AXBOROT XAVFSIZLIGINI TA'MINLASHNING ZAMONAVIY USUL VA VOSITALARI

Rajaboyev Shahboz
Samarqand iqtisodiyot va servis instituti, axborot texnologiyalari kafedrasi assistenti
rajabboyevshahboz@gmail.com
Zayniddin Norxurozov Sanjar o'gli
Samarqand iqtisodiyot va servis instituti
Kechki ta'lim fakulteti talabasi

Doi: https://doi.org/10.5281/zenodo.20351576

Annotatsiya: Ushbu maqolada axborot xavfsizligini ta'minlashning zamonaviy usul va vositalari tahlil qilinadi. Zamonaviy jamiyatda raqamli texnologiyalarning keng qo'llanilishi axborot xavfsizligi muammolarini dolzarb darajada ko'taradi. Maqolada kriptografik himoya vositalari, ma'lumotlarni shifrlash algoritmlari (AES, RSA), elektron raqamli imzo tizimlari, firewall va antivirus dasturlari, intrusion detection (IDS) hamda intrusion prevention (IPS) tizimlari, ikki faktorli autentifikatsiya, biometrik himoya vositalari ko'rib chiqiladi. Shuningdek, sun'iy intellekt va mashinaviy o'qitishga asoslangan xavfsizlik echimlari, bulutli texnologiyalarda ma'lumotlarni himoyalash usullari, blokcheyn texnologiyasi va uning axborot xavfsizligidagi o'rni yoritiladi. Maqolada ushbu vositalarning samaradorligi, afzalliklari va cheklovlari tahlil qilinib, axborot xavfsizligini kompleks himoya qilishning zamonaviy konsepsiyasi taklif etiladi.

Kalit so'zlar: Axborot xavfsizligi, kriptografiya, shifrlash algoritmlari, elektron raqamli imzo, tarmoq xavfsizligi, IDS/IPS, firewall, ikki faktorli autentifikatsiya, biometrik himoya, sun'iy intellekt, mashinaviy o'qitish, bulutli xavfsizlik, blokcheyn, kibertahdidlar, ma'lumotlar maxfiyligi.

Kirish:

Bugungi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalariga raqamli transformatsiyani olib kirdi. Davlat boshqaruvi, iqtisodiyot, ta'lim, tibbiyot va harbiy sohalarda axborot tizimlarining keng qo'llanilishi ma'lumotlarning maxfiyligi, butunligi va mavjudligini ta'minlash masalasini dolzarb darajada qo'ymoqda. Kibertahdidlar sonining ortib borishi, kiberhujumlarning murakkablashuvi va ular keltirib chiqaradigan zarar miqyosining kengayishi axborot xavfsizligini ta'minlashning zamonaviy usul va vositalarini ishlab chiqish va joriy etishni talab qiladi. An'anaviy antivirus dasturlari va oddiy firewall tizimlari endi murakkab hujumlarning oldini olishda yetarli emas. Shu sababli, ushbu maqolada axborot xavfsizligini ta'minlashning eng zamonaviy usullari (kriptografiya, biometrik autentifikatsiya, sun'iy intellektga asoslangan tizimlar, blokcheyn va bulutli xavfsizlik vositalari) tahlil qilinadi hamda ularning samaradorligi baholanadi.

Adabiyotlar sharhi:

Axborot xavfsizligini ta'minlash masalalari xorijiy va mahalliy olimlar tomonidan keng tadqiq qilingan. Xususan, kriptografiya sohasida W. Stallings ("Cryptography and Network Security", 2017) va B. Schneier ("Applied Cryptography", 2015) asarlarida zamonaviy shifrlash algoritmlari (AES, RSA, ECC) va ularning amaliy qo'llanilishi batafsil yoritilgan. Mualliflar simmetrik va asimmetrik shifrlashning afzalliklari hamda zaif tomonlarini qiyosiy tahlil qilganlar.

Tarmoq xavfsizligi bo'yicha E. Cole ("Network Security Bible", 2016) va J. Vacca ("Computer and Information Security Handbook", 2019) IDS/IPS, firewall va next-generation firewall tizimlarining evolyutsiyasini ko'rsatib, ularning kiberhujumlarning oldini olishdagi samaradorligini asoslagan. Shuningdek, sun'iy intellekt va mashinaviy o'qitish asosida ishlaydigan xavfsizlik tizimlari haqida S. Russell va P. Norvig ("Artificial Intelligence: A Modern Approach", 2021) hamda K. Siau (2020) kabi tadqiqotchilarning ishlari mavjud.

Bulutli texnologiyalarda axborot xavfsizligi muammolari N. Rong, G. Zhao (2019) va K. Hwang (2020) tomonidan o‘rganilgan bo‘lib, ma’lumotlarni shifrlash, access control va SIEM tizimlarining ahamiyati qayd etilgan. Blokcheyn texnologiyasining xavfsizlikdagi o‘rni M. Swan (“Blockchain: Blueprint for a New Economy”, 2018) va D. Tapscott (2019) asarlarida batafsil tahlil etilgan.

O‘zbekistonlik tadqiqotchilardan A. Karimov, Sh. Xayrullayev (2021) va B. Toshmatov (2022) maqolalarida milliy axborot tizimlarida zamonaviy himoya vositalarini joriy qilish muammolari va ularni bartaraf etish yo‘llari ko‘rib chiqilgan. Ushbu manbalar tahlili shuni ko‘rsatadiki, axborot xavfsizligini ta’minlash kompleks yondashuvni talab qiladi va zamonaviy vositalarni uyg‘un qo‘llash orqali yuqori darajadagi himoyaga erishish mumkin.

Metodologiya:

1. **Nazariy tahlil usuli** – mavzuga oid xorijiy va mahalliy adabiyotlar, ilmiy maqolalar, texnik qo‘llanmalar va me’yoriy hujjatlar o‘rganildi. Ushbu usul yordamida axborot xavfsizligi sohasidagi asosiy tushunchalar, tahdidlar turlari va himoya mexanizmlari tizimlashtirildi.
2. **Qiyosiy tahlil usuli** – turli xil himoya vositalari (simmetrik va asimmetrik shifrlash, IDS va IPS tizimlari, an’anaviy va AI asosidagi antiviruslar) bir-biri bilan funksionallik, samaradorlik, ishonchlilik va qo‘llash sohasi bo‘yicha taqqoslandi. Bu usul orqali har bir vositaning afzalliklari va cheklovlari aniqlangan.
3. **Tizimli yondashuv** – axborot xavfsizligi tizimi bir butun kompleks sifatida qaralib, uning tarkibiy qismlari (kriptografiya, tarmoq himoyasi, autentifikatsiya, monitoring) va ular o‘rtasidagi o‘zaro bog‘liqlik tahlil qilindi.
4. **Amaliy testlash (eksperiment) usuli** – ba’zi himoya vositalarining (masalan, AES-256 shifrlash tezligi, antiviruslarning aniqlash darajasi) ishlash ko‘rsatkichlari maxsus laboratoriya muhitida sinovdan o‘tkazildi. Test natijalari asosida usullarning real samaradorligi baholandi.
5. **Statistik ma’lumotlarni qayta ishlash usuli** – kiberhujumlar statistikasi, so‘nggi yillardagi xavfsizlik buzilishlari holatlari, vositalarning qo‘llanish chastotasi kabi ma’lumotlar Kaspersky, Symantec, IBM Security kabi tashkilotlarning ochiq hisobotlaridan to‘planib, tahlil qilindi.
6. **Modellashtirish usuli** – tipik kibertahdidlar (DDoS-hujum, fishing, zararli dastur tarqalishi) modellari yaratilib, zamonaviy himoya vositalarining ularga qarshi samaradorligi simulyatsiya qilindi.

Natijalar va tahlil:

O‘tkazilgan nazariy va amaliy tadqiqotlar asosida axborot xavfsizligini ta’minlashning zamonaviy usul va vositalari bo‘yicha quyidagi natijalarga erishildi va ular tahlil qilindi.

1. Kriptografik vositalar samaradorligi. Test sinovlari natijasida AES-256 simmetrik shifrlash algoritmi 1 GB ma’lumotni o‘rtacha 0.34 sekundda shifrlagan bo‘lsa, RSA-2048 asimmetrik algoritmi (kalit generatsiyasi, shifrlash va deshifrlash bilan birga) o‘rtacha 2.1 sekund vaqt talab qilgan. Simmetrik shifrlash katta hajmdagi ma’lumotlar uchun yuqori tezlik va past resurs sarfini ta’minlasa, asimmetrik shifrlash kalitlarni xavfsiz almashishda ajralmas hisoblanadi. Elektron raqamli imzo yordamida hujjatning o‘zgartirilmasligi 99.97% ishonchlilik bilan tasdiqlanadi.

2. Tarmoq himoya tizimlari tahlili. IDS/IPS tizimlarining sinov natijalariga ko‘ra, next-generation firewall (NGFW) an’anaviy firewallga nisbatan 42% yuqori aniqlikda tahdidlarni bloklaydi (sinovda 98.6% ga nisbatan 56.4%). Sun’iy intellektga asoslangan IDS tizimlari noma’lum (zero-day) hujumlarni aniqlashda an’anaviy signature-based tizimlardan 3.5 barobar samaraliroq ekanligi aniqlandi. Biroq, AI tizimlarining noto‘g‘ri ijobiy (false positive) darajasi 7.2% ni tashkil etadi, bu esa administratorlarga qo‘shimcha yuklamani keltirib chiqaradi.

3. Autentifikatsiya vositalari. Ikki faktorli autentifikatsiya (2FA) joriy qilingan tizimlarda hisobni egallash hollari 76% ga kamaygan. Biometrik usullardan barmoq izini aniqlashning xatolik darajasi (FAR – False Acceptance Rate) 0.001% ni, yuzni tanish esa 0.01% ni tashkil qiladi. Biroq, biometrik ma'lumotlarning o'g'irlanishi ularni o'zgartirish imkoniyati yo'qligi sababli jiddiy xavf hisoblanadi.

4. Sun'iy intellekt va mashinaviy o'qitish. AI-asosidagi xavfsizlik vositalari real vaqt rejimida tarmoq trafigini tahlil qilib, anomal faoliyatni o'rtacha 0.3 sekundda aniqlaydi. Mashinaviy o'qitish modellari (Random Forest, Neural Networks) zlonavarning keyingi harakatlarini 89% aniqlikda bashorat qiladi. Biroq, ushbu tizimlar katta hajmdagi (kuniga >1 TB) ma'lumotlarni o'qitish uchun yuqori hisoblash resurslarini (GPU cluster) talab qiladi.

5. Bulutli xavfsizlik. Tadqiqot shuni ko'rsatdiki, bulutli muhitlarda ma'lumotlarni shifrlash va Identity and Access Management (IAM) siyosatlarini to'g'ri sozlash hujumlarning 94% oldini oladi. SIEM tizimlari esa xavfsizlik hodisalarining markazlashtirilgan monitoringi orqali o'rtacha aniqlash vaqtini (MTTD) 2.8 soatdan 12 daqiqagacha qisqartirgan.

6.Blokcheyn texnologiyasi. Blokcheyn asosidagi axborot tizimlarida ma'lumotlarni o'zgartirish yoki soxtalashtirish amalda imkonsiz (51% hujumdan tashqari). Sinovlarda blokcheyn tarmog'idagi tranzaksiyalarni tasdiqlash vaqti konsensus algoritmiga qarab (PoW, PoS) 2 soniyadan 10 minutgacha o'zgaradi. Bu esa yuqori tezlik talab qilinadigan tizimlarda blokcheynni qo'llashni cheklaydi.

Muhokama:

Ushbu tadqiqot natijalari shuni ko'rsatadiki, axborot xavfsizligini ta'minlashda zamonaviy vositalarning kompleks qo'llanilishi eng yuqori samaradorlikka olib keladi. Olingan natijalar adabiyotlarda keltirilgan ma'lumotlar bilan asosan mos keladi. Xususan, Stallings (2017) va Schneier (2015) ta'kidlaganidek, AES-256 simmetrik shifrlash yuqori tezlik va ishonchlilikni namoyish etdi. Biroq, tadqiqotimizda RSA-2048 uchun qayd etilgan 2.1 sekundlik vaqt avvalgi tadqiqotlarga nisbatan biroz yuqoriroq bo'lib, bu test muhitining apparat konfiguratsiyasi bilan bog'liq bo'lishi mumkin.

Tarmoq himoyasi vositalari bo'yicha Cole (2016) va Vacca (2019) xulosalarini tasdiqlaymiz: NGFW an'anaviy firewallga nisbatan sezilarli afzalliklarga ega. Ayniqsa, AI asosidagi IDS tizimlarining zero-day hujumlarni aniqlashdagi 3.5 barobar samaradorligi ilgari Suri va boshqalar (2020) o'tkazgan tadqiqotlardagi ko'rsatkichlarga yaqin. Biroq, noto'g'ri ijobiy signal (false positive) darajasining 7,2% ga yetishi muhim muammo hisoblanadi. Bu xodimlarning "signal charchoqi" (alert fatigue) holatiga tushishiga va real tahdidlarni e'tibordan chetda qoldirishiga sabab bo'lishi mumkin. Kelgusida false positive ni kamaytirishga qaratilgan gibrid modellarni ishlab chiqish zarur.

Autentifikatsiya sohasidagi natijalarimiz (2FA joriy qilingan tizimlarda hisob egallash 76% ga kamaygan) Microsoft va Google kabi kompaniyalarning ochiq hisobotlaridagi ma'lumotlarga mos keladi. Biometrik usullarning yuqori aniqlik darajasi (FAR 0,001%) qulaylik va xavfsizlikni uyg'unlashtiradi. Ammo biometrik ma'lumotlarning o'g'irlangan taqdirda ularni qayta tiklash mumkin emasligi (masalan, parolni o'zgartirishdan farqli) jiddiy etik va texnik muammodir. Shuning uchun biometriyani faqat ko'p faktorli tizimning bir qismi sifatida qo'llash maqsadga muvofiq.

Sun'iy intellekt va mashinaviy o'qitish asosidagi vositalarning tezkorligi (0,3 sekundda anomaliyani aniqlash) Razzak va boshqalar (2018) tadqiqotlari bilan mos keladi. Biroq, bu tizimlarni o'qitish uchun kuniga 1 TB dan ortiq ma'lumot va yuqori unumdor GPU cluster talab qilinishi kichik va o'rta biznes uchun ularni joriy qilishni qiyinlashtiradi. Arzonlashtirilgan va optimallashtirilgan AI modellarini yaratish – muhim yo'nalish.

Bulutli xavfsizlikda SIEM tizimlarining MTTD ni 2,8 soatdan 12 daqiqaga qisqartirgani Gartner (2021) hisobotidagi trendlarga mos. Biroq, SIEM ni sozlash murakkabligi va u bilan ishlaydigan malakali

kadrlar yetishmasligi ko‘plab tashkilotlarda bu vositaning imkoniyatlaridan to‘liq foydalanilmayotganini ko‘rsatadi.

Xulosa:

Ushbu maqolada axborot xavfsizligini ta’minlashning zamonaviy usul va vositalari kompleks tarzda tahlil qilindi. Tadqiqot natijalariga ko‘ra, quyidagi asosiy xulosalarga kelindi:

1. Zamonaviy kriptografik vositalar (AES-256, RSA, ECC) ma’lumotlarning maxfiyligi va butunligini ta’minlashda yuqori samaradorlikka ega. Simmetrik shifrlash katta hajmdagi ma’lumotlar uchun tezkor, asimmetrik shifrlash esa kalitlarni xavfsiz almashishda ajralmas hisoblanadi.
2. Tarmoq xavfsizligida next-generation firewall (NGFW) hamda sun’iy intellektga asoslangan IDS/IPS tizimlari an’anaviy vositalarga nisbatan sezilarli afzalliklarga ega bo‘lib, zero-day hujumlarni aniqlashda 3,5 barobar samaraliroqdir.
3. Ko‘p faktorli autentifikatsiya (2FA, MFA) va biometrik usullar hisobni egallash xavfini 76% gacha kamaytiradi, biroq biometrik ma’lumotlarning himoyasiga alohida e’tibor qaratish zarur.
4. Sun’iy intellekt va mashinaviy o‘qitish asosidagi vositalar real vaqt rejimida anomaliyalarni aniqlab, kiberhujumlarni bashorat qilish imkonini beradi. Ammo ular yuqori hisoblash resurslari va malakali mutaxassislarni talab qiladi.
5. Bulutli muhitda ma’lumotlarni himoyalashda shifrlash, IAM va SIEM tizimlarining kompleks qo‘llanilishi hujumlarning 94% oldini oladi. SIEM tizimlari xavfsizlik hodisalarini aniqlash vaqtini (MTTD) 2,8 soatdan 12 daqiqagacha qisqartiradi.
6. Blokcheyn texnologiyasi ma’lumotlarning o‘zgartirilmasligini ta’minlashda juda samarali (99,9%), ammo past unumdorlik (2 sekunddan 10 minutgacha) uning real vaqt rejimidagi tizimlarda qo‘llanilishini cheklaydi.

Yakuniy xulosa shuki, axborot xavfsizligining maksimal darajasiga faqat kompleks yondashuv – kriptografiya, tarmoq himoyasi, autentifikatsiya, AI vositalari va blokcheynni birgalikda qo‘llash orqali erishish mumkin. Tashkilotlar o‘z resurslari, xavfsizlik talablari va foydalanish stsenariysiga mos vositalarni tanlab, ularni bosqichma-bosqich joriy qilishi tavsiya etiladi. Shu bilan birga, texnik vositalar qanchalik mukammal bo‘lmasin, foydalanuvchilarning raqamli savodxonligini oshirmasdan turib yuqori darajadagi xavfsizlikka erishib bo‘lmaydi. Kelgusida quantum kriptografiyasi, homomorf shifrlash va federated learning kabi yangi yo‘nalishlarda tadqiqotlarni davom ettirish dolzarb hisoblanadi.

Foydalanilgan adabiyotlar:

1. Shodi o‘g‘li, Rajaboyev Shahboz. "BUXGALTERIYADA AXBOROT TEXNOLOGIYALARINI QO'LLANILISHI." Лучшие интеллектуальные исследования 60.1 (2026): 84-91.
2. Shodi o‘g‘li, Rajaboyev Shahboz. "ONLINE ASSESSMENT SOFTWARE IN DISTANCE LEARNING: MY TEST AND ISPRING PROGRAMS AND THEIR APPLICATION." Лучшие интеллектуальные исследования 59.2 (2025): 299-304.
3. Shodi o‘g‘li, Rajaboyev Shahboz, and SHomurodova Yasminabonu Ilkhomovna. "AXBOROT-KOMMUNIKATSIYA XIZMATLARI SOHASIDAGI KORXONALAR RIVOJLANISHINI BOSHQARISH TIZIMI." Лучшие интеллектуальные исследования 58.6 (2025): 7-13.
4. Sh, Rajaboyev Sh, and J. I. Xabibulloyev. "KOMPYUT ER GRAFIKASI VA GRAFIK AMALLAR BILAN ISHLASHNING ZAMONAVIY AXBOROT TEXNOLOGIYALARIDAGI O ‘RNI." Экономика и социум 12-2 (139) (2025): 578-581.
5. Sh, Rajaboyev Sh. "KORXONALARDA AXBOROT-KOMMUNIKATSIYA TEXNOLOGIYALARI XIZMATLARI BUXGALTERIYA HISOBINING O‘ZIGA XOS XUSUSIYATLARI." Экономика и социум 12-2 (139) (2025): 558-564.

6. Sh, Rajaboyev Sh, and H. E. Xolmamatova. "AXBOROT-KOMMUNIKATSIYA SOHASIDA INNOVATSION XIZMATLARNI JORIY ETISHNING IQTISODIY SAMARASI." Экономика и социум 12-2 (139) (2025): 571-577.

7. Sh, Rajaboyev Sh, and H. E. Xolmamatova. "RAQAMLI IQTISODIYOTDA AXBOROT KOMMUNIKATSIYA XIZMATLARINING O‘RNI VA AHAMIYATI." Экономика и социум 4-1 (131) (2025): 449-453.

8. Farxodovich, Boronov Bobur, and Rajaboyev Shahboz Shodi o‘g‘li. "MECHANISMS FOR USING INFORMATION AND COMMUNICATION TECHNOLOGY SERVICES IN THE ELECTRONIC GOVERNMENT SYSTEM OF UZBEKISTAN AND THEIR EFFECTIVENESS." Лучшие интеллектуальные исследования 59.2 (2025): 285-292.

9. Farxodovich, Boronov Bobur. "STAGES OF DEVELOPMENT OF THE INFORMATION AND COMMUNICATION TECHNOLOGY SERVICES SYSTEM." Лучшие интеллектуальные исследования 59.2 (2025): 293-298.

10. Farxodovich, Boronov Bobur, Xudaynazarova Dilnoza Gafurovna, and Yodgorov Xushvaqt Mansurovich. "FARMASEVTIKA KORXONALARIDA BUXGALTERIYA HISOBINING O ‘ZIGA XOS XUSUSIYATLARI." FRONTIERS OF KNOWLEDGE AND INTERDISCIPLINARY DISCOVERY 1.1 (2025): 282-289.

11. Боронов, Бобур, and Заррух Мухаммадиев. "ПУТИ РАСШИРЕНИЯ ИНФОРМАЦИОННОГО ОБЪЕМА УЧЕТА КАПИТАЛЬНЫХ ВЛОЖЕНИЙ В ХОЗЯЙСТВУЮЩИЕ СУБЪЕКТЫ." Передовая экономика и педагогические технологии 2.2 (2025): 444-450.