RAQAMLI TA'LIM MUHITLARIDA KIBERXAVFSIZLIK MASALALARI

Tursunbek Sadriddinovich Jalolov
Ilmiy rahbar Osiyo xalqaro universiteti Dotsenti p.f.f.d.(PhD)
Raximov Ravshonbek Razzakberdiyevich
Osiyo xalqaro universiteti magistri

Annotatsiya. Ushbu maqolada raqamli ta’lim muhitida yuzaga kelayotgan kiberxavfsizlik muammolari tahlil qilinadi. Internet texnologiyalarining ta’lim sohasida keng joriy etilishi, onlayn darslar, elektron jurnal va baholash tizimlari, hamda masofaviy ta’lim shakllarining ommalashuvi kiberxavfsizlik masalalarini dolzarb etmoqda. Maqolada kiberhujum turlari, ularning ta’lim tizimiga salbiy ta’siri, shuningdek, talaba va o‘qituvchilarning shaxsiy ma’lumotlarini himoya qilish zarurati haqida fikr yuritiladi. Muallif axborot xavfsizligini ta’minlash bo‘yicha zamonaviy yondashuvlar, xavfsizlik siyosatlari va profilaktika choralarini ko‘rib chiqadi

Kalit so’zlar: kiberxavfsizlik, ta'lim, Raqamli ta'lim, axborot tizimlari, masofaviy ta’lim, himoya.

Аннотация. В статье анализируются проблемы кибербезопасности, возникающие в среде цифрового обучения. Широкое внедрение интернет-технологий в образование, популярность онлайн-занятий, электронных журналов и систем оценки, дистанционных форм обучения делают вопросы кибербезопасности все более актуальными. В статье рассматриваются виды кибератак, их негативное влияние на систему образования, а также необходимость защиты персональных данных учащихся и преподавателей. Автор рассматривает современные подходы к обеспечению информационной безопасности, политику безопасности и превентивные меры.

Ключевые слова: кибербезопасность, образование, цифровое образование, информационные системы, дистанционное обучение, защита.

Abstract. This article analyzes the emerging cybersecurity problems in the digital educational environment. The widespread introduction of Internet technologies in the field of education, the popularity of online classes, electronic journals and assessment systems, as well as distance learning forms, make cybersecurity issues relevant. The article discusses the types of cyberattacks, their negative impact on the education system, as well as the need to protect the personal data of students and teachers. The author considers modern approaches to ensuring information security, security policies and preventive measures.

Keywords: cybersecurity, education, Digital education, information systems, distance learning, protection.

ISSN 3030-3907

Kirish

Raqamli texnologiyalarning jadal rivojlanishi O‘zbekistonda ta’lim sohasini, xususan, onlayn platformalar, elektron darsliklar va masofaviy ta’lim tizimlari kabi raqamli ta’lim muhitlarini o‘zlashtirish orqali sezilarli darajada o‘zgartirdi. 2020-yilda boshlangan COVID-19 pandemiyasi ushbu o‘tishning katalizatori bo‘lib, ta’lim muassasalarini an’anaviy sinf sharoitlaridan raqamli formatlarga o‘tishga majbur qildi. Ushbu siljish Prezidentning 2021-yil 6-oktabrdagi qarori bilan yanada qo‘llab-quvvatlanib, unda ta’lim tizimini raqamlashtirishga alohida e’tibor qaratilib, ta’lim olishda kirish, sifat va samaradorlikni oshirishga qaratilgan.

Raqamli ta'lim muhitlari ko'plab afzalliklarni taklif etadi, jumladan moslashuvchanlik, qulaylik va ta'lim tajribasini individual ehtiyojlarga moslashtirish qobiliyati. Masalan, onlayn ta'lim platformalari geografik to'siqlarni yo'q qilib, istalgan vaqtda va istalgan joyda ta'lim resurslariga kirishni osonlashtiradi. Bundan tashqari, elektron darsliklar o'rganish tajribasini boyitishi mumkin bo'lgan interaktiv kontentni taqdim etadi. Biroq, ta'limni jadal raqamlashtirish, ayniqsa, kiberxavfsizlik bilan bog'liq muhim muammolarni ham keltirib chiqardi.

Ta'lim muassasalari raqamli texnologiyalarga tobora ko'proq tayanar ekan, ular o'quvchilarning nozik ma'lumotlarini buzishi va ta'lim jarayonlarini buzishi mumkin bo'lgan kibertahdidlarga nisbatan zaifroq bo'lib qoladi. Ushbu kiberxavfsizlik muammolarini hal qilish O‘zbekistonda raqamli ta’lim islohotlarini muvaffaqiyatli amalga oshirish, raqamli ta’limning afzalliklari xavf-xatarlar soyasida qolmasligini ta’minlash uchun juda muhim. Xulosa qilib aytadigan bo'lsak, O'zbekistonda ta'limni raqamlashtirish o'rganishni kengaytirish uchun katta imkoniyatlar yaratsa-da, ta'lim muassasalarining yaxlitligini hamda talabalar va o'qituvchilarning ma'lumotlarini himoya qilish uchun paydo bo'layotgan kiberxavfsizlik muammolarini bir vaqtda hal qilish zarur.

Kiberxavfsizlik ta’lim jarayonida shaxsiy ma’lumotlarning himoyasi, zararli dasturlardan saqlanish va onlayn firibgarlikning oldini olishni o‘z ichiga oladi. O‘zbekistonda raqamli ta’lim muhitlarida kiberxavfsizlik bilan bog‘liq tadqiqotlar hali yetarlicha rivojlanmagan. Ushbu maqola O‘zbekistondagi raqamli ta’lim muhitlarida kiberxavfsizlik muammolarini aniqlash va ularni hal qilish yo‘llarini taklif qilishga qaratilgan.

Adabiyotlar sharxi

Raqamli ta'lim muhitlarining rivojlanishi global ta'lim sektorini sezilarli darajada o'zgartirib, moslashuvchanlik, qulaylik va shaxsiylashtirilgan o'rganish tajribasi kabi ko'plab afzalliklarni taqdim etdi. Biroq, bu raqamli siljish kiberxavfsizlik xavfini ham keltirib chiqardi, buni onlayn ta'lim platformalarida

ISSN 3030-3907

kiberhujumlarning ko'payishi tasdiqlaydi. Tadqiqotlar raqamli ta'limning afzalliklari va muammolarini ta'kidlab, xavflarni yumshatish bilan birga imkoniyatlarni maksimal darajada oshiradigan muvozanatli yondashuv zarurligini ta'kidlaydi.

Raqamli o‘quv muhiti o‘quvchilarga istalgan vaqtda va istalgan joyda ta’lim resurslaridan foydalanish imkoniyatini beradi, bu esa ta’limni yanada inklyuziv va individual ehtiyojlarga moslashtirish imkonini beradi[1]. Ta'limni boshqarish tizimlari (LMS) va Virtual ta'lim muhitlari (VLE) kabi texnologiyalar har bir talabaning o'ziga xos sur'ati va uslubiga mos ravishda o'rganish tajribasini moslashtirishga imkon beradi[2]. Raqamli ta'limda interfaol vositalar va multimedia resurslarining integratsiyasi o'quvchilarning faolligini oshiradi va yanada dinamik o'rganish tajribasini osonlashtiradi.

Raqamli ta'limning o'sishi kiberhujumlarning ko'payishi bilan birga keldi, 2020 va 2022 yillar orasida onlayn ta'lim platformalariga hujumlar 30% ga oshgan[3]. Ta'limni raqamlashtirish muhim maxfiylik muammolarini keltirib chiqaradi, chunki talabalar va o'qituvchilarning shaxsiy ma'lumotlari tobora ko'proq onlayn saqlanadi va almashiladi, bu ularni buzilishlarga qarshi himoyasiz qiladi. Raqamli muhit, shuningdek, noto'g'ri ma'lumotlarning tarqalishiga va chalg'itishning kuchayishiga olib kelishi mumkin, bu esa o'quv jarayoniga salbiy ta'sir ko'rsatishi mumkin.

O'qituvchilar uchun doimiy kasbiy rivojlanish ularni raqamli ta'lim muhitida samarali harakat qilish va himoya qilish uchun zarur bo'lgan ko'nikmalar bilan jihozlash uchun juda muhimdir. Kiberxavfsizlikning kuchli protokollarini joriy etish va ularni muntazam yangilab turish ta’lim platformalarini potentsial tahdidlardan himoya qilishga yordam beradi[4]. Ham o'qituvchilar, ham talabalar texnologiyadan xavfsiz va samarali foydalanishlarini ta'minlash uchun raqamli kompetensiyalarni rivojlantirishga rag'batlantirilishi kerak.

Raqamli ta'lim muhitlari katta foyda keltirsa-da, ular xavfsiz va samarali ta'lim tajribasini ta'minlash uchun hal qilinishi kerak bo'lgan muammolarni ham taqdim etadi. Tadqiqotlar shuni ko'rsatadiki, raqamli ta'lim bilan bog'liq kiberxavfsizlik xatarlarini yumshatish uchun uzluksiz trening, mustahkam xavfsizlik choralari va raqamli vakolatlarni rivojlantirishni o'z ichiga olgan kompleks yondashuv muhim ahamiyatga ega. Bundan tashqari, barcha manfaatdor tomonlar o'rtasida raqamli savodxonlik va xabardorlik madaniyatini oshirish raqamli ta'lim muhitlarining potentsial tahdidlarga chidamliligini yanada oshirishi mumkin.

Ta'lim muhitida kiberxavfsizlikni ta'minlash ko'p qirrali muammo bo'lib, u ham texnik choralarni, ham foydalanuvchilarning xabardorligini oshirishni talab qiladi. Shaxsiy ma'lumotlarni himoya qilish, zararli dasturlardan himoya qilish va

ISSN 3030-3907

tizimlarning barqaror ishlashi ta'limda kiberxavfsizlikning muhim tarkibiy qismlari hisoblanadi. Biroq, Tadqiqotchilar ta'kidlaganidek, agar talabalar va o'qituvchilarda kiberxavfsizlik bo'yicha tegishli bilimlar bo'lmasa, bu chora-tadbirlarning samaradorligi sezilarli darajada pasayadi. Bu, ayniqsa, foydalanuvchilarning kiberxavfsizlikdan xabardorlik darajasi yetarlicha o‘rganilmagan O‘zbekiston kabi sharoitlarda dolzarbdir. Keyingi bo'limlar ta'limda kiberxavfsizlikning asosiy jihatlarini o'rganib, foydalanuvchilarni o'qitish va xabardorligini oshirish muhimligini ta'kidlaydi.

Kiberxavfsizlik bo'yicha ta'lim juda muhim, chunki inson xatosi xavfsizlik hodisalarining 95 foizini tashkil qiladi, bu ijtimoiy muhandislik hujumlari va beparvolikning oldini olish uchun xabardorlik zarurligini ta'kidlaydi[5]. Ta'lim muassasalari zaifliklarni kamaytirish va xavfsizroq onlayn muhitni yaratish uchun o'qituvchilar, xodimlar va talabalarni tegishli onlayn xatti-harakatlarga o'rgatishlari kerak. Talabalarni raqamli dunyoga tayyorlash va ularni kiber tahdidlardan himoya qilish uchun kiberxavfsizlik bo'yicha ta'lim o'quv dasturlariga kiritilishi kerak[6].

Maktablar o'zlarining nozik ma'lumotlari va yangi zaifliklarni keltirib chiqaradigan IoT qurilmalari kabi raqamli texnologiyalardan keng foydalanishlari tufayli kiberhujumlar uchun jozibador maqsadlardir[7]. Raqamli texnologiyalarning ta'limga tez tatbiq etilishi foydali bo'lishiga qaramay, kiberxavfsizlik xavfini oshiradi[8]. Kiberxavfsizlikning ahamiyatiga qaramay, ta'lim muassasalari samarali kiberxavfsizlik amaliyotlarini joriy etishda ko'pincha boshqa tarmoqlardan orqada qoladilar.

Kiberxavfsizlik bo'yicha keng qamrovli siyosatlarni amalga oshirish, dasturiy ta'minotni muntazam yangilash va tajovuzlarni aniqlash tizimlari ta'lim muhitini himoya qilish uchun zarurdir. Xavflarni tahlil qilish, kirish testlari va xavfsizlik auditini o'tkazish zaifliklarni aniqlashga va kiberxavfsizlik himoyasi samaradorligini ta'minlashga yordam beradi. Tarkibiy ta'lim dasturlari va kampaniyalari orqali foydalanuvchilarning xabardorligini oshirish kiber tahdidlarni yumshatish uchun juda muhimdir[9].

Foydalanuvchilarning xabardorligi kiberhujumlarga qarshi kurashda muhim komponent hisoblanadi, chunki xabardor foydalanuvchilarsiz texnik choralarning o‘zi yetarli emas. Xabardorlik dasturlari foydalanuvchilarni kiberxavfsizlik tahdidlari va xavfsiz amaliyotlar haqida samarali o'rgatish uchun yaxshi rejalashtirilgan va tuzilgan bo'lishi kerak. Yoshlarni kiberjinoyatlardan himoya qilish va raqamli dunyoda xavfsiz harakat qilishlarini ta’minlash uchun yoshlarni xavfsiz internet amaliyotiga o‘rgatish muhim.

Texnik choralar kiberxavfsizlik uchun ajralmas bo'lsa-da, inson omili muhim zaiflik bo'lib qolmoqda. Talabalar va o'qituvchilar orasida kiberxavfsizlik bo'yicha

ISSN 3030-3907

xabardorlikning yo'qligi hatto eng ilg'or xavfsizlik tizimlarini ham buzishi mumkin. Shu sababli, ta'lim muassasalari xavfsiz raqamli ta'lim muhitini yaratish uchun kiberxavfsizlik bo'yicha ta'lim va xabardorlikni birinchi o'ringa qo'yishlari kerak. Ushbu yondashuv nafaqat shaxsiy ma'lumotlar va tizimlarni himoya qiladi, balki foydalanuvchilarga kiber tahdidlarga qarshi birinchi himoya chizig'i sifatida harakat qilish imkoniyatini beradi.

O‘zbekistonda raqamli ta’limning rivojlanishi “Raqamli O‘zbekiston 2030” strategiyasi va Prezidentning 2021-yil 6-oktyabrdagi “Ta’lim tizimini raqamlashtirish to‘g‘risida”gi qarori kabi siyosiy tashabbuslar bilan qo‘llab-quvvatlanmoqda[10]. Ushbu hujjatlar ta’limda raqamli texnologiyalarni joriy etishga qaratilgan bo‘lsa-da, kiberxavfsizlik masalalari yetarlicha batafsil ko‘rib chiqilmagan. Mahalliy adabiyotlarda raqamli ta’limning infratuzilmasi va pedagogik jihatlari haqida bir qator tadqiqotlar mavjud bo‘lsa-da, kiberxavfsizlikka oid maxsus ishlanmalar deyarli yo‘q. Bu esa ushbu sohada katta tadqiqot bo‘shlig‘ini ko‘rsatadi.

Xalqaro tajribada kiberxavfsizlik muammolari va ularni hal qilish yo‘llari bo‘yicha bir qator yondashuvlar taklif qilingan. Masalan, Evropada raqamli ta’lim platformalarida ma’lumotlarni shifrlash va ikki faktorli autentifikatsiya tizimlari keng qo‘llanilmoqda. Shu bilan birga, Osiyo mamlakatlarida, xususan, Janubiy Koreyada o‘quvchilar va o‘qituvchilar uchun kiberxavfsizlik bo‘yicha majburiy treninglar tashkil etilishi ijobiy natijalar bergan. O‘zbekistonda esa bunday amaliyotlar hali joriy etilmagan, bu esa mahalliy ta’lim tizimining kiberxavfsizlikka tayyor emasligini ko‘rsatadi.

Adabiyotlar sharxi shuni ko‘rsatadiki, raqamli ta’lim muhitlarida kiberxavfsizlik global miqyosda dolzarb muammo bo‘lib, O‘zbekistonda bu masalaga yetarlicha e’tibor berilmagan. Mavjud tadqiqotlar asosan texnik infratuzilma yoki ta’lim sifatiga qaratilgan bo‘lib, kiberxavfsizlikning inson omili (xabaradorlik, tajriba) va mahalliy xususiyatlari chuqur o‘rganilmagan. Shu sababli, ushbu maqola O‘zbekistonning raqamli ta’lim muhitlarida kiberxavfsizlik muammolarini aniqlash va mahalliy sharoitga mos yechimlar taklif qilishga qaratilgan.

Metodologiya va natijalar

Ushbu tadqiqotda O'zbekistondagi raqamli ta'lim muhitlarida kiberxavfsizlik holatini o'rganish uchun kompleks yondashuv qo'llanildi. Tadqiqot 2024-yilning yanvar-may oylari davomida o'tkazilgan bo'lib, asosan ".uz" domen zonasidagi veb-saytlarga qaratilgan kiberhujumlar statistik tahlili amalga oshirildi.
Tadqiqot metodologiyasi quyidagi yo'nalishlarda olib borildi:

ISSN 3030-3907

Veb-saytlarga qaratilgan kiberhujumlar monitoringi: Milliy domen zonasidagi veb-saytlarga qaratilgan kiberhujumlar soni, turi va ta'siri o'rganildi.

Zaifliklar tahlili: Davlat organlari va ta'lim muassasalariga tegishli veb-saytlardagi mavjud xavfsizlik zaifliklari aniqlandi va tasniflanadi.

Kibertahdidlar monitoringi: Davlat organlari va boshqa tashkilotlarning axborot tizimlarida mavjud bo'lgan kibertahdidlar aniqlandi va tahlil qilindi.

Tadqiqot natijalarini tahlil qilish uchun statistik ma'lumotlarni vizualizatsiya usullaridan foydalanildi hamda aniqlangan zaifliklar va kibertahdidlar tipologiyasi ishlab chiqildi.

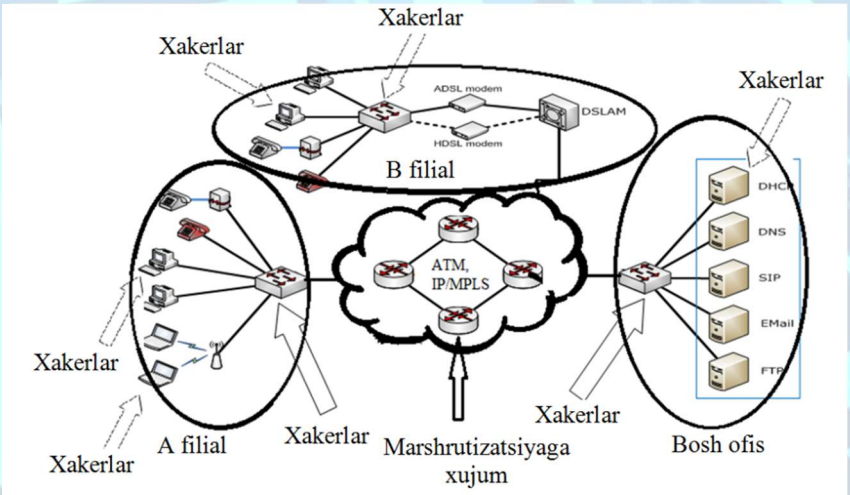
Tadqiqot natijalariga ko'ra, 2024-yilning yanvar-may oylari davomida ".uz" domen zonasidagi veb-saytlarga jami 6,615,900 ta kiberhujum amalga oshirilganligi aniqlandi. Bu raqam O'zbekistondagi raqamli muhitlarga bo'lgan kibertahdidlar miqyosining jiddiyligini ko'rsatadi.

Tadqiqot davomida quyidagi muhim natijalar olindi:

1. **Xavfsizlik talablariga rioya etilmagan veb-saytlar**: Milliy domen zonasidagi 74 ta veb-saytda kiberxavfsizlik talablari buzilganligi aniqlandi. Ayniqsa, ushbu veb-saytlarning 26 tasi (35%) davlat organlariga tegishli ekanligi alohida tashvish uyg'otadi. Bu davlat organlarining ham kiberxavfsizlik masalalariga yetarlicha e'tibor bermasligini ko'rsatadi.

2. **Aniqlangan va tuzatilgan zaifliklar**: Tashkilot va davlat idoralarining 60 ta veb-saytida 183 ta zaiflik aniqlandi va tuzatildi. Bu natija proaktiv kiberxavfsizlik tadbirlari samaradorligini ko'rsatadi.

3. **Kibertahdidlar soni**: Monitoring davomida davlat organlari va boshqa tashkilotlarning axborot tizimlarida 478,132 ta kibertahdid aniqlandi. Bu juda katta raqam bo'lib, kiberhujumlar intensivligini ko'rsatadi.



1-rasm. KT arxitekturasi va mumkin bo‘lgan hujumlar yo‘nalishlari

Birinchi rasm O'zbekistonda raqamli muhitlarga qaratilgan kiberhujumlar dinamikasini ko'rsatadi. Grafik ma'lumotlarga ko'ra, kiberhujumlar soni vaqt o'tishi

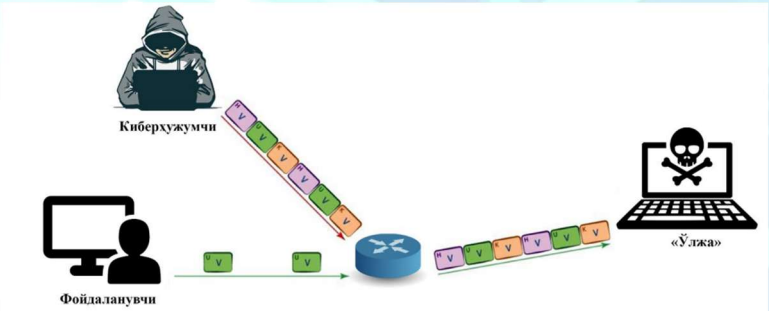
ISSN 3030-3907

bilan oshib bormoqda. Bu tendensiya raqamli ta'lim muhitlari ham borgan sari kibertahdidlarga duch kelishi mumkinligini ko'rsatadi.

Rasmda kiberhujumlarning asosiy turlari ham ko'rsatilgan bo'lib, eng keng tarqalgan hujumlar:

- Xizmatni rad etish hujumlari (DDoS)
- Ma'lumotlar bazalariga noqonuniy kirish urinishlari (SQL Injection)
- Foydalanuvchi autentifikatsiyasini chetlab o'tish urinishlari
- Veb-saytlarni yopish yoki buzish uchun bo'lgan urinishlar

Bu ma'lumotlar O'zbekistondagi raqamli ta'lim platformalari ham shunga o'xshash tahdidlarga duch kelishi mumkinligini ko'rsatadi.



2-расм. IP-spoofing ҳужумини амалга ошириш жараёни

Ikkinchi rasm (media/image2.png) kiberhujumlarga qarshi ko'rilgan choralar samaradorligini ko'rsatadi. Grafikka ko'ra, aniqlangan zaifliklarning katta qismi tuzatilgan bo'lsa-da, ba'zi zaifliklar hali ham mavjud. Bu holatning davom etishi, ayniqsa ta'lim muhitlarida, ma'lumotlar xavfsizligi uchun xavf tug'diradi.

Rasmda davlat organlari va ta'lim muassasalarida aniqlangan zaifliklar turlari ham ko'rsatilgan:

- Parollar bilan bog'liq zaifliklar
- So'nggi versiyaga yangilanmagan tizimlar
- Shifrlash mexanizmlarining yetarli emasligi
- Xavfsizlik siyosatlarining to'liq ishlab chiqilmaganligi

Tadqiqot natijalari O'zbekistondagi raqamli ta'lim muhitlarida kiberxavfsizlik bo'yicha kompleks choralar ko'rish zarurligini ko'rsatadi. Bunda nafaqat texnik choralar, balki foydalanuvchilar xabardorligini oshirish, xavfsizlik siyosatlarini takomillashtirish va muntazam monitoring o'tkazish muhim ahamiyatga ega.

Xulosa

Tadqiqot natijalariga asoslanib, O'zbekistondagi raqamli ta'lim muhitlarida kiberxavfsizlik masalalari bo'yicha quyidagi xulosalarga kelindi:

Birinchidan, 2024-yilning yanvar-may oylari davomida ".uz" domen zonasidagi veb-saytlarga 6,615,900 ta kiberhujum amalga oshirilganligi,

ISSN 3030-3907

shuningdek, 74 ta veb-saytda kiberxavfsizlik talablari buzilganligi (ularning 26 tasi davlat organlariga tegishli ekanligi) kiberxavfsizlik masalalarining O'zbekistonda juda dolzarb ekanligini ko'rsatadi. Bu raqamli ta'lim muhitlari ham potentsial xavf ostida ekanligini anglatadi.

Ikkinchidan, tadqiqot davomida tashkilot va davlat idoralarining 60 ta veb-saytida 183 ta zaiflik aniqlandi va tuzatildi. Bu raqamli ta'lim platformalarida kiberxavfsizlik instrumentlarini joriy etish va muntazam monitoringni amalga oshirish zarurligini ko'rsatadi. Ayniqsa, parollar bilan bog'liq zaifliklar, so'nggi versiyaga yangilanmagan tizimlar, shifrlash mexanizmlarining yetarli emasligi va xavfsizlik siyosatlarining to'liq ishlab chiqilmaganligi kabi muammolar keng tarqalgani aniqlandi.

Uchinchidan, davlat organlari va boshqa tashkilotlarning axborot tizimlarida 478,132 ta kibertahdid aniqlangani raqamli ta'lim muhitlarida ham kiberxavfsizlik choralarini kuchaytirish zarurligini ko'rsatadi. Bu tadqiqot natijalariga ko'ra, kiberhujumlarning eng keng tarqalgan turlari – xizmatni rad etish hujumlari (DDoS), ma'lumotlar bazalariga noqonuniy kirish urinishlari (SQL Injection), foydalanuvchi autentifikatsiyasini chetlab o'tish urinishlari hamda veb-saytlarni yopish yoki buzish uchun bo'lgan urinishlardir.

To'rtinchidan, tadqiqot natijalari kiberxavfsizlik bo'yicha texnik choralar bilan bir qatorda foydalanuvchilar xabardorligini oshirish zarurligini ko'rsatdi. Chunki, adabiyotlar tahlilida ko'ringanidek, inson xatosi xavfsizlik hodisalarining 95 foizini tashkil qiladi. Shu sababli, O'zbekistonda raqamli ta'lim muhitlarining kiberhimoyasini kuchaytirish uchun talabalar, o'qituvchilar va ta'lim tizimi xodimlari uchun kiberxavfsizlik bo'yicha treninglar tashkil etish zarur.

Beshinchidan, raqamli ta'lim muhitlarida kiberxavfsizlikni ta'minlashning samarali modeli texnik, tashkiliy va ta'limiy komponentlarni o'z ichiga olishi kerak. Texnik komponent sifatida zamonaviy antivirus dasturlari, firewall tizimlari, ma'lumotlarni shifrlash va foydalanuvchilarni autentifikatsiyalash mexanizmlari joriy etilishi lozim. Tashkiliy komponent sifatida kiberxavfsizlik siyosatlari va reglamentlari ishlab chiqilishi, muntazam monitoring o'tkazilishi zarur. Ta'limiy komponent sifatida esa barcha manfaatdor tomonlar uchun kiberxavfsizlik bo'yicha o'quv dasturlari, treninglar va xabardorlikni oshirish kampaniyalari tashkil etilishi muhim.

Yakuniy xulosada aytish mumkinki, O'zbekistonda raqamli ta'lim muhitlarining kiberxavfsizligini ta'minlash bo'yicha kompleks yondashuv zarur. Bu yondashuv texnik infratuzilmani mustahkamlash, ma'lumotlarni himoya qilish mexanizmlarini takomillashtirish, foydalanuvchilar xabardorligini oshirish va milliy kiberxavfsizlik standartlarini ishlab chiqishni o'z ichiga olishi lozim. Bunday

ISSN 3030-3907

yondashuv orqali raqamli ta'lim muhitlarining barqaror va xavfsiz ishlashini ta'minlash mumkin, bu esa o'z navbatida ta'lim sifatini oshiradi va raqamli ta'limning afzalliklaridan to'liq foydalanish imkoniyatini yaratadi.

FOYDALANILGAN ADABIYOTLAR.

1. Kasymaliev, M., Ashymbaeva, T., Kozhobekov, K., & Erdolatov, S. (2023). Advantages of using digital technologies in the educational process. *Alatoo Academic Studies*. https://doi.org/10.17015/aas.2023.232.09
2. Yadav, N. (2024). *The Impact of Digital Learning on Education*. https://doi.org/10.61778/ijmrast.v2i1.34
3. Côgo, C. E., Louzada Supeletto, E. F., Mariani, J. V., Andrade, M. G. de A., Carlette, M. L. M., da Silva, M. C. D., Lopes, S. C., & Vargas, V. L. F. (2024). Ambiente digital e educação: benefícios e riscos no modelo educacional contemporâneo. *Revista Ibero-Americana de Humanidades, Ciências e Educação*. https://doi.org/10.51891/rease.v10i10.16395
4. Lolić, T., Stefanović, D., Dionísio, R., Dakić, D., & Havzi, S. (2022). *Learning Environment Digital Transformation: Systematic Literature Review* (pp. 87–94). Springer International Publishing. https://doi.org/10.1007/978-3-030-97947-8_12
5. Bulai, R., Turcanu, D. S., & Ciorbă, D. (2022). Education in Cybersecurity. *Central and Eastern European eDem and eGov Days*, *335*, 33–44. https://doi.org/10.24989/ocg.v335.2
6. Khalidov, A. A. (2024). Cybersecurity in educational environment: training and practice. *Èkonomika i Upravlenie: Problemy, Rešeniâ*, *8/3*(147), 127–134. https://doi.org/10.36871/ek.up.p.r.2024.08.03.015
7. Coleman, C. D., & Reeder, E. (2018). *Three Reasons for Improving Cybersecurity Instruction and Practice in Schools*. 1020–1025. https://www.learntechlib.org/p/182648/
8. Rajakumari, R. F., & Ramkumar, M. S. (2024). *Essentials of Cybersecurity Education to Mitigate Industrial Sector Challenges*. 289–302. https://doi.org/10.1201/9781032711300-20
9. Sharif, A. M., & Al-Ammary, J. (2025). Development of Cyber Security Awareness and Education Framework. *International Journal of Computing and Digital Systems*, *17*(1), 1–13. https://doi.org/10.12785/ijcds/1571048308
10. O‘zbekiston Respublikasi Prezidentining “Ta’lim tizimini raqamlashtirish to‘g‘risida”gi qarori, 2021-yil 6-oktyabr

ISSN 3030-3907