriteriyalar üzrə (10) düsturu ilə hesablanmış qiymətləri göstərilir.

Cədvəl 6

Təhdidlərin obyektiv kriteriyalar üzrə çəkili normallaşdırılmış qiymətləri

	T_1	T_2	T_3
C_1	(0.014; 0.028; 0.032)	(0.011; 0.024; 0.027)	(0.016; 0.029; 0.029)
C_2	(0.007; 0.022; 0.026)	(0.016; 0.03; 0.035)	(0.024; 0.038; 0.043)
C_3	(0.03; 0.043; 0.046)	(0.01; 0.023; 0.036)	(0.008; 0.021; 0.032)
C_4	(0.02; 0.028; 0.033)	(0.007; 0.017; 0.026)	(0.006; 0.015; 0.023)
C_5	(0.026; 0.027; 0.028)	(0.053; 0.057; 0.061)	(0.153; 0.18; 0.204)
C_6	(0.0265; 0.027; 0.0271)	(0.155; 0.182; 0.204	(0.146; 0.17; 0.189)
C_7	(0.001; 0.0014; 0.0017)	(0.002; 0.003; 0.004)	(0.025; 0.035; 0.177)
C_8	(0.099; 0.115; 0.126)	(0.069; 0.092; 0.138)	(0.035; 0.046; 0.069)

Çəkili normallaşmış matris qurulduqdan sonra (11) və (12) düsturuna əsasən qeyri-səlis pozitiv və neqativ ideal həllər müəyyən edilir:

$$I^+ = [(0.032,0.032,0.032),(0.043,0.043,0.043),(0.046,0.046,0.046),(0.033,0.033,0.033),$$
$$(0.204,0.204,0.204),(0.204,0.204,0.204),(0.177,0.177,0.177),(0.138,0.138,0.138)],$$
$$I^- = [(0.011,0.011,0.011),(0.007,0.007,0.007),(0.008,0.008,0.008),(0.006,0.006,0.006),$$
$$(0.026,0.026,0.026),(0.026,0.026,0.26),(0.001,0.001,0.001),(0.035,0.035,0.035)].$$

Bundan sonra hər bir təhdidlə pozitiv və neqativ ideal həll arasındakı məsafə hər bir kriteriyaya görə (4) düsturuna əsasən hesablanır. Nəticələr uyğun olaraq cədvəl 7-də və 8-də verilib.

Cədvəl 7

Təhdid və pozitiv ideal həll arasında hər bir kriteriya üzrə məsafə

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
$d(T_1, I^+)$	0.0106	0.026	0.0094	0.0080	0.177	0.1771	0.1756	0.0270
$d(T_2, I^+)$	0.0133	0.0179	0.0253	0.0181	0.1470	0.0310	0.1740	0.0479
$d(T_3, I^+)$	0.0096	0.0113	0.0275	0.0196	0.0325	0.0398	0.1201	0.0891

Cədvəl 8

Təhdid və neqativ ideal həll arasında hər bir kriteriya üzrə məsafə

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
$d(T_1, I^-)$	0.0157	0.0140	0.0324	0.0217	0.0013	0.0009	0.0005	0.0791
$d(T_2, I^-)$	0.0119	0.0216	0.0184	0.0132	0.0312	0.1556	0.0022	0.0707
$d(T_3, I^-)$	0.0150	0.0291	0.0158	0.0111	0.1544	0.1434	0.1044	0.0206

Nəhayət, (13) və (14) düsturlarına əsasən hər bir təhdidin müvafiq olaraq pozitiv və neqativ ideal həllərdən məsafələri və (15) düsturuna əsasən yaxınlıq əmsalları hesablanır.

Yaxınlıq əmsalları əsasında təhdidlərin ranqları müəyyən edilir. Müvafiq nəticələr cədvəl 9-da verilir.

Cədvəl 9

İdeal həllərdən məsafələr, yaxınlıq əmsalları və ranqlar

	D_i^+	D_i^-	C_i	Ranq
T_1	0.6107	0.1656	0.2133	3
T_2	0.4745	0.3248	0.4064	2
T_3	0.3495	0.4938	0.5856	1

Cədvəl 9-a əsasən təhdidlərin ranq sırası T_3, T_2, T_1 olacaq.

Nəticə

İşdə informasiya təhlükəsizliyi risklərinin idarə edilməsi üçün qeyri-səlis TOPSIS metodu əsasında təhdidlərin ranqlaşdırılması metodu təklif edilmişdir. Kriteriyalar sistemi təhdidlərin, informasiya təhlükəsizliyi mexanizmlərinin, İT-servislərin və biznes-proseslərin qarşılıqlı əlaqəsi nəzərə alınmaqla təklif edilmişdir. Kriteriyalar qeyri-səlis üçbucaqlı ədədlərlə ifadə edilmiş linqvistik dəyişənlərlə qiymətləndirilir. Təhdidlərin ranqlaşdırılması pozitiv və neqativ ideal təhdidlərdən nisbi yaxınlıq əmsalı əsasında aparılır. Təklif edilmiş metodun hesablama prosesi mürəkkəb deyil və nümayiş üçün ədədi eksperimentin nəticələri verilmişdir.

Ədəbiyyat

1. İmamverdiyev Y.N., Derakshandeh S.Ə. İnformasiya təhlükəsizliyi risklərinin optimal idarə edilməsi modeli və onun genetik həll alqoritmi/ İnformasiya texnologiyaları problemləri, 2010, №2, s. 36–46.
2. Алгулиев Р.М., Имамвердиев Я. Н., Деракшанде С.А. Сравнительный анализ методологий управления рисками информационной безопасности // Azərbaycan Milli Aerokosmik Agentliyinin Xəbərləri, 2010, №2-3, s. 77–85.
3. Hwang C.L., and Yoon K.S. Multiple attribute decision making: methods and applications. New York: Springer, 1981.
4. Abdullah L., and Zamri N. Ranking of the factors associated with road accidents using correlation analysis and fuzzy TOPSIS / Australian Journal of Basic and Applied Sciences, 2010, v.4, no.2, pp.314–320.
5. Chen C.T., Lin C.T., and Huang S.F. A fuzzy approach for supplier evaluation and selection in supply chain management / International Journal of Production Economics, 2006, v.102, no.2, pp. 289–301.
6. Chu T.-C., and Lin Y.-C. A Fuzzy TOPSIS method for robot selection / Int. Journal of Advanced Manufacturing Technology, 2003, v.21, no. 4, pp. 284–290.
7. Chui Y.C., and Chan S.P. Fuzzy cash flow analysis using present worth criterion / Engineering Economist, v.39, no.2, pp. 113-138.
8. Wanga Y.-J., and Lee H.-S. Generalizing TOPSIS for fuzzy multiple-criteria group decision-making / Computers and Mathematics with Applications, 2007, v.53, no.11, pp.1762–1772.
9. Саати Т. Л. Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993. – 320 с.
10. Подиновский В.В., Подиновская О.В. О некорректности метода анализа иерархий // Проблемы управления, 2011, № 1, с. 8–13.
11. Вихорев С.В., Кобцев Р.Ю. Как узнать – откуда напасть или откуда исходит угроза безопасности информации // Защита информации. Конфидент, 2002, № 2, с. 44–49.
12. Swiderski F., and Snyder W. Threat modeling. Redmond, WA: Microsoft Press, 2004.

13. Stoneburner G., Goguen A., Feringa A. NIST Special Publication 800-30: Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology, 2002.
14. OWASP risk rating methodology.
https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
15. Имамвердиев Я.Н., Деракшанде С.А., Сервис - ориентированная эталонная модель для управления рисками информационной безопасности // Информационные технологии, 2011, №3, с. 35–40.
16. Алгулиев Р.М., Имамвердиев Я.Н., Деракшанде С.А. Пути повышения точности методов оценки рисков информационной безопасности // Информационные технологии, 2010, №12, с. 6–11.
17. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. Пер. с англ., М.: Мир, 1976, 165 с.
18. Bojadziev G., Bojadziev M. Fuzzy logic for business, finance, and management (Advances in Fuzzy Systems: Applications and Theory, v.23), 2nd Edition, World Scientific Publishing Company, 2007, 232 p.
19. Hsu H.M., Chen C.T., Fuzzy credibility relation method for multiple criteria decision-making problems / Information Sciences, 1997, v.96, no. 1-2, pp.79–91.

УДК 004.056

Имамвердиев Ядигар Н.[1], Деракшанде Садик А.[2]
Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]yadigar@lan.ab.az; [2]smdk364@yahoo.com

Об одном методе ранжирования угроз информационной безопасности

Предложен нечеткий TOPSIS метод ранжирования угроз информационной безопасности. Оценки угроз по субъективным критериям и веса всех критериев оцениваются в лингвистических переменных, представленных нечеткими числами. Значения по объективным критериям преобразуются к безразмерным индексам для обеспечения совместимости с оценками по субъективным критериям. Для ранжирования угроз определяются коэффициенты близости как расстояния от идеального позитивного и негативного решений. Численный пример демонстрирует вычислительный процесс предложенного метода.

Ключевые слова: *информационная безопасность, риски информационной безопасности, угроза, уязвимость, нечеткий TOPSIS, ранжирование угроз.*

Yadigar N. Imamverdiyev[1], Sadegh A. Derakhshandeh[2]
Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]yadigar@lan.ab.az; [2]smdk364@yahoo.com

About one method for information security threat ranking

A fuzzy TOPSIS method for information security threat ranking is proposed. The ratings of threats by subjective criteria and the weight of all criteria are assessed in linguistic terms represented by triangle fuzzy numbers. The values of objective criteria are converted into dimensionless indices to ensure compatibility between the values of objective criteria and the linguistic ratings of subjective criteria. A closeness coefficient is defined to determine the ranking order of threats by calculating the distances to both the ideal and negative-ideal solutions. A numerical example demonstrates the computational process of the proposed method.

Keywords: *information security, information security risk, threat, vulnerability, fuzzy TOPSIS, threat ranking.*