PEDAGOGICAL MODEL FOR DEVELOPING INFORMATION SECURITY COMPETENCIES AND ITS EFFECTIVENESS CRITERIA

KUTLIMURATOV ANVAR SABUROVICH

Computer Science Teacher, Specialized State General Secondary School No. 65, Beruniy District

Abstract

This thesis proposes a pedagogical model aimed at developing information security competencies among learners and defines its effectiveness criteria. Competence is interpreted not merely as the memorization of knowledge but as a combination of abilities to identify threats, apply protective measures, make safe decisions, and demonstrate responsible behavior in the digital environment. The NICE Framework provides a methodological basis for linking knowledge, skills, and tasks with competencies [1; 2]. DigComp 2.2, in turn, defines the protection of devices, data, and privacy within the framework of digital security [3]. Based on these principles, a pedagogical model consisting of motivational-goal-oriented, content-based, activity-oriented, and reflective-assessment components has been developed, along with cognitive, practical, analytical, and behavioral effectiveness criteria.

Keywords

information security, cybersecurity, competence, pedagogical model, digital competence, assessment criteria, NICE Framework.

AXBOROT XAVFSIZLIGI KOMPETENSIYALARINI SHAKLLANTIRISHNING PEDAGOGIK MODELI VA UNING SAMARADORLIK MEZONLARI

KUTLIMURATOV ANVAR SABUROVICH

Beruniy tumani 65-ixtisoslashgan Davlat umumiy o‘rta ta’lim makabi informatika fani o‘qituvichisi

Annotatsiya

Mazkur tezisda ta’lim oluvchilarda axborot xavfsizligi kompetensiyalarini shakllantirishga yo‘naltirilgan pedagogik model va uning samaradorlik mezonlari taklif etiladi. Kompetensiya bilimni yodlash bilan cheklanmay, xavfni aniqlash, himoya choralarini qo‘llash, xavfsiz qaror qabul qilish va raqamli muhitda mas’uliyatli xatti-harakatni amalga oshirish qobiliyatlarining birligi sifatida talqin qilinadi. NICE Framework bilim, ko‘nikma va vazifalarni kompetensiya bilan bog‘lash uchun metodik asos beradi [1; 2]. DigComp 2.2 esa raqamli xavfsizlik doirasida qurilmalar, ma’lumotlar va maxfiylikni himoyalashni belgilaydi [3]. Shu asosda motivatsion-maqsadli, mazmuniy, faoliyatli va refleksiv-baholash bloklaridan iborat pedagogik model hamda kognitiv, amaliy, analitik va xulq-atvor mezonlari ishlab chiqildi.

Kalit so‘zlar: axborot xavfsizligi, kiberxavfsizlik, kompetensiya, pedagogik model, raqamli kompetensiya, baholash mezonlari, NICE Framework.

Kirish

Raqamli muhitning ta’limga keng kirib borishi ta’lim oluvchidan nafaqat texnik ko‘nikmalarni, balki axborot bilan xavfsiz va mas’uliyatli ishlashni ham talab etmoqda. DigComp 2.2 raqamli kompetensiyaning xavfsizlik yo‘nalishida qurilmalar va raqamli kontentni himoyalash, xavf va tahdidlarni farqlash, maxfiylik hamda shaxsiy ma’lumotlarni himoyalashni muhim kompetensiyalar sifatida ko‘rsatadi [3].

NICE Framework esa Task, Knowledge va Skill elementlari orqali kiberxavfsizlik faoliyatini tavsiflaydi; Competency Areas esa o‘zaro bog‘liq bilim va ko‘nikmalarni muayyan sohadagi qobiliyat sifatida birlashtiradi [1; 2]. NIST 2026-yil 28-aprelda Framework Components v2.2.0 versiyasini e’lon qilgan bo‘lib, unda Work Roles, Competency Areas va TKS statements o‘rtasidagi aloqalar yangilangan [4]. Bu holat

kompetensiyaga yo‘naltirilgan ta’lim modelini zamonaviy kiberxavfsizlik talablari bilan uyg‘unlashtirish zarurligini ko‘rsatadi.

Kompetensiyaning tarkibiy tuzilishi

Tadqiqotda axborot xavfsizligi kompetensiyasi besh o‘zaro bog‘liq komponentdan iborat tizim sifatida qaraladi: kognitiv, amaliy, analitik, xulq-atvor va refleksiv. Bunday tuzilma bilimni real faoliyatga aylantirish va natijani kompleks baholash imkonini beradi [1–3].

Komponent	Asosiy natija
Kognitiv	Tahdidlar, zaifliklar va himoya vositalarini tushuntira oladi.
Amaliy	Xavfsiz sozlamalar va himoya choralarini mustaqil qo‘llaydi.
Analitik	Xavfli vaziyatni aniqlaydi va qarorini asoslaydi.
Xulq-atvor	Raqamli muhitda xavfsiz va mas’uliyatli harakat qiladi.
Refleksiv	O‘z xatosini tahlil qilib, uni tuzatish yo‘lini belgilaydi.

Pedagogik model

Taklif etilayotgan model to‘rt blokdan tashkil topadi. 1) Motivatsion-maqsadli blok — xavfsizlikning ahamiyatini anglash va o‘quv maqsadini belgilash. 2) Mazmuniy blok — tahdidlar, autentifikatsiya, maxfiylik, phishing, zararli dasturlar va xavfsiz xulq-atvorni tizimlashtirish. 3) Faoliyatli blok — vaziyatli topshiriqlar, simulyatsiyalar, amaliy mashqlar va testlar orqali bilimni faoliyatga aylantirish. 4) Refleksiv-baholash blokida natijalar mezonlar asosida aniqlanib, xatolar va rivojlanish dinamikasi tahlil qilinadi.

Modelning umumiy ketma-ketligi: Diagnostika → Maqsad → Mazmun → Faoliyat → Baholash → Refleksiya → Korrektsiya. NICE Framework Competency Areas ta’lim, trening va boshqa o‘quv tajribalari orqali kompetensiyani rivojlantirish va baholashga xizmat qilishi mumkinligini ko‘rsatadi [2].

Samaradorlik mezonlari

Model samaradorligini faqat yakuniy test bilan o‘lchash yetarli emas. Shu sababli besh mezonli kompleks baholash taklif etiladi:

Mezon	Indikator	Vosita
Kognitiv	Tushunchalarni bilish va farqlash	Test
Amaliy	Himoya choralarini bajarish	Amaliy topshiriq
Analitik	Xavfni aniqlash va qarorni asoslash	Case/simulyatsiya
Xulq-atvor	Xavfsiz qarorni qo‘llash	Kuzatuv/vaziyat
Refleksiv	Xatoni aniqlash va tuzatish	Portfolio/refleksiya

Kompleks baholash indeksini metodik model sifatida quyidagicha ifodalash mumkin:

K_as = 0,20K_kog + 0,25K_am + 0,25K_an + 0,20K_xul + 0,10K_ref

Bu yerda K_kog, K_am, K_an, K_xul va K_ref mos ravishda kognitiv, amaliy, analitik, xulq-atvor va refleksiv natijalarni bildiradi. Koeffitsiyentlar tajriba-sinov bosqichida ekspert bahosi va statistik tahlil asosida aniqlashtirilishi mumkin.

Baholashni boshlang‘ich, bazaviy, yetarli va yuqori darajalarga ajratish mumkin. Pre-test va post-test natijalari, amaliy topshiriqlar hamda xulq-atvor indikatorlarini birgalikda tahlil qilish kompetensiya rivojlanishini aniqroq ko‘rsatadi [2; 3].

Natijalar va muhokama

Taklif etilgan modelning asosiy afzalligi — maqsad, mazmun, faoliyat va baholashning yagona tizimga birlashtirilishidir. NICE Framework kompetensiyani bilim va ko‘nikmalarning muayyan vazifalarni bajarish qobiliyati bilan bog‘laydi [1; 2]. Shu sababli ta’lim oluvchining natijasi faqat nazariy savollarga javob bilan emas, balki xavfli vaziyatni tahlil qilishi va xavfsiz qaror qabul qilishi bilan ham baholanadi.

Modelni tajriba-sinovda nazorat va tajriba guruhlari orqali tekshirish, pre-test va post-test natijalarini taqqoslash, amaliy topshiriqlar uchun rubrikalar qo‘llash va natijalarni statistik tahlil qilish maqsadga muvofiq. Bunda indikatorlarning ishonchliligi va o‘lchash vositalarining validligi ham tekshirilishi kerak.

NISTning 2026-yilgi NICE Framework Components v2.2.0 yangilanishida yangi Work Role va Competency Area elementlari kiritilgani kompetensiyalarning zamonaviy texnologik muhitga mos ravishda yangilanib borishini ko‘rsatadi [4]. Demak, pedagogik model ham statik emas, balki yangi tahdidlar va texnologiyalar paydo bo‘lishiga mos ravishda takomillashtiriladigan tizim bo‘lishi lozim.

Xulosa

Axborot xavfsizligi kompetensiyasini shakllantirish bilim, amaliy harakat, tahliliy fikrlash, xavfsiz xulq-atvor va refleksiyaning integratsiyasini talab qiladi. Tadqiqotda ushbu komponentlarni rivojlantirishga qaratilgan to‘rt blokli pedagogik model hamda besh mezonli baholash tizimi taklif qilindi.

Modelning samaradorligini tajriba-sinov asosida tekshirishda kognitiv va amaliy natijalar bilan bir qatorda real yoki simulyatsion vaziyatlarda xavfsiz qaror qabul qilish ko‘rsatkichlarini ham hisobga olish maqsadga muvofiq. Bu yondashuv axborot xavfsizligi ta’limini kompetensiyaga yo‘naltirilgan, o‘lchanadigan va yangilanib boruvchi pedagogik tizimga aylantirish imkonini beradi [1–4].

Foydalanilgan adabiyotlar

1. Petersen R., Santos D., Wetzel K., Smith M., Witte G. Workforce Framework for Cybersecurity (NICE Framework). NIST SP 800-181 Rev. 1. Gaithersburg: NIST, 2020. DOI: 10.6028/NIST.SP.800-181r1.

2. Wetzel K. NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce. NISTIR 8355. Gaithersburg: NIST, 2023. DOI: 10.6028/NIST.IR.8355.

3. Vuorikari R., Kluzer S., Punie Y. DigComp 2.2: The Digital Competence Framework for Citizens. Luxembourg: Publications Office of the European Union, 2022. DOI: 10.2760/115376.

4. National Institute of Standards and Technology. NICE Framework Components v2.2.0. NIST/NICE, 2026.