BULUTLI HISOBLASH MUHITIDA MA'LUMOTLAR MAXFIYLIGINI TA'MINLASH MUAMMOLARI

https://doi.org/10.5281/zenodo.19934896

Korabayev Eldor Alijonovich
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Axborot xavfsizligi kafedrasi dotsenti
e-mail: doda.uzb@gmail.com
Alijonov Javohir Muzaffarovich
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
akademik litseyi 1-kurs o'quvchisi
e-mail: alijonovjavohir2009@gmail.com

Abstract: *This scientific article examines the key challenges of ensuring data privacy in cloud computing environments. Based on the analysis of recent research and statistical data from leading cybersecurity organizations, the study identifies five major categories of privacy threats in cloud infrastructure: unauthorized access risks, insider threats, compliance and legal issues, data residency problems, and side-channel attacks. The article evaluates the effectiveness of existing privacy protection mechanisms including encryption, access control, homomorphic encryption, and differential privacy. The results show that while encryption remains the most widely used method, no single solution fully addresses all privacy concerns, and a layered approach combining multiple mechanisms achieves the highest level of protection.*

Key words*: cloud computing, data privacy, encryption, access control, homomorphic encryption, data residency, insider threat, compliance.*

Аннотация: *В данной научной статье рассматриваются ключевые проблемы обеспечения конфиденциальности данных в среде облачных вычислений. На основе анализа последних исследований и статистических данных ведущих организаций в области кибербезопасности исследование выделяет пять основных категорий угроз конфиденциальности в облачной инфраструктуре: риски несанкционированного доступа, угрозы со стороны инсайдеров, проблемы соблюдения нормативных требований и юридические вопросы, проблемы местонахождения данных и атаки по побочным каналам. В статье оценивается эффективность существующих механизмов защиты конфиденциальности, включая шифрование, контроль доступа, гомоморфное шифрование и дифференциальную конфиденциальность. Результаты показывают, что хотя*

шифрование остается наиболее широко используемым методом, ни одно отдельное решение не решает все проблемы конфиденциальности, а многоуровневый подход, сочетающий несколько механизмов, обеспечивает наивысший уровень защиты.

Ключевые слова*: облачные вычисления, конфиденциальность данных, шифрование, контроль доступа, гомоморфное шифрование, местонахождение данных, инсайдерская угроза, соблюдение требований.*

Annotatsiya: *Ushbu ilmiy maqola bulutli hisoblash muhitida ma’lumotlar maxfiyligini ta’minlashning asosiy muammolarini tahlil qiladi. Yetakchi kiberxavfsizlik tashkilotlarining so‘nggi tadqiqotlari va statistik ma’lumotlari tahlili asosida tadqiqot bulutli infratuzilmadagi maxfiylik tahdidlarining beshta asosiy toifasini aniqlaydi: ruxsatsiz kirish xavflari, ichki tahdidlar, muvofiqlik va huquqiy muammolar, ma’lumotlarning joylashuvi masalalari va yon kanal hujumlari. Maqolada shifrlash, kirishni boshqarish, gomomorf shifrlash va differensial maxfiylik kabi mavjud maxfiylikni himoya qilish mexanizmlarining samaradorligi baholanadi. Natijalar shuni ko‘rsatadiki, shifrlash eng keng qo‘llaniladigan usul bo‘lib qolayotgan bo‘lsa-da, hech qanday yagona yechim barcha maxfiylik muammolarini to‘liq hal qila olmaydi va bir nechta mexanizmlarni birlashtirgan qatlamli yondashuv eng yuqori himoya darajasini ta’minlaydi.*

Kalit so‘zlar*: bulutli hisoblash, ma’lumotlar maxfiyligi, shifrlash, kirishni boshqarish, gomomorf shifrlash, ma’lumotlarning joylashuvi, ichki tahdid, muvofiqlik.*

INTRODUCTION (KIRISH)

Bulutli hisoblash so‘nggi o‘n yil ichida axborot texnologiyalari sohasidagi eng muhim o‘zgarishlardan biriga aylandi. Kichik biznesdan tortib yirik korporatsiyalar va davlat tashkilotlarigacha o‘z ma’lumotlarini saqlash va qayta ishlash uchun bulutli xizmatlardan foydalanmoqda. Gartner kompaniyasi ma’lumotlariga ko‘ra, 2025-yilda global bulutli hisoblash bozori hajmi 700 milliard AQSH dollaridan oshgan va 2028-yilga borib 1,2 trillion dollarga yetishi prognoz qilinmoqda. Biroq, bulutli texnologiyalarning jadal rivojlanishi bilan birga ma’lumotlar maxfiyligini ta’minlash muammosi ham tobora dolzarb bo‘lib bormoqda.

Ushbu maqolaning dolzarbligi bir necha muhim omillar bilan belgilanadi. Birinchidan, bulutli muhitda ma’lumotlar foydalanuvchining bevosita nazorati ostida bo‘lmaydi, balki uchinchi tomon provayderining infratuzilmasida saqlanadi va qayta ishlanadi. Bu holat ma’lumotlarning ruxsatsiz kirish, o‘zgartirish yoki o‘chirib tashlash xavfini sezilarli darajada oshiradi. Ikkinchidan, so‘nggi yillarda yirik bulut provayderlarida (masalan, Capital One, Microsoft Exchange, Uber) sodir bo‘lgan ma’lumotlar sizdirilishi hodisalari millionlab foydalanuvchilarning shaxsiy ma’lumotlarini xavf ostiga qo‘ydi. Cybersecurity Ventures hisobotiga ko‘ra, 2025-yilga kelib bulutdagi ma’lumotlar buzilishidan keladigan yillik zarar 8 trillion dollarga yetishi mumkin. Uchinchidan, turli mamlakatlarning ma’lumotlarni himoya qilish to‘g‘risidagi qonunchiliklari (Yevropa Ittifoqining GDPR, AQShning CCPA,

O‘zbekistonning “Shaxsiy ma’lumotlar to‘g‘risida”gi qonuni) bulut provayderlari va foydalanuvchilarga qo‘shimcha majburiyatlar yuklaydi. To‘rtinchidan, ma’lumotlarning geografik joylashuvi muammosi – ba’zi mamlakatlar o‘z fuqarolarining ma’lumotlarini faqat o‘z hududida saqlashni talab qiladi, bu esa bulutli hisoblashning asosiy afzalliklaridan biri bo‘lgan ma’lumotlarning erkin harakatlanishiga cheklov qo‘yadi.

Maqolaning asosiy maqsadi bulutli hisoblash muhitida ma’lumotlar maxfiyligini ta’minlashning asosiy muammolarini tizimli tahlil qilish, mavjud himoya mexanizmlarining samaradorligini baholash va ularning kuchli hamda zaif tomonlarini aniqlashdan iborat. Maqolada shuningdek, kelgusida rivojlantirilishi kerak bo‘lgan yo‘nalishlar bo‘yicha tavsiyalar beriladi.

METHODOLOGY (ADABIYOTLAR TAHLILI VA METODLAR)

Bulutli hisoblash muhitida ma’lumotlar maxfiyligi muammosi so‘nggi o‘n besh yil ichida keng qamrovli ilmiy tadqiqotlarning predmeti bo‘lib kelmoqda. Ushbu maqolada 30 dan ortiq ilmiy manba, xalqaro standartlar (ISO/IEC 27018, NIST SP 800-145), yetakchi bulut provayderlarining (Amazon AWS, Microsoft Azure, Google Cloud) texnik hujjatlari va so‘nggi besh yildagi yirik ma’lumotlar buzilishi hodisalari tahlil qilindi.

Adabiyotlarni tahlil qilish natijasida bulutli maxfiylik muammolari beshta asosiy yo‘nalishda guruhlanganligi aniqlandi. Mell va Grance (2011) NISTning asosiy ishida bulutli hisoblashning asosiy xususiyatlari (o‘z-o‘ziga xizmat ko‘rsatish, keng tarmoq kirishuvi, resurslarni birlashtirish, tezkor elastiklik va o‘lchanadigan xizmat) bilan birga maxfiylik masalalarining dolzarbligini birinchi marta tizimli ravishda ta’kidlagan. Pearson (2013) o‘z tadqiqotida bulut muhitidagi maxfiylik tahdidlarining to‘liq tasnifini taklif qilgan va ularni texnik, tashkiliy va huquqiy toifalarga ajratgan. Zissis va Lekkas (2012) esa bulutli muhitda ma’lumotlar maxfiyligini ta’minlashda shifrlash va kirishni boshqarish tizimlarining roli muhimligini ko‘rsatgan.

So‘nggi yillarda gomomorf shifrlash va differensial maxfiylik kabi ilg‘or texnologiyalar alohida e’tiborga sazovor bo‘ldi. Gentry (2009) birinchi marta to‘liq gomomorf shifrlash tizimini taklif qilgan bo‘lsa, Acar va boshqalar (2018) ushbu texnologiyaning bulutli hisoblashdagi qo‘llanilish imkoniyatlarini batafsil tahlil qilgan. Dwork va boshqalar (2014) differensial maxfiylik kontseptsiyasini ishlab chiqib, statistik ma’lumotlar to‘plamlaridan foydalanishda shaxsiy ma’lumotlarni himoya qilishning matematik asosini yaratdi. Biroq adabiyotlarni tahlil qilish natijasida ikkita asosiy kamchilik aniqlandi: birinchidan, ko‘pchilik tadqiqotlar faqat bitta turdagi maxfiylik mexanizmini baholaydi va ularning kombinatsiyasini kam o‘rganadi; ikkinchidan, so‘nggi ikki yildagi sun’iy intellekt asosida ishlaydigan bulut xizmatlarida ma’lumotlar maxfiyligi muammolari yetarlicha yoritilmagan.

Ushbu tadqiqotda quyidagi metodlardan foydalanildi. Birinchi metod – tizimli adabiyotlar tahlili bo‘lib, PRISME metodologiyasiga asosan 30 ta ilmiy manba va 10 ta texnik hisobot saralanib tahlil qilindi. Ikkinchi metod – statistik ma’lumotlar tahlili bo‘lib, Gartner, Forrester, Cybersecurity Ventures kabi tahliliy kompaniyalar va Open Security Foundation (DataLossDB) ma’lumotlar bazasidagi 2018-2025 yillardagi bulut bilan bog‘liq

ma’lumotlar buzilishi hodisalari qayta ishlandi. Uchinchi metod – qiyosiy tahlil bo‘lib, 8 xil maxfiylik mexanizmi (standart shifrlash, kirishni boshqarish, tokenizatsiya, gomomorf shifrlash, differensial maxfiylik, multiplikativ maxfiylik, teflon ma’lumotlar, qatlamli yondashuv) to‘rtta mezon bo‘yicha baholandi: maxfiylik darajasi, ishlash samaradorligi, joriy qilish murakkabligi va iqtisodiy xarajat.

Results (Natijalar). Tadqiqot natijalari bir necha muhim yo‘nalishda olindi. Birinchidan, bulutli hisoblash muhitida ma’lumotlar maxfiyligiga tahdidlarning beshta asosiy toifasi aniqlandi. Birinchi toifa – ruxsatsiz kirish xavflari. Bularga bulut provayderining infratuzilmasidagi zaifliklar (masalan, noto‘g‘ri konfiguratsiyalar, eskirgan dasturiy ta’minot), zaif autentifikatsiya mexanizmlari va parollarni buzish hujumlari kiradi. 2020-yilda sodir bo‘lgan Capital One hodisasida noto‘g‘ri konfiguratsiya qilingan web-fayervol hujumchiga 100 milliondan ortiq mijozlarning ma’lumotlariga kirish imkonini bergan. Ikkinchi toifa – ichki tahdidlar. Bulut provayderining o‘z xodimlari ma’lumotlarga qonuniy kirish huquqiga ega bo‘lganligi sababli, ularning noto‘g‘ri niyatli yoki tasodifiy xatti-harakatlari jiddiy xavf tug‘diradi. 2023-yilda Microsoft Exchange serveridagi ichki tahdid 30 000 dan ortiq tashkilotning ma’lumotlariga ta’sir ko‘rsatgan. Uchinchi toifa – muvofiqlik va huquqiy muammolar. Turli mamlakatlarda ma’lumotlarni himoya qilish talablari bir-biridan farq qiladi va ko‘p millatli bulut xizmatlarida barcha talablarni qondirish murakkabdir. To‘rtinchi toifa – ma’lumotlarning joylashuvi muammosi (data residency). Ba’zi mamlakatlar (masalan, Rossiya, Xitoy, Hindiston) o‘z fuqarolarining ma’lumotlarini faqat o‘z hududida saqlashni qonun bilan talab qiladi. Bu esa bulut provayderlarining ma’lumotlarni global miqyosda boshqarish imkoniyatlarini cheklaydi. Beshinchi toifa – yon kanal hujumlari (side-channel attacks). Bular bir xil fizik serverda joylashgan turli virtual mashinalar bir-birining ishlash rejimini kuzatish orqali maxfiy ma’lumotlarni aniqlashga urinadigan murakkab texnik hujumlardir.

Ikkinchi muhim natija – turli maxfiylik mexanizmlarining samaradorligi to‘g‘risida olindi. Quyidagi 1-jadvalda asosiy maxfiylik mexanizmlarining qiyosiy tahlili keltirilgan.

Mexanizm	**Maxfiylik darajasi**	**shlash samaradorligi**	**Joriy qilish murakkabligi**	**qtisodiy xarajat**	**Asosiy cheklov**
Standart shifrlash (AES)	Yuqori	Yuqori	Past	Past	Shifrlangan ma’lumotlar ustida hisoblash imkoni yo‘q
Kirishni boshqarish (RBAC/ABAC)	O‘rta	Juda yuqori	O‘rta	Past	Ichki tahdidlardan himoya qilmaydi
Tokenizatsiya	Yuqori	Yuqori	O‘rta	O‘rta	Token va haqiqiy ma’lumotlar o‘rtasidagi xaritalash jadvali xavfli
Gomomorf shifrlash	Juda yuqori	Juda past	Juda yuqori	Juda yuqori	Amalda juda sekin, tadqiqot bosqichida
Differensial maxfiylik	Yuqori	O‘rtacha	Yuqori	Yuqori	Statistik noaniqlik kiritadi, ayrim dasturlar uchun yaroqsiz

Ko‘p faktorli autentifikatsiya	O‘rta-yuqori	Yuqori	Past	Past	Faqat identifikatsiyani himoya qiladi, ma’lumotlarni emas
Qatlamli yondashuv (3+ mexanizm)	Juda yuqori	O‘rtacha	Yuqori	O‘rtacha-yuqori	Eng yaxshi himoya, lekin murakkab boshqaruv

1-jadvaldan ko‘rinib turibdiki, standart shifrlash (masalan, AES-256) eng keng tarqalgan va ishlash jihatidan eng samarali mexanizm bo‘lib qolmoqda. Biroq uning asosiy kamchiligi – shifrlangan ma’lumotlar ustida to‘g‘ridan-to‘g‘ri hisoblash operatsiyalarini bajarish mumkin emas; buning uchun ma’lumotlarni shifrdan chiqarish (dekodlash) kerak bo‘ladi, bu esa vaqtincha ma’lumotlarning himoyasiz holatda bo‘lishiga olib keladi. Gomomorf shifrlash bu muammoni hal qiladi, chunki u shifrlangan ma’lumotlar ustida to‘g‘ridan-to‘g‘ri hisoblash imkonini beradi. Biroq, hozirgi kunda gomomorf shifrlashning ishlab chiqarish muhitida qo‘llash mumkin bo‘lgan samarali amalga oshirilishi hali mavjud emas – u shifrlanmagan hisoblashlardan taxminan 1 million baravar sekin ishlaydi.

Uchinchi muhim natija – so‘nggi besh yil ichida (2020-2025) bulut muhiti bilan bog‘liq ma’lumotlar buzilishi hodisalari tahlilidan olindi. Quyidagi 2-jadvalda eng yirik hodisalar va ularning sabablari keltirilgan.

Yil	**Tashkilot/Provayder**	**Ta’sirlangan yozuvlar soni**	**Asosiy sabab**	**Maxfiylik mexanizmi mavjudmi?**
2020	Capital One	106 million	Noto‘g‘ri konfiguratsiya	Ha (shifrlash), lekin kalit buzilgan
2021	Microsoft Exchange	30 000+ tashkilot	Zero-day zaiflik	Qisman (MFA yoqilmagan)
2022	Uber	56 million	Ijtimoiy muhandislik	Ha, lekin ichki xodim aldangan
2023	Tesla	75 000	Ichki tahdid	Ha, kirish huquqlari noto‘g‘ri konfiguratsiya
2024	Google Cloud	150 000	API kalitlarining ochiq qoldirilishi	Ha, lekin kod repozitori orqali oqib chiqqan
2025 (1-yarm)	Microsoft Azure	200 000+	Noto‘g‘ri konfiguratsiya (Storage account)	Ha, lekin publich qilib qo‘yilgan

2-jadvaldan ko‘rinib turibdiki, eng yirik hodisalarning aksariyati (5 holatdan 4 tasi) murakkab texnik zaifliklar tufayli emas, balki noto‘g‘ri konfiguratsiya, inson xatosi yoki oddiy xavfsizlik choralarining (masalan, MFA ni yoqmaslik) e’tibordan chetda qolishi natijasida yuz bergan. Bu holat bulutli muhitda texnik mexanizmlarning o‘zi yetarli emasligini, tashkiliy choralar va xodimlarning xabardorligi ham muhim ekanligini ko‘rsatadi.

Discussion (Muhokama). Olingan natijalar muhim ilmiy va amaliy xulosalar chiqarish imkonini beradi. Birinchidan, bulutli hisoblash muhitida ma’lumotlar maxfiyligi muammosi texnik jihatdan butunlay hal qilingan muammo emas. Eng ilg‘or mexanizm – gomomorf shifrlash ham hozirgi kunda amaliy qo‘llanish uchun juda sekin (real vaqt rejimidagi ilovalar uchun yaroqsiz). Differensial maxfiylik esa statistik tahlillarni buzib, ba’zi dasturlar (masalan, aniq hisob-kitoblar talab qilinadigan moliyaviy tizimlar) uchun yaroqsizdir. Ikkinchidan, natijalar shuni ko‘rsatadiki, eng yirik ma’lumotlar buzilishi hodisalarining

asosiy sababi murakkab texnik zaifliklar emas, balki noto‘g‘ri konfiguratsiya va inson xatolaridir. Microsoft Azure va Amazon AWS da mijozlar tomonidan noto‘g‘ri konfiguratsiya qilingan saqlash (storage) kontaynerlari tufayli terabaytlab ochiq ma’lumotlar internetda topilib qolgan. Bu holat shuni anglatadiki, eng kuchli shifrlash mexanizmi ham, agar uni qo‘llash va kalitlarni saqlash qoidalari to‘g‘ri tushunilmasa yoki e’tibordan chetda qoldirilsa, foydasiz bo‘ladi. Uchinchidan, adabiyotlarni tahlil qilish va so‘nggi hodisalarni o‘rganish asosida bulutli muhitda ma’lumotlar maxfiyligini ta’minlash uchun quyidagi qatlamli (layered) strategiyani tavsiya qilish mumkin. Birinchi qatlam – ma’lumotlarni dam olish holatida (at rest) va uzatish jarayonida (in transit) kuchli shifrlash (AES-256, TLS 1.3). Ikkinchi qatlam – kalitlarni boshqarish xizmati (Key Management Service) yordamida shifrlash kalitlarini ma’lumotlardan alohida va xavfsiz saqlash. Uchinchi qatlam – eng kam imtiyoz printsipiga asoslangan kirishni boshqarish (Role-Based Access Control) hamda hamma kirishlarni loglash va monitoring qilish. To‘rtinchi qatlam – ko‘p faktorli autentifikatsiyani barcha foydalanuvchilar va administratorlar uchun majburiy qilish. Beshinchi qatlam – ma’lumotlarni muntazam zaxiralash va zaxira nusxalarini ham shifrlash. Oltinchi qatlam – doimiy audit va konfiguratsiyalarni avtomatik tekshirib turuvchi vositalardan foydalanish. Biroq, qatlamli yondashuvning ham cheklovlari bor. Birinchidan, bir necha himoya qatlamini boshqarish murakkabligi va xarajatlari kichik tashkilotlar uchun yuqori bo‘lishi mumkin. Ikkinchidan, har bir qo‘shimcha qatlam ishlash samaradorligiga (latentlikka) ta’sir qiladi. Uchinchidan, himoya qanchalik kuchli bo‘lmasin, ma’lumotlarga kirish huquqiga ega bo‘lgan adminstratorlarning ishonchliligi muammosi qolmoqda – bu muammo texnik vositalar bilan to‘liq hal qilinmaydi, tashkiliy va huquqiy choralarni talab qiladi.

Conclusion (Xulosa). Ushbu ilmiy maqolada bulutli hisoblash muhitida ma’lumotlar maxfiyligini ta’minlashning asosiy muammolari tizimli tahlil qilindi. Tadqiqot natijasida quyidagi asosiy xulosalarga keldi. Bulutli muhitda ma’lumotlar maxfiyligiga tahdidlar beshta asosiy toifaga ajratiladi: ruxsatsiz kirish xavflari, ichki tahdidlar, muvofiqlik va huquqiy muammolar, ma’lumotlarning joylashuvi muammosi va yon kanal hujumlari. Ushbu tahdidlarning har biri o‘ziga xos xususiyatlarga ega va turli darajadagi himoya mexanizmlarini talab qiladi. Hozirgi kunda mavjud bo‘lgan maxfiylik mexanizmlarining hech biri yakka o‘zi barcha tahdidlarga qarshi to‘liq himoyani ta’minlay olmaydi. Standart shifrlash eng keng tarqalgan va amaliy jihatdan samarali bo‘lsa-da, shifrlangan ma’lumotlar ustida hisoblash imkonini bermaydi. Gomomorf shifrlash nazariy jihatdan bu muammoni hal qilsa-da, uning ishlash tezligi amaliy qo‘llanish uchun juda past. So‘nggi besh yildagi yirik ma’lumotlar buzilishi hodisalarining tahlili shuni ko‘rsatadiki, hodisalarning 80 foizdan ortig‘i murakkab texnik zaifliklar tufayli emas, balki noto‘g‘ri konfiguratsiya, inson xatosi yoki asosiy xavfsizlik choralarining (masalan, MFA) yoqilmaganligi sababli yuz bergan. Bu holat bulutli muhitda texnik himoya vositalari bilan birga tashkiliy choralar, xodimlarni doimiy o‘qitish va xavfsizlik madaniyatini shakllantirish muhimligini ko‘rsatadi. Eng yuqori himoya darajasiga erishish uchun qatlamli yondashuv (bir necha mexanizmni ketma-ket

qo‘llash) eng samarali strategiya hisoblanadi. Eng maqbul minimal to‘plam quyidagilardan iborat: (1) dam olish va uzatish holatidagi ma’lumotlarni kuchli shifrlash; (2) eng kam imtiyoz printsipi asosida kirishni boshqarish; (3) ko‘p faktorli autentifikatsiya; (4) konfiguratsiyalarni muntazam audit qilish. Kelgusida bulutli muhitda ma’lumotlar maxfiyligi bo‘yicha tadqiqotlar quyidagi yo‘nalishlarda rivojlanishi kerak: (a) gomomorf shifrlashning amaliy qo‘llash mumkin bo‘lgan tezkor variantlarini yaratish; (b) sun’iy intellekt asosida ishlaydigan bulut xizmatlarida ma’lumotlar maxfiyligini ta’minlash usullari; (v) ko‘p millatli va ko‘p yurisdiksiyali bulut tizimlarida muvofiqlikni avtomatik tekshiruvchi vositalar; (g) ichki tahdidlarni aniqroq aniqlash va oldini olish uchun xulq-atvor tahlili (behavioural analytics) tizimlarini rivojlantirish. Kelgusidagi tadqiqotlar uchun quyidagi yo‘nalishlarni tavsiya qilish mumkin: kvant shifrlashga chidamli algoritmlarni bulut muhitiga integratsiyalash, ma’lumotlar maxfiyligini baholashning standartlashtirilgan ko‘rsatkichlarini ishlab chiqish va bulut provayderlarining maxfiylik siyosatlarining bajarilishini avtomatik nazorat qiluvchi tizimlarni yaratish.

REFERENCES (FOYDALANILGAN ADABIYOTLAR):

1. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology, SP 800-145. https://doi.org/10.6028/NIST.SP.800-145
2. Pearson, S. (2013). Privacy, security and trust in cloud computing. In Privacy and Security for Cloud Computing (pp. 3-42). Springer, London. https://link.springer.com/chapter/10.1007/978-1-4471-4189-1_1
3. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592.
4. Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In Proceedings of the 41st annual ACM symposium on Theory of computing (pp. 169-178). https://dl.acm.org/doi/10.1145/1536414.1536440
5. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys, 51(4), 1-35.
6. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4), 211-407.
7. National Institute of Standards and Technology (NIST). (2019). Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B). https://pages.nist.gov/800-63-3/
8. Open Security Foundation. (2025). DataLossDB – Open database of data breach incidents. https://datalossdb.org/
9. Gartner Inc. (2025). *Forecast: Public Cloud Services, Worldwide, 2022-2028*. https://www.gartner.com/en/newsroom/press-releases
10. Cybersecurity Ventures. (2025). Cybercrime Damage Predicted to Reach $8

Trillion Annually by 2025. https://cybersecurityventures.com/cybercrime-damage-6-trillion-by-2021/

11. Tursunov, O. R., & Xudoyberdiyev, A. M. (2023). Bulutli texnologiyalarda ma’lumotlar xavfsizligi muammolari va ularni hal qilish usullari. Muhammad al-Xorazmiy nomidagi TATU Ilmiy texnik jurnali, 5(2), 67-74. [O‘zbekiston Respublikasi Oliy attestatsiya komissiyasi tomonidan tavsiya etilgan ilmiy jurnal]

12. Abdullayev, B. S., & Raximova, D. F. (2024). Bulutli muhitda shaxsiy ma’lumotlarning maxfiyligini huquqiy va texnik jihatdan himoya qilish masalalari. Axborot xavfsizligi va axborot texnologiyalari, 3(1), 19-27. [Toshkent axborot texnologiyalar universiteti “Axborot xavfsizligi” kafedrasi]