

KIBERXAVFSIZLIK MADANIYATINI SHAKLLANTIRISHDA ADAPTIV TA'LIM PLATFORMALARINING ILMIY-PEDAGOGIK ASOSLARI

Ibragimov Sodiqjon Sadridinovich

University of Business and Science o'qituvchisi

Annotatsiya. Ushbu maqolada raqamli transformatsiya sharoitida yoshlarning kiberxavfsizlik madaniyatini shakllantirish masalasi tahlil qilinadi. Tadqiqotda sun'iy intellekt, o'quv analitikasi va simulyatsion muhitga asoslangan adaptiv ta'lim platformalarining pedagogik imkoniyatlari o'rganilgan. Muallif tomonidan ishlab chiqilgan xavf-indeks modeli va metodik tizimning samaradorligi eksperimental guruhlarda kiberxavfsizlik kompetensiyasining sezilarli darajada oshishi bilan isbotlangan.

Kalit so'zlar: kiberxavfsizlik madaniyati, adaptiv ta'lim, sun'iy intellekt, raqamli pedagogika, yoshlar tarbiyasi, axborot xavfsizligi, o'quv analitikasi.

SCIENTIFIC AND PEDAGOGICAL BASIS OF ADAPTIVE EDUCATIONAL PLATFORMS IN FORMING A CYBERSECURITY CULTURE

Ibragimov Sodiqjon Sadridinovich

Teacher at the University of Business and Science

Abstract. This article analyzes the issue of forming a cybersecurity culture among young people in the context of digital transformation. The study explores the pedagogical potential of adaptive learning platforms based on artificial intelligence, learning analytics, and simulation environments. The effectiveness of the risk-index model and methodological system developed by the author is proven by a significant increase in cybersecurity competence in experimental groups.

Keywords: cybersecurity culture, adaptive learning, artificial intelligence, digital pedagogy, youth education, information security, learning analytics.

Kirish

Raqamli texnologiyalar va sun'iy intellektning ommalashuvi yoshlarning axborot makonidagi faolligini oshirish bilan birga, kiberjinoyatchilik va fishing kabi xavflarni ham ko'paytirdi. Global miqyosda kiberhujumlar keltirayotgan ulkan iqtisodiy zarar

sharoitida yoshlarning ongli xulq-atvorini va kiberxavfsizlik madaniyatini shakllantirish dolzarb pedagogik vazifaga aylandi.

Kiberxavfsizlik madaniyati nafaqat texnik bilimlarni, balki shaxsning mas'uliyati va refleksiv tafakkurini ham qamrab oladi. An'anaviy ta'lim usullari zamonaviy talablarga to'liq javob bermayotganligi sababli, individual trayektoriya va real simulyatsiyalarni taqdim etuvchi adaptiv ta'lim platformalari innovatsion yechim sifatida namoyon bo'lmoqda. Maqolaning maqsadi – yoshlar kiberxavfsizlik madaniyatini shakllantirishning ilmiy-pedagogik asoslarini ishlab chiqish va samarali tajriba-sinov modelini taklif etishdir.

1. Kiberxavfsizlik madaniyatining nazariy asoslari

1.1. Kiberxavfsizlik tushunchasining evolyutsiyasi. Axborot xavfsizligi dastlab texnik muhofaza choralariga asoslangan bo'lsa, zamonaviy yondashuv inson omilini markaziy element sifatida ko'rib chiqadi. ISO/IEC 27001 standarti axborot xavfsizligini boshqaruv tizimi sifatida belgilaydi [4:3]. Biroq ko'plab kiberhujumlar inson xatosi tufayli yuzaga kelishi aniqlangan.

Tarmoq jamiyati nazariyasiga ko'ra, axborot infratuzilmasi ijtimoiy tuzilmaning asosiy elementi hisoblanadi [2:51]. Demak, kiberxavfsizlik muammosi faqat texnik emas, balki ijtimoiy-madaniy xarakterga ega.

1.2. Kiberxavfsizlik madaniyatining komponentlari. Ilmiy adabiyotlar asosida kiberxavfsizlik madaniyati quyidagi komponentlardan iborat deb qaraladi:

1. **Kognitiv komponent** – xavf turlarini bilish.
2. **Operatsion komponent** – amaliy himoya ko'nikmalari.
3. **Aksiologik komponent** – axborotga qadriyat sifatida munosabat.
4. **Refleksiv komponent** – o'z xatti-harakatlarini tahlil qilish.

Bandura nazariyasiga ko'ra, o'z-o'ziga ishonch (self-efficacy) xavfsiz xulq-atvorni shakllantirishda muhim omil hisoblanadi [1:21]. Shaxs o'zining raqamli makondagi harakatlarini boshqarish qobiliyatiga ishonsa, xavfsizlikka nisbatan mas'uliyat ham ortadi.

1.3. Yoshlar va kiberxavf omillari. OECD tadqiqotlariga ko'ra, yoshlarning 70% dan ortig'i internetdan kuniga 5 soatdan ko'proq foydalanadi [6:18]. Ijtimoiy tarmoqlar, onlayn o'yinlar va elektron savdo platformalari orqali ma'lumot almashinuvi kuchaymoqda. Shu bilan birga:

- fishing hujumlari,
- zararli havolalar,
- ijtimoiy muhandislik,
- shaxsiy ma'lumotlarni oshkor qilish

holatlari keng tarqalgan.

Demak, yoshlar uchun kiberxavfsizlik madaniyatini shakllantirish uzluksiz pedagogik jarayon sifatida qaralishi lozim.

2. Adaptiv ta'lim texnologiyalarining pedagogik mohiyati

2.1. Adaptiv ta'lim tushunchasi. Adaptiv ta'lim – bu o'quvchining bilim darajasi, qiziqishi, xatolari va o'zlashtirish tezligiga qarab o'quv kontentini avtomatik moslashtiruvchi raqamli tizimdir [5:34].

Sun'iy intellekt asosidagi algoritmlar o'quvchining javoblarini tahlil qiladi va individual o'quv trayektoriyasini shakllantiradi. Bu esa differensial yondashuvni real vaqt rejimida ta'minlaydi.

2.2. O'quv analitikasi va ma'lumotlar modeli. O'quv analitikasi (learning analytics) o'quvchilarning faoliyati haqidagi ma'lumotlarni yig'ish, tahlil qilish va bashorat qilish imkonini beradi. Hattie tadqiqotlariga ko'ra, individual yondashuv o'zlashtirish samaradorligini sezilarli oshiradi [3:89].

Adaptiv tizim quyidagi bosqichlarda ishlaydi:

1. Diagnostika.
2. Tahlil.
3. Moslashtirish.
4. Monitoring.
5. Refleksiya.

2.3. Adaptiv platformalarning afzalliklari

- Individual tezlikda o'qish.
- Real vaziyatga yaqin simulyatsiya.
- Doimiy teskari aloqa.
- Motivatsiyani oshirish.

Mashinali o'rganish algoritmlari inson va sun'iy intellekt integratsiyasini ta'minlaydi [5:72].

3. Taklif etilayotgan ilmiy-metodik model

3.1. Modelning umumiy tuzilishi. Taklif etilayotgan model 5 ta moduldan iborat:

1. **Diagnostic modul**
2. **Risk-indeks hisoblash moduli**
3. **Adaptiv kontent moduli**
4. **Simulyatsion modul**
5. **Monitoring va refleksiya moduli**

3.2. Risk-indeks formulasi. Kiberxavfsizlik darajasi quyidagicha aniqlanadi:

$$RK = (B \times 0.4) + (A \times 0.3) + (X \times 0.3)$$

Bu yerda:

- B – bilim darajasi,
- A – amaliy ko'nikma,
- X – xavfsiz xulq ko'rsatkichi.

Natijada har bir talaba uchun individual xavf darajasi aniqlanadi.

3.3. Simulyatsion muhit. Simulyatsiya moduli real fishing xabarlari, zararli saytlar, parol mustahkamligi testlari va ijtimoiy muhandislik vaziyatlarini modellashtiradi. Tajriba natijalari shuni ko'rsatadiki, amaliy mashqlar nazariy ma'lumotga nisbatan 2 baravar samarali [3:112].

4. Tajriba-sinov ishlari

4.1. Tadqiqot dizayni. Tajriba 120 nafar talaba ishtirokida o'tkazildi:

- 60 nafari – nazorat guruhi
- 60 nafari – eksperimental guruh

Muddat: 4 oy.

4.2. Natijalar. Eksperimental guruhda:

- Fishingni aniqlash ko'rsatkichi 42% ga oshdi.
- Kuchli parol yaratish ko'nikmasi 38% ga yaxshilandi.
- Xavfli havolalarga bosish darajasi 35% ga kamaydi.

Nazorat guruhida esa o'sish 10–12% atrofida bo'ldi.

4.3. Statistik tahlil. Student t-mezoni asosida farq ishonchli ($p < 0.05$) deb topildi.

5. Muhokama

Natijalar shuni ko'rsatadiki, adaptiv platformalar yoshlarning nafaqat bilimini, balki real xulq-atvorini ham o'zgartira oladi. Bu jarayonda:

- individual motivatsiya,
- o'z-o'zini nazorat qilish,
- refleksiv fikrlash

kuchayadi. Bandura nazariyasi nuqtai nazaridan qaraganda, o'ziga ishonch oshishi xavfsiz xatti-harakatni mustahkamlaydi [1:33].

Xulosa

Tadqiqot natijalari quyidagilarni ko'rsatdi:

1. Kiberxavfsizlik madaniyati kompleks pedagogik jarayondir.
2. Adaptiv ta'lim individual xavf omillarini aniqlash imkonini beradi.
3. Simulyatsiya va analitika asosidagi model an'anaviy usulga nisbatan samaraliroq.
4. Eksperimental natijalar metodikaning samaradorligini tasdiqladi.

Kelgusida modelni maktab bosqichiga moslashtirish va milliy ta'lim platformalariga integratsiya qilish maqsadga muvofiq.

FOYDALANILGAN ADABIYOTLAR

1. Bandura A. Self-efficacy: The exercise of control. New York: Freeman, 1997.
2. Castells M. The Rise of the Network Society. Oxford: Wiley-Blackwell, 2010.
3. Hattie J. Visible Learning. London: Routledge, 2009.
4. ISO/IEC 27001:2018 Information Security Management Systems – Requirements.

5. Luckin R. Machine Learning and Human Intelligence. London: UCL IOE Press, 2018.
6. OECD. Digital Education Outlook 2021. Paris: OECD Publishing, 2021.