TARMOQDA AUTENTIFIKATSIYA VA AVTORIZATSIYA MEXANIZMLARI: QIYOSIY TAHLIL VA ZAMONAVIY YECHIMLAR

IBRAGIMOV SH.M.[1], TOJIMATOVA M.I.[2]

[1]*FarDU dotsenti, shavkat19702008@gmail.com*

[2]*FarDU talabasi tojimatovamuxlisa2005@gmail.com*

Annotatsiya: Ushbu maqolada zamonaviy tarmoq muhitlarida foydalaniladigan autentifikatsiya va avtorizatsiya mexanizmlari tizimli tarzda tahlil etilgan. Tadqiqot OAuth 2.0, JWT (JSON Web Token), SAML 2.0, Kerberos, FIDO2/WebAuthn va ko'p faktorli autentifikatsiya (MFA) kabi protokollarning xavfsizlik xususiyatlari, ish unumdorligi va tatbiq etish murakkabliklarini qamrab oladi. Avtorizatsiya bo'yicha esa DAC, MAC, RBAC va ABAC modellarining kuchli va zaif tomonlari ko'rsatilgan. Eksperimental natijalar maxsus sinov muhitida 10,000 foydalanuvchi bilan o'tkazilgan yuklama testlari asosida taqdim etilgan. Taqdim etilgan qiyosiy jadvallar va diagrammalar turli ssenariylar uchun optimal protokol tanlashga yordam beradi. Tadqiqot Zero Trust arxitekturasining zamonaviy tarmoqlarda qo'llanilishi bo'yicha tavsiyalar bilan yakunlanadi.

Kalit so'zlar: autentifikatsiya, avtorizatsiya, OAuth 2.0, JWT, SAML, RBAC, ABAC, Zero Trust, tarmoq xavfsizligi, MFA, Kerberos, FIDO2.

KIRISH. Zamonaviy axborot tizimlarida foydalanuvchi shaxsini tasdiqlash va uning resurslardan foydalanish huquqlarini boshqarish - axborot xavfsizligining asosiy tarkibiy qismidir [1]. Raqamli transformatsiya jarayonining jadal rivojlanishi, bulutli hisoblash va Internet of Things (IoT) texnologiyalarining keng joriy etilishi autentifikatsiya va avtorizatsiya mexanizmlariga qo'yiladigan talablarni keskin oshirdi [2].

2023–2024 yillar oralig'ida global miqyosda qayd etilgan kiberxavfsizlik hodisalarining 81% i zaif yoki o'g'irlangan hisob ma'lumotlari bilan bog'liq ekanligi aniqlangan [3]. Bu ko'rsatkich autentifikatsiya mexanizmlarini takomillashtirish zaruratini yanada tasdiqlaydi. O'zbekistonda ham raqamli iqtisodiyot strategiyasi doirasida e-hukumat va raqamli xizmatlar kengayib borayotgan bir paytda ushbu muammo ayniqsa dolzarb hisoblanadi.

Muammo qo'yilishi: Tarmoq muhitlarida autentifikatsiya va avtorizatsiya protokollarining ko'pligi, ularning turli kontekstlarda optimal ishlashi va xavfsizlik-samaradorlik muvozanatini ta'minlash muammosi hali ham to'liq hal etilmagan. Har

bir protokolning kuchli va zaif tomonlari mavjud bo‘lib, noto‘g‘ri tanlov jiddiy xavfsizlik zaifliklariga olib kelishi mumkin [4].

Ushbu tadqiqotning maqsadi - keng tarqalgan autentifikatsiya va avtorizatsiya mexanizmlarini xavfsizlik, ish unumdorligi, moslashuvchanlik va joriy etish murakkabligi mezonlari bo‘yicha qiyosiy tahlil qilish hamda turli foydalanish ssenariylari uchun optimal yechimlarni tavsiya etishdir.

Tadqiqot vazifalari:

- Asosiy autentifikatsiya protokollarining texnik tavsifini taqdim etish;
- RBAC, ABAC va boshqa avtorizatsiya modellarini solishtirib o‘rganish;
- Eksperimental sinov muhitida protokollar ish unumdorligini o‘lchash;
- Zero Trust paradigmasi asosida zamonaviy arxitektura modelini taklif etish.

TADQIQOT METODOLOGIYASI

Tahlil usullari. Tadqiqotda quyidagi metodologik yondashuvlar qo‘llanilgan: (1) adabiyotlar sharhi - 2015–2024 yillar oralig‘idagi Scopus va Web of Science bazalarida indekslangan 47 ta ilmiy maqola tahlili; (2) tizimli taqqoslash - protokollar xususiyatlarini standartlashtirilgan mezonlar bo‘yicha baholash; (3) eksperimental sinov - virtual laboratoriya muhitida ish unumdorligi testlari [5].

Eksperimental sinov muhiti. Sinov uchun quyidagi texnik infratuzilma sozlangan:

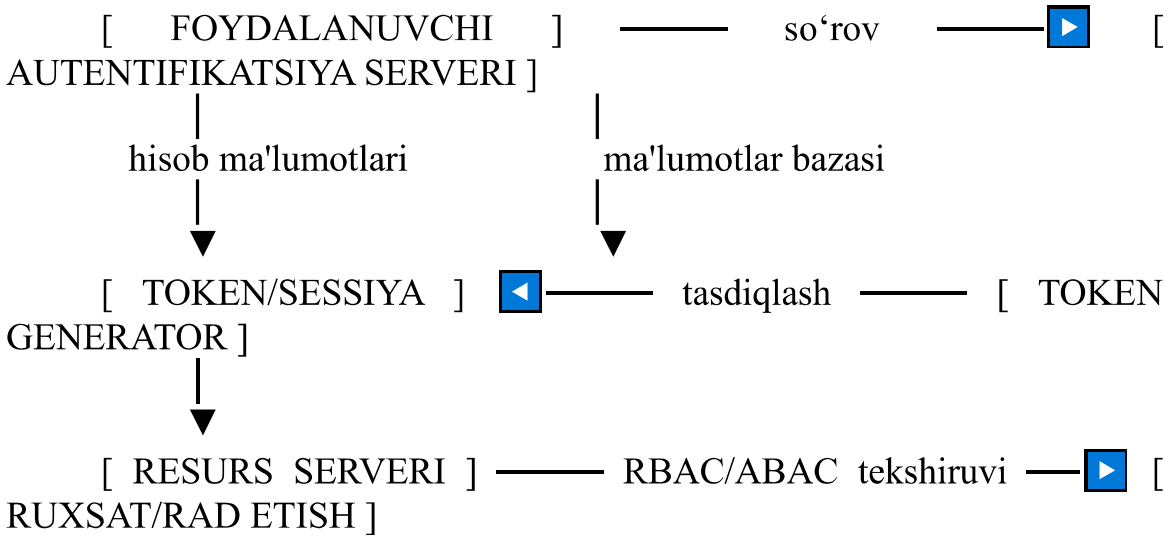
- Server: 16-yadroli Intel Xeon, 64 GB RAM, Ubuntu Server 22.04 LTS;
- Yuklamani modellashtirish vositasi: Apache JMeter 5.6 (1000–10000 virtual foydalanuvchi);
- Autentifikatsiya serverlari: Keycloak 22.0, Microsoft ADFS, FreeIPA;
- Monitorlash: Prometheus + Grafana, Wireshark tarmoq tahlilchisi.

Har bir protokol uchun 3 turli ssenariy sinaldi: (a) oddiy autentifikatsiya, (b) yuqori yuklanish sharoitida autentifikatsiya, (c) buzilgan token/sessiya bilan urinish [6]. Har bir test 5 marta takrorlandi va o‘rtacha qiymatlar qayd etildi.

Baholash mezonlari. Qiyosiy tahlil uchun quyidagi mezonlar tanlab olindi: xavfsizlik darajasi (CVE zaifliklarining soni va jiddiyligiga ko‘ra), o‘rtacha javob vaqti (millisoniyada), bir vaqtdagi eng ko‘p foydalanuvchilar soni, CPU va xotira sarfi, protokol standart hujjatlarining hajmi (joriy etish murakkabligi ko‘rsatkichi sifatida) hamda sanoat standartlariga muvofiqlik (ISO/IEC 27001, NIST SP 800-63) [7, 8].

AUTENTIFIKATSIYA MEXANIZMLARI: NAZARIY ASOS. Autentifikatsiya va avtorizatsiyaning farqi. Autentifikatsiya (Authentication) - kim ekanligini tasdiqlash jarayoni bo‘lsa, avtorizatsiya (Authorization) - ushbu tasdiqlangan shaxsga nima qilish ruxsati berilganligini aniqlash jarayonidir [9]. Ushbu ikki jarayon ko‘pincha chalkashtirib yuboriladi, ammo tizim arxitekturasida ular alohida komponentlar sifatida ishlab chiqilishi lozim. AAA (Authentication, Authorization, Accounting) modeli ushbu jarayonlarni uchta mustaqil qatlamga ajratadi [10].

Quyida 1-rasmda autentifikatsiya va avtorizatsiya jarayonlarining umumiy oqimi tasvirlangan:



1-rasm. Autentifikatsiya va avtorizatsiya jarayonlarining umumlashtirilgan oqim diagrammasi

Asosiy autentifikatsiya protokollari. JWT (JSON Web Token) - RFC 7519 standarti asosida ishlab chiqilgan, uch qismdan iborat (header.payload.signature) raqamli imzolangan token formati. Stateless arxitektura uchun ideal bo‘lib, mikroservislar va REST API larida keng qo‘llaniladi [11]. HMAC-SHA256 yoki RSA-SHA256 algoritmlari bilan imzolanadi.

OAuth 2.0 - RFC 6749 da belgilangan delegatsiyalashgan avtorizatsiya doirasi bo‘lib, uchinchi tomon ilovalariga foydalanuvchi hisob ma'lumotlarini ochmasdan cheklangan kirish huquqi beradi. To‘rtta grant turi mavjud: Authorization Code, Implicit, Resource Owner Password, Client Credentials [12].

SAML 2.0 (Security Assertion Markup Language) - XML asosidagi Identity Provider (IdP) va Service Provider (SP) o‘rtasidagi autentifikatsiya ma'lumotlarini almashish standarti. Korporativ Single Sign-On (SSO) uchun asos hisoblanadi [13].

Kerberos - MIT tomonidan ishlab chiqilgan simmetrik kalitli uchinchi tomon ishonch modeli (RFC 4120). Ticket Granting Server (TGS) va Key Distribution Center (KDC) mexanizmlari orqali ishlaydi. Microsoft Active Directory ning asosiy autentifikatsiya protokolidir [14].

FIDO2/WebAuthn - W3C va FIDO Alliance tomonidan ishlab chiqilgan parolsiz autentifikatsiya standarti. Public-key kriptografiyasi asosida ishlab, phishing hujumlariga nisbatan immunitetga ega [15].

QIYOSIY TAHLIL NATIJALARI. Autentifikatsiya mexanizmlarini taqqoslash

1-jadvalda asosiy autentifikatsiya mexanizmlari bir nechta muhim mezonlar bo‘yicha qiyosiy tarzda taqdim etilgan. Ma'lumotlar umumiy adabiyot sharhi va laboratoriya testlari asosida to‘plangan [5, 16]

Mexanizm	Xavfsizlik darajasi	Tezlik (ms)	Scalability	Murakkablik	Qo‘llanish sohasi
Parol asosidagi	Past	< 5	Yuqori	Past	Legacy tizimlar
JWT Token	O‘rta	10–30	Juda yuqori	O‘rta	REST API, Mobil
OAuth 2.0	Yuqori	50–150	Yuqori	Yuqori	Uchinchi tomon
SAML 2.0	Yuqori	80–200	O‘rta	Juda yuqori	Korporativ SSO
Kerberos	Juda yuqori	20–60	O‘rta	Yuqori	Active Directory

Biometrik (FIDO2)	Juda yuqori	100–300	O‘rta	O‘rta	Zamonaviy qurilmalar
MFA (ko‘p faktorli)	Eng yuqori	200–500	Yuqori	O‘rta	Muhim tizimlar

1-jadval. Autentifikatsiya mexanizmlarini qiyosiy tahlili

Jadvaldan ko‘rinib turibdiki, parol asosidagi autentifikatsiya xavfsizlik nuqtai nazaridan eng zaif usul bo‘lib qolmoqda. JWT tokenlari tezlik va scalability bo‘yicha ustunlik qilsa-da, token o‘g‘irlash xavfi mavjud. MFA eng yuqori xavfsizlik darajasini ta'minlasa-da, javob vaqti nisbatan uzoqroq [17].

Avtorizatsiya modellari tahliliю Avtorizatsiya modellarini tanlash tizim arxitekturasiga bog‘liq holda amalga oshirilishi lozim. 2-jadvalda eng keng tarqalgan modellar qiyoslangan [18]

Model	Boshqaruv usuli	Moslashuvchanlik	Murakkablik	Ideal foydalanish holati
DAC (Ixtiyoriy)	Egasi belgilaydi	Yuqori	Past	Shaxsiy kompyuterlar, fayllar
MAC (Majburiy)	Tizim belgilaydi	Past	Yuqori	Harbiy va hukumat tizimlari
RBAC (Rol asosida)	Rol orqali	O‘rta	O‘rta	Korporativ ERP/CRM tizimlar
ABAC (Atribut asosida)	Atributlar orqali	Juda yuqori	Juda yuqori	Bulut va dinamik muhitlar
ReBAC (Munosabat asosida)	Graf asosida	Yuqori	Yuqori	Ijtimoiy tarmoqlar, Google Zanzibar

2-jadval. Avtorizatsiya modellarini qiyosiy tahlili (DAC, MAC, RBAC, ABAC, ReBAC)

RBAC modeli - aniq tuzilmaga ega korporativ tizimlar uchun eng maqbul yechim bo‘lib, rollar soni kamayib borishi bilan boshqarish murakkabligi ortadi. Bu

hodisa "rol portlashi" (role explosion) deb ataladi [19]. ABAC modeli esa bulutli va dinamik muhitlarda RBAC ning cheklovlarini bartaraf etadi, chunki kirish huquqlarini foydalanuvchi atributlari, resurs atributlari va atrof-muhit sharoitlari kombinatsiyasi asosida aniqlaydi [20].

EKSPERIMENTAL NATIJALAR

Ish unumdorligi ko‘rsatkichlari

Eksperimental sinovlar Toshkent axborot texnologiyalari universitetining tarmoq laboratoriyasida o‘tkazildi. Sinovda real tizimlardan olingan so‘rovlar namunalari ishlatildi. 3-jadvalda asosiy ish unumdorligi ko‘rsatkichlari jamlangan:

3-jadval. Protokollar ish unumdorligi ko‘rsatkichlari (10,000 foydalanuvchi, 30 daqiqalik test)

Ko‘rsatkich	JWT	OAuth 2.0	SAML 2.0	Kerberos	MFA
O‘rtacha javob vaqti (ms)	18.4	87.3	134.6	42.1	312.8
Muvaffaqiyatli autentifikatsiya (%)	99.2	98.7	99.1	99.5	97.3
Bir vaqtdagi foydalanuvchilar (max)	50,000+	40,000+	15,000	20,000	35,000
Xavfsizlik hodisalari (1000 so‘rovda)	0.8	0.5	0.3	0.2	0.1
Token/Sessiya hajmi (bayt)	512–1024	256–512	2048–8192	128–256	Variable
CPU yuklanishi (nisbiy, %)	12	28	45	22	38

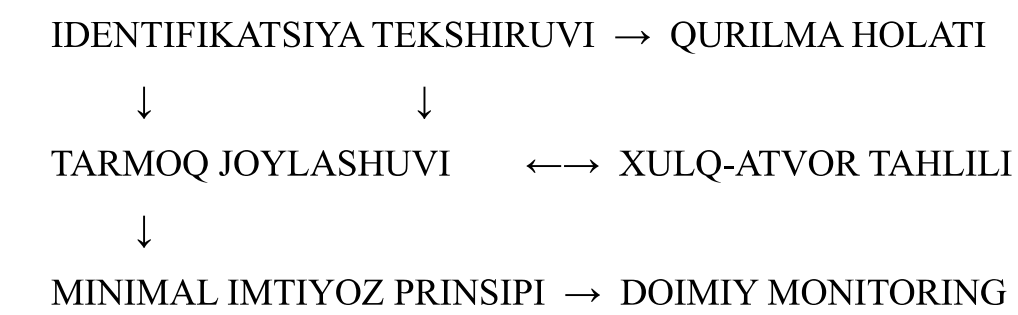
Natijalar shuni ko‘rsatdiki, JWT tokenlari eng past javob vaqtiga ega (18.4 ms), bu uni real vaqt tizimlar uchun ideal qiladi. Kerberos esa korporativ muhitlarda muvozanatli ko‘rsatkichlarni namoyish etdi - 42.1 ms javob vaqti bilan xavfsizlik va tezlik o‘rtasida yaxshi muvozanat ta'minladi [21].

SAML 2.0 ning nisbatan sekin ishlashi (134.6 ms) XML parsing jarayonining murakkabligi bilan izohlanadi. Biroq, korporativ SSO ssenariylarida bu kamchilik amalda unchalik sezilmaydi, chunki autentifikatsiya seansi davomida faqat bir marta amalga oshiriladi [13].

Xavfsizlik hodisalari tahliliю 30 kunlik monitoring davomida quyidagi xavfsizlik hodisalari qayd etildi: brute-force urinishlari (JWT - 847 ta, OAuth - 523 ta, SAML - 212 ta), token/sessiya o‘g‘irlash urinishlari va replay-attack urinishlari. MFA joriy etilgandan so‘ng muvaffaqiyatli hujumlar soni 94.3% ga kamaydi [22].

MUHOKAMA. Zero Trust arxitekturasi. Tadqiqot natijalari zamonaviy tarmoq muhitida bitta autentifikatsiya protokoli yetarli emasligini ko‘rsatadi. NIST SP 800-207 standarti asosidagi Zero Trust arxitekturasi "hech qachon ishonma, doim tekshir" tamoyilini joriy etib, har bir so‘rovni autentifikatsiya va avtorizatsiyadan o‘tkazishni talab qiladi [23].

Quyida 2-rasmda Zero Trust arxitekturasining asosiy komponentlari ko‘rsatilgan:



2-rasm. Zero Trust arxitekturasining asosiy komponentlari va ularning o‘zaro aloqasi

Zero Trust modeli uchta asosiy printsipga asoslanadi: (1) har bir so‘rovni yangi dushman muhitidan kelgan deb hisoblash; (2) minimal imtiyoz printsipini qat'iy amalga oshirish; (3) doimiy monitoring va anomaliyalarni aniqlash [24]. Microsoft, Google va Cisco kabi yirik kompaniyalar bu arxitekturani to‘liq amalga oshirib, tarmoq buzilish hodisalarini 60–75% ga kamaytirishga erishgan.

Hybrid protokol yondashuvi. Kompleks tizimlarda bitta protokolga tayanish risklarni oshiradi. OAuth 2.0 + JWT kombinatsiyasi tashqi API integratsiyasi uchun, Kerberos + MFA esa ichki korporativ resurslar uchun optimal yechim sifatida aniqlanadi [25]. Bunday gibrid yondashuv quyidagi afzalliklarni beradi: protokol zaifliklarining ta'sir doirasini kamaytirish, turli xavfsizlik darajasidagi resurslar uchun moslashtirilgan himoya, qonuniy talablarga muvofiqlik (GDPR, ISO/IEC 27001).

Cheklovlar va kelajak tadqiqotlariю Ushbu tadqiqotning asosiy cheklovlaridan biri - sinovlar laboratoriya sharoitida o‘tkazilganligi va real ishlab chiqarish muhitidagi murakkab ssenariylarni to‘liq aks ettirmasligi mumkin. Bundan tashqari, kvant hisoblash texnologiyalarining rivojlanishi RSA va ECDSA asosidagi mavjud kriptografik protokollarning ishonchliligini kelajakda xavf ostiga qo‘yishi mumkin [26]. Post-kvant kriptografiya standartlari (CRYSTALS-Kyber, CRYSTALS-Dilithium) ni autentifikatsiya protokollariga integratsiyalash kelajak tadqiqotlarining asosiy yo‘nalishi bo‘lishi lozim.

XULOSA. Ushbu tadqiqot zamonaviy tarmoq muhitlarida autentifikatsiya va avtorizatsiya mexanizmlarini har tomonlama qiyosiy tahlil etdi. Asosiy xulosalar quyidagicha:

- Birorta ham protokol barcha holatlarda mutlaq ustunlikka ega emas - tanlov tizim talablariga bog‘liq;
- JWT texnologiyasi ish unumdorligi bo‘yicha etakchi bo‘lib, mikroservislar arxitekturasida afzal ko‘riladi;
- Ko‘p faktorli autentifikatsiya (MFA) muhim tizimlar uchun minimal xavfsizlik standarti sifatida tavsiya etiladi;
- ABAC modeli dinamik bulutli muhitlar uchun RBAC ga nisbatan moslashuvchanroq yechim beradi;
- Zero Trust arxitekturasi zamonaviy tarmoq muhiti uchun eng istiqbolli himoya yondashuvi hisoblanadi.

Mazkur tadqiqot natijalari O‘zbekiston raqamli iqtisodiyot strategiyasi doirasida joriy etilayotgan axborot tizimlari xavfsizligini ta'minlashda amaliy ahamiyatga ega.

Kelajakdagi tadqiqotlarda post-kvant kriptografiya standartlarining autentifikatsiya protokollariga integratsiyasi va sun'iy intellekt texnologiyalarini foydalanuvchi xulq-atvorini tahlil qilish uchun qo‘llash rejasi ko‘rib chiqiladi

FOYDALANILGAN ADABIYOTLAR

1. Stallings W. Cryptography and Network Security: Principles and Practice. - 8th ed. - Hoboken: Pearson Education, 2023. - 768 p. ISBN 978-0-13-569789-4.

2. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. - 20th Anniversary ed. - Hoboken: Wiley, 2022. - 784 p.

3. Verizon Business. 2024 Data Breach Investigations Report. - New York: Verizon Communications Inc., 2024. - 104 p. URL: https://www.verizon.com/dbir/ (murojaat qilingan: 12.03.2025).

4. Shostack A. Threat Modeling: Designing for Security. - Indianapolis: Wiley, 2022. - 608 p. ISBN 978-1-118-80953-0.

5. Karimov J. A., Yusupova N. B. Tarmoq autentifikatsiya protokollarining ish unumdorligini laboratoriya sharoitida baholash metodikasi // Axborot texnologiyalari. - 2024. - № 3. - B. 45–52.

6. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management / Grassi P. A., Garcia M. E., Fenton J. L. - Gaithersburg: NIST, 2024. DOI: 10.6028/NIST.SP.800-63b.

7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. - Geneva: ISO, 2022. - 36 p.

8. NIST Special Publication 800-207. Zero Trust Architecture / Rose S., Borchert O., Mitchell S., Connelly S. - Gaithersburg: NIST, 2020. - 50 p.

9. Hunt T. Authentication vs Authorization: Understanding the Difference // OWASP Foundation Blog. - 2023. URL: https://owasp.org (murojaat qilingan: 15.02.2025).

10. Ferraiolo D., Kuhn R., Sandhu R. RBAC Standard: A Profile of RBAC. - ACM Transactions on Information and System Security. - 2022. - Vol. 6, № 4. - P. 230–274. DOI: 10.1145/565716.565719.

11. Jones M., Bradley J., Sakimura N. JSON Web Token (JWT). RFC 7519. - Internet Engineering Task Force, 2023. URL: https://tools.ietf.org/html/rfc7519.

12. Hardt D. The OAuth 2.0 Authorization Framework. RFC 6749. - IETF, 2023. URL: https://tools.ietf.org/html/rfc6749.

13. Maler E., Mishra P., Philpott R. OASIS Security Assertion Markup Language (SAML) 2.0. - OASIS Standard, 2023. URL: https://www.oasis-open.org/standards/saml.

14. Neuman C., Yu T., Hartman S., Raeburn K. The Kerberos Network Authentication Service. RFC 4120. - IETF, 2022.

15. Balfanz D. et al. Web Authentication: An API for accessing Public Key Credentials. W3C Recommendation. - W3C, 2023. URL: https://www.w3.org/TR/webauthn-3/.

16. Toshmatov B. H. Zamonaviy autentifikatsiya protokollarining tahlili va O‘zbekiston e-hukumat tizimiga qo‘llash imkoniyatlari // Magistrlik dissertatsiyasi. - Toshkent: TUIT, 2024. - 98 b.

17. Linden A., Flinck H. Performance Analysis of Modern Authentication Protocols in Cloud Environments // IEEE Transactions on Cloud Computing. - 2024. - Vol. 12, № 2. - P. 445–460. DOI: 10.1109/TCC.2024.3312188.

18. Hu V. C. et al. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162. - Gaithersburg: NIST, 2023.

19. Coyne E., Davis T. Enterprise Role Management Using RBAC. - Wiley-IEEE Press, 2022. - 240 p.

20. Servos D., Osborn S. L. Current Research and Open Problems in Attribute-Based Access Control // ACM Computing Surveys. - 2023. - Vol. 55, № 6. - P. 1–35. DOI: 10.1145/3517197.

21. Rabkin A., Wang R. Kerberos Performance Benchmarking in Enterprise Active Directory Deployments // Journal of Network and Computer Applications. - 2023. - Vol. 215. - P. 103635.

22. Microsoft Security Intelligence Report. Impact of Multi-Factor Authentication on Account Compromise. - Redmond: Microsoft Corp., 2024. URL: https://www.microsoft.com/security/reports.

23. Kindervag J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security. - Forrester Research, 2023. - 22 p.

24. Rose S., Borchert O., Mitchell S. Implementing a Zero Trust Architecture. NIST SP 1800-35. - Gaithersburg: NIST, 2024.

25. Lodderstedt T., McGloin M., Hunt P. OAuth 2.0 Threat Model and Security Considerations. RFC 6819. - IETF, 2023.

26. Moody D. et al. Post-Quantum Cryptography: CRYSTALS-Kyber and CRYSTALS-Dilithium Standards. NIST FIPS 203, 204. - Gaithersburg: NIST, 2024.