SUN'IY INTELEKTDAN PEDAGOGIKADA FOYDALANGAN HOLDA KOMPYUTER TIZIMLARI VA TARMOQLARINING KIBERXAVSIZLIGI TA'MINLASH ALGORITMLARINI ISHLAB CHIQISH

Namangan muhandislik texnologiya instituti
Informatika texnologiyalari kafedrasi katta o'qituvchisi
Mansurov E'zozbek Islomxonovich

Annotatsiya: *Ushbu maqola sun'iy intellekt (SI) texnologiyalaridan pedagogik usullar bilan uyg'unlashtirilgan holda kompyuter tizimlari va tarmoqlarining kiberxavfsizligini ta'minlash uchun yangi algoritmlarni ishlab chiqishga bag'ishlangan. Maqolada kiberxavfsizlik sohasidagi mavjud muammolar va ularni hal etishda SIning o'rni tahlil qilinadi. Shuningdek, ta'lim jarayonida SI algoritmlarini qo'llash orqali kiberxavfsizlik bo'yicha bilim va ko'nikmalarni oshirish imkoniyatlari ko'rib chiqiladi. Maqolada ishlab chiqilgan yangi algoritmlarning arxitekturasi, ishlash mexanizmi va ularni amaliyotga tatbiq etish yo'llari batafsil yoritilgan. Algoritmlarning samaradorligi turli xil kiberhujumlar simulyatsiyasi orqali baholanadi va olingan natijalar muhokama qilinadi.*

Kalit So'zlar: *Sun'iy intellekt, kiberxavfsizlik, pedagogika, algoritmlar, kompyuter tizimlari, kompyuter tarmoqlari, kiberhujumlar, ta'lim, xavfsizlikni ta'minlash.*

Annotation: *This article is dedicated to the development of novel algorithms for ensuring the cybersecurity of computer systems and networks, utilizing artificial intelligence (AI) technologies integrated with pedagogical methods. The paper analyzes the existing challenges in the field of cybersecurity and the role of AI in addressing them. Furthermore, it explores the potential of applying AI algorithms in the educational process to enhance knowledge and skills in cybersecurity. The article details the architecture, operational mechanism, and implementation approaches of the newly developed algorithms. The effectiveness of the algorithms is evaluated through simulations of various cyberattacks, and the obtained results are discussed.*

Keywords: *Artificial intelligence, cybersecurity, pedagogy, algorithms, computer systems, computer networks, cyberattacks, education, security assurance.*

Kirish

Zamonaviy axborot-kommunikatsiya texnologiyalarining (AKT) jadal rivojlanishi barcha sohalarga chuqur kirib borishi bilan kompyuter tizimlari va tarmoqlarining ahamiyati beqiyos oshib bormoqda. Bank sektori, davlat boshqaruvi, sanoat, ta'lim va boshqa muhim infratuzilmalar faoliyati tobora ko'proq raqamli platformalarga bog'liq bo'lib qolmoqda [^1]. Bunday sharoitda kiberxavfsizlikni

ta'minlash dolzarb vazifaga aylanadi, chunki kompyuter tizimlari va tarmoqlariga yo'naltirilgan zararli hujumlar nafaqat moliyaviy yo'qotishlarga, balki muhim ma'lumotlarning yo'qolishiga, infratuzilma faoliyatining buzilishiga va hatto insonlar xavfsizligiga ham tahdid solishi mumkin [^2].

Kiberxavfsizlik sohasidagi mavjud tahdidlarning murakkablashuvi va ko'payishi an'anaviy xavfsizlik mexanizmlarining cheklanganligini ko'rsatmoqda. Kiberhujumlar tobora aqlli, maqsadli va moslashuvchan bo'lib bormoqda, bu esa ularni aniqlash va bartaraf etishda yangi, innovatsion yondashuvlarni talab qiladi [^3]. So'nggi yillarda sun'iy intellekt (SI) texnologiyalari kiberxavfsizlik sohasida katta qiziqish uyg'otmoqda. SI algoritmlari katta hajmdagi ma'lumotlarni tahlil qilish, anomaliyalarni aniqlash, tahdidlarni bashorat qilish va avtomatik ravishda javob berish qobiliyati tufayli kiberxavfsizlikni ta'minlashda yangi imkoniyatlar yaratmoqda [^4].

Shu bilan birga, kiberxavfsizlik bo'yicha mutaxassislarga bo'lgan talabning ortishi va bu sohada malakali kadrlarning yetishmasligi ham muhim muammodir. Kiberxavfsizlikning texnik jihatlari bilan bir qatorda, inson omili ham xavfsizlikni ta'minlashda muhim rol o'ynaydi. Foydalanuvchilarning xabardorligi, xavfsizlik qoidalariga rioya qilishlari va potentsial tahdidlarni aniqlash ko'nikmalari kiberxavfsizlikni ta'minlashning ajralmas qismidir [^5].

Ushbu maqola sun'iy intellekt texnologiyalaridan pedagogik usullar bilan uyg'unlashtirilgan holda kompyuter tizimlari va tarmoqlarining kiberxavfsizligini ta'minlash uchun yangi algoritmlarni ishlab chiqishga qaratilgan. Maqsad kiberxavfsizlik sohasidagi mavjud muammolarni SI yordamida hal etishning innovatsion yechimlarini taklif qilish va ta'lim jarayonida SI algoritmlarini qo'llash orqali kiberxavfsizlik bo'yicha bilim va ko'nikmalarni oshirish imkoniyatlarini ko'rsatishdir.

Asosiy qism: Sun'iy Intellektning Kiberxavfsizlikdagi O'rni

Sun'iy intellekt (SI) kiberxavfsizlik sohasida inqilobiy o'zgarishlar olib kelish potentsialiga ega bo'lib, katta hajmdagi ma'lumotlarni tez va samarali tahlil qilish, murakkab naqshlarni aniqlash va avtomatik ravishda javob berish qobiliyati bilan ajralib turadi [^6]. Kiberhujumlarning tobora murakkablashib borayotgan sharoitida SI algoritmlari an'anaviy xavfsizlik vositalari ko'pincha ojiz qoladigan vaziyatlarda ustunlikni ta'minlashi mumkin.

SIning kiberxavfsizlikdagi asosiy qo'llanilish yo'nalishlari quyidagilarni o'z ichiga oladi: Intruziv hujumlarni aniqlash (Intrusion Detection Systems - IDS): SI algoritmlari tarmoq trafigi va tizim loglarini tahlil qilib, anomaliyalarni va potentsial xavfli harakatlarni real vaqt rejimida aniqlay oladi [^7]. Mashinaviy o'rganish (Machine Learning - ML) usullari, xususan, nazorat ostidagi va nazorat ostisiz o'rganish algoritmlari normal xatti-harakat profilini yaratish va undan chetga chiqishlarni belgilash uchun samarali qo'llaniladi [^8].

- **Zararli dasturlarni aniqlash (Malware Detection):** SI zararli dasturlarning xatti-harakatlarini, kod strukturasini va boshqa xususiyatlarini tahlil qilib, yangi va noma'lum zararli dasturlarni (zero-day attacks) aniqlashga yordam beradi [^9]. Chuqur o'rganish (Deep Learning - DL) modellari, masalan, konvolyutsion neyron tarmoqlar (Convolutional Neural Networks - CNNs) va qaytariluvchi neyron tarmoqlar (Recurrent Neural Networks - RNNs), zararli dasturlarning murakkab naqshlarini o'rganishda yuqori natijalarni ko'rsatmoqda [^10].
- **Fishing hujumlarini aniqlash:** SI algoritmlari elektron pochta xabarlari, veb-saytlar va boshqa aloqa kanallaridagi fishing belgilarini (masalan, shubhali havolalar, grammatik xatolar, so'rovlarning g'ayrioddiy tabiati) aniqlash orqali foydalanuvchilarni himoya qilishi mumkin [^11]. Tabiiy tilni qayta ishlash (Natural Language Processing - NLP) texnikalari matnni tahlil qilish va potentsial tahdidlarni belgilash uchun qo'llaniladi [^12].
- **Xavfsizlik zaifliklarini tahlil qilish (Vulnerability Assessment):** SI kod tahlili va dinamik sinovlar orqali dasturiy ta'minot va tizimlardagi potentsial xavfsizlik zaifliklarini avtomatik ravishda aniqlashi mumkin [^13]. Bu xavfsizlik mutaxassislariga zaifliklarni erta bosqichda bartaraf etish imkoniyatini beradi.
- **Xavfsizlik choralarini avtomatlashtirish va javob berish (Security Automation and Response):** SI algoritmlari aniqlangan tahdidlarga avtomatik ravishda javob berish, masalan, zararli trafikni bloklash, infeksiyalangan tizimlarni izolyatsiya qilish va xavfsizlik siyosatlarini qo'llash uchun ishlatilishi mumkin [^14]. Bu xavfsizlik insidentlariga tezkor va samarali javob berish imkoniyatini oshiradi.

Pedagogikaning Kiberxavfsizlik Ta'minlashdagi Ahamiyati

Kiberxavfsizlikni faqat texnologik yechimlar bilan ta'minlashning o'zi yetarli emas. Inson omili, xususan, foydalanuvchilarning bilim va ko'nikmalari, xavfsizlikni ta'minlashda muhim rol o'ynaydi [^15]. Pedagogik usullar kiberxavfsizlik bo'yicha ta'lim va xabardorlikni oshirish, foydalanuvchilarda xavfsiz xatti-harakat ko'nikmalarini shakllantirish va kiberxavfsizlik madaniyatini rivojlantirish uchun samarali vosita bo'lib xizmat qilishi mumkin [^16]. Pedagogikaning kiberxavfsizlikni ta'minlashdagi asosiy jihatlari quyidagilarni o'z ichiga oladi:Kiberxavfsizlik bo'yicha bilim berish: Pedagogik usullar, masalan, interaktiv darslar, amaliy mashg'ulotlar, simulyatsiyalar va o'yinlashtirish (gamification) orqali foydalanuvchilarga kiberxavfsizlikning asosiy tushunchalari, tahdid turlari, ulardan himoyalanish yo'llari va xavfsiz xatti-harakat qoidalari tushunarli va qiziqarli tarzda yetkazilishi mumkin [^17]. Xavfsiz xatti-harakat ko'nikmalarini shakllantirish: Pedagogik yondashuvlar foydalanuvchilarga xavfsiz parollarni yaratish va saqlash, shubhali havolalar va ilovalardan ehtiyot bo'lish, shaxsiy ma'lumotlarni himoya qilish va onlayn xavfsizlik qoidalariga rioya qilish kabi amaliy ko'nikmalarni egallashlariga yordam beradi [^18]. Kiberxavfsizlik madaniyatini rivojlantirish: Uzluksiz ta'lim va xabardorlik oshirish

orqali tashkilotlarda va jamiyatda kiberxavfsizlikka mas'uliyatli munosabatni shakllantirish, xavfsizlik qoidalariga rioya qilishni odatga aylantirish va kiberinsidentlar haqida xabar berishni rag'batlantirish muhimdir [^19]. SIga asoslangan ta'lim vositalarini ishlab chiqish: Sun'iy intellekt texnologiyalari pedagogik jarayonni yanada samarali va moslashuvchan qilish uchun ishlatilishi mumkin. SIga asoslangan ta'lim platformalari foydalanuvchilarning bilim darajasi va o'zlashtirish tezligiga moslashgan holda individual ta'lim trayektoriyalarini yaratishi, interaktiv mashqlar va testlar taklif qilishi va real vaqt rejimida fikr-mulohazalar berishi mumkin [^20].

Sun'iy Intellekt va Pedagogikaning Integratsiyasi orqali Kiberxavfsizlikni Ta'minlash Algoritmlarini Ishlab Chiqish

Ushbu tadqiqotda sun'iy intellektning analitik va avtomatlashtirish imkoniyatlarini pedagogikaning ta'limiy va xabardorlikni oshirish usullari bilan uyg'unlashtirgan holda kompyuter tizimlari va tarmoqlarining kiberxavfsizligini ta'minlash uchun yangi algoritmlarni ishlab chiqishga e'tibor qaratiladi. Ushbu yondashuv kiberxavfsizlikni ta'minlashda nafaqat texnologik, balki inson omilini ham hisobga olgan holda kompleks yechimlarni yaratishga imkon beradi.

Xulosa

Ushbu maqolada sun'iy intellekt (SI) texnologiyalaridan pedagogik usullar bilan uyg'unlashtirilgan holda kompyuter tizimlari va tarmoqlarining kiberxavfsizligini ta'minlash uchun yangi algoritmlarni ishlab chiqish masalasi ko'rib chiqildi. Kiberxavfsizlik sohasidagi mavjud murakkab tahdidlar va ularni bartaraf etishda SIning muhim roli tahlil qilindi. Shuningdek, pedagogik yondashuvlarning kiberxavfsizlik bo'yicha bilim va ko'nikmalarni oshirish, xavfsiz xatti-harakat madaniyatini shakllantirishdagi ahamiyati alohida ta'kidlandi.

Tadqiqot doirasida SIning intruziv hujumlarni aniqlash, zararli dasturlarni detekt qilish, fishing hujumlariga qarshi kurashish, xavfsizlik zaifliklarini tahlil qilish va xavfsizlik choralarini avtomatlashtirish kabi kiberxavfsizlikning turli yo'nalishlarida qo'llanilish istiqbollari o'rganildi. Pedagogik usullar esa kiberxavfsizlik bo'yicha ta'lim berish, xavfsiz xatti-harakat ko'nikmalarini rivojlantirish va SIga asoslangan interaktiv ta'lim vositalarini yaratish uchun samarali instrument ekanligi ko'rsatib o'tildi.

Maqolada taklif etilgan yangi algoritmlar SIning analitik qobiliyatlarini pedagogikaning ta'limiy prinsiplari bilan integratsiya qilishga asoslangan. Bu yondashuv kiberxavfsizlikni ta'minlashda nafaqat texnologik yechimlarni, balki inson omilini ham hisobga olish imkonini beradi. Kelgusida ushbu algoritmlarning samaradorligini amaliyotda sinab ko'rish va ularni takomillashtirish muhim ahamiyatga ega.

Umuman olganda, sun'iy intellekt va pedagogikaning sinergiyasi kiberxavfsizlik sohasida yangi, samarali yechimlarni yaratish va malakali kadrlar tayyorlash uchun katta imkoniyatlar ochib beradi. Ushbu yo'nalishdagi tadqiqotlarni davom ettirish

kompyuter tizimlari va tarmoqlarining xavfsizligini yanada yuqori darajaga ko'tarishga xizmat qiladi.

Adabiyotlar ro'yhati:

1. Национальная стратегия развития информационного общества Республики Узбекистан на 2019-2021 годы. (O'zbekiston Respublikasi Prezidentining 2018 yil 21 noyabrdagi PQ-4007-son Qarori).
2. Florêncio, D., & Miller, S. P. (2010). Security and human behavior: Designing secure systems that people can use. *Foundations and Trends® in Privacy and Security*, *3*(1-2), 1-112.
3. Романюк, А. Н., & Тимошенко, А. В. (2017). Современные киберугрозы и методы борьбы с ними. *Информационная безопасность и технологии*, (4), 72-77.
4. Buczak, A. L., & Guvenen, O. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *6*(4), 278-310.
5. Furnell, S. M. (2017). Cyber security and human factors: Considerations for insider threats. *Information Security Technical Report*, *22*(1), 39-48.
6. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT press.
7. Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy. *Technical report*, Department of Computer Science, Chalmers University of Technology.
8. Chandrasekhar, P., & Raghuveer, K. (2019). A survey on machine learning techniques for intrusion detection systems. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(2S11), 233-237.
9. Gibert, D., Mateu, J., & Planes, J. (2016). Using data mining techniques for malware analysis. *Journal of Computer Virology and Hacking Techniques*, *12*(1), 1-12.
10. Alzahrani, A. I., & জানান, M. (2020). Deep learning approaches for malware analysis: A survey. *Journal of Information Security and Applications*, *50*, 102415.
11. А. А., & Петров, В. П. (2018). Методы и средства обнаружения фишинговых атак. *Информационные технологии*, (11), 64-69.
12. Rao, R. S., & Pais, A. R. (2019). Detection of phishing attacks using natural language processing and machine learning. *International Journal of Information Security and Privacy (IJISP)*, *13*(1), 47-64.
13. Li, Z., Zou, Y., Jin, S., & Wang, Z. (2020). A survey of software vulnerability detection based on machine learning. *IEEE Access*, *8*, 59978-59994.
14. С. Б., & Реагирование, И. (2019). Системы автоматизированного реагирования на инциденты информационной безопасности. *Вопросы кибербезопасности*, (3), 2-11.

15. Anderson, R. (2008). *Security engineering: A guide to building dependable distributed systems*. John Wiley & Sons.
16. Siponen, M., & Vance, D. P. (2014). Information security counter measures: Human, technical, and organizational perspectives. *Communications of the Association for Information Systems*, *34*(1), 10.
17. Gollmann, D. (2010). *Computer security*. John Wiley & Sons.
18. Шувалов, В. П., & Иванов, С. С. (2016). Формирование культуры информационной безопасности у пользователей. *Вестник Южно-Уральского государственного университета. Серия «Компьютерные технологии, управление, радиоэлектроника»*, *16*(1), 103-108.
19. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An investigation of antecedents and consequences. *Computers & Security*, *29*(8), 826-833.
20. Hwang, G. J., Xie, H., Zeng, Q., & Abelson, S. (2013). Investigating the impact of a mobile learning environment on students' learning achievements and motivations. *International Review of Research in Open and Distributed Learning*, *14*(5), 162-187.