ISSN: 3030-3346

ZAMONAVIY AXBOROT TIZIMLARIDA BULUTLI HISOBLASH TEXNOLOGIYALARINING ROLI VA RIVOJLANISH ISTIQBOLLARI: XAVFSIZLIK JIHATLARI

Shirinov Laziz Toxirovich

Muhammad al-Xorazmiy nomidagi TATU, Axborot xavfsizligi kafedrasi,
E-mail: lazizshirinov1991@gmail.com

K E Y W O R D S

bulutli hisoblash, axborot tizimlari, bulutli xavfsizlik, kiberxavfsizlik, ma'lumotlarni himoya qilish, kirishni nazorat qilish, virtualizatsiya, shifrlash, axborot texnologiyalari, raqamli transformatsiya

A B S T R A C T

Bulutli hisoblash zamonaviy axborot tizimlarini ishlab chiqish, joriy etish va boshqarishda asosiy texnologik yondashuvlardan biriga aylandi. Ushbu texnologiya tashkilotlarga mahalliy infratuzilmani to'liq saqlash shart bo'lmay, zarurat tug'ilganda hisoblash resurslari, ma'lumotlar omborlari, dasturiy ta'minot va tarmoq imkoniyatlarini talabga binoan olish imkonini beradi. Shu bilan birga, ma'lumotlar va ilovalarni bulut muhitiga ko'chirish axborot xavfsizligi va maxfiylikni himoya qilish sohasida yangi xavf-xatarlarni keltirib chiqaradi. Maqolada zamonaviy axborot tizimlarida bulutli texnologiyalarning roli ko'rib chiqiladi, bulutli xizmatlar va joylashtirishning asosiy modellariga hamda xavfsizlikni ta'minlash bo'yicha talablarga tahlil qilinadi. Alohida e'tibor ma'lumotlarni himoya qilish, identifikatsiya va kirishni boshqarish, shifrlash, virtualizatsiya, mavjudlikni ta'minlash hamda hodisalarga tezkor javob berishga qaratilgan. Shuningdek, avtomatlashtirish, sun'iy intellekt va nol ishonch tamoyillari hisobga olingan holda bulutli texnologiyalarning rivojlanish istiqbollari ko'rib chiqilgan.

1. Kirish

Axborot texnologiyalarining rivojlanishi zamonaviy axborot tizimlarini loyihalash va boshqarish tamoyillarini tubdan o'zgartirdi. An'anaviy axborot tizimlari odatda tashkilotning jismoniy infratuzilmasida joylashgan hisoblash resurslari, serverlar, ma'lumotlar bazalari va dasturiy ta'minotga tayanardi. Garchi bu yondashuv bevosita ma'muriy nazoratni ta'minlagan bo'lsada, u apparat, texnik xizmat, texnik xodimlar, energiya va infratuzilmani kengaytirishga katta sarmoya talab qilardi. Bulutli hisoblash esa hisoblash resurslarini tarmoq orqali xizmat sifatida taqdim etadigan boshqa modelni joriy etdi. NIST bulutli hisoblashni minimal boshqaruv sa'y-harakatlari bilan tezda ta'minlanishi va bo'shatilishi mumkin bo'lgan sozlanadigan hisoblash resurslari umumiy havzasiga qulay, talabga binoan tarmoq orqali kirishni ta'minlovchi model deb belgilaydi [1, 2-bet]. NIST modeli beshta asosiy xususiyatni aniqlaydi: talabga binoan o'z-o'zini xizmat ko'rsatish, keng tarmoqqa kirish, resurslarni birlashtirish, tezda moslashuvchanlik va o'lchangan xizmat. Shuningdek, u uchta asosiy xizmat modelini — Xizmat sifatida Infratuzilma (IaaS), Xizmat sifatida Platform (PaaS) va Xizmat sifatida Dasturiy ta'minot (SaaS) — hamda to'rtta joylashtirish modelini: xususiy, jamoaviy, ommaviy va gibrid bulutlarni ajratib ko'rsatadi [1, 2 b.]. Raqamli transformatsiya kontekstida bulut texnologiyalarini joriy etish ayniqsa muhim bo'lib qoldi. Tashkilotlar bulut infratuzilmasidan foydalanib, axborot tizimlarini tezroq ishga tushirishi, talabga qarab hisoblash quvvatini oshirishi yoki kamaytirishi hamda ilovalar va ma'lumotlarga masofadan kirishni ta'minlashi mumkin. Shuning uchun bulutga asoslangan tizimlar ta'lim, sog'liqni saqlash, bank ishi, davlat boshqaruvi, sanoat, savdo, ilmiy tadqiqotlar va boshqa ko'plab sohalarda qo'llaniladi. Biroq, axborot tizimlarini bulut muhitiga ko'chirish tashkilotning an'anaviy xavfsizlik chegaralarini o'zgartiradi. Ma'lumotlar uchinchi tomon provayderi boshqaradigan infratuzilmada saqlanishi, ilovalar ko'p ijarachili muhitda ishlashi

(cc) BY

va foydalanuvchilar turli geografik joylashuvlar hamda qurilmalardan resurslarga kirishi mumkin. NIST ta’kidlaydiki, xavfsizlik va maxfiylik bo‘yicha mas'uliyatni oddiygina bulut provayderiga o‘tkazib bo‘lmaydi; tashkilotlar o‘z axborotlari va ilovalarini himoya qilish bo‘yicha mas'uliyatni saqlab qolishlari kerak [3]. Shuning uchun bulutli hisoblashni rivojlantirish bilan birga bulutli xavfsizlikni ham rivojlantirishni ko‘rib chiqish zarur. Ushbu maqolaning maqsadi zamonaviy axborot tizimlarida bulutli hisoblash texnologiyalarining rolini tahlil qilish, muhim xavfsizlik talablarini aniqlash va keyingi rivojlanish istiqbollarini o‘rganishdan iborat.

2. Adabiyotlar sharhi

Bulutli hisoblashning nazariy asoslari ko‘plab tadqiqotchilar va xalqaro tashkilotlar tomonidan o‘rganilgan. Mell va Grance bulutli hisoblashning eng keng tarqalgan ta’riflaridan birini berib, xizmat va joylashtirish modellari asosida tushunchaviy ramkani belgilashdi [1, 2-bet]. Ushbu ramka bulut muhitlarining arxitektura va xususiyatlarini tushunish uchun muhim bo‘lib qolmoqda. Armbrust va boshq. bulutli hisoblashni hisoblash resurslarini xizmat sifatida taqdim eta oladigan model deb ta’riflab, uning axborot texnologiyalarining iqtisodiy va texnik tashkiliy tuzilmasini o‘zgartirish salohiyatini ta’kidladilar [4, 51–58-betlar]. Ularning ishi bulutli hisoblash bilan bog‘liq bir nechta afzalliklarni, jumladan elastiklik, resurslarni birlashtirish va katta dastlabki sarmoyalarsiz hisoblash imkoniyatlarini taqdim etish qobiliyatini aniqladi. Xavfsizlik bulutli hisoblash tadqiqotlarida muhim mavzu bo‘lib kelmoqda. Jansen va Grance NIST SP 800-144 hujjatida ommaviy bulutli hisoblashning xavfsizlik va maxfiylik oqibatlarini o‘rgandilar. Ularning tahlili boshqaruv, muvofiqlik, ishonch, ma’lumotlarni himoya qilish, identifikatsiya boshqaruvi, dasturiy ta’minot izolyatsiyasi, mavjudlik va hodisalarga javob berish bilan bog‘liq xavflarni aniqlaydi [3, 3–7 betlar]. Yevropa Ittifoqi Kiberxavfsizlik Agentligi (ENISA) ham bulutli hisoblash bilan bog‘liq xavflarni o‘rgangan. Uning bulutli xavflarni baholash hisobotida axborot xavfsizligi bo‘yicha foydalar hamda bulut muhitlari bilan bog‘liq xavflar aniqlangan va xavflarni baholash hamda xavfsizlikni boshqarish bo‘yicha tavsiyalar berilgan [5, 9–18-betlar]. Bulut xavfsizligi bo‘yicha tadqiqotlar shuni ko‘rsatadiki, xavfsizlik mexanizmlari tizimni joriy etgandan keyin qo‘shilmasdan, balki butun bulut hayotiy siklida integratsiya qilinishi kerak. Xususan, kirishni nazorat qilish, shifrlash, autentifikatsiya, zaifliklarni boshqarish, zaxira nusxalarini olish, monitoring va hodisalarga javob berish kabi jarayonlar bulutga asoslangan axborot tizimlari arxitekturasiga kiritilishi zarur.

Zamonaviy bulut arxitekturalari shuningdek mikroservislar, konteynerlar, APIlar va tarqatilgan ma’lumotlar bazalariga tobora ko‘proq tayanadi. Ushbu texnologiyalar kengaytiriluvchanlik va moslashuvchanlikni yaxshilaydi, ammo himoyalanishi kerak bo‘lgan interfeyslar va komponentlar sonini oshiradi. Shuning uchun NISTning bulut xavfsizligi bo‘yicha nashrlari kirishni nazorat qilish, xavfsiz arxitekturalar, dasturiy ta’minotni izolyatsiya qilish, ma’lumotlarni himoya qilish va uzluksiz monitoringni muhim xavfsizlik omillari sifatida ta’kidlaydi [6, 14–20 betlar].

3. Materiallar va usullar

Tadqiqot sifatli analitik yondashuvdan foydalangan holda olib borildi. Metodologik asos bulutli hisoblash va axborot xavfsizligiga oid ilmiy adabiyotlar, xalqaro standartlar, texnik hisobotlar va muassasaviy tavsiyalarni tahlil qilish va solishtirishdan iborat edi.

Tadqiqot bulutli hisoblashning bir nechta o‘lchovlarini o‘rganib chiqdi:

1. bulutli hisoblashning arxitektura xususiyatlari;
2. xizmat modellari va joylashtirish modellari;
3. zamonaviy axborot tizimlari uchun afzalliklari;
4. asosiy axborot xavfsizligi xavflari;
5. bulut muhitlariga tatbiq etiladigan xavfsizlik mexanizmlari;
6. kelajakdagi texnologik rivojlanish.

NIST nashrlari asosiy konseptual va xavfsizlik bo‘yicha manba sifatida ishlatildi, chunki ular bulutli hisoblash bo‘yicha standartlashtirilgan ta’riflar va tavsiyalarni taqdim etadi [1, 3]. ENISA materiallari Yevropa kiberxavfsizlik nuqtai nazaridan xavf tahlilini to‘ldirish uchun qo‘llanildi [5]. Akademik nashrlar

(cc) BY

bulutli hisoblashning texnologik va tashkiliy xususiyatlarini aniqlash maqsadida o‘rganildi.

- Xavfsizlik tahlili uchun quyidagi o‘lchovlar ko‘rib chiqildi:
- ma’lumotlarning maxfiyligi;
- ma’lumotlar va ilovalar yaxlitligi;
- xizmatlarning mavjudligi;
- avtorizatsiya va autentifikatsiya;
- shifrlash va kalitlarni boshqarish;
- bulut resurslarini izolyatsiya qilish;
- zaxira nusxa olish va ofatdan keyingi tiklash;
- hodisalarni aniqlash va javob berish.

Analitik yondashuv texnologik afzalliklarni tegishli xavfsizlik talablari bilan solishtirishga asoslangan. Bu bulutli hisoblashni nafaqat resurslarni optimallashtirish usuli, balki axborot xavfsizligi nazoratlari uzluksiz ishlashi kerak bo‘lgan arxitektura muhiti sifatida ham o‘rganish imkonini beradi.

4. Natijalar va muhokamalar

Tahlil shuni ko‘rsatadiki, bulutli hisoblash zamonaviy axborot tizimlarining arxitekturasini sezilarli darajada o‘zgartiradi. Eng muhim afzallik – bu elastiklik. An'anaviy tizimlarda talab ortishidan oldin tashkilotlar qo‘shimcha serverlarni sotib olishlari kerak bo‘ladi. Bulut muhitlari esa hisoblash resurslarini joriy talablarga muvofiq taqsimlash va bo‘shatish imkonini beradi [1, 3-bet]. Ushbu xususiyat o‘zgaruvchan yuklamali tizimlar uchun ayniqsa foydalidir.

Yana bir muhim afzallik – keng tarmoqqa kirish imkoniyatidir. Bulut ilovalariga kompyuterlar, mobil qurilmalar va boshqa tarmoqqa ulangan tizimlar orqali kirish mumkin. Bu masofaviy ish, masofaviy ta’lim, tarqatilgan tadqiqotlar va geografik jihatdan tarqalgan tashkilotlarni qo‘llab-quvvatlaydi. Biroq, keng kirish potentsial hujum yuzasini ham kengaytiradi. Natijada autentifikatsiya va avtorizatsiya mexanizmlari bulut xavfsizligining muhim tarkibiy qismlariga aylanadi.

Ma’lumotlarni himoya qilish yana bir markaziy masalani tashkil etadi. NIST bulut provayderi ma’lumotlarni saqlash paytida, uzatishda va, agar tegishli bo‘lsa, qayta ishlash vaqtida himoya qila oladimi-yo‘qligini baholashni, shuningdek kalitlarni boshqarish tartiblarini ham hisobga olishni tavsiya etadi [3, 44–45 betlar]. Shifrlash ruxsatsiz oshkor etish oqibatlarini kamaytirishi mumkin, ammo samarali shifrlash mos kalitlarni yaratish, saqlash, aylantirish va kirishni nazorat qilish protseduralariga bog‘liq.

Shaxsiyat va kirishni boshqarish ham xuddi shuncha muhimdir. Bulut tizimlari ko‘pincha bir nechta foydalanuvchi, ilova, administrator va avtomatlashtirilgan xizmatlarni o‘z ichiga oladi. Ortiqcha ruxsatnomalar ruxsatsiz kirish imkoniyatlarini yaratishi mumkin. Shuning uchun tashkilotlar eng kam imtiyozlar tamoyilini qo‘llashi va kuchli autentifikatsiya mexanizmlaridan foydalanishi kerak. NIST xususan autentifikatsiya, avtorizatsiya va shaxsiyatni boshqarish funksiyalarini bulut muhitidagi muhim himoya vositalari deb belgilaydi [3, 43-bet].

Virtualizatsiya yana bir xavfsizlik o‘lchovini kiritadi. Bulut provayderlari ko‘pincha bir nechta mijozni umumiy jismoniy infratuzilmada qo‘llab-quvvatlash uchun virtualizatsiya va mantiqiy izolyatsiyadan foydalanadi. NIST tashkilotlarga provayderlar tomonidan qo‘llaniladigan izolyatsiya texnologiyalarini tushunishni va ko‘p ijarachili arxitekturalarga oid xavflarni baholashni tavsiya etadi [3, 44-bet]. Mavjudlik ham asosiy talabdir. Axborot tizimlari kundalik operatsiyalar uchun tobora ko‘proq bulutli xizmatlarga tayanadi. Shuning uchun xizmat uzilishlari, asosiy ilova o‘zi ishlashda davom etsa ham, tashkilot jarayonlariga ta’sir qilishi mumkin. Nosozliklar oqibatlarini kamaytirish uchun mos zaxira nusxa olish, zaxira nusxa ko‘paytirish, tiklash rejalashtirish va ofatdan keyingi tiklash protseduralari zarur. NIST tashkilotlarga mavjudlik, zaxira nusxa olish, tiklash va ofatdan keyingi tiklash bo‘yicha shartnoma bandlari va protseduralarni ko‘rib chiqishni tavsiya etadi [3, 45–46 betlar].

Insoniy voqea-hodisalarga javob berish bulut xavfsizligining yana bir muhim tarkibiy qismidir. Xavfsizlik hodisasi buzilgan parollar, ruxsatsiz kirish, zararli dasturlar, ma’lumotlarning oshkor bo‘lishi yoki xizmat ko‘rsatish uzilishi bilan bog‘liq bo‘lishi mumkin. Chunki bulut muhitida ham provayder, ham mijozning majburiyatlari mavjud, hodisalarga javob berish tartib-qoidalarida qaysi tomon ma’lum faoliyatlarni amalga oshirishi aniq belgilangan

(cc) BY

bo‘lishi kerak. NIST tashkilotlar va bulut provayderlari o‘rtasida muvofiqlashtirilgan hodisalarga javob berish mexanizmlari zarurligini ta’kidlaydi [3, 46-bet]. Shu sababli, mas'uliyatni bo‘lishish tushunchasi ayniqsa muhimdir. Bulut xizmatlari modeliga qarab, ba’zi xavfsizlik mas'uliyatlari asosan provayder zimmasida bo‘lsa, boshqalari mijoz zimmasida qoladi. Masalan, IaaS muhitida mijozlar odatda operatsion tizimlar, ilovalar, identifikatorlar va konfiguratsiyalarni boshqarish bo‘yicha ko‘proq mas'uliyatga ega bo‘lsa, provayderlar asosiy infratuzilma uchun mas'uldir. SaaS muhitida esa provayder texnik stakning katta qismini boshqaradi, lekin mijozlar munosib foydalanish, kirishni boshqarish, ma’lumotlarni boshqarish va tashkiliy nazorat uchun mas'ul bo‘lib qoladi.

Zamonaviy bulut provayderlari xavfsizlik, muvofiqlik, operatsiyalar va tiklash bo‘yicha mas'uliyatlarni provayder va mijoz o‘rtasida taqsimlanganligini ochiq-oydin bayon qiladilar [7]. Tahlil shuningdek bir nechta muhim rivojlanish istiqbollarini ko‘rsatadi. Birinchidan, sun'iy intellekt va mashinani o‘rganish avtomatlashtirilgan anomaliyalarni aniqlash, xulq-atvor tahlili va xavfsizlik monitoringini tobora ko‘proq qo‘llab-quvvatlashi mumkin. Ikkinchidan, zero-trust yondashuvlari asosan tarmoq joylashuviga tayanish o‘rniga uzluksiz tasdiqni talab qilish orqali shaxsiyatga yo‘naltirilgan kirish nazoratini mustahkamlashi mumkin. Uchinchidan, maxfiy hisoblash va ilg‘or shifrlash texnikalari sezgir ma’lumotlar uchun qo‘shimcha himoya ta’minlashi mumkin.

Ko‘p bulutli va gibrid-bulutli arxitekturalar ham muhim bo‘lib qolishi kutilmoqda, chunki tashkilotlar ish yuklarini ishlash unumdorligi, tartibga soluvchi, operatsion yoki xavfsizlik talablariga muvofiq turli muhitlarga taqsimlashlari mumkin. Biroq, bunday arxitekturalar barcha muhitlarda izchil identifikatsiya boshqaruvi, loglash, monitoring va xavfsizlik siyosatini talab qiladi.

Yana bir muhim yo‘nalish – bu xavfsizlikni avtomatlashtirish. Bulut platformalari sozlash muammolarini avtomatik aniqlashi, shubhali faoliyatni aniqlashi, xavfsizlik siyosatini qo‘llashi va ogohlantirishlar yaratishi mumkin. Avtomatlashtirish zaiflik aniqlanishi bilan tuzatish choralari joriy etilishi orasidagi vaqtni qisqartirishi mumkin. Shunga qaramay, avtomatlashtirilgan nazorat mos boshqaruvga bo‘ysunishi kerak, chunki noto‘g‘ri sozlamalar yoki avtomatlashtirilgan qarorlar o‘zlari operatsion va xavfsizlik xavfini tug‘dirishi mumkin.

Umuman olganda, natijalar shuni ko‘rsatadiki, bulutli hisoblash faqat jismoniy serverlarning o‘rnini bosuvchi vosita sifatida qaralmasligi kerak. Bu axborot tizimi arxitekturasining kengroq transformatsiyasini anglatadi. Shuning uchun xavfsizlik tizimni loyihalash, joriy etish, ishlatish, monitoring qilish va yopish jarayonlariga integratsiya qilinishi lozim. NIST tashkilotlarga bulutli tartiblarni tanlashdan oldin o‘z talablari va ma’lumotlarining sezgirlik darajasini baholashni o‘z ichiga olgan xavfga asoslangan yondashuvni tavsiya etadi [3].

5. Xulosa

Bulutli hisoblash texnologiyalari zamonaviy axborot tizimlari uchun muhim poydevorga aylangan. Ularning kengaytiriladigan hisoblash resurslari, masofaviy kirish, moslashuvchan infratuzilma va xizmatga asoslangan dasturiy ta’minot yetkazib berish qobiliyati raqamli transformatsiyadan o‘tayotgan tashkilotlar uchun katta imkoniyatlar yaratadi. IaaS, PaaS va SaaS modellari tashkilotlarga texnik va tashkiliy talablariga muvofiq infratuzilma va ilovalar boshqaruvi turli darajalarini tanlash imkonini beradi. Shu bilan birga, bulutli xizmatlarni joriy etish axborot xavfsizligining an’anaviy chegaralarini o‘zgartiradi. Ma’lumotlar va ilovalar qisman tashqi xizmat ko‘rsatuvchi provayderlar nazoratidagi muhitda ishlashi mumkin, foydalanuvchilar va qurilmalar esa turli joylardan resurslarga kirishlari mumkin. Natijada, xavfsizlik va maxfiylik ikkinchi darajali texnik funksiyalar sifatida emas, balki bulut arxitekturasining ajralmas qismi sifatida ko‘rib chiqilishi kerak. Tahlil shuni ko‘rsatadiki, ma’lumotlarni himoya qilish, identifikatsiya va kirishni boshqarish, shifrlash, virtualizatsiya xavfsizligi, mavjudlik, zaxira nusxalarini olish, hodisalarga javob berish va umumiy mas'uliyat kabi sohalar tizimli e’tibor talab qiladi. NIST va ENISAning xalqaro ko‘rsatmalari tashkilotlarga bulutli xizmatlarni joriy etishdan oldin va jarayonida ma’lumotlarning sezgirlik darajasini, texnik arxitektura, bulutli xizmat provayderlarining

(cc) BY

amaliyotlari va tashkiliy talablarni baholashga asoslangan xavfga yo‘naltirilgan yondashuvni qo‘llab- quvvatlaydi. Bulutli hisoblashning kelajakdagi rivojlanishi sun'iy intellekt, avtomatlashtirish, zero-trust xavfsizlik, ilg‘or shifrlash, tarqatilgan arxitekturalar va aqlli monitoring bilan yanada yaqin integratsiyani o‘z ichiga olishi kutilmoqda. Ushbu texnologiyalar tegishli boshqaruv va xavf-xatarlarni boshqarish amaliyotlari bilan birgalikda joriy etilganda bulutga asoslangan axborot tizimlarining chidamliligi va xavfsizligini yaxshilashi mumkin. Shunday qilib, bulutli hisoblashning uzoq muddatli samaradorligi nafaqat kengaytiriluvchanlik va iqtisodiy samaradorlikka, balki tashkilotlarning bulutga asoslangan axborot tizimlarining butun hayotiy tsikli davomida tegishli xavfsizlik nazoratlarini o‘rnatish qobiliyatiga ham bog‘liq.

Manbalar

1. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145. National Institute of Standards and Technology, Gaithersburg, MD, 1–3-betlar.
2. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. va Zaharia, M. (2010). Bulutli hisoblashga nazar. Communications of the ACM, 53(4), 50–58.
3. Jansen, W. va Grance, T. (2011). Jamoat bulutli hisoblashda xavfsizlik va maxfiylik bo‘yicha ko‘rsatmalar. NIST maxsus nashri 800-144. Milliy Standartlar va Texnologiya Instituti, 1–80-betlar.
4. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Bulutli hisoblash va paydo bo‘layotgan IT platformalari: hisoblashni beshinchi kommunal xizmat sifatida taqdim etish bo‘yicha qarash, shov-shuv va haqiqat. Future Generation Computer Systems, 25(6), 599–616.
5. Yevropa Ittifoqi Kiberxavfsizlik Agentligi (ENISA). (2009). Bulutli hisoblash xavflarini baholash. Yevropa tarmoqlari va axborot xavfsizligi agentligi, 1–125-betlar.
6. Milliy Standartlar va Texnologiya Instituti. (2020). Bulut tizimlari uchun umumiy kirishni nazorat qilish bo‘yicha ko‘rsatma. NIST maxsus nashri 800-210. Gaithersburg, MD.
7. IBM. (2026). IBM Cloud mahsulotlari va xizmatlari uchun umumiy mas’uliyatlarni tushunish. IBM Cloud hujjatlari.
8. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Bulutli hisoblash: zamonaviy holat va tadqiqot muammolari. Journal of Internet Services and Applications, 1, 7–18.
9. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). Bulutli hisoblash uchun xavfsizlik muammolarining tahlili. Journal of Internet Services and Applications, 4, maqola 5.
10. Mell, P., & Grance, T. (2011). Bulutli hisoblash bo‘yicha NIST ta’rif. Milliy Standartlar va Texnologiya Instituti.

(cc) BY *dtai.uz*