International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

MAKTAB O‘QUVCHILARINI KIBERMAKONDA XAVFSIZLIKKA O‘RGATISH

https://doi.org/10.5281/zenodo.13892933

Norbekov Doston Keldibekovich
Jizzax viloyati pedagogik mahorat markazi katta o‘qituvchisi

Annotatsiya

Ushbu maqolada boshlang‘ich maktabning turli sinflarida o‘quvchilarga taklif qilinadigan raqobatbardosh vazifalar tizimini ishlab chiqishning kontseptual asoslari keltirilgan va ularni hal qilish bilan bog‘liq muammolar misollari keltirilgan. Fikrimizcha, bunday vazifalarning maktab informatika darsliklari mazmuniga kiritilishi o‘qituvchilarga o‘quvchilarni kiber tahdidlarni tan olishga va ular bilan duch kelganda o‘zini to‘g‘ri tutishga tayyorlash uchun chinakam samarali vositalarni taqdim etadi.

Аннотация

В методической рекомендации приведена контекстуальная основадля разработки системы конкурсных заданий, которые предлагаются учащимся в разных классах начальной школы, и приведены примеры задач, связанных с их решением.

На наш взгляд, включение таких заданий в содержание школьных учебников информатики дает учителям по-настоящему эффективные инструменты для подготовки учащихся к распознаванию киберугроз и правильному поведению при столкновении с ними.

Annotation

The methodological recommendation provides contextual basis for developing a system of competitive tasks that students are offered in different classes of primary school and provides examples of problems related to solving them. In our view, the inclusion of such tasks in the content of school informatics textbooks provides teachers with truly effective tools to prepare students to recognize cyber threats and behave properly when confronted with them.

KIRISH

O‘quvchilarni Internetda xavfsiz hatti-harakatlarga tayyorlash davlat darajasida tan olingan u mumta’lim maktabining eng muhim vazifalaridan biri bo‘lib, “Kiberxavfsizlik to‘g‘risida”gi QL-869-sonli O‘zbekiston Respublikasi qonuni loyihasi haqidaO‘zbekiston Respublikasi Oliy Majlisining Qonunchilik palatasi qaror qiladi: O‘zbekiston Respublikasi Vazirlar Mahkamasi tomonidan 2022-yil 5-yanvarda kiritilgan “Kiberxavfsizlik to‘g‘risida”gi QL-869-sonli

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

O‘zbekiston Respublikasi qonuni loyihasi qabul qilindi. O‘zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasining Innovatsion rivojlanish, axborot siyosati va axborot texnologiyalari masalalari qo‘mitasi kelib tushgan tuzatishlarni hisobga olgan holda mazkur qonun loyihasini uch oy ichida maromiga yetkazsin va ikkinchi o‘qishda Qonunchilik palatasi muhokamasiga kiritildi va tasdiqlandi.

Global tarmoqning zamonaviy jamiyat hayotining barcha jabhalariga kirib borishi yosh avlodni axborot makoniga jalb qilishga olib keldi. Ota-onalar farzandlari uchun kompyuter va mobil hisoblash qurilmalarini sotib olayotganda, har doim ham farzandlari kibermakonda qanday xavf-xatarlarga duch kelishi haqida o‘ylamaydilar. Maktab hududida ushbu tahdidlar o‘quvchilarning Internet orqali tarqatiladigan, ularning sog‘lig‘i yoki rivojlanishiga zarar yetkazadigan va ta’lim maqsadlariga mos kelmaydigan ma’lumotlar turlaridan foydalanishini cheklash orqali minimallashtiriladi. Maktab devorlari tashqarisida bolalar bu tahdidlar bilan yuzma-yuz turishadi. Boshlang‘ich sinf o‘quvchilari Internetda qancha vaqt sarflashadi? Ularni kiberkosmosga nima jalb qiladi? Ular Internetda o‘tkazadigan o‘rtacha vaqt 1,5 dan 4 soatgacha. Bolalar bu vaqtni uy vazifalarini bajarish, filmlar tomosha qilish, onlayn o‘yinlar o‘ynash va ijtimoiy tarmoqlarda muloqot qilish bilan o‘tkazadilar. Shu bilan birga, respondentlarning 72 foizi Internetda salbiy, yoqimsiz va hatto xavfli ma’lumotlarga duch kelganini qayd etdi. Maktab o‘quvchilari orasida intruziv reklama, «g‘ayrioddiy» guruhga a’zo bo‘lish taklifi, shaxsiy ma’lumotlar (uyali telefon raqami, ijtimoiy tarmoqqa kirish uchun foydalanuvchi nomi va parol va boshqalar) evaziga katta chegirmalar taklifi, taklifnoma kiradi. Yangi onlayn tanishlar bilan haqiqiy hayotda uchrashish. Bolalar ba’zi vaziyatlarda noqulaylik va hatto qo‘rquv hissini boshdan kechirganliklarini ta’kidlashdi, ammo ularning hammasi ham ota-onalari va do‘stlariga yordam so‘rab murojaat qilishmadi.

O‘quvchilarga kibermakonning yuzaga kelishi mumkin bo‘lgan xavf-xatarlarini ochib berish, ularni kibertahdidga duch kelganda to‘g‘ri xulq-atvorga o‘rgatish – bugungi kunda uni hal etish umumta’lim maktablari zimmasiga yuklatilgan vazifadir. Ushbu muammoni hal qilishda maktablarga yordam berish uchun “Kiberxavfsizlik asoslari” kursini umumta’lim maktablari o‘quv dasturlariga kiritish va o‘quvchilarni internetda xavfsiz xulq-atvorga o‘rgatish uchun mavjud fanlar o‘quv dasturlarini modernizatsiya qilish bo‘yicha Maqola ishlab chiqildi. Ushbu kursning asosiy maqsadi talabalarga axborot jamiyati xavfsizligi haqida umumiy tushuncha berish, shu asosda talabalarda axborot xavfsizligi texnologiyalari haqida tushuncha va faoliyatning barcha sohalarida kiberxavfsizlik qoidalarini qo‘llash ko‘nikmalarini shakllantirishdan iborat.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

Metodik tavsiya kiber tahdidning u yoki bu turiga qarshi kurashish usullarini ochib beruvchi modullarda taqdim etilgan: “Internetga qaramlik muammolari”, “Internetdagi firibgarlik harakatlari. Kiberjinoyatlar”, “Kibermakonni himoya qilishning huquqiy jihatlari” va boshqalar. Maqolada modullar ro‘yxati va ularni o‘zlashtirish natijalariga qo‘yiladigan talablardan tashqari, turli fanlarga oid o‘quv mashg‘ulotlaridan namunalar keltirilgan va talabalarni o‘qitish muammolarini hal etishga qaratilgan.

Kiberxavfsizlikni fundamental atamalari

Konfidensiallik – axborot yoki uni eltuvchining shunday holati bo‘lib, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi. Konfidensiallik axborotni ruxsatsiz “o‘qish” dan himoyalash bilan shug‘ullanadi. Yaxlitlik axborotning buzilmagan ko‘rinishida (axborotning qandaydir qaydetilgan holatiga nisbatan o‘zgarmagan shaklda) mavjud bo‘lishi ifodalangan xususiyati.

Risk – potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilganida risk paydo bo‘ladi. ISO “risk – bu noaniqlikning maqsadlarga ta’siri” sifatida ta’rif bergan [14]. Masalan, universitetga o‘qishga kirish jarayonini ko‘raylik. Umumiy holda bu jarayonni o‘zi risk hisoblanmaydi. Faqatgina abituriyent hujjatlarini va kirish imtihonlarini topshirganda, u o‘qishga kirishi yoki kira olmasligi mumkin. Bu o‘z navbatida qabul qilinish yoki qabul qilinmaslik riskini yuzaga kelishiga olib keladi. Kiberxavfsizlik yoki axborot xavfsizligida risklar salbiy ko‘rinishda qaraladi.

Hujumchi kabi fikrlash - bo‘lishi mumkin bo‘lgan xavfni oldini olish uchun qonuniy foydalanuvchini hujumchi kabi fikrlash jarayoni.

Tizimli fikrlash - kafolatlangan amallarni ta’minlash uchun ijtimoiy va texnik cheklovlarning o‘zaro ta’sirini hisobga oladigan fikrlash jarayoni. Bundan tashqari quyidagi tushunchalar ham kiberxavfsizlik sohasini chuqur o‘rganishda muhim hisoblanadi.

Axborot xavfsizligi - axborotning holati bo‘lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta’sir etishga yoki ruxsatsiz undan foydalanishga yo‘l qo‘yilmaydi. Yoki, axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalanish sathi holati.

Axborotni himoyalash – axborot xavfsizligini ta’minlashga yo‘naltirilgan choralar kompleksi. Amalda axborotni himoyalash deganda ma’lumotlarni kiritish, saqlash, ishlash va uzatishda uning yaxlitligini, foydalanuvchanligini va agar, kerak bo‘lsa, axborot va resurslarning konfidensialligini madadlash tushuniladi.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

Aktiv - himoyalanuvchi axborot yoki resurslar. Yoki, tashkilot uchun qimmatli barcha narsalar.

Tahdid – tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. Yoki, tahdid - axborot xavfsizligini buzuvchi potensial yoki real mavjud xavfni tug‘diruvchi sharoit va omillar majmui. Tahdid tashkilotning aktivlarigaqaratilgan bo‘ladi. Masalan, aktiv sifatida korxonaga tegishli biror bir saqlanuvchi hujjat bo‘lsa, u holda ushbu hujjat saqlanadigan xonaga nisbatan tahdid amalga oshirilish mumkin.

Zaiflik – bir yoki bir nechta tahdidlarni amalga oshirishga imkon beruvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik hisoblanadi. Masalan, xonada saqlanayotgan tashkilot hujjati qog‘oz ko‘rinishda bo‘lganligi sababli, yonib ketishi mumkin.

Boshqarish vositasi – riskni o‘zgartiradigan harakatlar bo‘lib, boshqarish natijasi zaiflik yoki tahdidlarni o‘zgarishiga ta’sir qiladi. Bundan tashqari boshqarish vositasining o‘zi turli tahdidlar foydalanishi mumkin bo‘lgan zaiflikka ega bo‘lishi mumkin. Masalan, tashkilotda saqlanayotgan qog‘oz ko‘rinishidagi axborotni yong‘indan himoyalash uchun o‘chirish vositalari boshqarish vositasi sifatida ko‘rilishi mumkin. Bundan tashqari, yong‘in bo‘lganda xodimlarning hattiharakatlari va yong‘inni oldini olish bo‘yicha ko‘rilgan chora-tadbirlar ham boshqarish vositasi hisoblanishi mumkin. Yong‘inga qarshi kurashish tizimining ishlamay qolish holatiga esa boshqarish vositasidagi kamchilik sifatida qarash mumkin.

Axborot xavfsizligi va kiberxavfsizlik o‘rtasidagi farq

“Kiberxavfsizlik” va “axborot xavfsizligi” atamalaridan, tez-tez o‘rnilari almashingan holatda, foydalaniladi. Ba’zilar kiberxavfsizlikni axborot xavfsizligi, axborot texnologiyalari xavfsizligi va (axborot) risklarni boshqarish tushunchalariga sinonim sifatida foydalanadilar. Ayrimlar esa, xususan, hukumat sohasidagilar kiberxavfsizlikka kompyuter jinoyatchiligi va muhim infratuzilmalar himoyasini o‘zichiga olgan milliy xavfsizlik bilan bog‘liq bo‘lgan texnik tushuncha sifatida qaraydilar. Turli soha xodimlari tomonidan o‘z maqsadlariga moslashtirish holatlari mavjud bo‘lsada, axborot xavfsizligi va kiberxavfsizlik tushunchalari orasida ba’zi muhim farqlar mavjud. Axborot xavfsizligi sohasi axborotning ifodalanishidan qat’iy nazar – qog‘oz ko‘rinishdagi, elektron va insonlar fikrlashida, og‘zaki va vizual aloqada intelektual huquqlarini himoyalash bilan shug‘ullanadi. Kiberxavfsizlik esa elektron shakldagi axborotni (barcha holatlardagi, tarmoqdan to qurilmagacha bo‘lgan, o‘zaro birga ishlovchi tizimlarda saqlanayotgan, uzatilayotgan va ishlanayotgan axborotni) himoyalash bilan

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

shug‘ullanadi. Bundan tashqari, hukumatlar tomonidan moliyalashtirilgan hujumlar va rivojlangan doimiy tahidlar (Advanced persistentthreats, APT) ham aynan kiberxavfsizlikka tegishlidir. Qisqacha aytganda, kiberxavfsizlikni axborot xavfsizligining bir yo‘nalishi deb tushunish uni to‘g‘ri anglashga yordam beradi.

Kiberxavfsizlik vazifalarini ishlab chiqishning nazariy asoslari.

Vazifalar mazmunini ishlab chiqish uchun asos sifatida “Kiberxavfsizlik asoslari” Maqolaining tematik modullari olindi. Talabalarning yosh xususiyatlari, qiziqishlari va kibermakondagi faolligini hisobga olgan holda ular batafsil yoritib berildi. Shunday qilib, 5-sinfda “Kompyuter va internet xavfsizligi haqida umumiy ma’lumot” moduli doirasida kompyuter o‘yinlari (bepul va pullik) hamda internetda xarid qilish xususiyatlari ko‘rib chiqildi; 6-sinfda mobil qurilmalarga kibertahdidlar masalalari, 7-sinfda shaxsiy ma’lumotlarni himoya qilish xususiyatlarini ochib berishga qaratilgan topshiriqlar, 8-9-sinflarda topshiriqlar o‘quvchilarni kiberjinoyatlarni ochish, ularning oldini olish va ularga qarshi kurashish bo‘yicha faoliyatni qamrab oldi. Turli yoshdagi talabalar uchun «Kiberxavfsizlik asoslari» kursining «Kompyuter va Internet xavfsizligi haqida umumiy ma’lumot» moduli mazmunini o‘zlashtirishni sinovdan o‘tkazadigan topshiriqlar beriladi.

1-muammo (5-sinf)

Ko‘rsatmalar. Berilganlardan bir nechta to‘g‘ri javob variantlarini tanlang.

Mashq qilish. «Stoon» o‘yinini ishlab chiquvchi uni yaratish uchun besh yil sarfladi. «Stoon» chiqarilganda, Rustamjon ushbu o‘yinni sotib olishni juda xohladi. Do‘konga kelib, u narxning yuqori ekanligini bilib, yordam uchun Internetga murojaat qilishga qaror qildi. Tarmoqdagi birinchi havolani bosgandan so‘ng, Rustam yozuvni ko‘rdi: «Stoon» o‘yini bepul va uni quyidagi havoladan yuklab olishingiz mumkin. Quyida keltirilgan variantlardan Rustamga taklif qiladigan variantni tanlang.

A) O‘yinni ushbu saytdan yuklab oling, chunki u yerda bepul.

B) Ota-onangizdan pul so‘rang va uni do‘konda sotib oling.

C)O‘yinni chegirma bilan sotib olish imkoniyati bilan Internetda qidirishni davom eting.

To‘g‘ri javoblar: B va C.

2-masala (6-sinf)

Ko‘rsatmalar. Vaziyatning tavsifini o‘qing va berilgan savollarga batafsil javob bering.

Mashq qilish. E’zozaning onasi ish joyiga kelib, uyida mobil telefonini unutib qo‘yganini aniqladi. U E’zozaga ish telefonidan qo‘ng‘iroq qilib, uni ish joyiga olib

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

kelishni so‘radi. Suhbatni tugatgandan so‘ng, E’zoza qo‘shni xonada onasining mobil telefoniga SMS kelganini eshitdi. E’zoza va uning onasi ishonchli munosabatlarga ega bo‘lganligi sababli, qiz unga kelgan SMS-xabarni o‘qidi. E’zoza xabar noma’lum jo‘natuvchidan kelganini payqadi. Unda quyidagi matn bor edi: “Xayrli kun! Pasport ma’lumotlariga ko‘ra, 30000 so‘m miqdorida sug‘urta to‘lovlari topilgan. Tafsilotlar veb-saytda: http://snils-gost.online.» Qiz, oqibatlari haqida o‘ylamasdan, havolaga ergashdi. Ochilgan brauzer oynasida onasining pasport ma’lumotlari haqida hech qanday ma’lumot yo‘q edi va E’zoza uni yopdi. Bir necha daqiqadan so‘ng mobil telefoningizga mobil operatordan SMS-xabar keldi: «Sizning balansingiz 5000 so‘mdan kam.» Pulning yo‘qolishi SMS-xabardagi havolani bosish bilan bog‘liq deb gumon qilib, E’zoza qo‘rqib ketdi va onasining ishiga yugurdi.

E’zoza qanday xatolarga yo‘l qo‘ydi?

E’zozaning harakatlari natijasida qanday oqibatlarga olib kelishi mumkin? Javobingizni asoslang.

Bolalar uchun SMS-firibgarlik belgilari va ular bilan uchrashishda o‘zini tutish qoidalari tasvirlangan tavsiyalar bering.

To‘g‘ri javoblar:

a) Men unga yuborilmagan xabarni o‘qib chiqdim va shubhali havolaga ergashdim.

b) Havolani bosish 1) hisobdan pul yechib olinishiga, 2) telefonga viruslar yuklanishiga olib kelishi mumkin, bu esa qurilmaning normal ishlashini to‘xtatadi va barcha shaxsiy ma’lumotlarni yuklab oladi, 3) qachon telefonni kompyuterga ulaganda, bu qurilma ham zararlanadi.

c) SMS-firibgarlik belgilari: noma’lum jo‘natuvchining raqami; raqam juda qisqa; xabarda yutuq haqidagi ma’lumotlar mavjud bo‘lib, uni olish uchun siz ko‘rsatilgan havolaga o‘tishingiz kerak; qayta qo‘ng‘iroq qilishni so‘rash; pul o‘tkazish bilan bog‘liq yordam so‘rash. Xulq-atvor qoidalari: hech qachon qo‘ng‘iroq qilish yoki pul o‘tkazish; SMS xabarni o‘chirish; «muammo» ni hal qilish uchun uyali aloqa operatoringizga qo‘ng‘iroq qiling; Telefoningizga antivirus dasturini o‘rnating.

Keltirilgan misollar topshiriqlarning asosan vaziyatli harakterga ega bo‘lganligini, ya’ni ularda o‘quvchilar hayotda duch kelgan yoki duch kelishi mumkin bo‘lgan vaziyatlar tasvirlanganligini ko‘rsatadi. Vazifa talablari talabalarni «Kiberxavfsizlik asoslari» kursi mazmunini o‘zlashtirishning turli darajalari bilan bog‘liq tadbirlarga jalb qiladigan tarzda tuzilgan.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

Darajalar V.P.Bespalko tomonidan bilimlarning rivojlanish darajalari taksonometriyasiga muvofiq aniqlandi: bilim - ko‘rinishlar, bilim - nusxalar, bilim ko‘nikmalar, bilim - o‘zgarishlar. Shunday qilib, birinchi darajadagi murakkablikdagi vazifalar talabalardan kiber tahdidning mavjudligi va turini to‘g‘ri tan olishni talab qildi. Ikkinchi darajaning vazifalari vaziyatdan taklif qilingan chiqishlar orasidan tavsiflangan kiber tahdidga mos keladiganini tanlashdir. Uchinchi darajaning vazifalari kiber tahdidga duch kelganda standart vaziyatda o‘zlashtirilgan harakat usullarini qo‘llashdir. To‘rtinchi darajaning vazifalari - kiber tahdidga qarshi nostandart vaziyatda o‘z qaroringizni qabul qilish.

“Xavfsiz internet” sinf soatlari, kiberxavfsizlik xususiyatlarini ochib beruvchi mavzudagi eng yaxshi insholar tanlovi, bolalarning ijodiy salohiyatini ochib berish va ularning kibermakon haqidagi g‘oyalarini aks ettirish maqsadida rasmlar tanlovi, ota-onalar yig‘ilishlari “Kiberxavfsizlik” bo‘yicha tashkil etilsa maqsadga muvofiq bo‘ladi.

Xulosa

Har bir o‘quvchilar kiberxavfsizlik sohasida malakali bo‘lishi kerak. U nafaqat kibermakon tahdidlaridan xabardor bo‘lishi, balki kiberjinoyatchilarga duch kelgan vaziyatlarda ham to‘g‘ri qaror qabul qila olishi kerak.

XXI asrning birinchi o‘n yilligiga kelib axborotning ahamiyati keskin oshib ketdi. Ma’lumotning qimmatbaholigi faqat davlat sirlarini qo‘riqlash nuqtai nazaridangina emas, balki tijorat rivoji sababli ham oshib bormoqda, chunki axborotga ega bo‘lgan mamlakat jahonni boshqaradi.

Yangi innovatsion texnologiyalarni loyihalashtirish jarayoniga sarf qilinayotgan vaqt iqtisodi, telekommunikatsion tizimlar va qurilmalar bozoridagi sobitqadam sifat o‘zgarishi natijasida raqobatbardoshlik talablari oshib bormoqda. Demak, har qanday tashkilot o‘zini “chaqirilmagan” kuzatuvchilardan xalos qilishi zarur bo‘ladi. Farzandlarimizni ushbu tahdidlardan ogoh qilishimiz, har qanday firibgarlarga ishonib qolmaydigan qilib tarbiyalash zarur bo‘ladi.

ADABIYOTLAR:

1. A.Axmedov, N Tayloqov. Informatika. AL va KHK uchun darslik. - T.:O‘zbekiston-2004
2. S.G‘aniyev, A.G‘aniyev. Kiberxavfsizlik asoslari. O‘quv qo‘llanma-2010y
3. N.Tayloqov, A.Axmedov va boshqalar. Informatika. 11-sinf uchun darslik. “Extremum-press”. Toshkent - 2018

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

4. K.Polyakov Информатика. 10-11 классы. Базовый и углубленный уровни:

методические пособие. - М. Бином. Лаборатория знаний, 2016.