IQRO JURNALI , IQRO JOURNAL, ИКРО ЖУРНАЛИ
ISSN:2181-4341| wordlyknowledge.uz/index.php/iqro
Volume 21 Issue 2 May 2026

BULUTLI HISOBLASH (CLOUD COMPUTING) TEXNOLOGIYALARI YORDAMIDA KORPORATIV AXBOROT TIZIMLARINING XAVFSIZLIGINI TA'MINLASH VA MA'LUMOTLARNI HIMOYALASH USULLARI

Gulmirzayeva Zulayho Ko'klanboy qizi
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
magistri
gulmirzayevazulya@gmail.com
+998940477439
Doi; https://doi.org/10.5281/zenodo.20322987

Annotatsiya: Mazkur maqolada bulutli hisoblash texnologiyalarining korporativ axborot tizimlari xavfsizligini ta'minlashdagi o'rni va ma'lumotlarni himoyalash usullari tahlil qilinadi. Zamonaviy tashkilotlarda ma'lumotlar hajmining ortishi va masofaviy xizmatlardan foydalanish kengayishi natijasida axborot xavfsizligi masalalari dolzarb ahamiyat kasb etmoqda. Maqolada IaaS, PaaS va SaaS modellarida xavfsizlikni boshqarish, ma'lumotlarni shifrlash, autentifikatsiya, xavfsizlik monitoringi, tarmoq himoyasi va zaxiralash texnologiyalari ilmiy manbalar asosida yoritilgan. Shuningdek, xalqaro standartlar va statistik ma'lumotlar asosida bulutli infratuzilmada yuzaga keladigan tahdidlar hamda ularni bartaraf etish mexanizmlari ko'rib chiqilgan. Tadqiqot natijalari korporativ tizimlarda bulutli xavfsizlik mexanizmlaridan samarali foydalanish axborot resurslarini himoyalash darajasini oshirishini ko'rsatadi.
Kalit so'zlar: Bulutli hisoblash, Cloud Computing, axborot xavfsizligi, ma'lumotlarni himoyalash, shifrlash, autentifikatsiya, korporativ tizimlar, kiberxavfsizlik, bulutli xizmatlar, xavfsizlik monitoringi.

Аннотация: В данной статье анализируется роль технологий облачных вычислений в обеспечении безопасности корпоративных информационных систем и методы защиты данных. В современных организациях вопросы информационной безопасности приобретают особую актуальность в связи с увеличением объема данных и расширением использования удалённых сервисов. В статье на основе научных источников освещаются вопросы управления безопасностью в моделях IaaS, PaaS и SaaS, шифрования данных, аутентификации, мониторинга безопасности, защиты сетей и технологий резервного копирования. Также на основе международных стандартов и статистических данных рассмотрены угрозы, возникающие в облачной инфраструктуре, и механизмы их устранения. Результаты исследования показывают, что эффективное использование механизмов облачной безопасности в корпоративных системах повышает уровень защиты информационных ресурсов.
Ключевые слова: облачные вычисления, Cloud Computing, информационная безопасность, защита данных, шифрование, аутентификация, корпоративные системы, кибербезопасность, облачные сервисы, мониторинг безопасности.

Abstract: This article analyzes the role of cloud computing technologies in ensuring the security of corporate information systems and methods of data protection. In modern organizations, information security issues have become increasingly important due to the growing volume of data and the expanding use of remote services. The article, based on scientific sources, highlights security management in IaaS, PaaS, and SaaS models, data encryption, authentication, security monitoring, network protection, and backup technologies. In

addition, threats arising in cloud infrastructures and mechanisms for mitigating them are examined based on international standards and statistical data. The research results demonstrate that the effective use of cloud security mechanisms in corporate systems increases the level of protection of information resources.

Keywords: Cloud Computing, information security, data protection, encryption, authentication, corporate systems, cybersecurity, cloud services, security monitoring.

Kirish

Raqamli iqtisodiyotning rivojlanishi bilan korporativ axborot tizimlarida ma'lumotlarni saqlash, qayta ishlash va uzatish jarayonlari tobora ko'proq bulutli texnologiyalar asosida amalga oshirilmoqda. Bulutli hisoblash texnologiyasi foydalanuvchilarga internet orqali serverlar, dasturlar va ma'lumotlar bazalaridan foydalanish imkonini beradi [3]. Ushbu texnologiyalar tashkilotlarga xarajatlarni kamaytirish, tizimlarning moslashuvchanligini oshirish va ma'lumotlardan tezkor foydalanishni ta'minlash imkonini yaratadi.

Gartner kompaniyasi ma'lumotlariga ko'ra, 2025-yilga kelib global bulutli xizmatlar bozori hajmi 700 milliard AQSh dollaridan oshishi prognoz qilingan [4]. Shu bilan birga, bulutli infratuzilmadan foydalanishning ortishi axborot xavfsizligi bilan bog'liq xavflarni ham kuchaytirmoqda. Xususan, ma'lumotlarning noqonuniy qo'lga kiritilishi, DDoS hujumlari, zararli dasturlar va autentifikatsiya tizimlaridagi zaifliklar korporativ tizimlar uchun jiddiy tahdid hisoblanadi [5].

Bulutli muhitda ma'lumotlar uchinchi tomon serverlarida saqlanishi sababli ularning maxfiyligi, yaxlitligi va mavjudligini ta'minlash muhim vazifaga aylanadi. Shu sababli, korporativ axborot tizimlarida zamonaviy xavfsizlik mexanizmlarini qo'llash va xalqaro standartlarga mos himoya usullarini joriy etish zarur hisoblanadi [6].

Metodologiya

Tadqiqot davomida ilmiy adabiyotlar, xalqaro tashkilotlar hisobotlari hamda bulutli texnologiyalar bo'yicha statistik ma'lumotlar tahlil qilindi. Tadqiqot metodlari sifatida qiyosiy tahlil, statistik tahlil, tizimli yondashuv va ilmiy manbalarni o'rganish usullaridan foydalanildi.

Bulutli hisoblash xizmatlari uchta asosiy model asosida faoliyat yuritadi: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) va Software as a Service (SaaS) [7]. Ushbu modellar bo'yicha xavfsizlikni boshqarish mexanizmlari alohida o'rganildi.

Ma'lumotlarni himoyalash usullari sifatida quyidagi texnologiyalar tahlil qilindi:

- Simmetrik va assimetrik shifrlash algoritmlari;
- Ko'p faktorli autentifikatsiya (MFA);
- Virtual xususiy tarmoqlar (VPN);
- Tarmoq xavfsizlik devorlari (Firewall);
- IDS/IPS monitoring tizimlari;
- Zaxira nusxalash va avariyadan tiklash mexanizmlari [8].

Shuningdek, ISO/IEC 27001, NIST Cybersecurity Framework va Cloud Security Alliance standartlari asosida bulutli xavfsizlikning zamonaviy talablari o'rganildi [9].

Natijalar

Tahlillar natijasida bulutli hisoblash texnologiyalari korporativ tizimlar xavfsizligini oshirishda muhim ahamiyatga ega ekanligi aniqlandi. Xususan, ma'lumotlarni markazlashgan holda boshqarish va xavfsizlik monitoringini avtomatlashtirish tahdidlarni tez aniqlash imkonini beradi.

IBM Security hisobotiga ko'ra, 2024-yilda ma'lumotlar sizib chiqishi bilan bog'liq o'rtacha zarar miqdori 4,45 million AQSh dollarini tashkil etgan [10]. Tadqiqotlar shuni ko'rsatadiki,

kuchli shifrlash algoritmlaridan foydalanish ma’lumotlarning noqonuniy o‘g‘irlanish xavfini sezilarli darajada kamaytiradi.

Bulutli xavfsizlikda autentifikatsiya tizimlari muhim o‘rin tutadi. Microsoft ma’lumotlariga ko‘ra, ko‘p faktorli autentifikatsiya hisoblarni noqonuniy egallash holatlarining 99 foizini oldini olish imkonini beradi [11]. Shu sababli, zamonaviy korporativ tizimlarda MFA texnologiyasidan keng foydalanilmoqda.

Tarmoq xavfsizligini ta’minlashda firewall va IDS/IPS tizimlari samarali vosita hisoblanadi. Ushbu texnologiyalar tarmoqqa noqonuniy kirish urinishlarini aniqlash va bloklash imkonini beradi [12]. Bundan tashqari, SIEM (Security Information and Event Management) platformalari yordamida xavfsizlik hodisalarini real vaqt rejimida monitoring qilish mumkin.

Bulutli texnologiyalarda zaxiralash tizimlari ham muhim ahamiyatga ega. Amazon Web Services va Microsoft Azure platformalarida avtomatik backup va disaster recovery tizimlari qo‘llanilishi xizmatlarning uzluksizligini ta’minlaydi [13]

Tahlil va muhokama

Bulutli hisoblash texnologiyalarining jadal rivojlanishi zamonaviy korporativ axborot tizimlarida ma’lumotlarni boshqarish va saqlash usullarini tubdan o‘zgartirdi. An’anaviy lokal serverlarga asoslangan infratuzilmalardan farqli ravishda, bulutli texnologiyalar foydalanuvchilarga masofaviy serverlar orqali xizmatlardan foydalanish imkoniyatini beradi. Ushbu texnologik o‘zgarish tashkilotlarga moslashuvchanlik, iqtisodiy samaradorlik va resurslardan unumli foydalanish imkonini yaratgan bo‘lsa-da, axborot xavfsizligi bilan bog‘liq yangi tahdidlarni ham yuzaga keltirdi [1].

Bulutli hisoblash infratuzilmasida ma’lumotlar bir nechta geografik hududlarda joylashgan serverlarda saqlanishi mumkin. Bu esa ma’lumotlarning xavfsizligini boshqarishni murakkablashtiradi. Ayniqsa, xalqaro kompaniyalarda ma’lumotlarning turli mamlakatlar hududida joylashgan ma’lumot markazlarida saqlanishi milliy qonunchilik va xalqaro standartlar bilan bog‘liq muammolarni yuzaga keltiradi. Masalan, Yevropa Ittifoqining GDPR (General Data Protection Regulation) qoidalari foydalanuvchi ma’lumotlarini himoya qilish bo‘yicha qat’iy talablarni belgilaydi [2]. Shu sababli, korporativ tashkilotlar bulutli platformalarni tanlashda ma’lumotlarning qayerda saqlanishi va qanday himoya qilinishiga alohida e’tibor qaratmoqda.

Bulutli texnologiyalarda xavfsizlikni ta’minlashning asosiy tamoyillari maxfiylik (Confidentiality), yaxlitlik (Integrity) va mavjudlik (Availability) prinsiplariga asoslanadi. Ushbu CIA modeli axborot xavfsizligining fundamental konsepsiyasi sifatida qabul qilingan [3]. Maxfiylik ma’lumotlardan faqat ruxsat etilgan foydalanuvchilar foydalanishini ta’minlaydi. Yaxlitlik ma’lumotlarning noqonuniy o‘zgartirilmasligini nazorat qiladi. Mavjudlik esa tizim va xizmatlarning uzluksiz ishlashini anglatadi. Bulutli hisoblash muhitida aynan ushbu uch tamoyilning birgalikda ishlashi xavfsizlik darajasini belgilab beradi.

So‘nggi yillarda bulutli muhitdagi eng katta tahdidlardan biri noto‘g‘ri konfiguratsiya bilan bog‘liq holatlar hisoblanadi. Gartner tahlillariga ko‘ra, bulutli infratuzilmadagi xavfsizlik buzilishlarining katta qismi inson omili va noto‘g‘ri sozlangan tizimlar natijasida yuzaga kelmoqda [4]. Masalan, ochiq holatda qoldirilgan ma’lumotlar bazalari yoki noto‘g‘ri sozlangan bulutli saqlash xizmatlari orqali millionlab foydalanuvchilarning ma’lumotlari internetga sizib chiqishi kuzatilgan. Bu esa tashkilotlarning moliyaviy zarar ko‘rishiga va obro‘siga salbiy ta’sir ko‘rsatadi.

Bulutli xavfsizlikda ma’lumotlarni shifrlash eng muhim himoya mexanizmlaridan biri hisoblanadi. Zamonaviy bulutli platformalarda AES-256, RSA va ECC kabi kriptografik algoritmlar keng qo‘llaniladi [5]. AES-256 algoritmi yuqori darajadagi himoya imkoniyati sababli davlat va korporativ tizimlarda standart sifatida foydalaniladi. Shifrlash ikki asosiy

bosqichda amalga oshiriladi: ma’lumotlarni saqlash jarayonida (Data at Rest) va uzatish vaqtida (Data in Transit). Ma’lumotlarni uzatishda SSL/TLS protokollaridan foydalanish tarmoq orqali uzatilayotgan ma’lumotlarning maxfiyligini ta’minlaydi.

Bulutli texnologiyalarda autentifikatsiya va avtorizatsiya tizimlari xavfsizlikning muhim tarkibiy qismi hisoblanadi. Oddiy login-parol tizimlari bugungi kunda yetarli himoya darajasini ta’minlay olmaydi. Shu sababli, ko‘p faktorli autentifikatsiya (Multi-Factor Authentication – MFA) texnologiyasi keng joriy qilinmoqda [6]. Ushbu tizim foydalanuvchini identifikatsiya qilishda bir nechta bosqichdan foydalanadi: parol, SMS kod, biometrik ma’lumot yoki autentifikatsiya ilovasi. Microsoft Security ma’lumotlariga ko‘ra, MFA tizimi akkauntlarni noqonuniy egallash holatlarining 99 foizigacha oldini olishi mumkin [7].

Shuningdek, bulutli xavfsizlikda Zero Trust konsepsiyasi keng tarqalmoqda. Ushbu model “Hech kimga ishonma, har doim tekshir” tamoyiliga asoslanadi [8]. Zero Trust yondashuvi foydalanuvchilar va qurilmalarni tarmoq ichida joylashgan bo‘lsa ham doimiy ravishda tekshirib boradi. Bu esa ichki tahdidlarni kamaytirishda samarali hisoblanadi. An’anaviy xavfsizlik modellarida ichki tarmoq ishonchli deb hisoblangan bo‘lsa, Zero Trust konsepsiyasida barcha kirish urinishlari tekshiriladi va monitoring qilinadi.

Bulutli muhitdagi xavfsizlikni ta’minlashda tarmoq himoyasi ham muhim ahamiyatga ega. Firewall, IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) tizimlari tarmoqqa noqonuniy kirish urinishlarini aniqlash va oldini olish imkonini beradi [9]. Ayniqsa, DDoS hujumlari bulutli xizmatlar uchun katta xavf hisoblanadi. Distributed Denial of Service hujumlari serverlarni haddan tashqari yuklab, xizmatlarning ishlashini to‘xtatishga qaratilgan bo‘ladi. Amazon Web Services, Microsoft Azure va Google Cloud kabi platformalarda DDoS himoya xizmatlari integratsiyalashgan holda taqdim etiladi.

Sun’iy intellekt va mashinaviy o‘qitish texnologiyalarining rivojlanishi bulutli xavfsizlik tizimlarining samaradorligini oshirishga xizmat qilmoqda. AI asosidagi monitoring tizimlari tarmoqdagi anomal faoliyatni real vaqt rejimida aniqlash imkonini beradi [10]. Masalan, foydalanuvchi odatiy faoliyatidan farqli ravishda boshqa geografik hududdan tizimga kirishga urinsa, AI tizimi buni xavf sifatida baholashi mumkin. Ushbu texnologiyalar kiberhujumlarni erta aniqlash va avtomatik javob qaytarish imkoniyatini yaratmoqda.

Bulutli texnologiyalarda xavfsizlik monitoringi SIEM (Security Information and Event Management) platformalari orqali amalga oshiriladi. SIEM tizimlari turli manbalardan kelayotgan log ma’lumotlarini tahlil qilib, xavfsizlik hodisalarini markazlashgan holda nazorat qiladi [11]. Bu esa administratorlarga tahdidlarni tez aniqlash va zarur choralarni ko‘rish imkonini beradi. Korporativ tashkilotlarda SIEM tizimlari xavfsizlik operatsion markazlari (SOC) bilan birgalikda ishlatiladi.

Bulutli infratuzilmada ma’lumotlarni zaxiralash va avariyadan tiklash (Disaster Recovery) tizimlari ham muhim rol o‘ynaydi. Tabiiy ofatlar, texnik nosozliklar yoki kiberhujumlar natijasida ma’lumotlarning yo‘qolishi korporativ faoliyatga katta zarar yetkazishi mumkin [12]. Shu sababli, bulutli xizmat ko‘rsatuvchi provayderlar avtomatik backup va avariyadan tiklash xizmatlarini taklif qilmoqda. Disaster Recovery mexanizmlari ma’lumotlarni qisqa vaqt ichida tiklash imkonini beradi va xizmatlarning uzluksizligini ta’minlaydi.

Bulutli xavfsizlikning yana bir muhim jihati foydalanuvchi huquqlarini boshqarish bilan bog‘liq. Identity and Access Management (IAM) tizimlari foydalanuvchilarning tizimga kirish darajasini nazorat qiladi [3]. Ushbu tizim yordamida foydalanuvchilarga faqat zarur resurslardan foydalanish huquqi beriladi. Least Privilege prinsipi asosida foydalanuvchilarning ortiqcha huquqlarga ega bo‘lishining oldi olinadi. Bu esa ichki tahdidlarni kamaytirishga yordam beradi.

Korporativ axborot tizimlarida xavfsizlik siyosatini shakllantirish ham muhim ahamiyatga ega. ISO/IEC 27001 standarti axborot xavfsizligini boshqarish bo‘yicha xalqaro standart hisoblanadi [4]. Ushbu standart tashkilotlarga xavfsizlik siyosatini ishlab chiqish, xavflarni

baholash va nazorat mexanizmlarini joriy etish imkonini beradi. NIST Cybersecurity Framework esa xavfsizlikni boshqarishning amaliy yondashuvlarini taklif etadi.

Bulutli xavfsizlikning iqtisodiy jihatlari ham alohida e'tiborga loyiq. IBM Security hisobotlariga ko'ra, ma'lumotlar sizib chiqishi bilan bog'liq o'rtacha zarar miqdori millionlab dollarni tashkil etadi [5]. Shu sababli, tashkilotlar xavfsizlikka investitsiya kiritishni strategik zarurat sifatida baholamoqda. Bulutli xavfsizlikka yo'naltirilgan investitsiyalar uzoq muddatda moliyaviy yo'qotishlarning oldini olishga yordam beradi.

Bundan tashqari, bulutli xavfsizlikni ta'minlashda inson omili muhim rol o'ynaydi. Xodimlarning kiberxavfsizlik bo'yicha savodxonligi past bo'lsa, phishing, social engineering va zararli havolalar orqali tizimlarga noqonuniy kirish xavfi ortadi [6]. Shu sababli, korporativ tashkilotlarda muntazam ravishda xavfsizlik treninglari va auditlar o'tkazilishi tavsiya etiladi.

Kelajakda bulutli xavfsizlik texnologiyalarining rivojlanishi kvant kriptografiyasi, blockchain asosidagi autentifikatsiya va AI yordamida avtomatlashtirilgan himoya tizimlari bilan bog'liq bo'lishi kutilmoqda. Kvant hisoblash texnologiyalarining rivojlanishi mavjud shifrlash algoritmlariga tahdid tug'dirishi mumkin [7]. Shu sababli, post-kvant kriptografiyasi bo'yicha tadqiqotlar jadal olib borilmoqda.

Umuman olganda, bulutli hisoblash texnologiyalarida xavfsizlikni ta'minlash kompleks yondashuvni talab qiladi. Shifrlash, autentifikatsiya, monitoring, zaxiralash va xavfsizlik siyosatini birgalikda qo'llash orqali korporativ axborot tizimlarining himoya darajasini sezilarli oshirish mumkin. Zamonaviy raqamli iqtisodiyot sharoitida bulutli xavfsizlik tashkilotlarning barqaror faoliyat yuritishi va ma'lumotlar ishonchliligini ta'minlashning asosiy omillaridan biri bo'lib qolmoqda.

Xulosa

Bulutli hisoblash texnologiyalari korporativ axborot tizimlarini modernizatsiya qilish va ma'lumotlarni samarali boshqarishda muhim vosita hisoblanadi. Tadqiqot natijalari shuni ko'rsatdiki, bulutli infratuzilmada xavfsizlikni ta'minlash uchun shifrlash, ko'p faktorli autentifikatsiya, tarmoq monitoringi va zaxiralash texnologiyalaridan kompleks foydalanish zarur.

ISO/IEC 27001 va NIST standartlari asosida xavfsizlik siyosatini shakllantirish korporativ tizimlarning himoya darajasini oshiradi. Shuningdek, sun'iy intellekt asosidagi monitoring tizimlari tahdidlarni tezkor aniqlash va oldini olish imkonini beradi.

Kelgusida bulutli xavfsizlik texnologiyalarini yanada takomillashtirish, kvant shifrlash va AI asosidagi himoya tizimlarini joriy etish korporativ axborot tizimlarining barqarorligini oshirishda muhim rol o'ynaydi.

Foydalanilgan adabiyotlar ro'yxati

1. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2017. – pp. 45–78.
2. Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. Prentice Hall, 2016. – pp. 102–145.
3. Erl T., Puttini R., Mahmood Z. Cloud Computing: Concepts, Technology & Architecture. Pearson, 2018. – pp. 15–67.
4. Gartner Inc. Forecast Analysis: Public Cloud Services Worldwide, 2024. – pp. 8–15.
5. Easttom C. Cloud Computing Fundamentals. Pearson IT Certification, 2021. – pp. 90–126.
6. NIST. Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0, 2024. – pp. 12–39.
7. Hurwitz J., Bloor R., Kaufman M., Halper F. Cloud Computing for Dummies. Wiley Publishing, 2020. – pp. 55–110.

8. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing, 2023. – pp. 21–74.
9. ISO/IEC 27001:2022. Information Security Management Systems Requirements. ISO Organization, 2022. – pp. 5–32.
10. IBM Security. Cost of a Data Breach Report 2024. IBM Corporation, 2024. – pp. 3–29.
11. Microsoft Security. The Importance of Multi-Factor Authentication, 2023. – pp. 6–18.
12. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems. NIST Special Publication, 2019. – pp. 11–44.
13. Amazon Web Services. AWS Disaster Recovery Whitepaper, 2023. – pp. 17–48.