FOYDALANUVCHILAR KIBERXAVFSIZLIGINI RAQAMLI SAVODXONLIK ORQALI OSHIRISH

Yuldashev Azamat Shodimurodovich
Telefon: +998(94) 477-67-70
Email: azik_06@bk.ru

Annotatsiya. *Ushbu tezis raqamli savodxonlikning foydalanuvchilar kiberxavfsizligini oshirishdagi rolini asoslaydi. Unda phishing, ijtimoiy injeneriya, parol xavfsizligi, ko‘p faktorli autentifikatsiya va shaxsiy ma’lumotlarni himoya qilish bo‘yicha amaliy ko‘nikmalar muhim profilaktik omil sifatida ko‘rsatiladi.*

Kalit so‘zlar: *raqamli savodxonlik, kiberxavfsizlik, phishing, ijtimoiy injeneriya, ko‘p faktorli autentifikatsiya, kibergigiyena.*

Аннотация. *В данном тезисе обосновывается роль цифровой грамотности в повышении кибербезопасности пользователей. Практические навыки распознавания фишинга и социальной инженерии, защиты паролей, применения многофакторной аутентификации и охраны персональных данных рассматриваются как важный профилактический фактор.*

Ключевые слова: *цифровая грамотность, кибербезопасность, фишинг, социальная инженерия, многофакторная аутентификация, кибергигиена.*

Abstract. *This thesis substantiates the role of digital literacy in improving users’ cybersecurity. Practical skills in recognizing phishing and social engineering, protecting passwords, using multi-factor authentication, and safeguarding personal data are considered an important preventive factor.*

Keywords: *digital literacy, cybersecurity, phishing, social engineering, multi-factor authentication, cyber hygiene.*

Raqamli xizmatlar kundalik hayotning ajralmas qismiga aylandi: bank to‘lovlari, davlat xizmatlari, ta’lim platformalari, ijtimoiy tarmoqlar va elektron tijorat doimiy ravishda foydalanuvchi ma’lumotlariga tayanadi. Shu bilan birga, kiberjinoyatchilar texnik buzib kirishdan tashqari, foydalanuvchining e’tiborsizligi, ishonuvchanligi yoki raqamli bilim yetishmasligidan foydalanadi. Shuning uchun kiberxavfsizlikni oshirishda raqamli savodxonlik mustaqil himoya omili sifatida qaralishi zarur.[1]

Asosiy tezis shundan iboratki, foydalanuvchilarning raqamli savodxonligi oshsa, ko‘plab kiberjinoyatlar sodir bo‘lishidan oldin to‘xtatiladi. Texnik himoya vositalari muhim, ammo foydalanuvchi SMS-kodni firibgarga aytsa, zararli havolani bossa yoki bir xil paroldan hamma joyda foydalansa, himoya tizimi zaiflashadi. Verizon DBIR

[1] O‘zbekiston Respublikasi “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘RQ-764, 15.04.2022.

2025 hisobotida inson omili ko‘plab ma’lumotlar sizib chiqishi holatlarida muhim rol o‘ynashi qayd etiladi.[2]

Tezisning maqsadi - foydalanuvchi darajasidagi kiberxavfsizlikni raqamli savodxonlik orqali oshirishning nazariy va amaliy asoslarini ko‘rsatish. Bu maqsadga erishish uchun uch vazifa ajratiladi: birinchidan, foydalanuvchi duch keladigan asosiy xavflarni aniqlash; ikkinchidan, raqamli savodxonlik elementlarini tizimlashtirish; uchinchidan, ta’lim, tashkilot va davlat darajasida amaliy takliflar ishlab chiqish.

Raqamli savodxonlik faqat kompyuterdan foydalanishni bilish degani emas. U xabar va havolani tekshirish, kuchli parol yaratish, ko‘p faktorli autentifikatsiyadan foydalanish, shaxsiy ma’lumotni himoya qilish, soxta investitsiya va firibgarlik belgilarini tanish, qurilmalarni yangilab borish va shubhali hodisani xabar qilish kabi ko‘nikmalarni o‘z ichiga oladi.

Birinchi fikr: phishing va ijtimoiy injeneriya raqamli savodxonlik yetishmasligidan eng ko‘p foydalanadigan hujumlardir. ENISA Threat Landscape 2025 ma’lumotlariga ko‘ra, phishing dastlabki kirish vektorlari ichida taxminan 60 foizni tashkil qilgan.[3] Foydalanuvchi domen nomini tekshirish, shoshilinch va qo‘rqituvchi matnga tanqidiy qarash, maxfiy kodni bermaslik kabi oddiy qoidalarni bilsa, ko‘plab hujumlar muvaffaqiyatsiz bo‘ladi.

Ikkinchi fikr: raqamli savodxonlik bir martalik ma’ruza emas, doimiy o‘quv jarayoni bo‘lishi kerak. NIST SP 800-50r1 kiberxavfsizlik va maxfiylik bo‘yicha o‘quv dasturlarini rejalashtirish, joriy etish, rollarga moslashtirish va baholab borishni tavsiya qiladi.[4] Demak, maktab, oliy ta’lim muassasasi yoki korxonada “kiberxavfsizlik kuni” o‘tkazish yetarli emas; real holatlar asosida muntazam mashg‘ulot, test va simulyatsiya zarur.

Uchinchi fikr: foydalanuvchi savodxonligi texnik nazorat bilan birga ishlaganda samarali bo‘ladi. NIST CSF 2.0 himoya funksiyasida identifikatsiya, autentifikatsiya, kirishni nazorat qilish, xabardorlik va treninglarni bir tizimda ko‘rsatadi.[5] Masalan, foydalanuvchi kuchli parolni bilishi kerak, tashkilot esa parol siyosati, MFA va shubhali kirishlarni aniqlash tizimini joriy etishi kerak.

To‘rtinchi fikr: raqamli savodxonlik moliyaviy xavfsizlik bilan bevosita bog‘liq. Bank kartasi ma’lumotlarini bermaslik, SMS-kodni hech kimga aytmaslik, “oldindan to‘lov” firibgarligini tanish, onlayn xarid paytida sotuvchi va platformani tekshirish kabi ko‘nikmalar foydalanuvchi mablag‘ini himoya qiladi. O‘zbekiston Markaziy banki PQ-153-sonli qaror bo‘yicha press-relizida banklar va to‘lov tashkilotlari

[2] Verizon, 2025 DBIR Executive Summary, 2025.
[3] ENISA, Threat Landscape 2025 Booklet, p. 4.
[4] NIST, SP 800-50r1, Building a Cybersecurity and Privacy Learning Program, 2024.
[5] NIST, Cybersecurity Framework (CSF) 2.0, 2024.

aholining kibermadaniyatini yuksaltirish bo‘yicha chora ko‘rishi zarurligini qayd etgan.[6]

Beshinchi fikr: sun’iy intellekt davrida raqamli savodxonlikning mazmuni kengaymoqda. AI yordamida xat, ovoz, rasm va video ko‘rinishidagi soxta xabarlar ancha ishonchli bo‘lishi mumkin. IBM Security 2025-yilgi hisobotida AI boshqaruvi va kirish nazorati yetishmasligi tashkilotlar uchun yangi xavf ekanini ta’kidlaydi.[7] Foydalanuvchilar esa chiroyli yozilgan xat yoki tabiiy eshitiladigan ovozning o‘zi ishonchlilik dalili emasligini bilishi kerak.

Amaliy takliflar

Birinchi taklif: ta’lim muassasalarida raqamli savodxonlik moduli majburiy amaliy mashg‘ulotlar bilan o‘qitilishi kerak. Unda phishing xatini aniqlash, maxfiy ma’lumotlarni himoya qilish, xavfsiz parol va MFA, shaxsiy ma’lumotlar bilan ishlash, internetdagi firibgarlik va kiberetikaga oid mavzular bo‘lishi lozim.

Ikkinchi taklif: tashkilotlarda xodimlar uchun rolga asoslangan treninglar tashkil etilishi kerak. Oddiy xodimga havola va ilovani tekshirish, moliya bo‘limiga to‘lov rekvizitlarini mustaqil tasdiqlash, rahbarlarga esa qaror qabul qilish va hodisalarga javob berish tartibi o‘rgatiladi. Trening natijasi faqat qatnashganlar ro‘yxati bilan emas, balki amaliy sinovlar va xatolar kamayishi bilan baholanishi lozim.

Uchinchi taklif: banklar, to‘lov tashkilotlari va davlat xizmatlari foydalanuvchiga xavfsizlik ogohlantirishlarini sodda tilda yetkazishi kerak. Xabarlar qisqa, tushunarli va real misollar bilan beriladi: “SMS-kodni hech kimga aytmang”, “bank xodimi karta PIN-kodini so‘ramaydi”, “notanish havolada shaxsiy ma’lumot kiritmang”.

To‘rtinchi taklif: kiberhodisani xabar qilish osonlashtirilishi kerak. Foydalanuvchi shubhali xat, soxta sayt yoki firibgarlik qo‘ng‘irog‘i haqida tez xabar bera olsa, nafaqat o‘zini, balki boshqa foydalanuvchilarni ham himoya qiladi. Buning uchun yagona aloqa kanallari, qisqa ko‘rsatmalar va tezkor teskari aloqa mexanizmlari zarur.

Xulosa

Foydalanuvchilar kiberxavfsizligini oshirishda raqamli savodxonlik markaziy omillardan biridir. Chunki ko‘plab hujumlar texnik zaiflikdan avval inson xatti-harakatini nishonga oladi. Raqamli savodxonlik foydalanuvchiga xavfni oldindan ko‘rish, axborotni tekshirish, maxfiy ma’lumotni himoya qilish va hodisaga to‘g‘ri javob berish imkonini beradi.

Shu sababli kiberxavfsizlik siyosati faqat texnologiya xarid qilishdan iborat bo‘lmasligi kerak. U ta’lim, profilaktika, foydalanuvchi madaniyati, tashkilot ichki qoidalari va texnik nazoratning birlashgan tizimi bo‘lishi zarur. Raqamli savodxon

[6] O‘zbekiston Respublikasi Markaziy banki, PQ-153 yuzasidan press-reliz, 06.05.2025.
[7] IBM Security, Cost of a Data Breach Report 2025.

foydalanuvchi esa kiberxavfsizlikning passiv obyekti emas, balki faol himoya ishtirokchisidir.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni, O‘RQ-764-son, 15.04.2022. URL: https://lex.uz/docs/-5960604 (murojaat sanasi: 13.05.2026).
2. Verizon. 2025 Data Breach Investigations Report: Executive Summary. Verizon Business, 2025. URL: https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf (murojaat sanasi: 13.05.2026).
3. ENISA. Threat Landscape 2025 Booklet. European Union Agency for Cybersecurity, 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf (murojaat sanasi: 13.05.2026).
4. NIST. Building a Cybersecurity and Privacy Learning Program. Special Publication 800-50r1, September 2024. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf (murojaat sanasi: 13.05.2026).
5. NIST. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 26.02.2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (murojaat sanasi: 13.05.2026).
6. O‘zbekiston Respublikasi Markaziy banki. “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ-153-sonli qaror yuzasidan press-reliz, 06.05.2025. URL: https://cbu.uz/uz/press_center/releases/2408879/ (murojaat sanasi: 13.05.2026).
7. IBM Security. Cost of a Data Breach Report 2025. IBM, 2025. URL: https://www.ibm.com/reports/data-breach (murojaat sanasi: 13.05.2026).
8. Federal Bureau of Investigation, Internet Crime Complaint Center. 2025 IC3 Annual Report. FBI IC3, 2026. URL: https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf (murojaat sanasi: 13.05.2026).