ZAMONAVIY TEXNOLOGIYALAR ASOSIDA HIMOYA (AXBOROT XAVFSIZLIGI VA DASTURLASHDA ZAMONAVIY YONDASHUVLAR)

Jaloldinova F.E.
Farg‘ona Davlat Texnika Universiteti
“Axborot texnologiyalari va telekommunikatsiya”
fakulteti 2-bosqich talabasi

Annotatsiya. Zamonaviy axborot tizimlarida ma’lumotlar xavfsizligini ta’minlash muhim masalalardan biri hisoblanadi. Axborot texnologiyalari tez sur’atlarda rivojlanib borayotgan bir davrda kiberxavfsizlikka bo‘lgan tahdidlar ham murakkablashib bormoqda. Shu sababli dasturiy tizimlar va tarmoq infratuzilmalarini himoya qilishda zamonaviy texnologiyalar va ilg‘or yondashuvlardan foydalanish zarur. Ushbu maqolada axborot xavfsizligini ta’minlashda qo‘llaniladigan asosiy texnologiyalar va usullar tahlil qilinadi. Jumladan, kriptografik himoya algoritmlari, autentifikatsiya mexanizmlari, rollarga asoslangan kirishni boshqarish modeli (RBAC), bulutli xizmatlarda ma’lumotlarni himoyalash hamda sun’iy intellekt yordamida xavfsizlik monitoringi masalalari yoritiladi. Shuningdek, ma’lumotlarni shifrlash, ikki faktorli autentifikatsiya va foydalanuvchi faoliyatini nazorat qilish kabi amaliy misollar orqali zamonaviy xavfsizlik mexanizmlarining qo‘llanish imkoniyatlari ko‘rsatib beriladi. Tadqiqot natijalari dasturiy tizimlar, veb-ilovalar va korporativ axborot infratuzilmalarida ma’lumotlar xavfsizligini oshirish, ruxsatsiz kirishlarning oldini olish hamda tizimlarning barqaror ishlashini ta’minlashda muhim ahamiyatga ega.

Kalit so‘zlar: Zamonaviy texnologiyalar, axborot xavfsizligi, dasturlash, kriptografiya, autentifikatsiya, RBAC, sun’iy intellekt, ma’lumotlarni himoya qilish

Kirish

Hozirgi davrda axborot texnologiyalarining jadal rivojlanishi natijasida turli sohalarda raqamli tizimlar keng qo‘llanilmoqda. Davlat boshqaruvi, ta’lim, sanoat, tibbiyot, bank-moliya tizimi hamda kundalik hayotda ko‘plab jarayonlar axborot tizimlari orqali amalga oshirilmoqda. Bunday tizimlarda katta hajmdagi ma’lumotlar

saqlanadi, qayta ishlanadi va uzatiladi. Shu sababli ushbu ma’lumotlarning xavfsizligini ta’minlash muhim masalalardan biri hisoblanadi. Axborot tizimlarining rivojlanishi bilan bir qatorda kiberxavfsizlikka tahdidlar ham ko‘payib bormoqda. Ruxsatsiz kirish, ma’lumotlarni o‘g‘irlash, zararli dasturlar va turli xil kiberhujumlar zamonaviy axborot tizimlari uchun jiddiy xavf tug‘diradi.

Axborot xavfsizligini ta’minlash uchun turli texnologik yondashuvlar va himoya mexanizmlaridan foydalaniladi. Zamonaviy dasturlash jarayonida xavfsizlik masalalarini dastur yaratishning dastlabki bosqichlaridan boshlab hisobga olish zarur. Chunki dasturiy tizimlarda yuzaga keladigan kichik xatoliklar ham katta xavfsizlik muammolariga olib kelishi mumkin.

Shu sababli kriptografiya, autentifikatsiya, foydalanuvchi huquqlarini boshqarish, tarmoq xavfsizligi hamda monitoring tizimlari kabi texnologiyalar axborot xavfsizligini ta’minlashda muhim o‘rin tutadi.

So‘nggi yillarda bulutli texnologiyalar va sun’iy intellekt asosidagi tizimlar ham axborot xavfsizligini ta’minlashda keng qo‘llanila boshladi. Bulutli xizmatlar ma’lumotlarni saqlash va ulardan foydalanishni osonlashtiradi, biroq ular bilan ishlash jarayonida ma’lumotlarni himoya qilish masalasi alohida e’tibor talab qiladi. Sun’iy intellekt texnologiyalari esa tizim faoliyatini tahlil qilish, anomal holatlarni aniqlash va kiberhujumlarni oldindan aniqlash imkoniyatini beradi.

Ushbu maqolaning maqsadi zamonaviy texnologiyalar asosida axborot xavfsizligini ta’minlash usullarini tahlil qilish hamda dasturlash jarayonida qo‘llaniladigan asosiy himoya mexanizmlarini ko‘rsatib berishdan iborat.

Shuningdek, kriptografik usullar, autentifikatsiya tizimlari, rollarga asoslangan kirishni boshqarish modeli hamda sun’iy intellekt asosidagi xavfsizlik monitoringi kabi yondashuvlarning amaliy ahamiyati yoritiladi.

Misol: Ma’lumotlarni shifrlash zamonaviy himoya texnologiyalarining asosiy qismidir. Masalan, **AES-256** algoritmi yordamida ma’lumotlarni shifrlash:

```python
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes

key = get_random_bytes(32)  # AES-256 uchun 32 bayt
cipher = AES.new(key, AES.MODE_EAX)
data = b"Maxfiy ma'lumot"
ciphertext, tag = cipher.encrypt_and_digest(data)
print(ciphertext)
```

Bu misol ma’lumotlarni ruxsatsiz foydalanuvchilar tomonidan o‘qilishidan himoya qiladi.

Zamonaviy tizimlarda ikki faktorli autentifikatsiya (2FA) xavfsizlikni oshiradi. Masalan, foydalanuvchi login va parol bilan kirgach, SMS yoki mobil ilova orqali tasdiqlash kodi talab qilinadi.

```python
import pyotp
totp = pyotp.TOTP("base32secret3232")
print(totp.now())  # Har 30 soniyada yangi kod hosil qiladi
```

RBAC yordamida tizim foydalanuvchilari turli rollarga ajratiladi va ularga faqat zarur huquqlar beriladi:

Administrator – barcha funksiyalar

Dasturchi – ma’lumotlarni o‘qish va yangilash

Oddiy foydalanuvchi – faqat o‘qish huquqi

```sql
CREATE ROLE 'developer';
GRANT SELECT, INSERT, UPDATE ON project_db.* TO 'developer';
GRANT 'developer' TO 'user1'@'localhost';
```

AI tizimlar tarmoq trafigini kuzatib, anomal faoliyatni aniqlashi mumkin. Masalan, noto‘g‘ri login urinishlari avtomatik ravishda bloklanadi.

```python
# Misol: oddiy barmoq izi autentifikatsiyasi (Python kutubxonasi)
from biometric_sdk import FingerprintScanner
scanner = FingerprintScanner()
if scanner.verify(user_id="12345"):
    print("Foydalanuvchi tasdiqlandi")
```

Yuz tanish, barmoq izi yoki ovoz orqali autentifikatsiya qilish tizimlari tizim xavfsizligini oshiradi:

Mobil ilovalar va smart qurilmalarda qo‘llaniladi

Ruxsatsiz kirish ehtimolini kamaytiradi

Xulosa

Zamonaviy texnologiyalar asosida ma’lumotlarni himoya qilish bir nechta jihatlarni o‘z ichiga oladi: kriptografiya, autentifikatsiya, RBAC, AI monitoringi va foydalanuvchi faoliyatini audit qilish. Ushbu yondashuvlar ma’lumotlar bazasi, veb-ilovalar va korporativ tizimlarda xavfsizlikni sezilarli darajada oshiradi. Misollar va amaliyotlar ko‘rsatadiki, zamonaviy texnologiyalar yordamida tizimni samarali himoya qilish va ruxsatsiz kirishlarni oldini olish mumkin. Kelajakda AI va avtomatlashtirilgan xavfsizlik tizimlari xavfsizlikni yanada kuchaytirishi kutilmoqda.

Foydalanilgan adabiyotlar

1. Stallings, W. (2022). *Cryptography and Network Security: Principles and Practice.* Pearson.
2. Schneier, B. (2019). *Applied Cryptography.* Wiley.
3. DuBois, P. (2019). *MySQL Cookbook.* O‘Reilly Media.
4. MySQL Documentation. (2025). Security Guidelines. Oracle. https://dev.mysql.com/doc/refman/8.0/en/security.html
5. Murach, J., & Murach, S. (2020). *Murach’s MySQL.* Mike Murach & Associates.
6. Kaspersky, E. (2021). *Modern Threats and Security Solutions.* Kaspersky Lab Publications.
7. Microsoft Docs. (2024). Role-Based Access Control (RBAC). https://learn.microsoft.com/en-us/azure/role-based-access-control/overview