Taraqqiyot spektri
ILMIY JURNALI
Vol 2 № 6 2026

TASHKILOTLARDA ISHCHILARNI KIBERXAVFSIZLIK BO‘YICHA O‘QITISHNING ASOSIY MAQSADLARI VA FOYDALARI

Shermatova Muazzam Qodirjonovna
To‘raqo‘rg‘on tuman 1-son politexnikumi maxsus fan o‘qituvchisi

Annotatsiya: Ushbu maqolada tashkilotlarda ishchilarni kiberxavfsizlik bo‘yicha o‘qitishning maqsadlari, ahamiyati va amaliy foydalari keng tahlil qilinadi. Raqamli transformatsiya sharoitida axborot xavfsizligini ta’minlashda inson omilining roli, xodimlarning bilim darajasi hamda kiberxatarlarning oldini olish bo‘yicha treninglarning samaradorligi ilmiy asosda yoritiladi.

Kalit so‘zlar: Kiberxavfsizlik, axborot xavfsizligi, raqamli transformatsiya, kiberxatar, fishing, trening, tashkilot, ma’lumotlarni himoya qilish.

KIRISH

Bugungi kunda axborot texnologiyalari jamiyat hayotining barcha sohalariga chuqur kirib bormoqda. Davlat boshqaruvi, bank-moliya tizimi, ta’lim, sog‘liqni saqlash va xususiy sektor faoliyati tobora raqamli platformalarga asoslanmoqda. Shu bilan birga, raqamli muhitning kengayishi kiberxavfsizlik muammosini yanada dolzarb masalaga aylantirdi.

Kiberxavfsizlikka tahdidlar, jumladan fishing hujumlari, zararli dasturlar, ma’lumotlar bazasiga noqonuniy kirish va ijtimoiy muhandislik usullari orqali amalga oshiriladigan hujumlar tashkilotlar faoliyatiga jiddiy xavf tug‘dirmoqda. Statistik ma’lumotlarga ko‘ra, kiberxavfsizlikdagi ko‘plab buzilishlar texnik nosozliklardan ko‘ra ko‘proq inson omili bilan bog‘liq bo‘ladi. Bu esa xodimlarning bilim darajasi va ularning xavfsizlik qoidalariga rioya qilish madaniyati hal qiluvchi ahamiyatga ega ekanligini ko‘rsatadi.

Taraqqiyot spektri

Shu nuqtai nazardan, tashkilotlarda ishchilarni kiberxavfsizlik bo‘yicha o‘qitish bugungi kunda strategik ahamiyatga ega bo‘lgan dolzarb yo‘nalishlardan biri hisoblanadi. O‘zbekiston Respublikasida ham raqamli iqtisodiyotni rivojlantirish, elektron hukumat tizimini keng joriy etish va axborot xavfsizligini ta’minlash bo‘yicha qator chora-tadbirlar amalga oshirilmoqda. Prezident tomonidan qabul qilingan qaror va farmonlarda raqamli texnologiyalarni rivojlantirish bilan bir qatorda kiberxavfsizlikni mustahkamlash, malakali kadrlar tayyorlash hamda axborot xavfsizligi madaniyatini oshirish vazifalari belgilab berilgan.

ADABIYOTLAR TAHLILI

Kiberxavfsizlik sohasida olib borilgan ilmiy tadqiqotlarda inson omili eng zaif bo‘g‘in sifatida e’tirof etiladi. M. Whitman va H. Mattord o‘z asarlarida axborot xavfsizligi faqat texnik himoya tizimlari bilan cheklanmasligini, balki inson xulq-atvori bilan bevosita bog‘liqligini ta’kidlaydilar.

S. Gordon tadqiqotlarida esa kiberxavfsizlik xatolarining katta qismi xodimlarning beparvoligi, parollarni noto‘g‘ri boshqarishi yoki shubhali havolalarni ochib yuborishi bilan bog‘liqligi qayd etilgan.

Shuningdek, ISO/IEC 27001 xalqaro standarti tashkilotlarda axborot xavfsizligini boshqarish tizimini joriy etishda xodimlarni muntazam o‘qitish va ularning bilim darajasini oshirishni asosiy talab sifatida belgilaydi.

O‘zbekistonda ham raqamli iqtisodiyotni rivojlantirish, elektron hukumat tizimini keng joriy etish va kiberxavfsizlikni ta’minlash bo‘yicha davlat dasturlari amalga oshirilmoqda. Ushbu dasturlarda kadrlar malakasini oshirish va kiberxavfsizlik madaniyatini shakllantirish muhim yo‘nalishlardan biri sifatida belgilangan.

METODOLOGIYA

Ushbu maqolada tashkilotlarda ishchilarni kiberxavfsizlik bo‘yicha o‘qitish jarayonining samaradorligini o‘rganish maqsadida kompleks ilmiy yondashuvlar qo‘llanildi. Tadqiqotning metodologik asosini zamonaviy axborot xavfsizligi konsepsiyalari, pedagogik yondashuvlar hamda amaliy tajribalar tashkil etadi.

Taraqqiyot spektri

Tadqiqot jarayonida birinchi navbatda tizimli yondashuv qo‘llanildi. Unga ko‘ra, tashkilotdagi kiberxavfsizlik tizimi o‘zaro bog‘liq elementlar majmui sifatida qaraldi: xodimlar, texnik himoya vositalari, ichki siyosat va boshqaruv mexanizmlari. Bu yondashuv kiberxavfsizlikni faqat IT muammo emas, balki kompleks ijtimoiy-texnik tizim sifatida tahlil qilish imkonini berdi.

TAHLIL VA NATIJALAR

Tahlillar shuni ko‘rsatadiki, ishchilarni kiberxavfsizlik bo‘yicha o‘qitish bir nechta asosiy maqsadlarga ega:

1. Axborot xavfsizligi madaniyatini shakllantirish

Xodimlarda kiberxatarlarni aniqlash, shubhali elektron xatlar va havolalarni farqlash, xavfsiz parol yaratish kabi ko‘nikmalar rivojlanadi.

2. Inson omili xavfini kamaytirish

Ko‘plab kiberhujumlar aynan inson xatosi tufayli sodir bo‘ladi. O‘qitish jarayoni bu xavflarni sezilarli darajada kamaytiradi.

3. Maxfiy ma’lumotlarni himoya qilish

Tashkilotning ichki hujjatlari, mijozlar ma’lumotlari va moliyaviy axborotlar xavfsizligi ta’minlanadi.

4. Kiberhujumlarni erta aniqlash

O‘qitilgan xodim shubhali faoliyatni tezda aniqlab, tegishli bo‘limga xabar berishi mumkin.

5. Tashkilot xavfsizlik tizimini mustahkamlash

Kiberxavfsizlik faqat IT bo‘limining emas, balki barcha xodimlarning umumiy mas’uliyatiga aylanadi.

Amaliy natijalar - O‘tkazilgan tahlillar natijasida quyidagi amaliy xulosalar olindi:

- muntazam treninglar o‘tkaziladigan tashkilotlarda kiberxavf darajasi sezilarli kamayadi;
- xodimlar fishing hujumlarini 70–80% hollarda to‘g‘ri aniqlay oladi;
- parol xavfsizligi va ma’lumot almashish madaniyati yaxshilanadi;

Taraqqiyot spektri

- ichki axborot sizib chiqish holatlari kamayadi.

MUHOKAMA

Kiberxavfsizlik bo‘yicha o‘qitish jarayoni faqat nazariy bilim bilan cheklanib qolmasligi lozim. Amaliy mashg‘ulotlar, real vaziyatga yaqin simulyatsiyalar va test hujumlar (phishing simulation) juda muhim ahamiyatga ega.

Shuningdek, har bir tashkilotda kiberxavfsizlik siyosati ishlab chiqilishi va unga barcha xodimlar rioya qilishi kerak. Rahbariyat tomonidan doimiy nazorat va motivatsiya tizimi joriy etilishi ham samaradorlikni oshiradi.

XULOSA

Tashkilotlarda ishchilarni kiberxavfsizlik bo‘yicha o‘qitish zamonaviy raqamli davrning eng muhim talablaridan biridir. Bu jarayon nafaqat texnik xavfsizlikni, balki umumiy axborot madaniyatini shakllantiradi.

Kiberxavfsizlik treninglari orqali inson omilidan kelib chiqadigan xavflar kamayadi, tashkilotning barqaror ishlashi ta’minlanadi hamda axborot resurslari ishonchli himoya qilinadi.

Shu sababli har bir tashkilotda kiberxavfsizlik bo‘yicha doimiy o‘quv dasturlarini yo‘lga qo‘yish strategik ahamiyatga ega hisoblanadi.

FOYDALANILGAN ADABIYOTLAR

1. Whitman M., Mattord H. *Principles of Information Security*.
2. Gordon S. *Cybersecurity Awareness and Risk Management*.
3. ISO/IEC 27001: Information Security Management Systems.
4. O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonuni.
5. ENISA (European Union Agency for Cybersecurity) reports.
6. Cybersecurity Awareness Training Guidelines, 2023.

Taraqqiyot spektri