ISSN 2181-

AXBOROT TIZIMLARIDA MA'LUMOTLARNI HIMOYA QILISH USULLARI.

Abdullayev Botirjon Mirzabaxrom o‘g‘li
Talaba, Andijon Davlat Texnika Inistituti

Annotatsiya. Ushbu tezisda axborot tizimlarida ma'lumotlarni himoya qilishning zamonaviy usullari va texnologiyalari tahlil qilinadi. Ma'lumot xavfsizligi sohasida uchraydigan asosiy xavflar, ularning oqibatlari va bularning oldini olish uchun qo‘llaniladigan usullar yoritiladi. Tadqiqotda kriptografik usullar, autentifikatsiya va tarmoq xavfsizligi texnologiyalari chuqur o‘rganiladi. Shuningdek, ma'lumotlarni shifrlash algoritmlari, tarmoq himoya protokollari va zararsizlantirish strategiyalari haqidagi bilimlar keltiriladi.

Kalit so‘zlar: axborot xavfsizligi, ma'lumotlarni himoya qilish, kriptografiya, autentifikatsiya, tarmoq xavfsizligi, xavf boshqaruvi.

Kirish. Axborot texnologiyalarining jadal rivojlanishi zamonaviy dunyo uchun yangi imkoniyatlar yaratmoqda, lekin shu bilan birga, axborot xavfsizligi sohasida ko‘plab muammolar va tahdidlarni ham keltirib chiqarmoqda. Har kuni bizneslar, davlat idoralari va oddiy foydalanuvchilar ulkan hajmdagi ma'lumotlarni yaratadi, saqlaydi va almashadi. Bunday ma'lumotlarning o‘z vaqtida va to‘g‘ri himoyalanmasligi ularga zarar yetishi yoki yo‘qotilishiga olib kelishi mumkin, bu esa iqtisodiy zarar va obro‘ga putur yetkazadi.

Ma'lumotlarni himoya qilish usullarini chuqur o‘rganish nafaqat texnik yondashuvlar, balki strategik qarorlar qabul qilish uchun ham muhim ahamiyatga ega. Ushbu tadqiqotda axborot xavfsizligi tamoyillari – maxfiylik, yaxlitlik va mavjudlik asoslari ko‘rib chiqiladi, shuningdek, ularni ta'minlash uchun zamonaviy texnologiyalar va usullar tahlil qilinadi.

Tadqiqotning maqsadi – axborot tizimlarida qo‘llaniladigan himoya choralarini tahlil qilish va ularning samaradorligini oshirish usullarini tavsiya etishdir. Bu kirish

qismi tezisning asosiy mavzusi va muhim ahamiyatini tushuntirishga qaratilgan bo‘lib, keyingi bo‘limlarda keltiriladigan ilmiy izlanishlar va amaliy tavsiyalarga zamin yaratadi.

Ma'lumotlarni himoya qilishning asosiy tamoyillari

Axborot xavfsizligi sohasida ma'lumotlarni himoya qilishning asosiy tamoyillari – maxfiylik, yaxlitlik va mavjudlik (CIA triadasi) – asosiy o‘rinda turadi. Ushbu tamoyillar ma'lumotlarni samarali himoya qilish tizimini yaratish uchun zarur bo‘lgan asosiy elementlardir.

Maxfiylik ma'lumotlarning faqat ruxsat etilgan shaxslar tomonidan ko‘rilishi va ishlatilishini ta'minlaydi. Bu tamoyilni buzilishidan turli kiberhujumlar, jumladan, ma'lumotlarning noqonuniy ravishda o‘g‘irlanishi sabab bo‘lishi mumkin. Maxfiylikni ta'minlash uchun shifrlash algoritmlari, parol va autentifikatsiya tizimlari qo‘llaniladi.

Yaxlitlik ma'lumotlarning to‘g‘riligi va o‘zgartirilmagan holda saqlanishini ta'minlashni anglatadi. Bu tamoyil ma'lumotlarga noqonuniy kirish yoki tasodifiy o‘zgartirishlar tufayli yuzaga keladigan xatolarni aniqlash uchun muhimdir. Yaxlitlikni ta'minlashda kriptografik hash funksiyalari, raqamli imzolar va boshqa texnologiyalar ishlatiladi.

Mavjudlik ma'lumotlar va resurslarning foydalanuvchilarga kerakli vaqtda ochiq bo‘lishini ta'minlaydi. DDoS hujumlari va boshqa tarmoq xavflari mavjudlikni buzishi mumkin, shu sababli tarmoq xavfsizligi va zahira nusxalar yaratish texnologiyalari ushbu tamoyilni qo‘llab-quvvatlash uchun zarur.

Kriptografik usullar va ma'lumotlarni shifrlash

Kriptografiya ma'lumotlarni himoya qilishning eng asosiy usullaridan biri bo‘lib, u ma'lumotlarni shifrlash orqali ularning maxfiyligini ta’minlaydi. Kriptografik usullar ikki asosiy turga bo‘linadi: simmetrik va assimetrik shifrlash.

Simmetrik shifrlashda bitta kalitdan foydalaniladi, ya'ni ma'lumotlarni shifrlash va deshifrlash uchun bitta kalit ishlatiladi. Bu turdagi algoritmlar oddiyligi va yuqori tezligi bilan ajralib turadi. AES (Advanced Encryption Standard) simmetrik

shifrlashning eng keng tarqalgan turlaridan biri bo‘lib, u zamonaviy axborot tizimlarida yuqori xavfsizlikni ta'minlaydi.

Assimetrik shifrlashda esa ikkita kalit qo‘llaniladi – ochiq va yopiq kalit. Ochiq kalit ma'lumotlarni shifrlash uchun ishlatilsa, yopiq kalit ma'lumotlarni deshifrlash uchun qo‘llaniladi. RSA (Rivest-Shamir-Adleman) algoritmi assimetrik shifrlashning eng mashhur misolidir va ko‘pincha ma'lumotlarni uzatishda xavfsizlikni ta'minlashda ishlatiladi.

Hashlash funksiyalari ham ma'lumotlarning yaxlitligini ta'minlashda muhim ahamiyatga ega. SHA-256 (Secure Hash Algorithm), masalan, ma'lumotlarning o‘zgarmasligini tekshirish va tasdiqlashda keng qo‘llaniladi. Hashlash orqali ma'lumotlarning qisqa, lekin o‘zgarmas o‘lchamdagi qiymati yaratiladi, bu esa ma'lumotlarning noto‘g‘ri yoki o‘zgartirilganligini aniqlash imkonini beradi.

Shuningdek, kriptografik protokollar, masalan, SSL/TLS (Secure Sockets Layer/Transport Layer Security), internet orqali ma'lumotlarni uzatishda xavfsizlikni ta’minlash uchun qo‘llaniladi. Ushbu protokollar tarmoqdagi ma'lumotlarning maxfiyligi va yaxlitligini himoya qiladi.

Tarmoq xavfsizligi va autentifikatsiya

Axborot tizimlarida ma'lumotlarni himoya qilishda tarmoq xavfsizligi va autentifikatsiya tizimlari muhim rol o‘ynaydi. Tarmoq xavfsizligi turli texnologiyalar, usullar va siyosatlarni o‘z ichiga olib, ma'lumotlarning tarmoq orqali uzatilishida himoya qilinishini ta'minlaydi. Autentifikatsiya esa foydalanuvchilarni aniqlash va ularga ruxsat berilgan resurslarga kirishni nazorat qilish jarayonidir.

Tarmoq himoyasi texnologiyalari xavfsizlik devorlari (firewalls), kirish aniqlash va oldini olish tizimlari (IDS/IPS), hamda VPN (Virtual Private Network) kabi texnologiyalarni o‘z ichiga oladi. Xavfsizlik devorlari tarmoqdan kiruvchi va chiquvchi trafikni nazorat qilish uchun ishlatiladi va u noto‘g‘ri kirishlarning oldini olishga yordam beradi. IDS/IPS tizimlari esa tarmoqqa kiruvchi tahdidlarni aniqlaydi va ularga qarshi chora ko‘radi.

DDoS (Distributed Denial of Service) hujumlari tarmoq xavfsizligi uchun katta tahdidlardan biri bo‘lib, ular tarmoq yoki serverlarni haddan tashqari yuklash orqali ishdan chiqarishga qaratilgan. Bunday hujumlardan himoyalanish uchun yuklamani muvozanatlash texnologiyalari va hujumlarni aniqlash tizimlari ishlatiladi.

Autentifikatsiya va identifikatsiya tizimlari foydalanuvchilarni aniqlash va ularning kirish huquqlarini tekshirishda muhim ahamiyatga ega. Zamonaviy autentifikatsiya usullari orasida ko‘p faktorli autentifikatsiya (MFA) va yagona kirish tizimi (SSO) mavjud. MFA foydalanuvchilarni identifikatsiya qilishda bir nechta omildan, masalan, parol va SMS-kod yoki biometrik ma'lumotlardan foydalanishni ta’minlaydi. Bu tizimlar ma'lumotlarning maxfiyligi va xavfsizligini yanada oshiradi.

SSL/TLS protokollari ma'lumotlarni uzatishda tarmoq orqali himoyalangan kanal yaratishga imkon beradi. Bu protokollar ma'lumotlarning maxfiyligini saqlash va ularni tarmoqqa tushgan paytda uchinchi tomonlar tomonidan o‘qib bo‘lmasligini ta’minlaydi.

FOYDALANILGAN ADABIYOTLAR

1. G‘ulomov, S. S., & Raximov, A. T. (2010). ***Axborot texnologiyalari va tizimlari***. Toshkent: O‘zbekiston Milliy Universiteti nashriyoti. — Ushbu kitob axborot texnologiyalari asoslari va ularning amaliy qo‘llanilishiga bag‘ishlangan.

2. Karimov, B. E., & Hamdamov, N. X. (2015). ***Axborot xavfsizligi va kriptografiya asoslari***. Toshkent: Toshkent axborot texnologiyalari universiteti. — Kriptografik usullar va axborot xavfsizligi tamoyillari haqida.

3. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. Pearson Education. — Axborot xavfsizligi va shifrlash algoritmlari bo‘yicha fundamental qo‘llanma.

4. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley. — Shifrlash usullari va ma'lumotlarni himoya qilishda foydalaniladigan protokollar haqida batafsil ma'lumot.

FOYADALANILGAN INTERNET RESURSLARI

1. OWASP Foundation. (2023). Open Web Application Security Project (OWASP).
2. NIST. (2023). National Institute of Standards and Technology (NIST) Cybersecurity Framework.
3. Kaspersky. (2023).
4. **Cisco Networking Academy.**