KIBERJINOYATCHILIKKA QARSHI KURASHISH BO‘YICHA PROFILAKTIKA CHORA-TADBIRLARINI AMALGA OSHIRISH

Idiyev Jamshid Ja’far o‘g‘li
O‘zbekiston Respublikasi Ichki ishlar vazirligi Akademiyasi 3-o’quv kursi kursanti

Annotatsiya: *Maqolada O‘zbekiston Respublikasida kiberjinoyatchilikning keskin o‘sishi, uning iqtisodiy va ijtimoiy hayotga yetkazayotgan zarari tahlil qilinadi. 2025-yil holatiga ko‘ra kiberjinoyatlar soni 2024-yilga nisbatan 52 % oshgani, yillik zarar miqdori esa 1 trillion so‘mdan ortgani qayd etiladi. Eng keng tarqalgan xavf-xatarlar sifatida fishing/smishing, ransomware (Akira, LockBit, Makop), bank kartasi firibgarligi, CEO Fraud/BEC, kriptovalyuta firibgarligi, SIM-swapping va deepfake hujumlari keltiriladi. Kiberjinoyatchilikning oldini olish bo‘yicha profilaktika choralar batafsil yoritiladi.*

Kalit so‘zlar: *kiberjinoyat, axborot tizimi, fishing, noyob parol, 2FA, VPN, DLP, “Raqamli O’zbekiston – 2030”, zaxira nusxa, Parental control*

IMPLEMENTATION OF PREVENTIVE MEASURES AGAINST CYBERCRIME

Abstract: *The article analyzes the sharp increase in cybercrime in the Republic of Uzbekistan and the damage it causes to the economy and society. As of 2025, the number of cybercrimes increased by 52 % compared to 2024, with annual damage exceeding 1 trillion UZS. The most common threats include phishing/smishing, ransomware (Akira, LockBit, Makop), bank card fraud, CEO Fraud/BEC, cryptocurrency scams, SIM-swapping, and deepfake attacks.*

Key words: *cybercrime, information system, phishing, strong password, 2FA, VPN, DLP, “Digital Uzbekistan – 2030”, backup, parental control*

РЕАЛИЗАЦИЯ ПРЕВЕНТИВНЫХ МЕР ПО БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Аннотация: В статье анализируется резкий рост киберпреступности в Республике Узбекистан и наносимый ею ущерб экономике и обществу. По состоянию на 2025 год количество киберпреступлений выросло на 52 % по сравнению с 2024 годом, годовой ущерб превысил 1 трлн сумов. Наиболее распространённые угрозы: фишинг/смишинг, ransomware (Akira, LockBit, Makop), мошенничество с банковскими картами, CEO Fraud/BEC, криптовалютное мошенничество, SIM-swapping и атаки с использованием deepfake.

Ключевые слова: киберпреступность, информационная система, фишинг,

надёжный пароль, 2FA, VPN, DLP, «Цифровой Узбекистан – 2030», резервная копия, родительский контроль

Bugungi kunda internet va raqamli texnologiyalar hayotimizning ajralmas qismiga aylandi. Biroq, bu jarayon bilan birga kiberjinoyatchilik ham keskin oʻsib bormoqda. Oʻzbekiston Respublikasi statistik maʼlumotlariga koʻra, 2024-yilda kiberjinoyatlar soni 2023-yilga nisbatan 40 foizdan ortiq oshgan. Firibgarlik, shaxsiy maʼlumotlarni oʻgʻirlash, fishing hujumlari, ransomware (toʻlov talab qiluvchi zararli dasturlar) va boshqa turdagi kiberhujumlar fuqarolar, korxonalar va davlat organlariga jiddiy zarar yetkazmoqda. 2025-yil boshidan beri Oʻzbekistonda kiberjinoyatlar soni 2024-yilga nisbatan yana 52% oshdi (Ichki ishlar vazirligi maʼlumotlari). Har kuni oʻrtacha 120–150 ta yangi fishing kampaniyasi, 30–40 ta ransomware hujumi va minglab shaxsiy akkauntlarni oʻgʻirlash holatlari qayd etilmoqda. Zarar miqdori esa yiliga 1 trillion soʻmdan oshib ketdi.Bu raqamlar shuni koʻrsatadiki, kiberxavfsizlik endi “IT boʻlimining ishi” emas, balki har bir fuqaro, har bir oila, har bir korxona va davlatning milliy xavfsizlik masalasidir.

Kiberjinoyatlar – kibermakonda kompyuter texnologiyalari va internetdan foydalangan holda sodir etiladigan jinoyatlar hisoblanadi. Bu axborot texnologiyalarining rivojlanishi natijasida paydo bo'lgan yangi turdagi jinoyatlar bo'lib, moliyadan tortib sog'liqni saqlash, ta'lim va davlat idoralarigacha bo'lgan ko'plab sohalarga ta'sir qiladi. Kiberjinoyatlarning quyidagi asosiy xususiyatlarini tahlil qilamiz:

Axborot tizimiga zarar yetkazish – maʼlumotlarni oʻgʻirlash, yoʻq qilish yoki oʻzgartirish.

Moliyaviy va iqtisodiy zarar – onlayn firibgarlik, bank kartalaridagi mablagʼlarni oʻgʻirlash.

Shaxsiy hayotga tajovuz – shaxsiy maʼlumotlarni noqonuniy toʻplash, shantaj qilish.

Davlat xavfsizligiga tahdid – kibersabotaj, kiberterrorchilik, terrorizmni moliyalashtirish.

Shu sababli, kiberjinoyatchilikning oldini olish – profilaktika choralarini kuchaytirish har bir fuqaro, tashkilot va davlatning eng muhim vazifalaridan biridir.

Kiberjinoyatchilikning eng keng tarqalgan turlari:

Fishing / Smishing, Ransomware, bank kartasi firibgarligi, CEO Fraud \

BEC, Kiriptovalyuta firibgarligi, SIM-swapping, deepfake hujumlari va boshqalar.

Fishing /Smishing soxta bank , uzcard, telegram, posilka xabarlari orqali;

Rasomware – fayllarni shifrlash va pul talab qilish orqali;

Bank kartasi firibgarligi – kartani oʼgʼirlash;

CEO Fraund / BEC – rahbar nomidan xodimga “ tezkina pul oʼtkaz” buyrugʼi

Kriptovalyuta firibgarligi – soxta investitsiya loyihalari, wallet drine orqali

SIM-swapping – operator xodimni aldab sim-kartaga oʼtkazish orqali sodir etilishi mumkin.

Kiberjinoyatchilikning O’zbekistonda keng tarqalgan shakllari:

Fishing/smishing – “karta bloklanadi”, “posilka keldi” ,“Davlat xizmatlari”

Ransoware hujumlari – akira, LockBit, RansomHub, Makop

Bank kartasi firibgarligi – payme, uzcard, click orqali to’lov so’rash

CEO Fraud/BEC – O’zbekiston korxonalarida 2025-yilda 300+ holat

Kriptovalyuta firibgarligi – telegramdagi “signal guruhlari, soxta airdroplar”

SIM-swapping – bank va telegram accountlarni o’g’rilash uchun

1.Shaxsiy darajadagi profilaktika choralari

• Kuchli va noyob parollar ishlatish. Har bir xizmat uchun alohida, kamida 12 belgidan iborat parol yarating. Katta-kichik harflar, raqamlar va maxsus belgilar (!@#$%^&*) majburiy. Parollarni hech qachon qog‘ozga yozib qo‘ymang yoki boshqalar bilan baham ko‘rmang.

• Ikki bosqichli autentifikatsiya (2FA) ni yoqish. Gmail, Telegram, bank ilovalari, ijtimoiy tarmoqlar – 2FA mavjud bo‘lgan har bir xizmatda uni majburiy yoqing. SMS, authenticator ilovasi (Google Authenticator, Authy, Microsoft Authenticator) yoki apparat kaliti (YubiKey) orqali.

• **Fishing vaqtida yangilanmaydigan dasturiy ta’minot orqali hujumchilar tizimga kirishi osonlashadi. Operatsion tizim (Windows, macOS, Android, iOS), brauzer, antivirus va barcha ilovalarni doimiy ravishda yangilab boring.

• Fishing va boshqa ijtimoiy muhandislik hujumlaridan ehtiyot bo‘lish

oNoma’lum raqamlardan kelgan SMS yoki messenger xabarlaridagi havolalarni bosmang.

o“Sizning bankingiz bloklandi”, “Lotereyada yutdingiz”, “Posilka keldi” kabi shubhali xabarlarga ishonmang.

oBank yoki davlat organi nomidan kelgan xatni tekshirish uchun rasmiy veb-saytga o‘zingiz kirib tekshiring, havola orqali emas.

• Jamoat Wi-Fi tarmoqlaridan foydalanishda VPN ishlatish Ochik Wi-Fi (kafe, aeroport, universitet) orqali banking, elektron pochta yoki shaxsiy ma’lumotlar bilan ishlash xavfli. VPN (NordVPN, ProtonVPN, Surfshark va h.k.) majburiy.

• Zaxira nusxa (backup) yaratish Muhim hujjatlarni kamida ikki xil joyda (bulutli xizmat + tashqi qattiq disk) saqlang. Ransomware hujumida fayllar shifrlansa ham, zaxira nusxa orqali tiklab olishingiz mumkin.

2. Korxona va tashkilotlar darajasidagi profilaktika

• Xodimlarga muntazam kiberxavfsizlik bo‘yicha treninglar o‘tkazish (kamida yilda 2 marta).

• Tarmoqqa kirish huquqlarini “eng kam imtiyoz” printsipi (least privilege) bo‘yicha taqsimlash.

• DLP (Data Loss Prevention) tizimlarini joriy etish.

• SIEM (Security Information and Event Management) tizimlari orqali doimiy monitoring.

• Tashqi xizmatlar bilan ishlashda NDA va kiberxavfsizlik talablarini shartnomaga kiritish.

3. Davlat darajasidagi choralar (O‘zbekistonda amalda)

• 2023-yil 14-apreldagi PF-58-son Farmon bilan “Kiberxavfsizlik to‘g‘risida”gi qonun qabul qilindi.

• Kiberxavfsizlik markazi (Cybersecurity Center) faoliyati kuchaytirildi.

• “Kiberjinoyatlarga qarshi kurashish boshqarmasi (Ichki ishlar vazirligi huzuridagi) tuzilgan.

• 2024–2026 yillarga mo‘ljallangan “Raqamli O‘zbekiston – 2030” strategiyasi” doirasida kiberxavfsizlik bo‘yicha alohida yo‘nalish belgilangan.

• Maktab va oliy o‘quv yurtlarida “Axborot xavfsizligi” fanining majburiy o‘qitilishi joriy etilmoqda.

4. Bolalar va o‘smirlarni himoya qilish bo‘yicha alohida choralar

• Ota-onalar uchun “Parental control” ilovalarini (Qustodio, Kaspersky Safe Kids, Google Family Link) o‘rnatish.

• Bolalarga internetdagi xavflar haqida 7–8 yoshdan boshlab oddiy tilda tushuntirish.

• Ijtimoiy tarmoqlarda shaxsiy ma’lumotlar (maktab, manzili, telefon raqami, uy manzili) joylashtirishni taqiqlash.

F O Y D A L A N I L G A N A D A B I Y O T L A R :

1. O‘zbekiston Respublikasining Qonuni – “O’zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o’zgartirish va qo’shimchalar kiritish to’g’risida”, O‘RQ – 1003-sonli 21.11.2024-yil

2. O‘zbekiston Respublikasining Qonuni – “Kiberxavfsizlik to’g’risida”, O‘RQ – 764, 15.04.2022-yil

3. O‘zbekiston Respublikasining Qonuni – “Normativ-huquqiy hujjatlar to‘g‘risida”, O‘RQ – 681, 20.04.2021-yil

4. Holt, T. J., & Bossler, A. M. (2021). Cybercrime: Victimization, perpetration, and techniques. American Journal of Criminal Justice, 46(4), 567–589. (Umumiy kiberjinoyatlar va profilaktika choralari bo‘yicha tahlil.)

5. Tran, T. N. K. (2023). A comprehensive review for improved cybercrime prevention. International Journal of Cyber Criminology, 17(2), 45–62. (Kiberjinoyatlarni oldini olish bo‘yicha keng qamrovli sharh.)

6. Karimov, A. A., & Rakhimov, S. S. (2024). The role of cybersecurity and data privacy in Uzbekistan: Safeguarding digital landscapes in the 21st century. ResearchGate Publication. (O‘zbekiston Milliy universiteti professori A. A. Karimov rahbarligidagi ish; raqamli transformatsiya va shaxsiy ma’lumotlar himoyasi.)

7. Xo‘jayev, M. X. (2022). Cybersecurity issues in Uzbekistan. International Journal of Business, Digital Economy and Sustainable Development, 2(3), 78–92.

(O‘zbekiston Iqtisodiyot va moliya universiteti professori M. X. Xo‘jayevning ilmiy ishi; mamlakatdagi kiberxavfsizlik muammolari va “Raqamli O‘zbekiston-2030” strategiyasi.)