O‘ZBEKISTON RESPUBLIKASI
MARKAZIY BANKI

Bank va to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda shubhali (frod) operatsiyalarni oldini olish bo‘yicha Markaziy bank “CERT-CBU” kiberxavfsizlik markazi tomonidan 2024-yilda amalga oshirilgan ishlar

CERT-CBU
KIBERXAVFSIZLIK MARKAZI

Toshkent 2025

01 Markaziy bank “CERT-CBU” kiberxavfsizlik markazi

CERT-CBU
KIBERXAVFSIZLIK MARKAZI

O‘zbekiston Respublikasi Prezidentining 2021-yil iyuldagi tegishli qaroriga muvofiq Markaziy bank to‘lov tizimi operatorlari, kredit va to‘lov tashkilotlari faoliyatida kiberxavfsizlik tahdidlarini aniqlash, ularni oldini olish hamda ularga qarshi ta’sirchan choralar ko‘rish bo‘yicha muvofiqlashtiruvchi organ etib belgilandi.

Shu bilan birga, Markaziy bank markaziy apparati tarkibiy tuzilmasida Markaziy bank “CERT-CBU” kiberxavfsizlik markazi (keyingi o‘rinlarda – Markaz) tashkil etildi.

Markazning asosiy vazifalari:

- Muhim axborot infratuzilmasi obyektlarini aniqlash hamda ularning reestrini shakllantirish va kiberxavfsizlikni ta’minlash bo‘yicha talablar ishlab chiqish.
- Axborot tizimlari va resurslari hamda muhim axborot infratuzilmasi obyektlarini kiberxavfsizlik talablariga muvofiqligi yuzasidan ekspertizadan o‘tkazish.
- Axborotlashtirish obyektlari hamda muhim axborot infratuzilmasi obyektlarida kiberxavfsizlik holati va ularning uzluksiz ishlashini ta’minlash bo‘yicha monitoring ishlarini olib borish.
- Axborotlashtirish obyektlarini axborot xavfsizligi auditi hamda attestatsiyadan o‘tkazish (vakolatli organ tomonidan tegishli ruxsatnoma olgan holda).
- Axborot tizimlari va resurslarida sodir bo‘lgan kiberxavfsizlik hodisalari oqibatlarini bartaraf etilishini nazorat qilish.
- Kiberxavfsizlikni ta’minlash sohasidagi vakolatli organ hamda boshqa huquqni muhofaza qiluvchi organlar, vazirlik va idoralar, xalqaro tashkilotlar bilan hamkorlikni yo‘lga qo‘yish.
- Axborot xavfsizligi va kiberxavfsizlik hodisalari, xatarlarini aniqlash.
- Axborot xavfsizligi va kiberxavfsizlik hodisalarni oldini olish maqsadida zaruriy ta’sir choralarini ko‘rish bo‘yicha ko‘rsatmalar berish.
- Chet el tashkilotlarining axborot xavfsizligi va kiberxavfsizlik bo‘yicha tegishli bo‘linmalari, CERT xizmatlari bilan hamkorlik qilish.

02 Kiberxavfsizlikni ta’minlash hamda shubhali (frod) operatsiyalarni oldini olish bo‘yicha ishlab chiqilgan normativ-huquqiy hujjatlar

- O‘zbekiston Respublikasining “Kiberxavfsizlikni ta’minlash sohasidagi qonunchilik takomillashtirilishi munosabati bilan O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartirish va qo‘shimchalar kiritish to‘g‘risida”gi O‘RQ-964-son (2024-yil 20-sentabr) Qonuni.

- Markaziy bank boshqaruvining “To‘lov tizimlari operatorlari va to‘lov xizmatlarini yetkazib beruvchilarning to‘lov tizimlarida axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda raqamli texnologiyalar vositasida sodir etiladigan huquqbuzarliklarni oldini olish choralarini ko‘rish to‘g‘risida”gi qarori (ro‘yxat raqami 3513, 2024-yil 21-maydagi).

- Markaziy bank Bank nazorati qo‘mitasining 2024-yil 24-sentabrdagi “Onlayn kredit (mikroqarz) rasmiylashtirish orqali fuqarolarning pul mablag‘larini noqonuniy o‘zlashtirish holatlarini oldini olish choralarini ko‘rish to‘g‘risida”gi qarori.

03 Hamkorlik aloqalari

Vazirlik va idoralar

- KIBERXAVFSIZLIK MARKAZI
- O'ZBEKISTON RESPUBLIKASI MUDOFAA VAZIRLIGI
- O'ZBEKISTON RESPUBLIKASI ICHKI ISHLAR VAZIRLIGI
- O'ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI
- CENTRAL ASIAN FINTECH ASSOCIATION

Xalqaro tashkilotlar

- ROSSIYA MARKAZIY BANKI
- VISA
- MASTERCARD
- KASPERSKY LAB KZ
- FINANCIAL SECURITY INSTITUTE
- TREND MICRO INC
- GROUP-IB
- ELINC CHINA CO. LTD
- CHECKPOINT
- HUNEED TECHNOLOGIES CO
- SOTERYAN LLC

2024-yilda Markaziy bank va **Soteryan LLC** xalqaro tashkiloti o‘rtasida kiberxavfsizlik masalalarida tajriba almashish hamda kibertahdidlarni aniqlash, oldini olish va yangi turlariga qarshi kurashish bo‘yicha anglashuv memorandumi imzolandi.

Shuningdek, 2024-yil oktabr oyida kiberxavfsizlik sohasidagi yangi yechimlar ustida hamkorlikda ishlashni qo‘llab-quvvatlash hamda kiberhujumlar yuz berganda a’zo tashkilotlarga yordam ko‘rsatish maqsadida tashkil etilgan **OIC-CERT** hamda 2024-yil dekabr oyida fishinga qarshi kurashish bo‘yicha **APWG** xalqaro tashkilotlar a’zoligiga qabul qilindi.

Soxta qo‘ng‘iroq

Firibgar dastlab fuqaro to‘g‘risidagi ma’lumotlarni to‘plab, ijtimoiy muhandislik usullarini qo‘llagan holda fuqarolar bilan bog‘lanib, ularning soddaligi hamda raqamli moliyaviy savodxonlik darajasi yetishmasligidan foydalanib, avvaldan ishlab chiqilgan ssenariy asosida bank kartalaridagi mablag‘larni o‘g‘irlashning uddasidan chiqmoqda.

Shubhali havola

Ijtimoiy tarmoqlarda firibgarlar tomonidan tijorat banklari, to‘lov tashkilotlari va boshqa davlat tashkilotlari nomi ostidagi shubhali (soxta) havolalar tarqatilmoqda. Mazkur havolalar foydalanuvchini “fishing” saytga yo‘naltirib, fuqarolarning shaxsga doir hamda bank karta ma’lumotlarini olish vazifasini bajaradi.

Zararli ilovalar

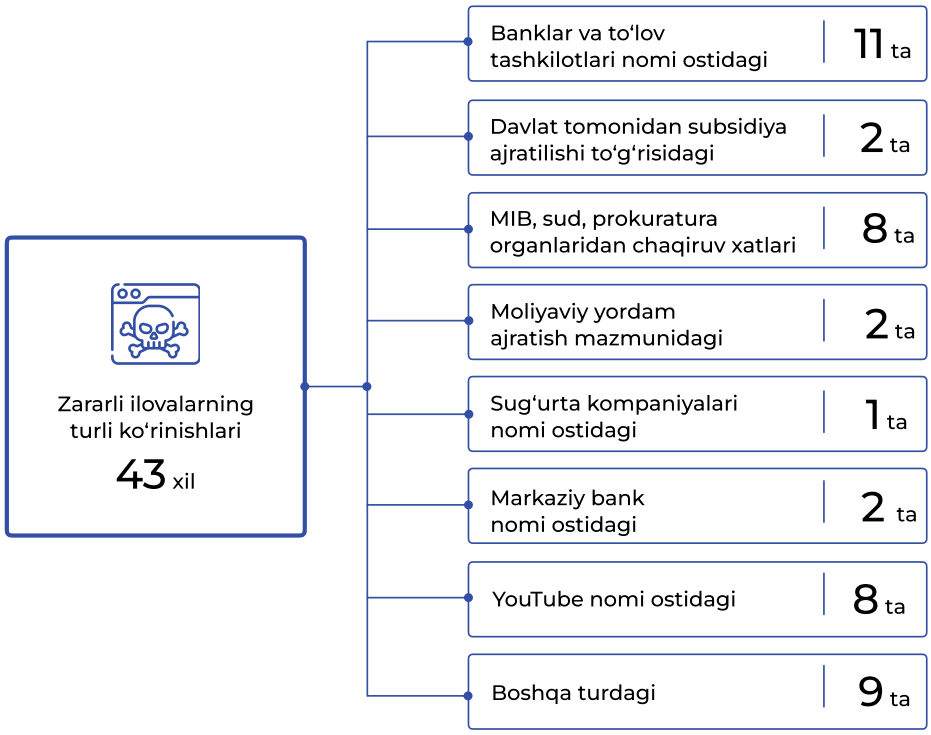
Zararli ilovalar “RAT (Remote Access Trojan) - masofadan boshqariluvchi troyan” sinfiga mansub bo‘lib, tajovuzkorga ilova o‘rnatilgan smartfondagi texnik parametrlar, SMS-xabarlar va boshqa turdagi axborotni masofadan olish imkonini beradi.

“Deepfake” videolar

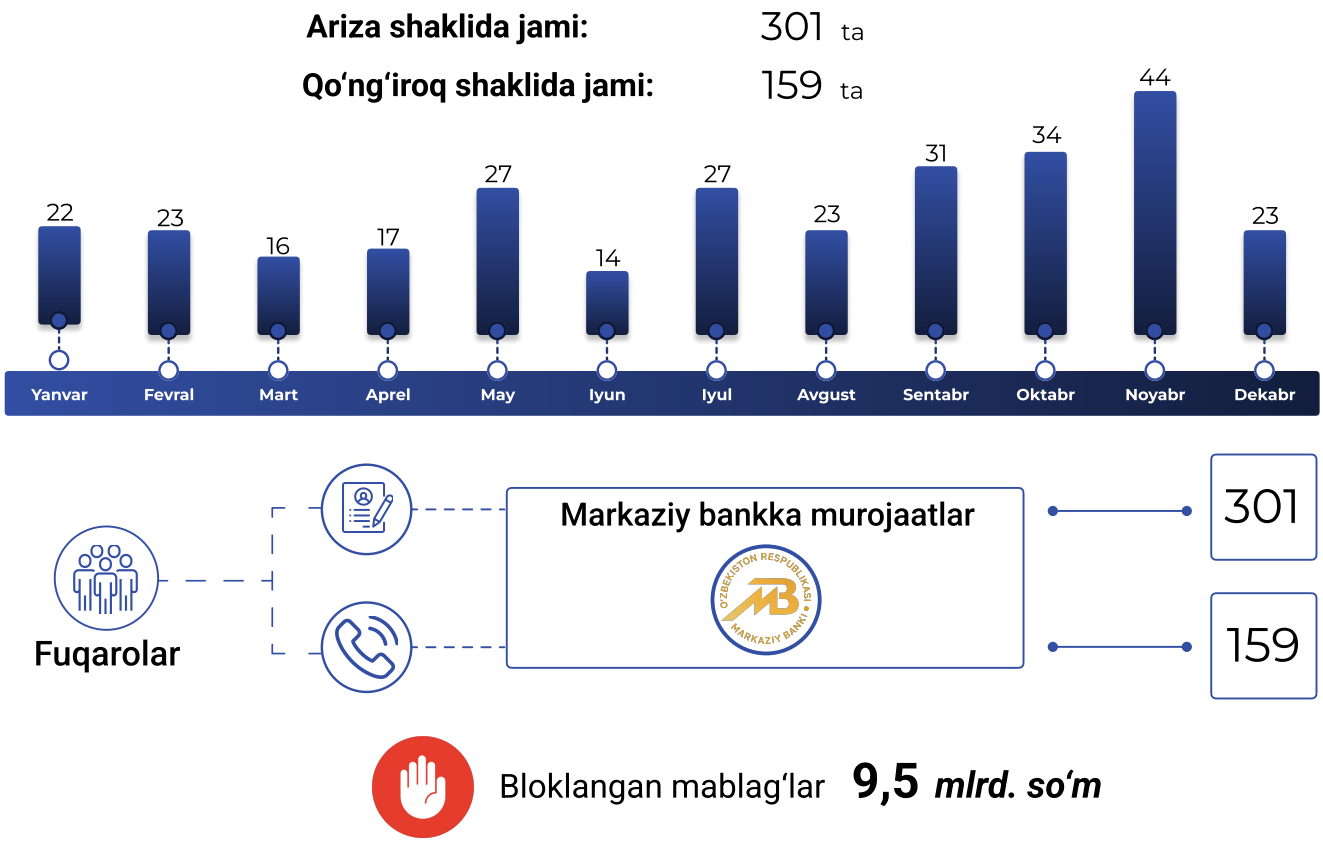
Firibgarlar fuqarolarning ishonchiga kirish uchun sun’iy intellekt texnologiyalari yordamida soxtalashtirilgan videolardan foydalanishmoqda. Bunda firibgarlar mashhur shaxslarning internet tarmog‘idagi rasmlaridan foydalangan holda “oson yo‘l bilan pul topish”, “xayriya puli”, “davlat rahbari tomonidan bir martalik yordam”, “bola puli” kabi mavzularda soxta havolalar yaratib, ijtimoiy tarmoqlar orqali tarqatishmoqda.

Ushbu videomateriallarga ishongan fuqarolarimiz taqdim etilgan soxta havolalarga o‘zining shaxsga doir hamda bank karta ma’lumotlarini qoldirmoqda.

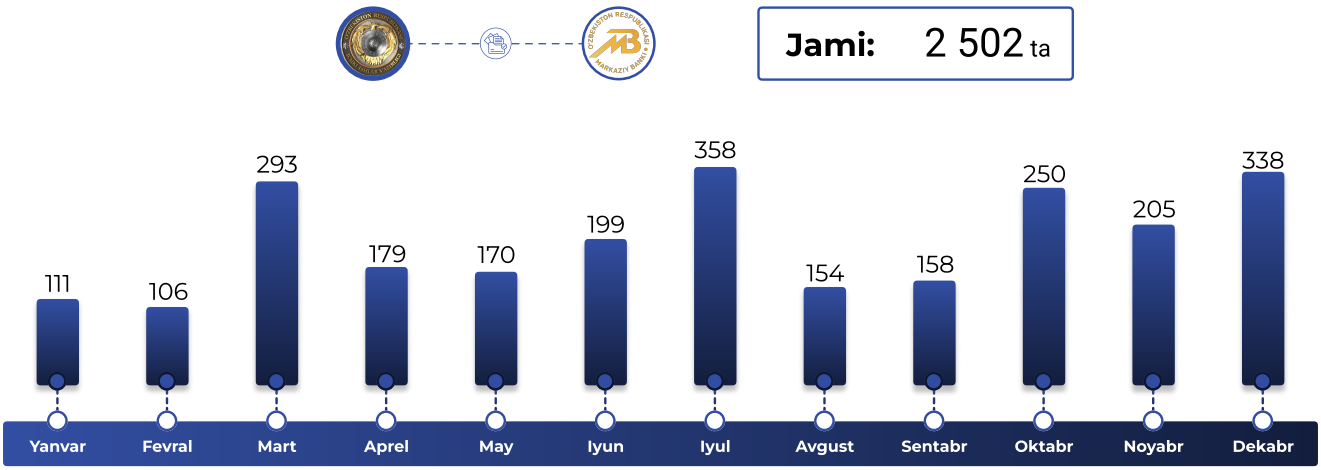
Firibgarlar tomonidan ijtimoiy tarmoqlarda tarqatilgan zararli ilovalar



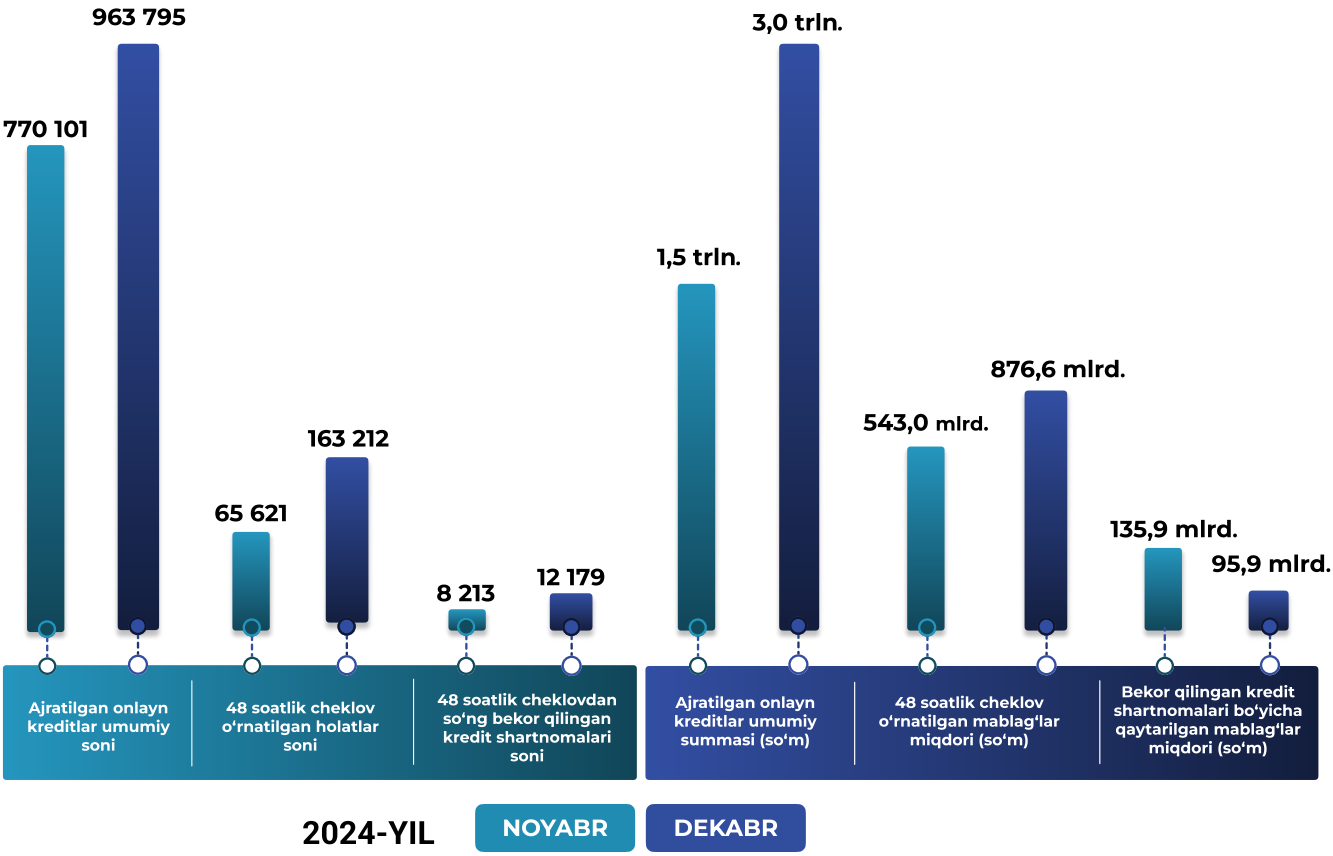
2024-yilda Markaziy bankka fuqarolar tomonidan bank kartalari bilan bog‘liq firibgarlik holatlari to‘g‘risida kelib tushgan murojaatlar statistikasi



2024-yilda Markaziy bankka huquqni muhofaza qiluvchi organlardan bank sirini tashkil etuvchi ma’lumotlarni qonunchilikka muvofiq olish bo‘yicha kelib tushgan murojaatlar statistikasi



05 Onlayn kredit rasmiylashtirish bilan bog‘liq firibgarlik holatlarining oldini olish bo‘yicha amalga oshirilgan ishlar natijalari

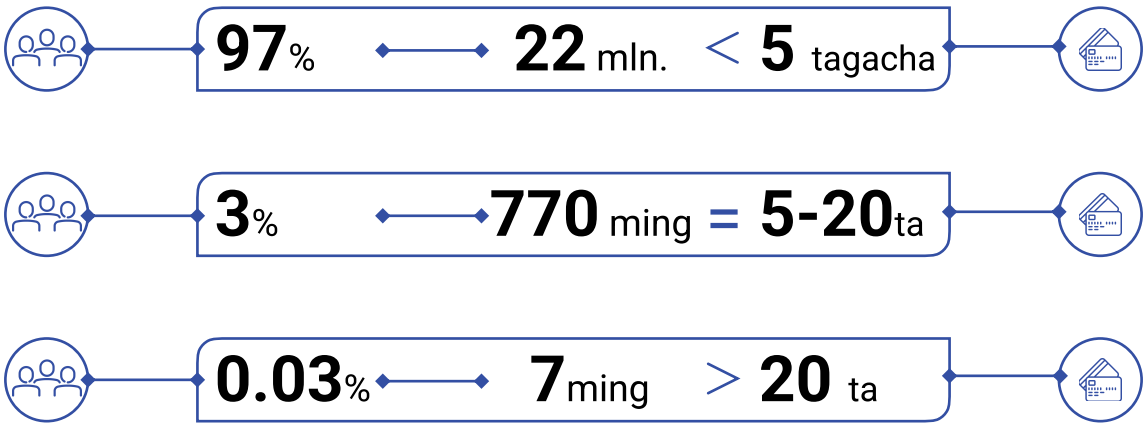


Markaziy bank tomonidan firibgarlik holatlarini bartaraf etish maqsadida jismoniy shaxslarga onlayn kredit (mikroqarz) ajratishda kredit tashkilotlari **2024-yil 1-noyabrdan - 2025-yilning 1-apreliga** qadar amal qiladigan Vaqtinchalik tartib belgilangan.

Bugungi kunda, Vaqtinchalik tartibda belgilangan talablarga muvofiq **12 ta tijorat bank**i hamda **1 ta mikromoliya tashkiloti** mobil ilovalari orqali fuqarolarga onlayn kredit ajratish yo‘lga qo‘yilgan.

Shuningdek, 2025-yil yanvar va fevral oylarida fuqarolar kredit olishga arizani firibgarlar ta’sirida berib, **48 soat davomida** qo‘shimcha tasdiqdan o‘tmaganliklari hamda kredit mablag‘lari sarflanmaganligi sababli jami **316,1 mlrd. so‘m** miqdoridagi mablag‘lar kredit tashkilotlari hisobiga qaytarildi.

06 Firibgarlik sxemalarida bank kartalari ishtirokini kamaytirish



Tahlillar natijasiga ko‘ra, bir tijorat bankining o‘zida jismoniy shaxslar nomiga **30 tadan – 651 tagacha** bo‘lgan an’anaviy va virtual bank kartalar emissiya qilinganligi aniqlandi. Bunda, bir fuqaro nomida **377 tagacha** faol bank kartasi mavjudligi aniqlandi.

Bundan tashqari, internet tarmog‘ida ommalashgan investitsion loyihalar niqobi ostidagi platformalarda 67 nafar shaxsning 1 626 ta bank kartasidan foydalanilayotganligi hamda 24 nafar shaxsning 715 ta bank kartasi internet orqali faoliyat ko‘rsatayotgan “**TradeZone AI**”, “**Consulting Control Session**”, “**Scode Capital**” kabi moliyaviy piramida alomatlariga ega platformalarda pul o‘tkazmalarini amalga oshirish uchun foydalanilayotganligi ma’lum bo‘ldi.

Endilikda, O‘zbekiston Respublikasi hududidagi barcha tijorat banklari tomonidan bir nafar mijoz nomiga virtual va kobeyjing kartalarini inobatga olgan holda ko‘pi bilan jami 20 dona bank kartasi, bitta bankda esa 5 tacha bank kartasi emissiya qilinishi mumkin.

Ushbu talab **chet el valyutasida ochilgan** bank kartalariga tatbiq etilmaydi.

07 Bank va to‘lov tizimi xodimlarining bilim va malakasini oshirish

O‘tgan 2024-yil davomida Markaziy bank tomonidan tijorat banklari hamda vendor tashkilotlar bilan hamkorlikda banklar, to‘lov tizimi operatorlari va to‘lov tashkilotlarining axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda bank kartalari bilan ishlash yo‘nalishida faoliyat olib boruvchi 350 dan ziyod xodimlar uchun o‘quv-seminarlar tashkil etildi.

Shuningdek, 2024-yilda axborot xavfsizligi va kiberxavfsizlikni ta’minlash hamda kiberxavfsizlik bilan bog‘liq risklarni baholash va boshqarish mavzulari bo‘yicha Markazning 15 nafar xodimi AQSh, Avstriya, Malayziya, Ozarbayjon, Xitoy Xalq Respublikasi, Birlashgan Arab Amirligi va Rossiya Federatsiyasida tashkil etilgan seminar hamda o‘quv kurslarida qatnashib o‘z bilim va malakalarini oshirishdi.

08 2025-yilda kutilayotgan trendlar

2025-yilda jahon miqyosida sun’iy intellektga asoslangan texnologiyalarni yaratish bo‘yicha yuzaga kelgan kuchli raqobat barcha sohalar uchun yangi imkoniyatlar hamda xatarlarni yuzaga keltirishi mumkin.

Shu jumladan, kiberxavfsizlikni ta’minlashga ixtisoslashgan xalqaro tashkilotlar joriy yilda yangi turdagi kiberxatarlar hamda firibgarlik usullari ommalashishini tahmin qilmoqda.

Xususan:

- **Sun’iy intellekt texnologiyalari yordamida kiberhujumlarni avtomatlashtiriladi.** Firibgarlar aslidan deyarli farq qilmaydigan “yasama” (deepfake) videolar, “fishing” xatlar hamda ijtimoiy muhandislikning murakkab sxemalarini tuzishadi.

- **Internet buyumlar (IoT) infratuzilmalariga hujumlar ortadi.** “Aqlli” qurilmalar sonining o‘sishi bilan ularni “buzib kirish” ehtimoli ham oshib bormoqda, tajovuzkorlar kuzatuv kameralari, “aqlli” qulflar va boshqa qurilmalar boshqaruvini qo‘lga kirita boshlashadi.

- **Zararli fayllarni o‘rnatishga bo‘lgan ehtiyoj yo‘qoladi.** Zamonaviy hujumlarda tizimlarga “buzib” kirish uchun brauzerlar hamda “bulutli” xizmatlardagi zaifliklardan foydalanish darajasi ortib boradi.

- **Fuqarolarning tibbiy ma’lumotlariga kiberhujumlar amalga oshiriladi.** Sog‘liqni saqlash tizimi raqamlashgani sayin tajovuzkorlar bemorlarning tibbiy ma’lumotlarini qo‘lga kiritish uchun harakat qilishadi.

- **“Bulutli” ma’lumotlarni saqlash xizmatlariga hujumlar ortadi.** Tajovuzkorlar foydalanuvchi ma’lumotlarini shifrlab, “deshifrlash” kalitlarini sotib olishni taklif qiladi, shuningdek, tizimlardagi konfidensial ma’lumotlarni qo‘lga kiritish payida bo‘ladi.