GCCR

Global Conference on Contemporary Research

GLOBAL CONFERENCE ON CONTEMPORARY RESEARCH



CONFERENCE THEME:

SUSTAINABLE FUTURES:
INNOVATION, DIGITAL TRANSFORMATION AND GLOBAL COLLABORATION THROUGH CONTEMPORARY RESEARCH

INNOVATION | DIGITAL TRANSFORMATION | GLOBAL COLLABORATION | SUSTAINABLE FUTURES

JOURNAL

PEER-REVIEWED PROCEEDINGS

NOVEMBER 2026

TORONTO, CANADA

gccr.academy

BULUTLI TEXNOLOGIYALARDA AXBOROT XAVFSIZLIGINI TA'MINLASHNING ZAMONAVIY USULLARI VA MEXANIZMLARI

O'zbekiston davlat jahon tillari universiteti
Zamonaviy axborot texnologiyalari va sun'iy intellekt kafedrasi
dotsenti p.f..f.d (PhD) Mamarajabov Odil Elmurzayevich

Annotatsiya: Mazkur maqolada bulutli texnologiyalardan foydalanish jarayonida axborot xavfsizligini ta'minlashning zamonaviy usullari va mexanizmlari ilmiy-nazariy jihatdan tahlil qilinadi. Bulutli hisoblash muhitida ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash, foydalanuvchilarni autentifikatsiyadan o'tkazish, kirish huquqlarini boshqarish, kriptografik himoya vositalaridan foydalanish hamda kiberxavfsizlik tahdidlarining oldini olish masalalariga alohida e'tibor qaratiladi. Shuningdek, bulutli infratuzilmalarda uchraydigan asosiy xavfsizlik muammolari tasniflanib, ularni kamaytirishga qaratilgan kompleks himoya modeli taklif etiladi.

Kalit so'zlar: bulutli texnologiyalar, axborot xavfsizligi, bulutli hisoblash, kiberxavfsizlik, ma'lumotlarni shifrlash, autentifikatsiya, avtorizatsiya, ma'lumotlar maxfiyligi.

Bugungi raqamli transformatsiya jarayonida bulutli texnologiyalar axborot resurslarini saqlash, qayta ishlash va uzatishning muhim texnologik vositalaridan biriga aylandi. Mazkur texnologiyalar tashkilotlarga katta hajmdagi hisoblash resurslaridan masofaviy foydalanish, infratuzilma xarajatlarini kamaytirish va axborot tizimlarining moslashuvchanligini oshirish imkonini beradi.

Bulutli hisoblash texnologiyalarining keng joriy etilishi bilan bir qatorda axborot xavfsizligini ta'minlash muammosi ham dolzarb ahamiyat kasb etmoqda. Chunki ma'lumotlarning tashkilotning ichki infratuzilmasidan tashqarida, xizmat ko'rsatuvchi provayderlar tomonidan boshqariladigan muhitda saqlanishi yangi xavfsizlik talablarini yuzaga keltiradi.

Bulutli muhitda foydalanuvchi ma'lumotlarining ruxsatsiz qo'lga kiritilishi, hisob yozuvlarining buzilishi, noto'g'ri konfiguratsiya, zararli dasturlar, xizmat ko'rsatishni rad etish hujumlari va ma'lumotlar yo'qolishi kabi xavflar mavjud.

ENISA tomonidan e'lon qilingan kiberxavfsizlik tahdidlari tahlillarida ma'lumotlarga qarshi tahdidlar, ransomware, zararli dasturlar va xizmatlar mavjudligiga qaratilgan hujumlar muhim xavf omillari sifatida qayd etilgan [1].

Shu sababli bulutli texnologiyalardan samarali foydalanish nafaqat hisoblash resurslarini boshqarish, balki ularni kompleks axborot xavfsizligi mexanizmlari bilan himoyalashni ham talab qiladi.

Maqolaning maqsadi bulutli texnologiyalarda axborot xavfsizligini ta’minlashning zamonaviy mexanizmlarini tahlil qilish va ularning o‘zaro integratsiyasiga asoslangan himoya modelini ishlab chiqishdan iborat.

Tadqiqot jarayonida tizimli tahlil, qiyosiy tahlil, ilmiy umumlashtirish va konseptual modellashtirish metodlaridan foydalanildi.

Bulutli texnologiyalarda axborot xavfsizligi quyidagi uchta asosiy tamoyilga asoslanadi:

1. **Maxfiylik (Confidentiality)** – ma’lumotlardan faqat tegishli vakolatga ega foydalanuvchilarning foydalanishini ta’minlash.

2. **Yaxlitlik (Integrity)** – axborotning ruxsatsiz o‘zgartirilishi yoki buzilishining oldini olish.

3. **Mavjudlik (Availability)** – axborot resurslari va xizmatlarining zarur vaqtda foydalanuvchilar uchun ochiq bo‘lishini ta’minlash.

Ushbu tamoyillar CIA triadasi sifatida tanilgan bo‘lib, axborot xavfsizligini tashkil etishning fundamental asosini tashkil qiladi.

Bulutli muhitdagi asosiy xavfsizlik tahdidlari

Tahdid turi	Mazmuni	Himoyalash mexanizmi
Ma’lumotlar sizib chiqishi	Maxfiy axborotning ruxsatsiz tarqalishi	Shifrlash, DLP
Hisob yozuvining buzilishi	Foydalanuvchi hisobiga noqonuniy kirish	MFA
Noto‘g‘ri konfiguratsiya	Bulutli resurslarning xato sozlanishi	Konfiguratsiya auditi
Zararli dasturlar	Tizimga zarar yetkazuvchi dasturlar	Antimalware, monitoring
DDoS hujumlari	Xizmat mavjudligining buzilishi	Trafik filtrlash
Ma’lumotlarning yo‘qolishi	Axborot resurslarining tiklab bo‘lmaydigan yo‘qolishi	Backup va Recovery

Ma’lumotlarni kriptografik himoyalash. Bulutli texnologiyalarda axborot xavfsizligini ta’minlashning eng muhim usullaridan biri kriptografik himoya hisoblanadi. Kriptografik usullar ma’lumotlarni ruxsatsiz o‘qish va o‘zgartirishdan himoyalash imkonini beradi.

Ma’lumotlarni shifrlash ikki asosiy holatda amalga oshiriladi:

- Saqlash jarayonida shifrlash (Encryption at Rest).

• Uzatish jarayonida shifrlash (Encryption in Transit).

Saqlanayotgan ma’lumotlarni shifrlashda AES kabi simmetrik algoritmlardan, kalitlarni almashish va elektron imzo mexanizmlarida esa tegishli ochiq kalitli kriptografik usullardan foydalanish mumkin.

Bunda kriptografik kalitlarni xavfsiz saqlash va boshqarish alohida ahamiyatga ega. Kalitlarni boshqarish tizimi orqali kalitlarning yaratilishi, saqlanishi, yangilanishi va bekor qilinishi nazorat qilinadi.

Autentifikatsiya va avtorizatsiya mexanizmlari. Bulutli tizimlarda foydalanuvchining shaxsini tasdiqlash autentifikatsiya, uning qanday resurslardan foydalanishi mumkinligini aniqlash esa avtorizatsiya deb ataladi.

Ko‘p faktorli autentifikatsiya (MFA) foydalanuvchi hisoblarini himoyalashda muhim ahamiyatga ega. Ushbu mexanizm paroldan tashqari qo‘shimcha tasdiqlash omillaridan foydalanadi.

Role-Based Access Control (RBAC) modeli orqali foydalanuvchilarga ularning lavozimi yoki vazifalariga mos huquqlar beriladi. Bu esa ortiqcha vakolatlar berilishining oldini olishga yordam beradi.

Bulutli infratuzilmani monitoring qilish. Bulutli muhitda xavfsizlik holatini doimiy kuzatib borish tahdidlarni erta aniqlash imkonini beradi. Monitoring tizimlari foydalanuvchi faoliyati, tarmoq trafigi, tizim konfiguratsiyasi va ma’lumotlardan foydalanish holatlarini tahlil qiladi.

SIEM (Security Information and Event Management) texnologiyalari turli manbalardan xavfsizlik hodisalari haqidagi ma’lumotlarni yig‘ish, o‘zaro bog‘lash va tahlil qilish imkonini beradi.

Bulutli texnologiyalarda axborot xavfsizligini ta’minlashda texnik vositalar bilan bir qatorda tashkiliy va boshqaruv mexanizmlari ham muhim ahamiyatga ega.

Birinchidan, tashkilot bulutli xizmat provayderi bilan hamkorlik qilganda xavfsizlik bo‘yicha mas’uliyat taqsimotini aniq belgilashi kerak. Provayder infratuzilmaning muayyan qismlari uchun javobgar bo‘lishi mumkin, biroq foydalanuvchi hisoblari, ma’lumotlar va kirish siyosatining to‘g‘ri tashkil etilishi mijoz zimmasida ham qoladi.

Ikkinchidan, bulutli muhitda xavfsizlikni ta’minlash doimiy monitoring va audit jarayonlarini talab qiladi. Tizimdagi o‘zgarishlar, yangi foydalanuvchilar va ruxsatlar muntazam tekshirilishi lozim.

Uchinchidan, zaxiralash siyosatini ishlab chiqish zarur. Zaxira nusxalarini asosiy tizimdan mustaqil muhitda saqlash va tiklash jarayonlarini muntazam sinovdan o‘tkazish ma’lumotlar yo‘qolishi bilan bog‘liq xavflarni kamaytiradi.

Mualliflik taklifi sifatida bulutli infratuzilmalarda xavfsizlikning integratsiyalashgan boshqaruv modelini joriy etish taklif qilinadi. Ushbu modelda shifrlash, MFA, RBAC, SIEM, avtomatik konfiguratsiya nazorati va zaxiralash mexanizmlari yagona xavfsizlik siyosati asosida boshqariladi.

Xulosa. Bulutli texnologiyalarda axborot xavfsizligini ta’minlash raqamli infratuzilmaning barqaror ishlashini belgilovchi asosiy omillardan biridir. Tadqiqot davomida ma’lumotlarni kriptografik himoyalash, ko‘p faktorli autentifikatsiya, foydalanuvchi huquqlarini boshqarish, monitoring va zaxiralash mexanizmlarining ahamiyati tahlil qilindi.

Bulutli muhitda axborot xavfsizligi ko‘p qatlamli himoya tamoyiliga asoslanishi lozim.

Ma’lumotlarni saqlash va uzatish jarayonlarida shifrlash mexanizmlaridan foydalanish zarur.

MFA va RBAC kabi vositalar ruxsatsiz kirish xavfini kamaytiradi.

Monitoring va audit xavfsizlik hodisalarini o‘z vaqtida aniqlashga yordam beradi.

Zaxiralash va tiklash mexanizmlari axborot resurslarining uzluksizligini ta’minlaydi.

Shunday qilib, bulutli texnologiyalarda axborot xavfsizligini samarali tashkil etish texnologik, tashkiliy va boshqaruv mexanizmlarining o‘zaro integratsiyasini talab etadi.

Foydalanilgan adabiyotlar

1. Mamarajabov, M. E. (2021). *Sun’iy intellekt va ulkan ma’lumotlarni (Big Data) qayta ishlash texnologiyalari*. Toshkent: O‘zbekiston Milliy universiteti nashriyoti, 142-b.

2. Mamarajabov, O. E. (2022). Formation of students’ competence in the use of cloud technologies in the information educational environment. *World Bulletin of Social Sciences*, 8, 79–80.

3. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. 2024.

4. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020.

5. NIST. Security and Privacy Controls for Information Systems and Organizations. SP 800-53, Revision 5. 2020.

6. Chandramouli R., Butcher Z. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments. NIST SP 800-207A. 2023.

7. ENISA. Cloud Computing Security for SMEs. European Union Agency for Cybersecurity.