O‘ZBEKISTON MILLIY PEDAGOGIKA UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/30.2020.Ped.26.01 RAQAMLI ILMIY KENGASH

O‘ZBEKISTON MILLIY PEDAGOGIKA UNIVERSITETI

MUXTAROV FARRUX MUXAMMADOVICH

AXBOROT XURUJI DAVRIDA “KIBERXAVFSIZLIK ASOSLARI” FANINI O‘QITISHNING DASTURIY-METODIK TA’MINOTINI TAKOMILLASHTIRISH

13.00.06 – Raqamli ta’lim nazariyasi va metodikasi

PEDAGOGIKA FANLARI DOKTORI (DSc) DISSERTATSIYASI AVTOREFERATI

Toshkent – 2025

Fan doktori (DSc) dissertatsiyasi avtoreferati mundarijasi

Оглавление автореферата диссертатсии доктора наук (DSc)

Doctor of science (DSc) dissertation abstract content

O‘ZBEKISTON MILLIY PEDAGOGIKA UNIVERSITETI HUZURIDAGI ILMIY DARAJALAR BERUVCHI DSc.03/30.2020.Ped.26.01 RAQAMLI ILMIY KENGASH

O‘ZBEKISTON MILLIY PEDAGOGIKA UNIVERSITETI

MUXTAROV FARRUX MUXAMMADOVICH

AXBOROT XURUJI DAVRIDA “KIBERXAVFSIZLIK ASOSLARI” FANINI O‘QITISHNING DASTURIY-METODIK TA’MINOTINI TAKOMILLASHTIRISH

13.00.06 – Raqamli ta’lim nazariyasi va metodikasi

PEDAGOGIKA FANLARI DOKTORI (DSc) DISSERTATSIYASI AVTOREFERATI

Toshkent – 2025

Fan doktori (DSc) dissertasiyasi mavzusi O‘zbekiston Respublikasi Oliy attestasiya komissiyasida B2024.3.DSc/Ped981 raqam bilan ro‘yxatga olingan.

Dissertatsiyasi O‘zbekiston milliy pedagogika universitetida bajarilgan.

Dissertatsiya avtoreferati uch tilda (o‘zbek, rus, ingliz (rezyume)) veb-sahifasida www.tdpu.uz hamda “ZiyoNet” axborot ta’lim portalida www.ziyonet.uz manzillariga joylashtirilgan.

Ilmiy maslahatchi:	**Abdullayeva Barno Sayfutdinovna** pedagogika fanlari doktori, professor
Rasmiy opponentlar:	**Qayumova Nasiba Ashurovna** pedagogika fanlari doktori, professor
	Sultanova O‘g‘iloy Nabievna pedagogika fanlari doktori, professor
	Abdullayeva Ozoda Safibullaevna pedagogika fanlari doktori, professor
Yetakchi tashkilot:	**Guliston davlat universiteti**

Dissertatsiya himoyasi O‘zbekiston milliy pedagogika universiteti huzuridagi ilmiy darajalar beruvchi DSc.03/30.2020.Ped.26.01 raqamli ilmiy kengashning 2025-yil “___” _____soat _____dagi majlisida bo‘lib o‘tadi (manzil: 100011, Toshkent shahri, Chilonzor tumani, Bunyodkor ko‘chasi, 27 uy. Tel.: (+99871) 276-79-11, faks (+99871) 276-80-86.

Dissertasiya bilan O‘zbekiston milliy pedagogika universiteti huzuridagi DSc03/30.01.2020 O‘zbekiston milliy pedagogika universiteti axborot-resurs markazida tanishish mumkin (_____ raqam bilan ro‘yxatga olingan). Manzil: 100011, Toshkent shahri, Chilonzor tumani, Bunyodkor ko‘chasi, 27-uy. Tel.: (+99871) 276-79-11, faks (+99871) 276-80-86.

Dissertatsiya avtoreferati 2025-yil “_____” _____kuni tarqatildi.
(2025-yil “_____” _____ dagi _____ raqamli reestr bayonnomasi).

Z.N.Mamarajabova
Ilmiy darajalar beruvchi ilmiy kengash raisi, p.f.d., professor

R.G.Isyanov
Ilmiy darajalar beruvchi ilmiy kengash kotibi, p.f.n., dotsent

M.E.Mamarajabov
Ilmiy darajalar beruvchi ilmiy kengash qoshidagi Ilmiy seminar raisi, p.f.d., professor

KIRISH (fan doktori (DSc) dissertatsiyasi annotatsiyasi)

Dissertatsiya mavzusining dolzarbligi va zarurati. Jahon ta’lim muassasalarida axborot va kiberxavfsizlikni ta’minlash o‘z axborot resurslarini rivojlantirish va himoya qilish, boshqa mamlakatlarning axborot resurslariga ta’sir qilish texnologiyalari amaliyotga tadbiq etilmoqda. AQSH, Rossiya, Yevropa Ittifoqi, Xitoy, Hindistonda tarmoqlardan foydalanishga mas’ul maxsus bo‘linmalar faoliyatini rivojlantirish, kiberxavfsizlik soha mutaxassislarini bilim darajasini oshirish, innovatsion pedagogik usullardan foydalangan holda bo‘lajak mutaxassislarning axborot savodxonligi hamda axborot xurujlariga qarshi mafkuraviy immunitetini rivojlantirish jarayonini takomillashtirish bo‘yicha tizimli ishlar olib borilmoqda.

Jahon ta’lim va ilmiy tadqiqot markazlarida talabalarning axborot va kiberxavfsizlik bo‘yicha bilim va ko‘nikmalarini rivojlantirish, informativ – kognitiv kompetensiyalarni takomillashtirish, kasbiy kompetentlik doirasida izchil tarzda tashkil etishning zamonaviy dasturiy – pedagogik metodologik asoslarini takomillashtirish bo‘yicha ilmiy izlanishlar olib borilmoqda. Ta’limning zamonaviy didaktik vositalari asosida bo‘lajak mutaxassislarda kasbiy kompetensiyalarning takomillashuvini o‘zaro axborot almashinuvi va xavfsizligi bo‘yicha zamonaviy texnologiyalar asosida baholash, kiberxavfsizlik madaniyatini rivojlantirish modellarining samaradorligini oshirish, informativlikka interaktiv tarzda ta’limga keng tatbiq qilish bo‘yicha tadqiqotlarga e’tibor berilmoqda.

Respublikamizda so‘nggi yillarda ta’lim muassasalarida talaba-yoshlarning axborot xavfsizligi bo‘yicha bilimlar doirasini kengaytirish, axborot texnologiyalari boshqaruvi hamda resurslarning fanlararo integratsiyasini amalga oshirishning me’yoriy asoslari yaratilmoqda. 2017-2021-yillarda O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasida ketirilgan “...axborot xavfsizligini ta’minlash va axborotni himoyalash tizimini takomillashtirish, axborot sohasidagi tahdidlarga qarshi o‘z vaqtida va munosib qarshilik ko‘rsatish”[1] hamda 2023-yil 11-sentabrda qabul qilingan “O‘zbekiston – 2030” strategiyasi to‘g‘risidagi O‘zbekiston Respublikasi Prezidentining 158-son Farmonida keltirilgan “…Internet jahon axborot tarmog‘idan to‘siqlarsiz foydalanish uchun zarur shart-sharoitlarni yaratish, milliy internet makonida kiberxavfsizlikni ta’minlash hamda fuqarolarning internetdan foydalanish borasidagi savodxonligini oshirish”[2] vazifalari belgilangan. Natijada kiberhujumlarning oldini olish, ularni aniqlash va oqibatlarini bartaraf etishning muqobil imkoniyatlari kengayadi.

O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi PQ-167-son “O‘zbekiston Respublikasining muhim axborot infratuzilmasi obyektlari kiberxavfsizligini ta’minlash tizimini takomillashtirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida”gi Qarori, “O‘zbekiston Respublikasida kriptologiya sohasida ta’lim va ilm-fanni rivojlantirish bo‘yicha qo‘shimcha chora-tadbirlar to‘g‘risida” 2024-yil 15-avgustdagi PQ-293-son Qarori, O‘zbekiston Respublikasi Prezidentining 2025-yil 30-

[1] O‘zbekiston Respublikasi Prezidentining 2017-yil 7-fevraldagi “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida”gi PF-4947-sonli Farmoni

[2] O‘zbekiston Respublikasi Prezidentining 2023-yil 11-sentyabrdagi ““O‘zbekiston — 2030” strategiyasi to‘g‘risida”gi PF-158-sonli Farmoni

apreldagi PQ-153-sonli “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi Qarori, 2017-yil 20-apreldagi PQ-2909-son “Oliy ta’lim tizimini yanada rivojlantirish chora-tadbirlari to‘g‘risida”gi Qarori hamda mazkur faoliyatga tegishli boshqa me’yoriy-huquqiy hujjatlarda belgilangan vazifalarni amalga oshirishda mazkur dissertatsiya tadqiqoti muayyan darajada xizmat qiladi.

Tadqiqotning respublika fan va texnologiyalarni rivojlantirishning ustuvor yo‘nalishlariga mosligi. Mazkur tadqiqot respublika fan va texnologiyalar rivojlanishining. 1 “Axborotlashgan jamiyat va demokratik davlatni ijtimoiy, huquqiy, iqtisodiy, madaniy, ma’naviy-ma’rifiy rivojlantirishda innovatsion g‘oyalar tizimini shakllantirish va ularni amalga oshirish yo‘llari” ustuvor yo‘nalishiga mos ravishda bajarilgan.

Dissertatsiya mavzusi bo‘yicha xorijiy ilmiy tadqiqotlar sharhi

“Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy hamda uslubiy ta’minotini takomillashtirish bilan bog‘liq masalalarni o‘rganish va axborot xavfsizligi, kiberxavfsizlik, kriptografik masalalarga zamonaviy yondashuvlar bo‘yicha jahonning ko‘p mamlakatlari ilmiy tadqiqotlar olib bormoqda. Jumladan, AQSHning Carnegie Mellon University, Buyuk Britaniyaning University of Oxford va University of Cambridge universitetlari hamda Queen’s University Belfast - CSIT tadqiqotlar markazi, Germaniyaning ATHENE (Darmstadt) - Evropaning eng yirik IT-xavfsizlik markazi, Turkiyaning TÜBİTAK BİLGEM - axborot xavfsizligi va kriptografiya bo‘yicha ilmiy-texnologik markaz, Janubiy Koreyaning Korea University CIST, Xitoyning Tsinghua University, Beijing University of Posts and Telecommunications va boshqa nufuzli universitet, ilmiy-tadqiqot markazlarida mazkur soha va uning o‘qitilishi bilan bog‘liq muammolar o‘z yechimini topib kelmoqda.

Amerika Qo‘shma shtadlarining Carnegie Mellon universitetida IoT xavfsizligi, mashina o‘rganish va AI, tarmoq va tizimlar xavfsizligi, shaxsiylik va maxfiylik yo‘nalishlari bo‘yicha 160 dan ortiq magistr va tadqiqotchilar ilmiy faoliyat olib bormoqda. Tadqiqotchilarining 10%i sohani o‘qitish bo‘yicha shug‘ullanib, asosan metodologiya va dasturiy-metodik vositalarni takomillashtirish bilan bog‘liq faoliyatni olib boradi. Stanford universitetida Stanford Online’da “Advanced Cybersecurity Program” va “Cybersecurity and Executive Strategy” kurslari mavjud bo‘lib, uning faoliyat maqsadi risklarni aniqlash, baholash va strategik javob berish bo‘yicha tajriba oshirishdan iborat. Buyuk Britaniyaning Oxford universitetida “Software and Systems Security”, “Software Engineering” va “Social Science of the Internet” magistratura va doktorantura dasturlari taklif etilgan bo‘lib, dastur doirasida yosh tadqiqotchilar cloud security, steganografiya, formal tasdiqlash, mobil va tarmoq xavfsizligi, kriptografiya sohalarini rivojlantirish va bu sohalarning o‘qitilishiga xizmat qiluvchi dasturiy-metodik ta’minotni takomillashtirish bilan shug‘illanadi, bundan tashqari ijtimoiy va kompyuter fanlarini birlashtirgan OII “Information Governance and Security” kabi sohalarda ijtimoiy kiberxavfsizlik masalalarini ham o‘rganadi. Germaniyada joylashgan ATHENE (Darmstadt) - yevropaning eng yirik IT xavfsizlik markazi 2015 yilda qayta tashkil etilgan bo‘lib hozirda ID raqamli tizimlar hamda kritikal infratuzilmalarni yo‘lga qo‘yish, xavfsizlik, maxfiylik va kiberxavfsizlik sohalarida ilmiy-tadqiqotlar olib boradi. Turkiyaning BİLGEM – 2010 yilda tashkil etilgan bo‘lib,

UEKAE (Elektronika va Kriptologiya), BTE, SGE, İLTAREN, YTE, YZE kabi 6 ta ilmiy institutni o‘z ichiga oladi. Markazning maqsadi kriptologiya, axborot xavfsizligi va ilg‘or elektronika sohalarida milliy darajada, mustaqil va raqobatbardosh texnologiyalar ishlab chiqish, sohaning yetuk mutaxassislarini tayyorlashda Turkiyaning barcha ta’lim muassasalari uchun amaliyotlar jamlanmasi va o‘qitishning amaliyotiga bag‘ishlangan texnologiyalar bilan ta’minlash. Buni yordamida “Kiberxavfsizlik asoslar” va bunga turdosh fanlarning o‘qitilishida amaliyotga asoslangan o‘qitish strategiyasi shakllanadi. Janubiy Koreyaning Korea universiteti tarkibiga kiruvchi CIST markazi kriptografiya, tarmoq va tizim xavfsizligi, hamda raqamli forenzika sohalarida keng ko‘lamli ilmiy tadqiqotlar olib boradi. Kriptografiya, tarmoq va tizim xavfsizligi ilmiy yo‘nalishlarida bajarilgan ishlari jaxon miqyosida ahamiyatga molik xisoblanadi, shu bilan birga axborot xavfsigiga oid fundamental fanlarni o‘qitishda markazning metodist tadqiqotchilari tomonidan ishlab chiqilgan texnologiya va metodologiyalar asosida Koreya universiteti bakalavriat va magistratura boshqichi talabalariga o‘quv mashg‘ulotlari tashkil etiladi. Xitoyning Tsinghua universitetida axborot xavfsizligi bilan shug‘illanuvchi institute, laboratoriya va markazlar ko‘plab mavjud, bu yerda talabalar Kiberxavfsizlik va unga turdosh fanlarni o‘rganishda institut tomonidan nazariy bilimlar beriladi, laboratoriyalarda nazariy bilimlar mustahkamlanib markazlarda talabalar buyurtmalar bilan ishlash imkoniyatiga ega bo‘ladi. Markazlarda, tashkilotlar va korxonalar, shuningdek jismoniy shaxslar tomonidan ham kiberxujum, shaxsiy elektron ma’lumotlarining o‘g‘irlanish va tahdidlar borasidagi murojaatlar yig‘ilgan bo‘lib, bu muammolarni talabalar erkin, ixtiyoriy va ijodiy yondashib, yechim uchun takliflar tayyorlash imkoniga ega, ularning aralashuvi bilan hal qilingan masalalar, talabalar baholanishini ham ta’minlaydi.

Post-kvant kriptografiyasi (PQC) — chuqur tadqiqot talab qiluvchi zamonaviy yo‘nalishlardan biridir. AI yordamida kiberhujumlarni oldindan aniqlash, botnetlarni aniqlash, soxta ma’lumotlar (deepfake) tahlilini avtomatlashtirish ustida ish olib borilmoqda. Bugungi kunning o‘rganilishi kutilayotgan sohalaridan. Bugun kunda asosiy ilmiy izlanishlari, yangi avlod mobil tarmoqlar (6G) xavfsizlik protokollarini yaratish, signalga hujumlarga qarshi chidamli tizimlar ishlab chiqish sohalariga qaratilmoqda, sabab o‘rnida 6G tarmoqlarida millisoniya tezlikda axborot uzatiladi, bu esa maxfiylik va avtentifikatsiya tizimlarining qayta ko‘rib chiqilishini talab qilinishi bilan izohlangan. Ayni paytda 5–10-sinflar bosqichidan boshlab axborot xavfsizligi, kiberxavfsizlik va kriptografiya sohalariga oid parol xavfsizligi, fishingdan himoyalanish, internetda xulq-odob normalari kabi kiberxavfsizlik savodxonligini shakllantirishga qaratilgan darslar ta’lim tizimiga joriy etilmoqda. Ushbu chora-tadbirlarning asosiy maqsadi — yosh avlodni raqamli tahdidlarga nisbatan xabardor, ongli va himoyalangan tarzda voyaga yetkazishdan iborat.

Muammoning o‘rganilganlik darajasi. Ta’limni axborotlashtirish muammolari, metodik tayyorlashning konseptual asoslarini ishlab chiqish borasida

U.SH.Begimqulov[3], T.T.Kalekeyeva[4], M.Quronov[5], M.X.Lutfillayev[6], Q.Olimov[7], D.J.Saidov[8], N.I.Tayloqov[9], F.Zakirova[10]lar; axborot xavfsizligi va kiberxavfsizlik bo‘yicha ko‘nikma, mexanizm hamda modellarini takomillashtirish T.F.Bekmuratov[11], S.K.G‘aniyev[12], O.G‘.Davlatov[13], O.U.Xalmuratov[14], B.X.Xodjayev[15], A.H.Muxitdinov[16], A.B.Radjiev[17], K.A.Tashayev[18], B.Tahirov[19], U.L.Yoziyeva[20]lar tomonidan tadqiq qilingan.

MDH davlatlaridan axborot xavfsizligi va kiberxavfsizlikka oid A.A.Altufeva[21], A.B.Babash, E.K.Baranova[22], E.V.Bondarevskaya[23], Y.V.Boradakiy[24], V.A.Krasilnikova[25], A.V.Lukatskiy[26], N.N.Moiseev[27]lar ilmiy izlanishlar olib borganlar.

Ta’lim sohasi va turli soha tarmoqlarida kiberholatdan xabardorlik va kiber muhitni monitoring qilish, kiberxavfsizlikka oid yondashuvlar S.Alter[28], Ross J.

---

[3] Begimqulov U.Sh. Pedagogik ta’lim jarayonini axborotlashtirishni tashkil etish va boshqarish nazariyasi va amaliyoti.ped.fan. dok...diss.-T..2007. -305 b.

[4] Kalekeeva T. T. Ta’limni axborotlashtirish sharoitida bo‘lajak informatika o’qituvchilarini tayyorlash mazmunini takomillashtirish. Dis... dok (PhD). – T., 2018. – 135 b.

[5] Quronov M. Milliy xavfsizlik tizimida kiberxavfsizlikning o‘rni va uni ta’lim jarayonida integratsiyalash muammolari // Oliy ta’limda innovatsiyalar. – Toshkent: TDPU, 2021. – №4. – B. 120–128.

[6] Lutfillayev M.H. Oliy ta’lim jarayonini takomillashtirishda axborot texnologiyalarini integrasiyalash nazariyasi va amaliyoti. (Informatika va tabiiy fanlar misolida). ped.fan. dok...diss. Samarqand 2005 - 236 b.

[7] Олимов Қ. Проблема создания учебников специалных дисциплин нового поколения в сфере средного специального образования. Монография. – Т.: “Фан”, 2004. – 144 б.

[8] Saidov D.J., To‘rayeva O.X. Axborot tizimlari va ularning rivojlanishi omillari // Central Asian journal of multidisciplinary research and management studies. Volume 1, Issue 4, March 2024. 67-68-b.

[9] Tayloqov N.I., Rustamov N. Elektron o’quv adabiyotlarini yaratish-davr talabi // Ta’lim va tarbiya. – Toshkent, 2003. -1-2-son. – B. 23 – 25.

[10] 169. Закирова Ф.М. Теоретические и практические основы методической подготовки будущих преподавателей информатики в педагогических ВУЗах. Автореф. дис. ... док-ра. пед.наук. – Ташкент, 2009.

[11] Бекмуратов Т.Ф., 52. G‘aniyev S.K., Karimov M.M., Tashayev K.A. Axborot xavfsizligi. Oliy o‘quv yurt talabalari uchun mo‘ljallangan o‘quv qo‘llanma. “Fan va texnologiya” nashriyoti, Toshkent -2016.Б. 125 – 126.

[12] G‘aniyev S.K., Karimov M.M., Tashayev K.A. Axborot xavfsizligi. Oliy o‘quv yurt talabalari uchun mo‘ljallangan o‘quv qo‘llanma. “Fan va texnologiya” nashriyoti, Toshkent -2016.

[13] Davlatov O.G‘. Talabalarda axborot xavfsizligini ta’minlash kompetenstligini tarixiy-madaniy meros vositasida rivojlantirish. Ped.fan.fals.dok…diss. Toshkent-2018. -21 b.

[14] Xalmuratov O.U.Axborot xavfsizligi ko‘rsatkich va mezonlari tizimini shakllantirish usullari va algoritmlari.Tex.fan.fals.dok.(PhD). …diss. Toshkent-2019. -163 b.

[15] Xodjayev B.X. Umumta’lim maktablari talabalarida tarixiy tafakkurni modernizatsiyalashgan didkatik ta’minot vositasida rivojlantirish. Ped.fan.dok….diss. –T., 2016. – 120-122 b.

[16] Muxitdinov A.H. Axborot xavfsizligini ta’minlashning iqtisodiy mexanizmi. iqt.fan.nomz…diss.Toshkent. 2012.-178 b.

[17] Radjiyev A.B. Xalq ta’limi tizimida rahbar xodimlarni qayta tayyorlash va malakasini oshirishni boshqarish samaradorligini oshirish (umumta’lim maktab direktorlari misolida): ped. fanl. bo‘y. fals. dokt. (PhD) diss. ... avt. –T.: 2020. – 61 b.

[18] G‘aniyev S.K., Karimov M.M., Tashayev K.A. Axborot xavfsizligi. Oliy o‘quv yurt talabalari uchun mo‘ljallangan o‘quv qo‘llanma. “Fan va texnologiya” nashriyoti, Toshkent -2016.

[19] Tahirov B.N. Axborot xavfsizligi asoslari [Matn] : o‘quv qo‘llanma / B.N. Tahirov - Buxoro: Fan va ta’lim, 2022.-156 b.

[20] Yozieva U.L. Ta’lim-tarbiya jarayonida o’quvchilarni zararli axborotlar tahdididan himoya qilishning takomillashtirilgan texnologiyasi (boshlang’ich ta’lim misolida). Pedagogika fanlari bo’yicha falsafa doktori (PhD) dissertatsiyasi. – Nukus, 2018. – 134 b.

[21] Алтуфьева А.А. Методические основы обучения информационной безопасности на базе телекоммуникационных ресурсов сети интернет. Дисс. на соиск. ученой степени канд. пед. наук. - Санкт-Петербург, 2008. – 132 с.

[22] Баранова Э.К. Бабаш А.Б. Информационная безапасност и зашита информации / - М.: ИНФРА-М -РИОР, 2014 г., 216 с.

[23] Бондаревская, Е.В. Гуманистическая парадигма личностно-ориентированного образования / Е.В.Бондаревская // Педагогика.1997. - №4.-С. 11-17.

[24] Бородакий.Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века.

[25] Красильникова В.А. Использование информационных и коммуникационных технологий в образовании. Учебное пособие. Оренбургский гос. ун-т.– 2-е изд. – Оренбург: ОГУ, 2012. – 291 с.

[26] Лукацкий А.В.Краткий толковый словар по информационной безопасности. М.2000. с 72

[27] Моисеев Н.Н. Расставание с простотой. –М., 2000. -473 с

[28] Alter S. The Work System Method: Connecting People, Processes, and IT for Business Results. Works System Press, CA. 2006 y.

Anderson[29], Thomas A. Johanson, Yar Majid va Kevin F[30]. Steinmetz, Ujjwal Rao[31], Howard Schmidt[32], Bruce Schneier[33]lar tomonidan tadqiq etilgan.

Dissertatsiya tadqiqotining dissertatsiya bajarilgan oliy ta'lim muassasasi ilmiy-tadqiqot ishlari rejalari bilan bog'liqligi. Dissertatsiya tadqiqoti Toshkent davlat pedagogika universiteti ilmiy tadqiqot rejasining "Psixologiya tarixini o'rganish, umumiy psixologiya mazmunini o'zlashtirish, shaxs psixologiyasini tasniflash, psixofiziologik tadqiqotlar ko'lamini kengaytirish, tibbiy va kasb psixologiyasi qonuniyatlarini o'rganish, ijtimoiy psixologiya, etnopsixologiya hamda yosh davrlari va pedagogik psixologiyaning konseptual asoslarini tadqiq qilish" nomli ustuvor yo'nalish doirasida bajarilgan (2020-2024 yy.).

Tadqiqotning maqsadi bo'lajak o'qituvchilarning intellektual kompetentligini rivojlantirishning dasturiy ta'minotini takomillashtirishga doir tavsiyalar ishlab chiqishdan iborat.

Tadqiqot vazifalari:

axborotlar xuruji davrida "Kiberxavfsizlik asoslari" fanini o'qitishning pedagogik imkoniyatlarini aniqlash;

axborotlar xuruji davrida "Kiberxavfsizlik asoslari" fanini o'qitishning dasturiy-metodik ta'minoti mazmunini takomillashtirish;

"Kiberxavfsizlik asoslari" fanini o'qitish jarayonida talabalar kiberetika madaniyatini shakllantirish modelini takomillashtirish;

"Kiberxavfsizlik asoslari" fanini o'qitishning o'quv-metodik ta'minotini boyitishga asoslangan dasturiy-metodik ta'minotni joriy etish metodikasini takomillashtirish;

axborotlar xuruji davrida "Kiberxavfsizlik asoslari" fanini o'qitishning dasturiy-metodik ta'minotini takomillashtirishga qaratilgan elektron platformani joriy etish samaradorligini aniqlashtirish.

Tadqiqotning obyekti sifatida axborotlar xuruji davrida "Kiberxavfsizlik asoslari" fanini o'qitishning dasturiy-metodik ta'minotini takomillashtirish jarayoni bo'lib, tajriba-sinov ishlarida Toshkent axborot texnologiyalari universitetining Samarqand, Qarshi va Farg'ona filiallarining 1–4 bosqich talabalaridan 497 nafari jalb etildi.

Tadqiqotning predmetini axborotlar xuruji davrida "Kiberxavfsizlik asoslari" fanini o'qitishning dasturiy-metodik ta'minotini takomillashtirish, shakl, metod va vositalari tashkil etadi.

Tadqiqotning usullari. Tadqiqot jarayonida pedagogik kuzatuv, qiyosiy tahlil, umumlashtirish, sotsiologik metodlar (anketa, savol-javob, suhbat, ekspert baholash) pedagogik tajriba-sinov, matematik-statistik tahlil kabi usullardan foydalanildi.

Tadqiqotning ilmiy yangiligi quyidagilardan iborat**:**

---

[29] Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems (2nd ed.). Indianapolis: Wiley. ISBN: 978-0-470-06852-5. 2008 y.

[30] Yar Majid and Kevin F. Steinmetz. Cybercrime and society. SAGE. 2019 y.

[31] Ujjwal Rao. Student, B. Tech, Department of Computer Science and Engineering Dronacharya College of Engineering, Gurgaon, Haryana, India

[32] Jan de Lange and William Schmidt. What are PISA and TIMSS? What do they tell us? https://www.researchgate.net/publication/41537659 What are PISA and TIMSS What do they tel us.

[33] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in *C* (2nd ed.). New York: John Wiley & Sons. ISBN: 978-0-471-11709-4.

axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishni takomillashtirishning pedagogik imkoniyatlari himoya qilish usullarining qonuniylikka mos ravishda kibermakonda shaxs, jamiyat va davlat manfaatlari ustuvorligini ta’minlashga qaratilgan yagona yondashuv muhitini shakllantirish hamda kibertahdidlar sharoitida talabalarning kiberetika madaniyatini rivojlantirishga ta’sir qiluvchi asosiy tamoyillarni tasniflash asosida aniqlashtirilgan;

axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minoti mazmuni xavfsizlik terminlarning semantik tuzilmasini ta’limiy maqsadlarga mosligini aniqlash, shifrlash-kodlash, kriptografik algoritmlar, tarmoq xavfsizligi va ma’lumotlarni saqlash bo‘yicha zamonaviy himoya usullarini kiritish hamda foydalanuvchi interfeysini identifikatsiya, autentifikatsiya va konfidensiallik jarayonlariga proporsional mosligini ta’minlash asosida takomillashtirilgan;

“Kiberxavfsizlik asoslari” fanini o‘qitish jarayonida talabalar kiberetika madaniyatini shakllantirish modeli axborot xavfsizligini ta’minlashning dolzarb muammolarini darajalash, axborot va kiberxavfsizlikning o‘ziga xos differensial xususiyatlarini kolloboratsiyalash hamda global muammolar yechimini tizimli-tuzulmaviy tahlil qilish va argumentlash, uzluksizlik, fanlararo aloqadorlik tamoyillarini informativ, kontekstli, integrativ, faoliyatli yondashuvlarga maqsadli uyg‘unlashtirish asosida takomillashtirilgan;

axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotni joriy etish metodikasi interaktiv usullar, virtual makonda axborot tahdidlari va kiberhujum strategiyalariga tezkor javob berish imkonini beruvchi audiovizual axborot, blokcheyn, bulut texnologiyalar, nazorat va o‘z-o‘zini nazorat qilish metodlari imkoniyatlardan unumli foydalanish, o‘qish bilan bog‘liq derivativ, assotsiativ birliklarni raqamli ta’lim vositalariga moslashtirish hamda kiberetika madaniyatining rivojlanganligini asoslovchi komponentlarni ierarxik tizimlashtirish asosida takomillashtirilgan.

“Kiberxavfsizlik asoslari” fanini o‘qitish jarayonida talabalar kiberetika madaniyatini shakllantirish samaradorligi axborot xavfsizligini ta’minlash, dasturiy va texnik vositlardan maqsadli foydalanish, tarmoqlararo klassifikatsiyasini aniqlashtirish hamda axborot xurujining ta’lim jarayoniga ta’sir jihatlarini o‘rganish va talabalarda kibertahdidlarga qarshilik ko‘rsatishning o‘quv kognitiv, kommunikativ tafakkur qilish, integrativ-kreativ ko‘nikmalarni barqaror rivojlantirish darajalariga dinamik ustuvorlik berish asosida takomillashtirilgan.

Tadqiqotning amaliy natijalari quyidagilardan iborat:

axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish modeli takomillashtirilgan;

bo‘lajak o‘qituvchilar uchun ilg‘or pedagogik va innovatsion metodlarni ta’lim jarayoniga joriy qilish bo‘yicha metodik-ta’minot nashr qilingan “Kiberxavfsizlik asoslari” darslik (Oliy ta’lim, fan va innovatsiyalar vazirligining № 11-05-7601/04 raqamli guvohnomasi), “EduCyberSecurity” onlayn o‘qitish platformasi (O‘zbekiston Respublikasi Adliya vazirligining № DGU 46759 raqamli guvohnomasi) va “Kiberxavfsizlik asoslari” mobil ilova (O‘zbekiston Respublikasi Adliya vazirligining № DGU 46916 raqamli guvohnomasi) yaratilgan.

Tadqiqot natijalarining ishonchliligi muammoga falsafiy, pedagogik va psixologik, metodik yondashish hamda texnologik yo‘nalishlar bo‘yicha respublikamiz va chet ellik olimlar tajribalariga asoslangani, tadqiqot vazifalariga mos, o‘zaro bir-birini to‘ldiradigan tadqiqot metodlari qo‘llangani, tahlil va tavsifning miqdor va sifat jihatdan ta’minlangani; tajriba-sinov ishlari samaradorligining matematik-statistik metodlar vositasida asoslanganligi, olingan natijalarning vakolatli tuzilmalar tomonidan tasdiqlangani hamda xulosa va tavsiyalarning amaliyotga joriy qilingani bilan belgilanadi.

Tadqiqot natijalarining ilmiy va amaliy ahamiyati. Tadqiqotning ilmiy ahamiyati bo‘yicha kiberetika madaniyatini shakllantirishda amaliyotga yo‘nalganligi, stilistik differensiatsiya, ta’limning ijodiy yo‘nalganligi, fanlararo integratsiya va fan ichidagi integratsiya tamoyillari; kompetentlik, shaxsga yo‘naltirilgan, ijtimoiy-lingvistik, integrativ, ijtimoiy-madaniy, kommunikativ va tizimli yondashuvlari; ta’lim mazmuni komponentlari (lingvistik, ijtimoiy-lingvistik, ijtimoiy-madaniy, pragmatik) va elektron-didaktik vositalarni uzviy ta’minlashni innovatsion ta’lim sharoitida pedagogik muammolarning maqbul yechimlarini topish va natijaga erishish kabi to‘rt bosqichi aniqlashtirilganligi bilan izohlanadi.

Tadqiqotning amaliy ahamiyati axborot xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish bo‘yicha natija, taklif va tavsiyalar, shuningdek ishlab chiqilgan dasturiy va uslubiy materiallar o‘quv jarayoniga tadbiq qilinishi mumkinligidan iborat. Ulardan zamonaviy resurs va usullardan foydalangan holda o‘quv qo‘llanmalarini yaratish va yangilashda, shuningdek, talabalarning bilim, ko‘nikma va malaka darajasini baholash uchun monitoringni tashkil etishda foydalanish mumkin.

Tadqiqot natijalarining joriy qilinishi. Axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish bo‘yicha olingan ilmiy natijalar asosida:

axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishni takomillashtirishning pedagogik imkoniyatlari himoya qilish usullarining qonuniylikka mos ravishda kibermakonda shaxs, jamiyat va davlat manfaatlari ustuvorligini ta’minlashga qaratilgan yagona yondashuv muhitini shakllantirish hamda kibertahdidlar sharoitida talabalarning kiberetika madaniyatini rivojlantirishga ta’sir qiluvchi asosiy tamoyillarni tasniflash asosida aniqlashtirishga oid tavsiyalar “Kiberxavfsizlik asoslari” nomli darslik mazmuniga singdirilgan (Toshkent davlat pedagogika universitetining 2024-yil 28-dekabrdagi 11-05-7601/04 raqamli nashr ruxsatnomasi). Natijada “Kiberxavfsizlik asoslari” fanini o‘qitish mazmuni kengaytirilgan;

axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minoti mazmuni xavfsizlik terminlarning semantik tuzilmasini ta’limiy maqsadlarga mosligini aniqlash, shifrlash-kodlash, kriptografik algoritmlar, tarmoq xavfsizligi va ma’lumotlarni saqlash bo‘yicha zamonaviy himoya usullarini kiritish hamda foydalanuvchi interfeysini identifikatsiya, autentifikatsiya va konfidensiallik jarayonlariga proporsional mosligini ta’minlash asosida takomillashtirishga oid tavsiyalar “Kiberxavfsizlik asoslari” nomli darslik mazmuniga singdirilgan (Toshkent davlat pedagogika universitetining 2024-yil 28-dekabrdagi 11-05-7601/04 raqamli

nashr ruxsatnomasi). Natijada “Kiberxavfsizlik asoslari” fanini o‘qitishning o‘quv-metodik ta’minoti mazmuni kengaytirilgan;

“Kiberxavfsizlik asoslari” fanini o‘qitish jarayonida talabalar kiberetika madaniyatini shakllantirish modeli axborot xavfsizligini ta’minlashning dolzarb muammolarini darajalash, axborot va kiberxavfsizlikning o‘ziga xos differensial xususiyatlarini kolloboratsiyalash hamda global muammolar yechimini tizimli-tuzulmaviy tahlil qilish va argumentlash, uzluksizlik, fanlararo aloqadorlik tamoyillarini informativ, kontekstli, integrativ, faoliyatli yondashuvlarga maqsadli uyg‘unlashtirish asosida takomillashtirishga oid tavsiyalar “Kiberxavfsizlik asoslari” nomli darslik mazmuniga singdirilgan (Toshkent davlat pedagogika universitetining 2024-yil 28-dekabrdagi 11-05-7601/04 raqamli nashr ruxsatnomasi). Natijada talabalardan axborot xavfsizligini ta’minlash va kompetensiyalarini rivojlantirishning dolzarb muammolarini aniqlashga erishilgan;

axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotni joriy etish metodikasi interaktiv usullar, virtual makonda axborot tahdidlari va kiberhujum strategiyalariga tezkor javob berish imkonini beruvchi audiovizual axborot, blokcheyn, bulut texnologiyalar, nazorat va o‘z-o‘zini nazorat qilish metodlari imkoniyatlardan unumli foydalanish, o‘qish bilan bog‘liq derivativ, assotsiativ birliklarni raqamli ta’lim vositalariga moslashtirish hamda kiberetika madaniyatining rivojlanganligini asoslovchi komponentlarni ierarxik tizimlashtirish asosida takomillashtirishga oid tavsiyalar “Kiberxavfsizlik asoslari” nomli darslik mazmuniga singdirilgan. Natijada “Kiberxavfsizlik asoslari” fanini o‘zlashtirishning ijobiy natijalariga erishilgan.

“Kiberxavfsizlik asoslari” fanini o‘qitish jarayonida talabalar kiberetika madaniyatini shakllantirish samaradorligi axborot xavfsizligini ta’minlash, dasturiy va texnik vositlardan maqsadli foydalanish, tarmoqlararo klassifikatsiyasini aniqlashtirish hamda axborot xurujining ta’lim jarayoniga ta’sir jihatlarini o‘rganish va talabalarda kibertahdidlarga qarshilik ko‘rsatishning o‘quv kognitiv, kommunikativ tafakkur qilish, integrativ-kreativ ko‘nikmalarni barqaror rivojlantirish darajalariga dinamik ustuvorlik berish asosida takomillashtirishga oid tavsiyalar “Kiberxavfsizlik asoslari” nomli darslik mazmuniga singdirilgan (Toshkent davlat pedagogika universitetining 2024-yil 28-dekabrdagi 11-05-7601/04 raqamli nashr ruxsatnomasi). Natijada axborotlar xuruji davrida talabalarda kiberetika madaniyatini shakllantirishning aspektlari aniqlashtirilgan.

Tadqiqot natijalarining aprobatsiyasi. Mazkur tadqiqot natijalari 2 ta xalqaro va 2 ta respublika ilmiy-amaliy anjumanida muhokamadan o‘tkazilgan.

Tadqiqot natijalarining e’lon qilinganligi. Tadqiqot mavzusi bo‘yicha jami 26 ta ilmiy-uslubiy ish, Oliy attestatsiya komissiyasining doktorlik dissertatsiyalari asosiy ilmiy natijalari chop etish tavsiya qilingan ilmiy nashrlarda 1 ta monografiya, 11 ta maqola, jumladan, 10 tasi respublikada va 1 tasi xorijiy jurnallarda nashr ettirilgan.

Dissertatsiyaning tuzilishi va hajmi. Dissertatsiya kirish, 4 bob, xulosa, foydalanilgan adabiyotlar ro‘yxatidan iborat. Dissertatsiyaning hajmi 240 betni tashkil etadi.

DISSERTATSIYANING ASOSIY MAZMUNI

Kirish qismida ilmiy tadqiqot ishining dolzarbligi ilmiy asoslanib, muammoning o‘rganilganlik darajasi tavsiflangan. Tadqiqot ishining maqsadi va vazifalari, ob’yekti va predmeti aniqlangan, tadqiqot ishining fan va texnologiyalarni rivojlantirishning muhim yo‘nalishlariga mosligi asoslab berilgan. Shuningdek, tadqiqot ishining ilmiy yangiligi, natijalarning ishonchliligi, ishning nazariy va amaliy ahamiyati, erishilgan natijalarning amaliyotga joriy etilishi, natijalarning ilmiy ishlarda e’lon qilinganligi, ishning tuzilishi borasida ma’lumotlar keltirilgan.

Dissertatsiyaning “**Axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishni rivojlantirishning ilmiy-nazariy asoslari”** deb nomlangan birinchi bobida axborot xavfsizlik va kiberxavfsizlikni rivojlantirishning ilmiy-metodologik asoslari, o‘ziga xos differensial xususiyatlari mohiyati, axborot xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning metodik ta’minoti tavsifi bayon qilingan.

Bugungi kunda har bir soha vakili – rahbarlar, xodimlar, o‘quvchilar, talabalar hamda barcha yoshlar uchun ijtimoiy tarmoqlar, kompyuter texnologiyalari bilan ishlash, ulardan axborot izlash va foydalanish odatiy holga aylangan. Shu sababli, axborot tizimlaridan samarali foydalanish, sohaga tegishli ma’lumotlarni izlash va ulardan foydali maqsadlar yo‘lida foydalanish muhim ahamiyatga ega. Buning natijasida insonning dunyoqarashi, badiiy tafakkuri, nutqiy qobiliyati va ilmiy-intellektual salohiyati rivojlanib, kundalik faoliyatning turli sohalarida axborotlashtirish jarayonining ahamiyati ortib boradi. Bu esa zamonaviy voqelikdan xabardor bo‘lish imkonini yaratadi. Umuman olganda, kasbiy va shaxsiy hayotda axborot bilan samarali ishlash mazkur sohaning rivojiga ijobiy ta’sir ko‘rsatadi. Shu bois, axborot izlash jarayonida uning ishonchliligi, foydaliligi va samaradorligi kabi jihatlarga e’tibor qaratish muhimdir. Shuningdek, aniq maqsadlarga yo‘naltirilgan ma’lumotlarning xavfsizligiga ham alohida e’tibor berish lozim.

Davlatimizning axborot xavfsizligini ta’minlash sohasida olib borayotgan siyosati bugungi kungacha davom etayotganligini amalda qabul qilinayotgan yangi qonun hujjatlari misolida ham ko‘rishimiz mumkin. O‘zbekiston Respublikasi Prezidentining 2017-yil 7-fevraldagi PF-4947-son Farmoni bilan tasdiqlangan “2017-2021 yillarda O‘zbekiston Respublikasini rivojlantirishning beshta ustuvor yo‘nalishi bo‘yicha “Harakatlar strategiyasi”ning “Xavfsizlik, millatlararo totuvlik va diniy bag‘rikenglikni ta’minlash hamda chuqur o‘ylangan, o‘zaro manfaatli va amaliy tashqi siyosat sohasidagi ustuvor yo‘nalishlar” deb nomlangan beshinchi ustuvor yo‘nalishida axborot xavfsizligini ta’minlash va axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o‘z vaqtida va munosib qarshilik ko‘rsatish masalasi alohida yo‘nalish sifatida belgilanib, bunda talabalar ongiga tahdid soluvchi axborot xurujlarining oldini olish, talabalardan internet va boshqa axborot resurslaridan foydalanish madaniyatini shakllantirishga qaratilgan seminar treninglar tashkil qilishga alohida e’tibor qaratilgan.

Shu o‘rinda yurtimizda olimlarimizdan B.Xodjayev, M.Qurbonovlar o‘zining tadqiqotida axborot xurujlari, axborot xurujidan saqlanish texnologiyalari, O.G‘.Davlatov “Talabalarda axborot xavfsizligini ta’minlash kompetentligini tarixiy-madaniy meros vositasida rivojlantirish” mavzusidagi tadqiqotida: “Axborot xuruji

yoki tahdidi – bu axborot sohasida shaxs, jamiyat va davlatning hayotiy muhim manfaatlariga xavf tug‘diruvchi sharoit va omillar yig‘indisidir”, deya ta’kidlaydi. Bunda axborot va uning xavfsizligini ta’minlashda, u bo‘yicha choralar majmuini ishlab chiqish zarur deb o‘ylaymiz.

Modomiki, axborot xuruji kuzatilayotgan ekan, axborot xavfsizligini ta’minlash muhim masalalardan biri hisoblanadi. S.K.G‘aniyev, M.M.Karimov, K.A.Tashayevlarning fikricha, “Axborot xavfsizligi – axborotning nomaqbul (axborot munosabatlarining tegishli subyektlari uchun) oshkor qilinishidan (konfidensialligining buzilishidan), yaxlitligining buzilishidan, sirqib chiqishidan, yo‘qotilishidan, modifikatsiyalanishidan yoki foydalanuvchanlik darajasining pasayishidan hamda noqonuniy tirajlanishidan himoyalanganligi bilan xarakterlanadi. Ushbu hodisalarning sababchisi tasodifiy ta’sirlar yoki buzg‘unchining (niyati buzuqning) atayin ruxsatsiz foydalanishi natijasidagi ta’sirlar bo‘lishi mumkin. A.H.Muxitdinovning ta’kidlashicha, ”Axborot xavfsizligi o‘zida shunday axborot tizimi holatini ifoda etadiki, bunda u tizim elementlari va tashqi muhit uchun ichki va tashqi tahdidlar paydo bo‘lishiga yo‘l qo‘ymay, ularning ta’siriga tura oladi”. A.Lukatskiyning e’tiroficha, “Axborot xavfsizligi muammosi ko‘rib chiqilar ekan, axborot xavfsizligiga tahdidlar kabi muhim jihatlarga batafsil to‘xtalish lozim. Negaki, aynan ular axborot xavfsizligini buzish manbai hisoblanadi. Axborot xavfsizligiga tahdid axborotning maxfiyligiga putur yetishiga, shuningdek, noqonuniy tarqalishiga olib kelish ehtimoli yuqori bo‘lgan xatti-harakatlar, jarayon va hodisalar sifatida belgiladi.

Yuqoridagi tahlillarga tayanib, axborot xavfsizligi – bu ma’lumotlarga ruxsatsiz kirish, ulardan foydalanish, oshkor qilish, buzish, o‘zgartirish, tadqiq qilish, yozib olish yoki yo‘q qilishning oldini olishga qaratilgan amaliyotdir. Ushbu umumiy tushuncha ma’lumotlarning har qanday shaklda – elektron yoki jismoniy holda bo‘lishidan qat’i nazar amal qiladi.

U.G‘ofurovning ta’kidlashicha, “axborot iste’moli madaniyati, eng umumiy ma’noda axborot oqimidan inson manfaatlari, kamoloti hamda jamiyat taraqqiyotiga xizmat qiluvchi ma’lumotlarni qabul qilish, saralash, tushunish va talqin etishga xizmat qiladigan bilim, qobiliyat va malakalar tizmini anglatadi. Axborotni himoya qilish – bu: axborotning fizik butunligini ta’minlash, ya’ni axborot elementlarini xalaqitlarga uchrashi va yo‘qolishiga yo‘l qo‘ymaslik; axborot butunligini saqlashda uning elementlarini almashtirishga (modifikatsiyaga) yo‘l qo‘ymaslik; mos vakolatlarga ega bo‘lmagan shaxslar yoki jarayonlar tomonidan axborotni ruxsat etilmagan holda olinishiga yo‘l qo‘ymaslik; egalariga uzatilayotgan resurslar faqatgina tomonlar kelishgan shartlarga mos ravishda ishlatilishiga ishonch hosil qilinishi kerak, demakdir.

Hind olimi Ujjwal Raoning fikricha, kiberxavfsizlik – bu kibermuhit va tashkilot va foydalanuvchi aktivlarini himoya qilish uchun ishlatilishi mumkin bo‘lgan vositalar, siyosatlar, xavfsizlik tushunchalari, xavfsizlik choralari, ko‘rsatmalar, xatarlarni boshqarish yondashuvlari, harakatlar, treninglar, eng yaxshi amaliyotlar, ishonch va texnologiyalar to‘plami. Tashkilot va foydalanuvchi aktivlariga ulangan hisoblash moslamalari, xodimlar, infratuzilma, dasturlar, xizmatlar, telekommunikatsiya tizimlari va kiber muhitda uzatiladigan yoki saqlanadigan ma’lumotlarning yig‘indisi

kiradi”. Hozirgi kundagi kiberxavfsizlik muammosi soha mutaxassislari tomonidan ilmiy-nazariy o‘rganish va o‘quv dasturiy-metodik ta’minot yaratish bo‘yicha muayyan darajadagi ishlar amalga oshirilgan. Kiberxavfsizlik, kibermuhofaza va unda himoya tizimini rivojlantirish metodikasi asosiy muammo sifatida qaralmoqda. Kibervaziyatdan xabardorlik va kibermuhitni monitoring qilish masalalari bilan M. Ekxart, U.Frank, J.S. Okolica va boshqalar bu masala yechimiga oid muammolar doirasida izlanishlar olib borilganliklari yoritilgan.

Yuqorida olimlar keltirgan fikrlardan kelib chiqqan holda, “Kiberxavfsizlik – bu barqaror, ishonchli va samarali tizim orqali ma’lumotlarni himoya qilish, nazorat qilish va oldini olish jarayonidir” degan mualliflik ta’rifi yaratdik.

Shuningdek, ushbu bobda axborot xavfsizligi va kiberxavfsizlikning o‘ziga xos xususiyatlari va differensial jihatlari, ayrim xalqaro standartlar (ISO/IEC 27001, NIST Cybersecurity Framework), kiberxavfsizlik lug‘aviy semantikasi (tasodifiy hamda maqsadli tahdidlar), axborot xavfsizligini ta’minlash muammosining dolzarbligi, axborot xavfsizligi va kiberxavfsizlik o‘rtasidagi asosiy farqlar, ularning ilmiy asoslari va funksional chegaralari tahlili, eng muhim bo‘lgan tushuncha (axborotning yaxlitligi, identifikatsiya, autentifikatsiya, avtorizatsiya, foydalanishni nazoratlash, mulklik huquqi)larning ilmiy ta’riflari keltirilib izohlangan.

Ushbu jarayonlar axborot xavfsizligi boshqaruvi tizimining ajralmas qismi bo‘lib, ma’lumotlarni himoya qilishda fundamental ahamiyat kasb etadi.

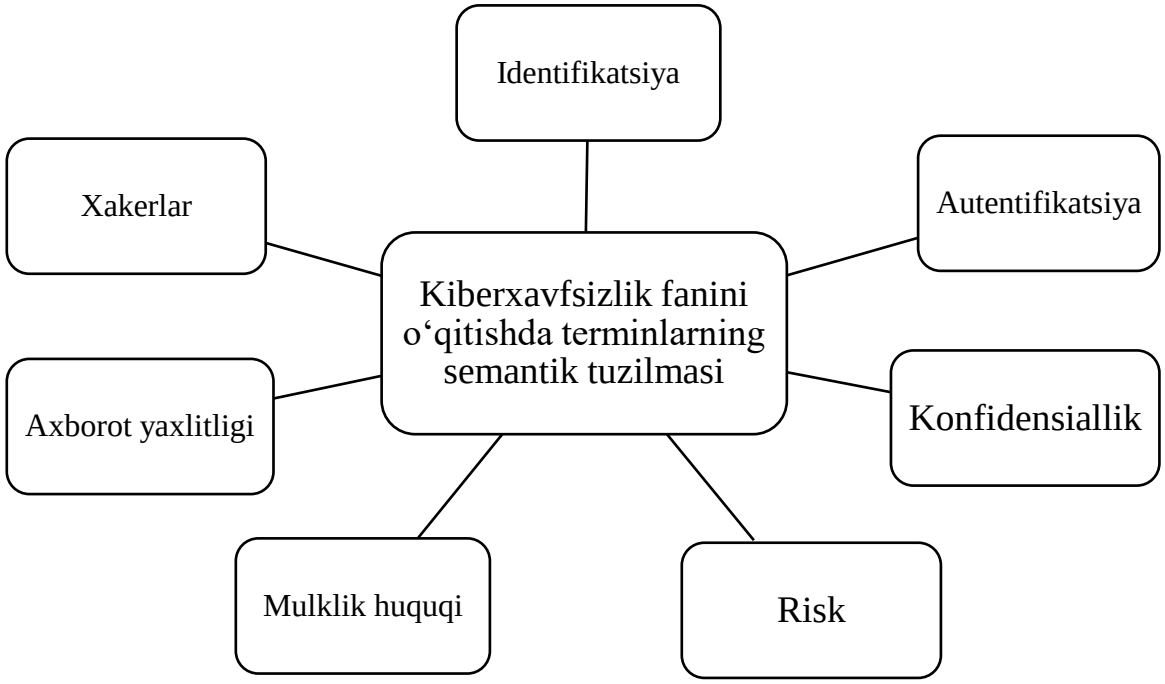
Kiberxavfsizlikni fundamental atamalarini aniqlashga turli yondashuvlar mavjud. Xususan, ba’zi mutaxassislar kiberxavfsizlikka oid atamalarga quyidagicha ta’rif berishgan:

“Konfidentsiallik jarayoni – axborot yoki uni eltuvchining shunday holati bo‘lib, undan ruxsatsiz tanishishning yoki nusxalashning oldi olinadi. Konfidensiallik jarayoni axborotni ruxsatsiz “o‘qish”dan himoyalash bilan shug‘ullanadi. Ayniqsa, bank sistemasida bank uchun konfidensiallik jarayoni juda muhim.

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. Axborot riski – bu korxonalarda axborot texnologiyalarini qo‘llash natijasida yuzaga kelishi mumkin bo‘lgan zarar yoki shikast yetishining ehtimollik darajasi. Shunday qilib, axborot risklari elektron tushunchalar va boshqa aloqa vositalari yordamida har qanday axborotni uzatish, saqlash, undan foydalanish bilan bog‘liq.

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 qayta ishlash jarayonida uning maxfiylik (konfidensiallik), yaxlitlik va foydalaniluvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalanlik holati. Kiberxavfsizlik sakkizta bilim sohasiga bo‘lingan: ma’lumotlar xavfsizligi; dasturiy ta’minot xavfsizligi; tashkil etuvchilar xavfsizligi; aloqa xavfsizligi; tizim xavfsizligi; inson xavfsizligi; tashkilot xavfsizligi; ijtimoiy xavfsizlik”.

Kiberxavfsizlik sohasini takomillashtirishda dasturiy-ta’minot yaratish mazkur fanning terminlarini, glossariy tuzish va mustaqil taqdimot yaratish vazifasi berilishi natijasiga yo‘naltiradi.



1-rasm. Kiberxavfsizlik fanini o‘qitishda terminlarning semantik tuzilmasi

S.K.G‘aniev, A.A.G‘aniev, Z.T.Xudoyqulov ”Kiberxavfsizlik asoslari” deb nomlangan o‘quv qo‘llanmasi nashr qilingan. O‘quv qo‘llanmada kiberxavfsizlik va uning asosiy tushunchalari, axborotning kriptografik himoyasi, foydalanishni nazoratlash, tarmoq xavfsizligi, foydalanuvchanlikni ta’minlash usullari, dasturiy vositalar xavfsizligi, axborot xavfsizligi siyosati va xavf-xatarlarni boshqarish, kiberjinoyatchilik, kiberhuquq, kiberetika hamda inson xavfsizligini nazariy va amaliy asoslarini qo‘llanilishi ifoda qilingan.

Axborot xavfsizligi va kiberxavfsizlik fanini o‘qitishda yana bir o‘quv obyekti bu B.Tahirov tomonidan tuzilgan “Axborot xavfsizligi asoslari” o‘quv qo‘llanmasidir. Mazkur o‘quv qo‘llanmada axborot tizimlari xavfsizligi fanining mazmuni, axborot xavfsizligining predmeti, audit mohiyati, uning maqsadi va vazifalari, axborot xavfsizligini ta’minlashning asosiy tushunchalari, tahdidlar, himoya usullari, kiberxavfsizlik va kiberhujumlardan himoyalanish bosqichlari, shularga tegishli tushunchalar tahlili va atamalar izohi, axborot xavfsizligini ta’minlashning asosiy dasturiy va texnik vositalari yuzasidan mavzular va nazariy ma’lumot, soha mutaxassislarining ilmiy qarashlari, tahliliy yondashuvlar, va tadqiqiy xulosalar yoritilgan. Qo‘llanmadagi I bobga tegishli axborotni xavfsizligi, kiberjinoyatchilik va axborotga tahdidlar mavzusida axborot xavfsizligi, maxfiy axborot, hujjatlashtirilgan axborot, konfidensial axborot kabi lug‘aviy birliklar izohlari ifoda qilingan. Axborotni muhofaza qilish – axborot xavfsizligining (ma’lumotlarning butunligi, foydalana olish va zarur bo‘lganda, ma’lumotlarni kiritish, saqlash, qayta ishlash va uzatishda foydalaniluvchi axborot va uning zahiralari konfedensialligi) muhim jihatlarini ta’minlashga yo‘naltirilgan tadbirlar majmuidir. Xavfsiz tizimda tegishli apparat va

dasturiy vositalardan foydalanib, axborotni o‘qish, yozish, hosil qilish va o‘chirish huquqiga ega shaxslar yoki ular nomidan amalga oshiradigan jarayonlar orqali axborotdan foydalana olish boshqariladi. Shuningdek, Axborot himoyasi konsepsiyasini ishlab chiqish bosqichlari tavsifi o‘rin egallagan.

1- bosqich. Himoyalanuvchi obyekt qiymatini aniqlash;

2- bosqich. Buzg‘unchining bo‘lishi mumkin bo‘lgan harakatlarini tahlil qilish;

3-bosqich. Axborotni himoyalash vositalarini baholash.

Axborotni himoyalash konsepsiyasi himoyalanish obyekti bo‘lishi va unda kerakli, zaruriy o‘quv materiali joylashtirilgan bo‘lishi ayni muddaodir. Shu nuqtayi nazardan obyekt yonida axborotni himoyalash vositalari va ularning mexanizmini baholash muhim tajribalardan biri.

Shunday qilib, “Kiberxavfsizlik asoslari” fanini o‘qitish jarayonini kompleks tarzda takomillashtirish, uning metodik ta’minotini innovatsion texnologiyalar va xalqaro standartlar asosida ishlab chiqish hamda xavfsizlik siyosati, huquqiy asoslar va amaliy qo‘llash usullari bilan boyitish raqamli infratuzilmaning himoyalanganligi va barqarorligini ta’minlashda muhim omil hisoblanadi.

Dissertatsiya ishining **“Axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishning konseptual mazmuni”** deb nomlangan ikkinchi bobida “Kiberxavfsizlik asoslari” fanini o‘qitishda tushunchalar tahlilining semantikasi, dasturiy-ta’minotini rivojlantirishda axborot tizimining xususiyatlari, fanni o‘qitishda kasbiy rivojlanishning o‘ziga xosligi ko‘rib chiqilgan.

Ta’lim sohasida ijtimoiy-iqtisodiy taraqqiyotiga munosib hissa qo‘shuvchi yuqori malakali mutaxassislar tayyorlash, elektron ta’lim nazariyasi va metodikasi yanada takomillashtirilishini ta’minlash, mamlakatga kasbiy malakaga ega kadrlar tayyorlash, o‘quv mashg‘ulotiga innovatsion metodlar va ilg‘or texnologiyalarni tatbiq qilish asosiy vazifalardan biri sanaladi. Bunda axborotlar bilan ishlash va ulardan foydalanish, kiberxavfsizlik talablarini o‘rgatish asosiy o‘rin egallaydi. Shuningdek, O‘zbekiston Respublikasi Qonunchilik palatasining 2022-yil 15-aprelda “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonuni qabul qilingan. Ushbu Qonunda kiberxavfsizlikni ta’minlashning asosiy prinsiplari belgilangan bo‘lib, ular quyidagilar: qonuniylik; kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi; kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv; kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi; O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi yuzasidan qator vazifalar belgilab berilgan.

Ma’lumki, innovatsion rivojlanish davrida zamonaviy yangi texnologiyalar, elektron xizmatlar bizning kundalik hayotiy faoliyatimizning ajralmas qismiga aylanganining guvohi bo‘lmoqdamiz. Ta’lim tizimi va o‘quv jarayonida yuqori tezlik bilan axborot kommunikatsiya va informatsion yondashuvlarni me’yoriy amal qilish va ularni himoya qilish hamda ulardan foydalanish, samara beruvchi maqsadlarga yo‘naltirish muhim ahamiyatga ega bo‘lib, dolzarb masalaga aylanmoqda. Xususan, bu borada har bir tashkilot, korxona, muassasa uchun kiberxavfsizlikni ta’minlash maqsadida mazkur soha bilan shug‘ullanuvchi xodimlar jalb qilinmoqda hamda xodimlarni kiberxavfsizlikka oid bilimlar bilan doimiy tanishtirib borish uchun qator

seminar trening mashg‘ulotlari tashkil etilmoqda. Shuni ham aytib o‘tish joizki, oliy ta’lim muassasalarida ham kiberxavfsizlikni fan sifatida o‘qitilishi, bu fanning o‘rganilish maqsad va vazifalari belgilab berilgan. Axborot xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish muhim ahamiyat kasb etadi. O‘zbekiston Respublikasi Prezidentining, 2021 yil 17 fevraldagi PQ-4996-son qarorida qator vazifalar belgilab berilgan. Bir qator ilg‘or davlatlarning sun’iy intellekt sohasidagi milliy strategiyalarini tahlil qilish mamlakatimiz uchun ustuvor yo‘nalish sifatida quyidagi beshta yo‘nalishni ajratib ko‘rsatish imkonini beradi: sun’iy intellekt sohasida fundamental amaliy tadqiqotlar o‘tkazish - matematik usullardan foydalangan holda yangi sun’iy intellekt algoritmlarini yaratish; sun’iy intellekt injiniringini rivojlantirish - fundamental amaliy tadqiqotlar natijasida olingan algoritmlarni turli amaliy muammolarni hal qilishda qo‘llash, yangi dasturiy ta’minot va texnologik yechimlarni ishlab chiqish; ma’lumotlar – ularni yig‘ish, saqlash, qayta ishlash va optimallashtirish (algoritmlarni o‘rgatish uchun); kadrlar tayyorlash – sun’iy intellekt sohasida yuqori malakali ilmiy kadrlar va mutaxassislarni tayyorlash, yangi ta’lim dasturlarini yaratish; qonunchilik bazasi – sun’iy intellekt texnologiyalarini rivojlantirishni qo‘llab-quvvatlovchi qonunlar, standartlar va axloqiy qoidalarni ishlab chiqish va amalga oshirish.

Kiberxavfsizlik siyosati kiberxavfsizlik maqsadlariga erishish strategiyasini ifodalaydi va uning tarkibiy qismlariga kiberxavfsizlik choralaridan to‘g‘ri foydalanish bo‘yicha ko‘rsatmalar beradi. Yo‘nalish ijtimoiy kelishuv yoki boshqaruv organi tomonidan belgilanishi mumkin. Biz, shuningdek, mustaqil korxonalar kiberxavfsizlik strategiyasini qo‘llab-quvvatlash uchun boshqaruv ko‘rsatmalarini o‘rnatishi kerakligini tan olamiz va biz o‘zgartirilgan “korxona siyosati” atamasidan faqat ma’lum bir korxona hamjamiyatida amal qiladigan siyosatlarga ishora qilish uchun foydalanamiz. Odatda bunday korporativ siyosat ko‘pincha Xalqaro Standartlashtirish Tashkiloti (ISO) (ISO/IEC 2005 a,b) va NIST (Ross, Katzke va boshq. 2007) tomonidan o‘rnatilgan kiberxavfsizlik standartlariga asoslanadi. Bunday standartlar odatda texnologik nazorat bo‘yicha tavsiyalar bilan texnologik yo‘riqnomaning kombinatsiyasini o‘z ichiga oladi kabi jihatlar to‘xtalgan.

Kiberxavfsizlik ta’limining samaradorligi nafaqat texnologik bilimlarga asoslangan, balki asosiy tushunchalar tahlilining semantik jihatdan to‘g‘ri va izchil yoritilishi bilan ham bevosita bog‘liqdir. Semantika – bu tushunchalarning mazmunini, ularning kontekstual ishlatilishini va turli fanlar hamda texnologiyalar bilan o‘zaro bog‘liqligini o‘rganish bilan shug‘ullanadi. Kiberxavfsizlik doirasidagi terminlar xalqaro axborot xavfsizligi standartlari, huquqiy meyorlar, texnik regulativ hujjatlar hamda ilmiy adabiyotlar bilan uyg‘un holda tahlil qilinishi kerak.

Mazkur fan bo‘yicha ta’lim jarayonida semantik tahlil quyidagi asosiy tamoyillarni qamrab olishi lozim:

Tizimlilik – kiberxavfsizlik tushunchalarining turli kontekstlarda qo‘llanilishi va ularning axborot texnologiyalari ekotizimidagi o‘rnini aniqlash.

Terminologik izchillik – kiberxavfsizlik bilan bog‘liq atamalarni xalqaro miqyosda qabul qilingan standartlarga moslashtirish va ularni milliy ta’lim tizimiga integratsiya qilish.

Strukturaviy yondashuv – kiberxavfsizlik konseptlarini kriptografiya, autentifikatsiya jarayoni, tarmoq xavfsizligi, kiberjinoyatchilik va huquqiy aspektlarni turli yo‘nalishlarga ajratib o‘rganish.

Nazariy jihatdan, kiberxavfsizlik tushunchalarining semantik tahlili fan va texnologiyalar o‘rtasidagi o‘zaro bog‘liqlikni tushunishga, shuningdek, talabalar va mutaxassislar uchun terminlarning aniq va tushunarli bo‘lishini ta’minlashga xizmat qiladi.

Kiberxavfsizlik bo‘yicha tushunchalarni semantik jihatdan chuqur anglash ularni amaliyotga tatbiq etishda ham muhim ahamiyatga ega. Amaliy ta’lim jarayonida quyidagi metodlar samarali hisoblanadi:

Interaktiv o‘qitish usullari – talabalarga kiberxavfsizlikning asosiy tushunchalarini virtual laboratoriyalar, simulyatsiyalar va real kiberhujumlar tahlili orqali tushuntirish.

Case-study va real voqealar tahlili – amaliyotda yuz bergan kiberhujum holatlarini chuqur o‘rganish va ular bilan bog‘liq terminlarning semantik tahlilini olib borish.

Kompyuter xavfsizligi protokollarini modellashtirish – kriptografiya, autentifikatsiya va avtorizatsiya kabi jarayonlarning dasturiy ta’minot doirasida qanday ishlashini vizualizatsiya qilish.

Xalqaro standartlarga asoslangan terminologiya tizimi – ISO/IEC 27001, NIST Cybersecurity Framework, GDPR, OWASP kabi xalqaro axborot xavfsizligi standartlariga mos keladigan tushunchalarni milliy ta’lim tizimiga integratsiya qilish.

Amaliy jihatdan yondashilsa, kiberxavfsizlik tushunchalarini semantik jihatdan to‘g‘ri tahlil qilish orqali foydalanuvchilarning xavfsizlik xulq-atvori, axborotni muhofaza qilish bo‘yicha malaka va ko‘nikmalari oshiriladi. Ayniqsa, zamonaviy sun’iy intellekt va mashinaviy o‘rganish algoritmlariga asoslangan tahdidlarni aniqlash va oldini olish usullarida to‘g‘ri terminologiya va tushuncha tahlili muhim rol o‘ynaydi.

“Kiberxavfsizlik asoslari” fanining samarali o‘qitilishi va tushunchalar tahlili uchun semantik yondashuv muhim ahamiyatga ega. Semantik tahlil tushunchalarning mazmunini, ularning texnologik, huquqiy va strategik kontekstlarda qo‘llanilishini tahlil qilishga yordam beradi. “Kiberxavfsizlik asosi” fanida ishlatiladigan kiberxavfsizlik, axborot xavfsizligi, kriptografiya, tarmoq xavfsizligi, kiberjinoyatchilik, kibertahdidlar, kiberhujumlar, identifikatsiya va autentifikatsiya jarayoni, vakolat berish, foydalanishni nazorat qilish, axborot xavfsizligi siyosati, kiberetika, kiberhuquq, kiberhimoya vositalari. xavf-xatarlarni boshqarish, xavfsizlik tahlili va auditi, axborot aktivlarini himoya qilish. sun’iy intellekt va kiberxavfsizlik kabi asosiy tushunchalar mazmuniga e’tibor qaratildi.

“Kiberxavfsizlik asoslari” fanini o‘qitishda semantik tahlil o‘quv jarayonining muhim tarkibiy qismi hisoblanadi. Tushunchalarni to‘g‘ri va izchil o‘rganish, ularni xalqaro va milliy standartlarga mos ravishda talqin qilish orqali talabalarning axborot xavfsizligi bo‘yicha fundamental bilim va amaliy ko‘nikmalarini rivojlantirish mumkin. Shu bilan birga, amaliy mashg‘ulotlar, simulyatsiyalar va tahliliy tadqiqotlar orqali bu tushunchalarni mustahkamlash kiberxavfsizlik fanlarining samaradorligini oshirishga xizmat qiladi.

Yuqoridagi keltirilgan ta’rifga ko‘ra, axborot tizimlarining kiberxavfsizlik nuqtayi nazaridan asosiy xususiyatlarga (tuzilmaviy murakkablik, ko‘p darajali xavfsizlik modeli, axborotga kirish va vakolatni boshqarish, axborotning yaxlitligi va konfidensialligi, tarmoq xavfsizligi va trafik monitoring, xavfsizlikni auditi va tahdidlarni monitoring qilish) ajratildi.

“Kiberxavfsizlik asoslari” fanining dasturiy-ta’minotini rivojlantirishda axborot tizimining o‘rni salmoqli. “Axborot tizimi(AT) — axborotni saqlash, qidirish va qayta ishlash uchun mo‘ljallangan, axborotni ta’minlovchi va tarqatuvchi hamda tegishli tashkiliy resurslar (inson, texnik, moliyaviy va boshqalar) tizimidir”. Kompyuter axborot tizimi esa— axborotni qayta ishlovchi yoki sharhlovchi odamlar va kompyuterlardan tashkil topgan tizim hisoblanadi.

Zamonaviy kompyuter tizimlari va ularning tarmoqlaridan foydalanish axborotni ko‘rib chiqish, ma’lum matnlarni nusxalash, maxsus dasturiy va apparat resurslari bilan ishlash, turli xil xabarlarni qabul qilish kabi talablarni o‘z ichiga oladi. Shu bilan birga, kiberxavfsizlik soha bo‘yicha ta’lim berish jarayonini takomillashtirish, xususan, dasturiy-metodik ta’minotni rivojlantirish muhim omillardan biri hisoblanadi. Tadqiqot davomida axborot xurujlari davrida “Kiberxavfsizlik asoslari” fanini o‘qitish metodikasini takomillashtirish uchun internet resurslaridan foydalangan holda kasbiy rivojlanish metodlarini ilgari surish, bu jarayonda interaktiv yondashuvni tatbiq etish va ilmiylik hamda ko‘rsatmalilik tamoyillariga ustuvorlik berish asosiy maqsad sifatida belgilandi.

Bizning fikrimizcha, axborot xurujlari muhitida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini rivojlantirishda yuqori natijaviylikka erishish uchun axborotni uzatish va yig‘ishning zamonaviy usullarini yaratish, elektron axborot xavfsizligi bo‘yicha intellektual va ijodiy salohiyatni rivojlantirish, pedagogik mahorat va texnologik vositalardan samarali foydalanish kabi yo‘nalishlar dolzarb ahamiyat kasb etadi. Shuningdek, mustaqil kasbiy tafakkurni shakllantirish va o‘z-o‘zini rivojlantirish imkoniyatini beruvchi akmetexnologiyalarni ishlab chiqish ham ushbu jarayonning ajralmas qismi hisoblanadi.

Ushbu bobda Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini rivojlantirishda muhim yondashuvlar (kompetensiyaviy yondashuv nazariyasi, konstruktivistik o‘qitish nazariyasi, tajriba asosida o‘qitish nazariyasi, bloom taksonomiyasi va kiberxavfsizlik ta’limi, o‘zaro ta’sirli o‘qitish nazariyasi)ga to‘xtalgan. Yuqorida keltirilgan yondashuvlar asosan, kasbiy rivojlanishning o‘ziga xosligini amaliyot bilan uyg‘unlashgan holda kompetensiyaviy, konstruktivistik o‘qitish, tajriba asosida o‘qitish, Bloom taksonomiyasiga asoslangan bosqichma-bosqich o‘qitish, interaktiv o‘qitish kabi yondashuvlar asosida tashkil etish maqsadga muvofiqligi o‘rganilib chiqilgan. Shu sababli, kiberxavfsizlik bo‘yicha mutaxassis tayyorlashda an’anaviy ta’lim usullari bilan bir qatorda, interaktiv va amaliy yondashuvlar qo‘llanilishi muhimdir. Ushbu ilmiy nazariyalarning integratsiyalashuvi zamonaviy kibermuhit talablariga javob beradigan yuqori malakali mutaxassislarni tayyorlash imkonini beradi.

Shuningdek, kiberxavfsizlik asoslari fanini o‘qitishda shaxsiy va kasbiy o‘zini o‘zi rivojlantirish komponentlari mantiqiy faoliyat sxemasiga ketma-ketlikda mos keladi: ichki motivatsiyani shakllantirish va o‘z-o‘zini rivojlantirish jarayonini

loyihalash; individual kasbiy rivojlanish trayektoriyasiga muvofiq harakatlarni bajarish; shaxsiy va kasbiy o‘z-o‘zini rivojlantirish jarayoni natijalariga asoslangan aks ettirish va tuzatuvchi harakatlarni amalga oshirishdan iboratligi bayon qilingan.

Dissertatsiya ishining **“Axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish”** deb nomlangan uchinchi bobida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish modeli, didaktik tamoyillar ishlab chiqilgan texnologiya va rivojlantirishning innovatsion metodlari ifoda qilingan.

O‘quv jarayonida pedagogik, metodik, psixologik, texnik, tashkiliy imkoniyatlarni o‘rganish obyekti zamonaviy texnologiyalar ta’lim muhitini tubdan o‘zgarishlar bilan chambarchas bog‘liq.

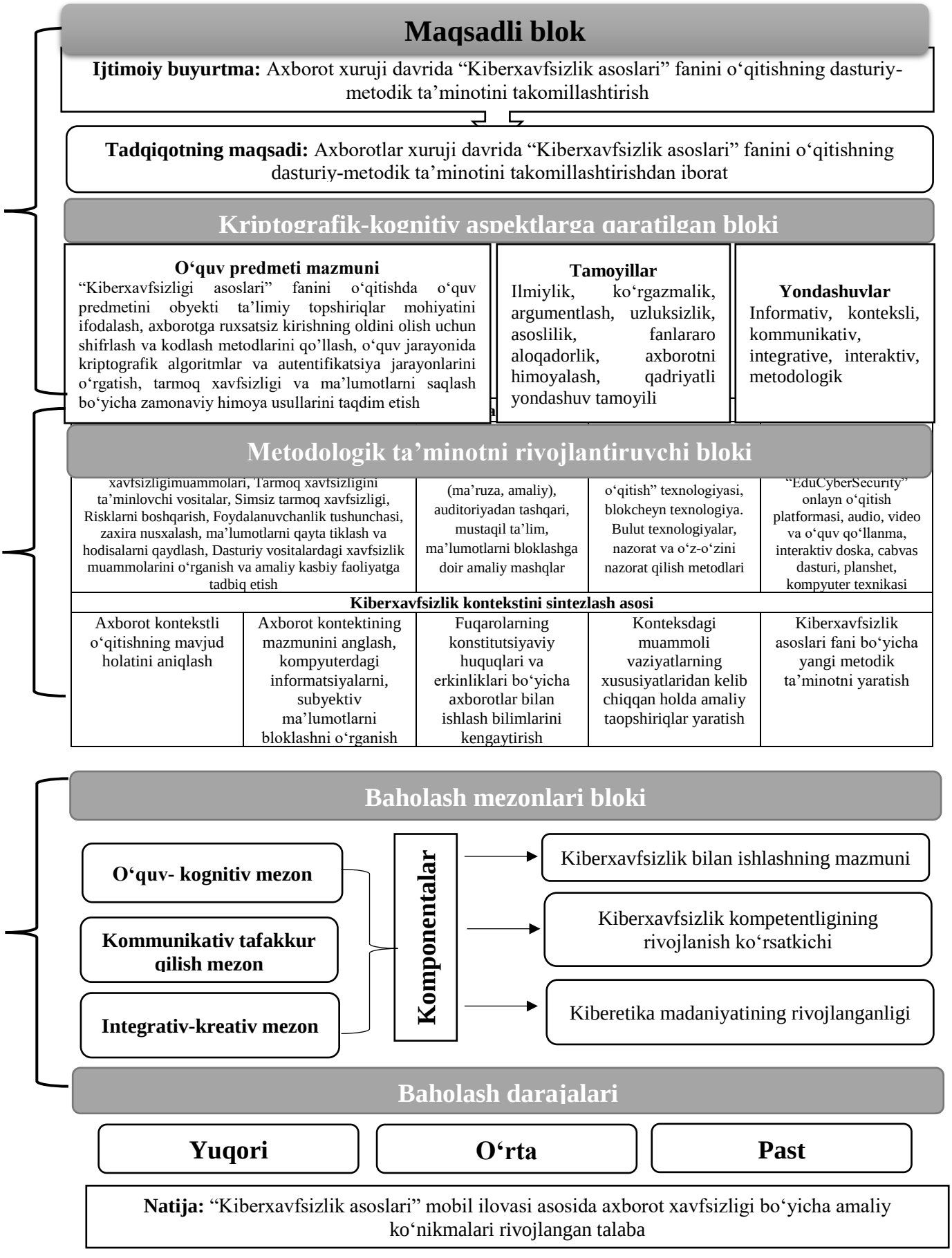
Olib borilgan ilmiy tadqiqot va tahliliy kuzatuvlar natijalariga ko‘ra, axborot xurujlari sharoitida “Kiberxavfsizlik asoslari” fanini o‘qitish jarayonida dasturiy-metodik ta’minotni takomillashtirish quyidagi tarkibiy elementlarga tayanuvchi uzviy tizimni shakllantirishni taqozo etadi: o‘quv-metodik tamoyillar, o‘qitish prinsiplari, baholash mezonlari, ta’limiy tendensiyalar hamda rivojlantirish modellari. Bu komponentlar kiberxavfsizlik ta’limi mazmunini shakllantirish, o‘qitish sifatini oshirish va o‘quv jarayonining samaradorligini ta’minlashga xizmat qiluvchi asosiy vositalar sifatida qaraladi. Shu tariqa, mazkur fan doirasida ilg‘or ta’limiy yondashuvlar va texnologiyalarni joriy etish orqali o‘qitishning zamonaviy metodologik bazasini yaratish imkoniyati yuzaga keladi

Talabalarda axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishda kiberxavfsizlik terminlarining konseptual asoslarini va ularning amaliy tatbig‘i va kompyuter ma’lumotlaridan foydalanishda shaxsiy-kasbiy, kreativ-mantiqiy, individual kasbiy rivojlanish, psixologik o‘sish qobiliyatlari o‘qitishning bosh maqsadi sanaladi.

Talaba yoshlarda axborot etikasiga asoslangan, jamiyat, inson uchun foydali, axborot bilan ishlashda fuqarolarning konstitutsiyaviy huquqlari va erkinliklarini inobatga olish, intellektual mulk obyektlariga tahdid qilmaslik, milliy ma’naviy merosni saqlash, ma’naviy-insoniy an’analarni rivojlantirish, axloq-odob meyorlarini targ‘ib qilish, huquqiy aksiologik bilimlarni o‘stirish singdirilishi dolzarb mazmun kasb etadi. O‘quv-metodik ta’minot yaratishda zamonaviy informatsion texnologiyalarini taraqqiy etishini izohlash, fanga doir ustuvor tamoyillar, prinsiplar ilmiylik potensialini rivojlantirish muhitini yaratish va bu jihat biz tomonimizdan yaratilgan modelda ifodalangan.

Axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish modeli to‘rt blokni o‘z ichiga oladi. Bular: kognitiv-grammatik yondashuvlarga qaratilgan blok, kontekstli-informativ aspektlarga oid blok, metodologik ta’minotini rivojlantiruvchi blok, baholash mezonlari bloki kabi komponentlardan iborat. Modelning kriptografik-kognitiv aspektlarga qaratilgan blokda ishlov berilayotgan va uzatilayotgan axborotlarga noqonuniy kirishni oldini oluvchi shifrlash va kodlashni tatbiq etish bo‘yicha o‘quv predmeti mazmuni, vazifalar, tamoyillarni qamrab oladi.

“Kiberxavfsizlik asoslari” fanini o‘qitish jarayonida talabalar kiberetika madaniyatini shakllantirish modeli axborot xavfsizligini ta’minlashning dolzarb muammolarini darajalash, axborot va kiberxavfsizlikning o‘ziga xos differensial



2-rasm. Axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish modeli

xususiyatlarini kolloboratsiyalash hamda global muammolar yechimini tizimli-tuzulmaviy tahlil qalish va argumentlash, uzluksizlik, fanlararo aloqadorlik tamoyillarini informativ, kontekstli, integrativ, faoliyatli yondashuvlarga maqsadli uygunlashtirish asosida takomillashtirilgan bo‘lib, unda talaba yoshlarning axborot etikasiga asoslangan bilim va ko‘nikmalarini shakllantirish, jamiyat va inson manfaatlariga mos ravishda axborot bilan ishlash tamoyillarini o‘zlashtirish, shuningdek, fuqarolarning konstitutsiyaviy huquq va erkinliklarini inobatga olish, intellektual mulk obyektlariga zarar yetkazmaslik kabi masalalar bugungi kunda dolzarb ahamiyat kasb etmoqda. Shu bilan birga, milliy ma’naviy merosni saqlash, insoniy qadriyatlar va an’analarni rivojlantirish, axloqiy-meyorlarni targ‘ib qilish hamda huquqiy va aksiologik bilimlarni oshirish talabalar uchun muhim yo‘nalishlardan biridir.

Zamonaviy informatsion texnologiyalar taraqqiyoti axborot xavfsizligini ta’minlash bilan bog‘liq muammolarni yanada chuqur o‘rganishni talab qiladi. Shu sababli, fan doirasida ilmiy tamoyillar va ustuvor prinsiplarni rivojlantirish, metodik ta’minotni modernizatsiya qilish hamda innovatsion ta’lim muhitini shakllantirish dolzarb hisoblanadi. Ushbu jihatlar biz tomonidan ishlab chiqilgan modelda aks ettirilgan.

Axborot xurujlari tahdidi ortib borayotgan sharoitda “Kiberxavfsizlik asoslari” fanini o‘qitish metodikasini takomillashtirish uchun ishlab chiqilgan model to‘rtta asosiy blokni o‘z ichiga oladi:

Kriptografik-kognitiv aspektlarga qaratilgan bloki – axborot xavfsizligining asosiy tushunchalari, nazariy tamoyillari va huquqiy asoslarini shakllantirish bo‘yicha ta’lim jarayonini tashkil etadi.

Konfedensiallik, riskni boshqarishga oid bloki – kiberxavfsizlik bo‘yicha amaliy mashg‘ulotlar, real muammolar va masalalarni tahlil qilish hamda talabalarning axborot xavfsizligiga oid bilimlarini kengaytirish vazifalarini qamrab oladi.

Metodologik ta’minotni rivojlantiruvchi bloki – o‘qitishning zamonaviy texnologiyalarini qo‘llash, o‘quv jarayonining interaktiv usullari, tajriba asosida o‘qitish va mustaqil ta’lim traektoriyalarini shakllantirishga yo‘naltirilgan metodikalar asosida tashkil etiladi.

Baholash mezonlari bloki – talabalar kiberxavfsizlik bo‘yicha bilim va amaliy ko‘nikmalarini aniqlash, ularning refleksiv fikrlash qobiliyatini baholash va ularning kasbiy rivojlanishini kuzatib borish tizimini o‘z ichiga oladi.

Modelning kriptografik-kognitiv aspektlarga qaratilgan blokida axborotlarni himoya qilish texnologiyalariga alohida e’tibor qaratilgan.

Ushbu blokda o‘quv pedagogik jarayonda “Kiberxavfsizlik asoslari” fanini o‘qitishda o‘quv predmetini obyekti ta’limiy topshiriqlar mohiyatini ifodalash, axborotga ruxsatsiz kirishning oldini olish uchun shifrlash va kodlash metodlarini qo‘llash, o‘quv jarayonida kriptografik algoritmlar va autentifikatsiya jarayonlarini o‘rgatish, tarmoq xavfsizligi va ma’lumotlarni saqlash bo‘yicha zamonaviy himoya usullarini tatbiq etish masalalari va boshqalar singdirib o‘tilgan.

Shu bilan birga, axborot xavfsizligiga oid asosiy tamoyillar, yondashuvlar, o‘quv fanining mazmuni va asosiy vazifalari mazkur model doirasida keng qamrovli tarzda yoritilgan. Ushbu metodologik yondashuv talabalarning axborot bilan ishlash

madaniyatini oshirish, intellektual mulkni himoya qilish tamoyillarini o‘zlashtirish va kiberxavfsizlik bo‘yicha amaliy ko‘nikmalarga ega bo‘lishlarini ta’minlashga xizmat qiladi.

Xalqaro va mahalliy ilmiy tadqiqotlar hamda me’yoriy hujjatlar tahlili natijalarini umumlashtirish orqali axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishda talabalarning axborotlardan ijobiy maqsadga yo‘naltirib foydalanish va ularning mustaqil va uzluksiz shaxsiy- metodik rivojlanishi yuqori darajada samarali amaliyotga joriy etish uchun quyidagi didaktik tamoyillar ishlab chiqildi.

“Kiberxavfsizlik asoslari” fanini o‘qitish jarayonini takomillashtirish va uning metodik-dasturiy ta’minotini rivojlantirish bir qator fundamental tamoyillarga asoslanadi. Ushbu tamoyillar ilmiylik, ko‘rgazmalik, argumentlash, uzluksizlik, asoslilik, fanlararo aloqadorlik, axborotni himoyalash, kiberetika va qadriyatli yondashuvlarini o‘z ichiga oladi.

Argumentlash tamoyili. Ushbu tamoyil asosida talabalar o‘quv jarayonida o‘rganilgan bilimlarni asoslash, dalillar bilan mustahkamlash, mantiqiy izchillikda fikr yuritish va nuqtayi nazarni asosli tarzda himoya qilishni o‘rganadilar. Har qanday fikr yoki taklif aniq dalil, fakt, tajriba yoki nazariy asosga tayangan bo‘lishi kerak. Argumentlash jarayoni muloqot, bahs yoki muhokama shaklida bo‘lib, bunda fikrlar sintezlanadi va aniqlashtiriladi. Shu nuqtayi nazaridan, dasturiy ta’minotimizda keltirilgan mavzular o‘zaro bog‘liq, mantiqiy ketma-ketlikda bayon etilgan. Natijada, talabalarning tanqidiy va mantiqiy fikrlash ko‘nikmalarini rivojlantirish, mustaqil qaror qabul qilish va uni asoslash ko‘nikmalari rivojlanadi. Darsda o‘z fikrini aniq va dalillarga tayangan holda ifodalashni o‘rgatadi.

Shunday qilib, argumentlash tamoyili asosida talabalar har qanday fikr, g‘oya yoki yechimni asosli, dalillarga tayangan va mantiqiy tarzda ifodalash ko‘nikmalari rivojlanadi.

Ko‘rgazmalik tamoyili. Talabalarning “Kiberxavfsizlik asoslari” fanini mukammal o‘zlashtirishi, o‘qitish jarayonida o‘quv materialini ko‘rish, eshitish, tajriba qilish orqali tushunarli, ta’sirchan va esda qoladigan shaklda yetkazishga asoslangan. “Kiberxavfsizlik asoslari” fanini dasturiy ta’minot asosida infografika, prezentatsiya, grafik illyustratsiyalar, simulyatsiyalar orqali nazariy bilimlarni amaliy ko‘rsatishga mo‘ljallangan. Natijada talabalarning tafakkurini jonlantiradi, faol ishtirokini ta’minlaydi va bilimlarni mustahkam egallashga xizmat qiladi.

Ilmiylik tamoyili. Talabalarning “Kiberxavfsizlik asoslari” fanini mukammal o‘zlashtirishi ushbu fanning ilmiy-nazariy hamda kasbiy metodologik asoslarini tizimli o‘qitish orqali amalga oshiriladi. Ilmiy bilish jarayoni olamdagi hodisalar, voqealar, obyektlar va ularning inson ongida aks etishi, shuningdek, qadriyatlarni anglash qonuniyatlarini tahlil qilish hamda ularni baholash mezonlarini aniqlash bilan bevosita bog‘liqdir.

Uzluksizlik tamoyili. Kiberxavfsizlik bo‘yicha ta’lim doimiy rivojlanish va axborot oqimining uzluksizligini ta’minlash orqali talabalar bilimini oshirishga qaratilgan. Axborot tahdidlari dinamik tarzda o‘zgarib borayotgan sharoitda ushbu fan muntazam ravishda takomillashtirilib, yangi tahdid va hujum modellari asosida boyitib borilishi lozim. Ushbu tamoyil kasbiy rivojlanish jarayonini tizimli tarzda yo‘lga

qo‘yish, axborot xavfsizligi bo‘yicha amaliy ko‘nikmalarni rivojlantirish va uzluksiz ta’lim sharoitida bilimlarni amaliyotga tadbiq qilishni ta’minlaydi.

Asoslilik tamoyili (fundamentallik). Mazkur tamoyil kiberxavfsizlik asoslari fanining nazariy asoslarini chuqur o‘rganish, uning huquqiy, texnik va amaliy jihatlarini to‘liq qamrab olishga yo‘naltirilgan. Bunda talabalar mustaqil ravishda kasbiy bilimlarini boyitish, axborot xavfsizligi bo‘yicha ilg‘or texnologiyalarni o‘rganish asnosida real amaliyotda qo‘llash imkoniyatiga ega bo‘ladilar.

Fanlararo aloqadorlik tamoyili. Kiberxavfsizlik sohasi faqatgina informatika yoki texnik fanlar bilan chegaralanib qolmay, balki matematika, fizika, huquqshunoslik, falsafa kabi fanlar bilan uzviy bog‘liq. Ushbu tamoyil quyidagilarni o‘z ichiga oladi: kiberxavfsizlikni o‘rganishda huquqiy va axloqiy mezonlarni tushunish; kriptografiya, kodlash va axborot himoyasi bo‘yicha matematik usullarni tadbiq qilish; axborot texnologiyalari bilan bog‘liq muammolarni hal qilishda turli fanlarning integratsiyalashuvi.

Xalqaro tajribalarga ko‘ra, elektron va axborot-didaktik vositalarni joriy qilish orqali turli geografik hududlardan ta’lim oluvchilarning interaktiv muloqotini tashkil etish pedagogik samaradorlikni oshirishga xizmat qiladi.

Axborotni himoyalash tamoyili. Bu tamoyil axborot xavfsizligini ta’minlash, ma’lumotlarni shifrlash va kodlash orqali ularning maxfiyligini himoya qilishga qaratilgan. Ushbu tamoyil quyidagi asosiy jihatlarni qamrab oladi: kodlashtirish – axborotni boshqa formatga o‘tkazish orqali ularning buzilishining oldini olish; kriptografiya – maxfiy ma’lumotlarni himoya qilish uchun shifrlash algoritmlarini ishlab chiqish; kalit boshqaruvi – shifrlangan ma’lumotlarni ochish va qayta tiklash mexanizmlarini yaratish. Shuningdek, kriptoanaliz texnologiyalari ham o‘rgatiladi, bu esa shifrlangan ma’lumotlarni himoya qilish tizimlarini yanada mustahkamlash imkonini beradi.

Qadriyatli yondashuv tamoyili. Axborot xavfsizligi nafaqat texnik bilimlarni, balki kasbiy va axloqiy qadriyatlarni shakllantirishni ham talab qiladi. Ushbu tamoyil axborot etikasiga rioya qilish, inson huquqlari va axborot xavfsizligi tamoyillariga asoslangan holda ma’lumotlardan foydalanish kabi muhim masalalarni o‘z ichiga oladi.

Konfedensiallik, riskni boshqarishga oid blokda bu “Kiberxavfsizlik asoslari” fanini o‘qitishda axborotni himoyalashga qaratilgan nazariy bilimlar bilan amaliy ko‘nikmalarni uyg‘unlashtirishga xizmat qiladigan yadro blok bo‘lib, u orqali talabalar axborotni himoyalashning texnik, huquqiy va boshqaruv jihatlarini chuqur o‘zlashtiradi. Konfedensiallik, riskni boshqarishni 4 bosqich doirasida olib boriladi.

Modelning metodologik ta’minotni rivojlantiruvchi blokda axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishdagi o‘qitish strukturasi, shakllari, metodlari, vositalari va shularni amalga oshirish uchun maqsad va vazifalarni, tushunchalar tahlilini funksiyasini o‘z ichiga oladi. Metodologik ta’minotni rivojlantiruvchi blokdagi asosiy quyidagi omillarni muhim ahamiyat kasb etadi: “Kiberxavfsizlik asoslari” fanini o‘qitishda bo‘lajak o‘qituvchilarda axborotlar bilan ishlash va uni saqlash bo‘yicha pedagogik-metodik tayyorgarlik tubdan rivojlantirish; Mazkur fanni chuqur o‘rgatish va

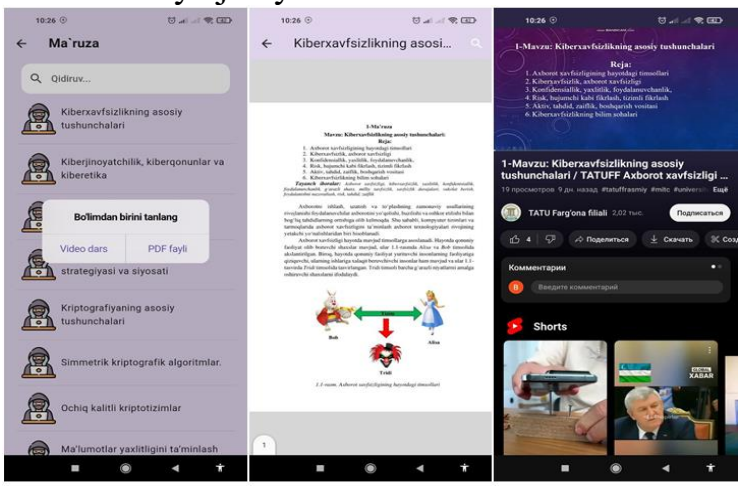
ma’lumotlarni o‘zlashtirish bo‘yicha jahon standartlariga mos ta’minotni o‘zlashtirishga yo‘naltirish.

Modelning kiberxavfsizlik asosini sintezlash asosi blokida axborot kontekstli o‘qitishning mavjud holatini aniqlash, axborot kontekstining mazmunini anglash, kompyuterdagi informatsiyalarni, subyektiv ma’lumotlarni bloklashni o‘rganish, fuqarolarning konstutsiyaviy huquqlari va erkinliklari bo‘yicha axborotlar bilan ishlash bilimlarini kengaytirish, kiberxavfsizlik fani bo‘yicha yangi metodik ta’minotni yaratishga yo‘naltirishni qamrab oladi.

Keltirilgan takomillashtirish modeli asosida o‘quv jarayonini tashlil etishda mobil ilovalarning o‘rni beqiyosdir. Hozirda ta’lim sohasida mobil ilovlardan foydalanish muhim axamiyat kasb etmoqda, yaratilgan ko‘plab mobil ilovalardan talabalar foydalanib kelishmoqda, ammo yaratilgan mobil ilovalarning ko‘p qismi to‘g‘ri va asosli ma’lumotlar joylashtirilmaganligini kuzatish mumkin. Bu vaziyatning yuzaga kelishiga asosiy sabab sifatida milliy va zamonaviy mobil ilovalarning ozligida deyishimiz mumkin. Buning oldini olishda biz asosan milliyligimizni o‘zida aks ettirgan mobil ilovalarni yaratish zaruriyati paydo bo‘ldi. Mazkur ilova “Kiberxavfsizlik asoslari” fanini o‘qitish uchun mo‘ljallangan bo‘lib, unda kiberxavfsizlik asoslari fanining asosiy tushunchalari, kiberhujumlardan himoyalanishning nazariy asoslari keltirildi.

Natijada mobil ilovaning asosiy menyusida ma’lumotlar va bo‘limlarning qidiriv bloki, fanning ma’ruza mashg‘lotlari keltirilgan qism, fanning amaliy mashg‘ulotlari keltirilgan qism va egallangan bilimlarni baholash jarayonini amalga oshirish uchun testlar bloki keltirilgan. Har bir bo‘linmalarning joylashuvi, belgilari va tanlangan dizayini o‘qitish uchun xizmat qiladigan mobil ilovalarga qo‘yilgan meyorlar asosida hamda fanning xususiyatlarini inobatga olib ishlab chiqildi.

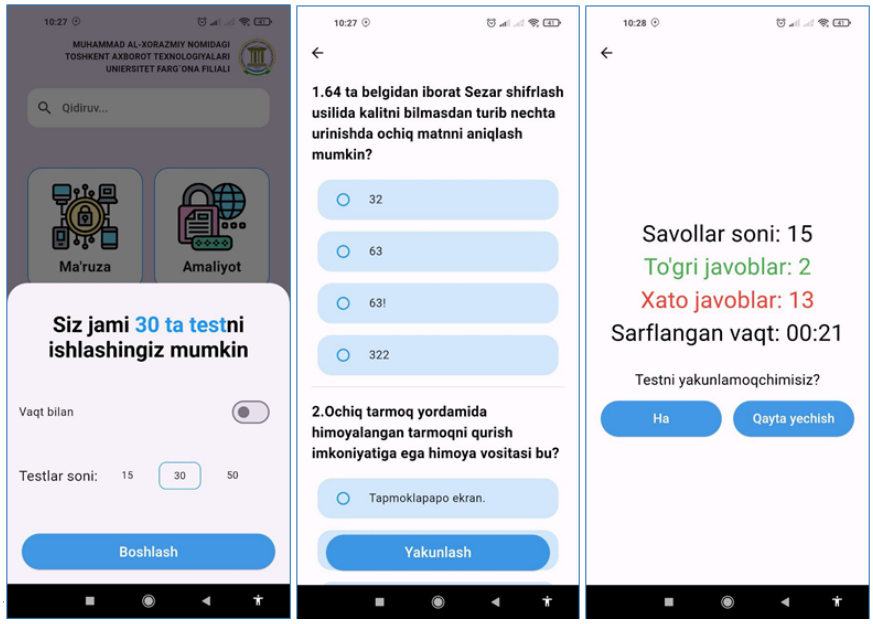
Ilovaning Ma’ruza va amaliy bo‘limida “Kiberxavfsizlikning asosiy tushunchalari”, “Kiberjinoyatchilik, kiberqonunlar va kiberetika”, “Inson faoliyati xavfsizligi”, “Kiberxavfsizlik arxitekturasi, strategiyasi va siyosati”, “Kriptografiyaning asosiy tushunchalari”, “Simmetrik kriptografik algoritmlar”, “Ochiq kalitli kriptotizimlar”, “Ma’lumotlar yaxlitligini ta’minlash usullari”, “Disklarni va fayllarni shifrlash”, “Ma’lumotlarni xavfsiz o‘chirish usullari”, “Identifikatsiya va autentifikatsiya jarayonini tashkil etuvchi vositalari”,



3-rasm. “Kiberxavfsizlik asoslari” fanini o‘qitish mobil ilovasi

“Ma’lumotlardan foydalanishni mantiqiy boshqarish”, “Ko‘p sathli xavfsizlik modellari”, “Ma’lumotlarni fizik himoyalash”, “Kompyuter tarmoqlari va tarmoq xavfsizligi muammolari”, “Tarmoq xavfsizligini ta’minlovchi vositalar”, “Simsiz tarmoq xavfsizligi”, “Risklarni boshqarish”, “Foydalanuvchanlik tushunchasi: zaxira nusxalash, ma’lumotlarni qayta tiklash va hodisalarni qaydlash”, “Dasturiy vositalardagi xavfsizlik muammolari”, “Kompyuter viruslari va virusdan himoyalanish muammolari”, “Qayd yozuvini himoyalash”, “Ijtimoiy injineriyaga qarshi himoya” mavzulari pdf shaklda hamda videodars ko‘rinishida ma’lumotlar keltirilgan.

Bundan tashqari ilovada talabalar va foydalanuvchilar ushbu fandan olgan bilimlarini nazorat qilish va baholash uchun test topshiriqlari bo‘limi mavjud bo‘lib, unda foydalanuvchi o‘zi bajarmoqchi bo‘lgan testlar sonini tanlashi (15. 30 va 50 ta testdan iborat) hamda topshiriqlarning bajarish muddatini ma’lum vaqt doirasida yoki vaqtni belgilamasdan amalga oshirish imkoniyati mavjud.



4-rasm. Talabalar bilimlarini nazorat qilish va baholash uchun test topshiriqlari

Dasturiy-metodik ta’minot yaratish individual tarkibiy qismlarini rivojlantirish, zarur kasbiy bilimlarni kengaytirish va ko‘nikmalarni takomillashtirish, pedagogik va texnologik shart-sharoitlarni tashkil etish, kasbiy kompetentlik darajasini oshirish va kasbiy mavqega erishish darajasini ta’minlash, kasbiy faoliyat samaradorligining natijasini aniqlash, mustaqil va uzluksiz kasbiy rivojlantirish texnologiyalarini qo‘llash algoritmini pedagogik faoliyat va kasbiy rivojlantirish kombinatsiyasi imkoniyatlari hamda qayta aloqani ta’minlovchi majmuani mujassamlashtirgan obyekt va subyekt o‘rtasidagi o‘zaro ta’sir tizimi uzluksiz kasbiy rivojlantirish texnologiyalarini takomillashtirishga xizmat qiladi.

“Differensial o‘qitish” texnologiyasi (“Differential teaching” technology)

Maqsadi: talaba – professor o‘qituvchining individual xususiyatlari – axborot xavfsizligi bilan ishlash qobiliyati va turli informatsiyalarni himoyalashdagi

kiberxavfsizlik bo‘yicha bilimlarini oshirish hamda uning imkoniyatini hisobga olgan holda o‘qitishdan iborat.

Mohiyati: ushbu texnologiya axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishda har bir ta’lim oluvchining intellectual rivojlanish doirasiga mos keluvchi faoliyatini hisobga olgan pedagogik sharoit yaratishni va differensial darajali o‘qitishni ko‘zda tutadi.

Mexanizmi: axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishda shaxsning dinamik xarakteristikasi tashxisi va o‘quv malakalarni egallash darajasi asosida o‘qitish; bilim olish va qiziqishlari yo‘nalishlariga bog‘liq holda tanlash; profil o‘qitish variantlari bo‘yicha tashkil etish; bilish mazmunini faollashtirish va talaba yoshlarning bilish faoliyatlarini rag‘batlantirish; o‘quv materialini o‘zlashtirish darajasini ixtiyoriy tanlash, kompyuter tizimida elektron shaklda mustaqil ishlarini joriy etish; o‘quv jarayonini yakka, guruhiy va jamoaviy shakllarda tashkil etish; o‘quv materiali o‘zlashtirilishi ustidan nazorat o‘tkazish; o‘qitiladigan fanlarni o‘qitish zamonaviy metodikasini yaratishga intilish; shaxsiy ta’lim rejasi bo‘yicha tezkor o‘qitishva axborotni himoya qilish bo‘yicha tavsiyalar berishdan iborat.

Dissertatsiya ishining **“Axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish bo‘yicha o‘tkazilgan tajriba-sinov ishlari natijalari va samaradorligi”** deb nomlanib, unda pedagogik tajriba-sinov ishlarini tashkil etishning baholash mezonlari, tajriba sinov ishlari tahliliva samaradorligi hamda natijalari bayon qilingan.

Tajriba-sinov ishlari Toshkent axborot texnologiyalari universitetining Samarqand, Qarshi va Farg‘ona filiallarida olib borildi. Tajriba-sinov ishlariga birinchidan to‘rtinchi bosqichning 497 nafar talabalari jalb etildi. Bundan tajriba guruhlarida – 248 nafar va nazorat guruhlarida – 249 nafar talaba ishtirok etdi

Tajriba sinov ishlari “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishga qaratilgan tajriba-sinov ishlari uch bosqich (ta’kidlovchi, rivojlantiruvchi, yakunlovchi)da amalga oshirildi.

Tajriba-sinov ishlarini amalga oshirishda boshlang‘ich, joriy va yakuniy monitoring olib borildi. Bunda kuzatish, suhbat, so‘rovnoma, test va pedagogik eksperiment usullaridan foydalanildi. Tajriba o‘tkazish davomida talabalarda axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’miontini takomillashtirish, kiberxavfsizlikka oid kasbiy kompetensiyalarini rivojlantirish maqsadida, o‘quv hamda auditoriyadan tashqari mashg‘ulotlar jarayonida innovatsion ta’lim texnologiyalarining nazariy-pedagogik, amaliy asoslarini ilmiy asoslashdan iborat bo‘ldi.

Tadqiqotning shakllantiruvchi tajriba-sinov bosqichida axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish bo‘yicha o‘quv fani dasturi asosida respondent-talabalarning innovatsion ta’lim metodlari va zamonaviy texnologiyalari vositasida axborotlar bilan ishlash kiberxavfsizlikka oid quyidagi mezonlari rivojlantirildi:

O‘quv kognitiv mezonlar: axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish bo‘yicha o‘quv fani dasturi asosida integrativ yondashuv asosida bo‘lajak mutaxassis kasbiy

kompetentligini rivojlantirish bo‘yicha talabalarning elektron tarzdagi axborotlarning egallanishi va ular yuzasidan ilmiy- nazariy bilimini kengaytirish, psixologik-pedagogik bilimlari yosh va individual, psixofiziologik xususiyatlarini, o‘quv jarayonini tashkil qilish shakl, metod va vositalarini, talabalarni tashxislashning asosiy metodikasini, innovatsion pedagogik texnologiyalarni bilishi;

Kommunikativ tafakkur qilish mezon: talabalarda axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish bo‘yisha o‘quv fani dasturi asosida kommunikativ bilim, ko‘nikma va malakalar – o‘quv- pedagogik ta’lim jarayonida talabalar bilan metodik ta’minotni yaratish layoqatini o‘stirish, tafakkur qilish mahoratini va muloqot qilish kompetentligini takomillashtirish;

Integrativ-kreativ mezonlar: axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish bo‘yicha o‘quv fani dasturi asosida turli fanlararo o‘zaro aloqadorlikni kasb etuvchi integrativ yondashuv asosida axborotlar xavfsizligi bilan ishlash kasbiy kompetentligini rivojlantirish qobiliyati, kreativ sifat va salohiyati o‘sishga xizmat qiluvchi adabiyotlar bilan tanishib chiqishga yo‘naltirish, fikrlash qobiliyatini o‘stirish.

Tajriba-sinov ishlarini o‘tkazish jarayonida integrativ yondashuv asosida bo‘lajak mutaxassisning kasbiy kompetentligini rivojlantirish darajalari aniqlashtirildi. Dissertatsiyada integrativ yondashuv asosida bo‘lajak mutaxassislarning “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishning samaradorligini “yuqori”, “o‘rta”, “past” darajalari mezonlari ko‘rsatib berildi.

1-jadval. “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishga qaratilgan tajriba sinov ishlarida tajriba va nazorat guruhlarida ishtirok etgan respondentlar soni

1-jadval

Barcha oliy ta’lim muassasalarida tajriba sinov ishlarida tajriba va nazorat guruhlarida ishtirok etgan respondentlar soni

Tajriba-sinov ishlaridan “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishga va ularning ushbu fan doirasida bilish darajasini aniqlashga qaratilgan yuqorida keltirilgan talabalarda “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishning mavjud holatini aniqlashga yo‘naltirilgan anketa savollari, talabalarning kiberxavfsizlik, axborot xavfsizligini ta’minlash muammosi internetning ishlash

OTM	Tajriba guruhlari	Nazorat guruhlari	Jami
Toshkent axborot texnologiyalari universitetining Samaraqand filiali	83	82	165
Toshkent axborot texnologiyalari universitetining Qarshi filiali	82	83	165
Toshkent axborot texnologiyalari universitetining Farg‘ona filiali	83	84	167
Jami	**248**	**249**	**497**

sharoitlarida muhim kasbiy sifatlarini rivojlantirish tizimiga hamda kurs mavzusi asosida o‘quv va auditoriyadan tashqari mashg‘ulotlarda axborotlar bilan ishlash madaniyatni maqsadga muvofiq shakllantirish ko‘rsatkichlar va mezonlar asosida baholash ishlari olib borildi.

Berilgan anketa savollari bo‘yicha tajriba yakunidagi natijalarga nisbatan qo‘yilgan gipotezaga ko‘ra $\varphi_{emp} > \varphi_{krit}$ bo‘lgani uchun H1 gipoteza sifati qabul qilinadi. Bu esa olingan natijalarda farq mavjudligi va samaradorlikka ega ekanligini tasdiqlaydi.

Tajriba yakunida tajriba va nazorat guruhlarida umumiy hisobda “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’miontini takomillashtirish va kasbiy sifatlarini rivojlantirishning “Kiberxavfsizlik bilan ishlashning mazmuni”, “Kiberxavfsizlik kompetentligining rivojlanish ko‘rsatkichi”, “Kiberetika madaniyatining rivojlanganligi” komponentlarini rivojlantirishning bilish darajalarida farqlar kuzatildi, ya’ni:

2-jadval

Barcha oliy ta’lim muassasalarining tajriba-sinov ishlari bo‘yicha umumiy natijalarining yakuniy ko‘rsatkichlari

Mezonlar	Komponentalar	Guruhlar	Baholash darajasi		
			yuqori daraja	o‘rta daraja	past daraja
o‘quv kognitiv	Kiberxavfsizlik bilan ishlashning mazmuni	TG	38	177	33
		NG	19	77	153
kommunikativ tafakkur qilish		TG	39	171	38
		NG	19	75	155
integrativ-kreativ		TG	37	178	33
		NG	19	78	152
o‘quv kognitiv	Kiberxavfsizlik kompetentligining rivojlanish ko‘rsatkichi	TG	42	180	26
		NG	21	74	154
kommunikativ tafakkur qilish		TG	45	167	36
		NG	22	72	155
integrativ-kreativ		TG	43	174	31
		NG	21	73	155
o‘quv kognitiv	Kiberetika madaniyatining rivojlanganligi	TG	51	182	15
		NG	24	90	135
kommunikativ tafakkur qilish		TG	48	180	20
		NG	24	89	136
integrativ-kreativ		TG	52	187	9
		NG	27	88	134

Tajriba va nazorat guruhlarida umumiy hisobda “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish va kasbiy sifatlarini rivojlantirishning “Kiberxavfsizlik bilan ishlashning mazmuni”, “Kiberxavfsizlik kompetentligining rivojlanish ko‘rsatkichi”, “Kiberetika madaniyatining rivojlanganligi” komponentini rivojlantirishning bilish darajalari bo’yicha dastlabki natijalarning mezonlar va OTMlar bo’yicha statistik tahlili Styudent statistikasi asosida amalga oshirildi.

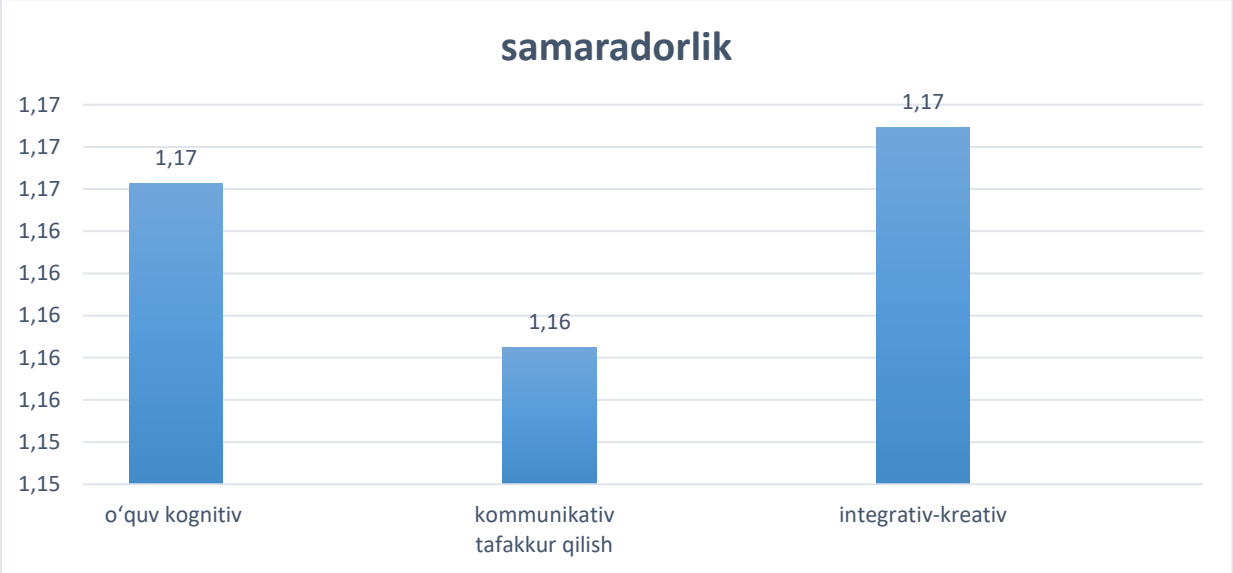
3-jadval

Barcha oliy ta’lim muassasalarining tajriba-sinov ishlari bo‘yicha statistik tahlil ko’rsatkichlari

Mezonlar	Komponentalar	Guruhlar	Styudent Statistikasi	Statistikaning ozodlik darajasi	Kritik qiymat	Kriteriy xulosasi	Ishonch chetlanishii	O‘qitish sifatini baholash	bilim darajasini baholash
o‘quv kognitiv	Kiberxavfsizlik bilan ishlashning mazmuni	TG	10,62	482,07	1,96	H1	0,04	1,13	0,57
		NG					0,05		
kommunikativ tafakkur qilish		TG	10,29	487,67	1,96	H1	0,04	1,13	0,56
		NG					0,05		
integrativ-kreativ		TG	10,49	480,97	1,96	H1	0,04	1,13	0,57
		NG					0,05		
o‘quv kognitiv	Kiberxavfsizlik kompetentligining rivojlanish ko‘rsatkichi	TG	11,38	473,99	1,96	H1	0,03	1,15	0,62
		NG					0,05		
kommunikativ tafakkur qilish		TG	10,38	486,83	1,96	H1	0,04	1,14	0,58
		NG					0,05		
integrativ-kreativ		TG	10,95	481,74	1,96	H1	0,04	1,14	0,6
		NG					0,05		
o‘quv kognitiv	Kiberetika madaniyatining rivojlanganligi	TG	11,26	458,89	1,97	H1	0,03	1,14	0,62
		NG					0,05		
kommunikativ tafakkur qilish		TG	10,59	465,68	1,97	H1	0,04	1,13	0,58
		NG					0,05		
integrativ-kreativ		TG	11,55	438,43	1,97	H1	0,04	1,14	0,63
		NG					0,05		

Ushbu natijalardan ko‘rinadiki, jadvaldagi yakunlovchi bosqichining xulosasiga ko‘ra tajriba va nazorat guruhlaridagi o‘zlashtirish ko‘rsatkichlarining bir biridan farqli ekanligi, samaradorligi birdan kattaligi, Styudent statistikasining emprik qiymati kritik qiymatdan kattaligi, ishonch oraliqlarining bir-biri bilan ustama-ust tushmasligi (kesishishmasli), tajriba-sinov ishlari samaradorligini baholovchi mezonning birdan ancha kattaligi, talabalarning bilish darajasini baholash mezonning noldan sezilarli kattaligi H1 gipotezaning qabul qilinishiga olib keladi.

Shunday qilib, statistik tahlil bo‘lajak o‘qituvchilarning mediakompetentligini rivojlantirishga yo‘naltirilgan tajriba-sinov ishlarining samarali kechganligini tasdiqladi. Olib borilgan tadqiqot ishidagi o‘rtacha o‘zlashtirish va samaradorlik ko‘rsakichlari qo‘yidagi diagrammalarda ko‘rsatildi



6-rasm. Kiberetika madaniyatining rivojlanganligi komponentini rivojlantirishning samaradorlik ko‘rsatkichlari

Olingan natijalardan barcha holat uchun tajriba guruhidagi o‘zlashtirishlar nazorat guruhidagi o‘zlashtirishlardan yuqori ekan.

Demak, talabalarning kiberxavfsizlik, axborot xavfsizligini ta’minlash muammosi internetning ishlash sharoitlarida muhim kasbiy sifatlarini rivojlantirish tizimiga hamda kurs mavzusi asosida o‘quv va auditoriyadan tashqari mashg‘ulotlarda axborotlar bilan ishlash madaniyatni maqsadga muvofiq shakllantirish, innovatsion ta’lim texnologiyalaridan foydalanish, kasbiy sifatlarni rivojlantirilganligining Kiberxavfsizlik bilan ishlashning mazmuni komponentining o‘quv kognitiv, kommunikativ tafakkur qilish va integrativ-kreativ mezonlari bo‘yicha samaradorlik o‘rtacha 1,16 barobarga, Kiberxavfsizlik kompetentligining rivojlanish ko‘rsatkichi komponentining o‘quv kognitiv, kommunikativ tafakkur qilish va integrativ-kreativ mezonlari bo‘yicha samaradorlik o‘rtacha 1,17 barobarga va Kiberetika madaniyatining rivojlanganligi komponentining o‘quv kognitiv, kommunikativ tafakkur qilish va integrativ-kreativ mezonlari samarali samaradorlik o‘rtacha 1,17 barobarga yuqori ekanligi statistik tahlildan ma’lum bo‘ladi.

XULOSALAR

1. Kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv va kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligini e’tiborga olgan holda huquqiy tashkiliy-iqtisodiy va texnologik tadbirlar orqali zamonaviy kibertahdidlar sharoitida talabalarning kiberetik madaniyatini shakllantirishga ta’sir qiluvchi asosiy tamoyillar asosida kiberxavfsizlikka oid bilimlar, kiberjinoyatchilik, kiberhuquq, kibertahdid, kiberetika, talaba yoshlarning internet tarmog‘i va unda axborotlar bilan ishlash etikasi va madaniyatiga rioya qilish ko‘nikmalarini o‘stirish hamda “Kiberxavfsizlik asoslari” fanini o‘qitishni takomillashtirishning pedagogik imkoniyatlari aniqlashtirilgan.

2. Axborotlar xuruji davrida talabalarda kiberetika madaniyatini shakllantirishda “Kiberxavfsizlik asoslari” fanini o‘qitishning aspektlari,

kiberxavfsizlik fanining predmet va maqsadidan kelib chiqib, “Kiberxavfsizlik asoslari” fanini o‘qitishdagi asosiy vazifalar qamrab olgan keng spektrli jarayonlar (konfidensiallik; yaxlitlik; identifikatsiya; autentifikatsiya; vakolat berish; foydalanishni nazoratlash; mulkka egalik huquqini anglash; sertifikatsiya; imzo; voz kechmaslik; sanasini yozish; olganligiga tilxat berish; bekor qilish; anonimlik) chuqur tahlil qilingan.

3. Axborot xavfsizligini ta’minlash vazifalari, axborot xavfsizligini ta’minlashning dasturiy va texnik vositalari, kiberxavfsizlikning tarmoqlaro klassifikatsiyasi: axborot xavfsizligi, Internet tarmog‘i xavfsizligi, ma’lumotlar xavfsizligi, turli informatsiyalar xavfsizligi, ma’lumotlarni saqlash va kodlashni aniqlashtirish orqali axborot xurujining ta’lim jarayoniga ta’siri jihatlarini aniqlash va talabalarda kibertahdidlarga qarshilik ko‘rsatish bo‘yicha barqaror ko‘nikmalarni shakllantirishni ta’minlaydigan turli xil texnologiyalarni joriy qilish asosida takomillashtirishga erishilgan.

4. Axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitish modeli 4ta: kriptografik-kognitiv aspektlarga qaratilgan blok, konfedensiallik, riskni boshqarishga oid blok, metodologik ta’minotni rivojlantiruvchi blok va baholash mezonlari bloklari asosida takomillashtirilgan bo‘lib, “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishda kiberxavfsizlik terminlarining konseptual asoslarini va ularning amaliy tatbig‘i va kompyuter ma’lumotlaridan foydalanishda shaxsiy- kasbiy, kreativ- mantiqiy, individual kasbiy rivojlanish, psixologik o‘sish qobiliyatlarini o‘qitishning bosh maqsadi qilib olingan.

5. Axborot xavfsizligini ta’minlashning dolzarb muammolarini inobatga olgan holda va kiberxurujlar davrida talabalarda kiberetika madaniyatini shakllantirish, Axborot xavfsizligi va kiberxavfsizlikning o‘ziga xos differensial xususiyatlarini inobatga olib, “Kiberxavfsizlik” va “Axborot xavfsizligi” atamalaridan bir-birini taqozo qiluvchi jarayonlar majmui tariqasida qarash natijasida kibertahdidlar juda global muammolarni yechimini tizimli-tuzulmaviy tahlil va faoliyatli yondashuvlarga uygunlashtirish asosida ishlab chiqilgan model asosida shaxsning dinamik xarakteristikasi tashxisi va o‘quv malakalarni egallash darajasi asosida o‘qitish, bilim olish va qiziqishlari yo‘nalishlariga bog‘liq holda tanlash, profil o‘qitish variantlari bo‘yicha tashkil etish, bilish mazmunini faollashtirish va talaba yoshlarning bilish faoliyatlarini rag‘batlantirish inobatga olingan.

6. “Kiberxavfsizlik asoslari” fanini o‘qitishning o‘quv-metodik ta’minotini boyitishga asoslangan dasturiy-metodik ta’minoti axborot xurujlaridan himoyalanish uchun zarur bo‘lgan kompetensiyalarni shakllantirishga alohida e’tibor qaratilgan holda, uzluksizlik, asoslilik, fanlararo aloqadorlik, axborotni himoyalash, qadriyatli yondashuv, aniqlik, shaxlararo munosabat tamoyili, refleksivlik tamoyillari mazmuni tahlilidan kelib chiqib, axborot xuruji davrida Kiberxavfsizlik asoslari fanini o‘qitishda talabalarga suhbat darslarini, qiziqarli ma’lumotlarni o‘zida birlashtiruvchi kurs ishlari taqdimotlarini tayyorlash, axborot va kiberxavfsizlik tahdidlaridan himoyalanuvchi tadbirlarini rejalashtirish va amaliy tarzda o‘tkazishni ko‘paytirish, turli tizimlarda kiberjinoyatchilikka qarshi kurashish bo‘yicha treninglar, kiber muhofaza bo‘yicha zamonaviy texnologiyalar va innovatsion metodlarga boy dasturiy-metodik ta’minot sifatida yaratilgan.

7. Axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minoti takomillashtirishda talabalarning axborotlardan ijobiy maqsadga yo‘naltirib foydalanish va ularning mustaqil va uzluksiz kasbiy rivojlanishi yuqori darajada samarali amaliyotga joriy etishga qaratilgan didaktik tamoyillari asosida takomillashtirilgan;

8. Axborot xurujlari davrida “Kiberxavfsizlik asoslari” fanini o‘qitish samaradorligini oshirishga qaratilgan elektron platforma (“https://edu-cyber.uz/”) “Kiberxavfsizlik asoslari” fanini o‘qitish uchun mo‘ljallangan mobil ilova va uslubiy tavsiyalar bilan qo‘shimcha ravishda boyitilib, interaktiv o‘quv usullari va virtual muhitda axborot tahdidlariga tezkor javob berish imkoniyatini berdi.

9. Tahlil va umumlashtirish metodlaridan foydalanilgan holda, verbal, simvolik va vizual toifalar, shuningdek, o‘qish bilan bog‘liq derivativ, assotsiativ va frazeologik birliklar ajratib olinib, raqamli ta’lim vositalariga moslashtirilishi asosida kiberxavfsizlik kompetentligining rivojlanish ko‘rsatkichlari va kiberetika madaniyatning rivojlanganligini asoslovchi komponentlari o‘quv kognitiv, kommunikativ tafakkur qilish va integrativ-kreativ mezonlariga asoslanib, “yuqori”, “o‘rta”, “past” darajalari ko‘rsatib berilgan. Natijada, talabalarda kiberxavfsizlik sohasida chuqur bilim va amaliy ko‘nikmalarni shakllantirishga yo‘naltirilgan samarali o‘quv jarayoni tashkil etilgan.

TAVSIYALAR

1. Axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish bo‘yicha xalqaro tajribalardan va ularning amaliy- metodik tatbiqiy jihatlarni o‘zlashtirishning adaptiv variantlarni ishlab chiqish zarur.

2. Kiberxavfsizlik muammolari va muhim yechimlariga oid ilmiy-amaliy yondashuvlarni tegishli soha mutaxasislarini tayyorlash jarayoniga joriy qilinishini ta’minlash uchun tadqiqot ishlari olib borilishi zarur.

3. Axborotlar xuruji davrida “Kiberxavfsizlik asoslari” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishning xalqaro va zamonaviy yondashuvlarini singdirish bo‘yicha turli ko‘rinish va tendensiyalar mohiyati keltirilgan o‘quv-metodik adabiyotlar nashr qilish kerak.

НАУЧНЫЙ СОВЕТ ПО ПРИСУЖДЕНИЮ УЧЁНЫХ СТЕПЕНЕЙ DSc.03/30.01.2020.Ped.26.01 ПРИ НАЦИОНАЛЬНОМ ПЕДАГОГИЧЕСКОМ УНИВЕРСИТЕТЕ УЗБЕКИСТАНА

НАЦИОНАЛЬНЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ УЗБЕКИСТАНА

МУХТАРОВ ФАРРУХ МУХАММАДОВИЧ

СОВЕРШЕНСТВОВАНИЕ ПРОГРАММНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ «ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ» В ЭПОХУ ИНФОРМАЦИОННЫХ АТАК

13.00.06 – Теория и методика цифрового образования

АВТОРЕФЕРАТ ДИССЕРТАЦИИ ДОКТОРА (DSc) ПО ПЕДАГОГИЧЕСКИМ НАУКАМ

Ташкент – 2025

Тема диссертации доктора наук (DSc) зарегистрирована в Высшей аттестационной комиссии за № B2024.3.DSc/Ped981.

Диссертация выполнена в национальном педагогическом университете Узбекистана.

Автореферат диссертации на трёх языках (узбекский, русский, английский (резюме)) размещён на веб-странице Научного совета www.tdpu.uz и на информационно-образовательном портале «ZiyoNet» по адресу www.ziyonet.uz.

Научный консультант:	**Абдуллаева Барно Сайфутдиновна** доктор педагогических наук, профессор
Официальные оппоненты:	**Каюмова Насиба Ашуровна** доктор педагогических наук, профессор
	Султанова Угилой Набиевна доктор педагогических наук, профессор
	Абдуллаева Озода Сафибуллаевна доктор педагогических наук, профессор
Ведущая организация:	**Гулистанский государственный университет**

Защита диссертации состоится «____» _____ 2025 года в ____ часов на заседании Научного совета DSc.03/30.01.2020.Ped.26.01 при Национальном педагогическом университете Узбекистана. (Адрес: 100185, город Ташкент, Чиланзарский район, улица Бунёдкор. Дом 27. Тел.: (99871) 276-79-11; факс: (99871) 276-80-86; e-mail: tdpu_kengash@edu.uz).

С диссертацией можно ознакомиться в Информационно-ресурсном центре Национального педагогического университета Узбекистана (зарегистрирована под № _____). (Адрес: 100185, город Ташкент, Чиланзарский район, улица Бунёдкор. Дом 27. Тел.: (99871) 276-75-87; факс: (99871) 276-80-86.

Автореферат диссертации разослан «_____ «_____ 2025 года.
(реестр протокола рассылки № _____ от «_____» _____ 2025 года).

З.Н.Мамаражабова
Председатель Научного Совета по присуждению учёных степеней, д.п.н., профессор

Р.Г.Исянов
Учёный секретарь Научного совета по присуждению учёных степеней, к.п. н., доцент

М.Э.Мамаражабов
Председатель Научного семинара при Научном Совете по присуждению учёных степеней, д.п.н., профессор

ВВЕДЕНИЕ (аннотация докторской диссертации)

Актуальность и востребованность темы диссертации. В мировых учебных заведениях внедряются технологии обеспечения информационной и кибербезопасности, в том числе в разработку и защиту собственных информационных ресурсов, а также воздействие на информационные ресурсы других стран. В США, России, Евросоюзе, Китае, Индии проводится системная работа по развитию деятельности специальных подразделений, ответственных за использование сетей, повышению уровня знаний специалистов по кибербезопасности, совершенствованию процесса формирования информационной грамотности и идеологической защищенности будущих специалистов от информационных атак с использованием инновационных педагогических методов.

В мировых образовательных и исследовательских центрах проводятся научные исследования по формированию знаний и навыков студентов в области информации и кибербезопасности, повышению информационно-когнитивных компетенций, совершенствованию современных программно-педагогических методических основ последовательной организации в рамках профессиональной компетентности. Уделяется внимание исследованиям по совершенствованию профессиональных компетенций будущих специалистов на основе современных дидактических средств образования, на основе современных технологий информационного обмена и безопасности, повышению эффективности моделей формирования культуры кибербезопасности, широкому внедрению интерактивной информации в образование.

В нашей республике в последние годы созданы нормативные основы для расширения объема знаний студентов и молодежи в области информационной безопасности, управления информационными технологиями, междисциплинарной интеграции ресурсов. В Стратегии действий по дальнейшему развитию Республики Узбекистан на 2017-2021 годы поставлены задачи «...обеспечения информационной безопасности и совершенствования системы защиты информации, своевременного и адекватного противодействия угрозам в информационной сфере»[34] и «...создания необходимых условий для беспрепятственного использования глобальной информационной сети, обеспечения кибербезопасности в национальном интернет-пространстве, повышения грамотности граждан в использовании сети интернет»[35], изложенные в Указе Президента Республики Узбекистан № 158 «О Стратегии «Узбекистан - 2030» от 11 сентября 2023 года. В результате будут расширяться альтернативные возможности предотвращения кибератак, их обнаружения и устранения их последствий.

Данное диссертационное исследование в определённой степени служит реализации задач, обозначенных в Постановление Президента Республики

[34] Указ Президента Республики Узбекистан от 7 февраля 2017 года № УП-4947 «О Стратегии действий по дальнейшему развитию Республики Узбекистан»

[35] Указ Президента Республики Узбекистан от 11 сентября 2023 года № УП-158 «О Стратегии «Узбекистан — 2030»»

Узбекистан от 31 мая 2023 года № ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан», Постановление Президента Республики Узбекистан от 15 августа 2024 года № ПП-293 «О дополнительных мерах по развитию образования и науки в области криптологии в Республике Узбекистан», Постановление Президента Республики Узбекистан от 30 апреля 2025 года № ПП-153 «О мерах по дальнейшему усилению деятельности по борьбе с преступлениями, совершаемыми с использованием информационных технологий», Постановление Президента Республики Узбекистан от 20 апреля 2017 года № ПП-2909 «О мерах по дальнейшему развитию системы высшего образования» и другие соответствующие документы, связанные с данной деятельностью.

Соответствие исследования приоритетным направлениям развития науки и технологий Республики. Диссертационное исследование выполнено в соответствии с приоритетным направлением науки и технологий в республике I. «Формирование системы и инновационных идей и пути их внедрения в социальном, правовом, экономическом, культурном, духовно-просветительском развитии информационного общества и демократического государства».

Обзор зарубежных исследований по теме диссертации. Во многих странах мира ведутся научные исследования по вопросам, связанным с совершенствованием программного и методического обеспечения преподавания дисциплины «Основы кибербезопасности» и современных подходов к вопросам информационной безопасности, кибербезопасности и криптографии. В частности, Университет Карнеги-Меллона в США, Оксфордский и Кембриджский университеты в Великобритании, а также Королевский университет Белфаста — исследовательский центр CSIT, ATHENE (Дармштадт) в Германии — крупнейший в Европе центр ИТ-безопасности, TÜBİTAK BİLGEM в Турции — научно-технологический центр информационной безопасности и криптографии, Корейский университет CIST в Южной Корее, Университет Цинхуа в Китае, Пекинский университет почты и телекоммуникаций и другие престижные университеты и исследовательские центры ищут решения проблем, связанных с этой областью и ее преподаванием.

Университет Карнеги-Меллона в США насчитывает более 160 аспирантов и научных сотрудников в области безопасности интернета вещей, машинного обучения и ИИ, сетевой и системной безопасности, а также конфиденциальности и приватности. 10% его исследователей занимаются преподаванием в этой области, в основном работая над совершенствованием методологии и программно-методических средств. В Стэнфордском университете есть курсы «Advanced Cybersecurity Program» и «Cybersecurity and Executive Strategy» на Stanford Online, целью которых является повышение квалификации в области идентификации рисков, оценки и стратегического реагирования. Оксфордский университет в Великобритании предлагает магистерские и докторские программы по направлениям «Безопасность программного обеспечения и систем», «Программная инженерия» и «Социальная наука интернета». В рамках программы молодые исследователи занимаются разработкой облачной

безопасности, стеганографии, формальной аутентификации, мобильной и сетевой безопасности, криптографии и совершенствованием программного и методического обеспечения для обучения по этим направлениям. Кроме того, OII, объединяющий социальные и компьютерные науки, также изучает вопросы социальной кибербезопасности в таких областях, как «Управление и безопасность информации». ATHENE (Дармштадт), расположенный в Германии, является крупнейшим центром ИТ-безопасности в Европе, реорганизованным в 2015 году и в настоящее время проводит исследования в области безопасности, конфиденциальности и кибербезопасности цифровых систем и критических инфраструктур. Турецкий BİLGEM был создан в 2010 году и включает в себя 6 научных институтов: UEKAE (Электроника и криптология), BTE, SGE, İLTAREN, YTE, YZE. Целью центра является разработка национально независимых и конкурентоспособных технологий в области криптологии, информационной безопасности и передовой электроники, а также предоставление всем учебным заведениям Турции набора практик и технологий, предназначенных для практики преподавания при подготовке передовых специалистов в этой области. При этом формируется стратегия обучения, основанная на практике, в преподавании «Основ кибербезопасности» и связанных с ними предметов. Центр CIST, который является частью Корейского университета в Южной Корее, проводит обширные научные исследования в области криптографии, сетевой и системной безопасности, а также цифровой криминалистики. Научная работа, проводимая в областях криптографии, сетевой и системной безопасности, считается имеющей мировое значение, при этом организовано обучение студентов бакалавриата и магистратуры корейских вузов на основе технологий и методик, разработанных исследователями-методистами центра в преподавании фундаментальных наук, связанных с информационной безопасностью. В Университете Цинхуа в Китае есть много институтов, лабораторий и центров, занимающихся информационной безопасностью, где студентам институт дает теоретические знания по изучению кибербезопасности и смежных дисциплин, теоретические знания закрепляются в лабораториях, а студенты имеют возможность работать с заказами в центрах. Центры собирают заявки от организаций и предприятий, а также частных лиц по кибератакам, краже персональных электронных данных и угрозам, и студенты имеют возможность свободно, добровольно и креативно подходить к этим проблемам и готовить предложения по решениям, а вопросы, решенные с их вмешательством, также предоставляют студентам оценку.

Постквантовая криптография (ПКК) — одно из современных направлений, требующее глубоких исследований. Ведутся работы по использованию ИИ для заблаговременного обнаружения кибератак, обнаружения ботнетов и автоматизации анализа фейковых данных (дипфейк). Это одно из направлений, которое, как ожидается, будет изучаться сегодня. Сегодня основные научные исследования сосредоточены на создании протоколов безопасности для мобильных сетей нового поколения (6G), разработке систем, устойчивых к сигнальным атакам, поскольку сети 6G передают информацию со скоростью миллисекунд, что объясняется необходимостью переосмысления систем

конфиденциальности и аутентификации. В настоящее время, начиная с 5-10 классов, в систему образования вводятся уроки, направленные на формирование киберграмотности в областях информационной безопасности, кибербезопасности и криптографии, таких как безопасность паролей, защита от фишинга, нормы поведения в Интернете. Основная цель этих мер — воспитать подрастающее поколение информированным, осознанным и защищенным по отношению к цифровым угрозам.

Многие ведущие зарубежные вузы вводят углубленную специализацию. В частности, постоянно совершенствуются такие программы, как «Инженерия кибербезопасности», «Прикладная криптография и безопасная связь», «Искусственный интеллект и киберзащита».

Степень изученности проблемы. Проблемы информатизации образования, разработка концептуальных основ методического обучения изучали У.Ш.Бегимкулов[36], Т.Т.Калеева[37], М.Куронов[38], М.Х.Лутфиллаев[39], К.Олимов[40], Д.Ж.Саидов[41], Н.И.Тайлоков[42], Ф.Закирова[43]; совершенствование навыков, механизмов и моделей информационной безопасности и кибербезопасности исследовали Т.Ф.Бекмуратов[44], С.К.Ганиев[45], О.Г.Давлатов[46], О.У.Холмуратов[47], Б.Х.Ходжаев[48], А.Х.Мухитдинов[49], А.Б.Раджиев[50], К.А.Ташаев[51], Б.Тахиров[52], У.Л.Ёзиева[53].

---

[36] Begimqulov U.Sh. Pedagogik ta'lim jarayonini axborotlashtirishni tashkil etish va boshqarish nazariyasi va amaliyoti.ped.fan. dok...diss.-T..2007. -305 b.

[37] Kalekeeva T. T. Ta'limni axborotlashtirish sharoitida bo'lajak informatika o'qituvchilarini tayyorlash mazmunini takomillashtirish. Dis... dok (PhD). – T., 2018. – 135 b.

[38] Quronov M. Milliy xavfsizlik tizimida kiberxavfsizlikning o'rni va uni ta'lim jarayonida integratsiyalash muammolari // Oliy ta'limda innovatsiyalar. – Toshkent: TDPU, 2021. – №4. – B. 120–128.

[39] Lutfillayev M.H. Oliy ta'lim jarayonini takomillashtirishda axborot texnologiyalarini integrasiyalash nazariyasi va amaliyoti. (Informatika va tabiiy fanlar misolida). ped.fan. dok...diss. Samarqand 2005 - 236 b.

[40] Олимов К. Проблема создания учебников специалных дисциплин нового поколения в сфере средного специального образования. Монография. – Т.: "Фан", 2004. – 144 б.

[41] Saidov D.J., To'rayeva O.X. Axborot tizimlari va ularning rivojlanishi omillari // Central Asian journal of multidisciplinary research and management studies. Volume 1, Issue 4, March 2024. 67-68-b.

[42] Tayloqov N.I., Rustamov N. Elektron o'quv adabiyotlarini yaratish-davr talabi // Ta'lim va tarbiya. – Toshkent, 2003. -1-2-son. – B. 23 – 25.

[43] 169. Закирова Ф.М. Теоретические и практические основы методической подготовки будущих преподавателей информатики в педагогических ВУЗах. Автореф. дис. ... док-ра. пед.наук. – Ташкент, 2009.

[44] Бекмуратов Т.Ф., 52. G'aniyev S.K., Karimov M.M., Tashayev K.A. Axborot xavfsizligi. Oliy o'quv yurt talabalari uchun mo'ljallangan o'quv qo'llanma. "Fan va texnologiya" nashriyoti, Toshkent -2016.Б. 125 – 126.

[45] G'aniyev S.K., Karimov M.M., Tashayev K.A. Axborot xavfsizligi. Oliy o'quv yurt talabalari uchun mo'ljallangan o'quv qo'llanma. "Fan va texnologiya" nashriyoti, Toshkent -2016.

[46] Davlatov O.G'. Talabalarda axborot xavfsizligini ta'minlash kompetenstligini tarixiy-madaniy meros vositasida rivojlantirish. Ped.fan.fals.dok…diss. Toshkent-2018. -21 b.

[47] Xalmuratov O.U.Axborot xavfsizligi ko'rsatkich va mezonlari tizimini shakllantirish usullari va algoritmlari.Tex.fan.fals.dok.(PhD). …diss. Toshkent-2019. -163 b.

[48] Xodjayev B.X. Umumta'lim maktablari talabalarida tarixiy tafakkurni modernizatsiyalashgan didkatik ta'minot vositasida rivojlantirish. Ped.fan.dok….diss. –T., 2016. – 120-122 b.

[49] Muxitdinov A.H. Axborot xavfsizligini ta'minlashning iqtisodiy mexanizmi. iqt.fan.nomz…diss.Toshkent. 2012.-178 b.

[50] Radjiyev A.B. Xalq ta'limi tizimida rahbar xodimlarni qayta tayyorlash va malakasini oshirishni boshqarish samaradorligini oshirish (umumta'lim maktab direktorlari misolida): ped. fanl. bo'y. fals. dokt. (PhD) diss. ... avt. –T.: 2020. – 61 b.

[51] G'aniyev S.K., Karimov M.M., Tashayev K.A. Axborot xavfsizligi. Oliy o'quv yurt talabalari uchun mo'ljallangan o'quv qo'llanma. "Fan va texnologiya" nashriyoti, Toshkent -2016.

[52] Tahirov B.N. Axborot xavfsizligi asoslari [Matn] : o'quv qo'llanma / B.N. Tahirov - Buxoro: Fan va ta'lim, 2022.-156 b.

[53] Yozieva U.L. Ta'lim-tarbiya jarayonida o'quvchilarni zararli axborotlar tahdididan himoya qilishning takomillashtirilgan texnologiyasi (boshlang'ich ta'lim misolida). Pedagogika fanlari bo'yicha falsafa doktori (PhD) dissertatsiyasi. – Nukus, 2018. – 134 b.

В странах СНГ по вопросам информационной безопасности и кибербезопасности провенли исследование А.А.Алтуфева[54], А.Б.Бабаш, Е.К.Баранова[55], Е.В.Бондаревская[56], Й.Й.Борадакий[57], В.А.Красильникова[58], А.В.Лукатский[59], Н.Н.Моисеев[60].

Осведомленность о киберситуации и мониторинг киберсреды, подходы к кибербезопасности в сфере образования и различных отраслях промышленности исследованы в работах S.Alter[61], Ross J. Anderson[62], Thomas A. Johanson, Yar Majid va Kevin F[63]. Steinmetz, Ujjwal Rao[64], Howard Schmidt[65], Bruce Schneier[66].

Связь темы диссертации с планами научно-исследовательской работы высшего образовательного учреждения, где выполнена диссертация. Диссертационная работа выполнена в рамках приоритетного направления плана научных исследований Ташкентского государственного педагогического университета под названием «Изучение истории психологии, освоение содержания общей психологии, классификация психологии личности, расширение сферы психофизиологических исследований, изучение закономерностей медицинской и профессиональной психологии, исследование социальной психологии, этнопсихологии и концептуальных основ молодежной и педагогической психологии» (2020-2024).

Целью исследования Разработка методических рекомендаций по совершенствованию программного обеспечения для развития интеллектуальной компетентности будущих учителей.

Задачи исследования:

определение педагогических возможностей преподавания дисциплины «Основы кибербезопасности» в период информационной атаки;

совершенствование содержания программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в период информационной атаки;

совершенствование модели формирования киберэтической культуры студентов в процессе преподавания дисциплины «Основы кибербезопасности»;

---

[54] Алтуфьева А.А. Методические основы обучения информационной безопасности на базе телекоммуникационных ресурсов сети интернет. Дисс. на соиск. ученой степени канд. пед. наук. - Санкт-Петербург, 2008. – 132 с.

[55] Баранова Э.К. Бабаш А.Б. Информационная безапасност и зашита информации / - М.: ИНФРА-М -РИОР, 2014 г., 216 с.

[56] Бондаревская, Е.В. Гуманистическая парадигма личностно-ориентированного образования / Е.В.Бондаревская // Педагогика.1997. - №4.-С. 11-17.

[57] Бородакий.Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века.

[58] Красильникова В.А. Использование информационных и коммуникационных технологий в образовании. Учебное пособие. Оренбургский гос. ун-т.– 2-е изд. – Оренбург: ОГУ, 2012. – 291 с.

[59] Лукацкий А.В.Краткий толковый словар по информационной безопасности. М.2000. с 72

[60] Моисеев Н.Н. Расставание с простотой. –М., 2000. -473 с

[61] Alter S. The Work System Method: Connecting People, Processes, and IT for Business Results. Works System Press, CA. 2006 y.

[62] Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems (2nd ed.). Indianapolis: Wiley. ISBN: 978-0-470-06852-5. 2008 y.

[63] Yar Majid and Kevin F. Steinmetz. Cybercrime and society. SAGE. 2019 y.

[64] Ujjwal Rao. Student, B. Tech, Department of Computer Science and Engineering Dronacharya College of Engineering, Gurgaon, Haryana, India

[65] Jan de Lange and William Schmidt. What are PISA and TIMSS? What do they tell us? https://www.researchgate.net/publication/41537659 What are PISA and TIMSS What do they tel us.

[66] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in *C* (2nd ed.). New York: John Wiley & Sons. ISBN: 978-0-471-11709-4.

совершенствование методики внедрения программно-методического обеспечения на основе обогащения учебно-методического обеспечения преподавания дисциплины «Основы кибербезопасности»;

определение эффективности внедрения электронной платформы, направленной на совершенствование учебно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в период информационной атаки.

Объектом исследования является процесс совершенствования учебно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в период информационной атаки, в экспериментальном исследовании приняли участие 497 студентов 1–4 курсов Самаркандского, Каршинского и Ферганского филиалов Ташкентского университета информационных технологий.

Предметом исследования являются, формы, методы и средства совершенствования учебно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в период информационной атаки.

Методы исследования. В процессе исследования использовались такие методы, как педагогическое наблюдение, сравнительный анализ, обобщение, социологические методы (анкетирование, вопросно-ответный опрос, интервью, экспертная оценка), педагогическое экспериментальное тестирование, математико-статистический анализ.

Научная новизна исследования заключается в следующем:

определены педагогические возможности совершенствования преподавания дисциплины «Основы кибербезопасности» в период информационной атаки на основе формирования единой подходовой среды, направленной на обеспечение приоритета интересов личности, общества и государства в киберпространстве в соответствии с законностью методов защиты, и классификации основных принципов, влияющих на формирование киберэтической культуры студентов в условиях киберугроз;

усовершенствовано содержание программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в период информационной атаки на основе определения соответствия смысловой структуры терминов безопасности образовательным целям, внедрения современных методов защиты шифрование-кодирование, криптографических алгоритмов, сетевой безопасности и хранения данных, обеспечения пропорциональной совместимости пользовательского интерфейса с процессами идентификации, аутентификации и конфиденциальности;

усовершенствована модель формирования киберэтической культуры студентов в процессе преподавания дисциплины «Основы кибербезопасности» на основе нивелирования актуальных проблем обеспечения информационной безопасности, соотнесения специфических дифференциальных признаков информации и кибербезопасности с системно-структурным анализом и аргументацией решений глобальных проблем, целенаправленного сочетания принципов преемственности, междисциплинарной релевантности с когнитивным, контекстным, интегративным и деятельностным подходами;

усовершенствована методика внедрения программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак на основе интерактивных методов, эффективного использования возможностей аудиовизуальной информации, блокчейна, облачных технологий, методов контроля и самоконтроля, позволяющих оперативно реагировать на информационные угрозы и стратегии кибератак в виртуальном пространстве, адаптации производных, ассоциативных единиц обучения к цифровым образовательным средствам, иерархической систематизации компонентов, лежащих в основе формирования киберэтической культуры.

усовершенствована эффективность формирования киберэтической культуры студентов в процессе обучения дисциплине «Основы кибербезопасности» на основе обеспечения информационной безопасности, целенаправленного использования программных и технических средств, уточнения классификации сетей, изучения влияния информационных атак на образовательный процесс, динамического приоритета уровней когнитивного, коммуникативного мышления, устойчивого развития интегративных и креативных навыков противодействия студентам киберугрозам.

Практические результаты исследования заключаются в следующем:

усовершенствована модель совершенствования программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в период информационной атаки;

создан учебник «Основы кибербезопасности» (Сертификат № 11-05-7601/04 Министерства высшего образования, науки и инноваций), оказывающий методическую поддержку будущим учителям по внедрению в образовательный процесс передовых педагогических и инновационных методов, платформа онлайн-обучения «EduCyberSecurity» (Сертификат № DGU 46759 Министерства юстиции Республики Узбекистан) и мобильное приложение «Основы кибербезопасности» (Сертификат № DGU 46916 Министерства юстиции Республики Узбекистан).

Достоверность результатов исследования определяется тем, что они базируются на опыте отечественных и зарубежных ученых в философских, педагогических и психологических, методологических подходах к проблеме и технологических направлениях, используются методы исследования, совместимые с задачами исследования и взаимодополняющие друг друга, анализ и описание которых количественно и качественно обеспечены; эффективность экспериментально-испытательной работы базируется на математических и статистических методах, полученные результаты подтверждены уполномоченными структурами, выводы и рекомендации реализованы на практике.

Научная и практическая значимость результатов исследования.

Научная значимость исследования заключается в его практической направленности в формировании киберэтической культуры, стилистической дифференциации, творческой направленности образования, принципах междисциплинарной интеграции и внутридисциплинарной интеграции;

компетентностном, личностно-ориентированном, социолингвистическом, интегративном, социокультурном, коммуникативном и системном подходах; Четыре этапа комплексного обеспечения компонентов образовательного контента (лингвистического, социолингвистического, социокультурного, прагматического) и электронно-дидактических средств в инновационных образовательных условиях поясняются уточнением оптимальных путей решения педагогических задач и достижения результатов.

Практическая значимость исследования заключается в том, что полученные результаты, предложения и рекомендации по совершенствованию программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак, а также разработанные программно-методические материалы могут быть применены в образовательном процессе. Их можно использовать при создании и обновлении учебников с использованием современных ресурсов и методов, а также при организации мониторинга для оценки уровня знаний, умений и квалификации студентов.

Внедрение результатов исследования. На основе результатов исследований по совершенствованию методики развития научно-исследовательских компетенций студентов магистратуры начального образования:

предложение по определению педагогических возможностей совершенствования преподавания дисциплины «Основы кибербезопасности» в период информационной атаки на основе формирования единой подходовой среды, направленной на обеспечение приоритета интересов личности, общества и государства в киберпространстве в соответствии с законностью методов защиты, и классификации основных принципов, влияющих на формирование киберэтической культуры студентов в условиях киберугроз включено в содержание учебника «Основы кибербезопасности» (Разрешение на издание Ташкентского государственного педагогического университета № 11-05-7601/04 от 28 декабря 2024 г.). В результате расширено содержание преподавания дисциплины «Основы кибербезопасности»;

предложение по усовершенствованию содержания программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в период информационной атаки на основе определения соответствия смысловой структуры терминов безопасности образовательным целям, внедрения современных методов защиты шифрование-кодирование, криптографических алгоритмов, сетевой безопасности и хранения данных, обеспечения пропорциональной совместимости пользовательского интерфейса с процессами идентификации, аутентификации и конфиденциальности включено в содержание учебника «Основы кибербезопасности» (Разрешение на издание Ташкентского государственного педагогического университета № 11-05-7601/04 от 28 декабря 2024 г.). В результате расширено содержание учебно-методического обеспечения преподавания дисциплины «Основы кибербезопасности»;

предложение по усовершенствованию модели формирования киберэтической культуры студентов в процессе преподавания дисциплины

«Основы кибербезопасности» на основе нивелирования актуальных проблем обеспечения информационной безопасности, соотнесения специфических дифференциальных признаков информации и кибербезопасности с системно-структурным анализом и аргументацией решений глобальных проблем, целенаправленного сочетания принципов преемственности, междисциплинарной релевантности с когнитивным, контекстным, интегративным и деятельностным подходами включено в содержание учебника «Основы кибербезопасности» (Разрешение на издание Ташкентского государственного педагогического университета № 11-05-7601/04 от 28 декабря 2024 г.). В результате студенты смогли выявить актуальные проблемы обеспечения информационной безопасности и развития своих компетенций;

предложение по усовершенствованию методики внедрения программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак на основе интерактивных методов, эффективного использования возможностей аудиовизуальной информации, блокчейна, облачных технологий, методов контроля и самоконтроля, позволяющих оперативно реагировать на информационные угрозы и стратегии кибератак в виртуальном пространстве, адаптации производных, ассоциативных единиц обучения к цифровым образовательным средствам, иерархической систематизации компонентов, лежащих в основе формирования киберэтической культуры включено в содержание учебника «Основы кибербезопасности» (Разрешение на издание Ташкентского государственного педагогического университета № 11-05-7601/04 от 28 декабря 2024 г.). В результате были достигнуты положительные результаты в освоении дисциплины «Основы кибербезопасности».

предложение по усовершенствованию эффективности формирования киберэтической культуры студентов в процессе обучения дисциплине «Основы кибербезопасности» на основе обеспечения информационной безопасности, целенаправленного использования программных и технических средств, уточнения классификации сетей, изучения влияния информационных атак на образовательный процесс, динамического приоритета уровней когнитивного, коммуникативного мышления, устойчивого развития интегративных и креативных навыков противодействия студентам киберугрозам включено в содержание учебника «Основы кибербезопасности» (Разрешение на издание Ташкентского государственного педагогического университета № 11-05-7601/04 от 28 декабря 2024 г.). В результате уточнены аспекты формирования киберэтической культуры у студентов в период информационной атаки.

Апробация результатов исследования. Результаты исследования были обсуждены на 2-х международных и 2-х республиканских научно-практических конференциях.

Публикация результатов исследования. Всего по теме диссертации опубликованы 26 научно-методических работ, в том числе 1 монография. 11 статьи опубликованы в научных изданиях, рекомендованных Высшей аттестационной комиссией публикации основных научных результатов

диссертаций, в том числе 10 - в республиканских журналах и 1 - в зарубежном журнале.

Структура и объём диссертации. Диссертация состоит из введения, 3 глав, заключения, списка использованной литературы и приложений, основной объём диссертации составляет 240 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обоснована актуальность и необходимость темы диссертации на научной основе, уровень изученности проблемы. Определяются цели и задачи, объект и предмет научно-исследовательской работы, обосновывается соответствие научно-исследовательской работы важным направлениям развития науки и техники. Также приводятся сведения о научной новизне научно-исследовательской работы, достоверности полученных результатов, теоретической и практической значимости работы, внедрении полученных результатов в практику, публикации результатов в научных трудах, структуре работы.

В первой главе диссертации под названием «**Научно-теоретические основы развития преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак»** излагаются научно-методические основы развития информационной безопасности и кибербезопасности, сущность их специфических дифференциальных признаков, а также дается характеристика методического обеспечения преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак.

Сегодня для представителей каждой отрасли — руководителей, служащих, учащихся, студентов и всех молодых людей — работа с социальными сетями, компьютерными технологиями, их поиск и использование стали обычной практикой. Поэтому важно эффективно использовать информационные системы, искать информацию, актуальную для отрасли, и использовать ее в полезных целях. В результате у человека развивается мировоззрение, художественное мышление, речевые способности, научно-интеллектуальный потенциал, повышается значимость процесса информатизации в различных сферах повседневной деятельности. Это позволяет быть в курсе современной действительности. В целом эффективная работа с информацией в профессиональной и личной жизни оказывает положительное влияние на развитие этой отрасли. Поэтому важно в процессе поиска информации уделять внимание таким аспектам, как ее надежность, полезность и эффективность. Также необходимо уделять особое внимание безопасности информации, направленной на конкретные цели.

О том, что политика нашего государства в сфере обеспечения информационной безопасности продолжается и по сей день, можно судить на примере принимаемых на практике новых законодательных актов. В пятом приоритетном направлении «Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан на 2017-2021 годы», утвержденной Указом Президента Республики Узбекистан от 7 февраля 2017

года № УФ-4947 под названием «Обеспечение безопасности, межнационального согласия и религиозной толерантности, приоритеты в области продуманной, взаимовыгодной и практичной внешней политики», в качестве отдельного направления выделен вопрос обеспечения информационной безопасности и совершенствования системы защиты информации, своевременного и адекватного противодействия угрозам в информационной сфере, а также особое внимание уделяется организации семинарских тренингов, направленных на предотвращение информационных атак, несущих угрозу сознанию студентов, и формирование у студентов культуры пользования Интернетом и другими информационными ресурсами.

В этой связи в нашей стране ученые Б.Ходжаев и М.Курбонов в своих исследованиях по информационным атакам, технологиям защиты от информационных атак, а также О.Г.Давлатов в своем исследовании на тему «Формирование компетентности студентов в обеспечении информационной безопасности посредством историко-культурного наследия» подчеркивают: «Информационная атака или угроза — это совокупность условий и факторов, создающих угрозу жизненно важным интересам личности, общества и государства в информационной сфере». В этой связи мы считаем, что необходимо разработать комплекс мер по обеспечению информации и ее безопасности.

Пока наблюдаются информационные атаки, обеспечение информационной безопасности является одним из важных вопросов. По мнению С.К.Ганиева, М.М.Каримова, К.А.Ташаева, «Информационная безопасность характеризуется защищенностью информации от неправомерного (для соответствующих субъектов информационных отношений) разглашения (нарушения конфиденциальности), нарушения ее целостности, утечки, утраты, изменения или снижения уровня полезности, а также неправомерного оборота. Причиной этих событий могут быть случайные воздействия или воздействия, возникшие в результате преднамеренного несанкционированного использования злоумышленником (злонамеренного умысла). А.Х.Мухитдинов утверждает, что «Информационная безопасность представляет собой состояние информационной системы, при котором она способна противостоять воздействию внутренних и внешних угроз элементам системы и внешней среде, не допуская их возникновения». По мнению А.Лукацкого, «При рассмотрении проблемы информационной безопасности такие важные факторы, как угрозы информационной безопасности, необходимо подробно остановиться на этих аспектах. Поскольку именно они являются источником нарушений информационной безопасности. Угрозы информационной безопасности определяются как действия, процессы и события, которые с высокой вероятностью могут нарушить конфиденциальность информации, а также привести к ее незаконному распространению.

Исходя из вышеприведенного анализа, информационная безопасность - это практика предотвращения несанкционированного доступа, использования, раскрытия, изменения, модификации, поиска, записи или уничтожения

информации. Эта общая концепция применяется независимо от того, находится ли информация в какой-либо форме - электронной или физической.

У.Гофуров отметил, что «культура потребления информации в самом общем смысле означает систему знаний, умений и навыков, которые служат получению, сортировке, пониманию и интерпретации информации из информационного потока, служащего интересам человека, развитию и общественному развитию. Защита информации – это: обеспечение физической целостности информации, то есть предотвращение компрометации и потери элементов информации; предотвращение замены (изменения) элементов информации при сохранении ее целостности; предотвращать несанкционированный доступ к информации со стороны лиц или процессов, не имеющих соответствующих полномочий; это означает, что переданные собственникам ресурсы должны использоваться только в соответствии с условиями, согласованными сторонами.

По мнению индийского ученого Уджвала Рао, кибербезопасность — это набор средств, политик, концепций безопасности, мер безопасности, руководств, подходов к управлению рисками, действий, обучения, передового опыта, доверия и технологий, которые могут быть использованы для защиты киберсреды и активов организации и пользователей. Она включает в себя набор вычислительных устройств, подключенных к организации и активам пользователей, персонал, инфраструктуру, приложения, услуги, телекоммуникационные системы и информацию, передаваемую или хранимую в киберсреде. «Текущая проблема кибербезопасности стала предметом научно-теоретического изучения и создания образовательного программного обеспечения и методической поддержки специалистами в этой области. Кибербезопасность, кибероборона и методология разработки защитной системы в ней считаются основными проблемами. Подчеркивается, что М.Экхарт, У.Франк, Дж.С.Околица и другие проводили исследования в рамках проблем, связанных с решением этой проблемы, в отношении киберситуационной осведомленности и мониторинга киберсреды.

На основе представленных выше идей ученых мы создали авторское определение: «Кибербезопасность — это процесс защиты, контроля и предотвращения информации посредством стабильной, надежной и эффективной системы».

В данной главе также приводятся и объясняются особенности и отличительные аспекты информационной безопасности и кибербезопасности, некоторые международные стандарты (ISO/IEC 27001, NIST Cybersecurity Framework), лексическая семантика кибербезопасности (случайные и целенаправленные угрозы), актуальность проблемы обеспечения информационной безопасности, основные различия между информационной безопасностью и кибербезопасностью, анализ их научных основ и функциональных границ, а также научные определения важнейших понятий (целостность информации, идентификация, аутентификация, авторизация, контроль доступа, владение).

Эти процессы являются неотъемлемой частью системы управления информационной безопасностью и имеют основополагающее значение для защиты данных.

Существуют различные подходы к определению основных терминов кибербезопасности. В частности, некоторые эксперты определяют термины кибербезопасности следующим образом:

процесс обеспечения конфиденциальности — это состояние информации или ее носителя таким образом, что к ней невозможно получить доступ или скопировать ее без разрешения. Процесс обеспечения конфиденциальности связан с защитой информации от несанкционированного «чтения». Процесс обеспечения конфиденциальности особенно важен для банка в банковской системе.

Риск — это потенциальная возможность получения прибыли или убытка, и обычно возникает, когда вероятность наступления события добавляется к любой ситуации. ISO определяет риск как влияние неопределенности на цели. Информационный риск — это вероятность потери или ущерба, которые могут возникнуть в результате использования информационных технологий на предприятиях. Таким образом, информационные риски связаны с передачей, хранением и использованием любой информации с использованием электронных концепций и других средств связи.

Рисунок 1. Семантическая структура терминов в преподавании науки о кибербезопасности

Информационная безопасность — состояние информации, при котором не допускается случайное или преднамеренное вмешательство в нее или ее использование без разрешения. Или состояние защищенности информации, при котором обеспечивается сохранение ее характеристик (свойств), таких как конфиденциальность, целостность и удобство использования при обработке

информации с использованием технических средств. Кибербезопасность подразделяется на восемь областей знаний: безопасность данных; безопасность программного обеспечения; организационная безопасность; безопасность коммуникаций; безопасность систем; безопасность человека; организационная безопасность; социальная безопасность.

Создание программного обеспечения для совершенствования сферы кибербезопасности приводит к задаче составления терминологии, глоссария и самостоятельного изложения этой дисциплины.

С.К.Ганиев, А.А.Ганиев, З.Т.Худойкулов выпустили учебник «Основы кибербезопасности». В учебнике изложены вопросы применения кибербезопасности и ее основных понятий, криптографической защиты информации, разграничения доступа, сетевой безопасности, методов обеспечения удобства использования, безопасности программного обеспечения, политики информационной безопасности и управления рисками, киберпреступности, киберправа, киберэтики, а также теоретические и практические основы безопасности человека.

Другим образовательным объектом в преподавании информационной безопасности и кибербезопасности является учебник «Основы информационной безопасности», составленный Б.Таировым. В данном учебнике рассматриваются содержание предмета безопасности информационных систем, предмет информационной безопасности, сущность аудита, его цели и задачи, основные понятия обеспечения информационной безопасности, угрозы, методы защиты, этапы защиты от кибербезопасности и кибератак, анализ смежных понятий и пояснения терминов, темы и теоретические сведения об основных программных и технических средствах обеспечения информационной безопасности, научные взгляды отраслевых специалистов, аналитические подходы, выводы исследований. Глава I учебника содержит пояснения таких словарных единиц, как информационная безопасность, секретная информация, документированная информация, конфиденциальная информация по теме информационной безопасности, киберпреступность и угрозы информации. Защита информации представляет собой комплекс мер, направленных на обеспечение важных аспектов информационной безопасности (целостность информации, доступность и при необходимости конфиденциальность информации и ее ресурсов, используемых при вводе, хранении, обработке и передаче информации). В защищенной системе доступ к информации контролируется лицами, имеющими право читать, писать, создавать и удалять информацию, или процессами, осуществляемыми от их имени, с использованием соответствующих аппаратных и программных средств. Также описаны этапы разработки Концепции защиты информации.

1 этап. Определение стоимости охраняемого объекта;

2 этап. Анализ возможных действий злоумышленника;

3 этап. Оценка средств защиты информации.

Понятие защиты информации совпадает с объектом защиты и в нем размещается необходимый, необходимый учебный материал. С этой точки

зрения одним из важных опытов является оценка средств защиты информации и их механизма вблизи объекта.

Таким образом, комплексное совершенствование процесса преподавания дисциплины «Основы кибербезопасности», развитие ее методического обеспечения на основе инновационных технологий и международных стандартов, обогащение ее политикой безопасности, нормативно-правовыми актами и методами практического применения являются важными факторами обеспечения безопасности и устойчивости цифровой инфраструктуры.

Во второй главе диссертации под названием **«Концептуальное содержание совершенствования программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак»** рассматриваются семантика концептуального анализа в преподавании дисциплины «Основы кибербезопасности», особенности информационной системы в разработке программного обеспечения, специфика повышения квалификации в преподавании дисциплины.

Одной из главных задач является подготовка высококвалифицированных специалистов, которые внесут достойный вклад в социально-экономическое развитие сферы образования, дальнейшее совершенствование теории и методологии электронного обучения, подготовка профессионально квалифицированных кадров для страны, внедрение в обучение инновационных методов и передовых технологий. В этой связи ключевую роль играет работа с информацией и ее использование, преподавание требований кибербезопасности. Также 15 апреля 2022 года Законодательной палатой Республики Узбекистан был принят Закон № O'RQ-764 «О кибербезопасности». В данном Законе установлены основные принципы обеспечения кибербезопасности, которыми являются: законность; приоритет защиты интересов личности, общества и государства в киберпространстве; единый подход к регулированию сферы кибербезопасности; приоритет участия местных производителей в создании системы кибербезопасности; Поставлен ряд задач по открытости Республики Узбекистан к международному сотрудничеству в обеспечении кибербезопасности.

Как известно, в эпоху инновационного развития мы являемся свидетелями того, что современные новые технологии и электронные услуги стали неотъемлемой частью нашей повседневной жизни. В системе образования и учебном процессе нормативное применение информационно-коммуникационных и информационных подходов, их защита и использование, направление на эффективные цели имеют большое значение и становятся актуальным вопросом. В частности, в этой связи для обеспечения кибербезопасности каждой организации, предприятия, учреждения привлекаются сотрудники, занятые в этой сфере, и организуется ряд семинарских занятий для постоянного ознакомления сотрудников со знаниями по кибербезопасности. Также стоит отметить, что кибербезопасность также преподается как предмет в высших учебных заведениях, определены цели и задачи изучения этого предмета. В эпоху информационных атак большое значение имеет совершенствование программного и методического обеспечения

преподавания дисциплины «Основы кибербезопасности». В Постановлении Президента Республики Узбекистан № ПП-4996 от 17 февраля 2021 года поставлен ряд задач. Анализ национальных стратегий ряда передовых стран в области искусственного интеллекта позволяет выделить следующие пять направлений в качестве приоритетных для нашей страны: проведение фундаментальных прикладных исследований в области искусственного интеллекта - создание новых алгоритмов искусственного интеллекта с использованием математических методов; развитие техники искусственного интеллекта — применение алгоритмов, полученных в результате фундаментальных прикладных исследований, для решения различных практических задач, разработка новых программных и технологических решений; данные - их сбор, хранение, обработка и оптимизация (для обучения алгоритмов); подготовка кадров - подготовка высококвалифицированных научных кадров и специалистов в области искусственного интеллекта, создание новых образовательных программ; законодательная база — разработка и внедрение законов, стандартов и этических правил, поддерживающих развитие технологий искусственного интеллекта.

Политика кибербезопасности представляет собой стратегию достижения целей кибербезопасности и предоставляет своим составляющим руководство по надлежащему использованию мер кибербезопасности. Направление может быть установлено общественным договором или руководящим органом. Мы также признаем, что независимые предприятия должны разрабатывать руководящие принципы управления для поддержки своей стратегии кибербезопасности, и мы используем измененный термин «политика предприятия» для обозначения только политик, которые применяются в рамках конкретного корпоративного сообщества. Как правило, такие корпоративные политики часто основаны на стандартах кибербезопасности, установленных Международной организацией по стандартизации (ISO) (ISO/IEC 2005 a,b) и NIST (Ross, Katzke и др. 2007). Такие стандарты обычно включают комбинацию технологических руководств с рекомендациями по технологическому контролю.

Эффективность образования в области кибербезопасности напрямую связана не только с технологическими знаниями, но и с семантически правильным и последовательным освещением анализа ключевых понятий. Семантика — это изучение смысла этих понятий, их контекстного использования и их взаимосвязей с различными дисциплинами и технологиями. Термины в области кибербезопасности должны анализироваться в соответствии с международными стандартами информационной безопасности, правовыми нормами, техническими нормативными документами и научной литературой.

Семантический анализ в учебном процессе по данной дисциплине должен охватывать следующие основные принципы:

системность — применение концепций кибербезопасности в различных контекстах и их место в экосистеме информационных технологий.

Терминологическая согласованность — приведение терминологии, связанной с кибербезопасностью, в соответствие с международно признанными стандартами и ее интеграция в национальную систему образования.

Структурный подход — изучение концепций кибербезопасности в различных областях, включая криптографию, процессы аутентификации, сетевую безопасность, киберпреступность и правовые аспекты.

Теоретически семантический анализ концепций кибербезопасности позволяет понять взаимосвязи между наукой и технологиями, а также обеспечить ясность и понятность терминологии для студентов и специалистов.

Глубокое семантическое понимание концепций кибербезопасности также важно для их практического применения. В процессе практического обучения эффективны следующие методы:

интерактивные методы обучения — объяснение студентам основных концепций кибербезопасности с помощью виртуальных лабораторных работ, моделирования и анализа реальных кибератак.

Анализ case-study и реальных ситуаций — углубленное изучение кибератак, произошедших на практике, и семантический анализ терминов, связанных с ними.

Моделирование протоколов компьютерной безопасности — визуализация того, как такие процессы, как криптография, аутентификация и авторизация, работают в рамках программной среды.

Терминологическая система, основанная на международных стандартах, — интеграция концепций, соответствующих международным стандартам информационной безопасности, таким как ISO/IEC 27001, NIST Cybersecurity Framework, GDPR, OWASP, в национальную систему образования.

С практической точки зрения правильный семантический анализ концепций кибербезопасности может улучшить поведение пользователей в сфере безопасности и навыки защиты информации. В частности, правильная терминология и концептуальный анализ играют важную роль в методах обнаружения и предотвращения угроз, основанных на современных алгоритмах искусственного интеллекта и машинного обучения.

Семантический подход важен для эффективного преподавания и анализа понятий по предмету «Основы кибербезопасности». Семантический анализ помогает анализировать содержание понятий, их применение в технологических, правовых и стратегических контекстах. Содержание основных понятий, используемых по предмету «Основы кибербезопасности»: кибербезопасность, информационная безопасность, криптография, сетевая безопасность, киберпреступность, киберугрозы, кибератаки, процесс идентификации и аутентификации, авторизация, контроль доступа, политика информационной безопасности, киберэтика, киберправо, средства киберзащиты. управление рисками, анализ и аудит безопасности, защита информационных активов. Внимание было уделено содержанию искусственного интеллекта и кибербезопасности.

Семантический анализ является важным компонентом учебного процесса при преподавании дисциплины «Основы кибербезопасности». Правильно и последовательно изучая понятия, интерпретируя их в соответствии с международными и национальными стандартами, можно сформировать у студентов фундаментальные знания и практические навыки в области

информационной безопасности. В то же время закрепление этих понятий с помощью практических упражнений, моделирования и аналитических исследований служит повышению эффективности дисциплин по кибербезопасности.

Согласно приведенному выше определению, информационные системы с точки зрения кибербезопасности подразделяются по ключевым характеристикам (структурная сложность, многоуровневая модель безопасности, управление доступом и полномочиями к информации, целостность и конфиденциальность информации, сетевая безопасность и мониторинг трафика, аудит безопасности и мониторинг угроз).

Роль информационных систем в разработке программного обеспечения для дисциплины «Основы кибербезопасности» значительна. «Информационная система (ИТ) — это система, предназначенная для хранения, извлечения и обработки информации, предоставления и распространения информации, а также предоставления связанных с ней организационных ресурсов (человеческих, технических, финансовых и т.д.)». Компьютерная информационная система — это система, состоящая из людей и компьютеров, которые обрабатывают или интерпретируют информацию.

Использование современных компьютерных систем и их сетей предполагает такие требования, как просмотр информации, копирование определенных текстов, работа со специальными программными и аппаратными ресурсами, получение различных сообщений. При этом совершенствование процесса обучения кибербезопасности в данной области, в частности разработка программного и методического обеспечения, является одним из важных факторов. В ходе исследования основной целью было популяризация методов повышения квалификации с использованием интернет-ресурсов для совершенствования методики преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак, реализация интерактивного подхода в данном процессе, а также приоритетность принципов научности и обучения.

По нашему мнению, для достижения высокой эффективности разработки программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в условиях информационных атак актуальны такие направления, как создание современных методов передачи и сбора информации, развитие интеллектуального и творческого потенциала в сфере электронной информационной безопасности, эффективное использование педагогического мастерства и технологических средств. Также неотъемлемой частью этого процесса является разработка акме-технологий, обеспечивающих возможность формирования самостоятельного профессионального мышления и саморазвития.

В данной главе рассматриваются важные подходы в разработке программного и методического обеспечения преподавания дисциплины «Основы кибербезопасности» (теория компетентностного подхода, конструктивистская теория обучения, теория обучения на основе опыта, таксономия Блума и образование в области кибербезопасности, теория интерактивного обучения). Перечисленные подходы в основном ориентированы

на целесообразность организации специфики профессионального развития в сочетании с практикой на основе таких подходов, как компетентностный, конструктивистский, опытный, пошаговое обучение на основе таксономии Блума и интерактивное обучение. Поэтому в подготовке специалистов по кибербезопасности важно использовать интерактивный и практический подходы, наряду с традиционными методами обучения. Интеграция этих научных теорий позволяет готовить высококвалифицированных специалистов, отвечающих требованиям современной киберсреды.

Также указано, что компоненты личностно-профессионального саморазвития при обучении основам кибербезопасности следуют логической последовательности действий: формирование внутренней мотивации и проектирование процесса саморазвития; выполнение действий в соответствии с индивидуальной траекторией профессионального развития; рефлексия и принятие корректирующих мер по результатам процесса личностно-профессионального саморазвития.

Во второй главе диссертации под названием **«Совершенствование программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности»** в эпоху информационных атак» представлена модель совершенствования программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности», технология, для которой разработаны дидактические принципы, и инновационные методы их разработки.

Предмет изучения педагогических, методических, психологических, технических и организационных возможностей образовательного процесса тесно связан с радикальными изменениями в образовательной среде, вызванными современными технологиями.

По результатам научных исследований и аналитических наблюдений совершенствование программно-методического обеспечения процесса преподавания дисциплины «Основы кибербезопасности» в условиях информационных атак требует формирования целостной системы, в основе которой лежат следующие структурные элементы: учебно-методические принципы, принципы обучения, критерии оценки, образовательные тенденции и модели развития. Данные компоненты рассматриваются как основные средства формирования содержания образования по кибербезопасности, повышения качества образования и обеспечения эффективности образовательного процесса. Таким образом, становится возможным создание современной методической базы преподавания данного предмета за счет внедрения передовых образовательных подходов и технологий.

Основной целью совершенствования программно-методического обеспечения обучения студентов по предмету «Основы кибербезопасности» в эпоху информационных атак является обучение их концептуальным основам терминологии кибербезопасности и ее практическому применению, а также навыкам личностно-профессионального, креативно-логического, индивидуально-профессионального развития и психологического роста в использовании компьютерной информации.

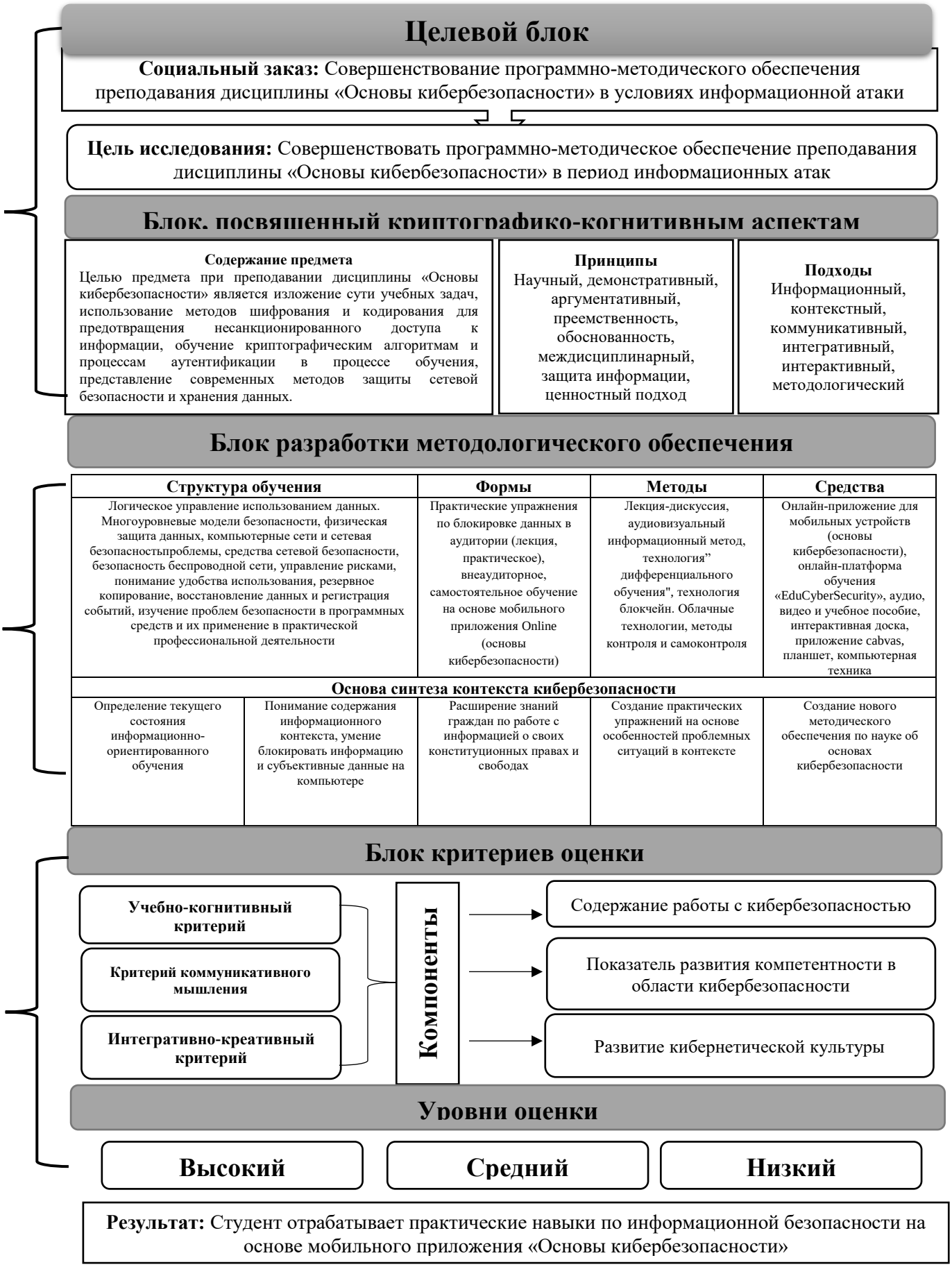


Рисунок 2. Модель совершенствования программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак

Большое значение имеет воспитание у студентов молодежи значимости информационной этики, полезной для общества и человека, учета конституционных прав и свобод граждан при работе с информацией, ненанесения ущерба объектам интеллектуальной собственности, сохранения национального духовного наследия, развития духовных и общечеловеческих традиций, пропаганды нравственных норм, формирования правовых аксиологических знаний. При создании учебно-методического обеспечения необходимо разъяснять развитие современных информационных технологий, создавать среду для развития научного потенциала, и этот аспект нашел свое отражение в созданной нами модели.

Модель совершенствования программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак включает четыре блока. К ним относятся: блок когнитивно-грамматических подходов, блок контекстно-содержательных аспектов, блок разработки методического обеспечения и блок критериев оценки. Блок криптографо-когнитивных аспектов модели охватывает содержание, задачи и принципы предмета реализации шифрования и кодирования, препятствующие несанкционированному доступу к обрабатываемой и передаваемой информации.

В процессе преподавания дисциплины «Основы кибербезопасности» совершенствовалась модель формирования киберэтической культуры у студентов на основе нивелирования актуальных проблем обеспечения информационной безопасности, учета специфических дифференциальных характеристик информации и кибербезопасности, системно-структурного анализа и аргументации решений глобальных проблем, целенаправленной адаптации принципов преемственности и междисциплинарных связей к когнитивному, контекстному, интегративному и деятельностному подходам, в рамках которой актуальными на сегодняшний день являются такие вопросы, как формирование знаний и умений студентов на основе информационной этики, овладение принципами работы с информацией в соответствии с интересами общества и человека, а также с учетом конституционных прав и свобод граждан, предотвращение нанесения ущерба объектам интеллектуальной собственности. При этом сохранение национального духовного наследия, развитие общечеловеческих ценностей и традиций, пропаганда этических норм, совершенствование правовых и аксиологических знаний студентов.

Развитие современных информационных технологий требует более глубокого изучения проблем, связанных с обеспечением информационной безопасности. Поэтому актуальны разработка научных основ и принципов приоритетности в рамках науки, модернизация методического обеспечения, формирование инновационной образовательной среды. Эти аспекты нашли отражение в разработанной нами модели.

Модель, разработанная с целью совершенствования методики преподавания дисциплины «Основы кибербезопасности» в условиях возрастающей угрозы информационных атак, включает четыре основных блока:

Блок, посвященный криптографо-когнитивным аспектам, формирует образовательный процесс по формированию базовых понятий, теоретических положений и правовых основ информационной безопасности.

Блок «Конфиденциальность и управление рисками» включает в себя практические занятия по кибербезопасности, анализ реальных проблем и вопросов, а также задания на расширение знаний студентов в области информационной безопасности.

Блок разработки методического обеспечения организован на основе методик, направленных на использование современных технологий обучения, интерактивных методов образовательного процесса, опытного обучения, формирование самостоятельных траекторий обучения.

Блок критериев оценки включает в себя систему определения знаний и практических навыков студентов в области кибербезопасности, оценку их навыков рефлексивного мышления, а также мониторинг их профессионального развития.

Блок модели, ориентированный на криптографо-когнитивные аспекты, фокусируется на технологиях защиты информации.

В данном блоке рассматриваются вопросы выражения сущности образовательных задач как объекта предмета при преподавании дисциплины «Основы кибербезопасности», использования методов шифрования и кодирования для предотвращения несанкционированного доступа к информации, обучения криптографическим алгоритмам и процессам аутентификации в образовательном процессе, внедрения современных методов защиты сетевой безопасности и хранения данных и т.д.

При этом в рамках данной модели комплексно освещаются основные принципы, подходы, содержание и основные задачи информационной безопасности. Данный методический подход служит обеспечению повышения студентами культуры работы с информацией, освоения ими принципов защиты интеллектуальной собственности, приобретения практических навыков в области кибербезопасности.

На основе обобщения результатов международных и отечественных научных исследований, анализа нормативных документов разработаны следующие дидактические принципы совершенствования программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в период информационных атак, позволяющие студентам использовать информацию в позитивных целях и реализовывать самостоятельное и непрерывное личностное и методическое развитие в высокоэффективной практике.

Совершенствование процесса преподавания дисциплины «Основы кибербезопасности» и разработка ее методического и программного обеспечения базируется на ряде основополагающих принципов. К таким принципам относятся научность, демонстрация, аргументация, преемственность, обоснованность, междисциплинарная релевантность, защита информации, киберэтика, ценностный подход.

Принцип аргументации. На основе этого принципа студенты учатся обосновывать полученные в процессе обучения знания, подкреплять их доказательствами, логически мыслить и аргументированно отстаивать свою точку зрения. Любая идея или предложение должны основываться на четких доказательствах, фактах, опыте или теоретической базе. Процесс аргументации принимает форму диалога, дебатов или обсуждения, в ходе которых синтезируются и проясняются идеи. С этой точки зрения темы, представленные в нашем программном обеспечении, взаимосвязаны и представлены в логической последовательности. В результате у студентов развиваются навыки критического и логического мышления, навыки самостоятельного принятия решений и обоснования. Урок учит тому, как четко и с опорой на доказательства выражать свое мнение.

Таким образом, основываясь на принципе аргументации, студенты развивают навыки выражения любой мысли, идеи или решения обоснованным, доказательным и логичным образом.

Принцип демонстрации. Совершенное освоение дисциплины «Основы кибербезопасности» студентами основано на представлении учебного материала в понятной, впечатляющей и запоминающейся форме посредством просмотра, прослушивания и экспериментирования в процессе обучения. Предмет «Основы кибербезопасности» предназначен для демонстрации теоретических знаний на практике посредством инфографики, презентаций, графических иллюстраций и моделирования на основе программного обеспечения. В результате он стимулирует мышление студентов, обеспечивает их активное участие и служит закреплению знаний.

Научный принцип. Совершенное освоение студентами дисциплины «Основы кибербезопасности» достигается путем систематического преподавания научно-теоретических и профессионально-методологических основ данного предмета. Процесс научного познания напрямую связан с анализом явлений, событий, объектов окружающего мира и их отражением в сознании человека, а также закономерностей понимания ценностей и определения критериев их оценки.

Принцип непрерывности. Образование в области кибербезопасности направлено на совершенствование знаний студентов посредством непрерывного развития и обеспечения непрерывности потока информации. В условиях динамично меняющихся информационных угроз данная дисциплина должна постоянно совершенствоваться и обогащаться на основе новых моделей угроз и атак. Данный принцип обеспечивает системность построения процесса профессионального развития, формирования практических навыков в области информационной безопасности и применения знаний на практике в непрерывной среде обучения.

Принцип фундаментальности. Данный принцип направлен на углубленное изучение теоретических основ науки о фундаментальной кибербезопасности, в полной мере охватывающих ее правовые, технические и практические аспекты. При этом у студентов будет возможность самостоятельно обогащать свои

профессиональные знания и применять передовые технологии в области информационной безопасности в реальной практике в процессе обучения.

Принцип междисциплинарной связи. Область кибербезопасности не ограничивается компьютерными науками или техническими науками, а неразрывно связана с такими дисциплинами, как математика, физика, право и философия. Этот принцип включает: понимание правовых и этических критериев при изучении кибербезопасности; применение математических методов в криптографии, кодировании и защите информации; и интеграцию различных дисциплин при решении проблем, связанных с информационными технологиями.

Как показывает международный опыт, организация интерактивного общения обучающихся из разных географических регионов путем внедрения электронных и информационно-дидактических средств способствует повышению педагогической эффективности.

Принцип информационной безопасности. Данный принцип направлен на обеспечение информационной безопасности, защиту конфиденциальности данных посредством шифрования и кодирования. Данный принцип охватывает следующие основные аспекты: кодирование - предотвращение искажения информации путем преобразования ее в другой формат; криптография - разработка алгоритмов шифрования для защиты конфиденциальной информации; управление ключами - создание механизмов расшифровки и восстановления зашифрованных данных. Также преподаются технологии криптоанализа, что позволяет дополнительно усилить системы защиты зашифрованных данных.

Принцип ценностного подхода. Информационная безопасность требует не только технических знаний, но и формирования профессиональных и этических ценностей. Данный принцип включает в себя такие важные вопросы, как соблюдение информационной этики, использование информации на основе принципов прав человека и информационной безопасности.

Блок конфиденциальности и управления рисками является базовым блоком, который служит для объединения теоретических знаний с практическими навыками, направленными на защиту информации в преподавании дисциплины «Основы кибербезопасности», с помощью которого студенты будут глубоко осваивать технические, правовые и управленческие аспекты защиты информации. Конфиденциальность и управление рисками осуществляется в рамках 4 этапов.

Блок разработки методического обеспечения модели включает структуру, формы, методы, средства обучения, цели и задачи их реализации, а также функцию анализа концепций совершенствования программно-методического обеспечения обучения предмету «Основы кибербезопасности» в эпоху информационных атак. В блоке разработки методического обеспечения имеют большое значение следующие основные факторы: фундаментально развивать педагогическую и методическую подготовку будущих учителей по работе с информацией и ее хранению при преподавании дисциплины «Основы

кибербезопасности»; особое внимание уделяется углубленному преподаванию данного предмета и разработке системы получения информации, отвечающей мировым стандартам.

Базовый блок синтеза модели кибербезопасности включает определение текущего состояния информационно-контекстного обучения, понимание содержания информационного контекста, изучение блокирования информации и субъективных данных на компьютере, расширение знаний по работе с информацией о конституционных правах и свободах граждан, а также направление создания нового методического обеспечения в области кибербезопасности.

Роль мобильных приложений в анализе образовательного процесса на основе представленной модели совершенствования несопоставима. В настоящее время использование мобильных приложений в сфере образования имеет большое значение, многие созданные мобильные приложения используются студентами, но можно наблюдать, что большинство созданных мобильных приложений не содержат корректной и обоснованной информации. Можно сказать, что основной причиной такой ситуации является отсутствие национальных и современных мобильных приложений. Чтобы этого не произошло, мы осознали необходимость создания мобильных приложений, отражающих нашу национальность. Данное приложение предназначено для преподавания дисциплины «Основы кибербезопасности», в котором излагаются основные понятия науки основ кибербезопасности, теоретические основы защиты от кибератак.

В результате основное меню мобильного приложения включает в себя блок поиска информации и разделов, раздел с лекционными занятиями по предмету, раздел с практическими занятиями по предмету и блок тестов для оценки полученных знаний. Расположение, символы и выбранный дизайн каждого раздела были разработаны на основе критериев, предъявляемых к мобильным приложениям, служащим для обучения, и с учетом особенностей предмета.

Лекционно-практическая часть приложения охватывает «Основные понятия кибербезопасности», «Киберпреступность, киберзаконы и киберэтика», «Безопасность человеческой деятельности», «Архитектура, стратегия и политика кибербезопасности», «Основные понятия криптографии», «Симметричные криптографические алгоритмы», «Криптосистемы с открытым ключом», «Методы обеспечения целостности данных», «Шифрование дисков и файлов», «Методы безопасного удаления данных», «Средства организации процесса идентификации и аутентификации», «Логический контроль доступа к данным», «Многоуровневые модели безопасности», «Физическая защита данных», «Компьютерные сети и проблемы сетевой безопасности», «Средства сетевой безопасности», «Безопасность беспроводных сетей», «Управление рисками», «Концепция удобства использования: резервное копирование, восстановление данных и ведение журнала событий», «Проблемы безопасности в программном обеспечении», «Компьютерные вирусы и проблемы защиты от

вирусов», «Защита записей». Информация по темам «Защита от социальной инженерии» предоставляется в формате pdf и в виде видеоурока.

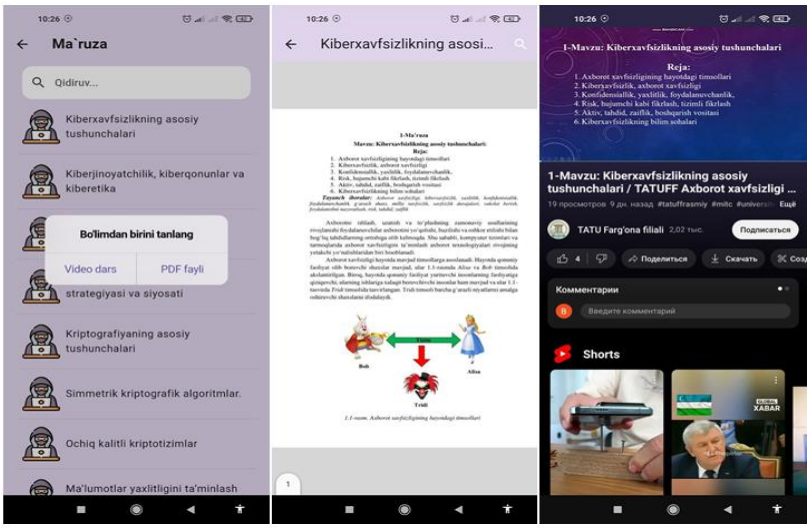


Рисунок 3. Мобильное приложение для обучения «Основам кибербезопасности»

Кроме того, в приложении предусмотрен раздел тестов, позволяющий студентам и пользователям контролировать и оценивать свои знания по данному предмету, где пользователь может выбрать количество тестов для выполнения (15, 30 и 50 тестов), а также срок выполнения заданий в течение определенного времени или без установки временного ограничения.

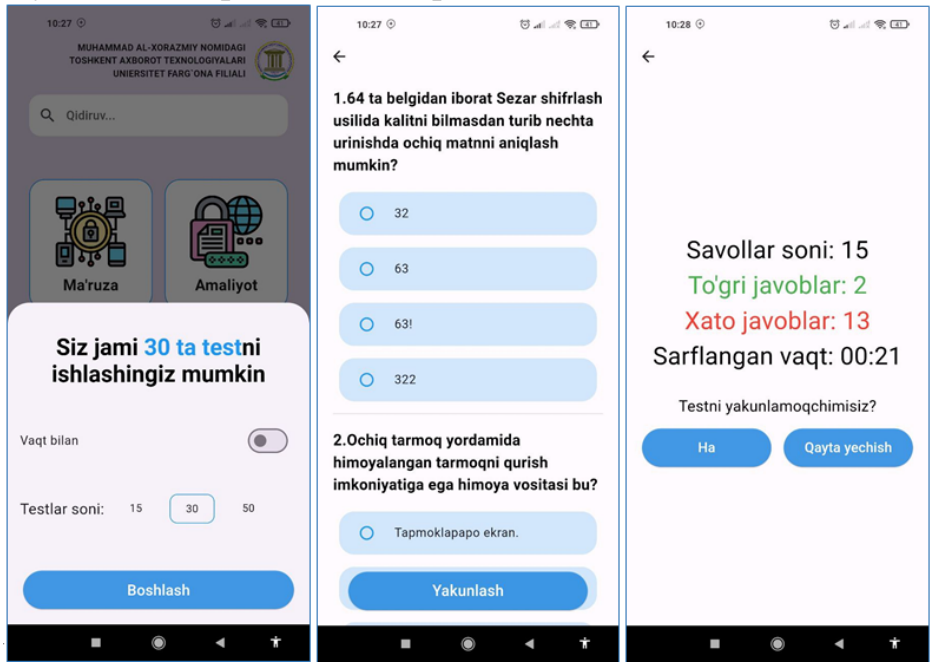


Рисунок 4. Тестовые задания для контроля и оценки знаний студентов

Система взаимодействия объекта и субъекта, воплощающая в себе комплекс возможностей сочетания педагогической деятельности и профессионального развития, обеспечивающая обратную связь, служит совершенствованию

технологий непрерывного профессионального развития, включающей разработку отдельных компонентов программно-методического творчества, расширение необходимых профессиональных знаний и совершенствование навыков, организацию педагогических и технологических условий, повышение уровня профессиональной компетентности и уровня достижения профессионального статуса, определение результата эффективности профессиональной деятельности, алгоритма применения технологий самостоятельного и непрерывного профессионального развития.

Технология «дифференциального обучения» (“Differential teaching” technology)

Цель: обучить студентов с учетом их индивидуальных особенностей - умениям работать с информационной безопасностью и повысить уровень их знаний в области кибербезопасности при защите различной информации, а также их возможностей.

Суть: данная технология направлена на совершенствование программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак, создание педагогических условий, учитывающих деятельность каждого обучающегося в соответствии с рамками интеллектуального развития и обеспечивающих дифференцированное обучение.

Механизм: в эпоху информационных атак совершенствование программного и методического обеспечения преподавания дисциплины «Основы кибербезопасности» на основе диагностики динамических характеристик личности и уровня освоения учебных навыков; отбор в зависимости от направлений получения знаний и интересов; организация по профильным вариантам обучения; активизация содержания знаний и стимулирование когнитивный деятельности студентов; добровольный выбор уровня освоения учебного материала, внедрение самостоятельной работы в электронном виде в компьютерной системе; организация учебного процесса в индивидуальной, групповой и коллективной формах; контроль освоения учебного материала; стремление к созданию современных методик преподавания преподаваемых дисциплин; предоставление рекомендаций по оперативному обучению и защите информации по индивидуальному учебному плану.

Третья глава диссертации под названием **«Результаты и эффективность опытно-экспериментальных работ по совершенствованию программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в период информационной атаки»** содержит описание критериев оценки организации педагогического опытно-промышленных работ, анализ и эффективность опытно-промышленных работ, полученные результаты.

Экспериментальная работа проводилась в Самаркандском, Каршинском и Ферганском филиалах Ташкентского университета информационных технологий. В экспериментальной работе приняли участие 497 студентов с первого по четвертый курсы. Из них 248 студентов участвовали в экспериментальных группах и 249 в контрольных группах.

Экспериментальные испытания, направленные на совершенствование программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности», проводились в три этапа (акцентный, разрабатывающий, заключительный).

В ходе реализации экспериментального исследования осуществлялся начальный, текущий и итоговый мониторинг. Применялись методы наблюдения, интервью, анкетирования, тестирования и педагогического эксперимента. В ходе экспериментального исследования ставилась цель совершенствования программно-методического обеспечения обучения студентов предмету «Основы кибербезопасности» в условиях информационной атаки, формирования профессиональных компетенций в области кибербезопасности, научного обоснования теоретических, педагогических и практических основ инновационных образовательных технологий в процессе обучения и внеучебной деятельности.

В ходе формирующего экспериментального этапа исследования с использованием инновационных методов обучения и современных технологий на основе учебной программы по совершенствованию программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в период информационных атак были разработаны следующие критерии кибербезопасности респондентов-студентов, работающих с информацией:

образовательно-когнитивные критерии: совершенствование программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак, формирование профессиональной компетентности будущих специалистов на основе интегративного подхода с опорой на учебный план, освоение студентами электронной информации и расширение их научно-теоретических знаний о ней, психолого-педагогических знаний о возрастных и индивидуальных, психофизиологических особенностях, формах, методах и средствах организации образовательного процесса, основных методах диагностики студентов, инновационных педагогических технологиях;

критерий коммуникативного мышления: совершенствование программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак, формирование коммуникативных знаний, умений и компетенций на основе учебной программы - развитие умения создавать методическое обеспечение со студентами в учебно-воспитательном процессе, совершенствование навыков мышления и коммуникативной компетентности;

интегративно-креативные критерии: формирование профессиональных компетенций в области информационной безопасности на основе интегративного подхода, интегрирующего различные дисциплины, на основе учебной программы совершенствовать программно-методическое обеспечение преподавания дисциплины «Основы кибербезопасности» в эпоху информационных атак, акцентировать внимание на ознакомлении с литературой,

способствующей повышению креативных качеств и потенциала, развитию мыслительных способностей.

В процессе проведения опытно-экспериментальной работы были определены уровни развития профессиональной компетентности будущего специалиста на основе интегративного подхода. В диссертации указаны критерии эффективности совершенствования программно-методического обеспечения обучения будущих специалистов предмету «Основы кибербезопасности» на основе интегративного подхода: «высокий», «средний», «низкий».

Таблица 1

Количество респондентов, участвовавших в экспериментальных и контрольных группах в экспериментальных испытательных работах во всех высших учебных заведениях

ВУЗ	Экспериментальные группы	Контрольные группы	Итого
Самаркандский филиал Ташкентского университета информационных технологий	83	82	165
Каршинский филиал Ташкентского университета информационных технологий	82	83	165
Ферганский филиал Ташкентского университета информационных технологий	83	84	167
Итого	**248**	**249**	**497**

Количество респондентов, принявших участие в экспериментальной и контрольной группах в экспериментальном тестировании, направленном на совершенствование программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности»

В ходе экспериментального исследования вопросы анкеты были направлены на определение современного состояния совершенствования программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» среди вышеуказанных студентов, проблемы обеспечения кибербезопасности и защиты информации в сети интернет, системы развития профессионально важных качеств студентов, формирования культуры работы с информацией в учебной и внеучебной деятельности с учетом темы курса.

Согласно гипотезе, выдвинутой относительно результатов эксперимента в конце анкеты, поскольку $\varphi_{emp} > \varphi_{krit}$, качество гипотезы H1 принимается. Это подтверждает, что разница в полученных результатах есть и что она эффективна.

По итогам эксперимента в экспериментальной и контрольной группах наблюдались различия по общему уровню знаний компонентов совершенствования программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» и развития профессиональных качеств: «Содержание работы с кибербезопасностью», «Показатель

сформированности компетентности в области кибербезопасности», «Формирование киберэтической культуры», а именно:

Таблица-2

Итоговые показатели общих результатов всех высших учебных заведений по экспериментальной работе

Критерии	Компоненты	Группы	Уровень рейтинга		
			высокий уровень	средний уровень	низкий уровень
учебно-когнитивный	Содержание работы с кибербезопасностью	ЭГ	38	177	33
		КГ	19	77	153
коммуникативное мышление		ЭГ	39	171	38
		КГ	19	75	155
интегративно-креативный		ЭГ	37	178	33
		КГ	19	78	152
учебно-когнитивный	Индикатор развития компетентности в области кибербезопасности	ЭГ	42	180	26
		КГ	21	74	154
коммуникативное мышление		ЭГ	45	167	36
		КГ	22	72	155
интегративно-креативный		ЭГ	43	174	31
		КГ	21	73	155
учебно-когнитивный	Развитие кибернетической культуры	ЭГ	51	182	15
		КГ	24	90	135
коммуникативное мышление		ЭГ	48	180	20
		КГ	24	89	136
интегративно-креативный		ЭГ	52	187	9
		КГ	27	88	134

В экспериментальной и контрольной группах проведен статистический анализ предварительных результатов по уровням знаний компонентов «Содержание работы с кибербезопасностью», «Показатель сформированности компетентности в области кибербезопасности», «Формирование культуры киберэтики» совершенствования программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» и формирования профессиональных качеств на основе критериев и статистики студентов вузов.

Из полученных результатов видно, что согласно заключению заключительного этапа в таблице тот факт, что показатели усвоения в экспериментальной и контрольной группах отличаются друг от друга, их эффективность больше единицы, эмпирическое значение статистики Стьюдента больше критического значения, доверительные интервалы не перекрываются (не пересекаются), критерий оценки эффективности экспериментальной и проверочной работы существенно больше единицы, а критерий оценки уровня знаний студентов существенно больше нуля, приводит к принятию гипотезы H1. Таким образом, статистический анализ подтвердил эффективность экспериментального исследования, направленного на развитие медиакомпетентности будущих учителей. Полученные средние показатели усвоения и результативности в исследовательской работе представлены на диаграммах ниже.

Таблица-3

Показатели статистического анализа для экспериментальных исследований всех высших учебных заведений

Критерии	Компоненты	Группы	Статистика студентов	Степени свободы статистики	Критическое значение	Сводка критериев	Отклонение доверия	Оценка качества обучения	оценка уровня знаний
учебно-когнитивный	Содержание работы с кибербезопасностью	ЭГ	10,62	482,07	1,96	H1	0,04	1,13	0,57
		КГ					0,05		
коммуникативное мышление		ЭГ	10,29	487,67	1,96	H1	0,04	1,13	0,56
		КГ					0,05		
интегративно-креативный		ЭГ	10,49	480,97	1,96	H1	0,04	1,13	0,57
		КГ					0,05		
учебно-когнитивный	Показатель развития компетентности в области кибербезопасности	ЭГ	11,38	473,99	1,96	H1	0,03	1,15	0,62
		КГ					0,05		
коммуникативное мышление		ЭГ	10,38	486,83	1,96	H1	0,04	1,14	0,58
		КГ					0,05		
интегративно-креативный		ЭГ	10,95	481,74	1,96	H1	0,04	1,14	0,6
		КГ					0,05		
учебно-когнитивный	Развитие кибернетической культуры	ЭГ	11,26	458,89	1,97	H1	0,03	1,14	0,62
		КГ					0,05		
коммуникативное мышление		ЭГ	10,59	465,68	1,97	H1	0,04	1,13	0,58
		КГ					0,05		
интегративно-креативный		ЭГ	11,55	438,43	1,97	H1	0,04	1,14	0,63
		КГ					0,05		

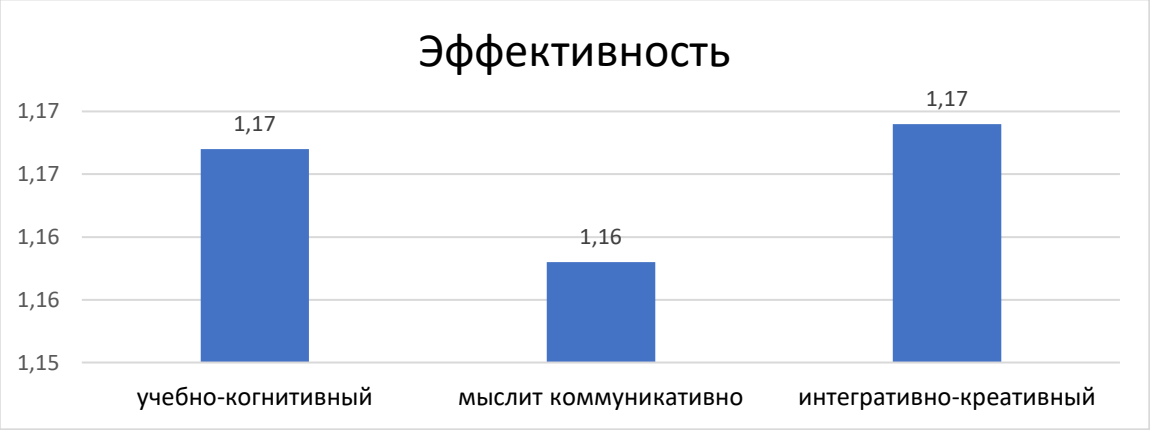


Рисунок 6. Показатели эффективности развития компонента киберэтической культуры

Результаты показали, что при всех условиях усвоение материала в экспериментальной группе было выше, чем в контрольной группе.

Таким образом, проблема обеспечения кибербезопасности и информационной безопасности студентов в условиях сети интернет и целенаправленного формирования культуры работы с информацией в учебной и внеучебной деятельности на основе темы курса, использования инновационных образовательных технологий, развития профессиональных качеств, эффективность содержательного компонента работы с кибербезопасностью по учебно-когнитивным, коммуникативным и интегративно-креативным критериям в среднем выше в 1,16 раза, эффективность компонента показателя развития компетентности в области кибербезопасности по учебно-когнитивным, коммуникативным и интегративно-креативным критериям в среднем выше в 1,17 раза, а эффективность компонента развития культуры киберэтики по учебно-когнитивным, коммуникативным и интегративно-креативным критериям в среднем выше в 1,17 раза.

ВЫВОДЫ

1. Определены педагогические возможности совершенствования преподавания дисциплины «Основы кибербезопасности» на основе единого подхода к регулированию сферы кибербезопасности и приоритетности участия отечественных производителей в создании системы кибербезопасности и повышения уровня знаний по кибербезопасности, киберпреступности, киберправу, киберугрозам, киберэтике, навыков студентов по соблюдению этики и культуры работы с сетью интернет и информацией в ней, а также основные принципы, влияющие на формирование киберэтической культуры студентов в условиях современных киберугроз, посредством правовых, организационных, экономических и технологических мер.

2. Рассмотрены аспекты преподавания дисциплины «Основы кибербезопасности» в формировании киберэтической культуры студентов в период информационной атаки. Исходя из предмета и цели кибербезопасности, был глубоко проанализирован широкий спектр процессов (конфиденциальность; целостность; идентификация; аутентификация; авторизация; контроль использования; понимание права собственности; заверение; подпись; неотказуемость; проставление даты; получение; отмена; анонимность), охватывающих основные задачи в преподавании дисциплины «Основы кибербезопасности».

3. Улучшения достигнуты на основе внедрения различных технологий, обеспечивающих выявление аспектов воздействия информационных атак на образовательный процесс и формирование у студентов устойчивых навыков противостояния киберугрозам, за счет уточнения задач обеспечения информационной безопасности, программных и технических средств обеспечения информационной безопасности, а также межсетевой классификации кибербезопасности: информационная безопасность, интернет-

безопасность, безопасность данных, безопасность различной информации, хранения и кодирования данных.

4. В ходе информационной атаки была усовершенствована модель преподавания дисциплины «Основы кибербезопасности» на основе 4 блоков: блок, ориентированный на криптографо-когнитивные аспекты, блок конфиденциальности, управления рисками, блок разработки методического обеспечения и блок критериев оценки. При совершенствовании программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» основной целью являлось обучение концептуальным основам терминов кибербезопасности и их практическому применению, а также навыкам личностно-профессионального, креативно-логического, индивидуально-профессионального развития и психологического роста в использовании компьютерной информации.

5. Принимая во внимание актуальные проблемы обеспечения информационной безопасности и формирования культуры киберэтики у студентов в эпоху кибератак, принимая во внимание специфические дифференциальные характеристики информационной безопасности и кибербезопасности, а также рассматривая термины «Кибербезопасность» и «Информационная безопасность» как совокупность взаимоисключающих процессов, киберугрозы рассматриваются как вполне глобальная проблема, на основе модели, разработанной на основе системно-структурного анализа и адаптации к деятельностным подходам, диагностики динамических характеристик личности и уровня усвоения учебных навыков, подбора обучения, усвоения знаний и интересов, организации по профильным вариантам обучения, активизации содержания знаний и стимулирования когнитивной деятельности студентов.

6. Программно-методическое обеспечение обогащения учебно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» создано как насыщенное современными технологиями и инновационными методами программно-методическое обеспечение преподавания дисциплины «Основы кибербезопасности» в период информационных атак, при этом особое внимание уделяется формированию компетенций, необходимых для защиты от информационных атак, на основе анализа содержания принципов преемственности, обоснованности, междисциплинарной релевантности, информационной защищенности, ценностного подхода, точности, принципа межличностных отношений, рефлексивности.

7. Усовершенствовано программно-методическое обеспечение преподавания дисциплины «Основы кибербезопасности» на основе дидактических принципов, направленных на приобщение студентов к высокоэффективной практике, нацеленной на позитивное использование информации и их самостоятельное и непрерывное профессиональное развитие в эпоху информационных атак;

8. Электронная платформа («https://edu-cyber.uz/»), направленная на повышение эффективности преподавания дисциплины «Основы кибербезопасности» в период информационных атак, дополнительно дополнена

мобильным приложением и методическими рекомендациями по преподаванию дисциплины «Основы кибербезопасности», обеспечивающими интерактивные методы обучения и возможность оперативного реагирования на информационные угрозы в виртуальной среде.

9. С использованием методов анализа и обобщения выделены и адаптированы к цифровым образовательным средствам вербальные, символические и изобразительные категории, а также производные, ассоциативные и фразеологические единицы, связанные с чтением, а также обозначены показатели сформированности компетентности в области кибербезопасности и компоненты, лежащие в основе формирования киберэтической культуры, как «высокий», «средний», «низкий» уровни на основе критериев учебно-когнитивного, коммуникативно-мыслительного и интегративно-креативного. В результате организован эффективный образовательный процесс, направленный на формирование у студентов глубоких знаний и практических навыков в области кибербезопасности.

РЕКОМЕНДАЦИИ

1. Необходима разработка адаптивных вариантов совершенствования программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» и освоения их практических и методических аспектов в эпоху информационных атак.

2. Необходимы исследования для обеспечения включения научных и практических подходов к проблемам кибербезопасности и ключевым решениям в подготовку соответствующих специалистов.

3. Необходимо издание учебно-методической литературы, в которой излагается суть различных взглядов и тенденций внедрения международных и современных подходов к совершенствованию программно-методического обеспечения преподавания дисциплины «Основы кибербезопасности» В эпоху информационных атак.

SCIENTIFIC COUNCIL OF DSc 03/30.01.2020.Ped.26.01 ON AWARDING ACADEMIC DEGREES AT THE NATIONAL PEDAGOGICAL UNIVERSITY OF UZBEKISTAN

THE NATIONAL PEDAGOGICAL UNIVERSITY OF UZBEKISTAN

MUKHTAROV FARRUKH MUKHAMMADOVICH

IMPROVING THE SOFTWARE AND METHODOLOGICAL SUPPORT FOR TEACHING THE DISCIPLINE "FUNDAMENTALS OF CYBERSECURITY" IN THE ERA OF INFORMATION ATTACKS

13.00.06 – Theory and methodology of digital education

ABSTRACT OF THE DOCTORAL THESIS (DSc) IN PEDAGOGICAL SCIENCES

Tashkent 2025

The dissertation topic of the Doctor of Science (DSc) is registered with the Higher Attestation Commission of the Republic of Uzbekistan under the number №B2024.3.DSc/Ped981.

The dissertation was completed at the National pedagogical university of Uzbekistan.

The abstract of the dissertation is available in three languages (Uzbek, Russian, English) on the website of the Scientific Council (www.tdpu.uz) and on the information and educational portal "Ziyonet" (www.ziyonet.uz).

Scientific supervisor:	**Abdullayeva Barno Sayfutdinovna** Doctor of Pedagogical Sciences, Professor
Official opponents:	**Kayumova Nasiba Ashurovna** Doctor of Pedagogical Sciences, Professor
	Sultanova Ugiloy Nabievna Doctor of Pedagogical Sciences, Professor
	Abdullayeva Ozoda Safibullayevna Doctor of Pedagogical Sciences, Professor
Leading organization:	**Gulistan State University**

The dissertation defense will take place "____" _____ 2025 year at ____ hours at the meeting of the Scientific Council 03/30.01.2020.Ped.26.01 at the Tashkent State Pedagogical University. (Address: 100185, Tashkent city, Chilanzar district, Bunyodkor street. House 27. Phone: (99871) 276-79-11; fax: (99871) 276-80-86; e-mail: tdpu_kengash@edu.uz).

The dissertation is available at the Information and Resource Center of Tashkent State Pedagogical University (registered under no. _____). (Address: 100185, Tashkent city, Chilanzar district, Bunyodkor street. House 27. Phone: (99871) 276-75-87; fax: (99871) 276-80-86.

The abstract of the dissertation was distributed on _____ day, "_____" 2025.
(Registered protocol number _____ from "_____" _____ 2025).

Z.N.Mamaradjabova
Chairman of the Scientific Council for Awarding Academic Degrees, DSc, Professor

R.G.Isyanov
Scientific Secretary of the Scientific Council for Awarding Academic Degrees, PhD, Associate Professor

M.E.Mamarajabov
Chairman of the Scientific Seminar at Scientific Council for Awarding Academic Degrees, DSc, Professor

INTRODUCTION (abstract of the doctoral thesis)

The purpose of the study is to develop practical recommendations for improving the software and methodological support for teaching the subject "Fundamentals of cybersecurity" during an information attack.

The object of the research is the process of improving the educational and methodological support for teaching the subject "Fundamentals of Cybersecurity" during an information attack. 497 students from grades 1-4 of the Samarkand, Karshi and Ferghana branches of the Tashkent University of Information Technologies participated in the pilot study.

The scientific novelty of the research is as follows**:**

the pedagogical possibilities of improving the teaching of the discipline "Fundamentals of Cybersecurity" during an information attack are identified based on the formation of a unified approach environment aimed at ensuring the priority of interests of the individual, society and the state in cyberspace in accordance with the legality of protection methods, and the classification of basic principles influencing the formation of cyberethical culture of students in the context of cyber threats;

the content of software and methodological support for teaching the discipline "Fundamentals of Cybersecurity" during an information attack has been improved based on determining the correspondence of the semantic structure of security terms to educational goals, introducing modern methods of protection encryption-coding, cryptographic algorithms, network security and data storage, ensuring proportional compatibility of the user interface with identification, authentication and confidentiality processes;

the model of formation of cyberethical culture of students in the process of teaching the discipline "Fundamentals of Cybersecurity" has been improved on the basis of leveling actual problems of ensuring information security, correlating specific differential features of information and cybersecurity with system-structural analysis and argumentation of solutions to global problems, a purposeful combination of principles of continuity, interdisciplinary relevance with cognitive, contextual, integrative and activity-based approaches;

the methodology of implementing software and methodological support for teaching the discipline "Fundamentals of Cybersecurity" in the era of information attacks based on interactive methods, effective use of the capabilities of audiovisual information, blockchain, cloud technologies, methods of control and self-control that allow for rapid response to information threats and cyberattack strategies in virtual space, adaptation of derivatives, associative learning units to digital educational systems has been improved. tools, hierarchical systematization of components, underlying the formation of cyberethic culture;

the effectiveness of the formation of students' cyberethical culture in the process of teaching the discipline "Fundamentals of Cybersecurity" has been improved on the basis of ensuring information security, targeted use of software and hardware, clarifying the classification of networks, studying the impact of information attacks on the educational process, dynamic priority levels of cognitive, communicative thinking,

sustainable development of integrative and creative skills to counter cyber threats to students.

Implementation of the research results. Based on the results of research on improving the methodology for the development of research competencies of students of the Master's degree in primary education:

a proposal to identify pedagogical opportunities for improving the teaching of the discipline "Fundamentals of Cybersecurity" during an information attack based on the formation of a unified approach environment aimed at ensuring the priority of interests of the individual, society and the state in cyberspace in accordance with the legality of protection methods, and the classification of basic principles, The content of the textbook "Fundamentals of Cybersecurity" (Permission for publication of Tashkent State Pedagogical University No. 11-05-7601/04 dated December 28, 2024) has been included in the content of the textbook "Fundamentals of Cybersecurity". As a result, the content of teaching the subject "Fundamentals of Cybersecurity" has been expanded;

a proposal to improve the content of software and methodological support for teaching the discipline "Fundamentals of Cybersecurity" during an information attack based on determining the correspondence of the semantic structure of security terms to educational goals, introducing modern methods of protection encryption-coding, cryptographic algorithms, network security and data storage, ensuring proportional compatibility of the user interface with identification processes, authentication and confidentiality are included in the content of the textbook "Fundamentals of Cybersecurity" (Permission for publication of Tashkent State Pedagogical University No. 11-05-7601/04 dated December 28, 2024). As a result, the content of educational and methodological support for teaching the discipline "Fundamentals of Cybersecurity" has been expanded;

a proposal to improve the model of formation of cyberethical culture of students in the process of teaching the discipline "Fundamentals of cybersecurity" based on leveling the current problems of ensuring information security, correlating specific differential features of information and cybersecurity with system-structural analysis and argumentation of solutions to global problems, a purposeful combination of principles of continuity, interdisciplinary relevance with cognitive, contextual, integrative and activity-based approaches are included in the content of the textbook "Fundamentals of Cybersecurity" (Permission for publication of Tashkent State Pedagogical University No. 11-05-7601/04 dated December 28, 2024). As a result, students were able to identify current problems of ensuring information security and developing their competencies;

a proposal to improve the methodology for implementing software and methodological support for teaching the discipline "Fundamentals of Cybersecurity" in the era of information attacks based on interactive methods, effective use of the capabilities of audiovisual information, blockchain, cloud technologies, control and self-monitoring methods that allow rapid response to information threats and cyberattack strategies in virtual space, adaptation of derivatives, associative learning units to digital educational tools, hierarchical systematization of components, The principles underlying the formation of cyberethic culture are included in the content of

the textbook "Fundamentals of Cybersecurity" (Permission for publication of Tashkent State Pedagogical University No. 11-05-7601/04 dated December 28, 2024). As a result, positive results were achieved in mastering the subject "Fundamentals of Cybersecurity";

a proposal to improve the effectiveness of the formation of cyberethical culture of students in the process of teaching the discipline "Fundamentals of cybersecurity" based on information security, the targeted use of software and hardware, clarifying the classification of networks, studying the impact of information attacks on the educational process, the dynamic priority of levels of cognitive, communicative thinking, The sustainable development of integrative and creative skills in countering cyber threats to students is included in the content of the textbook "Fundamentals of Cybersecurity" (Permission for publication of Tashkent State Pedagogical University No. 11-05-7601/04 dated December 28, 2024). As a result, aspects of the formation of cyberethic culture among students during the information attack are clarified.

The structure and scope of the dissertation. The dissertation consists of an introduction, 3 chapters, a conclusion, a list of references and appendices, the main volume of the dissertation is 240 pages.

E’LON QILINGAN ISHLARI RO‘YXATI
СПИСОК ОПУБЛИКОВАННЫХ РАБОТ
LIST OF PUBLISHED WORKS

I bo‘lim (I chast, part I)

1. Muxtarov F.M. Internet kontentlaridan xavfsiz foydalanish mexanizmini takomillashtirish // Monografiya – Farg‘ona: ISBN:978-9943-9720-3-2, Classik nashryoti, 2023-yil.
2. Muxtarov F.M. Axborotlar xuruji davrida “Kiberxavfsizlik” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishning nazariy asoslari // “Pedagogika” ilmiy-nazariy va metodik jurnal. Toshkent 2024. №1. (13.00.00 № 6)
3. Muxtarov F.M. Axborotlar xuruji davrida “Kiberxavfsizlik” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish mazmuni // “Pedagogika” ilmiy-nazariy va metodik jurnal. Toshkent 2024. №2. (13.00.00 № 6)
4. Muxtarov F.M. Axborotlar xuruji davrida “Kiberxavfsizlik” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishda tushunchalar semantikasi // “Pedagogika” ilmiy-nazariy va metodik jurnal. Toshkent 2024. №3. 271-274 b. (13.00.00 № 6)
5. Muxtarov F.M. Axborotlar xuruji davrida “Kiberxavfsizlik” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishda axborot xavfsizligining ahamiyati // “Pedagogika” ilmiy-nazariy va metodik jurnal. Toshkent 2024. №5. 144-146 b. (13.00.00 № 6)
6. Muxtarov F.M. Axborotlar xuruji davrida “Kiberxavfsizlik” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishda kompyuter tizimining axborotlashuv asosi // TDPU ilmiy axborotlari ilmiy-nazariy jurnali. Toshkent-2024. №5. 23-30b. (13.00.00 №32)
7. Muxtarov F.M. Axborotlar xuruji davrida “Kiberxavfsizlik” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirishning soha funksiyalari // TDPU ilmiy axborotlari ilmiy-nazariy jurnali. Toshkent-2024. №6. 57-64b. (13.00.00 №32)
8. Muxtarov F.M. Axborotlar xuruji davrida “Kiberxavfsizlik” fanini o‘qitishning dasturiy-metodik ta’minotini takomillashtirish kasbiy faoliyat sifatida // TDPU ilmiy axborotlari ilmiy-nazariy jurnali. Toshkent-2024. №7. 145-153b. (13.00.00 №32)
9. Muxtarov F.M. Axborot xavfsizligi va kiberxavfsizlikning o‘ziga xos differensial xususiyatlari mohiyat // TDPU ilmiy axborotlari ilmiy-nazariy jurnali. Toshkent-2024. №4. 494-503b. (13.00.00 №32)
10. Muxtarov F.M. Axborotlar xuruji davrida “Kiberxavfsizlik” fanini o‘qitishda tushunchalar tahlilining semantikasi // TDPU ilmiy axborotlari ilmiy-nazariy jurnali. Toshkent-2024. №5. 641-648b. (13.00.00 №32)
11. Muxtarov F.M. Axborotlar xuruji davrida “Kiberxavfsizlik” fanini o‘qitishning zamonaviy metodlari // TDPU ilmiy axborotlari ilmiy-nazariy jurnali. Toshkent-2024. №8. 641-648b. (13.00.00 №32)

12. Muxtarov F. Integrating artificial intelligence in IT curricula, preparing students for the future of technology. International Bulletin of Engineering and Technology, 3(11), USA 2023-yil, 111-113b. ReserarchBid IF 9.1
URL: https://internationalbulletins.com/intjour/index.php/ibet/article/view/1212
13. Muxtarov F. The role of gamification in it pedagogy, engaging students and promoting active learning. Theoretical aspectsin the formation of pedagogical sciences. International scientific-online conference Great Britain 2023. 14-16pp.
14. Мухтаров Ф. М. Прогрессвные подходы к обучению студентов в области кибербезопасности через факультативные занятия. Science and innovation in the education system. International scientific-online conference. Italy 2023 –P 87-91.
15. Muxtarov F.M. Axborot xavfsizligining muhimligi va uning pasayishlariga qarshi choralar // “Texnika va raqamli texnologiyalarni amaliyotda qo’llanilishi va ularning innovatsion yechimlari” Respublika ilmiy-texnik konferensiya materiallari. 2-kitob. 4-5 may, 2023 yil. Farg‘ona. 633-637 b.
16. Muxtarov F. Ensuring a safer digital future, the importance of cybersecurity education. “Kompyuter ilmlari va muhandislik Texnologiyalari” mavzusidagi Respublika ilmiy-texnik anjumani 2023. 13-Oktabr, O‘zMUJF Jizzax. 46-49b.
https://api.scienceweb.uz/storage/publication_files/7299/19869/65bc76b6ccf61__O'zMU%20JF_to'plam_1-qism_2023_xalqaro.pdf

II bo‘lim (II chast, part II)

17. Muxtarov F. M. Xavf-xatarlarni keltirib chiqaruvchi omillar, xavf-xatarlarni aniqlash usullari, muammo va yechim // Muhammad al-Xorazmiy nomidagi TATU Farg‘ona filiali “Al-Farg‘oniy avlodlari” elektron ilmiy jurnali. — Farg‘ona, 2023. — Tom 1, №3. — B. 5-9. — ISSN 2181-4252.
https://journals.indexcopernicus.com/api/file/viewByFileId/1827524
18. Muxtarov F. The complex of factors in improving the software and methodological provision of “Cyber security” science teaching in the period of information attacks // Science and innovation international scientific journal. — Volume 3, Issue 5, May 2024. — Pp. 205-207. — ISSN: 2181-3337. (13.00.00., (12) Index Copernicus). — URL: https://scientists.uz/view?id=7308
19. Muxtarov F. Applying the science of cyber security to the educational process of higher education // Eurasian Journal of Technology and Innovation. – 2023. – Vol. 1, № 9. – P. 72–78.
URL: https://in-academy.uz/index.php/ejti/article/view/20805
20. Muxtarov F. Ensuring information security in educational institutions: best practices and strategies // International Bulletin of Engineering and Technology. – 2023. – Vol. 3, № 10. – P. 42–44.
URL: https://www.internationalbulletins.com/intjour/index.php/ibet/article/view/1089
21. Muxtarov F. Improving the methodology of teaching the Science of "cybersecurity fundamentals" in the Conditions of ideological threats // International Bulletin of Engineering and Technology. – 2023. – Vol. 3, № 9. – P. 38–44.

URL: https://internationalbulletins.com/intjour/index.php/ibet/article/view/1030
22. Muxtarov F. Cybersecurity awareness training, empowering users to defend against social engineering attacks // International Bulletin of Engineering and Technology. – 2023. – Vol. 3, № 11. – P. 108–110.
URL: https://internationalbulletins.com/intjour/index.php/ibet/article/view/1211
23. Muxtarov F. Incorporating project-based learning in IT education, enhancing practical skills and problem-solving abilities // International Bulletin of Applied Science and Technology. – 2023. – Vol. 3, № 11. – P. 669–671.
24. Muxtarov F. M. Axborot tizimlarida xavfsizlik tahdidlarining tasnifi. “Yosh olimlar, doktorantlar va tadqiqotchilarning onlayn ilmiy forumi” ma’ruzalar to‘plami. 3-sho‘ba. 25-fevral 2023 yil. –B. 51-52
25. Мухтаров Ф. М. Цифровизация и цифровые технологии в образовании // Development of pedagogical thechnologies in modern sciences. International scientific-online conference Turkiye 2023 –P 32-39.
26. Muxtarov F. The power of cybersecurity education: defending against digital threats // Golden brain. – 2023. – Vol. 1, № 26. – P. 63-66. – URL: https://researchedu.org/index.php/goldenbrain/article/view/4816

Avtoreferat O‘ZMPU “Ilmiy axborotlari” jurnali tahririyati
tomonidan 2025-yil 23 iyunda tahrirdan o‘tkazildi.

Bosishga ruxsat etildi: 23.06.2025-yil
Bichimi 60x84 1/16, “Times New Roman”
garniturada raqamli bosma usulida bosildi.
Nashriyot bosma tabog‘i 5.0. Adadi: 100. Buyurtma: № 67
Bahosi kelishuv asosida

Nizomiy nomidagi O‘zbekiston milliy pedagogika
universiteti bosmaxonasida chop etildi.
Manzil: Toshkent shahar, Chilonzor tumani,
Bunyodkor ko‘chasi, 27-uy.