# INKLYUZIV TA’LIM MUHITIDA AXBOROT XAVFSIZLIGI FANINI O‘QITISH: TIZIMLI ADABIYOTLAR TAHLILI

# ОБУЧЕНИЕ ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» В УСЛОВИЯХ ИНКЛЮЗИВНОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ: СИСТЕМАТИЧЕСКИЙ ОБЗОР ЛИТЕРАТУРЫ

# TEACHING INFORMATION SECURITY IN AN INCLUSIVE EDUCATIONAL ENVIRONMENT: A SYSTEMATIC LITERATURE REVIEW

**G.O.UBAYDULLAYEVA1**
**Tayanch doktorant, Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti**

**Annotatsiya.** Mazkur maqolada raqamli texnologiyalar davrida maktabgacha va maktab yoshidagi bolalarda axborot xavfsizligi ko‘nikmalarini shakllantirish masalasi, xususan, alohida ta’lim ehtiyojiga ega o‘quvchilarning bu jarayondan chetda qolayotgani PRISMA metodologiyasi asosida 2013–2025-yillardagi ilmiy manbalar tahlili orqali yoritilgan. Tadqiqotda inklyuziv muhit uchun maxsus o‘quv materiallari va o‘qituvchilarni tayyorlash dasturlari yetishmasligi aniqlangan. Shuningdek, ta’limning universal dizayni (UDL), assistiv texnologiyalar va o‘yinlashtirilgan usullardan foydalanish yo‘llari ko‘rsatilib, O‘zbekiston sharoiti uchun amaliy tavsiyalar ishlab chiqilgan.

**Kalit so‘zlar:** inklyuziv ta’lim, axborot xavfsizligi, alohida ta’lim ehtiyoji, ta’limning universal dizayni (udl), raqamli fuqarolik, tizimli adabiyotlar tahlili, k-12 ta’limi.

**АННОТАЦИЯ.** В данной статье на основе методологии PRISMA проведен систематический анализ научных источников за 2013–2025 годы, посвященный формированию навыков информационной безопасности у детей, с акцентом на учащихся с особыми образовательными потребностями. Исследование показало дефицит адаптированных материалов и программ подготовки учителей для таких детей. Обосновано применение универсального дизайна обучения (UDL), ассистивных технологий и игровых методов, а также разработаны практические рекомендации для условий Узбекистана.

**Ключевые слова:** Инклюзивное образование, информационная безопасность, особые образовательные потребности, универсальный дизайн образования (UDL), цифровое гражданство, системный анализ литературы, образование K-12.

**ABSTRACT.** This article provides a systematic analysis of scientific sources from 2013 to 2025 using the PRISMA methodology, addressing information security education for children with a focus on students with special educational needs. The study reveals a significant shortage of adapted educational materials and teacher training programs for inclusive environments. It highlights the potential of Universal Design for Learning (UDL), assistive technologies, and gamified methods, and proposes practical recommendations for the context of Uzbekistan.

**Keywords:** Inclusive education, information security, special educational needs, universal design of education (UDL), digital citizenship, systematic literature analysis, K-12 education.

Lorem Ipsum Kirish. So‘nggi o‘n yillikda bolalar va o‘smirlarning raqamli qurilmalardan foydalanish yoshi muttasil pasayib bormoqda. Smartfon, planshet va onlayn ta’lim platformalari nafaqat o‘qitishning, balki ijtimoiylashuvning ham asosiy vositasiga aylandi. Ushbu jarayon bir qator yangi tahdidlarni - parollarning zaifligi, shaxsiy ma’lumotlarning oshkor bo‘lishi, kiberbulling, fishing hujumlari va ijtimoiy injiniring kabi xavflarni keltirib chiqaradi. Natijada dunyoning ko‘plab davlatlarida umumta’lim bosqichida axborot xavfsizligi asoslarini o‘qitish zarurati tobora ortib bormoqda.

Shu bilan birga, Birlashgan Millatlar Tashkilotining Nogironligi bo‘lgan shaxslar huquqlari to‘g‘risidagi Konvensiyasi (UNCRPD) va YUNESKOning inklyuziv ta’lim tamoyillari har bir bolaning, jumladan nogironligi yoki maxsus ta’lim ehtiyoji bo‘lgan bolalarning, sifatli va teng ta’lim olish huquqinikafolatlaydi.Raqamlita’limmuhitida bu tamoyil ikki tomonlama ahamiyat kasb etadi: bir tomondan, alohida ta’lim ehtiyoji bor o‘quvchilar texnologiyalar yordamida ta’limga kengroq kirish imkoniyatiga ega bo‘ladilar, ikkinchi tomondan, ular xuddi shu texnologiyalar orqali kiberxavflarga ham nisbatan ko‘proq moyil bo‘lib qolishadi. Negaki, ko‘pgina raqamli platformalar va o‘quv materiallari ularning idrok etish, sensor yoki kommunikativ xususiyatlarini hisobga olmagan holda ishlab chiqiladi.

Xalqaro tadqiqotlar shuni ko‘rsatadiki, nogironligi bo‘lgan o‘quvchilar onlayn muhitda ko‘proq zaiflikka duch keladi. Raqamli qurilmalarga ega bo‘lishdagi cheklangan imkoniyat, moslashtirilgan interfeyslarning yetishmasligi va maxfiylik tamoyillarini tushunishdagi qiyinchiliklar bunga sabab bo‘ladi. Shu bilan birga, axborot xavfsizligi ta’limi bo‘yicha mavjud dasturlarning aksariyati tipik rivojlanayotgan o‘quvchiga mo‘ljallangan bo‘lib, alohida ta’lim ehtiyojlarini hisobga olmaydi. Bu holat pedagogika fani oldida yangi, ammo hali yetarlicha tadqiq etilmagan muammoni - inklyuziv ta’lim muhitida axborot xavfsizligini o‘qitish muammosini keltirib chiqaradi.

Ushbu maqolaning maqsadi jahon ilmiy adabiyotlarini tizimli tahlil qilish orqali inklyuziv ta’lim sharoitida axborot xavfsizligi fanini o‘qitishga oid mavjud yondashuvlarni, ulardagi terminologik va metodik muammolarni, shuningdek maxsus ehtiyojli o‘quvchilarni o‘qitishda uchraydigan asosiy to‘siqlarni aniqlashdan iborat. Tadqiqot quyidagi ilmiy savolga javob berishga qaratilgan: “Inklyuziv ta’lim sharoitida turli ta’lim ehtiyojiga ega o‘quvchilarga axborot xavfsizligi bilim va ko‘nikmalarini shakllantirishda qanday mavzular, kompetensiyalar, metodik yondashuvlar va to‘siqlar ilmiy adabiyotlarda aks etgan?”

Butun jahon sog‘liqni saqlash tashkiloti ma’lumotlariga ko‘ra, dunyo aholisining taxminan15foiziuyokibuturdaginogironlikka ega bo‘lib, bu ko‘rsatkich bolalar orasida ham sezilarli ulushni tashkil etadi. Shu bilan birga, YUNESKOning «Barcha uchun ta’lim» (Education for All) konsepsiyasi va Barqaror rivojlanish maqsadlarining 4-bandi sog‘lig‘i, ijtimoiy holati yoki qobiliyatidan qat’i nazar, har bir bolaning zamonaviy raqamli ko‘nikmalarni, jumladan axborot xavfsizligi asoslarini egallashini, sifatli ta’limni talab qiladi. Ammo amaliyotda kiberxavfsizlik ta’limi ko‘pincha «neytral» yoki «universal» deb hisoblanadi, holbuki uning mazmuni va uslubi aslida faqat tipik rivojlanayotgan o‘quvchi ehtiyojlariga mo‘ljallab ishlab chiqiladi. Natijada, aynan himoyaga eng ko‘p muhtoj bo‘lgan toifa alohida ta’lim ehtiyojli o‘quvchilar kiberxavfsizlik bo‘yicha eng kambilimga ega bo‘lgan toifaga aylanib qolmoqda. Bu qarama-qarshilik «raqamli inklyuziya paradoksi» deb ta’riflanishi mumkin: texnologiyalar bir tomondan maxsus ehtiyojli o‘quvchilarga ta’lim va

muloqot imkoniyatlarini kengaytiradi, ikkinchi tomondan esa ularni yangi, o‘zlari uchun tushunarli bo‘lmagan xavflar oldida himoyasiz qoldiradi.

O‘zbekistonda so‘nggi yillarda inklyuziv ta’limni rivojlantirishga qaratilgan bir qator me’yoriy-huquqiy hujjatlar qabul qilindi, jumladan «Nogironligi bo‘lgan shaxslarning huquqlari va ularni ijtimoiy himoya qilish to‘g‘risida»gi O‘RQ-641-son Qonun [1] hamda umumta’lim maktablarida inklyuziv sinflarni tashkil etish bo‘yicha davlat dasturlari. Shu bilan bir qatorda, «Raqamli O‘zbekiston - 2030» strategiyasi doirasida axborot xavfsizligi savodxonligini oshirish umummilliy vazifa sifatida belgilangan.[2] Biroq bu ikki yo‘nalish - inklyuziv ta’lim va raqamli axborot xavfsizligi savodxonligi hozircha bir-biridan alohida rivojlanmoqda, ular kesishmasida maxsus ilmiy-metodik ishlanmalar deyarli mavjud emas. Aynan shu bo‘shliq ushbu tadqiqotning dolzarbligini belgilaydi.

Metodologiya . Tadqiqot Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA, 2020 versiyasi) uslubi asosida olib borildi [3]. PRISMA-tizimli adabiyotlar tahlilini o‘tkazish, tanlash, baholash va sintez qilishning xalqaro tan olingan yo‘riqnomasi bo‘lib, mazkur tadqiqot uch bosqichda amalga oshirildi: 1) manbalarni izlash va tanlash; 2) ularni baholash; 3) natijalarni sintez qilish. Ilmiy adabiyotlarni izlash uchun Scopus, Web of Science, ERIC va Google Scholar ma’lumotlar bazalaridan foydalanildi. Qidiruv 2013–2025-yillarni qamrab oldi. Qidiruv so‘zlari ikki asosiy semantik guruhga bo‘lindi: (a) axborot xavfsizligi/kiberxavfsizlik ta’limiga oid atamalar va (b) inklyuziv ta’lim/maxsus ehtiyojga oid atamalar. Ushbu ikki guruh mantiqiy AND operatori orqali bog‘landi. (1-jadval)

1-jadval

| Qidiruv guruhi | Kalit so‘zlar | Izoh |
|---|---|---|
| Kiberxavfsizlik guruhi | “cybersecurity” OR “cyber security” OR “information security” OR “cyber safety” OR “digital safety” | Xalqaro adabiyotda uchraydigan turli yozilish shakllari va sinonimlarni qamrab olish uchun kiritildi |
| Ta’lim bosqichi guruhi | “K-12” OR “primary school” OR “elementary school” OR “secondary school” OR “school-aged” | Tadqiqotni maktabgacha va umumta’lim bosqichi bilan cheklash uchun |
| Inklyuzivlik guruhi | “inclusive education” OR “students with disabilities” OR “special educational needs” OR “SEN” OR “neurodiverse” OR “accessibility” | Nogironligi yoki maxsus ta’lim ehtiyoji bo‘lgan o‘quvchilarga oid tadqiqotlarni aniqlash uchun |
| Metodik guruh | “curriculum” OR “pedagogy” OR “teaching method” OR “universal design for learning” | O‘qitish metodikasiga oid manbalarni ajratish uchun |

Dastlabki qidiruv natijasida jami 214 ta manba aniqlandi (Scopus — 96, Web of Science — 58, ERIC — 31, Google Scholar orqali qo‘shimcha grey literature — 29). Dublikatlar olib tashlangandan so‘ng 168 ta manba sarlavha va annotatsiya bo‘yicha ko‘rib chiqildi. Ushbu bosqichda 121 ta manba mavzuga mos kelmaganligi sababli chiqarib tashlandi. Bunda asosan, faqat kattalar auditoriyasiga yoki sof texnik masalalarga bag‘ishlangan ishlar olib tashlandi. Qolgan 47 ta manbaning to‘liq matni tahlil qilindi, ulardan 5 tasiga kirish imkoni bo‘lmadi. Yakuniy tahlilga 31 ta manba kiritildi. (2-jadval)

2-jadval

| Bosqich | Jarayon | Manbalar soni |
|---|---|---|
| Identifikatsiya | Ma'lumotlar bazalaridan (Scopus, Web of Science, ERIC) va boshqa manbalardan (Google Scholar, veb -qidiruv) topilgan yozuvlar | 214 |
| Dublikatlarni chiqarish | Bir xil manbalarning takroriy nusxalari olib tashlandi | 168 |
| Skrining (sarlavha/annotatsiya) | Kiritish/chiqarish mezonlariga mos kelmagan manbalar chiqarib tashlandi | 47 |
| Muvofiqlik (t o'liq matn) | To'liq matn asosida chuqur tahlil qilindi; 5 tasiga kirish imkoni bo'lmadi | 42 |
| Yakuniy tanlov | Sifat mezonlariga t o'liq javob bergan, sintezga kiritilgan manbalar | 31 |

Muhim metodologik topilma shundaki, axborot xavfsizligi va inklyuziv ta'limning kesishmasiga bevosita bag'ishlangan tadqiqotlar soni juda cheklangan bo'lib chiqdi — bu, o'z navbatida, ushbu sohaning hali shakllanish bosqichida ekanligidan dalolat beradi. Bu holat F.Hellems va S.Bhatia tomonidan ham alohida qayd etilgan. [4] Shu sababli tahlilga, bevosita mos manbalar yetishmagan joylarda, tutash sohalar-inklyuziv raqamli ta'lim, o'quvchilarga mo'ljallangan yordamchi texnologiyalar va umumiy K-12 kiberxavfsizlik ta'limi bo'yicha adabiyotlar ham jalb qilindi va ular alohida ajratib ko'rsatildi. Tahlilga kiritilgan 31 ta manbaning geografik taqsimoti xilma-xil bo'lib, ular AQSh (9 ta), Ispaniya (4 ta), Saudiya Arabistoni (3 ta), Buyuk Britaniya (3 ta), Avstraliya (2 ta) hamda Kanada, Indoneziya, Janubiy Koreya kabi davlatlarda o'tkazilgan tadqiqotlarni o'z ichiga oladi. Nashr turlari bo'yicha 14 tasi jurnal maqolasi, 11 tasi konferensiya materiali, 6 tasi hisobot yoki siyosat hujjati sifatida tasniflandi. Diqqatga sazovor jihati shundaki, tahlil qilingan manbalarning katta qismi oliy ta'lim bosqichiga qaratilgan bo'lib, bevosita umumta'lim bosqichiga bag'ishlangan tadqiqotlar nisbatan kam (atigi 9 ta) sonini tashkil etdi — bu esa maktab yoshidagi alohida ehtiyojli o'quvchilar bo'yicha tadqiqotlarning yetishmasligini yana bir bor tasdiqlaydi. Tahlil davomida adabiyotlarda takrorlanuvchi bir necha mavzu yo'nalishi aniqlandi. Ular quyidagi 3-jadvalda umumlashtirilgan:

3-jadval

| Mavzu | Tavsifi | Adabiyotdagi ulushi |
|---|---|---|
| Raqamli fuqarolik va xavfsiz xulq-atvor | Onlayn muhitda mas'uliyatli va xavfsiz harakat qilish, axloqiy me'yorlar | 24% |
| Maxfiylik va shaxsiy ma'lumotlar himoyasi | Shaxsiy ma'lumotlarni oshkor qilmaslik, ma'lumotlarni kuzatuv (data surveillance) dan himoya qilish | 21% |
| Parol va autentifikatsiya xavfsizligi | Kuchli parol yaratish, ikki bosqichli tasdiqlash tushunchalari | 13% |
| Kiberbulling va onlayn tazyiq | Texnologik vositalar orqali amalga oshiriladigan tajovuzkorlik | 12% |
| Ijtimoiy tarmoqlar va fishing xavfsizligi | Ijtimoiy injiniring, firibgarlik xabarlarni aniqlash | 15% |
| Sun'iy intellekt va ma'lumotlar xavfsizligi | AI asosidagi tizimlarda maxfiylik va adolat masalalari | 9% |
| Yordamchi texnologiyalar xavfsizligi | Nutq-matn, ko'z harakati, imo-ishora asosidagi interfeyslarning maxfiylik xavflari | 6% |

Ko‘rinib turibdiki, «raqamli fuqarolik» va «maxfiylik» eng ko‘p qamrab olingan mavzular hisoblanadi, bu esa A. Ibrahim va hammualliflarining umumiy K-12 kiberxavfsizlik tadqiqotlaridagi natijalarga o‘xshash tendensiyani tasdiqlaydi [5]. Shu bilan birga, «yordamchi texnologiyalar xavfsizligi» kabi maxsus ehtiyojli o‘quvchilarga xos mavzular adabiyotlarda eng kam yoritilgan yo‘nalish bo‘lib qolmoqda — bu esa muhim amaliy bo‘shliqni ko‘rsatadi, chunki aynan nutqni matnga aylantiruvchi, ko‘z harakatini kuzatuvchi va boshqa individual yordamchi vositalar orqali yig‘iladigan ma’lumotlar alohida maxfiylik xavflarini keltirib chiqaradi.

Natija. Tahlil qilingan adabiyotlar asosida maxsus ehtiyojli o‘quvchilarga axborot xavfsizligini o‘qitishda uchraydigan to‘siqlar quyidagi to‘rt asosiy guruhga birlashtirildi:

1) Texnologik-infratuzilmaviy to‘siqlar. Ko‘pgina ta’lim platformalari va kiberxavfsizlik bo‘yicha o‘quv materiallari ekran o‘quvchi dasturlar, subtitrlar, katta shrift yoki soddalashtirilgan interfeys kabi moslashtirilgan imkoniyatlarni ta’minlamaydi. F. Hellems va S. Bhatiyaning tahlili shuni ko‘rsatadiki, mavjud kiberxavfsizlik o‘quv dasturlarining aksariyati maxsus ehtiyojli o‘quvchilar uchun teng kirish imkoniyatini yaratmagan [4].

2) Kognitiv va idrok etish bilan bog‘liq to‘siqlar. Fishing, ijtimoiy injiniring yoki maxfiylik siyosati kabi mavhum tushunchalarni og‘zaki-mantiqiy shaklda taqdim etish intellektual rivojlanish xususiyatlariga ega o‘quvchilar uchun qiyinchilik tug‘diradi. Ispaniyada o‘tkazilgan tadqiqot shuni ko‘rsatdiki, yengil intellektual buzilishga ega ta’lim oluvchilar onlayn xavflarni umuman anglash darajasida yaxshi ko‘rsatkichlarga ega bo‘lsa-da, parol xavfsizligi kabi amaliy ko‘nikmalarda izchil emasligini namoyon etdi [6].

3) Kommunikativ va o‘qituvchi tayyorgarligi bilan bog‘liq to‘siqlar. Ko‘plab tadqiqotlar o‘qituvchilarning maxsus ehtiyojli o‘quvchilarga raqamli mavzularni moslashtirib o‘qitish bo‘yicha yetarli tayyorgarlikka ega emasligini qayd etadi. J. Fernández-Cerero va hamkasblarining tizimli tahlili o‘qituvchilarning texnologik tayyorgarligi nogironligi bo‘lgan talabalarning ta’limga jalb etilishi va hayot sifatiga bevosita ta’sir ko‘rsatishini isbotladi [7].

4) Institutsional va me’yoriy-huquqiy to‘siqlar. Ko‘pgina milliy ta’lim standartlari inklyuzivlik yoki moslashtirish talablarini alohida band sifatida kiritmagan, bu esa amaliyotda ixtiyoriy yondashuvga olib keladi.

Tahlil qilingan adabiyotlarda inklyuziv sharoitda axborot xavfsizligini o‘qitish samaradorligini oshiruvchi bir qator yondashuvlar ham aniqlandi. Bular:

Ta’limninguniversaldizayni(Universal Design for Learning, UDL). CAST (Center for Applied Special Technology) tomonidan ishlab chiqilgan ushbu konsepsiyasi o‘quv mazmunini bir necha usulda taqdim etish (vizual, audio, matnli), o‘quvchilarga bilimni namoyish etishning turli yo‘llarini taklif qilish va motivatsiyani turlicha shakllantirishga asoslanadi. Universal dizayn tamoyili dastlab arxitekturada qo‘llanilgan bo‘lib, keyinchalik ta’lim sohasiga moslashtirildi va bugungi kunda raqamli o‘quv resurslarini loyihalashning asosiy metodologik asosi hisoblanadi [8].

Assistiv texnologiyalar va moslashtirilgan baholash vositalari. Texnologiyalar yordamida maxsus ehtiyojli o‘quvchilarni aniqlash va ularga moslashtirilgan qo‘llab-quvvatlash ko‘rsatish bo‘yicha so‘nggi tadqiqotlar sun’iy intellekt asosidagi moslashuvchan baholash tizimlarining samaradorligini tasdiqlaydi, biroq bunday tizimlarning o‘zi ham maxfiylik va ma’lumotlar xavfsizligi nuqtai nazaridan qo‘shimcha e’tiborni talab qiladi [9].

O‘yin texnologiyalari. Kiberxavfsizlik tushunchalarini metaforik o‘yin ssenariylari

orqali tushuntirish — bu usul odatiy o‘quvchilar uchun samarali bo‘lgani kabi, xususan diqqatni jamlashda qiyinchilikka ega o‘quvchilar uchun ham qulay format hisoblanadi, chunki u mavhum tushunchalarni aniq, bosqichma-bosqich vaziyatlarga aylantiradi.[10]

Neyroxilma-xillikni resurs sifatida tan olish. So‘nggi tadqiqotlar diqqatni alohida qaratadigan yo‘nalish sifatida neyroxilma-xil o‘quvchi va mutaxassislarning kiberxavfsizlik sohasidagi salohiyatini ta’kidlaydi hamda ularni kamsituvchi emas, balki adolatli va shaffof sun’iy intellekt vositalaridan foydalangan holda ta’lim va kasbiy tayyorgarlik dasturlarini ishlab chiqishni tavsiya qiladi [11,12].

Yuqoridagi tahlil natijalariga tayanib, O‘zbekiston umumta’lim tizimida inklyuziv axborot xavfsizligi ta’limini rivojlantirish bo‘yicha quyidagi tavsiyalar ishlab chiqildi:

Moslashtirilgan o‘quv-metodik majmua yaratish. «Informatika va axborot texnologiyalari» fani doirasidagi kiberxavfsizlik mavzulari universal ta’lim dizayni (UDL) tamoyillari asosida qayta ishlab chiqilib, vizual, audio va taktil materiallar bilan boyitilishi lozim.

O‘qituvchilarni tayyorlash va malaka oshirish. Pedagogika oliy ta’lim muassasalarining informatika va defektologiya yo‘nalishlari o‘quv rejalariga «Inklyuziv sharoitda raqamli xavfsizlik» mavzusidagi maxsus modul kiritilishi tavsiya etiladi.

Yordamchi texnologiyalarni joriy etish. Ekran o‘quvchilari, imo-ishora tili video-tarjimasi va soddalashtirilgan matnformatidagi elektron o‘quv materiallarini davlat ta’lim portallariga integratsiya qilish zarur.

Monitoring va baholash tizimini yo‘lga qo‘yish. Maxsus ehtiyojli o‘quvchilarning kiberxavfsizlik bo‘yicha bilim va ko‘nikmalarini o‘lchashga mo‘ljallangan, mahalliy sharoitga moslashtirilgan diagnostik vositalar ishlab chiqilishi kerak.

Ota-onalar bilan ishlash tizimini kengaytirish. Umumta’lim maktablari, ta’lim markazlari orqali ota-onalar uchun “Bolangizni raqamli xavflardan qanday himoya qilish mumkin” mavzusida maxsus, tushunarli tilda ishlab chiqilgan qo‘llanmalar va treninglar tashkil etilishi lozim.

Fanlararo hamkorlikni institutsionallashtirish. Informatika o‘qituvchilari, maxsus pedagoglar (defektologlar), psixologlar va IT-mutaxassislarni birlashtiruvchi doimiy ishchi guruhlar yoki uslubiy kengashlar tashkil etilishi, bu esa dastur va materiallarni ishlab chiqishda barcha zarur ekspertizani jamlashga xizmat qiladi.

Xulosa. Ushbu tizimli adabiyotlar tahlili inklyuziv ta’lim muhitida axborot xavfsizligi fanini o‘qitish borasidagi jahon tajribasini umumlashtirdi va bir qator muhim xulosalarga kelishga imkon berdi. Birinchidan, kiberxavfsizlik ta’limi bo‘yicha mavjud tadqiqotlar va o‘quv dasturlarining katta qismi tipik rivojlanayotgan o‘quvchilarga mo‘ljallangan bo‘lib, maxsus ta’lim ehtiyojiga ega o‘quvchilar ushbu jarayonda yetarlicha e’tiborga olinmagan. Ikkinchidan, raqamli fuqarolik, maxfiylik va parol xavfsizligi kabi mavzular nisbatan yaxshi yoritilgan bo‘lsa-da, yordamchi texnologiyalar xavfsizligi kabi maxsus ehtiyojli o‘quvchilarga xos mavzular deyarli tadqiq etilmagan. Uchinchidan, Ta’limning universal dizayni (UDL), moslashtirilgan o‘yinlashtirish va sun’iy intellekt asosidagi shaxsiylashtirish samarali vositalar sifatida qayd etilgan bo‘lsa-da, ularning umumta’lim bosqichida tizimli va standartlashtirilgan tarzda qo‘llanilishi hali yetarli emas.

Tadqiqot, shuningdek, terminologik nomuvofiqlik, fanlararo hamkorlikning yetishmasligi va rivojlanayotgan mamlakatlar, jumladan O‘zbekiston kabi Markaziy Osiyo davlatlari bo‘yicha tadqiqotlarning deyarli mavjud emasligini aniqladi. Ushbu

bo‘shliqlarni bartaraf etish maqsadida maqolada moslashtirilgan o‘quv-metodik materiallar yaratish, pedagog kadrlarni tayyorlash, milliy standartlarni ishlab chiqish va mahalliy diagnostik vositalarni joriy etishga qaratilgan amaliy tavsiyalar taklif qilindi.

Minnatdorchilik. Ushbu tadqiqot O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi tomonidan « Kriptografiya fani bo‘yicha elektron o‘quv qo‘llanma yaratish» mavzusidagi AL-9624115223 raqamli ilmiy loyiha doirasida bajarildi.

**Foydalanilgan adabiyotlar :**

1. O‘RQ-641-son 15.10.2020 “Nogironligi bo‘lgan shaxslarning huquqlari to‘g‘risida” O‘zbekiston Respublikasining Qonuni, (Lex.uz). – URL: https://lex.uz/uz/docs/-5049511
2. O‘zbekiston Respublikasi Prezidentining Farmoni, 11.09.2023 yildagi PF-158-son “O‘zbekiston — 2030” strategiyasi to‘g‘risida - (Lex.uz). – URL: https://lex.uz/ru/docs/-6600413
3. Page, M. J., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. International Journal of Surgery, 88, Art. no. 105906. https://doi.org/10.1016/j.ijsu.2021.105906
4. Hellems, F., & Bhatia, S. (2022). Removing the Veil: Shining Light on the Lack of Inclusivity in Cybersecurity Education for Students with Disabilities. Sacred Heart University, School of Computer Science & Engineering. https://digitalcommons.sacredheart.edu/computersci_fac/183/
5. Ibrahim, A., McKee, M., Sikos, L. F., & Johnson, N. F. (2024). A Systematic Review of K-12 Cybersecurity Education Around the World. IEEE Access, 12, 59726–59738. https://doi.org/10.1109/ACCESS.2024.3393425
6. Digital Safety and Risk Perception in Higher Education: Insights from Spanish University Students with Intellectual Disabilities. (2025). Disabilities, 5(4), 108. https://doi.org/10.3390/disabilities5040108
7. Fernández-Cerero, J., Montenegro-Rueda, M., & Fernández-Batanero, J. M. (2023). Impact of University Teachers' Technological Training on Educational Inclusion and Quality of Life of Students with Disabilities: A Systematic Review. International Journal of Environmental Research and Public Health, 20(3), 2576. https://doi.org/10.3390/ijerph20032576
8. Rose, D., & Meyer, A. Universal Design for Learning. Center for Applied Special Technology (CAST), Wakefield, MA
9. Pradhapan, P., Griffioen, R., Clerx, M., & Mihajlovic, V. (2017). Personalized characterization of sustained attention/vigilance in healthy children. Proc. EHealth 360°, Budapest, Hungary, 271–281. https://doi.org/10.1007/978-3-319-49655-9_35
10. A.Matyakubov, F.Muxammadiyev. Raqamli ta’lim muhitida talabalarning kiberxavfsizlik madaniyatini rivojlantirishda Interaktiv metodlar va psixologik omillar.// O‘zMU xabarlari, 2026, [9] ISSN 2181-7324
11. Empowering Neurodiverse Talent in Cybersecurity Through Fair and Inclusive AI Education. (2026). Proceedings of the 57th ACM Technical Symposium on Computer Science Education V.2. https://doi.org/10.1145/3770761.3777172
12. Abdurazzokov, J., Abdurakhimov, B. Simmetrik kalitni shifrlash algoritmlarning nochiziqli komponentlarini tasniflash va shakllantirishda intellektual algoritmlarni qo‘llash masalalari – monografiya , Toshkent 2026, 147b.