

TOG'-KON SANOATIDA AXBOROT XAVFSIZLIGINI TA'MINLASHNING ZAMONAVIY USULLARI VA VOSITALARI

Xaydaraliyev Elbek Farxod o'g'li

“Olmaliq KMK” AJ xodimi

Annotatsiya

Hozirgi zamonaviy raqamlashtirish davrida insoniyat hayotining deyarli barcha yo'nalishlarida, jumladan, tog'-kon sanoatida ham raqamli texnologiyalardan foydalanish misli ko'rilmagan tezlik bilan rivojlanmoqda. Shu jihatdan qaralganda, raqamli tog'-kon sanoatida axborot xavfsizligini ta'minlash va ishlab chiqarish jarayonlarida to'planadigan ma'lumotlarni himoyalash dolzarb masalaga aylangan. Maqolada sun'iy intellekt texnologiyalarini qo'llash, kon ishlari bo'yicha ma'lumotlarni to'plash va qayta ishlash, har bir jarayonni tahlil qilish, kerakli aniq va ishonchli ma'lumotlarni yig'ish hamda ularga ta'sir etuvchi omillar yoritiladi. Bundan tashqari, xalqaro tajribalar asosida tog'-kon sanoatida zamonaviy axborot xavfsizligi yechimlarini qo'llashga oid xulosa va takliflar beriladi.

Kalit so'zlar: raqamli tog'-kon sanoati, axborot xavfsizligi, kiberxavfsizlik, shaxta boshqaruvi, geologik ma'lumotlar, sun'iy intellekt.

KIRISH

Raqamli tog'-kon sanoatini rivojlantirishning asosiy omillaridan biri bu axborot xavfsizligini ta'minlashdir. Texnologiyalar asrida konchilik jarayonlari tobora avtomatlashtirilmoqda: shaxta boshqaruvi, burg'ilash ishlari, rudani tashish, geologik ma'lumotlarni yig'ish va tahlil qilish – barchasi raqamli tizimlar orqali boshqarilmoqda. Shu bilan birga, bu tizimlar kiberxavfsizlik tahdidlariga ham ochiq bo'lib qolmoqda.

Bugungi kunda dunyo bo'ylab yirik kon kompaniyalari – Rio Tinto, BHP Billiton, Norilsk Nickel – axborot xavfsizligini ishlab chiqarish xavfsizligi bilan

teng darajada muhim deb hisoblaydi. Chunki shaxta boshqaruv tizimlariga yoki geologik ma'lumotlar bazasiga noqonuniy kirish katta iqtisodiy zarar va ishlab chiqarish jarayonining to'xtashiga olib kelishi mumkin.

O'zbekistonda ham davlat siyosati darajasida raqamli tog'-kon sanoatining axborot xavfsizligini oshirishga alohida e'tibor qaratilmoqda. "Raqamli O'zbekiston – 2030" strategiyasida konchilikda kiberxavfsizlikka oid milliy strategiya ishlab chiqish va kon ishlab chiqarishning muhim infratuzilmasini himoya qilish bo'yicha aniq vazifalar belgilangan.

ADABIYOTLAR TAHLILI. Kiberxavfsizlik – bu kompyuterlar, serverlar, mobil qurilmalar, elektron tizimlar, tarmoqlar va ma'lumotlarni zararli hujumlardan himoya qilish amaliyoti bo'lib, tog'-kon sanoatida bu tushuncha ishlab chiqarishning barcha raqamli elementlariga taalluqlidir. Konchilikdagi axborot xavfsizligi quyidagi yo'nalishlarni qamrab oladi:

- Tarmoq xavfsizligi – shaxta boshqaruv tizimlari va ishlab chiqarish tarmoqlarini zararli dasturlar yoki ruxsatsiz kirishdan himoya qilish.
- Dastur xavfsizligi – konchilikda qo'llaniladigan maxsus dasturiy ta'minot va SCADA tizimlarining zaifliklarini bartaraf etish.
- Operatsion xavfsizlik – geologik ma'lumotlar, ishlab chiqarish ko'rsatkichlari va texnologik jarayonlar bo'yicha axborotni boshqarish va himoya qilish.

Xalqaro tajriba shuni ko'rsatadiki, yirik kon kompaniyalarida axborot xavfsizligi siyosati faqat IT bo'limi darajasida emas, balki ishlab chiqarish boshqaruvi strategiyasining ajralmas qismi sifatida yuritiladi. BHP Billiton kompaniyasi tajribasida kiberhujumlar konveyer tizimlarini to'xtatib qo'ygan holatlar qayd etilgan, shuning uchun ular avtomatlashtirilgan xavfsizlik monitoringi va real vaqt rejimida tarmoq nazoratini joriy etgan.

METODOLOGIYA. Tadqiqot quyidagi metodlarga asoslandi:

1. Huquqiy hujjatlar tahlili – tog‘-kon sanoatida axborot xavfsizligini tartibga soluvchi milliy qonunchilik va xalqaro standartlar (ISO/IEC 27001, NIST Cybersecurity Framework) o‘rganildi.
2. Statistik tahlil – kiberxavfsizlik markazlari, xalqaro tashkilotlar (ITU, ICOMM) va yirik kon kompaniyalarining axborot xavfsizligi bo‘yicha hisobotlari tahlil qilindi.
3. Amaliy tajriba o‘rganish – Olmaliq kon-metallurgiya kombinati (OKMK), Navoiy kon-metallurgiya kombinati (NKMK) va boshqa yirik korxonalar faoliyatida axborot xavfsizligi bo‘yicha qo‘llanilayotgan texnologiyalar o‘rganildi.
4. Tizim xavfsizlik sinovlari – tog‘-kon ishlab chiqarishida ishlatiladigan avtomatlashtirilgan boshqaruv tizimlari (SCADA, DCS)ning kiberxavfsizlik darajasi tahlil qilindi.

NATIJALAR VA ULARNING TAHLILI

1. Muhim ishlab chiqarish infratuzilmasini himoyalash

SCADA va OT tarmoqlarini kiberxavfsizlik talablariga muvofiq himoya qilish, autentifikatsiya va ruxsat darajalarini qat’iy cheklash zarur.

Misol: Rio Tinto avtonom kon uskunalari himoya qilish uchun yopiq sanoat tarmoqlarini yaratgan.

2. Geologik va ishlab chiqarish ma’lumotlarini himoyalash

Geologik xaritalar, zaxira ma’lumotlari shifrlangan formatda saqlanishi va zaxira nusxalari offlayn bo‘lishi kerak.

Misol: Barrick Gold barcha ma’lumotlarni shifrlangan serverlarda saqlaydi.

3. Real vaqt rejimida xavfsizlik monitoringi

SOC va IDS/IPS tizimlarini joriy etish orqali tarmoq trafikini uzluksiz nazorat qilish.

Misol: Norilsk Nickel ishlab chiqarish obyektlarini real vaqt rejimida kuzatish tizimiga ega.

4. Kiberxavfsizlik bo‘yicha xodimlarni o‘qitish

OT security bo'yicha maxsus treninglar o'tkazish, fishing testlarini amalga oshirish.

5. Kiberhujumlar statistikasi (O'zbekiston, 2022)

45% – zararli dasturlar orqali kirish urinishlari.

30% – SCADA tizimlariga ruxsatsiz kirish.

15% – fishing va soxta domenlar.

10% – ichki xodimlar tomonidan xavfsizlik buzilishi.

XULOSA

Raqamli tog'-kon sanoatida axborot xavfsizligi ishlab chiqarishning uzluksizligi va xavfsizligini ta'minlaydi. Kiberhujumlarning oldini olish, infratuzilmani himoyalash va xodimlar malakasini oshirish sohadagi eng muhim vazifalar hisoblanadi. O'zbekiston tog'-kon sanoati uchun xalqaro standartlar asosida kompleks kiberxavfsizlik tizimini yaratish strategik ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR:

1. PQ-6079-sonli qaror, "Raqamli O'zbekiston – 2030 strategiyasi", 2020.
2. O'zbekiston Respublikasi Vazirlar Mahkamasi, "Axborot xavfsizligini ta'minlash tizimini takomillashtirish chora-tadbirlari to'g'risida", 2021.
3. ISO/IEC 27001:2022 – Information Security Management Systems.
4. NIST Cybersecurity Framework, 2021.
5. ICMC – Enhancing Mining Safety through Cybersecurity, 2020.
6. PwC – Mine 2022: A critical transition, 2022.
7. McKinsey & Company – The Future of Mining: Cybersecurity in the Digital Era, 2021.
8. Barrick Gold Corporation – Information Security and Risk Management Policy, 2022.
9. Rio Tinto – Cybersecurity in Autonomous Mining Systems, 2021.
10. Norilsk Nickel – OT Security Practices in Mining, 2022.
11. ISSUES OF UZBEKISTAN'S ACCESSION TO WTO AND ENHANCING INTERNATIONAL TRADE. Nuriddin R. Odinayev
<https://webgoldenbrain.com/index.php/gb/article/view/451>