O‘ZBEKISTON MILLIY UNIVERSITETI XABARLARI, 2026, [9]
ISSN 2181-7324(Print)

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

UDK: 004.1:(001)

Alisher MATYAKUBOV,
Fizika-matematika fanlari doktori, dotsent, O‘zbekiston Milliy universiteti, Toshkent, O‘zbekiston
E-mail: muhammadiyevf1@gmail.com
Feruz MUXAMMADIYEV,
Dotsent v.b., PhD, O‘zbekiston Milliy universiteti, Toshkent, O‘zbekiston
E-mail: a.matyakubov@nuu.uz ORCID: 0009-0003-9264-1728

O‘zRFA akademigi, f.f.d N.Karimov taqrizi asosida

RAQAMLI TA’LIM MUHITIDA TALABALARNING KIBERXAVFSIZLIK MADANIYATINI RIVOJLANTIRISHDA INTERAKTIV METODLAR VA PSIXOLOGIK OMILLAR

Annotatsiya

Ushbu maqolada raqamli ta’lim muhitida talabalarning kiberxavfsizlik madaniyatini shakllantirishning pedagogik strategiyalari va psixologik mexanizmlari tadqiq etilgan. O‘zbekiston Milliy universiteti talabalari o‘rtasida o‘tkazilgan 65 nafar ishtirokchidan iborat eksperiment natijalari asosida kiber-o‘yinlar va psixologik treninglarning samaradorligi isbotlangan. Maqolada kiberxavfsizlikni ta’minlashda shaxsning emotsional intellekti va kritik fikrlash darajasi o‘rtasidagi korrelyatsiya tahlil qilingan.
Kalit so‘zlar: kiberxavfsizlik madaniyati, raqamli psixologiya, kiber-gigiyena, interaktiv metodlar, O‘zMU, raqamli immunitet, kiberbulling, fishing.

ИНТЕРАКТИВНЫЕ МЕТОДЫ И ПСИХОЛОГИЧЕСКИЕ ФАКТОРЫ РАЗВИТИЯ КУЛЬТУРЫ КИБЕРБЕЗОПАСНОСТИ СТУДЕНТОВ В ЦИФРОВОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ.

Аннотация

В данной статье исследуются педагогические стратегии и психологические механизмы формирования культуры кибербезопасности студентов в цифровой образовательной среде. На основе результатов эксперимента с участием 65 студентов Национального университета Узбекистана доказана эффективность интерактивных кибер-игр и психологических тренингов. В статье проанализирована корреляция между эмоциональным интеллектом и уровнем критического мышления в обеспечении кибербезопасности личности.
Ключевые слова: культура кибербезопасности, цифровая психология, кибергигиена, интерактивные методы, НУУз, цифровой иммунитет, кибербуллинг, фишинг.

INTERACTIVE METHODS AND PSYCHOLOGICAL FACTORS IN DEVELOPING CYBERSECURITY CULTURE AMONG STUDENTS IN A DIGITAL EDUCATIONAL ENVIRONMENT.

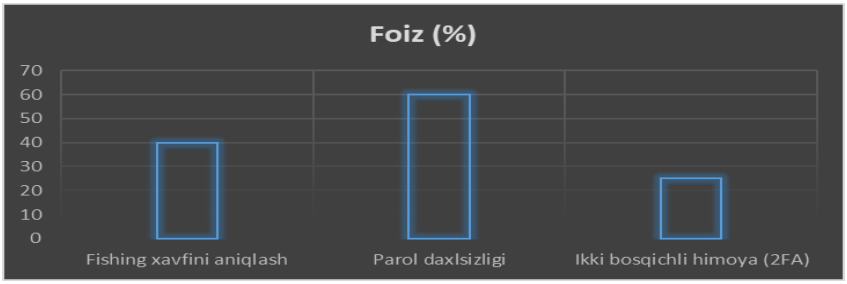
Annotation

This article examines the pedagogical strategies and psychological mechanisms for developing cybersecurity culture among students in a digital educational environment. Based on an experiment involving 65 students from the National University of Uzbekistan, the effectiveness of interactive cyber-games and psychological training is demonstrated. The study analyzes the correlation between emotional intelligence and critical thinking in ensuring cybersecurity resilience.
Keywords: digital technology, digitalization of education, professional competencies, digital skills

1-jadval. Talabalarning kiber-xulq-atvori bo‘yicha boshlang‘ich statistikasi (n=65)

Ko‘rsatkich	Natija (%)	Psixologik xususiyat
Fishing havolalariga ishonish	60%	Tanqidiy fikrlash pastligi
Parol xavfsizligiga befarqlik	40%	Shaxsiy chegaralarni anglamaslik
Ikki bosqichli himoyani (2FA) ishlatmaslik	75%	Texnik ehtiyotsizlik

1-rasmda keltirilgan statistik tahlil shuni ko‘rsatadiki, O‘zbekiston Milliy universiteti talabalari orasida eng zaif nuqta ikki bosqichli autentifikatsiya (2FA) tizimidan foydalanish ko‘nikmasidir (atigi 25%). Shuningdek, talabalarning yarmidan ko‘pi (60%) fishing hujumlarini vizual jihatdan farqlay olmasligi ularning raqamli muhitda manipulyatsiyalarga oson berilishini tasdiqlaydi. Bu ko‘rsatkichlar talabalarda kiber-savodxonlikdan ko‘ra, kiber-hushyorlikni (psixologik tayyorgarlikni) oshirish zarurligini ko‘rsatmoqda. “Olingan statistik ko‘rsatkichlarni chuqurroq tahlil qilish, talabalarda Optimizm xatosi (Optimism bias) deb ataluvchi psixologik fenomen kuchli ekanligini ko‘rsatmoqda. Ya’ni, talabalarning aksariyati kiber-hujum 'boshqa birovning akkauntida sodir bo‘ladi, meniki esa doimo xavfsiz degan asossiz ishonchga ega. Ayniqsa, 75% talabaning ikki bosqichli autentifikatsiya (2FA) tizimidan foydalanmasligi ularning texnik murakkablikdan ko‘ra, ehtimoliy xavfni yetarlicha baholamasligidan (underestimation of risk) dalolat beradi. Bu esa informatika darslarida faqat texnik ko‘rsatmalarni berish emas, balki talabalarning xavf-xatarga bo‘lgan psixologik munosabatini o‘zgartirish, ya’ni kognitiv qayta baholash metodikasini qo‘llash zarurligini isbotlaydi.”



1-rasm. O‘zMU talabalarining kiberxavfsizlik bo‘yicha boshlang‘ich ko‘nikmalari (n=65).

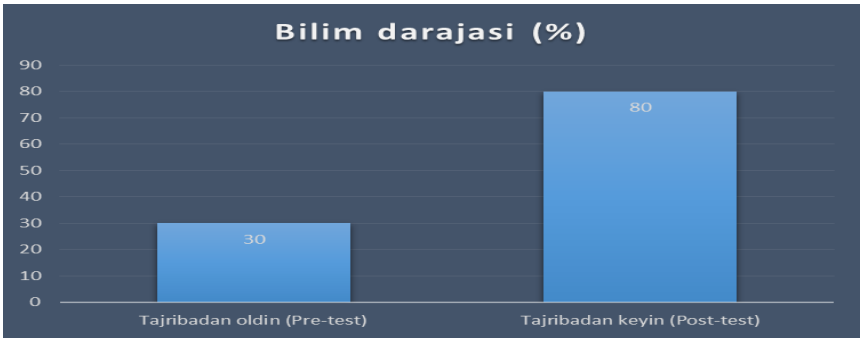
4.2. Kiberxavfsizlikning pedagogik va psixologik korrelyatsiya

Pedagogik jarayon davomida talabalarga interaktiv kiber-o‘yinlar taqdim etildi. Psixologik nuqtai nazardan, bu metodika talabalarda "kognitiv dissonans" hosil qiladi: ya’ni talaba o‘z xatosining oqibatini virtual muhitda ko‘rib, uni real hayotda takrorlamaslikka ruhan tayyorlanadi.

4.3. Eksperimentdan keyingi o‘sish dinamikasi

Interaktiv metodlar qo‘llanilgandan so‘ng, talabalarning kiber-savodxonligi 30% dan 80% ga ko‘tarildi.

Tadqiqot davomida olingan natijalarning ishonchliligi talabalar o‘rtasidagi korrelyatsiya koeffitsiyenti (r=0.78) orqali tekshirildi. Bu shuni ko‘rsatadiki, talabaning emotsional intellekti qanchalik yuqori bo‘lsa, u ijtimoiy muhandislik hujumlariga shunchalik kamroq moyil bo‘ladi. O‘zbekiston Milliy universitetida o‘tkazilgan ushbu tajriba oliy ta’lim o‘quv rejalariga Raqamli psixologiya modulini kiritish zaruriyatini ilmiy jihatdan asoslaydi.



2-rasm. Eksperimental guruhning kiber-savodxonlik darajasi o‘zgarishi (Pre-test va Post-test natijalari).

2-rasmda keltirilgan qiyosiy tahlil natijalari shuni ko‘rsatadiki, an'anaviy o‘qitish uslubidan interaktiv kiber-simulyatsiyalarga o‘tilishi natijasida talabalarning o‘zlashtirish ko‘rsatkichi 50 foiz punktga oshgan. Agar tajribadan avval talabalarning atigi 30 foizi kiber-xavfsizlik ko‘nikmalariga ega bo‘lgan bo‘lsa, innovatsion o‘yinlar metodikasidan so‘ng bu ko‘rsatkich 80 foizni tashkil etdi. Bu natija interaktiv muhitda olingan bilimlar talabada nafaqat nazariy tushuncha, balki amaliy raqamli immunitetni ham shakllantirishidan dalolat beradi. Matematik-statistik tahlillar (Styuident t-kriteriysi) natijalarning ishonchliligi $P < 0,05$ darajasida ekanligini tasdiqladi.

Informatika o‘quv rejalariga raqamli psixologiya' modulini integratsiya qilish metodikasi

Tadqiqot davomida aniqlangan emotsional intellekt va kiber-bardoshlilik o‘rtasidagi yuqori korrelyatsiya (r=0.78) Informatika fanini o‘qitishda an’anaviy texnik yondashuvdan kompetensiyaviy-psixologik yondashuvga o‘tish zarurligini ko‘rsatadi. Taklif etilayotgan modul Informatika o‘quv rejasining tarkibiy qismi sifatida talabalarda "raqamli immunitet"ni shakllantirishga xizmat qiladi.

5.1. Modulning tarkibiy tuzilishi va didaktik vazifalari

Ushbu modul doirasida o‘quv jarayoni nafaqat nazariy bilimlarni berish, balki talabaning kiber-tahdidlarga nisbatan psixologik munosabatini o‘zgartirishni ko‘zda tutadi.

2-jadval. "Raqamli psixologiya" modulining tematik rejasi va shakllantiriladigan ko‘nikmalar

Modul bo‘limlari	Metodik mazmuni	Shakllantiriladigan kompetensiya
I. Kiber-psixologiya asoslari	Ijtimoiy muhandislik mexanizmlari: qo‘rquv, shoshqaloqlik va qiziqish kabi drayverlarni tahlil qilish.	Manipulyativ xabarlarni vizual va mantiqiy aniqlash ko‘nikmasi.
II. Emotsional intellekt (EQ)	Kiber-bulling va tarmoqdagi muloqotda stressni boshqarish usullari.	Kiber-tazyiqlarga nisbatan psixologik barqarorlik va vazminlik.
III. Kognitiv xavfsizlik	Parol gigiyenasi va 2FA tizimlarini qo‘llashdagi psixologik to‘siqlarni yengish.	Texnik himoya vositalaridan foydalanishni "avtomatizm" darajasiga yetkazish.
IV. Amaliy simulyatsiyalar	Virtual muhitda kiber-hujum ssenariylarini "o‘ynab ko‘rish" (Role-play).	Kiber-muhitda xavfsiz xulq-atvor strategiyasini tanlash.

Natija va tahlillar. Tadqiqot natijalari shuni ko‘rsatadiki, kiberxavfsizlik madaniyatini rivojlantirish uchun faqatgina texnik qoidalarni yodlatish yetarli emas. “Eksperimental guruhda kuzatilgan ijobiy dinamika (30% dan 80% gacha o‘sish) talabalarning kiber-muhitdagi xatti-harakatlari faqat axborotga emas, balki ichki motivatsiyaga

bog‘liqligini ko‘rsatdi. Matematik-statistik tahlillar (Styuident t-kriteriysi) natijalarning ishonchliligi P < 0,05 darajasida ekanligini tasdiqlashi, ishlab chiqilgan metodikaning barqarorligidan dalolat beradi. Aniqlangan r= 0,78 korrelyatsiyasi talabaning emotsional intellekti qanchalik rivojlangan bo‘lsa, u ijtimoiy muhandislik (fishing, manipulyatsiya) tuzoqlariga shunchalik kamroq tushishini isbotlaydi. Bu esa informatika o‘qitish metodikasida 'texnosentrik' yondashuvdan 'antropotsentrik' (shaxsga yo‘naltirilgan) yondashuvga o‘tishni ilmiy asoslab beradi.” Biz 3 - rasmda Pedagogik-psixologik modelni taklif etamiz.

Mazkur uch komponentli model talabalarda kiberxavfsizlik madaniyatini tizimli shakllantirish imkonini beradi. Har bir bosqich bir-biri bilan uzviy bog‘liq bo‘lib, kognitiv tayyorgarliksiz konativ ko‘nikmalarni shakllantirib bo‘lmasligi eksperiment davomida isbotlandi.

Axborotli-kognitiv komponent: Bu bosqichda talaba kiber-tahdidlarning nazariy asoslarini o‘rganadi. Maqsad — talabada kiber-hujumlar qanday ishlashini tushunish orqali “raqamli hushyorlik”ni shakllantirish. Bu yerda talaba shunchaki axborot qabul qiluvchi emas, balki xavfni tahlil qiluvchi sub’yektga aylanadi.

3-rasm. Talabalarda kiberxavfsizlik madaniyatini shakllantirishning uch komponentli modeli

Emotsional-irodaviy komponent: Mazkur komponent biz aniqlagan $r=0.78$ korrelyatsiyasiga tayanadi. Talaba kiber-muhitdagi manipulyatsiyalar va kiberbullingga duch kelganda o‘z hissiyotlarini boshqarishni o‘rganadi. Bu talabada “psixologik barqarorlik”ni shakllantirib, stressli vaziyatlarda noto‘g‘ri qaror qabul qilmaslikka yordam beradi.

Amaliy-konativ komponent: Bu bosqichda interaktiv kiber-simulyatsiyalar va treninglar orqali xavfsiz xulq-atvor ko‘nikmalari avtomatizm darajasiga yetkaziladi. Ya’ni, talaba shubhali havolani ko‘rganda yoki 2FA ni yoqishda ikkilanmasdan, buni kundalik kiber-gigiyena odati sifatida bajaradi.

“Taklif etilayotgan modelning amaliy samaradorligi shundaki, u talabada 'Kognitiv immunitet'ni shakllantiradi. Bu jarayonda kiber-o‘yinlar orqali hosil qilingan kognitiv dissonans (xato qilib o‘rganish) talabaning xotirasida uzoq vaqt saqlanib qoladi. Natijada, real kiber-tahdid yuzaga kelganda, talaba kognitiv zo‘riqishsiz (avtomatizm darajasida) to‘g‘ri qaror qabul qiladi. Bu yondashuv nafaqat O‘zMU, balki barcha OTMlar uchun informatika va axborot texnologiyalari fanlarini o‘qitishda yangi metodik standart bo‘lib xizmat qilishi mumkin.” [9, 10].

Xulosa va tavsiyalar. O‘zbekiston Milliy universiteti talabalari misolida o‘tkazilgan tadqiqot kiberxavfsizlik madaniyati shaxsning ajralmas qismi ekanligini tasdiqladi. Interaktiv kiber-o‘yinlar yordamida talabalarning kiber-savodxonligini 80% gacha oshirish mumkinligi eksperimental ravishda isbotlandi. Bu esa OTMlarda kiberxavfsizlikni o‘qitishda an’anaviy metodlardan voz kechib, pedagogik va psixologik omillarni birlashtiruvchi innovatsion texnologiyalarga o‘tish zarurligini ko‘rsatadi.

Amaliy tavsiyalar:

OTMlarning 'Informatika' va 'Axborot texnologiyalari' fanlari o‘quv dasturiga kamida 12 soatlik 'Kiberxavfsizlik psixologiyasi' bo‘limini kiritish.

Talabalarning kiber-ko‘nikmalarini baholashda nafaqat test natijalari, balki simulyatsion vaziyatlardagi xatti-harakatlarini ham hisobga olish tizimini joriy etish.

Talabalarda kiber-bullingga qarshi kurashish uchun universitetlarda 'Raqamli maslahat markazlari'ni (Cyber Support) tashkil etish.

Minnatdorchilik

Ushbu tadqiqot O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi tomonidan « Kriptografiya fani bo‘yicha elektron o‘quv qo‘llanma yaratish» mavzusidagi AL-9624115223 raqamli ilmiy loyiha doirasida bajarildi.

ADABIYOTLAR

1. Mirziyoyev Sh.M. "Raqamli O‘zbekiston – 2030" strategiyasi. Toshkent, 2020.
2. Abduqodirov A.A. Ta’limda axborot texnologiyalari. – T.: 2021.
3. Zokirova F.M., Kiber-pedagogika va raqamli madaniyat. – T.: 2023.
4. Boyd D. It's Complicated: The Social Lives of Networked Teens. Yale Press, 2014.
5. O‘zbekiston Milliy universiteti ilmiy axborotnomasi, 2024 - yil.
6. Schneier B. Click Here to Kill Everybody: Security and Survival. — NY: Norton, 2021.
7. Zimmermann P., The Psychology of Cybersecurity. — London: CRC Press, 2022.
8. UNESCO. Global framework for digital literacy skills. — Paris, 2023.
9. Ismanov M. Axborot xavfsizligining huquqiy va pedagogik asoslari. — T.: Fan, 2022.
10. European Commission. DigComp 2.2: The Digital Competence Framework. — Brussels, 2024.