

Date: 5th September-2026

RAQAMLI GIGIYENA VA KIBERXAVFSIZLIK: ONLAYN FIRIBGARLIK (FISHING, DEEPFAKE) TURLARIDAN SHAXSIY MA'LUMOTLARNI VA MABLAG'LARNI HIMOYALASH

Sobirjonova Omina

Nizomiy nomidagi O'zMPU Tarix fakulteti "Milliy g'oya, ma'naviyat asoslari va
huquq ta'limi" yo'nalishi 2-bosqich talabasi

Annotatsiya: Mazkur maqolada raqamli gigiyena va kiberxavfsizlikning zamonaviy axborot makonidagi ahamiyati yoritiladi. Onlayn firibgarlikning keng tarqalgan turlari, xususan, fishing (phishing) va sun'iy intellekt texnologiyalari yordamida yaratiladigan deepfake kontentlarning xavfi tahlil qilinadi. Shuningdek, shaxsiy ma'lumotlar, bank hisoblari va moliyaviy mablag'larni kiberjinoyatchilardan himoyalashning samarali usullari ko'rib chiqiladi. Foydalanuvchilarning raqamli savodxonligini oshirish, shubhali havola va xabarlarini aniqlash, kuchli parollardan foydalanish, ikki bosqichli autentifikatsiyani yoqish hamda deepfake materiallarni aniqlash bo'yicha amaliy tavsiyalar beriladi. Tadqiqot natijalari raqamli muhitda xavfsiz xulq-atvorni shakllantirish va onlayn firibgarlik qurboniga aylanish xavfini kamaytirishga xizmat qiladi.

Kalit so'zlar: raqamli gigiyena, kiberxavfsizlik, onlayn firibgarlik, fishing, deepfake, shaxsiy ma'lumotlar, moliyaviy xavfsizlik, kiberjinoyat, raqamli savodxonlik, ikki bosqichli autentifikatsiya.

Аннотация: В данной статье рассматривается значение цифровой гигиены и кибербезопасности в современной информационной среде. Анализируются распространённые виды онлайн-мошенничества, в частности фишинг (phishing) и deepfake-контент, создаваемый с использованием технологий искусственного интеллекта. Особое внимание уделяется вопросам защиты персональных данных, банковских счетов и финансовых средств от киберпреступников. Рассматриваются эффективные меры безопасности, включая повышение цифровой грамотности пользователей, распознавание подозрительных сообщений и ссылок, использование сложных паролей, двухфакторной аутентификации, а также методы выявления поддельного аудио- и видеоконтента. Представленные рекомендации направлены на формирование безопасного поведения пользователей в цифровой среде и снижение риска стать жертвой онлайн-мошенничества.

Ключевые слова: цифровая гигиена, кибербезопасность, онлайн-мошенничество, фишинг, deepfake, персональные данные, финансовая безопасность, киберпреступность, цифровая грамотность, двухфакторная аутентификация.

Abstract: This article examines the importance of digital hygiene and cybersecurity in the modern information environment. It analyzes common types of online fraud, particularly phishing and deepfake content generated using artificial intelligence technologies. Special attention is paid to protecting personal data, bank accounts, and financial assets from cybercriminals. The article discusses effective security measures, including improving users' digital literacy, identifying suspicious messages and links, using strong passwords,



Date: 5th September-2026

enabling two-factor authentication, and detecting manipulated audio and video content. The proposed recommendations are aimed at promoting safe digital behavior and reducing the risk of becoming a victim of online fraud.

Keywords: digital hygiene, cybersecurity, online fraud, phishing, deepfake, personal data, financial security, cybercrime, digital literacy, two-factor authentication.

XXI asr insoniyat tarixiga texnologik burilishlar va misli ko‘rilmagan axborotlashuv davri sifatida kirib keldi. Bugun internet va raqamli qurilmalar kundalik turmushimizning, muloqotimizning va moliyaviy faoliyatimizning ajralmas qismiga aylanib ulgurdi. Birgina smartfon orqali bank amaliyotlarini bajarish, hujjatlar yuritish, dunyoning boshqa chekkasidagi inson bilan lahzalarda bog‘lanish va xaridlarni amalga oshirish imkoniyatiga egamiz. Biroq har bir texnologik taraqqiyot o‘zining orqa tomonida ulkan xatarlarni ham yetaklab keladi. Virtual olamning cheksiz imkoniyatlari bilan bir qatorda, kiberhududda inson xavfsizligiga, uning shaxsiy ma’lumotlari hamda jamg‘argan mablag‘lariga raxna soluvchi yangi turdagi tahdidlar paydo bo‘ldi. Mening nazrimda, bugungi kunda har birimiz uchun eng ustuvor va hayotiy masalalardan biri — bu raqamli gigiyena qoidalariga amal qilish va kiberxavfsizlik madaniyatini shakllantirishdir. “Gigiyena” tushunchasi traditionally jismoniy salomatlikni saqlash, toza yurish va mikroblardan himoyalaniшни anglatadi, ammo zamonaviy dunyoda bu ibora yangicha ma’no-mazmun kashf etdi. Raqamli gigiyena — bu virtual makonda xavfsiz harakat qilish, kiber-tuzoqlarga tushmaslik, axborot oqimini to‘g‘ri saralash va shaxsiy raqamli izlarni muhofaza qilish bo‘yicha ko‘nikmalar majmuasidir. Biz har kuni qo‘limizni yuvishni kanda qilmaganimizdek, smartfonimiz va kompyuterimiz xavfsizligiga ham shunday mas’uliyat bilan yondashishimiz shart bo‘lib, e’tiborsizlik va loqaydlik nafaqat moddiy yo‘qotishlarga, balki ma’naviy-ruhiy zararlarga ham olib kelishi mumkin. Onlayn firibgarlikning eng keng tarqalgan va klassik turlaridan biri bu fishing (phishing) texnikasidir. Fishing — inglizcha “baliq ovlash” so‘zidan olingan bo‘lib, kiberjinoyatchilar tomonidan foydalanuvchilarning maxfiy ma’lumotlarini (parollar, bank karta raqamlari, PIN-kodlar va shaxsiy ma’lumotlar) aldov yo‘li bilan qo‘lga kiritishga qaratilgan bo‘lib, fishing amaliyotining asosida texnik buzib kirishdan ko‘ra ko‘proq ijtimoiy muhandislik, ya’ni inson psixologiyasi bilan o‘ynash yotadi. Firibgarlar inson ruhiyatidagi zaif nuqtalarni — qo‘rquv, qiziqish, shoshqaloqlik yoki ochko‘zlikni juda yaxshi bilishadi. Masalan, so‘nggi paytlarda Telegram va boshqa ijtimoiy tarmoqlarda “Sizga davlat tomonidan moddiy yordam ajratildi”, “Prezident sovg‘asi o‘ynalmoqda”, “Karta bloklandi, darhol rasmiy saytga o‘ting” yoki “Yaqin do‘stingizga ovoz bering” kabi xabarlar tez-tez uchramoqda va ushbu xabarlar ostiga qo‘yilgan havola (link) bir qarashda rasmiy bank yoki tashkilot saytiga o‘xshab ketadi, ammo u firibgarlarning soxta (klon) sayti bo‘lib chiqadi. Foydalanuvchi bilmasdan bu saytga o‘z karta ma’lumotlarini yoki SMS orqali kelgan tasdiqlash kodini kiritsa, soniyalar ichida uning hisobidagi barcha mablag‘lar g‘oyib bo‘ladi. Menimcha, bunday vaziyatlarda insonni qutqarib qoladigan yagona narsa — bu sovuqqonlik va tanqidiy fikrlashdir. Har qanday xabarni tekshirish, shubhali havolalarga bosmaslik va rasmiy manbalardan axborot qidirish har bir internet

Date: 5th September-2026



foydalanuvchisining birinchi qoidasi bo'lishi kerak. Biroq, texnologiya bir joyda to'xtab turgani yo'q. Sun'iy intellekt (AI) rivojlanishi bilan kiberjinoyat sohasi ham sifat jihatidan yangi va xavfli bosqichga ko'tarildi, bugun biz Deepfake (chuqur soxtalashtirish) deb ataluvchi murakkab kiber-tahdid bilan yuzlashmoqdamiz. Deepfake texnologiyasi neyron tarmoqlari yordamida muayyan insonning yuz tuzilishi, ovoz tembri va mimikalarini aniqlik bilan nusxalab, mutlaqo soxta video yoki audio fayllarni yaratish imkonini beradi. Tasavvur qiling, sizga yaqin do'stingiz yoki qarindoshingiz videochalingizga qo'ng'iroq qiladi yoki ovozli xabar yuboradi. Video va ovoz ayni o'ziniki, u shoshilinch ravishda baxtsiz hodisaga uchraganini va zudlik bilan pul o'tkazib berishingizni so'raydi. Insoniy tuyg'ular va hamdardlik sababli siz hech qanday shubhasiz pul yuborasiz, ammo keyinroq buni sun'iy intellekt yaratgan soxta tasvir va ovoz ekanini bilasiz. Bu shunchaki uydirma emas, bugungi kunning real voqeligidir. Deepfake insonlar o'rtasidagi azaliy qadriyat — ishonch tushunchasiga zarba bermoqda. Endilikda biz "o'z ko'zim bilan ko'rdim, o'z qulog'im bilan eshitdim" degan iboraga ham to'liq ishonolmaydigan davrda yashayapmiz. Xo'sh, bunday murakkab va makkor tahdidlar qarshisida shaxsiy ma'lumotlarimiz va mablag'larimizni qanday himoya qilishimiz kerak? Mening fikrimcha, kiberxavfsizlikni ta'minlash kompleks va muntazam amallarni talab etadi:

1. parol siyosatiga amal qilish. Ko'pchilik eslab qolish qulay bo'lishi uchun "123456", "password" yoki tug'ilgan yilini parol sifatida ishlatadi. Bu kiberjinoyatchilar uchun ochiq eshikdir. Har bir ijtimoiy tarmoq va bank ilovasi uchun murakkab, harflar, raqamlar va maxsus belgilardan iborat takrorlanmas parollarni o'rnatish lozim.

2. ikki bosqichli autentifikatsiya (2FA) tizimini barcha akkauntlarda yoqib qo'yish shart. Bu usul parolingiz bilib olingan taqdirda ham, ikkinchi bosqichdagi maxfiy kodsiz akkauntga kirishga yo'l qo'ymaydi.

3. bank kartalari xavfsizligi. Bank kartasining orqa tomonidagi CVV/CVC kodini hamda telefonga SMS orqali keladigan bir martalik tasdiqlash kodlarini hech qachon va hech kimga (xatto o'zini bank xodimi yoki huquq-tartibot organi vakili deb muloqot qilayotgan shaxslarga ham) aytmalik kerak. Esda tutish lozimki, haqiqiy bank xodimlari hech qachon sizdan SMS kodni so'ramaydi.

4. axborot va kontentni qayta tekshirish (Fact-checking). Agar yaqiningizdan kutilmagan pul so'ralgan xabar yoki audio kelsa, darhol boshqa aloqa kanali orqali uning o'ziga telefon qilib, holatni aniqlashtirish lozim. Shuningdek, operatsion tizimlar va dasturlarni o'z vaqtida yangilab borish xavfsizlik tirqishlarini yopishga yordam beradi.

Xulosa qilib aytganda, raqamli makon bu shunchaki virtual olam emas, u bizning real hayotimizning uzviy davomidir. Unda xavfsiz yashash va harakat qilish uchun yuksak raqamli madaniyat hamda hushyorlik talab etiladi. Kiberxavfsizlik — bu faqatgina IT-mutaxassislari yoki davlat organlarining vazifasi emas, balki har bir fuqaroning shaxsiy mas'uliyatidir. Biz raqamli gigiyena qoidalarini yoshlikdan bilishimiz, oilamiz va yaqinlarimizga, ayniqsa, kiber-tuzoqlarga eng ko'p tushuvchi keksalar va yosh bolalarga tushuntirishimiz zarur, faqatgina texnik bilimlarni oshirish va tanqidiy fikrlash ko'nikmasini shakllantirish orqali biz o'z shaxsiy daxlsizligimizni, moddiy va ma'naviy halovatimizni kiber-tahdidlardan ishonchli muhofaza qila olamiz.

Date: 5th September-2026

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasi. “Kiberxavfsizlik to‘g‘risida”gi Qonun. — O‘RQ-764-son, 15.04.2022.
2. O‘zbekiston Respublikasi qonunchilik ma’lumotlari milliy bazasi — LexUZ. Qonun hujjatlari va normativ-huquqiy hujjatlar elektron bazasi. LexUZ
3. O‘zbekiston Respublikasi Raqamli hukumat markazi. Raqamli texnologiyalar va axborot xavfsizligi bo‘yicha materiallar.
4. O‘zbekiston Respublikasi Ichki ishlar vazirligi. Internetdagi firibgarlik va kiberjinoyatlardan himoyalaniş bo‘yicha tavsiyalar.
5. Whitman, M. E., Mattord, H. J. Principles of Information Security. — Cengage Learning, 2021.
6. Mirsky, Y., Lee, W. The Creation and Detection of Deepfakes: A Survey. — ACM Computing Surveys, 2021.