SUN'IY INTELLEKT TEXNOLOGIYALARI ASOSIDA TELEKOMMUNIKATSIYA TARMOQLARIDA KIBERXAVFSIZLIKNI TA'MINLASHNING ZAMONAVIY USULLARI

Nabiyeva Ziyodaxon Abdusattor qizi
Farg'ona davlat texnika universiteti, Telekommunikatsiya va kiberxavfsizlik fakulteti

Ilmiy rahbar: **Jo'rayev Nurmakhamad Mamatovich**
Farg'ona davlat texnika universiteti Telekommunikatsiya muhandisligi kafedrasi dotsenti
DOI:https://doi.org/10.5281/zenodo.23945238

ANNOTATSIYA

Maqolada zamonaviy telekommunikatsiya tarmoqlarida kiberxavfsizlikni ta'minlash uchun sun'iy intellekt va mashinaviy o'qitish usullaridan foydalanish imkoniyatlari tahlil qilinadi. Tadqiqotning maqsadi tarmoqdagi noodatiy faollikni aniqlash, xavfsizlik hodisalarini baholash va mutaxassis nazoratida javob choralarini tashkil etishga mo'ljallangan konseptual intellektual himoya modelini ishlab chiqishdan iborat. Tahlil natijasida ma'lumotlarni yig'ish, qayta ishlash, intellektual tahlil, xavfni tasniflash va mutaxassis nazorati bosqichlaridan iborat model taklif etiladi. Modelni amaliy baholash uchun Precision, Recall, F1-score va noto'g'ri ogohlantirishlar ulushi kabi mezonlar tavsiya qilinadi.

Kalit so'zlar: sun'iy intellekt, telekommunikatsiya, kiberxavfsizlik, mashinaviy o'qitish, 5G, tarmoq monitoringi, anomaliyalarni aniqlash.

АННОТАЦИЯ

В статье анализируются возможности применения искусственного интеллекта и машинного обучения для обеспечения кибербезопасности современных телекоммуникационных сетей. Цель исследования — разработка концептуальной интеллектуальной модели защиты, предназначенной для выявления аномальной активности, оценки инцидентов безопасности и организации реагирования под контролем специалиста. Предлагаемая модель включает сбор и обработку данных, интеллектуальный анализ, классификацию рисков и экспертный контроль. Для практической оценки модели рекомендуются показатели Precision, Recall, F1-score и доля ложных предупреждений.

Ключевые слова: искусственный интеллект, телекоммуникации, кибербезопасность, машинное обучение, сети 5G, мониторинг сети, обнаружение аномалий.

ABSTRACT

This article analyzes the use of artificial intelligence and machine learning to strengthen cybersecurity in modern telecommunication networks. The study aims to develop a conceptual intelligent protection model for detecting abnormal activity, assessing security incidents, and organizing responses under human supervision. The proposed model consists of data collection, preprocessing, intelligent analysis, risk classification, and expert review. Precision, Recall, F1-score, and false-alarm rate are recommended for subsequent empirical evaluation.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

Keywords: artificial intelligence, telecommunications, cybersecurity, machine learning, 5G networks, network monitoring, anomaly detection.

1. KIRISH (INTRODUCTION)

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi telekommunikatsiya tarmoqlarini davlat boshqaruvi, bank-moliya, ta'lim, tibbiyot va sanoat kabi sohalarning muhim infratuzilmasiga aylantirdi. 5G, buyumlar interneti (IoT), bulutli hisoblash va katta hajmdagi ma'lumotlar almashinuvi tarmoq imkoniyatlarini kengaytirishi bilan birga, axborot xavfsizligiga qo'yiladigan talablarni ham kuchaytirmoqda.

An'anaviy himoya vositalari ko'pincha oldindan belgilangan qoidalar yoki ma'lum tahdid belgilariga tayanadi. Tarmoq trafikining o'zgaruvchanligi va yangi turdagi tahdidlarning paydo bo'lishi esa moslashuvchan tahlil mexanizmlariga ehtiyoj tug'diradi. Mashinaviy o'qitish algoritmlari tarmoqning odatiy faoliyatini o'rganish va undan farq qiluvchi holatlarni aniqlash imkonini berishi mumkin [1, 3].

Tadqiqotning maqsadi — telekommunikatsiya tarmoqlarida sun'iy intellekt asosida ishlaydigan, anomaliyalarni aniqlash va xavfsizlik hodisalarini baholashga yo'naltirilgan konseptual himoya modelini taklif etish. Tadqiqot doirasida quyidagi vazifalar belgilandi: kiberxavfsizlik muammolarini tizimlashtirish; AI/ML usullarining qo'llanilish yo'nalishlarini ko'rib chiqish; himoya modelining bosqichlarini shakllantirish; modelni kelgusida baholash mezonlarini belgilash.

2. TADQIQOT METODOLOGIYASI (METHODS)

Tadqiqot nazariy-tahliliy va konseptual modellashtirish yondashuvlariga asoslandi. Telekommunikatsiya va IoT xavfsizligiga oid xalqaro tavsiyalar hamda sun'iy intellekt xavflarini boshqarish bo'yicha metodik hujjatlar o'rganildi [1–4]. Shuningdek, mualliflarning telekommunikatsiya tarmoqlarini monitoring qilishga oid avvalgi ilmiy ishlari mavzuning amaliy kontekstini belgilashda hisobga olindi [6].

Tahlil jarayonida tarmoq xavfsizligining asosiy vazifalari — maxfiylik, yaxlitlik, xizmatlarning mavjudligi, ruxsatsiz kirishlarni aniqlash va hodisalarni kuzatish — mezon sifatida olindi. Ushbu vazifalarga mos ravishda ma'lumotlarni yig'ish, oldindan qayta ishlash, mashinaviy o'qitish orqali tahlil qilish, xavfni tasniflash va mutaxassis nazoratida javob choralarini belgilash bosqichlari birlashtirildi.

Maqolada real tarmoqda tajriba o'tkazilgani yoki muayyan algoritmning sonli samaradorligi o'lchangani da'vo qilinmaydi. Taklif etilgan yechim konseptual model bo'lib, uning amaliy samaradorligi keyingi bosqichda belgilangan ma'lumotlar to'plami va sinov muhiti asosida tekshirilishi lozim.

3. NATIJALAR (RESULTS)

Tahlil natijasida telekommunikatsiya tarmoqlari uchun besh bosqichli intellektual himoya modeli shakllantirildi:

1-bosqich — ma'lumotlarni yig'ish: tarmoq qurilmalari, serverlar va monitoring vositalaridan trafik ko'rsatkichlari, ulanish metama'lumotlari hamda tizim jurnallari olinadi.

2-bosqich — ma'lumotlarni qayta ishlash: takroriy yoki noto'liq yozuvlar tekshiriladi, ma'lumotlar standartlashtiriladi va maxfiylik talablariga muvofiq zarur himoya choralari qo'llanadi.

3-bosqich — intellektual tahlil: mashinaviy o'qitish algoritmlari tarmoqning odatiy xulq-atvorini o'rganadi va undan sezilarli farq qiluvchi holatlarni belgilaydi. Decision Tree, Random Forest va KNN kabi algoritmlar sinov uchun ko'rib chiqilishi mumkin.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

4-bosqich — xavfni baholash: aniqlangan hodisalar ustuvorlik va ehtimoliy ta'sir darajasi bo'yicha tasniflanadi; tizim tekshiruv uchun ogohlantirish yaratadi.

5-bosqich — mutaxassis nazorati: administrator ogohlantirishni tekshiradi, hodisani tasdiqlaydi yoki rad etadi hamda tegishli javob choralarini belgilaydi.

Modelning umumiy ketma-ketligi: tarmoq ma'lumotlari → oldindan qayta ishlash → AI/ML tahlili → xavfni baholash → ogohlantirish → mutaxassis tekshiruvi → javob chorasi.

Modelni amaliy sinovdan o'tkazishda Precision, Recall, F1-score, noto'g'ri ijobiy ogohlantirishlar ulushi (False Positive Rate) va tahlilga ketgan vaqtni o'lchash tavsiya etiladi. Ushbu ko'rsatkichlar modelning aniqligi, tahdidlarni qamrab olish darajasi va operatsion samaradorligini baholashga xizmat qiladi.

4. MUHOKAMA (DISCUSSION)

Taklif etilgan modelning asosiy afzalligi — xavfsizlik monitoringini yagona ketma-ket jarayonga birlashtirishidir. Mashinaviy o'qitish katta hajmdagi trafik ma'lumotlaridan qonuniyatlarni aniqlashga yordam berishi mumkin. Random Forest kabi ansambl algoritmlari turli xususiyatlar asosida tasniflash uchun sinovdan o'tkazilishi mumkin, biroq ularning samaradorligi ma'lumotlar sifati, sinflar muvozanati va tanlangan parametrlariga bog'liq.

Modelni joriy etishda noto'g'ri ogohlantirishlar, ma'lumotlar to'plamining yetarli emasligi, yangi tahdidlar sabab model samaradorligining pasayishi va maxfiylik bilan bog'liq xavflar hisobga olinishi zarur. Sun'iy intellekt tizimining o'zi ham himoyaga muhtoj: o'qitish ma'lumotlariga zararli ta'sir ko'rsatish yoki model xulosalarini manipulyatsiya qilish ehtimoli mavjud [3].

Shu sababli AI/ML yechimlarini mavjud xavfsizlik vositalarini to'ldiruvchi mexanizm sifatida qo'llash, muhim qarorlarni inson nazoratida qoldirish va modellarni muntazam qayta baholash maqsadga muvofiq. ITU hujjatlarida ham IoT va telekommunikatsiya muhitida intellektual tahlilni joriy etishda xavfsizlik hamda ishonchlilik talablariga e'tibor qaratiladi [1, 2, 4].

Tadqiqotning cheklovi shundaki, maqolada taklif etilgan model real operator tarmog'ida sinovdan o'tkazilmagan. Shu bois hozircha aniqlik yoki samaradorlik bo'yicha sonli natijalar keltirilmaydi. Keyingi tadqiqot bosqichida ochiq tarmoq trafik ma'lumotlari yoki maxsus laboratoriya muhiti asosida algoritmlarni qiyosiy baholash rejalashtirilishi mumkin.

5. XULOSA (CONCLUSION)

Tadqiqotda telekommunikatsiya tarmoqlarida kiberxavfsizlikni kuchaytirish uchun sun'iy intellekt va mashinaviy o'qitishdan foydalanish imkoniyatlari tahlil qilindi. Natijada ma'lumotlarni yig'ish, qayta ishlash, intellektual tahlil, xavfni baholash va mutaxassis nazoratini birlashtiruvchi besh bosqichli konseptual model taklif etildi.

Taklif etilgan yondashuv tarmoqdagi noodatiy faollikni aniqlash jarayonini tizimlashtirish, xavfsizlik hodisalarini ustuvorlik bo'yicha saralash va mutaxassislar faoliyatini qo'llab-quvvatlashga qaratilgan. Uning amaliy samaradorligini aniqlash uchun real yoki laboratoriya ma'lumotlari asosida sinov o'tkazish, algoritmlarni qiyoslash va Precision, Recall hamda F1-score kabi ko'rsatkichlarni hisoblash zarur. Kelgusidagi tadqiqotlar mahalliy telekommunikatsiya infratuzilmasiga mos, xavfsiz va izohlanadigan intellektual monitoring yechimlarini ishlab chiqishga yo'naltirilishi lozim.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.

FOYDALANILGAN ADABIYOTLAR

1. International Telecommunication Union (ITU-T). Intelligent anomaly detection system for Internet of Things. Technical Report YSTR-IADIoT, July 2024. https://www.itu.int/epublications/publication/itu-t-ystr-iadiot-2024-07-intelligent-anomaly-detection-system-for-internet-of-things
2. International Telecommunication Union (ITU-T). Potential requirements and methodology for deploying and assessing generative AI models in telecom networks. Technical Report TR.GenAI-Telecom, March 2025. https://www.itu.int/epublications/publication/itu-t-tr-genai-telecom-2025-03-potential-requirements-and-methodology-for-deploying-and-assessing-generative-ai-models-in-telecom-networks
3. National Institute of Standards and Technology (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0). 2023. https://www.nist.gov/itl/ai-risk-management-framework
4. International Telecommunication Union (ITU-T). Security framework for Internet of Things based on the gateway model. Recommendation ITU-T X.1361, 2018.
5. Juraev N., Nabiyeva Z. An Integrated Information System for Parcel Tracking and Last-Mile Delivery Efficiency in National Postal Operators // Bulletin of Contemporary Researches. – 2026. – Vol. 2, No. 4. – pp. 36–44. https://bulconre.com/index.php/mult/article/view/38
6. Juraev N.M., Nabiyeva Z.A. TeleTwin AI: An AI-based digital twin for intelligent telecommunication network monitoring and fault prediction // Descendants of Al-Farghani electronic scientific journal. – 2026. – Vol. 1, Iss. 3. – pp. 427–431.
7. Jo'rayev N.M., Nabiyeva Z.A. Sun'iy intellekt asosida talabalarning ta'lim jarayonini individuallashtirishning raqamli modeli // "Sun'iy intellekt asosida aqlli raqamli tizimlarning ilmiy va innovatsion yechimlari" respublika ilmiy-texnikaviy anjumani. – 2026.

© Ushbu material Creative Commons Attribution 4.0 International (CC BY 4.0) litsenziyasi asosida tarqatiladi.