ZAMONAVIY KORXONALARDA BULUTLI HISOBLASH XAVFSIZLIGI MUAMMOLARI VA YECHIMLARI

Toirova Dilfuza Fayzullayevna
Ilmiy maslahatchi.
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali f.f.d. dotsent.
Murodov A'zamjon
Telefon raqam: +998945756761
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali talabasi.
E-pochta: murodovazamjon28@gmail.com
https://doi.org/10.5281/zenodo.20106038

Annotatsiya Ushbu maqolada zamonaviy korxonalarda bulutli hisoblash (cloud computing) texnologiyalaridan foydalanish jarayonida yuzaga keladigan xavfsizlik muammolari va ularni hal etishning zamonaviy usullari tahlil qilingan. An'anaviy infratuzilmadan bulutli arxitekturaga o'tish axborot xavfsizligi sohasida yangicha yondashuvlarni talab etmoqda. Maqola davomida ma'lumotlar sizib chiqishi (data breach), kiberhujumlar va noto'g'ri konfiguratsiyalar kabi asosiy tahdidlar ko'rib chiqiladi. Shuningdek, xavfsizlikni ta'minlashda shifrlash (encryption), identifikasiya va ruxsatlarni boshqarish (IAM), ko'p faktorli autentifikatsiya (MFA) hamda "Zero Trust" (Nol ishonch) modeli kabi texnologiyalarning o'rni ilmiy jihatdan asoslab berilgan. Sun'iy intellektning kiberxavfsizlikdagi roli va gibrid bulut tizimlaridagi xalqaro tajribalar chuqur yoritilgan.

Kalit so'zlar: Bulutli hisoblash, kiberxavfsizlik, ma'lumotlar sizib chiqishi, Zero Trust modeli, sun'iy intellekt, shifrlash, identifikasiyani boshqarish, gibrid bulut.

Cloud Computing Security Challenges and Solutions in Modern Enterprises

Annotation This article analyzes the security challenges that arise during the use of cloud computing technologies in modern enterprises and modern methods of solving them. The transition from traditional infrastructure to cloud architecture requires new approaches in the field of information security. Throughout the article, major threats such as data breaches, cyber attacks, and misconfigurations are considered. Furthermore, the role of technologies such as encryption, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), and the Zero Trust model in ensuring security is scientifically justified. The role of artificial intelligence in cybersecurity and international experiences in hybrid cloud systems are deeply highlighted.

Keywords: Cloud computing, cybersecurity, data breach, Zero Trust model, artificial intelligence, encryption, identity management, hybrid cloud.

Аннотация В данной статье анализируются проблемы безопасности, возникающие в процессе использования технологий облачных вычислений (cloud computing) на современных предприятиях, и передовые методы их решения. Переход от традиционной инфраструктуры к облачной архитектуре требует новых подходов в сфере информационной безопасности. В статье рассматриваются такие основные угрозы, как утечка данных (data breach), кибератаки и неправильная конфигурация. Кроме того, научно обоснована роль таких технологий, как шифрование (encryption), управление идентификацией и доступом (IAM), многофакторная аутентификация (MFA)

и модель "Zero Trust" (Нулевое доверие) в обеспечении безопасности. Глубоко освещены роль искусственного интеллекта в кибербезопасности и международный опыт использования гибридных облачных систем.

Ключевые слова: Облачные вычисления, кибербезопасность, утечка данных, модель Zero Trust, искусственный интеллект, шифрование, управление идентификацией, гибридное облако.

Kirish Axborot texnologiyalarining mislsiz sur'atlarda rivojlanishi biznes jarayonlarini avtomatlashtirish va raqamlashtirishda yangi ufqlarni ochib berdi. Xususan, bulutli hisoblash (cloud computing) texnologiyalari zamonaviy korxonalar uchun nafaqat qulaylik, balki iqtisodiy samaradorlikni ham ta'minlovchi asosiy vositaga aylandi. Jismoniy serverlar va murakkab apparat ta'minotiga bo'lgan tobe'likning kamayishi korxonalarga o'z resurslarini istalgan joydan va istalgan vaqtda boshqarish imkonini bermoqda. Biroq, ma'lumotlarning uchinchi tomon provayderlari serverlarida saqlanishi va tarmoq orqali uzatilishi kiberxavfsizlik masalasini har qachongidan ham jiddiyroq qilib qo'ydi. Bugungi kunda bulutli tizimlarning xavfsizligi faqatgina texnik masala bo'lib qolmay, balki butun bir biznesning yashovchanligini belgilab beruvchi strategik omilga aylangan.

Dolzarbligi Ushbu mavzuning dolzarbligi shundaki, global miqyosda yirik va o'rta korxonalar o'zlarining muhim ma'lumotlar bazalarini to'liq yoki qisman bulutli infratuzilmalarga ko'chirmoqda. Garchi bulut provayderlari yuqori darajadagi xavfsizlik choralarini taklif qilsalar ham, amaliyotda mijoz va provayder o'rtasidagi mas'uliyatning taqsimlanishidagi tushunmovchiliklar, tizim ma'murlari tomonidan yo'l qo'yiladigan xatolar tufayli yirik ma'lumotlar sizib chiqishi (data breach) holatlari tez-tez kuzatilmoqda. Korporativ ma'lumotlarning qiymati oshib borayotgan bir davrda, ularni ishonchli himoya qilish mexanizmlarini o'rganish va amaliyotga tatbiq etish o'ta muhim ahamiyat kasb etadi.

Maqsadi Maqolaning asosiy maqsadi zamonaviy korxonalarda bulutli hisoblash muhitida yuzaga keladigan potentsial xavf va tahdidlarni ilmiy-tahliliy o'rganish hamda ularni bartaraf etishga qaratilgan ilg'or texnologik yechimlarni (jumladan, AI, Zero Trust va IAM tizimlarini) tizimlashtirilgan holda taqdim etishdan iborat.

Asosiy qism

Bulutli hisoblash texnologiyalari o'zining mohiyatiga ko'ra, hisoblash resurslari (serverlar, saqlash omborlari, ma'lumotlar bazalari, tarmoqlar va dasturiy ta'minot) ni internet orqali taqdim etish modelidir. Ushbu model korxonalarga katta kapital xarajatlar qilsdan, zaruratga qarab o'sib yoki qisqarib boruvchi moslashuvchan IT-infratuzilmaga ega bo'lish imkonini beradi. Bugungi kunda jahon bozorida uchta yirik gigant – Amazon Web Services (AWS), Microsoft Azure va Google Cloud Platform (GCP) yetakchilik qilmoqda. Ushbu platformalar nafaqat ma'lumotlarni saqlash, balki murakkab mashinali o'qitish modellari, katta ma'lumotlar (Big Data) tahlili va narsalar interneti (IoT) kabi xizmatlarni ham bulutda taqdim etadi. Ammo infratuzilmaning bunday kengayishi xakerlar uchun hujum sirtining (attack surface) kattalashishiga ham olib keladi.

Zamonaviy korxonalarda cloud texnologiyalaridan foydalanish jarayonida duch kelinadigan eng katta xavfsizlik muammolaridan biri bu ma'lumotlar sizib chiqishi (data breach) hisoblanadi. Ma'lumotlarning tashqi muhitga chiqib ketishi ko'pincha bulut xizmatlarining noto'g'ri konfiguratsiya qilinishi oqibatida yuz beradi. Misol uchun, AWS S3 bulut omborlarining ochiq qoldirilishi natijasida bir qator yirik kompaniyalarning millionlab

mijozlari haqidagi shaxsiy ma'lumotlari o'g'irlanganligi haqida ko'plab xalqaro hisobotlar mavjud. Bundan tashqari, zararli dasturlar, to'lov talab qiluvchi viruslar (ransomware) va taqsimlangan xizmat ko'rsatishni rad etish (DDoS) hujumlari bulutli tizimlar uchun o'ta xavfli hisoblanadi.

Xavfsizlikni ta'minlash maqsadida qo'llaniladigan asosiy usullardan biri bu ma'lumotlarni shifrlash (encryption) texnologiyasidir. Ma'lumotlar tarmoq orqali uzatilayotganida (in transit) ham, serverlarda saqlanayotganida ham (at rest) kuchli kriptografik algoritmlar yordamida shifrlanishi shart. Bu jarayon hujumchilar ma'lumotlarni qo'lga kiritgan taqdirda ham, kalitsiz ularni o'qiy olmasligini kafolatlaydi. Shuningdek, tizimga ulanishni nazorat qilishda Identifikasiya va ruxsatlarni boshqarish (Identity and Access Management - IAM) siyosati markaziy o'rin tutadi. IAM tizimlari faqatgina vakolatli foydalanuvchilarning kerakli ma'lumotlarga kirishini ta'minlaydi. Buni kuchaytirish uchun esa Ko'p faktorli autentifikatsiya (MFA) joriy qilinadi, bu yerda foydalanuvchi tizimga kirish uchun paroldan tashqari yana bir tasdiqlovchi vositadan (masalan, mobil qurilmaga keluvchi kod yoki biometrik ma'lumot) foydalanishi talab etiladi.

An'anaviy xavfsizlik modellari "ishonchli ichki tarmoq" va "ishonchsiz tashqi tarmoq" tushunchalariga asoslangan edi. Biroq, bulut texnologiyalari va masofaviy ishlashning ommalashishi bu chegaralarni yo'qqa chiqardi. Shu sababli, bugungi kunda Zero Trust (Nol ishonch) modeli eng maqbul yechim sifatida ko'rilmoqda. Zero Trust konsepsiyasining asosiy qoidasi – "hech qachon ishonma, doim tekshir". Ushbu modelga ko'ra, korxona tarmog'ining ichida yoki tashqarisida bo'lishidan qat'i nazar, har bir foydalanuvchi, qurilma va ilova doimiy ravishda autentifikatsiyadan o'tkazilishi va xavfsizlik holati tasdiqlanishi kerak. Micro-segmentatsiya orqali tarmoq kichik bo'laklarga ajratiladi va bitta segmentga qilingan hujum butun tizimni izdan chiqarmasligi ta'minlanadi.

Korxonalarning katta qismi faqat bitta provayder xizmatiga bog'lanib qolishni istamaydi va shuning uchun gibrid (Hybrid) yoki ko'p bulutli (Multi-cloud) yondashuvlarni tanlaydi. Gibrid bulut korxonaning o'z serverlari (on-premise) va ommaviy bulut xizmatlarini birlashtirsa, multi-cloud bir nechta turli xil bulut provayderlaridan foydalanishni anglatadi. Bunday arxitektura biznesning barqarorligini oshirsa-da, turli platformalar o'rtasida ma'lumotlarni xavfsiz almashish murakkabligini keltirib chiqaradi. Bu jarayonda API xavfsizligi, ma'lumotlar sinxronizatsiyasidagi himoya mexanizmlari va markazlashtirilgan monitoring tizimlariga ehtiyoj ortadi.

Kiberhujumlarning tobora aqlli va murakkablashib borishi sun'iy intellekt (AI) va mashinali o'qitish (ML) texnologiyalarini kiberxavfsizlikka joriy etishni taqozo etmoqda. Sun'iy intellekt tarmoqdagi gigabaytlab log fayllarni soniyalar ichida tahlil qila oladi va inson ko'zi ilg'ay olmaydigan anomaliyalarni aniqlaydi. AI algoritmlari nafaqat yuz bergan hujumlarni aniqlash, balki kelajakdagi potensial xatarlarni bashorat qilish (predictive threat hunting) xususiyatiga ham ega. Ular noto'g'ri foydalanuvchi xulq-atvorini o'rganish orqali an'anaviy himoya tizimlarini chetlab o'tuvchi Zero-day (nol kun) hujumlarini tezkor bloklay oladi.

Xalqaro tajribaga nazar tashlaydigan bo'lsak, Yevropa Ittifoqida qabul qilingan GDPR (General Data Protection Regulation) kabi standartlar bulutdagi ma'lumotlarni himoyalashda yuridik jihatdan katta burilish yasadi. Jahonning yetakchi korxonalari nafaqat texnik, balki tashkiliy xavfsizlik choralarini – jumladan, xodimlarning kiber-gigiyena malakasini oshirish va xavfsizlik madaniyatini shakllantirishni doimiy nazorat qilib boradilar. Yirik korporatsiyalar

misolida ko'rish mumkinki, xavfsizlikni ta'minlash bu bir martalik jarayon emas, balki monitoring, tahlil va yangilanishlardan iborat uzluksiz sikldir.

Muhokama va Natijalar

Olib borilgan tahlillar shuni ko'rsatadiki, bulutli hisoblashda xavfsizlikni ta'minlash uchun faqatgina bitta vosita yordamida himoyalanish yetarli emas. Xavfsizlik yechimlari ko'p qatlamli (multilayered) bo'lishi talab etiladi. Zero Trust modelining korporativ muhitga tatbiq etilishi texnik jihatdan murakkab va dastlabki bosqichda katta mablag' talab qilsa-da, uzoq muddatda u korxonani millionlab dollar zarar keltirishi mumkin bo'lgan kiberhujumlardan asrab qoladi.

Muhokamalar markazida turadigan yana bir masala bu tizim unumdorligi va xavfsizlik o'rtasidagi muvozanatdir. Ma'lumotlarni haddan tashqari ko'p shifrlash va tinimsiz autentifikatsiya jarayonlari tizimning ishlash tezligini tushirib yuborishi, bu esa foydalanuvchilar qulayligiga salbiy ta'sir qilishi kuzatiladi. Ushbu muammoning zamonaviy yechimi sifatida sun'iy intellektga asoslangan kontekstga qarab moslashuvchi (context-aware) autentifikatsiya tizimlaridan foydalanish samarali natijalar bermoqda. Ya'ni, agar tizim foydalanuvchining harakatlarini odatiy deb topsa, qo'shimcha tekshiruvlarni qisqartiradi, shubhali harakat sezilganda esa zudlik bilan MFA talab qiladi. Amaliy va tahliliy natijalar gibrid bulut infratuzilmalarida markazlashtirilgan xavfsizlik monitoringi vositalari (masalan, SIEM – Security Information and Event Management) orqali tahdidlarga reaksiya bildirish vaqtini (incident response time) sezilarli darajada qisqartirish mumkinligini ko'rsatdi.

Xulosa

Xulosa qilib aytganda, zamonaviy korxonalar uchun bulutli texnologiyalar biznesni rivojlantirishning muqobilsiz yo'li bo'lib qolmoqda. Biroq, xavfsizlik muammolariga yuzaki yondashish katta iqtisodiy va reputatsion yo'qotishlarga olib kelishi muqarrar. Bulutli hisoblash muhitini himoya qilishda ma'lumotlar ob'ektlarini shifrlash, IAM tizimlarini to'g'ri sozlash hamda arxitekturani Zero Trust prinsiplari asosida qayta qurish zarurati har qachongidan ham dolzarbdir.

Sun'iy intellekt va avtomatlashtirilgan himoya tizimlarining kiberxavfsizlikka integratsiyasi kelajakda xavflarni oldindan aniqlash va neytrallashning eng samarali usuli bo'lib xizmat qiladi. Korxonalar bulut provayderi bilan tuziladigan kelishuvlarda umumiy javobgarlik (Shared Responsibility) modelini to'g'ri tushunishlari hamda o'z ma'lumotlari xavfsizligi uchun ichki siyosatlarni jahon standartlari (masalan, ISO/IEC 27001) asosida takomillashtirib borishlari lozim. Shu tariqa, innovatsion xavfsizlik choralari va inson omili xatarlarini minimallashtirish uyg'unligida xavfsiz raqamli transformatsiyaga erishish mumkin bo'ladi

Foydalanilgan adabiyotlar:

1.Mell, P., and Grance, T. (2011). The NIST Definition of Cloud Computing. Gaithersburg: National Institute of Standards and Technology, pp. 2–7.
2.Stallings, W. (2020). Cryptography and Network Security: Principles and Practice. 8th Edition. New York: Pearson Education, pp. 110–250.
3.Ganiyev, S. K., and Karimov, M. M. (2018). Axborot xavfsizligi asoslari. Toshkent: Aloqachi nashriyoti, s. 45–190.
4.Singh, A., and Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, pp. 88–115.

5.Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. Washington: U.S. Department of Commerce, pp. 10–55.
6.Xalilov, M., va Qodirov, A. (2022). Zamonaviy axborot tizimlarida ma'lumotlarni himoyalashning kriptografik usullari. Toshkent: Fan va Ta'lim, s. 15–90.
7.Abdullayev, R. (2021). Bulutli texnologiyalar va kiberxavfsizlikning huquqiy asoslari. Toshkent: Ilmiy nashriyot, s. 30–120.
8.Murodov, J. (2020). Raqamli iqtisodiyotda ma'lumotlar xavfsizligini ta'minlash metodologiyasi. Samarqand: Zarafshon nashriyoti, s. 50–165.