УДК 004.056.5

RISK MENEJMENTDA XATARLARNI BAHOLASH VA BOSHQARISH USULLARI TAHLILI

Islamova Dildora Sultanovna
Osiyo texnologiyalar universiteti katta o‘qituvchi
Тел:+998883840307.
E-mail: islamovadildora2@gmail.com
ORCID ID: 0009-0005-7590-8915

Annontatsiya. Ushbu maqolada axborot xavfsizligi, ishlab chiqarish jarayonlari va boshqa sohalarda uchraydigan xavf-xatarlarni kamaytirish bo‘yicha risk-menejment yondashuvlarining qo‘llanish imkoniyatlari tahlil etilgan. Tadqiqotda mavjud ilmiy manbalar, xorijiy tajribalar asosida xatarlarni baholash usullarining afzalliklari va kamchiliklari ko‘rib chiqilgan bo‘lib, xatarlarni boshqarishning zamonaviy metodlari sifatida matematik modellashtirish, noaniqlik sharoitida qaror qabul qilish nazariyasi, ehtimollik yondashuvi va lingvistik baholash usullarining qo‘llanishi bo‘yicha tahlillar yoritilgan.

Kalit so‘zlar: risk, risk tahlili, risklarni baholash, nigativ holatlar, xavf darajasi, QQQ, monitoring.

Аннотация. В данной статье анализируются возможности применения подходов к управлению рисками для снижения рисков, возникающих в сфере информационной безопасности, производственных процессов и других отраслях. В исследовании рассматриваются достоинства и недостатки методов оценки рисков на основе имеющихся научных источников, зарубежного опыта, освещается анализ применения математического моделирования как современных методов управления рисками, теории принятия решений в условиях неопределенности, вероятностного подхода и методов лингвистической оценки.

Ключевые слова: риск, анализ рисков, оценка рисков, негативные состояния, уровень риска, QQQ, мониторинг.

Abstract. This article analyzes the possibilities of applying risk management approaches to reduce risks encountered in information security, production processes, and other areas. The study examined the advantages and disadvantages of existing scientific sources, methods for assessing risks based on foreign experiments, and covered mathematical modeling as modern methods of risk management, analysis on the theory of decision making in conditions of uncertainty, a probabilistic approach and the application of linguistic assessment methods.

Keywords: risk, risk Analysis, Risk Assessment, positive cases, risk level, QQQ, monitoring.

Kirish.

Korxona yoki tashkilotning xavsizligini ta’minlash tushinchasi- undagi ma’lumotlar ombori va tarmog‘iga bo‘lgan tahdidlar spektridan himoyalash va uning ko‘p yillik biznes rejalarini oshkor qilmasdan bozorda o‘z o‘rnini saqlab qolishdan iborat bo‘lmoqda.

Axborot va uni himoya qiluvchi vositalar - axborot tizimlari va tarmoq infratuzilmasi, biznesning bebaho aktivlari bo‘lib hisoblanadi. Axborot xavfsizligini aniqlash, ta’minlash, saqlab turish va yaxshilash tashkilotning raqobatbardoshliligi, qadrliligi, daromadliligi, qonun hujjatlariga muvofiqligini va ishbilarmonlik obro‘sini ta’minlashda katta ahamiyatga ega.

Tashkilotlar, ularning axborot tizimlari va tarmoqlari xavfsizlikning turli kompyuter firibgarligi, shpionlik, zararkunandalik, vandalizm, yong‘inlar yoki suv toshqinlari kabi tahdidlar bilan ko‘proq to‘qnashmoqdalar. Zararning bunday “kompyuter viruslari”, “kompyuterni buzib kirish” va “xizmat ko‘rsatishdan bosh tortish” turidagi hujumlar manbalari keng tarqalmoqda, agressivroq bo‘lib bormoqda va ko‘proq mahorat bilan shakllanmoqda. Axborot xavfsizligi biznesning jamoat va xususiy sektorida, shuningdek kritik infratuzilmalarni muhofaza qilishda muhim hisoblanmoqda.

Ko‘pgina axborot tizimlarini loyihalashtirishda xavfsizlik masalalari e’tiborga olinmas edi. Texnik vositalar bilan erishilishi mumkin bo‘lgan xavfsizlik darajasi bir qator cheklashlarga ega bo‘lib, tegishli boshqaruv vositalari va protseduralar bilan ta’minlanishi kerak. Axborot xavfsizligini boshqarish bo‘yicha zarur tadbirlarni tanlash, puxtalik bilan rejalashtirish va detallashtirishni talab qiladi. Tashkilotda xavfsizlikni nazorat qilish va uni samaradorligini oshirishning birinchi qadamlari esa axborot risklarini to‘g‘ri boshqarish va baholay olish natijalariga ko‘ra choralarni ishlab chiqish hisoblanadi.

Axborot xavfsizligi risklarini aniqlash – bu tizimning zaif joylari, tahdidlar va ushbu tahdidlarning imkoniyati hamda oqibatlarini baholash jarayonidir. Bu jarayonda tashkilotdagi axborot resurslariga salbiy ta’sir ko‘rsatishi mumkin bo‘lgan xatarlar va zaifliklar aniqlanadi va ularga tegishli xavflar baholanadi.

“Risk” atamasining turli faoliyat sohalarida qo‘llanilishi va predmet sohasining ontologik modelini yaratish risklarni baholash va boshqarish vazifalarining asosiy xususiyatlarini aniqlash imkonini berdi.

Risk-menejment – bu komplekslashtirilgan vazifa bo‘lib, quyidagilarni o‘z ichiga oladi:

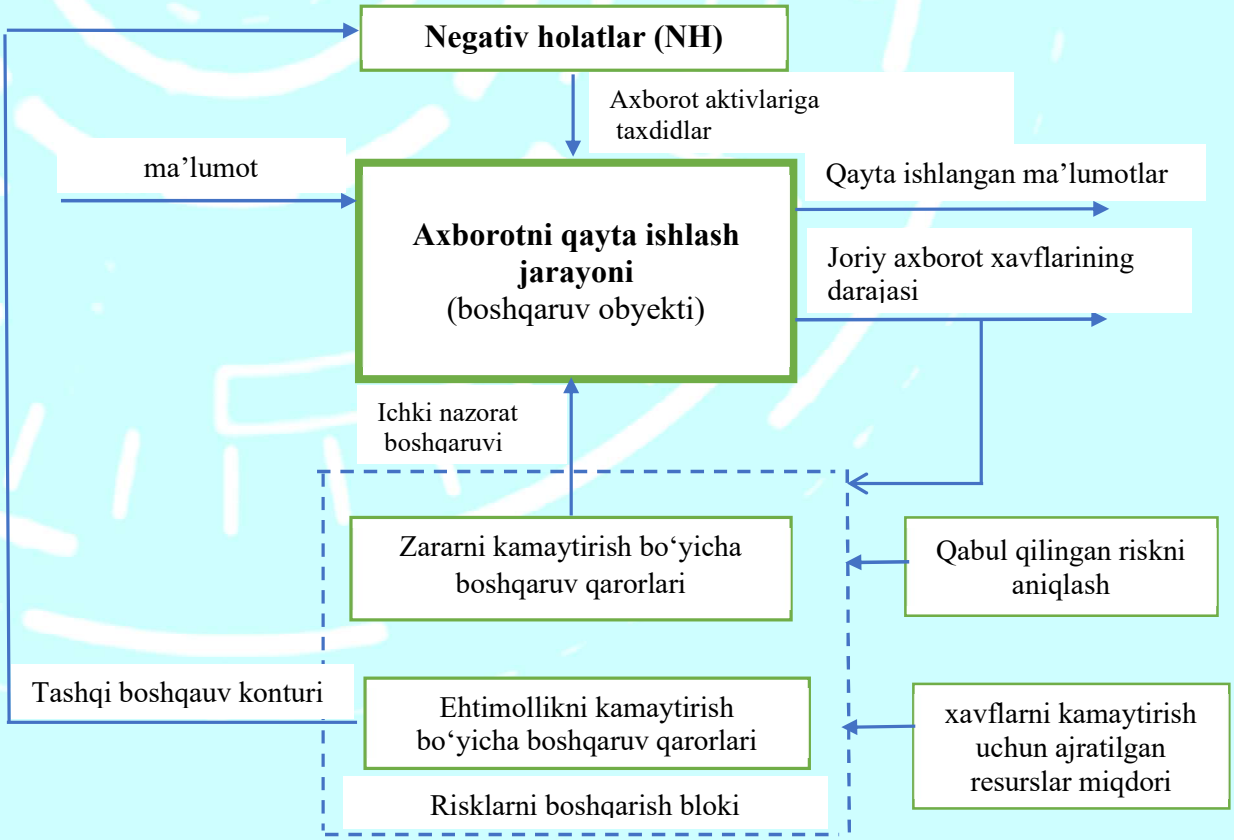
1. Qabul qilinadigan xavf darajasi bo‘yicha muvofiqlashtirilgan fikrni ishlab chiqish: Bu jarayonda turli manfaatdor tomonlarning xavfni qanday qabul qilishlari va qanday darajada xavfga bardosh berishlari to‘g‘risidagi umumiy nuqtai nazar shakllantiriladi.

ISSN 3030-3907

2. Negativ holatlar (NH) sodir bo‘lishining ehtimoliy imkoniyatlaridan kelib chiqqan holda joriy xavflarni baholash: Bu bosqichda mavjud xavflarning hozirgi holati tahlil qilinadi va ulardan kelib chiqishi mumkin bo‘lgan zararlar baholanadi.

3. Xavf darajasini QQQ (qaror qabul qiluvchilar) tomonidan belgilangan qiymatlargacha tushirish bo‘yicha choralarni sintez qilish va amalga oshirish: Bu jarayonda xavflarni kamaytirish uchun samarali choralar ishlab chiqiladi va amalga oshiriladi.

1-rasmda axborotni qayta ishlash jarayonida yuzaga keladigan xavflarni boshqarishning umumiy sxemasi ko‘rsatilgan. Bu sxema xavflarni aniqlashdan tortib, ularni baholash, monitoring qilish va kamaytirishgacha bo‘lgan jarayonlarni o‘z ichiga oladi. Ushbu sxema turli bosqichlarni qamrab oladi:



1-rasm. Axborot risklarini boshqarish sxemasi

1. *Xavflarni aniqlash* – Axborotni qayta ishlashda potensial xavflarni topish va ularning ehtimoliy oqibatlarini aniqlash.

2. *Xavflarni baholash* – Aniqlangan xavflarning jiddiyligi va ularning yuzaga kelishi ehtimolini baholash.

3. *Xavflarni kamaytirish choralari* – Xavflarning ta’sirini kamaytirish yoki bartaraf etish uchun muvofiq chora-tadbirlarni ishlab chiqish va amalga oshirish.

4. *Monitoring va kuzatish* – Har bir bosqichda xavflarning holatini nazorat qilish va zarurat tug‘ilganda choralarni qayta ko‘rib chiqish.

Bu sxema xavflarni samarali boshqarish va axborotni ishonchli qayta ishlashni ta’minlash uchun qo‘llaniladi.

ISSN 3030-3907

Mavzuga oid adabiyotlarning tahlili.

Risk-menejmentning ayrim masalalari turli ilmiy ishlarda turli xil ilmiy usul va metodlar yordamida o‘rganilgan va yoritilgan.

Jumladan D.S.Nefedyevning “Sanoat korxonasi risklarini boshqarish tamoyillari va vositalari” mavzusidagi izlanishlarida sanoat korxonasiga xos bo‘lgan xavflarni boshqarish tamoyillari ro‘yxati va ularning mazmuni belgilab berilgan. Unda integratsiya, uzluksiz faoliyat yuritish, axborotning yetarliligi va boshqalar kabi xususiyatlar o‘rganilgan. Shuningdek, muallif tomonidan risklarni boshqarish elementlari uchta tarkibiy guruhga ajratilgan mantiqiy sxema taklif etilgan:

- analitik (xavflarni identifikatsiya qilish, o‘lchash va baholash);
- axborotli (normativ-metodik baza, monitoring va tahlil);
- amaliy (xavflarni boshqarishga oid tadbirlar) chora-tadbirlari ishlab chiqilgan.

“Axborot tizimi aktivlari xavfini baholashning lingvistik modelini ishlab chiqish” nomli ilmiy maqolada esa mualliflar: V. O. Shaporin, P. M. Tishin, R. O. Shaporin, N. B. Kopitchuklar tomonidan axborot aktivlari xavflarini Coras metodologiyasiga asoslangan holda lingvistik baholash usuli taklif qilingan. Unga ko‘ra xavfsizlik risklarini lingvistik o‘zgaruvchilar va noaniq bilimlar bazasini o‘z ichiga olgan noaniq ierarxik model qurilgan.

I.V. Anikinning “Korporativ axborot tizimlarida axborot xavfsizligi risklarini baholash va boshqarish usullari” nomli monografiyasida korporativ axborot tarmoqlarida (KAT) axborot xavfsizligi xavflarini baholash va boshqarishga asoslangan bo‘lib, muallif tomonidan nazariy-to‘plam yondashuvdan foydalangan holda KAT modeli taklif qilingan. U quyidagi elementlar majmuasini o‘z ichiga oladi:

- axborot aktivlari komponenti;
- texnik ta’minot komponenti;
- IT-xizmatlar komponenti;
- KATning mantiqiy tuzilishi;
- axborot ta’minotidan foydalanish modeli;
- IT-xizmatlarni taqdim etish modeli.

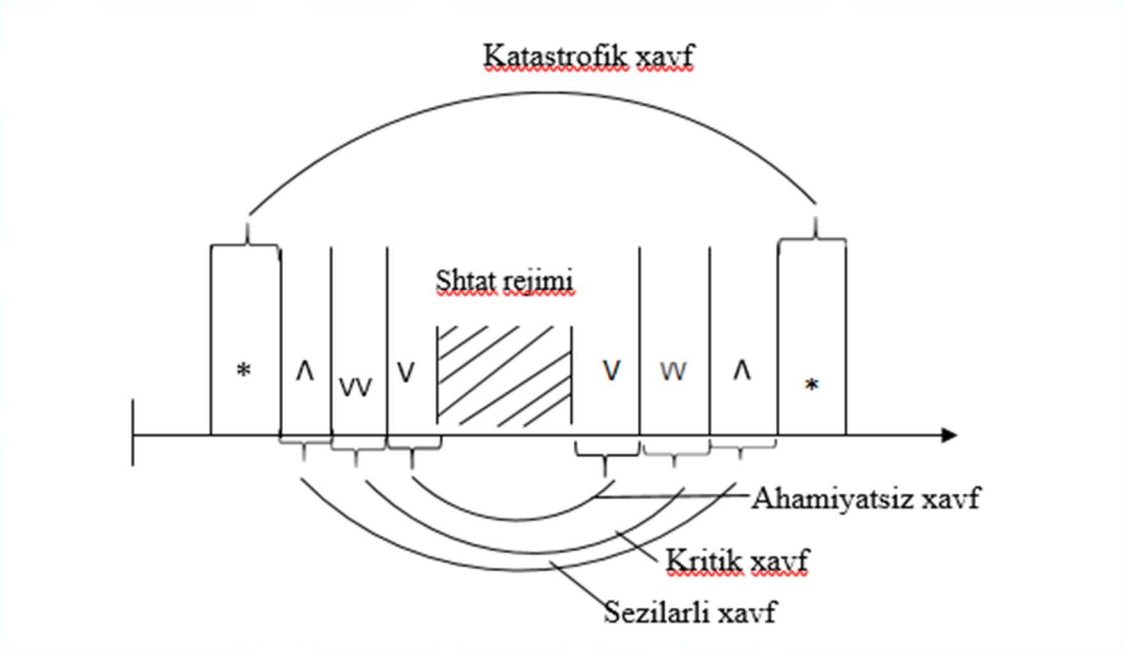
Shu bilan birga, KATning mantiqiy tuzilishi va uning komponentlari Graf modeli ko‘rinishida formallashtirilgan.

Bundan tashqari, muallif tomonidan noaniq to‘plamlar nazariyasiga asoslangan axborot xavfsizligi xavflarini noaniq miqdoriy baholash usullari ishlab chiqilgan. Biroq muallif taklif etgan metodikalarda aktivlarning tashkilot faoliyatining yakuniy natijasiga ta’siri hisobga olinmagan.

“Murakkab texnik tizimlarning ishdan chiqishi xavfi” nomli N.K.Yurkovning ilmiy tadqiqotida esa murakkab texnik tizimlar ishdan chiqishi

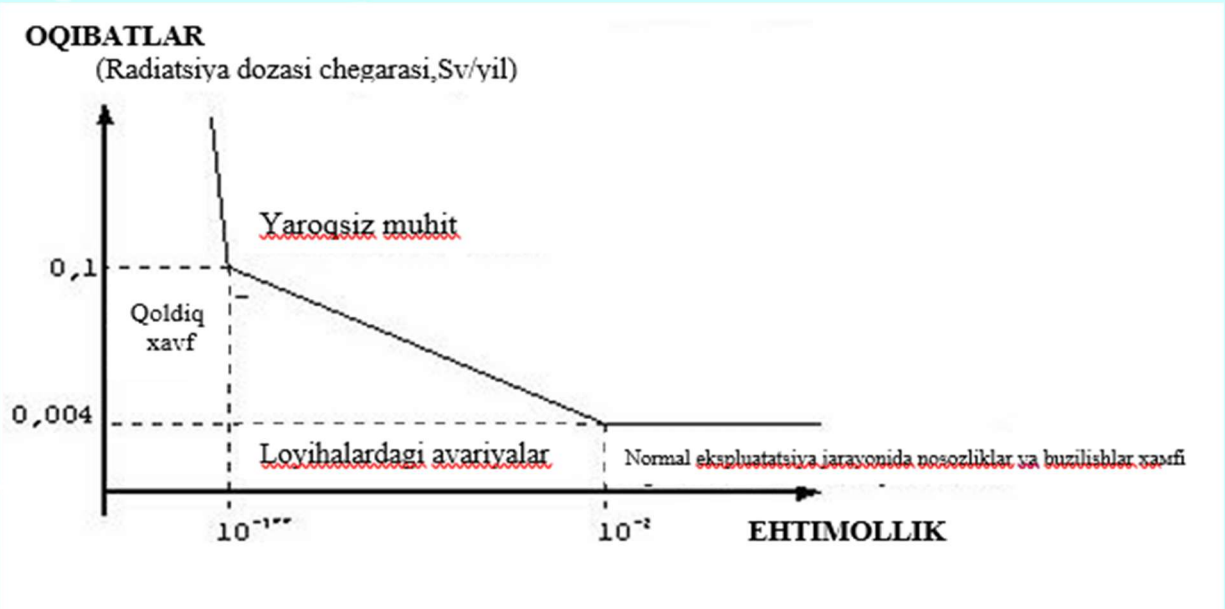
ISSN 3030-3907

bilan bog‘liq xavflar ko‘rib chiqilib, riskli vaziyatlarning xususiyatlari kiritilgan: ahamiyatsiz xavf (tizimning nostandart holatda ishlashiga mos kelishi), sezilarli xavf (tanqidiy holatga mos kelishi), kritik xavf (favqulodda vaziyatga mos kelishi) va katastrofik xavf (avariya holatiga mos kelishi) larning bartaraf etish usullari tadqiq etilgan (2-rasm).



2-Rasm. Xavfli vaziyatlarning mumkin bo‘lgan holatlari uchun ichma-ich joylashgan intervallar sxemasi.

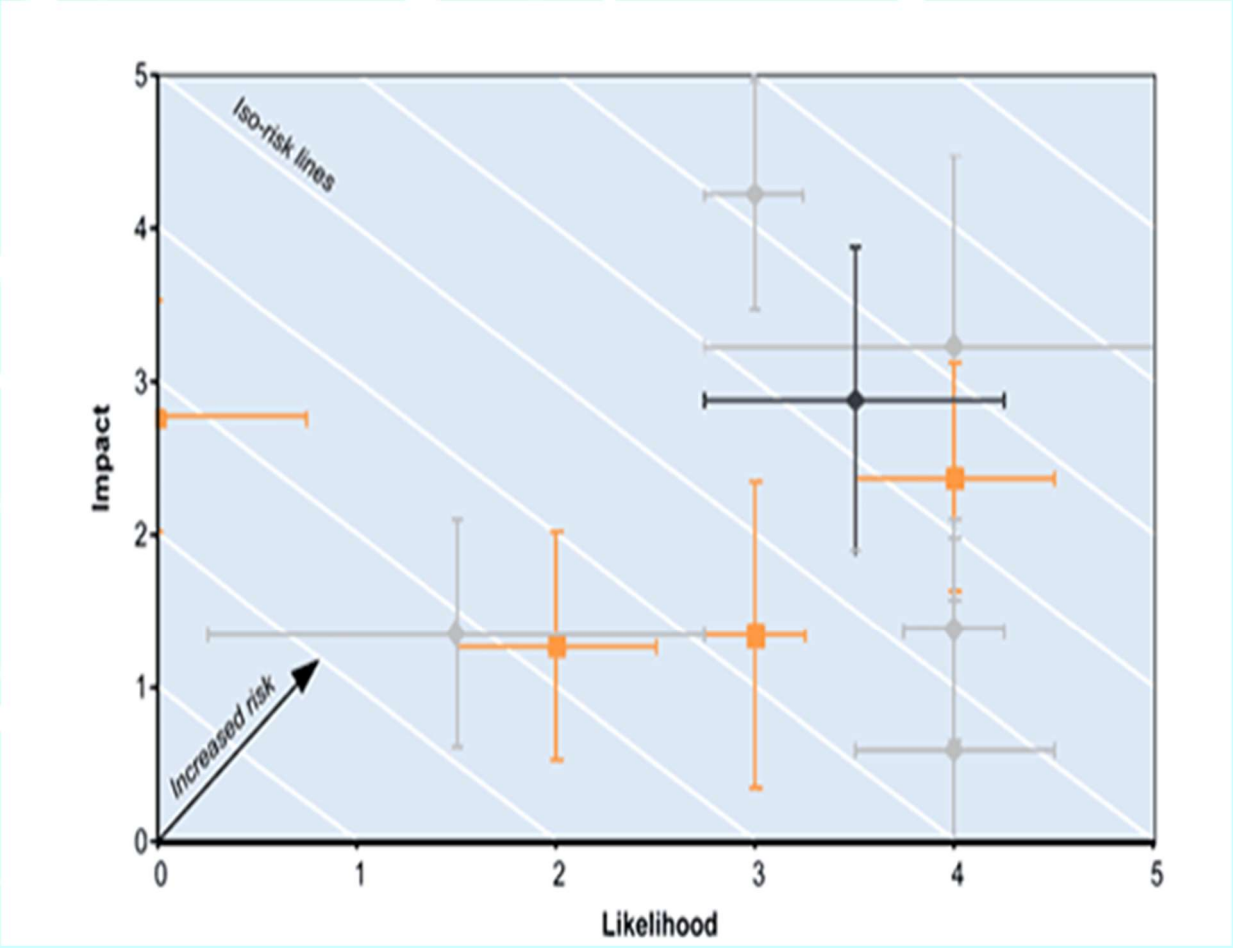
Qator risklarni baholash metodikalarida: texnik, axborot, ekologik yo‘nalishlarda salbiy hodisaning yuzaga kelish ehtimoli bilan uning oqibatlari darajasi o‘rtasidagi bog‘liqlikni grafik tarzda tasvirlashga ifodalashga urinishlar qilingan. Bunda, masalan, Farmer egri chizig‘iga o‘xshash egri chiziqlardan foydalanilgan (3-rasm).



3-rasm. Fermer egri chizig‘i.

ISSN 3030-3907

Kanada metodologiyasida xavflar va xatarlarni umumiy baholash doirasida siyosiy, iqtisodiy, ijtimoiy hamda sanoat xavfsizligi masalalari ko‘rib chiqilgan bo‘lib, xatar miqdorini aniqlashda miqdoriy ko‘rsatkichlar (moliyaviy zarar, vayron bo‘lish maydoni, vaqt va hokazo) baholash shkalasi qiymatlariga o‘tkaziladi. Biroq, og‘zaki (verbal) shaklda ifodalangan ko‘rsatkichlar inobatga olinmaydi. Natija esa ma’lum ehtimollik va ta’sir diapazoni ko‘rinishida ifodalanadi (4-rasm).



4- rasm. Risk diagrammasi.

Tadqiqot metodologiyasi. Risklarni boshqarish jarayoni quyidagi o‘ziga xos xususiyatlarga ega bo‘lib, bu jarayonning tuzilmasi kam yaqqol shakllangan va obektiv hamda subektiv noaniqliklarni qamrab oladi:

– *“Risk” tushunchasining noaniqligi:* Xavfning ko‘plab turlari va namoyon bo‘lish shakllari mavjud bo‘lib, ularning salbiy oqibatlarini bartaraf etish uchun turli usullar mavjud. Turli vaziyatlarda va turli sohalarda «xavf» tushunchasi har xil talqin qilinishi mumkin. Bu esa sohaning asosiy konseptlari o‘rtasida aniq bog‘liqlik yo‘qligiga olib keladi.

– *Axborotning to‘liq emasligi:* Axborot aktivlariga bo‘lgan tahdidlar to‘g‘risidagi statistik ma’lumotlarning yetishmasligi obektiv noaniqliklarni yuzaga keltiradi. Bu xavflarni baholash va ularni boshqarish jarayonida qiyinchiliklar keltirib chiqaradi.

ISSN 3030-3907

– *Parametrlarning aniq emasligi:* Xavflarni baholash va boshqaruv qarorlarini qabul qilishda ko‘plab parametrlar aniq (sonli) emas, balki og‘zaki shaklda ifodalanadi. Bu esa masalani formallashtirishni qiyinlashtiradi va aniq bir uslubni qo‘llashni cheklaydi.

Shu sababli xavflarni baholashda multidissiplinar yondashuvdan foydalanish talab etiladi.

Xavflarni baholash vazifasi ko‘p meyorlidir. Masalan, aktivlarning qiymatini va zarar ko‘rsatkichlarini baholashda quyidagi mezonlar qo‘llaniladi:

- Tashkilotning reputatsiyasiga zarar,
- Hodimlarning xavfsizligi,
- Moliyaviy yo‘qotishlar,
- Tashkilotning normal ishlash imkoniyatining yo‘qolishi,
- Huquqni muhofaza qilish organlari bilan muammolar va boshqalar.

Bu mezonlarni yagona o‘lchov shkalasiga keltirish zarur bo‘ladi.

Xavflarni baholash va boshqarish jarayonining yana bir o‘ziga xosligi bu jarayonda ekspertlarning subektivligidir. Har qanday baholashda olinadigan xavf ko‘rsatkichlari nisbiy bo‘ladi va bu ko‘rsatkichni qaror qabul qiluvchilarning (QQQ) qabul qilinadigan xavf darajasi bilan taqqoslash kerak bo‘ladi.

Axborot texnologiyalari va axborot xavfsizligi sohasidagi xavf-menejment tizimining o‘ziga xos xususiyati shundaki, ushbu tizim yordamida hal qilinadigan masalalar qanchalik dolzarb bo‘lmasin, xavf-menejment tizimi mustaqil ravishda mavjud bo‘la olmaydi va uni korxonaning umumiy boshqaruv tizimiga integratsiya qilish zarur.

Tahlil va natijalar. Axborot xatarlarini baholash va boshqarishga doir asosiy yondashuvlar tahlili shuni ko‘rsatdiki, risklarni boshqarish kompleks muammo bo‘lib, u bir qator turli faoliyat yo‘nalishlarini o‘z ichiga oladi: qabul qilinadigan xatar darajasini aniqlash, joriy (aktual) xatarlarni baholash hamda xatarlarni “qayta ishlash” (mitigatsiya) jarayonlari.

Rossiyalik va xorijiy olimlarning, jumladan, so‘nggi yillarda amalga oshirilgan dissertatsion tadqiqotlar hamda risk-menejment standartlari tahlili shuni ko‘rsatdiki, xatarlarni o‘rganish va ularni baholash usullariga bag‘ishlangan ko‘plab ilmiy ishlarga qaramay, qabul qilinadigan va joriy xatarlarning miqdoriy kattaligini baholashning, shuningdek, joriy xatarlarni qaror qabul qiluvchi shaxs uchun maqbul darajagacha kamaytirish bo‘yicha boshqaruv qarorlarini izlashning formalashtirilgan metodikalari deyarli mavjud emas. Bunda, ayniqsa, ekspert baholari jarayonida yuzaga keladigan sub’ektiv noaniqlikni hisobga oluvchi yondashuvlar yetarli darajada ishlab chiqilmagan.

Xulosa. Shunday qilib, adabiyotlarni tahlil qilish natijasida risk-menejmentning ayrim masalalariga, jumladan, xatarlarni baholashga bag‘ishlangan

ISSN 3030-3907

umumiy-nazariy yo‘nalishdagi ko‘plab ilmiy ishlar mavjudligi aniqlangan. Bunda xatarlarni baholash metodikalarining aksariyatida baholash natijasi yagona son ko‘rinishida ifodalanadi, biroq uni qaror qabul qiluvchi shaxs (QQQ) tomonidan talqin qilish qiyinchilik tug‘diradi. Bundan tashqari, axborot xatarlarini boshqarish sohasidagi ishlanmalarni tahlil qilish shuni ko‘rsatdiki, ularda keltirilgan metodikalar xatarlarni to‘liq va samarali baholash imkonini bermaydi, chunki baholash faqat aktivlar darajasigacha olib boriladi va ularning tashkilot faoliyatiga ta’siri inobatga olinmaydi. Natijada olingan qiymatlar yetarlicha informativ bo‘lmay, QQQ tomonidan boshqaruv qarorlarini asosli tanlash imkonini cheklaydi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI.

1. O’z Dst ISO/IEC 27005:2013 “Axborot texnologiyalari. Xavfsizlik usullari. Axborot xavfsizligi risklarini boshqarish”
2. Нефедьев Д. С. Принципы и инструменты управления рисками промышленного предприятия: автореф. дис. канд. эконом. наук : 08.00.05 / Нефедьев Денис Сергеевич. – Санкт-Петербург, 2015. – 20 с.
3. Шапорин В. О. Разработка лингвистической модели оценки рисков активов информационной системы / В. О. Шапорин, П. М. Тишин, Р. О. Шапорин, Н. Б. Копытчук // Восточно-Европейский журнал передовых технологий. – 2015. – №4/2 (76). – С. 30-35.
4. Аникин И. В. Методы оценки и управления рисками информационной безопасности в корпоративных информационных системах: Монография / И. В. Аникин.– Казань: редакционно-издательский центр «Школа», 2015. – 224 с.
5. Юрков, Н. К. Риски отказов сложных технических систем / Н. К. Юрков // Надежность и качество сложных систем. – 2014. – №1. – С. 18-24.
6. All Hazards Risk Assessment Methodology Guidelines 2012-2013 [Электронный ресурс]. – Режим доступа: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ll hzrds-ssssmnt/index-en.aspx (дата обращения: 01.09.2016г.).
7. Бурков, В.Н. Управление риском: механизмы взаимного и смешанного страхования / В.Ы. Бурков, А.Ю. Заложнев, Д.А. Новиков. // Автоматика и телемеханика. - 2001. - № 10. - С. I 25 - 131.
8. Современные средства управления информационными рисками.-March 2012.Ukrainian Information Security Research Journal 14(1 (54)).DOI:10.18372/2410-7840.14.2054
9. Филатов, А. А. Управление информационными рисками в организации / А. А. Филатов. — Текст : непосредственный // Молодой ученый. — 2020. — № 21 (311). — С. 199-202. — URL: https://moluch.ru/archive/311/70311/.

ISSN 3030-3907

10. Исламова, Д. С. (2024). Управление информационными рисками и «уровень зрелости» корпоративных систем. Экономика и социум, (5-1 (120)), 1983-1988.

11. Irgasheva, D. (2021, November). Indicators of Efficiency of Synthesis of Access Control Systems. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.

ISSN 3030-3907