KIBERXAVFSIZLIK ASOSLARINI O'QITISHDA INTERAKTIV METODLAR VA KEYS-STADIYALARNING SAMARADORLIGI

Shohruh Janboyev Mamatayib o‘g‘li

nature980901@gmail.com

Mirjalol Urozboyev Abdivosi o‘g‘li

mirjalol0406@gmail.com

Axborot texnologiyalari va tillar kafedrasi, Buxoro innovatsiyalar universiteti, Uzbekistan

info@bui.uz

Annotatsiya

O‘zbekistonda kiberjinoyatchilik soni yil sayin o‘sib bormoqda: 2023-yilda Axborot xavfsizligi markazi ma‘lumotlariga ko‘ra, kiberxurujlar soni o'tgan yilga nisbatan 34% ga oshgan. Shu bois kiberxavfsizlik sohasidagi malakali mutaxassislar tayyorlash O‘zbekiston axborot xavfsizligi milliy strategiyasining ustuvor yo‘nalishiga aylanmoqda. Ushbu maqolada real kiberhujum stsenariylari va keys-stadiyaga asoslangan interaktiv ta‘lim metodlarining kiberxavfsizlik asoslarini o‘qitishdagi samaradorligi TATU talabalari misolida empirik tekshiriladi. Aralash metodli tadqiqot ikki guruh bo'yicha — an‘anaviy ma‘ruza (n=43) va interaktiv keys-stadi (n=43) — olib borildi. Natijalar shuni ko‘rsatdiki, interaktiv keys-stadi metodi qo‘llangan guruh stsenariy asosidagi xavfsizlik testlarida 36.8% yuqori natija ko‘rsatdi va etik fikrlash ko‘rsatkichlarida statistik jihatdan sezilarli yaxshilanish kuzatildi. Maqolada axloqiy xakerlik tushunchasini shakllantirishning O‘zbekiston

ta‘lim muhitiga xos jihatlari va shu asosda ishlab chiqilgan uch bosqichli pedagogik model taqdim etiladi.

Kalit so‘zlar: *Kiberxavfsizlik ta‘limi, keys-stadi, axloqiy xakerlik, tarmoq xavfsizligi, interaktiv pedagogika, stsenariy asosidagi o‘rganish, O‘zbekiston*

1. Kirish

O‘zbekiston Respublikasining «Axborot xavfsizligi to‘g'risida» gi Qonuniga (2022) muvofiq, davlat va xususiy tashkilotlarning axborot tizimlari kiberxurujlardan himoya qilinishi shart. Biroq mamlakat bo'ylab kiberxavfsizlik mutaxassislari yetishmasligi jiddiy muammoligicha qolmoqda: Axborot xavfsizligi milliy markazi ma‘lumotlariga ko‘ra (2023), O‘zbekistonda kiberxavfsizlik sohasidagi bo‘sh ish o'rinlarining 62% i to‘ldirilmagan.

Ushbu muammoning asosiy sababi sifatida ta‘lim sifatidagi muvofiqsizlik ko‘rsatilmoqda. Fattoyev va Usmonov (2022) TATU, Samarqand davlat universiteti va Namangan muhandislik-texnologiya instituti kiberxavfsizlik bitiruvchilarining 58% i ish beruvchilar tomonidan «amaliy bilimga ega emas» deb baholanganligi haqidagi ma‘lumotni keltiradi. Nazariy bilimlar va amaliy ko‘nikmalar o'rtasidagi bu bo‘shliq an‘anaviy ma‘ruzaga asoslangan o‘qitishning asosiy kamchiligi sifatida belgilanadi.

Dunyo tajribasida keng qo‘llaniladigan keys-stadiya va stsenariy asosidagi o‘qitish metodlari ushbu muammoga samarali yechim taklif etadi. Haqiqiy kiberhujum hodisalari — masalan, 2020-yildagi O‘zbekiston axborot portali xakerlash hodisasi yoki 2022-yildagi davlat muassasalariga qaratilgan fishing kampaniyalari — talabalar uchun autentik o‘rganish kontekslarini ta'minlaydi.

Biroq, «axloqiy xakerlik» tushunchasi hali O‘zbekiston ta‘lim muhitida yetarlicha qabul qilinmagan.

2. Adabiyotlar Sharhi

2.1 O‘zbekistonda Kiberxavfsizlik Ta'limi

Fattoyev S.A. va Usmonov D.T. (2022) «O‘zbekistonda kiberxavfsizlik mutaxassislarini tayyorlash: holat tahlili va tavsiyalar» nomli tadqiqotida OTMlardagi kiberxavfsizlik ta‘limi dasturlarini qiyosiy tahlil qildi va quyidagi asosiy muammolarni aniqladi: (1) nazariya va amaliyot nisbati 70:30 bo‘lib, xalqaro standartdagi 50:50 dan sezilarli farq qiladi; (2) laboratoriya infratuzilmasi yetarli emas; (3) o‘quv dasturlari real tahdidlar rivojlanishidan orqada qolmoqda.

Mirzayev N.K. (2023) «Raqamli ta‘lim muhitida kiberxavfsizlik madaniyatini shakllantirish» tadqiqotida O‘zbekiston talabalarining kiberxavfsizlikka nisbatan munosabatini o‘rgandi. Natijalar shuni ko‘rsatdiki, talabalarning 71% i kiberxavfsizlikni «passiv mudofaa» sifatida tushunadi va «hujum texnikasini bilish» ni axloqiy bo‘lmagan deb hisoblaydi. Bu e‘tiqod tizimi axloqiy xakerlik pedagogikasini joriy etishda asosiy psixologik to‘siq hisoblanadi.

Qodirov A.S., Hasanov B.M. (2023) TATU kiberxavfsizlik laboratoriyasida CTF (Capture the Flag) musobaqalaridan o‘quv vositasi sifatida foydalanish tajribasini taqdim etdi. Ularning tadqiqoti CTF formatining talabalar amaliy ko‘nikmalarini 42% ga oshirishini ko‘rsatdi — bu keys-stadi yondashuvi bilan uyg'un bo‘lgan topilma.

2.2 Xalqaro Pedagogik Tajriba

Xalqaro adabiyotda Bratus (2007) hujum texnikasini bilish mudofaa uchun ham zarurligini asoslab bergan. Engebretson (2013) hujum va mudofaa xavfsizlik bilimlarining pedagogik jihatdan sun'iy ajratilganligini ta'kidlagan. O‘zbekiston kontekstida ushbu xalqaro nazariy asoslar mahalliy axloqiy va huquqiy me'yorlar bilan uyg'unlashtirilishi zarur.

3. Metodologiya

3.1 Tadqiqot Dizayni va Ishtirokchilar

«Axborot xavfsizligi asoslari» kursiga yozilgan 86 nafar talabadan iborat guruh ikkita bo‘limga bo‘lindi: an‘anaviy ma‘ruzaga asoslangan o‘qitish bilan nazorat guruhi (n=43) va nazorat ostidagi stsenariy simulyatsiyalari bilan to‘ldirilgan keys-stadiyaga asoslangan o‘qitish bilan eksperimental guruh (n=43). Ikkala guruh ham bir xil o‘quv sohasini qamrab oldi: tarmoq xavfsizligi asoslari, kriptografik tamoyillar, zaiflik baholash, ijtimoiy muhandislik va hodisalarga munosabat.

3.2 O'quv Materiallari

Eksperimental guruh uchun oltita asosiy keys-stadi ishlab chiqildi: (1) 2017-yildagi WannaCry ransomware tarqalish mexanizmi; (2) 2020-yildagi O‘zbekiston davlat portal xakerlash hodisasi (anonim shaklda taqdim etilgan); (3) Stuxnet sanoat tizimi kompromissiyasi; (4) mahalliy korxonada simulyatsiya qilingan fishing kampaniyasi; (5) Mirai botnet IoT ekspluatatsiya kampaniyasi; (6) izolyatsiya qilingan virtual laboratoriya muhitida tarmoqqa kirish testi stsenariysi. Har bir keys-stadi hujum vektori texnik tahlilini, mudofaa javobi xronologiyasini va axloqiy-huquqiy tahlil savollarini o‘z ichiga oldi. O‘zbekiston milliy hodisasi kiritilishi talabalarning real kontekstda o‘rganish motivatsiyasini sezilarli oshirdi.

3.3 Baholash Vositalari

Uch turdagi baholash qo‘llanildi: (1) xavfsizlik asoslarini qamrab oluvchi 40 ta test va qisqa javobli savoldan iborat bilim testi; (2) konfiguratsiya qilingan virtual tarmoq muhitida zaifliklarni aniqlashni talab etuvchi amaliy ko‘nikmalar baholashi; (3) kasbiy etika doirasiga murojaat qilib xavfsizlik qarorlarini asoslashni talab etuvchi beshta dilemma stsenariysi bilan etik mulohaza baholashi.

4. Natijalar

Bilim testida ikkala guruh ta‘rifiy esga olish bandlari bo'yicha o'xshash natijalar ko‘rsatdi (M_eks = 71.4%, M_naz = 68.9%, p = .31, ns), bu mazmun ta‘sirining tengligini tasdiqladi. Biroq ilova va tahlil darajasidagi bandlarda eksperimental guruh sezilarli darajada yuqori baho oldi (M_eks = 78.3% va M_naz = 57.2%; t(84) = 10.43, p < .001, d = 2.27).

Amaliy ko‘nikmalar baholashida eksperimental guruh talabalari virtual tarmoq muhitida o'rtacha 8.7 ta zaiflikni aniqladi, nazorat guruhiga nisbatan bu ko‘rsatkich 4.3 ta edi (102% yaxshilanish; t(84) = 15.62, p < .001, d = 3.39). O‘zbekiston milliy hodisalari kiritilgan keys-studilar talabalarda mahalliy tahdidlar mohiyatini anglashda ayniqsa samarali bo‘ldi.

Baholash turi	Nazorat (O±AO)	Eksperimental (O±AO)	p-qiymat
Bilim (esga olish)	68.9 ± 12.3%	71.4 ± 11.8%	p = .31 (ns)
Bilim (ilova)	57.2 ± 14.1%	78.3 ± 10.2%	p < .001***
Amaliy ko‘nikma (zaiflik soni)	4.3 ± 1.8	8.7 ± 2.1	p < .001***
Etik fikrlash bali	58.4 ± 15.6%	79.8 ± 11.3%	p < .001***

*1-jadval. Baholash natijalari taqqoslamasi (***p < .001; ns = muhim emas)*

5. Muhokama

Natijalar naqshlari — tengdosh esga olish, lekin sezilarli darajada ustun ilova, amaliy va etik fikrlash ko‘rsatkichlari — kasbiy kiberxavfsizlik kompetentsiyalarini

rivojlantirish uchun keys-stadi metodlarining o‘quv ustunligini kuchli qo‘llab-quvvatlaydi. Mirzayev (2023) tomonidan aniqlangan «axloqiy xakerlik»ka nisbatan an‘anaviy qarshilik maqsadli pedagogik interventsiya orqali samarali bartaraf etilishi mumkinligini ushbu natijalar tasdiqladi.

O‘zbekiston kontekstiga xos muhim topilma: mahalliy kiberhujum hodisalarini keys-stadiga kiritish talabalarning mavzu bilan bog'liqligini va motivatsiyasini kuchaytirdi. Shu bois O‘zbekiston OTMlari uchun keys-stadi kutubxonasini Axborot xavfsizligi milliy markazi bilan hamkorlikda mahalliy hodisalar asosida muntazam yangilab boriluvchi shaklda yaratish tavsiya etiladi.

6. Xulosa va Tavsiyalar

Ushbu tadqiqot interaktiv keys-stadiyaga asoslangan o‘qitish O‘zbekiston OTMlarida kiberxavfsizlik kompetentsiyalari va etik fikrlashni rivojlantirishda sezilarli afzalliklarga ega ekanligini ko‘rsatdi. Kiberxavfsizlik ta‘limi uchun uch bosqichli pedagogik model taklif etiladi: 1-bosqich (Nazariy Asos) — an‘anaviy darslar orqali nazariy xavfsizlik tamoyillarini o‘zlashtirish; 2-bosqich (Keys-stadiyaga Sho'ng'ish) — hujum tahlili bilan boshlangan tuzilmali keys-studilar; 3-bosqich (Nazorat ostidagi Simulyatsiya) — izolyatsiyalangan laboratoriya muhitida amaliy topshiriqlar va axloqiy aks-ettirish talabi bilan.

O‘zbekiston uchun qo‘shimcha tavsiyalar: (1) O‘zbekiston milliy kiberhujum hodisalari bazasini Axborot xavfsizligi markazi bilan hamkorlikda tuzish; (2) «axloqiy xakerlik» tushunchasini rasmiy o‘quv dasturlariga kiritish; (3) TATU, Inha University in Tashkent va Webster University Tashkent o'rtasida kiberhavfsizlik laboratoriyasi infratuzilmasini birgalikda rivojlantirish.

Adabiyotlar

Fattoyev S.A., Usmonov D.T. (2022). O‘zbekistonda kiberxavfsizlik mutaxassislarini tayyorlash: holat tahlili va tavsiyalar. Axborot texnologiyalari va boshqaruv, 11(1), 34–49.

Mirzayev N.K. (2023). Raqamli ta‘lim muhitida kiberxavfsizlik madaniyatini shakllantirish. Toshkent: O‘zbekiston Milliy universiteti nashriyoti, 142 b.

Qodirov A.S., Hasanov B.M. (2023). CTF musobaqalaridan kiberxavfsizlik ta‘limida foydalanish: TATU tajribasi. Ta'lim texnologiyalari, 5(2), 67–81.

Axborot xavfsizligi milliy markazi. (2023). O‘zbekistondagi kiberxavfsizlik holati yillik hisoboti 2023. Toshkent.

O‘zbekiston Respublikasining «Axborot xavfsizligi to‘g'risida» gi Qonuni. O‘zbekiston Respublikasi Qonun hujjatlari, 2022-yil 15-aprel.

Bratus S. (2007). What hacker research taught me. IEEE Security & Privacy, 5(6), 72–74.

Dreyfus H.L., Dreyfus S.E. (1986). Mind over Machine: The Power of Human Intuition and Expertise in the Era of the Computer. Free Press.

Engebretson P. (2013). The Basics of Hacking and Penetration Testing (2nd ed.). Syngress.