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 RİSKLƏRİNİN OPTİMAL İDARƏ EDİLMƏSİ MODELİ VƏ ONUN GENETİK HƏLL ALQORİTMİ

İnformasiya təhlükəsizliyi risklərinin optimal idarə edilməsi üçün riyazi model təklif edilir. Risk amillərinin parametrləri və təhlükəsizlik mexanizmlərinin effektivliyi qeyri-səlis mənsubiyyət funkiyaları ilə ifadə olunmuşdur. Təklif edilmiş model verilmiş büdcə daxilində qalıq riskin minimallaşdırılması üçün təhlükəsizlik mexanizmlərinin optimal seçilməsi məsələsini həll edir. Optimal seçim tamqiymətli proqramlaşdırma məsələsi kimi formalizə olunmuş və onun həlli üçün genetik alqoritm təklif edilmişdir.

Açar sözlər: *informasiya təhlükəsizliyi, risk amilləri, riskin qiymətləndirilməsi, riskin idarə edilməsi, qeyri-səlis ədəd, genetik alqorit.*

Giriş

İnformasiya texnologiyalarının geniş tətbiq edildiyi indiki şəraitdə informasiya təhlükəsizliyi (İnT) riskləri istənilən təşkilatın fəaliyyətinin mühüm amilidir. İnformasiya texnologiyaları biznes-proseslərin effektivliyini artırmağa imkan verir, eyni zamanda təşkilatın mövcudluğunu sual altında qoyan informasiya təhlükəsizliyi insidentlərinin mənbəyi də ola bilər. İnT-nin təmin edilməsinə müasir yanaşmalar risklərin idarə edilməsinə əsaslanır, buna görə də İnT risklərinin idarə edilməsi müasir təşkilatın biznes-proseslərinin dəstəklənməsi üçün həlledici əhəmiyyətə malikdir. Beləliklə, İnT-in risklərinin idarə edilməsi əməliyyat risklərinin növlərindən biri kimi risklərin idarə edilməsi üzrə təşkilatın ümumi sisteminin əhəmiyyətli hissəsinə çevrilir [1].

İnT risklərinin idarə edilməsi risklərin analizi və qiymətləndirilməsi, risklərin dəyərləndirilməsi, risklərin emalı və istifadəçilərin risklər barəsində məlumatlandırılması proseslərini əhatə edir [2, 3]. Risklərin dəyərləndirilməsi mərhələsində riskin yolverilən səviyyəsi müəyyən edilir və bundan çıxış edərək səviyyəsi yolveriləni aşmayan risklər qəbul edilir. Gerçəkləşməsi zamanı yolverilən səviyyəni aşan risklər emal mərhələsini tələb edirlər. Risklərin əsas emal tədbirlərinə riskdən imtina (riskin mənbəyinin tam aradan qaldırılması), riskin ötürülməsi (və ya riskin sığortalanması), riskin azaldılması – mühafizə mexanizmlərinin seçilməsi və tətbiqi aid edilir.

İnT risklərinin idarə edilməsinin məqsədi təhlükəsizlik mexanizmlərinə minimal xərc çəkməklə risklərin yolverilən səviyyəyə qədər azaldılmasıdır. İnT riskləri təhdidlərin və boşluqların ehtimalından və bu təhdidlərin reallaşması nəticəsində təşkilata dəyən ziyanın kəmiyyətindən asılı funksiya kimi müəyyənləşdirilir. Riskə təsir edən qeyri-müəyyən faktorların sayı çox olduğuna görə həm ehtimalların, həm də vurulan ziyanın kəmiyyətinin hesablanması çox mürəkkəb məsələdir [4]. Riskin qiymətləndirilməsinin mövcud kəmiyyət və keyfiyyət metodları bir sıra nöqsanlara malikdir və seçilən təhlükəsizlik mexanizmlərinin xərc-səmərə baxımından analizini aparmağa imkan vermir. Buna görə də İnT risklərinin qiymətləndirilməsi üçün adekvat metrikaların işlənməsi xüsusi aktuallıq kəsb edir. Bu problem risklərin idarə edilməsi prosesini çətinləşdirən, əsaslandırılmayan və düzgün olmayan idarəetmə qərarlarının qəbul edilməsi ehtimalını artıran xarici mühitin qeyri-müəyyənlik amillərinin sayının artması

ilə daha da aktual olur. İnT risklərinin qiymətləndirilməsində qeyri-müəyyənlik amillərinin nəzərə alınması üçün qeyri-səlis yanaşmanın perspektivləri və problemləri [4] işində analiz edilir.

Bu məqalədə informasiya təhlükəsizliyi risklərinin genetik alqoritm vasitəsilə optimal idarə edilməsi metodu təklif edilir. Riskin hesablanmasında istifadə edilən giriş verilənlərinin (risk amillərinin) qeyri-səlis olduğunu nəzərə alaraq təhlükəsizlik tədbirlərinin seçilməsi məsələsi qeyri-səlis riyazi proqramlaşdırma məsələsi kimi formalizə olunur və bu məsələnin həlli üçün genetik alqoritm təklif edilir.

Mövcud yanaşmaların analizi

Müəssisə səviyyəsində İnT risklərinin idarə edilməsi üçün bir neçə standartlaşdırılmış metodologiya mövcuddur, məsələn, ISO/IEC 13335-3, ISO/IEC 27005 beynəlxalq standartları, həmçinin NIST SP 800-30, BSI, COBIT, SAS 55/78 milli standartları və digər standartlar [1].

Tarixən belə alınmışdır ki, risklərin idarə edilməsinin mövcud metodologiyalarının əksəriyyəti ISO/IEC 17799 (indi ISO/IEC 27005) İnT-in idarə edilməsi standartına əsaslanmışdır [3]. Bu standart konseptual xarakter daşıyır və riskin analizi və qiymətləndirilməsinin konkret metod və metodikalarını məcburi göstərmir. Bu standart əsasında müxtəlif metodikalar və İnT risklərinin idarə edilməsinin 20-yə yaxın instrumental vasitələri işlənilmiş və reallaşdırılmışdır [5─7].

Qeyd etmək lazımdır ki, tədqiqatçılar risklərin təsnifatı, sistemləşdirilməsi, qiymətləndirilməsi və analizi metodlarının işlənməsi üzrə böyük iş aparmışlar [8]. Bununla yanaşı, gələcəkdə həlli vacib olan bir sıra problemlər də mövcuddur. Bu günə qədər İnT risklərini təyin edən amillərin müəyyənləşdirilməsinə vahid yanaşma və risklərin qiymətləndirilməsinin ümumi qəbul edilmiş metodları yoxdur.

İnT risklərinin qiymətləndirilməsi, başlıca olaraq yüksək dərəcədə subyektiv olan ekspert qiymətləndirmələrinə əsaslandığına görə, lazımi adekvatlığa malik deyillər. Risklərin müxtəlif metodlarla hesablanmış kəmiyyətləri öz aralarında pis korrelyasiya olunur, bəzən onlar bir neçə tərtib fərqlənirlər [8, 9].

Tədqiqatlar göstərir ki, İnT risklərinin analizi zamanı istifadə olunan praktiki yanaşmalar çox zaman yaxşı işlənmiş formal əsaslanmaya və uyğun riyazi aparata malik deyillər. Bundan başqa, İnT risklərinin analizinin yeni metodikalarının işlənməsi və mövcud olanlarının modifikasiyası zamanı predmet sahəsindəki əsaslı nəticələrə deyil, praktiki məsələlərin xüsusiyyətlərinə əsaslanırlar.

İnT risklərinin əksər qiymətləndirmə metodları kəmiyyət və keyfiyyət yanaşmalarına və ya onların kombinasiyasına əsaslanır [1, 4].

Kəmiyyət yanaşmanın üstünlükləri qiymətləndirmələrin elmi əsaslandırılması, onların nəticəsinin idarəetmə terminlərində (maliyyə göstəriciləri və faizlə ehtimallar) təqdim edilməsi imkanı, təşkilatda statistik verilənlərin toplanması ilə qiymətləndirmələrin dəqiqliyinin artırılmasıdır. Kəmiyyət yanaşmanın çatışmazlıqlarına, ilk növbədə, əsas ədədi göstəriciləri dəqiq təyin etməyə imkan verən effektiv formal metodların olmaması aid edilir. Bu göstəricilər qiymətləndirməni yerinə yetirən şəxslərin subyektiv qiymətləri əsasında müəyyənləşdirilir. Belə yaxınlaşma isə həmin şəxslərin peşəkarlığına yüksək tələblər irəli sürür. Bundan başqa, kəmiyyət yanaşmanın reallaşması kifayət qədər çox vaxt və böyük hesablama resursu tələb edir.

Keyfiyyət yanaşmasının üstünlükləri, qiymətləndirməni aparan şəxslərin daha mülayim tələblər irəli sürməsi və ədədi qiymətləndirmələrin müəyyənləşdirilməsinin mürəkkəb prosedurlarından imtina imkanıdır. Bu yanaşmanın çatışmazlıqları odur ki, alınan nəticələri birqiymətli interpretasiya etmək olmur, keyfiyyət qiymətləndirməsi zamanı alınan nisbi qiymətlər qərar qəbul edən şəxsləri təmin etməyə bilər.

Qeyd edək ki, risk anlayışlarının əksəriyyəti riskin mövcudluğunu qeyri-müəyyənliklə bağlayırlar, qeyri-müəyyənlik qərarların qəbulunda riskin zəruri və kafi şərti kimi meydana çıxır [9, 10]. İnT məsələləri ilə bağlı qərarlar çox vaxt xarici və daxili mühitin, məqsədlərin, mənbələrin və təhlükələrin nəticələrinin, İnT üzrə tədbirlərin və s. qeyri-müəyyənliyi şəraitində qəbul edilir.

Ona görə də risklərin qiymətləndirilməsinin mövcud metodlarının yuxarıda göstərilən məhdudiyyətlərinin dəf edilməsi ilkin informasiyanın qeyri-müəyyənliyinin və bu informasiyanın emal keyfiyyətinin nəzərə alınmasından əhəmiyyətli dərəcədə asılıdır. Qeyri-müəyyənliyin modelləşdirilməsinin müxtəlif yanaşmaları (ehtimallı, qeyri-səlis və ekspert yanaşmaları) arasında qeyri-səlis yanaşmasının aşağıdakı üstünlüklərini göstərmək olar [9─11]. 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. Qeyri-səlis yanaşma əsasında alınan nəticə mənsubiyyət funksiyasının şəklinin dəyişməsinə az həssasdır, ona görə də qeyri-səlis yanaşma mənsubiyyət funksiyasının mütləq dəqiq verilməsini tələb etmir. Bu üstünlüklər sayəsində son vaxtlar qeyri-səlis modelləşdirmə texnogen sistemlərdə [12, 13], maliyyə sektorunda [10, 11], informasiya təhlükəsizliyi sahəsində [14─17] risklərin idarə edilməsi üçün uğurla tətbiq edilir.

Növbəti bölmələrdə qeyri-səlis ədədlər üzrə zəruri məlumat verilir və informasiya təhlükəsizliyi risklərinin qiymətləndirilməsi üçün qeyri-səlis yanaşma əsasında metod təklif edilir.

Qeyri-səlis ədədlər

Bu bölmədə qeyri-səlis ədədlərin bəzi anlayışları verilir [18─20].

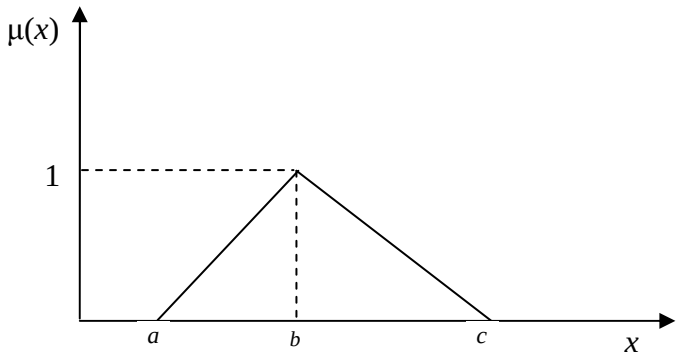
Tərif 1. Həqiqi ədədlər çoxluğunun $\mu(x)$ mənsubiyyət funksiyası aşağıdakı şərtləri ödəyən qeyri-səlis altçoxluğuna qeyri-səlis ədəd deyilir:

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

Tərif 2. Üçbucaq qeyri-səlis ədəd 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. Üçbucaq qeyri-səlis ədədi (a,b,c) üçlüyü kimi işarə etmək olar.



Şəkil 1. Üçbucaqlı qeyri-səlis ədəd

Tərif 3. A qeyri-səlis ədədinin α-kəsiyi $A^{\alpha} = \{x|\mu_A(x) \geq \alpha\}$ səlis çoxluğuna deyilir, burada $x \in R, \alpha \in [0,1]$.

A^{α} çoxluğu R-də boş olmayan qapalı məhdud intervaldır və onu $A^{\alpha} = [A_L^{\alpha}, A_U^{\alpha}]$ kimi işarə etmək olar, burada A_L^{α} və A_U^{α} – uyğun olaraq qapalı intervalın aşağı və yuxarı sərhədləridir. Məsələn, üçbucaq qeyri-səlis $A = (a,b,c)$ ədədi üçün α-kəsiyini

$$A^{\alpha} = [A_L^{\alpha}, A_U^{\alpha}] = [(b-a)\alpha + a, (b-c)\alpha + c] \quad (2)$$

kimi ifadə etmək olar.

Tutaq ki, A və B qeyri-səlis ədədləri verilib, $A, B \in R^+$. A və B-nin α-kəsiyini uyğun olaraq $A^{\alpha} = [A_L^{\alpha}, A_U^{\alpha}]$ və $B^{\alpha} = [B_L^{\alpha}, B_U^{\alpha}]$ ilə işarə edək. A və B qeyri-səlis ədədlərinin toplanmasını $(\oplus)$ və vurulmasını $(\otimes)$ aşağıdakı düsturlarla təyin etmək olar:

$$(A \oplus B)^{\alpha} = [A_L^{\alpha} + B_L^{\alpha}, A_U^{\alpha} + B_U^{\alpha}], \quad (3)$$

$$(A \otimes B)^{\alpha} = [A_L^{\alpha} B_L^{\alpha}, A_U^{\alpha} B_U^{\alpha}], \quad (4)$$

$$(A \otimes r)^{\alpha} = [A_L^{\alpha} r, A_U^{\alpha} r], \; r \in R^+. \quad (5)$$

Bu işdə $A = (a,b,c)$ üçbucaqlı qeyri-səlis ədədinin səlisləşdirilməsi üçün

$$D(A) = \frac{1}{3} \times (a+b+c) \quad (6)$$

düsturu istifadə edilir.

İnformasiya təhlükəsizliyi risklərinin qiymətləndirilməsi

İnT risklərinin idarə edilməsinin ənənəvi yanaşmalarında risk iki (təhdid, ziyan) və ya üç amil (təhdid, boşluq, ziyan) üzrə qiymətləndirilir [1]. Bu işdə riskin iki amil (təhdid, ziyan) üzrə qiymətləndirilməsinə baxılır. Adətən, hesab edirlər ki, təhdid ehtimalı və ziyanın kəmiyyəti nə qədər böyük olarsa, risk də bir o qədər böyük olar. Risklərin sadəcə qiymətləndirilməsi aşağıdakı düsturla ifadə edilə bilər:

$$R = p \cdot D, \quad (7)$$

burada R – İnT riski, p – təhdidin reallaşması ehtimalı, D – ziyandır.

Tutaq ki, təhdidin reallaşması ehtimalı üçün aşağıdakı keyfiyyət qiymətləri müəyyən edilmişdir: çox aşağı (VLR), aşağı (LR), orta (MR), yüksək (HR), çox yüksək

(VHR). [18─20] işlərində keyfiyyət göstəricilərinin qeyri-səlis yanaşma metodlarının köməyi ilə kəmiyyət göstəricilərə çevirmə metodikaları verilmişdir. Bu işdə "Təhdidin reallaşması ehtimalı" p linqvistik dəyişəninin qiymətləri üçün aşağıdakı üçbucaq mənsubiyyət funksiyalı qeyri-səlis ədədlər istifadə olunur: VLR = (0, 0.1, 0.3), LR = (0.2, 0.3, 0.4), MR = (0.4, 0.5, 0.6), HR = (0.6, 0.7, 0.8), VHR = (0.8, 0.9, 1).

Təhdidin reallaşması nəticəsində vurulan ziyanı qiymətləndirmək üçün bu işdə maliyyə sektorunda geniş istifadə edilən VaR (Value-at-Risk) qiymətləndirməsi əsasında yanaşma təklif edilir. Bank sektorunda riskin müxtəlif növlərinin – qiymət riskinin, valyuta riskinin, kredit riskinin, likvidlik riskinin qiymətləndirilməsi üçün VaR metodu 1990-cı illərin ortalarından de-fakto standart rolunu oynayır [21]. VaR metodunun mahiyyəti maliyyə əməliyyatlarının aparılması zamanı meydana çıxan aşağıdakı suala birqiymətli və dəqiq cavabdır: investor müəyyən zaman periodunda verilmiş ehtimalla hansı maksimal ziyana risk edir? Buradan anlaşılır ki, VaR kəmiyyəti investorun məlum zaman periodunda verilmiş ehtimalla məruz qala biləcəyi maksimal gözlənilən ziyan kimi müəyyən edilir.

VaR metodu ilə İnT risklərinin qiymətləndirilməsinə bir neçə cəhd edilib [22, 23]. Bu işdə aşağıdakı yanaşma təklif edilir.

Fərz edək ki, müəssisədə VaR qiymətləndirilib. Təhdidin vurduğu ziyanın VaR qiymətinin maksimum neçə faizini təşkil edə biləcəyi, onun aşağı və yuxarı sərhədləri ekspertlər tərəfindən müəyyən edilir. Bu qiymətləndirməni üçbucaq qeyri-səlis ədədlərlə ifadə etmək əlverişlidir. Üçbucaq qeyri-səlis ədədlər parametrlərin təqribi qiymətlərini ifadə etmək üçün istifadə edilir. Tutaq ki, ziyanın faiz göstəricisi L üçbucaq qeyri-səlis ədədidir, VaR qiymətini isə sadəcə VaR kimi işarə edək, bu halda riski qeyri-səlis ədədlər üzərində yuxarıda təyin edilmiş (3)─(5) əməllərindən istifadə etməklə aşağıdakı düsturla hesablamaq olar:

$$R = p \otimes (L \otimes VaR). \qquad (8)$$

Risklərin optimal idarə edilməsinin riyazi modeli

Risklərin idarə edilməsinə istənilən yanaşmanın mahiyyəti risk amillərinin analizində, risklərin qiymətləndirilməsində və risklərin emalı üzrə adekvat qərarların qəbulundadır. Riskin emalı prosesində onun yolverilən səviyyəsi müəyyən edilir və bundan çıxış edilərək, yolverilən səviyyəni keçməyən risklər qəbul edilir (onların təsirini azaltmaq üçün heç bir əks-tədbir həyata keçirilmir). Yolverilən səviyyəni keçən risklər sonrakı emal mərhələsini tələb edirlər. Belə risklərin əsas emal üsulları risklərdən yayınma (risklərin mənbələrinin tam aradan qaldırılması), risklərin ötürülməsi (risklərin sığortalanması) və risk səviyyəsinin aşağı salınması – təhlükəsizlik tədbirlərinin seçilməsi və tətbiqidir.

Risklərin emalından sonra qalıq risk qiymətləndirilir. Qalıq riskin qəbul edilməməsi halında başlanğıca qayıdılır və proses təkrarlanır. Qeyd edək ki, qalıq risk görülən mühafizə tədbirlərinin effektivliyindən asılıdır, onu qalıq ehtimal və qalıq ziyan əsasında (8) düsturu ilə hesablamaq olar.

Riskin emalı üsulları arasında təhlükəsizlik mexanizmlərinin – aparat və proqram vasitələrinin və təşkilati tədbirlərin seçilməsi və tətbiqi mühüm yer tutur. Müasir təhlükəsizlik mexanizmləri yüksək mürəkkəblik və çoxfunksiyalılıqla xarakterizə olunurlar. Əgər onların obyektiv və subyektiv xarakteristikalarına (onların sayı yüzlərlə ola bilər) ətraflı baxıb, müqayisəsini aparsaq, onda çətin ki birqiymətli seçim etmək

mümkün olsun. Hər bir konkret halda seçim iqtisadi və siyasi mülahizələrlə, sifarişçinin tələbləri və fəaliyyət mühiti ilə müəyyənləşdirilir. Müasir təhlükəsizlik mexanizmlərinin mürəkkəbliyi, müxtəlifliyi və həllin çoxmeyarlılığı onların seçimi üçün müasir optimallaşma metodlarını tələb edir. Mövcud yanaşmalarda, adətən, bir təhlükəsizlik mexanizminin yalnız bir təhdidi neytrallaşdırması halına baxılır [24, 25].

Aşağıdakı dəyişənləri daxil edək.

Fərz edək ki, informasiya sistemində risk səviyyələri yolverilən qiymətdən yüksək olan $Y_i, i = 1,...,n$ təhdidləri aşkarlanmışdır. Hər bir təhdid üçün riskin yolverilən qiyməti müəyyən edilmişdir, $r_i, i = 1,...,n$. Bu təhdidlərin təsirini azaltmaq – uyğun riskləri aşağı salmaq üçün S_j, $j = 1,...,m$ mexanizmləri arasından bəzilərini verilmiş büdcə çərçivəsində seçmək tələb edilir. Təhdidlərin sayının təhlükəsizlik mexanizmlərinin sayından çox olmasını fərz etmək təbiidir: $n \geq m$. Təhlükəsizlik mexanizmlərinin təhdidə "qarşı olması" $\|x_{ij}\|_{n\times m}$ matrisi ilə göstərilir. S_j təhlükəsizlik mexanizmi Y_i təhdidinə təsir edirsə, $x_{ij} = 1$, əks halda $x_{ij} = 0$ qəbul edək. Bir təhlükəsizlik mexanizmi bir neçə təhdidə qarşı dura bilər. Tutaq ki, *j*-ci təhlükəsizlik mexanizminin *i*-ci təhdidə qarşı effektivliyi p_{ij} qalıq risk qiyməti ilə xarakterizə edilir. Təhlükəsizlik mexanizmlərinin verilmiş seçimi üçün qalıq risk aşağıdakı düsturla hesablanır:

$$C_R = \sum R_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij}\, p_{ij} \,. \tag{9}$$

Təhlükəsizlik mexanizmlərinin seçilməsini göstərmək üçün y_j dəyişənini daxil edək. Əgər *j*-ci təhlükəsizlik mexanizmi seçilibsə, onda $y_j = 1$, əks halda $y_j = 0$ qəbul edək.

Təhlükəsizlik mexanizmlərinə çəkilən xərclər bu məqsədə ayrılmış C büdcəsini aşa bilməz:

$$\sum_{j=1}^{m} c_j y_j \leq C\,, \tag{10}$$

burada c_j – *j*-cu təhlükəsizlik mexanizminə çəkilən xərcdir.

Məsələnin qoyuluşuna görə hər bir təhdidə qarşı heç olmasa bir təhlükəsizlik mexanizmi qarşı qoyulmalıdır: $\sum_{j=1}^{m} x_{ij} \geq 1,\ i = 1,...,n$.

Beləliklə, aşağıdakı optimallaşma məsələsini alırıq. Təhlükəsizlik mexanizmlərinin alınmasına ayrılan büdcə daxilində qalıq risklərin minimumlaşdırılması tələb olunur:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij}\, p_{ij} \rightarrow \min \tag{11}$$

$$\sum_{j=1}^{m} y_j c_j \leq C\,, \tag{12}$$

$$\max_j p_{ij} x_{ij} \leq r_i,\ i = 1,...,n\,, \tag{13}$$

$$\sum_{j=1}^{m} x_{ij} \geq 1,\ i = 1,...,n\,, \tag{14}$$

$$x_{ij} \leq y_i, \quad \forall\ i, j \tag{15}$$

Fərz olunur ki, p_{ij} və c_j dəyişənlərindən hamısı və ya bəziləri qeyri-səlis dəyişənlərdir. Hesablamaları asanlaşdırmaq üçün onları (6) düsturu ilə səlisləşdirmək olar. (13) şərti təhlükəsizlik mexanizmləri tətbiq edildikdə qalıq risklərin yolverilən səviyyəni aşmamalı olduğunu göstərir.

Risklərin optimal idarə edilməsi üçün genetik alqoritm

Genetik alqoritmlər optimallaşma məsələlərinin həlli üçün geniş istifadə edilən metodlardandır. Bu metod 1975-ci ildə J.Holland tərəfindən təklif edilmiş və müxtəlif tədqiqatçılar tərəfindən inkişaf etdirilməkdədir [26, 27]. Genetik alqoritmlərin qeyri-səlis yanaşma ilə kombinasiyası istiqamətində də tədqiqatlar aparılır [28, 29].

Genetik alqoritm məsələnin həlli üçün təbii seçmə prinsipindən istifadə edir və aşağıdakı mərhələlərdən ibarətdir [30, 31]:

1) həllin xromosom şəklində kodlaşdırılması;
2) başlanğıc populyasiyanın generasiyası;
3) populyasiyanın xromosomları üçün uyğunlaşma (fitness) funksiyasının hesablanması;
4) cari populyasiyadan xromosomların seçilməsi (seleksiya);
5) çarpazlaşma;
6) mutasiya;
7) genetik alqoritmin dayanma meyarı.

Həllin kodlaşdırılması. Xromosomun kodlaşdırılması üsulu seçilərkən onun həllin spesifik xassələrini əks etdirməsindən çıxış edirlər. Baxılan məsələdə bunu nəzərə almaqla xromosomun iki sətirdən ibarət cədvəl şəklində kodlaşdırılması təklif edilir, birinci sətirdə təhdidlərin nömrəsi, ikinci sətirdə təhlükəsizlik mexanizminin nömrəsi göstərilir. Şəkil 2-də 8-təhdid və 3 mexanizm üçün xromosom nümunə göstərilib.

Təhdidlərin nömrəsi	1	2	3	4	5	6	7	8
Təhlükəsizlik mexanizmlərinin nömrəsi	3	1	2	2	3	1	2	3

Şəkil 2.

Xromosomun uzunluğu təhdidlərin sayı n-ə bərabər olduğundan matrisin birinci sətrini yazmamaq olar. Bu zaman təhdidin nömrəsi kimi lokus (genin mövqeyi) götürülür (şəkil 3, $x_{21} = x_{61}$, $x_{31} = x_{41} = x_{71} = 1$, $x_{11} = x_{51} = x_{81} = 1$, digər dəyişənlər sıfra bərabərdir).

Xromosom	3	1	2	2	3	1	2	3

Şəkil 3.

Başlanğıc populyasiyanın generasiyası. Başlanğıc populyasiya təsadüfi generasiya edilir. Generasiya prosesi zəruri miqdarda xrosom generasiya edilənə kimi təkrarlanır. Xromosonların sayı çox olduqda populyasiyada optimal həllin əldə edilməsi ehtimalı artır, lakin bu halda böyük hesablama resursları tələb edilir.

$$f(X_k) = \max_j f_j(X_k), \qquad (16)$$

burada $f_j(X_k)$ – j-ci mexanizmin X_k xromosomuna uyğun qalıq riskdir, $k = 1,\ldots,n$ və N – populyasiyadakı xromosomların sayıdır.

Bütün $X = (X_1,\ldots X_N)^T$ populyasiyasının uyğunlaşma funksiyası aşağıdakı kimi müəyyən ediləcək:

$$F(X) = \min_k f(X_k). \quad (17)$$

Seleksiya operatoru. Seleksiya operatorunun köməyi ilə cari populyasiyadan yeni populyasiya alınır, bu və ya digər xromosomun yeni populyasiyada iştirakı uyğunlaşma funksiyasının qiyməti ilə müəyyən edilir. Seleksiya operatorunun çox sayda müxtəlif növləri var: ruletka (roulette-wheel selection), mütənasib seçmə (proportional selection), turnir (tournament selection), kəsik (truncation selection), ranq üzrə seçmə (ranking selection). Təklif edilən metodda ranq üzrə seçmə istifadə edilir.

Çarpazlaşma operatoru. Uşaq-xromosomların generasiyası zamanı yalnız iki valideynin iştirak etdiyi ənənəvi birnöqtəli, ikinöqtəli, çoxnöqtəli və bircins çarpazlaşma operatorları ilə yanaşı, qeyri-klassik çarpazlaşma operatorları da mövcuddur - GOX (Generalized Order Crossover), PPX (Precedence Preservative Crossover), PMX (Partialy Mapped Crossover) və ya GPMX (Generalized PMX) və tsiklik çarpazlaşma operatorları (cycle crossover).

Uşaq-xromosomların generasiyası zamanı ikidən çox valideyn iştirak edən çarpazlaşma operatorları da istifadə edilir.

Bu işdə PMX operatoru istifadə edilir. PMX çarpazlaşma operatoru xromosomun strukturunu pozmur. Başqa sözlə, əgər xromosom mümkündürsə, PMX operatorunun təsirindən sonra da mümkün olan xromosom alınır.

Mutasiya. Mutasiya xromosomun istənilən geninin (bitinin) təsadüfi (verilmiş kiçik ehtimalla) dəyişməsidir (inversiyasıdır). Adətən mutasiya ehtimalı $1/n$-ə yaxın götürülür, burada n – xromosomun genlərinin sayıdır. Mutasiya populyasiyanın genefondunu zənginləşdirir (müxtəlifliyi artırır) və alqoritmin vaxtından əvvəl yığılmasının (staqnasiyanın) qarşısını alır, lokal ekstremumdan çıxmağa kömək edir.

Dayanma meyarı. Əgər müəyyən sayda r^* iterasiya (nəsil generasiyası) ərzində (bu say əvvəlcədən verilib) ən yaxşı uyğunlaşma funksiyasının qiymətində nəzərə çarpacaq yaxşılaşma baş verməzsə, daha doğrusu, iki ən yaxşı uyğunlaşma qiyməti arasındakı fərq əvvəlcədən verilmiş səviyyəni aşmırsa, $|F_{r+r^*} - F_r| \langle \delta$, onda genetik alqoritm işini dayandırır.

Praktikada digər kriteriyalardan da istifadə olunur. Məsələn, nəsil generasiyasının (iterasiyanın) sayı əvvəlcədən verilir. Bu iterasiya ərzində tapılmış ən yaxşı həll qoyulmuş məsələnin həlli kimi qəbul edilir.

Nəticə

Məqalədə informasiya təhlükəsizliyi risklərinin genetik alqoritm vasitəsi ilə optimal idarə edilməsi metodu təklif edilir. Risk amillərinin parametrləri – təhdidin gerçəkləşməsi ehtimalı və ziyanın həcmi, riskin qiyməti və təhlükəsizlik mexanizmlərinin effektivliyi qeyri-səlis mənsubiyyət funksiyaları ilə ifadə olunur. Qalıq riskin minimumlaşdırılması üçün verilmiş büdcə daxilində təhlükəsizlik mexanizmlərinin optimal seçilməsi məsələsi riyazi şəkildə ifadə edilir və onun genetik alqoritm ilə həlli üçün zəruri olan həllin kodlaşdırılması, ilkin populyasiyanın generasiyası, seçmə, çarpazlaşma və mutasiya əməliyyatları təyin olunur.

Minnətdarlıq

Müəlliflər bu məqalənin hazırlanması zamanı faydalı müzakirələri, şərhləri və təklifləri ilə məqalənin təkmilləşdirilməsinə xüsusi kömək göstərmiş f.-r.e.n. R.M.Alıquliyevə dərin minnətdarlıqlarını bildirirlər.

Ədəbiyyat

1. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: ДМК Пресс, 2004, 384 с.
2. ISO Guide 73:2009 - Risk Management – Vocabulary, 2009.
3. ISO/IEC 27005:2007, Information Technology – Security Techniques – Information Security Risk Management, November 2007.
4. Алгулиев Р.М., Имамвердиев Я.Н., Деракшанде С.А. Пути повышения точности методов оценки рисков информационной безопасности // Информационные технологии, 2010, № 12.
5. 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.
6. Barber B., Davey J. The use of the CCTA Risk Analysis and Management Methodology CRAMM // Proc. MEDINFO92, Amsterdam, North Holland, 1992, pp.1589-1593.
7. Alberts C.J., Behrens S. G., et al. Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Framework. Pittsburg, Carnegie Mellon, 1999, pp.1-69.
8. Buyens K., De Win B., Joosen W. Empirical and Statistical Analysis of Risk Analysis-driven Techniques for Threat Management / Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES'07), Vienna, Austria, 2007, pp. 1034-1041.
9. Деревянко П.М. Сравнение нечеткого и имитационного подхода к моделированию деятельности предприятия в условиях неопределенности // Сов. проблемы экономики и управления народным хозяйством: Сб. науч. статей. СПб.: СПбГИЭУ, 2005, с.289-292.
10. Недосекин А.О. Нечеткий финансовый менеджмент. М.: Аудит и финансовый анализ, 2003, 184 с.
11. Недосекин А.О. Нечетко-множественный анализ риска фондовых инвестиций. СПб.: Сезам, 2002, 181 с.
12. Karimi I., Hüllermeier E. Risk Assessment System of Natural Hazards: A New Approach Based on Fuzzy Probability // Fuzzy Sets and Systems, 2007, v.158, № 9, pp. 987-999.
13. Dikmen I., Birgonul M. T. Han S., Using Fuzzy Risk Assessment to Rate Cost Overrun Risk in İnternational Construction Projects // International Journal of Project Management, 2007, v.25, № 5, pp. 494-505.
14. Alguliev R.M., Imamverdiev Y.N., About One Method of Risk Measurement of Maintenance of Information Security of Corporative Networks Because of Fuzzy Sets / Proc. of the 4-th International Conference on New Information Technologies, Minsk, Belarus, 2000, pp.76-81.

15. Авдошин А.С. Оценка защищенности информационной системы методами нечеткой логики // Вестн. Самар. гос. техн. ун-та, 2005, № 32, с.191-193.
16. Балашов П.А., Кислов Р.И., Безгузиков В.П. Оценка рисков информационной безопасности на основе нечеткой логики // Безопасность компьютерных систем. Конфидент, 2003, № 5, с. 56-59.
17. Доценко С.М., Зайчиков А.А., Малыш В.Н. Повышение объективности исходных данных как альтернатива методу нечеткой логики при оценке риска информационной безопасности // Защита информации. Конфидент, 2004, № 5, с. 83-85.
18. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. Пер. с англ., М.: Мир, 1976, 165 с.
19. 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.
20. Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решений на основе нечетких моделей. Примеры использования. Рига: Зинатне, 1990, 184 с.
21. Supervisory framework for the use of «backtesting» in conjunction with the internal models approach to market risk capital requirements. Basel Committee on Banking Supervision, 1996, 15 p. http://www.bis.org/publ/bcbs22.htm
22. Wang J., Chaudhury A., Rao H.R., Research Note – A Value-at-Risk Approach to Information Security Investment // Information Systems Research, 2008, v.19, №1, pp.106-120.
23. Qi W., Liu X., Zhang J., Yuan W. Dynamic Assessment and VaR-based Quantification of Information Security Risk // Proc. of the 2nd International Conference on e-Business and Information System Security (EBISS), Wuhan, China, 2010, pp.1-4.
24. Корт С.С. Теоретические основы защиты информации: Учебное пособие. М.: Гелиос АРВ, 2004, 240 с.
25. Завгородний В.И. Системное управление информационными рисками: выбор механизмов защиты // Проблемы управления, 2009, № 1, с.53-58.
26. Holland J.H., Adaptation in Natural and artificial Systems. The University of Michigan Press, Ann Arbor, 1975, 218 p.
27. Kureichik V.M. Genetic algorithms: state of the art, problems and perspectives // Journal of Computer and Systems Sciences International, 1999, v.38, № 1, pp.137-152.
28. Herrera F., Lozano M. Fuzzy adaptive genetic algorithms: design, taxonomy, and future directions // Soft Computing, 2003, v.7, №8, pp.545-562.
29. Cordon O., Gomide F., Herrera F., Hoffmann F., Magdalena L. Ten years of genetic fuzzy systems: current framework and new trends // Fuzzy Sets and Systems, 2004, v.141, № 1, pp.5-31.
30. Алгулиев Р.М. Алыгулиев Р.М. Генетический подход к оптимальному назначению заданий в распределенной системе // Искусственный интеллект, 2004, № 4, с. 79-88.
31. Алгулиев Р.М., Алыгулиев Р.М. Быстрый генетический алгоритм решения задачи кластеризации текстовых документов // Искусственный интеллект, 2005, №3, с.698-707.

УДК 004.056

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

Оптимальное управление рисками информационной безопасности на основе генетического алгоритма

Предлагается математическая модель для оптимального управления рисками информационной безопасности. Параметры факторов риска и эффективность механизмов защиты выражены через соответствующие функции принадлежности. Предложенный метод решает задачу оптимального выбора механизмов защиты для минимизации остаточных рисков при заданном бюджете. Оптимальный выбор формализован как задача целочисленного программирования, и для ее решения предложен генетический алгоритм.

Ключевые слова: *информационная безопасность, факторы риска, оценка риска, управление рисками, нечеткое число, генетический алгоритм.*

İmamverdiyev Y.N.[1], Derakshandeh S.A.[2]
Institute of Information Technology ANAS, Baku, Azerbaijan
[1]yadigar@lan.ab.az, [2]smdk364@yahoo.com

Optimal information security risk management based on genetic algorithm

The paper proposes a mathematical model for optimal management of information security risks. The parameters of the risk factors and the effectiveness of security mechanisms are expressed by fuzzy membership functions. The proposed model solves the problem of optimal selection of security mechanisms for residual risk minimization at the given budjet. The optimal selection is formulated as a integer programming problem (IPP) and a genetic algorithm is proposed to solve the IPP

Keywords: *information security, risk factors, risk assessment, risk management, fuzzy number, genetic algorithm.*