TALABALARDA PHISHING HUJUMLARINI ANIQLASH KOMPETENSIYASINI SHAKLLANTIRISH METODIKASI

K.H.Obloyev[1]

1. Osiyo Xalqaro Universiteti "Aniq fanlar va raqamli texnologiyalar" kafedrasi stajyor-o'qituvchisi, Buxoro, O'zbekiston

Mas'ul muallif: Obloyev Komronbek Hamza o'g'li, Osiyo Xalqaro Universiteti "Aniq fanlar va raqamli texnologiyalar" kafedrasi stajyor-o'qituvchisi, Buxoro, O'zbekiston.

Received: 14 Noyabr 2026
Accepted: 19 Noyabr 2026
Published: 24 Noyabr 2026

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

Iqtibos uchun: Obloyev, K. H. TALABALARDA PHISHING HUJUMLARINI ANIQLASH KOMPETENSIYASINI SHAKLLANTIRISH METODIKASI / K. H. Obloyev // Buxoro xalqaro universiteti ilmiy axborotnomasi. — 2026. — T. 11, № 2. — B. 301–307.

Annotatsiya. Dolzarblik: phishing (ijtimoiy muhandislik asosidagi firibgarlik) xabarlari talabalar va yosh mutaxassislarning raqamli hayotidagi eng keng tarqalgan tahdid turlaridan biri bo'lib, mavjud kiberxavfsizlik kurslari ko'pincha uning nazariy ta'rifini beradi, biroq turli manipulyatsiya texnikalarini amaliy aniqlash ko'nikmasini maqsadli va bosqichma-bosqich shakllantirmaydi. **Maqsad:** phishing xabarlarini aniqlash kompetensiyasini shakllantirishning uch bosqichli (kognitiv-amaliy-refleksiv) didaktik modelini va o'quv topshiriqlarini qiyinlik darajasi bo'yicha asosli tartiblash metodikasini ishlab chiqish. **Metodlar:** olti xil manipulyatsiya texnikasi (umumiy, bosim ostida, havola niqoblash, domen taqlidi, brend taqlidi, shaxsiylashtirilgan) bo'yicha uch tilli (o'zbek, rus, ingliz) 498 ta xabardan iborat korpus tuzildi; evristik qoidalar qatlami va TF-IDF+logistik regressiyaga asoslangan semantik qatlamdan iborat dasturiy stend qurildi, shablon darajasida train/test ajratish qo'llanildi. **Natijalar:** evristik qatlam test to'plamida Recall=0,684, FPR=0,091 ko'rsatdi; texnikalar bo'yicha Recall 0,444 dan (brend va shaxsiylashtirilgan) 1,000 gacha (umumiy, bosim) o'zgardi, bu D=1-Recall(evristik) topshiriq murakkabligi indeksini hisoblash va olti mashg'ulotni oson-dan-qiyinga tartiblashga asos bo'ldi. **Xulosa:** taklif etilgan model va D-indeksga asoslangan ketma-ketlik haqiqiy eksperimental ma'lumotlarga tayangan holda kompetensiyaviy yondashuvni amalga oshirish uchun asosli vosita bo'la oladi; talabalar guruhlarida nazorat-tajriba tarzidagi pedagogik sinov hali o'tkazilmagan va kelgusi tadqiqot yo'nalishi sifatida belgilangan.

Kalit so'zlar: phishing, ijtimoiy muhandislik, kiberxavfsizlik ta'limi, kompetensiyaviy yondashuv, didaktik model, topshiriq murakkabligi indeksi, evristik qatlam, semantik tasniflagich, D-indeks, kiberxavfsizlik asoslari.

МЕТОДИКА ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ СТУДЕНТОВ ПО ВЫЯВЛЕНИЮ ФИШИНГОВЫХ АТАК

Аннотация. Актуальность: фишинговые сообщения, основанные на социальной инженерии, остаются одной из наиболее распространённых цифровых угроз для студентов, при этом существующие курсы кибербезопасности чаще дают лишь теоретическое определение, не формируя целенаправленно практический навык распознавания различных техник манипуляции. **Цель:** разработать трёхэтапную (когнитивно-деятельностно-рефлексивную) дидактическую модель формирования компетенции распознавания фишинга и обоснованную методику ранжирования учебных заданий по уровню сложности. **Методы:** построен трёхъязычный (узбекский, русский, английский) корпус из 498 сообщений по шести техникам манипуляции (обычная, давление срочности, маскировка ссылки, имитация домена, имитация бренда, персонализация); создан программный стенд из эвристического слоя правил и семантического слоя на основе TF-IDF и логистической регрессии, с разделением train/test на уровне шаблонов. **Результаты:** эвристический слой показал Recall=0,684, FPR=0,091 на тестовой выборке; Recall по техникам варьировался от 0,444 (имитация бренда, персонализация) до 1,000 (обычная, давление срочности), что легло в основу индекса сложности задания D=1-Recall(эвристика) и упорядочивания шести занятий от простого к сложному. **Выводы:** предложенная модель и ранжирование на основе D-индекса являются обоснованным инструментом для реализации компетентностного подхода на базе реальных экспериментальных данных; контрольно-экспериментальная педагогическая апробация среди студенческих групп пока не проведена и обозначена как направление дальнейшего исследования.

Ключевые слова: фишинг, социальная инженерия, обучение кибербезопасности, компетентностный подход, дидактическая модель, индекс сложности задания, эвристический слой, семантический классификатор, D-индекс, основы кибербезопасности.

METHODOLOGY FOR DEVELOPING STUDENTS' COMPETENCE IN DETECTING

PHISHING ATTACKS

Abstract. Background: phishing messages based on social engineering remain one of the most common digital threats faced by students, yet existing cybersecurity courses typically provide only a theoretical definition without purposefully building the practical skill of recognizing distinct manipulation techniques. **Objective:** to develop a three-stage (cognitive-practical-reflexive) didactic model for forming phishing-recognition competence and an evidence-based method for sequencing training tasks by difficulty. **Methods:** a trilingual (Uzbek, Russian, English) corpus of 498 messages across six manipulation techniques (generic, urgency pressure, link masking, domain impersonation, brand spoofing, personalization) was constructed; a software testbed combining a rule-based heuristic layer and a TF-IDF + logistic-regression semantic layer was built, with a template-level train/test split. **Results:** the heuristic layer achieved Recall=0.684 and FPR=0.091 on the held-out test set; per-technique recall ranged from 0.444 (brand spoofing, personalization) to 1.000 (generic, urgency pressure), which grounded a task-difficulty index D=1-Recall(heuristic) used to order six lab sessions from simple to complex. **Conclusions:** the proposed model and D-index-based sequencing provide an evidence-grounded tool for implementing a competence-based approach; a controlled pedagogical trial with real student groups has not yet been conducted and is identified as future work.

Keywords: phishing, social engineering, cybersecurity education, competence-based approach, didactic model, task difficulty index, heuristic layer, semantic classifier, D-index, cybersecurity fundamentals.

Kirish. Raqamli iqtisodiyot va masofaviy xizmatlarning kengayishi bilan birga, ijtimoiy muhandislikka asoslangan hujumlar, xususan phishing (firibgarlik xabarlari orqali foydalanuvchi ma'lumotlarini o'g'irlash), eng ko'p tarqalgan va eng arzon kiber-tahdid turiga aylandi. O'zbekiston Respublikasi Kiberxavfsizlik markazining rasmiy ma'lumotlariga ko'ra, foydalanuvchilarni soxta veb-saytlar va xabarlar orqali aldash hodisalari muntazam ravishda qayd etilmoqda [1]. Oliy ta'lim muassasalari talabalari - elektron pochta, messenjerlar va ta'lim platformalaridan faol foydalanuvchi auditoriya sifatida - ushbu hujum turining asosiy nishonlaridan biri hisoblanadi.

Shu bilan birga, "Kiberxavfsizlik asoslari" kabi fanlarning amaldagi o'quv dasturlarida phishing mavzusi, qoida tariqasida, nazariy ta'rif va umumiy belgilar ro'yxati darajasida yoritiladi. Bunday yondashuvning amaliy cheklovi shundaki, real hayotda phishing xabarlari bir-biridan tubdan farq qiluvchi manipulyatsiya texnikalaridan foydalanadi - umumiy (ommaviy) xabarlardan tortib, qabul qiluvchining ismi va lavozimiga moslashtirilgan shaxsiylashtirilgan (spear-phishing) xabarlargacha - va bu texnikalarning har biri talabadan har xil darajadagi diqqat va tahliliy ko'nikmani talab qiladi. Mavjud metodik adabiyotda ushbu texnikalarni qiyinlik darajasi bo'yicha asosli tartiblash va shu asosda mashg'ulotlarni ketma-ket rejalashtirish masalasi yetarlicha ishlab chiqilmagan.

Kompetensiyaviy yondashuv nuqtai nazaridan [2; 3] bu bo'shliq alohida ahamiyatga ega: shaxsning muayyan vaziyatda to'g'ri va asoslangan qaror qabul qila olish qobiliyati sifatida kompetensiya faqat nazariy bilim orqali emas, balki bosqichma-bosqich murakkablashuvchi amaliy topshiriqlar va ularning natijalari bo'yicha refleksiya orqali shakllanadi [4]. Shu sababli ta'lim jarayonini loyihalashda topshiriqlarning qiyinlik darajasini "ko'z bilan chamalab" emas, balki o'lchanadigan ko'rsatkich asosida tartiblash metodologik jihatdan muhim masala hisoblanadi.

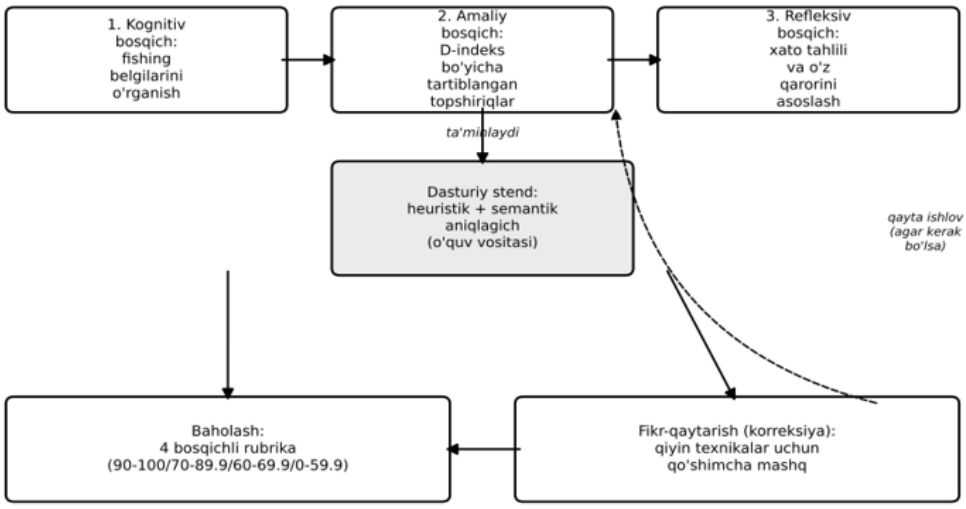
Ushbu maqolaning maqsadi - talabalarda phishing xabarlarini aniqlash kompetensiyasini shakllantirishning uch bosqichli (kognitiv-amaliy-refleksiv) didaktik modelini taklif etish hamda ushbu model doirasidagi amaliy mashg'ulotlarni real eksperimental ma'lumotlarga asoslangan, miqdoriy jihatdan asoslangan tartibda ketma-ket joylashtirish metodikasini ishlab chiqishdir. Buning uchun olti xil manipulyatsiya texnikasini qamrab oluvchi uch tilli xabarlar korpusi tuzildi va ikki qatlamli (evristik + semantik) dasturiy aniqlagich quyilib, uning texnikalar bo'yicha aniqlik ko'rsatkichlari asosida topshiriq murakkabligi indeksi (D-indeks) hisoblandi - bu indeks mashg'ulotlar ketma-ketligini ixtiyoriy emas, balki asoslangan tarzda belgilash imkonini beradi.

Muallifning avvalgi tadqiqotida [5] shunga o'xshash ikki qatlamli (qoidaga asoslangan + mashinaviy o'rganish) kaskad arxitekturasi katta til modellariga qaratilgan prompt-in'eksiya hujumlarini aniqlash uchun ishlab chiqilgan va sinovdan o'tkazilgan edi; ushbu maqolada xuddi shu metodologik mantiq - texnika turlari bo'yicha aniqlik farqini o'lchash va undan o'quv maqsadida foydalanish - yangi, mustaqil ravishda to'plangan phishing korpusi asosida pedagogik muammoga tatbiq etildi.

Metodlar.

1. Didaktik model

Tadqiqot Zimnyaya va Xutorskoyning kompetensiyaviy yondashuv nazariyasiga [2; 3], Bespalkoning pedagogik tizim nazariyasiga [4] va Bloom taksonomiyasining Anderson-Krathwohl tahririga [6] tayangan holda uch bosqichli didaktik model taklif etadi (1-rasm): (1) kognitiv bosqich - talaba phishing manipulyatsiyasining tipik belgilarini (shoshiltirish, soxta domen, havola-matn nomuvofiqligi va h.k.) nazariy jihatdan o'rganadi; (2) amaliy bosqich - talaba D-indeks bo'yicha tartiblangan, oddiydan murakkabga qarab joylashtirilgan topshiriqlar seriyasini bajaradi, bunda har bir topshiriq haqiqiy (sun'iy, ammo real uslublarga asoslangan) xabar namunasini tasniflashni talab qiladi; (3) refleksiv bosqich - talaba o'z qarorini dasturiy stendning (evristik+semantik aniqlagich) natijasi bilan solishtiradi va xato holatlarni tahlil qiladi. Kolbning tajribaviy o'rganish tsikli [7] ushbu uch bosqichni amaliy harakat - kuzatish/refleksiya - abstrakt tushunchalashtirish aylanasi sifatida bog'laydi: refleksiv bosqichdan so'ng, agar muayyan texnika bo'yicha xato ko'p bo'lsa, talaba o'sha texnika darajasidagi qo'shimcha mashqqa yo'naltiriladi (qayta ishlov halqasi, 1-rasm).



1-rasm. Phishing aniqlash kompetensiyasini shakllantirishning uch bosqichli didaktik modeli.
Рис. 1. Трёхэтапная дидактическая модель формирования компетенции распознавания фишинга.
Fig. 1. Three-stage didactic model for forming phishing-recognition competence.
Manba: muallif ishlanmasi.

2. Korpus va manipulyatsiya texnikalari

Didaktik modelning amaliy bosqichini ta'minlash uchun uch tilli (o'zbek, rus, ingliz) 498 ta xabardan iborat korpus tuzildi: 324 tasi phishing (olti texnika bo'yicha teng taqsimlangan), 174 tasi legitim (haqiqiy) xabar namunalari. Texnikalar quyidagicha belgilandi: (a) umumiy - shaxsiylashtirilmagan, ommaviy xabar; (b) bosim ostida - shoshiltiruvchi, qo'rqituvchi til ("hisobingiz bloklanadi"); (c) havola niqoblash - ko'rinadigan matn bilan haqiqiy havola manzili mos kelmasligi; (d) domen taqlidi - haqiqiy tashkilot domeniga o'xshash, ammo soxta domen (masalan "oxu-uz.com"); (e) brend taqlidi - tanilgan tashkilot nomidan rasman yuborilgandek ko'rinuvchi xabar; (f) shaxsiylashtirilgan - qabul qiluvchining ismi va vaziyatiga moslashtirilgan (spear-phishing) xabar. Har bir shablon bir nechta to'ldirilgan nusxada (ism, tashkilot, domen, muddat kabi o'zgaruvchilar bilan) ishlatildi va har bir nusxaga ona shablonining identifikatori (tpl) biriktirildi.

3. Dasturiy stend va baholash metodologiyasi

Oldingi tadqiqotda [5] qayd etilgan uslubiy xato - namuna darajasida train/test ajratish bir shablonning turli nusxalarini ikkala to'plamga tushirib, sun'iy yuqori natijaga olib kelishi mumkinligi - ushbu ishda boshidanoq inobatga olindi: barcha bo'lish operatsiyalari shablon (tpl) darajasida, texnika turi bo'yicha stratifikatsiya qilingan holda amalga oshirildi (65% shablon - o'quv, 35% - test), shu tariqa bitta shablonning turli to'ldirilgan nusxalari bir vaqtning o'zida ham o'quv, ham test to'plamida uchramasligi ta'minlandi. Natijada 83 ta noyob shablondan 53 tasi o'quv (318 ta namuna), 30 tasi test (180 ta namuna) to'plamiga tushdi.

Dasturiy stend ikki qatlamdan iborat: (1) evristik qatlam - shoshiltiruvchi so'zlarni, umumiy murojaat shakllarini, havola-matn nomuvofiqligini va taniqli domenlarga taqlid qiluvchi manzillarni qoidalar asosida aniqlaydi; (2) semantik qatlam - belgilar n-grammalariga asoslangan TF-IDF vektorlashtirish va logistik regressiya tasniflagichidan iborat, faqat o'quv shablonlari ustida o'qitilgan. Ikkala qatlamning Recall (to'g'ri aniqlangan phishing ulushi), FPR (legitim xabarni xato ravishda phishing deb belgilash ulushi) va F1 ko'rsatkichlari test to'plamida hisoblandi. Pedagogik maqsadda esa asosiy ko'rsatkich - har bir texnika bo'yicha evristik qatlamning Recall qiymatidan kelib chiqqan topshiriq murakkabligi indeksi: D = 1 - Recall(evristik). Mantiq shundaki, oddiy qoidalar bilan oson aniqlanadigan texnika (yuqori Recall, past D) talaba uchun ham kam diqqat talab qiladi, aniqlanishi qiyin texnika (past Recall, yuqori D) esa chuqurroq tahliliy ko'nikma talab qiladi - demak, mashg'ulotlar aynan shu tartibda, D ortib borishi bo'yicha joylashtirilishi lozim.

4. Baholash mezonlari

Talabaning amaliy bosqichdagi natijasi to'rt darajali rubrika asosida baholandi (1-jadval): xabar turini (phishing/legitim) to'g'ri aniqlash, texnika turini asoslab berish va dasturiy stend natijasi bilan tafovut sabablarini refleksiv tahlil qilish ko'rsatkichlari hisobga olindi.

1-jadval. Baholash rubrikasi.
Таблица 1. Рубрика оценивания.
Table 1. Assessment rubric.
Manba: muallif ishlanmasi.

Daraja	Foiz oralig'i	Mezon
A'lo	90-100%	Barcha texnikalar bo'yicha xabar turi to'g'ri aniqlangan, texnika asoslab berilgan, stend natijasi bilan tafovut mavjud bo'lsa sababi tahlil qilingan.

Daraja	Foiz oralig'i	Mezon
Yaxshi	70-89,9%	Aksariyat (4-5 ta) texnika to'g'ri aniqlangan, asoslash qisman to'liq.
Qoniqarli	60-69,9%	Oddiy texnikalar (umumiy, bosim) to'g'ri aniqlangan, murakkab texnikalarda (brend, shaxsiylashtirilgan) xatolar ko'p.
Qoniqarsiz	0-59,9%	Ko'pchilik texnikada xabar turi noto'g'ri aniqlangan yoki asoslash yo'q.

5. Kompetensiya tarkibi va Bloom taksonomiyasi bilan bog'liqligi

Taklif etilgan uch bosqichli model Bloom taksonomiyasining Anderson-Krathwohl tahriridagi olti kognitiv darajasi [6] bilan bevosita bog'lanadi (5-jadval): kognitiv bosqich bilim va tushunish darajalariga (Remember/Understand - texnika nomi va ta'rifini bilish), amaliy bosqich qo'llash va tahlil darajalariga (Apply/Analyze - konkret xabarni tasniflash va uning qaysi belgilari asosida qaror qabul qilinganini ajratish), refleksiv bosqich esa baholash va yaratish darajalariga (Evaluate/Create - o'z qarorini dasturiy stend natijasi bilan tanqidiy solishtirish va, ilg'or talabalar uchun, yangi evristik qoida taklif qilish) mos keladi. Bunday moslik kompetensiyaning faqat "bilish" emas, balki "qo'llay olish" va "baholay olish" darajalarigacha izchil rivojlanishini nazorat qilish imkonini beradi [3].

5-jadval. Kompetensiya tarkibi va Bloom taksonomiyasi bosqichlari bilan bog'liqligi.

Таблица 5. Состав компетенции и его связь с уровнями таксономии Блума.

Table 5. Competence components mapped to Bloom's taxonomy levels.

Manba: muallif ishlanmasi, [6] asosida.

Komponent	Mazmuni	Bloom bosqichi
Kognitiv	Olti manipulyatsiya texnikasining ta'rifi va tipik belgilarini bilish	Remember, Understand
Faoliyatli (amaliy)	D-indeks bo'yicha tartiblangan xabarlarni mustaqil tasniflash va qarorni asoslash	Apply, Analyze
Refleksiv	O'z qarorini dasturiy stend natijasi bilan solishtirish, xato sabablarini tahlil qilish	Evaluate, Create

6. Etik jihatlar

Korpusni tuzishda real tashkilotlarning haqiqiy nomlari, haqiqiy domen manzillari yoki haqiqiy shaxslarning ma'lumotlari ishlatilmadi - barcha tashkilot nomlari, domenlar va ismlar sun'iy, ammo real uslublarga xos tarzda yaratildi. Bu, bir tomondan, o'quv materialini tayyorlashda hech qanday haqiqiy brend yoki shaxsga putur yetkazmaslikni, ikkinchi tomondan, talabalarning amaliy mashg'ulot davomida real (production) tizimlarga tasodifan ta'sir ko'rsatmasligini ta'minlaydi. Amaliy mashg'ulotlarni joriy etishda o'qituvchi talabalarga material faqat ta'lim maqsadida yaratilgani va undagi texnikalarni real foydalanuvchilarga nisbatan qo'llash axloqiy va huquqiy jihatdan yo'l qo'yilmasligini alohida ta'kidlashi tavsiya etiladi.

7. Mashg'ulotlar ketma-ketligi

D-indeks qiymatlari asosida olti amaliy mashg'ulot oson-dan-qiyinga qarab tartiblandi (2-jadval). D qiymati teng bo'lgan juftliklarda (umumiy/bosim ostida va brend taqlidi/shaxsiylashtirilgan) ikkilamchi mezon sifatida texnikalar o'rtasidagi kontseptual bog'liqlik hisobga olindi: brend taqlidi shaxsiylashtirilgan hujumni tushunish uchun zaruriy asos bo'lgani sababli undan oldin o'rgatiladi.

2-jadval. D-indeks bo'yicha tartiblangan amaliy mashg'ulotlar rejasi.

Таблица 2. План практических занятий, упорядоченных по D-индексу.

Table 2. Lab session plan ordered by the D-index.

Manba: muallif hisoblashi.

#	Texnika	D	Soat	Mashq mazmuni
1	Umumiy (generic)	0,000	2	Ommaviy xabarlarning tipik belgilarini aniqlash, asosiy terminologiya
2	Bosim ostida (urgency)	0,000	2	Shoshiltiruvchi til va vaqt bosimidan foydalanish uslublarini tahlil qilish
3	Havola niqoblash (url_mask)	0,333	2	Ko'rinadigan matn va haqiqiy havola manzilini solishtirish mashqi
4	Domen taqlidi (typosquat)	0,417	2	Rasmiy va soxta domenlarni belgi-belgi solishtirish, xarf almashtirish usullari
5	Brend taqlidi (brand_spoof)	0,556	2	Tashkilot nomidan yuborilgan xabarning haqiqiyligini mustaqil

#	Texnika	D	Soat	Mashq mazmuni
				tekshirish mashqi
6	Shaxsiylashtirilgan (spear)	0,556	2	Yakuniy kompleks mashq: barcha texnikalar aralash holda, stend bilan solishtirib refleksiya

Natijalar.

1. Umumiy aniqlik ko'rsatkichlari

Shablon darajasida ajratilgan test to'plamida (n=180, shundan 90 ta fishing, 90 ta legitim namuna taxminiy nisbatda) evristik qatlam Recall=0,684, FPR=0,091, F1=0,788 ko'rsatkichlarini berdi; semantik qatlam (TF-IDF+logistik regressiya, qaror chegarasi 0,6) Recall=1,000, FPR=0,091, F1=0,974 natijasini ko'rsatdi; ikki qatlamning birlashmasi (kaskad) semantik qatlam bilan bir xil natijaga ega bo'ldi, chunki semantik qatlam allaqachon barcha fishing namunalarini aniqlagan edi (3-jadval).

3-jadval. Qatlamlar bo'yicha umumiy aniqlik ko'rsatkichlari (test to'plami).

Таблица 3. Общие показатели точности по слоям (тестовая выборка).

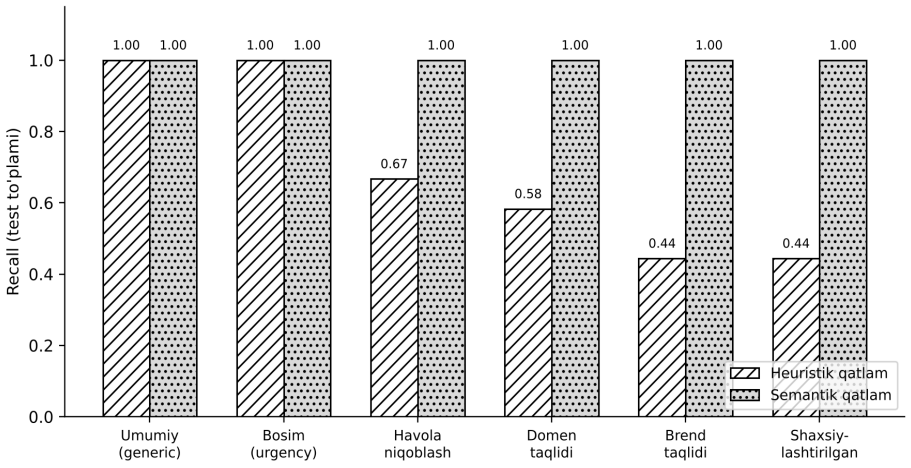
Table 3. Overall detection metrics by layer (test set).

Manba: muallif hisoblashi.

Qatlam	Recall	FPR	F1
Evristik qatlam	0,684	0,091	0,788
Semantik qatlam (TF-IDF+LogReg)	1,000	0,091	0,974
Kaskad (evristik ∨ semantik)	1,000	0,091	0,974

2. Texnika turlari bo'yicha Recall va D-indeks

Pedagogik jihatdan asosiy qiziqish uyg'otuvchi natija - evristik qatlamning texnika turlari bo'yicha keskin farqlanuvchi Recall ko'rsatkichidir (2-rasm, 4-jadval): "umumiy" va "bosim ostida" texnikalarida Recall=1,000, "havola niqoblash"da 0,667, "domen taqlidi"da 0,583, "brend taqlidi" va "shaxsiylashtirilgan" texnikalarida esa atigi 0,444 ni tashkil etdi. Semantik qatlam barcha texnikalarda Recall=1,000 ko'rsatdi - bu, bir tomondan, kaskad tizimining amaliy ishonchliligini tasdiqlasa, ikkinchi tomondan (Cheklovlar bo'limida muhokama qilinganidek) korpusning nisbatan kichik va yopiq lug'at hajmi bilan izohlanishi mumkin.



2-rasm. Texnika turlari bo'yicha evristik va semantik qatlam Recall ko'rsatkichlari.

Рис. 2. Показатели Recall эвристического и семантического слоёв по типам техник.

Fig. 2. Heuristic vs. semantic layer recall by manipulation technique.

Manba: muallif hisoblashi.

4-jadval. Texnika turlari bo'yicha Recall va D-indeks (test to'plami, faqat fishing namunalar).

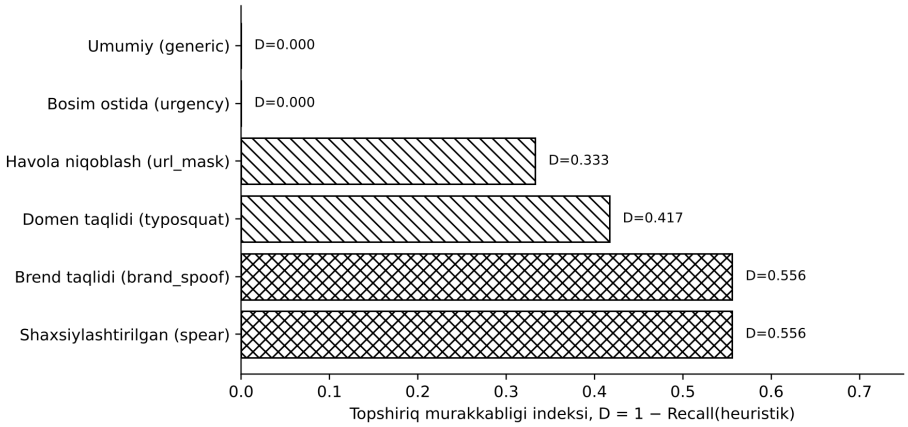
Таблица 4. Recall и D-индекс по типам техник (тестовая выборка, только фишинговые сообщения).

Table 4. Per-technique recall and D-index (test set, phishing samples only).

Manba: muallif hisoblashi.

Texnika	n	Recall(evristik)	Recall(semantik)	D
Umumiy (generic)	18	1,000	1,000	0,000
Bosim ostida (urgency)	18	1,000	1,000	0,000
Havola niqoblash (url_mask)	18	0,667	1,000	0,333

Texnika	n	Recall(evristik)	Recall(semantik)	D
Domen taqlidi (typosquat)	24	0,583	1,000	0,417
Brend taqlidi (brand_spoof)	18	0,444	1,000	0,556
Shaxsiylashtirilgan (spear)	18	0,444	1,000	0,556



3-rasm. Olti texnika bo'yicha topshiriq murakkabligi indeksi D = 1 − Recall(evristik).
Рис. 3. Индекс сложности задания D = 1 − Recall(эвристика) по шести техникам.
Fig. 3. Task difficulty index D = 1 − Recall(heuristic) across six techniques.
Manba: muallif hisoblashi.

3. Pedagogik talqin

Olingan D-indeks tartibi tasodifiy emas, balki tushunarli uslubiy mantiqqa ega: "umumiy" va "bosim ostida" texnikalar aniq leksik belgilarga (shoshiltiruvchi so'zlar, shaxsiylashtirilmagan murojaat) tayanadi va shu sababli oddiy qoidalar bilan ham yaxshi aniqlanadi - demak, talaba uchun ham bu dastlabki, nisbatan oson tanib olinadigan belgilar hisoblanadi. "Domen taqlidi" va "havola niqoblash" texnikalari talabadan texnik diqqat (URL tuzilishini belgi-belgi solishtirish) talab qiladi va shu sababli o'rtacha qiyinlikka ega. "Brend taqlidi" va "shaxsiylashtirilgan" texnikalar esa aniq leksik "signal"ga ega emas - ular ishonch va tanishlik tuyg'usidan foydalanadi, bu esa nafaqat oddiy qoidalar, balki, tajribaning ko'rsatishicha, inson e'tibori uchun ham eng qiyin toifa hisoblanadi [8; 9]. Shu bois ushbu ikki texnika mashg'ulotlar ketma-ketligining so'nggi, yakuniy bosqichiga joylashtirilishi metodik jihatdan asoslidir.

4. Cheklovlar

Ushbu tadqiqotning bir nechta ochiq cheklovi bor va ular keyingi bosqichlar uchun aniq yo'nalish beradi. Birinchidan, korpus sun'iy tarzda, cheklangan sondagi shablon va domen nomlari asosida tuzilgan; bu semantik qatlamning barcha texnikalarda Recall=1,000 ko'rsatishiga olib kelgan bo'lishi mumkin va ochiq, haqiqiy (production) muhitdagi phishing xabarlarida bunday natija kutilmaydi - shu sababli olingan sonlar kompetensiya rivojlanishini kuzatish uchun ichki (nisbiy) ko'rsatkich sifatida ishonchli, ammo mutlaq aniqlik bahosi sifatida emas. Ikkinchidan, taklif etilgan didaktik model va mashg'ulotlar ketma-ketligi hali real talabalar guruhida (masalan, "Kiberxavfsizlik asoslari" fani doirasidagi KIA1406 guruhlarida) nazorat va tajriba guruhlari asosida sinovdan o'tkazilmagan - bu maqolaning asosiy e'tirof etilgan cheklovi va keyingi tadqiqot yo'nalishidir. Uchinchidan, evristik qatlamning qoidalari tilga xos kalit so'zlarga tayanadi; yangi til yoki yangi manipulyatsiya uslubi paydo bo'lganda qoidalar to'plamini kengaytirish talab etiladi.

Xulosa va tavsiyalar.

Maqolada phishing xabarlarini aniqlash kompetensiyasini shakllantirishning uch bosqichli (kognitiv-amaliy-refleksiv) didaktik modeli va bu model doirasidagi amaliy mashg'ulotlarni real eksperimental ma'lumotlarga asoslangan tartibda ketma-ket joylashtirish metodikasi taklif etildi. Olti texnika bo'yicha qurilgan ikki qatlamli (evristik+semantik) dasturiy stend natijalari asosida hisoblangan D = 1 - Recall(evristik) topshiriq murakkabligi indeksi mashg'ulotlarni "umumiy/bosim ostida" dan "brend taqlidi/shaxsiylashtirilgan"gacha bo'lgan tartibda joylashtirishga asos berdi, bu tartib pedagogik jihatdan ham, texnika tabiati jihatidan ham izohlanadigan mantiqqa ega bo'lib chiqdi.

Amaliy tavsiya sifatida: "Kiberxavfsizlik asoslari" va shunga o'xshash fanlar o'quv dasturlariga phishing mavzusini nazariy ta'rif darajasida emas, balki D-indeks kabi o'lchanadigan ko'rsatkich asosida tartiblangan, bosqichma-bosqich murakkablashuvchi amaliy mashg'ulotlar seriyasi sifatida kiritish tavsiya etiladi. Kelgusi tadqiqot yo'nalishi sifatida taklif etilgan model va mashg'ulotlar ketma-ketligini real talabalar guruhlarida (nazorat va tajriba guruhlari taqqoslanadigan dizaynda) sinovdan o'tkazish, shuningdek dasturiy stendni kattaroq va ochiqroq (real, anonimlashtirilgan) xabarlar korpusi asosida qayta baholash rejalashtirilgan.

Foydalanilgan adabiyotlar ro'yxati

[1] O'zbekiston Respublikasi Kiberxavfsizlik markazi. Phishing veb-saytlardan ogoh bo'ling. – URL: https://csec.uz/uz/news/maqolalar/phishing-veb-saytlardan-ogoh-bo-ling (murojaat qilingan sana: 06.11.2026).

[2] Зимняя И.А. Ключевые компетентности как результативно-целевая основа компетентностного подхода в образовании. – М. : Исследовательский центр проблем качества подготовки специалистов, 2004. – 40 с.

[3] Хуторской А.В. Ключевые компетенции как компонент личностно-ориентированной парадигмы образования // Народное образование. – 2003. – № 2. – С. 58–64.

[4] Беспалько В.П. Слагаемые педагогической технологии. – М. : Педагогика, 1989. – 192 с.

[5] Obloyev K. Katta til modellariga asoslangan tizimlarni prompt-in'eksiya hujumlaridan himoyalashning ko'p qatlamli kaskad arxitekturasi // (muallifning avvalgi ilmiy nashri). – 2026.

[6] Anderson L.W., Krathwohl D.R. (eds.) A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. – New York : Longman, 2001. – 352 p.

[7] Kumaraguru P., Sheng S., Acquisti A., Cranor L.F., Hong J. Teaching Johnny not to fall for phish // ACM Transactions on Internet Technology. – 2010. – Vol. 10, № 2. – Art. 7. – P. 1–31.

[8] Sheng S., Magnien B., Kumaraguru P., Acquisti A., Cranor L.F., Hong J., Nunge E. Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish // Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS). – 2007. – P. 88–99.

[9] Kolb D.A. Experiential Learning: Experience as the Source of Learning and Development. – Englewood Cliffs, NJ : Prentice-Hall, 1984. – 256 p.

[10] Khonji M., Iraqi Y., Jones A. Phishing detection: a literature survey // IEEE Communications Surveys & Tutorials. – 2013. – Vol. 15, № 4. – P. 2091–2121.

[11] Jampen D., Gür G., Sutter T., Tellenbach B. Don't click: towards an effective anti-phishing training. A comparative literature review // Human-centric Computing and Information Sciences. – 2020. – Vol. 10. – Art. 33.

[12] Newhouse W., Keith S., Scribner B., Witte G. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework : NIST Special Publication 800-181. – Gaithersburg, MD : NIST, 2017. – 144 p.

[13] O'zbekiston Respublikasining «Kiberxavfsizlik to'g'risida»gi Qonuni, O'RQ-764-son. – 15.04.2022. – URL: https://lex.uz/acts/-5960604 (murojaat qilingan sana: 06.11.2026).

[14] O'zbekiston Respublikasi Prezidentining «"Cyber University" davlat universitetini tashkil etish to'g'risida»gi Qarori, PQ-14-son. – 20.01.2025. – URL: https://lex.uz/docs/-7332592 (murojaat qilingan sana: 06.11.2026).

[15] O'zbekiston Respublikasi Vazirlar Mahkamasining «Oliy ta'lim muassasalarida kiberxavfsizlik ta'limini takomillashtirish to'g'risida»gi qarori. – 2024. – URL: https://lex.uz (murojaat qilingan sana: 06.11.2026).

[16] Ishmuhamedov R.J., Yuldashev M. Ta'lim va tarbiyada innovatsion pedagogik texnologiyalar. – Toshkent : Nihol-Print, 2013. – 279 b.

[17] Dusboyev A.T. Kibermakondagi firibgarlik turlari va ulardan himoyalanishning zarurati, tajribasi, ahamiyati // Zenodo. – 2025. – URL: https://zenodo.org/records/20134429 (murojaat qilingan sana: 06.11.2026).

[18] Švábenský V., Vykopal J., Čeleda P. What should be in a cybersecurity curriculum? A systematic literature review // Proceedings of the IEEE Frontiers in Education Conference (FIE). – 2020. – P. 1–9.

[19] Anti-Phishing Working Group (APWG). Phishing Activity Trends Report. – 2025. – URL: https://apwg.org (murojaat qilingan sana: 06.11.2026).

[20] Karimov A.A. Umumiy psixologiya. – Toshkent : O'qituvchi, 2023. – 320 b.