



AXBOROT TEXNALOGIYALARIDAN FOYDALANGAN HOLDA FIRIBGARLIKKA QARSHI KURASHISH

ASAMOV JALOLIDDIN NIZAMETDINOVICH

2007-yil IIV Akademiyasi bitiruvchisi

ANNOTATSIYA: *Axborot texnologiyalari va internetning jadal rivojlanishi bilan birga, firibgarlikning yangi turlari paydo bo'lmoqda. Bugungi kunda, firibgarliklar ko'pincha onlayn platformalarda amalga oshirilmoqda, bu esa ularni aniqlash va oldini olishni murakkablashtirmoqda. Ushbu maqolada, axborot texnologiyalaridan foydalanib firibgarlikka qarshi kurashishning samarali usullari tahlil qilingan. Maxsus dasturiy ta'minotlar, sun'iy intellekt va blokcheyn texnologiyalari orqali firibgarlik holatlarining oldini olish imkoniyatlari ko'rsatilgan. Maqola, axborot xavfsizligini ta'minlash, elektron to'lov tizimlarida firibgarlikning oldini olish va internetda xavfsizlikni oshirish uchun zarur choralarni ishlab chiqishni maqsad qiladi. Bundan tashqari, huquqiy normalar va qonunchilikda amalga oshirilishi kerak bo'lgan o'zgarishlar haqida fikrlar bildirilgan.*

Kalit so'zlar: *Axborot texnologiyalari, firibgarlik, kiberxavfsizlik, sun'iy intellekt, blokcheyn, elektron to'lov tizimlari, axborot xavfsizligi, onlayn firibgarlik, huquqiy himoya, internet xavfsizligi.*

KIRISH

Axborot texnologiyalarining jadal rivojlanishi va internetning keng tarqalishi, global miqyosda turli sohalarda yangi imkoniyatlarni yaratgan bo'lsa-da, bir vaqtning o'zida yangi turdagi xavflarni, xususan firibgarlikni ham keltirib chiqarmoqda. Axborot texnologiyalaridan foydalangan holda amalga oshiriladigan firibgarliklar, an'anaviy firibgarlik usullariga qaraganda ancha murakkab va xavfli



bo‘lib, ko‘plab shaxsiy va tashkilotlar uchun katta xavf tug‘dirmoqda. Ushbu firibgarliklar odatda internet, elektron tijorat, ijtimoiy tarmoqlar, to‘lov tizimlari va boshqa axborot platformalarida amalga oshiriladi.

Firibgarlikka qarshi kurashish borasida axborot texnologiyalari yangiliklari va ilg‘or texnologiyalarni qo‘llashning ahamiyati ortib bormoqda. Bunga sun‘iy intellekt, blokcheyn, va boshqa ilg‘or texnologiyalarning xavfsizlik tizimlarida qo‘llanilishi misol bo‘la oladi. Ushbu maqolada, firibgarlikning oldini olishda axborot texnologiyalarining samarali foydalanishi, ularning xavfsizlikni ta‘minlashdagi roli, shuningdek, firibgarlikni aniqlash va bartaraf etish uchun qo‘llaniladigan vositalar ko‘rib chiqiladi.

Maqolada shuningdek, huquqiy normativ-huquqiy muhit va qonunchilikdagi o‘zgarishlar, firibgarlikni oldini olish uchun davlat va xususiy sektor tomonidan amalga oshirilishi lozim bo‘lgan chora-tadbirlar tahlil qilinadi. Maqsad – axborot texnologiyalaridan foydalangan holda firibgarlikka qarshi samarali kurashish usullarini ishlab chiqish va amaliy tavsiyalar berish.

ASOSIY QISM

Axborot texnologiyalari firibgarlikka qarshi kurashish uchun bir qator innovatsion usullarni taqdim etadi. Ularning samarali qo‘llanilishi nafaqat firibgarlikni aniqlash va oldini olish, balki firibgarliklarni tahlil qilish va ularga qarshi samarali choralar ko‘rishda ham muhim ahamiyatga ega. Quyidagi amaliy misollar axborot texnologiyalarini firibgarlikka qarshi kurashishda qanday kreativ yondashuvlar bilan ishlatilishini ko‘rsatadi:

1. Sun‘iy intellekt va mashina o‘rganish algoritmlari. Sun‘iy intellekt va mashina o‘rganish algoritmlari firibgarlikni aniqlash va oldini olishda juda muhim vositalar hisoblanadi. Masalan, elektron tijorat saytlari va onlayn to‘lov tizimlari, foydalanuvchilarning xaridlarida noan‘anaviy xatti-harakatlarni aniqlash uchun algoritmlardan foydalanadi. Ushbu tizimlar, odatdagi xarid qilish davranishini



tahlil qilib, firibgarlikka o'xshash xatti-harakatlarni (masalan, tez-tez kartalarni almashtirish yoki katta miqdorda mahsulot sotib olish) avtomatik ravishda belgilab, operatsiyalarni bloklashi mumkin. Bu jarayon firibgarlarning tizimga kirib, foydalanuvchi ma'lumotlarini o'g'irlashiga to'sqinlik qiladi.

2. Blokcheyn texnologiyasi. Blokcheyn texnologiyasi firibgarlikka qarshi kurashishda yangi imkoniyatlarni yaratmoqda. Ayniqsa, moliyaviy operatsiyalar va shaxsiy ma'lumotlarni himoya qilishda blokcheynning rolini e'tiborsiz qoldirib bo'lmaydi. Blokcheynning o'ziga xos xususiyati shundaki, har bir tranzaksiya shifrlangan va tarixi o'zgartirilmaydi, bu esa firibgarlikni aniqlash va oldini olish uchun mukammal vosita bo'ladi. Misol uchun, onlayn to'lov tizimlari blokcheynni qo'llash orqali har bir to'lovning kelib chiqish manbasini tekshirish imkoniyatiga ega bo'ladi. Bu firibgarlikning aniqlanishini sezilarli darajada tezlashtiradi.

3. Biometrik autentifikatsiya. Biometrik autentifikatsiya tizimlari, masalan, yuzni tanib olish yoki barmoq izlarini skanerlash, firibgarlikka qarshi kurashishda juda samarali vosita sifatida foydalaniladi. Bu tizimlar foydalanuvchilarning haqiqiylikni tasdiqlashda yordam beradi va ular faqat o'zlari uchun mo'ljallangan xizmatlarga kirish imkoniyatiga ega bo'lishlarini ta'minlaydi. Biometrik ma'lumotlar firibgarlikni oldini olish uchun juda muhim hisoblanadi, chunki ular hech qachon boshqa shaxs tomonidan taqlid qilinishi qiyin.

4. Ijtimoiy tarmoqlarda xavfsizlik tizimlari. Ijtimoiy tarmoqlarda firibgarlikning ko'p uchraydigan turlaridan biri — odamlarni noto'g'ri yoki aldovli reklama orqali chalg'itishdir. Shu sababli, ijtimoiy tarmoqlar foydalanuvchilarni firibgarlikdan himoya qilish uchun avtomatik tizimlar ishlab chiqmoqda. Masalan, Facebook va Instagram kabi platformalar foydalanuvchi faoliyatini tahlil qilib, firibgarlik, spamming yoki phishing xabarlarini aniqlash uchun sun'iy intellektdan foydalanadi. Bu tizimlar tezda soxta reklama yoki firibgar saytlarga havola beruvchi postlarni aniqlaydi va ularga qarshi tegishli choralarni ko'radi.



5. To'lov tizimlarida xavfsizlik va kripto valyutalar. Kripto valyutalar va to'lov tizimlarida xavfsizlikni ta'minlash uchun zamonaviy shifrlash usullari qo'llaniladi. Masalan, PayPal va boshqa onlayn to'lov tizimlari, foydalanuvchilarning moliyaviy ma'lumotlarini himoya qilish uchun ikki faktorli autentifikatsiya tizimidan foydalanadi. Bu foydalanuvchilar o'z hisoblariga faqatgina maxsus kodni kiritish orqali kirishlari mumkin bo'ladi, bu esa firibgarlikni sezilarli darajada kamaytiradi. Kripto valyutalar esa tranzaksiyalarni izlab topishning deyarli imkonsiz bo'lishi sababli, firibgarlikni oldini olishda kuchli vosita hisoblanadi.

6. Tarmoqdagi xavfli manbalarni avtomatik aniqlash. Internetda firibgarlikni oldini olishda xakerlik yoki viruslar orqali amalga oshiriladigan hujumlar ham muhim xavf omili hisoblanadi. Zamonaviy xavfsizlik tizimlari internetdagi xavfli saytlarni va manbalarni avtomatik ravishda aniqlashga yordam beradi. Masalan, biror bir saytdan ko'plab soxta ma'lumotlar yoki zararli dasturlar tarqatilayotganini aniqlash uchun maxsus algoritmlar ishlab chiqiladi. Bu saytlarga kirish taqiqlandi yoki foydalanuvchiga ogohlantirish yuboriladi.

Yuqoridagi misollar axborot texnologiyalaridan firibgarlikka qarshi kurashishda foydalanishning amaliy jihatlaridan ba'zilarini tashkil qiladi. Har bir texnologiya o'ziga xos tarzda firibgarlikni aniqlash, oldini olish yoki minimalizatsiya qilishda samarali bo'lib, butun tizimning xavfsizligini ta'minlaydi. Bu tizimlarni kengroq qo'llash va rivojlantirish firibgarlikni kamaytirishga xizmat qiladi.

Firibgarlikka qarshi kurashish bo'yicha misollar jadval shaklida keltirilgan:

Amaliy Yondashuv	Tavsifi	Qo'llash Sohasi
Elektron pochta filtratsiyasi	Maxsus xavfsizlik dasturlari yordamida shubhali manzillardan kelgan spam va fishing xabarlarini avtomatik saralash va to'g'ridan-to'g'ri "spam"ga o'tkazish.	Tashkiliy elektron aloqa



Amaliy Yondashuv	Tavsifi	Qo'llash Sohasi
QR kodni skanerlashda ogohlantirish tizimi	Foydalanuvchilar telefon orqali noma'lum QR kodni skanerlaganda, brauzer xavfli manba haqida avtomatik ogohlantirish beradi.	Mobil qurilmalar xavfsizligi
CAPTCHA tizimlaridan foydalanish	Saytlarda avtomatlashtirilgan botlar orqali firibgarlikni oldini olish uchun "Men robot emasman" kabi tekshiruvlardan foydalanish.	Ro'yxatdan o'tish va kirish jarayonlari
Vaqt bo'yicha cheklangan kirish tizimi	Moliyaviy va shaxsiy ma'lumotlarga faqat ma'lum vaqtlarda yoki IP manzil asosida kirishga ruxsat berish.	Bank tizimlari, shaxsiy hisoblar
Plastik karta bloklash opsiyasi	Mobil ilovalar orqali foydalanuvchilar o'z kartasini vaqtincha bloklashi yoki faqat onlayn to'lovlarga ruxsat berishini sozlashi mumkin.	Onlayn bank xizmatlari
Xavfsizlik bo'yicha ogohlantiruvchi SMS xizmati	Har qanday to'lov yoki harakatdan so'ng foydalanuvchiga SMS orqali xabarnoma yuboriladi, noto'g'ri holatda tezda chora ko'rish imkonini beradi.	To'lov tizimlari, mobil banklar
Elektron shartnoma tizimi	Raqamli imzo bilan tasdiqlangan shartnomalar orqali firibgarlikning oldi olinadi, chunki har bir imzo maxsus kalit bilan tekshiriladi.	Huquqiy hujjatlar almashinuvi



XULOSA

Firibgarlikka qarshi kurashish zamonaviy jamiyatda dolzarb muammolardan biri hisoblanadi. Axborot texnologiyalari jadal rivojlanayotgan bir paytda, ular nafaqat yangi imkoniyatlar balki firibgarlik holatlarining yangi ko‘rinishlarini ham yuzaga keltirmoqda. Shunday sharoitda, texnologiyalardan to‘g‘ri va oqilona foydalanish, xavfsizlik choralari kuchaytirish, foydalanuvchilarning xabardorligini oshirish eng samarali chora-tadbirlar sifatida namoyon bo‘lmoqda.

Kreativ va amaliy yondashuvlar orqali, masalan, elektron pochta filtratsiyasi, CAPTCHA tizimlari, vaqt bo‘yicha cheklangan kirish, va xavfsizlik ogohlantirish tizimlaridan foydalanish orqali ko‘plab firibgarlik holatlari oldi olinmoqda. Bundan tashqari, ommaviy axborot vositalari va ta’lim muassasalari orqali foydalanuvchilarni muntazam ravishda xabardor qilish ham muhim ahamiyat kasb etadi.

Xulosa qilib aytganda, firibgarlikka qarshi kurashish faqat texnik vositalar bilan emas, balki ongli yondashuv, hamkorlik va doimiy ogohlik orqali amalga oshirilishi lozim. Har bir foydalanuvchi o‘z xavfsizligi uchun mas’uliyatni his qilgan holda harakat qilsa, firibgarlik holatlarini sezilarli darajada kamaytirish mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. To‘laganov, A. (2020). Axborot xavfsizligi va zamonaviy tahdidlar. Toshkent: Fan va texnologiya nashriyoti.
2. G‘oziyev, E. (2019). Kompyuter savodxonligi va axborot texnologiyalari asoslari. Samarqand: SamDU nashriyoti.
3. Shomurodov, M. (2021). Kriminalistika: Firibgarlik turlari va ularni aniqlash usullari. Toshkent: Yuridik adabiyotlar.
4. Karimova, D. (2022). Raqamli xavfsizlik: Firibgarlikka qarshi kurashish yo‘llari. Toshkent: Innovatsiya nashriyoti.