BULUTLI HISOBLASHDA XAVFSIZLIK: XAVF-XATARLAR VA ULARNI BOSHQARISH

Rahmonova Afruza
Qarshi davlat universiteti talabasi
afruzarahmonova7@gamil.com

Annotatsiya. *Ushbu maqolada bulutli hisoblash infratuzilmasida yuzaga keladigan xavfsizlik muammolari, kiberxavfsizlik tahdidlari va ularni boshqarish usullari keng tahlil qilinadi. Tadqiqot zamonaviy xavfsizlik strategiyalari, ma'lumotlarni shifrlash texnologiyalari, autentifikatsiya usullari va monitoring tizimlariga asoslangan. Shu bilan birga, real holatlar, statistik ma'lumotlar va ilmiy manbalar yordamida xavf-xatarlarni aniqlash va ularni kamaytirish usullari batafsil ko'rib chiqiladi.*

Kalit so'zlar: *bulutli hisoblash, kiberxavfsizlik, ma'lumotlar xavfsizligi, bulut infratuzilmasi, risklarni boshqarish, autentifikatsiya, shifrlash.*

Аннотация. В данной статье представлен всесторонний анализ проблем безопасности, угроз кибербезопасности и методов управления ими в инфраструктуре облачных вычислений. Исследование основано на современных стратегиях безопасности, технологиях шифрования данных, методах аутентификации и системах мониторинга. Одновременно подробно рассматриваются методы выявления и снижения рисков с использованием реальных сценариев, статистических данных и научных источников.

Ключевые слова: облачные вычисления, кибербезопасность, защита данных, облачная инфраструктура, управление рисками, аутентификация, шифрование.

Abstract. This article provides a comprehensive analysis of security issues, cybersecurity threats, and methods for managing them in cloud computing infrastructure. The research is based on modern security strategies, data encryption technologies, authentication methods, and monitoring systems. At the same time,

methods for identifying and mitigating risks using real-world scenarios, statistical data, and scientific sources are examined in detail.

Keywords: cloud computing, cybersecurity, data security, cloud infrastructure, risk management, authentication, encryption.

Kirish. So'nggi o'n yil ichida bulutli hisoblash texnologiyalari axborot tizimlarining markaziy elementi sifatida rivojlanmoqda. Bulutli hisoblash foydalanuvchilarga masofaviy serverlar resurslaridan internet orqali foydalanish imkonini beradi, bu esa IT xarajatlarini kamaytirish, xizmatlarning tezligini oshirish va ma'lumotlarni markazlashgan holda boshqarish imkonini yaratadi. Bulutli hisoblashning keng qo'llanilish sohalari: Bank tizimi: tranzaksiyalarni tezkor va xavfsiz bajarish, ma'lumotlar markazlashgan saqlanishi. Elektron tijorat: foydalanuvchi ma'lumotlari va tranzaksiyalarni saqlash. Sog'liqni saqlash: elektron tibbiy kartalar, ma'lumotlar zaxiralari va tahlil tizimlari. Ta'lim: masofaviy o'quv platformalari va resurslar. Bulutli hisoblashning rivojlanishi bilan birga, kiberxavfsizlik masalalari ham kuchaymoqda.

Bulutli muhitda xavfsizlik tahdidlari asosiy toifalarga bo'linadi.

1.Ma'lumotlarning sizib chiqishi – serverlar yetarlicha himoyalanmagan bo'lsa, hujumchilar maxfiy ma'lumotlarga kira oladi.

2.Ruxsatsiz kirish – foydalanuvchi hisoblariga noqonuniy kirish, ma'lumotlarni o'zgartirish yoki o'g'irlash xavfi.

3.DDoS hujumlari – server xizmatining vaqtincha to'xtashi va tizimning ishlamasligi.

4.Ichki tahdidlar – xodimlar yoki ichki foydalanuvchilar tomonidan ma'lumotlardan noto'g'ri foydalanish.

2-jadval. Bulutli muhitda xavfsizlik tahdidlari

Tahdid turi	Tavsifi	Oldini olish vositalari

Ma’lumotlar sizib chi-qishi	Maxfiy ma’lumotlarning oshkor bo’lishi	Shifrlash, autentifikatsiya, monitoring
Ruxsatsiz kirish	Tizimga noqonuniy kirish	MFA, kirish nazorati, audit
DdoS hujumlari	Server faoliyatining to’xtashi	Trafik filtratsiyasi, server klasterlash
Ichki tahdidlar	Xodimlar tomonidan noto’g’ri foydalanish	Xodimlarni o’qitish, log monitoring

Bulutli tizimlarda xavfsizlikni ta’minlash uchun asosiy vositalar:

1.Ma’lumotlarni shifrlash: AES, RSA, ECC algoritmlari yordamida ma’lumotlar xavfsizligi ta’minlanadi. Shifrlash ma’lumotlar uzatilishida va saqlanishida himoya qatlamini yaratadi.

2.Ko’p faktorli autentifikatsiya (MFA): Foydalanuvchi identifikatsiyasi bir nechta bosqichda tekshiriladi, ruxsatsiz kirish xavfi kamayadi.

3.Monitoring va audit tizimlari: Bulut infratuzilmasidagi jarayonlar real vaqt rejimida kuzatib boriladi, log fayllar tahlil qilinadi va potentsial tahdidlar aniqlanadi.

4.Zaxira nusxalar va Disaster Recovery: Ma’lumotlarni yo’qotishdan himoya qilish, tizim nosozliklarida tez tiklash imkonini beradi.

Bulutli muhitdagi xavf-xatarlarni boshqarish quyidagi jarayonlarni o’z ichiga oladi:

1.Xavf-xatarlarni identifikatsiya qilish: Tashkilot ichidagi va tashqaridagi xavf manbalarini aniqlash, tasniflash va prioritetlash.

2.Tahlil va baholash: Har bir xavfning ehtimoli va potentsial ta’sirini o’rganish.

3.Oldini olish strategiyalari: Shifrlash, MFA, DDoS himoyasi, tarmoq segmentatsiyasi, foydalanuvchi huquqlarini cheklash.

4.Monitoring va uzluksiz audit: Real vaqt kuzatuv, loglar tahlili va xavfsizlik hisobotlari.

5.Xodimlar malakasini oshirish: Ichki tahdidlardan himoya qilish uchun xodimlarni muntazam o'qitish va xavfsizlik madaniyatini shakllantirish.

Bosqich	Amalga oshirish usuli
Identifikatsiya	Xavf-xatarlar ro'yxatini tuzish
Tahlil	Risklarni baholash va prioritetlash
Oldini olish	Shifrlash, MFA, DdoS hImoyasi
Monitoring	Real vaqt kuzatuv, log tahlili, audit
Xodimlarni tayyorlash	Xavfsizlik bo'yicha treninglar

Xulosa

Bulutli hisoblash zamonaviy axborot tizimlarining ajralmas qismiga aylandi. Shu bilan birga, ma'lumotlarni himoya qilish va xavf-xatarlarni kamaytirish dolzarb masaladir. Tashkilotlar zamonaviy shifrlash texnologiyalari, ko'p faktorli autentifikatsiya, monitoring va audit tizimlarini integratsiya qilishi, xodimlarni muntazam o'qitishi zarur. Asosiy tavsiyalar: Bulutli muhitda ma'lumotlar shifrlanishi majburiy bo'lsin. MFA va kirish nazorati tizimlari barcha foydalanuvchilarga joriy etilsin. Real vaqt monitoring va log tahlili doimiy amalga oshirilsin. Ichki xodimlar xavfsizligi bo'yicha muntazam treninglar o'tkazilsin. Risklarni boshqarish strategiyasi har yili yangilanib tursin.

FOYDALANILGAN ADABIYOTLAR

1. Mell P., Grance T. The NIST Definition of Cloud Computing.
2. Stallings W. Network Security Essentials.
3. Hashizume K. Security Issues in Cloud Computing.
4. CSA Cloud Security Alliance Reports.
5. NIST Cloud Security Guidelines.
6. Zhang Q. Cloud Computing Research and Future Trends.
7. Pearson S. Privacy and Security for Cloud Computing.
8. Saidova D. Teaching Programming Collaboratively Through Google Colab AND Github Integration //Green Economy and Development. – T. 3. – №. 11. – C. 667884.
9. Saidova D. E. Analysis of the problems of the teaching object-oriented programming to students //International Journal of Social Science Research and Review. – 2022. – T. 5. – №. 6. – C. 229-234.