УДК 004.056.5

XAVFSIZLIK RISKLARINI KAMAYTIRISH UCHUN OPTIMAL TAKTIKANI ANIQLASHDA BOSHQARUV QARORLARINI ISHLAB CHIQISH METODIKASI

ISLAMOVA DILDORA SULTANOVNA

Osiyo texnologiyalar universiteti katta o'qituvchisi

Тел:+998883840307. E-mail: islamovadildora2@gmail.com

Annotatsiya: *Risklarni tahlil qilish, tashkilot xavfsizligini oldini olish chora-tadbirlaridan biri bo'lib, aktivlarning kritikligiga, ma'lum zaifliklarning va tashkilotga taalluqli bo'lgan oldingi insidentlarning tarqalganligiga bog'liq ravishda, turlicha detallashtirish darajasi bilan amalga oshiriladi. Risklarni tahlil qilish metodologiyasi vaziyatga bog'liq holda, sifatli yoki miqdoriy yoki ularning birikmasi yordamida xatarlarni bartaraf etish uchun qo'llaniladi. Ushbu maqolada ular to'g'risida batafsil ma'lumotlar yoritilib berilgan.*

Kalit so'zlar: *risk, risk tahlili, risklarni baholash, sifatli tahlil, miqdoriy tahlil.*

МЕТОДИКА РАЗРАБОТКИ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ ПРИ ОПРЕДЕЛЕНИИ ОПТИМАЛЬНОЙ ТАКТИКИ СНИЖЕНИЯ РИСКОВ БЕЗОПАСНОСТИ.

Аннотация*:*Анализ рисков является одной из мер по обеспечению безопасности организации и осуществляется с различной степенью детализации в зависимости от критичности активов, наличия определённых уязвимостей и распространённости предыдущих инцидентов, относящихся к организации. Методология анализа рисков применяется в зависимости от ситуации — с использованием качественного, количественного анализа или

их комбинации — для нейтрализации потенциальных угроз. В данной статье подробно освещены данные подходы.

Ключевые слова: *риск, анализ рисков, оценка рисков, качественный анализ, количественный анализ.*

METHODOLOGY FOR DEVELOPING MANAGEMENT DECISIONS IN DETERMINING THE OPTIMAL STRATEGY FOR REDUCING SECURITY RISKS.

Abstract: The concept of enterprise security is to protect the security of its data warehouse and network from threats and to maintain its position in the market without exposing its malicious business plans. Information security is considered important in the public and private sectors of business, as well as in protecting critical infrastructure. Security issues were not taken into account when designing information systems. The level of security that can be achieved with technical means has a number of forms and must be ensured by appropriate management tools and procedures. The selection of the necessary measures for information security management requires careful planning and detailing. The first step in controlling and improving the effectiveness of security in an organization is to properly manage and develop measures based on the results of the assessment of information risks.

Keywords: *risk, risk analysis, risk assessment, qualitative analysis.*

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‘rroq 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.

Asosiy qism. Risklarni boshqarish modellari korporativ tizimlardagi xavflarni aniqlash, baholash va nazorat qilishda yordam beradi. Ular xavflarni aniqlash va tahlil qilish va ularning salbiy oqibatlarini oldini olish yoki yumshatish uchun strategiyalarni ishlab chiqish uchun tizimli yondashuvni taqdim etadi.

“Axborot xavfsizligi riskini boshqarish” atamasi, odatda, axborot xavfsizligi sohasidagi normativ-huquqiy bazasi va shaxsiy korporativ xavfsizlik siyosatiga

muvofiq kompaniyalarning axborot risklarini aniqlash, boshqarish va kamaytirishning tizimli jarayonini anglatadi. Yuqori sifatli xatarlarni boshqarish samaradorlik va xarajatlar nuqtai nazaridan maqbul bo‘lgan, kompaniya faoliyatining hozirgi maqsad va vazifalariga mos keladigan, risklarni boshqarish va axborotni himoya qilish vositalaridan foydalanishga imkon beradi

Risk tahlili va ehtimolligini baholash - bir tashkilot faoliyatining mavjud va keyingi risklarini aniqlash va ularni qo‘llab-quvvatlash ushun quyidagi usullardan foydalanishni talab qiladi:

– *Risklarining turlari va shakllarini aniqlash:* Tashkilot faoliyatining mavjud va keyingi risklarini aniqlash ushun faoliyatning barcha bo‘limlarini va protseslarini mukammal bilish lozim.

– *Risklarning ehtimollik va zararliligini baholash:* Tashkilotda mavjud risklar ehtimolligi va zararliligi baholanadi. Ehtimollik, riskning qaysi darajada va qanday kelib chiqishiga bog‘liq. Zararlilik esa, riskning tashkilotga qanday zarar keltirishi haqidagi fikrni bildiradi.

– *Risklar bilan qarama-qarshi strategiyalar tuzish:* Tashkilot risklar bilan qarama-qarshi strategiyalarni tuzishi lozim. Bu, risklar yuz bergan vaqtda zararlarni kamaytirish va tashkilotni risklardan himoya qilishga yordam beradi.

– *Risklar va strategiyalarning amalga oshirilishini baholash*: Tashkilot risklar va strategiyalarning amalga oshirilishi baholanadi, bu tashkilotning risklar bilan qarama-qarshi strategiyalarning yaxshi ishlayotganligini aniqlashda yordam beradi.

Xatarlarni baholashning turli usullari mavjud bo‘lib, ularga: iqtisodiy, matematik va statistik, ekspert baholash usuli, birlashtirilgan (uchta usulning birlashtirgan majmui: matematik-statistik usul va ekspert baholash usuli yoki ekspert baholash va iqtisodiy tahlil usullarning birga qo‘llanilishi bilan) kiradi.

Xavflarni baholashda ikkita asosiy yondashuv mavjud:

– ***Riskni sifat jihatdan tahlil qilish.*** Sifat jihatdan tahlil qilishda potensial oqibatlar ko‘lamini (masalan, “past”, “o‘rtacha” va “yuqori”) va bu oqibatlar yuzaga kelishi ehtimolligini tavsiflash uchun malaka xossalari shkalasidan foydalaniladi. Sifat jihatdan tahlil qilishning afzalligi, xavlarni bartaraf etish buyicha ma’sul barcha xodimlarning uni tushunishining soddaligida bo‘lsa, kamchiligi yesa, shkalaning subyektiv tanlanishga bog‘liqligi hisoblanadi.

Bunday shkalalar vaziyatni qanoatlantiradigan darajada moslashtirilishi yoki to‘g‘rilanishi, turli risklar uchun standartlarga mos ravishda turli tavsiyalardan foydalanilishi mumkin.

Sifat jihatdan tahlil qilishda:

a) birmuncha batafsil tahlil qilishni talab qiladigan risklarni aniqlash uchun tekshirish bo‘yicha faoliyatni oldindan ko‘rib chiqish sifatida;

b) tahlil qilishning bu turi qaror qabul qilish uchun mos bo‘lgan joyda;

c) sonli ma’lumotlar yoki resurslar risklarni miqdor jihatdan tahlil qilish ushun adekvat bo‘lmagan joyda foydalanilishi mumkin.

Sifat darajasi bo‘yicha baholashda 5 ta darajadan foydalanish eng qulaydir:

1. Ahamiyatsiz.
2. Past.
3. O‘rtacha.
4. Yuqori.
5. Halokatli.

– ***Riskni miqdor jihatdan tahlil qilish.*** Riskni miqdor jihatdan tahlil qilishda turli manbalardan olingan ma’lumotlarni qo‘llagan holda, oqibatlarga va ehtimollikka tayanib, sonli qiymatlar bo‘lgan shkaladan (sifat jihatdan tahlil qilishda foydalaniladigan ko‘rgazmali shkalalar bundan mustasno) foydalaniladi. Tahlil qilish sifati sonli qiymatlarning to‘laligi va aniqligiga hamda foydalaniladigan modellarning asoslanganligiga bog‘liq. Ko‘pgina holatlarda, miqdor jihatdan tahlil qilishda o‘tgan davr ichidagi insidentlar bo‘yicha ma’lumotlardan foydalaniladi.

Uning afzalligi shundan iboratki, u axborot xavfsizligi va tashkilotning muammolari bilan to‘g‘ridan-to‘g‘ri bog‘liq bo‘lishi mumkin. Miqdor jihatdan tahlil qilishning kamchiligi yangi risklar yoki axborot xavfsizligi muammolari bo‘yicha bunday ma’lumotlarning yetishmasligi hisoblanadi. Miqdor jihatdan tahlil qilishning kamchiliklari haqiqatda tekshiriladigan ma’lumotlardan foydalanib bo‘lmaganda ko‘rinadi. Shuning uchun, riskni baholashning aniqligi va ahamiyatliligi illuziyasi hosil bo‘ladi. Oqibatlar va ehtimollikni ifodalash usuli va risk darajasi to‘g‘risidagi ma’lumotlarni ta’minlash uchun ularni birlashtirish usullari, risk turiga va riskni baholashning chiqish ma’lumotlaridan foydalaniladigan maqsadga muvofiq o‘zgaradi. Oqibatlar va ehtimollikning noaniqligi va o‘zgaruvchanligini tahlil qilishda hisobga olinishi va u haqida samarali tarzda xabar qilinishi zarur.

1-jadval

Risk darajalari va ularning oqibatlarga ta’siri

Risk darajasi	**Tahdidning ta’siri**
Yuqori (51dan 100 gacha)	Agar tekshiruv natijasida risk yuqori deb hisoblansa, tuzatuvchi harakatlar tezda bajarilishi kerak. Mavjud tizim ishlashini davom ettirishi mumkin, ammo tuzatuvchi harakatlar darhol amalga oshirilishi kerak.
O‘rtacha (11 dan 50 gacha)	Agar tadqiqot natijasida risk o‘rtasha deb hisoblansa, bu faoliyatni oqilona vaqt ichida amalga oshirish uchun riskni kamaytirish rejasining asosini tashkil etadigan tuzatuvchi harakatlar zarur.
Past (1 dan 10 gacha)	Agar tadqiqot natijasida risk past deb hisoblansa, tashkilot rahbariyati darajasida tuzatuvchi xatti-harakatlarni amalga oshirish yoki riskni qabul qilish kerakligini aniqlash kerak.

Ushbu jadval yodamida har bir boshlang‘ich xavfsizlik darajasiga raqamli koeffitsiyent beriladi.

Miqdoriy baholashda, dastlabki xavfsizlik darajasi quyidagicha aniqlanadi:

– qimmatli aktivning dastlabki xavfsizlik darajasini sifat bo‘yicha baholash amalga oshiriladi;

– ma’lum bir reyting shkalasi yordamida sifat bahosi miqdoriga o‘tkaziladi.

Bundan tashqari, kombinatsiyalangan yondashuvdan foydalanish ham mumkin. Bunda sifat va miqdoriy baholashdan foydalanishni birgalikda qo‘llash nazarda tutiladi.Tadqiqot natijalariga ko‘ra:

– statistik tavakkalchilikni baholash usullari asosan, texnik-ishlab chiqarish va moliyaviy tavakkalchilikni boshqarishda keng qo‘llaniladi;

– sifat jihatdan baholash usullari tabiiy-texnogen, ekologik, ijtimoiy-demografik, siyosiy va reputatsion tavakkalchilikni baholashda ustuvorlikka ega;

– statistik ma’lumotlarni yig‘ish qiyin bo‘lgan tavakkalchiliklar (masalan, makroiqtisodiy tajribalar, qonunchilikdagi o‘zgarishlar, ma’lumotlar xususiyatlarining buzilishi bilan bog‘liq xavflar) ekspertlar usuli yordamida baholanadi.

Har qanday korporativ tizim yoki tashkilotning tabiiy hoxishi risklarning kelib chiqish sabablaridan qat’i nazar, kutilajak yo‘qotishlar hajmini kamaytirish hisoblanadi. Bu xavflarni boshqarish tizimining (risk-menejment) asosiy vazifalaridan biri bo‘lib, tashkilot yoki hodimlarga salbiy ta’sir ko‘rsatishi mumkin bo‘lgan nojo‘ya voqealarning ehtimolini kamaytirishga qaratilgan boshqaruv qarorlarini ishlab chiqish va amalga oshirish jarayoni hisoblanadi.

Tadqiqot metodologiyasi. Xavfsizlk risklarini boshqarishda qaror qabul qiluvchi shaxs xatarni saqlab qolishi (ya’ni, joriy xatar darajasini qabul qilishi yoki oqibatlar uchun javobgarlikni to‘liq yoki qisman uchinchi tomonga yuklab qo‘yishi mumkin) yoki xatarlarni belgilangan qabul qilinadigan darajalargacha kamaytirishga qaratilgan choralarni qo‘llashi mumkin. Bunga javoban, axborot

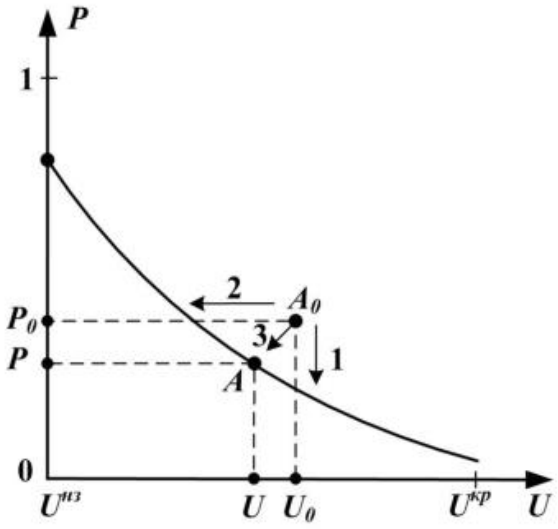
xavfsizligi darajasini oshirish maqsadida xatarlarni kamaytirish strategiyasini amalga oshirishda qo‘yidagi turdagi uslubiy yo‘llar orqali chora tadbirlar amalga oshiriladi:

- tahdiddan qochish yoki tahdid manbaini bartaraf etish;
- himoya choralari va vositalarini qo‘llash orqali zaiflik darajasini pasaytirish;
- tahdidlarning amalga oshishi natijasidagi salbiy oqibatlarni kamaytirish.

Joriy axborot risklarini tavsiflovchi barcha ko‘rsatkichlar qabul qilinadigan xatarlar zonasida bo‘lsa aksariyat hollarda xatarlarni saqlab qolish strategiyasidan foydalanish samarali natija beradi. Shuningbek ba’zi hollarda ushbu strategiyani qabul qilinmaydigan qiymatlar mavjud bo‘lgan hollarda ham qo‘llash mumkin (masalan, xatarlarni keskin kamaytirish imkoni bo‘lmasa yoki juda katta xarajatlarni talab qilsa). Bunday holatlarda ushbu qaror va uni qabul qilish sabablarini hujjatlashtirish tavsiya etiladi.

Agar joriy (aktual) risklarni tavsiflovchi hech bo‘lmaganda bir nuqta qabul qilinadigan risk darajasidan yuqorida joylashgan bo‘lsa, xatarlarni kamaytirish zarur. 1-rasmda ko‘rsatilgan risklarni kamaytirish strategiyalari, joriy axborot xavfsizligi risklarining miqdorini ifodalovchi nuqtani qabul qilinadigan risk muhitiga o‘tkazishni nazarda tutadi. Bu muhit qabul qilinadigan xatar egri chizig‘idan pastda joylashgan bo‘ladi.

Birinchi ikki harakat varianti favqulodda holatlarning yuzaga kelish ehtimolini kamaytirishga qaratilgan, ya’ni A_0 (U_0; P_0) nuqtasini ordinata o‘qidan pastga siljitadi (1-rasmdagi 1-trayektoriya). Uchinchi variant esa noqulay ta’sirlar oqibatlarini kamaytirish bilan bog‘liq: A_0 nuqtasini abssissa o‘qidan chapga siljitadi (1-rasmdagi 2-trayektoriya). Sanab o‘tilgan strategiyalar bir vaqtda ham zararni, ham favqulodda holatlarning yuzaga kelish ehtimolini kamaytirish maqsadida birlashtirilishi mumkin (1-rasmdagi 3-trayektoriya).



1-rasm. Risklarni kamaytirish taktikasi tanlovi.

Axborot xavfsizligi xatarlarini kamaytirish uchun optimal taktikani aniqlash maqsadida quyidagi elementlarni o‘z ichiga olgan boshqaruv qarorlarini ishlab chiqish metodikasi yaratildi:

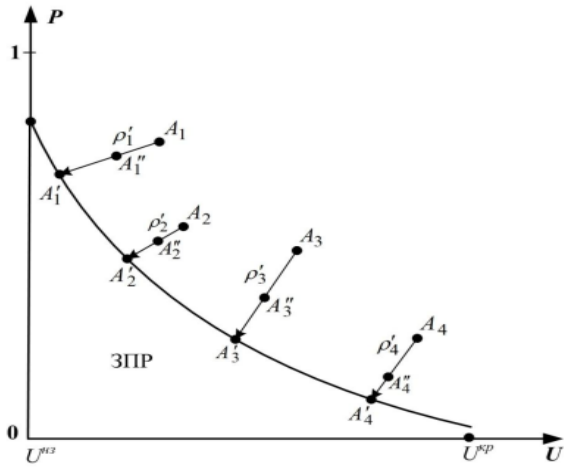
– ekspertlar guruhini shakllantirish va ularning fikrlarini kelishish tartibi;

– xatarlarni kamaytirishga yo‘naltirilgan xarajatlarning “qiymati”ni baholash bo‘yicha tavsiyalar;

– cheksiz (1-vazifa) va cheklangan (2-vazifa) resurslar sharoitida boshqaruv qarorlarini izlash algoritmi.

Ushbu metodika xatarlarni boshqarish jarayonini samarali va iqtisodiy jihatdan to‘g‘ri yo‘naltirishga yordam beradi.

Bunda cheklangan resurslar tushunchasi shunday vaziyatni anglatadiki, ajratilgan mablag‘lar xatarlarni qaror qabul qiluvchi shaxs uchun qabul qilinadigan darajagacha kamaytirish uchun yetarli emas. Qo‘yilgan vazifalarni yechish uchun “risklarni kamaytirish trayektoriyasi” tushunchasi joriy qilingan bo‘lib, bu joriy xatar darajasini ifodalovchi nuqtani qabul qilinadigan xatar egri chizig‘idagi nuqta bilan bog‘lovchi chiziqdir.



2-rasm. Cheklangan va cheklanmagan resurslar sharoitida risklarni kamaytirish.

Bu trayektoriya xatarlarni kamaytirish uchun resurslar taqsimotini aniqlashda yordam beradi.

Qo‘yilgan vazifalarni yechish uchun “xavfni kamaytirish trayektoriyasi” tushunchasi joriy qilindi – bu egri chiziq xavf darajasini ifodalovchi nuqtani qabul qilinishi mumkin bo‘lgan xavf qiymatini aks ettiruvchi nuqta bilan bog‘laydigan chiziqdir.

Berilgan vazifalarni rasmiylashtirish va yechish uchun quyidagi belgilarni kiritamiz (2-rasm): A_i – “joriy xavf”ni tasvirlovchi nuqtalar; A_i' $(i=1..n)$ – qabul qilinadigan xavf qiymatini aks ettiruvchi egri chiziqdagi nuqtalar, ularga A_i dan o‘tish xarajatlar bo‘yicha optimal hisoblanadi; ρ_i' – $A_i$dan A_i' gacha bo‘lgan masofa; A_i'' – xavfni kamaytirishga ajratilgan resurslar yetarli bo‘lmagan holatda erishilgan holatga mos keladigan nuqtalar; ρ_i'' – $A_i$dan A_i''gacha bo‘lgan masofa.

“Xarajatlar qiymati”ni baholash bo‘yicha tavsiyalar:

i-nuqta uchun quyidagi belgilarni kiritamiz:

S_{Ui} – zararni kamaytirish “qiymati”(abssissa o‘qi bo‘ylab harakat);

S_{Pi} – xavf ehtimolini kamaytirish “qiymati” (ordinata o‘qi bo‘ylab harakat).

Bu yerda “qiymat” deganda, axborot xavfsizligi xatarlarini qabul qilinishi mumkin bo‘lgan xavf darajasigacha kamaytirish choralarini amalga oshirish uchun

zarur bo‘lgan inson resurslari, moddiy vositalar, vaqt va boshqa resurslar majmuasi nazarda tutiladi.

“Harajat”ning raqamli xususiyatlarini aniqlash uchun turli resurslar hajmining miqdorini 0 dan 1 gacha chegaraga ega bo‘lmagan shkalaga olib kelish va keyin esa quyidagi additiv svertka usulini topish kerak:

$$S = \alpha_i S^{(inson)} + \alpha_i S^{(moddiy)} + \alpha_i S^{(vaqt)} + \cdots, \quad (1)$$

bu yerda α_i– “vazn” koeffitsiyentlari, ular qaror qabul qilivchilar uchun “axamiyat”ni belgilaydi, ya’ni inson ($S^{(inson)}$), moddiy ($S^{(moddiy)}$), vaqt ($S^{(vaqt)}$) va boshqa qo‘shimcha resurslarning xatarlarni kamaytirish choralari amalga oshirishdagi ahamiyatini belgilaydi.

Verbal baholarni qo‘llashda 0 dan 1 gacha bo‘lgan raqamli qiymatlarga o‘tish Xarrington shkalasiga muvofiq amalga oshiriladi. “Vazn” koeffitsiyentlarini aniqlashda formula (1) bo‘yicha ekspertlarga aniq raqamli baholar berishda qiynalishlari mumkin. Bu holda, engillashtirilgan ranjirlash usulidan foydalanish mumkin, bu esa talab qilinayotgan baholarni Fishbernning umumlashtirilgan vaznlari shaklida topish imkonini beradi.

Bu yondashuvning samaradorligi “yumshoq” sifatli o‘lchovlar, masalan, taqqoslash, sinflash, tartiblash kabi, subyektiv ehtimollar, kriteriylarning miqdoriy ahamiyati baholari, “vazn”larning foydali nuqtasi va boshqalarni belgilashdan ko‘ra aniq va ishonchli bo‘lganida, kelib chiqadi.

Shuni ta’kidlash kerakki, agar axborot aktivi bir necha oxirgi parametrda ishtirok etsa, ya’ni bir hujumni bir necha nuqta «zarar-ehtimol» koordinatalarining tekshirishini xarakterlasa, vazifalarni hal qilish jarayonida zarari ko‘proq bo‘lgan nuqtani tanlash kerak bo‘ladi. Ushbu nuqtaga muhofaza choralarini qo‘llash natijasida uni qabul qilingan xavf darajasiga ko‘chirish mumkin, bundan tashqari,

mazkur hujumga tegishli, ammo kam zarar keltiradigan nuqtalar avtomatik ravishda zararni kamaytirish rejasiga ko‘chiriladi.

Tadqiqot natijalarining muhokamasi.Tahlillar natijasida, axborotni ishlash jarayonidagi xavflarni boshqarish algoritmini quyidagicha shakllantirish mumkin mumkin:

1. Havf miqdorini hisoblash.

2. Tashkilotning samaradorligini ta’minlovchi asosiy biznes jarayonlarini aniqlash (masalan, IDEF0 funksional modellash usulidan foydalanish orqali).

3. Asosiy jarayonlarni dekompozitsiya qilish: kichik jarayonlarni ajratish.

4. Ajratilgan jarayonlarning normal faoliyatini ta’minlash uchun kerak bo‘lgan axborot resurslari (aktivlari) ni aniqlash.

5. Ma’lumotlarning axborot aktivlariga tahdid solishi mumkin bo‘lgan xavflarni shakllantirish. Mazkur xavflar paydo bo‘lishi mumkin bo‘lgan salbiy oqibatlarning ehtimolini aniqlash va ularning amalga oshirilishi natijasidagi oqibatlarning jiddiylik darajasini baholash (tahdidlar intensifikatsiyasi).

6. Tashkilotning axborot aktivlariga potensial tahdidlarni neytrallashtirish bo‘yicha olib borilgan choralarning ro‘yxatini tuzish. Ularning samaradorligini tahlil qilish.

7. Aniq bo‘lmagan kognitiv model uchun axborotni ishlash xavflarini baholash.

8. Olingan aniq bo‘lmagan kognitiv model orqali tashkilotning asosiy jarayonlari faoliyati buzilishi bilan bog‘liq ravishda kelib chiqadigan zararning turli darajadagi ehtimollarini hisoblash,

9. Agar mavjud riskni aks ettiruvchi nuqtalar qabul qilinadigan xavf egri chizig'idan yuqori bo‘lsa, risk darajasini kamaytirish uchun qo‘shimcha resurslarni ajratish kerak yoki qabul qilinadigan risk darajasini oshirish bo‘yicha qaror qabul qilish lozim.

Xulosa qilib aytganda, xatarlarni boshqarish ko‘p bosqichli jarayon bo‘lib, xavflarning biznes operatsiyalariga ta’sirini yumshatishga qaratilgan. Turli sohalarning rahbarlari biznesning barcha jihatlarini potentsial tahdidlardan himoya qilish uchun xavf tahlilidan foydalanadilar. Xavflarni boshqarish faoliyati umumiy boshqaruv qarorlari qabul qilish va amalga oshirish jarayoniga integratsiya qilingan bo‘lishi tashkilotda hatarlarni boshqarish asosiy o‘rinni belgilab beradi. Xatarlarni muntazam boshqarish va baholash, shuningdek, biznesning kutilmagan hodisalarga zaifligini kamaytiradi. Ma’lum metodlar risklarni baholash va boshqarishda muhim rol o‘ynaydi, chunki ular orqali tashkilotlar o‘z xavfsizlik strategiyalarini takomillashtirishi va xatarlarni samarali boshqarishi, xavf-xatarlarni baholash usullari orqali ularni baholab, korxona va tashkilotlarda yetkazilishi mumkin bo‘lgan zararlarni oldini olish, korxonaning ortiqcha sarf-xarajatlarini kamaytirish va bozorda obro‘sizlantirishning oldini olishning eng maqbul chora-tadbirlari hisoblanadi.

Foydalanilgan adabiyotlar:

[1] **O‘z Dst ISO/IEC 27005:2013 «Информационные технологии. Методы обеспечения безопасности. Управления рисками информационной безопасности».**

[2] ISO/IEC 27005:2011 standarti "Axborot texnologiyalari. Xavfsizlik usullari. Axborot xavfsizligi xatarlarini boshqarish" .

[3] ISO/IEC 27002:2013, Information technology — Security Technikues — Code of practice for information security controls.

[4] **Yakubdjanovna, I. D., & Ubaydullayevna, X. I. (2021, November). Analysis of Information Security Problems in Electronic Management with Possible Solutions. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-5). IEEE.**

[5] Axborot xavfsizligi xavfini baholash. - Umarov A.M. Scientific Progress Volume 2 | Issue 8 | 2021 Issn: 2181-1601.

[6] Алексеев, В.М. Комплекс защиты информации для автоматизированных информационных систем с использованием баз данных / В.М. Алексеев [и др.] // Безопасность информационных технологий. - 1994. - №3-4.-С. 128- 130.

[7] Арзуманов, СВ. Оценка эффективности инвестиций в информационную безопасность / СВ. Арзуманов // Информационно-методический журнал «Защита информации. ИНСАЙД». - 2005. - № 1(1). — С. 23-25.

[8] 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.

[9] Современные средства управления информационными рисками.- March 2012.Ukrainian Information Security Research Journal 14(1 (54)).DOI:10.18372/2410-7840.14.2054

[10] 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/.

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

[12] https://www.rapid7.com/fundamentals/information-security-risk-management.

[13] Korporativ tizimlarda axborot xavfsizligi risklarini boshqarish usullari. Islamova D. S. Muhammad Al-Xorazmiy Avlodlari. 1(27)/2024- 187-bet/

[14] https://www.rapid7.com/fundamentals/information-security-risk-management.

[15] https://safetyculture.com/topics/risk-assessment.

[16] https://www.belgelendirme.com/uz/belgelendirme/sistem-belgelendirme/iso-27001-bilgi-guvenligi-yonetim-sistemi

Osiyo texnologiyalar universiteti 27/12/2025 yil.