

KORXONA AXBOROT TIZIMLARIDA MA'LUMOTLAR ZAXIRA NUSXALARINING XAVFSIZLIGINI TA'MINLASHDA TAHDIDLAR VA ULARGA QARSHI ZAMONAVIY YECHIMLAR

G'aniyeva Shaxrizod Nurmaxamadovna

*Farg'ona davlat texnika universiteti "Dasturiy injiniring va kiberxavfsizlik" kafedrası dotsent v.v.b.,
(PhD)*

shaxrizodganiyeva@gmail.com

Yo'Ichiboyeva Saxovatxon Jamolidin qizi

Farg'ona davlat texnika universiteti "Axborot xavfsizligi" yo'nalishi magistri

yolchiboyevasaxovatxon@gmail.com

Annotatsiya. Ushbu maqolada axborot tizimlarida zaxira jarayonining mohiyati, uning axborot xavfsizligini ta'minlashdagi o'rni hamda zamonaviy tahdidlar sharoitidagi ahamiyati yoritilgan. Tadqiqotda ma'lumotlar yo'qolishining oldini olish, ularni tiklash va tizim uzluksizligini ta'minlashga qaratilgan zaxira nusxalash tizimlarining asosiy funksiyalari tahlil qilingan. Shuningdek, ransomware, ichki tahdidlar, fizik nosozliklar va tarmoq hujumlari kabi asosiy xavf omillari ko'rib chiqilib, ularning zaxira nusxalash tizimlariga ta'siri baholangan. Maqolada 3-2-1 qoidasiga asoslangan saqlash modeli, doimiy zaxira nusxalash, shifrlash va zero trust yondashuvi kabi zamonaviy himoya usullari ham tahlil qilingan. Natijada, zaxira nusxalash tizimlarining samaradorligini oshirish va axborot xavfsizligini mustahkamlash uchun kompleks yondashuv zarurligi asoslab berilgan.

Kalit so'zlar: zaxira nusxalash, zaxira nusxa, kiberxavfsizlik, ransomware, cloud storage, disaster recovery, ma'lumotlar himoyasi

Kirish. Hozirgi raqamli transformatsiya sharoitida korxona axborot tizimlari tashkilot faoliyatining ajralmas qismi sifatida muhim ahamiyat kasb etmoqda. Ushbu tizimlarda saqlanayotgan ma'lumotlar strategik resurs bo'lib, ularning yo'qolishi yoki buzilishi korxona faoliyatiga jiddiy salbiy ta'sir ko'rsatishi mumkin. Shu sababli ma'lumotlarni ishonchli saqlash va ularning uzluksizligini ta'minlash dolzarb masalalardan biri hisoblanadi.

Zaxira nusxalash texnologiyalari ma'lumotlarni himoya qilishning asosiy vositalaridan biri bo'lib, ular turli nosozliklar va kiberxavflar sharoitida ma'lumotlarni tiklash imkonini beradi. Biroq so'nggi yillarda ransomware hujumlari, ichki tahdidlar, bulutli texnologiyalardagi zaifliklar kabi omillar zaxira nusxalash tizimlarining o'zini ham xavf ostiga qo'yimoqda. Shu nuqtai nazardan, zaxira nusxalarining xavfsizligini ta'minlash, mavjud tahdidlarni tahlil qilish va samarali zamonaviy yechimlarni ishlab chiqish ilmiy va amaliy jihatdan muhim hisoblanadi.

Zaxira nusxalash – bu axborot tizimlarida mavjud ma'lumotlarning ishonchli nusxalarini yaratish va ularni asosiy tizimdan mustaqil, alohida saqlash muhitlarida joylashtirish jarayonidir. Mazkur jarayon axborot xavfsizligini ta'minlashning muhim tarkibiy qismi hisoblanib, ma'lumotlarning yaxlitligi, mavjudligi va tiklanish imkoniyatini kafolatlashga xizmat qiladi. Zaxira nusxalashning asosiy funksional vazifalari quyidagilardan iborat: birinchidan, turli texnik nosozliklar, inson omili yoki dasturiy xatoliklar natijasida yuzaga kelishi mumkin bo'lgan ma'lumotlar yo'qolishining oldini olish; ikkinchidan, favqulodda holatlar, jumladan, tizim ishdan chiqishi yoki kiberhujumlar sodir bo'lgan vaziyatlarda ma'lumotlarni tezkor va to'liq tiklash imkonini yaratish; uchinchidan, axborot tizimlarining uzluksiz ishlashini ta'minlash orqali ularning barqarorligini oshirish; to'rtinchidan esa, kiberxavfsizlik hodisalari, xususan zararli dasturlar ta'siridan keyin tizimni dastlabki holatga qaytarish imkoniyatini ta'minlashdir. Shu jihatdan, zaxira nusxalash nafaqat texnik jarayon, balki korxona axborot infratuzilmasining

uzluksizligi va xavfsizligini ta'minlovchi strategik mexanizm sifatida ham muhim ahamiyat kasb etadi.

1- Zaxira nusxalash tizimlariga tahdidlar

№	Tahdid turi	Tavsifi
1	Ransomware	Zaxira fayllarni shifrlab qo'yadi
2	Ichki tahdid	Xodimlar tomonidan buzilish
3	Fizik nosozlik	Disk yoki server ishdan chiqishi
4	Noto'g'ri konfiguratsiya	Zaxira nusxalash noto'g'ri sozlanishi
5	Tarmoq hujumlari	Zaxira nusxalash serverga kirish hujumlari
6	Ma'lumot buzilishi	Fayllarning shikastlanishi

1-jadvalda korxona axborot tizimlarida ma'lumotlarning zaxira nusxalariga tahdid soluvchi asosiy xavf turlari va ularning qisqacha tavsifi berilgan. Ushbu tahdidlar zaxira nusxalash tizimlarining ishonchliligi va samaradorligiga bevosita ta'sir ko'rsatadi.

Birinci tahdid turi - ransomware bo'lib, u zararli dasturlar orqali zaxira fayllarni shifrlab qo'yadi va ularni tiklashni imkonsiz holatga keltiradi. Bunday hujumlar ko'pincha moliyaviy talablar bilan birga keladi va tashkilot faoliyatiga jiddiy zarar yetkazadi. Ikkinchi tahdid - ichki tahdid (insider threat) bo'lib, u tashkilot xodimlari tomonidan qasddan yoki bilmasdan sodir etiladigan xatolar natijasida yuzaga keladi. Bu holat ma'lumotlarning o'chirilishi, o'zgartirilishi yoki oshkor bo'lishiga olib kelishi mumkin. Uchinchi tahdid fizik nosozliklar bilan bog'liq bo'lib, unda serverlar, qattiq disklar yoki boshqa saqlash qurilmalari ishdan chiqishi natijasida zaxira ma'lumotlarga zarar yetadi. To'rtinchi tahdid noto'g'ri konfiguratsiya hisoblanadi, bunda zaxira nusxalash tizimining noto'g'ri sozlanishi sababli ma'lumotlar to'liq yoki muntazam ravishda saqlanmasligi mumkin. Bu esa zarur paytda ma'lumotlarni tiklash imkoniyatini cheklaydi. Beshinchi tahdid tarmoq hujumlari bilan bog'liq bo'lib, bunda hujumchilar zaxira nusxalash serverlarga noqonuniy kirish orqali ma'lumotlarni o'chirishi yoki o'zgartirishi mumkin. Oltinchi tahdid esa ma'lumot buzilishi (data corruption) bo'lib, unda fayllar turli sabablarga ko'ra shikastlanadi va ularni to'liq tiklash imkoni kamayadi.

Zamonaviy tahdidlarning tahlili

Ransomware hujumlari zamonaviy kiberxavfsizlikdagi eng xavfli tahdidlardan biri hisoblanadi. Bunday dasturlar foydalanuvchi yoki tashkilotning muhim ma'lumotlarini shifrlab, ularga kirishni bloklab qo'yadi. Hozirgi ransomware turlari faqat asosiy fayllarni emas, balki zaxira nusxalash tizimlarini ham nishonga oladi. Bu esa ma'lumotlarni tiklash jarayonini ancha murakkablashtiradi. Ko'pincha hujumchilar ma'lumotni qaytarish uchun to'lov talab qiladi. Biroq to'lov amalga oshirilsa ham, ma'lumotlar har doim ham qaytarilmasligi mumkin. Shu sababli tashkilotlar preventiv himoya choralariga katta e'tibor qaratadi.

Bulut xavfsizligi muammolari ham zamonaviy IT tizimlarida jiddiy xavf tug'diradi. Bulutli zaxira nusxalash tizimlarida noto'g'ri sozlamalar ma'lumotlarning ochiq qolishiga olib kelishi mumkin. Ba'zan foydalanuvchilar kirish huquqlarini to'g'ri boshqarmaydi, bu esa ma'lumot sizib chiqish xavfini oshiradi. Bundan tashqari, bulut xizmatlarida autentifikatsiya zaif bo'lsa, tashqi hujumchilar tizimga kirishi mumkin. Shuning uchun cloud tizimlarda shifrlash va ko'p bosqichli autentifikatsiya muhim hisoblanadi.

Ichki tahdidlar ham axborot xavfsizligida katta muammo hisoblanadi. Xodimlarning xatolari ba'zan katta ma'lumot yo'qotilishiga sabab bo'ladi. Ayrim hollarda esa xodimlar qasddan zarar yetkazishi mumkin. Bunday holatlar tashkilot ichida nazorat tizimi kuchli bo'lishini talab

qiladi. Ruksatlarni cheklash va monitoring tizimlari ichki tahdidlarni kamaytiradi. Shuningdek, xodimlarni muntazam o'qitish ham muhim rol o'ynaydi. Umuman olganda, ransomware, bulut xavfsizligi va ichki tahdidlar bir-biri bilan bog'liq kompleks xavf sifatida qaraladi.

Zamonaviy yechimlar va texnologiyalar

1. 3-2-1 qoidasi - ma'lumotlarni ishonchli saqlash uchun eng oddiy va samarali yondashuvlardan biridir. Unda 3 ta nusxa yaratiladi, 2 xil saqlash muhiti ishlatiladi va 1 ta nusxa albatta offline (internetdan uzilgan) holatda saqlanadi.
2. O'zgarish zaxira nusxalash - bu o'zgartirib yoki o'chirib bo'lmaydigan zaxira nusxa hisoblanadi. U ransomware hujumlariga qarshi eng samarali himoya usullaridan biri sifatida qo'llaniladi.
3. Shifrlash (Encryption) - fayllarni tashqi kirishlardan himoya qilish uchun ishlatiladi. Unda AES va RSA kabi kuchli kriptografik algoritmlar qo'llanilib, ma'lumot xavfsizligi ta'minlanadi.
4. Zero Trust (Hech kimga ishonma)yondashuvi - har bir kirish so'rovi doimiy ravishda tekshirib boriladi. Zaxira nusxalash tizimlariga faqat zarur va cheklangan ruksatlar asosida kirish imkoniyati beriladi.
5. AI asosidagi monitoring - tizimlari xavfsizlik tahdidlarini oldindan aniqlashga yordam beradi. Ular tizimdagi anomaliyalarni kuzatib, shubhali harakatlarni tezda aniqlaydi.

2-jadval.

Himoya usullarining qiyosiy jihatlari

Usul	Afzalligi	Kamchiligi
3-2-1 Zaxira nusxalash	Ishonchli	Ko'p resurs talab qiladi
Cloud Zaxira nusxalash	Moslashuvchan	Internetga bog'liq
Immutable Zaxira nusxalash	Juda xavfsiz	Qimmat
Encryption	Maxfiylik	Hisoblash resursi kerak
AI Monitoring	Tez aniqlash	Murakkab

Ma'lumotlarni himoya qilishda turli zamonaviy usullar qo'llaniladi. 3-2-1 qoidasi asosida 3 ta nusxa yaratiladi va ular 2 xil saqlash muhitida joylashtiriladi. Bu usulda 1 ta nusxa albatta offline holatda saqlanib, tashqi hujumlardan himoya qilinadi. Immutable zaxira nusxalash esa o'zgartirib yoki o'chirib bo'lmaydigan zaxira nusxa bo'lib, ransomware hujumlariga qarshi kuchli himoya beradi. Bu usul ma'lumotni tiklash imkoniyatini yuqori darajada saqlab qoladi.

Natijalar. Tadqiqot natijalari shuni ko'rsatdiki, korxona axborot tizimlarida zaxira nusxalash jarayonlari ko'plab xavflarga duch keladi va bu xavflar tizim ishonchliligiga sezilarli darajada ta'sir ko'rsatadi. Xususan, ransomware hujumlari zaxira nusxalarni ham shifrlash orqali ularni tiklash imkoniyatini cheklashi aniqlandi. Bundan tashqari, ichki tahdidlar, noto'g'ri konfiguratsiya va fizik nosozliklar ham ma'lumotlar xavfsizligiga jiddiy xavf tug'diradi.

Tahlillar natijasida zamonaviy himoya usullarining samaradorligi baholandi. Jumladan, 3-2-1 qoidasi ma'lumotlarni turli muhitlarda saqlash orqali xavfsizlikni oshirishi, immutable zaxira nusxalash texnologiyasi esa zaxira nusxalarni o'zgartirishdan himoya qilishi aniqlandi. Shuningdek, shifrlash texnologiyalari ma'lumot maxfiyligini ta'minlashda muhim rol o'ynashi, Zero Trust yondashuvi esa tizimga kirishni qat'iy nazorat qilish imkonini berishi isbotlandi. AI asosidagi monitoring tizimlari esa tahdidlarni erta bosqichda aniqlash orqali xavfsizlikni sezilarli darajada oshiradi.

Xulosa. Korxona axborot tizimlarida ma'lumotlar zaxira nusxalarining xavfsizligini ta'minlash bugungi kunda muhim ilmiy va amaliy muammolardan biri hisoblanadi. Tadqiqotlar shuni ko'rsatadiki, zaxira nusxalash tizimlari mavjud bo'lishi bilan birga, ularning himoyalanganligi ham yuqori darajada ta'minlanishi zarur. Zamonaviy tahdidlar, xususan ransomware, ichki xavflar va tarmoq hujumlari zaxira tizimlarining zaif tomonlarini ochib bermoqda. Shu sababli, ma'lumotlarni himoya qilishda kompleks yondashuvni qo'llash muhim ahamiyatga ega. 3-2-1 qoidasi, immutable zaxira nusxalash, shifrlash, Zero Trust va sun'iy intellekt asosidagi monitoring kabi texnologiyalarni birgalikda qo'llash orqali yuqori darajadagi xavfsizlikni ta'minlash mumkin. Kelgusida zaxira nusxalash tizimlarini yanada takomillashtirish, ularni avtomatlashtirish va intellektual boshqaruv tizimlari bilan integratsiya qilish orqali ma'lumotlar xavfsizligini yangi bosqichga olib chiqish mumkin.

Foydalanilgan adabiyotlar:

1. National Institute of Standards and Technology. *Contingency Planning Guide for Federal Information Systems (SP 800-34 Rev. 1, yangilangan tavsiyalar bilan)*, 2022.
2. ISO. *ISO/IEC 27001:2022 – Information Security Management Systems Requirements*, 2022.
3. ISO. *ISO/IEC 27002:2022 – Information Security Controls*, 2022.
4. ENISA. *ENISA Threat Landscape Report*, 2023.
5. IBM. *Cost of a Data Breach Report*, 2023.
6. Veritas Technologies. *Data Protection Trends Report*, 2023.
7. Veeam Software. *Data Protection Trends Report*, 2024.
8. Acronis. *Cyberthreats Report*, 2024.
9. Kaspersky. *IT Threat Evolution Report*, 2023.
10. Bruce Schneier. *Cybersecurity and Data Protection (zamonaviy maqolalar to'plami)*, 2022–2024.