ISNN 3030-3907

2026/2
VOLUME 5

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/2 VOLUME 5

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Асадова Раъно Дилмуратовна
Тошкент Давлат техника университети доценти

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

AXBOROT XAVFSIZLIGINI TA’MINLASHDA DASTURIY TA’LIM VOSITALARIDAN FOYDALANISHNING PEDAGOGIK ASOSLARI

Bobobekov Shokir Ravshanovich
Jizzax Sambhram universiteti katta o‘qituvchisi
E-mail: sh.r.bobobekov16@gmail.com
Sindorqul Ibragimovich Qulmamatov
Guliston davlat pedagogika instituti pedagogika fanlari nomzodi, dotsent

Annotatsiya. Maqolada raqamli jamiyat sharoitida oliy ta’lim muassasalari talabalarining axborot xavfsizligi bo‘yicha kompetentligini shakllantirishning pedagogik asoslari tadqiq etilgan. O‘qitishda real kiberxavf jarayonlarini modellashtirishga asoslangan amaliy yondashuvning zarurati ilmiy asoslangan. Tadqiqot obyekti sifatida ishlab chiqilgan 14 ta funksional modulni o‘z ichiga olgan "CyberEdu" dasturiy vositalar kompleksi tahlil qilingan. Dasturning har bir moduli pedagogik, didaktik va psixologik yondashuvlar integratsiyasi nuqtai nazaridan yoritilgan. Natijalar shuni ko‘rsatadiki, amaliy va simulyatsion dasturiy muhit talabalarda mustaqil qaror qabul qilish va kiberhujumlarni bartaraf etish malakasini sezilarli darajada oshirdi.

Kalit so‘zlar: Raqamli ta’lim, axborot xavfsizligi, dasturiy ta’lim vositasi, pedagogik modellashtirish, kiberxavfsizlik kompetentligi, simulyatsion ta’lim, kriptografiya, ijtimoiy muhandislik, Virtual laboratoriya, Kiber poligon.

Аннотация. В статье исследуются педагогические основы формирования компетенций в области информационной безопасности у студентов высших учебных заведений в условиях цифрового общества. Научно обоснована необходимость практического подхода к обучению, основанного на моделировании реальных процессов киберугроз. В качестве объекта исследования проанализирован разработанный программный комплекс «CyberEdu», включающий 14 функциональных модулей. Каждый модуль программы освещен с точки зрения интеграции педагогических, дидактических и психологических подходов. Результаты показывают, что практическая и симуляционная программная среда значительно повысила навыки студентов по самостоятельному принятию решений и отражению кибератак.

Ключевые слова: Цифровое образование, информационная безопасность, программное средство обучения, педагогическое моделирование, компетенции в области кибербезопасности, симуляционное обучение, криптография, социальная инженерия, виртуальная лаборатория, киберполигон.

ISSN 3030-3907

Abstract: The article explores the pedagogical foundations for developing information security competence among higher education students within the context of a digital society. The necessity of a practical approach to teaching based on the modeling of real-world cyber threat processes is scientifically substantiated. The "CyberEdu" software suite, comprising 14 functional modules developed as the object of research, is analyzed. Each module of the program is discussed through the lens of integrating pedagogical, didactic, and psychological approaches. The results indicate that the practical and simulated software environment significantly enhanced students' skills in independent decision-making and cyberattack mitigation.

Keywords: Digital education, information security, educational software tool, pedagogical modeling, cybersecurity competence, simulated learning, cryptography, social engineering, virtual laboratory, cyber range.

KIRISH

Zamonaviy raqamli jamiyat sharoitida axborot xavfsizligi sohasi o‘zining o‘ta murakkabligi, doimiy yangilanib boruvchi tahdidlar tizimi hamda turli fan sohalarining o‘zaro integratsiyalashuvi bilan tavsiflanadi. O‘zbekiston Respublikasining raqamli transformatsiya yo‘lidagi strategik maqsadlari bevosita ushbu sohada yetuk kadrlar tayyorlash bilan bog‘liqdir. Xususan, O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida"gi PF-6079-son Farmoni mamlakatimizda raqamli iqtisodiyot va elektron hukumatni rivojlantirish bilan bir qatorda, kiberxavfsizlikni ta’minlash hamda aholining raqamli ko‘nikmalarini shakllantirish bo‘yicha ustuvor vazifalarni belgilab berdi[1].

Ushbu vazifalar doirasida oliy ta’lim muassasalari oldida nafaqat nazariy bilimga ega, balki raqamli muhitda ongli, mas’uliyatli va kiberhujumlarga qarshi amaliy immunitetga ega bo‘lgan mutaxassislarni tayyorlash muhim vazifa sifatida qo‘yilgan. Bugungi kunda axborot xavfsizligiga tahdidlar faqatgina texnik xarakter bilan chegaralanib qolmay, balki ijtimoiy-psixologik, iqtisodiy va huquqiy omillar bilan ham uzviy bog‘liq holda namoyon bo‘lmoqda.

Axborot xavfsizligi sohasida kadrlar tayyorlash jarayonida faqatgina quruq nazariy bilimlarni berish hozirgi zamon talablariga, xususan, “Raqamli O‘zbekiston - 2030" strategiyasida ko‘zda tutilgan amaliy natijadorlik tamoyillariga muvofiq kelmaydi. Real kiberxavf jarayonlarini modellashtirish, tahdidlarni erta aniqlash va ularni bartaraf etish bo‘yicha mustahkam ko‘nikmalarni shakllantirish zamonaviy dasturiy vositalar va simulyatsion platformalarni ta’lim jarayoniga tizimli tatbiq etishni taqozo etadi. Zero, talaba real axborot muhitidagi

ISSN 3030-3907

xavflarni dasturiy vositalar orqali bevosita tahlil qilib ko‘rgandagina, unda to‘laqonli kasbiy kompetentlik shakllanadi.

ADABIYOTLAR TAHLILI

Ta’lim jarayonini raqamlashtirish va maxsus dasturiy ta’minotlardan o‘quv vositasi sifatida foydalanish ko‘plab olimlar tomonidan tadqiq etilgan. Bugungi kunda kiber xavf-xatarlar o‘zining dinamik xarakteri bilan ajralib turadi, masalan zararli dasturlar, zaifliklardan foydalanishga asoslangan hujumlar, fishing va tarmoq hujumlari doimiy ravishda o‘zgarib boradi. Yurtimiz olimlaridan A. A. Ganiyev va I.R. Bekmuratovlar kiberxavfsizlik sohasida mutaxassislar tayyorlashda amaliy laboratoriya ishlarining ahamiyatini asoslab, virtualizatsiya texnologiyalari asosida o‘quv jarayonini tashkil etish bo‘yicha metodik tavsiyalar berganlar. Shuningdek, T.S. Qilichev virtual laboratoriyalarning zamonaviy ta’lim tizimidagi o‘rni va ahamiyatini tadqiq etar ekan, ularning talabalarda amaliy ko‘nikmalarni shakllantirishdagi didaktik imkoniyatlarini yuqori baholagan [6].

Xorijiy tajribada esa, R.R. Panakka tomonidan o'tkazilgan tahlillarga ko'ra, avtomatlashtirilgan vositalar va real vaziyatga asoslangan simulyatsiyalar yordamida bilim olgan talabalarning o'zlashtirish ko‘rsatkichi 90% ga yaxshilangan. Shu bilan birga, bunday interaktiv muhit talabalarda murakkab texnik vazifalarni bajarishdagi xavotir va qo‘rquvni sezilarli darajada kamayishi ta’kidlagan [2]. Yildirim va Alilar virtual laboratoriyalarning pedagogik rolini tahlil qilib, kiberxavfsizlikni o‘qitishda "bajarish orqali o‘rganish" (learning by doing) tamoyili eng yuqori natija berishini asoslab bergan [5].

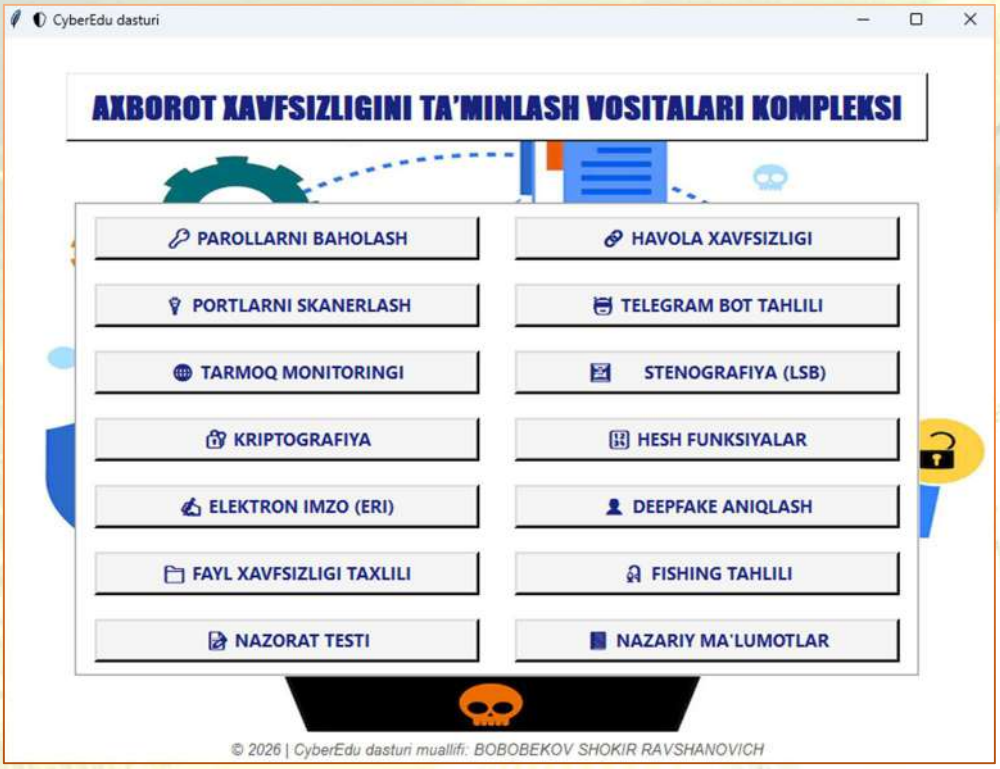
Avtomatlashtirilgan tahdidlar – zararli botnetlar, skriptlar va sun’iy intellekt vositalari yordamida avtomatik tarzda amalga oshirilayotgan hujumlar shuni ko‘rsatadiki, talabalarda axborot xavfsizligi kompetentligini shakllantirishda faqatgina ma’ruza bilan chegaralanib qolish umuman samarasizdir [7]. Shu sababli, ilmiy adabiyotlarda o‘quv muhitida virtual poligonlar, kiber-arenalar va simulyatorlardan foydalanish bo‘yicha qator tavsiyalar ilgari surilgan. Aynan shunday sharoitda talabalarda kognitiv faollik, amaliy tafakkur, refleksiv tahlil qilish va muammoli vaziyatlarda mustaqil qaror qabul qilish kompetensiyalari yuzaga keladi.

TADQIQOT METODOLOGIYASI

Ushbu tadqiqotda shaxsga yo‘naltirilgan, faoliyatga asoslangan va integrativ yondashuvlar ustuvor metodologiya sifatida qabul qilindi. Bu yondashuvlar pedagogik ehtiyoj sifatida axborot xavfsizligi bo‘yicha kompetentlikni shakllantirishning ilmiy-metodologik asosini belgilaydi.

Tadqiqot doirasida muallif tomonidan mahsus "CyberEdu" dasturiy vositalar kompleksi ishlab chiqildi va ta’lim jarayoniga tatbiq etildi.

ISSN 3030-3907



1 - rasm. Axborot xavfsizligini ta'minlashning dasturiy vositalari kompleksi

Mazkur kompleks 14 ta mustaqil, ammo mantiqan bir-biri bilan bog‘langan funksional modullarni o‘z ichiga oladi. Ta'lim jarayonini loyihalashda muammoli ta'lim va konstruktiv tamoyillaridan foydalanildi. Dasturiy ta'minot yordamida talabalarga nazariyotchi emas, balki real muammolarni hal qiluvchi amaliyotchi mutaxassis roliga kirishish imkoniyati yaratildi. Baholash metodologiyasi sifatida avtomatlashtirilgan test va diagnostika vositalari qo‘llanildi.

MUHOKAMA VA NATIJALAR

Ishlab chiqilgan “CyberEdu” dasturiy vositalar kompleksi talabalarda axborot xavfsizligini ta'minlash kompetentligini rivojlantirishning asosiy pedagogik vositasi sifatida sinovdan o‘tkazildi. Ushbu dasturiy mahsulot talabaning nazariy bilimlarini amaliy faoliyat bilan uzviy bog‘lashga, axborot xavfsizligi jarayonlarini real muhitga eng yaqin sharoitda amalga oshirishga xizmat qiladi.

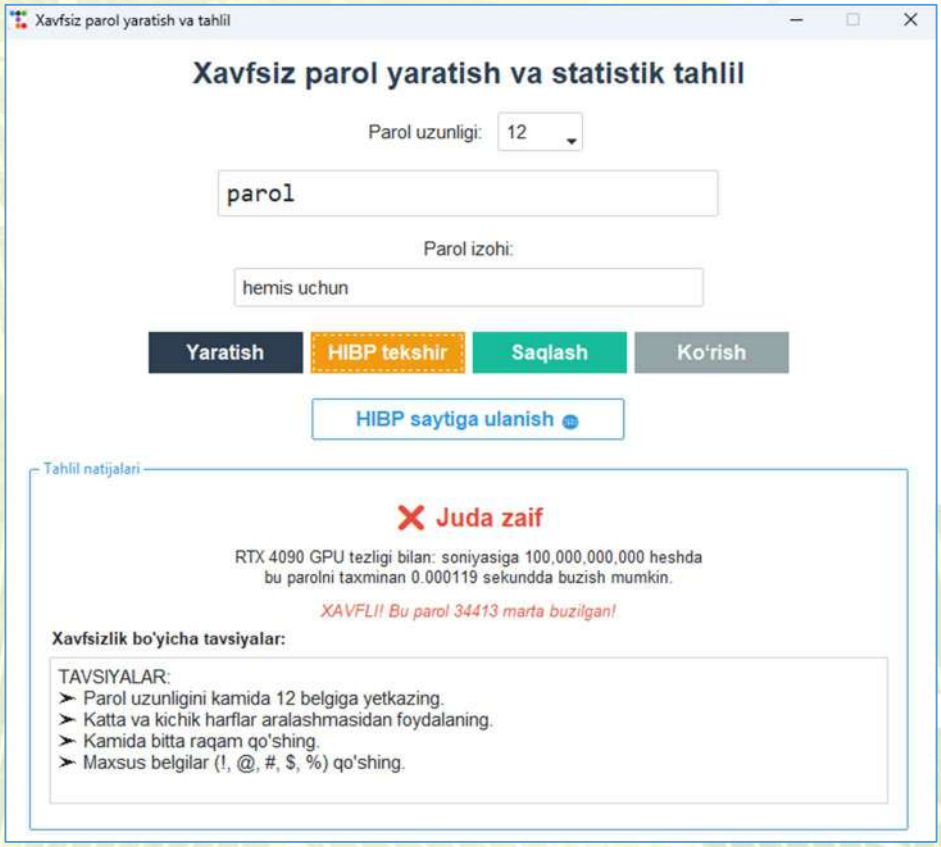
Barcha modullar axborot xavfsizligining asosiy yo‘nalishlarini to‘liq qamrab olgan holda mantiqiy guruhlarga ajratildi: texnik xavfsizlik (parollarni baholash, portlarni skanerlash, tarmoq monitoringi, fayllar tahlili); kriptografik yo‘nalish (kriptografik algoritmlar, elektron raqamli imzo, hesh funksiyalar); axborot tahdidlari va ijtimoiy muhandislik (fishing hujumlarini modellashtirish va tahlil, havola xavfsizligi, telegram bot xavfsizligi); zamonaviy tahdidlar va deepfake (soxta) media, steganografiya; ta'limiy-nazorat komponentlari (nazorat testi, nazariy ma'lumotlar)

ISSN 3030-3907

Quyida har bir modulning pedagogik va didaktik mohiyati hamda kutilgan o‘quv natijalari keng qamrovli tahlil etiladi.

Parollarni baholash moduli va uning pedagogik asoslari

Modulning funksional vazifasi foydalanuvchilarga kuchli va kriptobardoshli har bir tizim uchun alohida parollarni yaratishni amalda o‘rgatish, mavjud parollarning xavfsizlik darajasini avtomatik baholash, shuningdek xavfsiz saqlash imkonini berishdir. Pedagogik nuqtai nazardan bu amaliylik tamoyiliga asoslanadi. Talabalar o‘zlarining kundalik parollarini tekshirib ko‘rib, hayotiylik tamoyili asosida mas’uliyatni his qiladilar. Didaktik ahamiyati shundaki, talabalarda shaxsiy axborot resurslarini himoya qilish kibermadaniyati hosil qilinadi (2-rasm).



2 – rasm. Xavfsiz parol yaratish va tahlil modul oynasi

Havola xavfsizligi moduli

Modul URL manzillarning ishonchliligini baholash va zararli havolalarni aniqlashga yo‘naltirilgan. Ilmiylik tamoyiliga tayangan holda, jarayon zamonaviy URL tahlil algoritmlari (qora ro‘yxatlar, SSL sertifikat tekshiruvi) yordamida bajariladi. Faoliyatga asoslangan yondashuv talabani faqat kuzatuvchi emas, balki kiber hujumlarni aniqlovchiga aylantiradi.

Portlarni skanerlash moduli

Ushbu modul kompyuter tarmoqlaridagi zaif nuqtalarni (ochiq portlarni) izlab topishga qaratilgan. Tizimlilik tamoyili qo‘llanilib, himoya yaxlit bir zanjir

ISSN 3030-3907

sifatida tushuntiriladi. Talaba tarmoqni mustaqil skanerlash orqali amaliy xavfsizlik choralarini loyihalashtirish qobiliyatini rivojlantiradi.

Steganografiya (LSB) moduli

Ma’lumotlarni rasm fayllar ichiga yashirin tarzda joylashtirish usullarini o‘rgatadi. Pedagogik jihatdan bu qismda ijodkorlik tamoyili ustuvor bo‘lib, talabalarni standart shifrlashdan tashqari nostandart yechimlar izlashga undaydi.

Tarmoq monitoringi moduli

Tarmoqdagi harakatlarni real vaqt rejimida kuzatish va xavfli paketlarni aniqlash qobiliyatini shakllantiradi. Talabalarga xavfsizlik jarayoni to‘xtovsiz davom etadigan monitoring ekanligi uqtiriladi. Muammoli ta’lim yondashuvi ularni kutilmagan kiberhujumlar (masalan, DoS hujumlar) sodir bo‘lganda tezkor qaror qabul qilishga o‘rgatadi.

Telegram bot tahlili moduli

Bugungi kunda ommabop bo‘lgan Telegram messenjerida botlar orqali tarqaladigan zararli kontentlarni aniqlashni o‘rgatadi. Simulyatsiya yondashuvi yordamida talabalar xavfsiz sun’iy muhitda bot hujumlarini tahlil qiladilar. Bu hayotiylik tamoyilining yorqin ko‘rinishidir.

Kriptografiya moduli

Ma’lumotlarni simmetrik va asimmetrik usullarda shifrlash va deshifrlash mexanizmlarini ko‘rsatib beradi. Nazariya va amaliyot birligi tamoyili doirasida oson va qiyin matematik algoritmlar (RSA) vizual va amaliy dasturiy interfeys orqali oson tushuntiriladi.

Hesh funksiyalar moduli

Ma’lumotlarning yaxlitligini ta’minlash, fayllar o‘zgartirilmaganini tekshirish uchun MD5, SHA-256 kabi algoritmlardan foydalanishni o‘z ichiga oladi. Talabalar ma’lumotning kichik bir o‘zgarishi ham heshni butunlay o‘zgartirib yuborishini amalda ko‘rib, axborot butunligi konsepsiyasini anglaydi.

Deepfakelarni aniqlash moduli

Sun’iy intellekt orqali yaratilgan soxta kontentlarni aniqlash. Tanqidiy tafakkur tamoyili asosida talabalar piksel anomaliyalari va tovushdagi sun’iylikni ajratishni o‘rganadilar. Bu ularni zamonaviy axborot-psixologik manipulyatsiyalarga qarshi immunitetini oshiradi.

Fayl xavfsizligi tahlili moduli

Ushbu modul fayllarning tarkibiy tuzilmasini tekshirish, ya’ni zararli kod yoki havolalarning bor yoki yo‘qligini tekshirishni taqdim etadi. Kasbiy yo‘naltirilganlik tamoyili ularni kelajakdagi haqiqiy axborot xavfsizligi mutaxassisi bo‘lishiga tayyorlaydi.

Elektron imzo moduli

ISSN 3030-3907

Elektron hujjatlarning huquqiy ishonchliligini ta’minlash mexanizmlari. Huquqiylik va ilmiylik tamoyillari asosida talaba raqamli kalitlarni generatsiya qilish va hujjatlarni tasdiqlashni o‘rganadi.

Fishing tahlili moduli

Foydalanuvchilarni aldashga qaratilgan soxta tizimlarni yaratish va ularning qurboniga aylanmaslikni o‘rgatuvchi modul. Kiberhujumchining psixologiyasini tushunish orqali eng ishonchli himoya strategiyasi ishlab chiqiladi.

Nazorat testi moduli

Avtomatlashtirilgan baholash tizimi. Obyektivlik tamoyili asosida inson omilisiz talabaning kuchli va zaif tomonlari diagnostika qilinadi. Bu pedagogik monitoring uchun asosiy vositadir.

Nazariy ma’lumotlar moduli

Kiberxavfsizlikning barcha yo‘nalishlari o‘rtasidagi mantiqiy bog‘liqlikni tizimli ravishda tushuntiruvchi ma’lumotnomalar bazasi.

1-jadval.

“CyberEdu” dasturiy kompleksining pedagogik yondashuvlar matritsasi

№	Dastur moduli	Shakllanadigan kompetensiya	O‘quv faoliyati turi
1	Parollar tahlili	Kibermadaniyat, shaxsiy ma’lumotlarni himoyalash	Analitik tekshiruv
2	Kriptografiya va Raqamli imzo	Algoritmik fikrlash, huquqiy savodxonlik	Konstruktiv yaratuvchanlik
3	Fishing va Deepfake	Manipulyatsiyalarni va ijtimoiy muhandislikni farqlash	Simulyatsion muammo yechish
4	Tarmoq va Port skaner	Tarmoq zaifliklarini izlash va bartaraf etish	Amaliy diagnostika

XULOSA VA TAKLIFLAR

O‘tkazilgan tahlillar va tatbiq etish natijalari shuni ko‘rsatadiki, “CyberEdu” dasturining yuqorida bayon etilgan modullari talabalarda axborot xavfsizligini ta’minlash kompetentligini kompleks, tizimli va uzluksiz shakllantirishga bevosita xizmat qiladi. Har bir modul o‘zining alohida pedagogik vazifasini bajarish bilan bir qatorda, ularning o‘zaro integratsiyalashuvi talabalarda nazariy bilimlarni real amaliy faoliyat bilan uyg‘unlashtirish ko‘nikmalarini yuqori darajada rivojlantiradi.

Mazkur dasturiy muhit raqamli pedagogika tamoyillariga asoslangan bo‘lib, o‘quvchini axborotni shunchaki passiv qabul qiluvchi obyekt darajasidan, faol ishtirokchi va muammoli vaziyatlarda muammoni yechuvchi subyekt darajasiga olib chiqadi. Talabalar kiberxavfsizlikning texnik, tashkiliy, huquqiy va psixologik jihatlarini o‘zaro uzviy bog‘liq holda o‘zlashtiradilar.

ISSN 3030-3907

Tadqiqot natijalaridan kelib chiqib, oliy ta’lim tizimida axborot xavfsizligi bo‘yicha mutaxassislar tayyorlash sifatini oshirish maqsadida quyidagi takliflar ilgari suriladi:

1. O‘quv jarayoniga simulyatsion va himoyalangan poligonli yondashuvni tatbiq etish.

Oliy ta’lim muassasalarida “Axborot xavfsizligi” va unga turdosh fanlarni o‘qitishda amaliy mashg‘ulotlar ulushini oshirish. Bunda “CyberEdu” kabi ko‘p modulli simulyatsion dasturiy vositalar kompleksidan foydalanish. Bu talabalarga real kibertahdidlarni xavfsiz boshqarish imkonini beradi.

2. Baholash tizimini kompetensiyaga asoslangan modelga o‘tkazish.

Talabalarning bilimlarini baholash mezonlarini quruq nazariy ma’lumotlarni yodlashga emas, balki kiberhujum vaqtida dasturiy modullarda ko‘rsatgan amaliy reaksiyasi, tahdidni tahlil qilish va tanlagan himoya strategiyasining samaradorligiga qarab belgilash tizimini ishlab chiqish.

3. Virtual laboratoriyalar va masofaviy kiber poligonlar tarmog‘ini yaratish. Dasturiy majmuaning ta’lim platformasini yaratish orqali talabalarga nafaqat dars vaqtida, balki mustaqil ravishda istalgan joydan turib topshiriqlarni bajarish imkoniyatini yaratish.

4. Doimiy yangilanuvchi tizimini yo‘lga qo‘yish.

Kiberfazodagi tahdidlar doimiy o‘zgarib turishini inobatga olib, dasturiy ta’lim vositalarining modullarini real vaqtdagi yangi zaifliklar va kiberhujum ssenariylari bilan doimiy boyitib borish mexanizmini yaratish. Bu o‘quv materiallarining eskirib qolishining oldini oladi.

Ushbu takliflar hayotga tatbiq etilsa, oliy ta’lim bitiruvchisi kasbiy faoliyatini boshlaganda real kiberhujumlarni aniqlash, ularni tahlil qilish va bartaraf etishga tayyor mutaxassis bo‘lib yetishadi. Bu esa kadrlar tayyorlashda nazariya va amaliyot o‘rtasidagi uzilish muammosini pedagogik jihatdan to‘liq hal etadi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida"gi PF-6079-son Farmoni.

2. Panakkadan, R. R., Meher, P., More, S. A., & Sudhakaran. Enhancing Cybersecurity Education: The Impact of Simulated Learning and Interactive Tutorials on Student Performance and Anxiety Reduction. Florida Institute of Technology, United States. 2023

ISSN 3030-3907

3. Kure, H. I., Islam, S., & Razzaque, M. A. “An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System.” *Applied Sciences*, 2018. 8(6), 898.
4. G‘ulomov S.S., Shermuxamedov A.T., Begalov B.A. “Raqamli iqtisodiyot: axborot xavfsizligini ta’minlash va boshqarish”. Toshkent, Fan va texnologiyalar nashriyoti. 2020.
5. Yildirim, M., & Ali, A. “Pedagogical Approaches to Teaching Information Security: The Role of Virtual Labs.” *International Journal of Information Security and Privacy*, 2022. 16(2).
6. Qilichev, T. S., Virtual laboratoriyalar va ularning ta’lim tizimidagi ahamiyati. Ta’lim va taraqqiyot, 2025 (6)
7. https://www.av-test.org/en/statistics/malware/.

ISSN 3030-3907