INFORMATIKA VA TA'LIM MUHITIDA KIBERXAVFSIZLIK VA MA'LUMOTLAR HIMOAYASI KO‘NIKMALARINI SHAKLLANTIRISH METODIKASI

Abdurahimova Muhlisa Zaynobiddin qizi

https://doi.org/10.5281/zenodo.23891003

Annotatsiya. Ushbu ilmiy maqolada umumta'lim va oliy ta'lim muassasalarida informatika fanini o‘qitish doirasida o‘quvchilar va talabalarda kiberxavfsizlik hamda shaxsiy ma'lumotlar muhofazasi bo‘yicha amaliy ko‘nikmalarni shakllantirishning ilmiy-metodik va amaliy asoslari yoritilgan. Raqamli ta'lim muhitida axborot xavfsizligi tahdidlari, kiber-gigiyena qoidalari va fishing xujumlariga qarshi barqarorlikni oshirishga qaratilgan kompyuter simulyatsiyalari hamda loyihaga asoslangan ta'lim (PBL) metodikasining samaradorligi tajriba-sinov ishlari orqali baholangan. Tadqiqot yakunida ta'lim oluvchilarning kibersavodxonlik darajasini oshirish bo‘yicha ilmiy-amaliy tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: informatika, kiberxavfsizlik, ma'lumotlar himoyasi, kiber-gigiyena, raqamli ta'lim, fishing, interfaol simulyatsiya, ta'lim samaradorligi.

Abstract. This scientific article highlights the scientific, methodological, and practical foundations of developing practical skills in cybersecurity and personal data protection among students within the framework of teaching computer science in secondary and higher education institutions. The effectiveness of computer simulations and project-based learning (PBL) methodology aimed at increasing resistance to information security threats, cyber-hygiene rules, and phishing attacks in a digital educational environment was evaluated through experimental work. At the end of the study, practical and scientific recommendations were developed to improve students' cyber literacy levels.

Keywords: computer science, cybersecurity, data protection, cyber hygiene, digital education, phishing, interactive simulation, educational efficiency.

KIRISH

Bugungi jamiyatning jadal raqamlashuvi va barcha sohalarga axborot-kommunikatsiya texnologiyalarining kirib kelishi bir tomondan ulkan imkoniyatlar yaratayotgan bo‘lsa, ikkinchi tomondan axborot xavfsizligi va kiberxavfsizlik bilan bog‘liq jiddiy tahdidlarni keltirib chiqarmoqda. Ayniqsa, yosh avlodning raqamli makonda faol ishtirok etishi, ijtimoiy tarmoqlar va masofaviy ta'lim platformalaridan keng foydalanishi ularni turli kiberxujumlar, fishing, shaxsiy ma'lumotlarning sizib chiqishi hamda fishing kabi firibgarlik harakatlarining nishoniga aylantirmoqda.

O‘zbekiston Respublikasining 'Kiberxavfsizlik to‘g‘risida'gi Qonuni, 'Raqamli O‘zbekiston – 2030' strategiyasi va tegishli normativ-huquqiy hujjatlarda yoshlarning raqamli savodxonligini oshirish, kiberxavfsizlik madaniyatini shakllantirish hamda axborot xavfsizligi bo‘yicha ko‘nikmalarni ta'lim jarayoniga integratsiya qilish muhim ustuvor vazifa sifatida belgilangan. Informatika darslarida an'anaviy ravishda faqat kompyuter qurilmalari va dasturlash tillari o‘rgatilib kelingan bo‘lsa, bugungi kunda kiber-gigiyena va shaxsiy ma'lumotlar daxlsizligi tushunchalarini chuqur o‘rgatish zaruriyati tug‘ilmoqda.

Ushbu tadqiqotning maqsadi – informatika va axborot texnologiyalari darslarida kiberxavfsizlik va ma'lumotlar himoyasi bo‘yicha amaliy ko‘nikmalarni shakllantirish metodikasini ishlab chiqish hamda uning samaradorligini tajriba-sinov ishlari orqali tasdiqlashdan iborat.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Kiberxavfsizlik ta'limi va raqamli xavfsizlik madaniyatini shakllantirish masalalari ko‘plab xorijiy va mahalliy olimlar tomonidan izchil o‘rganib kelinmoqda. Xususan, Whitman va Mattord (2021) o‘z ilmiy ishlarida axborot xavfsizligini ta'minlashda inson omili (Human Factor) eng zaif halqa hisoblanishini ta'kidlab, kiberxavfsizlik bo‘yicha doimiy ta'lim va treninglarning zarurligini ko‘rsatib

© 2026 International Conference on Artificial Intelligence and Applications . All Rights Reserved.

o‘tadilar. Bada va Sasse (2018) tadqiqotlarida foydalanuvchilarning kiber-gigiyena ko‘nikmalari xulq-atvor psixologiyasi va o‘quv metodikalariga bevosita bog‘liqligi isbotlangan.

Mahalliy olimlardan A.A. Abduqodirov, M.A. Aripov va M.Z. Ziyoyev o‘z tadqiqotlarida ta'lim tizimini axborotlashtirish hamda kompyuter tarmoqlarida ma'lumotlarni muhofaza qilish metodikasini ishlab chiqqanlar. Biroq, umumta'lim va oliy ta'lim muassasalarida zamonaviy kibertahdidlarga (social engineering, ransomware, deepfake) qarshi barqaror ko‘nikmalarni shakllantirishning amaliy-simulyatsion metodikasi yetarlicha yoritilmagan.

Tadqiqot usullari sifatida ilmiy adabiyotlar tahlili, kiberxavfsizlik simulyatsiyalari va interfaol keys-stadi usullari, shuningdek, tajriba va nazorat guruhlarida olingan natijalarni matematik-statistik tahlil qilish metodlari tanlab olindi.

ASOSIY QISM VA ERISHILGAN NATIJALAR

Informatika fanini o‘qitishda kiberxavfsizlik va ma'lumotlar himoyasi modullarini samarali tashkil etish uchun interfaol va amaliy yondashuvlardan foydalanish yuqori natija beradi. Tadqiqot doirasida quyidagi asosiy metodik yo‘nalishlar ishlab chiqildi va dars jarayoniga joriy etildi:

1. Kiber-gigiyena va parollar xavfsizligi bo‘yicha interfaol mashg‘ulotlar. O‘quvchilarga murakkab parollarni yaratish, ikki bosqichli autentifikatsiya (2FA) va parollar menejerlaridan foydalanish ko‘nikmalari amaliy ko‘rsatib beriladi.

2. Fishing va ijtimoiy muhandislik xujumlarini simulyatsiya qilish. O‘quvchilarga soxta e-mail va xabarlarni haqiqiylaridan ajratishni o‘rgatish uchun nazorat qilinadigan simulyatsion keyslar yaratiladi.

3. Shaxsiy ma'lumotlarni kriptografik himoyalash va shifrlash asoslari. Ma'lumotlarni shifrlash va ochiq Wi-Fi tarmoqlarida VPN texnologiyalaridan foydalanish bo‘yicha amaliy topshiriqlar bajariladi.

Informatika darslarida an'anaviy va interfaol kiberxavfsizlik ta'limining qiyosiy xususiyatlari 1-jadvalda keltirilgan.

1-jadval

An'anaviy va amaliy-simulyatsion kiberxavfsizlik ta'limining qiyosiy tahlili

Taqqoslama mezonlari	An'anaviy ta'lim usuli	Amaliy-simulyatsion usul
O‘quv shakli	Nazariy ma'ruza va ta'riflar	Interfaol simulyatsiyalar, laboratoriya
Fishiingga bardoshlilik	Faqat nazariy tushunchaga ega	Soxta havolalar va e-maillarni aniqlay oladi
Parol xavfsizligi	Oddiy va takrorlanuvchi parollar	2FA va murakkab parol strategiyalari
Amaliy ko‘nikma	Past (muammoni amalda yecholmaydi)	Yuqori (kibertahdidni vaqtida bartaraf etadi)

TAJRIBA-SINOV ISHLARI VA TAHLIL

Tadbirlar samaradorligini tekshirish maqsadida 2025-2026-o‘quv yilida 130 nafar ta'lim oluvchilar o‘rtasida tajriba-sinov ishlari o‘tkazildi. Ular ikkita guruhga ajratildi: Nazorat guruhi (65 nafar) va Tajriba guruhi (65 nafar).

Nazorat guruhida kiberxavfsizlik mavzulari an'anaviy darslik bo‘yicha nazariy shaklda o‘tildi. Tajriba guruhida esa interfaol kiber-simulyatorlar va amaliy topshiriqlar metodikasi qo‘llanildi. O‘quvchilarning kiberxavfsizlik ko‘nikmalari 2-jadvalda keltirilgan dinamika bo‘yicha baholandi.

2-jadval

O‘quvchilarning kiberxavfsizlik va ma'lumotlar himoyasi bo‘yicha ko‘rsatkichlari (%)

Guruhlar	Past daraja (%)	O‘rta daraja (%)	Yuqori daraja (%)
Nazorat guruhi (Dastlab)	38.5%	46.1%	15.4%
Nazorat guruhi	27.7%	50.8%	21.5%

© 2026 International Conference on Artificial Intelligence and Applications . All Rights Reserved.

(Yakuniy)			
Tajriba guruhi (Yakuniy)	6.1%	32.3%	61.6%

Natijalar shuni ko‘rsatdiki, tajriba guruhida kiberxavfsizlik va ma'lumotlar himoyasi bo‘yicha yuqori ko‘rsatkichga ega bo‘lganlar ulushi 15.4% dan 61.6% gacha ko‘tarildi. Past o‘zlashtiruvchilar soni esa 6.1% gacha qisqardi. Bu esa taklif etilayotgan amaliy-simulyatsion metodikaning samaradorligini ilmiy jihatdan isbotlaydi.

MUHOKAMA

Tadqiqot natijalari shuni ko‘rsatadiki, informatika ta'limida kiberxavfsizlik va ma'lumotlar himoyasini faqat nazariy tushuncha sifatida emas, balki amaliy kiber-gigiyena ko‘nikmasi sifatida o‘qitish zarur. Biroq, amaliyotda maktablar va kollejlarning laboratoriya bazalari doim ham eng so‘nggi dasturiy va apparat ta'minoti bilan jihozlanmaganligi muammo bo‘lib qolmoqda.

Shuningdek, o‘qituvchilarning kiberxavfsizlik sohasidagi bilimlari va amaliy malakasini doimiy ravishda oshirib borish zarur. Sababi, kibertahdidlar (phishing, social engineering, malware) doimiy ravishda evolyutsiya qilib boradi. O‘qituvchi o‘quvchilarga ushbu o‘zgarishlarga mos ravishda bilim berishi lozim.

XULOSA VA TAVSIYALAR

O‘tkazilgan tadqiqotlar va tajriba-sinov ishlari asosida quyidagi xulosalarga kelindi:

1. Informatika darslarida kiberxavfsizlik va ma'lumotlar himoyasiga oid amaliy mashg‘ulotlarni ko‘paytirish o‘quvchilarning raqamli makonda xavfsiz harakat qilish ko‘nikmalarini sezilarli darajada oshiradi.

2. Interfaol simulyatsiya va keys-stadi usullari o‘quvchilarda fishing xujumlariga va shaxsiy ma'lumotlarning sizib chiqishiga qarshi amaliy immunitet hosil qiladi.

Tadqiqot natijalaridan kelib chiqqan holda quyidagi amaliy tavsiyalar ilgari suriladi:

– Informatika fanining o‘quv dasturlariga 'Kiberxavfsizlik va kiber-gigiyena asoslari' amaliy modulini kengaytirilgan holda kiritish;

– O‘quvchilar uchun kiberxavfsizlik bo‘yicha interfaol onlayn simulyatorlar va test sinovlari platformasini yaratish;

– Informatika o‘qituvchilarining kiberxavfsizlik va ma'lumotlar muhofazasi bo‘yicha malakasini oshirish kurslarini muntazam tashkil etish.

FOYDALANILGAN ADABIYOTLAR

1. O‘zbekiston Respublikasining 2022-yil 15-apreldagi 'Kiberxavfsizlik to‘g‘risida'gi O‘RQ-764-son Qonuni.
2. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi 'Raqamli O‘zbekiston – 2030' strategiyasini tasdiqlash to‘g‘risida'gi PF-6079-son Farmoni.
3. Whitman M.E., Mattord H.J. Principles of Information Security. 7th Edition. – Cengage Learning, 2021. – 656 p.
4. Bada M., Sasse A.M. Cyber Hygiene and the Human Factor: The Weakest Link or the Strongest Defence? // Cyber Security: Critical Infrastructure Protection. – 2018. – P. 123-138.
5. Abduqodirov A.A., Pardaev A.H. Masofaviy o‘qitish nazariyasi va amaliyoti. – Toshkent: Fan va texnologiya, 2018. – 216 b.
6. Aripov M.A., Tillayev AI. Axborot xavfsizligi va kriptografiya asoslari. Darslik. – Toshkent: Университет, 2020. – 280 b.
7. Ziyoyev M.Z. Raqamli ta'lim muhitida ma'lumotlar muhofazasi va kiber-gigiyena // Ta'lim va innovatsion tadqiqotlar. – 2023. – №3. – B. 88-94.
8. Hadlington L. Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, and cyberloafing // Computers in Human Behavior. – 2017. – Vol. 76. – P. 320-325.

© 2026 International Conference on Artificial Intelligence and Applications . All Rights Reserved.