

AXBOROT TEXNALOGIYALARIDAN FOYDALANGAN HOLDA FIRIBGARLIKKA QARSHI KURASHISH

ASAMOV JALOLIDDIN NIZAMETDINOVICH

2007-yil IIV Akademiyasi bitiruvchisi

ANNOTATSIYA: Mazkur ilmiy ishda zamonaviy axborot texnologiyalaridan foydalangan holda firibgarlik holatlarining oldini olish va ularga qarshi samarali kurashish masalalari yoritilgan. Internet tarmog'ida keng tarqalgan moliyaviy va ma'lumot firibgarliklari, ularning usullari hamda aniqlash yo'llari tahlil qilingan. Shuningdek, sun'iy intellekt, blokcheyn texnologiyalari, biometrik tizimlar va kiberxavfsizlik vositalari yordamida firibgarlikning oldini olishda qo'llanilayotgan ilg'or yondashuvlar ko'rib chiqilgan. Tadqiqotda real hayotdan olingan misollar asosida firibgarlikni aniqlash, ogohlantirish va profilaktika qilish bo'yicha amaliy tavsiyalar ishlab chiqilgan. Ish natijalari davlat tashkilotlari, moliya muassasalari va axborot xavfsizligi sohasida faoliyat yurituvchi mutaxassislar uchun foydali bo'lishi mumkin.

KALIT SO'ZLAR: axborot texnologiyalari, firibgarlik, kiberxavfsizlik, sun'iy intellekt, blokcheyn, biometrik identifikatsiya, xavfsizlik tizimlari, ma'lumotlarni himoyalash

KIRISH

Bugungi kunda axborot texnologiyalari hayotimizning deyarli barcha jabhalariga chuqur kirib bormoqda. Davlat boshqaruvi, moliya, ta'lim, sog'liqni saqlash, savdo va boshqa ko'plab sohalarda raqamlashtirish jarayonlari tez sur'atlar bilan rivojlanmoqda. Shu bilan birga, bu jarayonlar inson hayotini yengillashtirishi bilan bir qatorda, turli xavf-xatarlarga ham sabab bo'lmoqda. Ayniqsa, firibgarlikning zamonaviy shakllari — kiberfiribgarlik, ma'lumotlarni





noqonuniy egallash, onlayn moliyaviy aldovlar va boshqa shu kabi holatlar tobora ko'paymoqda.

Axborot texnologiyalaridan noto'g'ri yoki jinoyat maqsadida foydalanish nafaqat alohida shaxslarga, balki jamiyat va davlat xavfsizligiga ham jiddiy tahdid tug'diradi. Shu sababli, firibgarlikka qarshi kurashishda axborot texnologiyalarining o'zi ham muhim vosita sifatida xizmat qilmoqda. Yangi avlod xavfsizlik tizimlari, sun'iy intellekt asosidagi nazorat mexanizmlari, tahliliy dasturlar va blokcheyn texnologiyalari firibgarlik holatlarini aniqlash va ularning oldini olishda keng qo'llanilmoqda.

Mazkur bitiruv malakaviy ishida axborot texnologiyalarining firibgarlikka qarshi kurashishdagi o'rni, imkoniyatlari va amaliy jihatlari tahlil qilinadi. Shu bilan birga, mavjud muammolar, ularni hal etish yo'llari hamda ilg'or xorijiy tajribalar asosida taklif va tavsiyalar ishlab chiqiladi.

ASOSIY QISM

Axborot texnologiyalarining rivojlanishi insoniyat hayot tarzini tubdan o'zgartirdi. Bugungi kunda deyarli barcha sohalarda raqamli tizimlar va onlayn platformalardan foydalanish zaruratga aylanmoqda. Aynan shu holat firibgarlikning ham yangi ko'rinishlarini yuzaga keltirdi. Endilikda firibgarlar zamonaviy texnik vositalar orqali ishlamoqda. Ammo shu bilan birga, axborot texnologiyalari ularni aniqlash, fosh qilish va oldini olish uchun kuchli vosita bo'lib xizmat qila boshladi.

Firibgarlikka qarshi kurashishda birinchi navbatda sun'iy intellekt texnologiyalarining imkoniyatlari e'tiborga loyiq. Masalan, banklar yoki sug'urta kompaniyalari sun'iy intellekt yordamida tranzaksiyalarni real vaqt rejimida tahlil qilmoqda. Shubhali yoki odatdagidan farqli harakatlar aniqlansa, tizim avtomatik tarzda ogohlantirish beradi yoki operatsiyani vaqtincha to'xtatadi. Bu jarayon inson nazoratiga bog'liq bo'lmagan, tezkor va ishonchli himoya tizimini shakllantirishga xizmat qilmoqda.



Bundan tashqari, biometrik ma'lumotlardan foydalanish ham firibgarlikka qarshi samarali vosita sifatida e'tirof etilmoqda. Barmoq izi, yuzni aniqlash, ovoz orqali identifikatsiya kabi metodlar shaxsni aniq tasdiqlash imkonini beradi. Bu texnologiyalar foydalanuvchi ma'lumotlarini himoya qilishda yuqori darajadagi xavfsizlikni ta'minlaydi.

Kiberxavfsizlik sohasi mutaxassislari firibgarlikka qarshi kurashishda katta rol o'ynaydi. Ular muntazam tarzda tarmoq zaifliklarini aniqlash, dasturiy vositalarni yangilash va foydalanuvchilarni xabardor qilish bilan shug'ullanadi. Chunki har qanday texnologiya bilan bir qatorda inson omili ham muhim hisoblanadi. Foydalanuvchilar o'z ma'lumotlarini qanday himoyalashi, qanday havfsizlik qoidalariga amal qilishi ham firibgarlik xavfini kamaytirishga xizmat qiladi.

Shuningdek, ta'lim muassasalarida axborot madaniyatini shakllantirish ham muhim ahamiyatga ega. O'quvchilar va talabalar raqamli xavfsizlik, shaxsiy ma'lumotlarni himoya qilish, ijtimoiy tarmoqlarda ehtiyotkorlik bilan harakat qilish kabi mavzularda yetarli bilimga ega bo'lishi zarur. Bu orqali ular kelajakda raqamli firibgarlik qurboni bo'lishdan himoyalaniishi.

Amaliy jihatdan qaralganda, blokcheyn texnologiyasi ham firibgarlikning oldini olishda keng imkoniyatlarga ega. Bu texnologiya ma'lumotlarni markazsiz tarzda saqlash va ularni o'zgartirib bo'lmazligiga kafolat beradi. Shuningdek, shaffoflikni ta'minlagani sababli firibgarlar uchun imkoniyatlar deyarli yo'qoladi.

Yana bir samarali usul — onlayn firibgarlik holatlarini avtomatik aniqlash algoritmlarini ishlab chiqishdir. Bu algoritmlar foydalanuvchining xatti-harakatlaridagi noodatiy o'zgarishlarni kuzatadi, masalan: parollarni doimiy almashtirish, turli joylardan kirish urinishlari, noodatiy tranzaksiyalar va hokazo. Ushbu algoritmlar firibgarlik aniqlanmagan holatlarda ham xavfni oldindan baholash imkonini beradi.

“Axborot texnologiyalaridan foydalangan holda firibgarlikka qarshi kurashish” mavzusiga oid kreativ va amaliy misollar jadval shaklida taqdim



etilgan. Har bir texnologiya yoki yondashuvning qisqacha tavsifi, amaliy qo'llanilishi va natijasi ko'rsatilgan.

Texnologiya / Yondashuv	Amaliy qo'llanilishi (misol)	Kutilayotgan natija / foydasi
Sun'iy intellekt (AI) algoritmlari	Banklarda shubhali tranzaksiyalarni aniqlovchi tizim: mijoz odatdagi soatlarda emas, boshqa davlatdan pul yechsa — tizim ogohlantiradi yoki bloklaydi.	Firibgarlik holatlarini oldindan aniqlash, tezkor blokirovka qilish
Biometrik identifikatsiya	Talabalarni masofadan turib imtihon topshirishda yuzni aniqlash orqali shaxsni tasdiqlash (plagiat yoki o'rniga kirishni oldini olish)	Soxta identifikatsiyani yo'qotish, shaxsiy xavfsizlikni ta'minlash
Blokcheyn texnologiyasi	Onlayn shartnomalar (smart contracts) orqali davlat xaridlarida hujjatlarni qalbakilashtirishdan saqlash	Shaffoflik, o'zgartirib bo'lmaydigan yozuvlar orqali firibgarlikni yo'q qilish
QR-kodli xavfsizlik tizimi	Konferensiya yoki imtihonlarga kirishda QR-kodli individual chipta orqali faqat ruxsat etilganlar kiradi	Begona shaxslarning kirishini oldini olish, tartibni ta'minlash
Kiberxavfsizlik treninglari	O'quvchilarga phishing xatlari namunalarini ko'rsatish va ularni qanday aniqlashni o'rgatish	Xabardorlik oshadi, foydalanuvchi firibgar tuzog'iga tushmaslikni o'rganadi



Texnologiya / Yondashuv	Amaliy qo'llanilishi (misol)	Kutilayotgan natija / foydasi
Mobil ilova orqali ogohlantirish	Foydalanuvchi bank kartasidan pul yechilganida yoki noma'lum joydan tizimga kirish bo'lganda, darhol ilova orqali xabarnoma yuboriladi	Mijoz voqeadan tezda xabardor bo'ladi va chora ko'rish imkoniga ega bo'ladi
AI asosidagi video monitoring	Do'konlarda yoki ATM joylarda yuzni aniqlovchi kameralar o'rnatilib, ilgari aniqlangan firibgarlarni avtomatik tanib olish tizimi	Jinoyatchilarni erta aniqlash va nazoratga olish
Foydalanuvchi xulqini tahlil qilish	Onlayn do'konlarda mijoz odatda kitob xarid qilsa-yu, to'satdan qimmatli elektronika buyurtma qilsa — tizim shubhali harakat deb baholaydi	Noodatiy xaridlarni nazorat qilib, firibgarlik ehtimolini kamaytirish
Fake website skanerlari	Maxsus brauzer plaginlari orqali soxta bank sahifalari yoki phishing sahifalar aniqlanadi	Foydalanuvchini aldov sahifalaridan himoya qilish
E-mail autentifikatsiyasi	Har bir tizimga kirishda elektron pochtaga yuboriladigan maxfiy kod orqali kirish (2 bosqichli himoya)	Login ma'lumotlari o'g'irlangan taqdirda ham kirish imkonini bermaslik

Buning uchun texnik vositalar bilan birga, insonlarning raqamli madaniyati, ogohliligi va axborot xavfsizligiga bo'lgan e'tibori ham yuqori bo'lishi zarur.





XULOSA

Axborot texnologiyalarining jadal rivojlanishi nafaqat inson hayotini yengillashtirmoqda, balki turli sohalarda, xususan, firibgarlikka qarshi kurashishda ham samarali vositaga aylanmoqda. Bugungi kunda firibgarlik usullari tobora murakkablashib, raqamli shaklga o'tmoqda. Shunday sharoitda innovatsion texnologiyalardan foydalanish zarurati yanada ortib bormoqda.

Sun'iy intellekt, blokcheyn, biometrik tizimlar, foydalanuvchi xatti-harakatlarini tahlil qilish, phishing va soxta saytlarni aniqlovchi dasturlar orqali firibgarlikni erta bosqichda aniqlash, oldini olish va tezkor chora ko'rish mumkin bo'lmoqda. Xususan, interaktiv o'quv mashg'ulotlari va kiberxavfsizlik bo'yicha treninglar orqali ham aholining raqamli savodxonligini oshirish dolzarb ahamiyat kasb etmoqda.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Jumaev, A. (2021). Axborot texnologiyalarining xavfsizligi: nazariy asoslar va amaliy yondashuvlar. Toshkent: O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi.
2. Tursunov, R. (2019). Kiberxavfsizlik va firibgarlikning oldini olish: metodologiya va amaliyot. Samarqand: Samarqand Davlat universiteti nashriyoti.
3. Mirzaev, B. (2020). Internet firibgarligi va unga qarshi kurashish vositalari. Toshkent: Ma'naviyat va ma'rifat nashriyoti.
4. Qodirov, S. (2022). Raqamli texnologiyalar va ularning firibgarlikka qarshi kurashishdagi ro'li. Buxoro: Buxoro davlat universiteti nashriyoti.