

BO'LAJAK KIBERXAVFSIZLIK MUTAXASSISLARIDA PROMPT-IN'EKSIYA HUJUMLARIDAN HIMOYALANISH KOMPETENSIYASINI SHAKLLANTIRISH METODIKASI

K.H.Obloyev¹ 

1. Osiyo xalqaro universiteti «Aniq fanlar va raqamli texnologiyalar» kafedrası stajyor-o'qituvchisi, Buxoro shahri, O'zbekiston Respublikasi

Mas'ul muallif: Obloyev

Komronbek Hamza o'g'li, Osiyo xalqaro universiteti «Aniq fanlar va raqamli texnologiyalar» kafedrası stajyor-o'qituvchisi, Buxoro shahri, O'zbekiston Respublikasi.

Accepted: 25 Sentabr 2026

Published: 25 Sentabr 2026

Copyright: © 2026 by the author(s). Licensee Buxoro xalqaro universiteti ilmiy axborotnomasi.

Iqtibos uchun: Obloyev, K. H. BO'LAJAK KIBERXAVFSIZLIK MUTAXASSISLARIDA PROMPT-IN'EKSIYA HUJUMLARIDAN HIMOYALANISH KOMPETENSIYASINI SHAKLLANTIRISH METODIKASI / K. H. Obloyev // Buxoro xalqaro universiteti ilmiy axborotnomasi. — 2026. — T. 9, № 2. — B. 433-439.

Annotatsiya. Katta til modellariga asoslangan tizimlarning keng ommalashuvi prompt-in'eksiya (ing. prompt injection) hujumlarini axborot xavfsizligining yangi tahdidiga aylantirdi, biroq amaldagi kiberxavfsizlik o'quv dasturlarida bu tahdidga qarshi himoyalaniş ko'nikmalarini shakllantirish masalasi yetarlicha yoritilmagan. Tadqiqotning maqsadi bo'lajak kiberxavfsizlik mutaxassislarida prompt-in'eksiya hujumlaridan himoyalaniş kompetensiyasini shakllantirish metodikasini ishlab chiqishdan iborat. Tadqiqotda me'yoriy hujjatlar va xalqaro o'quv dasturlarini tahlil qilish, kompetensiyaviy yondashuv asosida pedagogik modellashtirish hamda o'quv laboratoriyasi uchun hisoblash tajribasi usullari qo'llanildi; tajribada ingliz, rus, o'zbek va aralash tillardagi 1650 ta namunadan foydalanildi. Natijada kompetensiyaning kognitiv, faoliyatli va refleksiv tarkibiy qismlari aniqlandi, didaktik model hamda yetti mashg'ulotdan iborat 16 soatlik laboratoriya praktikumi ishlab chiqildi. Topshiriqlar murakkabligi ekspert bahosi asosida emas, balki tajriba ma'lumotlari asosida hisoblangan indeks yordamida tartiblandi, baholash mezonlari esa talaba yaratgan himoya vositasining o'lchanadigan ko'rsatkichlariga bog'landi. Ingliz tiliga mo'ljallangan himoya vositasi rus va o'zbek tilidagi hujumlarning barchasini o'tkazib yuborishi aniqlandi, bu esa ko'p tilli o'quv materiallari zarurligini asoslaydi. Taklif etilgan metodika «Kiberxavfsizlik asoslari» fani mazmuniga alohida modul sifatida kiritilishi mumkin.

Kalit so'zlar: prompt-in'eksiya, kiberxavfsizlik ta'limi, kasbiy kompetensiya, katta til modellari, laboratoriya praktikumi, didaktik model, murakkablik indeksi, ko'p tilli ta'lim, sun'iy intellekt xavfsizligi.

МЕТОДИКА ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ ЗАЩИТЫ ОТ АТАК ТИПА «PROMPT INJECTION» У БУДУЩИХ СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ

Аннотация. Широкое распространение систем на основе больших языковых моделей превратило атаки типа промпт-инъекция (англ. prompt injection) в новую угрозу информационной безопасности, однако в действующих учебных программах по кибербезопасности вопрос формирования навыков защиты от этой угрозы освещён недостаточно. Цель исследования – разработка методики формирования у будущих специалистов по кибербезопасности компетенции защиты от промпт-инъекций. В исследовании применялись анализ нормативных документов и международных учебных программ, педагогическое моделирование на основе компетентностного подхода, а также вычислительный эксперимент для учебной лаборатории на корпусе из 1650 образцов на английском, русском, узбекском и смешанном языках. В результате выделены когнитивный, деятельностный и рефлексивный компоненты компетенции, разработаны дидактическая модель и 16-часовой лабораторный практикум из семи занятий. Сложность заданий упорядочена не на основе экспертной оценки, а с помощью индекса, рассчитанного по экспериментальным данным, а критерии оценивания привязаны к измеримым показателям созданного студентом средства защиты. Установлено, что англоязычное средство защиты пропускает все атаки на русском и узбекском языках, что обосновывает необходимость многоязычных учебных материалов. Предложенная методика может быть включена в содержание дисциплины «Основы кибербезопасности» в качестве отдельного модуля.

Ключевые слова: промпт-инъекция, обучение кибербезопасности, профессиональная компетенция, большие языковые модели, лабораторный практикум, дидактическая модель, индекс сложности, многоязычное обучение, безопасность искусственного интеллекта.

METHODOLOGY FOR DEVELOPING PROMPT INJECTION DEFENSE COMPETENCE IN FUTURE CYBERSECURITY SPECIALISTS

Abstract. The widespread adoption of systems based on large language models has turned prompt injection attacks into a new information security threat, yet existing cybersecurity curricula pay insufficient attention to developing the skills needed to defend

against it. The aim of this study is to develop a methodology for building prompt injection defence competence in future cybersecurity specialists. The study employed analysis of regulatory documents and international curricula, pedagogical modelling based on the competence approach, and a computational experiment for a teaching laboratory using a corpus of 1650 samples in English, Russian, Uzbek and mixed language. As a result, the cognitive, activity-based and reflective components of the competence were identified, and a didactic model together with a 16-hour, seven-session laboratory practicum was developed. Task difficulty was sequenced not by expert judgement but by an index calculated from experimental data, and assessment criteria were linked to measurable indicators of the defence tool built by the student. It was found that an English-oriented defence tool missed every Russian and Uzbek attack, which justifies the need for multilingual teaching materials. The proposed methodology can be incorporated into the course «Fundamentals of Cybersecurity» as a separate module.

Keywords: prompt injection, cybersecurity education, professional competence, large language models, laboratory practicum, didactic model, difficulty index, multilingual education, artificial intelligence security.

Kirish. Raqamli transformatsiya jarayonida sun'iy intellekt texnologiyalari davlat boshqaruvi, bank-moliya, sog'liqni saqlash va ta'lim tizimlarining ajralmas qismiga aylanmoqda. O'zbekiston Respublikasida mazkur yo'nalish davlat siyosati darajasiga ko'tarilgan: «Ta'lim to'g'risida»gi Qonun [1] ta'lim mazmunini fan va texnika yutuqlariga muvofiq muntazam yangilab borishni talab etsa, sun'iy intellekt texnologiyalarini jadal joriy etishga oid Prezident qarori [2] ushbu soha uchun malakali kadrlar tayyorlashni ustuvor vazifa sifatida belgilaydi. «Kiberxavfsizlik to'g'risida»gi Qonun [3] esa axborot tizimlarini himoya qilish bo'yicha mutaxassislar tayyorlash tizimini takomillashtirish zaruratini qonuniy jihatdan mustahkamlaydi.

Sun'iy intellekt tizimlarining, xususan, katta til modellari (KTM) asosidagi amaliy dasturlarning keng tarqalishi bilan an'anaviy dasturiy ta'minotda uchramaydigan yangi zaiflik turi paydo bo'ldi. Prompt-in'eksiya hujumida tajovuzkor foydalanuvchi so'rovi yoki model qayta ishlaydigan hujjat ichiga buyruq ko'rinishidagi matn joylashtiradi va natijada model tizim ko'rsatmalarini buzib, ruxsat etilmagan amalni bajaradi. OWASP xalqaro tashkiloti bu hujumni KTM ilovalari uchun eng xavfli tahdidlar ro'yxatining birinchi o'rniga qo'ygan [4]. Perez va Ribeiro [5] hujumning bevosita shaklini, Greshake va hammualliflari [6] esa tashqi hujjatlar orqali amalga oshiriladigan bilvosita shaklini tizimli tavsiflagan.

Atamashunoslik jihatidan izoh berish o'rinli. Ingliz tilidagi prompt injection birikmasining o'zbekcha muqobili ilmiy adabiyotda hali barqarorlashmagan. Mazkur maqolada milliy adabiyotda qo'llanib kelinayotgan SQL-in'eksiya atamasi [7] bilan uyg'unlikni saqlash maqsadida prompt-in'eksiya shakli qabul qilindi. Har ikkala hujumning mohiyati bir xil: buyruq bilan ma'lumot o'rtasidagi chegaraning yo'qolishi zaiflikni keltirib chiqaradi.

Muammoning pedagogik jihati shundaki, kiberxavfsizlik bo'yicha mutaxassislar tayyorlashga asos bo'luvchi xalqaro me'yoriy hujjatlar – ACM va IEEE tomonidan ishlab chiqilgan CSEC2017 o'quv dasturi [8] hamda NIST tashkilotining NICE kasbiy malakalar tizimi [9] – KTM paydo bo'lishidan oldin tuzilgan va sun'iy intellekt tizimlari xavfsizligini alohida bilim sohasi sifatida ajratmaydi. Milliy oliy ta'lim muassasalarida ham ushbu mavzu bo'yicha o'quv-uslubiy ta'minot deyarli mavjud emas. Bundan tashqari, mavjud o'quv resurslari va himoya vositalari ingliz tiliga yo'naltirilgan. Deng va hammualliflari [10], shuningdek, Yong va hammualliflari [11] kam resursli tillarga o'girilgan zararli so'rovlar xavfsizlik mexanizmlarini ancha osonroq chetlab o'tishini ko'rsatgan. O'zbek, rus va ingliz tillari aralash qo'llaniladigan milliy axborot muhitida faqat inglizcha misollar asosida tayyorlangan mutaxassis real tahdidga tayyor bo'lmaydi.

Tadqiqotning maqsadi bo'lajak kiberxavfsizlik mutaxassislarida prompt-in'eksiya hujumlaridan himoyalash kompetensiyasini shakllantirish metodikasini ishlab chiqishdan iborat. Maqsadga erishish uchun quyidagi vazifalar belgilandi: kompetensiyaning tarkibiy qismlari va ko'rsatkichlarini aniqlash; kompetensiyani shakllantirishning didaktik modelini ishlab chiqish; ko'p tili o'quv to'plami va dasturiy stend asosida laboratoriya praktikumini loyihalash; topshiriqlar murakkabligini tajriba ma'lumotlari asosida asoslash; o'quv natijalarini baholash mezonlarini ishlab chiqish.

Tadqiqotning ilmiy yangiligi laboratoriya topshiriqlarining murakkablik darajasi ekspert bahosi asosida emas, balki dasturiy stendda o'tkazilgan hisoblash tajribasi natijalaridan olingan miqdoriy indeks asosida belgilanishida hamda o'quv mazmuniga o'zbek va rus tilidagi hujum namunalari tizimli ravishda kiritilishidir.

Tadqiqotning amaliy ahamiyati ishlab chiqilgan o'quv to'plami, dasturiy stend, laboratoriya topshiriqlari va baholash mezonlarining oliy ta'lim muassasalarida kiberxavfsizlik va sun'iy intellekt yo'nalishlari bo'yicha o'quv jarayonida bevosita qo'llanishi mumkinligi bilan belgilanadi. Metodika qo'shimcha qimmat dasturiy ta'minot yoki maxsus jihozlarni talab qilmaydi va oddiy kompyuter sinfida amalga oshiriladi.

Metodlar. Tadqiqotda nazariy va empirik metodlar majmuasidan foydalanildi. Nazariy bosqichda ta'lim va kiberxavfsizlik sohasidagi me'yoriy-huquqiy hujjatlar [1–3], xalqaro o'quv dasturlari [8, 9] hamda «Kiberxavfsizlik asoslari» fanining amaldagi o'quv dasturi qiyosiy tahlil qilindi. Tahlil maqsadi – sun'iy intellekt tizimlari xavfsizligiga oid mavzular dasturlarda qay darajada aks etganini aniqlash va yangi modulning dastur tuzilmasidagi o'rnini belgilash edi.

Tahlil shuni ko'rsatdiki, CSEC2017 dasturi [8] kiberxavfsizlik mazmunini ma'lumotlar, dasturiy ta'minot, komponentlar, aloqa, tizim, inson, tashkilot va jamiyat xavfsizligi kabi bilim sohalariga ajratadi, biroq ularning birortasida mashinali o'qitish modellari yoki til modellariga qaratilgan hujumlar alohida mavzu sifatida ko'rsatilmagan. NICE tizimida [9] ham sun'iy intellekt tizimlarini himoya qilish vazifasi alohida kasbiy rol sifatida ajratilmagan. «Kiberxavfsizlik asoslari» fanining amaldagi dasturida esa veb-ilovalar zaifliklari, jumladan, SQL-in'eksiya mavzusi mavjud. Shu sababli yangi modulni aynan shu mavzudan keyin joylashtirish maqsadga muvofiq deb topildi: talaba buyruq va ma'lumot chegarasining buzilishi haqidagi tushunchani SQL-in'eksiya misolida o'zlashtirgach, uni yangi turdagi tizimga ko'chirish imkoniga ega bo'ladi. Bu ta'limdagi uzviylik va vorisilylik tamoyiliga mos keladi.

Kompetensiya tarkibini aniqlashda kompetensiyaviy yondashuvning nazariy asoslariga tayanildi. I.A. Zimnyaya kompetensiyani bilim, tajriba va qadriyatli munosabatga asoslangan, faoliyatda namoyon bo'ladigan integrativ sifat sifatida talqin qiladi [12, s. 38]. A.V. Xutorskoy esa kompetensiya tarkibida shaxsning tayyor bilimi bilan bir qatorda uni amaliy vaziyatda qo'llash qobiliyatini alohida ajratadi [13]. Ushbu yondashuvlar asosida kompetensiya uch tarkibiy qism – kognitiv, faoliyatli va refleksiv qismlar ko'rinishida tavsiflandi. Har bir tarkibiy qismning o'zlashtirish darajasi L. Anderson va D. Krathwohl tomonidan qayta ishlangan B. Blum taksonomiyasi [14] bosqichlariga moslashtirildi.

Laboratoriya praktikumini loyihalashda D. Kolbning tajriba orqali o'qitish sikli [15] asos qilib olindi: aniq tajriba (hujumni kuzatish), mulohazali kuzatish (hujum sababini tahlil qilish), abstrakt tushunchalashtirish (himoya tamoyilini shakllantirish) va faol tajriba o'tkazish (himoya vositasini yaratish va sinash). Didaktik modelni ishlab chiqishda V.P. Bepalkoning pedagogik tizim tarkibiy qismlari haqidagi konsepsiyasi [16] hamda milliy pedagogikada ishlab chiqilgan innovatsion ta'lim texnologiyalari tamoyillari [17] inobatga olindi.

Empirik bosqichda o'quv laboratoriyasi uchun dasturiy stend yaratildi va unda hisoblash tajribasi o'tkazildi. Stend tarkibiga ingliz, rus, o'zbek hamda aralash tillarda tuzilgan 1650 ta namunadan iborat o'quv to'plami kiritildi; ularning 715 tasi hujum, 935 tasi zararsiz so'rovdir. Har bir hujum shabloniga olti xil niqoblash usuli qo'llanildi: niqobsiz holat, hujjat ichiga joylashtirish (bilvosita in'eksiya), so'z ichiga ajratgich qo'shish, nol kenglikdagi belgilar kiritish, kirill harflari bilan gomoglif almashtirish va Base64 usulida kodlash. To'plam shablon darajasida o'qitish va sinov qismlariga ajratildi, sinov qismi 493 ta namunani tashkil etdi. Stendda to'rt xil himoya konfiguratsiyasi sinovdan o'tkazildi: ingliz tilidagi kalit so'z filtri, ko'p tilli signatura qatlami, semantik tasniflagich va ko'p qatlamli kaskad himoya.

Hisoblash tajribasining vazifasi himoya vositasini takomillashtirish emas, balki didaktik qarorlar uchun ob'ektiv asos olish edi. Shu maqsadda har bir niqoblash turi uchun topshiriq murakkabligi indeksi quyidagicha aniqlandi:

$$D_k = 1 - R_k, (1)$$

bu yerda R_k – ko'p tilli signatura qatlamining k-turdagi hujumlarni aniqlash to'liqligi (Recall). Indeksning mazmuni quyidagicha: bazaviy himoya vositasi qancha ko'p hujumni o'tkazib yuborsa, talaba shuncha chuqur bilim va murakkabroq himoya mexanizmini qo'llashi talab etiladi. Topshiriqlar D indeksining ortib borishi tartibida joylashtirildi, bu esa «oddiydan murakkabga» didaktik tamoyilining miqdoriy asoslangan ko'rinishidir.

Kompetensiyaning tarkibiy qismlari

Natijalar va mulohaza. Nazariy tahlil natijasida prompt-in'eksiya hujumlaridan himoyalash kompetensiyasi uch tarkibiy qism va ularning ko'rsatkichlari ko'rinishida tavsiflandi (1-jadval). Kognitiv qism hujumning mohiyati va turlari haqidagi bilimlarni, faoliyatli qism hujumni aniqlash va himoya vositasini yaratish ko'nikmalarini, refleksiv qism esa himoya samaradorligini baholash va asoslangan qaror qabul qilish malakasini qamrab oladi.

1-jadval.

Prompt-in'eksiyadan himoyalash kompetensiyasining tarkibi

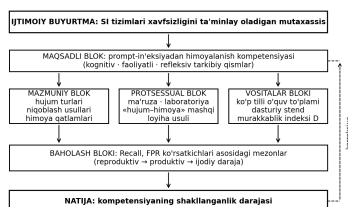
Table 1. Structure of the prompt injection defence competence

Tarkibiy qism	Ko'rsatkichlar	Taksonomiya bosqichi
Kognitiv	hujumning mohiyatini, bevosita va bilvosita turlarini, niqoblash usullarini biladi; SQL-in'eksiya bilan o'xshashlik va farqini tushuntiradi	Eslash, tushunish
Faoliyatli	hujum namunalarini ko'p tilli matnda aniqlaydi; normalizatsiya va signatura qoidalarini yozadi; himoya qatlamlarini birlashtiradi	Qo'llash, tahlil qilish
Refleksiv	himoya samaradorligini Recall va FPR ko'rsatkichlari bo'yicha baholaydi; aniqlik va xarajat o'rtasidagi muvozanatni asoslaydi	Baholash, yaratish

Manba: muallif ishlanmasi.

Kompetensiyani shakllantirishning didaktik modeli

Kompetensiyani shakllantirish jarayoni o'zaro bog'liq bloklardan iborat didaktik model ko'rinishida ifodalandi (1-rasm). Model ijtimoiy buyurtmadan boshlanadi, ya'ni sun'iy intellekt tizimlari xavfsizligini ta'minlay oladigan mutaxassisga bo'lgan ehtiyojdan kelib chiqadi. Maqsadli blok kompetensiyaning uch tarkibiy qismini belgilaydi. Mazmuniy blok hujum turlari, niqoblash usullari va himoya qatlamlaridan tashkil topadi. Protsessual blokda ma'ruza, laboratoriya mashg'uloti, «hujum–himoya» mashqi va loyiha usuli qo'llaniladi. Vositalar bloki ko'p tilli o'quv to'plami, dasturiy stend va murakkablik indeksini o'z ichiga oladi. Baholash bloki natijalarni o'lchanadigan mezonlar asosida aniqlaydi va teskari aloqa orqali jarayonga tuzatish kiritish imkonini beradi.



1-rasm. Kompetensiyani shakllantirishning didaktik modeli

Fig. 1. Didactic model for developing the competence

Manba: muallif ishlanmasi.

Til omilining didaktik ahamiyati

Dasturiy stendda o'tkazilgan hisoblash tajribasi o'quv mazmunini tanlash uchun muhim xulosa berdi (2-jadval, 2-rasm). Ingliz tiliga mo'ljallangan kalit so'z filtri rus va o'zbek tilidagi hujumlarning yuz foizini o'tkazib yubordi, ingliz tilida esa hujumlarning atigi 46,2 foizini to'xtatdi. Ko'p tilli signatura qatlami holatni qisman yaxshiladi, biroq aralash tildagi hujumlarning 76,9 foizi baribir aniqlanmadi. Faqat bir necha qatlamni birlashtirgan kaskad himoya barcha til guruhlarida hujum samaradorligini sezilarli pasaytirdi.

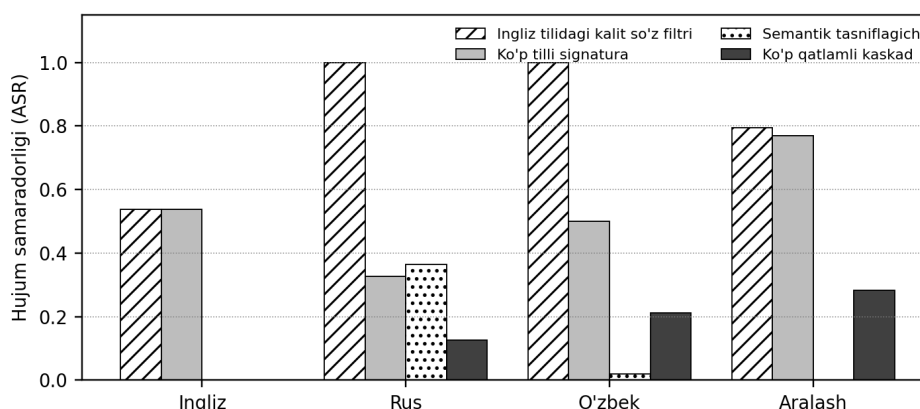
2-jadval.

Himoya vositalarining til kesimidagi hujum samaradorligi (ASR)

Table 2. Attack success rate (ASR) of defence tools by language

Himoya vositasi	Ingliz	Rus	O'zbek	Aralash
Ingliz tilidagi kalit so'z filtri	0,538	1,000	1,000	0,795
Ko'p tilli signatura qatlami	0,538	0,327	0,500	0,769
Semantik tasniflagich	0,000	0,365	0,019	0,000
Ko'p qatlamli kaskad	0,000	0,125	0,212	0,282

Manba: muallif tomonidan o'tkazilgan hisoblash tajribasi natijalari (sinov to'plami: 493 ta namuna).



2-rasm. Til guruhlari bo'yicha hujum samaradorligi

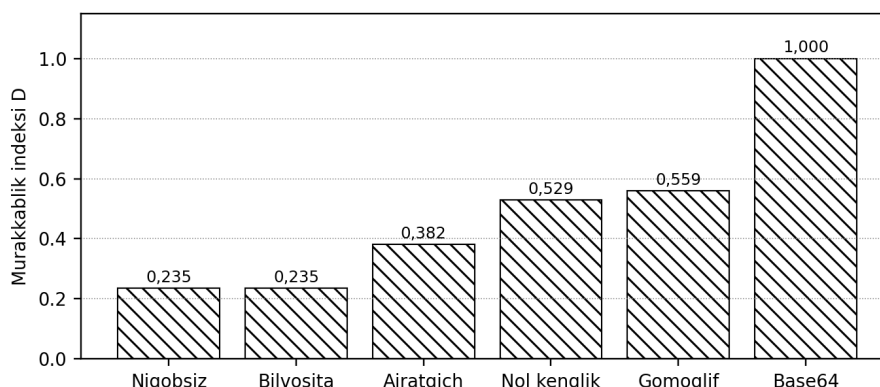
Fig. 2. Attack success rate by language group

Manba: muallif tomonidan o'tkazilgan hisoblash tajribasi natijalari.

Ushbu natijaning pedagogik ahamiyati shundan iboratki, faqat inglizcha misollar asosida o'qitilgan talabada himoya vositasining samaradorligi haqida noto'g'ri tasavvur shakllanadi: vosita o'quv misollarida yaxshi natija ko'rsatadi, real milliy muhitda esa deyarli ishlamaydi. Shu sababli o'quv to'plamiga o'zbek, rus va aralash tildagi namunalar majburiy tarzda kiritildi, laboratoriya topshiriqlarida esa himoya vositasini har bir til guruhida alohida sinash talab etiladi.

Laboratoriya praktikumining tuzilishi

Murakkablik indeksi (1) formula bo'yicha hisoblandi. Eng past qiymat niqobsiz va bilvosita hujumlarda ($D = 0,235$), eng yuqori qiymat esa Base64 usulida kodlangan hujumlarda ($D = 1,000$) qayd etildi (3-rasm). Oxirgi holat bazaviy signatura qatlami kodlangan matndagi birorta hujumni ham aniqlay olmaganini bildiradi: bunday hujumni to'xtatish uchun talaba avval matnni dekodlovchi normalizatsiya qatlamini yaratishi lozim.



3-rasm. Niqoblash turlari bo'yicha topshiriqlar murakkabligi indeksi

Fig. 3. Task difficulty index by obfuscation technique

Manba: muallif tomonidan o'tkazilgan hisoblash tajribasi natijalari.

Olingan qiymatlar asosida yetti mashg'ulotdan iborat laboratoriya praktikumi tuzildi (3-jadval). Dastlabki ikki mashg'ulot hujumni tanib olishga, keyingi to'rttasi niqoblangan hujumlarga qarshi normalizatsiya usullarini o'zlashtirishga bag'ishlangan. Yakuniy mashg'ulot loyiha shaklida o'tkaziladi: talaba barcha qatlamlarni yagona kaskad himoyaga birlashtiradi va uni dasturiy stendda sinovdan o'tkazadi.

3-jadval.

Laboratoriya praktikumining mazmuni

Table 3. Content of the laboratory practicum

No	Mashg'ulot mavzusi	D	Taksonomiya bosqichi	Soat
1	Bevosita prompt-in'eksiyani tanib olish	0,235	Tushunish	2
2	Hujjat ichiga joylashtirilgan bilvosita in'eksiya	0,235	Qo'llash	2
3	So'z ichidagi ajratgichlarni bartaraf etish	0,382	Qo'llash	2
4	Nol kenglikdagi belgilarni aniqlash va tozalash	0,529	Tahlil qilish	2
5	Kirill-lotin gomogliflarini normalizatsiya qilish	0,559	Tahlil qilish	2
6	Base64 usulida kodlangan hujumlarni ochish	1,000	Baholash	2
7	Loyiha: ko'p qatlamli kaskad himoyani yaratish	—	Yaratish	4
	Jami			16

Manba: muallif ishlanmasi.

Har bir mashg'ulot Kolb siklining to'rt bosqichi bo'yicha tashkil etiladi. Masalan, beshinchi mashg'ulotda talaba avval gomoglif bilan niqoblangan hujum signatura filtridan o'tib ketishini kuzatadi, keyin bunga sabab lotin harfi o'rniga tashqi ko'rinishi bir xil kirill harfi qo'yilgani ekanini aniqlaydi, so'ngra aralash yozuvli so'zlarni aniqlash tamoyilini shakllantiradi va nihoyat normalizatsiya funksiyasini yozib, uning samaradorligini stendda o'lchaydi.

Praktikumning muhim tarkibiy qismi «hujum-himoya» mashqidir. Unda talabalar juftliklarga bo'linadi: birinchi talaba o'rganilgan niqoblash usullaridan foydalanib stend himoyasini chetlab o'tuvchi yangi hujum namunalarini tuzadi, ikkinchisi esa o'z himoya vositasini shu namunalarga qarshi takomillashtiradi. Keyingi mashg'ulotda rollar almashtiriladi. Mashq ikki xil pedagogik vazifani hal qiladi. Birinchidan, talaba himoya vositasini qo'lda tuzilgan statik misollarda emas, balki faol va o'zgaruvchan raqibga qarshi sinaydi. Ikkinchidan, hujum namunalarini o'zi tuzish jarayonida tajovuzkor fikrlash tarzini tushunadi, bu esa kiberxavfsizlik mutaxassisi uchun muhim kasbiy sifat hisoblanadi. Talabalar tuzgan yangi namunalar o'qituvchi tomonidan tekshirilib, o'quv to'plamiga qo'shib boriladi; shu tariqa to'plam har bir o'quv yilida kengayib, zamonaviy hujum usullarini aks ettirib boradi.

Mashg'ulotlarni tashkil etishda axloqiy jihatlariga alohida e'tibor qaratiladi. Barcha hujum mashqlari faqat izolyatsiyalangan o'quv stendda bajariladi; har bir praktikum boshida talabalar ruxsat etilmagan tizimlarga hujum qilishning huquqiy oqibatlarini va «Kiberxavfsizlik to'g'risida»gi Qonun [3] talablari bilan tanishtiriladi. Bu kompetensiyaning refleksiv qismini kasbiy mas'uliyat bilan boyitadi.

O'quv natijalarini baholash mezonlari

Baholash mezonlari universitetda qabul qilingan baholash tizimiga moslashtirildi (4-jadval). Mezonlarning muhim xususiyati shundaki, ular o'qituvchining sub'ektiv fikriga emas, balki talaba yaratgan himoya vositasining dasturiy stendda o'lchangan ko'rsatkichlariga tayanadi. Eng yuqori daraja uchun belgilangan Recall $\geq 0,80$ chegarasi hisoblash tajribasida ko'p qatlamli kaskad erishgan natijaga (Recall = 0,842) asoslanadi.

4-jadval.

Kompetensiyaning shakllanganlik darajalari va baholash mezonlari

Table 4. Levels of competence formation and assessment criteria

Ball	Daraja	Mezonlar
90–100	Ijodiy	ko'p qatlamli himoyani mustaqil loyihalaydi; stendda Recall $\geq 0,80$ va FPR $\leq 0,05$ ga erishadi; qarorlarini dalillar bilan asoslaydi
70–89,9	Produktiv	barcha niqoblash turlarini aniqlaydi; kamida ikki qatlamli himoya yaratadi; Recall va FPR ko'rsatkichlarini hisoblab izohlaydi
60–69,9	Reproduktiv	asosiy hujum turlarini namunalar bo'yicha

Ball	Daraja	Mezonlar
		tanib oladi; tayyor signatura qoidalarini to'g'ri qo'llaydi
0-59,9	Past	hujum turlarini farqlamaydi; himoya vositasini sinash va baholash ko'nikmasiga ega emas

Manba: muallif ishlanmasi.

Mulohaza

Olingan natijalarni mavjud tadqiqotlar bilan qiyoslash quyidagi xulosalarga olib keladi. V. Švábenský va hammualliflarining tizimli sharhida [18] kiberxavfsizlik ta'limiga oid ishlarining katta qismi amaliy mashg'ulotlar va o'yin shaklidagi topshiriqlarga bag'ishlangani, biroq topshiriqlar murakkabligi odatda muallifning ekspert bahosi asosida belgilanishi qayd etilgan. Mazkur ishda taklif etilgan murakkablik indeksi bu kamchilikni bartaraf etadi: topshiriqlar ketma-ketligi takrorlanadigan hisoblash tajribasi natijalariga tayanadi va yangi himoya vositalari paydo bo'lganda qayta hisoblanishi mumkin.

Ikkinchidan, xalqaro o'quv dasturlari [8, 9] va ommaviy o'quv musobaqalari [20] materiallari ingliz tilida tuzilgan. Tajriba natijalari (2-jadval) bunday materiallarni milliy ta'limga to'g'ridan-to'g'ri ko'chirish yetarli emasligini ko'rsatadi: o'quv mazmuniga o'zbek va rus tilidagi namunalar kiritilmasa, talaba real muhitda samarasiz bo'lgan himoya usullarini o'zlashtiradi. Uchinchidan, kontekstni ajratish kabi zamonaviy himoya usullari [19] ham yakka holda to'liq himoya bermaydi; shu sababli praktikum yakuniy loyihada qatlamlı mudofaa tamoyilini shakllantirishga qaratilgan.

Tadqiqotning cheklovlarini ham qayd etish lozim. Maqolada metodikaning nazariy asoslari, didaktik modeli, o'quv mazmuni va baholash vositalari ishlab chiqildi hamda topshiriqlar murakkabligi tajriba yo'li bilan asoslandi. Metodikaning talabalar o'quv natijalariga ta'siri esa tadqiqotning keyingi bosqichida nazorat va tajriba guruhlarida o'tkaziladigan pedagogik tajriba-sinov ishlari orqali aniqlanadi; 4-jadvaldagi mezonlar aynan shu bosqich uchun o'lchov vositasi bo'lib xizmat qiladi.

Xulosa va tavsiyalar. Tadqiqot natijasida bo'lajak kiberxavfsizlik mutaxassislarida prompt-in'eksiya hujumlaridan himoyalaniş kompetensiyasini shakllantirish metodikasi ishlab chiqildi. Ishning asosiy natijalari quyidagilardan iborat.

1. Kompetensiyaviy yondashuv asosida kompetensiyaning kognitiv, faoliyatli va refleksiv tarkibiy qismlari hamda ularning taksonomiya bosqichlariga mos ko'rsatkichlari aniqlandi.

2. Maqsadli, mazmuniy, protsessual, vositalar va baholash bloklaridan iborat, teskari aloqaga ega didaktik model ishlab chiqildi.

3. Ingliz, rus, o'zbek va aralash tillardagi 1650 ta namunadan iborat o'quv to'plami va dasturiy stend yaratildi. Hisoblash tajribasi ingliz tiliga mo'ljallangan himoya vositasi rus va o'zbek tilidagi hujumlarning barchasini o'tkazib yuborishini ko'rsatdi, bu ko'p tilli o'quv mazmunining zarurligini isbotlaydi.

4. Topshiriqlar murakkabligini tajriba ma'lumotlari asosida belgilovchi indeks taklif etildi va uning yordamida 16 soatlik, yetti mashg'ulotdan iborat laboratoriya praktikumi tuzildi.

5. Himoya vositasining o'lchanadigan ko'rsatkichlariga tayanuvchi, to'rt darajali baholash mezonlari ishlab chiqildi.

Tadqiqot natijalaridan kelib chiqib quyidagi tavsiyalar beriladi: ishlab chiqilgan praktikumni «Kiberxavfsizlik asoslari» fanining amaliy mashg'ulotlariga alohida modul sifatida kiritish; sun'iy intellekt yo'nalishidagi ta'lim dasturlariga sun'iy intellekt tizimlari xavfsizligi mavzusini qo'shish; kiberxavfsizlik bo'yicha o'zbek tilidagi o'quv to'plamlarini yaratishni davom ettirish; murakkablik indeksi yondashuvini boshqa amaliy mavzular bo'yicha topshiriqlar tizimini loyihalashda qo'llash.

Foydalanilgan adabiyotlar ro'yxati

[1] O'zbekiston Respublikasining «Ta'lim to'g'risida»gi Qonuni. – 23.09.2020. – URL: <https://lex.uz/docs/5013007> (murojaat qilingan sana: 20.09.2026).

[2] O'zbekiston Respublikasi Prezidentining «Sun'iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to'g'risida»gi qarori. – 17.02.2021. – URL: <https://lex.uz/docs/5297046> (murojaat qilingan sana: 20.09.2026).

[3] O'zbekiston Respublikasining «Kiberxavfsizlik to'g'risida»gi Qonuni. – 15.04.2022. – URL: <https://lex.uz/docs/5960604> (murojaat qilingan sana: 20.09.2026).

[4] OWASP Top 10 for Large Language Model Applications. – URL: <https://owasp.org/www-project-top-10-for-large-language-model-applications/> (murojaat qilingan sana: 20.09.2026).

[5] Perez F., Ribeiro I. Ignore previous prompt: attack techniques for language models // arXiv. – 2022. – URL: <https://arxiv.org/abs/2211.09527> (murojaat qilingan sana: 20.09.2026).

[6] Greshake K., Abdelnabi S., Mishra S. [et al.] Not what you've signed up for: compromising real-world LLM-integrated applications with indirect prompt injection // Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security. – 2023. – P. 79–90.

[7] Dilshodov A., Zokirjonova X. SQL in'eksiyasi hujumlaridan himoyalanişning zamonaviy usullari // Avtomatlashtirish, elektronika va sun'iy intellekt asosida texnologik muammolar va yechimlar : respublika ilmiy-amaliy konferensiyasi materiallari. – 2025. – T. 1, № 1. – B. 557–560. – URL: <https://publisher-hub.uz/index.php/AEISTMY/article/view/111>.

- [8] Joint Task Force on Cybersecurity Education. Cybersecurity Curricula 2017 : Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. – New York : ACM ; IEEE Computer Society, 2017.
- [9] Petersen R., Santos D., Smith M.C. [et al.] Workforce Framework for Cybersecurity (NICE Framework) : NIST Special Publication 800-181 Rev. 1. – Gaithersburg : NIST, 2020. – 24 p. – URL: <https://doi.org/10.6028/NIST.SP.800-181r1>.
- [10] Deng Y., Zhang W., Pan S., Bing L. Multilingual jailbreak challenges in large language models // arXiv. – 2023. – URL: <https://arxiv.org/abs/2310.06474> (murojaat qilingan sana: 20.09.2026).
- [11] Yong Z.-X., Menghini C., Bach S.H. Low-resource languages jailbreak GPT-4 // arXiv. – 2023. – URL: <https://arxiv.org/abs/2310.02446> (murojaat qilingan sana: 20.09.2026).
- [12] Зимняя И.А. Ключевые компетенции – новая парадигма результата образования // Высшее образование сегодня. – 2003. – № 5. – С. 34–42.
- [13] Хуторской А.В. Ключевые компетенции как компонент личностно-ориентированной парадигмы образования // Народное образование. – 2003. – № 2. – С. 58–64.
- [14] Anderson L.W., Krathwohl D.R. A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. – New York : Longman, 2001. – 352 p.
- [15] Kolb D.A. Experiential Learning: Experience as the Source of Learning and Development. – Englewood Cliffs : Prentice Hall, 1984. – 256 p.
- [16] Беспалько В.П. Слагаемые педагогической технологии. – Москва : Педагогика, 1989. – 192 с.
- [17] Ishmuhamedov R.J., Yuldashev M. Ta'lim va tarbiyada innovatsion pedagogik texnologiyalar. – Toshkent : Nihol, 2013. – 279 b.
- [18] Švábenský V., Vykopal J., Čeleda P. What are cybersecurity education papers about? A systematic literature review of SIGCSE and ITiCSE conferences // Proceedings of the 51st ACM Technical Symposium on Computer Science Education. – 2020. – P. 2–8.
- [19] Hines K., Lopez G., Hall M. [et al.] Defending against indirect prompt injection attacks with spotlighting // arXiv. – 2024. – URL: <https://arxiv.org/abs/2403.14720> (murojaat qilingan sana: 20.09.2026).
- [20] Schulhoff S., Pinto J., Khan A. [et al.] Ignore this title and HackAPrompt: exposing systemic vulnerabilities of LLMs through a global prompt hacking competition // Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing. – 2023. – P. 4945–4977.