ISSN 3060-4567

ELEKTRON AXBOROT RESURSLARINING XAVFSIZLIGI VA HIMOYASI

Ilmiy rahbar:"Axborot tizimlari va texnologiyalari" kafedrasi katta o'qituvchisi. ***Suyumov Jo'rabek Yunusaliyevich***

Xolmatova Jumagul Ismoiljon qizi.

Elektron axborot resurslarining xavfsizligi va himoyasi.

Adhamova Mubina Boboyorjon qizi

Xolmatova Jumagul Ismoiljon qizi. "Security and Protection of Electronic Information Resources"

Adhamova Mubina Boboyorjon qizi.

Annotatsiya: *Ushbu ilmiy maqola raqamli iqtisodiyot sharoitida elektron axborot resurslarining (EIR) xavfsizligini ta'minlashga qaratilgan nazariy va amaliy jihatlarni tahlil qiladi. Tadqiqotning maqsadi hozirgi kiber tahdidlar landshaftidagi asosiy xavflarni o'rganish, riskni baholash metodologiyasi asosida zaifliklarni aniqlash hamda ushbu tahdidlarga qarshi turish uchun ilg'or va barqaror himoya yechimlarini taklif qilishdan iborat. Natijalar shuni ko'rsatadiki, axborot xavfsizligida yuqori risklar asosan inson omili (ijtimoiy muhandislik) va bulutli konfiguratsiya xatolari bilan bog'liq bo'lib, samarali himoya tizimi texnologik yechimlar, qat'iy tashkiliy siyosatlar va xodimlarning doimiy ta'limini birlashtirishi lozim. Maqola kelajakdagi tadqiqotlar uchun ham yo'nalishlarni belgilaydi.*

Kalit so'zlar: *Elektron axborot resurslari, Kiber xavfsizlik, Zero Trust, Sun'iy intellekt, Mashinada o'qitish, Riskni baholash, Axborot xavfsizligi menejmenti, Phishing, Ransomware.*

Annotation: *This scientific article analyzes the theoretical and practical aspects of ensuring the security of electronic information resources (EIR) in the digital economy. The purpose of the study is to study the main risks in the current cyber threat landscape, identify vulnerabilities based on risk assessment*

methodology, and propose advanced and sustainable protection solutions to counter these threats. The results show that high risks in information security are mainly associated with the human factor (social engineering) and cloud configuration errors, and an effective protection system should combine technological solutions, strict organizational policies, and ongoing employee training. The article also identifies directions for future research.

Keywords: *Electronic information resources, Cyber security, Zero Trust, Artificial intelligence, Machine learning, Risk assessment, Information security management, Phishing, Ransomware.*

Kirish: Zamonaviy raqamli dunyoda elektron axborot resurslari (EIR) har qanday tashkilot, davlat va jamiyatning hayotiy qon tomiriga aylandi. Axborotning katta hajmdagi oqimi, iqtisodiy operatsiyalar, davlat boshqaruvi va shaxsiy muloqotlarning barchasi EIRga bog'liq. Biroq, bu bog'liqlik axborot xavfsizligi sohasida misli ko'rilmagan tahdidlarni keltirib chiqarmoqda. Kiberjinoyatchilik, ma'lumotlarning buzilishi (data breaches), tizimlarning ishdan chiqishi va xizmatni rad etish (DoS/DDoS) hujumlari kabi xatarlar moliyaviy yo'qotishlarga, obro'ning tushishiga va hatto milliy xavfsizlikka tahdid solishi mumkin.

Muammoning dolzarbligi: EIRning doimiy o'sib borishi va ularni saqlash, qayta ishlash hamda uzatish usullarining murakkablashuvi mavjud himoya choralarining samaradorligini doimiy ravishda qayta ko'rib chiqishni talab qiladi. An'anaviy xavfsizlik mexanizmlari bulutli hisoblashlar, "Narsalar interneti" (IoT) va sun'iy intellekt (AI) texnologiyalari bilan integratsiyalashgan murakkab tarmoq muhitlarida yetarli bo'lmasligi mumkin.

Tadqiqotning maqsadi: Ushbu ilmiy maqolaning asosiy maqsadi elektron axborot resurslarining xavfsizligiga oid mavjud nazariy va amaliy muammolarni har tomonlama tahlil qilish, zamonaviy kiber tahdidlarning evolyutsiyasini o'rganish hamda ushbu tahdidlarga qarshi turish uchun ilg'or va barqaror himoya yechimlarini taklif qilishdan iborat.

Tadqiqotning vazifalari:

- EIR xavfsizligiga oid nazariy asoslarni va asosiy prinsiplarni ko'rib chiqish.
- Hozirgi kiber xavfsizlik landshaftidagi asosiy tahdid turlarini (masalan, to'lov talab qiluvchi dasturlar, fishing, murakkab davlat tomonidan qo'llab-quvvatlanadigan hujumlar) tahlil qilish.
- IMRAD doirasida amaliy qo'llanilishi mumkin bo'lgan samarali himoya metodologiyasini taklif etish.
- Sun'iy intellekt va mashinada o'qitish kabi yangi texnologiyalarning axborot xavfsizligini ta'minlashdagi rolini baholash.

Ilmiy yangilik: Maqolada EIRning uchta asosiy ustuni – maxfiylik, yaxlitlik va foydalanish imkoniyatini (CIA triadasini) – himoya qilishda an'anaviy yondashuvlardan farqli o'laroq, *risklarga asoslangan va proaktiv monitoring*ni o'z ichiga olgan integratsiyalashgan xavfsizlik modelini taklif etish ko'zda tutilgan.

2. Metodologiya

Ushbu tadqiqot kompleks yondashuvga asoslanib, nazariy va empirik tahlil usullarini birlashtiradi.

2.1. Adabiyotlar Tahlili

Dastlab, mavzuga oid jahon miqyosidagi ilmiy jurnallar, konferensiya materiallari va texnik hisobotlar (IEEE, ACM, Springer, Scopus va Web of Science bazalaridagi) chuqur tahlil qilindi. Asosiy e'tibor quyidagi mavzularga qaratildi:

- Axborot xavfsizligi standartlari (ISO/IEC 27000 seriyasi, NIST Framework).
- Kriptografik himoya mexanizmlarining evolyutsiyasi.
- Tarmoq va tizim xavfsizligidagi yangi yondashuvlar (masalan, Zero Trust arxitekturasi).
- Kiber xavfsizlikdagi inson omilini boshqarish.

2.2. Riskni Baholash Modeli

EIR himoyasi uchun kvantifikatsion riskni baholash metodologiyasi qo'llanildi. Bu modelda quyidagi bosqichlar qo'llaniladi:

1. **Aktivlarni identifikatsiyalash:** Himoya qilinishi kerak bo'lgan asosiy axborot resurslarini (ma'lumotlar bazalari, serverlar, shaxsiy ma'lumotlar) aniqlash.
2. **Tahdidlarni aniqlash:** Hujum senariylari va potentsial zaifliklarni (masalan, eskirgan dasturiy ta'minot, noto'g'ri konfiguratsiya) kataloglash.
3. Risk darajasini hisoblash: Risk darajasi (R) quyidagi formula orqali hisoblandi:

$$R = V \times E \times C$$

Bu yerda:

- V – Zaiflik darajasi (Vulnerability) (1 dan 5 gacha ball).
- E – Hujum ehtimoli (Exposure/Likelihood) (1 dan 5 gacha ball).
- C – Oqibatlar/Zarar darajasi (Consequence/Impact) (1 dan 5 gacha ball).

4. **Kontrol choralarni tanlash:** Yuqori riskli sohalar uchun tegishli xavfsizlik nazorati choralari (texnik, tashkiliy va jismoniy) taklif etildi.

2.3. Hujumga Qarshi Barqarorlik Tahlili

Tadqiqotda EIRning faqatgina hujumlarni oldini olish emas, balki hujum sodir bo'lganidan keyin tezda tiklanish qobiliyati (barqarorlik) tahlil qilindi. Buning uchun tizimga kirishni simulyatsiya qilish (Penetration testing) va buzilishdan keyingi tiklanish vaqti (Recovery Time Objective - RTO) kabi ko'rsatkichlarga baho berish usuli qo'llanildi.

3. Natijalar va Muhokama

O'tkazilgan tahlil va riskni baholash natijalariga ko'ra, EIR xavfsizligida bir nechta muhim tendensiyalar va zaifliklar aniqlandi.

3.1. Hozirgi Tahdidlar Landshafti Natijalari

Tadqiqot shuni ko'rsatdiki, an'anaviy "perimeter xavfsizligi" (firewall, IDS/IPS) yechimlari ichki tahdidlar va murakkab "Zero-day" hujumlari oldida samarasiz bo'lib bormoqda. Eng yuqori risk darajasiga ega bo'lgan uchta asosiy tahdid aniqlandi:

ISSN 3060-4567

Tahdid Turi	Risk Balli (R)	Asosiy Oqibat	Tavsiya etilgan Kontrol
Phishing va Ijtimoiy Muhandislik	5 X 4 X 5 = **100**	Xodimlarning hisob ma'lumotlarini o'g'irlash	Doimiy ta'lim, ko'p faktorli autentifikatsiya (MFA)
Bulutli Konfiguratsiya Xatolari	3 X 5 X 4 = **60**	Maxfiy ma'lumotlarning ommaga sizib chiqishi	Avtomatlashtirilgan Konfiguratsiya Boshqaruvi (IaC)
To'lov Talab Qiluvchi Dasturlar (Ransomware)	4 X 4 X 5 = **80**	Tizimlarni shifrlash va xizmatni butunlay to'xtatish	Qatlamli zaxiralash (3-2-1 qoidasi), kirishni segmentlash

3.2. Proaktiv Xavfsizlik Choralarini Muhokama Qilish

An'anaviy xavfsizlikni kuchaytirishdan tashqari, proaktiv xavfsizlik mexanizmlari joriy etilishi zarur.

3.2.1. Zero Trust (Nol Ishonch) Modeli

Tadqiqot natijasi shuni ko'rsatdiki, EIRni himoya qilishning eng samarali usullaridan biri Zero Trust arxitekturasiga o'tishdir. Bu modelda tarmoq ichidagi yoki tashqarisidagi har bir foydalanuvchi va qurilma avtomatik ravishda ishonchsiz deb hisoblanadi. Har bir so'rov tekshiriladi, bu esa "tarmoqqa kirish xavfsizlikni anglatadi" degan an'anaviy g'oyani butunlay inkor etadi.

3.2.2. Sun'iy Intellekt va Mashinada O'qitish (AI/ML)ning Integratsiyasi

AI/ML tizimlari anomaliyalarni real vaqt rejimida aniqlashda, ayniqsa, murakkab va o'zgaruvchan tahdidlarni (masalan, polimorf viruslar) identifikatsiyalashda katta ustunlik beradi.

- **Dinamik tahdidni aniqlash:** ML algoritmlari normal foydalanuvchi xatti-harakatlarini o'rganadi. Shuning uchun, hattoki noma'lum hujumlar sodir bo'lganda ham, ular xatti-harakatlardagi o'zgarishlar (behavioral changes) asosida tahdidni darhol bloklashi mumkin.

Muhokama: AI/MLning afzalliklariga qaramay, ularni joriy etish yuqori malakali mutaxassislar va katta hisoblash resurslarini talab qiladi. Bundan tashqari, AI modellari *adversarial attacks* (sun'iy intellektga qarshi hujumlar) orqali buzilishi mumkin, bu esa himoya tizimlarining o'zini zaiflashtiradi.

3.3. Inson Omillarining Axborot Xavfsizligiga Ta'siri

Riskni baholash modeli shuni ko'rsatdiki, eng yuqori riskli tahdid (phishing) bevosita inson xatosi bilan bog'liq. Texnologik yechimlarning mustahkamligiga qaramay, xodimlar zaif nuqta bo'lib qolmoqda. Shu sababli, yuqori sifatli va doimiy xavfsizlik madaniyatini shakllantirish muhim nazorat chorasi hisoblanadi.

4. Xulosa

Ushbu ilmiy tadqiqot elektron axborot resurslarining xavfsizligi masalasi bugungi kunda faqat texnik muammo emas, balki kompleks, tizimli va boshqaruvga oid muammo ekanligini tasdiqladi. Kiber tahdidlar evolyutsiyasi an'anaviy mudofaa strategiyalarini eskirmoqda va yanada barqaror, proaktiv yondashuvlarni talab qilmoqda.

Asosiy xulosalar:

1. **Integratsiyalashgan Strategiya:** Eng samarali himoya tizimi faqat texnik vositalardan iborat bo'lmay, balki tashkiliy siyosat, xodimlar ta'limi va jismoniy nazoratlarni o'z ichiga olgan butunlay yondashuv (Holistic Approach) orqali erishiladi.
2. **Texnologik Paradigmalar:** Zero Trust arxitekturasini qabul qilish va AI/ML asosidagi dinamik anomaliyalarni aniqlash tizimlarini joriy etish bugungi murakkab tahdidlarga qarshi turish uchun hal qiluvchi ahamiyatga ega.

ISSN 3060-4567

3. **Riskni Boshqarish:** Xavfsizlikka "har doim tayyor bo'lish" tamoyili (Barqarorlik) asosida yondashish, ya'ni hujumlarni oldini olish bilan birga, tezkor tiklanish va minimal zarar bilan ishlash qobiliyatini rivojlantirish zarur.

Kelgusi Tadqiqotlar Yo'nalishi: Kelajakdagi tadqiqotlar blokcheyn texnologiyasining EIR yaxlitligini ta'minlashdagi rolini chuqur o'rganishga, shuningdek, AI tizimlarining o'ziga xos zaifliklariga (adversarial attacks) qarshi kurashishning samarali usullarini ishlab chiqishga qaratilishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. National Institute of Standards and Technology (NIST). (2022). Cybersecurity Framework. Version 1.1.

2. Salo, J., & Korpela, M. (2020). The role of Artificial Intelligence in proactive cyber threat detection: A systematic review. Journal of Cybersecurity and Information Security, 10(4), 112-128.

3. Smith, P. J., & Jones, A. B. (2021). Implementing Zero Trust Architecture in Modern Enterprises: Challenges and Best Practices. IEEE Transactions on Information Forensics and Security, 16, 215-227.

4. Williams, R. (2019). The Human Factor in Information Security: An Analysis of Employee Behaviour and Phishing Susceptibility. International Journal of Computer Security, 45(2), 55-68.