GLOBAL JOURNAL OF
CROSS-DISCIPLINARY
INNOVATIONS
Multidisciplinary peer-reviewed scholarly journal

GJCDI
Vol. 1 | Issue 3
Year: 2026

KIBERXAVFSIZLIK VA SHAXSIY MA'LUMOTLARNI HIMOYA QILISHNING DOLZARB MASALALARI

Muallif: Usmonov Oyatulla Yoldoshali ogli
Universitet nomi: Fargona davlat Texnika universituti

Annotatsiya

Mazkur maqolada kiberxavfsizlik va shaxsiy ma'lumotlarni himoya qilish masalalarining zamonaviy axborot makonidagi o'rni tahlil qilinadi. Raqamli xizmatlar, bulutli platformalar, mobil ilovalar, ijtimoiy tarmoqlar hamda elektron boshqaruv tizimlarining keng qo'llanilishi natijasida foydalanuvchi haqidagi ma'lumotlar hajmi keskin ortib bormoqda. Shu bilan birga, noqonuniy kirish, fishing, zararli dasturlar, ijtimoiy muhandislik, ma'lumotlarning sizib chiqishi va identifikatsiya vositalarining o'g'irlanishi kabi tahdidlar ham murakkablashmoqda. Tadqiqotda kiberxavfsizlikka doir ilmiy manbalar hamda axborot xavfsizligi bo'yicha fundamental o'quv adabiyotlar asosida shaxsiy ma'lumotlarni himoya qilishning tashkiliy, huquqiy va texnologik jihatlari yoritildi. Maqolada xavfsizlikni faqat texnik muammo sifatida emas, balki boshqaruv, madaniyat, raqamli savodxonlik va xavf-xatarlarni oldindan baholashga tayangan kompleks tizim sifatida ko'rish zarurligi asoslab berildi. Shuningdek, oliy ta'lim muassasalari, kichik biznes subyektlari va davlat xizmatlarida ma'lumotlar bilan ishlashda ko'p bosqichli autentifikatsiya, ma'lumotlarni shifrlash, ehtiyot nusxa yaratish, minimal vakolat tamoyili va foydalanuvchi mas'uliyatini oshirishning ahamiyati ko'rsatildi. Tadqiqot natijasida shaxsiy ma'lumotlar xavfsizligini ta'minlash uzluksiz jarayon bo'lib, u texnologiya, tashkiliy nazorat va inson omilining uyg'unligiga tayangan holda samarali amalga oshirilishi haqidagi xulosa ilgari surildi.

Kalit so'zlar: kiberxavfsizlik, shaxsiy ma'lumot, axborot xavfsizligi, fishing, zararli dastur, shifrlash, autentifikatsiya, raqamli savodxonlik, maxfiylik, ma'lumotlarni boshqarish.

Kirish

Raqamli iqtisodiyot va elektron kommunikatsiya vositalarining jadallik bilan rivojlanishi inson faoliyatining deyarli barcha sohalarini o'zgartirdi. Bugungi kunda bank

amaliyotlari, masofaviy ta'lim, elektron savdo, tibbiy axborot tizimlari, davlat xizmatlari va korporativ boshqaruv jarayonlari raqamli platformalar vositasida amalga oshirilmoqda. Mazkur jarayon qulaylik, tezkorlik va samaradorlikni ta'minlayotgani bilan birga, foydalanuvchilarning shaxsiy ma'lumotlari va tashkilotlarga tegishli axborot resurslarini himoya qilish masalasini ham nihoyatda dolzarb etib qo'ymoqda.

Shaxsiy ma'lumotlar insonning shaxsi, identifikatsiyasi, ijtimoiy mavqei, salomatligi, moliyaviy holati yoki raqamli xulq-atvoriga oid axborotlarni o'z ichiga oladi. Bunday ma'lumotlar noto'g'ri boshqarilganda yoki uchinchi shaxslar qo'liga tushganda, shaxsiy hayot daxlsizligi buzilishi, moliyaviy zarar, obro'ga putur yetishi, hatto ruhiy bosim kabi oqibatlar yuzaga keladi. Shu sababli shaxsiy ma'lumotlar xavfsizligi masalasi bugungi kunda nafaqat texnik mutaxassislar, balki pedagoglar, huquqshunoslar, menejerlar va keng jamoatchilik uchun ham muhim mavzuga aylandi.

Kiberxavfsizlik tushunchasi ko'pincha tarmoqlar, dasturiy vositalar va qurilmalarni himoya qilish bilan bog'liq tarzda talqin qilinadi. Biroq zamonaviy yondashuvga ko'ra, u faqat apparat va dasturiy darajadagi himoya emas, balki xavf-xatarlarni aniqlash, ularga tayyorgarlik ko'rish, hodisaga tezkor javob berish, tiklanish jarayonlarini boshqarish hamda foydalanuvchilar ongida xavfsiz xulq-atvorni shakllantirishni ham qamrab oladi.

Mazkur maqolaning maqsadi kiberxavfsizlik va shaxsiy ma'lumotlarni himoya qilishning nazariy asoslarini yoritish, mavjud tahdidlarni tizimlashtirish hamda turli sohalarda qo'llanilishi mumkin bo'lgan amaliy himoya mexanizmlarini tahlil qilishdan iborat.

Adabiyotlar tahlili va metodlar

Axborot xavfsizligi bo'yicha fundamental adabiyotlarda kiberxavfsizlikning markaziy maqsadi axborotning maxfiyligi, yaxlitligi va mavjudligini saqlash ekani ta'kidlanadi. Ushbu uchlik ko'pincha xavfsizlik siyosatini ishlab chiqish va nazorat mexanizmlarini baholashning metodologik asosi sifatida qo'llaniladi. William Stallings, Lawrie Brown, Michael E. Whitman, Herbert J. Mattord, Ross Anderson va Mark Rhodes-Ousley kabi mualliflarning darslik va qo'llanmalarida himoya vositalarining texnik ko'rinishidan tashqari, boshqaruv jarayonlari, risklarni tahlil qilish, foydalanuvchi intizomi va tashkiliy siyosatlarning o'rni ham alohida ko'rsatib o'tilgan.

Mavzuga doir kitoblarda shaxsiy ma'lumotlarni himoya qilish ko'p qatlamli model asosida ko'rib chiqiladi. Birinchi qatlam texnologik himoya bo'lib, bunda shifrlash,

xavfsiz aloqa protokollari, antivirus vositalari, tarmoq ekrani va autentifikatsiya tizimlari asosiy o'rin tutadi. Ikkinchi qatlam tashkiliy boshqaruv bilan bog'liq bo'lib, unda ma'lumotlarga kirish siyosati, xodimlarning vakolat darajasi, audit, zaxira nusxalar va favqulodda vaziyat rejalari belgilab olinadi. Uchinchi qatlam esa inson omiliga daxldor bo'lib, raqamli gigiyena, parol intizomi, fishing xabarlarini farqlash, ijtimoiy muhandislikka berilmaslik va maxfiy axborot bilan ehtiyotkor ishlash ko'nikmalarini o'z ichiga oladi.

Tadqiqotda tahliliy, qiyosiy va tizimli yondashuv metodlaridan foydalanildi. Tahliliy metod orqali kiberxavfsizlikka oid asosiy kategoriyalar va tahdid turlari ajratib ko'rsatildi. Qiyosiy metod yordamida turli tashkilotlar uchun umumiy bo'lgan va o'ziga xos xavf omillari solishtirildi. Tizimli yondashuv asosida esa shaxsiy ma'lumotlarni himoya qilish texnologik vosita, boshqaruv siyosati va foydalanuvchi xulqini birlashtiruvchi uzluksiz jarayon sifatida ko'rib chiqildi.

Metodik jihatdan maqola ta'lim muassasalari, biznes subyektlari va davlat xizmatlari misolida universal amaliy tavsiyalar ishlab chiqishga yo'naltirildi. Bu yondashuv mavzuni faqat nazariy doirada emas, balki amaliy boshqaruv muammosi sifatida yoritish imkonini berdi.

Muhokama

Zamonaviy kiberxavfsizlik muhitining eng murakkab jihati shundaki, tahdidlarning aksariyati faqat texnik zaifliklar sababli emas, balki inson omili bilan bog'liq kamchiliklar tufayli ham yuzaga keladi. Ko'plab holatlarda foydalanuvchilar kuchsiz parollardan foydalanadi, noma'lum havolalarni ochadi, umumiy Wi-Fi tarmoqlarida himoyasiz ishlaydi yoki maxfiy ma'lumotlarni uchinchi shaxslarga yuboradi. Shu bois eng zamonaviy xavfsizlik vositalari joriy etilgan tashkilotlarda ham xodimlar va foydalanuvchilar raqamli madaniyati yetarli darajada bo'lmasa, xavfsizlik tizimi barqaror ishlamaydi.

Shaxsiy ma'lumotlarni himoya qilishda yana bir dolzarb masala ma'lumotlarni ortiqcha yig'ish va ularni uzoq muddat nazoratsiz saqlash bilan bog'liq. Raqamli platformalar ko'pincha xizmat ko'rsatish jarayonini qulaylashtirish maqsadida foydalanuvchidan turli ko'rinishdagi ma'lumotlarni to'playdi. Ammo ma'lumotlar hajmi oshgani sari ularni boshqarish murakkablashadi, tizimlarda xavf yuz berish ehtimoli ham

ortadi. Minimal yetarlilik tamoyili, ya'ni xizmat ko'rsatish uchun zarur bo'lgan ma'lumotnigina yig'ish, xavfsizlik siyosatining muhim qismi sifatida qaralishi lozim.

Bulutli texnologiyalar va mobil qurilmalar kiberxavfsizlikning hududiy chegaralarini deyarli yo'q qildi. Xodimlar va talabalar ma'lumotlar bilan istalgan joyda ishlash imkoniga ega bo'ldi. Bu esa bir tomondan ta'lim va boshqaruv jarayonlarini yengillashtirsa, ikkinchi tomondan ruxsatsiz kirish, qurilma yo'qolishi, ma'lumotlarni noto'g'ri almashish, sinxronlashda zaif himoya va noma'lum ilovalar orqali ma'lumot sizib chiqishi kabi xavflarni kuchaytirdi. Shuning uchun xavfsizlikni faqat markaziy server darajasida emas, balki har bir foydalanuvchi qurilmasi darajasida ham ta'minlash zarur.

Muhokama doirasida ta'lim sohasiga alohida e'tibor qaratish muhim. Chunki masofaviy ta'lim, LMS platformalari, test tizimlari va onlayn konferensiya vositalari talabalar va o'qituvchilarga oid katta hajmdagi axborotni qayta ishlaydi. Bunda login-parollar, o'quv natijalari, shaxsiy profil, aloqa ma'lumotlari va ba'zan to'lov ma'lumotlari ham tizimlarda saqlanadi. Agar bu tizimlar yetarli darajada himoyalanmasa, nafaqat shaxsiy daxlsizlik, balki ta'lim sifati va institutsional ishonchga ham zarar yetadi.

Kichik biznesda esa muammo ko'pincha resurslar cheklanganligi bilan bog'liq bo'ladi. Barcha korxonalar alohida xavfsizlik bo'limi tashkil etish imkoniga ega emas. Shu bois ular uchun xavfsizlikning ustuvor yo'nalishlarini to'g'ri belgilash muhim: litsenziyali dasturiy ta'minotdan foydalanish, muntazam yangilash, zaxira nusxa yaratish, xodimlarni o'qitish va ikki faktorli autentifikatsiyani yo'lga qo'yish kam xarajat bilan yuqori natija beruvchi choralardan hisoblanadi.

Jadval. Kiberxavfsizlik va shaxsiy ma'lumotlarni himoya qilishdagi asosiy muammolar hamda tavsiya etiladigan choralar

Dolzarb muammo	Kelib chiqish sababi	Ehtimoliy oqibat	Tavsiya etiladigan chora
Kuchsiz autentifikatsiya	Oddiy parollar, bir xil parolni qayta ishlatish, nazoratsiz kirish	Hisob yozuvining egallanishi, ma'lumotlar o'g'irlanishi	Murakkab parol siyosati, ikki faktorli autentifikatsiya, muntazam parol yangilash
Fishing va ijtimoiy muhandislik	Foydalanuvchining ogohligi pastligi, soxta xabarlarga ishonish	Bank rekvizitlari va shaxsiy ma'lumotlarning sizib chiqishi	Xodim va talabalar uchun trening, xabar manbasini tekshirish, shubhali havolalarni

			bloklash
Qurilma va tizimlarning yangilanmasligi	Eski dasturiy ta'minot, zaifliklar uchun yamoqlarning o'rnatilmasligi	Zararli dastur yuqtirish, ruxsatsiz kirish	Avtomatik yangilash, litsenziyali dasturlardan foydalanish, audit
Ma'lumotlarni ortiqcha yig'ish	Xizmat dizaynida minimal yetarlilik tamoyilining yo'qligi	Noqonuniy foydalanish xavfi, bazaning katta hajmda sizib chiqishi	Faqat zarur ma'lumotni yig'ish, saqlash muddatini cheklash, ma'lumotlarni segmentlash

Natijalar

Tahlil natijalari shuni ko'rsatadiki, kiberxavfsizlikni samarali tashkil etish uchun yagona vosita yoki bir martalik texnik yechim yetarli emas. Natijadorlikka ko'p qatlamli yondashuv orqali erishiladi. Birinchidan, texnik himoya vositalari doimiy yangilanib turishi va xavf-xatarlarga mos ravishda konfiguratsiya qilinishi kerak. Ikkinchidan, tashkilotda ma'lumotlar bilan ishlash siyosati aniq belgilanishi, kim qanday ma'lumotga qachon va qancha darajada kirishi mumkinligi tartibga solinishi zarur. Uchinchidan, har bir foydalanuvchi o'zining raqamli harakati uchun ma'lum darajada javobgar ekanini anglab yetishi kerak.

Shaxsiy ma'lumotlarni himoya qilish bo'yicha amaliy samaradorlik, ayniqsa, quyidagi yo'nalishlarda yuqori bo'lishi aniqlanadi: ma'lumotlarni toifalarga ajratish, maxfiy axborot uchun alohida saqlash va uzatish rejimini belgilash, kirishni jurnalga yozib borish, ko'p bosqichli autentifikatsiyani joriy etish, favqulodda vaziyatlarda tiklanish rejasini ishlab chiqish va foydalanuvchilarning muntazam o'quv mashg'ulotlarini tashkil etish.

Natijalar asosida ta'lim muassasalari uchun alohida tavsiya sifatida talabalar va o'qituvchilarda raqamli xavfsizlik ko'nikmalarini o'quv jarayoni bilan integratsiya qilish zarurligi ko'rinadi. Ya'ni kiberxavfsizlik faqat IT bo'limi masalasi bo'lib qolmasdan, raqamli ta'lim madaniyatining tarkibiy qismi sifatida shakllanishi lozim. Kichik biznes va tashkilotlar uchun esa xavfsizlikni soddalashtirilgan, ammo qat'iy tartiblar orqali yo'lga qo'yish mumkinligi ayon bo'ladi.

Tadqiqot natijalari kiberxavfsizlikning barqaror modeli texnologik, tashkiliy va pedagogik choralar uyg'unlashgandagina shakllanishini tasdiqlaydi. Bu yondashuv nafaqat ma'lumotlar xavfsizligini, balki foydalanuvchining raqamli muhitga bo'lgan ishonchini ham mustahkamlaydi.

Xulosa

Xulosa qilib aytganda, kiberxavfsizlik va shaxsiy ma'lumotlarni himoya qilish zamonaviy jamiyatda strategik ahamiyatga ega bo'lgan kompleks masaladir. Uning dolzarbligi raqamli xizmatlar ulushining ortishi, ma'lumotlar bazalarining kengayishi va kiberhujumlar usullarining murakkablashuvi bilan yanada kuchaymoqda.

Shaxsiy ma'lumotlarni himoya qilishni samarali tashkil etish uchun uch asosiy tamoyilga tayanish zarur: birinchisi - zaruriy texnik vositalarni joriy etish; ikkinchisi - tashkiliy boshqaruv va nazoratni takomillashtirish; uchinchisi - foydalanuvchilarning raqamli savodxonligini oshirish. Mazkur uchlikdan biri sust bo'lsa, butun xavfsizlik tizimining barqarorligi pasayadi.

Kelgusida kiberxavfsizlikni ta'minlash bo'yicha siyosat va amaliyotda sun'iy intellekt asosidagi monitoring, hodisalarni erta aniqlash, xavf-xatarlarni bashoratlash hamda foydalanuvchiga yo'naltirilgan xavfsizlik ta'limi yanada muhim ahamiyat kasb etadi. Shu bois har bir tashkilot va har bir foydalanuvchi ma'lumotlar xavfsizligini davriy emas, balki uzluksiz boshqaruv jarayoni sifatida qabul qilishi lozim.

Foydalanilgan adabiyotlar

1. Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson.
2. Stallings, W., Brown, L. Computer Security: Principles and Practice. Pearson.
3. Whitman, M. E., Mattord, H. J. Principles of Information Security. Cengage.
4. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
5. Rhodes-Ousley, M. Information Security: The Complete Reference. McGraw-Hill.
6. Kahate, A. Cryptography and Network Security. McGraw-Hill Education.