RAQAMLI QALQON: 2026-YILDA KIBERXAVSIZLIK VA INSON OMILI

Jabborova Sabrina Asomiddin qizi
Qarshi davlat universiteti talabasi

Annotatsiya: *Ushbu maqola 2026-yilda kiberxavfsizlikning dolzarb muammolarini, raqamli tahdidlarning rivojlanishini va axborot xavfsizligini ta’minlashda inson omilining muhim rolini o‘rganadi. Sun’iy intellekt, bulutli hisoblash va masofaviy ish tizimlarining keng qo‘llanilishi fonida kiberhujumlarning tobora murakkablashib borishi tahlil qilinadi. Maqolada texnik himoya choralaridan tashqari, xodimlarning axborot madaniyati, bilim va mas’uliyat hissini rivojlantirish kiberxavfsizlikni ta’minlashda muhim omil ekani ta’kidlanadi. Shuningdek, maqola tashkilot va jamiyat darajasida “inson–texnologiya–xavfsizlik” triadasini uyg‘unlashtirish bo‘yicha tavsiyalar va xulosalarni taqdim etadi.*

Kalit so‘zlar: *kiberxavfsizlik, inson omili, raqamli tahdidlar, sun’iy intellekt, axborot xavfsizligi, ijtimoiy muhandislik, raqamli madaniyat*

Annotation: *This article analyzes the pressing issues of cybersecurity in the context of 2026, the evolution of digital threats, and the role of the human factor in ensuring information security. Against the backdrop of the widespread adoption of artificial intelligence, cloud technologies, and remote work systems, the increasing sophistication of cyberattacks is examined. In addition, the article substantiates that alongside technical protection measures, enhancing employees’ information culture, knowledge, and sense of responsibility constitutes a crucial element of cybersecurity. The paper also presents proposals and conclusions aimed at ensuring the harmony of the “human–technology–security” triad at the organizational and societal levels.*

Keywords: *cybersecurity, human factor, digital threats, artificial intelligence, information security, social engineering, digital culture*

Kirish

Raqamli transformatsiya jarayonlari XXI asrning eng muhim tendensiyalaridan biriga aylandi. Davlat boshqaruvi, ta’lim, sog‘liqni saqlash, bank-moliya tizimi va sanoat sohalarining deyarli barchasi axborot-kommunikatsiya texnologiyalariga tayanmoqda. 2026-yilga kelib ushbu jarayonlar yanada jadallashib, sun’iy intellekt (SI), “Internet of Things” (IoT) va katta hajmdagi ma’lumotlar (Big Data) kundalik hayotning ajralmas qismiga aylandi.

Biroq raqamlashtirish bilan bir qatorda kiberxavfsizlik masalalari ham keskinlashmoqda. Bugungi kunda axborot tizimlariga qaratilgan hujumlar nafaqat texnik nosozliklar, balki inson xatolari tufayli ham yuzaga kelmoqda. Shu sababli kiberxavfsizlikni faqat texnologik muammo sifatida emas, balki ijtimoiy-psixologik hodisa sifatida ham ko‘rib chiqish zarur.

2026-yilda kiberxavfsizlik manzarasi

2026-yilda kiberhujumlar ko‘lami va murakkabligi sezilarli darajada oshdi. Avvallari oddiy virus va fishing xabarlar bilan cheklangan tahdidlar bugun sun’iy intellekt yordamida avtomatlashtirilgan, aniq nishonga yo‘naltirilgan hujumlarga aylandi. Xususan, “deepfake” texnologiyalari orqali soxta ovoz va video yaratish, moliyaviy firibgarliklar va obro‘ga putur yetkazish holatlari ko‘paymoqda.

Bulutli infratuzilmalar va masofaviy ish muhitining kengayishi ham xavfsizlik chegaralarini noaniq holga keltirdi. Avval tashkilot ichidagi yopiq tarmoqlar bilan cheklangan axborot resurslari bugun dunyoning istalgan nuqtasidan foydalaniladigan bo‘ldi. Bu esa kiberjinoyatchilar uchun yangi imkoniyatlar yaratmoqda.

Inson omili: eng zaif yoki eng kuchli bo‘g‘in?

Ko‘plab tadqiqotlar shuni ko‘rsatadiki, kiberxavfsizlik bilan bog‘liq hodisalarning katta qismi aynan inson omili bilan bog‘liq. Kuchli parol qo‘llamaslik, shubhali havolalarni ochish, begona qurilmalardan foydalanish kabi oddiy xatolar jiddiy oqibatlarga olib kelishi mumkin.

Shu bilan birga, inson omili faqat xavf manbai emas, balki eng kuchli himoya vositasi ham bo‘lishi mumkin. Agar foydalanuvchi kiberxavfsizlik asoslarini bilsa, tahdidlarni aniqlay olsa va mas’uliyat bilan harakat qilsa, eng zamonaviy hujumlar ham samarasiz bo‘lib qoladi. Demak, muammo insonning o‘zida emas, balki uning bilim darajasi va raqamli madaniyatida.

Ijtimoiy muhandislik va psixologik ta’sir

2026-yilda ijtimoiy muhandislik hujumlari yanada takomillashdi. Kiberjinoyatchilar texnik zaifliklardan ko‘ra, inson psixologiyasidan foydalanishni afzal ko‘rmoqda. Qo‘rquv, shoshilish, ishonch kabi hissiyotlar orqali foydalanuvchi aldovga tushiriladi.

Masalan, “rahbariyat nomidan yuborilgan shoshilinch xabar” yoki “hisobingiz bloklandi” mazmunidagi xatlar hali ham ko‘plab foydalanuvchilarni chalg‘itmoqda. Bu holat inson omilining kiberxavfsizlikdagi rolini yanada chuqurroq o‘rganish zarurligini ko‘rsatadi.

Ta’lim va raqamli madaniyatning ahamiyati

Kiberxavfsizlikni ta’minlashda texnik vositalar bilan bir qatorda ta’lim va treninglar muhim ahamiyatga ega. 2026-yil sharoitida axborot xavfsizligi bo‘yicha bilimlar faqat IT mutaxassislar uchun emas, balki barcha foydalanuvchilar uchun zarur ko‘nikmaga aylandi.

Tashkilotlarda muntazam treninglar, simulyatsion hujumlar va xabardorlik dasturlari xodimlarning hushyorligini oshiradi. Jamiyat miqyosida esa maktab va oliy ta’lim tizimida raqamli xavfsizlik madaniyatini shakllantirish uzoq muddatli barqarorlikni ta’minlaydi.

Xulosa

2026-yilda kiberxavfsizlik masalasi texnologiya va inson omilining uzviy uyg‘unligini talab qilmoqda. Eng zamonaviy texnik himoya vositalari ham xabardor va mas’uliyatli foydalanuvchisiz samarasiz bo‘lishi mumkin. Shu sababli “raqamli qalqon” tushunchasi nafaqat dasturiy va apparat himoyani, balki inson ongida shakllangan xavfsizlik madaniyatini ham o‘z ichiga olishi lozim.

Inson omilini zaif bo'g'in sifatida emas, balki kiberxavfsizlikning asosiy tayanchi sifatida rivojlantirish 2026-yil va undan keyingi davr uchun eng muhim vazifalardan biridir.

Foydalanilgan adabiyotlar:

1.Stallings, W. Cryptography and Network Security: Principles and Practice.Pearson Education, 2023

2.Schneier,B. Click Here to Kill Everybody:Security and Survival in a Hyper-connected World. W.W.Norton &Company, 2022

3.ISO/IEC 27001:2022- Information Security Management Systems.

4. ENISA, Cybersecurity Threat Landscape Report, 2024.

5. Anderson, R. Security Engineering. Wiley, 2021