AXBOROT XAVFSIZLIGI VA SHAXSIY MA'LUMOTLARNI HIMOYALASH TEXNOLOGIYALARI

Kodirova Malohat Komiljanovna
Andijon Ichki Ishlar akademik litseyi informatika fani o'qituvchisi

Annotatsiya: *Mazkur maqolada axborot xavfsizligi va shaxsiy ma'lumotlarni himoyalash texnologiyalarining dolzarbligi va ularni samarali qo'llash yo'llari tahlil qilinadi. Bugungi raqamli transformatsiya jarayonida davlat muassasalari, tijorat tashkilotlari va jismoniy shaxslar uchun axborot xavfsizligi eng muhim ustuvor yo'nalishlardan biri sifatida namoyon bo'lmoqda. Maqolada kriptografiya, autentifikatsiya, biometrik xavfsizlik, xavfsiz tarmoqlar, bulutli muhitda himoya, xavf tahlili va monitoring tizimlari kabi texnologik yondashuvlar ko'rib chiqiladi. Tadqiqotda mavjud muammolar va tahdidlar bilan bir qatorda, zamonaviy yechimlar ham tahlil qilinadi.*

Kalit so'zlar: *Axborot xavfsizligi, shaxsiy ma'lumotlar, kriptografiya, autentifikatsiya, kiberxavfsizlik, ma'lumotlarni shifrlash, tarmoq xavfsizligi.*

ulkan hajmdagi axborot resurslari bilan ishlamoqda. Shu bilan birga, bu axborotlarning, ayniqsa shaxsiy ma'lumotlarning, noqonuniy foydalanilishi, o'g'irlanishi yoki tarqalishi bilan bog'liq xavflar keskin oshdi. Global miqyosda kiberjinoyatlar sonining ortib borayotgani, axborot tizimlariga hujumlarning murakkablashgani shaxsiy va institutsional ma'lumotlarni himoya qilish zaruratini dolzarb masalaga aylantirmoqda.

Axborot xavfsizligi — bu axborotni ruxsatsiz kirish, o'zgartirish, yo'q qilish yoki tarqatishdan himoya qilishga qaratilgan kompleks chora-tadbirlar majmui bo'lib, u kriptografiya, autentifikatsiya, tarmoq xavfsizligi, xavfni tahlil qilish va monitoring qilish texnologiyalarini o'z ichiga oladi. Ayniqsa, shaxsiy ma'lumotlarni himoyalash sohasida xalqaro standartlar (masalan, ISO/IEC 27001), milliy qonunchilik va axloqiy me'yorlar asosida yondashuv zarurati ortib bormoqda.

Shaxsiy ma'lumotlar bugungi kunda eng muhim axborot aktivlaridan biri hisoblanadi. Ularning saqlanishi va uzatilishi bilan bog'liq xavfsizlik choralarini qo'llashda zamonaviy texnologiyalar hal qiluvchi rol o'ynaydi. Jumladan:

Kriptografik texnologiyalar

Kriptografiya axborotni shifrlash va ruxsatsiz kirishdan himoya qilish uchun mo'ljallangan matematik usullar va algoritmlar tizimidir. Bu texnologiya orqali yuborilayotgan yoki saqlanayotgan ma'lumotlar shifrlanadi va faqat ruxsat etilgan tomonlar tomonidan qayta ochilishi mumkin.

Asosiy algoritmlar:

AES (Advanced Encryption Standard) – 128, 192 yoki 256 bitli kalitlardan foydalanadigan simmetrik shifrlash algoritmi. Ko'plab hukumatlar va banklar tomonidan standart sifatida tan olingan.

RSA (Rivest-Shamir-Adleman) – assimetrik kriptografiyaga asoslangan bo‘lib, kalitlar juftligi (ochiq va maxfiy) orqali ishlaydi. Elektron imzolar, xavfsiz kalit almashinuvi va autentifikatsiyada keng qo‘llaniladi.

SHA (Secure Hash Algorithm) – bu algoritmlar ma’lumotni bitta noyob “xesh” (hash) qiymatiga aylantiradi. SHA-256, masalan, blokcheyn tizimlarida ishonchli tranzaktsiyalarni kafolatlash uchun qo‘llaniladi.

Amaliyotda kriptografiya nafaqat maxfiylikni, balki ma’lumotlarning yaxlitligi va autenfikligini ham ta’minlaydi

Autentifikatsiya va identifikatsiya tizimlari

Autentifikatsiya — bu foydalanuvchining kimligini tekshirish jarayonidir. Zamonaviy tizimlar bir nechta bosqichli va kombinatsiyalangan autentifikatsiya usullarini qo‘llaydi.

Turlari:

Bir bosqichli (Single-factor authentication) – odatda faqat parolga asoslanadi. Bu usul oddiy, ammo xavfsizlik darajasi past bo‘lishi mumkin.

Ko‘p bosqichli autentifikatsiya (MFA – Multi-Factor Authentication) – foydalanuvchidan bir nechta omillar talab qilinadi:

Nimani bilasiz? (parol)

Nimani egallagansiz? (telefon, karta)

Kimsiz? (biometrik belgi – barmoq izi, yuz skaneri)

Zamonaviy autentifikatsiya texnologiyalari:

OTP (One-Time Password) – vaqtga asoslangan bir martalik kodlar.

Biometrik autentifikatsiya – barmoq izi, yuz aniqlash, retina skaneri.

Afzalliklari: Ko‘p bosqichli autentifikatsiya tahdidlarning oldini oladi, ayniqsa, parol o‘g‘irlangan taqdirda ham himoyani saqlab qoladi.

Tarmoq xavfsizligi texnologiyalari

Tarmoq xavfsizligi – ma’lumotlar uzatish jarayonida tarmoq orqali amalga oshiriladigan har qanday ruxsatsiz kirish, tahlil yoki modifikatsiyaning oldini olishga qaratilgan texnologiyalar majmuasidir.

Muhim elementlar:

HTTPS (HyperText Transfer Protocol Secure) – veb-brauzerlar va serverlar o‘rtasidagi xavfsiz axborot almashinuvi uchun SSL/TLS shifrlashdan foydalanadi.

VPN (Virtual Private Network) – foydalanuvchi va tarmoq o‘rtasida shifrlangan, xavfsiz “tunel” yaratadi. Masofadan ishlashda ma’lumotlar himoyasi uchun juda foydali.

SSL/TLS (Secure Sockets Layer / Transport Layer Security) – internetda shifrlangan aloqani ta’minlaydi.

Firewall (Himoya devori) – tarmoq trafigini tahlil qiladi va zararli yoki ruxsatsiz kirishni bloklaydi.

IDS (Intrusion Detection Systems) – kiruvchi trafikni monitoring qiladi, tahdidli faoliyatni aniqlaydi va bu haqda ogohlantiradi.

Bu texnologiyalar tarmoq orqali ma’lumot o‘g‘irlanishini, man-in-the-middle (MITM) hujumlarini va zararli dasturlarning kirib kelishini oldini oladi.

Bulutli muhitdagi xavfsizlik – Bugungi kunda ko‘plab shaxsiy va korporativ ma’lumotlar bulutli platformalarda saqlanadi. Shu sababli, bulutli xavfsizlik choralarining kuchli bo‘lishi dolzarbdir (Zhou et al., 2010).

Qonunchilik va etik me’yorlar – Yevropa Ittifoqining GDPR reglamenti va boshqa xalqaro hujjatlar shaxsiy ma’lumotlar ustidan nazoratni mustahkamlab, foydalanuvchining axborot ustidan huquqini himoya qiladi.

Tadqiqotlar shuni ko‘rsatadiki, kompaniyalar yoki tashkilotlar axborot xavfsizligini ikkinchi darajali masala deb qaragan hollarda, katta moliyaviy va imij yo‘qotishlariga duch kelmoqda (Ponemon Institute, 2022). Shu sababli, texnologik, huquqiy va axloqiy yondashuvlarning uyg‘unligi axborotni samarali himoya qilishning muhim shartidir.

Axborot xavfsizligi zamonaviy raqamli jamiyatning eng muhim yo‘nalishlaridan biridir. Shaxsiy ma’lumotlarning keng miqyosda elektron muhitda saqlanishi, uzatilishi va qayta ishlanishi axborotni ruxsatsiz kirish, o‘g‘irlash yoki buzilish xavfiga duchor etadi. Mazkur maqolada tahlil qilingan kriptografik texnologiyalar (AES, RSA, SHA), ko‘p bosqichli autentifikatsiya tizimlari (OTP, biometrik xavfsizlik) hamda tarmoq xavfsizligi choralarining (VPN, SSL/TLS, IDS) joriy etilishi shaxsiy va korporativ ma’lumotlarni himoya qilishda muhim o‘rin tutadi.

Ushbu texnologiyalar orasidagi integratsiya, ularni kompleks tarzda qo‘llash axborot muhofazasining ishonchliligini sezilarli darajada oshiradi. Shu sababli, axborot xavfsizligi sohasi bo‘yicha mutaxassislar, IT infratuzilmani boshqaruvchilari va foydalanuvchilarning o‘zlari ham doimiy tarzda bilim va ko‘nikmalarini yangilab borishlari, xavfsizlik madaniyatini shakllantirishlari talab etiladi.

Axborot xavfsizligini ta’minlash — bu nafaqat texnologik, balki huquqiy, ijtimoiy va axloqiy muammolarni ham qamrab oladigan kompleks jarayondir. U milliy va global darajada doimiy nazorat va yondashuvni talab qiladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson Education. Kriptografiya va tarmoq xavfsizligi algoritmlarining nazariy va amaliy jihatlari tahlili.
2. Andress, J. (2019). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress. — Axborot xavfsizligining asosiy tamoyillari, real tahdidlar va himoya strategiyalari.
3. Pfleeger, C.P., & Pfleeger, S.L. (2015). Security in Computing. Prentice Hall. — Kompyuter tizimlarida xavfsizlikni ta'minlashga oid zamonaviy yondashuvlar.
4. Shavkatovna, T. M. (2024). ZAMONAVIY YONDASHUVLAR ASOSIDA BO’LAJAK O’QITUVCHILARNING NUTQ MADANIYATINI RIVOJLANTIRISH METODIKASI. TANQIDIY NAZAR, TAHLILIY TAFAKKUR VA INNOVATSION G ‘OYALAR, 1(3), 28-31.

5. Shavkatovna, T. M. (2024). INNOVATSION YONDASHUVLAR ASOSIDA BO'LAJAK O'QITUVCHILARNING NUTQ MADANIYATINI RIVOJLANTIRISH. MODERN PROBLEMS IN EDUCATION AND THEIR SCIENTIFIC SOLUTIONS, 1(3), 337-340.

6. LI, T., MN, A., & Shavkatovna, T. M. (2025). NUTQ BUZILISHLARINING KOMPLEKS KORREKSIYASI: LOGOPED VA OTA-ONANING HAMKORLIGI. TA'LIM, TARBIYA VA INNOVATSIYALAR JURNALI, 1(6), 66-69.

7. LI, T., MN, A., & Shavkatovna, T. M. (2025). NUTQ BUZILISHLARINING KOMPLEKS KORREKSIYASI: LOGOPED VA OTA-ONANING HAMKORLIGI. TA'LIM, TARBIYA VA INNOVATSIYALAR JURNALI, 1(6), 66-69.

8. Nasrullayev, E. (2021). ISTIQLOL DAVRI DRAMATURGIYASIDA NAVOIY TALQINI. Boshlang'ich ta'limda innovatsiyalar, (Архив№ 1).

9. Файзиллаева, С., & Тахирова, М. А. (2025, April). СОВЕРШЕНСТВОВАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОИЙ ПРИ ИЗУЧЕНИИ НАРЕЧИЯ РУССКОГО ЯЗЫКА. In CONFERENCE OF MODERN SCIENCE & PEDAGOGY (Vol. 1, No. 1, pp. 237-240).

10. Яценко, В., & Тахирова, М. А. (2025, April). ОСНОВНЫЕ ПОДХОДЫ К КЛАССИФИКАЦИИ ЭЛЛИПТИЧЕСКИХ КОНСТРУКЦИЙ. In CONFERENCE OF MODERN SCIENCE & PEDAGOGY (Vol. 1, No. 1, pp. 67-68).

11. Begmuradovich, S. A. (2025). EINSATZ VON INFORMATIONSTECHNOLOGIE IM FREMDSPRACHENUNTERRICHT. СОВРЕМЕННОЕ ОБРАЗОВАНИЕ И ИССЛЕДОВАНИЯ, 1(3), 97-102.

12. Bekmuradovich, S. A. (2025). The usage of modern educational technologies in teaching a foreign language in higher educational institutions. Ta'lim, tarbiya va innovatsiyalar jurnali, 1(2), 180-184.

13. Begmuradovich, S. A. (2023). INTEGRATION OF EDUCATIONAL PROCESS FORMS. PEDAGOGIKA, PSIXOLOGIYA VA IJTIMOIY TADQIQOTLAR| JOURNAL OF PEDAGOGY, PSYCHOLOGY AND SOCIAL RESEARCH, 2(2), 20-23.

14. Суяров, А. Б. (2025). ТЕХНОЛОГИИ ОРГАНИЗАЦИИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ. ZAMIN ILMIY TADQIQOTLAR JURNALI, 1(2), 9-15.

15. Суяров, А. Б. (2025). СОВРЕМЕННЫЕ МЕТОДЫ В МЕТОДИКЕ ПРЕПОДАВАНИЯ ИНОСТРАННЫХ ЯЗЫКОВ. YANGI O 'ZBEKISTON, YANGI TADQIQOTLAR JURNALI, 2(2), 217-225.