BULUTLI TIZIMLARDA MA’LUMOTLAR XAVFSIZLIGINI TA’MINLASHNING ZERO TRUST ASOSIDAGI MODELI

Abdullayev Baxtiyor Panji o‘gli
Termiz davlat universiteti, Matematik modellashtirish va kompyuter ilmlari kafedrasi katta o‘qituvchisi.
E–mail: abbaxti@gmail.com
Tel.Raqam: +998 (93)–261–37–87
Allaberdiyev Navruzbek Ikromovich
Termiz davlat universiteti, Axborot texnologiyalari fakulteti, Dasturiy injiniring yo‘nalishining 2-kurs talabasi.
E-mail: allaberdiyevnavroz17@gmail.com
Tel.Raqam: +998 (93)–072–12–21
Xursanova Sarvinoz Jo‘raqul qizi
Termiz Davlat universitetining Axborot texnologiyalari fakulteti Dasturiy injiniring yo‘nalishi 2-kurs talabasi.
E-mail: xursanovasarvinoz0704@gmail.com
Tel.Raqam : +998 (99)–073–99–47

ANNOTATSIYA.

Ushbu maqolada bulutli tizimlarda ma’lumotlar xavfsizligini ta’minlash muammolari va ularni hal etishda Zero Trust modelining ahamiyati tahlil qilinadi. Zamonaviy bulut infratuzilmalarida an’anaviy xavfsizlik yondashuvlari yetarli darajada samarali emasligi aniqlangan. Tadqiqotda autentifikatsiya, ruxsatlarni boshqarish, tarmoq segmentatsiyasi va monitoring kabi asosiy mexanizmlar ko‘rib chiqiladi. Natijalar shuni ko‘rsatadiki, Zero Trust modeli ruxsatsiz kirishlarni kamaytirish va tizim xavfsizligini oshirishda samarali yechim hisoblanadi.

ABSTRACT.

This paper analyzes data security challenges in cloud systems and highlights the importance of the Zero Trust model in addressing them. Traditional security approaches are insufficient for modern cloud infrastructures. The study examines key mechanisms including authentication, access control, network segmentation, and continuous monitoring. Results indicate that the Zero Trust approach effectively reduces unauthorized access and enhances overall system security.

АННОТАЦИЯ.

В статье анализируются проблемы безопасности данных в облачных системах и рассматривается значение модели Zero Trust. Установлено, что традиционные методы безопасности недостаточно эффективны в современных условиях. Исследуются ключевые механизмы: аутентификация, управление

доступом, сегментация сети и мониторинг. Результаты показывают, что модель Zero Trust эффективно снижает несанкционированный доступ и повышает уровень безопасности системы.

Kalit so‘zlar: Bulutli tizimlar, ma’lumotlar xavfsizligi, Zero Trust modeli, autentifikatsiya, ruxsatlarni boshqarish, tarmoq segmentatsiyasi, monitoring.

INTRODUCTION.

Zamonaviy raqamli transformatsiya jarayonlari natijasida bulutli hisoblash texnologiyalari (cloud computing) global miqyosda jadal rivojlanib, turli sohalarda keng qo‘llanilmoqda. Korxonalar, davlat tashkilotlari va ta’lim muassasalari o‘z infratuzilmalarini optimallashtirish, IT xarajatlarini kamaytirish hamda xizmatlar moslashuvchanligini oshirish maqsadida bulutli platformalarga faol o‘tmoqda [1, 7–8 betlar]. Ushbu jarayon axborot resurslaridan samarali foydalanish imkonini kengaytirish bilan birga, ma’lumotlar xavfsizligini ta’minlash muammosini ham keskin dolzarb masalaga aylantirmoqda.

Bulutli muhitning o‘ziga xos xususiyatlari—ma’lumotlarning markazlashmagan holda saqlanishi, ko‘p foydalanuvchili (multi-tenant) arxitektura, masofaviy kirish imkoniyatlari va xizmatlarning dinamik miqyosda kengayishi — xavfsizlikka yangi tahdidlarni yuzaga keltirmoqda. Xususan, ma’lumotlarga ruxsatsiz kirish, identifikatsiya ma’lumotlarining o‘g‘irlanishi, ichki tahdidlar va tarmoq hujumlari bulutli tizimlar uchun asosiy xavf omillari hisoblanadi [2, 15–17 betlar]. Shu sababli, ma’lumotlarning maxfiyligi (confidentiality), yaxlitligi (integrity) va mavjudligini (availability) ta’minlash masalasi ilmiy va amaliy jihatdan katta ahamiyat kasb etadi.

An’anaviy xavfsizlik yondashuvlari, xususan, perimetrga asoslangan himoya modeli (“ishonchli ichki tarmoq — ishonchsiz tashqi tarmoq”) uzoq vaqt davomida asosiy xavfsizlik mexanizmi sifatida qo‘llanilib kelgan. Biroq, zamonaviy bulutli va tarqatilgan tizimlar sharoitida ushbu model o‘zining samaradorligini yo‘qotib bormoqda. Tadqiqotlar shuni ko‘rsatadiki, ichki tarmoqqa avtomatik ishonch bildirilishi natijasida ichki tahdidlar, insayder hujumlar va ruxsatsiz kirishlar xavfi ortadi [3, 22–25 betlar]. Bundan tashqari, masofaviy ish rejimining kengayishi va mobil qurilmalar sonining ortishi perimetr tushunchasini yanada noaniq holga keltirmoqda.

Mazkur muammolarni bartaraf etish maqsadida zamonaviy kiberxavfsizlikda yangi yondashuv—**Zero Trust** ***(“hech kimga ishonma, har doim tekshir”)*** modeli taklif etilgan. Ushbu modelga ko‘ra, tizim ichida yoki tashqarisida joylashganligidan qat’i nazar, har bir foydalanuvchi va qurilma ishonchli deb qabul qilinmaydi va doimiy ravishda autentifikatsiya hamda avtorizatsiyadan o‘tkaziladi [4, 5–9 betlar]. Zero Trust modeli identifikatsiya va kirishni boshqarish (IAM), ko‘p bosqichli autentifikatsiya (MFA), minimal ruxsat prinsipi (least privilege), tarmoq mikrosegmentatsiyasi va

uzluksiz monitoring kabi mexanizmlar orqali xavfsizlikni kompleks tarzda ta’minlaydi. Shunga qaramay, mavjud ilmiy adabiyotlarda Zero Trust modelini aynan bulutli infratuzilmalarga moslashtirish, uning samaradorligini kompleks baholash va amaliy joriy etish mexanizmlarini ishlab chiqish masalalari yetarli darajada chuqur o‘rganilmagan. Ayniqsa, rivojlanayotgan hududlarda va mahalliy sharoitlarda ushbu modelni implementatsiya qilishning o‘ziga xos jihatlari bo‘yicha ilmiy asoslangan yondashuvlar yetishmaydi [5, 30–32 betlar]. Bu esa mazkur yo‘nalishda qo‘shimcha ilmiy tadqiqotlar olib borishni talab etadi.

Zero Trust modeli zamonaviy axborot xavfsizligi tizimlarida keng qo‘llanilayotgan innovatsion yondashuvlardan biri bo‘lib, u turli sohalarda ma’lumotlar himoyasini yuqori darajada ta’minlashga xizmat qiladi. Raqamli transformatsiya jarayonlarining jadallashuvi, masofaviy ish faoliyatining kengayishi hamda bulutli texnologiyalarning ommalashuvi natijasida an’anaviy xavfsizlik modellari o‘z samaradorligini yo‘qotib bormoqda. Shu sababli, Zero Trust modeli deyarli barcha muhim tarmoqlarda joriy etilmoqda.

Birinchidan, ushbu model **bulutli texnologiyalar (cloud computing)** sohasida alohida ahamiyat kasb etadi. Bulutli infratuzilmalarda foydalanuvchilar va xizmatlar turli joylardan kirish imkoniga ega bo‘lganligi sababli, ularni an’anaviy perimetr asosida himoyalash yetarli emas. Zero Trust yondashuvi esa har bir kirish so‘rovini individual tarzda tekshirish orqali ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlaydi.

Ikkinchidan, Zero Trust modeli **bank va moliya sektorida** keng qo‘llaniladi. Mazkur sohada moliyaviy operatsiyalar xavfsizligi, mijoz ma’lumotlarining himoyasi va firibgarlik holatlarining oldini olish ustuvor vazifa hisoblanadi. Modelning ko‘p faktorli autentifikatsiya, kontekstga asoslangan kirish nazorati va real vaqt monitoringi kabi mexanizmlari ushbu talablarni samarali bajarishga imkon beradi.

Uchinchidan, **davlat va hukumat axborot tizimlarida** Zero Trust modeli strategik ahamiyatga ega. Davlat tashkilotlarida saqlanadigan maxfiy ma’lumotlar, fuqarolar bazalari va boshqaruv tizimlari yuqori darajada himoyalanishi zarur. Zero Trust yondashuvi orqali har bir foydalanuvchi va qurilma qat’iy tekshiruvdan o‘tkazilib, ichki va tashqi tahdidlarga qarshi kompleks himoya ta’minlanadi.

Shuningdek, model **korporativ tarmoqlar va yirik tashkilotlar infratuzilmasida** ham keng joriy etilgan. Ayniqsa, masofaviy ish rejimi keng tarqalgan sharoitda xodimlar turli qurilmalar va tarmoqlar orqali tizimga ulanmoqda. Zero Trust modeli bu holatda har bir ulanishni tekshirish, qurilma xavfsizligini baholash va foydalanuvchiga faqat zarur resurslarga kirish huquqini berish orqali xavfsizlikni sezilarli darajada oshiradi. Bundan tashqari, **sog‘liqni saqlash tizimlarida** ushbu modelning qo‘llanilishi muhim hisoblanadi. Tibbiy ma’lumotlarning maxfiyligi va yaxlitligini ta’minlash, bemorlar haqidagi axborotlarni ruxsatsiz kirishlardan himoya qilish

dolzarb masalalardan biridir. Zero Trust modeli bu muammolarni samarali hal etishda zamonaviy yechim sifatida xizmat qiladi. Yana bir muhim yo‘nalish sifatida **ta’lim tizimi**ni keltirish mumkin. Universitetlar, ilmiy markazlar va onlayn ta’lim platformalarida katta hajmdagi foydalanuvchi va ilmiy ma’lumotlar saqlanadi. Zero Trust modeli ushbu tizimlarda foydalanuvchi autentifikatsiyasini kuchaytirish va ma’lumotlar xavfsizligini ta’minlashda muhim rol o‘ynaydi. Umuman olganda, Zero Trust modeli bugungi kunda turli sohalarda — bulutli xizmatlar, moliya tizimlari, davlat boshqaruvi, sog‘liqni saqlash, ta’lim va korporativ infratuzilmalarda keng qo‘llanilib, zamonaviy kiberxavfsizlikning ajralmas komponentiga aylanib bormoqda. Ushbu modelning moslashuvchanligi, yuqori darajadagi nazorat imkoniyatlari va kompleks himoya mexanizmlari uni kelajakda yanada keng joriy etilishiga zamin yaratadi.

Mazkur tadqiqotning asosiy maqsadi — bulutli tizimlarda ma’lumotlar xavfsizligini ta’minlashda Zero Trust modelining nazariy asoslarini chuqur tahlil qilish, uning asosiy komponentlarini tizimlashtirish va amaliy qo‘llash uchun optimal model ishlab chiqishdan iborat. Tadqiqot doirasida autentifikatsiya va avtorizatsiya jarayonlari, kirishni boshqarish siyosatlari, tarmoq segmentatsiyasi hamda monitoring tizimlari o‘zaro integratsiyalashgan holda o‘rganiladi. Natijada, bulutli muhitda yuqori darajadagi xavfsizlikni ta’minlashga xizmat qiluvchi samarali va moslashuvchan yondashuv ishlab chiqilishi ko‘zda tutiladi.

MATERIALS AND METHODS.

Ushbu tadqiqotda bulutli tizimlarda ma’lumotlar xavfsizligini ta’minlashda Zero Trust modelining samaradorligini o‘rganish uchun kompleks ilmiy-metodologik yondashuv qo‘llanildi. Tadqiqot metodologiyasi nazariy tahlil, tizimli modellashtirish, solishtirma (komparativ) tahlil va amaliy stsenariy asosida sinovdan o‘tkazish bosqichlarini o‘z ichiga oladi. Mazkur yondashuv orqali mavjud xavfsizlik muammolari aniqlanib, ularni bartaraf etishga qaratilgan samarali yechimlar ishlab chiqildi [6, 10–14 betlar]. Tadqiqotning axborot bazasini bulutli hisoblash va kiberxavfsizlik sohasiga oid ilmiy maqolalar, xalqaro standartlar va amaliy tavsiyalar tashkil etdi. Xususan, NIST (National Institute of Standards and Technology) hamda ISO/IEC xavfsizlik standartlari doirasidagi me’yoriy hujjatlar o‘rganilib, ular asosida xavfsizlik talablarining umumiy modeli shakllantirildi [7, 3–6 betlar]. Shu bilan birga, autentifikatsiya, avtorizatsiya va kirishni boshqarish tizimlariga oid zamonaviy texnologiyalar va platformalarning ishlash prinsiplari tahlil qilindi. Metodologik jihatdan tadqiqot bir necha izchil bosqichlarda amalga oshirildi.

Birinchi bosqichda bulutli tizimlarda uchraydigan asosiy xavfsizlik tahdidlari va zaifliklar aniqlanib, ular tizimli ravishda tasniflandi. Bu jarayonda ma’lumotlarga

ruxsatsiz kirish, insayder tahdidlar, identifikatsiya ma’lumotlarining o‘g‘irlanishi hamda tarmoq hujumlari asosiy xavf omillari sifatida ko‘rib chiqildi [2, 15–17 betlar].

Ikkinchi bosqichda an’anaviy perimetrga asoslangan xavfsizlik modeli bilan Zero Trust modeli o‘zaro solishtirildi. Ushbu solishtirma tahlil orqali har ikkala yondashuvning afzalliklari va kamchiliklari aniqlanib, Zero Trust modelining zamonaviy bulut infratuzilmalariga mosligi asoslab berildi [3, 22–25 betlar]. Natijada, statik ishonchga asoslangan tizimlardan dinamik va kontekstga asoslangan xavfsizlik modeliga o‘tish zarurati ilmiy jihatdan asoslandi.

Uchinchi bosqichda Zero Trust modelining asosiy komponentlari asosida konseptual arxitektura ishlab chiqildi. Ushbu model quyidagi asosiy elementlarni o‘z ichiga oladi: identifikatsiya va autentifikatsiya (Identity and Authentication), kirishni boshqarish (Access Control), tarmoq mikrosegmentatsiyasi va uzluksiz monitoring tizimi. Modelda foydalanuvchi va qurilmalarni tekshirish uchun ko‘p bosqichli autentifikatsiya (MFA), minimal ruxsat prinsipi (least privilege) hamda kontekstga asoslangan kirish nazorati mexanizmlari qo‘llanildi [8, 40–44 betlar].

Tarmoq xavfsizligini ta’minlash maqsadida mikrosegmentatsiya texnologiyasi joriy etilib, resurslar alohida himoyalangan zonalarga ajratildi. Bu yondashuv orqali tizim ichidagi harakatlar qat’iy nazorat ostiga olinib, tahdidlarning keng miqyosda tarqalishining oldi olindi [10, 50–55 betlar]. Shu bilan birga, barcha foydalanuvchi faoliyati va tizim hodisalarini kuzatish uchun real vaqt rejimidagi monitoring va loglarni tahlil qilish mexanizmlari ishlab chiqildi [9, 18–21 betlar].

Amaliy qismda ishlab chiqilgan model tipik bulutli muhit stsenariysi asosida sinovdan o‘tkazildi. Ushbu stsenariyda foydalanuvchining tizimga kirishi, autentifikatsiya jarayoni, resurslarga murojaat qilish va xavfsizlik tekshiruvlari bosqichma-bosqich modellashtirildi. Har bir bosqichda xavfsizlik siyosatlari qo‘llanilib, tizimning ruxsatsiz kirishlarga nisbatan bardoshliligi baholandi.

Natijada, qo‘llanilgan metodologiya Zero Trust modelining nazariy asoslarini amaliy mexanizmlar bilan uyg‘unlashtirish imkonini berdi hamda bulutli tizimlarda ma’lumotlar xavfsizligini ta’minlash uchun kompleks va moslashuvchan yondashuv ishlab chiqishga xizmat qildi.

RESULTS.

Mazkur tadqiqot doirasida ishlab chiqilgan Zero Trust asosidagi xavfsizlik modeli bulutli muhitda tipik stsenariylar asosida sinovdan o‘tkazildi va uning samaradorligi bir nechta asosiy mezonlar bo‘yicha baholandi. Olingan natijalar modelning an’anaviy xavfsizlik yondashuvlariga nisbatan sezilarli ustunliklarga ega ekanligini ko‘rsatdi hamda uning amaliy qo‘llanilish imkoniyatlarini tasdiqladi.

Birinchi navbatda, autentifikatsiya mexanizmlarining samaradorligi tahlil qilindi. Ko‘p bosqichli autentifikatsiya (MFA) joriy etilishi natijasida foydalanuvchini aniqlash aniqligi oshgani va ruxsatsiz kirish ehtimoli keskin kamaygani kuzatildi.

Tajriba davomida an’anaviy yagona parolga asoslangan tizim bilan solishtirganda, qo‘shimcha verifikatsiya bosqichlari mavjud bo‘lgan muhitda xavfsizlik darajasi sezilarli oshganligi aniqlandi [8, 40–44 betlar]. Bu esa identifikatsiya jarayonining ishonchliligini mustahkamlashda muhim omil ekanligini ko‘rsatdi.

Ikkinchi muhim natija sifatida kirishni boshqarish tizimining samaradorligi baholandi. Minimal ruxsat prinsipi (least privilege) asosida foydalanuvchilarga faqat zarur resurslarga kirish huquqi berilishi natijasida ortiqcha ruxsatlar soni kamaydi va ichki xavfsizlik zaifliklari minimallashtirildi. Natijalar shuni ko‘rsatdiki, ushbu yondashuv insayder tahdidlar xavfini kamaytirishda muhim rol o‘ynaydi hamda tizim ichidagi nazoratni kuchaytiradi [9, 18–21 betlar].

Uchinchi natija tarmoq xavfsizligi bilan bog‘liq bo‘lib, mikrosegmentatsiya texnologiyasining joriy etilishi orqali tizim ichidagi resurslar alohida segmentlarga ajratildi. Sinov natijalariga ko‘ra, bitta segmentda yuzaga kelgan xavfsizlik buzilishi boshqa segmentlarga tarqalish ehtimoli sezilarli darajada kamaygan. Bu esa tizimning umumiy barqarorligini oshirish va xavfsizlik hodisalarini lokal darajada cheklash imkonini berdi [10, 50–55 betlar].

Shuningdek, uzluksiz monitoring va real vaqt rejimidagi tahlil mexanizmlarining joriy etilishi muhim natijalardan biri sifatida qayd etildi. Tizimda barcha foydalanuvchi faoliyati, kirish urinishlari va tarmoq hodisalari doimiy ravishda kuzatilib, shubhali harakatlar tezkor aniqlangan. Natijada, xavfsizlik hodisalariga javob berish vaqti qisqargan va tahdidlarni erta bosqichda aniqlash imkoniyati oshgan [9, 18–21 betlar]. Amaliy stsenariy asosida o‘tkazilgan kompleks baholash natijalari shuni ko‘rsatdiki, Zero Trust modeli qo‘llanilganda bulutli tizimlarning umumiy xavfsizlik darajasi sezilarli darajada oshadi. Xususan, ruxsatsiz kirishlar sonining kamayishi, ma’lumotlar yaxlitligi va maxfiyligining yuqori darajada ta’minlanishi hamda tizimning moslashuvchan boshqaruv imkoniyatlarining kengayishi kuzatildi [4, 5–9 betlar].

Natijalar tahlili shuni ko‘rsatadiki, Zero Trust modeli nafaqat alohida xavfsizlik komponentlarini yaxshilaydi, balki ularning integratsiyalashgan holda ishlashini ta’minlab, kompleks xavfsizlik tizimini shakllantiradi. Bu esa bulutli muhitda barqaror va ishonchli xavfsizlik infratuzilmasini yaratish imkonini beradi.

Umuman olganda, olingan natijalar Zero Trust modelining bulutli tizimlarda ma’lumotlar xavfsizligini ta’minlashda yuqori samaradorlikka ega ekanligini tasdiqlaydi va uni zamonaviy kiberxavfsizlik tizimlarida qo‘llash maqsadga muvofiq ekanligini ko‘rsatadi.

DISCUSSION.

Mazkur tadqiqot natijalari Zero Trust modelining bulutli tizimlarda ma’lumotlar xavfsizligini ta’minlashdagi muhim afzalliklarini ko‘rsatib berdi. Olingan natijalar

asosida ushbu modelning nazariy va amaliy jihatlari chuqur tahlil qilinib, uning zamonaviy kiberxavfsizlik muammolarini hal etishdagi o‘rni aniqlashtirildi.

Birinchidan, tadqiqot natijalari shuni ko‘rsatdiki, an’anaviy perimetrga asoslangan xavfsizlik modellari bugungi kunda yetarli darajada samarali emas. Sababi, zamonaviy bulutli infratuzilmalarda foydalanuvchilar va resurslar tarmoq chegaralaridan tashqarida joylashgan bo‘lib, ularni faqat tashqi himoya bilan cheklash yetarli emas. Shu nuqtai nazardan, Zero Trust modeli “ishonma, har doim tekshir” tamoyiliga asoslanib, har bir kirish urinishini alohida tekshirish orqali xavfsizlikni yangi bosqichga olib chiqadi [1, 12–15 betlar].

Ikkinchidan, autentifikatsiya va avtorizatsiya mexanizmlarining kuchaytirilishi tizim xavfsizligining asosiy omillaridan biri sifatida namoyon bo‘ldi. Ko‘p faktorli autentifikatsiya (MFA) va kontekstga asoslangan kirish nazorati orqali foydalanuvchi haqiqiyligini aniqlash aniqligi sezilarli darajada oshdi. Biroq, bu yondashuv ayrim hollarda tizimdan foydalanish qulayligini pasaytirishi mumkinligi ham qayd etildi. Shu sababli, xavfsizlik va qulaylik o‘rtasida optimal muvozanatni ta’minlash muhim hisoblanadi [8, 40–44 betlar].

Uchinchi muhim jihat sifatida mikrosegmentatsiya va minimal ruxsat prinsipi samaradorligi muhokama qilindi. Tadqiqot natijalari ushbu yondashuvlar orqali ichki tahdidlar xavfi kamayishini ko‘rsatdi. Biroq, bu texnologiyalarni joriy etish murakkab konfiguratsiya va qo‘shimcha resurslarni talab qilishi mumkin. Ayniqsa, katta hajmdagi bulutli infratuzilmalarda segmentatsiya siyosatini to‘g‘ri tashkil etish muhim vazifa hisoblanadi [10, 50–55 betlar].

Shuningdek, uzluksiz monitoring va real vaqt rejimidagi tahlil tizimlari xavfsizlikni ta’minlashda muhim rol o‘ynashi aniqlandi. Bu tizimlar orqali tahdidlar tezkor aniqlanadi va ularga nisbatan choralar ko‘riladi. Shu bilan birga, katta hajmdagi ma’lumotlarni qayta ishlash zarurati hisoblash resurslariga bo‘lgan talabni oshiradi. Bu esa tizimni joriy etishda texnik va iqtisodiy omillarni hisobga olish zarurligini ko‘rsatadi [9, 18–21 betlar]. Tadqiqot davomida yana bir muhim jihat sifatida Zero Trust modelining moslashuvchanligi qayd etildi. Ushbu model turli bulut platformalari va infratuzilmalarga moslashuvchan tarzda integratsiya qilinishi mumkin. Bu esa uni universal xavfsizlik yechimi sifatida qo‘llash imkonini beradi. Biroq, uni to‘liq joriy etish tashkilotdan aniq strategiya, malakali mutaxassislar va bosqichma-bosqich implementatsiyani talab etadi [4, 5–9 betlar].

Umuman olganda, muhokama natijalari shuni ko‘rsatadiki, Zero Trust modeli zamonaviy bulutli tizimlar uchun eng istiqbolli xavfsizlik yondashuvlaridan biri hisoblanadi. U an’anaviy modellarning kamchiliklarini bartaraf etib, xavfsizlikni kompleks va integratsiyalashgan tarzda ta’minlaydi. Shu bilan birga, modelni joriy etishda texnik murakkablik, xarajatlar va foydalanuvchi tajribasi kabi omillarni ham e’tiborga olish zarur. Kelgusidagi tadqiqotlarda Zero Trust modelini sun’iy intellekt

va mashinaviy o‘rganish texnologiyalari bilan integratsiya qilish orqali yanada takomillashtirish, shuningdek, uning real sektor tizimlaridagi samaradorligini kengroq amaliy tajribalar asosida o‘rganish maqsadga muvofiq hisoblanadi.

ADABIYOTLAR RO‘YXATI.

1. NIST. *Zero Trust Architecture*. — Gaithersburg: National Institute of Standards and Technology, 2020.
2. Rose, S., Borchert, O., Mitchell, S., Connelly, S. *Zero Trust Architecture (NIST SP 800-207)*. — USA: NIST, 2020.
3. Kindervag, J. *Build Security Into Your Network’s DNA: The Zero Trust Network Architecture*. — Forrester Research, 2010.
4. Stallings, W. *Cryptography and Network Security: Principles and Practice*. — 7-nashr. — Pearson Education, 2017.
5. Kaufman, C., Perlman, R., Speciner, M. *Network Security: Private Communication in a Public World*. — 2-nashr. — Prentice Hall, 2016.
6. Aljawarneh, S., Aldwairi, M., Yassein, M. B. *Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model*. — Journal of Computational Science, 2018.
7. Behl, A., Behl, K. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. — Oxford University Press, 2017.
8. Grassi, P. A., Garcia, M. E., Fenton, J. L. *Digital Identity Guidelines (NIST SP 800-63)*. — NIST, 2017.
9. Scarfone, K., Mell, P. *Guide to Intrusion Detection and Prevention Systems (IDPS)*. — NIST Special Publication, 2019.
10. VMware. *Micro-Segmentation for Dummies*. — Wiley Publishing, 2019.