O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

ZAMONAVIY INNOVATSION TADQIQOTLARNING DOLZARB MUAMMOLARI VA RIVOJLANISH TENDENSIYALARI: YECHIMLAR VA ISTIQBOLLAR

mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami

(2024-yil 17-18-may)

(1-qism)

JIZZAX-2024

“Zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari: yechimlar va istiqbollar” mavzusidagi Respublika ilmiy-texnik anjuman materiallari to‘plami – Jizzax: O‘zMU Jizzax filiali, 2024-yil 17-18-may. 410-bet.

Respublika miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy innovatsion tadqiqotlarning dolzarb muammolari va rivojlanish tendensiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globallashuv sharoitida davlatimizni yanada barqaror va jadal sur’atlar bilan rivojlantirish bo‘yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e’tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma’ruza tezislari to‘plamida mamlakatimiz va xorijlik turli yo‘nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o‘qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarning ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Mas’ul muharrirlar: DSc.prof. Turakulov O.X., PhD. O‘ralov A.I.

Tahrir hay’ati a’zolari: p.f.d.(DSc), prof. Turakulov O.X., b.f.f.d. (PhD) O‘ralov A.I., t.f.f.d.(PhD), dotsent Abdumalikov A.A., t.f.n., dots. Baboyev A.M., t.f.f.d.(PhD), dots. Abduraxmanov R.A., p.f.f.d.(PhD) Eshankulov B.S., p.f.n., dots. Alimov N.N., p.f.f.d.(PhD), dotsent Alibayev S.X., p.f.f.d. (PhD) Halimov O‘.H., p.f.f.d.(PhD), dotsent Karshiyev A.A., f.f.f.d.(PhD), dotsent Sindorov L.K., t.f.f.d.(PhD), dotsent Nasirov B.U., b.f.f.d. (PhD), dotsent Mustafaqulov M.A., f.f.f.d. (PhD) Alibekov D.A.., f-m.f.f.d. (PhD) Sharipov X.F., ps.f.f.d.(PhD) Norbekova B.Sh., i.f.n., dots. Tsoy M.P., Qayumov O.A., Jo‘rayev M.M.

Mazkur to‘plamga kiritilgan ma’ruza tezislarining mazmuni, undagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligi hamda tanqidiy fikr-mulohazalar, keltirilgan takliflarga mualliflarning o‘zlari mas’uldirlar.

5. Кабулов А.В., Варисов А. Алгоритмические модели информационной безопасности на основе таблиц функционирования// Международный журнал «Наука и мир». №6,2017, том1 с. 28-33. Волгоград.

6. A.V. Kabulov, I.X. Normatov, I.I.Kalandarov, A.A.Karimov. Algorithmic Method of Organization of Specialized Workshops. International Journal of Advanced Research in Science, Engineering and Technology Vol. 5, Issue 4, April 2018, c.5670-5675, ISSN: 2350-0328.

INFOKOMMUNIKATSIYA OBYEKTLARINING ENERGIYA TARMOG‘INI KRIPTOGRAFIK XAVFSIZLIGINI TA’MINLASH

p.f.f.d, dots. Mingboev Ulug‘bek Xujayevich
O‘zbekiston Milliy universiteti Jizzax filiali
Abdurasulov Alijon Abdurasul o‘g‘li
O‘zbekiston Milliy universiteti Jizzax filiali magistranti
ulugbekmingboyev@gmail.com

Annotatsiya. Infokommunikatsiya obyektlaridagi aloqa va axborot uzatishni ta’minlashda muhim rol o‘ynaydi. Biroq, texnologiyalarning rivojlanishi va uzatiladigan ma’lumotlar hajmining ko‘payishi bilan infokommunikatsiya obyektlarning xavfsizligini ta’minlash zarurati tug‘iladi.Axborotni ruxsatsiz kirish va hujumlardan himoya qilish uchun asos bo‘lgan kriptografik energiya tizimining xavfsizligini ta’minlashga ham alohida e’tibor qaratilmoqda.

Kalit so‘zlar. Axborot xavfsizligi, infokommunikatsiya obyektlari, axborot hujumlari, kriptografiya, shifrlash, axborot ta’minoti,kiberxavfsizlik.

Respublikamizda raqamli iqtisod va axborot kommunikatsiya sohasini takomillashtirish asosida infokommunikatsiya obyektlarining elektr energiya ta’minoti ko‘rsatkichlarini monitoring tizimini takomillashtirishga qaratilgan keng qamrovli chora-tadbirlar amalga oshirilmoqda. 2022-2026 yillarga mo‘ljallangan yangi O‘zbekistonning taraqqiyot strategiyasida, jumladan «Yashil iqtisodiyot texnologiyalarini barcha sohalarga faol joriy etish orqali 2026 yilga qadar iqtisodiyotning energiya samaradorligini 20%ga oshirish va havoga chiqariladigan zararli gazlar hajmini 20%ga qisqartirish choralarini ko‘rish» vazifalari belgilangan. Mazkur vazifalarni bajarishda shu jumladan energiya manbalarini monitoring jarayonlarini modellashtirish, algoritmlash va ularni amaliy faoliyatga qo‘llash muhim vazifalardan biri hisoblanadi.

Hozirgi davrga kelib hayotimizni axborot texnologiyasi, kompyutersiz tasavvur qilish mumkin emas.“Axborot” tushunchasi sotib olish, sotish, biror boshqa tovarga almashtirish mumkin bo‘lgan maxsus tovar belgisi sifatida tez-tez ishlatilmoqda. Zamonaviy infokommunikatsiya obyektlari axborotni himoya qilish uchun kriptografik usullardan tobora ko‘proq foydalanmoqda.Biroq, kriptografik energiya tizimining xavfsizligi ma’lumotlarning yaxlitligi va maxfiyligini ta’minlashda ham muhim rol o‘ynashini unutmaslik kerak. Kriptografik energiya tizimining xavfsizligini

ta’minlash uchun bir qator choralarni ko‘rish kerak. Birinchidan, axborotni yuqori darajada himoya qilishni ta’minlaydigan ishonchli kriptografik algoritmlardan foydalanish kerak. Bundan tashqari, dasturiy ta’minotni muntazam yangilab turish va xavfsizlik yangilanishlarini kuzatib borish muhimdir. Shuningdek, ma’lumotlarni himoya qilishdagi zaifliklar va muammolarni aniqlash uchun kriptografik energiya tizimining xavfsizlik auditini o‘tkazish kerak.Bu zaifliklarni bartaraf etish va tizim xavfsizligini yaxshilash bo‘yicha o‘z vaqtida choralar ko‘rish imkonini beradi.[1]

Infokommunikatsiya obyektlarining kriptografik energiya tizimining xavfsizligini ta’minlash himoyalangan axborot muhitini yaratish va saqlashning asosiy jihatlaridan biridir. Kiberxavfsizlik tahdidlari tobora ortib borayotganini hisobga olgan holda,maxfiy ma’lumotlarning tarqalishi ehtimolini minimallashtirish va tizimga mumkin bo’lgan hujumlarning oldini olish uchun kriptografik energiya tizimining xavfsizligini ta’minlash bo‘yicha keng qamrovli chora-tadbirlarni ishlab chiqish muhimdir.

Kriptografik energiya tizimining xavfsizligini ta’minlashning asosiy prinsiplariga zamonaviy shifrlash algoritmlaridan foydalanish, himoya mexanizmlarini muntazam ravishda yangilash va tekshirish, ko'p darajali foydalanuvchi autentifikatsiyasi, maxfiy ma’lumotlarga kirishni boshqarish, tarmoq trafigini kuzatish va kirishni aniqlash kiradi.[2]

Shifrlash algoritmlar tahlili

1-jadval

Xususiyat	**DES**	**AES**	**Blowfish**
Muallif	IBM tashkiloti	Vinsent Rijman va Xuan Daymen	Bryus Shnaer
Kalit uzunligi (bit)	56	128, 192, 256	32-448, o‘zgaruvchan
Kirish blok uzunligi (bit)	64	128	64
Raund soni	16	10, 12, 14	16
Matematik asosi	XOR, surish va o‘rin almashtirish	Ko‘phadlar ustida amallar, XOR, surish	MOV, ADD, XOR
Yaratish asosi	Feystel tarmog‘i	SPN tarmoq	Feystel tarmog‘i
Yeng katta natijaga erishgan hujum turi	Brute-force hujumi	Side-channel hujumi	Kalit zaifligiga asoslangan hujum

Quyida ushbu algoritmlarning kriptotahlil tizimi sanalgan *Crypto++* dasturiy taminoti orqali tahlil qilinganda olingan natijalar berilgan. [3]

2-jadval

Shifrlashdagi tezliklar bo‘yicha tahlili

Algoritm	**Shifrlanadigan ma’lumot (MB)**	**Vaqt**	**MB/Sek**
Blowfish	256	3,976	64,386

Rijndael(128)	256	4,196	61,01
DES	128	5,998	21,34
3DES	128	6,159	20,783

Infokommunikatsiya obyektlarining ma’lumot uzatish tarmoqlarida xavfsizlikga bardoshli kalitlarni generatsiya qilish algoritmi.

Tub sonlarni generatsiya qilish algoritmlari. Tub sonlar kriptografik sxemalarda uzoq vaqtli parametr hisoblanishi bilan, kriptografik tizimlarda muhim ahamiyat kasb etadi. Ochiq kalitli kriptotizimlarda tub sonlarni generasiya qilish va ularni tublikka tekshirish muhim hisoblanadi.

Sonlar nazariyasi va kriptografiyaning ko’plab masalalarida berilgan uzunlikdagi tub sonlarni generasiya qilish zarurati tug’iladi. Tub sonlarni yaratishning yaxshi usullaridan biri, qandaydir funksiya yordamida hosil qilish usulidar. Misol sifatida L.Yeyler taklif qilgan ko’phadni qaraydigan bo’lsak

$$p(x) = x^2 + x + 41,$$

ko’phadni qiymatlarining dastlabki 40 hadi tub sondan iborat bo’ladi.

Biroq Yuriy Matiyasevich bundanda yaxshiroq natija olish mumkinligigi isbotladi, ya’ni butun koeffisentli bir nechta o’zgaruvchilardan tashkil topgan ko’p had mavjudki, uning barcha qiymatlari tub sondan iborat bo’ladi.

$$F(a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z) = (k+2)(1 -$$
$$(wz+h+j-q)^2 - (2n+p+q+z-e)^2 - (a^2y^2 - y^2 + 1 - x^2)^2 -$$
$$\left((e^4 + 2e^3)(a+1)^2 - o^2\right)^2 - (16(k+1)^3(k+2)(n+1)^2 + 1 - f^2)^2 -$$
$$\left(((a+u^4 - u^2a)^2 - 1)(n+4dy)^2 + 1 - (x+cu)^2\right)^2 - (ai + k + 1 - l - i^2 -$$
$$((gk+2g+k+1)(h+j) + h - z)^2 - (16r^2y^4(a^2-1) + 1 - u^2)^2 -$$
$$\left(p - m + l(a-n-1) + b(2an + 2a - n^2 - 2n - 2)\right)^2 - \left(z - pm + pla - p^2l +\right.$$
$$\left.t(2ap - p^2 - 1)\right)^2 - \left(q - x + y(a-p-1) + s(2ap + 2a - p^2 - 2p - 2)\right)^2 -$$
$$(a^2l^2 - l^2 + 1 - mr)^2 - (n + l + v - y)^2))$$

Yana shuni ta’kidlash kerakki, Yu.Matiyasevich ushbu ko’phad yordamida Gilbertning mashhur 10-muammosini, diafant tenglamalarining echimi butun sondan iborat bo’lishini aniqlaydigan umumiy algoritm yo’qligini isbotlagan holda echishga erishdi. Bu natija matematikaning turli yo’nalishlaridagi echilmagan masalalarni yechishga xizmat qildi.[4]

Infokommunikatsiya obyektlari hozirgi kunda xar bir sohaning tayanch qismlaridan biriga aylangan. Telekommunikatsiya signal o‘tkazish stansiyalari hamda ma’lumotlar markazi (Data base) infokommunikatsiya obyektlarini tashkiliy bo‘limlari sanaladi. Energiya ta’minoti stansiyalari ma’lumotlar markazlarining muhim tarkibiy qismidir. Elektr energiyani talab qiladigan boshqa har qanday obyekt singari, ma’lumotlar markazlarining xam deyarli xar bir ishlash jarayonlari uzluksiz energiya quvvati manbaiga tayanadi. Tahlil erish natijasida aloqa tarmoqlarida tizim xavfsizligini ta’minlashda kriptografik algoritmlarning katta uzunlikdagi tub sonlarni hosil qilish bu tizimlarda ahamiyati tahlil etildi.

Foydalanilgan adabiyotlar ro‘yxati:

1. Mingboyev Ulug‘bek and Abdurasulov Alijon, “AXBOROT XAVFSIZLIGI MONITORINGI”, IJCSTR, pp. 275–279, May 2023. Vol 1

2. Мингбоев, У., & Абдурасулов, А. (2023). Информационная безопасность и ее составляющие. *Информатика и инженерные технологии*, *1*(1), 56–60. извлечено от https://inlibrary.uz/index.php/computer-engineering/article/view/25330

3. Mingboyev, U. K., & Abdurasulov, A. A. o‘g‘li. (2024). IN NETWORKS OF INFOCOMMUNICATION OBJECTS USER INFORMATION INFORMATION INFORMATION SECURITY CLASSIFICATION OF METHODS AND MEANS OF SUPPLY. *GOLDEN BRAIN*, *2*(1), 51–54. Retrieved from https://researchedu.org/index.php/goldenbrain/article/view/5909

4. Абдурасулов, А. А. у., & Гулмуродова, Д. А. к. (2024). АНАЛИЗ РИСКОВ И АУТЕНТИФИКАЦИЯ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ В СЕТЯХ ОБЪЕКТОВ ИНФОКОММУНИКАЦИЙ В ВЕБ-ПРИЛОЖЕНИЯХ И ПОЛЬЗОВАТЕЛЯХ. *Educational Research in Universal Sciences*, *3*(4 SPECIAL), 74–78. Retrieved from http://erus.uz/index.php/er/article/view/6044

REVOLUTIONIZING X-RAY ANALYSIS: THE ROLE OF COMPUTER VISION IN DETECTING FRACTURES, TUMORS AND ABNORMALITIES

PhD., Turgunov Abrorjon, Xolmuminov Yusuf, Abdullaev Hayotjon, Rahmatullaev Jasurbek, Abdulxamidov Abrorbek, Berdiqulov Abdulaziz
Tashkent University of Information Technologies
abrorjon26@mail.ru

Abstract - This article explores the transformative impact of computer vision in the realm of X-ray analysis, focusing on its role in detecting fractures, tumors, and various abnormalities. The integration of advanced algorithms brings precision and efficiency to diagnostic imaging, revolutionizing traditional methods. Key applications include fracture detection, tumor identification, and the ability to discern a spectrum of abnormalities in X-ray images. The article discusses the clinical implications, future perspectives, challenges, and ethical considerations associated with this dynamic synergy between technology and healthcare.

Keywords - computer vision, X-ray analysis, fracture detection, tumor identification, abnormality detection, artificial intelligence, clinical impact, future perspectives, diagnostic medicine.

Introduction.

In recent years, the intersection of medicine and technology has given rise to groundbreaking advancements, with computer vision emerging as a transformative force in diagnostic imaging. One particularly fascinating application is in the analysis of X-ray images, where computer vision algorithms play a pivotal role in the detection of fractures, tumors, and various abnormalities. This article explores the innovative strides made in X-ray analysis through the integration of computer vision.