MULTIDISCIPLINARY JOURNAL: FUNDAMENTAL RESEARCH SCIENTIFIC JOURNAL
VOLUME 01. ISSUE 06. JUNE 2025.
ResearchBib Impact Faktor: 9.943 ISSN: 3060-513X

AXBOROT XAVFSIZLIGINI TA'MINLASHNING ZAMONAVIY YONDASHUVLARI VA MUAMMOLARI

Bekpo'latov Ozodbek Asqarali o'g'li
O'zbekiston jurnalistika va ommaviy kommunikatsiyalar universiteti

Anotatsiya: Mazkur ilmiy maqolada axborot xavfsizligi tushunchasi, uning mohiyati va dolzarbligi chuqur o‘rganiladi. Avvalo, axborot xavfsizligining asosiy komponentlari — maxfiylik, butlilik va mavjudlik (confidentiality, integrity, availability) — atroflicha sharhlanadi. Keyinchalik, zamonaviy axborot tizimlariga tahdid solayotgan omillar, jumladan, kiberjinoyatchilik, zararli dasturiy ta’minotlar, tarmoq hujumlari va ichki tahdidlar yoritiladi. Maqolada, shuningdek, texnik va notexnik himoya vositalari, kriptografik algoritmlar, autentifikatsiya tizimlari, xavfsizlik siyosati ishlab chiqish usullari va xavf-xatarlarni boshqarish mexanizmlari muhokama qilinadi. Xalqaro axborot xavfsizligi standartlari (masalan, ISO/IEC 27001) va milliy qonunchilik asosida xavfsizlikni ta’minlashda yondashuvlar qiyosiy tahlil qilinadi. Tadqiqot yakunida axborot xavfsizligini samarali tashkil etish bo‘yicha takliflar va amaliy tavsiyalar beriladi.

Kalit so‘zlar: Axborot xavfsizligi; kiberxavfsizlik; maxfiylik; ma’lumotlarni himoyalash; raqamli tahdidlar; tarmoq xavfsizligi; zararli dasturlar; autentifikatsiya; kriptografiya; xavf-xatarlarni boshqarish; axborot siyosati; ISO/IEC 27001; axborot tizimlari xavfsizligi; raqamli identifikatsiya; ma’lumotlar butligi.

Axborot texnologiyalari taraqqiyoti bilan bir qatorda, ularni suiiste’mol qilish holatlari, kiberjinoyatlar va ma’lumotlarga noqonuniy kirish holatlari ham ko‘payib bormoqda. Bugungi kunda axborot resurslari nafaqat iqtisodiy faoliyatda, balki siyosiy, ijtimoiy va madaniy sohalarda ham strategik ahamiyat kasb etadi. Axborot xavfsizligini ta’minlash — bu faqat texnik vositalarni joriy etish emas, balki tashkiliy, yuridik va axloqiy jihatlarni ham qamrab oluvchi kompleks faoliyatdir.

Zamonaviy tahdidlar, xususan, zararli dasturlar, fishing hujumlari, ijtimoiy muhandislik (social engineering), tarmoq hujumlari va raqamli josuslik axborot tizimlari barqarorligiga jiddiy xavf tug‘dirmoqda. Shu sababli, axborot xavfsizligi masalalari har qanday tashkilot strategiyasining muhim tarkibiy qismiga aylangan. Ushbu maqolada axborot xavfsizligining nazariy asoslari, amaliy xavflar, himoya usullari va yondashuvlar tizimli tarzda tahlil qilinadi.

Ushbu tadqiqotda axborot xavfsizligiga oid dolzarb muammolarni aniqlash va ularni bartaraf etish yo‘llarini o‘rganish uchun bir nechta ilmiy yondashuvlardan foydalanildi.

Avvalo, **analitik yondashuv** asosida axborot xavfsizligi sohasidagi ilmiy adabiyotlar, xalqaro standartlar (jumladan, ISO/IEC 27001) va amaliyotdagi xavfsizlik siyosatlari o‘rganildi. Shuningdek, turli davlat va xususiy tashkilotlarda qo‘llanilayotgan axborot xavfsizligi amaliyotlari qiyosiy tahlil qilindi.

Empirik tadqiqotlar doirasida foydalanuvchilar orasida so‘rovnomalar o‘tkazildi. Unda ularning axborot xavfsizligiga bo‘lgan yondashuvi, parol yaratish odatlari, ijtimoiy tarmoqlarda shaxsiy ma’lumotlar bilan ishlash madaniyati tahlil qilindi.

Vaziyatli tahlil (case study) metodi yordamida bir nechta real tashkilotlarda yuzaga kelgan axborot tahdidlariga nisbatan ko‘rilgan choralar tahlil qilindi.

Shuningdek, **statistik ma’lumotlar** asosida turli turdagi tahdidlar va ularning oqibatlari son jihatdan o‘rganildi va grafik shaklida tasvirlandi. Tadqiqot jarayonida axborot xavfsizligiga oid zamonaviy dasturiy vositalar (antivirus, tarmoq monitoringi, firewall) imkoniyatlari ham sinovdan o‘tkazildi.

Tadqiqot natijalari quyidagicha xulosa qilishga imkon berdi:

Axborot xavfsizligiga tahdid soluvchi asosiy omillar — foydalanuvchilarning e’tiborsizligi, parol siyosatining zaifligi, ijtimoiy muhandislik (social engineering) usullarining keng tarqalgani hamda texnik himoya vositalarining yetarlicha joriy qilinmagani hisoblanadi.

So‘rovnoma natijalariga ko‘ra, respondentlarning 65% hollarda oddiy yoki takrorlanuvchi parollardan foydalanishi aniqlangan. 42% foydalanuvchi esa o‘zining shaxsiy ma’lumotlarini ijtimoiy tarmoqlarda ochiq holatda saqlaydi.

Tashkilotlar faoliyatida xavfsizlik siyosati mavjud bo‘lsa-da, u amalda yetarli darajada bajarilmayotgani kuzatildi. Xodimlar uchun muntazam axborot xavfsizligi bo‘yicha treninglar yetarlicha yo‘lga qo‘yilmagan.

Qiyosiy tahlillar axborot xavfsizligi darajasini oshirishda texnik vositalar bilan bir qatorda inson omiliga asoslangan yondashuvlar — masalan, xodimlarni muntazam o‘qitish, xavfsizlik madaniyatini shakllantirish kabi choralar ham muhim rol o‘ynashini ko‘rsatdi.

Kriptografik himoya vositalari (AES, RSA, 2FA) tizim xavfsizligini sezilarli darajada oshirishi aniqlandi, biroq ularning to‘liq va samarali ishlashi uchun kompleks yondashuv zarur.

Tadqiqot davomida olingan ma’lumotlar shuni ko‘rsatadiki, zamonaviy jamiyatda axborot xavfsizligini ta'minlash nafaqat texnik, balki tashkiliy, psixologik va yuridik yondashuvlarni ham o‘z ichiga olishi kerak. Kiberxavflarning murakkab va tez o‘zgaruvchan tabiati bu sohadagi yondashuvlarni doimiy ravishda yangilab borishni talab qiladi.

Tadqiqot natijalari foydalanuvchilarning axborot xavfsizligiga nisbatan beparvoligi, parol siyosatining yetarli darajada amalga oshirilmasligi, xodimlar orasida axborot madaniyati yetarli darajada shakllanmaganligini ko‘rsatdi. Shuningdek, tashkilotlarda axborot xavfsizligi siyosatining mavjud bo‘lishi yetarli emas — uning amaliyotda qo‘llanishi va nazorat qilinishi ham muhim ahamiyatga ega.

Muhokama shuni ko‘rsatdiki, samarali xavfsizlik siyosatini yaratishda texnik vositalardan tashqari inson omilini boshqarish, xodimlarni doimiy o‘qitish va motivatsiyalash, ijtimoiy muhandislikka qarshi immunitet shakllantirish hal qiluvchi rol o‘ynaydi. Shuningdek, xalqaro tajriba va ISO/IEC 27001 kabi standartlarga mos yondashuvlar milliy kontekstda qo‘llanilsa, xavfsizlik darajasi sezilarli darajada oshishi mumkin.

Ushbu tadqiqot natijalariga asoslanib quyidagi xulosalar chiqarildi:

1. Axborot xavfsizligi – bu faqat texnik masala emas, balki inson omili, yuridik me’yorlar va tashkilotning umumiy madaniyati bilan chambarchas bog‘liq kompleks jarayondir.
2. Kiberxavflarning oldini olish uchun parol siyosatini mustahkamlash, foydalanuvchilarni muntazam ravishda o‘qitish, ikki bosqichli autentifikatsiya tizimlarini joriy etish va doimiy monitoring zarur.
3. Tashkilotlar axborot xavfsizligi siyosatini ishlab chiqish bilan cheklanib qolmasdan, ularni real amaliyotda qo‘llashi, xodimlar orasida nazorat va motivatsiya tizimini joriy etishi kerak.
4. Kriptografik vositalar va xavfsizlik protokollarining samarali ishlashi uchun ularni uzluksiz yangilab borish va axborot texnologiyalari sohasidagi yangiliklardan xabardor bo‘lish zarur.
5. Axborot xavfsizligini ta’minlashda xalqaro standartlar asosida harakat qilish, milliy qonunchilikni takomillashtirish va ko‘p darajali himoya tizimlarini yaratish bugungi kunda dolzarb vazifadir.

Foydalanilgan adabiyotlar

1. ISO/IEC 27001:2022 — *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*
2. Stallings, W. (2020). *Computer Security: Principles and Practice*. Pearson Education.
3. Schneier, B. (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley.
4. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
5. Касперская, Н. (2021). *Кибербезопасность: новые вызовы и решения*. Москва: Инфра-М.
6. Uzbekistan Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonuni, 2003-yil.
7. Jalolov, N. (2022). *Axborot xavfsizligi asoslari*. Toshkent: TDYU nashriyoti.
8. National Institute of Standards and Technology (NIST). (2022). *Framework for Improving Critical Infrastructure Cybersecurity*.
9. Whitman, M. E., & Mattord, H. J. (2017). *Principles of Information Security*. Cengage Learning.