AXBOROT XAVFSIZLIGINI QATTIYMAS MANTIQ ASOSIDA TAHLIL QILISH

K.I. Kalimbetov[1], A.E. Bekturdiev[2], M.B. O‘rozboyeva [3]

[1]Ajiniyoz nomidagi NDPI, dotsent

[2]Muhammad al-Xorazmiy nomidagi TATU Nukus filiali, assistent

[3]Muhammad al-Xorazmiy nomidagi TATU Nukus filiali, 2-kurs magistarnti

Annotastiya

Qattiymas mantiqdan foydalanilgan holda axborot xavfsizligini tahlil qilish zamonaviy bilimlar berish, malakalarini shakllantirish, olingan bilimlarni ijodiy qo‘llash zamonaviy ta’limning asosiy masalalaridan biridir. Ushbu maqalada Sezarning shifrlash va Vijinerning shifrlash qiymatlariga qarab, Matlab dasturiy vositasi asosida qattiymas mantiqdan foydalanilgan holda axborot xavfsizligini tahlil qilish taxminini hisoblab chiqadi.

Kalit so’zlar: Qattiymas mantiq, sub’ektiv, lingvistik, a’lo, yaxshi, o‘rta, axborot xavfsizligi, qaror qabul qilish.

Asosiy qism: Qat’iymas to’plam tushinchasi insonlar bilan lingvistik qiymatlar va aniq bo‘lmagan sonlar formasida ifodalanadigan sifatli baholashlarni matematik ko‘rsatish imkoniyatini vujudga keltiradi. 1959-yili Iranli professor Lyutfi Zade matematika sahosida FUZZY (rus tilida nechyotkaya matematika, o‘zbek tilida ikki terminda ishlatiladi naravshon yoki qa’tiymas deyiladi) tushinchasini alib kiragan [1-2].

Fuzzy Logic - bu ma‘lumotlardagi noaniqlik va noaniqlik bilan shug‘ullanadigan matematik yondashuv. Bu sizga ma‘lumot noaniq yoki qisman mavjud bo‘lgan sharoitlarda fikrlash va qaror qabul qilishni simulyatsiya qilish imkonini beradi. Klassik ikkilik mantiqdan farqli o‘laroq, o‘zgaruvchilar faqat ikkita qiymatni qabul qilishi mumkin - rost (1) yoki noto‘g'ri (0), loyqa mantiq 0 dan 1 gacha bo‘lishi mumkin bo‘lgan a‘zolik darajasidan foydalanadi. Loyqa mantiqning asosiy tushunchalari quydagisha [3].

Loyqa to‘plamlar - Klassik mantiqda elementlar to‘plamga tegishli yoki ular yo‘q. Loyqa mantiqda to‘plamdagi elementning a’zolik darajasi 0 dan 1 gacha bo‘lgan raqam bilan ifodalanadi [4].

A’zolik funktsiyalari – biz a’zolik funktsiyalarini uchburchakli tegishlilik funkstiyasi orqali axborot xavfsizligini qat’iymas mantiq usullari bilan modellashtirish va qaror qabul qilishnihg bitta holatini keltirib o‘tamiz.

Materiallar va uslublar: Masalan, bunday ma’lumotlar sirasiga axborot xavfsizligini lingvistik baholariga doir ma’lumotlar kiradi. Ixtiyoriy turdagi ma’lumotlarga, xususan qat’iymas ko’rinishdagi ma’lumotlarga ishlov berishning samarali uslubi – qat’iymas mantiq usulidir.

Qattiymas mantiqdan foydalanilgan holda axborot xavfsizligini aniqlashda quyidagicha qat’iymas o‘zgaruvchilarni kiritishimiz mumkun:

x_1 = {*Sezarning shifrlash tizimi*}, x_2 = {*Vijinerning shifrlash tizimi*}.

Sezarning shifrlash tizimi: Sezarning shifrlash usuli oddiy almashtirish shifrining xususiy holidir. Bu usulda alfavitning har bir harfi *K* songa surilgan harfga almashtirilgan. Surilish alfavit oxiriga yetganda, uning boshidan boshlangan. Sezar *K*=3 bo‘lgan siljitishni qo‘llagan.

Vijinerning shifrlash tizimi: XVI asrda fransuz diplomati Vijiner tomonidan yaratilgan shifrlash tizimi 1586 yilda chop etilgan. U mashhur ko‘p alfavitli tizim hisoblanadi [5].

Yuqoridagi axborot xavfsizligini shifrlash tizimi vektorlar bo‘yicha qaralib chiqiladi va quyidagicha yozishimiz mumkin:

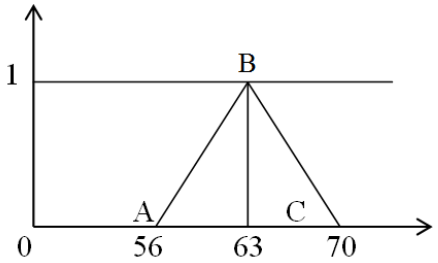
$T(x_1)=\left(t_{x_{1_1}}, t_{x_{1_2}}, t_{x_{1_3}}\right)$, bunda $t_{x_{1_1}}$ – {*quyi darajada*}, $t_{x_{1_2}}$ – {*yaxshi darajada*}, $t_{x_{1_3}}$ – {*oliy darajada*}.

$T(x_2)=\left(t_{x_{2_1}}, t_{x_{2_2}}, t_{x_{2_3}}\right)$, bunda $t_{x_{2_1}}$ – {*quyi darajada*}, $t_{x_{2_2}}$ – {*yaxshi darajada*}, $t_{x_{2_3}}$ – {*oliy darajada*}.

Axborot xavfsizligini tahlil qilish (x_1, x_2) qattiymas mantiqdan foydalanilgan holda aniqlaymiz va uchta turga ajratib baholashimiz mumkin.

Bunda "*a'lo*", "*yaxshi*", "*o'rta*", "*qoniqarli*", "*qoniqarsiz*" lingivistik o'zgaruvchilar uchun ballar taqsimoti bo'yicha uchburchakli tegishlilik funkstiyasi quriladi (1-3 rasmlar).

$$\mu(x_i)=\begin{cases} 0, & c_i \le x \le a_i \\ \dfrac{x-a_i}{b_i-a_i}, & a_i \le x \le b \\ \dfrac{c_i-x}{c_i-b_i} & b_i \le x \le c_i \end{cases}$$



1-rasm. "*O'rta*" bahoning uchburchakli tegishlilik funkstiyasi.

Rasmga ko'ra *A(56;0), B(63;1), C(70;0)* deb olish mumkin.

AB: $\dfrac{x-56}{63-56}=\dfrac{x-0}{1-0}, \quad \mu_{AB}=\dfrac{x-56}{7} \quad \mu_{AB}(56)=0, \quad \mu_{AB}(63)=1$

CB: $\dfrac{x-70}{63-70}=\dfrac{y-0}{1-0}, \quad \mu_{AB}=\dfrac{70-x}{7} \quad \mu_{CB}(70)=0, \quad \mu_{CB}(63)=1, \quad U_1=\{56;70\}.$

O'rta baho {56; 70} universumni tashkil etadi. Bunda, baho {56; 70} ga qanchalik yaqin bo'lishiga qarab, o'rta darajaning mustaxkam yoki bo'sh asosolangani xaqida fikr yuritish mumkin. U_1 universumda o'rta daraja

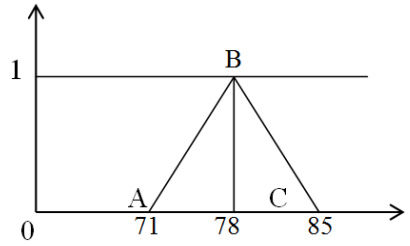
a_1 – {*quyi darajada*}, a_2 – {*yaxshi darajada*}, a_3 – {*oliy darajada*}.

kabilar asosida aniqlashtiriladi va o'rta baho $a_1 \to a_2 \to a_3$ sxema asosida aniqlanadi. Bundan, $P(a_1 \to a_2 \to a_3)=P(a_1)\cdot P_{a_1}(a_2)\cdot P_{a_1 \to a_2}(a_3)$ konstrukstiyaga kelish mumkin, ya'ni shifrlash tizimi o'rtacha va a_1 asosida tavsiflansa, to'g'ridan-to'g'ri a_1 dan a_3 ga o'tish o'rinli emas. Shuning uchun $a_1 \to a_2 \to a_3$ bosqichni amalga oshiramiz va quyidagi echimlarni ishlab chiqamiz:

$a_1 \to a_2$: – {bir xil harflarning o'z navbatida bir xil harflarga almashish, matn tezgina rasshifrovka qilish};

$a_2 \to a_3$: – {kalit harfdan harfga almash, ko‘p alfavitli almashtirish shifrini shifrlash}.

A’lo hamda yaxshi daraja uchun lingvistik o‘zgaruvchilar va echimlar yuqoridagi o‘rta daraja uchun keltirilgan lingvistik o‘zgaruvchilar va echimlar kabi keltiriladi.

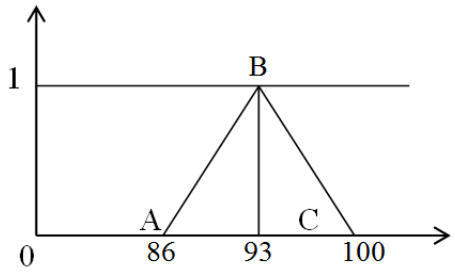


2-rasm. “*Yaxshi*” darajaning uchburchakli tegishlilik funkstiyasi.

AB: $\frac{x-71}{78-71}=\frac{y-0}{1-0}$ $\mu_{AB}=\frac{x-71}{7}$, $\mu_{AB}(71)=0$, $\mu_{AB}(78)=1$

CB: $\frac{x-85}{78-85}=\frac{y-0}{1-0}$ $\mu_{AB}=\frac{85-x}{7}$, $\mu_{CB}(85)=0$, $\mu_{CB}(78)=1$

U_2: yaxshi daraja, $U_2=\{71;85\}$;



3-rasm. “Alo” darajaning uchburchakli tegishlilik funkstiyasi.

AB: $\frac{x-86}{93-86}=\frac{y-0}{1-0}$ $\mu_{AB}=\frac{x-86}{7}$, $\mu_{AB}(86) = 0$, $\mu_{AB}(93) = 1$

CB: $\frac{x-100}{93-100}=\frac{y-0}{1-0}$ $\mu_{AB}=\frac{100-x}{7}$, $\mu_{CB}(100) = 0$, $\mu_{CB}(93) = 1$

U_3: a’lo baho, $U_3=\{86;100\}$.

Xulosa: Qat’iymas ma’lumotlarning ko‘pligi sharoitida Matlab dasturiy vositasi asosida qattiymas mantiqdan foydalanilgan holda axborot xavfsizligini tahlil qilishning tuzilishi qaror qabul qilish tizimining shakliga muvofiq kreativ fikrlashlarini shakllantirishning ahamiyatli ekanligini bevosita hisobga olish orqali FUZZY qoidalarini integrativ qo‘llash asosida imkonini yaratadi.

Foydalanilgan adabiyotlar

1. Ilalovich, K. K. (2022). The Structure of the Nonlinear-Cumulative Model of Students’ Assessment. European Journal Of Innovation In Nonformal Education, 2(1), 147-150.

2. Seitnazarov, K. K., & Kalimbetov, K. I. (2021). Informatika fanini o’qitishda samarali metodlarni tanlab olishda qarorlar qabul qilish tizimi. Academic research in educational sciences, 2(CSPI conference 1), 755-759.

3. Tahirov Behzod Nasriddinovich Axborot xavfsizligi asoslari. "FAN VA TA`LIM" nashriyoti Buxoro-2022

4. Makarenko S. I., Informatsionnaya bezopasnost. Uchebnoe posobie. Stavropol, 2009.

5. Michael Ye. Whitman. Herbert J. Mattord. Principles of Information Security, Fourth Edition. Course Technology, Cengage Learning. 2012.