NORMATOV Sh.B.
RAXMATULLAYEV M.A.

ELEKTRON KUTUBXONALAR AXBOROT XAVFSIZLIGI

NORMATOV Sh.B, RAXMATULLAYEV M.A.

ELEKTRON KUTUBXONALAR AXBOROT XAVFSIZLIGI

Toshkent 2021

UO'K: 02:005.992.1 (075)
KBK: 78ya73
N 79

Normatov Sh.B., Raxmatullayev M.A.
Elektron kutubxonalar axborot xavfsizligi. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti. Toshkent. "KALEON PRESS". 2021 yil. 130 bet.

Мухаммад ал-Хоразмий номидаги ТАТУ Илмий техник кенгашининг 2021 йил 25 июндаги 5-21-сонли йиғилишида маъқулланган.

Ushbu monografiyaning asosiy maqsadi elektron kutubxonalarda axborot xavfsizligini ta'minlash muammolarni bartaraf etish masalalari hamda ularning hozirgi holatini tahlil qilgan holda axborot kutubxona tizimlari, elektron kutubxonalar, arxiv va axborot resurs markazlarida ma'lumotlarni himoyalash bo'yicha tavsiyalar berishdan iborat. Shuningdek, himoyalanuvchi resurslar muhimliligini baholash, resurslarga nisbatan bo'lishi mumkin bo'lgan tahdidlarni aniqlash hamda tahdidlarga qarshi himoya choralarini tavsiya etish bo'yicha ekspert tizimini yaratishga doir tadqiqotlar keltirilgan.

Monografiya kutubxona, arxiv, axborot resurs markazlari xodimlari, axborot kutubxona tizimlari sohasida faoliyat yurituvchi o'qituvchilar, tadqiqotchilar va talabalar uchun mo'ljallangan.

ISBN 978-9943-7432-3-6

MUNDARIJA

Qisqartmalar ro‘yxati

AX – axborot xavfsizligi;
AXT – axborot xavfsizligini ta’minlash;
ARM – axborot resurs markazi;
AKM – axborot kutubxona markazi;
DT – dasturiy ta’minot;
KAKT – korporativ axborot kutubxona tarmoqlari;
MB – ma’lumotlar bazasi
NMM – noravshan moslik modeli;
NT – noravshan to‘plam;
ITT – ilmiy-texnik va ta’limga oid.

KIRISH

Ma’lumki, kutubxonalar insoniyatning ming yillar davomida rivojlanib kelayotgan urf-odatlari, madaniy me’roslari, ijod va fanning turli sohalariga oid axborolarni saqlash orqali kelajak avlodga yetkazishda hamda davlat va jamiyatning rivojlanishida muhim ahamiyatga ega bo‘lib kelgan. Kompyuter texnologiyalarining rivojlanib borishi ko‘pgina sohalar kabi kutubxona jarayonlarini ham avtomatlashtirishga o‘zining ijobiy ta’sirini ko‘rsatdi. Natijada bir qancha qulay imkoniyatlarni taqdim etuvchi avtomatlashtirilgan kutubxona tizimlari yaratildi va yaratilmoqda. Bunday kutubxonalar axborot resurslariga masofadan turib murojaat qilish mumkinligi, qidirib topish tezligining keskin oshishi, vaqt va makon chegaralarining yo‘qligi evaziga foydalanuvchilarga ularning geografik joylashuvidan qat’iy nazar, onlayn o‘qish va izlanish imkoniyatlarini yaratdi.

Ma’lumki, elektron kutubxonalarning barcha resurslari ham tekin bo‘lmay, ba’zida axborot elektron kutubxona foydalanuvchilariga ma’lum bir shart evaziga taqdim etiladi. Bundan tashqari ba’zi kontentlar barcha foydalanuvchilar uchun emas, balki ma’lum foydalanuvchilar guruhi uchun mo‘ljallangan bo‘lishi ham mumkin. Bundan ko‘rish mumkinki, elektron kutubxona resurslari xavfsizligini ta’minlash anchayin dolzarb ahamiyatga ega.

Hozirgi vaqtda elektron kutubxonalar ko‘plab imkoniyatlarni taqdim etmoqda va uning foydalanuvchilari soni ham shunga monand ko‘paymoqda. Kutubxonalar xavfsizlik nuqtai nazaridan har bir foydalanuvchilar haqidagi shaxsiy ma’lumotlar, ularning qaysi mazmundagi adabiyotlardan foydalangani, qidiruv tizimiga ko‘proq qanday so‘rovlarni berishi to‘g‘risidagi ma’lumotlarni shakllantirib boradi. Ammo ushbu ma’lumotlarga shaxsiy ma’lumotlar sifatida qarash mumkin bo‘lib, uning kimdir tomonidan nazorat qilinishi foydalanuvchining axborot borasidagi erkinligiga salbiy ta’sir ko‘rsatishi mumkin. Bu esa kubuxona foydalanuvchilarining shaxsiy, shu jumladan, resurslardan foydalanishi borasidagi statistik ma’lumotlari xavfsizligini ta’minlash yo‘nalishidagi muhim masalalarni keltirib chiqaradi.

Bugungi kunda jahonda, jumladan O‘zbekistonda ham bank, soliq, harbiy sohalardagi davlat organlarining konfidensial axborotlari xavfsizligini ta’minlash bo‘yicha qator usul va vositalar ishlab chiqilgan. Ammo intellektual boylik hisoblangan ilmiy-texnik va ta’limga oid axborotlarni himoyalash muammolari yetarli darajada hal etilmagan.

Ilmiy-texnik va ta’limga oid axborotlar hajmi va muhimliligining oshishi, foydalanuvchilari ko‘lamining kengayishi, shu bilan bir qatorda bunday axborotlardan ruxsatsiz foydalanishga bo‘lgan urinishlarning ortishi ularni himoyalash bilan bog‘liq muammolarni keltirib chiqarmoqda. Masalan, 2017 yilda Web of Science ilmiy ma’lumotlar bazasini Clarivite Analitics kompaniyasi sotib olayotganida u 2.7 mlrd. dollarga baholangan. Yoki bo‘lmasa hozirda O‘zbekistonning birgina Elsevier (Scopus) ilmiy ahborotlar bazasiga obuna narxi 2 mln. dollar, Springer Nature bazasiga kirish bir yilga 300 min dollar tashkil etadi. Bundan ko‘rish mumkinki, ilmiy-texnik va ta’limga oid axborotlar o‘z qiymatiga ega va himoyalashni talab qiladi.

Xavfsizlik elektron kutubxonalarni loyihalashda muhim masala hisoblanadi. Elektron kutubxonalarda axborot xavfsizligini ta’minlash bo‘yicha mavjud kamchiliklar hujumlarni yoki boshqa tipdagi nuqsonlarni vujudga keltirishi yoki saqlanayotgan ma’lumotlar butunligining yo‘qolishiga olib kelishi mumkin. Shu bilan birga foydalanuvchilarining elektron kutubxonada saqlanayotgan kontentga ishonchli kira olishi qanchalik muhim bo‘lsa, elektron kutubxonada saqlanayotgan adabiyotlar mualliflarining intellektual mulk huquqini himoyalash ham shunchalik muhimdir.

Shuni qayd etish lozimki, har qanday axborot tizimining xavfsizligini ta’minlash kompleks xarakterga ega bo‘lib, tizimlarning xususiyatlaridan kelib chiqib usul va vositalarni to‘g‘ri tanlash hamda xavfsizlik siyosatini yuritish muhim ahamiyatga ega. Mamlakatimiz axborot resurs markazlarida hozirgi kunda KaDaTa, IRBIS va ARMAT++ avtomatlashgan kutubxona tizimlaridan foydalanilayotgan bo‘lib, ushbu tizimlarning barchasida axborot xavfsizligini ta’minlash foydalanuvchilarni parol va login asosida autentifikatsiya qilish bilan amalga

oshiriladi. Shuningdek, ushbu tizimlarda foydalanuvchining ma’lumotlarni qidirgan yoki o‘qiganligini o‘z ichiga oluvchi log yoki boshqa fayllarni saqlash imkoniyati mavjud bo‘lib, foydalanuvchilar haqidagi ma’lumotlarni shifrlanmaydi.

Umuman olganda ochiq axborotni himoyalanuvchi axborotlar sirasiga kiritishda eng asosiy mezon uning bahosi hisoblanadi. Chunki aynan axborotning bahosi uni qanchalik darajada himoyalash zarurligini ko‘rsatadi. Axborotning bahosini aniqlash ustida olib borilgan tadqiqotlar axborotning muhim strategik aktiv ekanligini ko‘rsatadi [77]. Aslida axborot, agar tashkilot uchun qiymatga ega bo‘lsa unga aktiv sifatida qarash mumkin. Masalan, hozirda keng ko‘lamda faoliyat olib borayotgan Web of Science, Scopus, EBSCO, Emeraldinsight, Springer kabi yirik ilmiy-tahliliy axborot bazalari ularning egalari uchun muhim moliyaviy ahamiyatga ham ega.

Mazkur monografiyada elektron kutubxonalarda saqlanuvchi resurslar muhimliligini baholash hamda ularning xavfsizligi ta’minlashga doir tadqiqot natijalari keltiriladi.

Ushbu monografiyaning asosiy maqsadi elektron kutubxonalarda axborot xavfsizligini ta’minlash muammolarni bartaraf etish masalalari hamda ularning hozirgi holatini tahlil qilgan holda korporativ axborot kutubxona tizimlari, elektron kutubxonalar, arxiv va axborot markazlarida ma’lumotlarni himoyalash bo‘yicha tavsiyalar berishdan iborat.

Monografiya kutubxona, arxiv, axborot markazlari xodimlari, axborot kutubxona tizimlari sohasida faoliyat yurituvchi o‘qituvchilar, tadqiqotchilar va talabalar uchun mo‘ljallangan.

I BOB. FAN VA TA’LIMGA OID RESURSLARNI BAHOLASH VA ULARNI HIMOYALASH USULLARI VA VOSITALARI TAHLILI

1.1. Fan va ta’limga oid resurslarni baholash va ularni himoyalashning asosiy tushunchalari va zamonaviy holati

Ilmiy-texnik va ta’limga oid (ITT) axborotlar va bilimlar davlatning strategik resurslaridan biriga aylanib ulgurdi va ulardan foydalanish davlatning ijtimoiy-iqtisodiy rivojlanishga o‘z ta’sirini ko‘rsatmoqda [34; 23-b.]. ITT resurslar deganda kutubxonalar, axborot resurs markazlari, patent idoralari va axborot markazlaridagi barcha turdagi ilmiy-texnik va ta’limga oid resurslar kabi litsenzion axborotlar nazarda tutiladi.

Kompyuter texnologiyalarining rivojlanib borishi ko‘pgina sohalar kabi kutubxona jarayonlarini ham avtomatlashtirishga o‘zining ijobiy ta’sirini ko‘rsatib, natijada bir qancha qulay imkoniyatlarni taqdim etuvchi avtomatlashtirilgan kutubxona tizimlari yaratilgan [86; 83-b.] va ular doimiy takomillashtirilib borilmoqda. Ayniqsa, keyingi vaqtlarda elektron kutubxonalardan foydalanish borasida katta o‘sish kuzatildi [79]. Biroq kompyuter tarmoqlarida aylanayotgan axborot oqimlarining keskin ortishi, undan foydalanuvchilar sonining doimiy o‘sib borishi hamda ITT resurslar aktivlik xususiyatining kuchayishi bu turdagi axborotlarning yaxlitligi va foydalana olishligini ta’minlash, foydalanuvchilarning shaxsiy ma’lumotlarini himoyalash muammolarining ham paydo bo‘lishiga olib keldi [49; 837-b.]. Axborot xavfsizligi (AX) aspektlarining bu kabi buzilishi tizimning noto‘g‘ri ishlashi yoki ishlamay qolishiga, foydalanuvchilar ishonchining susayishiga va hatto iqtisodiy yo‘qotishlarga ham sabab bo‘ladi [68; 403-b.].

Bugungi kunda ko‘pgina sohalar kabi kutubxonachilikda ham ayniqsa elektron kutubxonalar rivojlanishi bilan birga axborot xavfsizligini ta’minlash muammosining dolzarbligi yanada ortdi. Bunga sabab qilib quyidagilarni keltirish mumkin:

• Axborot kutubxona tizimlarida va tarmoqlarida saqlanayotgan axborotlar hajmi hamda kutubxona foydalanuvchilari sonining keskin oshib borishi;

• Axborotning muhim ijtimoiy, iqtisodiy strategik aktivlik xususiyatlarining ortishi;

• Axborot xavfsizligini ishonchli ta’minlash vositalari narxining nisbatan qimmatliligi;

• Elektron kutubxonalar xavfsizligini ta’minlashning usullari, vositalari va boshqa ta’minotlarining to‘liq shakllanmaganligi;

• Kutubxona egalari va xodimlarida axborot xavfsizligi bo‘yicha bilim va ko‘nikmalarining yuqori emasligi;

• Ilmiy texnikaning so‘nggi yutuqlaridan xavfsizlik tizimlarini buzishda ham foydalanishning mumkinligi va hakozolar.

Yuqorida keltirilgan masalalar kutubxonalarda axborot xavfsizligini ta’minlash tizimini qurishni taqozo etadi. Ushbu tizimga kutubxona axborotlarining quyidagi xususiyatlarini ta’minlash va doimiy saqlab turishning umumiy talablarlari qo‘yilishi mumkin:

• elektron kutubxonaning qonuniy foydalanuvchilari uchun resurslardan erkin foydalana olishlik;

• axborot tizimlarida qayta ishlanayotgan va saqlanayotgan hamda aloqa kanali bo‘ylab uzatilayotgan kutubxona axborot resurslarining yaxlitligi va haqiqiyligi;

• axborotlarning konfidensialligi,

• shaxsiy ma’lumotlar daxlsizligi.

Elektron kutubxonalarda axborot xavfsizligini ta’minlash (AXT) muammosining dolzarbligi elektron hujjat aylanish va elektron to‘lov tizimlari hamda kutubxona xodimlari va foydalanuvchilarining shaxsiy ma’lumotlarini himoyalash zarurligi bilan bog‘liqdir [89; 21-b.]. Axborot kutubxona tizimi foydalanuvchilari tizimdan qaysidir ma’lumotlarni izlashi, ularni o‘qishi yoki tizimga o‘zi haqidagi konfidensial ma’lumotlarni kiritishi mumkin [50; 53-b.]. Kutubxona etikasiga ko‘ra, bu kabi axborotlar bilan uchinchi tomondagi shaxslarning tanishishi yoki ularga taqdim etish taqiqlanadi [72; 14-b.].

Hozirda axborot kutubxona sohasida faoliyat ko‘rasatib kelayotgan, yirik ilmiy axbortlar bazasiga ega bo‘lgan Auto-Graphics, Biblio Commons, Biblionix, EBSCO, SirsiDynix, OCLC, Ex Libris va Koha kabi axborot tizimlari ma’lumotlarni himoyalash bo‘yicha o‘z yechimlarini qabul qilishgan [72; 13-b.]. Xalqaro va O‘zbekistondagi mavjud axborot-kutubxona tizimlarining qiyosiy tahlili 1.1 va 1.2-jadvallarda keltirilgan.

Ba’zi hollarda ITT resurslarning barchasi ham ochiq bo‘lmay, axborot foydalanuvchilarga ma’lum bir shart asosida taqdim etilishi mumkin [85; 83-b.]. Bu esa resurslarni *ruxsatsiz foydalanishlardan* himoyalash, Ya’ni uning *konfidensialligini* ta’minlash, agar axborot resursi ochiq bo‘lganda ham uning *yaxlitligini* ta’minlash zaruriyatini keltirib chiqaradi. Bundan tashqari ba’zi resurslar barcha foydalanuvchilar uchun emas, balki ma’lum guruhdagilar uchun mo‘ljallangan bo‘lishi ham mumkin [42; 236-b.]. Demak, axborotni ruxsatsiz foydalanishdan himoyalash qanchalik muhim bo‘lsa, unga kirishga vakolatli bo‘lgan foydalanuvchilar uchun axborot resurslaridan foydalana olishlikni ta’minlash ham shunchalik ahamiyatlidir.

ITT axborotlar himoyasini tadqiq etish va uning yangi usullari va vositalarini yaratishning muhimligini quyidagi omillar va tendensiyalar bilan ko‘rsatish mumkin:

– ilmiy axborotlar hajmi va uning foydalanuvchilari sonining keskin oshishi;

– ilmiy-tadqiqotlar natijalarining texnologiyalar, harbiy, iqtisod va biznes hamda ta’lim tizimi rivojlanishiga ta’sir darajasining yuqoriligi;

– ilmiy axborotlar (elektron ilmiy jurnallar, kitoblar, ma’lumotlar bazalari va h k.) va ularga obuna qiymatining oshib borishi;

– lokal va global tarmoqlarda elektron ilmiy resurslarga kirishga mo‘ljallangan zamonaviy axborot texnologiyalari va telekommunikatsiya vositalarining rivojlanishi;

1.1-jadval

Ilg‘or jahon axborot-kutubxona tizimlarining himoya choralaridan foydalanishi bo‘yicha qiyosiy tahlili

	Kutubxona tizimlari / Himoya choralari	Auto-Graphics	Biblio Commons	Biblionix	EBSCO	SirsiDynix	OCLC	Ex Libris
1	Tizimda foydalanuvchi ishtirok etgan har qanday tranzaksiyaning HTTPS bilan shifrlanishi	Yo‘q	Ha	Ha	Ha	Ha	Ha	AES
2	Ma’lumotlarni shifrlashda foydalaniladigan protokollar	TLS 1.2, SSL 3	TLS 1.2	TLS 1.2	TLS1.2 2048 bit	TLS 1.2	TLS 3 SSL	TLS1.2 SHA 256 AES 256
3	Foydalanuvchi ma’lumotlarni qidirgan yoki o‘qiganligini o‘z ichiga oluvchi log yoki boshqa fayllarning shifrlanishi	Yo‘q	Loglar anonimlashti-riladi	Ha	Ha	Boshqa yo‘llar bilan himoya-lanadi	Yo‘q	Ushbu fayllar shaxsiy axborotlar deb qaralmaydi
4	Kutubxona xodimi ishtirok etgan har qanday tranzaksiya HTTPS yoki boshqa mexanizm bilan shifrlanishi	Ha	Ha	Ha, (HTTPS)	Ha, (TLS 1.2)	Ha, (HTTPS)	Ha, (HTTPS)	Ha, (HTTPS)
5	Boshqaruvning moliyaviy axborotlarini o‘z ichiga olgan tranzaksiyalarda	Ha	Ha	Ha	Ha	Ha	Ha	Ha

Himoya choralari / Kutubxona tizimlari		Auto-Graphics	Biblio Commons	Biblionix	EBSCO	SirsiDynix	OCLC	Ex Libris
	shifrlashning qo‘llanilishi							
6	Tashkilotning hamkorlar va xizmat ko‘rstuvchilar bilan aloqalarida xavfsizlikning qaysi choralarini qo‘llashi		Shartnoma tuzadi. OverDrive, 3M Cloud Library, Axis 360, Content Cafe, Zola Books	Ishlab chiqarish ma’lumotlariga uchinchi tomonning kirishiga yo‘l qo‘yilmaydi. SIP protokoli ishlati-ladi				O‘zining xususiy bulut muhiti mavjud va axborotlari umumiy bulutga qo‘yilmaydi
7	Tizimda foydalanuvchilar parol va pin kodlarining shifrlanmagan matn ko‘rinishida saqlanishi	Ha	Yo‘q	Ushbu ma’lumotlar xesh qiymat va shifrlash yordamida saqlanadi	Yo‘q	Ha, xeshla-nadi	Ha, xeshlanadi	Ha, LDAP i SAML2 protokollari ishlatiladi
8	Tizimda saqlanayogan foydalanuvchilar haqidagi ma’lumotlarning shifrlanishi	Yo‘q	Ha	Ha	Ha	Ha	Faqat paroli xeshlanadi	Ha
9	API interfeysining foydalanuvchilar savol yoki javoblarini shifrlashi	Ha, SSL	Ha, HTTPS	Ha	Ha	Yo‘q	Faqatgina ochiq bo‘lmagan API interfeys-larida shifrlash mavjud	Ha, HTTPS

1.2-jadval

O‘zbekistondagi mavjud axborot-kutubxona tizimlarining himoya choralaridan foydalanishi bo‘yicha qiyosiy tahlili

Kutubxona tizimlari / Himoya choralari		KaDaTa	IRBIS	Concourse	ARMAT
1	Ishlab chiqaruvchi	BePro dasturchilar markazi (O‘zbekiston)	EBNIT assotsiatsiyasi (Rossiya)	Book Systems (AQSH)	ARMAT PLUS (O‘zbekiston)
2	Boshqa tizimlar bilan integratsiya qilish imkoniyati	Bor	Bor	Bor	Bor
3	Bibliografik ma’lumot formati	UNIMARC, MARC21, UZMARC	RUSMARC, UNIMARC	US/MARC	MARC21, UZMARC
4	Foydalanuvchi ma’lumotlarni qidirgan yoki o‘qiganligini o‘z ichiga oluvchi log yoki boshqa fayllarning saqlanishi	Mavjud	Mavjud	Mavjud	Mavjud
5	Tizimda foydalanuvchi ishtirok etgan har qanday tranzaksiyaning HTTPS bilan shifrlanishi	Yo‘q	Yo‘q	Bor	Yo‘q
6	Tizimda saqlanayogan foydalanuvchilar haqidagi ma’lumotlarning shifrlanishi	Yo‘q	Yo‘q	Yo‘q	Yo‘q
7	Bitta tashkilot uchun foydalanish narxi	30 mln. so‘m	10 ming AQSH dollori	55 ming AQSH dollori	7.5 mln. so‘m
8	Axborot xavfsizligini ta’minlashning asosiy mexanizmlari	Login va parol asosida autentifikatsiya	Login va parol asosida autentifikatsiya	Login va parol asosida autentifikatsiya	Login va parol asosida autentifikatsiya

– tashkilot rahbarlari va mutaxassislarining mavjud tahdidlar, axborotdan ruxsatsiz foydalanish vositalari va himoya choralaridan yetarli darajada xabardor emasligi [44; 110–111-b.];

– qimmatli ilmiy axborotlarni tarqatish bo‘yicha axborot konsorsiumlar va birlashmalarning rivojlanishi.

Bundan tashqari ITT resurslarning boshqa turdagi axborotlar bilan qiyoslaganda quyidagi xususiyatlari ularning himoyasiga mos yondashuvni talab qiladi:

– ITT axborot resurslari bahosi o‘zgaruvchan. Ya’ni, bunday turdagi axborotlarning bahosi vaqtga bog‘liq holda bir qancha omillar ta’sirida o‘zgarib boradi;

– axborot resurslarining ochiqligi. Ya’ni, bunday axborotlarning ko‘proq konfidensialligi emas, balki ulardan foydalana olishlikni va yaxlitligini ta’minlash talab etiladi;

– turli ko‘rinishlarda taqdim etilishi. Ya’ni, axborot kutubxona tarmoqlarida turli xil muhimlilik darajasiga va foydalanuvchilariga ega bo‘lgan matn, jadval, grafik, audio, video kabi ko‘rinishlardagi axborotlarning mavjudligi [60; 92-b.];

– ilmiy axborotlarning egalari va ularni ishlab chiqaruvchilar o‘rtasidagi raqobatning rivojlanishi;

– ilmiy axborotlarning iqtisodiyot va biznesni yurituvchi muhim omil sifatida qiymatining oshib borishi [52; 35-b.].

Shunday qilib, elektron resurslardan onlayn foydalanish imkoniyatlarining ortishi, AXga bo‘lgan tahdidlarning kuchayishi hamda ishonchli va qimmatli ITT resurslarga bo‘lgan ehtiyojning ortishi ularning xavfsizligini yetarli darajada ta’minlash usul va vositalarini ishlab chiqishni taqozo etadi.

Bugungi kunda hududiy bo‘limlariga ham ega bo‘lgan katta masshtabdagi tashkilotlar o‘zlarining korporativ tarmog‘iga ega bo‘lib, u tashkilot faoliyatining samaradorligi va boshqaruvchanligini oshirishda qator afzalliklarga ega [34].

Jumladan, axborot kutubxona tizimlarida ham korporativ tarmoqlar muhim ahamiyat kasb etadi [64].

Korporativ axborot-kutubxona tarmoqlari (KAKT) uning ishtirokchilariga elektron katalog va to‘liq matnli resurslarni birgalikda samarali shakllantirish, foydalanuvchilarga tarmoq resurslardan keng foydalanishni ta’minlash, ichki korporativ imkoniyatlardan birgalikda foydalanish kabi afzalliklarini taqdim etishi bilan birga resurslar xavfsizligini ta’minlash muammosini ham keltirib chiqarmoqda. KAKT da AXT muammosini tadqiq etish jarayoni, avvalo, KAKTda himoyani talab etuvchi axborotlarni ajratish va ularni tasniflash masalasini yechishni talab qiladi. Keyingi bo‘limda KAKT resursini himoyani talab etuvchi axborotlar qatoriga kiritish omillari va ularning tasnifi keltiriladi.

1.2. Axborot kutubxona tarmoqlarida himoyalanuvchi resurslar tasnifi

1.2.1 Axborot kutubxona tarmoqlarida himoyalanuvchi obyektlar turlari

«Himoya qilinuvchi axborot» tushunchasiga ikki xil yondashuv mavjud. Birinchi yondashuvga ko‘ra, himoyalanuvchi axborot deganda foydalanilishi va tarqatilishiga cheklov uning egasi tomonidan belgilanuvchi ma’lumotlar tushuniladi. Ikkinchi yondashuvga ko‘ra esa himoyalanuvchi axborotlar tarkibiga nafaqat foydalanish cheklangan u yoki bu ko‘rinishdagi maxfiy axborotlar, balki ochiq axborotlar ham kiritiladi [28; 118-b.]. Ochiq axborotlarni himoyalash ulardan foydalanishni cheklash emas, balki ularni qayta ishlash va foydalanishda yaxlitligini, shuningdek foydalana olishligini ta’minlash maqsadida amalga oshiriladi. Ushbu yondashuvga asoslanib, ITT axborotlarni himoyani qilinuvchi axborotlar qatoriga kiritish mumkin.

Bundan tashqari ochiq axborotlarni himoya qilinuvchi axborotlar qatoriga kiritishda axborotning ishlab-chiqarish faoliyati uchun muhimligi (ilmiy-tadqiqot, tajriba-konstruktorlik, texnologik va boshqa sohalarga oid bo‘lgan axborotlar) mezoni ITT axborotlar uchun ham o‘rinlidir [53; 837–838-b.].

Umuman olganda ochiq axborotni himoyalanuvchi axborotlar sirasiga kiritishda uning bahosi eng asosiy mezon bo‘lib xizmat qiladi. Chunki aynan axborotning bahosi uni qanchalik darajada himoyalash zarurligini ko‘rsatadi.

Axborotning bahosini aniqlash ustida olib borilgan tadqiqotlar axborotning muhim strategik aktiv ekanligini ko‘rsatadi [69; 3-b., 77; 81]. Aslida axborot, agar tashkilot uchun qiymatga ega bo‘lsa unga aktiv sifatida qarash mumkin. Masalan, hozirda keng ko‘lamda faoliyat olib borayotgan Web of Science, Scopus, EBSCO, Emeraldinsight, Springer kabi yirik ilmiy-tahliliy axborot bazalari ularning egalari uchun muhim moliyaviy ahamiyatga ham ega. Bu kabi ITT resurslarlarni axborot aktivlari qatoriga kiritish mumkin. Shuning uchun ham ularning himoyasi uchun muayyan choralar ko‘rilgan (1.1-jadvalga qarang).

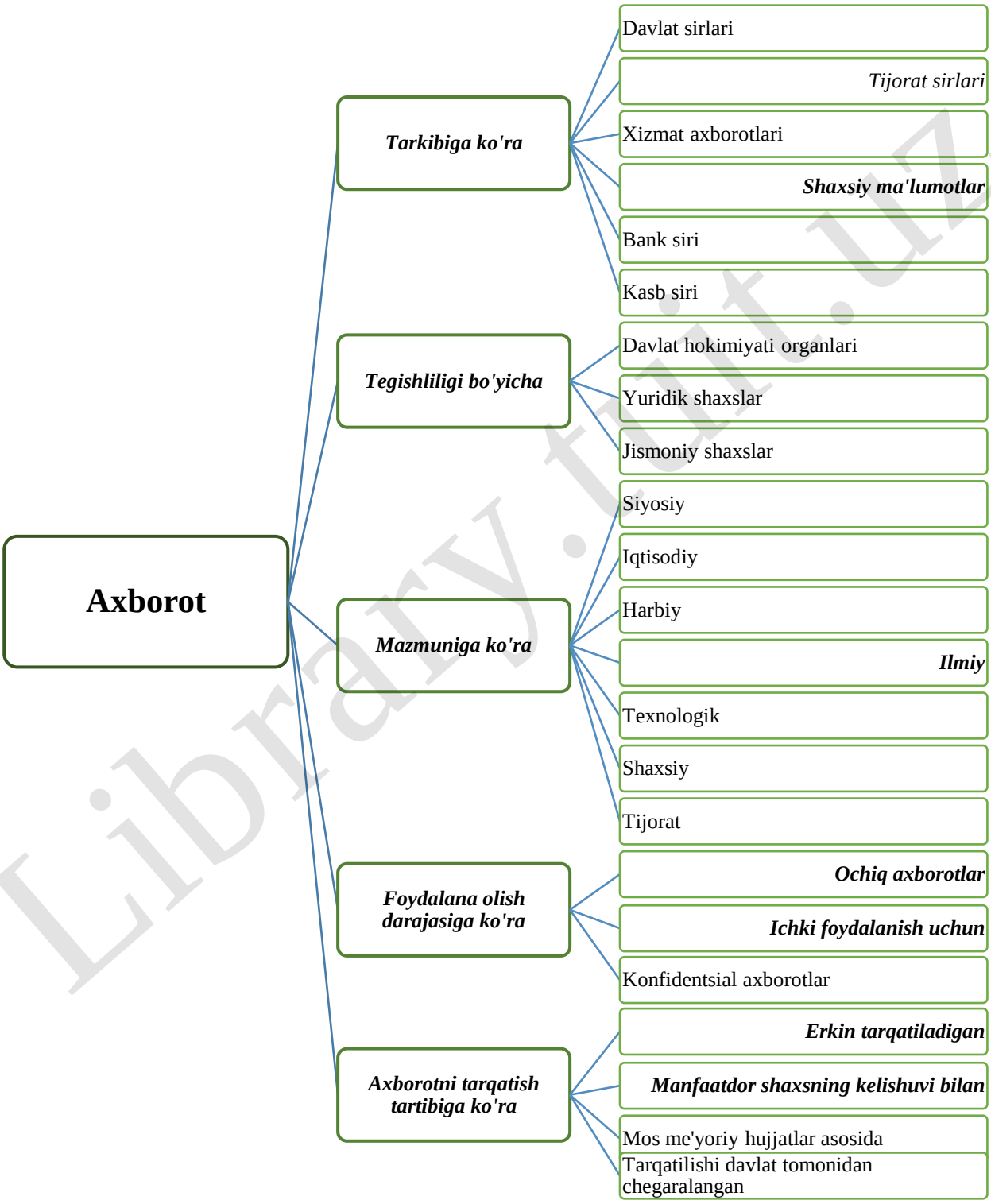
Aslida barcha axborotlarni O‘zbekiston Respublikasining «Davlat sirlarini saqlash to‘g‘risida»gi qonuni va boshqa meyoriy hujjatlarga ko‘ra xavfsizlik nuqtai nazaridan 1.1-rasmda keltirilganidek tasniflash mumkin [51; 14-b.]. Tadqiqot ishida barcha turdagi axborotlar emas, balki faqatgina ITT resurslar xavfsizligini ta’minlash masalasi qaralayotganligi uchun ushbu sinfga oid bo‘lgan axborot turlarini 1.1-rasmning oxirgi ustunda ajratilib ko‘rsatilgan.

1.1-rasmda keltirilganidek, shaxsiy va ilmiy, ochiq va ichki foydalaniladigan hamda erkin va kelishuv asosida tarqatiladigan axborotlarning ayrimlarini ITT axborotlar qatoriga kiritish mumkin. Buning to‘liq tavsifi [49] da keltirilgan.

Ma’lumki, himoya obyektidagi biror resursni himoyalash boshqasining himoyasi bilan uzviy bog‘liqdir [66]. Ya’ni, KAKT axborot resursining xavfsizligini ta’minlash uchun u saqlanayotgan server, tarmoq va boshqa komponentlarning ham xavfsizligini ta’minlash zarurdir. Umumiy holda KAKTdagi himoyalanuvchi resurslarni 1.3-jadvalda ko‘rsatilganidek tasniflash mumkin. Odatda tasniflashning asosiy tamoyillari sifatida axborotning tashkilotga nisbatan bahosi, qonuniy talablari, ta’sirchanligi, ishonchliligi va kritikligi qaraladi [5].

Resurslarning o‘ziga xos talablariga ularning konfidensiallik, yaxlitlik va foydalana olishlik darajalari hamda ularni ta’minlash uchun zaruriy choralar

ko‘rsatiladi. Resursning dastlabki qiymati deganda uni ishlab chiqish, qo‘lga kiritish yoki sotib olish uchun sarf etilgan xarajat qiymati tushuniladi. Shuni qayd etish lozimki, resursning dastlabki qiymati va uning bahosi bir-biridan farq qilishi mumkin.



1.1-rasm. Axborotlarning xavfsizlik nuqtai nazaridan tasniflanishi

1.3-jadval

Korporativ axborot-kutubxona tarmoqlarining himoya obyektlari tasnifi

№	*Resurs tipi*	*Resurs nomi*	*O‘ziga xos talablar*	*Joylashuv o‘rni*	*Dastlabki qiymati (mln, so‘m)*	*Foydalanuvchilar-ning foydalanish huquqi*
Himoya ob’yektlari sinflari						
1	***Axborot resurslari***					
1.1	Maqola	Maqola 1	Konfidensiallik, yaxlitlik va foydalana olishlik darajalari	Serverda	0.2	F1 (R1, R2, t1)
1.2	Dissertatsiya	Dissertatsiya 1		Serverda	0.4	F2 (R1, R3, t2)
. . .	. . .	. . .		. . .	. . .	. . .
2	***Apparat vositalari***					
2.1	Kompyuter	Kompyuter 1	Fizik foydalanish darajasi	Xodim ish o‘rnida	3.2	F1 (R2, t3)
2.2	Server	Server 1		Axborot markazida	6.5	F2 (R1, R3, t2)
. . .	. . .	. . .		. . .	. . .	. . .
3	***Dasturiy ta’minot***					
3.1	Tizimli DT	Linux	Konfidensiallik darajasi	Serverda	10.6	F3 (R3, t4)
3.2	Amaliy DT	ARMAT++		Ishchi stansiyada	3.4	F1, F2, F3, F4 (R1, t5)
. . .	. . .	. . .		. . .	. . .	. . .
4	***Tarmoq qurilmalari***					
4.1	Marshrutizator	Fast Ethernet, Gigabit, Token Ring, 100VGAnyLAN, FDDI	Yaxlitlikni ta’minlash darajasi	Axborot markazida	12.5	F4 (R3, t4)
4.2	Optik tolali	Gigabit Ethernet,		Tarmoq uzellari	4.5	F4 (R1, t5)

Foydalanuvchilarning huquqi ustuniga resurslarga kirishga ruxsat etilgan foydalanuvchilar, ularning kirish huquqlari ro‘yxati va resursdan foydalanish muddati ko‘rsatiladi.

KAKTning barcha himoyalanuvchi resurslarini moddiy va nomoddiy turlarga ajratib, 1.4-jadvaldagidek tasvirlash mumkin. Ko‘rish mumkinki, himoyani talab etuvchi obyektlar hajmi yetarli darajada katta.

1.4-jadval

Axborot kutubxona tarmoqlarida himoya obyektlarining turlari

Himoya obyektlari	
Moddiy	**Nomoddiy**
- jihozlar; - serverlar va tarmoq qurilmalari; - axborot tashuvchilari (qattiq disk, optik disk, flesh xotiralar); - fizik himoya vositalari; - apparat himoya vositalari.	- elektron katalog; - kutubxona resurslarining ma’lumotlar bazasi; - foydalanuvchilar va xodimlarning shaxsiy ma’lumotlari; - tizimli va amaliy dasturiy taminotlar tuzilmalari; - kutubxona veb sayti; - mualliflik huquqi; - elektron xizmatlar.

Shunday qilib, tadqiqot ishida faqatgina KAKTda saqlanayotgan ITT resurslar xavfsizligini baholash masalasi ajratib olindi.

ITT axborotlar AXni baholash muammosini tadqiq etishda bo‘lishi mumkin bo‘lgan tahdidlarni tahlil qilish zaruriy masalalardan biri hisoblanadi. Keyingi bo‘limda KAKTda AXga nisbatan tahdidlar tahlili keltiriladi.

Yuqorida ilmiy-texnik va ta’limga oid axborot resurslarini himoyani talab etuvchi axborotlar toifasiga kiritish omillari tadqiq etildi hamda ular tasniflandi.

1.2.2 Ilmiy-ta’limiy axborot tarmoqlarda resurslar va foydalanuvchilarni tasniflash

Elektron resurslarni umumiy holda ijtimoiy ahamiyatiga ko‘ra rasmiy, ilmiy, ta’limiy, badiiy, ko‘ngilochar, tijorat va reklamaga oid, ilmiy-ommabop, ommaviy-siyosiy va boshqa turlarga bo‘lish mumkin. Quyidagi 1-jadvalda ilmiy axborotlar tasnifi keltirilgan (1.5-jadval).

1.5-jadval.

Ilmiy axborotlar tasnifi

№	***Ilmiy axborotlar***
1.	Monografiya
2.	Ilmiy ishlar to‘plami
3.	Konferensiya materiallari
4.	Ilmiy-tadqiqot va tajriba konstruktorlik hisobotlari
5.	Taqrizlar
6.	Ilmiy maqolalar
7.	Bitiruv ishlari
8.	Magistrlik dissertatsiyalari
9.	Patent va ixtiro hujjalari
10.	Dissertatsiya avtoreferati
11.	Boshlang‘ich doktorlik dissertatsiyalari (PhD)
12.	Dotorlik dissertatsiyalari

Ta’lim, ilm va innovatsion faoliyatlarni informatsion qo‘llab-quvvatlash uchun ta’limiy axborot resurslari muhim ahamiyat kasb etadi. Quyidagi 1.6-jadvalda ta’limiy axborotlar tasnifi keltirilagan.

1.6-jadval

Ta’limiy axborotlar tasnifi

Ta’limiy axborotlar tasnifi				
O‘quv nazariy	***O‘quv uslubiy***	***O‘quv amaliy***	***O‘quv dasturiy***	***O‘quv ma’lumotli***
Darslik	Uslubiy qo‘llanma	Masalalar to‘plami	O‘quv rejalar	Izohli lug‘at
O‘quv qo‘llanma	Uslubiy ko‘rsatma	Praktikumlar	O‘quv dasturlar	Atamashunoslik lug‘ati
Ma’ruzalar matni	O‘quv uslubiy majmua	Testlar	Tematik rejalar	Ensiklopediya

Yuqorida aytilganidek, ushbu ilmiy-ta’limiy axborot resurslari ularning qiymatiga bog‘liq holda turli xil xavfsizlik darajalariga ega. Masalan, ma’ruzalar matni deb qaralayotgan obyektning faqatgina butunligi va unga kira olishligini ta’minlash zarur bo‘lsa, ayrim ilmiy maqolalar bilan tanishish bepul bo‘lmaganligi bois ularning konfidensialligini ham ta’minlash talab qilinadi. Demak, elektron kutubxona axborot resurslarining butunligi va konfidensialligi ta’minlash, foydalanuvchilarning resurslarga kirishini samarali amalga oshirish uchun kutubxona resurslaridan foydalanuvchilar – subyektlarni ham guruhlarga ajratish lozim.

Ilmiy-talimiy axborot resurslaridan foydalanuvchilar – subyektlar kategoriyalari 1.7-jadvalda keltirilgan.

1.7-jadval

Ilmiy-ta’limiy axborot resurslardan foydalanuvchilar kategoriyalari

№	Foydalanuvchi turi	Foydalanuvchi maqsadi
1.	Olimlar	*Ilmiy axborotlarga kirish, xamkorlar qidirish, mablag‘ bilan ta’minlashga tavsiyalar ishlab chiqish*
2.	Professor-o‘qituvchilar	*Ilmiy tadqiqot ishlarini olib borish, adabiyotlar bilan tanishish*
3.	Talabalar	*Ilm va texnika yutuqlari bilan tanishish*
4.	Investorlar va sanoat vakillari	*Istiqbolli ilmiy ishlanmalarni va yangi texnologiyalarni izlash uchun. Shuningdek, ekspertlar, yangi ilmiy natijalar va texnologiyalarni baholash, ularni ishlab chiqarishga joriy etishga ko‘maklashish*
5.	Davlat boshqaruvi organlari rahbarlari va xodimlari	*Ilm-fanni boshqarish, ilm-fan rivojida olimlar va ilmiy muassasalar rolini aniqlash*
6.	Fuqarolar	*Ilm va texnika yutuqlari bilan tanishish*
7.	Huquqlarni boshqaruvchi ma’mur	*Tizim faoiyatini to‘liq boshqarish*
8.	Kataloglashtiruvchi	*Elektron katalogni shakllantirish*
9.	Komplektlovchi	*Bibliografik ma’lumotlar bilan ishlash*
10.	Kutubxonachi	*Kitoblarni berish va qaytarib olish*

Yuqorida ta’kidlanganidek, axborot resursi xavfsizligini ta’minlashda kirishlarni boshqarish asosiy masalalardan biri hisoblanadi. Kirishlarni boshqarish uchun subyektlarning obyektlarga kirish huquqlarini belgilab olish lozim.

Foydalanuvchilarning qayd yozuvlarini shakllantirish jarayonida ularning obyektlardan foydalanish huquqlari aniq belgilanadi. Kirish huquqlarini belgilashda asosiy omil hisoblangan obyekt va subyekt o‘rtasidagi munosabatlarni quyidagicha keltirish mumkin (1.8-jadval).

1.8-jadval

Obyekt va subyekt o‘rtasidagi munosabatlar

Муносабат номи	**Шартли белги**
Объектга киришга рухсат йўқ	0
Маълум қисмни ўқиш	1
Ўқиш	2
Маълум қисмдан нусха олиш	3
Нусха олиш	4
Ўчириш	5

Quyidagi jadvalda axborot kutubxona tizimi obyektlariga subyektlarning kirish huquqlari bo‘yicha tasnifi keltirilgan (1.9-jadval).

1.9-jadval

Obyektlar va subyektlarning o‘zaro munosabatga ko‘ra tasniflanishi

Resurslar	Subyektlar / Obyektlar	Olimlar	Professor-o‘ qituvchilar	Talabalar	Investorlar va sanoat vak.	Davlat boshqaruvi organlari rahbarlari va xodimlari	Fuqarolar	Kataloglashtiruvchi	Komplektlovchi	Kutubxonachi	Huquqlarni beruvchi admin
Ilmiy	Monografiya	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-5
	Ilmiy ishlar to‘plami	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-5
	Konferensiya materiallari	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-5
	Ilmiy-tadqiqot va tajriba konstruktorlik hisobotlari	2	2	0	2	2-4	0	2-4	2-4	2-4	2-5
	Taqrizlar	2	2	2	2	2-4	2	2-4	2-4	2-4	2-5

		Ilmiy maqolalar	2	1	1	1	2	1	2-4	2-4	2-4	2-5
		Bitiruv ishlari	2	2	1	2	2	2	2-4	2-4	2-4	2-5
		Magistrlik dissertatsiyalari	2	2	1	2	2	2	2-4	2-4	2-4	2-5
		Patent va ixtiro hujjalari	2-4	2	2	2	2-4	2	2-4	2-4	2-4	2-5
		Dissertatsiya avtoreferati	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-5
		Boshlang‘ich doktorlik dissertatsiyalari (PhD)	2-3	2-3	2-3	2-3	2-4	2-3	2-4	2-4	2-4	2-5
		Dotorlik dissertatsiyalari	2-3	2-3	2-3	2-3	2-4	2-3	2-4	2-4	2-4	2-5
Ta’ limiy	O‘ quv nazariy	Darslik	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
		O‘quv qo‘llanma	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
		Ma’ruzalar matni	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
	O‘ quv uslubiy	Uslubiy qo‘llanma	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
		Uslubiy ko‘rsatma	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
		O‘quv uslubiy majmua	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
	O‘ quv amaliy	Masalalar to‘plami	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
		Praktikumlar	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
		Testlar	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
	O‘ quv dasturiy	O‘quv rejalar	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
		O‘quv dasturlar	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
		Tematik rejalar	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
	O‘ quv ma’lumotli	Izohli lug‘at	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
		Atamashunoslik lug‘ati	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-5
		Ensiklopediya	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-4	2-7	2-7

Shunday qilib, 3 ta: obyektlar, subyektlar hamda ular o‘rtasidagi munosabatlar sinflari qaralmoqda. Yuqorida keltirilgan tasniflashlar ilmiy-ta’limiy axborot resurslari xavfsizligini ta’minlash borasidagi quyidagi masalalarni yechishga asos bo‘lib xizmat qiladi:

1. Subyektlarni ro‘yxatga olish jarayonida ularning huquqlarini belgilash;

2. Tizimga yangi obyekt qo‘shilganda yoki subyektning xususiyatlari o‘zgarganda uning huquqlari tarkibini yangilash;

3. Bir subyekt bir nechta kategoriyalarga mansub bo‘lganda uning huquqlarini belgilash;

4. Tizim ma’murlarini vakolatlar asosida iyerarxik tasniflash.

1.3 Shaxs, jamiyat va davlat axborot xavfizligini ta’minlashda axborot-kutubxona resurslarini himoyalashning o‘rni

Jamiyatning axborotlashuvi axborotga bo‘lgan dunyoqarashning o‘zgarishiga olib kelmoqda. Axborotning tovar sifatida qaralayotganligi va qiymatining oshib borishi axborot xavfsizligining dolzarligini yanada kuchaytiradi. O‘zbekiston Respublikasining 2002 yil 12 dekabrdagi №439-II sonli “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonunida axborot xavfsizligi axborot borasidagi xavfsizlik deb belgilangan va u axborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holatini anglatadi[1].

Shunday qilib, axborot xavfsizligining maqsadi nafaqat kompyuter tizimlari va tarmoqlarida uzatilayotgan, saqlanayotgan va qayta ishlanilayotgan axborotlarning ishonchliligini tizimli tarzda ta’minlash, balki fuqarolarga ruxsat etilgan axborotlarni o‘z vaqtida olishini kafolatlash hamdir.

Ma’lumki, kutubxonalar shaxs va jamiyatning axborot xavfsizligi borasidagi manfaatlarini qondirishda, ishonchli axborotlar bilan ta’minlash orqali yoshlarni milliy qadriyatlar ruhida ilmli, vatanparvar qilib tarbiyalashda va axborot-psixologik xavfsizligini ta’minlashda muhim rol o‘ynaydi. Shuning uchun ham kutubxona fondlarida saqlanayotgan axborotlarni noqonuniy yo‘qotilish va o‘zgartirilishlar kabi

[1] O‘zbekiston Respublikasining “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi Qonuni.

salbiy ta’sirlardan himoyalash shaxs, jamiyat va davlat axborot xavfsizligini ta’minlashda sezilarli o‘rin egallaydi deb hisoblash mumkin. 1.10-jadvalda xavfsizlikning asosiy ko‘rinishlari va ularning axborot kutubxona resurslari himoyasiga bog‘liqligi keltirilgan.

1.10-jadval

Shaxs, jamiyat va davlat xavfsizligining axborot-kutubxona resurslari himoyasiga bog‘liqligi

Shaxs, jamiyat va davlat xavfsizligining sohalari	Turlari	Axborot-kutubxona resurslari himoyasiga bog‘liqligi
Ijtimoiy	Huquqiy	-
	Intellektual	+
	Ma’naviy	+
	Madaniy	+
	Psixologik	+
	Demografik	-
Iqtiodiy	Moliyaviy	-
	Xo‘jalik	+
	Soliq	-
	Ilmiy-texnik	+
	Texnologik	+
Sanoat	Yong‘in	-
	Radiatsion	-
	Kimyoviy	+
	Texnikaviy	+
Hududiy	Ekologik	-
	Biologik	-
	Oziq-ovqat	-
	Xom-ashyo	-
Axborot	Axborot xavfsizligi	+
Siyosiy	Siyosiy xavfsizlik	-
Mudofaa	Mudofaa xavfszligi	+

Intellektual xavfsizlik o‘zida yosh avlodni ularning barkamol bo‘lib voyaga yetishishida zaruriy axborotlar bilan ta’minlanganlikni, o‘z qobiliyatlarini ro‘yobga

chiqarishda yetarli sharoitlarning yaratilganligi, aholining intellekiual salohiyati va yutuqlaridan samarali foydalanishni ifodalaydi.

Ma'naviy xavfsizlik deganda esa xalqimizning yillar davomida saqlanib kelinayotgan ma'naviy qadriyatlari, ajdodlarimizning hayot haqidagi falsafiy, diniy va g'oyaviy qarashlari, xalqimizning boy ma'naviy merosining butun saqlanishi, shuningdek, yoshlarimizning ongini turli zararli g'oyalardan, ta'sirlardan himoyalanganigini tushunamiz.

Kutubxonalar tasnifi. Yuqorida xavfsizlikning asosiy turlari va ularning axborot-kutubxona resurslari himoyasiga bog'liqligi haqida so'z yuritildi. Endi esa kutubxonalarning o'zini tasniflashni ko'rib chiqiladi. Quyidagi jadvalda kutubxonalarni ularning bir necha mezonlariga ko'ra tasnifini va ularning xavfizlik darajasini keltirilgan (1.11-jadval).

Kutubxonalar xavfsizlik darajalarini ularda saqlanayotgan kontentning qiymatiga ko'ra quyidagicha tasniflash mumkin:

A1 – xavfsizlikning quyi darajasi. Ushbu kutubxonalarda faqatgina ochiq ma'lumotlar joylashgan bo'lib, ularning butunligi va foydalanuvchanligini ta'minlash kerak. Ma'lumotlarning chiqib ketishi shaxs, jamiyat va davlat xavfsizligiga ta'sir qilmaydi;

A2 – xavfsizlikning o'rta darajasi. Mazkur turdagi kutubxonalarda ochiq, pullik yoki korporativ foydalanishga mo'ljallangan ma'lumotlar bo'lib, ularning butunligi va foydalanuvchanligini ta'minlash talab etiladi. Ma'lumotlarning chiqib ketishi shaxs yoki korporatsiya va tashkilotlar manfaatiga zarar keltirishi mumkin;

A3 – xavfsizlikning o'rta darajasi. Bunday kutubxonalarda pullik yoki cheklangan doiradagigina shaxslarga mo'ljallangan, davlat ahamiyatiga ega bo'lgan ma'lumotlar saqlanib, ularning butunligi, foydalanuvchanligi va konfidensialligini ta'minlash kerak. Ma'lumotlarning chiqib ketishi shaxs, jamiyat va davlat manfaatlariga ta'sir ko'rsatadi.

1.11-jadval

Kutubxonalarning xavfsizlik darajalari bo‘yicha tasnifi

Kutubxonalar tasnifi	**Kutubxonalar turlari**	**Xavfsizlik darajasi**
Ijtimoiy ko‘rinishi bo‘yicha	Universal kutubxonalar	A3
	Jamoat kutubxonalari	A1
	Imkoniyati cheklanganlar uchun	A1
	Bolalar kutubxonasi	A1
	Ozodlikdan maxrum etilganlar kutubxonasi	A1
	Ta’lim muassasalari kutubxonalari	A2
	Akademik kutubxonalar	A3
Sohalari bo‘yicha	Tibbiyotga oid kutubxonalar	A2
	Qishloq xo‘jaligiga oid kutubxonalar	A1
	Harbiy sohaga oid kutubxonalar	A3
	Texnik kutubxonalar	A2
	Badiiy kutubxonalar	A1
	Muzey kutubxonalari	A3
	Patent kutubxonalari	A3
Ish faoliyati bo‘yicha	An’anaviy kutubxonalar	A1-A3
	Avtomatlashtirilgan kutubxonalar	A1-A3
	Elektron kutubxonalar	A1-A3
	Virtual kutubxonalar	A1-A3
Foydalana olishlik darajasi bo‘yicha	Bepul kutubxonalar	A1
	Pullik kutubxonalar	A2
	Cheklangan doiradagi foydalanuvchilar uchun	A3
Hududi bo‘yicha	O‘zbekiston Milliy kutubxonasi	A1-A3
	Axborot kutubxona markazlari	A1-A3
	Axborot resurs markazlari	A1-A3
	Davlat hokimiyati va boshqaruv organlari kutubxonalari	A1-A3
Darajasi bo‘yicha	Prezident kutubxonasi	A3
	Parlament kutubxonasi	A3
	Xususiy kutubxonalar	A3
	Shaxsiy kutubxonalar	A1

Ko‘rinib turganidek, ikkinchi va uchinchi turga mansub bo‘lgan kutubxonalarning axborot resurslari xavfsizligini ta’minlash talab etiladi. Himoyaning usul va vositalarini tanlashdan oldin himoya obyektlarini, ularning xavfsizligiga bo‘lishi mumkin bo‘lgan tahdidlarni tasniflash va tahlil qilish maqsadiga muvofiq bo‘ladi.

Shaxsiy ma’lumotlar xavfsizligi. Shaxsiy ma’lumotlar xavfsizligini ta’minlash bugungi kunning dolzarb masalalaridan biridir. Bunday ma’lumotlar allaqachon yuqori

qiymatli tovarga aylanib ulgurgan. Chunki u firibgar qo‘lida jinoyat uchun qurol, bo‘shatilgan xodim qo‘lida muammo uchun vosita, insayder qo‘lida esa raqobatchilarga sotish uchun tovar va hakozo. Shuning uchun ham shaxsiy ma’lumotlar ishonchli himoyalashni talab qiladi.

Ma’lumotlardan nusxa olish va tarqatishdagi texnik imkoniyatlarning oshishi shaxsiy ma’lumotlarni himoyalash muammosining dolzarbligini kuchaytirmoqda. Bugungi kunda hech bir korxona yo‘qki xodimlari to‘g‘risidagi shaxsiy ma’lumotlarga ega bo‘lmay faoliyat yuritsa. Shu nuqtai nazardan davlat ham o‘z fuqarolarining manfaatlarini himoyalash maqsadida korxonalardan shaxsiy ma’lumotlarning ishonchli himoyasini talab qiladi.

Shaxsiy ma’lumotlarning 3 kategoriyasi ajratib ko‘rsatiladi:

1) Umumfoydalaniluvchi shaxsiy ma’lumotlar: Ismi, familiyasi, sharifi, tug‘ilgan vaqti va joyi, yashash manzili, telefon raqami, kasbi haqidagi ma’lumotlar va boshqa;
2) Maxsus kategoriyali shaxsiy ma’lumotlar: irqi, milliy mansubligi, siyosiy, diniy va falsafiy qarashlari, sog‘ligining holati va intim hayoti haqidagi ma’lumotlar;
3) Biometrik shaxsiy ma’lumotlar.

1.4 Fan va ta’limga oid resurslarni himoyalashning dasturiy komplekslari va tizimlari tahlili

Ushbu bo‘limda axborot resurslariga nisbatan tahdidlar hamda axborot xavfsizligini baholashning zamonaviy dasturiy komplekslari tahlil etiladi.

Axborot resurslari himoyasini tashkil etishda avvalo ushbu resurslarga qiziquvchi tomonlar va bo‘lishi mumkin bo‘lgan tahdidlar o‘rganiladi. Tahdidlarning tahlil qilinishi va modellarining qurilishi munosib himoya usullari va vositalarini tanlashga imkon beradi. AXga tahdidlar tahlili deyilganda ma’lumotlarni qayta ishlash tizimiga salbiy ta’sir etishi mumkin bo‘lgan harakatlar va hodisalarni tadqiq etish tushuniladi.

Axborot-kommunikatsiya texnologiyalarining to‘xtovsiz rivojlanishiga bog‘liq holda konfidensial axborotlar hajmining ortishi hamda insoniyatning axborotga nisbatan maqsad va qarashlarining o‘zgarib borishi hujumning yangi ko‘rinishdagi turlarini keltirib chiqaradi. Bu esa o‘z o‘rnida axborotlarga nisbatan tahdidlarning yagona modelini qurish masalasini qiyinlashtiradi.

Elektron kutubxona tizimlariga nisbatan tahdidlarni birinchilardan bo‘lib Joanne Kuzma [79], Roesnita Ismail [78] va Mohamed ElSherbiny [74, 83] lar o‘z ishlarida keltirib o‘tishgan. Ba’zi elektron kutubxonalar axborot resurslariga obuna bo‘lish narxining qimmatligi ushbu resurslarga nisbatan buzg‘unchilar qiziqishini oshirishi mumkin [91].

Har qanday axborot tizimiga, jumladan KAKTga nisbatan tahdidlarni ularning manbasi, maqsadi, AXning qaysi jihatlariga qaratilganligi kabi belgilariga ko‘ra umumiy holda 1.12-jadvaldagi kabi tasniflash mumkin [47]. Jadvalda keltirilgan tahdidlarning turli xilligi himoyalanayotgan tizim xavfsizligi uchun mos himoya usullari va vositalarini qo‘llashni taqozo etadi.

Kutubxona tizimining tahdidga duchor bo‘luvchi resurslari, ularga nisbatan tahdidlar, AXning buzulish xususiyatlari va tahdidlarga qarshi usul va vositalarni umumlashtirib, 1.13-jadval ko‘rinishida tasvirlash mumkin [43; 132-b.].

Elektron kutubxona resurslari ko‘proq *XSS, DoS* va *SQL kiritish* ko‘rinishdagi tahdidlarga uchraydi [79, 66].

Tarmoqlararo skripting (XSS – Cross-site scripting) – serverda joylashgan veb sahifaga uchinchi shaxs tomonidan zararli dasturiy kodning kiritilishidir. Bunda buzg‘unchiga veb saytlarga ruxsatsiz kirish va hujum qilish, Ya’ni ma’lumotlarni kiritish shaklini ko‘rish va zararli ma’lumotlarning sayt kontentiga jo‘natish imkonini beradi [24].

1.12-жадвал

Tahdidlarning umumiy belgilari bo‘yicha tasniflanishi

Parametrlari	Belgilari	Tavsifi
Keltirgan oqibatlar	Passiv	Himoyalanayotgan axborotning konfedensialligi buziladi. Ya’ni, axborotni o‘qish, nusxa olish evaziga uning mazmuni fosh etildi.
	Aktiv	Himoyalanayotgan axborotning nafaqat konfedensialligi, balki axborotning yo‘q qilinishi evaziga uning yaxlitligi buziladi.
Maqsad	Maqcadli	Bevosita inson ishtirokida amalga oshirilib, axborotdan ruxsatsiz foydalanish, kompyuter jinoyatchiligi, zararli dasturlar orqali hujum uyushtiriladi.
	Tasodifiy	AX texnik va dasturiy nosozliklar, tabiiy falokatlar va xodimlar yoki foydalanuvchilarning xatolari evaziga buziladi.
Manba	Ichki	Tahdidlar korxonaning rahbar yoki ishchi xodimlari tomonidan amalga oshiriladi.
	Tashqi	Tahdidlar begona shaxslar, jinoyatchilar, raqib korxona vakillari yoki xakerlik hujumlari va zararli dasturlar yordamida uyushtiriladi.
Obyekt holati	Saqlashda	Tahdid tizimda saqlanayotgan ma’lumotlarga uyushtiriladi. Masalan axborot resurlari.
	Uzatishda	Tahdid ma’lumotlarning tarmoqlarda uzatish chog‘ida uyushtiriladi. Masalan, foydalanuvchi elektron kutubxonaga masofadan kirishda.
	Qayta ishlashda	Tahdid ma’lumotlar qayta ishlanayotgan vaqtda uyushtiriladi. Masalan, foydalanuvchilarga huquqlarni belgilashda.
Axborot tizimining komponentlari	Ma’lumotlar	Axborot resurslari yo‘q qilinadi.
	Infrastruktura	Axborot tizimi tarkibi noqonuniy o‘zgartiriladi.
	Dasturlar	Dasturiy ta’minot shikastlanadi yoki xizmat ko‘rsatishni rad etadi.
	Mualliflik	Natijada muallif huquqi o‘zlashtiriladi.
Aktiv xususiyati	Konfidensiallik	Ma’lumotlarning maxfiyligi buziladi.
	Yaxlitlik	Axborot noqonuniy o‘zgartiriladi yoki yo‘q qilinadi.
	Foydalana olishlik	Tizimga kirish yoki axborotdan foydalanish rad etiladi.

Xizmatdan voz kechish (DoS – Denial of Service). Bu tarmoq resursiga murojat qilishni to‘xtatish, Ya’ni tarmoqning trafik bilan to‘lib qolishi orqali aloqa liniyasini

«bo‘g‘ish» natijasida qonuniy foydalanuvchilarning tarmoq xizmatlariga murojaatini to‘xtatib qo‘yishdagi hujum turidir.

SQL kiritish (Structured Query Language injection). Bu ma’lumotlarni kiritish maydoniga tegishli ma’lumotlar o‘rniga SQL buyruqlari kiritilib, ushbu SQL operatori bajarilgan vaqtda o‘z ta’sirini ko‘rsatuvchi hujum turi. SQL kiritish veb ilovalarga oddiy tahdid bo‘lib, foydalanuvchilar SQL so‘rovlarini kiritish vaqtida ishlatiladi [75].

Tahdidlar o‘z usullariga ko‘ra biror bir aktivning qaysidir xususiyatini buzishga qaratilgan bo‘ladi. Ko‘pgina tizimlarda axborot aktivlarining asosiy xususiyatlari sifatida *yaxlitlik, foydalana olishlik* va *konfidensiallik* qaraladi [35].

Yaxlitlik ma’lumotlar himoyasida o‘ta muhim hisoblanib, hisoblash tizimida yoki tizimdan uzatilayotganda axborotni har qanday qasddan o‘zgartirishni o‘zida mujassamlaydi. Agar axborotni uzatish jarayonida u faol o‘zgartirilsa yaxlitlik buzilgan hisoblanadi [19].

Foydalana olishlik subyektlarning axborotlarga o‘z vaqtida qarshiliklarsiz kirishini ta’minlab beruvchi hamda ixtiyoriy vaqtda murojaat etilganda subyektlarning so‘rovlariga javob beruvchi tizimning xususiyatidir. Yuqori darajada foydalana olishlikni ta’minlovchi tizimlarning maqsadi ixtiyoriy vaqtda kirishni ta’minlashda texnik uzilishlar sabab xizmat ko‘rsatishning to‘xtab qolishlarning va xizmat qilishni rad qilish hujumining oldini olishni qamrab oladi.

Axborotning *konfidensiallik* xususiyati buzilganda uning mazmuni undan foydalanishga ruxsat berilmagan tomonlar uchun fosh bo‘ladi. Bu holat konfedensial axborot saqlanuvchi tizimda yoki tarmoqda noqonuniy foydalana olishlikni qo‘lga kiritish orqali yuzaga keladi [83; 16-b.].

Shunday qilib, axborot aktivlarining yuqorida keltirilgan asosiy xususiyatlariga nisbatan tahdidlarning quyidagi ko‘rinishlarini ajratish mumkin:

1) *konfidensiallikning* buzilishiga tahdidlar: o‘g‘irlash (chiqib ketish, tutib qolish, yig‘ish), yo‘qolish, oshkor bo‘lish;

1.13-жадвал

Ресурслар, таҳдидлар ҳамда ҳимоя воситалари таснифи

Kutubxona resursi	Tahdid turlari	Resursning buziladigan xususiyatlari	Himoya usullari va vositalari
Ma’lumotlar bazasi	DoS/DdoS	Foydalana olishlik	Dasturiy, apparat Blokirovkalash.
	Zararli dasturlardan foydalanish	Butunlik, foydalana olishlik, konfidensiallik	Dasturiy, apparat Foydalanishni boshqarish.
	SQL-kiritish	Butunlik, foydalana olishlik, konfidensiallik	Dasturiy, apparat. Filtrlash, tahlillash.
Veb-sayt	DoS/DdoS	Foydalana olishlik	Dasturiy, apparat
	SQL-kiritish	Butunlik, foydalana olishlik, konfidensiallik	Dasturiy, apparat. Filtrlash, tahlillash.
	XSS-hujum	Butunlik, foydalana olishlik, konfidensiallik	Dasturiy, apparat. Filtrlash, tahlillash.
Dasturiy ta’minot	Zararli dasturlardan foydalanish	Butunlik, foydalana olishlik	Dasturiy, apparat. autentifikatsiya. Shifrlash.
Qurilmalar va jihozlar	Buzg‘unchining jismoniy harakatlari	Butunlik, foydalana olishlik, konfidensiallik	Fizik. Signalizatsiya, Qo‘riqlash.
Tarmoq qurilmalari	Tarmoq hujumlari, Buzg‘unchining jismoniy harakatlari	Butunlik, foydalana olishlik, konfidensiallik	Fizik, apparat. Blokirovkalash.
To‘lov tizimlari	Tizimdan ruxsatsiz foydalanish, firibgarlik	Tizimning ish qobiliyati	Dasturiy, apparat. Shifrlash, Autentifikatsiya
Mualliflik huquqlari	Axborotdan noqonuniy foydalanish	Mualliflik huquqi	Huquqiy, tashkiliy. Stenografiya.
Shaxsiy ma’lumotlar	Tarmoq hujumlari, firibgarlik	Shaxs huquq va erkinligi	Huquqiy, tashkiliy, dasturiy, apparat. Shifrlash, Xeshlash, Autentifikatsiya.
Statistik axborotlar	Tarmoq hujumlari, firibgarlik	Shaxs huquqi va erkinligi	Tashkiliy, dasturiy, apparat. Shifrlash, Autentifikatsiya

2) *yaxlitlikning* buzilishiga tahdidlar: o‘zgartirish, axborotning haqiqiyligini rad etish, yolg‘on axborotni o‘tkazish;

3) *foydalana olishlikning* buzilishiga tahdidlar: axborotni bloklash, axborot va vositalarni yo‘q qilish.

Mazkur bo‘limda axborot resurslari va tizimlariga bo‘ladigan namunaviy tahdidlar belgilari va himoyalanayotgan obyektlarga nisbatan manbalari bo‘yicha tasniflandi, shuningdek, konfidensiallik, yaxlitlik va foydalana olishlikning buzilishiga nisbatan tahlillar keltirildi.

Bugungi kunda AX risklarni tahlil qilish va boshqarishning bir qancha metodologiyalarga asoslangan CRAMM, FRAP, RiskWatch, NIST SP 800-30, OCTAVE, Microsoft Security Assessment Tool (MSAT), GRIF, CORAS kabi zamonaviy dasturiy komplekslari mavjud [20, 59]. Bu dasturiy vositalarda tatbiq etilgan usullarni risklarni baholash shakliga ko‘ra sifat darajada baholash, son jihatdan baholash, aralash baholashda foydalaniladigan kabi usullarga ajratish mumkin. Quyida mazkur dasturiy ta’minotlar asosiy vazifalari va kamchiliklari qaraladi.

AQShning Standartlar va texnologiyalari milliy instituti tomonidan ishlab chiqilgan NIST SP 800-30 quyidagi qadamlardan iborat: tizim xarateristikasining tavsifi; tahdidlarni identifikatsiyalash; zaifliklarni identifikatsiyalash; himoya choralarining tahlili; ehtimollikni aniqlash; risklarni aniqlash; himoya choralarini taklif qilish; natijalarni hujjatlashtirish [33].

NIST SP 800-30 risklarni baholash metodologiyasi korxonaning ichki mas’ullari va xavfsizlik bo‘yicha mutaxassislari tomonidan keng foydalaniladi. Biriktirilgan mas’ul yoki kichik guruh xavfsizlik amaliyoti qo‘llanilayotgan tizimdan va kompaniyada ishlayotgan kishilardan ma’lumotlarni yig‘adi. Bu yig‘ilgan ma’lumotlar NIST SP 800-30 hujjatida ko‘rsatilgan risklarni tahlil qilish qadamlarini bajarish uchun dastlabki manba hisoblanadi.

FRAP (Facilitated Risk Analysis Process – hamkorlikda risklarni tahlil qilish jarayoni) turli metodologiyalardan foydalangan holda har xil jihatlar bo‘yicha tekshiruvni o‘tkazishga imkon berib, risklarni sifat jihatdan baholashni o‘tkazish uchun

yaratilgan. FRAPning samarasi jamoa ishining professional tashkil qilinishiga bog‘liq [15].

Yana boshqa ko‘rinishdagi metodologiya OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation – kritik tahdidlar, zaifliklar va aktivlarni baholash) hisoblanadi. Ushbu metodologiya AX risklarini tahlil qilishning barcha jarayonini faqat kompaniya xodimlari yordamida o‘tkaziladigan vaziyatlardagina qo‘llaniladi. U oldinda qanday risklar borligini kompaniya xodimlarining hammadan ko‘ra yaxshiroq tushunishi g‘oyasiga asoslanadi. Baholash jarayonida qatnashish uchun tanlangan xodimlar kompaniyalarida xavfsizlikni baholashda qaysi usul eng yaxshi ekanligini o‘zlari belgilashadi [21].

Buyuk Britaniyada ishlab chiqilgan ***CRAMM*** (CCTA[2] Risk Analysis and Management Method – CCTAning tahdidlarni tahlil qilish va boshqarish usuli) dasturiy mahsuloti davlat standartiga asos sifatida qabul qilingan. CRAMM dasturiy vositasi davlat va biznes sektorining katta va kichik tashkilotlari uchun qo‘llanilib, u son va sifat jihatdan tahlil qilish usullarining birikmasi asosida risklarni baholashga kompleks yondashuvni amalga oshiradi.

Ya’ni, *birinchi* bosqichda himoyalanayotgan resurs baholanadi. Agar birinchi bosqich natijasiga ko‘ra resurslarning kritiklik natijasi past bo‘lsa, himoya vositalariga ham minimal talab qo‘yiladi.

Ikkinchi bosqichda avval xavfsizlik tahdidi identifikatsiyalanadi va baholanadi, zaifliklarni qidirish va baholash o‘tkaziladi. Auditor tahdid va zaifliklarni baholash uchun boshlang‘ich ma’lumotlarni tashkilotning vakolatli vakillaridan maxsus savollar asosida oladi. Tahdid darajasi sifat shkalasi bo‘yicha juda yuqori, o‘rta, past, juda past kabi, o‘z navbatida zaiflik darajasi yuqori, o‘rta va past kabi baholanadi. Ushbu axborotlar asosida yetti balli shkalada risk darajasi ishlab chiqiladi. CRAMM

[2] *Central Computer and Telecommunications Agency* – Markaziy kompyuter va telekommunikatsiya agentligi

ekspertlardan olingan sifat ko‘rinishidagi baholarga tayanib, ular asosida son jihatdan baho aniqlanadi.

Uchinchi bosqichda maqbul himoya choralarini tanlash amalga oshiriladi, Ya’ni tashkilot talabini eng yaxshi tarzda qoniqtiradigan xavfsizlik tizimi varianti qidiriladi. CRAMM bilimlar bazasiga ega va ma’lum vaziyatda himoyani qanday tashkil etish bo‘yicha yechimlar taklif etadi [58].

CRAMM quyidagi kamchiliklarga ega: CRAMM usulidan foydalanish ijrochilardan maxsus tayyorgarlik va yuqori malaka talab qiladi; CRAMM usuli bo‘yicha tekshiruv jarayoni sermashaqqat bo‘lib, hatto bir necha oy to‘xtovsiz ishlashni talab qiladi; foydalanuvchilar CRAMMning bilimlar bazasiga qo‘shimcha o‘zgartirishlar kiritish imkoniyati yo‘q, Ya’ni usulni aniq bir tashkilot ehtiyojiga moslashtirish qiyinchiliklar keltirib chiqaradi [14].

Risklarni tahlil qilish va boshqarishning RiskWatch dasturiy ta’minoti Amerikada ishlab chiqilgan bo‘lib, u risklarni tahlil qilish va xavfsizlik auditini o‘tkazishda quyidagilarni baholaydi: axborot risklarini; axborot tizimlari himoyasining fizik usularini; ISO 17 799 standartiga mosligining bahosi [65; 8-b.].

RiskWatch dasturining CRAMMdan farqi shundan iboratki, u ko‘proq axborotni himoyalash tizimini yaratish xarajatlari va xavfsizlik tahdidi natijasidagi yo‘qotishlarning o‘zaro nisbatini aniq son jihatdan baholashga mo‘ljallangan. RiskWatch dasturida risklarni tahlil qilish to‘rt bosqichda amalga oshiriladi.

Birinchi bosqichda qaralayotgan tizimning tarkibi tavsiflanadi, himoyalanayotgan resurslarning kategoriyalari, yo‘qotishlar, tahdidlar, zaifliklar va himoya choralari ro‘yxati tuziladi.

Ikkinchi bosqichda resurslar, yo‘qotishlar va insidentlar sinflari batafsil tavsiflanadi. Ma’lumotlar hisobotlardan, kompyuter tarmoqlarida zaifliklarni tadqiq qiluvchi vositalardan olinib, qo‘lda kiritilishi mumkin. Shuningdek, zaifliklarni aniqlash uchun so‘roq varaqasidan foydalaniladi.

Uchinchi bosqichda risklar aniqlanadi va xavfsizlikni ta’minlash choralari tanlanadi. Avval resurslar, tahdidlar, zaifliklar va yo‘qotishlar o‘rtasida bog‘liqliklar o‘rnatiladi.

To‘*rtinchi* bosqichda hisobotlar shakllantiriladi. Tayyorlangan hisobotlar va grafiklar tashkilot xavfsizlik tizimidan foydalanish bo‘yicha qaror qabul qilish uchun yetarli bo‘ladi.

Risklarni baholashning zamonaviy metodologiyalarida axborot aktivlarini baholash usullari 1.14-jadvalda keltirilgan.

1.14-jadval

Dasturiy komplekslarning resurslarni baholash usullari bo‘yicha qiyosiy tahlili

Risklarni baholash metodologiyasi	**Axborot aktivini baholash usuli**
CRAMM	Aktivlar fizik, dasturiy va axborot aktivlariga ajratiladi. Fizik resurslar bahosi shikastlanganda ularni tiklash qiymati bilan aniqlanadi. Ma’lumotlar va DT bahosi quyidagi vaziyatlarda aniqlanadi: - ma’lum vaqt oralig‘ida resursdan foydala olmaslik; - resursning shikastlanishi yoki yo‘q qilinishi; - ruxsat etilmagan foydalanish orqali konfidensiallikning buzilishi; - foydalanuvchilar hamda DT xatoliklari tufayli axborotning o‘zgartirilishi;
FRAP	Himoya qilinuvchi aktivlarni aniqlash so‘rovnoma o‘tkazish, tizimdan dokumentatsiyalarni o‘rganish, tarmoqni avtomatik tahlil qilish vositalaridan foydalanish yordamida amalga oshiriladi.
OCTAVE	Axborotning bahosi tashkilotda faoliyat yurituvchi xodimlarning bilim va tajribalari asosida aniqlanadi.
RiskWatch	Himoya qilinuvchi axborotning bahosi 600 dan ziyod savollar bazasiga ega bo‘lgan so‘rovnomani o‘tkazish orqali amalga oshiriladi.
MSAT	Aktivlarni moddiy va nomoddiy turlarga ajratadi va ularni sifat jihatdan quyidagi sinflarga ajratiladi: - biznesga yuqori, o‘rta va past darajada ta’sir etuvchi;

Jadvaldan ko’rish mumkinki Risklarni baholashning zamonaviy metodologiyalarining barchasida ham axborot aktivlarini baholash masalasi qaralib, u asosan so’rovnoma yoki savol-javob o’tkazish asosida aniqlanadi.

Yuqorida qarab o‘tilgan NIST SP 800-30, FRAP, OCTAVE, CRAMM, RiskWatch kabi AX risklarini boshqarish usullarining ayrim mezonlar bo‘yicha qiyosiy tahlilini 1.15-jadvaldagidek keltirish mumkin.

Risklarni tahlil qilish tashkilotda qancha qiymatdagi aktivlar borligi, ularning zaifliklari va bo‘lishi mumkin bo‘lgan tahdidlarni identifikatsiyalash, potensial tahdidlarning amalga oshish ehtimolligi va oxirida tahdid natijasida tashkilot qancha zarar ko‘rishini aniqlash imkonini beradi. Ushbu tahlil asosida tashkilot uchun har jihatdan maqbul bo‘lgan himoya vositalarini va usullarini tanlash mumkin.

1.15-jadval

Risklarini boshqarish dasturiy komplekslarini tahlili

Taqqoslash mezonlari	**CRAMM**	**RiskWatch**	**NIST**	FRAP	OCTAVE
Son jihatdan baholash	+	+	-	-	-
Sifat jihatdan baholash	+	-	+	+	+
Auditorlarni maxsus tayyorgarlikdan o‘tkazishning lozimligi	+	+	-	+	-
Risklarni kamaytirish bo‘yicha tadbirlar rejasi	-	+	-	-	+
Risklarni tashkiliy darajada baholash	+	-	+	+	+
Risklarni texnik darajada baholash	+	+	+	+	+
Moddiy aktiv elementlaridan foydalanish	+	+	+	+	+
Nomoddiy aktiv elementlaridan foydalanish	+	+	+	+	+
Ativlarni baholash	+	+	+	+	+

Mazkur bo‘limda axborot xavfsizligi risklarini boshqarishning zamonaviy dasturiy komplekslari tahlil etildi va asosiy mezonlari bo‘yicha tasniflandi. Tahlillar shuni ko‘rsatadiki, risklarni boshqarishning mavjud usullari umumiy holda to‘liq detallashtirilmagan va risklarni tahlil qilish vositasi o‘z tarkibida yopiq algoritmlarga ega.

II BOB. ELEKTRON RESURSLAR XAVFSIZLIGINI TA’MINLASH DARAJASINI BAHOLASH VA ULARNI HIMOYALASH CHORALARINI TANLASH

2.1 Korporativ axborot kutubxona tarmoqlarida resurslarni himoyalashning usullari va vositalari

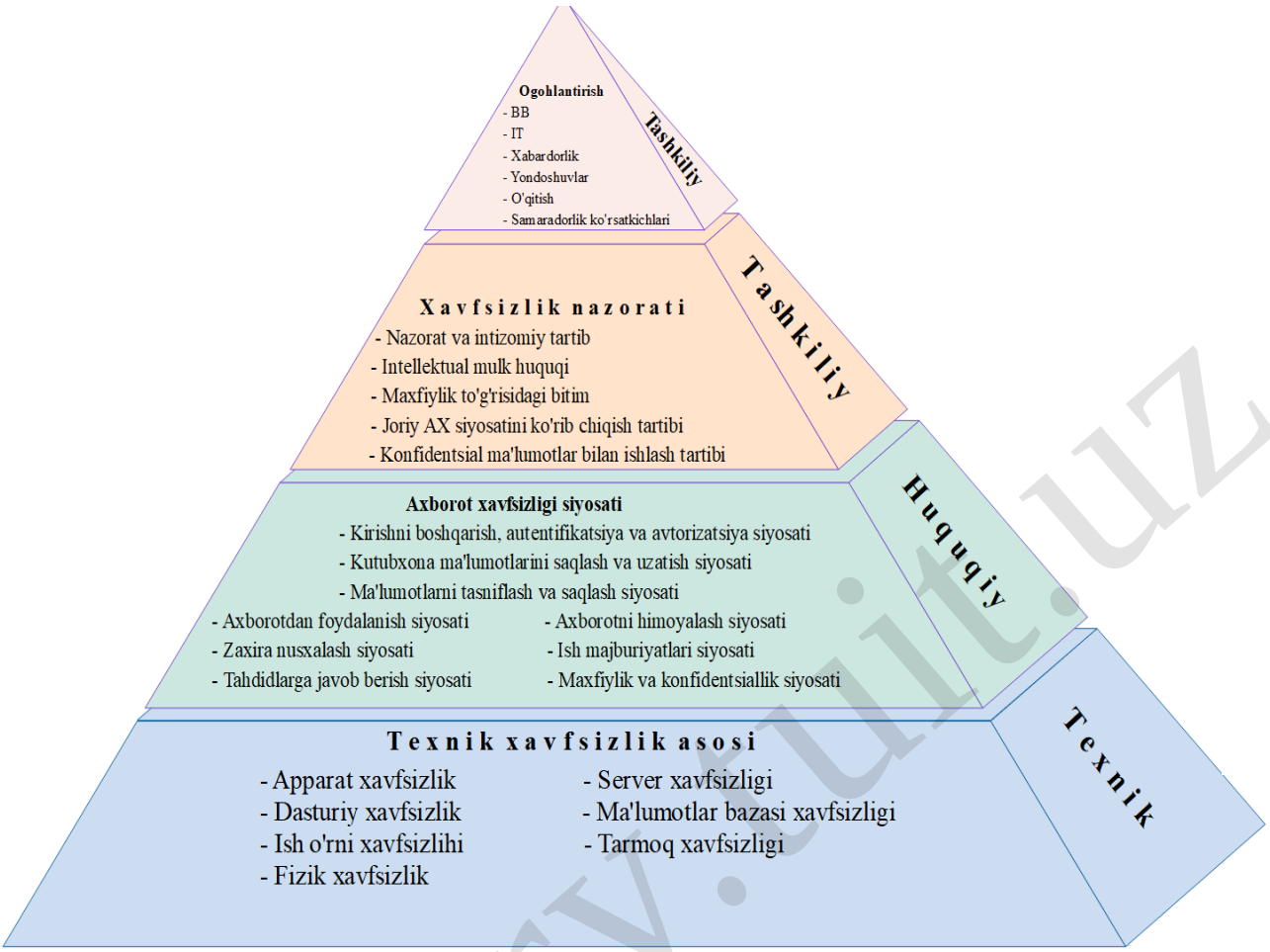
Ushbu bo‘limda korporativ axborot-kutubxona tarmoqlarida ilmiy-texnik va ta’limga oid resurslarni himoyalashning mos usul va vositalarini tanlash masalasi bayon etiladi.

KAKT xavfsizligini ta’minlashning kompeks ta’minoti 1.2-rasmda keltirilgan. Bu yerda kompleks ta’minotni uchta: huquqiy, tashkiliy va texnik pog‘onalarga ajratilgan [46; 43-44-b.].

Huquqiy choralarga axborot-kutubxona tizimlari xavfsizligi sohasidagi standartlar, bitimlar, kodekslar, kelishuvlar, shartnomalar, qonunlar, qarorlar, ustavlar, nizomlar, yo‘riqnomalar kabi barcha xalqaro va milliy meyoriy hujjatlarga asoslangan AX siyosati hujjatini o‘z ichiga oladi va tashkilotda AX bilan bog‘liq barcha munosabatlarni reglamentlaydi [45; 38-b.]. Kutubxona tizimlari xavfsizligi sohasidagi xorijiy va milliy meyoriy hujjatlar 2.1-jadvalda keltirilgan.

Dasturiy ta’minot xavfsizligi. Dasturiy ta’minotlarga kutubxona axborot tizimlari, OPAC[3] lar, Internet orqali kirish mumkin bo‘lgan ma’lumotlar bazalari va resurslari kiradi [73]. Dasturiy ta’minot xavfsizligi masalasi dasturiy ta’minot komponentlarini buzilishlardan himoya qilish muammosini o‘z ichiga oladi. Shu o‘rinda qayd etish kerakki, turli amaliy dasturlarni ishga tushiruvchi operatsion tizimlar muhim ahamiyatga ega bo‘lib, boshqa tizimlarning umumiy xavfsizligini ta’minlashda bu operatsion tizimni tanlash va xavfsizligi asosiy rolga ega bo‘ladi.

[3] Online public access catalog – Onlayn ommaviy kirish kataloglari



2.1-rasm. Axborot xavfsizligini ta’minlashning kompleks ta’minoti.

Tashkiliy choralar AXT tizimining eng yuqori pog‘onasi bo‘lib, AX tizimini boshqarish, mavjud xavfsizlik siyosatini qayta ko‘rib chiqish, AX xodisalari yuzasidan qarorlar qabul qilish tartiblarini o‘z ichiga oladi.

Texnik choralar bazaviy ta’minot hisoblanib, u himoyaning minimal vositalarini o‘z ichiga oladi [38; 290-b.]. Texnik choralar asosiy mexanizm bo‘lganligidan quyida uning elementlari tadqiqini keltiramiz.

Apparat vositalari xavfsizligi. Apparat vositalari telefon liniyalari, RFID[4] qurilmalar, modemlar, tarmoq kabellari, skanerlar, printerlar, ma’lumot tashuvchilar kabilarni o‘z ichiga olib, ular qurilmalar va kitoblarni o‘g‘irlashlar, ta’minotdagi

[4] Radio-Frequency Identification

uzilishlar, qurilmalarning o‘zaro mos kelmasligi, ehtiyotsizlik kabi tahdidlardan ishonchli himoyalanishni ta’minlaydi [92; 483-b.]. Apparat vositalardan samarali foydalanish uchun ularning *fizik xavfsizligini* ta’minlash zarur.

2.1-jadval

Kutubxona tizimlari xavfsizligi sohasidagi xorijiy va milliy meyoriy hujjatlar

Mamlakatlar	Me’riy hujjatlar
Amerika Qo‘shma Shtatlari	Amerika Kutubxonalar Assotsiatsiyasining «Kutubxona xavfsizligi qo‘llanmasi (Library Security Guidelines)» (2001),
Ispaniya	«Ma’lumotlar xavfsizligi to‘g‘risida»gi Direktivasi (2003)
Fransiya	«Ma’lumotlar xavfsizligi to‘g‘risida»gi Direktivasi (2004)
Buyuk Britaniya	«Ma’lumotlar himoyasi to‘g‘risida»gi Qonun (1998).
Rossiya Federatsiyasi	Rossiya Federatsiyasining axborot xavfsizligi Doktrinasi (2000), Rossiya Milliy Kutubxonasining axborot xavfsizligi to‘g‘risidagi Nizomi (2016)
O‘zbekiston Respublikasi	O‘zbekiston Respublikasi Vazirlar Mahkamasining Qaroriga[5] ko‘ra «...Elektron axborot-kutubxona resurslarini saqlash, zararli dasturiy ta’minlashdan va ruxsat berilmagan nusxa ko‘chirishdan himoya qilish tarmoqning umumiy xavfsizlik mexanizmlari bilan ta’minlanadi» (2011), O‘zbekiston Respublikasi Vazirlar Mahkamasining Qarori[6]ga ko‘ra Milliy kutubxona «...axborot-kutubxona fondi saqlanishini, elektron resurslarning axborot xavfsizligini ta’minlash ishlarini amalga oshiradi» (2012).

Ishchi stansiyalar xavfsizligi. Kutubxonalar ishchi stansiyalari Internet tarmog‘i va foydalanuvchilar tomonidan sodir etiluvchi viruslar, o‘g‘irliklar va ruxsat etilmagan kirishlarga eng ko‘p duchor bo‘ladi [73]. Ishchi stansiyalar xavfsizligining buzilishi nafaqat konfidensiallikka, balki axborotdan foydalana olishlikka ham ta’sir etishi mumkin. Kutubxona ishchi stansiyalari xavfsizligi viruslar va bashqa zararli dasturiy kodlardan himoyalash tizimlari, elektron pochtani filtrlash tizimi, tarmoqlararo ekran va boshqa yechimlar bilan ta’minlanishi mumkin.

[5] O‘zbekiston Respublikasi Vazirlar Mahkamasining «Elektron kutubxona to‘g‘risidagi namunaviy nizomni hamda axborot-kutubxona va axborot-resurs markazlarida va kutubxonalarda to‘liq matnli elektron axborot-kutubxona resurslari fondini yaratish reja-jadvalini tasdiqlash haqida»gi Qarori. O‘zbekiston Respublikasi qonun hujjatlari to‘plami, 2011 y., 27-son, 285-modda; 2012 y., 33-34-son, 391-modda

[6] «O‘zbekiston Respublikasi Prezidentining «Alisher Navoiy nomidagi O‘zbekiston Milliy Kutubxonasi – axborot resurs markazi faoliyatini tashkil etish chora-tadbirlari to‘g‘risida» 2012 yil 20 martdagi pq-1729-son qarorini amalga oshirish chora-tadbirlari to‘g‘risida»gi O‘zbekiston Respublikasi Vazirlar Mahkamasining Qarori. O‘zbekiston Respublikasi qonun hujjatlari to‘plami, 2012 y., 14-son, 157-modda;

Tarmoq xavfsizligi. Tarmoq xavfsizligi qonuniy foydalanuvchilarga kirish ruxsatini to‘liq ta’minlashi bilan bir vaqtda ruxsat etilmagan foydalanuvchilar kirishini taqiqlay olishi kerak. KAKT xavfsizligi ma’lumotlarni ma’lumotlarni shifrlash, identifikatsiya va autentifikatsiya, foydalanishlarni cheklash kabi mexanizmlar va raqamli sertifikatlar, elektron raqamli imzo, tarmoqlararo ekran, dasturiy va apparat vositalarni qo‘llash orqali yechilishi mumkin. Kutubxona kompyuterlari uchun simli tarmoqlar asosan binolarda, simsiz tarmoqlar esa ajratilgan tashqi qurilmalar (misol uchun planshet, noutbuk) orqali foydalanuvchilarning tarmoqqa ulanishlari uchun ishlatiladi. Tarmoqning fizik xavfsizligini ta’minlash maqsadida foydalanuvchilarning ruxsat etilmagan qurilmalarini o‘rnatishga yo‘l qo‘ymaslik, asosiy ulanish joylarida ishonchli autentifikatsiyalash tizimlaridan hamda aloqa usullari va ularni himoyalovchilardan foydalanish kerak [82; 41-b.].

Server xavfsizligi. Kutubxonalar elektron pochta va veb server ilovalarini har qanday bostirib kirishlar (vtorjeniye), viruslar, xakerlik hujumlari va tabiiy ofatlar tufayli qurilmalar yoki ilovalarning ishdan chiqishidan himoyalash choralarini ko‘rishi kerak. Serverlar xavfsizligi fayervollar, VPN texnologiyalar, HTTPS shifrlash, auditlash, tarmoqlararo ekran, foydalanishni boshqarish kabi bir qancha usul va vositalarning kompleks ta’minoti bilan ta’minlanadi [70; 29-b.].

Ma’lumotlar bazasi xavfsizligi. Kutubxona uchun o‘z ma’lumotlari xavfsizligini tasodifiy yo‘qolishlar va ruxsat etilmagan o‘zgartirishlardan himoyalash, qabul qilingan qoidalarga muvofiq kirishni ta’minlash uchun ma’lumotlar boshqaruvining ishonchli tizimi zarur [92; 483-b.]. Ma’lumotlar bazasi metama’lumotlar va boshqa ma’muriy axborotlarga egaligi nuqtai nazaridan axborot kutubxona tizimlarining o‘zak qismi hisoblanadi. Ma’lumotlar yaxlitligini saqlashning asosiy chorasi bu rezerv nusxalashdir [76]. Rezerv nusxalash malakali mutaxassislar tomonidan amalga oshirilishi va rezerv nusxalar har tomonlama himoyalangan maxsus joyda saqlanishi kerak.

Shaxsiy ma'lumotlar xavfsizligi. Shaxsiy ma'lumot «shaxs to'g'risidagi hamma uchun ruxsat etilmagan axborotdir» [71; 379-b.]. ALA (American Library Association) axloq kodeksiga muvofiq kutubxonachi va kutubxona xodimlari barcha kutubxona foydalanuvchilarining qanday ma'lumotlarni qidirganligi va olganligi to'g'risidagi axborotlarning konfedensialligini saqlashlari kerak [68].

Shunday qilib, himoya qilinuvchi barcha axborot resurslarini quyidagi

$$R = \{R_{ij}^{k}, N, M_{slci}, S_{tn}, S_{kyf}, H_{str}\}\ (j = 1 \ldots qr)$$

ko'rinishda tavsiflash mumkin. Bu yerda,

R_{ij}^{k} - k – resurs sinfi, i – resurs tipi, j – resurs identifikatsiya raqami;

N – resursning narxi;

M_{slci} – resurs joylashgan muhit (s-shaxsiy kompyuterda, l-lokal tarmoqda, c-korporativ tarmoqda, i-internet tarmog'ida);

S_{tn} – bu t vaqt intervalida n foydalanishlar soni;

S_{kyf} – resursning konfidensiallik (k), yaxlitlik (y) va foydalana olishlik (f) shkalalari;

H_{str} – s subyektning, t vaqtgacha, r roldan foydalanishi;

qr – barcha resusrlar soni.

Axborot resurslarining saqlanish sharoiti, ulardan foydalanish tartibi, bahosi va foydalanish muhiti kabi barcha bo'lishi mumkin bo'lgan holatlarini o'z ichiga oluvchi $V = \{v_1,\ v_2,\ \ldots v_{nv}\}$ – vaziyatlar to'plami, nv – vaziyatlar soni;

Yuqorida axborot-kutubxona tizimlari va resurslariga nisbatan tahdidlar bir necha parametrlariga ko'ra tasniflangan edi. Ushbu tahdidlarni identifikatsiyalash usulini ko'rib chiqamiz. Barcha tahdidlar ularning xususiyatlarini aniqlovchi sinflar, tiplar, identifikatsiya raqamlaridan tashkil topgan.

Shunday qilib, barcha tahdidlarni $T = \{T_{ij}^{k}, R_{cyf}, U_e, V_n\}\ (j = 1 \ldots kt)$ formal ko'rinishda tavsiflash mumkin. Bu yerda,

T_{ij}^{k} - k – tahdid sinfi (antropogen, texnogen, tabiiy), i – tahdid tipi (ichki, tashqi), j – tahdid identifikator raqami;

R_i^{cyf} – resurs tipi va AX aspektlari (c – konfidensiallik, y – yaxlitlik, f – foydalana olishlik)ni buzish maqsadini xarakterlovchi tahdidlar obyekti identifikatori;

U_e – tahdidni amalga oshiruvchi e-usulning identifikatori;

V_n – tahdidni amalga oshiruvchi n-vositasining identifikatori;

kt – barcha tahdidlar soni.

AXT choralarini ham sinflar, tiplar va identifikator raqamlari ko‘rinishida tasvirlash mumkin. Barcha choralarni formallashgan ko‘rinishda quyidagicha tavsiflash mumkin: $C = \{C_{ij}^{k}, R_{kyf}\}(j = 1 \ldots mc)$. Bu yerda, C_{ij}^{k} - k – chora sinfi (Ogohlantirish, maskirovkalash, reglamentlash, boshqarish, to‘sish, aniqlash, xabar berish, tiklash, rezerv nusxa olish, monitoring qilish, majburlash, undash) [9], i – chora tipi (huquqiy, tashkiliy, apparat, fizik, dasturiy, psixologik) [39], j – tahdid identifikator raqami;

C_i^{kyf} – resurs tipi va AX aspektlari (k – konfidensiallik, y – yaxlitlik, f – foydalana olishlik)ni himoyalash maqsadini xarakterlovchi choralar identifikatori;

mc – barcha choralar soni.

KAKTda AXni baholash masalasi mavjud axborot resurslarni tasniflash, ularning muhimliligini baholash, himoyalanuvchi resurslarga nisbatan bo‘lishi mumkin bo‘lgan tahdidlarni hamda ularni bartaraf etish bo‘yicha himoya choralarini aniqlash asosida yechiladi. Chunki aniq bir tashkilotning AXni baholash uchun avvalo mavjud himoyalanuvchi resurslar muhimligini baholash talab etiladi. Shuning uchun ham himoyalanuvchi resurslar muhimliligi va bo‘lishi mumkin bo‘lgan tahdidlarga nisbatan mos himoya choralarini aniqlash masalasi ajratib olindi.

Xavfsizlikni baholash deganda, tizimni, belgilangan muhofaza modeliga, muhofaza qilishni ta’minlash standarti va texnik shartlarga mos kelish darajasini aniqlash maqsadida tekshirish tushuniladi [8, 340-b.].

Shunday qilib, KAKTda AXni baholash masalasi aniq v_i vaziyat(lar) uchun t_v tahdid(lar)ni hamda shu tahdidlarni bartaraf etish bo‘yicha c_t ratsional chora(lar)ni aniqlashga olib kelinadi. Shuningdek, himoyalanuvchi resurslarning bahosi himoya choralarining bahosiga teng yoki undan katta ($B_c \leq B_r$) bo‘lishi kerak.

Himoya choralari deganda, axborotni himoyalash uchun zarur bo‘lgan barcha usul, vosita va mexanizmlarni nazarda tutilmoqda.

Ushbu bo‘limda korporativ axborot-kutubxona tarmoqlarida ilmiy-texnik va ta’limga oid resurslarni himoyalashning kompleks ta’minoti tadqiq etildi. Himoyalanuvchi resurslar, axborot xavfsizligiga tahdidlar va himoya choralari identifikatsiyalandi va tasniflandi.

2.2 Elektron kutubxona axborot xavfsizligini baholash va ta’minlashning noravshan moslik modeli

Ushbu bo‘limda korporativ axborot-kutubxona tarmoqlarida axborot xavfsizligini baholash masalasining matematik modeli ishlab chiqiladi.

Himoyani talab etuvchi axborot resurslari hamda ularga nisbatan parametrlari oldindan ma’lum bo‘lmagan yoki noto‘liq va noravshan xususiyatga ega bo‘lgan tahdidlar sonining doimiy oshib borishi AXT tizimlariga ham yangicha talablar qo‘yib, ularni intellektuallashtirishni taqozo etmoqda [25; 49-b.]. AXning intellektual tizimlariga quyidagi vazifalar qo‘yiladi: 1) xususiyatlari dinamik o‘zgarib boruvchi tahdidlar tiplarini identifikatsiyalash; 2) identifikatsiyalangan tahdidlarni zudlik bilan bartaraf etish bo‘yicha himoya mexanizlarini aniqlash yoki himoya mexanizmlarining yangi tiplariga talablarni shakllantirish; 3) axborot tizimi AX holatini intellektual

monitoring qilish; 4) AXT tizimining ma’lumotlar va bilimlar bazasini shakllantirish, boyitib borish va boshqalar [16; 4–5-b.];

Bunday tizimlarni tavsiflash va tadqiq qilishning bir qancha usullari bo‘lib, quyida noravshan kognitiv kartalar, noravshan moslik modellari va iyerarxik tahlil usullari haqida bayon etiladi.

Noravshan kognitiv kartalar. Noravshan kognitiv kartalar qaror qabul qilishga va sust shakllangan jarayonlarni boshqarishga ko‘maklashuvchi nazariyaning zamonaviy yo‘nalishlardan biri hisoblanadi [26; 59-b.]. Kognitiv yondashuv muammoni yechishning intellektual jarayonlarini qo‘llab quvvatlovchi, kognitiv (idrok etish, tasavvur qilish, anglash, tushunish, tushuntirish) imkoniyatlarni o‘z ichiga olgan formal usul va modellarini ishlab chiqishga asoslanadi. Kognitiv modellashtirish kognitiv kartalarni o‘z ichiga olib, ular tadqiq etilayotgan muammo yoki vaziyatlar yuzasidan subyektiv (individual yoki jamoaviy) qarashlarni tavsirlaydi. Kognitiv kartalarning asosiy elementi omillar (yoki konseptlar) va ular o‘rtasidagi sabab-oqibat bog‘liqliklar hisoblanadi [29; 317-b.].

Kognitiv modellashtirishning noravshan mantiq apparati bilan qo‘llanilishi uning imkoniyatlarini yanada oshiradi. Modellashtirish jarayonida noravshan kognitiv kartalarni qo‘llash birinchi bo‘lib B.Kosko tomonidan taklif etilgan [11; 218-b.]. Noravshan kognitiv kartalar noravshan yo‘naltirilgan graf ko‘rinishida berilib, uning cho‘qqilari noravshan to‘plamlar bo‘ladi. Grafning yo‘naltirilgan qobiqlari nafaqat konseptlar o‘rtasidagi sabab-oqibat bog‘lanishni tasvirlaydi, balki bog‘liq konseptlar o‘rtasidagi ta’sir darajasini (vaznni) aniqlaydi. Qobiqning vazni [-1, 1] kesmadagi sonni yoki masalan, {kichik, o‘rta, katta} turidagi bir nechta lingvistik shkalaning qiymatini ifodalaydi. Noravshan qoidalar AGAR-U HOLDA ko‘rinishida beriladi [10]. 2.2-rasmda «Vaziyat-Tahdid-Chora» turidagi noravshan kognitiv kartalar tasvirlangan.

Noravshan kognitiv kartalar formal ko‘rinishida quyidagicha beriladi:

$$NKK = \{C_n, L_{ij}, G_{ij}, W_{ij}\},$$

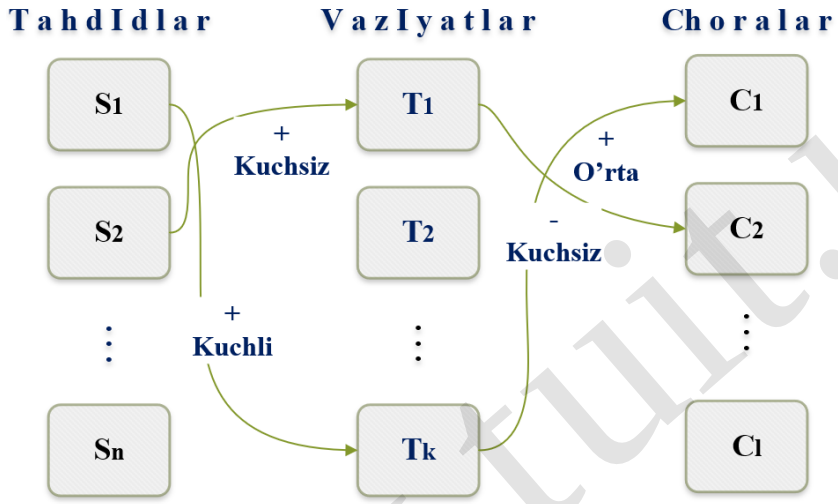
bu yerda,

C_n – cho‘qqi (konsept)larning chekli to‘plami;

L_{ij} – konseptlar o‘rtasidagi sabab-oqibat bog‘lanishlarning chekli to‘plami;

G_{ij} – (+, –) bog‘liqliklar belgilarining chekli to‘plami;

W_{ij} – bog‘liqliklar vaznlarining chekli to‘plami (kuchli, o‘rtacha, kuchsiz).



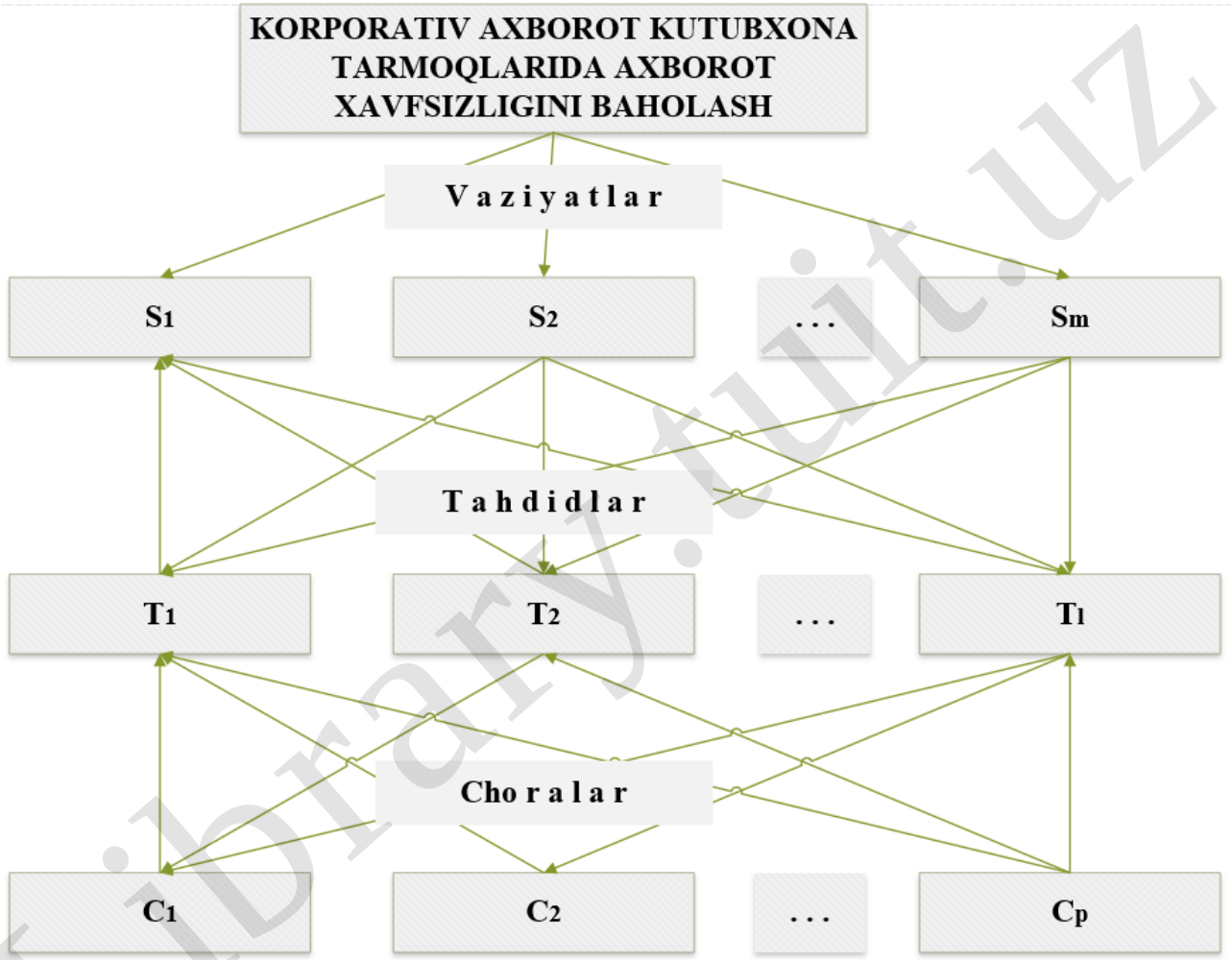
2.2-rasm. «Vaziyat-Tahdid-Chora» turidagi noravshan kognitiv karta

Har bir C_i konsept vaziyatning bir yoki bir nechta o‘zgaruvchilarini ifodalaydi. L_{ij} bog‘liqlik esa C_i omilning C_j omilga ta’sirini xarakterlaydi. Agar C_j konsept vaziyat o‘zgaruvchisining qiymati C_i konseptning kuchayishiga yoki kamayishiga qarab kuchaysa yoki kamaysa, ular orasidagi bog‘liqlik musbat ($G_{ij} = +$) bo‘ladi. Aksincha, C_j konsept vaziyat o‘zgaruvchisining qiymati C_i ning kamayishida kuchaysa va kuchayishida kamaysa, bog‘liqlik manfiy ($G_{ij} = -$) bo‘ladi. W_{ij} bog‘liqlik vazni C_i konseptning C_j konseptga ta’sir kuchini ifodalaydi va lingvistik termlarda aniqlanadi.

Konseptlarni, uning vaziyatlari o‘zgaruvchilarini va ular orasidagi bog‘liqliklarni aniqlash yuqori malakali ekspertlar zimmasiga yuklatiladi.

Iyerarxik tahlil usuli. Iyerarxik tahlil usuli o‘rganilayotgan muammoga ta’sir etuvchi omillarni iyerarxik tasvirlash uchun foydalanilib, qaror qabul qiluvchiga tegishli omillarning muhimliligini subyektiv baholash imkonini beradi [17; 68-b.]. Demak, AX

masalasini tadqiq qilishda bir yoki bir nechta ekspertlar fikrlari asosida tizimdagi har bir element vaznini baholashda iyerarxik tahlil usulidan foydalanish mumkin. Buning uchun avvalo muammoni iyerarxik ko‘rinishda tasvirlash lozim. Ya’ni bosh maqsad, unga ta’sir etuvchi omillar va shu omillar uchun muqobillar aniqlanadi. So‘ngra elementlar o‘rtasidagi ustuvorliklar aniqlanadi (2.3-rasm).



2.3-rasm. Korporativ axborot-kutubxona tarmoqlarida axborot xavfsizligini baholash muammosining iyerarxik tasvirlanishi

Iyerarxiyaning har bir darajasi uchun elementlar ustuvorliklarini iyerarxiyaning yuqori darajasidagi elementlarga nisbatan taqqoslash lozim. Birinchi bo‘lib, bosh maqsadni amalga oshirishda S_i vaziyat S_j vaziyatga nisbatan qanday darajada muhimligini ko‘rsatish orqali vaziyatlar ustuvorliklari aniqlanadi. Agar S_i ni S_j bilan

taqqoslash natijasida $s_{ji} = b$ bo‘lsa, u holda teskari taqqoslashda $a_{ij} = 1/b$ bo‘ladi. Natijada $A = (a_{ij})$ juft taqqoslash matritsasi hosil bo‘ladi:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

Shundan so‘ng, ekspertlar fikri hamjihatligining buzilish darajasini ko‘rsatuvchi hamjihatlik indeksi (HI) aniqlanadi. Hamjihatlik indeksi quyidagi formula orqali aniqlanadi:

$$HI = \frac{\lambda_{max} - n}{n-1}, \qquad (2.1)$$

bu yerda λ_{max} – matritsaning maksimal xususiy qiymati; n – obektlar soni.

A matritsaning maksimal xususiy qiymatiga mos xususiy vektorni topish uchun quyidagi amallarni bajarish kerak:

1. A matritsaning har bir satri uchun xususiy vektor komponentini hisoblash:

$$a_i = \sqrt[n]{a_{i1} * a_{i2} * a_{i3} * a_{i4}} \qquad (2.2)$$

2. a vektor elementlarini shunday normalashtirish kerakki, ularning yig‘indisi 1 ga teng bo‘lsin. Normallashgan vektorning elementlari vaziyatlarning mos ustuvorliklari hisoblanadi va u quyidagi formula bilan hisoblanadi [13]:

$$k_i = \frac{a_i}{\sum_i a_i} = \frac{\sqrt[n]{\prod_j a_{ij}}}{\sum_i a_i} \qquad (2.3)$$

3. A matritsaning har bir j ustuni uchun uning a_{ij} elementlari summasi tuziladi:

$$b_j = a_{1j} + \cdots + a_{nj} = \sum_{i=1}^{l} a_{ij}. \qquad (2.4)$$

4. Matritsaning maksimal xususiy qiymati quyidagi formula bo‘yicha hisoblanadi:

$$\lambda_{max} = b_1 * k_1 + \cdots + b_n * k_n. \qquad (2.5)$$

Endi hamjihatlik munosabati (HM) quyidagi formula bo‘yicha hisoblanadi [17]:

$$HM = \frac{HI}{TI}, \qquad (2.6)$$

bu yerda TI – tasodifiy indeks. Hamjihatlik munosabati 10 % dan oshmasligi kerak. Aks hoda juft taqqoslash matritsasi hamjihat emas deb hisoblanadi.

Endi iyerarxiyaning uchinchi darajasidagi elementlar (tahdidlar)ning ikkinchi darajadagi elementlar (vaziyatlar)ga nisbatan muhimliligining qiyosiy tahlilini amalga oshirish zarur. Ushbu harakatning algoritmi ham huddi iyerarxiyaning ikkinchi darajasidagi kabi bo‘lib, $T = \{T_i\}$ tahdidlar to‘plamining har bir $S_j \in S(j = \overline{1,m})$ vaziyat bo‘yicha ustuvorliklarini topish lozim. j vaziyat uchun tahdidlar to‘plamining ustuvorlik vektorini $Q\left(S_j = \left\{Q_i\left(S_j\right), i = l,\ j = m\right\}\right)$ ko‘rinishda tasvirlash mumkin.

T to‘plamning T_i elementi uchun w_i umumiy vazn quyidagi formula bilan hisoblanadi.

$$w_i = \sum_j^m \sum_i^l q_j * Q_i\left(S_j\right). \qquad (2.7)$$

Navbatdagi masala iyerarxiyaning to‘rtinchi darajasidagi elementlar (himoya choralari) muhimliligini uchinchi darajadagi elementlar (tahdidlar)ga ko‘ra qiyosiy tahlilini amalga oshirishdan iborat. Buning ham algoritmi oldingi darajadagilar bilan o‘xshash bo‘ladi.

Umumiy vazn z_i himoya choralarini tanlashga ta’sir ko‘rsatuvchi tahdidlarning ustuvorliklarini hisobga olgan holda hisoblab chiqiladi.

Ekspertlar tomonidan olingan axborotlar hamjihatlikka tekshirilishi kerak. Uni W konkordatsiya koffitsenti yordamida baholash mumkin [12]. U quyidagi formula yordamida topiladi:

$$W = \frac{12S}{n^2 m(m^2-1)} \qquad (2.8)$$

bu yerda

$$S = \sum_{i=1}^m \left(\{\sum_{i=1}^n \mu_{ij} - \frac{n(m+1)}{2}\}\right)^2 \qquad (2.9)$$

n – ekspertlar soni;

m – omillar soni;

μ_{ij} – i-elementga j-ekspert tomonidan berilgan tegishlilik funksiyasi;

Jamoaviy ekspert baholash barcha ekspertlarning har bir element bo‘yicha individual ekspert bahosining o‘rta arifmetigi bilan hisoblanadi.

Axborot xavfsizligini baholashning xususiy noravshan moslik modeli. T.Nusratov o‘z ishida birinchilardan bo‘lib tuzilmaviy moslik modellari asosida qaror qabul qilish tizimlarini yaratish usullarini ko‘rsatgan [57]. M.Raxmatullev ishida esa noravshan texnologik muhitlarda yechimlar generatsiyasini qurishda noravshan moslik modellaridan foydalanilgan [61]. Noravshan moslik modellari Ti Min Fiong tomonidan tibbiyot sohasida texnologik jarayonlarni boshqarishda qo‘llanilgan [66].

Noravshan munosabatlar noravshan to‘plamlar nazariyasining muhim tushunchalaridan biri bo‘lib, u ko‘pgina qaror qabul qilish masalalarining matematik modellarini formallashtirish va tahlil qilishga imkon beradi [84; 65-b.].

1-ta’rif. $x_1, x_2, \dots, x_n$ to‘plamdagi $\tilde{R}$ noravshan munosabat deb, $x_1 \times x_2 \times \dots \times x_n$ dekart ko‘paytmasining noravshan ost to‘plamiga aytiladi. $\mu_{\tilde{R}}(x_1, x_2, \dots, x_n)$ tegishlilik darajasi [0, 1] kesmada berilib, $(x_1, x_2, \dots, x_n), x_i \in X_i, i = \overline{1,n}$ elementlar orasidagi $\tilde{R}$ munosabatning bajarilishini ko‘rsatadi va u subyektiv o‘lchovni xarakterlaydi [36; 183–185-б., 32; 8-б.].

Binar noravshan munosabatlar ikkita to‘plamning dekart ko‘paytmasi sifatida beriladi. Ushbu to‘plamlarni X va Y lar orqali belgilaymiz. Bunda $X \times Y$ dagi $\tilde{R}$ noravshan munosabat $\mu_{\tilde{R}}(x, y)$ ko‘rinishida berilib, bu yerda $(x, y) \in X \times Y$.

Noravshan moslik modeli (NMM) deganda, obyektning $\tilde{\Gamma} = (X, Y, \tilde{F})$ ko‘rinishidagi formallashgan tasvirlanishi tushuniladi. Bu yerda X, Y ravshan to‘plamlar. $\tilde{F}$ esa $X \times Y$ sohada noravshan to‘plam [55; 23–24-b.].

X va Y to‘plamlar chekli bo‘lganda noravshan moslik grafik va matritsa ko‘rinishida berilishi mumkin. Matritsa ko‘rinishida $\tilde{\Gamma} = (X, Y, \tilde{F})$ noravshan moslik R matritsa insidenti yoki moslikning tuzilmaviy modeli yordamida beriladi. Satrga $x_i \in$

$X(i \in I = \{1, 2, \dots, n\})$ elementlar, ustuniga $y_j \in Y(j \in J = \{1, 2, \dots, m\})$ elementlar joylashtiriladi. x_i satr va y_j ustunlar kesishmasiga $r_{ij} = \mu(x_i, y_j)$ elementi qo‘yiladi (2.2-jadval). Bu yerda μ, $X \times Y$ noravshan grafikning elementlari tegishlilik funksiyasi.

Noravshan modellarni qurishdagi asosiy bosqichlardan biri bu modelda foydalanish ko‘zda tutilgan lingvistik o‘zgaruvchilarning qiymatini tavsiflovchi tegishlilik funksiyasini qurishdir. Tegishlilik funksiyasini qurishda ekspert baholash usulidan foydalaniladi [32; 8-b.].

2.2-jadval

Noravshan moslik modelining matritsa ko‘rinishida berilishi

VAZIYATLAR	TAHDIDLAR				
	Y_1	Y_2	Y_3	...	Y_m
X_1	$\mu(x_1, y_1)$	$\mu(x_1, y)$	$\mu(x_1, y_3)$	...	$\mu(x_1, y_m)$
X_2	$\mu(x_2, y_1)$	$\mu(x_2, y_2)$	$\mu(x_2, y_3)$	...	$\mu(x_2, y_m)$
X_3	$\mu(x_3, y_1)$	$\mu(x_3, y_2)$	$\mu(x_3, y_3)$	...	$\mu(x_3, y_m)$
.....	.....	.....	.....	.....	.....
X_n	$\mu(x_n, y_1)$	$\mu(x_n, y_2)$	$\mu(x_n, y_3)$	...	$\mu(x_n, y_m)$

X, Y va Y,Z to‘plamlari uchun kompozitsion noravshan moslik modeli: $\tilde{G} = \tilde{\Gamma}_1 \circ \tilde{\Gamma}_2$ ko‘rinishida beriladi [25]. Bu yerda $\tilde{\Gamma}1 = (X, Y, \tilde{F}1)$, $\tilde{\Gamma}2 = (Y, Z, \tilde{F}2)$ yoki $\tilde{G} = (X, Y, Z\ \tilde{F})$, bu yerda $\tilde{F}$ – $\tilde{F}1$ va $\tilde{F}2$ kompozitsiyasi grafigi.

$\tilde{F}1$ uchun satrga $x_i \in X(i \in I = \{1, 2, \dots, n\})$ elementlar, ustunga $y_j \in Y(j \in J = \{1, 2, \dots, p\})$ elementlar joylashtiriladi. Mos holda $\tilde{F}2$ uchun satrga $y \in Y_j$, ustunga $z_k \in Z(k \in K = \{1, 2, \dots, m\})$ elementlar joylashtiriladi. x_i satr va y_j ustunga $g_{ij} = u_G(x_i, y_j)$, shuningdek y_j satr va z_k ustun kesishmasiga $g_{jk} = u_G(y_j, z_k)$ element qo‘yiladi. u_G – $\tilde{G}1$ va $\tilde{G}2$ noravshan grafiklar tegishli bo‘lgan X, Y, Z elementlarning tegishlilik funksiyasi.

2.3-jadvalda tasvirlangan «Vaziyat-Tahdid-Chora» tipidagi NMM parametrlarining fizik ma’nosi quyidagicha:

$V = \{v_1,\ v_2,\ \dots v_m\}$ – axborot resurslarining barcha bo‘lishi mumkin bo‘lgan holatlarini o‘z ichiga oluvchi vaziyatlar to‘plami;

$T = \{t_1,\ t_2,\ \dots t_n\}$ – axborot resurslari uchun barcha bo‘lishi mumkin bo‘lgan tahdidlar to‘plami;

$C = \{c_1,\ c_2,\ \dots c_l\}$ – tahdidlarni bartaraf etish choralari to‘plami.

Vaziyatlar to‘plami amaliyotda AXni ta’minlash jarayonida yuzaga kelgan aniq holatlar asosida shakllantiriladi. Tahdidlar va himoya choralari to‘plami sifatida esa umumqabul qilingan tahdidlar va himoya choralarining bazalari hamda Davlat standartlardan [5,7] foydalanish mumkin[7].

Amaliyotda R, T va C to‘plamlar o‘rtasidagi moslikni aniqlash nisbatan murakkab masala hisoblanib, ularni mavjud determinanlashgan usullar bilan yechish ijobiy natija bermaydi [87, 56; 240-b.]. Shuning uchun ham bir nechta asoslar borki, ushbu masalani yechishda noravshan to‘plamlar nazariyasi usullarini qo‘llash ehtiyojini tug‘dirdi.

Birinchidan, axborot muhitining o‘zgarib turuvchi sharoitida axborot manbaini baholash uchun real kattalikning istalgan aniqligida o‘lchashning mumkin emasligi. Masalan, ayni vaqtda ilmiy axborotlarning qiymatini baholash juda qiyin. U murojaatlar va shu sohadagi ilm-fanning rivojlanish darajasiga bog‘liq holda o‘zgarib turadi.

Ikkinchidan, ko‘plab obyektlar va vaziyatlarni to‘liq va aniq tavsiflashning mumkin emasligi. Axborotni himoyalash bo‘yicha qaror qabul qilish uchun ma’lum darajadagi formallashtirish va sonli baholarning (taxminiy bo‘lsa ham, ammo ilmiy asoslangan) mavjudligi talab etiladi;

Uchinchidan, model o‘lchamining yetarli darajada katta emasligi axborot muhiti obyektlarining barcha muhim xususiyatlarini aks ettirishga imkon bermaydi. Ilmiy axborotlarni baholash parametrlari va axborot muhitining turli vaziyatlarini ifodalovchi

[7] https://bdu.fstec.ru/threat – Axborot xavfsizligi tahdidlarining ma’lumotlar banki.

ko‘rsatkichlarining barchasi ham son jihatdan baholash va qat’iy formallashtirishga tushmaydi. Ekspertlarning oldingi tajribalarini hisobga olib, intuitiv ravishda baholash talab etiladi.

To‘rtinchidan, axborot muhitining intuitiv ravishda baholash uchun talab etiladigan bir qancha xususiyatlarining kuzatilmasligi [63; 334-b.].

Shuning uchun ham KAKTda AXB masalasini yechish bilan bog‘liq usullarni rivojlantirishda, resurslarni himoya qilish bo‘yicha qaror qabul qilish uchun boshlang‘ich axborotlarning noaniqligi sharoitida noravshan mantiq apparatini qo‘llash zaruriyati paydo bo‘ladi. Ushbu sinfdagi masalalarni yechishda noravshan to‘plamlar nazariyasi usullarini qo‘llash AX sohasidagi ekspert-mutaxassislar tomonidan sust shakllangan, murakkab masalalarni yechish uchun to‘plangan qimmatli tajribalaridan foydalanish mumkinligi bilan izohlanadi. NMMning graf ko‘rinishi yo‘naltirilgan graf bo‘ladi. Har bir qobiq $\mu(x_i, y_j)$ tegishlilik funksiyasining qiymati bilan beriladi (2.3-rasm).

NMM biyektiv yoki inyektiv bo‘lmaganligini uchun noravshan syuryektiv moslikdan foydalanamiz. Syuryektiv moslik $V \rightarrow T(T \rightarrow C)$ ko‘rinishida bo‘lib, u bir yoki bir nechta $v_j \in V$ elementdan tashkil topgan har bir $t_i \in T$ elementni to‘liq akslantiradi. Bunda noravshan mulohazalar tizimi quyidagi ko‘rinishda bo‘ladi:
«Vaziyat-Tahdid» moslik bo‘yicha:

$$N = \begin{cases} N1\text{: (Агар } v_1\text{, у ҳолда } \mu/t_1) \\ N2\text{: (Агар } v_2\text{, у ҳолда } \mu/t_2) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ Nm\text{: (Агар } v_n\text{, у ҳолда } \mu/t_n) \end{cases},$$

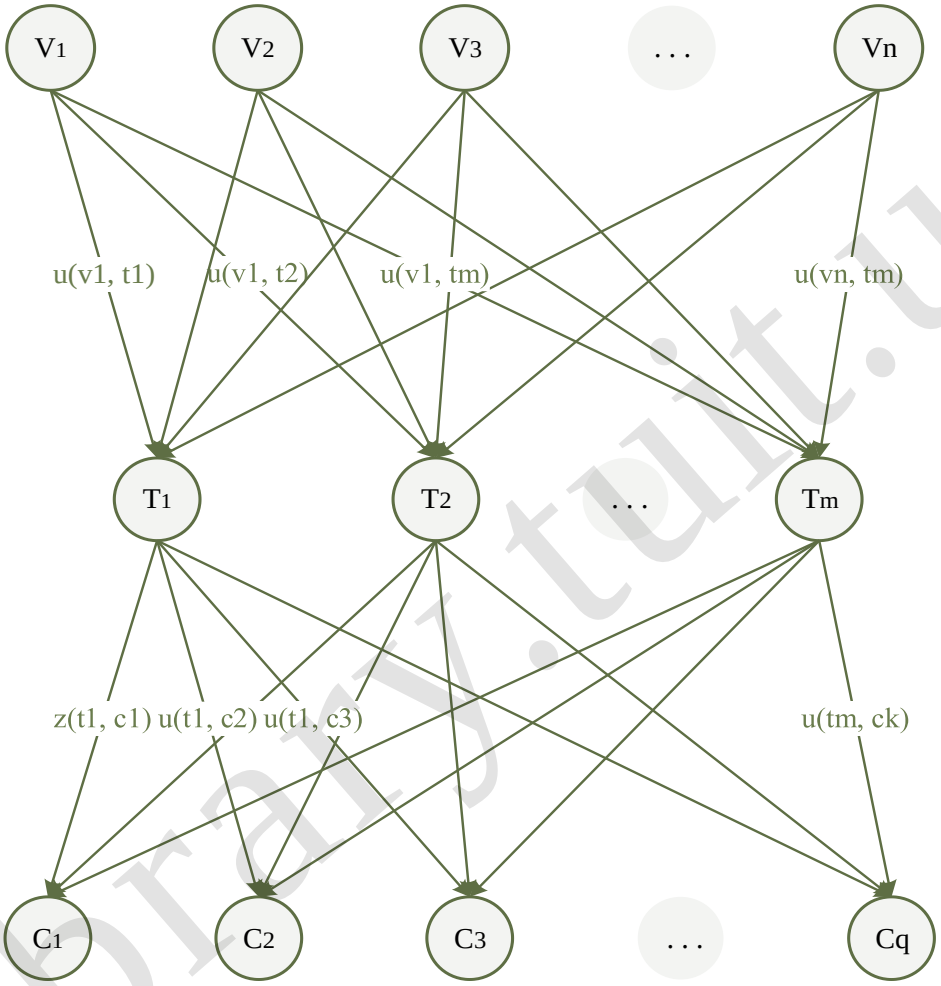
2.3-jadval

«Vaziyat-Tahdid-Chora» tipidagi noravshan moslik modeli

AXBOROT MUHITI VAZIYATLARI BELGILARI				**TAHDIDLAR**		**Tahdidlarni bartaraf etish CH O R A L A R I**			
						C_1	C_2	…	C_m
						t ye r m l a r			
V_1	V_2	…	V_n	Lingvis-tik o‘zgaruv-chilar	termlar	$t_c^1 \dots t_c^l$	$t_c^1 \dots t_c^n$		$t_c^1 \dots t_c^q$
$\mu(v_1, t_p^1)$	$\mu(v_2, t_p^1)$	…	$\mu(v_n, t_p^1)$	T_1	t_p^1	$\mu(t_p^1, t_c^1)$	$\mu(t_p^1, t_c^1)$	…	$\mu(t_p^1, t_c^1)$
$\mu(v_1, t_p^2)$	$\mu(v_2, t_p^2)$	…	$\mu(v_n, t_p^2)$		t_p^2	$\mu(t_p^2, t_c^2)$	$\mu(t_p^2, t_c^2)$	…	$\mu(t_p^2, t_c^2)$
…	…	…	…		…	…	…	…	…
$\mu(v_1, t_p^k)$	$\mu(v_2, t_p^k)$	…	$\mu(v_n, t_p^k)$		t_p^k	$\mu(t_p^k, t_c^l)$	$\mu(t_p^k, t_c^n)$	…	$\mu(t_p^k, t_c^q)$
…	…	…	…	…		…	…	…	…
$\mu(v_1, t_p^1)$	$\mu(v_2, t_p^1)$	…	$\mu(v_n, t_p^1)$	T_k	t_p^1	$\mu(t_p^1, t_c^1)$	$\mu(t_p^1, t_c^1)$	…	$\mu(t_p^1, t_c^i)$
$\mu(v_1, t_p^2)$	$\mu(v_2, t_p^2)$	…	$\mu(v_n, t_p^2)$		t_p^2	$\mu(t_p^2, t_c^2)$	$\mu(t_p^1, t_c^2)$	…	$\mu(t_p^1, t_c^i)$
…	…	…	…		…	…	…	…	…
$\mu(v_1, t_p^m)$	$\mu(v_2, t_p^m)$	…	$\mu(v_n, t_p^m)$		t_p^m	$\mu(t_p^m, t_c^l)$	$\mu(t_p^m, t_c^n)$	…	$\mu(t_p^m, t_c^q)$

«Tahdid-Chora» moslik bo‘yicha:

$$N = \begin{cases} N1: (Agar\ t_1,\ u\ holda\ \mu/c_1) \\ N2: (Agar\ t_2,\ u\ holda\ \mu/c_2) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ Nm: (Agar\ t_n,\ u\ holda\ \mu/c_n) \end{cases}.$$



2.4-rasm. Noravshan moslik modelining graf ko‘rinishida berilishi

Yuqorida keltirilganlar asosida axborot muhitining bo‘lishi mumkin bo‘lgan barcha V holatlarida unga nisbatan qanday T tahdidlar borligini va shu tahdidlarning resursga xavflilik darajasini, shu bilan birga bir vaqtning o‘zida ushbu tahdidlarga qarshi C choralar borligini va bu choralarning muayyan tahdidni samarali bartaraf etishga mosligini aniqlash masalasini yechish mumkin.

Korporativ axborot-kutubxona tizimlari xavfsizligini baholashda yuqorida keltirilgan uchta usulning ham bir xil kamchiligi bor. Ya’ni ushbu usullarda axborot

xavfsizligini baholash choralarini tanlashda uning himoya qilinuvchi axborot va unga nisbatan tahdidning bahosi e’tiborga olinmaydi.

Axborot xavfsizligi nazariyasidan ma’lumki axborotni himoyalash uchun talab etiladigan usul va vositalarning bahosi axborotning o‘zining bahosidan ortiq bo‘lmasligi, balki unga mutanosib bo‘lishi kerak. Ya’ni

$$B_c \leq B_r$$

tenglik bajarilishi kerak. Bu yerda B_r – resursning, B_c – choraning bahosi.

Keyingi bo‘limda resurslar, tahdidlar va himoya choralarining baholarini aniqlash usuli bayon etiladi.

Ushbu bo‘limda axborot resurslari xavfsizligini baholashning xususiy noravshan moslik modeli ishlab chiqildi. Shuningdek, noravshan moslik modellarining berilish shakllari keltirilgan.

2.3 Korporativ kutubxona tarmoqlarida resurslar muhimliligini baholash usuli

Ushbu bo‘limda himoyalanuvchi resurslarning muhimliligi va himoya choralarining tahdidlarni bartaraf etishga mosligini baholash usuli keltiriladi.

Yuqorida ta’kidlanganidek, himoya obyektining muhimliligini baholash obyektni himoyalash uchun usul va vositalarini tanlashda muhim omil hisoblanadi. Ya’ni, axborotni himoyalash uchun talab etiladigan usul va vositalarning bahosi axborotning o‘zining bahosidan ortiq bo‘lmasligi, balki unga mutanosib bo‘lishi kerak. Shuning uchun ham KAKTlarning ITT resurslarining muhimliligini baholash masalasi ishning vazifalaridan biri qilib qo‘yilmoqda.

Aslida vaqt o‘tishi bilan qiymati o‘zgarib turuvchi axborot resurslarini axborot xavfsizligi nuqtai nazaridan baholash sezilarli darajadagi murakkab masala hisoblanadi [88; 433-b.]. Chunki, AX sohasida mazkur masalaga qaratilgan standartlar, meyoriy hujjatlar yoki usullar yetarli darajada ishlab chiqilmagan. Hozirda axborot tizimlari xavfsizligini baholashning etalon bo‘yicha, riskka yo‘naltirilgan va iqtisodiy ko‘rsatkichlar asosida baholash usullari qo‘llaniladi [54; 448-b.].

Etalon bo‘yicha baholashda tashkilotning AXT bo‘yicha choralarini etalonda keltirilgan talablar bilan taqqoslanadi va so‘nggida tashkilot joriy holatining talablarga qanchalik mos kelishi ko‘rsatiladi. Talablar sifatida Davlatning AXT bo‘yicha qonunchiligi, AXT bo‘yicha sohaviy talablari, tashkilotning AXT bo‘yicha talablari, milliy va xalqaro standartlar, shuningdek, ekspertlarning baholari qaralishi mumkin.

Riskka yo‘naltirilgan baholashda axborotning bahosi uning xavfsizligi buzilganda yetkaziladigan zararning qiymati bilan aniqlanadi [23].

Bugungi kunga qadar axborot aktivlarini iqtisodiy ko‘rsatkichlar asosida baholashga qaratilgan bir qancha tadqiqot ishlari olib borilgan. Nikola Laskovskiy o‘z ishida axborot aktivlari bahosini aniqlashning olti usulini keltiradi: axborotning ichki qiymati, axborotning biznes uchun qiymati, axborotning samaradorlik qiymati, axborotning xarajatga nisbatan qiymati, axborotning iqtisodiy qiymati, axborotning bozorga nisbatan qiymati [80]. Dmitriy Belyayev esa axborot aktivlarini baholashning uch yo‘lini ajratib ko‘rsatadi [18]:

- daromadga qaratilgan baholash. Daromadga qaratilgan baholashda foydadagi imtiyozlar va xarajatdagi imtiyozlarga e’tibor qaratiladi. Foydadagi imtiyozlar mazkur axborot resursidan foydalanilganda keladigan foydani hisoblashga asoslanadi. Foydaga qaratilgan usulni qo‘llashning asosiy maummosi qo‘shimcha foydaning qiymatini hisoblashdir. Xarajatdagi
imtiyozlar usuli mazkur axborot resursini qo‘llash natijasida xarajatlarning kamayishiga asoslanadi;

- sarfga qaratilgan baholash. Sarfga qaratilgan usul mazkur axborot resursini yaratish va joriy etish bilan bog‘liq faktik sarflarni aniqlashga asoslangan.

- qiyosiy usul asosida baholash. Qiyosiy usul axborot resurslari bozori asosida axborot aktivi bahosini shakllantiradi. Bunda axborotning bahosi boshqa korxonalardagi o‘xshash axborot banklari asosida tahlil qilinadi.

Daniyel Mudiy va Piter Volsh o‘z ishlarida axborotning qiymati va bahosini ajratib, axborotning qiymati uni qo‘lga kiritish, saqlash va qayta ishlashga ketgan

xarajat bilan, uning bahosi esa tashkilot yoki korxona uchun qanchalik muhimliligi bilan aniqlanishini ko‘rsatadilar [81]. Bundan tashqari axborotning hamda axborot xizmatining qiymatlari ham ajratiladi.

Kris Haygson va Dav Valto fikriga ko‘ra, axborot aktivini baholashning xavfsizlikka yo‘naltirilgan yondashuvida texnik mutaxassislarning faolligi birinchi o‘ringa chiqishi kerak [77].

Axborot aktivini baholashda vaqt omili muhim ahamiyatga ega. Ayrim axborotlarning bahosi vaqt o‘tishi bilan o‘zgarib borishi mumkin (masalan, vaqt o‘tgan sari dissertatsiya ishlari yoki ilmiy maqolalar bahosi kamaysa, qadimiy va noyob asarlarning bahosi ortib boradi). Shuning uchun ham axborotning muhimliligini baholashni statik va dinamik formalarga ajratish lozim.

Axborot juda yuqori qiymatli bo‘lishiga qaramasdan, axborotdan o‘z vaqtida unumli foydalana olmaslik, axborot savodxonligi ko‘nikmasining kamligi yoki axborot to‘g‘risida xabardorlikning pastligi tufayli uning bahosi oshmasligi mumkin [81]. Ya’ni, agar axborotdan foydalanilmasa, uning bahosi o‘z-o‘zidan oshmaydi. Antonio Lerro va boshqalarning fikriga ko‘ra, axborot aktivini baholash jarayoni uni identifikatsiyalash, klassifikatsiyalashdan boshlanishi kerak [69; 466-b.].

Y.Maliy va V.Aleksandrovlarning bayon etishicha axborot aktivini baholashning universal usuli mavjud emas va u ekspertlar tomonidan aniqlanishi kerak [31; 196-b.].

Har bir tashkilot yoki korxona axborot tizimining AXni baholashda quyidagi omillar e’tiborga olinishi kerak: axborot o‘lchami, tashkiliy tuzilmasi; qayta ishlanadigan axborotlarning xususiyatlari (ilmiy-texnik, iqtisodiy, ishlab chiqarish, moliyaviy, harbiy, siyosiy) va ularning maxfiylik darajalari; tashkilotning moliyaviy imkoniyatlari; tashkilotning texnik imkoniyatlari; tashkilotning joylashuvi; ishlab chiqaradigan mahsulotlar nomenklaturasi; ichki hujjat aylanish tizimi; himoyani talab qiluvchi axborotlar hajmi; himoyani talab qiluvchi axborotlarga kirish nuqtalari; AXT bo‘yicha maxsus talablarning mavjudligi.

Resursning bahosini aniqlashda quyidagilar e’tiborga olinishi kerak: aktivni olish yoki ishlab chiqish uchun xarajatlar; aktivni qo‘llab-quvvatlash va himoyalash uchun xarajatlar; aktivning egasi va foydalanuvchilar uchun bahosi; aktivning raqobatchilar va buzg‘unchilar uchun bahosi; aktivni ishlab chiqishda foydalaniladigan intellektual mulk bahosi; aktiv uchun boshqalar to‘lashga tayyor turgan baho; aktiv yo‘qolganda uni almashtirish xarajati; aktivning kompaniyadagi ahamiyati va foyda miqdori [93].

Shunday qilib, KAKT resurslari muhimliligini baholash uchun $M = \{M_1,\ M_2,\ M_3,\ M_4\}$ noravshan qiymatlarni qabul qiluvchi $\Omega_R =$ *«Resursning axborot xavfsizligi nuqtai nazaridan muhimliligi» noravshan o‘zgaruvchisini kiritamiz. Bu yerda* $M_1 =$ *«Kam ahamiyatli»*, $M_2 =$ *«Ahamiyatli»*, $M_3 =$ *«Muhim»*, $M_4 =$ *«Juda muhim»* term qiymatlar.

M term-qiymatlardan iborat Ω_R to‘plamning tashuvchisini aniqlash uchun ekspert baholashning balli usulini keltiramiz. Resurslar muhimligiga ta’sir etuvchi omillar sifatida quyidagilar olinadi:

A_1 – resursning dastlabki qiymati (0 – bepul kelgan; 1 – 10 ming atrofida; 2 – 100 ming atrofida; 3 – 1 million atorida; 4 – 10 milliondan ortiq);

A_2 – resurs joylashgan muhit (0 – axborot tashuvchida; 1– kompyuterda; 2 – lokal tarmoqda; 3 – korporativ tarmoqda; 4 – global tarmoqda);

A_3 – resurs tipi (0 – ochiq axborotlar; 1 – korporativ axborotlar; 2 – pullik axborotlar; 3 – konfedensial axborotlar);

A_4 – resursdan foydalanish faolligi (0 – 1 yilda 1 marta ham foydalanilmasa; 1 – 1 yilda 10 martagacha foydalanilsa; 2 – 1 yilda 100 martagacha foydalanilsa; 3 – 1 yilda 1000 martagacha foydalanilsa; 4 – 1 yilda 1000 martadan ortiq foydalanilsa);

A_5 – butun axborot tizimining ishlashi jarayonida resursning muhimligi (0 – resurs xavfsizligi buzilishining butun tizim faoliyatiga ta’siri juda kam; 1 – resurs xavfsizligining buzilishi boshqa resurslar ayrim qismlarining ishlamay qolishiga sabab bo‘ladi; 2 – resurs xavfsizligining buzilishi boshqa resurslar bir qancha qismlarining ishlamay qolishiga sabab bo‘ladi; 3 – resurs xavfsizligining buzilishi

boshqa resurslar aksariyat qismlarining ishlamay qolishiga sabab bo‘ladi; 4 – resurs xavfsizligining buzilishi butun tizimning ishlamay qolishiga sabab bo‘ladi);

A_6 – tahdid amalga oshirilib resurs buzilganda uni tiklash qiymati (0 – past; 1– o‘rta; 2 – yuqori; 3 – juda yuqori; 4 – kritik);

A_7 – tahdid amalga oshib resurs buzilganda uni qayta tiklash vaqti (0 – kam; 1– o‘rta; 2 – ko‘p; 3 – juda ko‘p; 4 – kritik);

A_8 – resurs qisman yoki to‘liq buzilib, yo‘qotilgan vaziyatda uni tiklash imkoniyati (0 – oson; 1 – o‘rta; 2 – qiyin; 3 – juda qiyin; 4 – mumkin emas);

A_9 – resurs konfidensialligining buzilishi (0 – hech qanday zararni olib kelmaydi; 1 – ma’lum vaziyatlarda moddiy zararni olib keladi; 2 – kam miqdordagi ruhiy va/yoki moddiy zararni olib keladi; 3 – sezilarli darajadagi ruhiy va/yoki moddiy zararni olib keladi; 4 – yo‘l qo‘yib bo‘lmaydigan ruhiy va moddiy zararga yoki butun tizimning barbod bo‘lishiga olib keladi);

A_{10} – resurs yaxlitligining buzilishi (0 – hech qanday oqibatni keltirmaydi; (1 – oqbati seziladi, ammo ishning to‘xtab qolishiga sabab bo‘lmaydi; 2 – oqibati ortga qaytarish mumkin bo‘lgan noto‘g‘ri ishlashga olib keladi; 3 – oqibati noto‘g‘ri ishlashga olib kelib, uni ortga qaytarish ko‘p kuch va vaqtni talab qiladi; 4 – oqibati barcha resurslarning noto‘g‘ri ishlashi va oqibatni o‘zgartirib bo‘lmaslikka olib keladi);

A_{11} – foydalana olishlikning buzilishi (0 – foydalana olishlik bir necha kungacha buzilishga ruxsat etiladi; 1 – foydalana olishlik bir necha soatgacha buzilishga ruxsat etiladi; 2 – foydalana olishlik bir necha o‘n daqiqagacha buzilishga ruxsat etiladi; 3 – foydalana olishlik ko‘pi bir necha daqiqaga buzilishga ruxsat etiladi; 4 – foydalana olishlik buzilmasligi kerak);

A_1, A_2, A_3 ва A_4 omillar resurs haqidagi asosiy ma’lumotlarni, $A_5, A_6, A_7, A_8, A_9, A_{10}, A_{11}$ omillar esa resursning muhimlilik darajasini xarakterlaydi:

Jadvalni ekspertlar to‘ldirib, masalan Ω_R to‘plam tashuvchisi [0;28] kesmada bo‘ladi (2.4-jadval).

2.4-jadval

Ω_R to‘plam tashuvchisini hisoblash matritsasi

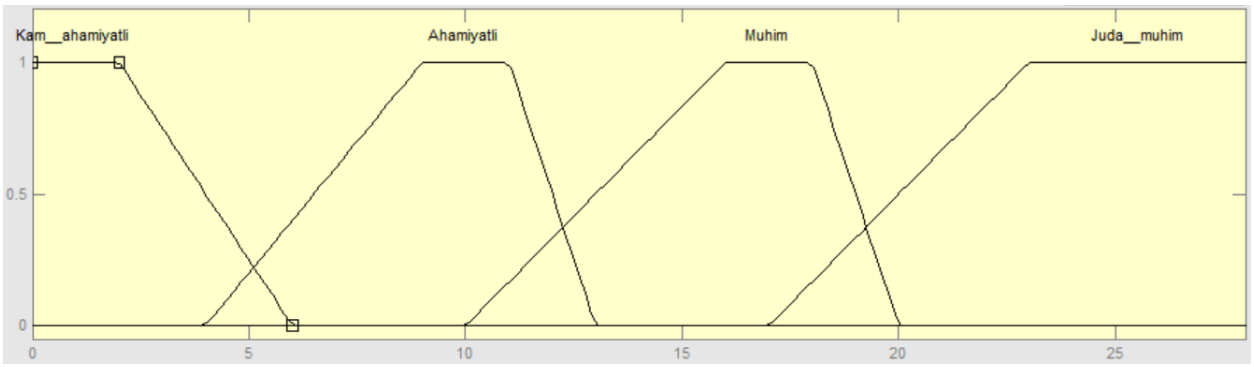
Omillar	Term-qiymatlar			
	M_1	M_2	M_3	M_4
A_5	0	0-1	1-2	2-4
A_6	0-1	1-2	1-3	2-4
A_7	0	1-2	2-3	2-4
A_8	0-1	0-2	1-3	3-4
A_9	0-2	1-2	2-3	2-4
A_{10}	0-1	0-2	1-3	3-4
A_{11}	0-1	1-2	2-3	3-4
$\sum M_i$	**0-6**	**4-13**	**10-20**	**17-28**

Har bir NT uchun M_1, M_2, M_3, M_4 term-qiymatlar bilan belgilanuvchi trapetsiyasimon ko‘rinishdagi $\mu_{M_j}(x_i)$ tegishlilik funksiyasining qiymatini belgilaymiz.

$$\mu_{M_1}(x) = \begin{cases} 1, & 0 \le x \le 2 \\ \frac{6-x}{4}, & 2 < x < 6 \\ 0, & 6 \le x \end{cases} \qquad \mu_{M_2}(x) = \begin{cases} 0, & x \le 4 \\ \frac{x-4}{5}, & 4 < x < 9 \\ 1, & 9 \le x \le 11 \\ \frac{13-x}{3}, & 11 < x < 13 \\ 0, & 13 \le x \end{cases}$$

$$\mu_{M_3}(x) = \begin{cases} 0, & x \le 10 \\ \frac{x-10}{6}, & 10 < x < 16 \\ 1, & 16 \le x \le 18 \\ \frac{20-x}{2}, & 18 < x < 20 \\ 0, & 20 \le x \end{cases} \qquad \mu_{M_4}(x) = \begin{cases} 0, & x \le 17 \\ \frac{x-17}{6}, & 17 < x < 23 \\ 1, & 23 \le x \le 28 \end{cases}$$

2.5-rasmda tegishlilik funksiya grafigi berilgan. Funksiya grafigi M_1, M_2, M_3, M_4 term-qiymatlarning tegishliligini ma’lum interval bilan tasvirlaydi.



2.5-rasm. Ω_R = «Resursning axborot xavfsizligi nuqtai nazaridan muhimliligi» noravshan o‘zgaruvchisining tegishlilik funksiyasi

Har bir resurs bo‘yicha ekspertlarning bali qo‘yiladi va 2.5-jadvaldagidek to‘ldiriladi.

2.5-jadval

Resurslar muhimliligi darajasining ko‘rsatkichlar matritsasi

Pecypc	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	K_{r_i}	μ_{D_1}	μ_{D_2}	μ_{D_3}	μ_{D_4}
r_1	2	3	1	2	2	2	1	0	2	1	3	*11(19)*	0	1	0.17	0
r_2	3	2	1	2	1	2	0	1	1	2	1	*8(16)*	0	0.8	0	0
r_3	4	2	3	1	2	3	2	1	2	1	2	*13(23)*	0	0	0.5	0
r_4	3	4	2	2	1	0	1	0	1	1	1	*5(16)*	0.25	0.2	0	0
r_5	1	2	3	1	4	4	3	3	4	2	4	*24(31)*	0	0	0	1

$K_{r_i} = \sum_{i=5}^{11} A_i$, $max\mu_{M_i}$ – resursning muhimlilik bahosi hisoblanadi.

2.5-jadvalda keltirilgan ma’lumotlar asosida quyidagi xuosalarni olish mumkin:

Masalan, r_1 resursning bahosi «1 vazn bilan ahamiyatli, 0.17 vazn bilan muhim»; r_2 resursning bahosi «0.8 vazn bilan ahamiyatli».

Tahdidlar xavfliligi va himoya choralarining mosligini baholash ham yuqorida keltirilgan usul yordamida amalga oshiriladi.

Tahdid xavfliligini baholash uchun $T = \{T_1,\ T_2,\ T_3,\ T_4,\ T_5,\}$ noravshan qiymatlarni qabul qiluvchi $\Omega_T =$ «Tahdid xavfliligi» lingvistik o‘zgaruvchisi beriladi. Bu yerda $T_1 =$ «Ahamiyatsiz», $T_2 =$ «Muhim», $T_3 =$ «Xavfli», $T_4 =$ «Juda xavfli», $T_5 =$ «Kritik».

Tahdidlar xavfliligiga ta’sir etuvchi shunday omillar olinadiki, ularning birinchi beshtasi – B_1, B_2, B_3, B_4, B_5 tahdid haqidagi asosiy ma’lumotlarni, qolgan $B_6, B_7, B_8, B_9, B_{10}, B_{11}, B_{12}, B_{13}$ – tahdidning xavflilik darajasini xarakterlaydi:

B_1 – tahdid manbai (1 – tabiiy; 2 – texnogen; 3 – antropogen);

B_2 – tahdid manbaining joylashgan o‘rni (1 – ichki; 2 – tashqi);

B_3 – tahdidning maqsadliligi (1 – ko‘zlanmagan; 2 – ko‘zlangan);

B_4 – tahdidning AX aspektini buzish maqsadi (1 – konfidensiallikni buzish; 2 – yaxlitlikni buzish; 3 – foydalana olishlikni buzish);

B_5 – tahdid obyekti (1 – fizik resurslar; 2 – axborot resurslari);

B_6 – buzg‘unchining darajasi (1 – eng past; 2 – o‘rta; 3 – yuqori; 4 – juda yuqori);

B_7 – tahdidni to‘xtatish imkoniyati (1 – oson; 2 – qiyin; 3 – juda qiyin; 4 – mumkin emas);

B_8 – tahdidning amalga oshishini payqash (1 – oson; 2 – qiyin; 3 – juda qiyin; 4 – mumkin emas);

B_9 – tahdid amalga oshgandan so‘ng obyektni qayta tiklash imkoniyati (1 – oson; 2 – qiyin; 3 – juda qiyin; 4 – mumkin emas);

B_{10} – tahdidning bir yil ichida yuzaga kelish chastotasi (1 – past; 2 – o‘rta; 3 – yuqori; 4 – juda yuqori);

B_{11} – tahdidning amalga oshishining obyekt uchun zarar nuqtai nazaridan xavfliligi (0 – ahamiyatsiz; 1 – past; 2 – o‘rta; 3 – yuqori);

B_{12} – tahdidni amalga oshirish uchun xarajatlar (1 – juda yuqori; 2 – yuqori; 3 – o‘rta; 4 – past);

B_{13} – tahdid amalga oshirishning osonligi (1 – juda qiyin; 2 – qiyin; 3 – nisbatan oson; 4 – oson);

AX choralarining resurs muhimliligiga va tahdidlarga nisbatan mosligini baholash uchun $P = \{P_1,\ P_2,\ P_3,\ P_4,\ P_5,\}$ noravshan qiymatlarni qabul qiluvchi $\Omega_C =$ «Choraning mosligi» noravshan o‘zgaruvchisi beriladi. Bu yerda $P_1 =$ «Mos emas», $P_2 =$ «Qisman mos», $P_3 =$ «O‘rtacha mos», $P_4 =$ «Deyarli mos», $P_5 =$ «To‘liq mos».

Choralarning mosligiga ta’sir etuvchi shunday omillar olinadiki, ularning birinchi to‘rttasi – $C_1,\ C_2,\ C_3,\ C_4$ choralar haqidagi ma’lumotlarni, qolgan $C_5,\ C_6, C_7$ – choralarning moslik darajasini xarakterlaydi:

C_1 – choraning axborot xavfsizligi aspektini himoyalash maqsadi (1 – konfidensiallikni himoyalash uchun; 2 – yaxlitlikni himoyalash uchun; 3 – foydala olishlikni himoyalash uchun);

C_2 – choraning yo‘nalishi (1 – fizik; 2 – huquqiy; 3 – tashkiliy; 4 – dasturiy-apparat);

C_3 – chora qaratilgan obyekt (1 – fizik resurslar; 2 – axborot resurslari);

C_4 – choraning qo‘llanilish nuqtasi (1 – kompyuterda; 2 – lokal tarmoqda; 3 – korporativ tarmoqda; 4 – global tarmoqda);

C_5 – choraning mos tahdid uchun muhimligi (1 – eng past; 2 – o‘rta; 3 – muhim; 4 – juda muhim);

C_6 – chorani qo‘llash uchun xarajatlar (1 – juda yuqori; 2 – yuqori; 3 – o‘rta; 4 – past);

C_7 – chorani amalga oshirishning osonligi (1 – juda qiyin; 2 – qiyin; 3 – nisbatan oson; 4 – oson);

Yuqorida taklif etilayotgan usul yordamida ixtiyoriy tashkilot axborot resurslarining muhimliligini, tahdidlar xavfliligini hamda himoya choralarining resurslar muhimliligi va tahdidlarga nisbatan mosligini baholash mumkin.

Ushbu bo‘limda himoyalanuvchi resurslarning muhimliligini baholash usuli keltirildi. Shuningdek, tahdidlar xavfliligiga hamda himoya choralarning mosligiga ta’sir etuvchi omillar aniqlandi.

Yuqorida keltirilgan model va usul yordamida himoyalanuvchi resurslar muhimliligi hamda ularga nisbatan mos himoya choralarini tanlash masalasini yechish mumkin. Keyingi bo‘limda ushbu moslikni aniqlash bo‘yicha bir nechta ekspertlardan olingan yechimlarning, himoya choralarining eng ustuvorlarini aniqlash masalasi qaraladi.

III BOB. ELEKTRON KUTUBXONA AXBOROT XAVFSIZLIGINI TA’MINLASH TIZIMI

3.1 Axborot xavfsizligini ta’minlash choralari ustuvorligini aniqlash algoritmi

Ushbu bo‘limda korporativ axborot-kutubxona tarmoqlarda axborot xavfsizligini ta’minlash choralari ustuvorligini aniqlash algoritmi bayon etiladi.

NMMga olib boruvchi sust shakllangan masalalarning yechimini bir nechta bosqichga ajratish mumkin:

1. Axborot muhitini tahlil qilish va vaziyatlarni tasniflash (vaziyatni tashkil etuvchilar).

2. Ekspert so‘rovnomalarida ishtirok etadigan ekspertlarni ajratish va ranjirlash.

3. Ekspertlar bilan so‘rovnoma o‘tkazish va muayyan vaziyatda bo‘lishi mumkin bo‘lgan tahdidlarni aniqlash (o‘rnatish).

4. Mos tahdid kuchli ta’sir etishi mumkin bo‘lgan vaziyat bo‘yicha ma’lum choralarni qabul qilishga doir ekspert so‘rovnomasini o‘tkazish.

5. Berilgan aniq vaziyat (yoki vaziyatlar) bo‘yicha mos tahdid (yoki tahdidlarni topish).

6. Topilgan tahdidlar bo‘yicha mos chora (yoki choralarni) topish.

7. Chorani bajarishning muhimliligini aniqlash.

8. Olingan natijalarni tahlil qilish.

V – vaziyatlar belgilari to‘plami, T – tahdidlar to‘plami, C – choralar to‘plami berilgan bo‘lsin.

$$V = \{v_1, v_2, \dots v_n\},$$

$$T = \{t_1, t_2, \dots t_m\},$$

$$C = \{c_1, c_2, \dots c_q\},$$

bu yerda

n – vaziyatlar belgilari soni, m – tahdidlar soni, q – choralar soni.

V, T, C to‘plamlar o‘rtasidagi moslik syuryektiv bo‘lgan umumlashgan holatni qaraymiz.

Ekspertlar so‘rovi natijasi bo‘yicha har bir ko‘rinishdagi tahdid uchun quyidagi noravshan to‘plamlar qabul qilingan:

$\tilde{A}_1 = \{\mu(v_1, t_1)\}$,

$\tilde{A}_2 = \{\mu(v_2, t_2)\}$,

. . . . . .

$\tilde{A}_k = \{\mu(v_n, t_m)\}$.

Va har bir harakat uchun

$\tilde{B}_1 = \{\mu(t_1, c_1)\}$,

$\tilde{B}_2 = \{\mu(t_2, c_2)\}$,

. . . . . .

$\tilde{B}_m = \{\mu(t_m, c_q)\}$.

Eng ishonchli «vaziyat-tahdid» moslik to‘plami quyidagi munosabat bo‘yicha topiladi:

$$\tilde{A} = \tilde{A}_1 \cup \tilde{A}_2 \cup \ldots \cup \tilde{A}_n.$$

Eng ishonchli «tahdid-chora» moslik to‘plami quyidagi formula bo‘yicha topiladi:

$$\tilde{B} = \tilde{B}_1 \cup \tilde{B}_2 \cup \ldots \cup \tilde{B}_m.$$

Birinchi navbatdagi choralarni topishda har bir chora uchun quyidagi shartni hisobga olgan holda tegishlilik funksiyasi summasi aniqlanadi:

$$R_j = \sum_{j=1}^{m} \mu(t_i, c_i).$$

Bu yerda m – tahdidlar soni.

Keyin eng ishonchli chora deb, tegishlilik funksiyasi summalarining eng kattasi olinadi:

$$R = maxR_j.$$

Demak, birinchi navbatda shunday harakatlar boshlanadiki, u ma’lum sabablar bo‘yicha R_j qiymatining katta summasiga ega bo‘ladi.

Himoya choralari ustuvorligini aniqlash uchun muhimlilik koeffitsentlari usuli. Birinchi navbatdagi choralarni topishning yuqorida keltirilgan usulini bir qancha vaziyatlarda choralarni aniqlash bo‘yicha qabul qilinadigan yechimlarning ishonchliligiga qat’iy talablar qo‘yilmaganda qo‘llash mumkin. Yechimlarning ishonchliligini oshirish uchun «Vaziyat-Tahdid» va «Tahdid-Chora» bosqichlarida ustuvor bo‘lgan yechimlarni aniqlashga mo‘lajallangan muhimlilik koeffitsentlari usulidan foydalaniladi. U yechimning eng muhim variantini tanlaydi va so‘nggida yakuniy natijalarning ishonchliligini oshiradi.

Axborot muhiti vaziyatlarining belgilar to‘plami berilgan:

$$V = \{v_1, v_2, \dots, v_n\}$$

Masalan, axborot-kutubxona tizimlari xavfsizligini baholashda vaziyatlar deganda, axborot tizimining turli bosqichlaridagi himoyalanuvchi resurslarning hamda ularning himoyasi uchun choralarning xususiyatlari tushuniladi. $V' \in V$ vaziyat deganda, axborot muhitining aniq holatini qoniqtiruvchi belgilar to‘plami tushuniladi.

Tahdid deganda, u yoki bu vaziyatda bo‘lishi mumkin bo‘lgan xatarlarni xarakterlovchi $T = \{T_1, T_2, \dots, T_m\}$ qiymatlarning noravshan parametrlar to‘plami tushuniladi. Har bir $T_i (i \in I,$ bu yerda $I = \{1,2,3, \dots, m\})$ parametr mos $T_i = (U_i, B_i, s_i)$ noravshan o‘zgaruvchi ko‘rinishida yoziladi.

Bu yerda $U_i - t_i$ noravshan o‘zgaruvchining term to‘plami;

$B_i - p_i$ belgilarining bazaviy to‘plami;

s_i – aniq vaziyatlar uchun t_i ning boshqa parametrlari bilan taqqoslanishida t_i salmog‘ini (vesini) xarakterlovchi koeffitsentdir. «Vaziyat-Tahdid» va «Tahdid-Chora»ning barcha tegishlilik funksiyalari shakllangan bo‘lsin. NMMni amalga oshirish ishonchli moslikni, harakatlar to‘plamini, ularning biridan boshqasining muhimliligini aniqlashga olib keladi va so‘nggida yuzaga keluvchi vaziyatlarda choralar strategiyasini shakllantiradi.

Muhimlilik koeffitsentlari usuli mos choralar uchun o‘rnatilgan vazn koeffitsentlariga bog‘liq holda tahdidlar to‘plami uchun vazn koeffitsentlarini

aniqlashni o‘z ichiga qamrab oladi. Ushbu koeffitsentlarning qiymati choraning muhimliligini (birinchiligini) qaytaradi va yuzaga kelgan vaziyatda qaror qabul qilish bo‘yicha choralar strategiyasini aniqlashga imkon beradi.

Muhimlilik koeffitsentlarini aniqlashda noravshan kiritish operatsiyasidan foydalanildi. A_i noravshan to‘plamning A_j noravshan to‘plamga kirish darajasini aniqlaymiz.

Bu yerda,

$A_i = \{\mu(v_1, t_i), \mu(v_2, t_i), \dots, \mu(v_k, t_i)\}$ – «vaziyat-tahdid» bosqichidagi t_i term (satr) bo‘yicha tegishlilik funksiyalari to‘plami;

$A_j = \{\mu(v_1, t_j), \mu(v_2, t_j), \dots, \mu(v_k, t_j)\}$ – «vaziyat-tahdid» bosqichidagi t_j term bo‘yicha tegishlilik funksiyalari to‘plami.

A_i noravshan to‘plamning A_j noravshan to‘plamga kirish kirish darajasi $\mathrm{v}(A_i, A_j)$ orqali belgilanadi va quyidagi ifoda bilan aniqlanadi:

$$\mathrm{v}(A_i, A_j) = min\left\{max\left(\left(1 - \mu_{A_i}(v_i, t_i)\right);\ \mu_{A_j}(v_i, t_j)\right)\right\},$$

bu yerda v – noravshan kirish munosabati bo‘lib, quyidagicha hisoblanadi [13]:

$$\mu_{A_i}(v, t_i) \to \mu_{A_j}(v, t_j) = max\left(\left(1 - \mu_{A_i}(v, t_i)\right), \mu_{A_j}(v, t_j)\right).$$

Misol. $S = \{s_1, s_2, s_3, s_4\}$ vaziyatlar to‘plamida mos ravishda t_i va t_j termlar uchun quyidagi noravshan to‘plamlar aniqlangan bo‘lsin:

$$A_i = \left(\frac{0.7}{s_1}\right), \left(\frac{0.6}{s_2}\right), \left(\frac{0.8}{s_3}\right), \left(\frac{0.5}{s_4}\right);$$

$$A_i = \left(\frac{0.4}{s_1}\right), \left(\frac{0.8}{s_2}\right), \left(\frac{0.7}{s_3}\right), \left(\frac{0.4}{s_4}\right);$$

A_i to‘plamning A_j to‘plamga kirish darajasi quyidagicha aniqlanadi:

v(A_i, A_j) = min [max(1–0.7; 04) & max (1–0.6; 0.8) & max (1–0.8; 0.7) & max (1–0.5; 0.4)] = min [max(0.3; 04) & max (0.4; 0.8) & max (0.2; 0.7) & max (0.5; 0.4)] = min [0.4 & 0.8 & 0.7 & 0.5] = 0.4.

A_j to‘plamning A_i to‘plamga kirish darajasi ham shu kabi aniqlanadi:

$v(A_j, A_i)$ = min [max(1–04; 0.7) & max (1–0.8; 0.6) & max (1–0.7; 0.8) & max (1–0.4; 0.5)] = min [max(0.6; 0.7) & max (0.2; 0.6) & max (0.3; 0.8) & max (0.6; 0.5)] = min [0.7 & 0.6 & 0.8 & 0.6] = 0.6.

Demak, quyidagi munosabatga egamiz: $(A_i \subseteq A_j) \rightarrow 0.4$; $(A_j \subseteq A_i) \rightarrow 0.6$.

Muhimlilik koeffitsenti usuli quyidagilarni bajarish orqali amalga oshiriladi:

1. A_i va A_j to‘plamlarning bir-biriga kirish darajasini aniqlash.

$$v(A_i, A_j) = min\left\{max\left(\left(1 - \mu_{A_i}(v_i, t_i)\right);\ \mu_{A_j}(v_i, t_j)\right)\right\},$$

$$v(A_j, A_i) = min\left\{max\left(\left(1 - \mu_{A_j}(v_i, t_j)\right);\ \mu_{A_i}(v_i, t_i)\right)\right\}.$$

Shunday qilib, kirish darajalari matritsasi quriladi [22] (3.1-jadval).

3.1-jadval

Noravshan kirish darajalari matritsasi

	A_1	A_2	…	A_n
A_1	1	$v(A_1, A_2)$	…	$v(A_1, A_n)$
A_2	$v(A_2, A_1)$	1	…	$v(A_2, A_n)$
…	…	…	…	…
A_n	$v(A_n, A_1)$	$v(A_n, A_2)$	…	1

2. Juft qiyoslash matritsasini yaratish (2.6-jadval).

3.2-jadval

Juft qiyoslash matritsasi

	A_1	A_2	…	A_n
A_1	1	$v\frac{(A_1, A_2)}{(A_2, A_1)}$	…	$v\frac{(A_1, A_n)}{(A_n, A_1)}$
A_2	$v\frac{(A_2, A_1)}{(A_1, A_2)}$	1	…	$v(A_2, A_n)$
…	…	…	1	…
A_n	$v\frac{(A_n, A_1)}{(A_1, A_n)}$	…	…	1

3. Har bir t bo‘yicha ustuvorlik koeffitsentini aniqlash. Ustuvorlik koeffitsenti juft qiyoslash natijasida olingan matritsaning xususiy vektori asosida topiladi. Buning uchun xususiy vektor komponentini hisoblashning o‘rta geometrik formulasidan foydalaniladi:

$$a_i = \sqrt[n]{a_{i1} * a_{i2} * a_{i3} * a_{i4}}$$

So‘ngra har bir har bir matritsa uchun xususiy vektor to‘plami hisoblanadi va natijalar normallashtirilib, vektorning ustuvorligi olinadi:

$$k_i = \frac{a_i}{\sum_i a_i} = \frac{\sqrt[n]{\prod_j a_{ij}}}{\sum_i a_i}.$$

Ammo ekspertlar tomonidan taqdim etilayotgan dastlabki ma’lumotlarning ishonligini aniqlash muhim ahamiyatga ega bo‘lganligi uchun ekspertlar fikri hamjihatlik indeksi HI ga tekshiriladi. Buning uchun matritsaning maksimal xususiy qiymati λ_{max} hisoblanadi:

$$\lambda_{max} = \sum_{i=1}^{n} a_{i1}k_1 + \sum_{i=1}^{n} a_{i2}k_2 + ... + \sum_{i=1}^{n} a_{in}k_n = \sum_{j=1}^{n}\sum_{i=1}^{n} a_{ij}k_j.$$

Ekspertlar fikrining to‘g‘riligini ifodalovchi hamjihatlik indeksi HI quyidagicha hisoblanadi:

$$HI = \frac{\lambda_{max} - n}{n - 1}$$

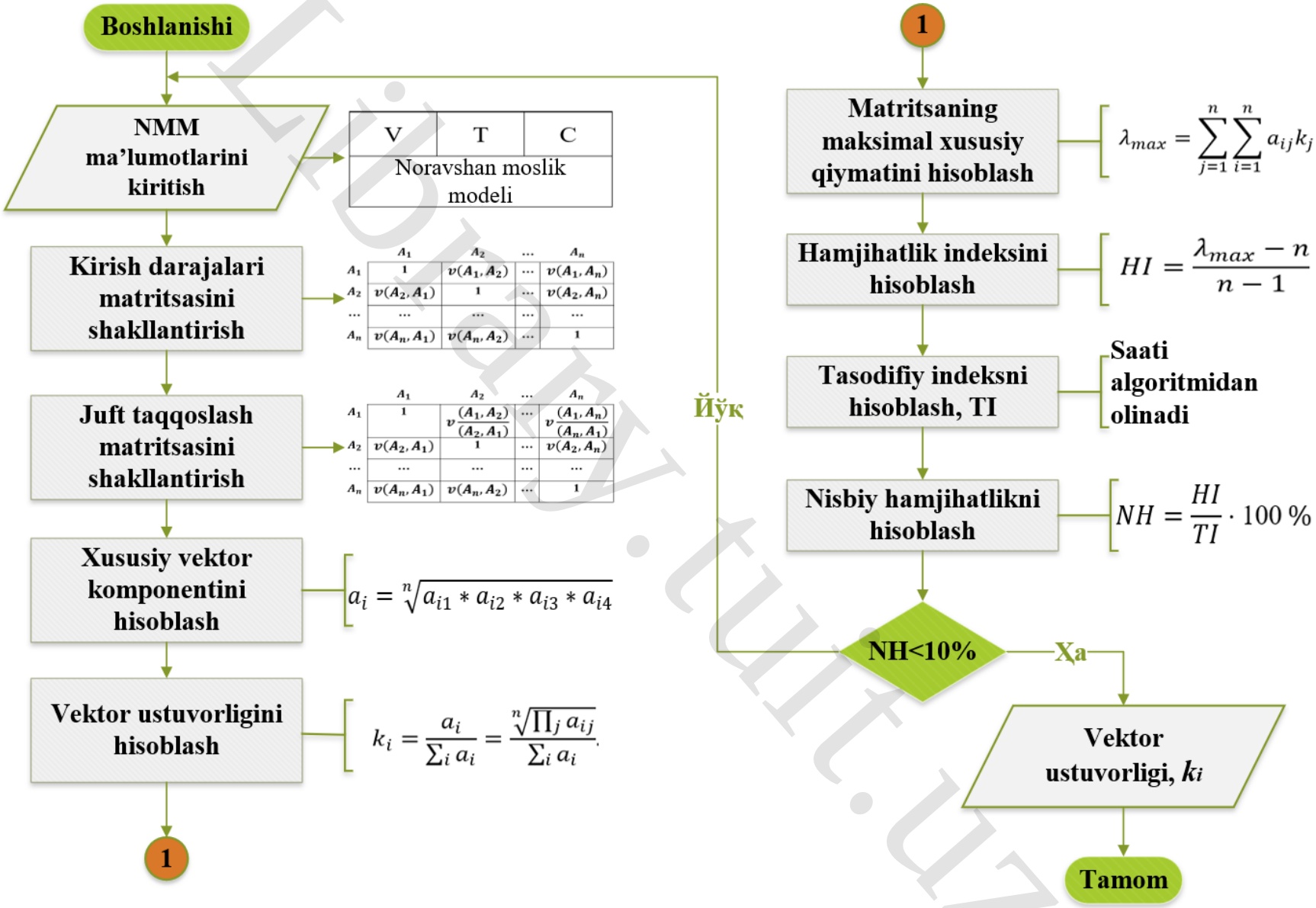
bu yerda n – obyektlar soni.

So‘ngra tasodifiy indeks TI topiladi. U juft qiyoslash matritsasining ma’lumoti bo‘lib, uning qiymati matritsa o‘lchamiga bog‘liq bo‘ladi. 3.3-jadvalda keltirilgan ma’lumotlar T.Saati tomonidan taklif etilgan [30; 1497-b.].

3.3-jadval

Tasodifiy hamjihatlik indeksi matritsa o‘lchamiga bog‘liq holdagi o‘rtacha qiymati

Matritsa o‘lchami	1	2	3	4	5	6	7	8	9	10
TI	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49



3.1-rasm. Axborot xavfsizligini ta' minlash choralari ustuvorligini aniqlash algoritmi

Ekspertlar fikrining to‘g‘riligini aniqlovchi nisbiy hamjihatlik (NH) esa quyidagicha hisoblanadi:

$$NH = \frac{HI}{TI} \cdot 100\ \%$$

Agar NH<10% bo‘lsa, u holda muhimlilikni aniqlash bo‘yicha olingan natijalar ishonchli. Aks holda, olib borilayotgan tadqiqot boshqatdan o‘tkazilishi kerak.

Umumiy holda axborot xavfsizligini ta’minlash choralari ustuvorligini aniqlash algoritmini 3.1-rasmdagidek tasvirlash mumkin.

Ushbu bo‘limda korporativ axborot-kutubxona tarmoqlarda axborot xavfsizligini ta’minlash choralari ustuvorligini aniqlash algoritmi keltirildi.

3.2 Axborot kutubxona muassasasi xavfsizligini baholash algoritmi

Ushbu bo‘limda axborot kutubxona muassasasi xavfsizligini baholash algoritmi keltiriladi.

KAKT axborot xavfsizligini ta’minlashda alohida ichki korporativ axborot kutubxona muassasalari (AKM)ning xavfsizligini baholash masalasi kelib chiqadi. Bu esa AKMda qo‘llanilayotgan himoya choralarining xavfsizlik talabiga yoki himoyalanuvchi resurslar muhimliligiga mosligini aniqlashni taqozo etadi.

Yuqorida resurslar (R), tahdidlar (T) va choralar (C) tasniflandi, identifiksiya qilindi va ularning bahosi ekspertlar tomonidan aniqlandi (2.2§). Umumiy holda R, V, C lar obyekt deb qaralib, quyidagicha berilgan bo‘lsin:

- $R = \{R_{ij}^k\}$ $(j = 1..qr)$ – resurslar to‘plami;
- $T = \{U_{ij}^k\}$ $(j = 1..kt)$ – tahdidlar to‘plami;
- $C = \{E_{ij}^k\}$ $(j = 1..mc)$ – choralar to‘plami;
- B_R, B_C – mos ravishda resurslar va choralar baholari.

Bu yerda k – resurs/tahdid/chora sinfi, i – resurs/tahdid/chora tipi, j – resurs/tahdid/chora identifikatsiya raqami.

Ma’lumki, T – tahdid R – resursga nisbatan amalga oshirilib, o‘z o‘rnida T – tahdidga qarshi C – himoya choralari ishlab chiqiladi. Bu yerda shuni e’tiborga olish kerakki, qaralayotgan obyektlarni tashkil etuvchi elementlari muhimlilik jihatdan o‘zaro bir-biri bilan kesishadi. Misol uchun turli resurslar muhimliligi, tahdidlarning xavfliligi va himoya choralarning moslik darajalari bir-biriga teng bo‘lishi mumkin. Bu obyektlarning ichki mosligi deb nomlanib, ularni diagonali 1 bo‘lgan simmetrik matritsa ko‘rinishida ifodalash mumkin (3.4-jadval).

Obyekt elementlarining o‘zaro mosligini aniqlashdan maqsad bir xil qiymatli obyektlarni olishdir. Masalan, aniqlangan bir nechta tahdidlarga qarshi qo‘yilayotgan choralarning biri qolgan bir nechta choralarning o‘rini bosishi mumkin.

3.4-jadval

a) resurslarning muhimlilik jadvali

Resurslar

	r_1	r_2	…	r_{qr}
r_1	1	$r_{1,2}$	…	$r_{1,qr}$
r_2		1	…	$\tilde{r}_{2,qr}$
…		…	1	…
r_{qr}				1

b) tahdidlarning xavflilik jadvali

Tahdidlar

	t_1	t_2	…	t_{kt}
t_1	1	$t_{1,2}$	…	$t_{1,kt}$
t_2		1	…	$t_{2,kt}$
…		…	1	…
t_{kt}				1

v) choralarning moslik jadvali

Choralar

	c_1	c_2	…	c_{mc}
c_1	1	$c_{1,2}$	…	$c_{1,mc}$
c_2		1	…	$c_{2,mc}$
…		…	1	…
c_{mc}				1

Endi resurslarga nisbatan tahdidlarning xavfliligini va ushbu taxdidlarga nisbatan choralarning bartaraf etish darajasini ifodalovchi «Resurs-Tahdid» va «Tahdid-Chora» moslik jadvallari quriladi. Ushbu moslik jadvallari identifikatsiyalangan har bir obyektlar (R,T, C) elementlarining bir-biriga moslik darajasini ko‘rsatadi va ularni 3.5-jadvallar ko‘rinishida ifodalash mumkin.

Keltirilgan «Resurs-Tahdid» va «Tahdid-Chora» munosabatlarini o‘zida mujassamlashtirgan ikki jadval «Tahdid» obyektiga «Resurs» va «Chora» obyektlarini birlashtirmoqda. Ya’ni, ushbu jadvallar natijasida «Resurs- Chora» munosabati kelib chiqmoqda. Xususan, «Tahdid-Chora» barcha tahdidlarga qarshi barcha choralar mosligini bildirsa, «Resurs-Chora» munosabati aynan har bir resursga (yoki resrurs tipi) tahdidlardan himoyalashdagi choralarning mosligini bildiradi.

Shunday qilib, «Resurs-Tahdid», «Tahdid-Chora» va «Resurs-Chora» jadvallar ekspertlar tomonidan to‘ldirilib, umumiy holda ularni moslikni ifodalovchi uchlik jadval deb yuritiladi.

«Resurs-Tahdid», «Tahdid-Chora» va «Resurs-Chora» jadvallarning natijalari bo‘lgan elementlar: $\eta_{i,j}\left(i=\overline{1,qr}, j=\overline{1,kt}\right), \tau_{i,j}\left(i=\overline{1,kt}, j=\overline{1,mc}\right), v_{i,j}(i=\overline{1,qr}, j=\overline{1,mc})$ moslikni ifodalayotganligi uchun ularning qiymatlari noravshan termlar bo‘ladi.

3.5-jadval

а) «Resurs-Tahdid» moslik jadvali

		Resurslar			
		r_1	r_2	…	r_{qr}
Taxdidlar	t_1	$\eta_{1,1}$	$\eta_{1,2}$	…	$\eta_{1,qr}$
	t_2	$\eta_{2,1}$	$\eta_{2,2}$	…	$\eta_{2,qr}$
	…	…	…	…	…
	t_{kt}	$\eta_{kt,1}$	$\eta_{kt,2}$	…	$\eta_{kt,qr}$

б) «Tahdid-Chora» moslik jadvali

		Choralar			
		c_1	c_2	…	c_{mc}
Taxdidlar	t_1	$\tau_{1,1}$	$\tau_{1,2}$	…	$\tau_{1,mc}$
	t_2	$\tau_{2,1}$	$\tau_{2,2}$	…	$\tau_{2,mc}$
	…	…	…	…	…
	t_{kt}	$\tau_{kt,1}$	$\tau_{kt,2}$	…	$\tau_{kt,mc}$

в) «Resurs-Chora» moslik jadvali

		Choralar			
		c_1	c_2	…	c_{mc}
Resurslar	r_1	$v_{1,1}$	$v_{1,2}$	…	$v_{1,mc}$
	r_2	$v_{2,1}$	$v_{2,2}$	…	$v_{2,mc}$
	…	…	…	…	…
	r_{qr}	$v_{qr,1}$	$v_{qr,2}$	…	$v_{qr,mc}$

AKM xavfsizligini baholash jarayoni bir nechta bosqichlarni o‘z ichiga oladi:

– AKM himoyalanuvchi resurslarini aniqlash;

– aniqlangan resurslar bilan bog‘liq vaziyatlarni aniqlash;

– AKM resurslar muhimliligini baholash;

– AKMda qo‘llanilayotgan himoya choralarini aniqlash va ularni baholash;

– AKM vaziyatlari asosida «Vaziyat-Tahdid-Chora» jadvalidagi vaziyatlar filtrlanadi;

– «Vaziyat-Tahdid-Chora» jadvalidagi vaziyatlar asosida «Vaziyat-Tahdid-Chora» jadvalidagi tahdidlar filtrlanadi;

– Ushbu tahdidlarga nisbatan «Vaziyat-Tahdid-Chora» jadvalidagi choralar filtrlanadi;

– AKM resurslari muhimliligi va «Vaziyat-Tahdid-Chora» jadvalidagi choralar muhimliligi qiymatining mosligi tekshiriladi;

– AKMda o‘rnatilgan choralarning mosligi aniqlanadi.

Axborot-kutubxona muassasasi xavfsizligini baholash algoritmi 3.1-rasmda keltirilgan.

AKM himoyalanuvchi resurslarini aniqlash. Buning uchun AKM resurslari identifikatsiyalangan resurslar ko‘rinishida quyidagi shaklda ajratib olinadi:

$$KR = KR_{ij}^{k}\ (j = 1 \ldots qkr), KR \subseteq R, qkr \leq qr.$$

bu yerda qkr – AKM resurs tiplari soni, qr – barcha resurs tiplari soni.

Aniqlangan resurslar bilan bog‘liq vaziyatlarni aniqlash. AKM resurslari KR ning holati va foydalanish shartlarini belgilovchi vaziyatlar aniqlanadi:

$$KV = KR_{ij}^{k}\ (j = 1 \ldots nkv), KV \subseteq V, nkv \leq nv.$$

bu yerda nkv – AKM vaziyatlari soni, nv – barcha vaziyatlar soni.

AKM resurslar muhimliligini baholash. AKM resurslari bahosi B_{KR} oldingi bo‘limda keltirilgan usul yordamida aniqlanadi.

AKMda qo‘llanilayotgan himoya choralarini aniqlash va ularni baholash. AKM resurslariga qo‘yilgan himoya choralari KC aniqlanadi.

$$KC = K_i C_j\ (i = 1 \ldots qkr, j = 1 \ldots mkc).$$

bu yerda mkc – AKM himoya choralari soni. AKM resurslarga qo‘yilgan choralar KC ning mavjudligi jadvali to‘ldiriladi. Jadvalning elementlari binar (0 yoki 1) qiymat qabul qiladi, Ya’ni:

$$kF(KR, C) = kr_i \times c_j = v_{\overline{i,j}} = \langle 0,1 \rangle\ (i = 1 \ldots nkr, j = 1 \ldots mkc).$$

Bu yerda v_{ij} AKMning resurlarni himoyalashga qaratilgan choralari. AKM himoya choralarining bahosi B_{KC} ham oldingi bo‘limda keltirilgan usul yordamida aniqlanadi.

AKM vaziyatlari asosida «Vaziyat-Tahdid-Chora» jadvalidagi vaziyatlar filtrlanadi.

1) $KV\Big|_{M}$ – tashkilotning *M* tipdagi resurslari filtrlanadi;

2) $KV\Big|_{M}$ ga mos «Vaziyat-Tahdid-Chora» jadvalidagi vaziyatlarning parametrlari aniqlanadi, Ya'ni

$$\overline{V} = KV \backslash V, \overline{V} \cup KV \subseteq V, \overline{V} \equiv KV;$$

«Vaziyat-Tahdid-Chora» jadvalidagi vaziyatlar asosida tahdidlar filtrlanadi.

$\bar{T}\Big|_{\overline{V}}$ – tanlangan vaziyatlarga mos tahdidlar.

Ushbu tahdidlarga nisbatan «Vaziyat-Tahdid-Chora» jadvalidagi choralar filtrlanadi.

$\bar{C}\Big|_{\bar{T}}$ – tanlangan tahdidlarga mos choralar.

AKM resurslari muhimliligi va «Vaziyat-Tahdid-Chora» jadvalidagi choralar muhimliligi qiymatining mosligi tekshiriladi:

$$B_{KR} \geq B_{KC}$$

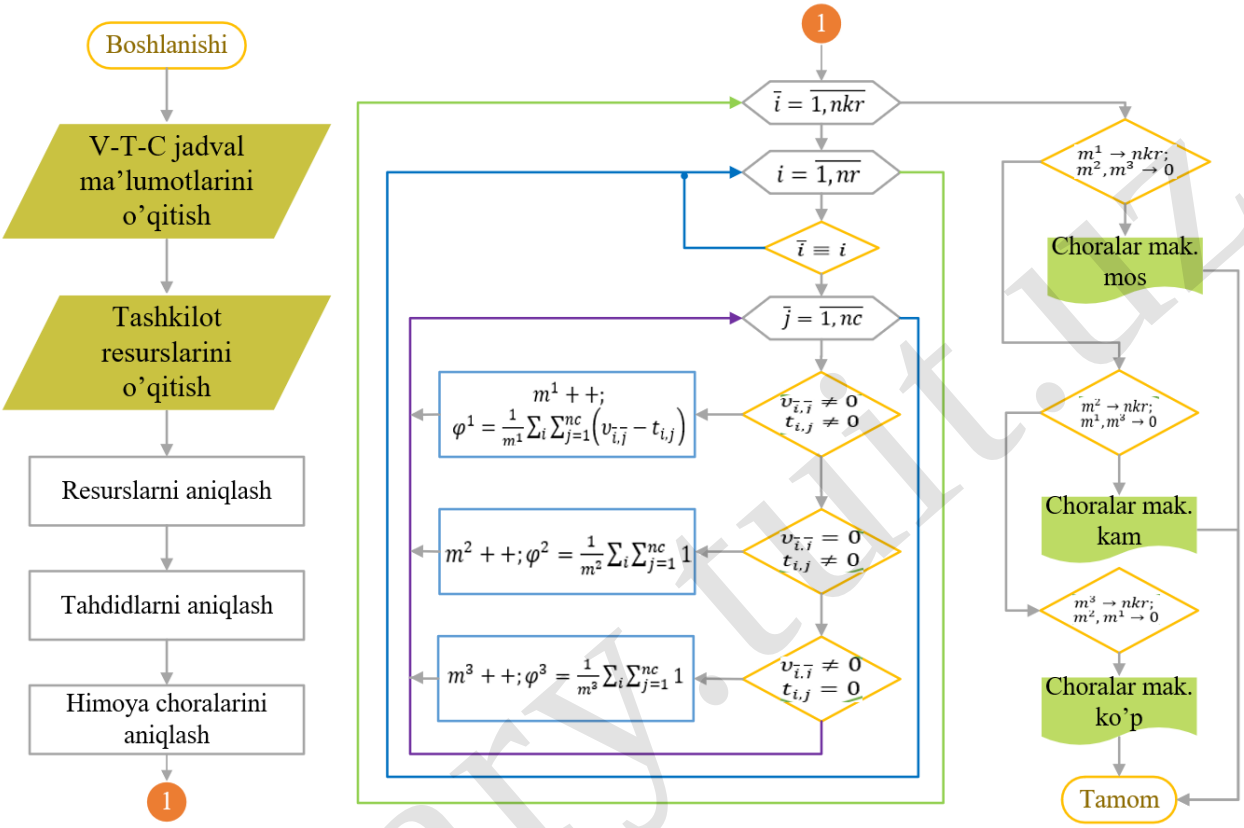
AKMda o'rnatilgan choralarining mosligini aniqlash. AKMning resurslarni himoyalashga qaratilgan choralari $\upsilon_{\bar{i},\bar{j}}\ (i = 1 \ldots qkr, j = 1 \ldots mkc)$ bilan «Vaziyat-Tahdid-Chora» jadvalidagi himoyalash choralari $\bar{C}\Big|_{\bar{T}} = \tau_{ij} (i = 1 \ldots nv, j = 1 \ldots mc)$ mos qo'yiladi. Unda $\bar{i} \equiv i$, Ya'ni matritsa indeksi absolyut teng bo'lgan holatda himoya choralarining o'zaro mosligi, ortiqchalik va kamlik omillari quyidagicha aniqlanadi:

- moslik: $\varphi^1 = \frac{1}{m^1} \sum_i \sum_{j=1}^{mc} \left(\upsilon_{\bar{i},\bar{j}} - \tau_{i,j} \right), \upsilon_{\bar{i},\bar{j}} \neq 0 \ \ \& \tau_{i,j} \neq 0;$
- kamchilik: $\varphi^2 = \frac{1}{m^2} \sum_i \sum_{j=1}^{mc} 1, \upsilon_{\bar{i},\bar{j}} = 0 \ \& \ \tau_{i,j} \neq 0;$
- ortiqchalik: $\varphi^3 = \frac{1}{m^3} \sum_i \sum_{j=1}^{nc} 1, \upsilon_{\bar{i},\bar{j}} \neq 0 \ \& \ \tau_{i,j} = 0.$

m^1 – AKMda va «Vaziyat-Tahdid-Chora» jadvalida mavjud bo'lgan, ma'lum darajada bir-biriga mos bo'lgan choralar soni;

m^2 – «Vaziyat-Tahdid-Chora» jadvaliga ko‘ra qo‘llanilishi kerak, ammo AKMda mavjud bo‘lmagan, yetishmayotgan choralar soni;

– m^3 – «Vaziyat-Tahdid-Chora» jadvaliga ko‘ra qo‘llanilishi shart emas, ammo AKMda ishlatilayotgan, ortiqcha choralar soni.



3.2-rasm. Axborot-kutubxona muassasasi xavfsizligini baholash algoritmi

Bu yerda m^1, m^2, m^3 sonlar shartlarni qanoatlantiruvchilar soniga teng, Ya’ni $qkr \cdot mkc = m^1 + m^2 + m^3 \leq qkr \cdot mkc$.

– Agar $m^1 \to qkr;\ m^2, m^3 \to 0$; у ҳолда $\varphi^1 \to 0$ chora maksimal mos;

– Agar $m^2 \to qkr;\ m^1, m^3 \to 0$; у ҳолда $\varphi^2 \to 1$ chora maksimal kam;

– Agar $m^3 \to qkr;\ m^1, m^2 \to 0$; $\varphi^3 \to 1$ choralarning barchasi ortiqcha.

Ushbu bo‘limda aniq axborot-kutubxona muassasasi axborot xavfsizligini baholash algoritmlari ishlab chiqilgan.

3.3 eLibIS tizimining funksional va tashkiliy tuzilmasi

Ushbu bo‘limda korporativ axborot-kutubxona tarmoqlarida axborot xavfsizligini baholashning dasturiy kompleksi – eLibIS (Electronic Library Information Security) ning funksional tuzilmasi va uning funksional talablari ishlab chiqiladi.

KAKTda axborot xavfsizligini baholash masalasini yechishga mo‘ljallangan bo‘lib, resurslarning muhimliligini baholash, ratsional himoya choralarini aniqlash hamda bilimlar bazasini shakllantirish kabi modullarga egaligi uchun eLibIS dasturiy kompleks deb nomlandi.

Dasturiy kompleksni yaratish uchun avvalo unga qo‘yiladigan funksional talablarni aniqlash zarur. Dasturiy kompleksni yaratish masalasi yechimining o‘ziga xos xususiyatlari quyidagilar: resurslar va ularga nisbatan tahdidlar to‘g‘risida dastlabki ma’lumotlarning noto‘liqligi va noaniqligi; ko‘p sonli xususiy ko‘rsatkichlarni hisobga olish zarurligi bilan bog‘liq vazifalarning ko‘pmezonliligi; dasturiy kompleksni ishlab chiqish va joriy etish masalalarini hal etishda hisobga olinishi kerak bo‘lgan sonli va sifat ko‘rsatkichlarining mavjudligi.

Dasturiy kompleks quyidagi talablarga javob berishi kerak:

1) himoya obyekti uchun ko‘rsatkichlar va talablarni shakllantirish usulining mavjudligi; ekspert baholashni amalga oshirish modulining mavjudligi; sonli va sifat ko‘rsatkichlarini baholash modulining mavjudligi;

2) universallik, uyg‘unlilik, foydalanishning qulayligi, amaliy yo‘naltirilganlik, bilimlar bazasini doimiy boyitib borish bilan dastlabki ma’lumotlarning noaniqligi sharoitida ishlay olish;

3) resurslar muhimliligini baholash modulining mavjudligi; himoya obyekti xavfsizligini baholash va tegishli tavsiyalarni berish modulining mavjudligi.

Ushbu talablarga bog‘liq holda, maxsus funksional talablar ishlab chiqilgan bo‘lib, ular dasturiy kompleks tomonidan tizimning kirish ma’lumotlariga qanday javob berishini va muayyan vaziyatlarda qanday ishlashini ifodalaydi (3.6-jadval).

Dasturiy kompleksga qo‘shimcha ravishda funksional bo‘lmagan tashkiliy talablar ham qo‘yiladi: 1) AXB tizimlarini ishlab chiqish va joriy etish standartlar asosida amalga oshiriladi (O’z DSt ISO/IES 27002:2016 «Xavfsizlikni boshqarish usullari», O’z DSt ISO/IES 27005:2013 «Axborot xavfsizligi risklarini boshqarish», O’z DSt ISO/IES 25408:2016 «Axborot texnologiyalari xavfsizligini baholash mezonlari») [2, 3, 4]; 2) predmet sohalarini modellashtirish, talablarni va ko‘rsatkichlarni ishlab chiqish standartlar va rahbariy hujjatlar asosida ishlab chiqiladi (RH 45-024:2009 «Aloqa va axborotlashtirish sohasida axborot xavfsizligini ta’minlash tizimi to‘g‘risida nizom») [6];

3.6-jadval

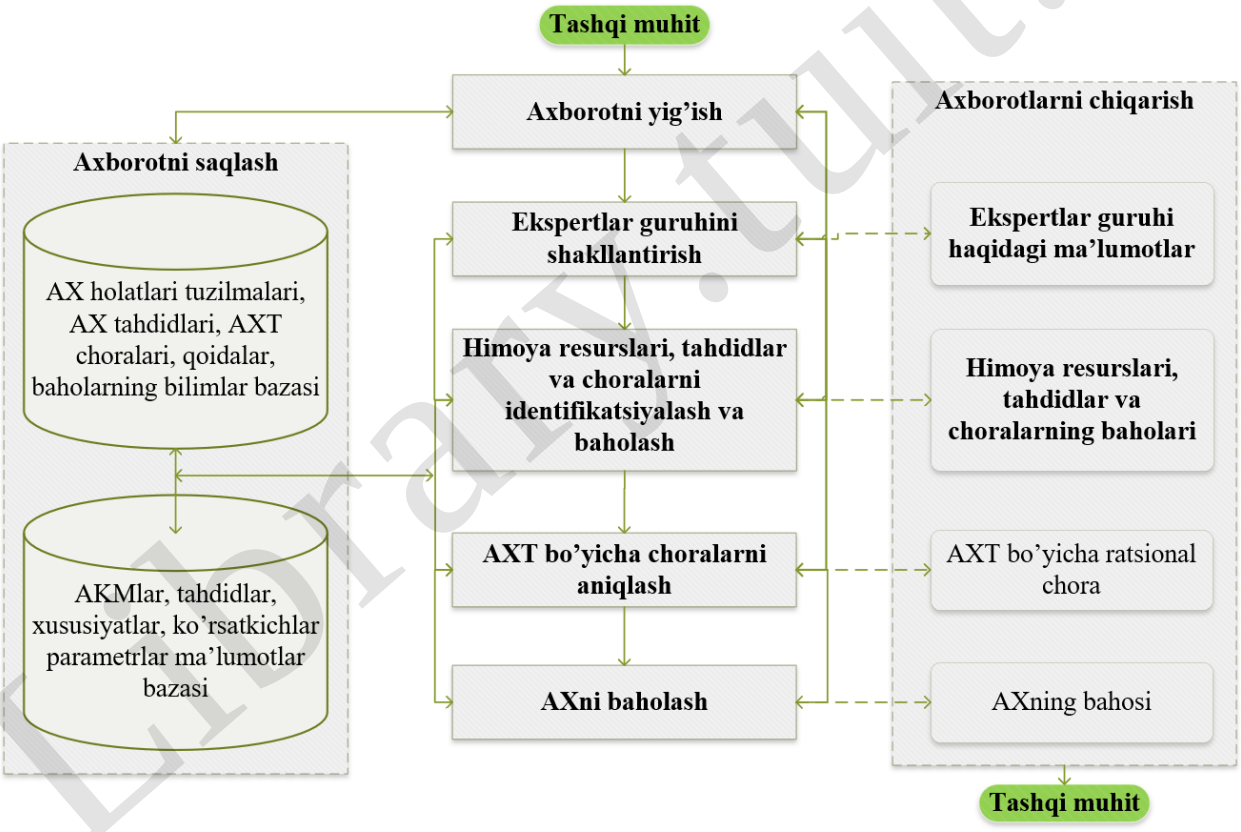
Maxsus funksional talablar

№	Talabning nomi	Tavsifi	Harakat
1	Foydalanuvchilar va ekspertlarni avtorizatsiyalash	Tizim foydalanuvchilar va ekspertlarni ro‘yxatga olish, avtorizatsiyalashi hamja keyingi safarlar identifikatsiya va autentifikatsiyalashi kerak.	<ro‘yxatdan o‘tish> funksiyasi tanlanganda tizim yangi foydalanuvchini tegishli talablar bilan ro‘xatga oladi. <kirish> funksiyasi foydalanuvchini autentifikatsiyalash va identifikatsiyalashni amalga oshiradi.
2	Jarayonni boshlash	Foydalanuvchi axborot kutubxona tizimining AXni baholash jarayonini boshlashi kerak	Tizim foydalanuvchi <Jarayonni boshlash> funksiyasini tanlamaguncha kutish rejimida turadi.
3	Himoya obyekti profilini yaratish	Tizim AKM profilini yaratadi, foydalanuvchi esa profilni tasdiqlash, o‘zgartirish, yangi ma’lumotlarni kiritish imkoniyatiga ega bo‘lishi kerak.	Tizim AKT profilida ko‘rsatilgan ma’lumotlarni taqdim etadi hamda foydalanuvchidan ushbu profilni tasdiqlashni so‘raydi.
4	Resurslarni identifikatsiyalash	Foydalanuvchi tavsiya etilgan resurslar to‘plamidan identifikatsiya qilish lozim bo‘lganlarini tanlash yoki yangilarini kiritish imkoniyatiga ega bo‘lishi kerak.	Tizim resurslar katalogidan keraklilarini tanlash imkoniyati bo‘lgan shaklni ko‘rsatadi. Shu bilan birga yangi rerurs tipini kiritish funksiyasini ko‘rsatadi.
5	Vaziyatlarni	Foydalanuvchi tavsiya etilgan	Tizim vaziyatlar katalogidan

№	Talabning nomi	Tavsifi	Harakat
	identifikatsiyalash	vaziyatlar to‘plamidan identifikatsiya qilish lozim bo‘lganlarini tanlash yoki yangilarini kiritish imkoniyatiga ega bo‘lishi kerak.	keraklilarini tanlash imkoniyati bo‘lgan shaklni ko‘rsatadi. Shu bilan birga yangi vaziyatni kiritish funksiyasini ko‘rsatadi.
6	Resurslarni baholash	Ekspert taklif etilayotgan ko‘rsatkichlarga muvofiq har bir resurs yoki resurs tipiga ball qo‘yadi.	Tizim resurslar ko‘rsatkichlarini baholash shaklini taqdim etadi. Ekspertdan har bir resurs uchun bahoning kiritishini kutadi navbatdagi resursni baholashga o‘tkazadigan <Keyingi> funksiyasini faollashtiradi.
7	Ma’lumotlarni taqdim etish	Foydalanuvchi AKM resurslari muhimliligi bahosi to‘g‘risidagi ma’lumotni olishi kerak.	Barcha resurslarni baholashdan so‘ng, tizim har bir resurs tipi yoki butun AKM uchun muhimlilikning umumiy bahosini hisoblab chiqadi.
8	«Vaziyat-Tahdid» moslikni kiritish	Ekspert muayyan AKM profilidagi vaziyatlarga nisbatan tahdidlarni va uning moslik darajasini ko‘rsatishi kerak.	Tizim ekspertga muayyan AKM profilidagi vaziyatlarni taqdim etish, tahdidlar katalogidan keraklisini tanlash yoki yangi tahdid kiritish va uning moslik darajasini ko‘rsatish imkonini berishi kerak.
9	«Tahdid-Chora» moslikni kiritish	Ekspert muayyan AKM profilidagi vaziyatlar va tahdidlarga nisbatan choralarni va uning moslik darajasini ko‘rsatishi kerak.	Tizim ekspertga muayyan AKM profilidagi vaziyatlar va tahdidlarga nisbatan choralar katalogidan keraklisini tanlash yoki yangi chora kiritish va uning moslik darajasini ko‘rsatish imkonini berishi kerak.
10	Himoya choralarining mosligini baholash	Foydalanuvchi AKMning himoya choralari mosligini baholash jarayonini boshlashi kerak.	Tizim foydalanuvchi uchun AKM profilidagi barcha resurslar hamda shu resurslarga qo‘llanayotgan himoya choralarini kiritish mumkin bo‘lgan shaklni taqdim etadi.
11	Himoya choralarining mosligini baholash	Foydalanuvchi AKMning himoya choralarining mosligini baholash jarayonini tugatishi kerak.	Tizim choralarni kiritishni <tugatish> va natijani <ko‘rish> funksiyalari ishga tushishi kerak.
12	Ma’lumotni taqdim etish	Foydalanuvchiga AKM himoya choralarining mosligi haqidagi axborot taqdim etilishi kerak.	Tizim etalondagi va AKMdagi joriy himoya choralarining mosligini hisoblab, natijasni chiqarishi kerak.
13	To‘xtatish	Foydalanuvchi har bir	Favqulodda holatlarda tizimdan

№	Talabning nomi	Tavsifi	Harakat
		bosqichda o‘rganish jarayonini to‘xtatish va qayd yozuvlarni saqlab yoki saqlamasdan dasturdan chiqishi mumkin.	chiqish zarur bo‘lganda natijalarni saqlashni yoki saqlamaslikni taklif qiladi.
14	Tavsiyalarni chiqarish	Foydalanuvchi AXB darajasini oshirish bo‘yicha hisobot (tavsiyalar)ni ko‘rish imkoniyatiga ega bo‘lishi kerak.	Tizim AKM resurslari bahosi, vaziyatlari, tahdidlar va joriy himoya choralari hisobga olgan holda tegishli tavsiyalar ishlab chiqarishi kerak.

Yuqorida keltirilgan funksional talablar asosida axborot xavfsizligini baholash qism tizimining funksional tuzilmasi ishlab chiqildi (3.3-rasm).



3.3-rasm. Axborot-kutubxona tizimida «Axborot xavfsizligini baholash» qism tizimining funksional tuzilmasi

«Axborot xavfsizligi» qism tizimi axborotlarni yig‘ish, ekspertlar guruhini shakllantirish, tizim elementlarini identifikatsiyalash va baholash, AXT bo‘yicha choralarni aniqlash, AXni baholash, axborotlarni saqlash modullar majmuasini o‘z

ichiga oladi. Qism tizim u qo‘llanilayotgan korporativ axborot-kutubxona tizimi bilan o‘zaro bog‘langan.

- *Axborotlarni yig‘ish moduli*. Ushbu modul AKMning resurslari, himoyaning mavjud usul va vositalari, axborot xavfsizligini baholash mezonlari haqidagi kiruvchi axborot oqimlarining tavsifini shakllantirish orqali axborot kutubxona muassasasi muhiti vaziyatlarini to‘playdi.

- *Ekspertlar guruhini shakllantirish moduli* ekspertlarni ro‘yxatga olish, identifikatsiya, autentifikatsiya va avtorizatsiyalashga mo‘ljallangan;

- *AKM resurslarini identifikatsiyalash va baholash moduli*. Ushbu modul himoyalanuvchi resurslarni, himoya choralarini identifikatsiyalash hamda ekspert baholari va statistik ma’lumotlarga tayanib, mezonlar asosida baholashni amalga oshiradi.

- *AXT bo‘yicha choralarni aniqlash moduli*. Ushbu modul avvalo «Vaziyat – Tahdid – Chora» turidagi NMMning bazasini shakllantiradi va ularning mosligi bo‘yicha ekspert baholarini o‘rnatadi. So‘ngra muhimlilik koeffitsenti usuli asosida AXT bo‘yicha ratsional choralarni aniqlaydi. Shu bilan birga ushbu modulda konkordatsiya koeffitsentini aniqlash orqali ekspertlar fikrining hamjihatligini tekshiradi.

- *AXni baholash moduli*. Ushbu modul avvalo AKMning mavjud resurslarini va ularga o‘rnatilgan himoya choralarini filtrlaydi hamda «AKM resurslarini identifikatsiyalash va baholash moduli» hamda «AXT bo‘yicha choralarni aniqlash moduli» yordamida qo‘llanilayotgan himoya choralarining mosligini aniqlaydi. Agar choralar mos bo‘lmasa tegishli tavsiyalarni shakllantiradi.

- *Axborotlarni saqlash qism tizimi* ma’lumotlar bazasi va bilimlar bazasidan tashkil topgan bo‘lib, u quyidagilarni o‘z ichiga oladi: AKMning resurslari, AXga tahdidlar, AXBning usullari va vositalari haqidagi ma’lumotlar majmuini; qoidalar, taqqoslash mezonlari, xulosalar; ma’lumotlar bazasi va bilimlar bazasini boshqarish uchun maxsus dasturiy ta’minot; ma’lumotlar bazasi va bilimlar bazasining normal

faoliyat ko‘rsatishi uchun lozim bo‘lgan xizmat ma’lumotlari. Bilimlar bazasi doimiy yangilanib boradi, ruxsatsiz kirishlardan himoyalangan.

- *Axborotlarni chiqarish moduli* har bir bosqichda taqdim etilgan natijalar asosida hisobotlarni shakllantirish imkonini beradi.

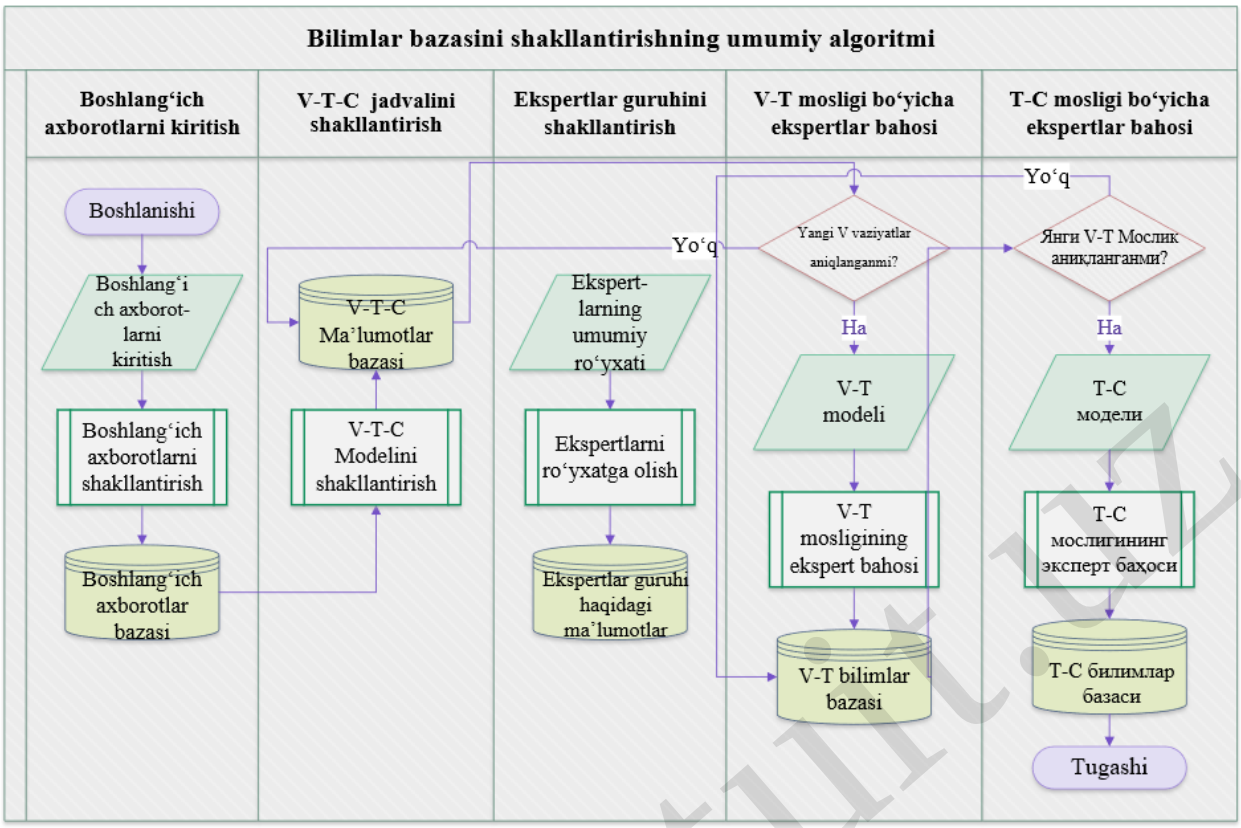
Ushbu bo‘limda korporativ axborot-kutubxona tizimi uchun axborot xavfsizligi qism tizimi hisoblangan eLibIS dasturiy kompleksining funksional tuzilmasi hamda uning funksional talablari ishlab chiqildi.

3.4 eLibIS dasturiy kompleksining ma’lumotlar va bilimlar bazasini shakllantirish

Oldingi bo‘limda eLibIS dasturiy kompleksining funksional tuzilmasi va asosiy modullarning asosiy vazifalari keltirildi. Ushbu bo‘limda eLibIS dasturiy kompleksining ma’lumotlar va bilimlar bazasini loyihalash model va algoritmlari yaratiladi, shuningdek dasturiy modullarning ishlash jarayonlari ochib beriladi.

Dasturiy kompleksning AXT bo‘yicha choralarni aniqlash moduli AKM uchun mavjud vaziyatlarga nisbatan tahdidlarning hamda aniqlangan tahdidlarga nisbatan himoya choralarining mosligini, Ya’ni bilimlar bazasini shakllantiradi. 3.4-rasmda ushbu jarayonning umumiy algoritmi keltirilgan.

Bilimlar bazasi «Vaziyat-Tahdid» va «Tahdid-Chora» mosligini aniqlash masalalarini yechishda foydalaniluvchi predmet sohasi haqidagi ekspert bilimlarini saqlashga mo‘ljallangan. Bilimlar bazasi freymlar to‘plami va qoida-mahsullardan iborat. Ma’lumotlar tuzilmalarining slotlardan tashkil topgan freymlari bilimlar bazasida obyektlar, hodisalar, vaziyatlar va ular o‘rtasidagi bog‘liqliklarni tavsiflash uchun ishlatiladi. Qoidalar ma’lumotlar bazasida obyektlar, voqealar va vaziyatlar o‘rtasidagi munosabatlarni tavsiflash uchun qo‘llaniladi. Qoidalarda beriluvchi munosabatlar asosida mantiqiy xulosalar beriladi.

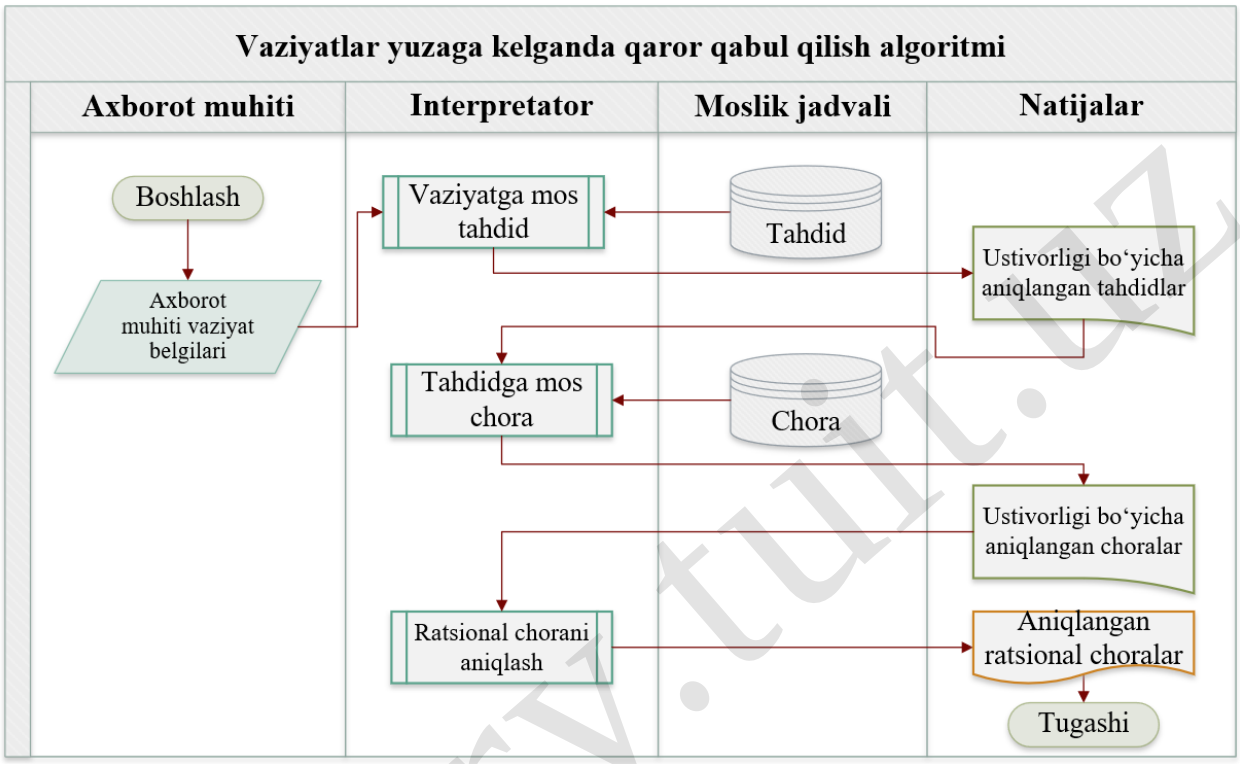


3.4-rasm. Bilimlar bazasini shakllantirishning umumiy algoritmi

Barcha bilimlar «Agar – U holda» turidagi mahsuliy qoidalar shaklida taqdim etiladi. Dasturiy kompleksning bilimlar bazasi ekspert-mutaxassislardan olingan noravshan mahsuliy qoidalardan tashkil topadi. Har safar AKMning AXni baholash jarayonida yangi vaziyatlar yuzaga kelganda bilimlar bazasi yangilanib boradi. Yangi vaziyat vujudga kelganda AXni ta’minlash choralarini aniqlash algoritmi 3.5-rasmda keltirilgan.

Bunda tizimga vaziyat belgilari haqidagi dastlabki axborotlar kiritiladi. Agar tizimga vaziyat belgilarini kiritish jarayoni yakunlansa, tizim ularni o‘zida saqlab oladi, aks holda barcha vaziyat beliglarini tizimga kiritib jarayonni yakunlash kerak. Aniqlangan vaziyatlar interpretatorga kelib tushadi. Agar u yerda vaziyatlarga nisbatan tahdidlar aniqlansa, tizim tahdidlarni ustuvorligi bo‘yicha o‘zida saqlab qo‘yadi, aks holda mos tahdidlarni kiritishni tugatish lozim. Ustuvorligi bo‘yicha aniqlangan choralar keyingi interpretatorga kelib tushadi. U yerda tahdidlarga nisbatan choralar aniqlanganligi sharti tekshiriladi. Agar shart bajarilgan bo‘lsa, ustuvorligi bo‘yicha aniqlangan choralarni tizim o‘zida saqlab oladi, aks holda

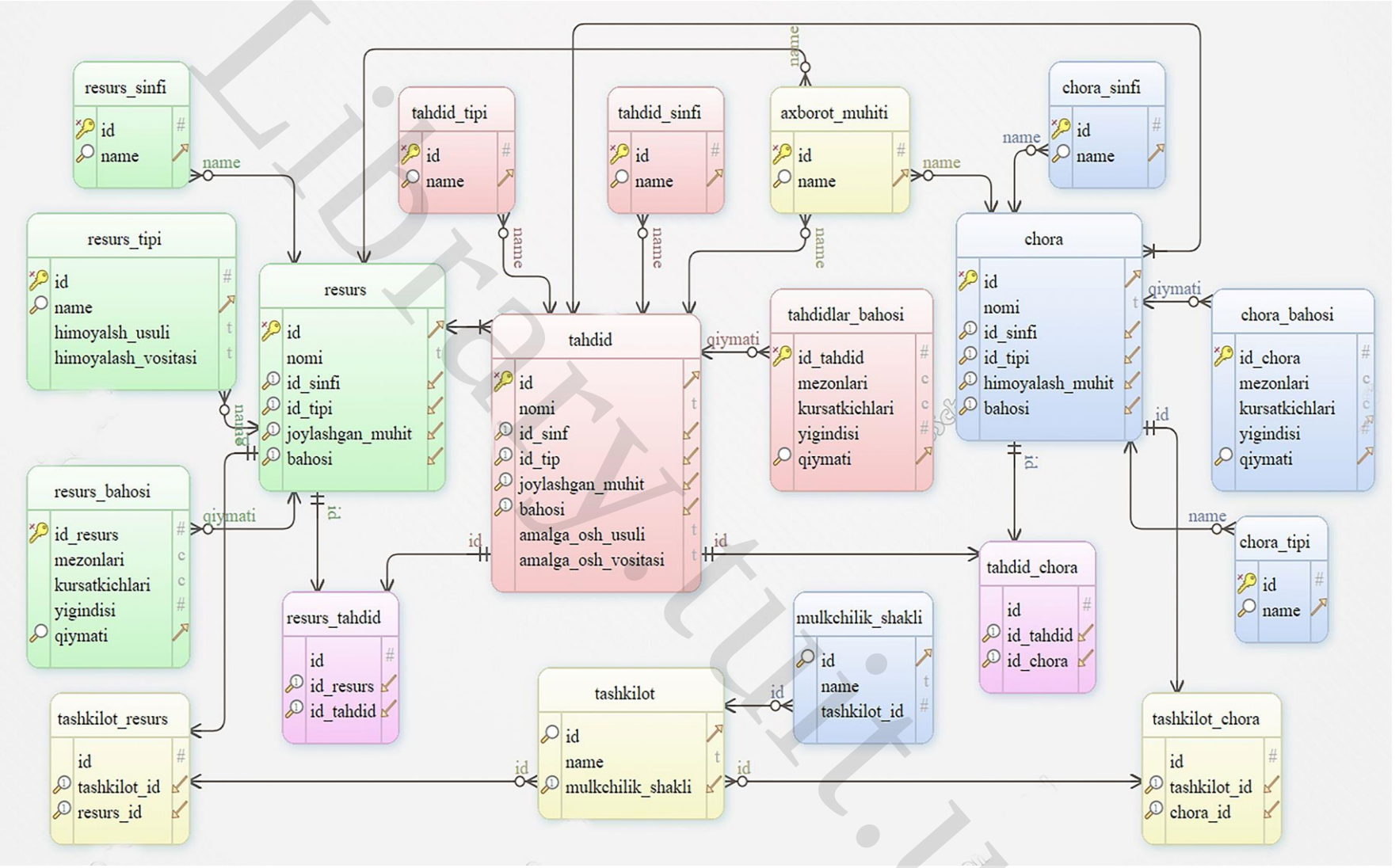
choralarni kiritishni yakunlash lozim. Ustuvorligi bo‘yicha aniqlangan choralar foydalanuvchiga taqdim etiladi. Agar foydalanuvchi o‘ziga ma’qul chorani tanlasa u tanlangan choralar sifatida qabul qilinadi, aks holda biror chorani tanlash lozim bo‘ladi.



3.5-rasm. Vaziyatlar yuzaga kelganda qaror qabul qilish algoritmi

Ma’lumotlar bazasi oraliq yechimlar yoki tizimning tashqi muhit bilan muloqot natijalari bo‘lgan ma’lumotlarni vaqtinchalik saqlashga mo‘ljallangan. Odatda tashqi muhit sifatida tizim bilan muloqotni olib boruvchi shaxs – tashkilotdagi AXni ta’minlash bo‘yicha mas’ul xodim nazarda tutiladi. Ma’lumotlar bazasini modellashtirish uchun dasturiy kompleksning barcha funksiyalarini amalga oshirish imkonini beruvchi infologik IDEF1X modeli ishlab chiqildi (3.6-rasm). Infologik model dasturni yaratish uchun yordamchi ma’lumot hisoblanib, u ma’lumotlar bazasi jadvallarining o‘zaro bog‘lanish shartlarini tavsiflaydi.

Yuqorida keltirilgan model va algoritmlar asosida eLibIS dasturiy kompleksining arxitekturasi ishlab chiqildi. Dasturiy kompleksning foydalanuvchi va ekspert uchun interfeysi yaratildi.



3.6-rasm Axborot xavfsizligi qism tizimi ma’ lumotlar bazasining IDEF 1.X modeli

Foydalanuvchi interfeysi foydalanuvchi bilan muloqotni boshqarishga mo‘ljallangan bo‘lib, uning davomida dasturiy kompleks foydalanuvchidan muloqot jarayoni uchun zarur bo‘lgan faktlarni so‘raydi, shuningdek,foydalanuvchiga ma’lum darajada tizimining mulohazalarini nazorat qilish va tuzatishga imkon beradi. Interfeys quyidagi funksiyalarni bajaradi: ekspertlarni ro‘yxatga olish; so‘rovlarni shakllantirish va ularni ekranda ko‘rsatish; ekspertlarning harakatlarini tasdiqlash va davom ettirish uchun muloqotni qo‘llab-quvvatlovchi xabarlarni ko‘rsatish; o‘rganishning umumiy bayonnomasini shakllantirish; butun tizim ishini muvofiqlashtirish. Foydalanuvchi AKM profilini yaratish va AKM resurslari va vaziyat belgilarini kiritish funksiyasini AKM xodimiga berishi mumkin.

Ushbu bo‘limda eLibIS dasturiy kompleksining ma’lumotlar bazasini loyihalashning IDEF1X metodologiyasiga asoslangan infologik modeli yaratildi. Bilimlar bazasini shakllantirishning umumiy algoritmi, vaziyatlar yuzaga kelganda AXni ta’minlash choralarini aniqlash algoritmlari yaratiladi.

IV BOB. AXBOROT XAVFSIZLIGINI TA’MINLASH TIZIMI FAOLIYATNINING TASHKILIY VA TEXNIK JIHATLARI

4.1 eLibIS tizimini boshqa axborot-kutubxona tizimlari bilan integratsiya qilish mexanizmlari

eLibIS dasturiy kompleksini ixtiyoriy axborot tizimiga qo‘llash mumkin bo‘lib, bo‘limda ARMAT++ avtomatlashgan kutubxona tizimi asosida yaratilgan KAKT bilan integratsiyasi qaraladi.

Ishlab chiqilgan eLibIS dasturiy kompleksi KAKTda qo‘llash maqsadida ishlab chiqilgan bo‘lsa-da, uni ixtiyoriy axborot tizimiga integratsiya qilish mumkin. Dastlabki bosqichda «Vaziyat-Tahdid» va «Tahdid-Chora» mosliklari bo‘yicha bilimlar bazasi mavjud bo‘lmay, u har safar tashkilotlar axborot xavfsizligini baholash jarayonida boyib boradi. Shunday qilib eLibIS dasturiy kompleksi quyidagi imkoniyatlarga ega:

– Ixtiyoriy tashkilot yoki axborot resurs markazlarining himoyalanuvchi resurslari haqida ma’lumotlari asosida resurslarning muhimlilik darajasini baholash.

– Tashkilotdagi resurslarni saqlash bilan bog‘liq barcha vaziyatlarni hisobga olgan holda bo‘lishi mumkin bo‘lgan tahdidlarni va ularning xavflilik darajasini aniqlash.

– Tashkilot resurslarining bahosi, vaziyatlari va qo‘llanilayotgan joriy himoya choralari asosida tashkilot axborot xavfsizligini baholash.

– Tashkilot axborot xavfsizligi samaradorligini oshirish bo‘yicha yechimlarni shakllantirish.

– Axborot-kutubxona tizimlari, elektron kutubxonalar kabi boshqa axborot tizimlari bilan integratsiyalashish va avtonom ishlay olish.

Dasturiy kompleksning axborot xavfsizligi bo‘yicha xodim ish o‘rni interfeysi 4.1-rasmda keltirilgan.

4.1-rasm. eLibIS dasturiy kompleksi interfeysi

«Resurslar» tugmasi tashkilot resurslari haqidagi ma’lumotlarni kiritish uchun mo‘ljallangan (4.2-rasm). «Vaziyatlar» tugmasi orqali tashkilot resurslari bilan bog‘liq vaziyatlarni kiritish mumkin. «Tahdidlar» tugmasi tashkilot resurslariga ta’sir etishi mumkin bo‘lgan tahdidlar ro‘yxatini kiritish imkonini beradi. «Himoya choralari» tugmasi orqali tashkilot tomonidan qo‘llanilayotgan himoya choralari hamda tahdidlarni bartaraf etish choralari kiritiladi. «Resurslarni baholash» tugmasi orqali tashkilotda resurslar muhimliligini baholash jarayonini boshlash mumkin.

eLibISda ikki xil avtomatlashgan ish o‘rni mavjud: tashkilotning axborot xavfsizligi bo‘yicha xodimi ish o‘rni hamda axborot xavfsizligi bo‘yicha ekspert ish o‘rni. Axborot xavfsizligi bo‘yicha xodim deganda tashkilotning axborot xavfsizligini ta’minlash bo‘yicha mas’ul shaxs tushuniladi. Oliy ta’lim muassasalarining axborot resurs markazlarida axborot xavfsizligi bo‘yicha xodim shtati ko‘zda tutilmagan. eLibIS joriy etilgan 4 ta tashkilotlar ichida Oliy va o‘rta maxsus ta’lim vazirligi huzuridagi Ta’lim muassasalarida elektron ta’limni joriy etish markazi axborot xavfsizligi bo‘yicha o‘z xodimiga ega.

Axborot xavfsizligi bo‘yicha ekspert sifatida elektron ilmiy-ta’limiy resurslarni yaratish, saqlash ular bilan ishlash, shuningdek axborot xavfsizligi sohasidagi yuqori malakali mutaxassislar taklif etilishi mumkin.

Axborot xavfsizligi bo‘yicha xodim tizimda quyidagi huquqlarga ega:

– tashkilot profilini yaratish, uning ma’lumotlarini o‘zgartirish;

– tashkilot resurslari haqidagi ma’lumotlarni tizimga kiritish, ularni o‘zgartirish;

– tashkilot resurslari bilan bog‘liq vaziyatlarni tizimga kiritish, ularni o‘zgartirish;

– tashkilot resurslariga bo‘lishi mumkin bo‘lgan tadidlarni tizimga kiritish, ularni o‘zgartirish;

– tashkilotning joriy himoya choralarini tizimga kiritish, ularni o‘zgartirish.

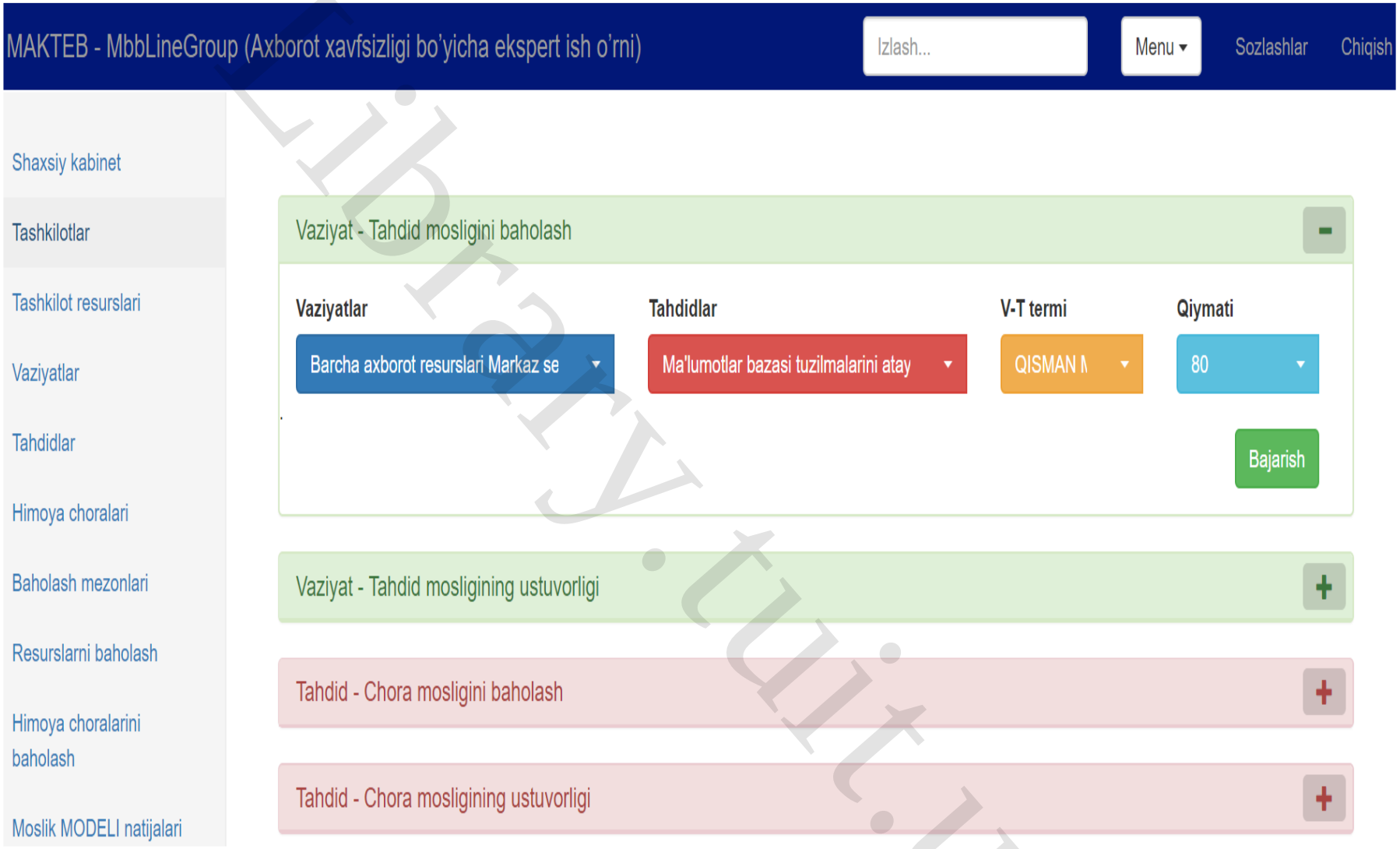
4.2-rasm. Tashkilot axborot resurslarini qo‘shish

Axborot xavfsizligi bo‘yicha ekspertning huquqlari quyidagilardan iborat:

– tashkilot haqidagi ma’lumotlarni, uning resurslari, vaziyatlari va

– himoya choralarini ko‘ra olish;

– tashkilot haqidagi ma’lumotlarni, uning resurslari, vaziyatlari va himoya choralarini ko‘ra olish;



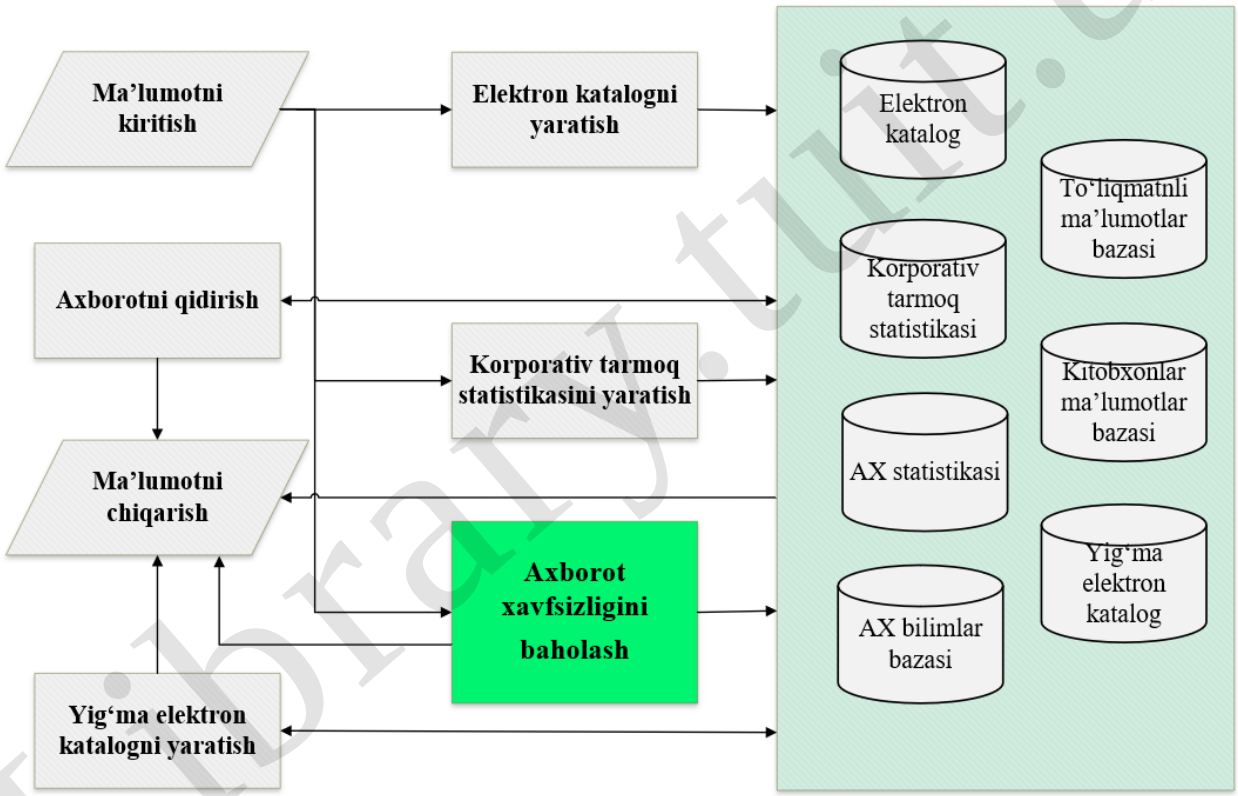
4.3-rasm. eLibIS dasturiy kompleksida ekspert ish o‘rni interfeysi

– tashkilot resurslari muhimliligini berilgan mezon va ko‘rsatkichlar asosida baholash;

– «Vaziyat-Tahdid» mosligini baholash;

– «Tahdid-Chora» mosligini baholash (4.3-rasm).

Axborot xavfsizligi bo‘yicha xodim va ekspert tizimga o‘z parol va loginlari bilan istalgan nuqtadan kirishlari mumkin. Bitta tashkilotga axborot xavfsizligi bo‘yicha bitta xodim va axborot xavfsizligi sohasidagi bir nechta ekspertlar biriktiriladi. Ba’zi hollarda tashkilot axborot xavfsizligi xodimlari ham ekspert sifatida ishtirok etishi mumkin.



4.4-rasm. ARMAT++ avtomatlashgan kutubxona tizimining funksional tuzilmasi va unda «Axborot xavfsizligini baholash» qism tizimining o‘rni

Tizim kiritilgan baholarning qaysi ekspertga tegishli ekanligini hisobga oladi. Ushbu ma’lumotni faqatgina axborot xavfsizligi bo‘yicha xodim ko‘ra olishi mumkin.

Hozirda mamlakatimizdagi barcha oliy ta’lim muassasalarining axborot resurs markazlari uchun ARMAT++ avtomatlashgan kutubxona tizimi asosida yaratilgan

KAKT ishlab turibdi [62; 43-b.]. KAKTni Oliy va o‘rta maxsus ta’lim vazirligi huzuridagi Ta’lim muassasalarida elektron ta’limni joriy etish markazi boshqaradi.

Hozirda tarmoq elektron katalogida 450 mingta bibliografik yozuvlar hamda 6 mingta to‘liq matnli resurslar bor. Shunga qaramasdan, ARMAT++ avtomatlashgan kutubxona tizimida axborot xavfsizligini baholash masalalari to‘liq yechilmagan. Shu sababli eLibIS dasturiy kompleksi ushbu tizimga Axborot xavfsizligini baholash qism tizimi bo‘lib kiritildi. 4.4-rasmda ARMAT++ avtomatlashgan kutubxona tizimining funksional tuzilmasi unda Axborot xavfsizligini baholash qism tizimining o‘rni keltirilgan.

ARMAT++ tizimi Yii Framework asosida ishlab chiqilgan bo‘lib, u PhP dasturlash tili va MySQL ma’lumotlar bazasini boshqarish tizimini birlashtiradi. Quyida tizimning asosiy qism tizimlari bayon etiladi:

1. Ma’lumotlarni kiritish qism tizimi. Qism tizim quyidagi vazifalarni bajaradi:

– MARC21 formatining talabi bo‘yicha ma’lumotlarni kiritish;

– bibliografik ma’lumotlar asosida elektron katalog ma’lumotlar bazasini yaratish;

– kiritilayotgan ma’lumotlarni tekshirish (ma’lumotning tipi bo‘yicha, nusxasiga tekshirish);

– kitobxonlar, kataloglashtiruvchi, administrator va komplektatorlarning shaxsiy qayd yozuvlarni (kabinetlarni) yaratish.

2. Ma’lumotlarni qidirish qism tizimi. Qism tizim quyidagi vazifalarni o‘z ichiga oladi:

– elektron katalogda soddalashtirilgan qidiruv;

– elektron katalogda kengaytirilgan qidiruv;

– yig‘ma elektron katalogda ma’lumotlarni qidirish;

3. Statistika qism tizimi. U quyidagilarni hisobga olishga mo‘ljallangan:

– ma’lum vaqt oralig‘ida resursdan foydalanish chastotasini;

– kitobxonning qaysi resursdan necha marta foydalanganligi to‘g‘risidagi statistikani;

– kitobxonning muayyan axborot resurs markazidagi elektron resursdan foydalanish chastotasini;

– kitobxonning manbaga murojaat qilish chastotasi;

– korporativ tarmoqdagi axborot resurs markaz elektron resursidan foydalanish chastotasi;

– tiplari bo‘yicha (darslik, o‘quv qo‘llanma, monografiya, dissertatsiya va boshqa) kataloglashtirilgan adabiyotlarning sonli parametrlari.

4. Yig‘ma elektron katalog qism tizimi. Qism tizim quyidagi vazifalarni bajaradi:

– axborot resurs markazining yig‘ma elektron katalog bazasini yaratish;

– axborot resurs markazning elektron katalogidan bibliografik yozuvlarni o‘zlashtirish;

– foydalanish shartlariga (bepul, ro‘yxatdan o‘tgandan so‘ng, pullik) muvofiq ravishda to‘liqmatnli manbalarni o‘zlashtirish;

5. Axborotni chiqarish qism tizimi. Qism tizim quyidagi vazifalarni o‘z ichiga oladi:

– elektron katalogni chiqarish;

– kitobxonning so‘roviga ko‘ra to‘liq matnli ma’lumotlarni chiqarish;

– qidiruv natijasida topilgan ma’lumotlarni (bibliografik ma’lumotlar ro‘yxati) chiqarish;

– kitobxonlar to‘g‘risidagi ma’lumotlarni chiqarish.

Ushbu bo‘limda ARMAT++ avtomatlashgan kutubxona tizimiga eLibIS dasturiy kompleksining integratsiyasi hamda dasturiy kompleks imkoniyatlari keltirildi.

4.2 Elektron kutubxonalar axborot xavfsizligini ta’minlashning tashkiliy va texnik jihatlari

KAKT yoki ixtiyoriy tashkilot AX masalalarini yechishda eLibIS dasturiy kompleksini qo‘llash uchun tashkilotning mavjud axborot resurslarining tasnifi, soni,

saqlash va foydalanish tartibi kabi barcha ma’lumotlarni o‘z ichiga olgan vaziyatlari hamda resurslar xavfsizligini ta’minlash bo‘yicha joriy himoya choralar ro‘yxati talab etiladi.

eLibIS dasturiy kompleksini qo‘llash uchun Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti va uning Qarshi filiali, Oliy va o‘rta maxsus ta’lim vazirligi huzuridagi Ta’lim muassasalarida elektron ta’limni joriy etish markazi hamda O‘zbekiston Respublikasi Madaniyat vazirligi Respublika markaziy ko‘zi ojizlar kutubxonalari tanlab olindi.

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti axborot resurs markaziga uning direktori rahbarlik qiladi. Axborot resurs markazi resurslarining tasnifi va soni, ularni saqlash va foydalanish tartibi bo‘yicha barcha vaziyatlar axborot resurs markazi direktori bilan yuzma-yuz suhbat hamda hisobotlaridan olindi. 4.1-jadvalda olingan vaziyatlar ro‘yxati keltirilgan.

4.1-jadval

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Axborot resurs markazining AX bo‘yicha vaziyatlari

Axborot muhiti vaziyatlari		Vaziyat belgilari
V1	Tashkilot nomi	Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
V2	Mulkchilik shakli	Oliy ta’lim muassasasi
V3	Bo‘lim nomi	Axborot resurs markazi (ilmiy-texnik kutubxonasi)
V4	axborot resurs markaz xodimlari soni	35 nafar
V5	Axborot resurs markazi foydanuvchilarining tarkibi va ularning soni	Axborot resurs markazi foydaluvchilari professor-o‘qituvchilar, ilmiy xodimlar, talabalar va boshqa turdagi kitobxonlar bo‘lib, ularning umumiy soni 6265 ta.
V6	Elektron kutubxona muhiti	Elektron kutubxona 2 ta elektron o‘quv zalidan iborat bo‘lib 70 ta kompyuterga ega.
V7	2018 yil davomida Elektron resurslarga murojaatlar soni	80869 ta
V8	Elektron resurslar tiplari va ularning nomlari soni	- 25431 nomda, shulardan - elektron darsliklar 3646; - elektron o‘quv qo‘llanmalar 6055; - elektron badiiy adabiyotlar 554; - elektron ilmiy adabiyotlar 15176; - elektron maqolalar 6000;

Axborot muhiti vaziyatlari		Vaziyat belgilari
		- dissertatsiyalar 1350
V9	Elektron axborot resurslaridan foydalanish muhiti	Lokal tarmoqda
V10	Elektron katalogdagi resurslar soni	44466 ta bo‘lib, undan TATU va uning 5 ta filiali foydalanadi.
V11	Avtomatlashgan kutubxona tizimi nomi	Irbis, Armat++.
V12	Elektron resurslar saqlanadigan muhit	Serverda
V13	Server uchun qo‘llangan himoya choralari	Standart (OTMlarga qo‘yilgan talablar asosida)
V14	Elektron kutubxona foydalanuvchilarini autentifikatsiyalash vositasi	Login va parol asosida
V15	Lokal tarmoq kompyuterlarining himoya choralari	Antivirus dasturi: Kasperskiy, dastur bazasi yangi; dastur litsenzion emas.
V16	Obuna yoki kitob sotib olishga oxirgi 3 yilda sarflangan mablag‘lar:	2018 yil 715 786 318 so‘m 2017 yil 350 544 106 so‘m 2016 yil 197 628 940 so‘m
V17	Sotib olingan kitoblarning oxirgi 3 yilda raqamli ko‘rinishga o‘tkazilib lokal tarmoqqa qo‘yilganligi	2018 -50 ta 2017 – 456 ta 2016 - 872 ta
V18	Xorijiy ilmiy bazalardan yuklab olingan ilmiy resurslar soni	5000 ta
V19	Scopus analitik tizimiga va Elsevier ilmiy bazasiga milliy obuna	3 yilga 2 million AQSH dollorini tashkil etadi
V20	Web of Science analitik tizimiga milliy obuna	1 yilga 500 ming AQSH dollorini tashkil etgan
V21	Ish vaqti	Kutubxona 8:00 dan 17:00 gacha, elektron resurslardan foydalanish uzluksiz ishlaydi.

Ushbu ma’lumotlar axborot resurs markaz resurslari bahosi va xavfsizlik darajasini aniqlashda ekspert(lar)ga boshlang‘ich axborot sifatida taqdim etiladi.

Respublika markaziy ko‘zi ojizlar kutubxonasida asosan brayl shriftidagi adabiyotlar va audio materiallar saqlanib, kutubxona viloyatlarda o‘zining hududiy bo‘limlariga ega. Kutubxona AX vaziyatlari tashrif chog‘ida, suhbat asosida aniqlandi.

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Qarshi filiali axborot resurs markazida asosan elektron ilmiy adabiyotlar (darsliklar, qo‘llanmalar, maqolalar, dissertatsiyalar, xorij ilmiy bazalaridan yuklab olingan materiallar va hakozo) saqlanib, 1000 dan ortiq foydalanuvchiga xizmat

ko‘rsatadi. AX bo‘yicha axborot resurs markazidagi vaziyatlar tashrif chog‘idagi o‘rganish va hisobotlar asosida aniqlandi.

4.2-jadval

Ta’lim muassasalarida elektron ta’limni joriy etish markazi KAKTning AX bo‘yicha vaziyatlari

Axborot muhiti holatilari		**Holat belgilari**
V1	Tashkilot nomi	Ta’lim muassasalarida elektron ta’limni joriy etish markazi
V2	Mulkchilik shakli	Markaz
V3	Bo‘lim nomi	Axborot ta’lim resurslarini rivojlantirish bo‘limi
V4	Bo‘lim xodimlari soni	4 ta
V5	Korporativ axborot-kutubxona foydaluvchilari soni	Tarmoq foydaluvchilari professor-o‘qituvchilar, ilmiy xodimlar va talabalar bo‘lib, ularning umumiy soni 47529 ta.
V6	Korporativ tarmoqqa ulangan OTMlar soni	82 ta
V7	2018 yil davomida Elektron kutubxonaga murojaatlar soni	95 mingdan ortiq
V8	Elektron resurslar tiplari va ularning soni	- elektron darsliklar; - elektron o‘quv qo‘llanmalar; - elektron badiiy adabiyotlar; - elektron ilmiy adabiyotlar; - elektron maqolalar; - dissertatsiyalar
V9	Elektron axborot resurslaridan foydalaniladigan muhit	Internet tarmog‘ida, korporativ tarmoqda
V10	Elektron katalogdagi resurslar soni	571200 nomda
V11	Ishlatilayotgan avtomatlashgan kutubxona tizimi	Armat++
V12	Elektron resurslar joylashgan muhit	HDD 3 TR, Server Windows 2012 R2
V13	Server uchun qo‘llangan himoya choralari	Firewall, ACL, NOD 32
V14	Elektron kutubxona foydalanuvchilarini identifikatsiyalash	Login va parol asosida.
V15	Scopus, Web of Science va Ebsco kabi ilmiy bazalardan yuklab olingan ilmiy resurslar soni	156 ta
V16	Scopus ilmiy bazasiga milliy obuna	3 yilga 2 million AQSH dollorini tashkil etadi
V17	Web of Science ilmiy bazasiga milliy obuna	1 yilga 500 ming AQSH dollorini tashkil etgan

Oliy va o‘rta maxsus ta’lim vazirligi huzuridagi Ta’lim muassasalarida elektron ta’limni joriy etish markazi 82 ta oliy ta’lim muassasasini birlashtiruvchi korporativ axborot-kutubxona tarmog‘iga ega. Markaz oliy ta’lim muassasalaridagi axborot resurs markazlari faoliyatini muvofiqlashtirib, uslubiy, axborot va texnik ko‘mak beradi. Markaz korporativ axborot-kutubxona tarmog‘ining axborot AX bilan bog‘liq vaziyatlari tizim ma’muri va bo‘lim boshliqlari bilan suhbat asosida aniqlandi (4.2-jadval).

Keyingi bo‘limda eLibIS dasturiy kompleksini korporativ axborot kutubxona tarmoqlarida qo‘llash haqida bayon etiladi.

4.3 Korporativ axborot kutubxona tarmoqlarida foydalanishni boshqarishning kengaytirilgan modeli

Xavfsizlik modellari himoyalangan tizim arxitekturasining bazaviy prinsiplarini tanlash va asoslash uchun xizmat qilib, subyektlarning obyektlardan foydalanish tartibini belgilaydi. Hozirda ko‘pgina axborot tizimlarida xavfsizlikning diskretsion, mandatli va rolli modellari qo‘llaniladi. Har bir model o‘zining afzallik va kamchiliklariga ega bo‘lib, optimal model korxona xavfsizligining maqsadi asosida tanlanadi. Axborot tizimlarida foydalanishni boshqarishning mavjud modellari haqida to‘xtalib o‘tamiz.

Xavfsizlikning diskretsion modeli

Ushbu konseptual model har bir subyektning har bir obyekt uchun huquqlarini aniqlaydi [90]. Obyektlarga murojaatlar belgilangan huquqlar asosida yoki ruxsat etiladi yoki taqiqlanadi. Ushbu model axborotdan foydalanuvchi subyektlar, himoyalanuvchi axborotga ega bo‘lgan obyektlar va mos harakatlarni anglatuvchi foydalanish xuquqlarining majmui ko‘rinishida ifodalanadi. Modelni amalga oshirish sodda va boshqarishda samarali hisoblanib, hech qanday murakkab algoritmlarni talab etmaydi va foydalanuvchilar vakolatlarini obyektlar ustida amal bajarilishigacha aniqlikda boshqarishga imkon beradi. Diskretsion modelning asosiy kamchiligi

shundan iboratki, u noqonuniy foydalanuvchining axborotdan foydalana olmasligini to‘liq kafolatlay olmaydi. Bu shunda ko‘rinadiki, axborotni o‘qishga ruxsati bo‘lgan subyekt axborotni obyektning egasini ogohlantirmasdan turib u bilan tanishishga ruxsati bo‘lmagan boshqa subyektga yuborishi mumkin. Yana bir kamchilik sifatida obyekt va subyekt o‘rtasidagi munosabatlarni batafsil yozishdagi qiyinchiliklar. Bu tufayli himoya tizimini boshqarish protsedurasi murakkablashadi.

Xavfsizlikning mandatli modeli

Mandatli modellarda tizimning barcha subyekt va obyektlari uchun mos xavfsizlik sathlari belgilab olinib, xavfsizlik sathlari subyektlar va obyektlar orasidagi joiz o‘zaro harakatlarni aniqlaydi. Demak, foydalanishni mandatli boshqarish bir xil xavfsizlik sathi berilgan subyektlar va obyektlarni farqlamaydi va ularning o‘zaro harakatiga cheklashlar mavjud emas. Mandatli model subyektning obyekt ustida bajariladigan amallari emas, balki axborot oqimi nazoratlanishi bilan izohlanadi [19]. Ushbu modelda foydalanuvchi va subyekt tushunchalarini ajratish ancha muhimdir. Xavfsizlik darajalari subyektlar uchun beriladi. Foydalanuvchilar esa subyektlar nomidan faoliyat yuritishlari mumkin. Bunda bir foydalanuvchi turli vaziyatlarda turli subyektlar nomidan xarKAKTlanishi mumkin. Bunday hollarda foydalanuvchi konkret vaqtda faqat bitta subyektning nomidan xarkatlanishini ajratish muhim hisoblanadi.

Xavfsizlikning rolli modeli

Rolga asoslangan foydalanishni nazorat qilish axborotga kirishni foydalanuvchining faoliyatini tartibga solish asosida boshqaruvni o‘z ichiga oladi. Bunday boshqaruv tizimda konkret ish faoliyati bilan bog‘liq harakatlar to‘plami va majburiyatlar asosida rollar aniqlashni talab qiladi. Kirish huquqlari alohida foydalanuvchilarga emas, balki rollarga tayinlanadi. Ushbu modelning asosiy afzalligi boshqarishning soddaligidadir. Foydalanuvchilarga vakolat tayinlash jarayoni ikki bosqichni o‘z ichiga oladi: birinchisi, foydalanuvchilarga rollarni tayinlash, ikkinchisi, rolning ma’lum obyektlarga kirishini nazorat qilishni aniqlash. Bunday yondashuv boshqaruv jarayonini ancha yengillashtiradi. Ushbu modelning

yana bir afzalligi agar foydalanuvchining funksiyasi o‘zgarsa, uning rolini qayta tayinlash bilan kifoyalanish hamda boshqa rollarni boshqarishi uchun imtiyozga ega bo‘lgan maxsus rollarni tayinlash mumkinligidir.

Mavjud klassik xavfsizlik modellari KAKTda himoyalanayotgan obyektlarga kirish huquqlarini o‘rnatishda kerakli moslashuvchanlikni ta’minlamaydi. Bu avvalo kitobxonlarga kirishning maksimal qulay, tez hamda uning autentifikatsiya va avtorizatsiyasi bo‘yicha qo‘shimcha qadamlarsiz taqdim etilishi lozimligi bilan bog‘liq. Ammo bu vaqtda kutubxona ish reglamenti va boshqa meyoriy-huquqiy hujjatlar talablarini e’tibordan chetda qoldirmaslik zarur. Bu axborotlarga, shu jumladan butunmatnli resurslarga (obyektlarga) erkin kirishdan tortib, to kirishning qat’iy chegeralanishgacha bo‘lgan turli variantlarini tashkillashtirishni ko‘zda tutadi. Bundan tashqari kirish vaqt bo‘yicha limitlanishi; ichki korporativ tasdiqlovchi markazlar yoki tashqi tasdiqlovchi markazlar tomonidan berilgan elektron imzolar bilan tasdiqlanishi; Internet tarmog‘ining faqat muayyan IP manzili (yoki uning diapozoni) bilan taqdim etilishi yoki boshqa biror shart bilan chegaralanishi mumkin [27].

Mavjud namunaviy modellarga tayangan holda, KAKT uchun resurslardan foydalanish huquqlarini boshqarish ishchi qobiliyati yuqori, kengaytirilgan modelni ishlab chiqishni tadqiq etamiz. Dastlab, nazarda tutilayotgan KAKTning kengaytirilgan va umumlashgan xavfsizlik boshqaruv modelini qurish uchun asos bo‘ladigan omillarini belgilab olamiz.

Asosiy elementlar:

$S = \{s_i = (i,\ t_{creat}, t_{end}) : i = \overline{1..sn}\}$ – *subyektlar (foydalanuvchilar) to‘plami bo‘lib, u maxsus kod, qaysi guruhga kirishi hamda yaratilgan va tugatilish vaqti parametrlarga ega;*

$G = \{g_j : j = \overline{1..gn}\}$ – *subyektlar guruhi to‘plami (foydalanuvchilarning turlari yoki sinflari);*

$SG = \{s_i, g_j\}$ – *subyekt mansub bo‘lgan guruhlar to‘plami (bir subyekt bir vaqtning o‘zida bir nechta guruhga mansub bo‘lishi mumkin);*

$PG = \{pg_i : i = \overline{1..pgn}\}$ – *imtiyozga ega bo‘lgan guruhlar to‘plami, uning a’zolari barcha obyektlarga to‘liq kirish huquqiga ega (imtiyozlilar to‘plamida bir vaqtning o‘zida bir necha guruhlarning elementlari bo‘lishi mumkin);*

$SPG = \{s_k,\ pg_i\}$ – *subyekt mansub bo‘lgan imtiyoz turlari to‘plami (subyekt birorta imtiyozga tegishli bo‘lmasligi ham mumkin);*

$O = \{o_j = (j,\ t_{cteat}, t_{end}) : j = \overline{1..on}\}$ – *obyektlar to‘plami (ba’zi obyektlarga kirish huquqlari aniq berilgan bo‘lishi mumkin, qolganlariga esa huquqlar dinamik aniqlanadi). U maxsus kod, qaysi guruhga kirishi hamda yaratilgan va tugatilish vaqti parametrlarga ega;*

$C = \{c_i : i = \overline{1..cn}\}$ – *obyektlar guruhi to‘plami (obyektlar, Ya’ni kutubxona resurslarining turlari yoki sinflari). Bir obyekt bir vaqtning o‘zida bir necha obyektlarlar guruhiga mansub bo‘lishi mumkin;*

R – *кириш ҳуқуқлари тўплами;*

$AGC = \{g_k, c_j, \{r\} : \forall k \le gn, j \le cn\}$ – *har bir subyektlar guruhining obyeklar guruhiga ruxsati to‘plami.*

$AGO = \{g_k, o_j, \{r\} : \forall k \le gn, j \le on\}$ – *har bir subyektlar guruhining obyeklarga ruxsati to‘plami.*

$ASC = \{s_k, c_j, \{r\} : \forall k \le sn, j \le cn\}$ – *har bir subyektning obyektlar guruhiga ruxsati to‘plami.*

$ASO = \{s_k, o, \{r\} : \forall k \le sn, j \le on\}$ – *har bir subyektning obyektlarga ruxsati to‘plami.*

$H = \{s_i,\ o_i\ ,\ t_i\}$ – subyektlarning obyektlarga eng so‘nggi kirish vaqtlari to‘plami;

$AUTH$– *subyektlarni autentifikatsiyalash usullarining to‘plami;*

IP– *ajratilgan maxsus -adreslar to‘plami;*

Biz yuqorida tadqiq etilayotgan model uchun zaruriy omillar to‘plamiga belgilashlar kiritdik. Endi foydalanishni boshqarish jarayonida amalga oshiriladigan asosiy funksiyalarni qaraymiz.

$S, O \rightarrow (s_i, t_i): (o_j, t_j) \rightarrow min(t_i, t_j)$ – *bu funksiya obyektga murojaat qilish muddati tugaganligini yoki subyektning KAKTdan foydalanish vaqti tugaganligini qaytaradi;*

$S, C \rightarrow (s_i, t_i) \rightarrow t_i$ – *bu funksiya subyektning obyektlar guruhidan foydalanish vaqti tugaganligini qaytaradi;*

$G, O \rightarrow (o_i, t_i) \rightarrow t_i$ – *bu funksiya subyektlar guruhining obyektdan foydalanish vaqti tugaganligini qaytaradi;*

$S, AUTH \rightarrow S_{AUTH}$ – *bu funksiya subyektni KAKTga kirishda tanlangan usul orqali autentifikatsiyalaydi;*

$IP, AUTH_{IP} \rightarrow S_{AUTH}^{IP}$ – *bu funksiya subyektlarni berilgan IP-adreslar bo'yicha tezkorlik bilan autentifikatsiyalaydi;*

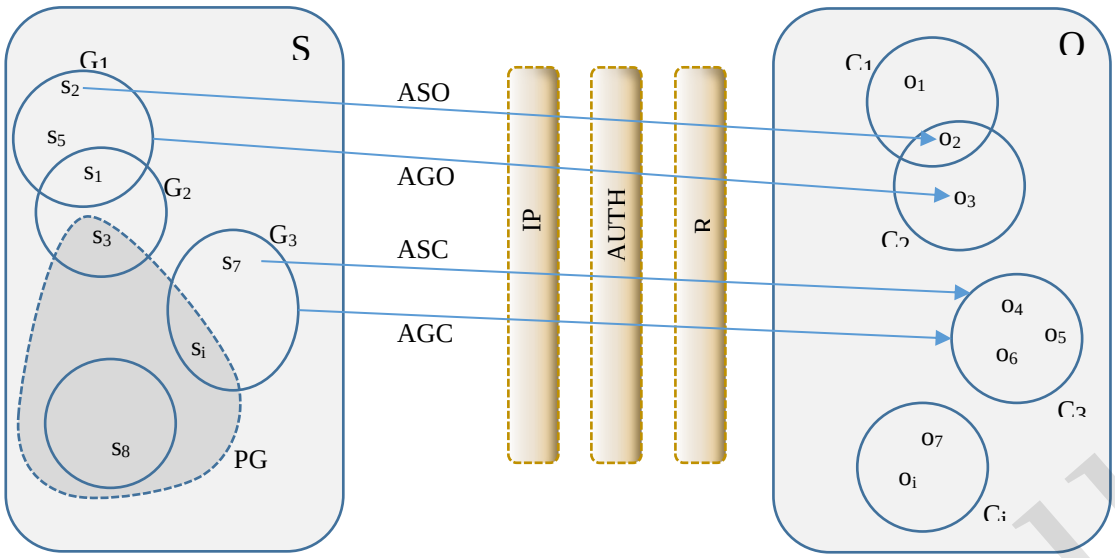
Avail : *S*,*O*,*R* → 1,0 – funksiya o obyektga s subyektning r kirish mumkinligini aniqlaydi.

Tadqiq etilayotgan modeldagi ixtiyoriy omillarning birortasining ta'siri natijasida keltirilgan boshqarish jarayoni funksiyalarning kompleks ishlashining o'zgarishiga olib keladi (masalan, qonuniy foydalanuvchi tizimda autentifikatsiyadan o'tadi va unga tizimning ma'lum obyektlaridan foydalanishga huquq beriladi). Ya'ni, tizim yangi holatga o'tadi va uni tizim holati deb ataymiz. Bundan kelib chiqqan holda KAKTning holatini quyidagicha ifodalash mumkin.

$$Q = \{q(S, G, O, C, AUTH, IP, SG, PG, SPG, AGS, AGO, ASC, ASO)\}$$

Bu yerda q – KAKT holatlari, Q – KAKTning barcha holatlari to'plami.

Taklif etilayotgan KAKTda foydalanishni boshqarish modelining umumlashgan tuzilmasini 1-rasmdagi kabi tasvirlash mumkin (4.5-rasm):



4.5-rasm. KAKTda foydalanishni boshqarish modelining umumlashgan tuzilmasi

Ushbu taklif etilayotgan modelda xavfsizlikning diskretsion va rolli modellari qoidalaridan baravar foydalandik. Mazkur modelda foydalaniluvchi operatorlarni quyidagi 4.3-jadval ko‘rinishinida tasvirlash mumkin:

4.3-jadval

Model operatorlarining funksiyalari

Operatorlar	**Bajarilish sharti**	**Tizim holatidagi o‘zgarish**
o' obyektni yaratish	$o' \notin O$	$O' = O \cup \{o'\}$
c' obyektlar guruhini yaratish	$c' \notin C$	$C' = C \cup \{c'\}$
o' obyektni c obyektlar guruhi to‘plamiga qo‘shish	$o' \in O$ $c' \in C$ $o' \notin c'$	$c' = c \cup o'$
c' obyektlar guruhiga {r} kirish huquqlar to‘plamiga ega g^'guruh yaratish	$g' \notin G$	$G' = G \cup \{g'\}$ $AGC' = AGC \cup (agc', \{r\})$
ago' foydalana olishni nazorat qilish ro‘yxatini o‘zgartirish/qo‘shish orqali g' guruh uchun o' obyektga r' huquqni qo‘shish	$g' \in G$ $r \in R$	$AGO' = AGO \cup \{ago'\}$
agc' ' foydalana olishni nazorat qilish ro‘yxatini o‘zgartirish/qo‘shish orqali g' guruh uchun c' obyektlar guruhiga r' huquqni qo‘shish	$g' \in G$ $r \in R$	$AGC' = AGC \cup \{agc'\}$
ago' foydalana olishni nazorat qilish ro‘yxatini o‘zgartirish/qo‘shish orqali g'	$\{g', o', r'\}$ $\in AGO$	$AGO' = AGO / \{ago'\}$

Operatorlar	**Bajarilish sharti**	**Tizim holatidagi o‘zgarish**
guruh uchun o' obyektga r' huquqni o‘chirish		
agc' ' foydalana olishni nazorat qilish ro‘yxatini o‘zgartirish/qo‘shish orqali g' guruhning c' obyektlar to‘plamiga r' huquqini o‘chirish	$\{g', c', r'\} \in AGC$	$AGC' = AGC \,/\, \{agc'\}$
$auth'$ autentifikatsiyalash usullari to‘plamidan foydalanuvchi va g' guruhlar to‘plamiga mansub s' subyektni yaratish	$g' \in G$ $s' \notin S$	$S' = S \cup \{s'\}$ $G' = G \,/\, \{g'\} \cup \{g' \cup s'\}$ $AUTH' = AUTH/$ $\{auth'\} \cup \{auth' \cup s'\}$
g' guruhlar to‘plamiga s' subyektni qo‘shish	$g' \in G$ $s' \in S$ $g \notin SG_{s'}$	$G' = G \,/\, \{g'\} \cup \{g' \cup s'\}$ $SG'_{s'} = SA'_s/\{g'\}$
g' guruhlar to‘plamidan s' subyektni olib tashlash	$g' \in SG_{s'}$	$G' = G \,/\, \{g'\} \cup \{g'/s'\}$ $SA'_{s'} = SA'_s \setminus \{g'\}$
g' guruhni imtiyozlilar to‘plamiga qo‘shish	$g' \in G$ $g' \notin SPG$	$SPG' = SPG \cup \{g'\}$
o' obyektni c obyektlar to‘plamidan olib tashlash	$o' \in O$; $c' \in C$ $o' \in c'$	$c' = c \setminus o'$
g' guruhni imtiyozlilar to‘plamidan olib tashlash	$g' \in G$ $g' \in SPG$	$SPG' = SPG \setminus \{g'\}$
o' obyektni o‘chirish	$o' \in O$	$O' = O \setminus \{o'\}$
s' subyektni o‘chirish	$s' \in S$	$S' = S \setminus \{s'\}$
g' guruhni o‘chirish	$g' \in G$	$G' = G \setminus \{g'\}$

Shunday qilib, s' subyekt uchun o' obyekt yoki c' obyektlar to‘plamidan r' foydalanish huquqi quyidagicha aniqlanadi:

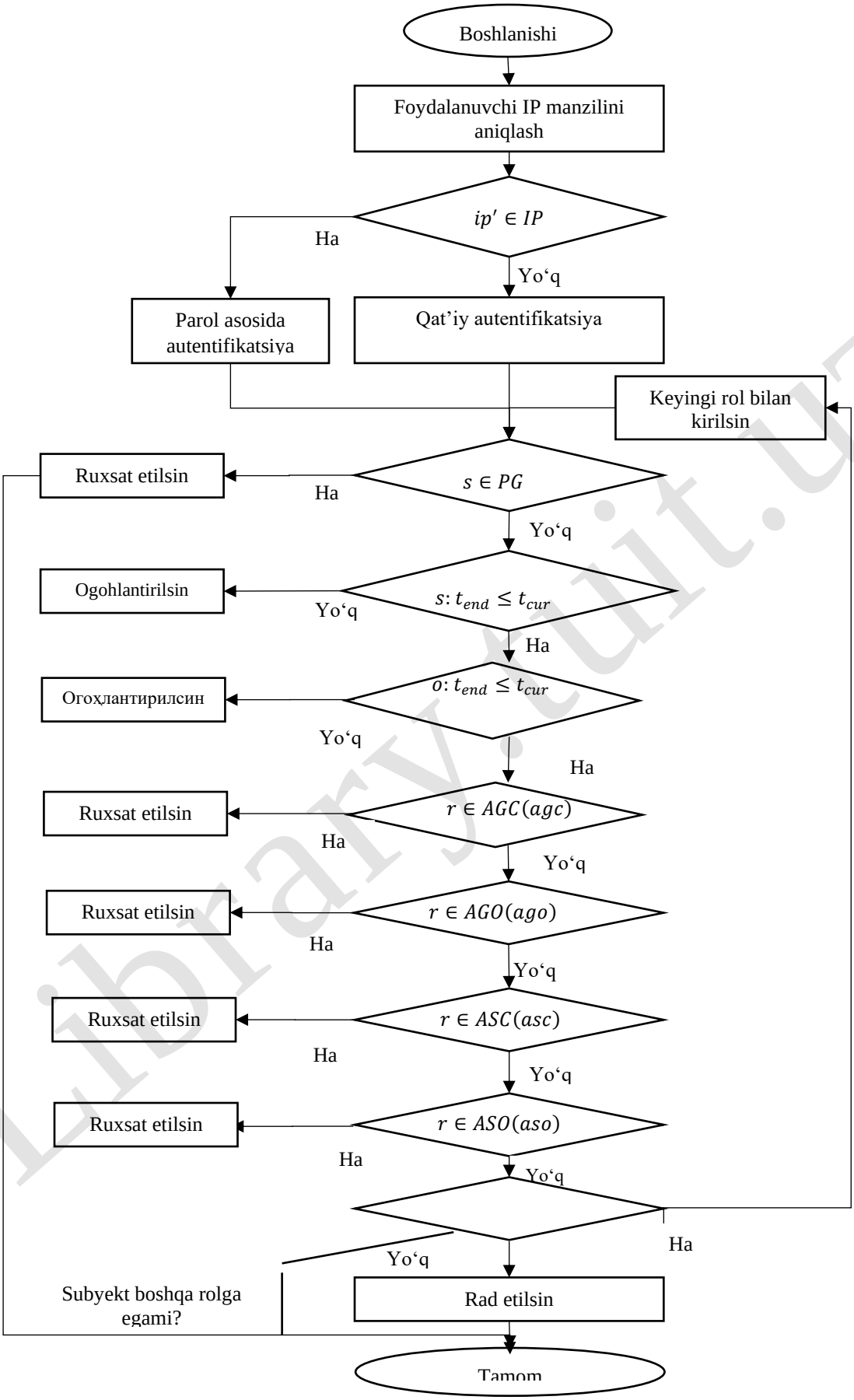
Agar $(SG_s \cap PG) \neq \emptyset$ bo‘lsa, $Avail = 1$ bo‘ladi. Aks holda, kirish huquqi quyidagicha aniqlanadi:

$$Avail = \begin{bmatrix} \left(t_{cur} < (s', t_{end})\right) \wedge \left(t_{cur} < (o', t_{end})\right) \wedge \\ \begin{pmatrix} r' \in AGC(agc') \vee \\ r' \in AGO(ago') \vee \\ r' \in ASC(asc') \vee \\ r' \in ASO(aso') \end{pmatrix} \end{bmatrix} = \langle 0,1 \rangle$$

Ya’ni, ixtiyoriy tashrif buyuruvchi tizimga kirishda avvalo uning IP manzili tekshiriladi. Agar manzil oldindan ajratilgan IP manzillar ro‘yxatida mavjud bo‘lsa, bu foydalanuvchinining autentifikatsiya jarayoni parol asosida amalga oshirilishi mumkin. Aks holda tashrif buyuruvchi o‘ziga biriktirilagan boshqa qat’iy

autentifikatsiya usulida (masalan raqamli imzo, sertifikatlar va boshq) tekshiriladi. Har bir subyekt o‘zining amal qilish muddati belgilangan kitobxonlik guvohnomasiga ega bo‘lib, bir yoki bir necha subyektlar guruhiga mansub bo‘ladi.

Har bir subyekt o‘zining amal qilish muddati belgilangan kitobxonlik guvohnomasiga ega bo‘lib, bir yoki bir necha subyektlar guruhiga mansub bo‘ladi. Agar foydalanuvchi murojaat qilayotgan obyektdan ayni paytda foydalanish mumkin bo‘lsa, u holda subyekt mansub bo‘lgan guruhning murojaat qilinayotgan obyektning guruhiga kirish huquqi tekshiriladi. Agar kirish huquqi mavjud bo‘lsa, u amalga oshiriladi, aks holda subyekt guruhining aynan obyektning o‘ziga kirish huquqi borligi tekshiriladi. Agar ushbu huquq mavjud bo‘lsa, u amalga oshiriladi, aks holda aynan subyektning mazkur obyekt guruhiga kirish huquqi tekshiriladi. Agar bunday huquq mavjud bo‘lsa, u amalga oshiriladi, aks holda subyektning aynan obyektga kirish huquqi tekshiriladi. Agar shunda ham obyektga kirish huquq mavjud bo‘lmasa, u holda subyektning boshqa subyektlar guruhigi tegishliligi tekshiriladi. Agar subyekt boshqa birorta guruhga mansub bo‘lsa, yuqoridagi jarayon takrorlanadi, aks holda subyektning tizimga kirishi rad etiladi. KAKTda foydalanishni boshqarishning mazkur kengaytirilgan modeli algoritmini 4.6-rasm ko‘rinishida tasvirlash mumkin.



4.6-rasm. Foydalanishni boshqarishning kengaytirilgan modeli

Taklif etilayotgan model uchun asosiy elementlar va funksiyalar tanlanib, modelning umumlashgan tuzilmasi, shuningdek algoritmi keltirildi.

XULOSA

Olib borilgan tadqiqotlar natijasida quyidagi xulosalar taqdim etiladi:

1. Barcha turdagi axborotlarning xavfsizlik nuqtai nazaridan tasnifi hamda unda ilmiy-texnik va ta’limga oid axborotlar o‘rnining muhimligi ko‘rsatildi. Ilmiy-texnik va ta’limga oid axborotlar o‘ziga xos xususiyatlarining tahlil etilishi va tizimlashtirilishi ularni tasniflash imkonini berdi.

2. Axborot xavfsizligini baholashning «Vaziyat-Tahdid-Chora» turidagi xususiy noravshan moslik modeli va axborot xavfsizligini ta’minlash choralari ustuvorligini aniqlash algoritmi ishlab chiqildi. Yaratilgan algoritm axborot muhitining aniq vaziyatlarida bo‘lishi mumkin bo‘lgan tahdidlarni hamda shu tahdidlarni bartaraf etish bo‘yicha ratsional himoya choralarini aniqlash imkonini berdi.

3. Korporativ axborot kutubxona tarmoqlari axborot resurslari muhimliligini noravshan o‘zgaruvchilar asosida baholash usuli ishlab chiqildi. Ushbu usul himoyalanuvchi resurslar haqidagi statistik ma’lumotlar va ekspert baholari asosida aniq axborot kutubxona muassasasi resurslarining muhimliligini baholash imkonini berdi.

4. Korporativ axborot-kutubxona muassasasining axborot xavfsizligi darajasini baholash algoritmi ishlab chiqildi. Ushbu algoritm asosida yaratilgan dasturiy modul ekspert baholarini hisoblagan holda aniq axborot-kutubxona muassasasi xavfsizligi darajasini baholash imkonini berdi.

5. Taklif etilgan usullar, algoritmlar va ma’lumotlar bazasini loyihalashning infologik modeli asosida axborot-kutubxona tarmoqlarining ilmiy-texnik va ta’limga oid resurslari xavfsizligini baholash dasturiy kompleksi yaratilgan. Dasturiy kompleks u joriy etilgan tashkilotlarda himoyalanuvchi resurslar muhimliligini hamda axborot xavsizligini baholash imkonini berdi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O’z DSt 2927:2015 O‘zbekiston Respublikasining davlat standarti. Axborot xavfsizligi. Atamalar va ta’riflar.
2. O’z DSt ISO/IES 27002:2016 O‘zbekiston Respublikasining davlat standarti. Xavfsizlikni boshqarish usullari.
3. O’z DSt ISO/IES 27005:2013 O‘zbekiston Respublikasining davlat standarti. Axborot xavfsizligi risklarini boshqarish.
4. O’z DSt ISO/IES 15408:2016 O‘zbekiston Respublikasining davlat standarti. Axborot texnologiyalari xavfsizligini baholash mezonlari.
5. O’z DSt ISO/IES 27010:2015 O‘zbekiston Respublikasining davlat standarti. Xavfsizlikni boshqarish usullari. Sohalararo va tashkilotlararo kommunikatsiyalarda axborot xavfsizligini boshqarish bo‘yicha qo‘llanma.
6. RH 45-024:2009 Rahbariy hujjat. Aloqa va axborotlashtirish sohasida axborot xavfsizligini ta’minlash tizimi to‘g‘risida nizom.
7. RH 45-133:2008 Axborot xavflarini sug‘urta qilish axborot xavflarida axborot tizimlari qiymatini hisoblash metodikasi.
8. Axborot xavfsizligiga oid atamalarning ruscha-o‘zbekcha izohli lug‘ati. «UNICON.UZ» Fan-texnika va marketing tadqiqotlari markazi Davlat unitar korxonasi. Toshkent – 2016. – 733 B.
9. Агурьянов И. Классификация методов и средств защиты информации, 18 Сентября, 2012, [сайт] URL: https://www.securitylab.ru/blog/personal/aguryanov/30011.php (мурожаат вақти: 16.10.2018).
10. Ажмухамедов И.М. Принципы обеспечения комплексной безопасности информационных систем // Вестник АГТУ. Серия: «Управление, вычислительная техника и информатика» №1/2011, С.7-11.

11. Ажмухамедов И.М. Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования. Монография. Астрахань 2012. – 344 С.
12. Арефьева Е.А., Сафронова М.А., Никитина А.В. Разработка системы исследования информационной безопасности организации на основе метода анализа иерархии. Известия ТулГУ. Технические науки. 2016. Вып. 11. Ч. 1
13. Афоничкин А. И., Михаленко Д. Г. А94 Управленческие решения в экономических системах: Учебник для вузов. – СПб.: Питер, 2009. – 480 с.
14. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности. Образовательные ресурсы и технологии, 2015’1(9).
15. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: ИНФРА-М_РИОР, 2014.
16. Бекмуратов Т.Ф. Концепция и задачи построения интеллектуальных систем информационной безопасности. Республиканская научно-техническая конференция “Проблемы информационной безопасности и кибербезопасности в сфере информационно-коммуникационной технологии”. Ташкент 2018.
17. Белим С.В., Богаченко Н.Ф. Применение метода анализ иерахий для оценки рисков утечки полномочий в системах с роловым разграничением доступа. Информацинного-управляющие системы. 2013, № 6(67). С. 67–72.
18. Беляев Д.А. Возможные подходы к оценке стоимости информационных ресурсов регионального вуза. Корпоративное управление и инновационное развитие Севера: Вестник Научно-исследовательского центра корпоративного права, управления и венчурного инвестирования Сыктывкарского государственного университета, Выпуск №4, 2011.
19. Ганиев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Дарслик. Тошкент-2016. -391бет.
20. Девянин П.Н. Модели безопасности компьютерных систем, - М.: Издательский центр «Академия», 2005. -144 с.

21. Дмитрий О. Информационная безопасность и управление рисками [сайт]. https://www.securitylab.ru/blog/personal/dorlov/18815.php (мурожаат вақти: 11.09.2017).
22. Домарев В. В. Безопасность информационных технологий. Методы создания систем защиты // Киев: ООО ТИД ДС. – 2001, 688 с.
23. Камаев В.А., Натров В.В. Моделирование и анализ состояния информационной безопасности организации. Известия ТулГУ, Технические науки, 2011, Вып. 3, С. 148-150
24. Карасёв П. А., Столяренко А. В. Информационная безопасность в корпоративных сетях. Таврический научный обозреватель. 2017, № 3 (20), С. 208-213
25. Клянчин В. К., Сашников Т. К. О Применении нечётких продукционных моделей в подсистемах обеспечения информационной безопасности автоматизированных систем управления специального назначения. Наукоемкие Технологии В Космических Исследованиях Земли, 2016, 8 (S2), 27-32.
26. Коврига С.В. Методические и аналитические основы когнитивного подхода к SWOT-анализу. Проблемы управления, 2005, №5. − С.58–63.
27. Койнов Р. С., Добрынин А. С. Модель управления доступом типовой библиотечной информационной системы. ISSN 2072-9502. Вестник АГТУ. Сер.: Управлене, вычислительная техника и информатика 2016. № 4
28. Коптенков М.М. Категорирование информации первый шаг к обеспечению информационной безопасности организации. Научно-технический журнал «Информационные системы и технологии». -2015. -№ 4. -с. 117-119.
29. Кузнецов О.П., Кулинич А.А., Марковский А.В. Анализ влияний при управлении слабоструктурированными ситуациями на основе когнитивных карт // Человеческий фактор в управлении / Под ред. Н.А. Абрамовой, К.С.Гинсберга, Д.А. Новикова. – М.: КомКнига, 2006. – С.313–344.

30. Кычкин А.В., Елтышев Д.К., Выголова Е.А. Интеллектуальная система оценки соответствия энергоменеджмента предприятия требованиям стандарта. Фундаментальные исследования. – 2014. – № 11-7. – С. 1496-1500;
31. Малий Ю.В., Александров В.В. Рекомендации по проведению анализа и оценки рисков нарушения безопасности информации в банковской сфере. Международный научно-теоретический журнал «Вестник Белгородского университета кооперации, экономики и права», 2015. № 1.
32. Малышев Н.Г и др. Нечеткие модели для экспертных систем в САПР. – М.: Энергоатомиздат, 1991. – 136 с.
33. Малюк А.А., Царегородцев А.В., Макаренко Е.В. Один из подходов к оценке рисков информационной безопасности в облачных средах. Безопасность информационных технологий, 2014, №4. − С.68–74.
34. Машкина И.В. Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий. Диссертация на соискание ученой степени доктора технических наук. Уфа – 2009.
35. Муханова А.А., Ревнивых А.В., Федотов А.М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах. Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2013. Т. 11, вып. 2. С. 55–72.
36. Мухитдинов М., Дадажонов Т., Кулматов Т., Matlab илмий-тадқиқот ишларида. – Тошкент: “O’zbekiston”, 2016. – 256 б.
37. Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Ахборот ресурс маркази веб сайти, https://tuit.uz/uz/axborot-resurs-markazi (мурожаат вақти: 15.03.2019).
38. Низамова Н., Норматов Ш. Архив муассасаларида ахборот хавфсизлигини таъминлашнинг долзарблиги. XIII Международной конференции «Central Asia – 2019». Интернет и информационно-библиотечные ресурсы в науке,

образовании, культуре и бизнесе. 24-26 апреля 2019 г., г. Ургенч, Узбекистан. -С. 288-293

39. Низамутдинова Р.Р. Классификация методов и средств защиты информации. Материалы IX Международной студенческой научной конференции «Студенческий научный форум» [сайт] URL: https://scienceforum.ru/2017/article/2017036043 (мурожаат вақти: 16.10.2018).
40. Николаевна Ф.М., Михайлович И.Э. Обеспечение информационной безопасности электронной библиотеки. Контентус . 2016 6(42):
41. Норматов Ш. Автоматлаштирилган кутубхона ахборот тизимларда фойдаланишни бошқаришнинг кенгайтирилган модели. “Muhammad al-Xorazmiy avlodlari” журнали, № 1(1), 2017 й. -Б. 25-30
42. Норматов Ш. Ахборот кутубхона ресурсларини ҳимоялаш муаммолари ва ечимлари. XII Международной конференции «Central Asia – 2018». Интернет и информационно-библиотечные ресурсы в науке, образовании, культуре и бизнесе. 19-20 апреля 2018 г., г. Термиз, Узбекистан. -С. 235-241
43. Норматов Ш. Жамоат соғлигини сақлашда саломатликка оид ахборот-кутубхона ресурслари хавфсизлигини таъминлашнинг долзарблиги. Сборник материалов международной научно-практической конференции “Modehed – Модернизация учебных курсов о здравоохранении в университетах”, Чимкент, Казахстан, 24-26 сентября, 2017 г. -С. 131-133
44. Норматов Ш. Илмий-таълимий тармоқларда ахборот ресурсларини ҳимоялашнинг асосий вазифалари. Oliy ta’lim taraqqiyoti istiqbollari. Maqolalar to’plami, №5, 2017, Toshkent. -B. 109-112
45. Норматов Ш. Кутубхона ресурслари хавфсизлигини таъминлашнинг ҳуқуқий жиҳатлари. “Иқтисодиётнинг реал тармоқларини инновацион ривожланишида ахборот- коммуникация технологияларининг аҳамияти” мавзусидаги Республика илмий – техник анжуманининг маърузалар тўплами, 3-қисм. Тошкент-2017. -Б. 37-39
46. Норматов Ш. Кутубхона ресурслари ҳимоясига комплекс ёндашув.

“Kutubxona.uz” журнали. № 1(37), 2018 й. -Б. 42-45

47. Норматов Ш. Кутубхона тизимларида ахборот хавфсизлигига таҳдидлар таҳлили. “Kutubxona.uz” журнали. № 1(33), 2017 й. -Б. 40-44
48. Норматов Ш. Ўзбекистонда фан ва таълимга оид электрон ахборот ресурслари хавфсизлигини таъминлашнинг таҳлили. “Технологик жараёнлар ва ишлаб чиқаришларни автоматлаштириш ва оптималлаштиришнинг долзарб муаммолари” Халқаро илмий-техникавий конференция маърузалари тўплами. Қарши, Ўзбекистон, 17-18 ноябрь 2017 й. -Б. 30-33
49. Норматов Ш. Фан ва таълимга оид ахборот ресурсларини ҳимоялашнинг илмий ва амалий муаммолари. “Ахборот-коммуникация технологияларининг ривожланиш истиқболлари” мавзусидаги Республика илмий – амалий анжуманининг маърузалар тўплами, 6-шўъба. Қарши-2018. -Б. 836-839
50. Норматов Ш. Фан ва таълимга оид ахборотларни ҳимоялаш соҳасидаги халқаро тажрибалар таҳлили. Научные информационные ресурсы для инновационного развития. Материалы 11-го ежегодного семинара и презентаций, 23 май 2019 г., -С 52-56
51. Норматов Ш. Шахс, жамият ва давлат ахборот хавфсизлигини таъминлашда ахборот-кутубхона ресурсларини ҳимоялашнинг ўрни. “Muhammad al-Xorazmiy avlodlari” журнали, № 1(1), 2017 й. -Б. 11-15
52. Норматов Ш. Электрон кутубхоналар хавфсизлигини таъминлашнинг долзарблиги. “Иқтисодиётнинг реал тармоқларини инновацион ривожланишида ахборот- коммуникация технологияларининг аҳамияти” мавзусидаги Республика илмий – техник анжуманининг маърузалар тўплами, 3-қисм. Тошкент-2017. -Б. 34-36
53. Норматов Ш., Жабборов Э. Ташкилотда фан ва таълимга оид ресурслар баҳосини ҳисоблашнинг умумлашган критериялари. Научные

информационные ресурсы для инновационного развития. 3-е форум и 10-е ежегодное мероприятие, 30 май 2018 г., -С 57-62

54. Норматов Ш., Солиев Н. Ахборотни ҳимоялаш даражасини баҳолаш критериялари. International Conference on Importance of “Information Technologies in Innovative Development of real Sectors of Economy”, April 5-6, 2018, Tashkent, Uzbekistan. -Б 447-450
55. Норматов Ш., Шукуров О. Ташкилот ахборот хавфсизлигини баҳолашнинг норавшан мослик модели. “Ахборот технологиялари ва коммуникациялари соҳасида ахборот хавфсизлиги ва киберхавфсизлик муаммолари” мавзусидаги Республика миқёсидаги илмий-техник конференцияси материаллари. Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети. 2018 йил 22-23 сентябрь. Тошкент-2018. -Б 23-26
56. Норматов Ш.. Ахборот-кутубхона тизимларида электрон ресурслар хавфсизлигини таъминлашнинг норавшан мослик модели. “Иқтисодиётнинг реал тармоқларини инновацион ривожланишида ахборот- коммуникация технологияларининг аҳамияти” мавзусидаги Республика илмий – техник анжуманининг маърузалар тўплами, 2-қисм. Тошкент-2019. -Б. 239-241
57. Нусратов Т.С. Разработка теории и практических методов реализации алгоритмических систем принятия решений на основе структурных моделей соответствий. Диссертация на соискание учёной степени доктора технических наук. 1983 г.
58. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. М.: Компания АйТи; ДМК Пресс, 2004.
59. Петров А. Б. Открытые информационные системы. Учебное пособие / А. Б. Петров. - М.: МИРЭА, 2000. -38 с.

60. Прохоренков П.А. Этапы формирования электронной-объразовательной среды вуза. Международной журнал экспериментального образования. 2016, № 2, С. 291-294
61. Рахматуллаев М.А. Теория и прикладные методы построения метасистемы генерации решений в детерминированной и нечеткой технологической среде. Диссертация на соискание учёной степени доктора технических наук. 1994 г.
62. Рахматуллаев М.А., Норматов Ш.Б, Каримов У.У. Интегрированная информационная система доступа к научно-образовательным ресурсам в корпоративных сетях. «Известия» Научно-Технического Общества «КАХАК», № 1(60). Алматы-2018 г. -С. 42-50
63. Рахматуллаев М.А., Норматов Ш.Б. Ташкилот ахборот хавфсизлигини таъминлаш масалаларини ечишда норавшан мослик моделларининг татбиқи. “Ахборот-коммуникация технологияларини ривожлантириш шароитида инновациялар” мавзусидаги Республика илмий – техник анжуманининг маърузалар тўплами, 4-шўъба. Қарши-2019. -Б. 332-334
64. Рахматуллаев М.А., Норматов Ш.Б. Электрон кутубхона тармоқларида илмий-таълимий ахборотлар яратиш ва улардан фойдаланиш технологиялари, Тошкент-2017. -Б. 52-57
65. Родина Ю. В. Оценка риска нарушения информационной безопасности по модели нечёткой логики с корректировкой параметров её терм-множеств. управление экономическими системами: Электронный научный журнал, 2011, 6 (30).
66. Ты Минь Фыонг. Композиционные модели и алгоритмы управления в нечетких технологических средах. Диссертация на соискание учёной степени доктора технических наук. 1995 г.
67. Alex W, How Do You Value Information, September 15, 2016, [сайт] https://www.datanami.com/2016/09/15/how-do-you-value-information/ (мурожаат вақти: 21.04.2018).

68. American Library Association. Code of ethics of the American Library Association. http://www.ala.org/advocacy/proethics/codeofethics/codeethics [сайт], (мурожаат вақти: 16.01.2018).
69. Antonio L., Francesca I., Giovanni S. Knowledge assets assessment strategies: organizational value, processes, approaches and evaluation architectures, Journal of Knowledge Management, 2012, Vol. 16 Issue: 4, pp.563-575.
70. Balas J. Close the gates, lock the windows, bolt the doors: securing library computers, Computers in Libraries, 2005, Vol. 25 No. 3, pp. 28-30.
71. Bowers, S. Privacy and library records. The Journal of Academic Librarianship, 2006, 32(4), 377-383.
72. Breeding M. The Current State of Privacy and Security of Automation and Discovery Products. Library Technology Reports, May/June 2016
73. Eisenberg J., Lawthers C. Library Computer and Network Security: Library Security Principles. Infopeople Project. [сайт] http://www.infopeople.org/resources/ security/basics/index.html (мурожаат вақти: 17.11.2017).
74. Fox E., Noha ElSherbiny. Security and Digital Libraries. Virginia Tech, USA, Published: April 4th 2011.
75. Guimarães B. Advanced SQL injection to operating system full control. Black Hat Briefings Europe, Amsterdam. Retrieved on 17th April 2011.
76. Hadow K. Data security for libraries: Prevent problems, don’t detect them. Feliciter, 2009 55(2).
77. Higson Ch, Waltho D. Valuing Information as an Asset, November 2009, [сайт], http://www.eurim.org.uk/activities/ig/voi/voi.php EURIM Value of Information Subgroup (мурожаат вақти: 14.12.2017).
78. Ismail R., Zainab A. N. Information systems security in special and public libraries: an assessment of status. Malaysian Journal of Library & Information Science, 2011, vol. 16, n. 2, pp. 45-62.

79. Kuzma J. European digital libraries: web security vulnerabilities, Library Hi Tech, 2010, Vol. 28 Iss 3 pp. 402 – 413. P
80. Laskowski N. May 2014, Six ways to measure the value of your information assets, [сайт] URL: http://searchcio.techtarget.com/feature/Six-ways-to-measure-the-value-of-your-information-assets (мурожаат вақти: 16710.2018).
81. Moody D., Walsh P. Measuring the Value of Information - An Asset Valuation Approach, [сайт], URL: http://si.deis.unical.it/zumpano/2004-2005/PSI/lezione2/ValueOfInformation.pdf (мурожаат вақти: 15.12.2017).
82. Myongho Y. Balanced Security Controls for 21st Century Libraries, Library & Archival Security, 2011, 24:1, 39-45.
83. Noha Ibrahim Mohamed ElSherbiny. Secure Digital Libraries. Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Master of Science In Computer Science and Applications. Alexandria, Arab Republic of Egypt:
84. Normatov Sh. Fuzzy math model to solving a problem ensuring the security science and educational information. Abstracts of the VI International Scientific Conference “Modern problems of the Applied Mathematics and Information Technology – Al-Khorezmiy 2018”, Tashkent, Uzbekistan, September 13-15, 2018. -P. 65
85. Normatov Sh. System approach to the problem of protection scientific and educational information resources. European Science Review. -Austria, Vienna-2018. № (5-6). -P. 82-85
86. Normatov Sh., Rakhmatullaev M.A. Extended Model of Access Control for the Library Information Systems. International Conference on Information Science and Communications Technologies (ICISCT). 2017. IEEE. – P. 1-6. (31.10.2017 243/3-сон раёсат қарори) DOI: 10.1109/ICISCT.2017.8188584
87. Rakhmatullaev M. Increase of determinacy of information environment for intellectualization of information retrieval. Proceeding of International

conference. WCIS 2014. Eighth World Conference on Intelligent Systems for Industrial Automation. 2014; 329-334.

88. Rakhmatullaev M., Normatov Sh. Analysis of criteria for ensuring information security of scientific and educational resources. “Society. Integration. Education.” Proceedings of the International Scientific Conference, Volume V, May 24th-26th , 2018, Rezekne, Rezekne Academy of Technologies, Latvia. -P. 430-435. DOI: http://dx.doi.org/10.17770/sie2018vol1.3264
89. Rodionova Z. V., Bobrov L. K. Protection of the Information Resources of a Library Based on Analysis of Business Processes. Scientific and Technical Information Processing, 2016, Vol. 43, No. 1, pp. 20–27.
90. Tolone, W., Ahn, G.-J., Pai, T. & Hong, S.-P. (2005). "Access Control in Collaborative Systems." *ACM Computing Surveys* 37(1): 29 - 41.
91. Thompson S. Helping the hacker? Library information, security and social engineering”, Information Technology and Libraries, 2006, Vol. 25 No. 4, pp. 222-5.
92. Yeh Q., Chang, A. Threats and countermeasures for information system security: A cross-industry study. Information & Management, 2007. Vol.44: 480-491.
93. Zhang S. A fuzzy and integrated evaluation in the security of digital library, 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, 2012, pp. 739-742.

ILOVA

Elektron kutubxonalar axborot xavfsizligiga tegishli lug‘at

AXBOROT RESURSI – axborot materialini matn, ovozli yoki tasvir xolidagi ko‘rinishlarining yig‘indisi.

AXBOROT-KUTUBXONA RESURSI – moddiy obyektda matn, ovozli yozuv yoki tasvir tarzida qayd etilgan hamda identifikatsiyalash, saqlash va foydalanishni ta’minlash uchun rekvizitlarga ega bo‘lgan axborot. Bu yerda «identifikatsiyalash uchun rekvizitlar» tushunchasi muhim o‘rin tutadi, chunki mazkur ko‘rsatkichlar asosida hujjatni (identifikatsiyalash) topish mumkin. Rekvizitlar qat’iy qoidalar va kutubxonachilik standartlari asosida qo‘yiladi. Bu an’anaviy hamda elektron, virtual kutubxonalardagi ma’lumotlar qidiruv jarayonini formallashtirishda muhim jihatdir.

AXBOROT XAFSIZLIGI – Ахборотнинг унинг эгасига зарар келтирадиган тасодифан ёки қасддан қилинган таҳдидларга (хавф-хатарларга) чидамлилигининг умумлашган хоссаси.

AXBOROT XAVFSIZLIGINI TA’MINLASH TIZIMI – Ахборот ҳимоясини яратиш, татбиқ этиш, ундан фойдаланиш, доимо назорат қилиш, таҳлиллаш, иш ҳолатида сақлаш ва яхшилашга қаратилган, иш хавф эҳтимоллари ёндашувига асосланган умумий менежмент тизимининг қисми.

ELEKTRON KUTUBXONA – axborot-kutubxona fondining elektron shakli.

AXBOROT ALMASHINUVI (Data communications) – axborotni alfavit-raqamli simvollardan iborat bo‘lgan elektrik impulslar ko‘rinishida yetkazib berishni, aks ettiradi. Ma’lumotlarni uzatish audio va video signallarini uzatishdan farq qiladi.

AVTOMATLASHTIRISH (automation) – jarayonlarni amalga oshirish uchun avtomatlashtirish vositalarini tatbiq etish, inson mehnati unumdorligini oshirish maqsadida bu mehnatning bir qismini EHM orqali bajariladigan tadbirlar

tizimi. Bu ishlar zamonaviy hisoblash texnikasi va ilmiy usullardan foydalangan holda bajariladi.

MUALLIFLIK HUQUQI – ijodiy asar muallifining mazkur asarni boshqalar tomonidan foydalanishini tartibga soluvchi huquqlari majmuyi. Xalqaro muvofiqlashtirishga erishilgan bo‘lsada, bu huquqlar turli mamlakatlarda turlicha. Ularni ikki guruhga ajratish mumkin: iqtisodiy va ahloqiy huquqlar.

MA’LUMOTLAR BAZASINING ADMINISTRATORI (database administrator) – ma’lumotlar bazasi haqida to‘liq axborotga ega bo‘lgan va uni yuritish, foydalanish, rivojlantirishga javobgar lavozimli shaxs (yoki shaxslar guruhi).

SERVER ADMINISTRATORI – web-serverni beto‘xtov ishlashini ta’minlovchi, xatolarni to‘g‘rilovchi, server va ma’lumotlarni himoya qiluvchi mutaxassis. Talab qilinadigan malaka: serverni sozlash va o‘rnatilgan operatsion tizimni bilish.

LOYIHA ADMINISTRATORI – Internet loyihasini, web-sahifa barcha faol elementlarni, web-saytni to‘ldirib borish va nazorat qilish, boshqarish va mualliflik huquqini himoya qilish vazifalarini bajaruvchi mutaxassis.

BIBLIOGRAFIK MA’LUMOTLAR BAZASI – kutubxonada saqlanayotgan kitoblar, jurnallar va boshqa hujjatlar yozuvlaridan iborat bo‘lgan ma’lumotlar bazasi.

MA’LUMOTLAR BAZASI (data base) – ma’lum bir qoidalar asosida tashkil qilingan, umumiy tavsif, saqlash va o‘zgartirish tamoyillari nazarda tutilgan ma’lumotlar majmuyi. Ma’lumotlar bazasiga ma’lumotlar bazasini boshqarish tizimi orqali murojaat qilinadi.

BRAUZER (brouzer) – grafik va matnli axborotlarni ko‘rish va qidirishga mo‘ljallangan dasturiy vosita.

MA’LUMOTLAR XAVFSIZLIGI (data cesurity) – ma’lumot va dasturlarni buzish, o‘zgartirish yoki o‘chirib tashlash maqsadida ruxsatsiz kirishdan himoya qilish. Ma’lumotlar xavfsizligi apparat, dasturiy, kriptografik usullar, himoya vositalari va kompleks tashkiliy tadbirlar o‘tkazish orqali amalga oshiriladi.

VIRTUAL REALLIK - multimediya vositasi yordamida (tovush, rang, tomosha effekti) reallik illyuziyasini hosil qilish.

VOIS – butun jahon intellektual mulk tashkiloti.

DOMEN – Internetdagi tarmoq yoki kompyuter nomi, @ belgisidan o‘ngda turuvchi belgilar yig‘indisi. Nomlarning domenli tizimi kompyuterning harflardan iborat nomini raqamli adresga aylantirish imkonini beradi.

KIRISH (access) – magnitli tashuvchilarda uzoq muddatli saqlanayotgan ma’lumotlarni qidirib topish, olish va bu ma’lumotlarni elektron xotiraga joylashtirish. Kompyuterlar elektron xotiraga joylashgan ma’lumotlar ustida operatsiyalar bajara oladi.

KO‘CHIRIB O‘TKAZISH – maxsus ma’lumotlarni o‘qib olish jarayoni. Kutubxona tizimlaridagi turli manbalardan mashina o‘qiy oladigan katalog yozuvlarini katalogga ko‘chirib o‘tkazish va uni doimo yangilash.

AXBOROT-KUTUBXONA INFRASTRUKTURASI (AKI) foydalanuvchilarni talablarini bajarishda respublika axborot-kutubxona muassasalarini (AKM) yagona standartlar asosida ma’lumotlarni almashish, tavsiflash, axborotni saqlash, uzatish maqsadida yagona tarmoqqa birlashuvi.

IDENTIFIKATOR (identifier) – leksik birlik, til elementi nomi sifatida foydalaniladi; ma’lumotga beriladigan nom; lotin harflari va raqamlaridan iborat bo‘lib, harfdan boshlanadi.

INTRANET (intranet) – Internet tarmog‘i mahsulotlari va texnologiyalaridan foydalanuvchi va korporativ axborot resurslariga o‘z foydalanuvchilarining kirishini ta’minlovchi taqsimlangan (vedemostvenniy) hisoblash tarmog‘i.

ILMIY-TA’LIMIY AXBOROT RESURSLARI – litsenziyalangan hamda taqrizdan o‘tgan ilmiy-ta’limiy axborotlar (jurnallar, maqola, kitoblar, multimedia va boshqalar) axborot resurslardir. Ilmiy-ta’limiy axborot resurslari muhim qiymatga ega bo‘lgan intellektual manbadir. Odatda har bir hujjat ma’lumotlar bazasi, jurnallar, tegishli to‘plamlarga kiritilishidan avval yetakchi olimlar, mutaxassislar tomonidan saralashdan o‘tadi. Bu hujjatlar tizimlashtiriladi, kataloglashtiriladi va ilmiy-ta’limiy

axborotlarning ma’lumot bazalariga joylashtiriladi. Asosiy foydalanuvchilari ilmiy xodimlar, o‘qituvchilar, magistr va talabalardir.

KATALOG – kutubxona fondidagi barcha hujjatlar ro‘yxati. Avtomatlashtirilgan tizimda bibliografik ma’lumotlar bazasini tashkil qiladi.

KONSORSIUM – bu muayyan maqsadalrni amalga oshirish uchun tashkilotlarni birlashishidir.

KUTUBXONALAR KONSORSIUMI – bu kutubxona assotsiatsiyalari va axborot markazlari axborot resurslarini, jumladan, elektron resurslarni birgalikda xarid qilish va ulardan foydalanish, Internet navigatsiyalar, ma’lumotlar bazasidan foydalanishni o‘rgatish bo‘yicha birgalikdagi sa’y-harakatlarni amalga oshirish uchun birlashuvidir.

KATALOGLASHTIRISH (catalogization) – ma’lumotlarni katalogga kiritish; hisoblash texnikasida fayl haqidagi yoki kutubxona haqidagi axborotni kiritish. Kutubxona katalogini yaratish jarayoni. Odatda integral kutubxona tizimi moduli hisoblanadi.

KONVERTATSIYA (translation) – bir xil tipdagi ma’lumotlarni boshqa tipga o‘tkazish. Bunda quyidagi operatsiyalar nazarda tutiladi: (ma’lumotlarni tahrir qilish, belgilarni o‘chirish, punktuatsiya, belgilar va qatorlar inversiyasiga ishlov berish), ma’lumotlarni shakl o‘zgartirish (formatlarning adres ko‘rsatkichlarini, parametrlarini, metkalarini perekodirovka qilish va o‘zgartirish), ma’lumotlarni qayta tashkil qilish (dekompozitsiya, kompanovka, yangi elementlar hosil qilish), fayllarni qayta tashkil qilish.

KOMPYUTERLASHTIRISH (computerization) – kompyuter mahsulotlari va xizmatlari industriyasining rivojlanish jarayoni va ulardan jamiyatda keng foydalanish. Korxonalar, muassasalar va o‘quv yurtlarini hisoblash texnikasi bilan ta’minlash va aholi umumta’lim darajasini kompyuterlarni qo‘llash orqali yuksaltirish.

KOMMUNIKATIV FORMAT, ALMASHUV FORMATI (exchange format) – turli tashkilotlarning avtomatlashtirilgan tizimlari o‘rtasida ma’lumot

almashishni ta’minlaydigan mashina o‘qiy oladigan format (MARC formatlar, UNIMARC, USMARC).

KOMMUNIKATSION ALOQA (communication link) – ikki qurilmaning elektrik va mantiqiy ulanishi. LVSda kommunikatsion aloqa bu jo‘natuvchidan qabul qiluvchigacha bosib o‘tgan yo‘li.

KORPORATIV KUTUBXONA-AXBOROT TARMOG‘I (YOKI TIZIMI) – bu ma’muriy va xo‘jalik yuritish jihatdan mustaqil bo‘lgan bir qator ARMlarning (kutubxonalar, axborot markazlari) ixtiyoriylik asosida tashkil topgan birlashmasi bo‘lib, ular funksional masalalarni, xususan, foydalanuvchilarga kutubxona-axborot xizmati ko‘rsatishni takomillashtirish va shunga o‘xshash bir qator masalalarni hal qiladilar. Bunda birinchi navbatda, kutubxona-axborot resurslarini yaratish va ulardan birgalikda foydalanish, jumladan, bosma nashrlarni hamda kichik tirajdagi adabiyotlarni korporativ kataloglashtirish masalalari yechiladi. Bunday tipdagi kooperatsiyada korporatsiya a’zolari orasida hech qanday moliyaviy munosabatlar bo‘lmaydi.

KONTENT-MENEDJER (KONTENT-OPERATOR) – kiruvchi axborotni tahrirlashni tashkil etadigan, hamda axborot to‘ldirilishini kuzatuvchi mutaxassis bo‘lib, savollarga javob beradi, foydalanuvchilarga maslahatlar beradi. Malaka – dasturlash tillarini bilishi, ma’lumotlar bazasi tuzilishini bilish talab etildi.

KORREKTOR – butun matnli materiallarni tekshiruvchi mutaxassis, bunga grafik obyektlar izohi, tugmalar, baner ham kiradi. Talab etilayotgan malaka: bozor xususiyatini bilish, Internetdagi axborot-qidiruv tilini bilish, Internetda reklama tashuvchilar qoidasini bilish talab etiladi.

QAYTA YOZILMAYDIGAN KOMPAKT DISK (CD-ROM COMPACT DISK READ ONLI MEMORY) – matnli, grafik, tovushli va turli axborotlarni saqlashga mo‘ljallangan optik disk. U taqsimlanayotgan dasturiy ta’minot, ma’lumotnoma materiallari, bibliografik ma’lumotlar bazasini saqlash vositasi hisoblanadi.

LOKAL HISOBLASH TARMOG‘I (LOCAL AREANETWORK) – uzatish kanallari (optik tolali kabel va boshqalar) orqali o‘zaro bog‘langan kompyuterlar majmui, kompyuter orqali boshqariladigan qurilmalar, bir yoki bir necha obyekt (binolar) doirasidagi axborot resurslaridan birgalikda foydalanish maqsadida birlashtiriladi.

LITSENZIYA – shartnoma huquqi bilan boshqariladigan ma’lum bir faoliyat olib borishga formal huquq beradigan ruxsatnomadir. Litsenziya – elektron mahsulotlar: kompyuter dasturlari, kompyuter o‘yinlari, onlayn filmlar, musiqiy asarlar, ma’lumot bazalaridan foydalanish huquqini berishni boshqarishda qo‘llaniladi. Bu shuni anglatadiki, kutubxonaga kelgan ko‘pgina elektron materiallar litsenziya shartnomalari bilan boshqariladi.

MENYU (MENU) – bir yoki bir necha tugmachasi bosish orqali, variantlardan birini tanlash imkonini beruvchi ro‘yxat tasviri.

MULTIMEDIA (multimedia) – tizimni matnli, grafik, tasviriy, ovozli ma’lumotlar bilan ishlash hajmi. Matn, ovozli, grafik, video kabi turli xil axborotni shakllantirish, saqlash va ijro etish imkoniyatiga ega kompyuter texnologiyalari.

JAHON AXBOROT RESURSLARI – dunyoning yetakchi nashriyotlarining axborot resurslaridir. Bu axborot qidiruv tizimiga ega jamiyat tomonidan tan olingan tizimlashtirilgan va tuzilmalashgan ilmiy-ta’limiy resurslarning ma’lumot bazalaridir. Jahon axborot resurslari ro‘yxatiga yuqori impakt faktorli jurnallar, iqtibos keltirilgan ilmiy monografiyalar, darsliklar, maqolalar kiritilgan.

ERKIN FOYDALANISH (Open Access) – kitobxonlarga Internet orqali bepul foydalanish, o‘qish, yuklab olish, nusxa ko‘chirish, tarqatish va chop etish, qidirish, indekslash, ma’lumot sifatida uzatish yoki qonun doirasida boshqa maqsadlarda moliyaviy va texnik to‘siqlarsiz muallifga iqtibos keltirgan holda foydalanish. «Erkin foydalanish»dagi jurnallar doimo bepul bo‘lmasligi mumkin. Ular muallif gonorarlari to‘lash uchun, jurnalni o‘z vazifalarini bajarish uchun qo‘llash maqsadida narx ham o‘rnatishlari mumkin, lekin rerkin foydalanishda bo‘lib,

kitobxonlar, foydalanuvchilar uchun ochiqdir. Foydalanish uchun hech qanday to‘lov talab etilmaydigan jurnallarni ba’zan «gibrid kirish» jurnallari deb ham ataydilar.

QIDIRISH SHAKLI – hujjat mazmuni ta’rifi, axborot-qidiruv tili qoidasi bo‘yicha qilingan, qidiruvni amalga oshirish uchun uning mazmuni va ko‘rinishining muhim belgilari aks etadigan hujjat.

PORTAL – 1) Internetdagi boshqa resurslarga murojaatning boshlang‘ich nuqtasini o‘zida aks ettirgan ko‘p xizmatli sayt [43 (439 b.)].2) ko‘plab turli kichik o‘lchamdagi tematik bo‘limlarni o‘z ichiga olgan yoki ko‘p bo‘lmagan miqdordagi mustaqil loyihalarni o‘z ichiga olgan yetarli katta virtual massiv axborotlari.

AMALIY DASTURIY TA’MINOT (Application software) – kompyuter foydalanuvchisi uchun aniq vazifani bajaradigan dastur yoki tanlov dasturi. Matnlarga ishlov beruvchi va elektron jadvallar bilan ishlovchi dastur – amaliy dasturiy ta’minot misollari.

PLAGIAT (plagiarism) – o‘zga muallif asarini atayin havolalarsiz, muallifga iqtiboslikni ko‘rsatmasdan shaxsiy asar sifatida ko‘rsatishga urinish. Plagiat – bu nusxa ko‘chirishning bir turi bo‘lib, mualliflik huquqini buzilishi hisoblanadi. O‘z faoliyatida (ilmiy maqola, kitob, hisobot, ma’ruzalarni yozishda) axborot resurslaridan foydalanish jarayonida mualliflik huquqlariga qat’iy rioya qilish lozim. Hujjatni yaratishda foydalanilgan manbalarga albatta havolalar keltirish lozim. Plagiarizmni tushunish yangi axborot resurslarini, ayniqsa ilmiy-axborot resurslarini yaratishda muhim hisoblanadi. Mualliflik huquqlari har bir mamlakatda mualliflik va turdosh huquqlari to‘risidagi tegishli qonunlar bilan muhofaza qilinadi.

PROVAYDER (provider) – tarmoq, axborot, Internet, elektron pochta xizmatlari ta’minotchisi.

PROTOKOL TSR/IP – Internet tarmog‘ida kompyuter tomonidan foydalaniladigan protokol. TCP (Transmission Control Protocol) – uzatishlarni nazorat qilish protokoli – protsessorlar orasidagi aloqani ta’minlashga javobgar. IP (Internet Protocol) – Internet protokoli – kompyuterlar orasidagi aloqalarni ta’minlashga javobgar.

PROTOKOL Z39.50 – ma’lumotlarni uzatishda yuqori darajada ishlaydigan 7 pog‘onalik model va turli xil dasturlar ishlash, foydalanuvchilarga ma’lumotlar bazasidan to‘liq qidirish imkonini beradigan protokol.

INTERNET PROMOUTERI – Internet loyiha marketingi bilan shug‘ullanadigan mutaxassis, reklama tadbirlari tashkiloti, axborot mahsulotlari bozorini o‘rganish, katalog resurslari va qidiruv tizimlari loyihalarida saytni ro‘yxatdan o‘tkazish, baner almashish tarmog‘ida qatnashish va h.k.

XIZMATCHI FAYL PROTSESSORI (FILE SERVER) – tarmoqdagi boshqa kompyuterlarga xizmat ko‘rsatuvchi, katta hajmdagi ma’lumotlarni saqlash qobiliyatiga ega kompyuter.

TEZAURUS – axborot qidiruvini samarali olib borish uchun turli darajadagi tushunchalar orasida aloqa bog‘lovchi tizimlashtirilgan lug‘at.

SHLYUZ (GATEWAY) –turli ikki tarmoqni birlashtiruvchi qurilma. Shlyuz o‘z protsessoriga va xotirasiga ega, u kanallar sig‘imini, protokolni o‘zgartira oladi.

SHTRIXLI KODLASHTIRISH (BARCODE) – alfavit-raqamli va raqamli ma’lumotlarni turli qalinlikdagi vertikal chiziqlar vositasida kodlashtirish. Maxsus qurilma yordamida o‘qiladi, aniqlanadi va kompyuter yordamida ishlov beriladi. Shtrixli kodlash kutubxonalarda berilayotgan adabiyotlarni hisobga olishda ishlatiladi.

FTP (FILE TRANSFER PROTOCOL) – (fayllarni uzatuvchi protokol) ixtiyoriy faylni uzeldagi mashinaga ko‘chirib o‘tkazuvchi ish quroli. Modem orqali fayldan nusxa olib o‘z kompyuteringizga yozib qo‘yishingiz mumkin.

ISBN (INTERNATIONAL STANDARD BOOK NUMBER) – kitob nashrlarining xalqaro standarti.

ISSN (INTERNATIONAL STANDARD SERIAL NUMBER) – davriy nashrlar xalqaro standart nomeri

OPAC (ONLINE PUBLIC ACCESS CATALOG) – jamoatchilik tomonidan foydalaniladigan tezkor katalog. Elektron kutubxona katalogidagi qidiruv tizimi.

ON-LINE – real vaqt rejimida kirish (hozir va shu yerda).

UMUMIY LITSENZIYA – individual muhokamalarsiz oldindan kelishilgan shartlar asosida ko‘p sondagi asarlardan foydalanishga ruxsat beradi. Mualliflik huquqi ma’nosida bunday litsenziya bir guruhga kiruvchi asarlar uchun beriladi. Shu yo‘l bilan bir qancha asarlardan foydalanish ruxsatini olish soddalashadi, chunki bir guruhga kiruvchi barcha asarlar uchun bitta kelishuv imzolanadi. Odatda minglab, hattoki millionlab himoyalangan asarlardan foydalanishni jamoaviy boshqaruvchi tashkilotlar tomonidan bunday litsenziya beriladi.

URL (Uniform Resouree locator) – bu WWW dagi adres, resursni ko‘rsatuvchi birlik ko‘rsatkich Internet orqali kirish mumkin bo‘lgan fayl yoki resurs nomi. O‘z ichiga protokol nomi, uzel nomi va faylgacha bo‘lgan yo‘lni oladi. Http, ftp, gopher, wais – tipik protokollar hisoblanadi.