SCIENCE HUB REVIEW
2026
Volume 1
Issue 5
www.sciencehubreview.uz
ILMIY ELEKTRON JURNAL

SUN'IY INTELLEKT ASOSIDA DASTURIY TA'MINOT XAVFSIZLIGINI TA'MINLASHNING ZAMONAVIY USULLARI VA ISTIQBOLLARI
СОВРЕМЕННЫЕ МЕТОДЫ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
MODERN METHODS AND PROSPECTS OF ENSURING SOFTWARE SECURITY BASED ON ARTIFICIAL INTELLIGENCE

Dehqonova Marjona Sherzodjon qizi

Talaba, Farg'ona davlat texnika universiteti, Farg'ona, O'zbekiston

marjonadeqonova@gmail.com

Annotatsiya

Ushbu maqolada sun'iy intellekt texnologiyalaridan foydalanish orqali dasturiy ta'minot xavfsizligini kuchaytirish yo'llari tahlil qilinadi. Statik va dinamik tahlil, zaifliklarni aniqlash, noodatiy faollikni kuzatish hamda kodni tekshirishda mashinaviy o'qitish imkoniyatlari ko'rib chiqiladi. Tadqiqot tizimli va qiyosiy tahlil usullariga asoslangan. Tahlil natijasida sun'iy intellekt xavfsizlik tekshiruvlarini tezlashtirishi va mutaxassisga yordam berishi, biroq inson nazorati o'rnini bosa olmasligi aniqlandi. Ma'lumotlar sifati, noto'g'ri ogohlantirishlar, izohlanuvchanlik va maxfiylik asosiy muammolar sifatida qayd etildi. Maqolada gibrid xavfsizlik yondashuvi bo'yicha takliflar beriladi.

Kalit so'zlar

sun'iy intellekt, dasturiy ta'minot xavfsizligi, mashinaviy o'qitish, zaifliklarni aniqlash, statik tahlil, dinamik tahlil, kiberxavfsizlik

Аннотация

В статье рассматриваются способы повышения безопасности программного обеспечения с использованием технологий искусственного интеллекта. Описаны возможности машинного обучения при статическом и динамическом анализе, выявлении уязвимостей, обнаружении аномальной активности и проверке программного кода. Исследование основано на системном и сравнительном анализе научных и методических источников. Показано, что искусственный интеллект способен ускорить проверки и поддержать работу специалиста, однако не заменяет человеческий контроль. В качестве основных проблем выделены качество данных, ложные срабатывания, объяснимость моделей и

конфиденциальность. Предложены рекомендации по применению гибридного подхода к обеспечению безопасности.
Ключевые слова
искусственный интеллект, безопасность программного обеспечения, машинное обучение, выявление уязвимостей, статический анализ, динамический анализ, кибербезопасность
Abstract
This article examines ways to improve software security through artificial intelligence technologies. It discusses the use of machine learning in static and dynamic analysis, vulnerability identification, anomaly detection, and code review. The study is based on systematic and comparative analysis of scientific and methodological sources. The analysis indicates that artificial intelligence can accelerate security checks and support specialists, but it cannot replace human oversight. Data quality, false alerts, model explainability, and confidentiality are identified as key challenges.
Recommendations for applying a hybrid security approach are proposed.
Keywords
artificial intelligence, software security, machine learning, vulnerability detection, static analysis, dynamic analysis, cybersecurity

Kirish

Raqamli texnologiyalar kundalik hayot, ishlab chiqarish, ta’lim, bank-moliya tizimi va davlat boshqaruvining ajralmas qismiga aylandi. Ushbu jarayonda dasturiy ta’minotning ishonchli ishlashi va unda saqlanadigan ma’lumotlarning himoyalanishi alohida ahamiyat kasb etmoqda. Dasturiy mahsulotlar ko‘lami kengaygani sari ularning ichki tuzilishi ham murakkablashmoqda. Ochiq kodli kutubxonalar, tashqi xizmatlar va turli dasturiy komponentlardan foydalanish ishlab chiqish jarayonini tezlashtiradi, biroq ular bilan bog‘liq xavfsizlik xatarlarini ham yuzaga keltiradi.

An’anaviy xavfsizlik tekshiruvlari — kodni qo‘lda ko‘rib chiqish, oldindan belgilangan qoidalar asosidagi statik tahlil va dastur ishga tushirilgandagi dinamik sinovlar — muhim vositalar hisoblanadi. Shunga qaramay, katta hajmdagi kodni muntazam tekshirish, yangi zaifliklarni erta aniqlash va noto‘g‘ri ogohlantirishlarni kamaytirish doim ham oson emas. Shu sababli sun’iy intellekt, xususan, mashinaviy o‘qitish va chuqur o‘qitish usullaridan foydalanishga qiziqish ortmoqda.

Mavzuning dolzarbligi shundaki, dasturiy ta’minot xavfsizligi faqat tayyor mahsulotni tekshirish bilan cheklanmaydi. Xavfsizlik talablari loyihalash, dasturlash, sinovdan o‘tkazish, joriy etish va keyingi texnik xizmat ko‘rsatish bosqichlarida ham hisobga olinishi lozim. NIST tomonidan ishlab chiqilgan Secure Software Development

Framework hujjatida ham xavfsiz dasturiy mahsulot yaratish amaliyotlarini butun ishlab chiqish hayotiy sikliga kiritish tavsiya etiladi [11].

Tadqiqotning maqsadi — sun’iy intellektdan foydalanish orqali dasturiy ta’minot xavfsizligini kuchaytirish yo‘llarini tahlil qilish, ularning imkoniyatlari va cheklovlarini aniqlash hamda amaliy tavsiyalar ishlab chiqish. Ushbu maqsadga erishish uchun quyidagi vazifalar belgilandi: sun’iy intellektning xavfsizlikdagi asosiy qo‘llanish yo‘nalishlarini ko‘rib chiqish; statik va dinamik tahlilda mashinaviy o‘qitish imkoniyatlarini tavsiflash; tahdidlarni aniqlash va zaifliklarni bashoratlash yondashuvlarini solishtirish; mavjud xatarlarni baholash; dasturiy ta’minot ishlab chiqish jarayoniga mos tavsiyalarni shakllantirish.

Tadqiqot obyekti — dasturiy ta’minotni ishlab chiqish va undan foydalanish jarayonida yuzaga keladigan xavfsizlik masalalari. Tadqiqot predmeti esa ushbu masalalarni hal etishda sun’iy intellekt usullaridan foydalanish imkoniyatlaridir.

Mavzuga oid adabiyotlar tahlili

Sun’iy intellekt va mashinaviy o‘qitish bo‘yicha fundamental manbalarda ma’lumotlardan qonuniyatlarni aniqlash, tasniflash va bashoratlash tamoyillari yoritilgan. Russell va Norvig sun’iy intellektni turli vazifalarni bajaruvchi intellektual agentlar nuqtayi nazaridan izohlaydi [1]. Goodfellow va hammualliflar chuqur o‘qitishning ko‘p qatlamli neyron tarmoqlar orqali murakkab belgilarni o‘rganish imkoniyatlarini bayon qiladi [2]. Bishop esa statistik o‘rganish, ehtimollik modellari va tasniflash usullarining nazariy asoslarini ko‘rsatadi [3]. Ushbu manbalar xavfsizlik vazifalarida qo‘llanadigan algoritmlarni tushunish uchun nazariy poydevor yaratadi.

Mashinaviy o‘qitish algoritmlarining amaliy qo‘llanilishi Hastie, Tibshirani va Friedman asarlarida batafsil ko‘rib chiqilgan [4]. Shalev-Shwartz va Ben-David mashinaviy o‘qitishning nazariy asoslari, umumlashtirish qobiliyati va modelni baholash masalalariga e’tibor qaratadi [5]. Chollet hamda Géronning qo‘llanmalari esa chuqur o‘qitish va amaliy mashinaviy o‘qitish modellarini yaratish jarayonini tushuntiradi [6; 7]. Sutton va Barto mustahkamlashtirilgan o‘qitish yondashuvlarini yoritib, muhit bilan o‘zaro ta’sir orqali qaror qabul qilish tamoyillarini bayon qiladi [8].

Dasturiy ta’minot xavfsizligi nuqtayi nazaridan NISTning SSDF hujjati muhim amaliy manba hisoblanadi. Unda xavfsiz dasturiy ta’minot ishlab chiqish uchun zarur bo‘lgan tashkiliy va texnik amaliyotlar, jumladan, xavfsizlik talablarini belgilash, ishlab chiqish muhitini himoyalash va komponentlar kelib chiqishini nazorat qilish masalalari keltirilgan [11]. OWASP Top 10 esa veb-ilovalarda keng uchraydigan xavfsizlik xatarlarini umumlashtiradi [12].

Chen va Babar tomonidan tayyorlangan ilmiy sharh mashinaviy o‘qitishga asoslangan dasturiy tizimlarni himoyalash, ularning zaifliklari va xavfsiz ishlab chiqish muammolarini tahlil qiladi [9]. Mazkur tadqiqotlar sun’iy intellektni xavfsizlik vazifalariga tatbiq etish bilan birga, sun’iy intellektning o‘zini ham himoyalash zarurligini ko‘rsatadi. Adabiyotlar tahlili shuni anglatadiki, samarali yechim bitta algoritmga tayanmasligi, balki dasturiy ta’minot hayotiy sikli, inson nazorati va an’anaviy xavfsizlik vositalarini birlashtirishi kerak.

Tadqiqot metodologiyasi

Maqola nazariy-tahliliy tadqiqot shaklida bajarildi. Tadqiqot davomida mavzuga oid ilmiy adabiyotlar, xalqaro tavsiyalar va dasturiy ta’minot xavfsizligiga doir ochiq metodik manbalar o‘rganildi. Asosiy usullar sifatida tizimli tahlil, qiyosiy tahlil, tasniflash va umumlashtirishdan foydalanildi. Bu yondashuvlar sun’iy intellektga asoslangan xavfsizlik vositalarining vazifalari, kuchli tomonlari va cheklovlarini bir-biri bilan taqqoslash imkonini berdi.

Tahlil bir necha bosqichda olib borildi. Birinchi bosqichda dasturiy ta’minot xavfsizligiga ta’sir qiluvchi asosiy muammolar ajratildi. Ikkinchi bosqichda sun’iy intellekt qo‘llanadigan yo‘nalishlar — kodni statik tahlil qilish, dinamik sinovlarni qo‘llab-quvvatlash, zararli yoki noodatiy xatti-harakatlarni aniqlash, zaifliklarni ustuvorlashtirish va kodni tekshirish — bo‘yicha guruhlandi. Uchinchi bosqichda har bir yo‘nalishning foydasi va ehtimoliy xatarlari baholandi.

Mazkur ishda yangi dasturiy mahsulot ustida laboratoriya tajribasi o‘tkazilgani yoki muayyan modelning aniqlik ko‘rsatkichi o‘lchangani da’vo qilinmaydi. Natijalar mavjud ilmiy va me’yoriy manbalarni tahlil qilish hamda ularni umumlashtirish asosida

shakllantirildi. Shu jihat tadqiqotning chegarasini belgilaydi: keltirilgan xulosalar amaliy tajriba natijasi emas, balki manbalar tahliliga asoslangan nazariy xulosalardir.

Tahlil va natijalar

1. Kodni statik tahlil qilish. Statik tahlil dastur ishga tushirilmasdan turib uning dasturiy kodini tekshirishga asoslanadi. An’anaviy vositalar oldindan belgilangan qoidalar, andozalar va ma’lum zaiflik belgilaridan foydalanadi. Mashinaviy o‘qitish yondashuvlari esa kodning sintaktik tuzilishi, operatorlar ketma-ketligi va ular o‘rtasidagi bog‘lanishlardan xususiyatlar ajratib, shubhali qismlarni tasniflashga yordam beradi. Bunda model dasturchi e’tiboridan chetda qolishi mumkin bo‘lgan murakkab bog‘lanishlarni ko‘rsatishi mumkin. Biroq model xulosasi yakuniy hukm emas: aniqlangan holat mutaxassis tomonidan tekshirilishi lozim.

2. Dinamik tahlil va sinovlarni qo‘llab-quvvatlash. Dinamik tahlilda dastur turli sharoitlarda ishga tushirilib, uning xatti-harakati kuzatiladi. Sun’iy intellekt sinov ma’lumotlarini tanlash, sinovlarni ustuvorlashtirish va bajarilish jarayonida to‘plangan ma’lumotlarni tahlil qilishda yordam berishi mumkin. Masalan, model ilgari kuzatilgan xatolarga o‘xshash holatlarni ajratib, tekshiruvchiga qaysi modulga ko‘proq e’tibor berish kerakligini ko‘rsatadi. Bu yondashuv sinov jarayonini maqsadli tashkil etishga xizmat qiladi, ammo barcha xatolarni topishni kafolatlamaydi.

3. Zararli dasturlar va noodatiy faollikni aniqlash. Mashinaviy o‘qitish modellari dastur yoki tizimning odatiy xatti-harakatlarini o‘rganib, undan keskin farq qiladigan holatlarni belgilashi mumkin. Tarmoq trafigi, tizim jurnallari va jarayonlar faolligi tahlil qilinib, shubhali o‘zgarishlar aniqlanadi. Bunday usul avvaldan ma’lum bo‘lmagan noodatiy holatlarni ham ko‘rsatishi mumkin. Shu bilan birga, odatiy ish jarayonidagi keskin o‘zgarishlar ham noto‘g‘ri ogohlantirishga sabab bo‘lishi ehtimoli mavjud.

4. Zaifliklarni ustuvorlashtirish. Katta dasturiy loyihalarda aniqlangan barcha muammolarni bir vaqtning o‘zida bartaraf etish imkoni bo‘lmasligi mumkin. Sun’iy intellekt zaiflikning turi, ta’sir doirasi, komponentning ahamiyati va mavjud kontekstni hisobga olib, tekshiruv navbatini shakllantirishga yordam beradi. Bunda model tavsiyasi xavf darajasini belgilashga ko‘maklashadi, lekin yakuniy qaror tashkilotning xavf siyosati va mutaxassis bahosiga asoslanishi kerak.

5. Kodni ko‘rib chiqish va tuzatish bo‘yicha tavsiyalar. Katta til modellari kodning vazifasini izohlash, ehtimoliy muammolarni ko‘rsatish va tuzatish variantlarini taklif qilishda qo‘llanishi mumkin. Bu ayniqsa dasturchi uchun dastlabki tahlilni tezlashtirishga yordam beradi. Biroq model taklif qilgan kod har doim ham to‘g‘ri yoki xavfsiz bo‘lavermaydi. Shuning uchun takliflar avtomatik ravishda asosiy tizimga kiritilmasdan, testdan o‘tkazilishi va mutaxassis tomonidan ko‘rib chiqilishi zarur.

Quyidagi jadvalda asosiy yo‘nalishlar, ularning amaliy foydasi va e’tibor talab qiladigan jihatlari umumlashtirilgan.

Jadval 1. Sun’iy intellektning dasturiy ta’minot xavfsizligidagi qo‘llanish yo‘nalishlari

Yo‘nalish	Amaliy foydasi	Cheklovi yoki xavfi
Statik tahlil	Koddagi shubhali qismlarni ajratish	Noto‘g‘ri ogohlantirishlar bo‘lishi mumkin
Dinamik tahlil	Sinovlarni maqsadli tanlash	Barcha holatlarni qamrab olmaydi
Anomaliyalarni aniqlash	Noodatiy faollikni ko‘rsatish	Odatiy o‘zgarishlar ham shubhali ko‘rinishi mumkin
Zaifliklarni ustuvorlashtirish	Muhim muammolarga avval e’tibor berish	Model bahosi mutaxassis tekshiruvini talab qiladi
Kod bo‘yicha tavsiya	Tuzatish variantlarini taklif qilish	Taklif qilingan kod sinovdan o‘tishi kerak

Jadval ma’lumotlari maqolada ko‘rib chiqilgan ilmiy manbalar va metodik tavsiyalar asosida muallif tomonidan umumlashtirildi.

Tahlil natijalarining muhokamasi

Tahlil shuni ko‘rsatadiki, sun’iy intellekt dasturiy ta’minot xavfsizligida bir necha vazifani qo‘llab-quvvatlaydi: katta hajmdagi ma’lumotlarni tez saralash, takrorlanuvchi belgilarni aniqlash, tekshiruvlarni ustuvorlashtirish va mutaxassisga qo‘shimcha tavsiyalar berish. Biroq bu imkoniyatlar xavfsizlikni to‘liq avtomatlashtirish degani emas. Model o‘qitilgan ma’lumotlar doirasidan tashqaridagi holatlarda xato qilishi, noto‘g‘ri ogohlantirish berishi yoki ayrim muammolarni sezmay qolishi mumkin.

Birinchi muhim muammo — ma’lumotlar sifati. Agar o‘qitish to‘plamida ayrim dasturlash tillari, kod uslublari yoki zaiflik turlari yetarli aks etmasa, modelning natijasi ham bir tomonlama bo‘lishi mumkin. Ikkinchi muammo — izohlanuvchanlik. Xavfsizlik bo‘yicha qaror nima sababdan chiqarilganini tushunish muhim, chunki noto‘g‘ri qaror

tizimning ishlashiga va foydalanuvchi ma’lumotlariga ta’sir qilishi mumkin. Uchinchi muammo — modelning o‘ziga qaratilgan hujumlar va ma’lumotlarni buzib ko‘rsatish ehtimoli. Shu bois modelni ishlab chiqish, o‘qitish va amaliyotga joriy etish jarayonlarining o‘zi ham xavfsizlik nazoratidan o‘tishi kerak.

Yana bir masala — maxfiy kod va ma’lumotlarni tashqi xizmatlarga yuborish bilan bog‘liq xavf. Tashkilotlar sun’iy intellekt xizmatidan foydalanishdan oldin ma’lumotlarni qayta ishlash qoidalari, saqlash muddati, kirish huquqlari va maxfiylik shartlarini o‘rganishi lozim. Ayniqsa, tijorat siri yoki shaxsiy ma’lumotlar mavjud bo‘lgan kodni ruxsatsiz tashqi tizimlarga yuborish mumkin emas.

Shu asosda eng maqbul yondashuv gibrid model hisoblanadi. Unda statik va dinamik tahlil kabi an’anaviy vositalar sun’iy intellekt tavsiyalari bilan birga ishlaydi, yakuniy qaror esa mutaxassis tomonidan qabul qilinadi. Bunday tashkil etish avtomatlashtirishning afzalliklaridan foydalanish bilan birga, inson nazoratini saqlab qoladi.

Xulosa va takliflar

O‘rganilgan manbalar va o‘tkazilgan tahlil asosida sun’iy intellekt dasturiy ta’minot xavfsizligini kuchaytirishda muhim yordamchi vosita bo‘lishi mumkin, degan xulosaga kelindi. Mashinaviy o‘qitish koddagi shubhali belgilarni aniqlash, tizim xatti-harakatlarini kuzatish, sinov jarayonini maqsadli tashkil etish va zaifliklarni ustuvorlashtirishda qo‘llanadi. Katta til modellari esa kodni tushuntirish va tuzatish bo‘yicha dastlabki tavsiyalar berishi mumkin.

Shu bilan birga, sun’iy intellekt vositalarining natijalariga to‘liq tayanish to‘g‘ri emas. Ma’lumotlar sifati, noto‘g‘ri ogohlantirishlar, modelning izohlanishi, maxfiylik va model xavfsizligi bilan bog‘liq masalalar doimiy nazoratni talab qiladi. Demak, sun’iy intellekt an’anaviy xavfsizlik usullarining o‘rnini to‘liq egallamaydi, balki ularning imkoniyatlarini kengaytiradi.

Tahlil natijalaridan kelib chiqib, quyidagi takliflar ishlab chiqildi: birinchidan, xavfsizlik talablarini dasturiy mahsulotni loyihalash bosqichidayoq belgilash; ikkinchidan, kodni statik va dinamik tekshirish vositalarini sun’iy intellektga asoslangan tahlil bilan uyg‘unlashtirish; uchinchidan, model aniqlagan muammolarni mutaxassis

tekshiruvidan o‘tkazish; to‘rtinchidan, o‘qitish va sinov ma’lumotlarining sifati hamda yangilanishini nazorat qilish; beshinchidan, maxfiy kodni tashqi xizmatlarga yuborishdan oldin tashkilot xavfsizlik siyosatini tekshirish; oltinchidan, sun’iy intellekt tizimlarining o‘zini ham muntazam audit qilish.

Kelgusidagi tadqiqotlarda turli dasturlash tillari va loyihalarida sun’iy intellekt vositalarining samaradorligini tajriba asosida baholash, noto‘g‘ri ogohlantirishlar ulushini o‘rganish hamda o‘zbek tilidagi texnik hujjatlar va dasturiy loyihalar uchun moslashtirilgan ma’lumotlar to‘plamlarini shakllantirish maqsadga muvofiq. Bu yo‘nalishlar dasturiy injiniring va kiberxavfsizlik sohalarida amaliy ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Pearson, 2020.

2. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.

3. Bishop C. M. Pattern Recognition and Machine Learning. Springer, 2006.

4. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning. 2nd ed. Springer, 2009.

5. Shalev-Shwartz S., Ben-David S. Understanding Machine Learning: From Theory to Algorithms. Cambridge University Press, 2014.

6. Chollet F. Deep Learning with Python. 2nd ed. Manning, 2021.

7. Géron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. 3rd ed. O’Reilly, 2022.

8. Sutton R. S., Barto A. G. Reinforcement Learning: An Introduction. 2nd ed. MIT Press, 2018.

9. Chen H., Babar M. A. Security for Machine Learning-based Software Systems: A Survey of Threats, Practices, and Challenges. ACM Computing Surveys, 2024, Vol. 56, No. 6, Article 151.

10. OWASP Foundation. OWASP Top 10: The Ten Most Critical Web Application Security Risks. 2021.

11. Scarfone K., Souppaya M., Dodson D. Secure Software Development Framework (SSDF) Version 1.1. NIST Special Publication 800-218, 2022.

12. Booth H., Souppaya M., Vassilev A., et al. Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile. NIST SP 800-218A, 2024.