IQTISODIY AXBOROT TIZIMLARIDA AXBOROTLARNI HIMOYALASH USULLARI

Rajaboyev Shahboz Shodi o'g'li
Samarqand iqtisodiyot va servis instituti
"Axborot texnologiyalari" kafedrasi assistenti.
shahbozrajabboyev@gmail.com
Ravshanov Nurbek Sharofiddin o'g'li
ravshanovnurbek06@gmail.com
Samarqand iqtisodiyot va servis instituti,
kechki ta'lim fakulteti talabasi.

Annotatsiya: Hozirgi raqamli iqtisodiyot davrida axborot resurslari muhim strategik ahamiyat kasb etmoqda. Iqtisodiy axborot tizimlari (IAT) moliyaviy, buxgalteriya va boshqaruv ma'lumotlarini saqlash, qayta ishlash hamda uzatishda markaziy rol o'ynaydi. Ushbu tizimlarning xavfsizligi ta'minlanmasa, moliyaviy yo'qotishlar, maxfiy ma'lumotlarning oshkor bo'lishi va biznes jarayonlarining to'xtab qolishi kabi jiddiy oqibatlar yuzaga kelishi mumkin. Ushbu maqolada iqtisodiy axborot tizimlarida axborotlarni himoyalashning asosiy usullari — kriptografiya, autentifikatsiya, kirishni nazorat qilish, zaxiralash va tarmoq xavfsizligi — ilmiy-amaliy jihatdan tahlil qilinadi. Shuningdek, zamonaviy kibertahdidlar va ulardan himoyalanish strategiyalari ko'rib chiqiladi.

Kalit so'zlar: Axborot xavfsizligi, kriptografiya, autentifikatsiya, kibertahdidlar, iqtisodiy axborot tizimlari, kirishni nazorat qilish, raqamli transformatsiya.

Kirish.

Raqamli iqtisodiyotning jadal rivojlanishi sharoitida axborot resurslari har qachongidan ko'ra muhimroq ahamiyat kasb etmoqda. Korxonalar, moliya muassasalari va davlat organlari kundalik faoliyatini axborot tizimlari orqali amalga oshiradi. Iqtisodiy axborot tizimlari (IAT) bu jarayonning asosini tashkil etib, moliyaviy operatsiyalar, buxgalteriya hisobi, ta'minot zanjiri boshqaruvi va qaror qabul qilish jarayonlarini avtomatlashtiradi.

Biroq axborot tizimlarining keng tarqalishi ularga bo'lgan tahdidlarning ham ortishiga olib keldi. Kiberhujumlar, ma'lumotlar sizib chiqishi, fishing hujumlari va zararli dasturlar iqtisodiy faoliyatga jiddiy zarar yetkazmoqda. Jahon iqtisodiy forumining 2025-yilgi ma'lumotlariga ko'ra, kiberjinoyatchilik yillik zarar hajmi 10 trillion dollarga yetib borishi kutilmoqda. Bunday sharoitda iqtisodiy axborot

tizimlarida axborotlarni himoyalash usullarini chuqur o'rganish va amaliyotga tatbiq etish dolzarb vazifaga aylanmoqda.

Ushbu maqola axborotni himoyalashning zamonaviy usullarini tizimli tahlil qilish, ularning iqtisodiy axborot tizimlaridagi qo'llanilish xususiyatlarini aniqlash va samarali himoya strategiyalarini ishlab chiqishga qaratilgan.

Mavzuga oid adabiyotlar tahlili.

Axborot xavfsizligi sohasida ko'plab tadqiqotlar olib borilgan. **Rajaboyev Sh.Sh., Jumayev L.G'.** (2024) "Ta'lim sohasida ma'lumotlar bazasini qo'llanishi" nomli maqolasida ma'lumotlar bazasi tizimlarini ta'lim muhitida qo'llash xususiyatlarini o'rganib, axborotni saqlash va himoyalashning asosiy tamoyillarini ko'rib chiqqan. Muallif ma'lumotlar bazasida kirishni nazorat qilish (access control) mexanizmlari rolini alohida ta'kidlagan [6].

Rajaboyev Sh.Sh., Ziyodullayev F.V. (2024) axborot-kommunikatsiya texnologiyalarini rivojlantirish bo'yicha qarorlar mohiyatini tahlil qilib, raqamli infratuzilmani himoyalashda normativ-huquqiy bazaning ahamiyatini ko'rsatgan. Tadqiqotda milliy axborot xavfsizligi siyosatining strategik yo'nalishlari yoritilgan [7].

Rajaboyev Sh.Sh., Umidov D.U. (2024) "Axborot kommunikatsiya texnologiyalarining buxgalteriya sohasidagi o'rni" nomli asarida axborot tizimlarining moliyaviy hisobotlashda tutgan o'rni va buxgalteriya ma'lumotlarini himoyalash zaruriyatini asoslab bergan. Moliyaviy axborotga nisbatan maxfiylik, yaxlitlik va mavjudlik (CIA triadi) tamoyillarini tatbiq etish metodologiyasi bayon etilgan [8].

Rajaboyev Sh.Sh., Raxmatov O.A. (2024) iqtisodiy axborotlarni qayta ishlash bazasining tarkibi va uni tashkil etish bosqichlarini o'rgangan. Tadqiqotda axborot tizimlarining strukturaviy tarkibi, ma'lumotlar oqimlarini nazorat qilish va axborot xavfsizligini ta'minlashning tashkiliy-texnik choralari ko'rib chiqilgan [9].

Rajaboev Sh.Sh., Raxmatov O.A. (2024) "Information Technology Is Now Used Everywhere" maqolasida zamonaviy axborot texnologiyalarining keng tarqalishi axborot xavfsizligi muammolarini ham global miqyosda kengaytirayotganligini ta'kidlagan. Turli sektarlarda axborotni himoyalashning dolzarbligi va zamonaviy yechimlar tahlil qilingan [10].

Rajaboev Sh.Sh., Gaffarov A.B. (2025) axborot-kommunikatsiya texnologiyalarini rivojlantirishga qaratilgan qarorlarning mohiyatini o'rganib, kiberhimoya choralarini milliy siyosat darajasida amalga oshirishning nazariy asoslarini bayon etgan [11].

Ражабоев Ш., Хамидова П. (2025) raqamli iqtisodiyot sharoitida axborot-kommunikatsiya xizmatlaridan foydalanish imkoniyatlarini tahlil qilib, onlayn muhitda axborot xavfsizligini ta'minlashning ustuvor yo'nalishlarini belgilab bergan [12].

Mohammad A.A.Sh. va boshq. (2025) moliyaviy texnologiyalar orqali onlayn buxgalteriyaning moliya institutlari samaradorligiga ta'sirini o'rganib, raqamli moliyaviy operatsiyalarda axborot xavfsizligi talab darajasida ta'minlanmasligining xatarlarini ko'rsatgan [5].

Tahlil va natijalar.

Iqtisodiy axborot tizimlariga asosiy tahdidlar.

Iqtisodiy axborot tizimlariga yo'naltirilgan tahdidlar ikki asosiy guruhga bo'linadi: tashqi tahdidlar (kiberhujumlar, xakerlik, zararli dasturlar, fishing) va ichki tahdidlar (xodimlarning qoidabuzarliklari, tasodifiy xatolar, ma'lumotlar o'g'irlash). Cisco Security Report 2024 ma'lumotlariga ko'ra, moliyaviy sektorda ro'yxatga olingan kiberinsidentlarning 43 foizini ichki tahdidlar tashkil etgan.

IAT ga yo'naltirilgan tahdidlarning tasnifi

Fishing hujumlari — foydalanuvchilarni aldab maxfiy ma'lumotlarni olish; Ransomware — ma'lumotlarni shifrlash va to'lov talab qilish; DDoS — tizim ishini to'xtatishga qaratilgan hujumlar; SQL-in'eksiya — ma'lumotlar bazasiga ruxsatsiz kirish; Insider tahdid — ichki foydalanuvchilar tomonidan ma'lumot sizib chiqishi.

Kriptografik himoya usullari.

Kriptografiya axborot xavfsizligining asosi hisoblanadi. Simmetrik shifrlash (AES-256) tezkorligi bilan ajralib turadi va katta hajmdagi ma'lumotlarni shifrlashda qo'llaniladi. Asimmetrik kriptografiya (RSA, ECC) esa kalitlarni xavfsiz almashish va raqamli imzo yaratishda ishlatiladi. Zamonaviy iqtisodiy axborot tizimlarida TLS/SSL protokollari ma'lumotlarni uzatishda, AES-256 esa saqlashda keng qo'llanilmoqda.

Blockchain texnologiyasi moliya sohasida kriptografik himoyaning yangi bosqichi sifatida ko'rilmoqda. Tranzaksiyalar zanjiri o'zgartirib bo'lmaydigan tarzda yozilishi tufayli moliyaviy hisobotlar yaxlitligi ta'minlanadi. O'zbekiston Respublikasida "Raqamli O'zbekiston – 2030" dasturi doirasida davlat axborot tizimlarida kriptografik himoyaning joriy etilishi kengaytirilmoqda.

Autentifikatsiya va kirishni nazorat qilish.

Ko'p bosqichli autentifikatsiya (Multi-Factor Authentication – MFA) zamonaviy iqtisodiy axborot tizimlarida majburiy element sifatida qabul qilinmoqda. NIST SP 800-63 standartiga muvofiq, moliyaviy tizimlar uchun kamida ikki faktorli autentifikatsiya tavsiya etiladi: bilim omili (parol), egalik omili (token, SMS kodi) va biometrik omil (barmoq izi, yuz tanish).

Rolga asoslangan kirishni nazorat qilish (Role-Based Access Control – RBAC) modeli xodimlarning lavozimiga qarab axborotga kirish huquqlarini cheklaydi. Bu model buxgalteriya, moliya va boshqaruv tizimlarida keng qo'llaniladi. "Minimal imtiyoz" tamoyili (Principle of Least Privilege) esa har bir foydalanuvchiga faqat o'z vazifalarini bajarishi uchun zarur minimal huquqlar berilishini ta'minlaydi.

Tarmoq xavfsizligi va monitoring.

Tarmoq xavfsizligi tizimlariga quyidagi elementlar kiradi: xavfsizlik devori (Firewall), bosqinni aniqlash va oldini olish tizimlari (IDS/IPS), virtual xususiy tarmoqlar (VPN) va tarmoq monitoringi vositalari. SIEM (Security Information and Event Management) tizimlari iqtisodiy axborot muhitidagi barcha hodisalarni real vaqt rejimida kuzatib, g'ayritabiiy faoliyatni avtomatik aniqlaydi.

Zero Trust arxitekturasi zamonaviy iqtisodiy tashkilotlarda tobora keng joriy etilmoqda. Bu yondashuv "hech kimga ishonma, hamma narsani tekshir" tamoyiliga asoslanib, tashqi va ichki tahdidlarga nisbatan bir xil darajada ehtiyotkorlikni talab etadi. Gartner tadqiqot markazi bashoratiga ko'ra, 2026 yilga kelib yirik tashkilotlarning 60 foizdan ko'prog'i Zero Trust modeliga o'tishi kutilmoqda.

Ma'lumotlarni zaxiralash va tiklash.

Moliyaviy axborot tizimlarining uzluksiz ishlashi uchun backup strategiyasi muhim ahamiyat kasb etadi. 3-2-1 qoidasi (3 nusxa, 2 xil muhit, 1 tashqi joy) sanoat standarti sifatida keng qabul qilingan. Bulutli zaxiralash yechimlari (AWS Backup, Azure Backup) iqtisodiy tashkilotlarga geografik jihatdan taqsimlangan himoyani ta'minlaydi. RPO (Recovery Point Objective) va RTO (Recovery Time Objective) ko'rsatkichlari tizimning hujumdan so'ng qanchalik tez tiklanishini belgilaydi.

Qiyosiy tahlil.

Himoya usullarining samaradorlik tahlili (ekspert baholash asosida)

Kriptografiya (AES-256/RSA): Samaradorlik — 95%; Joriy etish qiyinligi — O'rtacha; Qo'llanish sohasi — Ma'lumot saqlash va uzatish. MFA: Samaradorlik — 99.9% (Microsoft ma'lumotlari); Qiyinlik — Past; Qo'llanish — Tizimga kirish nazorati. RBAC: Samaradorlik — 85%; Qiyinlik — O'rtacha; Qo'llanish — Korporativ tizimlar. SIEM/IDS: Samaradorlik — 90%; Qiyinlik — Yuqori; Qo'llanish — Real vaqt monitoringi. Zero Trust: Samaradorlik — 92%; Qiyinlik — Yuqori; Qo'llanish — Zamonaviy tarmoqlar.

Axborot xavfsizligi investitsiyalari va zararlar nisbati (mlrd doll.)

Yil	Kiberzarar (mlrd $)	Himoya investitsiyasi (mlrd $)
2020	1000	123
2021	6000	150
2022	8000	172
2023	8500	188
2024	9500	215

Manba: Cybersecurity Ventures, Gartner (2024)

Jadval ma'lumotlari shuni ko'rsatadiki, kiberzarar hajmi himoya investitsiyalaridan ancha yuqori o'sish suratida ko'paymoqda. Bu esa proaktiv himoya strategiyasining iqtisodiy jihatdan asoslanganligini tasdiqlaydi.

Xulosa va taklif.

Iqtisodiy axborot tizimlarida axborotlarni himoyalash murakkab va ko'p qirrali muammo bo'lib, texnik, tashkiliy va huquqiy choralar majmuini talab etadi. Amalga oshirilgan tahlil asosida quyidagi xulosalarga kelish mumkin:

Birinchidan, kriptografik himoya (AES-256, RSA, ECC) moliyaviy ma'lumotlar xavfsizligining texnik asosini tashkil etadi va barcha IAT da majburiy element sifatida joriy etilishi lozim. Ikkinchidan, ko'p bosqichli autentifikatsiya (MFA) kiberhujumlarning 99.9 foizini oldini olish imkonini beradi — bu eng samarali va arzon himoya usuli hisoblanadi. Uchinchidan, Zero Trust arxitekturasi va RBAC modeli korporativ axborot muhitida ruxsatsiz kirishni minimallashtiradi. To'rtinchidan, SIEM tizimlari yordamida real vaqtda monitoring kiberhujumlarni erta bosqichda aniqlashga imkon beradi. Beshinchidan, axborot xavfsizligi faqat texnologiyadan iborat emas — xodimlarni muntazam o'qitish, xavfsizlik madaniyatini shakllantirish va tashkiliy siyosatni yangilash bir xil muhim ahamiyat kasb etadi.

O'zbekiston iqtisodiy tashkilotlari uchun tavsiya sifatida ISO/IEC 27001 xalqaro standarti asosida axborot xavfsizligi boshqaruv tizimini joriy etish, milliy kiberhimoya markazlari (CERT) bilan hamkorlikni kuchaytirish va axborot xavfsizligi mutaxassislari tayyorlashga investitsiyalarni oshirish maqsadga muvofiq hisoblanadi.

Foydalanilgan adabiyotlar

1. Xalilillayevna Y. X. ELEKTRON JADVALDA HISOBOTLAR YARATISH //Лучшие интеллектуальные исследования. – 2026. – Т. 65. – №. 2. – С. 320-327.
2. Musayevich S. A., Asqarovich A. J. EXCEL JADVAL HISOBLAGICHIDAGI MOLIYAVIY FUNKSIYALAR VA ULARDAN FOYDALANISH //Ustozlar uchun. – 2025. – Т. 86. – №. 1. – С. 354-357.
3. Musayevich S. A., Sadoqat A. EXCEL JADVAL HISOBLAGICHIDAGI MANTIQIY FUNKSIYALAR VA ULARDAN FOYDALANISH //Ustozlar uchun. – 2025. – Т. 86. – №. 2. – С. 115-119.
4. Ariana I. M., Bagiada I. M. Development of spreadsheet-based integrated transaction processing systems and financial reporting systems //Journal of Physics: Conference Series. – IOP Publishing, 2018. – Т. 953. – №. 1. – С. 012102.
5. Mohammad, A. A. Sh., Salinas, L., Muzrapova, Sh., Baxriddinov, N., Ahrorov, Z., & Boronov, B. (2025). The impact of online accounting through the expansion of financial technologies on improving the performance of financial institutions and banks. Economic Annals-XXI, 215(5-6), 16-21. doi: https://doi.org/10.21003/ea.V215-03

6. Rajaboyev Sh.Sh., and Jumayev L.G'. "TA'LIM SOHASIDA MA'LUMOTLAR BAZASINI QO'LLANISHI" Экономика и социум, no. 4-2 (119), 2024, pp. 407-411.
7. Rajaboyev Sh.Sh., and Ziyodullayev F.V. "AXBOROT-KOMMUNIKATSIYA TEXNOLOGIYALARINI RIVOJLANTIRISH CHORA-TADBIRLARI TO'G'RISIDAGI QARORLAR MOHIYATI" Экономика и социум, no. 5-1 (120), 2024, pp. 675-680.
8. Rajaboyev Sh.Sh., and Umidov D.U. "AXBOROT KOMMUNIKATSIYA TEXNOLOGIYALARINING BUXGALTERIYA SOHASIDAGI O'RNI" Экономика и социум, no. 4-2 (119), 2024, pp. 393-396.
9. Rajaboyev Sh.Sh., and Raxmatov O.A. "IQTISODIY AXBOROTLARNI QAYTA ISHLASH BAZASINING TARKIBI VA UNI TASHKIL ETISH BOSQICHLARI" Экономика и социум, no. 4-2 (119), 2024, pp. 397-402.
10. Rajaboev Shahboz Shodiyevich, and Raxmatov Ozodbek Aktam O'g'li. "Information Technology Is Now Used Everywhere". Miasto Przyszłości, vol. 44, Jan. 2024, pp. 114-21.
11. Rajaboev, Shahboz Shodiyevich, and Abdunazar Burkhonovich Gaffarov. "ESSENCE OF DECISIONS ON MEASURES FOR THE DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES." Bulletin news in New Science Society International Scientific Journal 2.1 (2025): 120-125.
12. Ражабоев Ш., и П. Хамидова. «ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ УСЛУГ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ». Экономическое развитие и анализ, т. 3, вып. 1, январь 2025 г., сс. 120-4.