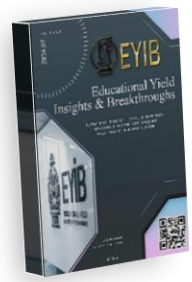
EYIB
EDUCATIONAL YIELD INSIGHTS & BREAKTHROUGHS
TA'LIMGA OID TUSHUNCHALAR VA YUTUQLAR
ISSN:3060-4648
Vol.1 №2
https://eyib.uz



ELEKTRON HUKUMAT TIZIMIDAGI AXBOROT XAVFSIZLIGI XABARLARINI TAHLILI VA VIZUALIZATSIYASI

[1] **Haydarov E.D.**
[2] **Gafurov Sh.R.**

[1] Muhammad al-Xorazmiy nomidagi TATU Axborot xavfsizligi kafedrasi mudiri, PhD
[2] Muhammad al-Xorazmiy nomidagi TATU mustaqil izlanuvchisi

Annotatsiya

Ushbu maqolada elektron hukumat tizimida axborot xavfsizligini monitoring qilish, xabarlarni tahlil qilish hamda tahlil natijalari asosida xabarlarni vizialuzatsiya qilish bo‘yicha taklif berilgan.

Kalit so‘zlar: elektron hukumat, filtrlash, yaxlitlik, tahlil, vizialuzatsiya, xavfsizlik monitoringi.

Odatda elektron hukumat tizimida axborot xavfsizligi monitoringini amalga oshiruvchi tizim arxitekturasidagi birinchi moduli imkon qadar ko‘proq axborot xavfsizligi xabarlarini yaratish uchun tuzilgan bo‘lishi kerak bo‘ladi. Ushbu real vaqtda elektron hukumat tizimidagi ma’lumot ikkinchi modulga yuborilishi yoki bir xil tamoyil asosida ishlaydigan ikkinchi modul tomonidan keyinchalik yig‘ish uchun mahalliy ma’lumot sifatida saqlanishi mumkin. Shu bilan birga, axborot xavfsizligi xabarlarini birlashtirish va korrelyatsiya qilish jarayonida keraksiz va takroriy ma’lumotlar olib tashlanadi. Biroq, axborot xavfsizligi xabarlari qanchalik ko‘p ishlab chiqilsa, birinchi moduldan ko‘proq ishlash talab qilinadi. Shunday qilib, ishlash cheklovlarini oldini olish uchun axborot xavfsizligi xabarlarini oldindan filtrlash eng yaxshi yondashuv hisoblanadi. Shuning uchun ham biinchi modulda filtrlash ikki usulda amalga oshirilishi mumkin:

- tuzilmaviy spetsifikatsiya - bu holda ba’zi axborot xavfsizligi xabarlari yaratilmaydi, chunki ular himoyalangan tizimda mavjud bo‘lmagan komponentlarga tegishli axborot hisobland;
- axborot xavfsizligi xabarlarining dastlabki filtrlari - bu filtrlar axborot xavfsizligi xabarlarini yaratishni blokirovka qilish uchun o‘rnatiladi, chunki texnik xavfsizlik qoidalariga rioya qilishni qat’iy talab etadi.

Elektron hukumat tizimidan axborot xavfsizligini ta’minlashda foydalaniladigan paketlarni filtrlash vositalari birinchi modulning bo‘sh resurslarini

sezilarli darajada oshiradi, ammo ularning ikkita asosiy kamchiliklari bor. Birinchisi, taqsimlangan filtrlarni boshqarishning murakkabligi. Har bir filtr aynan kerakli sozlanmalarni o‘z ichiga olishini ta’minlash uchun o‘zgartirishlar kiritishning aniq tartiblari bo‘lishi kerak. Bundan tashqari, oldindan filtrlashning aksariyati dastur darajasida o‘rnatilgan bo‘lib, ular turli xil konfiguratsiya fayllarini ishlatishi mumkin. Bu esa boshqaruvning murakkabligini sezilarli darajada oshiradi. Ikkinchisi, filtr qo‘llaniladigan tizim haqida bilim miqdorini kamaytirishdir. Natijada statistik ma’lumotlar ancha axborot xavfsizligi hodisasini tahlil qilishni qiyinlashtiradi [1].Axborot xavfsizligi monitoringi tizimida analitik ma’lumotlarni qayta ishlash bilan bog‘liq asosiy operatsiyalar axborot xavfsizligi xabarlarining korrelyatsiyasi, tizimli tahlil, hujumning tarqalish yo‘lini tahlil qilish va shu turdagi xatti-harakatlar tahlilidir. Axborot xavfsizligi xabarlarining korrelyatsiyasi - bu turli xil axborot xavfsizligi xabarlari o‘rtasidagi statistik munosabatlarni izlash jarayoni bo‘lib, undan so‘ng amalga oshiriladigan barcha keyingi tahlillarni amalga oshirish mumkin bo‘lgan kontekstlarni yaratishga olib keladi. Tahlil kontekstlarning hujum xususiyatlariga mos kelishini tekshirish orqali amalga oshiriladi.

Elektron hukumat tizimidagi axborot xavfsizligi xabarlarini vizualizatsiya qilishda foydalanuvchi interfeyslarining ikki turi mavjud: axborot xavfsizligi monitoringi tizimining boshqaruv konsoli va foydalanuvchi portali. Axborot xavfsizligi monitoringi tizimining boshqaruv konsoli axborot xavfsizligi hodisalarini tahlil qilishda yordam berish uchun ishlatiladi va elektron hukumat tizimining turli qismlaridan ma’lumotlarni birlashtiradi. Bu jarayon bilan parallel ravishda boshqaruv konsoli quyidagi interfeyslarni birlashtiradi:

- real vaqt rejimida axborot xavfsizligi xabarlarini monitoring qilish. Ushbu interfeys axborot xavfsizligi xabarlarini qidirish va saralash maqsadida filtrlash uchun asosiy funksiyalarni amalga oshirish imkonini beradi.
- axborot xavfsizligi hodisalarini qayta ishlash - axborot xavfsizligi hodisalari tarixini va ularga javob berish tartiblarini yaratish va keyinchalik yuritish uchun foydalaniladi.
- statistik tahlil - qisqa, o‘rta va uzoq vaqt oralig‘ida axborot xavfsizligi ma’lumotlarini analitik qayta ishlash natijalarini ta’minlaydi. Bu interfeys axborotni grafik ko‘rinishida (grafiklar, diagrammalar va boshqalar ko‘rinishida) ifodalaydi[2].

Vizualizatsiya jarayonida foydalanuvchi portali quyidagi interfeyslarni o‘z ichiga oladi:

- axborot xavfsizligi buzilishi xavfini baholash;
- axborot xavfsizligi hodisalari - hujumlar turlari, ularning chastotasi, manbalari va himoyalangan tizimlardagi oqibatlari to‘g‘risida o‘rta yoki uzoq vaqt davomida hisobot berish;
- tizim holati - bu interfeys oxirgi foydalanuvchiga joriy axborot xavfsizligi hodisalari, hujumlarga moyil bo‘lgan tizimlar va hujumchilar tomonidan ishlatiladigan hujumlar haqida real vaqt rejimida batafsil ma’lumot berish, shuningdek, hujumni kamaytirish uchun sodir bo‘lgan axborot xavfsizligi hodisasiga javob choralari va kuchayish tartiblari haqida ma’lumot berish.

Ma’lumotlarni tahlil qilish va vizualizatsiya qilish jarayonida axborot xavfsizligi xabarlari sonining ko‘payishi bilan axborot xavfsizligi monitoringi tizimining tarkibiy qismlariga qo‘yiladigan talablar soni sezilarli darajada oshadi,

chunki ma’lumotlar bazasi so‘rovlarini qayta ishlash uchun vaqt va resurslar talab qiladi. Zamonaviy hujumlar juda tez sodir bo‘lishi sababli, axborot xavfsizligi xabarlarini tez va o‘z vaqtida tahlil qilish va javob choralarini ko‘rishni talab etadi. Hozirda ma’lumotlarni qayta ishlash jarayonida axborot xavfsizligi xabarlarini tahlil qilish va vizualizatsiya qilish tezligi yaxshilanishi uchun axborot xavfsizligi xabarlarini saqlashning ko‘p bosqichli tizimini yaratish taklif etilmoqda [3].

Elektron hukumat tizimida ishlaydigan monitoring tizimlarida tizimning aniqligi va ishonchligini ta’minlaydigan asosiy nuqtda bu monitoring tizimi real vaqt davrida ishlaganligi sababli elektron hukumat tizimidagi ma’lumotlar oqimini nazorat qilishni anglatadi. Chunki elektron hukumat tizimidagi ma’lumotlar oqimida qanday o‘zgarishlar yoki buzilish sodir bo‘ladigan bo‘lsa bu holatni yuzaga kelishiga asosiy ikkita sabab mavjud bo‘ladi. Birinchi tizimdagi texnik xatolik, ikkinchisi esa tizim qaratilgan tarmoq hujumlarni amalga oshirilganligidir. Shundan kelib chiqqan holda elektron hukumat tizimida axborot xavfsizligi monitoringini amalga oshiruvchi tizimdalarda ma’lumotlar oqimida axborot xavfsizligini buzilishini aniqlashga qaratilgan usul va algoritmlarni ishlab chiqish zarur masala hisoblanadi.

Foydalanilgan adabiyotlar ro‘yxati

1. Alhitmi HK, Mardiah A, Al-Sulaiti KI, Abbas J (2024) Data security and privacy concerns of AI-driven marketing in the context of economics and business field: an exploration into possible solutions. Cogent Bus Manag 11(1).

2. Fayzullajon, B., Sharifjon, G., Sherzod, S. (2023). Methods for Assessing Information Security Incidents in the Enterprise and Making Decisions. In: Ranganathan, G., Fernando, X., Rocha, Á. (eds) Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems, vol 383. Springer, Singapore. https://doi.org/10.1007/978-981-19-4960-9_12.

3. Beckman L., Hultin Rosenberg J., Jebari K. Artificial intelligence and democratic legitimacy. The problem of publicity in public authority //AI & SOCIETY. – 2024. – Т. 39. – №. 3. – С. 975-984.