

## BULUTLI HISOBLASH XAVFSIZLIGI: MUAMMOLAR VA ULARNING YECHIMLARI

<sup>1</sup>Mamasoliyev Asilbek Azizbek o'g'li

Abdullayev Shaxriyor

O'zbekiston, Farg'ona

<sup>1</sup>Mamasoliyev Asilbek va Abdullayev Shaxriyor –

Farg'ona davlat texnika universiteti 3-bosqich

Kompyuter injenering It-Servis yo'nalishi talabasi [asilbekmi80@gmail.com](mailto:asilbekmi80@gmail.com)

**Annotatsiya.** So'nggi yillarda axborot texnologiyalarining jadal rivojlanishi natijasida bulutli hisoblash (cloud computing) texnologiyalari keng qo'llanila boshladi. Bulutli xizmatlar korxonalar, ta'lim muassasalari va individual foydalanuvchilar uchun qulayliklar yaratmoqda. Biroq, ushbu texnologiyaning keng tarqalishi bilan bir qatorda axborot xavfsizligi bilan bog'liq muammolar ham dolzarb ahamiyat kasb etmoqda. Ushbu maqolada bulutli hisoblash xavfsizligining asosiy muammolari, tahdid turlari va ularni bartaraf etish bo'yicha zamonaviy yechimlar tahlil qilinadi.

**Kalit so'zlar:** bulutli hisoblash, axborot xavfsizligi, ma'lumotlarni himoyalash, kiberxavfsizlik, autentifikatsiya, shifrlash

## БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ: ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

<sup>1</sup>Мамасолиев Асилбек Азизбек угли<sup>1</sup> Абдуллаев Шахрийор

Республика Узбекистан, г. Фергана

<sup>1</sup>Ферганский государственный технический университет, студент 3 курса  
направления «Компьютерная инженерия (IT-Service)»

[asilbekmi80@gmail.com](mailto:asilbekmi80@gmail.com)

В последние годы стремительное развитие информационных технологий привело к широкому внедрению облачных вычислений (cloud computing). Облачные сервисы предоставляют удобные возможности для хранения, обработки и удалённого доступа к данным, что делает их востребованными

среди предприятий, образовательных учреждений и индивидуальных пользователей.

Однако наряду с преимуществами активное использование облачных технологий сопровождается возникновением серьёзных проблем в области информационной безопасности. В данной статье рассматриваются ключевые проблемы безопасности облачных вычислений, основные виды угроз, а также современные методы и решения, направленные на обеспечение защиты данных в облачной среде.

**Ключевые слова:** облачные вычисления, информационная безопасность, защита данных, кибербезопасность, аутентификация, шифрование.

## CLOUD COMPUTING SECURITY: PROBLEMS AND THEIR SOLUTIONS

<sup>1</sup>Mamasoliyev Asilbek Azizbek o'g'li Abdullayev Shaxriyor

Uzbekistan, Fergana

<sup>1</sup>Fergana State Technical University, 3rd-year student

Department of Computer Engineering (IT Service) [asilbekmi80@gmail.com](mailto:asilbekmi80@gmail.com)

In recent years, the rapid development of information technologies has led to the widespread adoption of cloud computing technologies. Cloud services offer convenient solutions for data storage, processing, and remote access, making them highly attractive for enterprises, educational institutions, and individual users.

However, along with these advantages, the extensive use of cloud technologies has introduced significant challenges related to information security. This article analyzes the main security issues in cloud computing, identifies common types of threats, and examines modern approaches and solutions aimed at ensuring data protection in cloud environments.

**Keywords:** cloud computing, information security, data protection, cybersecurity, authentication, encryption.

**Kirish.** Axborot-kommunikatsiya texnologiyalarining rivojlanishi natijasida ma'lumotlarni saqlash, qayta ishlash va uzatishning yangi usullari paydo bo'ldi. Bulutli hisoblash texnologiyasi ana shunday innovatsion yechimlardan biri hisoblanadi. Bulutli hisoblash foydalanuvchilarga internet orqali serverlar, ma'lumotlar bazalari, tarmoqlar, dasturiy ta'minot va boshqa resurslardan foydalanish imkonini beradi [1]. Bugungi kunda Google Cloud, Amazon Web Services (AWS), Microsoft Azure kabi yirik bulutli platformalar dunyo miqyosida keng qo'llanilmoqda. Ta'lim tizimida, jumladan O'zbekiston oliy ta'lim muassasalarida ham bulutli texnologiyalar masofaviy ta'lim, elektron jurnal va axborot tizimlarida faol ishlatilmoqda. Biroq, ushbu texnologiyalardan foydalanish jarayonida ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash muhim muammolardan biri bo'lib qolmoqda [2]. Bulutli muhitda ma'lumotlar uchinchi tomon serverlarida saqlanishi sababli, axborot xavfsizligi masalasi yanada murakkablashadi. Shu boisdan, bulutli hisoblash xavfsizligini ta'minlash zamonaviy IT sohasining eng dolzarb masalalaridan biri hisoblanadi.

**Maqsad.** Ushbu maqolaning asosiy maqsadi — bulutli hisoblash tizimlarida yuzaga keladigan axborot xavfsizligi muammolarini aniqlash, ularning sabablarini tahlil qilish hamda ushbu muammolarni bartaraf etish bo'yicha samarali yechimlarni ilmiy asosda yoritishdan iborat. Shuningdek, maqola orqali:

- bulutli hisoblash modellari va ularning xavfsizlik jihatlari;
- asosiy xavf va tahdid turlari;
- zamonaviy himoya mexanizmlari;

Bulutli hisoblash tushunchasi va modellari: Bulutli hisoblash — bu hisoblash resurslarini (serverlar, saqlash xotirasi, tarmoqlar, dasturiy ta'minot) internet orqali talab asosida taqdim etish modelidir [3].

Xizmat ko'rsatish modellari:

1. IaaS (Infrastructure as a Service) – infratuzilma xizmat sifatida;
2. PaaS (Platform as a Service) – platforma xizmat sifatida;

3. SaaS (Software as a Service) – dasturiy ta'minot xizmat sifatida.

Joylashtirish modellari: Ommaviy bulut (Public Cloud), xususiy bulut (Private Cloud), gibrid bulut (Hybrid Cloud). Har bir model o'ziga xos xavfsizlik muammolariga ega bo'lib, ularni to'g'ri boshqarish talab etiladi [4]. Bulutli hisoblash xavfsizligidagi asosiy muammolar:

1. Ma'lumotlar maxfiyligining buzilishi: Bulutli muhitda ma'lumotlar masofaviy serverlarda saqlanadi. Bu esa ruxsatsiz kirish, ma'lumotlarning o'g'irlanishi xavfini oshiradi [5]. 2. Autentifikatsiya va avtorizatsiya muammolari: Zaif parollar, ikki faktorli autentifikatsiyaning yo'qligi foydalanuvchi akkauntlarining buzilishiga olib keladi [6]. 3. Ma'lumotlar yaxlitligining buzilishi: ma'lumotlarning o'zgartirilishi yoki buzilishi axborotning ishonchliligiga putur yetkazadi. 4. Xizmatdan voz kechish (DDoS) hujumlari: bulutli serverlarga katta hajmdagi so'rovlar yuborish orqali xizmatni ishdan chiqarish mumkin [7]. 5. Ichki tahdidlar: bulut provayderi xodimlari yoki tashkilot ichidagi foydalanuvchilar tomonidan sodir etiladigan xavflar [8].

Bulutli hisoblash xavfsizligini ta'minlash yechimlari:

1. Ma'lumotlarni shifrlash. Ma'lumotlarni uzatish va saqlash jarayonida kuchli kriptografik algoritmlardan foydalanish zarur [9].

2. Ko'p faktorli autentifikatsiya: Parolga qo'shimcha ravishda SMS, biometrik yoki token asosida himoya qilish.

3. Xavfsizlik siyosatini joriy etish: Tashkilotlarda axborot xavfsizligi bo'yicha aniq qoidalar ishlab chiqilishi lozim.

4. Zaxira nusxalar (backup)

Ma'lumotlarni muntazam zaxiralash orqali yo'qotish xavfini kamaytirish [10].

5. Tarmoq xavfsizligi vositalari: Firewall, IDS/IPS tizimlari orqali tarmoqni monitoring qilish.

**Olingan natijalar.** Tahlillar shuni ko'rsatadiki, bulutli hisoblash texnologiyalaridan samarali va xavfsiz foydalanish uchun kompleks yondashuv zarur. Faqat texnik vositalar emas, balki tashkiliy va huquqiy choralar ham muhim



ahamiyatga ega. To'g'ri joriy etilgan xavfsizlik strategiyasi orqali ma'lumotlar xavfsizligini yuqori darajada ta'minlash mumkin.

**Xulosa.** Bulutli hisoblash texnologiyalari zamonaviy axborot jamiyatining ajralmas qismiga aylanib bormoqda. Ularning afzalliklari bilan bir qatorda xavfsizlik muammolari ham mavjud. Ushbu maqolada ko'rib chiqilgan muammolar va yechimlar talaba uchun muhim nazariy asos bo'lib xizmat qiladi. Kelajakda bulutli hisoblash xavfsizligini yanada rivojlantirish uchun sun'iy intellekt va avtomatlashtirilgan himoya tizimlaridan foydalanish istiqbolli yo'nalish hisoblanadi.

#### **Foydalanilgan adabiyotlar:**

1. Mell P., Grance T. The NIST Definition of Cloud Computing. NIST, 2011.
2. Buyya R., Broberg J., Goscinski A. Cloud Computing: Principles and Paradigms. Wiley, 2011.
3. Armbrust M. et al. Above the Clouds: A Berkeley View of Cloud Computing. UC Berkeley, 2010.
4. Rittinghouse J, Ransome J. Cloud Computing: Implementation, Management and Security. CRC Press, 2017.
5. Pearson S. Privacy, Security and Trust in Cloud Computing. Springer, 2013.
6. Stallings W. Network Security Essentials. Pearson Education, 2018.
7. Zissis D., Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems, 2012.
8. CSA. Cloud Security Alliance Guidance. 2020.
9. Schneier B. Applied Cryptography. Wiley, 2015.
10. Behl A., Behl K. Cyberwar: The Next Threat to National Security. Oxford Press, 2017.