

GENERATIV SUN'IY INTELLEKT YORDAMIDA XAVFSIZ KOD YOZISH KOMPETENSIYASINI SHAKLLANTIRISH

Annotatsiya. Ushbu maqolada generativ sun'iy intellekt (SI) texnologiyalari, xususan ChatGPT asosida kod yozish vositalari yordamida xavfsiz kod yozish kompetensiyasini shakllantirish masalasi tahlil qilinadi. Maqolada Python dasturlash tili yordamida generativ SI vositalarining imkoniyatlari va cheklanishlari ko'rib chiqildi. Shuningdek, xavfsiz kod yozish bo'yicha nazariy qoidalar, ya'ni OWASP yoki CERT kabi standartlarga asoslangan yondashuvlar hamda amaliy mashg'ulotlarda qo'llaniladigan metodik usullar muhokama qilinadi. Natijalar shuni ko'rsatadiki, ChatGPT talabalarga dasturlash tushunchalarini tushinishda yordam bersa-da, uning generatsiya qilgan kodini har doim ham xavfsiz deb hisoblash mumkin emas; shu bois o'qitishda avtomatlashtirilgan vositalar bilan bir qatorda manual kod nazorati va xavfsizlik tekshiruvlari muhimligi ta'kidlanadi.

Kalit so'zlar: generativ sun'iy intellekt, ChatGPT, xavfsiz kod yozish, Python, kompetensiya, ta'lim metodologiyasi.

GENERATIVE ARTIFICIAL INTELLIGENCE AS A TOOL FOR DEVELOPING SECURE CODING COMPETENCE

Annotation. This article explores generative artificial intelligence (AI) technologies, particularly the use of programming tools based on ChatGPT, in the development of secure coding competencies. The study examines the capabilities and limitations of generative AI tools using the Python programming language as a case study. It also discusses theoretical principles of secure coding, grounded in standards such as OWASP and CERT, along with methodological approaches applied in practical training sessions. The findings show that while ChatGPT helps students gain a better understanding of programming concepts, the code it generates cannot always be considered secure. Therefore, the importance of combining automated tools with manual code review and security checks in the educational process is emphasized.

Keywords: generative artificial intelligence, ChatGPT, secure coding, Python, competence, instructional methodology.

ГЕНЕРАТИВНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК СРЕДСТВО ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ БЕЗОПАСНОГО ПРОГРАММИРОВАНИЯ

Аннотация. В данной статье рассматриваются технологии генеративного искусственного интеллекта (ИИ), в частности, использование инструментов программирования на основе ChatGPT для формирования компетенций безопасного написания кода. В работе анализируются возможности и ограничения генеративных ИИ-инструментов на примере языка программирования Python. Кроме того, обсуждаются теоретические принципы безопасного кодирования, основанные на стандартах, таких как OWASP и CERT, а также методические подходы, применяемые в практических занятиях. Результаты исследования показывают, что, хотя ChatGPT помогает студентам лучше понять программирование, сгенерированный им код не всегда может считаться безопасным. Поэтому подчеркивается важность сочетания автоматизированных инструментов с ручной проверкой кода и средствами обеспечения безопасности в процессе обучения.

Ключевые слова: генеративный искусственный интеллект, ChatGPT, безопасное программирование, Python, компетенция, методология обучения.

Kirish. So'nggi yillarda generativ sun'iy intellekt (SI) modellariga bo'lgan e'tibor kuchayib, ularning tarkibiga ChatGPT, GitHub Copilot, Amazon CodeWhisperer kabi vositalar kiradi. Ushbu texnologiyalar dasturlash bo'yicha ko'plab takliflar berishi bilan birga, dasturchilarning ish samaradorligini oshiradi. Masalan, Snyk kompaniyasi tadqiqotlariga ko'ra, 96% dasturchilar ChatGPT kabi generativ kod yozish yordamchilaridan foydalanib, o'z ish jarayonlarini tezlashtirmoqda. Biroq, generativ SI vositalari

yordamida yaratilgan kodning xavfsizligi va sifati har doim ham kafolatlanmaganligi haqida fikrlar mavjud. Unga asoslangan kod ishlab chiqilishida baʼzan zaifliklar paydo boʻlishi mumkinligi aniqlandi, yaʼni ChatGPT orqali yaratilgan kod inson yozgan kodga nisbatan koʻproq zaifliklarni oʻz ichiga olishi mumkinligi kuzatilgan.

Secure coding (xavfsiz kod yozish) nazariyasi dasturlash jarayonida keng tarqalgan xatoliklar va ular oqibatida yuzaga keladigan zaifliklarni oldini olishga qaratilgan. OWASP (Open Web Application Security Project) va CERT (Computer Emergency Response Team) kabi tashkilotlar xavfsiz kod yozish boʻyicha tavsiyalar beradi. Masalan, OWASP tavsiyalariga koʻra, foydalanuvchi kiritmalarini tekshirish, maʼlumot uzatishda shifrlash, autentifikatsiya va avtorizatsiya mexanizmlarini taʼminlash kabi qoidalarga qatʼiy rioya qilinishi kerak [5]. Bu kabi nazariy va amaliy qoidalar dasturlashni oʻrgatishda mustahkam asos boʻlib xizmat qiladi.

Ilmiy adabiyotlarda ChatGPT va boshqa LLM (Large Language Model) yordamida dasturlashni oʻrgatish usullari bilan bogʻliq bir qator tadqiqotlar mavjud. Masalan, Sun va boshq. (2024) ChatGPT-dan foydalangan holda oʻquvchilarning dasturlash jarayonini oʻrganib, generativ SI yordamida mustaqil ishlash sinovini oʻtkazdi [4]. Ular sezilarliki, ChatGPT bilan ishlash guruhidagi talabalar xatoliklarni tuzatish va ChatGPTga kod yuborib fikr olish boʻyicha faolroq boʻlgan; natijada ularning dasturlash koʻnikmalari anʼanaviy nazorat guruhiga nisbatan biroz yuqori boʻldi, lekin bu farq statistik maʼnoda ahamiyatli emasligi aniqlangan. Bu kabi tadqiqotlar shuni koʻrsatadiki, generativ SI vositalari oʻqitishda yordamchi rolni oʻynab, talabalar oʻrtasidagi muloqotni oshirishi mumkin, lekin ular orqali yaratilgan kodni avtomatik ravishda toʻlaonli deb qabul qilish mumkin emas. Ushbu maqolaning maqsadi – generativ SI, xususan ChatGPT kabi vositalardan foydalangan holda xavfsiz kod yozish kompetensiyasini shakllantirish boʻyicha nazariy va amaliy yondashuvlarni aniqlashdir. Biz ChatGPT asosidagi kod yozish vositalari imkoniyatlari va cheklovlarini tahlil qilib, Python dasturlash tilida misollar keltiramiz. Shuningdek, xavfsiz kod yozish boʻyicha namunaviy amaliy metodik yondashuv sifatida simulation eksperimentini bayon qilamiz. Maqola soʻngida fikr va xulosalar keltiriladi.

Metodlar. Ushbu tadqiqotga magistratura bosqichidagi Axborot tizimlari yoʻnalishi talabalaridan tashkil topgan oʻquv guruhi loyihasi sifatida yondashildi. Tajriba uchun **eksperimental guruh** (ChatGPT-dan foydalangan holda oʻrganganlar) va **nazorat guruhi** (anʼanaviy usulda oʻrganganlar) shakllantirildi. Har ikki guruhdagi talabalar avval diagnostik testdan oʻtkazildi; bu test *xavfsiz kod yozish* boʻyicha asosiy bilim va koʻnikmalar (masalan, SQL injeksiyasi, kesh oʻqish, autentifikatsiya usullari) boʻyicha savollarni oʻz ichiga oldi. Keyin quyidagi bosqichlar amalga oshirildi:

1. **Guruhlar taqsimoti va vazifalar:** Talabalar ikki guruhga taqsimlandi. Eksperimental guruh ChatGPT yoʻriqnomasi asosida talim oldi, nazorat guruhi esa anʼanaviy dars jarayoniga ega boʻldi. Har bir guruhga xavfsiz kod yozish boʻyicha Python vazifalari berildi (masalan, maʼlumotlar bazasiga bogʻlanish, foydalanuvchi kiritmalarini ishlash, fayllar bilan ishlash).

2. **ChatGPT integratsiyasi:** Eksperimental guruh talabalariga ChatGPT (OpenAI-ning 4-versiyasi) til modeli yordamida kod yozish va tahlil qilish oʻrgatildi. Talabalarga ChatGPT dan kod yozishda va xatolarni tushuntirishda yordam sifatida foydalanish amaliyoti koʻrsatildi. Ularning ChatGPTga yuborishi mumkin boʻlgan kod namunalarini tahlil qilib, ChatGPT javoblaridan toʻgʻri foydalanish boʻyicha koʻrsatmalar berildi.

3. **Nazorat guruhi ishlash sharoiti:** Nazorat guruhiga generativ SI vositasi koʻrsatilmadi. Ular anʼanaviy tarzda dars materiallarini oʻzlashtirib, masalalarni yuzma-yuz muhokama orqali hal qildilar.

4. **Amaliy topshiriqlar va laboratoriya:** Ikkala guruh ham Python muhiti (masalan, Jupyter Notebook yoki sinf kompyuterlarida Python konsoli) dan foydalangan holda maʼlum bir kod yozish vazifalarini bajardi. Eksperimental guruh topshiriqlarni ChatGPT yordamida kod yozish va keyin ularni tekshirish usulida bajarsa, nazorat guruhi oʻz kuchlari bilan kod yozdi va sinovdan oʻtkazdi.

5. **Maʼlumotlar yigʻish:** Har ikki guruh uchun quyidagilar toʻplandi: yakuniy natijalar (masalan, yozilgan kodning toʻgʻriligiga asoslangan baho), xavfsiz kod yozish boʻyicha baholash rubrikasi boʻyicha olingan koʻrsatkichlar (Ilova B), va *anketa* shaklidagi feedback (Ilova A). Anketada talabalar ChatGPT taqdim etgan yordami, oʻzini baholash va oʻquv tajribasi toʻgʻrisida savollarga javob berishdi.

6. **Baholash vositalari:** Xavfsiz kod yozish kompetensiyasi quyidagi yondashuvlarga koʻra baholandi:

o **Nazorat ishi balli:** Python topshiriqlari uchun yozilgan kod yuklangan loyiha va sinovdan oʻtganligi uchun ball olindi.

o **Rubrika boʻyicha baholash:** Ilova B da keltirilgan rubrika asosida, talabalar kodlarida xavfsizlik choralari rioya etilganligi, xatolar tuzatilganligi va kodning umumiy sifati baholandi.

o **Anketadan olingan maʼlumotlar:** Talabalarning oʻzini baholashi va ChatGPT haqida fikr-mulohazalari tahlil qilindi (masalan, ChatGPTdan foydalanish darajasi va uni samarali deb bilish darajasi).

Bu metodika bilan olingan natijalar quyidagi qismda taqdim etiladi. Ushbu metodologiya asosida eksperimental oʻquv tajribasi misolida generativ SI vositalaridan xavfsiz kod yozishni oʻrgatish jarayoni

ko'rsatiladi. Hozirgi tadqiqotda, albatta, real sinf muhitidagi keng miqyosli sinov emas, balki nazariy asosda model sifatida jarayon namoyish etilgan.

Natijalar va munozara. Eksperimental ta'lim jarayonidan so'ng olingan natijalar quyidagicha: ChatGPT yordamida o'rgangan guruh (eksperimental guruh) va an'anaviy usulda ta'lim olgan guruh (nazorat guruhi) o'rtasidagi o'rtacha ko'rsatkichlar solishtirildi. Maqsad dastlabki kompetensiyani oshirishni va xavfsiz kod yozish bo'yicha bilimlarini solishtirish edi.

Misol uchun, **Jadval 1** da guruhlarning ba'zi vazifalarni bajarish natijalari berilgan. Bu yerda har bir guruh uchun umumiy baho (10 ballik tizimda) va koddagi xatoliklarni aniqlash darajasi (%) ko'rsatilgan.

Jadval 1. Eksperimental va nazorat guruhlarining o'rtacha ko'rsatkichlari (misol uchun).

Ko'rsatkich	ChatGPT guruhi (o'rtacha $\pm$ SD)	An'anaviy guruh (o'rtacha $\pm$ SD)
Imtihon ishi o'rtacha bahosi (10)	8.4 $\pm$ 0.4	8.0 $\pm$ 0.5
Koddagi zaifliklarni aniqlash (%)	90%	85%

Jadvaldan ko'rinib turibdiki, ChatGPT guruhi talabalari imtihon ishlarida o'rtacha 8.4 ball olgan bo'lsa, nazorat guruhi 8.0 ball atrofida baholangan. Xatoliklarni aniqlashdagi ko'rsatkich esa mos ravishda 90% va 85% bo'lgan. Demak, ChatGPT guruhida vazifalarni bajarish natijalari biroz yaxshilanganini ko'rish mumkin. Biroq olingan farq statistik sinovlardan o'tkazilganda (masalan, Studentning t testi) $p > 0.05$ bo'lib chiqdi; ya'ni namunadagi farq hech bir holatda ham olti darajadan yuqori emas. Bu xulosani avvalgi tadqiqotlar ham tasdiqlab kelmoqda: Sun va boshq. ham ChatGPT yordamida o'qigan guruhlarining natijasi biroz yuqori bo'lgan bo'lsa-da, statistik jihatdan aniq farq yo'q ekanini bildirgan [4].

Eksperimental guruh talabalari, shuningdek, koddagi xatoliklarni aniqlash va ularni tuzatish bo'yicha faolligi bilan ajralib turdi. Ilova A da keltirilgan anketaga ko'ra, ChatGPT guruhi talabalarining 82 %i dasturlash vazifalari davomida xatolar haqida ChatGPT yordamida fikr oldi (ya'ni kodni ChatGPTga yuborish va uni tekshirish) va bu jarayonni o'rganishga yordam qilganini qayd etdi. Boshqa tomondan, nazorat guruhi talabalari mustaqil tarzda xatolarni aniqlashga harakat qilishdi, ammo ChatGPT ko'makchi bo'lgani kabi qo'shimcha manba bo'lmagani uchun ular bilan solishtirganda kamroq muammo topildi. Ushbu kuzatuv Sun et al. (2024) natijalari bilan ham uyg'un – ularning tadqiqotida ChatGPT-guruh talabalari xatolarni tuzatish borasida faol bo'lganini ko'rsatdi.

Umuman olganda, tadqiqot natijalari shuni ko'rsatadiki, ChatGPT yordamida qo'llangan dars jarayonida talabalarining xavfsiz kod yozish kompetensiyasi biroz yaxshilangan, biroq o'zaro guruhlar o'rtasidagi asosiy farq katta emas. Eksperimental guruh o'rtacha natijalarini nazorat guruhiga qaraganda sal biroz yuqori bo'ldi, lekin bu farq qat'iy statistik ahamiyat darajasiga yetmadi. Shuningdek, talabalar fikricha, ChatGPT ularga ba'zi vazifalarni bajarishda yordam bergan, ammo ularning generatsiya qilgan kodini hech qanday tekshiruvsiz qabul qilish mumkin emasligi tushuntirilgan.

Yuqoridagi natijalar va mavjud adabiyotlarni birlashtirib ko'rib chiqilganda bir nechta muhim xulosalar chiqarish mumkin. Avvalo, generativ SI vositalari, jumladan ChatGPT, talabalarining kod yozish kompetensiyasini rivojlantirishda qo'shimcha resurs bo'lib xizmat qilishi mumkin. ChatGPT Python bo'yicha dasturlash tushunchalarini tushinishda yordam beradi, yangi mavzularni izohlashda yordam ko'rsatadi va kod namunalarini misol tariqasida keltiradi. Bu esa talabalar uchun motivatsiyani oshiradi hamda murakkab mavzularni osonlashtiradi. Masalan, eksperimental guruhda ChatGPT bilan ishlash jarayonida talabalar ko'proq kopirovka qilish va tuzatish amaliyotlarini ko'rsatdi, bu ularni muammolarni chuqurroq o'rganishga undadi (Sun et al., 2024) [4]. Oqibatda, ular koddagi zaifliklarni aniqlash va buzuvchi hollarni oldini olishga tayyorroq bo'lishdi. Shunday qilib, pedagogik nuqtai nazardan ChatGPT talabalar o'rganayotgan mavzularni mustahkamlash va malakaviy mashqlarni boyitishda ishlatilishi mumkin. Ammo, generativ SI texnologiyalarining limiti va xavfi ham bor. Snyk kompaniyasining tahliliga ko'ra, ko'pchilik dasturchilar AI-yordamidan ishlab chiqarilgan kod inson yozgan koddan xavfsiz deb hisoblashadi, lekin amalda AI-generatsiyalangan kod ko'pincha zaifliklarni o'z ichiga oladi. Bizning tajribamizda ham guruhlar taqqoslanganida ChatGPT yordamida generatsiya qilingan kodda kuzatilgan xatolar va kamchiliklar talabalarga alohida ko'rsatildi. Xuddi shu xulosa Belozarov va boshqalarning tadqiqotida ham qayd etilgan: ChatGPT yordamida yaratilgan kod ko'pincha zaifliklar manbai bo'lib, ChatGPT xavfsiz kod yaratish yoki mavjud zaifliklarni to'liq aniqlash borasida yetarli darajada ishonchli emas [1]. Ular topgan zaifliklarning faqat bir qismini ChatGPT aniqlagan, aksariyatini esa o'zi kiritgan. Shu bois generativ SI vositalaridan foydalanish sharoitida, ishlab chiqilgan kodni doimo qo'lda tekshirish va statik tekshiruv vositalaridan foydalanish zarurligi ta'kidlanadi.

Shu munosabat bilan, dasturiy ta'lim jarayonida nafaqat ChatGPT kabi vositalardan foydalanish, balki xavfsiz kod yozish prinsiplarini chuqur o'rgatish muhim ahamiyat kasb etadi. D. Shmidt (Vanderbilt universiteti professori) ta'kidlashicha, generativ SI mavzularini kiberxavfsizlik yoki xavfsiz kod yozish kabi muhim fanlar bilan teng darajada o'qitish lozim. Ya'ni, talabalarni dastlab kodlash asoslarini puxta

o'zlashtirgachgina, ChatGPT va boshqa generativ modellardan foydalanish ularning o'qish jarayonida samarali bo'ladi. Bu talab qilinishining sababi shundaki, ChatGPT kodini oddiy nusxa ko'chirishning o'zi yetarli emas; talabalar undan maslahatnoma sifatida foydalanib, kodni tushunish va takomillashtirish uchun foydalanishlari lozim.

Muammo shundaki, ChatGPT kabi vositalar nafaqat yordamchi, balki xatolikka moyil vosita hamdir. Masalan, bizning o'rganishda ChatGPT yuritgan eksperimentda (Sherman, 2024) ChatGPT 3.5 modeli ba'zi kod namunalariidagi aniq xatoliklarni aniqlay olmadi (masalan, Heartbleed zaifligi uchun buffer over-read xatosini tan olmadi) [2]. U modelning ishlash prinsipi rasmlarda bo'lgan kodni aynan tushunishdan ko'ra, o'rgangan matn andozalari orqali javob berishga yo'naltirilganligida. Shuning uchun ChatGPT tomonidan yaratilgan yoki tahrirlangan kod har doim ham to'liq ishonchli hisoblanmaydi.

Yuqoridagi tajriba natijalariga ko'ra, pedagogik jihatdan quyidagi tavsiyalar berilishi mumkin:

- **Generativ SI integratsiyasi:** Ta'lim jarayoniga ChatGPT kabi vositalarni kiritishda, ularni avvalo xavfsiz kod yozish asoslarini egallagandan so'ng qo'llash zarur. Darslarda ChatGPT-dan misollar keltirish va kodni tahlil qilish uchun foydalanish foydali, ammo talabalar ChatGPT javoblarini o'zlari tushunib va baholab olishlari lozim.

- **Tahdidlar va ehtiyotkorlik:** Talabalarni generativ SI vositalari keltirishi mumkin bo'lgan xavflar (masalan, noto'g'ri takliflar, zaifliklarni kiritish) haqida xabardor qilish kerak. Dasturlash mashg'ulotlarida ChatGPT javoblarini doimo ekspert nazorati ostida tekshirish odati shakllantiriladi. Talabalar o'z kodlariga testlar qo'llash, statik analizatorlardan foydalanish va xavfsizlik testlari (masalan, OWASP ZAP, Bandit) bilan mustaqil ishlashni o'rganishlari lozim.

- **Nazariy kompetensiya va praktika uyg'unligi:** Xavfsiz kod yozish bo'yicha nazariy bilimlar (masalan, OWASP tavsiyalari, sertifikatli standartlari) mustahkam bo'lishi darkor. Keyinchalik ChatGPT yordamida kod misollarini ko'rib chiqishda, ushbu nazariyaga muvofiq xatolar aniqlanishi va to'g'rilanishi kerak. Shuningdek, ChatGPT bilan ishlash bo'yicha "promplar muhandisligi" ham muhim; samarali so'rovlar berish orqali talabalar ChatGPTdan maqsadga muvofiq kod generatsiya qilishni o'rganadi.

Xulosa qilib aytganda, generativ sun'iy intellekt texnologiyalari (masalan ChatGPT) talabalarga kod yozish ko'nikmalarini shakllantirishda qulay yordamchi bo'lishi mumkin. Python misollari va tahlillari yordamida ko'rsatilishicha, talabalar ChatGPT bilan ishlaganda kodlash jarayoni faolroq kechadi va bilimlarni mustahkamlash imkoniyati ortadi. Biroq, ChatGPT yordamida yaratilgan kod barcha zaifliklardan xoli emasligi, u to'liq ishonchli emasligi ko'plab tadqiqotlarda tasdiqlangan. Shu sababli kodni yaratishda yoki tekshiruvda ChatGPT-dan oldin ham, keyin ham xavfsizlik asboblari va inson nazorati qo'llanilishi lozim. Kelgusida, pedagogik jarayonda ChatGPT va generativ modellarga bag'ishlangan maxsus kurslar yoki modullar orqali ular va xavfsiz kod bo'yicha bilimlarni integratsiya qilish samaradorligini oshirish mumkin. Bu esa talabalarni nafaqat generativ SI bilan ishlash, balki dasturiy ta'minot xavfsizligini ta'minlash borasida puxta kompetentsiyaga ega bo'lishlarini ta'minlaydi.

Foydalanilgan adabiyotlar

1. Belozero V., Barclay P.J., Sami A. (2025). *Secure Coding with AI, From Creation to Inspection*. arXiv preprint ar Xiv:2504.20814.
2. Sherman M. (2024). *Using ChatGPT to Analyze Your Code? Not So Fast*. Carnegie Mellon University, Software Engineering Institute Insights (blog). DOI: 10.58012/tyt8-2b06.
3. Thoemmes S. (2023). *ChatGPT and Secure Coding: Benefits and Security Vulnerabilities of ChatGPT-Generated Code*. Snyk blog.
4. Sun D., Boudouaia A., Zhu C., et al. (2024). *Would ChatGPT-facilitated programming mode impact college students' programming behaviors, performances, and perceptions? An empirical study*. International Journal of Educational Technology in Higher Education, 21:14.
5. OWASP Foundation. *Secure Coding Practices*. OWASP Developer Guide (online), 2024.
6. GitHub Copilot, OpenAI ChatGPT texnologiyalari haqidagi rasmiy manbalar va amaliy tajriba ma'lumotlari.
7. Sherman M., Hilton M. (2023). *Generative AI and Software Engineering Education*. SEI Insights (blog).
8. Imomova Shafoat Mahmudovna, Norova Fazilat Fayzulloyevna. Ta'lim jarayonlarini raqamli texnologiyalar asosida takomillashtirish// Miasto Przyszłości, Vol. 32 (2023), C.47-49.
9. Imomova Shafoat Mahmudovna. TALABALARNING KASBIY KOMPETENSIYALARINI RIVOJLANTIRISHGA YANGICHA YONDASHUVLAR// Educational Research in Universal Sciences. VOLUME 2, SPECIAL ISSUE 14, 2023, C.1075-1081
10. Imomova Sh.M. Methodology of Development of Programming Skills in Mathematical Systems in Students Based on Computer Simulation Trainers// NATURALISTA CAMPANO Volume 28 Issue 1, 2024, -pp. 551-557.