O‘ZBEKISTON MILLIY UNIVERSITETI XABARLARI, 2026, [10]
ISSN 2181-7324(Print)

IJTIMOIY FANLAR
http://journals.nuu.uz
ISSN 3093-8996(Onlayn)

UDK: 004.8:004.056:37.01

Ma’murjon DAVRONOV,
Dotsent, Sarbon universiteti, Toshkent, O‘zbekiston
E-mail: davronovmamurjon@gmail.com, https://ORCID.org/0000-0003-0594-744X
Dadanur SHUKUROV,
Katta o‘qituvchi, Sarbon universiteti, Toshkent, O‘zbekiston
E-mail: dadanur0094@gmail.com, https://ORCID.org/0009-0001-9802-4793
Yusupali MINAMATOV,
O‘qituvchi, Sarbon universiteti, Toshkent, O‘zbekiston
E-mail: minamatovyu@gmail.com, https://ORCID.org/0000-0003-0594-744X

Dotsent M.Mannanov taqrizi asosida

PEDAGOGICAL PRINCIPLES OF ENSURING INFORMATION SECURITY USING ARTIFICIAL INTELLIGENCE

Annotation

This article examines the pedagogical principles of ensuring information security through artificial intelligence in higher education. The study treats AI not only as a technical tool, but also as a didactic environment for developing risk thinking, ethical responsibility, data culture and practical cybersecurity competence. Based on literature review, comparative analysis and pedagogical modeling, a principle-based model is proposed for curriculum design, laboratory tasks and assessment.

Key words: artificial intelligence, information security, cybersecurity education, pedagogical principles, digital competence, risk-based learning, data protection, ethical AI.

ПЕДАГОГИЧЕСКИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация

В статье рассматриваются педагогические принципы обеспечения информационной безопасности с использованием искусственного интеллекта в высшем образовании. ИИ трактуется не только как технический инструмент, но и как дидактическая среда, развивающая риск-ориентированное мышление, этическую ответственность, культуру данных и практические компетенции. На основе обзора литературы, сравнительного анализа и педагогического моделирования предложена модель для учебных программ, лабораторных заданий и оценивания.

Ключевые слова: искусственный интеллект, информационная безопасность, образование в области кибербезопасности, педагогические принципы, цифровая компетентность, риск-ориентированное обучение, защита данных, этический ИИ.

SUN’IY INTELLEKT YORDAMIDA AXBOROT XAVFSIZLIGINI TA’MINLASHNING PEDAGOGIK TAMOYILLARI

Annotatsiya

Mazkur maqolada oliy ta’lim muhitida sun’iy intellekt yordamida axborot xavfsizligini ta’minlashning pedagogik tamoyillari tahlil qilinadi. Sun’iy intellekt texnik himoya vositasi bilan birga xavfni anglash, ma’lumotlar madaniyati, kiberxavfsizlik etikasi va amaliy kompetensiyani rivojlantiruvchi didaktik muhit sifatida talqin qilinadi. Adabiyotlar sharhi, qiyosiy tahlil va pedagogik modellashtirish asosida o‘quv dasturi, laboratoriya va baholash uchun tamoyilga asoslangan model taklif etildi.

Kalit so‘zlar: sun’iy intellekt, axborot xavfsizligi, kiberxavfsizlik ta’limi, pedagogik tamoyillar, raqamli kompetensiya, xavfga yo‘naltirilgan ta’lim, ma’lumotlarni himoya qilish, etik sun’iy intellekt.

Kirish. Raqamli iqtisodiyotning jadal rivojlanishi, ta’lim jarayonining elektron axborot-ta’lim muhitiga ko‘chishi, masofaviy xizmatlar va bulutli platformalardan keng foydalanish axborot xavfsizligi masalasini ta’lim tizimining asosiy pedagogik vazifalaridan biriga aylantirdi. Bugungi kunda axborot xavfsizligini ta’minlash faqat tarmoq administratorlari yoki dasturchilar vazifasi emas; u har bir pedagog, talaba va boshqaruv xodimining raqamli madaniyati bilan chambarchas bog‘liq ijtimoiy-pedagogik jarayondir. Shu jihatdan sun’iy intellekt vositalari yordamida axborot xavfsizligini o‘rgatish nafaqat texnik bilim berishni, balki xavfni oldindan ko‘ra olish, ma’lumot bilan mas’uliyatli ishlash, yolg‘on yoki zararli kontentni tanib olish, shaxsiy va korporativ ma’lumotlarni himoya qilish ko‘nikmalarini rivojlantirishni ham nazarda tutadi.

O‘zbekiston sharoitida masalaning dolzarbligi mamlakatda raqamli transformatsiya, sun’iy intellekt texnologiyalarini rivojlantirish va kiberxavfsizlikni mustahkamlashga qaratilgan normativ-huquqiy asoslar bilan belgilanadi. “Raqamli O‘zbekiston - 2030” strategiyasi elektron hukumat, raqamli ta’lim, raqamli infratuzilma va raqamli industriyani rivojlantirishni davlat siyosatining muhim yo‘nalishi sifatida belgilagan [1]. 2024-yilda tasdiqlangan sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasi esa sun’iy intellektni ijtimoiy soha va iqtisodiyot tarmoqlariga joriy etish, kadrlar tayyorlash va mahalliy ekotizimni rivojlantirishni ustuvor vazifa sifatida ko‘rsatadi [2]. Kiberxavfsizlik to‘g‘risidagi Qonunda esa kiberxavfsizlik sohasidagi munosabatlarni tartibga solish, kiberxavfsizlik obyektlari va subyektlarining huquq hamda majburiyatlarini belgilash masalalari mustahkamlangan [3].

Shu asosda maqolaning maqsadi sun’iy intellekt yordamida axborot xavfsizligini ta’minlashga qaratilgan ta’lim jarayonini tashkil etishda qo‘llanishi mumkin bo‘lgan pedagogik tamoyillarni aniqlash va ularni amaliy model ko‘rinishida asoslashdan iborat. Tadqiqotning vazifalari: birinchidan, sun’iy intellekt va axborot xavfsizligi ta’limi bo‘yicha mavjud yondashuvlarni tahlil qilish; ikkinchidan, xalqaro standart va tavsiyalarni pedagogik nuqtai nazardan umumlashtirish; uchinchidan, oliy ta’limda axborot xavfsizligi kompetensiyasini shakllantirishga xizmat qiluvchi tamoyillar tizimini ishlab chiqish;

to‘rtinchidan, mazkur tamoyillar asosida didaktik model va amaliy tavsiyalarni taklif etishdan iborat.

Mavzuga oid adabiyotlarning tahlili. Mavzuga oid manbalar tahlili shuni ko‘rsatadiki, sun’iy intellekt va axborot xavfsizligi kesishmasida ikki asosiy yo‘nalish shakllanmoqda. Birinchi yo‘nalish sun’iy intellektdan kiberxavfsizlikni ta’minlash vositasi sifatida foydalanishga qaratilgan. Bunda mashinali o‘qitish, anomaliyalarni aniqlash, zararli dasturlarni tasniflash, tarmoq trafikidagi g‘ayritabiiy holatlarni kuzatish, foydalanuvchi xatti-harakatlarini tahlil qilish va avtomatlashtirilgan javob choralarini ishlab chiqish kabi vazifalar ustuvor ahamiyat kasb etadi. Ikkinchi yo‘nalish esa sun’iy intellektning o‘zi bilan bog‘liq xavflarni, ya’ni noto‘g‘ri qarorlar, ma’lumotlar buzilishi, algoritmik noxolislik, maxfiylikning buzilishi, prompt-inyeksiya, deepfake, fishing matnlarini avtomatik yaratish kabi muammolarni o‘rganishni talab qiladi.

UNESCO tomonidan tayyorlangan generativ sun’iy intellektni ta’lim va tadqiqotda qo‘llash bo‘yicha qo‘llanmada inson markazli yondashuv, ma’lumotlar maxfiyligi, pedagogik maqsadga muvofiqlik va o‘qituvchining nazorati alohida urg‘ulanadi [4]. Bu yondashuv axborot xavfsizligini o‘qitishda muhimdir, chunki talaba sun’iy intellekt natijasini ko‘r-ko‘rona qabul qilmasligi, balki uni tekshirishi, dalil bilan solishtirishi va xavf darajasini baholashi zarur. NIST tomonidan ishlab chiqilgan Artificial Intelligence Risk Management Framework sun’iy intellekt tizimlari bilan bog‘liq risklarni boshqarish uchun “govern, map, measure, manage” kabi bosqichlarni tavsiya qiladi [5]. Bu yondashuv pedagogik jarayonda o‘quv maqsadini xavf tahlili bilan bog‘lash, ma’lumotlar manbasini xaritalash, o‘quv natijalarini o‘lchash va xatolardan himoyalanish choralarini belgilash imkonini beradi.

NIST Cybersecurity Framework 2.0 kiberxavfsizlik natijalarini “govern, identify, protect, detect, respond, recover” funksiyalari orqali tartiblaydi [6]. Mazkur struktura ta’lim jarayonida mavzularni ketma-ket va mantiqan bog‘liq berishga qulay asos yaratadi: talaba avval axborot aktivlarini aniqlaydi, so‘ng xavfni baholaydi, himoya choralarini loyihalaydi, hodisani aniqlaydi, unga javob beradi va tiklanish rejasini ishlab chiqadi. NICE Framework kiberxavfsizlik mehnat faoliyatini bilim, ko‘nikma va vazifalar orqali umumiy tilga keltiradi [7]. Bu oliy ta’limda kompetensiyaga asoslangan dastur tuzish, amaliy topshiriqlarni real kasbiy vazifalar bilan bog‘lash, talaba natijalarini mehnat bozori talablari bilan solishtirish uchun muhim hisoblanadi.

ENISAning European Cybersecurity Skills Framework hujjatida kiberxavfsizlik bo‘yicha kasbiy rollar, kompetensiyalar va ko‘nikmalar tizimlashtiriladi [8]. ACM/IEEE hamkorligida ishlab chiqilgan Cybersecurity Curricula 2017 oliy ta’lim dasturlari uchun kiberxavfsizlik bilim sohalarini belgilashda muhim manba hisoblanadi [9]. So‘nggi tadqiqotlarda AI va kiberxavfsizlikni birgalikda o‘qitishda laboratoriya ishlari, interaktiv topshiriqlar, o‘yinlashtirilgan mashg‘ulotlar, dasturlash daftarlaridan foydalanish va real holatlarni tahlil qilish samarali ekani ko‘rsatiladi [10].

Adabiyotlar tahlili shuni ko‘rsatadiki, sun’iy intellekt yordamida axborot xavfsizligini ta’minlash texnik vositalar ro‘yxati emas, balki bilim, amaliy harakat, axloqiy pozitsiya, tanqidiy fikr va refleksiyani birlashtiradigan pedagogik tizimdir.

Tadqiqot metodologiyasi. Pedagogik modellashtirish bosqichida “tamoyil - o‘quv vazifasi - AI vositasi - xavfsizlik natijasi - baholash mezoni” zanjiri ishlab chiqildi. Ushbu zanjir shuni anglatadiki, sun’iy intellektdan foydalanish har bir mashg‘ulotda aniq pedagogik maqsadga xizmat qilishi kerak. Masalan, fishing xabarlarini aniqlash mavzusida AI vositasidan matnni semantik tahlil qilish uchun foydalanish mumkin, biroq asosiy o‘quv natijasi talabaning xavf belgilarini izohlashi, dalil keltirishi va himoya chorasini tanlashidir. Demak, AI o‘qituvchini almashtiruvchi vosita emas, balki o‘quv jarayonini tezlashtiruvchi, tahlilni chuqurlashtiruvchi va individual trayektoriyani moslashtiruvchi didaktik hamkor sifatida qaraladi.

Tahlil va natijalar. Tahlil natijasida sun’iy intellekt yordamida axborot xavfsizligini ta’minlashga qaratilgan ta’lim jarayoni uchun quyidagi yetti asosiy pedagogik tamoyil ajratildi. Birinchi tamoyil - inson markazliligi. Bu tamoyilga ko‘ra, sun’iy intellekt ta’lim jarayonida talabaning mustaqil fikrlashi, mas’uliyati va ijodiy qaror qabul qilishini cheklamasligi kerak. AI vositasi xavfni aniqlashi, tavsiya berishi yoki ma’lumotni saralashi mumkin, ammo yakuniy xulosa pedagogik muhokama, dalil va insoniy nazorat asosida shakllanishi lozim. Bu tamoyil ayniqsa axborot xavfsizligida muhim, chunki noto‘g‘ri avtomatik qaror foydalanuvchi huquqi, maxfiylik va ta’lim sifati uchun salbiy oqibat keltirishi mumkin.

Ikkinchi tamoyil - xavfga yo‘naltirilganlik. Axborot xavfsizligi mavzulari faqat nazariy ta’riflar asosida emas, balki real xavf ssenariylari orqali o‘rgatilishi zarur. Talaba zararli havola, ijtimoiy muhandislik, parol siyosati, ruxsatsiz kirish, ma’lumotlar sizib chiqishi, modelga noto‘g‘ri ma’lumot kiritish, prompt-inyeksiya yoki deepfake kabi holatlarda xavf darajasini baholay olishi kerak. Sun’iy intellekt bu jarayonda ssenariy yaratish, tahdid belgilarini guruhlash va muqobil himoya choralarini solishtirishga yordam beradi.

Uchinchi tamoyil - shaffoflik va tushuntiriluvchanlik. Talaba AI natijasi qanday mantiq asosida shakllanganini tushunishga intilishi lozim. “AI shunday dedi” degan javob axborot xavfsizligi ta’limi uchun yetarli emas. Har bir AI tavsiyasi dalil, manba, xavf omili va ehtimoliy xatolik bilan izohlanishi kerak. Shu bois o‘qituvchi talabalardan AI javobini verifikatsiya qilish, zaif tomonlarini ko‘rsatish va muqobil xulosalar bilan solishtirishni talab qilishi zarur.

To‘rtinchi tamoyil - maxfiylikni loyihalash bosqichidan ta’minlash. Ta’lim jarayonida sun’iy intellekt vositalariga real parollar, shaxsiy ma’lumotlar, talabalar baholari, yopiq tizim konfiguratsiyalari yoki tashkilot ichki hujjatlarini kiritish mumkin emas. O‘quv topshiriqlarida anonimizatsiya qilingan, sintetik yoki maxsus tayyorlangan ma’lumotlardan foydalanish zarur. Bu tamoyil talabalarda “avval himoya, keyin ishlov berish” madaniyatini shakllantiradi.

Beshinchi tamoyil - amaliy-laboratoriya faoliyatiga ustuvorlik berish. Axborot xavfsizligini o‘qitishda “tushuntirish - yodlash - test” modeli yetarli emas. Talaba log fayllarni tahlil qilishi, fishing xabarlarini aniqlashi, oddiy IDS/IPS signalini sharhlashi, koddagi xavfsizlik xatolarini topishi, zaif parol siyosatini tuzatishi, sun’iy intellekt yordamida xavf hisobotini tayyorlashi va bu hisobotni himoya qila olishi zarur. Oltinchi tamoyil - uzluksiz baholash. AI asosidagi ta’limda baholash faqat yakuniy test bilan cheklanmasligi, balki jarayonni kuzatish, oraliq hisobot, laboratoriya natijasi, refleksiv yozuv va jamoaviy muhokama orqali amalga oshirilishi kerak. Yettinchi tamoyil - refleksiv javobgarlik. Talaba AI vositasidan foydalanganini yashirmasligi, ishlatilgan prompt, olingan natija, tekshirish usuli va yakuniy qaror o‘rtasidagi bog‘liqlikni ko‘rsata olishi lozim.

1-jadval. Sun’iy intellekt yordamida axborot xavfsizligini o‘qitish tamoyillari

Tamoyil	Pedagogik mazmuni	AI vositasi orqali qo‘llanishi	Kutiladigan natija
Inson markazliligi	AI yordamchi vosita, yakuniy qaror inson nazoratida bo‘ladi.	AI javobini ekspert bahosi bilan solishtirish.	Mas’uliyatli va tanqidiy qaror qabul qilish.
Xavfga yo‘naltirilganlik	Mavzular real tahdid ssenariylari asosida o‘rgatiladi.	Fishing, anomaliya va zaiflik ssenariylarini generatsiya qilish.	Xavfni aniqlash va baholash ko‘nikmasi.
Shaffoflik	AI tavsiyasi dalil va izoh bilan tekshiriladi.	AI natijasini manba, belgi va mantiq bo‘yicha tahlil qilish.	Tushuntiriluvchan fikrlash va verifikatsiya.

Tamoyil	Pedagogik mazmuni	AI vositasi orqali qo‘llanishi	Kutiladigan natija
Maxfiylik	Shaxsiy va yopiq ma’lumotlar himoyalangan holda ishlatiladi.	Sintetik ma’lumotlar va anonimizatsiya qilingan datasetlardan foydalanish.	Ma’lumotlar xavfsizligi madaniyati.
Amaliy faoliyat	Laboratoriya, keys, loyiha va simulyatsiyalar ustuvor bo‘ladi.	SIEM, IDS, log-tahlil, kod tekshirish va chatbot yordamida mashq.	Kasbiy-amaliy kompetensiya.
Refleksiv javobgarlik	Talaba o‘z qarori, xatosi va himoya chorasini izohlaydi.	AI bilan olingan yechim bo‘yicha refleksiv hisobot tayyorlash.	Etik va huquqiy mas’uliyat.

Manba: mualliflar tomonidan NIST, UNESCO, NICE, ENISA va CSEC2017 yondashuvlari asosida ishlab chiqilgan.

Mazkur tamoyillar asosida axborot xavfsizligi ta’limini quyidagi pedagogik model ko‘rinishida tashkil etish mumkin.

1-rasm. Sun’iy intellekt asosida axborot xavfsizligini o‘qitishning pedagogik modeli. Manba: mualliflar ishlanmasi.

Modelda diagnostika orqali talabalarning boshlang‘ich xavfsizlik savodxonligi aniqlanadi, xavf xaritasi orqali aktiv, tahdid, zaiflik va oqibatlar belgilanadi. AI yordamida ssenariylar, log tahlili va tavsiyalar ishlab chiqiladi, keyingi bosqichda laboratoriya va keyslar bajariladi. Yakunda talaba AI natijasini tekshiradi, xatolarni ko‘rsatadi va o‘z qarorini dalillar bilan himoya qiladi.

Taklif etilayotgan model talabaning nazariy bilimini real xavf ssenariysi bilan bog‘laydi, sun’iy intellekt vositalaridan xavfsiz foydalanish madaniyatini shakllantiradi va o‘qituvchiga individual o‘quv trayektoriyasini moslashtirish imkonini beradi.

Shu bilan birga, AI vositalari noto‘g‘ri tavsiya berishi, maxfiy ma’lumotlarni saqlab qolishi yoki talabaning mustaqil fikrlashini kamaytirishi mumkin. Shu bois har bir topshiriqda “AIga qanday ma’lumot kiritildi?”, “natija qanday tekshirildi?” va “yakuniy qaror uchun kim javobgar?” savollari nazorat mezoni sifatida qo‘llanishi lozim.

Mazkur yondashuvni joriy etishda “Axborot xavfsizligi”, “Kiberxavfsizlik asoslari”, “Sun’iy intellekt asoslari”, “Kompyuter tarmoqlari” va “Dasturlash” fanlari o‘zaro bog‘lanishi kerak. Bu kiberxavfsizlikni alohida mavzu emas, balki barcha raqamli fanlar uchun kesishuvchi kompetensiya sifatida shakllantiradi.

Natijalar uch darajani ko‘rsatadi: mazmuniy darajada AI xavflari, kiberhujumlar va etik me’yorlar kiritiladi; metodik darajada laboratoriya, keys, simulyatsiya va refleksiv hisobot qo‘llanadi; boshqaruv darajasida AI vositalaridan foydalanish qoidalari, ma’lumotlar maxfiyligi va akademik halollik talablari belgilanadi.

Xulosa va takliflar. Xulosa qilib aytganda, sun’iy intellekt yordamida axborot xavfsizligini ta’minlash masalasi texnik muammo bilan bir qatorda pedagogik muammo hamdir. Chunki axborot xavfsizligi madaniyati talabaning bilim darajasi, qaror qabul qilish usuli, raqamli mas’uliyati, axloqiy pozitsiyasi va amaliy ko‘nikmalarida namoyon bo‘ladi. Maqolada tahlil qilingan manbalar va taklif etilgan model asosida sun’iy intellektni axborot xavfsizligi ta’limiga kiritishda inson markazliligi, xavfga yo‘naltirilganlik, shaffoflik, maxfiylikni loyihalash bosqichidan ta’minlash, amaliy faoliyat, uzluksiz baholash va refleksiv javobgarlik asosiy tamoyillar sifatida belgilandi.

Amaliy jihatdan quyidagi takliflarni ilgari surish mumkin. Birinchidan, oliy ta’lim muassasalarida sun’iy intellektdan foydalanish bo‘yicha axborot xavfsizligi qoidalari ishlab chiqilishi lozim. Ikkinchidan, axborot xavfsizligi fanlarida AI yordamida laboratoriya topshiriqlari, real keyslar va xavf ssenariylari kengaytirilishi zarur. Uchinchidan, talabalardan AI natijasini tekshirish, manba bilan solishtirish va xatolik ehtimolini izohlash talab etilishi kerak. To‘rtinchidan, o‘qituvchilar uchun generativ AI, kiberxavfsizlik etikasi va ma’lumotlar maxfiyligi bo‘yicha malaka oshirish mashg‘ulotlari tashkil etilishi maqsadga muvofiq. Beshinchidan, baholash tizimiga laboratoriya hisobotlari, refleksiv izohlar va xavfga asoslangan qarorlarni himoya qilish mezonlari kiritilishi kerak.

Kelgusida ushbu tadqiqot yo‘nalishi bo‘yicha tajriba-sinov ishlarini tashkil etish, taklif etilgan model asosida o‘quv moduli ishlab chiqish va talabalarning axborot xavfsizligi kompetensiyasidagi o‘zgarishlarni empirik o‘lchash muhim ilmiy-amaliy vazifa hisoblanadi. Bunday yondashuv raqamli ta’lim muhitida nafaqat xavfsiz texnologik infratuzilmani, balki xavfsiz fikrlaydigan, mas’uliyatli va raqamli madaniyatga ega mutaxassislarni tayyorlashga xizmat qiladi.

ADABIYOTLAR

1. O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston - 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi PF-6079-son Farmoni. 05.10.2020. URL: https://lex.uz/doc-passport/-5030957.
2. O‘zbekiston Respublikasi Prezidentining “Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida”gi PQ-358-son qarori. 14.10.2024. URL: https://lex.uz/docs/-7158604.
3. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni. 15.04.2022. URL: https://lex.uz/uz/docs/-5960604.
4. Miao F., Holmes W. Guidance for generative AI in education and research. Paris: UNESCO, 2023. URL: https://www.unesco.org/en/articles/guidance-generative-ai-education-and-research.
5. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg: NIST, 2023. URL: https://www.nist.gov/itl/ai-risk-management-framework.
6. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg: NIST, 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
7. National Institute of Standards and Technology. NICE Framework Resource Center. URL: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center.
8. European Union Agency for Cybersecurity. European Cybersecurity Skills Framework (ECSF). ENISA, 2022. URL: https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf.
9. Joint Task Force on Cybersecurity Education. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. ACM/IEEE/AIS SIGSEC/IFIP, 2017. URL: https://cybered.hosting.acm.org/wp/.
10. Tian J. Integrating Artificial Intelligence into the Cybersecurity Curriculum in Higher Education: A Systematic Literature Review // Education Sciences. 2025. Vol. 15, No. 11, Article 1540. DOI: 10.3390/educsci15111540.