

MUHAMMAD AL-XORAZMIY  
NOMIDAGI TATU FARG'ONA FILIALI  
FERGANA BRANCH OF TUIT  
NAMED AFTER MUHAMMAD AL-KHORAZMI

# “AL-FARG‘ONIIY 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



## 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'oniyl avlodlari» («The descendants of al-Fargani», «Potomki al-Fargani») 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

Qo'lyozmalar taqrizlanmaydi va qaytarilmaydi.

FARG'ONA - 2023 YIL

## TAHRIR HAY'ATI

### **Maxkamov Baxtiyor Shuxratovich,**

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti rektori, iqtisodiyot fanlari doktori, professor

### **Muxtarov Farrux Muhammadovich,**

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg'ona filiali direktori, texnika fanlari doktori

### **Arjannikov Andrey Vasilevich,**

Rossiya Federatsiyasi Sibir davlat universiteti professori, fizika-matematika fanlari doktori

### **Satibayev Abdugani Djunosovich,**

Qirg'iziston Respublikasi, Osh texnologiyalari universiteti, fizika-matematika fanlari doktori, professor

### **Rasulov Akbarali Maxamatovich,**

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Axborot texnologiyalari kafedrasida professori, fizika-matematika fanlari doktori

### **Yakubov Maksadxon Sultaniyazovich,**

Muhammad al-Xorazmiy nomidagi TATU «Axborot texnologiyalari» kafedrasida professori, t.f.d., professor, xalqaro axborotlashtirish fanlari Akademiyasi akademigi

### **G'ulomov Sherzod Rajaboyevich,**

Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik fakulteti dekani, Ph.D., dotsent

### **G'aniyev Abduxalil Abdujalilovich,**

Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik fakulteti, Axborot xavfsizligi kafedrasida t.f.n., dotsent

### **Zaynidinov Hakimjon Nasritdinovich,**

Muhammad al-Xorazmiy nomidagi TATU Kompyuter injiniringi fakulteti, Sun'iy intellekt kafedrasida texnika fanlari doktori, professor

### **Bo'taboyev Muhammadjon To'ychiyevich,**

Farg'ona politexnika instituti, Iqtisod fanlari doktori, professor

### **Abdullayev Abdujabbor,**

Andijon mashinosozlik instituti, Iqtisod fanlari doktori, professor

### **Qo'ldashev Abbosjon Hakimovich,**

O'zbekiston milliy universiteti huzuridagi Yarimo'tkazgichlar fizikasi va mikroelektronika ilmiy-tadqiqot instituti, texnika fanlari doktori, professor

### **Ergashev Sirojiddin Fayazovich,**

Farg'ona politexnika instituti, elektronika va asbobsozlik kafedrasida professori, texnika fanlari doktori, professor

### **Qoraboyev Muhammadjon Qoraboevich,**

Toshkent tibbiyot akademiyasi Farg'ona filiali fizika matematika fanlari doktori, professor, BMT ning maslahatchisi maqomidagi xalqaro axborotlashtirish akademiyasi akademigi

### **Polvonov Baxtiyor Zaylobiddinovich,**

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Ilmiy ishlar va innovatsiyalar bo'yicha direktor o'rinbosari

### **Zulunov Ravshanbek Mamatovich,**

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Dasturiy injiniring kafedrasida dotsenti, fizika-matematika fanlari nomzodi

### **Saliyev Nabijon,**

O'zbekiston jismoniy tarbiya va sport universiteti Farg'ona filiali dotsenti

### **Abdullaev Temurbek Marufovich,**

Muhammad al-Xorazmiy nomidagi TATU Axborot texnologiyalari kafedra mudiri, texnika fanlar bo'yicha falsafa doktori

### **Zokirov Sanjar Ikromjon o'g'li,**

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Ilmiy tadqiqotlar, innovatsiyalar va ilmiy-pedagogik kadrlar tayyorlash bo'limi boshlig'i, fizika-matematika fanlari bo'yicha falsafa doktori

Jurnal quyidagi bazalarda indekslanadi:



*Eslatma! Jurnal materiallari to'plamiga kiritilgan ilmiy maqolalardagi raqamlar, ma'lumotlar haqqoniyligiga va keltirilgan iqtiboslar to'g'riligiga mualliflar shaxsan javobgardirlar.*



**MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS**

Muxtarov Farrux Muhammadovich, TARMOQ TRAFIGI ANOMALIYALARINI IDENTIFIKATSIYA QILISHNING STATIK USULI	4-7
Daliyev Baxtiyor Sirojiddinovich, Abelning umumlashgan integral tenglamasini yechish uchun Sobolev fazosida optimal kvadratur formulalar	8-14
Umarov Shuxratjon Azizjonovich, KRIPTOBARDOSHLI KRIPTOGRAFIK TIZIMLAR VA ULARNING KLASSIFIKATSIYASI	15-21
Zulunov Ravshanbek Mamatovich, PYTHONDA NEYRON TARMOQNI QURISH VA BASHORAT QILISH	22-26
Djalilov Mamatisa Latibdjanovich, IKKI QATLAMLI NOELASTIK PLASTINKANING KO'NDALANG TEBRANISHI UMUMIY TENGLAMASINI TAHLIL QILISH	27-30
Erkin Uljaev, Azizjon Abdulkhamidov, Utkirjon Ubaydullayev, A Convolutional Neural Network For Classification Cotton Boll Opening Degree	31-36
Seytov Aybek Jumabayevich, Xusanov Azimjon Mamadaliyevich, Magistral kanallarda suv resurslarini boshqarish jarayonlarini modellashtirish algoritmini ishlab chiqish	37-43
Abdullayev Temurbek Marufjonovich, Algorithm of functioning of intellectual information-measuring system	44-49
Odinakhon Sadikovna Rayimjanova, Usmonali Umarovich Iskandarov, Reaserch of highly sensitive deformation semiconductor sensors based on AFV	50-53
S.S.Radjabov, G.R.Mirzayeva, A.O.Tillavoldiyev, J.A.Allayorov, BARG TASVIRI BO'YICHA MADANIY O'SIMLIKLARNING FITOSANITAR HOLATINI ANIQLASH ALGORITMLARI	54-59
Эргашев Отабек Мирзапулатович, Интеллектуальный оптоэлектронный прибор для учета и контроля расходом воды в открытых каналах	60-65
Xomidov Xushnudbek Rapiqjon o'g'li, Nurmatov Sardorbek Xasanboy o'g'li, Yo'ldashev Bilol Iqboljon o'g'li, O'lmasov Farrux Yorqinjon o'g'li, Konus setkali chang tozalovchi qurilma uchun chang namunalarning dispers tarkibi tahlili	66-69
Akhundjanov Umidjon Yunus ugli, VERIFICATION OF STATIC SIGNATURE USING CONVOLUTIONAL NEURAL NETWORK	70-74
Лазарева Марина Викторовна, Горовик Александр Альфредович, Цифровизация и цифровой менеджмент в современном управлении	75-81
D.X.Tojimatov, KIBERTAHDIDLARNI OLDINI OLIHDA KIBERRAZVEDKA AMALIYOTI VA UNING USTUVOR VAZIFALARI	82-85
Muxtarov Farrux Muhammadovich, Rasulov Akbarali Maxamatovich, Ibroximov Nodirbek Ikromjonovich, Kompyuter eksperimenti orqali kam atomli mis klasterlarining geometrik tuzilishini o'rganish	86-89
Umurzakova Dilnoza Maxamadjanovna, BOSHQARISH QONUNLARINI ADAPTATSIYALASH ALGORITMLARINI ISHLAB CHIQLASH	90-94
Muxamedieva Dildora Kabilovna, Muxtarov Farrux Muhammadovich, Sotvoldiev Dilshodbek Marifjonovich, JAMOAT TRANSPORTI MARSHRUTLARINI QURISH INTELLEKTUAL ALGORITMLARI	95-103
Нурдинова Разияхон Абдихаликовна, Перспективы применения элементов с аномальными фотовольтаическими напряжениями	104-108
Bozarov Baxromjon Pخomovich, UCH O'LCHOVLI FAZODAGI SFERADAANIQLANGAN FUNKSIYALARNI TAQRIBIY INTEGRALLASH UCHUN OPTIMAL KUBATUR FORMULALAR	109-113
Улжаев Эркин, Худойбердиев Элёр Фахриддин угли, Нарзуллаев Шохрух Нурали угли, РАЗРАБОТКА КОНСТРУКЦИИ И ФУНКЦИОНАЛЬНОЙ СХЕМЫ ПОЛУЦИЛИНДРИЧЕСКОГО ЁМКОСТНОГО ПОТОЧНОГО ВЛАГОМЕРА	114-122
Mamirov Uktam Farkhodovich, Buronov Bunyod Mamurjon ugli, ALGORITHMS FOR FORMATION OF CONTROL EFFECTS IN CONDITIONS OF UNOBSERVABLE DISTURBANCES	123-127
Sharibayev Nosirjon Yusubjanovich, Jabborov Anvar Mansurjonovich, YURAK-QON TOMIR KASALLIKLARI DIAGNOSTIKASI UCHUN TEXNOLOGIYALAR, ALGORITMLAR VA VOSITALAR	128-136
Marina Lazareva, Estimating development time and complexity of programs	137-141
Asrayev Muhammadmullo, ONLINE HANDWRITING RECOGNITION	142-146
Norinov Muhammadyunus Usibjonovich, SPEKTR ZONALI TASVIRLARGA INTELLEKTUAL ISHLOV BERISH USULLARI TAHLILI	147-152
Xudoynazarov Umidjon Umarjon o'g'li, PARAMETRLI ALGEBRAGA ASOSLANGAN EL-GAMAL SHIFRLASH ALGORITMLARINI GOMOMORFIK XUSUSIYATINI TADQIQ ETISH	153-157
D.M.Okhunov, M.Okhunov, THE ERA OF THE DIGITAL ECONOMY IS AN ERA OF NEW OPPORTUNITIES AND PROSPECTS FOR BUSINESS DEVELOPMENT BASED ON CROWDSOURCING TECHNOLOGIES	158-165

**MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS**

Солиев Бахромжон Набиджонович, Путеводитель по построению веб-API на Django - Шаг за шагом с Django REST framework — от моделей до проверки работоспособности	166-171
Sevinov Jasur Usmonovich, Boborayimov Okhunjon Khushmurod ogli, ALGORITHMS FOR SYNTHESIS OF ADAPTIVE CONTROL SYSTEMS WITH IMPLICIT REFERENCE MODELS BASED ON THE SPEED GRADIENT METHOD	172-176
Mamatov Narzullo Solidjonovich, Jalelova Malika Moyatdin qizi, Tojiboyeva Shaxzoda Xoldorjon qizi, Samijonov Boymirzo Narzullo o'g'li, SUN'IY YO'LDOSHDAN OLINGAN TASVIRDAGI DALA MAYDONI CHEGARALARINI ANIQLASH USULLARI	177-181
Обухов Вадим Анатольевич, Криптография на основе эллиптических кривых (ECC)	182-188
Turdimatov Mamirjon Mirzayevich, Sadirova Xursanoy Xusanboy qizi, AXBOROTNI HIMOYALASHDA CHETLAB O'TISHNING MUMKIN BO'LGAN EHTIMOLLIK XOLATINI BAHOLASH USULLARI	189-193
Musayev Xurshid Sharifjonovich, TRIKOTAJ MAHSULOTLARIDA NUQSONLI TO'QIMALARNING ANIQLASHNING MATEMATIK MODELI VA UNING ALGORITMLARI	194-196
Kodirov Ahkhmadkhon, Umarov Abdumukhtar, Rozaliyev Abdumalikjon, ANALYSIS OF FACIAL RECOGNITION ALGORITHMS IN THE PYTHON PROGRAMMING LANGUAGE	197-205
Suyumov Jorabek Yunusalievich, METHODOLOGICAL PROBLEMS OF QUALIMETRY IN CONDUCT OF PEDAGOGICAL EXPERIMENT-EXAMINATION	206-211
Хаджаев Саидакбар Исмоил угли, АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ МАЛОГО И СРЕДНЕГО БИЗНЕСА ОТ КИБЕРАТАК	212-217
M.M.Khalilov, Effect of Heat Treatment on the Photosensitivity of Polycrystalline PbTe Films AND PbS	218-221
Тажибаев Илхом Бахтиёрвич, ПОЛНОСТЬЮ ВОЛОКОННЫЙ СЕНСОР, ОСНОВАННЫЙ НА КОНСТРУКЦИИ ИЗ МАЛОМОДОВОГО ВОЛОКОННОГО СМЕЩЕНИЯ С КАСКАДНЫМ СОЕДИНЕНИЕМ ВОЛОКОННОЙ РЕШЕТКИ С БОЛЬШИМ ИНТЕРВАЛОМ, ИСПОЛЬЗУЕТСЯ ДЛЯ ОПРЕДЕЛЕНИЯ ИСКРИВЛЕНИЯ И ПРОВЕДЕНИЯ АКУСТИЧЕСКИХ ИЗМЕРЕНИЙ	222-225
Sharibaev Nosir Yusubjanovich, Djuraev Sherzod Sobirjanovich, To'xtasinov Davronbek Xoshimjon o'g'li, PRIORITIES IN DETERMINING ELECTRIC MOTOR VIBRATION WITH ADXL345 ACCELEROMETER SENSOR	226-230
Mukhammadjonov A.G., ANALYSIS OF AUTOMATION THROUGH SENSORS OF HEAT AND HUMIDITY OF DIFFERENT DIRECTIONS	231-236
Эрматова Зарина Кахрамоновна, АКТУАЛЬНОСТЬ ПРЕПОДАВАНИЯ ЯЗЫКА ПРОГРАММИРОВАНИЯ C++ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ	237-241
Saparbaev Rakhmon, ANALOG TO DIGITAL CONVERSION PROCESS BY MATLAB SIMULINK	242-245
Садикова М.А., Авазова Н.К., САМООБУЧЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, БАЗОВЫЕ ПРИНЦИПЫ РАБОТЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ПРОСТОМ ПРИМЕРЕ	246-250
Abduhafizov Tohirjon Ubaydullo o'g'li, Abdurasulova Dilnoza Botirali kizi, DEVELOPMENT OF ALGORITHMS IN THE ANALYSIS OF DEMAND AND SUPPLY PROCESSES IN ECONOMIC SYSTEMS	251-256
Kayumov Ahror Muminjonovich, CREATING MATHEMATICAL MODELS TO IDENTIFY DEFECTS IN TEXTILE MACHINERY FABRIC	257-261
Mirzakarimov Baxtiyor Abdusalomovich, Xayitov Azizjon Mo'minjon o'g'li, BIOMETRIC METHODS SECURE COMPUTER DATA FROM UNAUTHORIZED ACCESS	262-266
Soliyev B., Odilov A., Abdurasulova Sh., Leveraging Python for Enhanced Excel Functionality: A Practical Exploration	267-271
Жураев Нурмахамад Маматович, Системы Электроснабжения Оборудования Предприятий Связи: Надежность и Эффективность	272-276
Rasulova Feruzaxon Xoshimjon qizi, Isroilov Sharobiddin Mahammadyusufovich, OLIY TA'LIM MUASSASALARIDA MUTAXASSISILIK FANLARINI O'QITISHDA MULTIMEDIALI MOBIL ILOVADANDAN FOYDALANISHNING STATISTIK TAHLILI	277-280
Muxtarov Farrux Muxammadovich, Toshpulatov Sherali Muxamadaliyevich, SUN'IY INTELLEKT YORDAMIDA IJTIMOYIY TARMOQ MONITORINGI TIZIMINI YARATISH, AFZALLIKLARI VA MUHIM JIXATLARI	281-285
Sadikova Munira Alisherovna, APPLICATION OF ARTIFICIAL INTELLIGENCE DEVICES IN MANUFACTURING	286-290
Mamatov Narzullo Solidjonovich, Ibroximov Sanjar Rustam o'g'li, Fayziyev Voxid Orzumurod o'g'li, Samijonov Abdurashid Narzullo o'g'li, SUN'IY INTELLEKT VOSITALARINI TA'LIMNI NAZORAT QILISH VA BAHOLASHDA QO'LLASH	291-297

## 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" kafedrasida 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" kafedrasida 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 xolatlarini 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 hech kimga sir emas. Axborot xavfsizligi katta ahamiyatga ega va unga bo'lgan ehtiyoj 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 ishonchligini oshirish vositalari, ma'lumotlarning ishonchligi va zahiraviy nusxasini oshirish vositalari qo'llaniladi. Qasddan tahdidlardan himoyalashni 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 tannaxini 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 oqibatlarini):

- 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:

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

$$R = R_{tah} * R_{zaif} * C_{zar}, \quad \text{bu yerda:}$$

$R$ -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 zararining 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 choralarini 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 sifatleri haqiqiy vaziyatga mos kelgan taqdiridagina 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 uskunasi 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 xabarlarini 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  $\Delta t_1$  (raqamlar ketma- ketligi) ga aylantirilishi mumkin bo'lgan signalga aylantirilgan birlamchining uzluksiz  $\Delta t_2, \Delta t_3, \dots$  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

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

buyurda  $\delta(t)$  - 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  $\tau$  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 element xosil bo'lsa,  $y_k$  elementni yuborish  $x_i$  ehtimoli 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

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

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  $\Delta u$  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]:

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

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

$$D[\xi_i] = P_i \int_{u_{i-1/2}}^{u_{i+1/2}} (u - u_i)^2 du = \frac{1}{3} P_i [(u_{i+1/2} - u_i)^3 - (u_{i-1/2} - u_i)^3].$$

Birinchi hosilani nolga tenglashtirib, dispersiyaning minimalini topamiz

$$\frac{dD[\xi_i]}{du_i} \cdot P_i [(u_{i+1/2} - u_i)^2 - (u_{i-1/2} - u_i)^2] = 0, \text{ bu tenglikdan yengilgina quyidagini olamiz}$$

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

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

Turlicha belgilar bo'lganda  $u_i =$

$$-\frac{u_{i+1/2} + u_{i-1/2}}{2}, \text{ yoki } u_{i+1/2} = u_i + \frac{\Delta u}{2},$$

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

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

Dispersiya qiymatini topamiz:

$$D[\xi_i] = \frac{1}{3} P_i [(u_{i+1/2} - u_i)^3 - (u_{i-1/2} - u_i)^3] = \frac{1}{3} p_i \left[ \frac{\Delta u^3}{8} - \left( -\frac{\Delta u}{8} \right)^3 \right] = \frac{p_i \Delta u^3}{12} = (p_i \Delta u) \frac{\Delta u^2}{12}.$$

Barcha  $i$ -shartlarni jamlagan holda, bizda  $D[\xi] = \frac{\Delta u^2}{12}$ . bu oraliq bo'yicha  $\Delta u$  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:

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

o'rtacha xabar quvvati formula bo'yicha hisoblanadi

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

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 ishonchligini, 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 zashchita informatsii v korporativnykh sistemax», Uchebnoye posobiye. M.: ID. «FORUM» - INFRA M. 2019, 591s.
3. Biryukov, A.A. Informatsionnaya bezopasnost: zashchita 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., Kadiraliyev 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>.

