# FOYDALANUVCHILARNING KIBER-XAVF DARAJASINI AI YORDAMIDA MONITORING QILISH VA XATTI-HARAKATGA ASOSLANGAN ADAPTIV O‘QITISH MODELI

**Erkinov Zafarjon Bobir o'g'li**

*Sharof Rashidov nomidagi Samarqand davlat universiteti*

zafar_erkinov@samdu.uz

**Annotatsiya**. Ushbu maqolada tashkilot xodimlarining kiber-xavf darajasini sun'iy intellekt (AI) yordamida uzluksiz monitoring qilish va ularning xatti-harakatlariga asoslangan adaptiv o‘qitish modeli ishlab chiqilgan. Model foydalanuvchilarning raqamli muhitdagi harakatlarini tahlil qilish orqali individual xavf profilini shakllantiradi va har bir xodimning zaif tomonlariga yo'naltirilgan avtomatlashtirilgan o'quv materiallarini taqdim etadi. Ushbu yondashuv inson omili bilan bog'liq kiber-hodisalarni kamaytirishda an'anaviy yillik treninglarga nisbatan yuqori samaradorlik ko'rsatadi.

**Kalit so‘zlar**: sun'iy intellekt, kiberxavfsizlik, xavfni monitoring qilish, xatti-harakatlar tahlili (UBA), adaptiv o'qitish, inson omili, kiber-gigiyena.

**Аннотация**. В данной статье разработана модель непрерывного мониторинга уровня киберриска сотрудников организации с использованием искусственного интеллекта (ИИ) и адаптивного обучения, основанного на их поведении. Модель формирует индивидуальный профиль риска путем анализа действий пользователей в цифровой среде и предоставляет автоматизированные обучающие материалы, нацеленные на слабые стороны каждого сотрудника. Данный подход демонстрирует более высокую эффективность в снижении киберинцидентов, связанных с человеческим фактором, по сравнению с традиционными ежегодными тренингами.

Ключевые слова: искусственный интеллект, кибербезопасность, мониторинг рисков, анализ поведения (UBA), адаптивное обучение, человеческий фактор, кибергигиена.

**Abstract**. This article develops a model for continuous monitoring of the cyber-risk level of organization employees using artificial intelligence (AI) and adaptive training based on their behavior. The model forms an individual risk profile by analyzing users' actions in the digital environment and provides automated training materials targeted at the specific weaknesses of each employee. This approach demonstrates higher effectiveness in reducing cyber incidents associated with the human factor compared to traditional annual training.

Keywords: artificial intelligence, cybersecurity, risk monitoring, user behavior analytics (UBA), adaptive learning, human factor, cyber hygiene.

Zamonaviy axborot xavfsizligi tizimlarida eng zaif halqa texnologiyalar emas, balki inson omili hisoblanadi. Turli xalqaro kiberxavfsizlik tashkilotlari (masalan, Verizon Data Breach Investigations Report) ma'lumotlariga ko'ra, ma'lumotlar sizib chiqishi holatlarining 74% dan ortig'i foydalanuvchilarning xatolari, ijtimoiy muhandislik yoki parollarni noto'g'ri boshqarish oqibatida yuzaga keladi. Shu sababli, xodimlarning kiber-gigiyena ko'nikmalarini oshirish dolzarb masala bo'lib qolmoqda. Biroq, bugungi kunda ko'plab tashkilotlarda qo'llaniladigan "hammaga bir xil" (one-size-fits-all) yondashuvidagi yillik kiberxavfsizlik treninglari kutilgan natijani bermayapti. Xodimlar nazariy ma'lumotlarni tez ununtadilar va kundalik ish jarayonida ularni qo'llamaydilar. Ushbu muammoni hal qilish uchun sun'iy intellekt (AI) va Foydalanuvchi xatti-harakatlari tahlili (User Behavior Analytics - UBA) texnologiyalarini birlashtirgan uzluksiz, adaptiv o'qitish modeliga o'tish zarurati tug'ildi.

AI YORDAMIDA KIBER-XAVFNI MONITORING QILISH

Tavsiya etilayotgan modelning asosi foydalanuvchilarning raqamli xatti-harakatlarini doimiy monitoring va tahlil qilishga asoslanadi. Mashinali o'qitish (Machine Learning) algoritmlari quyidagi ma'lumotlar nuqtalarini (data points) to'playdi va tahlil qiladi:

1. Elektron pochta bilan ishlash: Shubhali havolalarni bosish, noma'lum biriktirilgan fayllarni ochish, tashqi manzillarga nozik ma'lumotlarni yuborish.

2. Tizimga kirish (Autentifikatsiya): Noodatiy vaqtlarda yoki joylardan tizimga kirishga urinishlar, parollarni tez-tez noto'g'ri kiritish.
3. Veb-syorfing: Xavfli yoki ruxsat etilmagan veb-saytlarga tashrif buyurish, brauzerda ishonchsiz kengaytmalardan foydalanish.
4. Ma'lumotlar bilan ishlash: Katta hajmdagi ma'lumotlarni nusxalash, flesh-karta yoki bulutli xotiralardan ruxsatsiz foydalanish.

Sun'iy intellekt ushbu ma'lumotlar asosida har bir xodim uchun individual "Kiber-xavf indeksi"ni (Cyber Risk Score) 0 dan 100 gacha bo'lgan shkalada hisoblab chiqadi. Agar xodim xavfsizlik qoidalariga rioya qilsa, uning xavf indeksi pasayadi, aksincha xavfli harakatlar qilsa, indeks oshadi.

XATTI-HARAKATGA ASOSLANGAN ADAPTIV O‘QITISH MODELI BOSQICHLARI

AI tomonidan hisoblangan xavf profili asosida avtomatik ravishda adaptiv o'qitish jarayoni ishga tushadi. Bu model quyidagi bosqichlarda ishlaydi:

1-bosqich: Trigger (Qo'zg'atuvchi holat) va Diagnostika

AI tizimi xodimning xavfli harakatini qayd etadi (masalan, xodim ochiq Wi-Fi tarmog'iga VPNsiz ulandi). Tizim buni zaiflik sifatida baholaydi va xodimning profilidagi tegishli ko'rsatkichni o'zgartiradi.

2-bosqich: Shaxsiylashtirilgan Micro-learning (Mikro-o'qitish)

Tizim zudlik bilan ushbu xodimga aynan "Ochiq Wi-Fi tarmoqlari va VPN xavfsizligi" mavzusiga oid qisqa (2-3 daqiqalik) interaktiv o'quv materialini yuboradi. Boshqa xodimlar bu materialni olmaydi, chunki ular bunday xato qilmagan. Material video, qisqa test yoki infografika ko'rinishida bo'lishi mumkin.

3-bosqich: Amaliy tekshiruv (Simulyatsiya)

Xodim nazariy qismni o'zlashtirgach, tizim ma'lum vaqt o'tib (masalan, bir haftadan so'ng) aynan shu mavzuga oid sun'iy sinov (simulyatsiya) tashkil qiladi. Masalan, tizim soxta "Ochiq tarmoqqa ulanish" ssenariysini yaratib, xodimning reaksiyasini tekshiradi.

4-bosqich: Qayta aloqa va Profilni yangilash

Agar xodim simulyatsiyadan muvaffaqiyatli o'tsa, uning "Kiber-xavf indeksi" yaxshilanadi va tizim uni bezovta qilishni to'xtatadi. Agar u yana xato qilsa, tizim muammoning ildizini tushuntiruvchi chuqurroq treningni belgilaydi yoki xavfsizlik xizmatiga (CISO) xabar beradi.

MODELNING AFZALLIKLARI

1. Maqsadli yondashuv: Xodimlar faqat o'zlari bilmagan yoki xato qilgan mavzular bo'yichagina o'qitiladi. Bu ularning ish vaqtini tejaydi va zerikishning oldini oladi.
2. Tezkor reaksiya: Xato qilingan vaqtning o'zidayoq o'qitish orqali bilimlarni amaliyot bilan bog'lash samaradorligi keskin oshadi (Just-in-time training).
3. Byudjetni optimallashtirish: Barcha uchun umumiy uzoq muddatli va qimmat kurslar o'rniga, faqat yuqori xavf guruhidagi xodimlar bilan intensiv ishlash imkoniyati yaratiladi.
4. Madaniyatning o'zgarishi: Doimiy va adolatli monitoring xodimlarda raqamli muhitda ehtiyotkorlik (kiber-hushyorlik) madaniyatini tabiiy ravishda shakllantiradi.

**XULOSA.**

Inson xulq-atvori statik emas, shuning uchun kiberxavfsizlikka o'qitish ham dinamik va adaptiv bo'lishi shart. Sun'iy intellekt va UBA texnologiyalari yordamida foydalanuvchilarning kiber-xavf darajasini doimiy monitoring qilish hamda xatti-harakatga asoslangan holda avtomatlashtirilgan, shaxsiylashtirilgan o'quv materiallarini taqdim etish bugungi kunning asosiy talablaridan biridir. Taklif etilayotgan model tashkilotlarga "odamlarga asoslangan" (human-centric) faol himoya tizimini qurish va axborot xavfsizligi insidentlarini proaktiv tarzda kamaytirish imkonini beradi.

**Foydalanilgan adabiyotlar:**

1. G‘aniyev S.K., Karimov M.M., Tashev K.A. "Axborot xavfsizligi asoslari". Toshkent, 2017.

2. Verizon, "Data Breach Investigations Report (DBIR)", 2023.
3. Bada, M., Sasse, A. M., & Nurse, J. R. "Cyber security awareness campaigns: Why do they fail to change behaviour?". arXiv preprint, 2019.
4. Erkinov Z.B. "Axborot xavfsizligida inson omili va xulq-atvor tahlili." Ilmiy xabarnoma jurnali, Samarqand, 2023.
5. Z. M. Fadlullah et al. "State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow’s Intelligent Network Traffic Control Systems." IEEE Communications Surveys & Tutorials, 2017.
6. O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni (O‘RQ-764-son). Toshkent, 2022.
7. Alseadoon, I., Othman, M., & Chan, T. "What is the impact of cyber-security awareness on user's behavior?". International Journal of Computer Science and Network Security, 2015.