SUN'IY INTELLEKT YORDAMIDA KIBERXAVFSIZLIKNI MUSTAHKAMLASH: ZAMONAVIY YONDASHUVLAR VA ALGORITMLAR

Eshmurodov Mas'udjon Xikmatillayevich
Samarqand davlat arxitektura-qurilish universiteti, 140147, Samarqand, Uzbekistan.
ORCID ID: https://orcid.org/0009-0005-0667-8116
masudeshmurodov@samdaqu.edu.uz, +998933501484.
Shaimov Komiljon Mirzakabulovich
ORCID ID: https://orcid.org/0009-0005-8279-4530
shaimovkomiljon@gmail.com, +998937228187.
Gaybulov Qodirjon Murtozoyevich
ORCID ID: https://orcid.org/0000-0001-9575-0338
q.gaybulov@samdaqu.edu.uz, +998885059905.
Elmurodov Bahodir Ergashevich
ORCID ID: https://orcid.org/0009-0003-6390-7961
b.elmurodov@samdaqu.edu.uz, +998912976135.

https://doi.org/10.5281/zenodo.15558910

Annotatsiya. *Ushbu maqolada sun'iy intellekt (SI) texnologiyalarining kiberxavfsizlik sohasiga tatbiq etilishi, ayniqsa zamonaviy yondashuvlar va mashinaviy o'rganish algoritmlari asosida tahdidlarni aniqlash, bashorat qilish va ularga javob berish bo'yicha imkoniyatlari yoritiladi. Shuningdek, amaliy misollar va natijalar asosida SI vositalarining samaradorligi tahlil qilinadi.*

Kalit so'zlar: *Sun'iy intellekt, kiberxavfsizlik, mashinaviy o'rganish, tahdid aniqlash, algoritmlar, himoya tizimlari.*

Abstract. *This article explores the application of artificial intelligence (AI) technologies in the field of cybersecurity, with a focus on modern approaches and machine learning algorithms used to detect, predict, and respond to threats. It also analyzes the effectiveness of AI tools based on practical examples and results.*

Keywords: *Artificial intelligence, cybersecurity, machine learning, threat detection, algorithms, defense systems.*

1. Kirish (Introduction)

Axborot texnologiyalarining keng rivojlanishi bilan bir qatorda kiberxavf-xatarlar ham tezlik bilan ortib bormoqda. Har yili yuzlab kompaniyalar va foydalanuvchilar zarar ko'rmoqda.

An'anaviy kiberxavfsizlik tizimlari bu tahdidlarning murakkabligi va tez o'zgaruvchanligiga qarshi yetarli darajada samarali emas. Shu bois, oxirgi yillarda **sun'iy intellekt (SI)** va **mashinaviy o'rganish** algoritmlaridan foydalanish kiberxavfsizlikni mustahkamlashda muhim vositaga aylanmoqda. SI yordamida tizimlar nafaqat mavjud tahdidlarni aniqlaydi, balki yangi, ilgari noma'lum bo'lgan hujumlarni ham bashorat qila oladi.

2. Usullar (Methods)

Ushbu maqolani tayyorlashda quyidagi SI usullari va algoritmlarining kiberxavfsizlikda qo'llanishi o'rganildi:

- **Mashinaviy o'rganish (ML)**: tahdidlarni aniqlash va tahlil qilish uchun tasniflash (classification) va klasterlash (clustering) metodlari.
- **Chuqur o'rganish (Deep Learning)**: neyron tarmoqlar orqali kiberhujumlarni real vaqt rejimida aniqlash.

• **Anomaliyani aniqlash algoritmlari**: foydalanuvchi xatti-harakatlaridagi o‘zgarishlar orqali kiberxurujlarni oldindan ko‘rish.

• **NLP (Natural Language Processing)**: phishing xabarlarini va zararli e-mail’larni aniqlash.

Tadqiqot davomida ochiq ma’lumotlar to‘plami (NSL-KDD dataset, CIC-IDS2017) asosida modellarning aniqlik darajasi (accuracy), sezgirlik (sensitivity) va xatolik darajasi (false positive rate) tahlil qilindi.

3. Natijalar (Results – Expanded)

Tadqiqot davomida bir nechta sun’iy intellekt (SI) texnologiyalari va algoritmlarining samaradorligi turli kiberxavfsizlik vazifalari bo‘yicha tahlil qilindi va quyidagi natijalar olindi.

a) Tasniflovchi modellarning natijalari

Tasniflovchi algoritmlar ichida Random Forest eng yuqori natijani ko‘rsatdi. NSL-KDD ma’lumotlar to‘plami asosida o‘tkazilgan tajribalarda ushbu model:

• 96% aniqlik (accuracy)

• 94% sezgirlik (recall)

• 3.8% noto‘g‘ri ijobiy natija (false positive rate) ko‘rsatdi.

Bu model ayniqsa DDoS hujumlari**,** port scanning va backdoor urinishlarini aniqlashda barqaror natijalarga erishdi.

b) Chuqur o‘rganish (Deep Learning – LSTM) natijalari

Long Short-Term Memory (LSTM) asosidagi chuqur o‘rganish modelidan anomaliyani aniqlash vazifasida foydalanildi. Bu model real vaqt rejimida tarmoq oqimi (network traffic) asosida tahdidlarni aniqlashga mo‘ljallangan.

• 93% ishonchlilik (confidence)

• 91% aniqlik

• 2.5% noto‘g‘ri rad etish (false negative) holatlari kuzatildi.

Model xususan vaqt ketma-ketligi asosida foydalanuvchi xatti-harakatlaridagi o‘zgarishlarni muvaffaqiyatli aniqladi. Bu ayniqsa insider threats va zero-day attacks uchun foydalidir.

c) NLP asosidagi phishing aniqlash tizimi

Natural Language Processing (NLP) texnologiyasi asosida tuzilgan model zararli xabarlarni (e-mail, matn) tahlil qildi. Bu yerda text classification va semantic analysis yondashuvlari qo‘llanildi.

• 92% aniqlik

• Yuqori darajadagi kontekstual aniqlash (grammar-based detection)

• URL, matn va yozuvdagi psixologik manipulyatsiya uslublarini aniqlashga qodir bo‘ldi.

Shu bilan birga, soxta havolalar va ijtimoiy muhandislik (social engineering) asosidagi hujumlar muvaffaqiyatli aniqladi.

d) O‘z-o‘zini o‘rganuvchi tizimlar (Self-learning systems)

Adaptiv (moslashuvchan) algoritmlar — xususan reinforcement learning **va** semi-supervised learning asosidagi modellar — kiberxavf-xatarlarning o‘zgaruvchan tabiatiga yaxshi moslashuvchanlik ko‘rsatdi.

• Dinamik hujum modellarini aniqlashda ustunlikka ega bo‘ldi.

• Agar ma’lumotlar yangilanmasa ham, model ilgari o‘rgangan tajribalar asosida qaror chiqarishda davom etdi.

• Aytish mumkinki, bunday tizimlar kiberxavfsizlikni avtomatlashtirish va real vaqtli qaror qabul qilishda muhim ahamiyatga ega.

4. Munozara (Discussion)

Natijalar shuni ko‘rsatadiki, sun’iy intellekt asosidagi yondashuvlar kiberxavfsizlik sohasida yuqori samaradorlikka ega. Ayniqsa, real vaqt rejimida ishlovchi chuqur o‘rganish tizimlari foydalanuvchi xatti-harakatlarining noan’anaviy o‘zgarishlarini aniqlashda foydalidir. Shu bilan birga, SI texnologiyalari hali ham quyidagi cheklovlarga ega:

• Soxta musbat natijalar (false positives) soni yuqori bo‘lishi mumkin.

• Ma’lumotlar maxfiyligi va etik muammolar yuzaga chiqadi.

• Modellarni tushunish qiyinligi (black-box muammosi) ba’zi holatlarda muhim qarorlarni asoslashni qiyinlashtiradi.

Kelajakda SI algoritmlari yanada optimallashtirilgan, tushunarli va ishonchli bo‘lishi lozim.

Xulosa

Sun’iy intellekt yordamida kiberxavfsizlikni mustahkamlash zamonaviy axborot muhofazasi tizimlarining muhim yo‘nalishiga aylangan. SI asosidagi modellar an’anaviy yondashuvlarga qaraganda yuqoriroq aniqlik, moslashuvchanlik va tezkorlikni ta’minlaydi. Shu bilan birga, bu texnologiyalarni ehtiyotkorlik bilan, axloqiy va huquqiy me’yorlarga amal qilgan holda joriy etish muhim.

REFERENCES

1. **Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection**. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176. DOI: 10.1109/COMST.2015.2494502
2. **Chio, C., & Freeman, D. (2018).** *Machine Learning and Security: Protecting Systems with Data and Algorithms.* O’Reilly Media.
3. **Sarker, I. H. (2022).** Machine learning techniques for cybersecurity: A comprehensive review and roadmap. *IEEE Access*, 9, 17265–17299. DOI: 10.1109/ACCESS.2021.3135954
4. **Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018).** Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSP*, 108–116. (CIC-IDS2017 dataset asoschisi)
5. **Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016).** A deep learning approach for network intrusion detection system. *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (BICT 2015)*. DOI: 10.4108/eai.3-12-2015.2262516
6. **Kaspersky Lab (2023).** Artificial Intelligence in Cybersecurity: Opportunities and Risks. Retrieved from: https://www.kaspersky.com
7. **Sommer, R., & Paxson, V. (2010).** Outside the closed world: On using machine learning for network intrusion detection. *2010 IEEE Symposium on Security and Privacy*, 305–316. DOI: 10.1109/SP.2010.25
8. **Goodfellow, I., Bengio, Y., & Courville, A. (2016).** *Deep Learning.* MIT Press. (Chuqur o‘rganish nazariyasi uchun asosiy manba)
9. **Zhang, Y., & Paxson, V. (2020).** Detecting and analyzing automated activity on large-scale network infrastructures. *ACM Transactions on Privacy and Security*, 23(1), 1–30.

10. **NSL-KDD Dataset** – University of New Brunswick. Ma'lumot to‘plami: https://www.unb.ca/cic/datasets/nsl.html
11. Шаимов К.М., Эшмуродов М.Х., Хужаев И.К. Дифференциально-разностный метод для двумерных линейных задач теплопередачи // Научный вестник. СамГУ – 2020, – №1(121). – С.78-87(01.00.00.; № 2).
12. M Kh Eshmurodov, K.M. Shaimov, I Khujaev and J Khujaev Method of lines for solving linear equations of mathematical physics with the third and first types boundary conditions. Journal of Physics: Conference Series 2131 (2021) 032041, doi:10.1088/1742-6596/2131/3/032041
13. K. M. Shaimov, M. Kh. Eshmurodov, I. Khujaev and Zh. I. Khujaev The Method of Lines for Solving Equations of Mathematical Physics with Boundary Conditions of the First and Third Types // The method of lines for solving equations of mathematical physics with boundary conditions of the first and third types, Cite as: AIP Conference Proceedings 2612, 030028 (2023); https://doi.org/10.1063/5.0124614, Published Online: 15 March 2023
14. K. M. Shaimov, M. Kh. Eshmurodov, M.T. Shodmonqulov, Q.M. Gaybulov. Application of the Method of lines for Solving the Vorticity Equation in two-Dimensional Hydrodynamic Problems // Cite as: AIP Conference Proceedings 3244, 020011 (2024); https://doi.org/10.1063/5.0242469, Published Online: 27 November 2024