DOI: https://doi.org/10.37547/supsci-oje-05-07-25 Pages: 196-200

Oriental Journal of Education

ORIENTAL JOURNAL OF EDUCATION

journal homepage:
https://www.supportscience.uz/index.php/oje

METHODOLOGY FOR INTEGRATING CYBERSECURITY ELEMENTS INTO THE INFORMATICS CURRICULUM OF GENERAL EDUCATION SCHOOLS

Nekruz Nurboyevich Norboyev
Jizzakh Regional Pedagogical Skills Center
Chief Specialist of the "Digital Technologies Development" Department
Jizzakh, Uzbekistan

ABOUT ARTICLE

Key words: Cybersecurity, digital literacy, internet safety, phishing, social engineering, teaching methodology of Informatics, digital competence, cyberattack, antivirus, information security, digital pedagogy.

Received: 04.12.25
Accepted: 05.12.25
Published: 06.12.25

Abstract: This article provides an extensive overview of the scientific-theoretical, methodological, and practical foundations of integrating cybersecurity elements into the Informatics curriculum of general education schools. In the context of growing digital transformation, developing students' digital literacy has become one of the key priorities of the education system. The increasing need to enhance students' skills for safe and responsible internet use further underscores the relevance of this topic. The article highlights the experiences of international organizations (UNESCO, OECD, UNICEF), the methodological approaches of leading countries in incorporating cybersecurity into school education, the normative and legal framework of Uzbekistan's education system, as well as the outcomes of pilot experiments. Finally, a customized "Basic Module of Cybersecurity" adapted for Informatics lessons is proposed.

KIBERXAVFSIZLIK ELEMENTLARINI UMUMTA'LIM MAKTABLARI INFORMATIKA KURSIGA INTEGRATSIYA QILISH METODIKASI

Nekro'z Nurboyevich Norboyev
"Raqamli texnalogiyalarni rivojlantirish" bo'limi bosh mutaxassisi
Jizzax viloyati pedagogik mahurat markazi
Jizzax, O'zbekiston

MAQOLA HAQIDA

Kalit so'zlar: Kiberxavfsizlik, raqamli madaniyat, internet xavfsizligi, phishing, social engineering, informatika fanini o'qitish metodikasi, raqamli kompetensiya, kiberhujum,

Annotatsiya: Mazkur maqolada umumta'lim maktablarida informatika faniga kiberxavfsizlik elementlarini integratsiya qilishning ilmiy-nazariy, metodik va amaliy

antivirus, axborot xavfsizligi, raqamli pedagogika.

asoslari keng yoritilgan. Raqamli transformatsiya jarayonlari kuchayib borayotgan bugungi sharoitda o‘quvchilarning raqamli madaniyatini shakllantirish ta’lim tizimining ustuvor yo‘nalishlaridan biridir. O‘quvchilarning internetdan xavfsiz va ongli foydalanish malakasini rivojlantirish zarurati bu mavzuning dolzarbligini oshiradi. Maqolada xalqaro tashkilotlar (UNESCO, OECD, UNICEF)ning tajribasi, dunyodagi ilg‘or davlatlarning kiberxavfsizlikni maktab ta’limiga joriy etish metodikasi, O‘zbekiston ta’lim tizimining normativ-huquqiy asoslari, shuningdek, tajriba-sinov ishlarining natijalari yoritiladi. Yakunda informatika darslariga moslashtirilgan “Kiberxavfsizlikning boshlang‘ich moduli” taklif etiladi.

МЕТОДИКА ИНТЕГРАЦИИ ЭЛЕМЕНТОВ КИБЕРБЕЗОПАСНОСТИ В КУРС ИНФОРМАТИКИ ОБЩЕОБРАЗОВАТЕЛЬНЫХ ШКОЛ

Некруз Нурбоевич Норбоев
Джизакский областной центр педагогического мастерства
Главный специалист отдела «Развитие цифровых технологий»
Джизак, Узбекистан

О СТАТЬЕ

Ключевые слова: Кибербезопасность, цифровая культура, интернет-безопасность, фишинг, социальная инженерия, методика преподавания информатики, цифровая компетентность, кибератака, антивирус, информационная безопасность, цифровая педагогика.

Аннотация: В данной статье всесторонне освещены научно-теоретические, методические и практические основы интеграции элементов кибербезопасности в учебный предмет «Информатика» общеобразовательных школ. В условиях усиливающихся процессов цифровой трансформации формирование цифровой культуры учащихся становится одним из приоритетных направлений системы образования. Возрастающая необходимость развития у школьников навыков безопасного и осознанного использования интернета делает данную тему особенно актуальной. В статье представлены опыт международных организаций (UNESCO, OECD, UNICEF), методики ведущих стран мира по внедрению кибербезопасности в школьное образование, нормативно-правовая база системы образования Узбекистана, а также результаты опытно-экспериментальной работы. В заключение предлагается адаптированный

для уроков информатики модуль «Основы кибербезопасности».

Kirish. XXI asrda raqamli iqtisodiyot, sun’iy intellekt hamda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalariga, ayniqsa ta’lim tizimiga sezilarli ta’sir ko‘rsatmoqda. Internet va raqamli texnologiyalar bugungi kunda o‘quvchilarning bilim olish jarayonida asosiy vositalardan biriga aylangan. Shu bilan birga, raqamli muhitning kengayishi kiberxavfsizlik bilan bog‘liq tahdidlarning ham ortishiga olib kelmoqda. Mazkur holat yoshlarning internetdan xavfsiz va ongli foydalanishini ta’minlash masalasini dolzarb muammolardan biriga aylantirmoqda.

O‘zbekiston umumta’lim maktablarida internetdan foydalanuvchi o‘quvchilar sonining keskin ortishi kiberxavfsizlik masalasiga alohida e’tibor qaratishni talab etadi. 2023–2024-yillarda internetdan faol foydalanayotgan o‘quvchilar soni 7,8 million nafardan oshgani ta’lim jarayonida raqamli texnologiyalarning qanchalik chuqur singib borayotganini ko‘rsatadi. Biroq olib borilgan kuzatuvlar shuni ko‘rsatadiki, o‘quvchilarning aksariyati phishing hujumlari, zararli dasturlar, ijtimoiy tarmoqlardagi firibgarliklar va shaxsiy ma’lumotlarni himoyalash masalalarida yetarli bilim va ko‘nikmalarga ega emas. Shu sababli kiberxavfsizlik elementlarini informatika faniga integratsiya qilish muhim pedagogik vazifa sifatida qaralmoqda.

Natijalar va muhokama. Tadqiqot jarayonida umumta’lim maktablari informatika faniga kiberxavfsizlik elementlarini integratsiya qilishning pedagogik samaradorligi amaliy tajriba-sinov ishlari orqali tahlil qilindi. Tadqiqot doirasida Toshkent, Jizzax va Farg‘ona viloyatlaridagi 6 ta umumta’lim maktabi tanlab olinib, ularda 5–11-sinf o‘quvchilari bilan maxsus ishlab chiqilgan kiberxavfsizlik o‘quv modullari asosida mashg‘ulotlar olib borildi. Tajriba jarayonida nazariy bilimlar amaliy mashg‘ulotlar, interfaol topshiriqlar, real hayotiy vaziyatlarga asoslangan keyslar va simulyatsiyalar bilan uyg‘unlashtirildi.

Tajriba-sinov ishlari boshlanishidan oldin o‘quvchilarning kiberxavfsizlik bo‘yicha bilim va ko‘nikmalari diagnostik testlar, so‘rovnomalar hamda amaliy vazifalar orqali aniqlandi. Dastlabki natijalar o‘quvchilarning aksariyatida raqamli muhitdagi xavf-xatarlar haqida umumiy tasavvur mavjud bo‘lsa-da, ularni amaliy jihatdan aniqlash va oldini olish bo‘yicha ko‘nikmalar yetarli emasligini ko‘rsatdi. Masalan, ko‘pchilik o‘quvchilar kuchli parol yaratish mezonlarini bilmasligi, phishing xabarlarini oddiy reklama yoki xizmat xabarlari bilan adashtirishi hamda shaxsiy akkauntlarda maxfiylik sozlamalarini to‘g‘ri o‘rnatishda qiyinchilikka duch kelayotgani aniqlandi.

Tajriba yakunida o‘tkazilgan takroriy baholash natijalari esa kiberxavfsizlik elementlarini informatika faniga tizimli integratsiya qilishning ijobiy samarasini yaqqol namoyon etdi. Quyidagi jadvalda tajriba-sinovdan oldingi va keyingi natijalar solishtirma ko‘rinishda keltirilgan:

1-jadval. O‘quvchilarning kiberxavfsizlik bo‘yicha ko‘nikmalari darajasining o‘zgarishi

Ko‘nikma turi	Sinovdan oldin (%)	Sinovdan keyin (%)
Kuchli parol yaratish	28	82
Phishing hujumlarini aniqlash	15	74
Maxfiylik sozlamalarini o‘rnatish	22	69
Zararli dasturlarni tanish	18	67

Jadval ma’lumotlari tahlili shuni ko‘rsatadiki, barcha ko‘rsatkichlar bo‘yicha sezilarli ijobiy o‘sish kuzatilgan. Xususan, kuchli parol yaratish bo‘yicha ko‘rsatkich 28 foizdan 82 foizga oshgani o‘quvchilarda shaxsiy akkauntlarni himoyalash bo‘yicha ongli yondashuv shakllanganini anglatadi. Bu holat parol yaratish bo‘yicha laboratoriya mashg‘ulotlari, real platformalar misolida ko‘rsatmalar berilishi va xatolar ustida tahlil olib borilgani bilan izohlanadi.

Phishing hujumlarini aniqlash bo‘yicha natijalarning 15 foizdan 74 foizga oshishi ayniqsa muhim hisoblanadi. Chunki amaliy kuzatuvlarga ko‘ra, o‘quvchilar internetda eng ko‘p aynan soxta havolalar va firibgarlik xabarlariga duch keladi. Mashg‘ulotlar davomida haqiqiy va soxta xabarlarni taqqoslash, “soxta linkni aniqlang” kabi interfaol topshiriqlarni bajarish o‘quvchilarning tanqidiy fikrlashini rivojlantirdi va ularni ehtiyotkorlikka o‘rgatdi.

Shuningdek, maxfiylik sozlamalarini o‘rnatish bo‘yicha ko‘nikmalar darajasining 22 foizdan 69 foizga oshgani o‘quvchilarning shaxsiy ma’lumotlar bilan ishlash madaniyati shakllanayotganidan dalolat beradi. O‘quvchilar amaliy mashg‘ulotlar davomida Google, Telegram va ijtimoiy tarmoqlarda ikki bosqichli himoyani yoqish, keraksiz ruxsatlarni cheklash va shaxsiy ma’lumotlarni yashirish bo‘yicha mustaqil harakatlarni bajara oldilar.

Zararli dasturlarni tanish bo‘yicha natijalarning oshishi ham muhim ahamiyatga ega. O‘quvchilar viruslar, josuslik dasturlari va boshqa zararli ilovalar qanday belgilar orqali aniqlanishini o‘rganib, antivirus dasturlarining vazifasi va ahamiyatini anglab yetdilar. Virus kirish jarayonini simulyatsiya qilish mashg‘ulotlari mavzuning amaliy jihatdan chuqur o‘zlashtirilishiga xizmat qildi.

Natijalar muhokamasi shuni ko‘rsatadiki, interfaol va amaliy yondashuvlarga asoslangan ta’lim shakllari o‘quvchilarning faolligini oshiradi, mavzuga bo‘lgan qiziqishini kuchaytiradi hamda bilimlarning uzoq muddatli mustahkamlanishiga yordam beradi. Shu bilan birga, tadqiqot davomida ayrim muammolar ham aniqlandi. Jumladan, ayrim o‘qituvchilarning kiberxavfsizlik bo‘yicha bilimlari yetarli emasligi, mavjud darsliklarda mazkur mavzuning cheklangan yoritilgani va o‘quvchilarning internet xavflarini dastlab yetarlicha jiddiy baholamaganligi kuzatildi.

Mazkur muammolarni bartaraf etish uchun o‘qituvchilarni qayta tayyorlash va malakasini oshirish kurslarini tashkil etish, kiberxavfsizlik bo‘yicha alohida o‘quv modullari va metodik qo‘llanmalar ishlab chiqish, shuningdek, ta’lim jarayonida zamonaviy pedagogik texnologiyalar va raqamli vositalardan keng foydalanish maqsadga muvofiqdir. Umuman olganda, olingan natijalar informatika faniga kiberxavfsizlik elementlarini integratsiya qilishning pedagogik va amaliy jihatdan samarali ekanini ilmiy asosda tasdiqlaydi.

Xulosa. O‘tkazilgan tadqiqot natijalari shuni ko‘rsatadiki, informatika faniga kiberxavfsizlik elementlarini tizimli ravishda integratsiya qilish o‘quvchilarning raqamli savodxonligini oshirishda muhim ahamiyatga ega. Bu jarayon o‘quvchilarni internet muhitidagi real xavf-xatarlardan himoyalash, shaxsiy ma’lumotlar bilan ishlash madaniyatini shakllantirish va ularni ongli raqamli foydalanuvchi sifatida tarbiyalashga xizmat qiladi.

Shuningdek, kiberxavfsizlikka oid bilim va ko‘nikmalarni maktab yoshidan boshlab shakllantirish o‘quvchilarning axborot texnologiyalari sohasiga bo‘lgan qiziqishini oshirib, ularning kelajak kasbiy faoliyatiga ijobiy ta’sir ko‘rsatadi. Umuman olganda, kiberxavfsizlikni umumta’lim maktablari informatika faniga integratsiya qilish ta’lim sifatini oshirish, davlatning raqamli xavfsizlik siyosatini qo‘llab-quvvatlash hamda jamiyatda xavfsiz raqamli muhitni shakllantirishning muhim omillaridan biri hisoblanadi.

Foydalanilgan adabiyotlar ro‘yxati:

1.Sh.M. Mirziyoyev. “Raqamli O‘zbekiston – 2030” strategiyasi bo‘yicha nutqlari.
2.O‘zbekiston Respublikasi Prezidentining Murojaatnomalari.
3.UNESCO. Digital Safety Education Framework, 2023.
4.UNICEF. “Cyber Safety for Children”, 2022.
5.OECD. Cybersecurity in Schools, 2023.
6.Microsoft Education Annual Report, 2024.
7.Tursunov A. Informatika o‘qitish metodikasi. – Toshkent, 2020.
8.Xudayberdiyev A. Axborot xavfsizligi asoslari. – Toshkent, 2022.
9.CERT Uzbekistan statistika hisobotlari, 2024.
10.Cisco Networking Academy Materials, 2023.
11.Kaspersky Lab Training Manual, 2024.