MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

"AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

4-SON 1(4)
2023-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG‘ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
Chop etish tili: O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
Язык издания: узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
Language of publication: Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2023 yil, Tom 1, №4
Vol.1, Iss.4, 2023 y

ELEKTRON ILMIY JURNALI **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O‘zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro‘yxatdan o‘tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo‘nalishida milliy nashrlar ro‘yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg‘ona sh.,
Aeroport ko‘chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz

FARG’ONA - 2023 YIL

Jurnal quyidagi bazalarda indekslanadi:

Google Scholar · zenodo · ORCID · CYBERLENINKA · WORLD of JOURNALS · DRJI Directory of Research Journals Indexing

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

AXBOROTNI HIMOYALASHDA CHETLAB O’TISHNING MUMKIN BO‘LGAN EHTIMOLLIK XOLATINI BAHOLASH USULLARI

Turdimatov Mamirjon Mirzayevich
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali, “Axborot xavfsizligi” kafedrasi texnika fanlari nomzodi, dotsent, Farg‘ona, O’zbekiston
turdimatovmamirjon1958@gmail.com

Sadirova Xursanoy Xusanboy qizi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali, “Axborot xavfsizligi” kafedrasi assistenti, Farg‘ona, O’zbekiston
sadirovaxursanoy@gmail.com

Annotatsiya. Ushbu maqolada avtomatlashtirilgan axborot xavfsizligi tizimining tarkibi va qurilish tamoyillari tahlil qilinib, uni chetlab o‘tishning mumkin bo‘lgan extimollik xolatlari matematik usullar bilan asoslandi, natijada axborotni himoya qilishning ikki tomonlama yopiq virtual qobig‘i yaratildi. Matematik yondashuv asosida tizimning ishlamay qolish(nosozlik) vaqti tasodifiy o‘zgaruvchi sifatida ko‘rib chiqildi.

Kalit so‘zlar: axborot, xavfsizlik, tizim, extimollik, virtual, nosozlik, tasodifiy, ximoya, loyihalash, model.

Kirish. Xozirgi davrda dunyoda xavfsizlik muammosi e’tiborni kuchaytirishni talab qiladigan asosiy vazifalardan biri xisoblanishi xech kimga sir emas. Axborot xavfsizligi katta ahamiyatga ega va unga bo‘lgan extiyoj kun sayn oshib boraveradi. Soat sayn yangi viruslar va zararli dasturlar ishlab chiqilmoqda, mavjud shifrlash usullarini chetlab o‘tish uchun yangi algoritmlar va turli usullar yaratilmoqda, shuning uchun yangi hujumlarga o‘z vaqtida javob berish va nafaqat tahdidni aniqlash, balki uni boshqarish ham zamon talabi xisoblanadi.

Bizga ma’lumki, axborot xavfsizligining amaliy muammolarini hal qilishda uning zaifligini miqdoriy baholash katta ahamiyatga ega. Shuning uchun axborot xavfsizligi sohasidagi bir qator mutaxassislar tasodifiy va qasddan tahdidlardan himoya qilish usullari va vositalarini takomillashtirish bilan shug‘ullanib kelmoqdalar[1-3]. Tasodifiy tahdidlardan himoya qilish uchun avtomatlashtirilgan tizimlar(AT) ishlashining ishonchliligini oshirish vositalari, ma’lumotlarning ishonchliligi va zahiraviy nusxasini oshirish vositalari qo‘llaniladi. Qasddan tahdidlardan himoyalanishni loyihalashda ro‘yxat va tasnif ma’lum bir ATda himoya qilinishi kerak bo‘lgan ma’lumotlarning tabiati, joylashuvi, ahamiyati va amal qilish muddati bilan belgilanadi. Ushbu ma’lumotlarning tabiati va ahamiyatiga ko‘ra, potensial bosqinchining kutilayotgan darajasi va xatti-harakati tanlanadi. Tahdid axborotga ruxsatsiz kirish orqali amalga oshiriladi, deb ishoniladi.

Adabiyotlar sharxi va metodologiya. Tadqiqot natijalariga ko‘ra tizimda buzg‘unchi modeliga muvofiq, himoyalangan ma’lumotlarga ruxsatsiz kirishning mumkin bo‘lgan kanallarining turlarini va ularni miqdorini aniqlash asosiy parametrlardan biri hisoblanadi. Aynan shu kanallar texnik jihatdan boshqariladigan va boshqarilmaydiganlarga bo‘linadi. Masalan, terminal klaviaturasidan tizimga kirish maxsus dastur orqali boshqarilishi mumkin, lekin mintaqaviy jihatdan taqsimlangan tizimning aloqa kanallari har doim ham boshqarilavermaydi. Kanallarni tahlil qilish asosida ushbu kanallarni blokirovka qilish uchun tayyor turish yoki yangi himoya vositalari qo‘llanilishi lozim.

Bizga ma’lumki, yagona doimiy himoya mexanizmini yaratish uchun maxsus ajratilgan markazlashtirilgan boshqaruv vositalari yordamida himoya vositalari yagona avtomatlashtirilgan axborot

xavfsizligi tizimiga birlashtirilib, uning tarkibi va qurilish tamoyillarini tahlil qilib, uni chetlab o‘tishning mumkin bo‘lgan usullari tekshiriladi. Natijada axborotni himoya qilishning yopiq virtual qobig‘i quriladi[1].

Himoya darajasi axborotning oqib chiqishi kanallarining to‘liq qoplanishi va himoya vositalarini chetlab o‘tishning mumkin bo‘lgan usullari, shuningdek, himoyaning mustahkamligi bilan belgilanadi. Buzg‘unchining xatti-harakatlarining qabul qilingan modeliga ko‘ra, himoya qilishning mustahkamligi ushbu qobiqni tashkil etuvchi vositalar kuchining eng past qiymati bilan himoya vositalari bilan belgilanadi.

Himoya kuchi(to‘siq) deganda tajovuzkor tomonidan uni yengib o‘tmaslik ehtimoli kattaligi tushuniladi. Agar buzg‘unchi tomonidan uni yengib o‘tish uchun kutilgan vaqt himoyalangan ob’ektning ishlash muddatidan yoki ushbu to‘siqni chetlab o‘tish yo‘llari bo‘lmasa, kirishni aniqlash va blokirovka qilish vaqtidan uzoqroq bo‘lsa, himoya to‘sig‘ining mustahkamligi yetarli deb xisoblanadi.

Himoya qobig‘i bir xil prinsip bo‘yicha qurilgan (nazorat qilish yoki oldini olish) kanallariga joylashtirilgan himoya vositalaridan iborat bo‘lishi kerak. Boshqariladigan kanallarda buzg‘unchi qo‘lga tushish xavfini tug‘diradi va nazoratsiz kanallarda u vaqt va pul bilan cheklanmagan qulay sharoitlarda ishlashi mumkin. Ikkinchi holatda himoya kuchi ancha yuqori bo‘lishi kerak. Shuning uchun, avtomatlashtirilgan tizimda alohida virtual himoya qobiqlariga ega bo‘lish tavsiya etiladi. Bundan tashqari, birgalikda o‘zlarining himoya qobig‘ini yaratishi mumkin bo‘lgan tashkiliy chora-tadbirlardan foydalanishni hisobga olish kerak.

Himoya vositasi talablarga javob bermasa, bu zvenodagi to‘siq kuchlirog‘i bilan almashtirilishi kerak yoki bu to‘siq yana bitta, ba’zan esa ikki yoki undan ortiq to‘siqlar bilan takrorlanadi. Qo‘shimcha to‘siqlar birinchisi kabi bir xil yoki undan ko‘p bo‘lgan aloqa kanallarini qamrab olishi kerak.

Resurslarni aniqlash va baholashning ikkinchi bosqichida-"Aktivlarni identifikatsiyalash va baholash"da aktivlar aniqlanadi[3,5]. Axborot aktivlarining tannarxini hisoblash sizga taklif qilinayotgan nazorat va himoya vositalariga ehtiyojni yetarliligini aniqlash imkonini beradi.

Tahdid va zaifliklarni baholashning uchinchi bosqichida - "Xavf va zaifliklarni baholash" - tashkilotning axborot aktivlarining tahdidlari va zaifliklari aniqlanadi va baholanadi[3,6].

CRAMM usulining tijorat versiyasida bunday baholash va identifikatsiyalash uchun quyidagi mezonlar to‘plamidan foydalaniladi (axborot xavfsizligi tahdidlarini amalga oshirish oqibatlari):

1 -mezon - tashkilot obro‘siga putur yetkazish;

2 - resurslarni tiklash bilan bog‘liq moliyaviy yo‘qotishlar;

3 - kompaniyaning tartibsizligi;

4-axborotni oshkor qilish va raqobatchilarga yetkazishdan moliyaviy yo‘qotishlar, shuningdek boshqa mezonlar.

Xatarlarni tahlil qilishning to‘rtinchi bosqichi - "Xatarlarni tahlil qilish" sizga xavflarning miqdoriy bahosini olish imkonini beradi. Bu taxminlarni quyidagi ifodalar yordamida hisoblash mumkin:

R = R_{zar}*C_{zar};

R = R_{tah}*R_{zaif}*C_{zar}, bu yerda:

R-tahdidni amalga oshirish natijasida xavf miqdori;

R_{zar}-tahdidni amalga oshirish natijasida zarar yetkazish ehtimoli;

R_{tah}-tahdidni amalga oshirish ehtimoli;

R_{zaif}-zaifliklarni amalga oshirish ehtimoli;

C_{zar}-tahdidni amalga oshirish natijasida zarar miqdori.

Agar axborot ob’ekti bir nechta N-ta tahdidlarga duch kelsa (mumkin bo‘lgan zararni baholash mezonlari), unda axborot ob’ektiga tajovuzkorlar yetkazgan zararning umumiy xavfi (umumiy qiymati) quyidagicha ifodalanishi mumkin:

$$R_{Um} = \sum_{i=1}^{N} P_i * C_i ;$$

bu yerda **C_i i**-chi tahdid uchun yetkazilgan zarar qiymati;

P_i-bu mutaxassislar tomonidan tanlangan **i**-tahdidning shikastlanish ehtimoli.

Xavflarni boshqarishning beshinchi bosqichida- "Xavflarni boshqarish" - tavakkalchilikni kamaytirish yoki oldini olish choralari va vositalari taklif qilinadi. Natijalarni to‘g‘rilash yoki boshqa baholash usullaridan foydalanish mumkin. Natijada yuzaga keladigan tahdidlar, zaifliklar va xavflar darajasi tahlil qilinadi va mijoz bilan kelishiladi. Shundagina usulning oxirgi bosqichiga o‘tish mumkin.

Natijalar va tahlillar. Olingan natijalarga asosan tahdidlar ro‘yxatini aniqlash va buzg‘unchi modelini yaratish himoya tizimini loyihalashda majburiy qadam xisoblanadi. Har bir tizim uchun xavfsizlikka ehtimoliy tahdidlar ro‘yxati, shuningdek, ehtimoliy bosqinchining xususiyatlari individualdir. Shuning uchun ro‘yxat va model norasmiy bo‘lishi kerak. Axborot xavfsizligi taxmin qilinayotgan tahdidlar va tajovuzkorning sifatlari haqiqiy vaziyatga mos kelgan taqdirdagina ta’minlanadi. Tizimda zaiflik mavjud bo‘lsa, potensial xavfsizlik tahdidi hujum shaklida amalga oshirilishi mumkin.

Hujumlar odatda maqsadlar, motivlar, foydalanilgan mexanizm, tizim arxitekturasidagi o‘rni va tajovuzkorning joylashuviga qarab tasniflanadi. Muvaffaqiyatli hujumlarning oldini olish uchun tizimning zaif tomonlarini qidirish va tahlil qilish kerak. Zaifliklar paydo bo‘lish manbasiga, xavf darajasiga, tarqalish darajasiga, AT himoyasi quyi tizimlari bilan bog‘liqligiga qarab farqlanadi. Zaiflikni tahlil qilish - axborotlashtirish ob’ektini sertifikatlashning majburiy tartibi. Yangi zaifliklar paydo bo‘lishi ehtimoli tufayli ularni allaqachon sertifikatlangan ob’ektda davriy tahlil qilish talab qilinadi.

Nazorat qilish va blokirovka qilish vositalari ruxsatsiz kirishning mumkin bo‘lgan kanallarida, texnik yoki tashkiliy jihatdan mumkin bo‘lgan joylarda o‘rnatiladi va bunday imkoniyatlar mavjud bo‘lmaganda ogohlantirish vositalari (profilaktika vositalari) qo‘llaniladi.

Himoya uskunasining kuchini hisoblashda vaqt omili hisobga olinadi, bu uning kuchining miqdoriy bahosini olish imkonini beradi - potensial buzuvchi tomonidan uni yengib o‘tmaslik ehtimolining kutilgan qiymati.

Himoyaning mustahkamligi to‘siqning xususiyatlariga bog‘liq. Yaratilgan to‘siqning kuchi, agar potensial tajovuzkor tomonidan uni yengib o‘tish uchun kutilayotgan xarajatlarning qiymati himoyalangan ma’lumotlarning narxidan oshsa, yetarli deb hisoblanadi.

Ikkinchi kutilayotgan xavf-xatarlarni axborotni qayta ishlash amaliyotida signal yoki akustik ko‘rinishdagi ma’lumotlarni odatda tegishli sensorlar yordamida o‘lchash yo‘li bilan xam aniqlash mumkin[5-7]. Ma’lumotlarni qayta ishlashda kuzatilayotgan ob’ekt ma’lumotlarda signal qismi va xavf(nosozlik) borligi hisobga olinadi. Bunday holda, signal bizni qiziqtiradigan ob’ekt haqida ma’lumotni olib yuradigan o‘lchangan maydonning tarkibiy qismi sifatida tushuniladi. Interferensiya deganda foydali signalni (shu jumladan tasodifiy komponentni) chiqarishga to‘sqinlik qiluvchi maydon komponentlari (uni o‘zgartirish paytida yuzaga keladigan xatolar) tushuniladi. Masalan, tasodifiy interferensiya deb tasniflanadi.

Ma’lumki, aloqa kanali koinotning bir nuqtasidan ikkinchisiga xabarlarni uzatish uchun texnik vositalar to‘plamidir. Ushbu uzatish ko‘pincha muqarrar shovqin sharoitida amalga oshiriladi. Ushbu ko‘rinishda, bo‘shliqlarni bartaraf etish uchun $x(t)$, oraliqlarda namuna olish jarayoni yordamida diskret shaklga Δt_1 (raqamlar ketma- ketligi) ga aylantirilishi mumkin bo‘lgan signalga aylantirilgan birlamchining uzluksiz Δt_2, Δt_3,…. xabariga yaqinlashish usuli qo‘llaniladi. Amaliy nuqtai nazardan, intervallar ba’zisiga teng deb qabul qilinadi , $ya'ni\ \Delta t = T_B$.

Agar vaqt bo‘yicha kvantlasak $U(k\Delta t)$ approksimatsiya natijasini quyidagicha yozish mumkin

$$u_{k_b(t)=\sum_k u\ (t)\delta(t+kT_B)},$$

buyerda $\delta(t) -$ delta funksiya.

Yechimlar(Results) Interferensiya natijasida har bir yuborilgan element qabul qiluvchi tomonidan $y_k(y_k \neq x_i)$ sifatida tan olinishi mumkin. Bu jarayon xatolikka moyil bo‘lganligi uchun doimiy xabar $x(t)$ sifatida qabul qilinishi mumkin, ya’ni $y(t) \neq ax(t - \tau)$ vaqtning barcha yoki ba’zi lahzalari uchun, bu yerda a va τ doimiylar, odatda axborot miqdori nuqtai nazaridan ahamiyatli emas. Axborot nazariyasi nuqtai nazaridan aloqa kanalining jismoniy tuzilishi muhim emas. Bunday holda, kanal xususiyatlari to‘liq o‘tish ehtimoli matritsasi bilan tavsiflanadi $P(x_i/y_k)$ yoki

$P(y_k/x_i)$ qabul qilingan $e$lement xosil bo‘lsa, y_k $e$lementni yuborish x_i $e$htimoli qayerda xosil bo‘lsa $P(x_i/y_k)$ va - $P(y_k/x_i)$ elementni x_i olish ehtimoli y_k $bo‘ladi$. Interferensiya ta’sirida yangi elementlarni yaratish mumkin emas deb taxmin qilinadi, shuning uchun

$$\sum_{K=1}^{M} P(y_k/x_i) = 1, \qquad \sum_{i=1}^{M} P(x_i/y_k) = 1.$$

Hech qanday xavf(shovqin) bo‘lmasa, u holda barcha diagonal elementlar $P(y_k/x_k)$ yoki P(x_k/ y_k) birga teng, qolganlari esa nolga teng. Juda yuqori shovqin bilan barcha matritsa elementlari taxminan bir xil bo‘lishi mumkin.

Agar biz yetarlicha kichik $\Delta u \ll U_{max} - U_{min}$ $uchun$ Δu $orliqda$ $P_U(u)$ doimiy va joriy qiymati $P_i = P_U(u_i)\Delta u$ ga $teng$ $bo‘ladi$. Shovqinni matematik kutilmasi i– qadam oralig‘ida quyidagicha yoziladi[4]:

$$M[\boldsymbol{\xi_i}] = P_i \int_{u_{i-1/2}}^{u_{i+1/2}} (u - u_i)\, du =$$

$$\frac{1}{2} P_i[(u_{i+\frac{1}{2}} - u_i)^2 - (u_{i-\frac{1}{2}} - u_i)^2].$$

Shovqin dispersiyasi $i-$ $qadam$ $oralig‘ida$ $quyidagicha$ $ifodalanadi$

$$D[\boldsymbol{\xi_i}] = P_i \int_{u_{i-1/2}}^{u_{i+1/2}} (u - u_i)^2\, du$$

$$= \frac{1}{3} P_i[(u_{i+\frac{1}{2}} - u_i)^3 - \left(u_{i-\frac{1}{2}} - u_i\right)^3].$$

Birinchi hosilani nolga tenglashtirib, dispersiyaning minimalini topamiz

$\frac{dD[\boldsymbol{\xi_i}]}{du_i}$:

$$P_i[(u_{i+\frac{1}{2}} - u_i)^2 - \left(u_{i-\frac{1}{2}} - u_i\right)^2] = 0,$$ bu tenglikdan yengilgina quyidagini olamiz

$$yo(u_{i+\frac{1}{2}} - u_i)^2 = yo(u_{i-\frac{1}{2}} - u_i)^2.$$

Teng belgilar asosida $u_{i+\frac{1}{2}} = u_{i-1/2}$ bu tenglik kvantlashning yo‘q xolatiga to‘g‘ri keladi ($\Delta u = 0$).

Turlicha belgilar bo‘lganda $u_i = -\frac{u_{i+\frac{1}{2}} + u_{i-\frac{1}{2}}}{2}$, $yoki$ $u_{i+\frac{1}{2}} = u_i + \frac{\Delta u}{2}$,

$$u_{i-1/2} = u_i - \frac{\Delta u}{2}.$$

Bu shuni anglatadiki, kvantlash darajasi kvantlash bosqichini ikkiga bo‘ladi. Bunday holda, kvantlash shovqinining matematik kutilishi nolga teng.

Dispersiya qiymatini topamiz:

$$D[\boldsymbol{\xi_i}] = \frac{1}{3} P_i[(u_{i+\frac{1}{2}} - u_i)^3 - \left(u_{i-\frac{1}{2}} - u_i\right)^3] =$$

$$\frac{1}{3} p_i[\frac{\Delta u^3}{8} - \left(-\frac{\Delta u}{8}\right)^3] = \qquad = \frac{p_i \Delta u^3}{12} =$$

$$(p_i \Delta u)\frac{\Delta u^2}{12}.$$

Barcha i- shartlarni jamlagan holda, bizda $D[\boldsymbol{\xi}] = \frac{\Delta u^2}{12}$. bu oraliq bo‘yicha Δu taqsimot bir xilligining dispersiyasidir $P_U(u)$.

Yendi biz kvantlangan xabarning ishonchliligini xabarning $\frac{P_c}{P_{sh}}$, o‘rtacha quvvati $P_{sh} -$, kvantlash shovqinining kuchi nisbati bilan baholashimiz mumkin. $P_c -$ Kvantlash shovqin kuchi quyidagi formula bo‘yicha hisoblanadi:

$$P_{sh} = \sigma_{\boldsymbol{\xi}}^2 = \frac{1}{\Delta u} \int_{-\frac{\Delta u}{2}}^{+\frac{\Delta u}{2}} \boldsymbol{\xi}^2 d\,\boldsymbol{\xi} = \frac{\Delta u^2}{12};$$

o‘rtacha xabar quvvati formula bo‘yicha hisoblanadi

$$P_s = \sigma_u^2 = \frac{1}{2U_M} \int_{-U_M}^{+U_M} u^2 d\,\mathbf{u} = \frac{U_M^2}{3}.$$

Kvantlashning aniqligini osongina baholash mumkin $P_k = (2\frac{U_M}{\Delta u})^2$.

Hulosa. Xozirgi axborotlashtirish davrining asosiy muammolaridan biri tasodifiy va qasddan tahdidlardan himoya qilish usullari va vositalarini takomillashtirishdan iborat. Axborot xavfsizligining amaliy muammolarini hal qilishda uning zaifligini miqdoriy baholash katta ahamiyatga ega. Tasodifiy tahdidlardan himoya qilish uchun avtomatlashtirilgan tizimlar ishlashining ishonchliligini oshirish usullari va vositalarini qo‘llash tavsiya etiladi.

Tadqiqot natijalariga ko‘ra tizimda buzg‘unchi modeliga muvofiq, himoyalangan ma’lumotlarga ruxsatsiz kirishning mumkin bo‘lgan kanallarining turlarini va ularni miqdorini aniqlash asosiy parametrlardan biri xisoblanib, aynan shu kanallar texnik jihatdan boshqarish terminal klaviaturasi orqali tizimga kirish uchun maxsus dastur orqali boshqarilishi ko‘zda tutilgan. Lekin mintaqaviy jihatdan taqsimlangan tizimning aloqa kanallari har

doim ham boshqarilavermaydi. Kanallarni tahlil qilish asosida ushbu kanallarni blokirovka qilish uchun tayyor turish uning tarkibi va qurilish tamoyillarini tahlil qilib, uni chetlab o‘tishning mumkin bo‘lgan xolatlarini extimolligi aniqlanadi va bartaraf etish choralari qo‘llanishi ko‘zda tutilgan, natijada axborotni himoya qilishning yopiq virtual qobig‘i yaratilgan.

Ikki tomonlama yopiq virtual qobig‘ini loyixalashni matematik modeli kutilayotgan xavf-xatarlarni aniqlashda axborotni signal ko‘rinishdagi ma’lumotlarni qayta ishlashda kuzatilayotgan ob’ekt ma’lumotlarda signal qismi va xavf(nosozlik) borligi hisobga olindi. Bunday holda, signal bizni qiziqtiradigan ob’ekt haqida ma’lumotni olib yuradigan o‘lchangan maydonning tarkibiy qismi sifatida uzatish ko‘pincha muqarrar shovqin sharoitida amalga oshiriladi, shuning uchun bu to‘siqlarni bartaraf etish uchun kvantlangan xabarning ishonchliligini, xabarning o‘rtacha quvvati, kvantlash shovqinining kuchi nisbati bilan baholandi, natijada kvantlash shovqin kuchini matematik modeli ishlab chiqildi.

Umumiy xulosa sifatida ta’kidlash mumkinki muvaffaqiyatli hujumlarning oldini olish uchun tizimning zaif tomonlarini qidirish va tahlil qilish kerak. Zaifliklar paydo bo‘lish manbasiga, xavf darajasiga, tarqalish darajasiga qarab zaiflikni tahlil qilish zarur, bu esa axborotlashtirish ob’ektini sertifikatlashning majburiy tartibiga amal qilish va ularni oldindan sertifikatlangan ob’ektda davriy tahlil qilish talab qilinadi.

ADABIYOTLAR

1. Turdimatov M.M., Mirzayev J.B. Axborotni himoyalashda yopiq virtual qobig‘ini loyixalashni matematik modeli. JOURNAL OF SCIENCE AND INNOVATION. https://doi.org/10.5281/zenodo.7178488, 2022 yil. 430-436 bet.
2. Shangin V.F. «Kompleksnaya zaщita informatsii v korporativnыx sistemax», Uchebnoye posobiye. M.: ID. «FORUM» - INFRA M. 2019, 591s.
3. Biryukov, A.A. Informatsionnaya bezopasnost: zaщita i napadeniye / A.A. Biryukov. - M.: DMK Press, 2013. - 474 c.
4. Borovkov A.Teoriya veroyatnostey: ucheb. posobiye dlya vuzov. M.: URSS, 2009. - 652 s.
5. Turdimatov M.M., Baratova G., Ashirmatov O.M. Distribution and Comprehensive Implementation of Information Security Responsibilities in Enterprises and Organizations. International Journal of Innovative Research in Science, Engineering and Technology. Volume 11, Issue 4, April 2022.
6. ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls.
7. Turdimatov M.M., Minamatov Y., Kadiraliev R. Methods for the effective use of digital signal processors in creating intelligent devices. JOURNAL OF SCIENCE AND INNOVATION. In Volume 1, Issue 8 of International scientific journal of”Science and Innovation” https://doi.org/10.5281/zenodo.7336445.