TECHNICAL SCIENCE RESEARCH IN UZBEKISTAN
ISSN (E): 2992-9148 SJIF 2024 = 5.333 ResearchBib Impact Factor: 10.77 / 2025 VOLUME-4, ISSUE-3

# KIBERXAVFSIZLIK TAHDIDLARINI ANIQLASHDA ANN SAMARADORLIGINI CONFUSION MATRIX ASOSIDA BAHOLASH

**Xo‘shboqov Abdulla Xudoymurodovich**

Termiz davlat universiteti

Axborot texnologiyalari fakulteti

Kompyuter tizimlari va ularning dasturiy ta‘minoti birinchi kurs magistranti

**Zaripova Mukaddas Djumayozovna**

Termiz davlat universiteti Kompyuter va dasturiy injiniring kafedrasi, dotsent

zaripovamuqaddas0407@gmail.com

**Annotatsiya:** Bugungi kunda kiberxavfsizlik tahdidlarining tezkor va samarali aniqlanishi tashkilotlar va tizimlar uchun muhim ahamiyat kasb etadi. Sun’iy neyron tarmoqlar (Artificial Neural Networks, ANN) ushbu tahdidlarni avtomatik ravishda aniqlashda samarali vosita sifatida keng qo‘llanilmoqda. Ushbu maqolada ANN yordamida tahdidlarni aniqlashning samaradorligi confusion matrix asosida baholandi. Tadqiqot davomida ANN modellarining haqiqiy pozitiv, haqiqiy negativ, noto‘g‘ri pozitiv va noto‘g‘ri negativ ko‘rsatkichlari tahlil qilindi, bu esa modelning aniqligi, sezgirligi, maxsusligi va F1-score kabi metrikalarni hisoblash imkonini berdi. Natijalar shuni ko‘rsatdiki, ANN kiberxavfsizlik tizimlarida tahdidlarni aniqlashda yuqori samaradorlikka ega bo‘lib, noto‘g‘ri signal (false positive) va o‘tish (false negative) holatlarini minimal darajada saqlashga yordam beradi. Ushbu tadqiqot, shuningdek, kiberxavfsizlik monitoring tizimlarida ANN modellari samaradorligini baholash va optimallashtirish uchun amaliy tavsiyalar beradi.

**Kalit so‘zlar:** kiberxavfsizlik, sun’iy neyron tarmoqlar, tahdidlarni aniqlash, confusion matrix, model samaradorligi, haqiqiy pozitiv, haqiqiy negativ, noto‘g‘ri pozitiv, noto‘g‘ri negativ, F1-score, aniqlik, sezgirlik

## Kirish

Kiberhujumlar va tahdidlar sonining ortishi tufayli, an’anaviy xavfsizlik monitoring vositalari ko‘pincha real vaqtda aniqlash imkoniyatini bermaydi. Sun’iy neyron tarmoqlar (ANN) – bu murakkab naqshlarni va anomal signallarni aniqlashda samarali algoritm bo‘lib, u kiberxavfsizlik tizimlarini avtomatlashtirish va noto‘g‘ri signal berishni kamaytirishga yordam beradi. Confusion

ISSN (E): 2992-9148 SJIF 2024 = 5.333 ResearchBib Impact Factor: 10.77 / 2025 VOLUME-4, ISSUE-3

matrix esa ANN modelining har bir aniqlash natijasini to‘liq baholash imkonini beradi: haqiqiy tahdidlar, noto‘g‘ri signal va o'tkazib yuborilgan tahdidlar aniqlanadi. Shu asosda modelning aniqligi, sezgirligi, maxsusligi va F1-score kabi metrikalar hisoblanadi.

**Materiallar va Metodlar**

Tadqiqotda quyidagi usullar ishlatildi: Ma’lumotlar to‘plami: 2000 ta hodisa (1000 tahdidli va 1000 normal holat) real va simulyatsiya qilingan kiberxavfsizlik monitoring loglaridan olingan. Model tuzilishi:

1. Kirish qatlami: 20 atribut (IP manzillar, portlar, paket uzunligi, trafik chastotasi)
2. Yashirin qatlamlar: 2 qatlam, har birida 64 neyron
3. Faollashtirish funksiyasi: ReLU
4. Chiqish qatlami: 2 neyron, softmax faollashtirish
5. Optimizer: Adam, o‘quv stavkasi 0,001, 50 epoch

Baholash metrikalari: Confusion matrix yordamida TP, TN, FP, FN ko‘rsatkichlari va aniqlik, sezgirlik, maxsuslik, Precision va F1-score hisoblandi.

**Natijalar**

ANN modeli test to‘plamida quyidagi natijalarni ko‘rsatdi:

1. Predicted Threat
2. Predicted Normal
3. Actual Threat
4. TP = 950
5. FN = 50
6. Actual Normal
7. FP = 20
8. TN = 980

Shundan kelib chiqib:

Accuracy = (TP + TN) / (TP + TN + FP + FN) = (950 + 980) / 2000 ≈ 0.968

Recall (Sezgirlik) = TP / (TP + FN) = 950 / (950 + 50) = 0.95

Specificity (Maxsuslik) = TN / (TN + FP) = 980 / (980 + 20) = 0.98

Precision = TP / (TP + FP) = 950 / (950 + 20) ≈ 0.979

F1-score = 2 * (Precision * Recall) / (Precision + Recall) ≈ 0.955

ISSN (E): 2992-9148 SJIF 2024 = 5.333 ResearchBib Impact Factor: 10.77 / 2025 VOLUME-4, ISSUE-3

Natijalar ANN modelining kiberxavfsizlik tahdidlarini aniqlashda yuqori samaradorligini ko‘rsatadi.

**Muhokama**

Tahlil shuni ko‘rsatadiki: ANN modeli real va simulyatsiya qilingan kiberxavfsizlik hodisalarini yuqori aniqlik bilan aniqlaydi. Confusion matrix yordamida modelning kuchli va zaif tomonlari aniq ko‘riladi: FP va FN minimal darajada. Sezgirlik va maxsuslik yuqori bo‘lishi ANN modelini real vaqtda monitoring tizimlari uchun ideal qiladi. Kelgusida modelni yanada takomillashtirish uchun: Ma’lumotlar to‘plamini kengaytirish va murakkab tahdidlarni qo‘shish. Hyperparameter tuning va dropout qatlamlari yordamida overfittingni kamaytirish. Real vaqtda o‘qitish (onlinelearning) usullarini qo‘llash tavsiya etiladi.

**Xulosa**

Sun’iy neyron tarmoqlar kiberxavfsizlik tizimlarida tahdidlarni aniqlashda yuqori samaradorlik ko‘rsatadi. Confusion matrix asosida baholash modelning kuchli va zaif tomonlarini aniqlashga yordam beradi. ANN modeli haqiqiy tahdidlarni yuqori aniqlik bilan aniqlaydi, noto‘g‘ri signal va o‘tish holatlarini minimal darajada saqlaydi. Ushbu tadqiqot kiberxavfsizlik monitoring tizimlarini optimallashtirish va real vaqtda tahdidlarni aniqlashga amaliy tavsiyalar beradi.

**Foydalanilgan adabiyotlar:**

1. Goodfellow I, Bengio Y, Courville A. Deep Learning. MIT Press; 2016.
2. Bishop CM. Pattern Recognition and Machine Learning. Springer; 2006.
3. Sommer R, Frühwirth R. Artificial neural networks in intrusion detection: A review. Computers & Security. 2016;57:1–16.
4. Dhanabal L, Shantharajah S. A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. Int J Adv Res Comput Commun Eng. 2015;4(6):446–452.
5. Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. IEEE Symposium on Computational Intelligence for Security and Defense Applications. 2009;1–6.
6. Kim H, Lee J. Evaluating the performance of neural networks in network intrusion detection using confusion matrix. J Inf Secur Appl. 2018;41:37–48.
7. Moustafa N, Slay J. UNSW-NB15: A comprehensive data set for network intrusion detection systems. Military Communications and Information Systems Conference (MilCIS). 2015;1–6.