AXBOROT TIZIMLARIDA KIBERXAVFSIZLIKNI TA’MINLASH USULLARI

Muallif: ***Zaripova Feruza Umidjon qizi***
Tashkilot: Buxoro davlat texnika universiteti, 708-22 ATT guruhi
Email: *zaripovaferuza60@gmail.com*

ANNOTATSIYA

Ushbu maqolada axborot tizimlarida kiberxavfsizlikni ta’minlashning asosiy usullari tahlil qilingan. Kriptografiya, autentifikatsiya, tarmoq xavfsizligi, zaxira nusxa olish va foydalanuvchilarni xabardor qilish kabi usullar samaradorlik nuqtayi nazaridan ko‘rib chiqildi. Natijalar shuni ko‘rsatadiki, kiberxavfsizlikni faqat kompleks yondashuv asosida ta’minlash mumkin. Shuningdek, kelajakda sun’iy intellekt va blokcheyn texnologiyalari yordamida axborot tizimlarini yanada samarali himoya qilish imkoniyatlari yoritilgan.

Kalit so'zlar: Axborot tizimlari, kiberxavfsizlik, kriptografiya, autentifikatsiya, tarmoq xavfsizligi, ma’lumotlarni zaxiralash, blokcheyn, sun’iy intellekt.

KIRISH

Hozirgi davrda axborot texnologiyalarining rivojlanishi insoniyat hayotining barcha sohalariga chuqur kirib bormoqda. Davlat boshqaruvi, ta’lim, sog‘liqni saqlash, moliya va biznes tizimlarining samarali ishlashi bevosita axborot tizimlariga bog‘liq. Shu bilan birga, kiberhujumlar sonining ortishi va ularning murakkablashuvi axborot tizimlarida kiberxavfsizlikni ta’minlash muammosini yanada dolzarb qilib qo‘ymoqda.

So‘nggi yillarda ma’lumotlarni o‘g‘irlash, firibgarlik, DDoS hujumlar va zararli dasturlar orqali ko‘plab korxonalar va tashkilotlarga zarar yetkazilmoqda. Masalan, xalqaro statistik ma’lumotlarga ko‘ra, 2024-yilda kiberjinoyatlar dunyo bo‘yicha iqtisodiyotga trillionlab dollar zarar yetkazgan. Shu sababli, axborot tizimlarini himoya qilishning samarali usullarini o‘rganish va qo‘llash muhim hisoblanadi.

Ushbu maqolaning maqsadi — axborot tizimlarida kiberxavfsizlikni ta’minlash usullarini tahlil qilish va ularning samaradorligini baholashdir

METODOLOGIYA

Axborot tizimlarida kiberxavfsizlikni ta’minlash uchun bir qator usullar qo‘llaniladi:

Kriptografiya (shifrlash) — ma’lumotlarni maxfiy holda uzatish va saqlash uchun matematik algoritmlar yordamida shifrlash texnologiyalari qo‘llaniladi. Masalan, AES va RSA algoritmlari.

AES (Advanced Encryption Standard) — simmetrik shifrlash algoritmi bo‘lib, bir xil kalit yordamida ham shifrlash, ham deshifrlash amalga oshiriladi. AES ma’lumotlarni 128-bitli bloklarga bo‘lib shifrlaydi va kalit uzunligiga qarab 10, 12 yoki 14 marta takrorlanadigan bosqichlardan o‘tadi.

AES juda tez ishlaydi va amaliyotda ko‘pincha **GCM (Galois/Counter Mode)** rejimida qo‘llaniladi. Bu nafaqat maxfiylik, balki ma’lumotning yaxlitligini ham ta’minlaydi. Shuningdek, disk shifrlash, VPN va TLS protokollarida keng ishlatiladi. AES xavfsizligi hozirgi kunda juda yuqori bo‘lib, asosiy xavf noto‘g‘ri implementatsiya (masalan, noto‘g‘ri IV ishlatish yoki zaif kalit yaratish) natijasida paydo bo‘ladi.

RSA (Rivest–Shamir–Adleman) esa asimmetrik shifrlash algoritmi bo‘lib, ikkita kalitdan foydalanadi:

- **Ochiq kalit** (public key) — ma’lumotni shifrlash yoki imzoni tekshirish uchun;
- **Yopiq kalit** (private key) — ma’lumotni ochish yoki imzo qo‘yish uchun.

RSA’da xavfsizlik katta sonlarni faktorlashning murakkabligiga asoslanadi. Odatda ma’lumot bevosita RSA bilan shifrlanmaydi, balki avval AES kaliti RSA orqali shifrlanadi, keyin katta ma’lumot AES bilan kodlanadi.

Amalda AES va RSA ko‘pincha birgalikda qo‘llanadi: RSA orqali kalit almashiladi, AES orqali esa asosiy ma’lumotlar tez va ishonchli shifrlanadi. **Autentifikatsiya va avtorizatsiya** — foydalanuvchini aniqlash va unga ruxsat darajasini belgilash orqali tizim xavfsizligi oshiriladi. Ikki bosqichli autentifikatsiya (2FA) keng qo‘llanilmoqda.

Ikki bosqichli autentifikatsiya (2FA) — bu foydalanuvchini tizimga kiritishda faqat parol emas, balki qo‘shimcha tekshiruv usuli ham ishlatiladigan xavfsizlik chorasi. Ya’ni, foydalanuvchi kirishda ikkita bosqichdan o‘tadi:

1. Birinchi bosqich — oddiy parol yoki login-parol kiritish.
2. Ikkinchi bosqich — qo‘shimcha tasdiqlash, masalan:
   - telefon raqamga yuborilgan SMS-kod;
   - mobil ilovada yaratiladigan vaqtinchalik kod (Google Authenticator, Duo va boshqalar);
   - barmoq izi yoki yuzni aniqlash (biometrik usul);
   - maxsus USB token yoki smart-karta.

Bunday autentifikatsiya tizim xavfsizligini sezilarli darajada oshiradi, chunki foydalanuvchining paroli o‘g‘irlangan taqdirda ham, qo‘shimcha kod yoki qurilmasiz tizimga kira olmaydi. Shu sababli, bank ilovalari, elektron pochta va ijtimoiy tarmoqlar keng qo‘llaydi.

Tarmoqlarni himoya qilish — firewall, IDS (Intrusion Detection System) va IPS

(Intrusion Prevention System) yordamida tarmoqqa ruxsatsiz kirishlarning oldi olinadi.
Zaxira nusxa olish (backup) va tiklash — kiberhujumlar natijasida yo‘qolgan yoki buzilgan ma’lumotlarni tiklash imkonini beradi.
Xodimlarni o‘qitish va xabardorlikni oshirish — kiberxavfsizlik siyosatining muhim qismi bo‘lib, foydalanuvchilarning xatolari ko‘pincha eng katta xavf manbai hisoblanadi.

NATIJALAR VA TAHLIL

O‘tkazilgan tahlillar shuni ko’rsatadiki:

- Kriptografiya ma’lumotlarning maxfiyligini saqlashda eng samarali vositalardan biri bo‘lib, u ko‘plab tizimlarda asosiy himoya mexanizmi sifatida qo‘llaniladi.
- Avtorizatsiya va autentifikatsiya foydalanuvchilarning ruxsatsiz kirishini kamaytiradi, ammo foydalanuvchi parolni zaif tanlasa, tizimning himoyasi pasayishi mumkin.
- IDS/IPS tizimlari tarmoqdagi hujumlarni tezkor aniqlaydi, biroq ularni to‘liq bartaraf etish uchun qo‘shimcha choralar talab etiladi.
- Zaxira nusxalar mavjud bo‘lsa, kiberhujum oqibatlarini tezda bartaraf etish mumkin. Masalan, “ransomware” hujumlaridan keyin backup nusxalari korxonani falokatdan saqlab qoladi.
- Xodimlarning xabardorligi oshirilgan tashkilotlarda phishing hujumlari sezilarli darajada kamaygan.

MUNOZARA

Kiberxavfsizlikni ta’minlashda yuqoridagi usullarning kompleks qo‘llanilishi muhim. Faqatgina bitta himoya chorasi bilan tizimni to‘liq himoya qilish mumkin emas.

Kelajakda sun’iy intellekt asosidagi hujumlar (AI-based attacks) kuchayishi kutilmoqda. Shu sababli, AI asosidagi himoya vositalarini ishlab chiqish dolzarb masalaga aylanmoqda. Masalan, neyron tarmoqlar asosida ishlaydigan anomaliya aniqlash tizimlari kiberhujumlarni oldindan bashorat qilishi mumkin.

Shuningdek, blokcheyn texnologiyasi ma’lumotlarni o‘zgarmas (immutable) shaklda saqlash imkoniyatini beradi va kiberxavfsizlikni mustahkamlash uchun istiqbolli yo‘nalishlardan biridir.

XULOSA

Xulosa qilib aytganda, axborot tizimlarida kiberxavfsizlikni ta’minlash zamonaviy jamiyat uchun zaruriy shartdir. Kriptografiya, autentifikatsiya, tarmoqni himoya qilish tizimlari, zaxira nusxa olish va foydalanuvchilarni xabardor qilish kabi choralar kompleks qo‘llanilganda yuqori samaradorlikka erishiladi.

Kelajakda yanada rivojlangan texnologiyalar — sun’iy intellekt, blokcheyn va “zero-trust security” modeli — kiberxavfsizlik sohasida asosiy rol o‘ynashi kutilmoqda. Shu bois, ilmiy izlanishlar va amaliy tadqiqotlarni kengaytirish dolzarbdir.

FOYDALANILGAN ADABIYOTLAR

1. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2020.
3. Pfleeger C., Pfleeger S., Margulies J. Security in Computing. Pearson, 2019.
4. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2021.
5. Эргашев А.Х., Норматов А. Axborot xavfsizligi asoslari. O‘quv qo‘llanma. Toshkent: TATU nashriyoti, 2019.
6. Xolmatov N., Rasulov F. Axborot texnologiyalarida xavfsizlik asoslari. O‘quv qo‘llanma. Toshkent: “Fan va texnologiya”, 2021.
7. Usmonov B., Islomov I. Axborot tizimlari va ularning xavfsizligi. O‘quv qo‘llanma. Samarqand: SamDU nashriyoti, 2020