ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ

KIBERMAKONDAGI FIRIBGARLIK TURLARI VA ULARDAN HIMOYALANISHNING ZARURATI, TAJRIBASI, AHAMIYATI

Quvandiqov Shahzod Burxon o‘g‘li
O‘zbekiston Respublikasi Ichki ishlar vazirligi Akademiyasi
2-o’quv kurs 229-guruh kursanti.
Email manzil: *Shahzodshox78@gmail.com Telefon raqam: +998 (94) 142-04-14*
https://doi.org/10.5281/zenodo.20134429

Annotatsiya. *Ushbu maqolada raqamli transformatsiya davrida kibermakonda firibgarlikning rivojlanish tendensiyalari, asosiy turlari va ularning global hamda O‘zbekiston miqyosidagi ko‘lami tahlil qilinadi. Maqolada zamonaviy firibgarlik usullari — Ai-fishing, deepfake texnologiyalari batafsil yoritilgan. Shuningdek, kiberfiribgarlikdan himoyalanishning huquqiy va texnik jihatlari, O‘zbekistonning ushbu sohadagi sa’y-harakatlari o‘rganilgan.*

Maqola yakunida kiberxavfsizlik madaniyatini yuksaltirish va ko‘p bosqichli himoya tizimlarini joriy etish bo‘yicha amaliy tavsiyalar berilgan.

Mavzuning dolzarbligi raqamli iqtisodiyot va masofaviy xizmatlar davrida shaxsiy ma’lumotlar hamda moliyaviy aktivlarning xavfsizligini ta’minlash zarurati bilan belgilanadi.

Tadqiqot davomida kiberxavfsizlik madaniyatini yuksaltirishning ahamiyati asoslab berilgan bo‘lib, nafaqat texnik choralar, balki inson omiliga bog‘liq bo‘lgan profilaktik harakatlar ham ko‘rib chiqiladi.

Bundan tashqari kiberjinoyatlarga qarshi kurashishda xalqaro tajriba va milliy qonunchilik asoslari ko‘rib chiqilib, davlat, xususiy sektor va fuqarolar o‘rtasidagi hamkorlikni kuchaytirish bo‘yicha ilmiy-amaliy tavsiyalar ilgari surilgan. Shuningdek, sun'iy intellektga asoslangan zamonaviy kiberhujumlardan himoyalanishning preventiv (oldini oluvchi) mexanizmlari taklif etiladi.

Kalit so‘zlar: *kiberfiribgarlik, kiberjinoyatchilik, Ai-fishing, deepfake, kiberxavfsizlik, ko‘p bosqichli himoya.*

TYPES OF FRAUD IN CYBERSPACE AND THE NEED, EXPERIENCE AND IMPORTANCE OF PROTECTION AGAINST THEM

Abstract. *This article analyzes the development trends of fraud in cyberspace in the era of digital transformation, its main types and their global and Uzbek scale. The article covers in detail modern fraud methods - phishing, deepfake technologies. It also examines the legal, technical and psychological aspects of protecting against cyber fraud, Uzbekistan's efforts in this area. At the end of the article, practical recommendations are given on improving the culture of cybersecurity and introducing multi-level protection systems.*

The relevance of the topic is determined by the need to ensure the security of personal data and financial assets in the era of the digital economy and remote services. The study substantiates the importance of improving the culture of cybersecurity, and considers not only technical measures, but also preventive actions related to the human factor.

In addition, international experience and national legislative frameworks in combating cybercrime are considered, and scientific and practical recommendations are put forward to strengthen cooperation between the state, the private sector and citizens.

Also, preventive mechanisms for protection against modern cyber attacks based on artificial intelligence are proposed.

Keywords: *cyber fraud, cybercrime, Ai-phishing, deepfake, cybersecurity, multi-level protection.*

ВИДЫ МОШЕННИЧЕСТВА В КИБЕРПРОСТРАНСТВЕ И НЕОБХОДИМОСТЬ, ОПЫТ, ВАЖНОСТЬ ЗАЩИТЫ ОТ НИХ

Аннотация. *В данной статье анализируются тенденции развития мошенничества в киберпространстве в эпоху цифровой трансформации, его основные виды и их глобальный и узбекский масштаб. В статье подробно рассматриваются современные методы мошенничества – ИИ-фишинг, технологии дипфейков. Также изучаются правовые и технические аспекты защиты от кибермошенничества, усилия Узбекистана в этой области. В конце статьи даны практические рекомендации по повышению культуры кибербезопасности и внедрению многоуровневых систем защиты.*

Актуальность темы определяется необходимостью обеспечения безопасности персональных данных и финансовых активов в эпоху цифровой экономики и удаленного обслуживания. В исследовании обосновывается важность повышения культуры кибербезопасности с учетом не только технических мер, но и профилактических действий, связанных с человеческим фактором.

Кроме того, рассматривается международный опыт и национальные законодательные рамки в борьбе с киберпреступностью, а также предлагаются научно-практические рекомендации по укреплению сотрудничества между государством, частным сектором и гражданами. Также предлагаются превентивные механизмы защиты от современных кибератак на основе искусственного интеллекта.

Ключевые слова: *кибермошенничество, киберпреступность, фишинг с использованием ИИ, дипфейки, кибербезопасность, многоуровневая защита.*

KIRISH

XXI asrda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida jamiyat hayotining ko‘plab sohalari raqamli muhitga ko‘chib bormoqda. Internet tarmoqlarining kengayishi, kompyuter texnologiyalari va mobil qurilmalarning ommalashuvi natijasida insonlar o‘rtasidagi aloqa, iqtisodiy munosabatlar, davlat boshqaruvi hamda boshqa ko‘plab jarayonlar virtual muhitda amalga oshirilmoqda.

Ushbu jarayonlar natijasida yangi ijtimoiy muhit – kibermakon shakllandi. Biroq kibermakonning rivojlanishi bilan bir qatorda unda sodir etiladigan noqonuniy harakatlar ham ko‘payib bormoqda. Ayniqsa, internet orqali sodir etiladigan firibgarlik holatlari global muammolardan biriga aylanmoqda. Shu sababli huquqshunoslik va kriminologiya sohalarida “kiberjinoyatchilik” hamda “kiberfiribgarlik” tushunchalari keng qo‘llanilmoqda.

Raqamli iqtisodiyotning jadal rivojlanishi insoniyatga yangi imkoniyatlar eshigini ochgan bo‘lsa-da, bu jarayon kiberjinoyatchilikning ham misli ko‘rilmagan darajada o‘sishiga olib keldi.

Bugungi kunda kibermakondagi firibgarlik nafaqat alohida shaxslar yoki kompaniyalarga, balki butun davlatlarning milliy xavfsizligiga jiddiy tahdid solmoqda.

Cybersecurity Ventures ma’lumotlariga ko‘ra, 2025 yilda global kiberjinoyatlar yetkazadigan zarar yiliga 10,5 trillion AQSh dollariga yetadi — bu ko‘rsatkich global giyohvand moddalar savdosidan oshib ketadi va kiberjinoyatni dunyoning uchinchi yirik “iqtisodiyoti”ga aylantiradi. O‘zbekiston ham ushbu global muammodan chetda qolmayapti. Rasmiy statistikaga ko‘ra, 2024 yilda kiberjinoyatchilar mamlakat fuqarolaridan 603 milliard so‘m o‘g‘irlagan bo‘lsa, so‘nggi uch yillik zarar 1,9 trillion so‘mni tashkil etgan. Eng tashvishlanarli jihati shundaki, ushbu jinoyatlarning 98 foizi bank kartalari bilan bog‘liq firibgarliklardir . Toshkent shahrida esa kiberjinoyatlarning 40 foizdan ortig‘i sodir etilmoqda va jabrlanuvchilarning 80 foizga yaqini 40 yoshdan 80 yoshgacha bo‘lgan aholi qatlamidir .

Mazkur maqolada kiberfiribgarlikning turlari, ularning psixologik va texnologik mexanizmlari, shuningdek, himoyalanishning samarali strategiyalari ilmiy-nazariy jihatdan tahlil qilinadi.

METODOLOGIYA VA MUHOKAMA

So’nggi yillarda kiberjinoyatchilikning eng keng tarqalgan turlaridan biri kiberfiribgarlik hisoblanadi. **Kiberfiribgarlik** deganda internet yoki boshqa axborot texnologiyalari orqali odamlarni aldash, ularning pul mablag‘lari yoki shaxsiy ma’lumotlarini noqonuniy egallashga qaratilgan harakatlar tushuniladi. Bunda firibgarlar turli texnik va psixologik usullardan foydalanib, foydalanuvchilarni yolg‘on ma’lumotlarga ishontirishga harakat qiladilar. Bugungi kunda kiberfiribgarlik ko‘plab shakllarda namoyon bo‘lmoqda.

Masalan, phishing xabarlari yuborish, soxta internet do‘konlari yaratish, bank kartalari ma’lumotlarini qo‘lga kiritish, ijtimoiy tarmoqlar orqali firibgarlik qilish kabi usullar keng tarqalgan. Bunday jinoyatlar nafaqat alohida fuqarolarga, balki banklar, kompaniyalar va davlat tashkilotlariga ham katta zarar yetkazishi mumkin. Shuningdek, kiberjinoyatlar transmilliy xarakterga ega bo‘lib, ularni aniqlash va tergov qilish jarayoni ko‘pincha murakkab kechadi.

Chunki jinoyatchilar boshqa davlat hududida bo‘lishi, anonim texnologiyalardan foydalanishi yoki o‘z faoliyatini yashirish uchun turli texnik vositalardan foydalanishi mumkin. Shu sababli kiberjinoyatchilikka qarshi kurashishda xalqaro hamkorlik, zamonaviy texnologiyalar va huquqiy mexanizmlarning rivojlanishi muhim ahamiyatga ega.

Kiberfiribgarlik oqibatida fuqarolar va tashkilotlar turli yo‘nalishlarda zarar ko‘rishadi.

Avvalo, moliyaviy yo‘qotishlar eng ko‘p uchraydigan zarar turi hisoblanadi — bu bank kartalaridan noqonuniy yechimlar, to‘lov tizimlarida mablag‘larning o‘g‘irlanishi yoki firibgarlik orqali investitsiya yo‘qotishlarida namoyon bo‘ladi. Shu bilan birga, shaxsiy ma’lumotlarning oshkor bo‘lishi, obro‘-e’tiborga putur yetishi, axborot tizimlarining ishlashining izdan chiqishi va ma’lumotlar bazasining buzilishi kabi holatlar ham keng tarqalgan. Tashkilotlar uchun esa bu jarayon nafaqat moliyaviy zarar, balki ishonchni yo‘qotish va mijozlar bilan munosabatlarning yomonlashishiga olib keladi. Bunday jinoyatlarni aniqlash va oldini olishda bir qator muammolar mavjud.

Eng avvalo, kiberjinoyatlar anonim tarzda, ya’ni jinoyatchining shaxsini aniqlash qiyin bo‘lgan muhitda amalga oshiriladi. Shuningdek, texnik izlarni yashirish, VPN yoki dark web kabi vositalardan foydalanish, transchegaraviy xususiyat — ya’ni jinoyat bir davlatda sodir etilib, zarari boshqa davlatda yetkazilishi — tergov jarayonini murakkablashtiradi. Fuqarolarning axborot savodxonligi pastligi ham kiberfiribgarlikka qarshi kurashda muhim to‘siq bo‘lib qolmoqda.

Kiberfiribgarlikning zamonaviy turlaridan biri **AI-phishing** — bu kiberfiribgarlikning yangi shakli bo‘lib, sun’iy intellekt (AI) texnologiyalaridan foydalanib, sun’iy intellekt yordamida tayyorlangan phishing xabarlari bo‘lib, ular oddiy phishing xabarlariga qaraganda ancha murakkab va ishonchli ko‘rinadi hamda insonlarga aldashga yo’naltirilgan bo’ladi. Sun’iy intellekt foydalanuvchilarning ijtimoiy tarmoqlardagi faoliyati, ochiq ma’lumotlari va yozishmalarini tahlil qilib, ularga moslashtirilgan xabarlar yaratishi mumkin.

Natijada foydalanuvchi ushbu xabarni haqiqiy deb qabul qiladi va o‘zining maxfiy ma’lumotlarini firibgarlarga taqdim etadi. An’anaviy phishing elektron pochta yoki SMS orqali amalga oshirilsa, AI-phishingda firibgarlar generativ AI modellar, deepfake texnologiyalari, shaxsiylashtirilgan chatbotlar va ovozli imitatorlar yordamida shaxsni aldaydi. AI-phishingning asosiy xususiyati shundaki, u foydalanuvchining xulq-atvori, yozuv uslubi va ijtimoiy tarmoq faolligini tahlil qilgan holda maksimal realistik xabar yoki qo‘ng‘iroq yaratadi. Shu bilan birga, firibgarlar odatda foydalanuvchini shoshilinch choralar ko‘rishga undashadi, bu esa odamni yanada sezgir qilmasdan aldash imkonini beradi. Bundan tashqari, zamonaviy kiberfiribgarlik usullari qatoriga soxta internet do‘konlari yaratish, kriptovalyuta orqali firibgarlik qilish, zararli dasturlar yordamida bank ma’lumotlarini o‘g‘irlash kabi usullar ham kiradi. Ushbu usullar texnologiyalarning rivojlanishi bilan birga doimiy ravishda takomillashib bormoqda.

AI-Phishingning amalga oshirilish mexanizmlari:

1. *Ma’lumot yig’ish (Reconnaissance)* – xakker avval muayyan shaxs haqida ochiq manbalardan ma’lumot yig’adi, ijtimoiy tarmoqlar, kompaniya saytlari, e-mail manzillari, ish joyi va lavozim, AI bu ma’lumotlarni tez tahlil qilib profil yaratadi.
2. *AI orqali ishonchli xabar yaratish* – Sun’iy intellekt yordamida juda real ko’rinadigan xabarlar yoziladi. Masalan, bankdan kelgandek e-mail kompaniya direktori yozgandek xabar do’st yoki hamkasbidan kelgandek SMS AI grammatik jihatdan mukammal va shaxsga mos matn yaratadi.
3. *Soxta sahifa yaratish* – xakker asl saytga o’xshagan fake (soxta) login sahifasi yaratadi. Masalan, bank sayti Instagram login sahifasi electron pochta login sahifasi va boshqalar. Agarda ushbu linkni bosilganda asl saytga o’xshagan sahifa ochiladi.
4. *Shaxsni ishontirish* – AI yozgan xabar odatda shoshilinchlilik hissini beradi. Misollar, “Akkauntingiz bloklandi”, “Parolni zudlik bilan tasdiqlang”, “To’lovni tasdiqlang”. Shunda odam o’ylamay login yoki karta ma’lumotlarini kiritadi.
5. *Ma’lumotlarni o’g’irlash* – Biror bir odam login yoki karta ma’lumotlarini kiritganda ma’lumotlar hujumchi serveriga yuboriladi. Keyin hujumchi akkauntiga kiradi yoki pulni o’g’irlaydi.
6. *AI yordamida avtomatlashtirish* – AI quyidagilarni avtomatlashtiradi: minglab phishing xabarlarni yaratish, qaysi xabar ishlayotganini tahlil qilish, odamlarni segmentlash. Shuning uchun AI phishing oddiy phishingdan ancha xavfli.

AI-Phishingning turlari:

1. *Generativ matn orqali phishing* - AI modellaridan foydalangan holda, firibgarlar foydalanuvchiga juda haqiqiy ko‘rinadigan elektron pochta xabarlari yuboradi. Masalan, bank, kompaniya yoki davlat organi nomidan yuborilgan xabarda foydalanuvchidan login, parol yoki kredit karta ma’lumotlari so‘raladi.

2. *Deepfake ovozli phishing* - Firibgarlar taniqli shaxslar yoki kompaniya rahbarlarining ovozini imitasiya qiluvchi AI dasturlarini ishlatadi. Telefon qo‘ng‘irog‘i orqali foydalanuvchini moliyaviy operatsiya yoki shaxsiy ma’lumotlarni berishga ishontirishadi.

3. *Deepfake video phishing* - Video orqali CEO yoki yuqori lavozimli shaxsning yuzini va harakatlarini soxtalashtirish orqali, xodimlarni soxta buyruqlarni bajarishga majbur qilishadi.

4. *Shaxsiylashtirilgan phishing* - Foydalanuvchining ijtimoiy tarmoqdagi faolligi, odatlari va yozuv uslubini tahlil qilib, individual tarzda aldaydigan xabarlar yaratish imkonini beradi.

So‘nggi yillarda sun’iy intellekt texnologiyalarining rivojlanishi kiberfiribgarlikning yanada murakkablashishiga sabab bo‘ldi. Ayniqsa deepfake texnologiyasi firibgarlik uchun yangi imkoniyatlar yaratmoqda. **Deepfake** – bu sun’iy intellekt yordamida yaratilgan soxta video yoki audio yozuv bo‘lib, unda ma’lum bir shaxsning tasviri yoki ovozi juda real ko‘rinishda aks ettiriladi. Bunday texnologiya yordamida firibgarlar mashhur shaxslar, davlat arboblari yoki tashkilot rahbarlari nomidan soxta videomurojaatlar yaratishlari mumkin. Deepfake texnologiyasi asosan mashinaviy o‘rganish (machine learning) va chuqur o‘rganish (deep learning) algoritmlariga asoslanadi. Maxsus dasturlar yordamida ma’lum bir shaxsning ko‘plab foto va video materiallari tahlil qilinadi va ular asosida sun’iy model yaratiladi. Keyinchalik ushbu model boshqa video yoki audio materiallarga qo‘llanilib, haqiqiydek ko‘rinadigan soxta tasvir yoki ovoz hosil qilinadi. Shu sababli deepfake texnologiyasi orqali yaratilgan materiallarni oddiy foydalanuvchilar uchun aniqlash juda qiyin bo‘lishi mumkin. Dastlab deepfake texnologiyasi kino sanoati, reklama va ko‘ngilochar sohalarda qo‘llanilgan. Masalan, filmlarda tarixiy shaxslarning tasvirlarini qayta tiklash yoki aktyorlarning yoshini sun’iy ravishda o‘zgartirish uchun ushbu texnologiyadan foydalanilgan. Biroq vaqt o‘tishi bilan ushbu texnologiya kiberjinoyatchilar tomonidan ham qo‘llanila boshladi.

Kiberfiribgarlikda deepfake texnologiyasidan foydalanish turli shakllarda namoyon bo‘lishi mumkin. Masalan, firibgarlar kompaniya rahbarining ovoziga o‘xshash sun’iy audio yozuv yaratib, xodimlarga favqulodda vaziyat bahonasida pul o‘tkazishni buyurishi mumkin.

Bunday holatlar amaliyotda bir necha bor kuzatilgan bo‘lib, natijada kompaniyalar katta miqdorda moliyaviy zarar ko‘rgan. Bundan tashqari, deepfake videolar orqali mashhur shaxslar yoki davlat arboblari nomidan soxta murojaatlar tarqatilishi ham mumkin. Masalan, firibgarlar mashhur insonning videosini sun’iy ravishda yaratib, unda investitsiya loyihalariga pul tikishga chaqiruvchi soxta reklama joylashtirishlari mumkin. Bunday videolar ko‘pincha ijtimoiy tarmoqlarda keng tarqalib, ko‘plab foydalanuvchilarni chalg‘itadi.

Deepfake amalga oshirilish mexanizmlari:

1. *Ma’lumotlarni yig‘ish (Data Collection)* - Deepfake yaratishning birinchi bosqichi kerakli shaxsga oid rasm, video yoki audio materiallarni yig‘ish hisoblanadi. Sun’iy intellekt modelini o‘qitish uchun odatda bir insonning yuz ifodalari, turli burchaklardan olingan suratlari va videolari kerak bo‘ladi. Qanchalik ko‘p ma’lumot yig‘ilsa, deepfake natijasi shunchalik real ko‘rinadi.

2. *Ma’lumotlarni tahlil qilish va tayyorlash (Data Processing)* - Yig‘ilgan ma’lumotlar maxsus algoritmlar yordamida qayta ishlanadi. Bu jarayonda dastur yuz shakli, mimika, ko‘z harakati, lab harakati va boshqa biometrik xususiyatlarni aniqlaydi. Shu orqali sun’iy intellekt modeliga inson yuzining asosiy strukturasi o‘rgatiladi.

3. *Yuzni almashtirish yoki sintez qilish (Face Swapping / Synthesis)* - Model o‘qitilgandan so‘ng, dastur bir insonning yuzini boshqa insonning videosiga joylashtirishi mumkin. Bunda yuz ifodalari, lab harakati va mimikalar avtomatik ravishda moslashtiriladi. Natijada video juda real ko‘rinadi.

4. *Video yoki audio montaj qilish (Post-processing)* - Yakuniy bosqichda video yoki audio materialga qo‘shimcha tahrirlar kiritiladi. Masalan, ranglarni moslashtirish, ovozni sinxronlashtirish, fonni moslashtirish. Bu jarayon deepfake materialining yanada ishonchli ko‘rinishini ta’minlaydi.

Deepfake uchun milliy qonunchiligimizdagi javobgarlik masalasiga to’xtaladigan bo’lsak, O’zbekiston Respublikasi Ma’muriy javobgarlik to’g’risidagi kodeksning 46^2-moddasi 2-qismiga muvofiq Sun’iy intellekt texnologiyalaridan foydalangan holda shaxsga doir ma’lumotlarga qonunga xilof ravishda ishlov berish, ularni ommaviy axborot vositalarida, telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog’ida tarqatganlik uchun ma’muriy huquqbuzarlikni sodir etish qurollari musodara qilinib, bazaviy hisoblash miqdorining 50 baravaridan 100 baravarigacha miqdorda jarima belgilab qo’yilgan.

Xorij tajribasi va Himoyalanish zarurati

Buyuk Britaniya modeli: Jabrlanuvchilarni himoya qilish modeli ya’ni kiberfiribgarlikka qarshi kurashda iste’molchilarni kompensatsiya qilishga e’tibor qaratgan:

1. *Bank protokoli (Banking Protocol)* — bank xodimlari mijoz firibgarlik qurboni bo‘layotganini sezsa, politsiyaga murojaat qiladi va tranzaksiyani to‘xtatadi. Natijada £374 million zararning oldi olingan, 68,000+ politsiya chaqiruvi amalga oshirilgan.

2. *APP to‘lovlari uchun majburiy qaytarib berish* — 2024-yil oktabrdan boshlab, banklar firibgarlik qurboni bo‘lgan mijozlarga £85,000 gacha pulni 5 ish kuni ichida qaytarishi shart.

3. *"To‘xta, o‘yla, himoya qil" (Take Five to Stop Fraud) kampaniyasi* — keng qamrovli aholini xabardor qilish dasturi .

4. *Onlayn xavfsizlik qonuni (Online Safety Act 2023)* — ijtimoiy tarmoqlar va qidiruv tizimlarini firibgar kontentni olib tashlamaganlik uchun global daromadning 10% gacha jarimaga tortish imkoniyati.

Avstraliya modeli: Oldini olishga yo‘naltirilgan yondashuv ya’ni profilaktikaga ustuvor ahamiyat beradi:

1. *Milliy firibgarlikka qarshi markaz (NASC)* — banklar, telekom va raqamli platformalar uchun majburiy majburiyatlar belgilangan.

2. *Firibgarlikning oldini olish bo‘yicha tizim (SPF)* — uch sektor (bank, telekom, texnologiya platformalari) uchun qonuniy javobgarlik joriy etilgan .

3. *Real vaqtda ma’lumot almashish* — tarmoqlararo tezkor razvedka almashinuvi tizimi.

Xalqaro tajriba asosida O‘zbekistonda quyidagi choralarni kuchaytirish muhim:

1. *Milliy firibgarlikka qarshi markaz tashkil etish* — banklar, telekom va IT-sektor o‘rtasida muvofiqlashtirishni ta’minlash

2. *Aholini muntazam xabardor qilish kampaniyalari* — maktab dasturlaridan tortib, ommaviy axborot vositalarigacha

3. *Banklar va telekom operatorlari uchun majburiy javobgarlik* — firibgarlikning oldini olish bo‘yicha standartlar joriy etish

4. *Xalqaro hamkorlikni kengaytirish* — INTERPOL, FATF va UNDP dasturlarida faol ishtirok etish
5. Sun’iy intellekt asosida ishlaydigan monitoring tizimlarini joriy etish

Ko‘p bosqichli himoya texnologiyalari

Zamonaviy kiberxavfsizlikning asosiy tamoyili — bir necha himoya bosqichlarining kombinatsiyasi. An’anaviy parolga asoslangan autentifikatsiya bugungi kunda yetarli emas. Veriff kompaniyasining 2025 yilgi tadqiqotiga ko‘ra, AQSh kompaniyalarining 72 foizi so‘nggi yilda firibgarlik hujumlari sonining oshganini qayd etgan. Samarali himoya tizimi quyidagi elementlarni o‘z ichiga oladi:

Biometrik autentifikatsiya — yuz, barmoq izi yoki ovozni tanish texnologiyalari.

Zamonaviy “liveness detection” (jonlilikni aniqlash) tizimlari haqiqiy foydalanuvchini uning fotosurati, video yoki 3D-maskasidan farqlay oladi .

Ko‘p bosqichli autentifikatsiya (MFA) — kamida ikki xil autentifikatsiya usulini talab qilish (masalan, parol + bir martalik SMS-kod yoki biometrik tekshiruv).

Xulq-atvorni tahlil qilish — foydalanuvchining klaviatura bosish dinamikasi, sichqoncha harakatlari, geolokatsiyasi kabi xususiyatlarini tahlil qilish. Ushbu tizimlar autentifikatsiyadan so‘ng ham foydalanuvchi xatti-harakatlarini doimiy ravishda monitoring qiladi va anomaliyalarni aniqlaydi .

AI asosida ishlaydigan fraud-deteksiya — 64 foiz kompaniyalar sun’iy intellektdan firibgarlikni aniqlashda foydalanmoqda, yana 20 foizi esa keyingi 12 oy ichida joriy etishni rejalashtirmoqda.

XULOSA

Kibermakondagi firibgarlik bugungi kunda insoniyat oldida turgan eng jiddiy xavflardan biriga aylandi. Global iqtisodiyotga yetkaziladigan zararning yiliga 10,5 trillion dollarga yetishi, bu muammoga qarshi kurashni nafaqat alohida shaxslar yoki kompaniyalar, balki butun xalqaro hamjamiyatning ustuvor vazifasiga aylantirmoqda. O‘zbekiston ushbu global muammoga qarshi kurashda muhim qadamlar qo‘ymoqda.

Huquqiy asoslarni mustahkamlash, texnik infratuzilmani rivojlantirish, xalqaro hamkorlikni kengaytirish va kibermadaniyatni yuksaltirish bo‘yicha amalga oshirilayotgan chora-tadbirlar ijobiy natijalar bermoqda. Kiberfiribgarlikdan himoyalanish texnik vositalar va huquqiy mexanizmlarning kombinatsiyasini talab qiladi. Parol xavfsizligi, ikki faktorli autentifikatsiya, dasturiy ta’minotni yangilash kabi oddiy qoidalarga rioya qilish, shuningdek, psixologik barqarorlikni shakllantirish har bir fuqaroning shaxsiy mas’uliyatidir.

Faqatgina texnik va psixologik himoyaning uyg‘unlashuvi kibermakonda xavfsiz faoliyat yuritish imkonini beradi. Biroq, kiberxavfsizlik sohasidagi ishlarni yanada kuchaytirish, ayniqsa aholining keksa qatlami va yoshlar o‘rtasida tushuntirish ishlarini olib borish, doimiy monitoring tizimlarini takomillashtirish zarur.

ADABIYOTLAR RO‘YXATI

1. Entrust. (2025). 2026 Identity Fraud Report. Business Wire.
2. World Economic Forum. (2025). Fighting Cyber-Enabled Fraud: A Systemic Defence Approach.

3. VOV. (2025). Cross-border fraud crime: global threat in the digital age.
4. Prawitasari, P.P. (2025). Fraud In The Digital Age: Assessing Cybercrime Through The Lens of The Fraud Hexagon. Journal of Accounting and Finance, 9(2).
5. LexisNexis Risk Solutions. (2026). Cybercrime Report.
6. FinTech Magazine. (2025). Multi-Layered Defence: Fraud Prevention in Digital Finance.
7. Gazeta.uz. (2025). “Kiberjinoyatlarning 40 foizdan ortig‘i Toshkent shahriga to‘g‘ri kelyapti” — poytaxt IIBB.
8. Cybersecurity Ventures. (2025). Cybercrime Is The Greatest Transfer Of Economic Wealth In History.
9. Anorboyev A.U Kiberjinoyatchilik, unga qarshi kurashish muammolari va kiberxavfsizlikni ta‟minlash istiqbollari. Monografiya – T.: Milliy gvardiya instituti, 2020. – 324 b.
10. Salayev N.S., Ro‟ziyev R.N Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya ., – T.: TDYU, 2018, 139-b