UO‘K: 37.016:004.056

O‘QUVCHILARDA KIBERXAVFSIZLIK MADANIYATINI SHAKLLANTIRISHNING ZAMONAVIY PEDAGOGIK YONDASHUVLARI

Rashidov Abdullo Rosuljon o‘g‘li

Toshkent davlat yuridik universiteti huzuridagi H.K. Muhitdinova nomidagi akademik litseyi Informatika va axborot texnologiyalari fani o‘qituvchisi

abdullo.rashidov.1998@gmail.com

Annotatsiya. Maqolada umumta’lim va akademik litsey o‘quvchilarida kiberxavfsizlik madaniyatini shakllantirishning zamonaviy pedagogik yondashuvlari tahlil qilinadi. Kiberxavfsizlik madaniyati tushunchasining mohiyati, O‘zbekiston Respublikasining tegishli me’yoriy-huquqiy asoslari hamda xalqaro tajriba (OECD, ITU, DigComp 2.1, NICE) yoritilgan. Kompetensiyaviy, muammoli va keysga asoslangan, loyihaviy, gamifikatsiyalashgan, hamkorlikda o‘qitish, teskari sinf hamda simulyatsiyaga asoslangan yondashuvlarning imkoniyatlari ko‘rsatilgan. Fishingga qarshi kurashga bag‘ishlangan dars namunasi, baholash mezonlari va ta’lim jarayonini tashkil etish bo‘yicha amaliy takliflar berilgan.

Kalit so‘zlar: kiberxavfsizlik, kiberxavfsizlik madaniyati, raqamli kompetensiya, pedagogik yondashuv, gamifikatsiya, fishing, shaxsiy ma’lumotlar, informatika ta’limi, o‘quvchilar.

Аннотация. В статье анализируются современные педагогические подходы к формированию культуры кибербезопасности у учащихся. Раскрыта сущность понятия «культура кибербезопасности», рассмотрены нормативно-правовая база Республики Узбекистан и международный опыт (OECD, ITU, DigComp 2.1, NICE). Показаны возможности компетентностного, проблемного и кейсового, проектного, геймифицированного подходов,

обучения в сотрудничестве, «перевёрнутого класса» и симуляционного обучения. Представлены пример урока по противодействию фишингу, критерии оценивания и практические рекомендации по организации образовательного процесса.

Ключевые слова: кибербезопасность, культура кибербезопасности, цифровая компетентность, педагогический подход, геймификация, фишинг, персональные данные, обучение информатике, учащиеся.

Abstract. The article examines modern pedagogical approaches to developing a culture of cybersecurity among students. It clarifies the concept of a cybersecurity culture and reviews the legal framework of the Republic of Uzbekistan and international practice (OECD, ITU, DigComp 2.1, NICE). The potential of competence-based, problem- and case-based, project-based, gamified, collaborative, flipped-classroom and simulation-based approaches is demonstrated. A sample lesson on countering phishing, assessment criteria and practical recommendations for organising the learning process are presented.

Keywords: cybersecurity, cybersecurity culture, digital competence, pedagogical approach, gamification, phishing, personal data, computer science education, students.

Kirish

Bugungi kunda raqamli texnologiyalar yoshlar hayotining ajralmas qismiga aylandi: o‘quvchilar ijtimoiy tarmoqlar, mobil ilovalar, onlayn o‘yinlar va masofaviy ta’lim platformalaridan kundalik foydalanadi. Bu imkoniyatlar bilan birga yangi xavflar ham paydo bo‘lmoqda: fishing, akkauntlarni buzish, shaxsiy ma’lumotlarning sizib chiqishi, kiberbulling, zararli dasturlar va yolg‘on axborot. M. Prenskiy “raqamli tub aholi” (digital natives) tushunchasini ilgari surgan bo‘lsa-da [13], keyingi tadqiqotlar shuni ko‘rsatadiki, texnologiyadan faol foydalanish avtomatik ravishda xavfsiz foydalanish malakasini bermaydi.

Yevropa mamlakatlarida 9–16 yoshli bolalar o‘rtasida o‘tkazilgan EU Kids Online tadqiqoti (25 ta mamlakatda, qariyb 25 ming bola) onlayn xavflar bilan to‘qnashuv keng tarqalganini ko‘rsatgan [11]. Rossiyalik tadqiqotchilar G.U. Soldatova va hammualliflari ham o‘smirlarning raqamli kompetentligi tarkibida xavfsizlik komponenti alohida o‘rin tutishini asoslagan [6].

O‘zbekistonda raqamlashtirish jarayonlarining kengayishi, “Raqamli O‘zbekiston – 2030” strategiyasining qabul qilinishi [5] hamda “Kiberxavfsizlik to‘g‘risida”gi Qonunning kuchga kirishi [1] ta’lim muassasalari oldiga yangi vazifa qo‘ymoqda: o‘quvchilarda faqat texnik bilim emas, balki xavfsiz xulq-atvor odatlari va mas’uliyat hissini, ya’ni kiberxavfsizlik madaniyatini shakllantirish.

Maqolaning maqsadi — o‘quvchilarda kiberxavfsizlik madaniyatini shakllantirishning zamonaviy pedagogik yondashuvlarini tahlil qilish va informatika darslarida qo‘llash bo‘yicha amaliy tavsiyalar ishlab chiqishdir. Tadqiqot usullari: me’yoriy hujjatlar va ilmiy manbalar tahlili, qiyoslash, umumlashtirish va pedagogik modellashtirish.

Kiberxavfsizlik madaniyati tushunchasi va mohiyati

“Xavfsizlik madaniyati” tushunchasi xalqaro hujjatlarda ancha oldin shakllangan. Iqtisodiy hamkorlik va taraqqiyot tashkiloti (OECD) 2002-yilda qabul qilgan axborot tizimlari va tarmoqlari xavfsizligi bo‘yicha qo‘llanmasida xavfsizlik madaniyatini ta’minlash uchun to‘qqizta tamoyil belgilangan: xabardorlik, mas’uliyat, javob choralari, etika, demokratiya, xavfni baholash, xavfsizlikni loyihalash va joriy etish, xavfsizlikni boshqarish hamda qayta baholash [7]. Ushbu tamoyillar ta’lim sohasida ham asos bo‘lib xizmat qila oladi.

Pedagogik nuqtayi nazardan kiberxavfsizlik madaniyatini o‘quvchining quyidagi komponentlarini o‘z ichiga olgan integrativ sifat sifatida talqin qilish mumkin:

– bilim komponenti — kiber tahdidlar turlari, himoya vositalari va huquqiy asoslar haqidagi tushunchalar;

– amaliy komponent — murakkab parol yaratish, ikki bosqichli autentifikatsiyadan foydalanish, dasturlarni yangilash, shubhali xabarni aniqlash kabi ko‘nikmalar;
– qadriyatli-motivatsion komponent — o‘z va boshqalarning ma’lumotlarini hurmat qilish, raqamli makonda mas’uliyatli bo‘lish;
– xulq-atvor komponenti — xavfsiz odatlarning barqaror shakllanishi va noaniq vaziyatda to‘g‘ri qaror qabul qila olish.

Yevropa Ittifoqining raqamli kompetensiya doirasi DigComp 2.1 ham xavfsizlikni raqamli kompetensiyaning beshta asosiy sohasidan biri sifatida ajratadi (qolganlari: axborot va ma’lumotlar savodxonligi, muloqot va hamkorlik, raqamli kontent yaratish, muammolarni hal etish). Bu doirada xavfsizlik qurilmalarni himoya qilish, shaxsiy ma’lumotlar va maxfiylikni himoyalash, sog‘liq va farovonlikni asrash hamda atrof-muhitni muhofaza qilish kabi kompetensiyalarni qamrab oladi [9].

Me’yoriy-huquqiy asoslar va xalqaro tajriba

O‘zbekiston Respublikasining 2022-yil 15-aprelda qabul qilingan “Kiberxavfsizlik to‘g‘risida”gi Qonuni kiberxavfsizlik sohasidagi munosabatlarni tartibga solib, kiberxavfsizlikni ta’minlashning huquqiy asoslarini belgilaydi [1]. “Ta’lim to‘g‘risida”gi Qonun (2020) ta’lim jarayoniga axborot-kommunikatsiya texnologiyalarini joriy etish va ta’lim oluvchilarning shaxs sifatida rivojlanishiga e’tibor qaratadi [2]. “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun (2019) shaxsiy ma’lumotlarni himoya qilish tamoyillarini belgilab, o‘quvchilarga raqamli maxfiylik huquqini tushuntirishda huquqiy poydevor vazifasini bajaradi [3]. “Bolalarni ularning sog‘lig‘iga zarar yetkazuvchi axborotdan himoya qilish to‘g‘risida”gi Qonun (2017) esa voyaga yetmaganlarni zararli axborotdan himoya qilish mexanizmlarini belgilaydi [4].

“Raqamli O‘zbekiston – 2030” strategiyasi raqamli iqtisodiyot va elektron xizmatlarni rivojlantirish bilan birga, aholining, xususan yoshlarning raqamli

savodxonligini oshirishni nazarda tutadi [5]. Bu yo‘nalishda maktab va litsey informatika ta’limi muhim bo‘g‘in hisoblanadi.

Xalqaro tajribada Xalqaro elektraloqa ittifoqining (ITU) 2020-yilgi “Bolalarni onlayn muhitda himoya qilish” bo‘yicha qo‘llanmalari siyosatchilar, ota-onalar va pedagoglar, sanoat vakillari hamda bolalarning o‘zi uchun alohida tavsiyalarni o‘z ichiga oladi [8]. AQShning NIST tomonidan ishlab chiqilgan NICE kiberxavfsizlik kadrlari doirasi (SP 800-181) esa kiberxavfsizlik bilim, ko‘nikma va vazifalarni tizimlashtirib, ta’lim dasturlarini kasbiy ehtiyojlar bilan bog‘lash imkonini beradi [10]. Bu hujjatlar litsey o‘quvchilari uchun kasb tanlash yo‘nalishida ham foydalidir.

Zamonaviy pedagogik yondashuvlar

Kiberxavfsizlik madaniyatini shakllantirishda an’anaviy axborot beruvchi ma’ruza yetarli emas, chunki xavfsiz xulq-atvor faqat bilim bilan emas, balki amaliy mashq va shaxsiy tajriba bilan mustahkamlanadi. 1-jadvalda asosiy zamonaviy yondashuvlar va ularning imkoniyatlari umumlashtirilgan.

1-jadval. Kiberxavfsizlik madaniyatini shakllantirishning pedagogik yondashuvlari

Yondashuv	**Mohiyati**	**Kiberxavfsizlik madaniyatini shakllantirishdagi o‘rni**
Kompetensiyaviy	Bilim, ko‘nikma va qadriyatlarni birgalikda rivojlantirish	Axborot xavfsizligi bo‘yicha amaliy harakat qila olish layoqatini (parol boshqaruvi, shubhali havolani aniqlash) shakllantiradi
Muammoli va keysga asoslangan ta’lim	Real vaziyatlarni tahlil qilish orqali yechim izlash	Fishing, akkauntni o‘g‘irlash, kiberbulling holatlarini tahlil qilib, qaror qabul qilish ko‘nikmasini beradi

Yondashuv	Mohiyati	Kiberxavfsizlik madaniyatini shakllantirishdagi o‘rni
Loyihaviy ta’lim	O‘quvchilar mustaqil loyiha ustida ishlaydi	Xavfsizlik bo‘yicha infografika, qo‘llanma, qisqa video tayyorlash orqali bilimni mustahkamlaydi va tengdoshlarga yetkazadi
Gamifikatsiya	O‘yin elementlarini o‘yinga aloqador bo‘lmagan kontekstda qo‘llash [12]	Viktorina, topshiriq-musobaqa va nishonlar orqali motivatsiyani oshiradi
Hamkorlikda o‘qitish va tengdoshlar ta’limi	Kichik guruhlarda birgalikda o‘rganish	Mas’uliyat hissini va o‘zaro nazoratni kuchaytiradi, yuqori sinf o‘quvchilari kichiklarga o‘rgatadi
Teskari sinf (flipped classroom)	Nazariy qism uyda, amaliy qism darsda	Dars vaqtini amaliy mashq va muhokamaga ajratish imkonini beradi
Simulyatsiya va virtual laboratoriya	Xavfsiz muhitda hujum va himoya holatlarini modellashtirish	Haqiqiy xavf tug‘dirmasdan, xatolardan o‘rganish imkonini beradi

Kompetensiyaviy yondashuv

Bu yondashuvda o‘quv natijalari “nimani biladi” emas, “nimani qila oladi” tarzida belgilanadi. Masalan, o‘quvchi elektron xatdagi fishing belgilarini (jo‘natuvchi manzilidagi nomuvofiqlik, shoshiltiruvchi ohang, shubhali havola) aniqlay olishi, parolni xavfsiz saqlashi, ikki bosqichli tasdiqlashni yoqa olishi lozim.

DigComp 2.1 doirasidagi xavfsizlik sohasi ushbu natijalarni rejalashtirish uchun tayanch bo‘la oladi [9].

Muammoli va keysga asoslangan ta’lim

O‘quvchilarga real hayotga yaqin vaziyatlar (masalan, “Do‘stingiz nomidan pul so‘ralgan xabar keldi”, “Ijtimoiy tarmoq akkauntingizga kimdir kirishga urindi”) taklif qilinadi. Ular vaziyatni tahlil qiladi, xavf omillarini aniqlaydi va harakatlar ketma-ketligini ishlab chiqadi. Bunday ish tanqidiy fikrlash va qaror qabul qilish ko‘nikmalarini rivojlantiradi. Soldatova va hamkorlarining tadqiqotlari ham o‘smirlarning xavfli vaziyatlarda o‘zini tutish strategiyalarini o‘rganishning ahamiyatini ko‘rsatadi [6].

Loyihaviy ta’lim

O‘quvchilar kichik guruhlarda “Xavfsiz raqamli hayot” mavzusida infografika, plakat, qisqa video yoki ota-onalar uchun eslatma tayyorlaydi. Loyiha jarayonida ular manbalarni izlaydi, ma’lumotni tizimlaydi va jamoada ishlaydi. Natijalar litsey axborot stendlarida yoki ijtimoiy tarmoqdagi rasmiy sahifada e’lon qilinishi mumkin.

Gamifikatsiya

Gamifikatsiya — o‘yin dizayni elementlarini o‘yin bo‘lmagan kontekstda qo‘llash [12]. Kiberxavfsizlikni o‘rgatishda ballar, darajalar, nishonlar, jamoaviy musobaqalar va “CTF” (Capture the Flag) uslubidagi sodda topshiriqlardan foydalanish o‘quvchilar qiziqishini oshiradi. Biroq o‘yin elementlari o‘quv maqsadiga bo‘ysunishi, ya’ni musobaqa ruhi mazmunni soyada qoldirmasligi zarur.

Hamkorlikda o‘qitish va tengdoshlar ta’limi

O‘smirlar uchun tengdoshlar fikri ko‘pincha kattalar nasihatidan ta’sirliroq bo‘ladi. Shu bois yuqori sinf yoki kurs o‘quvchilaridan “kiberxavfsizlik elchilari” guruhini tashkil etib, ular orqali kichik sinflarda qisqa mashg‘ulotlar o‘tkazish samarali. Bu o‘qituvchi uchun ham, o‘quvchi uchun ham bilimni mustahkamlash imkonini beradi.

Teskari sinf va simulyatsiyalar

Teskari sinf modelida o‘quvchilar qisqa video yoki matn bilan nazariy qismni darsdan oldin o‘rganadi, dars vaqti esa amaliy mashq va muhokamaga ajratiladi. Simulyatsiyalar (masalan, fishing xatini aniqlash mashqi yoki parol mustahkamligini baholash vositalari) xavfsiz o‘quv muhitida xatolardan o‘rganish imkonini beradi. Muhimi, mashqlarda faqat o‘quv uchun tayyorlangan yoki o‘qituvchi nazoratidagi muhitdan foydalaniladi, real tizimlar va boshqa shaxslarning hisoblariga hech qanday sinov o‘tkazilmaydi.

Oila va maktab hamkorligi

Kiberxavfsizlik madaniyati sinf xonasi bilan cheklanmaydi. Ota-onalar uchun qisqa seminarlar, Telegram guruhlari orqali eslatmalar, “oilaviy xavfsizlik qoidalari” varaqasi kabi vositalar o‘quvchining uy sharoitidagi xulq-atvoriga ta’sir qiladi. ITU qo‘llanmalari ham ota-onalar va pedagoglarning birgalikdagi roliga alohida urg‘u beradi [8].

AMALIY MODEL: “FISHINGNI TANIB OL” DARSI NAMUNASI

Quyida informatika fanida 45–80 daqiqalik dars (yoki ikki soatlik mashg‘ulot) uchun taklif etilayotgan model keltirilgan. Model muallifning pedagogik tavsiyasi bo‘lib, yuqorida ko‘rib chiqilgan yondashuvlarni uyg‘unlashtiradi.

– Motivatsiya (5–10 daqiqa): muammoli savol — “Sizga ‘yutuq yutdingiz’ degan xabar keldi, nima qilasiz?”. Sinf fikrlari yozib boriladi.
– Yangi bilim (10–15 daqiqa): fishingning mohiyati, asosiy belgilari va oqibatlari qisqa taqdimot orqali tushuntiriladi; avvaldan tayyorlangan video yoki matn bilan bog‘lanadi (teskari sinf).
– Guruhli keys-tahlil (15–20 daqiqa): har bir guruhga o‘quv uchun tayyorlangan 3–4 ta xabar namunasi beriladi; guruh qaysilari ishonchsiz ekanini asoslab, jadval to‘ldiradi.
– Gamifikatsiyalashgan mashq (10–15 daqiqa): “Ishonchli yoki soxta?” viktorinasi, jamoalar to‘g‘ri javoblar uchun ball to‘playdi.

– Refleksiya va uy vazifasi (5–10 daqiqa): har bir o‘quvchi “5 ta qoida” varaqasini tuzadi; uy vazifasi sifatida oila a’zolari uchun qisqa eslatma tayyorlaydi.

BAHOLASH VA MONITORING

Kiberxavfsizlik madaniyatining shakllanganligini faqat test bilan baholash yetarli emas. Quyidagi mezonlar majmuasi tavsiya etiladi: (1) bilim darajasi (test, savol-javob); (2) amaliy ko‘nikmalar (rubrika asosidagi topshiriq: akkauntni himoyalash sozlamalari, fishingni aniqlash); (3) loyiha va taqdimot sifati; (4) o‘z-o‘zini baholash va tengdoshlarni baholash; (5) xulq-atvor kuzatuvi (masalan, anonim so‘rovnoma orqali xavfsiz odatlardan foydalanish chastotasi). O‘quv yili boshida va oxirida bir xil so‘rovnoma o‘tkazish dinamikani ko‘rsatadi. Natijalar shaxsiy ma’lumotlar to‘g‘risidagi qonun talablariga rioya qilgan holda, anonim tarzda tahlil qilinishi lozim [3].

ASOSIY MUAMMOLAR VA TAKLIFLAR

Amaliyotda quyidagi qiyinchiliklar uchrashi mumkin: o‘qituvchilarning kiberxavfsizlik bo‘yicha metodik tayyorgarligi yetarli emasligi; o‘quv dasturlarida mavzuga ajratilgan soatlarning cheklanganligi; texnik jihozlar va xavfsiz laboratoriya muhitining yetishmasligi; uzluksiz va tizimli yondashuvning yo‘qligi. Ushbu muammolarni bartaraf etish uchun quyidagilar taklif etiladi:

– informatika o‘qituvchilari uchun malaka oshirish kurslarida kiberxavfsizlik metodikasi bo‘yicha modul kiritish;
– kiberxavfsizlik elementlarini informatika fanining mavjud mavzulariga (internet, axborot xavfsizligi, dasturlash) integratsiya qilish;
– litsey va maktablarda “kiberxavfsizlik elchilari” klublarini tashkil etish;
– ota-onalar bilan muntazam hamkorlikni yo‘lga qo‘yish;
– kasbga yo‘naltirish ishlarida NICE kabi doiralar asosida kiberxavfsizlik mutaxassisliklari haqida ma’lumot berish [10].

Xulosa

O‘quvchilarda kiberxavfsizlik madaniyatini shakllantirish bilim, amaliy ko‘nikma, qadriyat va xulq-atvor komponentlarini uyg‘un rivojlantirishni talab qiluvchi uzluksiz pedagogik jarayondir. Kompetensiyaviy, muammoli va keysga asoslangan, loyihaviy, gamifikatsiyalashgan, hamkorlikda o‘qitish, teskari sinf va simulyatsiyaga asoslangan yondashuvlar bir-birini to‘ldirib, an’anaviy ma’ruzaga nisbatan o‘quvchilarning faolligini va olingan bilimning amaliy qo‘llanilishini oshirish imkonini beradi.

O‘zbekiston Respublikasining kiberxavfsizlik, ta’lim va shaxsiy ma’lumotlarni himoya qilish sohasidagi qonunchiligi [1; 2; 3; 4] hamda xalqaro tajriba [7; 8; 9; 10] ushbu yo‘nalishda ta’lim muassasalari uchun mustahkam asos yaratadi. Informatika o‘qituvchisi bu jarayonda nafaqat bilim beruvchi, balki xavfsiz raqamli xulq-atvor namunasi sifatida ham muhim rol o‘ynaydi. Kelgusi tadqiqotlarda taklif etilgan modellarning samaradorligini pedagogik tajriba orqali miqdoriy baholash maqsadga muvofiq.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni. 15.04.2022-yil, O‘RQ-764-son. Lex.uz milliy qonunchilik ma’lumotlari bazasi.
2. O‘zbekiston Respublikasining “Ta’lim to‘g‘risida”gi Qonuni. 23.09.2020-yil, O‘RQ-637-son. Lex.uz milliy qonunchilik ma’lumotlari bazasi.
3. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. 02.07.2019-yil, O‘RQ-547-son. Lex.uz milliy qonunchilik ma’lumotlari bazasi.
4. O‘zbekiston Respublikasining “Bolalarni ularning sog‘lig‘iga zarar yetkazuvchi axborotdan himoya qilish to‘g‘risida”gi Qonuni. 08.09.2017-yil, O‘RQ-444-son. Lex.uz milliy qonunchilik ma’lumotlari bazasi.

5. O‘zbekiston Respublikasi Prezidentining “Raqamli O‘zbekiston – 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida”gi 2020-yil 5-oktyabrdagi PF-6079-son Farmoni. Lex.uz milliy qonunchilik ma’lumotlari bazasi.
6. Солдатова Г.У., Нестик Т.А., Рассказова Е.И., Зотова Е.Ю. Цифровая компетентность подростков и родителей: результаты всероссийского исследования. М.: Фонд Развития Интернет, 2013. 144 с.
7. OECD. Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Paris: OECD, 2002.
8. International Telecommunication Union. Guidelines for Policy-makers on Child Online Protection. Geneva: ITU, 2020.
9. Carretero S., Vuorikari R., Punie Y. DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use. Luxembourg: Publications Office of the European Union, 2017.
10. Newhouse W., Keith S., Scribner B., Witte G. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST Special Publication 800-181. Gaithersburg: NIST, 2017.
11. Livingstone S., Haddon L., Görzig A., Ólafsson K. Risks and Safety on the Internet: The Perspective of European Children. Full Findings. London: LSE, EU Kids Online, 2011.
12. Deterding S., Dixon D., Khaled R., Nacke L. From Game Design Elements to Gamefulness: Defining “Gamification” // Proceedings of the 15th International Academic MindTrek Conference. New York: ACM, 2011. pp. 9–15.
13. Prensky M. Digital Natives, Digital Immigrants // On the Horizon. 2001. Vol. 9, No. 5. pp. 1–6.