TA’LIM MUASSASALARIDA AXBOROT XAVFSIZLIGI MADANIYATINI SHAKLLANTIRISHDA AXBOROT TEXNOLOGIYALARIGA OID KAFEDRALARNING O‘RNI.

Ismoilova Dilrabo Sidikjonovna
FarDU axborot texnologiyalari kafedrasi katta o‘qituvchisi
dilraboxonismoilova59@gmail.com

Annotatsiya. Maqolada zamonaviy raqamli jamiyatda axborot xavfsizligi madaniyatini shakllantirishning dolzarb masalalari ko‘rib chiqilgan. Ta’lim muassasalari, xususan oliy ta’lim tizimida axborot texnologiyalariga oid kafedralarning axborot xavfsizligi madaniyatini rivojlantirishdagi o‘rni va imkoniyatlari tahlil qilingan. Maqolada axborot xavfsizligi madaniyatining tushunchasi, uning asosiy komponentlari (bilim, amaliy ko‘nikmalar, qiymat-qadriyatlar tizimi va xulq-atvor namunalari) batafsil ochib berilgan.

Ta’lim muassasalarining duch keladigan zamonaviy kibertahdidlar - phishing hujumlari, ransomware, DDoS hujumlari, ma’lumotlar o‘g‘irlash kabi tashqi tahdidlar hamda xodimlar va talabalarning axborot xavfsizligi qoidalaridan bexabar bo‘lishi, zaif parollar, eskirgan infrastruktura kabi ichki muammolar o‘rganilgan. O‘zbekiston ta’lim tizimining o‘ziga xos xususiyatlari va muammolari alohida ta’kidlangan.

Kalit so‘zlar: axborot xavfsizligi, axborot xavfsizligi madaniyati, ta’lim muassasalari, axborot texnologiyalari kafedralari, kiberxavfsizlik, kibertahdidlar, kadrlar tayyorlash, raqamli savodxonlik, ta’lim texnologiyalari, O‘zbekistonda raqamli ta’lim tizimi.

Аннотация. В статье рассматриваются актуальные вопросы формирования культуры информационной безопасности в современном цифровом обществе. Проанализированы роль и возможности кафедр информационных технологий в развитии культуры информационной безопасности в образовательных учреждениях, особенно в системе высшего образования. Подробно раскрыто понятие культуры информационной безопасности, её основные компоненты (знания, практические навыки, система ценностей и модели поведения). Изучены современные киберугрозы, с которыми сталкиваются образовательные учреждения - внешние угрозы (фишинг-атаки, программы-вымогатели, DDoS-атаки, кража данных) и внутренние проблемы (неосведомленность сотрудников и студентов о правилах информационной безопасности, слабые пароли, устаревшая инфраструктура). Отдельно подчеркнуты специфические особенности и проблемы системы образования Узбекистана.

ISSN 3030-3907

Ключевые слова: информационная безопасность, культура информационной безопасности, образовательные учреждения, кафедры информационных технологий, кибербезопасность, киберугрозы, подготовка кадров, цифровая грамотность, образовательные технологии, система образования Узбекистана.

Annotation. The article examines current issues of information security culture formation in modern digital society. The role and capabilities of information technology departments in developing information security culture in educational institutions, especially in the higher education system, are analyzed. The concept of information security culture and its main components (knowledge, practical skills, value system, and behavioral patterns) are thoroughly explained. Modern cyber threats faced by educational institutions are studied - external threats (phishing attacks, ransomware, DDoS attacks, data theft) and internal problems (lack of awareness among staff and students about information security rules, weak passwords, outdated infrastructure). The specific features and problems of Uzbekistan's education system are particularly emphasized.

Keywords: information security, information security culture, educational institutions, information technology departments, cybersecurity, cyber threats, personnel training, digital literacy, educational technologies, education system of Uzbekistan.

KIRISH.

Zamonaviy raqamli jamiyatda axborot xavfsizligi masalalari tobora dolzarb ahamiyat kasb etmoqda. Jahon maydoni bo‘yicha har yili kiberxujumlar soni ortib bormoqda va bu xavflar nafaqat yirik korporatsiyalar, balki ta’lim muassasalariga ham o‘z xujumini qaratmoqda. O‘zbekiston Respublikasida axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi, ta’lim tizimining raqamlashtirish jarayoniga faol kirib borishi axborot xavfsizligi madaniyatini shakllantirishni dolzarb vazifaga aylantirmoqda.

Ta’lim muassasalari, ayniqsa oliy ta’lim tizimi, nafaqat bilim beruvchi muassasa sifatida, balki axborot xavfsizligi sohasida malakali mutaxassislar tayyorlash va jamiyatda axborot xavfsizligi madaniyatini shakllantirish markazlari vazifasini bajarishi lozim. Bu jarayonda axborot texnologiyalariga oid kafedralar muhim rol o‘ynaydi.

Axborot xavfsizligi madaniyati deganda jamiyat a’zolarining, tashkilot xodimlarining axborot resurslari va texnologiyalari bilan ishlashda xavfsizlik tamoyillariga rioya qilish bo‘yicha shakllangan bilim, ko‘nikma, odatlari va qadriyatlari tizimi tushuniladi. Bu madaniyat nafaqat texnik bilimlarni, balki psixologik, axloqiy va tashkiliy jihatlarni ham o‘z ichiga oladi.

ISSN 3030-3907

Bilim komponenti - axborot xavfsizligining asosiy tushunchalari va tamoyillarini bilishni, zamonaviy kibertahdidlar va ularning xususiyatlarini tushunishni, xavfsizlik texnologiyalari va vositalaridan foydalanish qoidalarini o‘zlashtirishni hamda qonunchilik bazasi va normativ-huquqiy hujjatlar bilan tanishlikni o‘z ichiga oladi.

Amaliy ko‘nikmalar komponenti - murakkab parollar yaratish va ularni to‘g‘ri boshqarish, elektron pochta va ijtimoiy tarmoqlarda xavfsiz muloqot yuritish, shaxsiy ma’lumotlarni himoya qilish texnikalarini qo‘llash, viruslar va zararli dasturlardan himoyalanish usullarini amalda qo‘llash hamda zaxira nusxalarini to‘g‘ri tashkil etishni nazarda tutadi.

Qiymat-qadriyatlar tizimi - shaxsiy va tashkiliy ma’lumotlar maxfiyligini qadrlash, axborot resurslari yaxlitligiga mas'uliyatli munosabat, raqamli huquq va odobi tamoyillarini qabul qilish hamda kiberjinoyatchilik va uning oqibatlarini anglashni o‘z ichiga oladi.

Xulq-atvor namunalari - barcha qurilmalarda yangilanishlarni o‘z vaqtida o‘rnatish, noma’lum manbalardan kelgan havolalar va fayllarni tekshirmasdan ochmaslik, ommaviy Wi-Fi tarmoqlarida ehtiyotkorlik bilan ishlash va shubhali holatlar haqida darhol xabar berish kabi amaliy ko‘nikmalarni aks ettiradi.

Ta’lim muassasalarida axborot xavfsizligi madaniyatini shakllantirish bir necha muhim sabablar tufayli zarur:

- Birinchidan, ta’lim muassasalari katta hajmdagi shaxsiy ma’lumotlarni saqlaydi va qayta ishlaydi. Talabalar, o‘qituvchilar va xodimlarning shaxsiy ma’lumotlari, akademik natijalar, moliyaviy ma’lumotlar va boshqa maxfiy axborotlar xavfsiz muhofaza qilinishi kerak.
- Ikkinchidan, ta’lim muassasalari kiberxujumchilar uchun jozibador maqsaddir. Statistik ma’lumotlarga ko‘ra, ta’lim sohasidagi muassasalar boshqa sohalarga nisbatan ko‘proq kiberxujumlarga duchor bo‘ladi. Bu muassasalarning ko‘pincha cheklangan moliyaviy resurslari, eskirgan texnologiyalari va xavfsizlik xizmatlarining zaif bo‘lishi bilan bog‘liq.
- Uchinchidan, ta’lim muassasalari kelajak mutaxassislarni tayyorlaydi. Talabalar universitet davrida shakllantirgan axborot xavfsizligi odatlari va qadriyatlari ularning butun professional faoliyati davomida saqlanadi. Shuning uchun, ta’lim jarayonida axborot xavfsizligi madaniyatini shakllantirishning keng ta’siri va uzoq muddatli ahamiyati mavjud.

Zamonaviy ta’lim muassasalari duch keladigan asosiy tahdidlar quyidagilardan iborat. ***Tashqi taxdidlar:***

ISSN 3030-3907

1. Phishing hujumlari - o‘qituvchi va talabalar elektron pochtalari orqali amalga oshiriladigan firibgarlik urinishlari. Kiberxujumchilar universitet nomidan xat yuborib, foydalanuvchilarni shaxsiy ma’lumotlarini kiritishga undaydi.
2. Ransomware (to‘lov talqini) - ta’lim muassasasi ma’lumotlar bazasini shifrlash va to‘lov talab qilish. Bu xujumlar natijasida akademik ma’lumotlar, tadqiqotlar va boshqaruv tizimlari ishdan chiqishi mumkin.
3. DDoS hujumlari - ta’lim portallari va masofaviy ta’lim tizimlarini ishdan chiqarish. Bu ayniqsa imtihon davrlari va muhim akademik hodisalar paytida katta zarar keltirishi mumkin.
4. Ma’lumotlarni o‘g‘irlash - talabalar va xodimlarning shaxsiy ma’lumotlarini noqonuniy ravishda olish. Bunday ma’lumotlar qora bozorda sotilishi yoki identifikatsiyani o‘g‘irlash uchun ishlatilishi mumkin.

Ichki tahdidlar:

1. Xodimlar va talabalarning axborot xavfsizligi qoidalaridan bexabar bo‘lishi. Ko‘pchilik foydalanuvchilar asosiy xavfsizlik tamoyillarini bilmaydi yoki ularni jiddiy qabul qilmaydi.
2. Zaif parollar va ularni bir necha tizimda takror ishlatish. Ko‘plab foydalanuvchilar “123456” yoki “password” kabi oddiy parollardan foydalanadi.
3. Shaxsiy qurilmalarni ta’lim muassasasi tarmog‘iga noxolis ulash (BYOD muammosi). Bu tashqi zaifliklarni tashkilot tarmog‘iga kiritishi mumkin.

Infrastruktura muamolari:

1. Eskirgan server va tarmoq uskunalari. Ko‘plab ta’lim muassasalari moliyaviy cheklovlar tufayli texnologiyalarini yangilay olmaydi.
2. Yangilanmagan operatsion tizimlar va dasturiy ta’minot. Ma’lum zaifliklar va xavfsizlik teshiklari tuzatilmagan holda qoladi.
3. Ma’lumotlar zaxira nusxalari tizimining yo‘qligi yoki noto‘g‘ri tashkil etilishi Ransomware hujumi yoki texnik nosozlik holatida ma’lumotlarni tiklash qiyin bo‘ladi.

O‘zbekiston ta’lim tizimida axborot xavfsizligi bo‘yicha bir qator o‘ziga xos muammolar mavjud. Ko‘pchilik ta’lim muassasalarida axborot xavfsizligi bo‘yicha alohida mutaxassislar yo‘q, bu vazifa ko‘pincha sistema administratorlari yoki IT xodimlari zimmasiga yuklanadi. Axborot xavfsizligi tushunchasi ko‘pincha faqat texnik masala sifatida qaraladi, uning inson omili, tashkiliy va madaniy jihatlariga yetarlicha e‘tibor berilmaydi.

O‘zbek tilida sifatli ta’lim materiallari va qo‘llanmalar yetishmasligi ham katta muammo hisoblanadi. Ko‘pgina resurslar faqat ingliz yoki rus tillarida mavjud bo‘lib, bu bazi o‘qituvchi va talabalar uchun to‘siq yaratadi. Bundan

ISSN 3030-3907

tashqari, axborot xavfsizligi madaniyati hali jamiyatda to‘liq shakllanmagan va raqamli savodxonlik darajasi turli guruhlar orasida farq qiladi.

Oliy ta’lim muassasalarida axborot texnologiyalariga oid kafedralar axborot xavfsizligi madaniyatini shakllantirishda markaziy rol o‘ynaydi. Ushbu kafedralar bir vaqtning o‘zida bir necha muhim funksiyalarni bajaradi va turli yo‘nalishlarda faoliyat yuritadi.

Axborot texnologiyalari kafedralari “Axborot xavfsizligi asoslari”, “Kriptografiya va ma’lumotlarni shifrlash”, “Tarmoq xavfsizligi”, “Veb-ilovalar xavfsizligi”, “Mobil ilovalar xavfsizligi”, “Zaif tomonlarni aniqlash va pentesting”, “Kiberjinoyatchilik bilan kurash”, “Ma’lumotlar bazalari xavfsizligi” va “Bulutli texnologiyalar xavfsizligi” kabi fanlarni o‘qitish orqali bevosita axborot xavfsizligi mutaxassislarini tayyorlaydi.

Barcha yo‘nalishlardagi talabalar uchun “Informatika” kursida shaxsiy ma’lumotlar himoyasi va xavfsiz internetdan foydalanish, “Dasturlash” kurslarida xavfsiz kod yozish tamoyillari, “Ma’lumotlar bazalari” kursida SQL-injection va boshqa hujumlardan himoyalanish, “Operatsion tizimlar” kursida foydalanuvchilar huquqlarini boshqarish va tizim xavfsizligi mavzulari kiritilishi kerak.

Qisqa muddatli kurslar va treninglar, sertifikatlashtirish dasturlari (CISSP, CEH, CompTIA Security+ ga tayyorlov), o‘qituvchilar va tashkilotlar xodimlari uchun mahorat oshirish kurslari hamda onlayn ta’lim platformalari yaratish va boshqarish ham kafedra vazifalariga kiradi.

Axborot texnologiyalari kafedralari mahalliy tahdidlar landshaftini o‘rganish, o‘zbek tiliga moslashtirilgan axborot xavfsizligi yechimlari ishlab chiqish, sun'iy intellekt va mashinani o‘rgatish texnologiyalaridan xavfsizlik sohasida foydalanish, blokcheyn texnologiyalarining qo‘llanilishi, kvant kriptografiyasi sohasida tadqiqotlar, IoT qurilmalari xavfsizligi va biometrik autentifikatsiya tizimlari kabi yo‘nalishlarda ilmiy izlanishlar olib boradi.

Ilmiy nashrlar va konferensiyalar orqali kafedra o‘z tadqiqot natijalarini taqdim etadi. Xalqaro va mahalliy ilmiy jurnallarda maqolalar chop etish, ilmiy-amaliy konferentsiyalar tashkil etish, talabalarga ilmiy tadqiqot metodologiyasini o‘rgatish hamda magistrlik va doktorlik dissertatsiyalariga rahbarlik qilish kafedra ilmiy faoliyatining muhim qismidir.

Real sektorga xizmat ko‘rsatish bo‘yicha kafedra korxonalar uchun xavfsizlik auditi o‘tkazish, axborot xavfsizligi siyosati va tartib-qoidalarini ishlab chiqishda yordam berish, kichik va o‘rta biznes uchun axborot xavfsizligi maslahatlari berish va davlat muassasalari bilan hamkorlik qilish kabi faoliyatlarni amalga oshiradi.

ISSN 3030-3907

Talabalarni amaliyotga jalb etish orqali ular haqiqiy loyihalarda ishtirok etish imkoniyatiga ega bo‘ladi. Startap-loyihalar yaratish, CTF musobaqalari platformalari va xavfsizlik sinovlari vositalarini ishlab chiqish, kompaniyalar bilan birgalikda diplomga tayyorgarlik ko‘rish kabi tadbirlar talabalarga amaliy tajriba beradi.

Universitetda ommaviy tadbirlar tashkil etish kafedra faoliyatining muhim qismidir. Axborot xavfsizligi haftasi yoki oyi o‘tkazish, kundalik maslahatlar va vorkshoplar uyushtirish, ochiq eshiklar kunlari tashkil etish - bu tadbirlar talabalarning qiziqishini oshiradi va ularni soha bilan yaqindan tanishtirishga yordam beradi. Musobaqalar va hackathonlar o‘tkazish ham samarali vositadir. CTF (Capture The Flag) musobaqalari, bug bounty dasturlari universitetning tizimlari uchun, kiberxavfsizlik stsenariylarini hal qilish bo‘yicha turnirlar va talabalararo dasturlash marafonlari xavfsizlik yo‘nalishida o‘tkazilishi mumkin.

Onlayn platforma va resurslar yaratish zamonaviy ta’limning ajralmas qismidir. Axborot xavfsizligi bo‘yicha onlayn kurslar, video darsliklar va webinarlar arxivi, interaktiv simulyatorlar va amaliy mashqlar, testlar va sertifikatlar tizimi orqali talabalar o‘z bilimlarini mustaqil ravishda oshirishlari mumkin.

Sifatli ta’lim berish uchun kafedra xodimlari yuqori malakaga ega bo‘lishi kerak. O‘qituvchilar axborot xavfsizligining fundamental asoslari, kriptografiya va tarmoq protokollari bo‘yicha chuqur nazariy bilimga ega bo‘lishlari kerak. Shu bilan birga, ular real loyihalarda ishtirok etgan va haqiqiy kiberhujumlarga javob bergan amaliy tajribaga ham ega bo‘lishlari zarur.

Xalqaro sertifikatlar (CISSP, CISM, CEH, OSCP, GIAC va boshqalar) egasi bo‘lish kafedra o‘qituvchilari uchun muhim talabdir. Bundan tashqari, murakkab texnik tushunchalarni tushunarli tarzda tushuntira oladigan pedagogik mahorat ham zarur. O‘qituvchilar doimiy ravishda yangi texnologiyalar va tahdidlardan xabardor bo‘lishlari kerak. Kadrlar tayyorlash strategiyasi magistratura va aspiranturaga iqtidorli talabalarni jalb etishni, amaliy tajribaga ega mutaxassislarni kafedralarga taklif qilishni, o‘qituvchilarni xalqaro konferentsiyalar va treninglarga yuborishni hamda ishlab chiqarish sektorida vaqtincha ishlash imkoniyatini yaratishni o‘z ichiga oladi.

Maxsus laboratoriyalar yaratish axborot xavfsizligi ta’limining muhim qismidir. Penetration Testing laboratoriyasi izolyatsiya qilingan tarmoq muhiti, turli xil zaif tizimlar va ilovalar to‘plami, hujumlar va mudofaa vositalari hamda paket analizatorlaridan iborat bo‘lishi kerak. Kriptografiya laboratoriyasi shifrlash algoritmlarini tahlil qilish vositalari, kvant kompyuterlar simulyatorlari, blokcheyn texnologiyalari platformasi va PKI tizimini o‘z ichiga olishi kerak. Tarmoq

ISSN 3030-3907

xavfsizligi laboratoriyasida Firewall va IDS/IPS tizimlari, SIEM tizimlari, VPN texnologiyalari va tarmoq monitoring vositalari bo‘lishi zarur. Malware tahlili laboratoriyasi izolyatsiya qilingan virtual muhit, reverse engineering vositalari, statik va dinamik tahlil platformalari hamda sandbox muhitlaridan tashkil topishi kerak. Bulutli texnologiyalar xavfsizligi laboratoriyasi AWS, Azure, Google Cloud platformalari, container texnologiyalari, DevSecOps vositalari va Cloud Security Posture Management tizimlarini o‘z ichiga olishi lozim.

Universitetlararo hamkorlik ikki diplom dasturlari, talabalar va o‘qituvchilar almashinuvi, umumiy onlayn kurslar va MOOC platformalari hamda birgalikda magistratura dasturlarini o‘z ichiga oladi. Ilmiy hamkorlik qo‘shma tadqiqot loyihalari, grantlar uchun birgalikda ariza topshirish, xalqaro jurnallarda ko‘p muallifli maqolalar va birgalikda konferensiyalar o‘tkazish orqali amalga oshiriladi.

Grantlar va fond mablag‘lari xalqaro donor tashkilotlar, ilmiy fondlar va IT-kompaniyalar grant dasturlari orqali olinadi. Xizmatlar ko‘rsatishdan daromad konsalting xizmatlari, attestatsiya va sertifikatlashtirish, qo‘shimcha ta’lim dasturlari, maxsus kurslar va treninglar hamda xavfsizlik auditi va pentesting xizmatlaridan tushadi.

Axborot xavfsizligi madaniyatini shakllantirish metodologiyasi to‘rt asosiy bosqichdan iborat:

Birinchi bosqich - xabardorlik (Awareness) - barcha ta’lim jarayoni ishtirokchilarini axborot xavfsizligining ahamiyati bilan tanishtirish maqsadini ko‘zlaydi. Bu bosqichda universitet portalida maxsus bo‘lim yaratiladi, kirish darslarida axborot xavfsizligi mavzusi joriy etiladi, plakatlar, bukletlar va infografikalar tarqatiladi.

Ikkinchi bosqich - ta’lim (Training) - amaliy ko‘nikmalarni rivojlantirish va xavfsiz ish odatlarini shakllantirish maqsadiga ega. Bu bosqichda barcha talabalar uchun majburiy “Axborot xavfsizligi asoslari” kursi o‘qitiladi, xodimlar uchun yillik treninglar o‘tkaziladi, rolga qarab maxsus kurslar tashkil etiladi va onlayn modullar hamda interaktiv mashqlar taqdim etiladi.

Uchinchi bosqich - mahorat (Skill Development) - murakkab vaziyatlarda to‘g‘ri qaror qabul qilish qobiliyatini rivojlantirishga qaratilgan. Bu bosqichda maxsus mutaxassislar uchun chuqur kurslar, sertifikatlashtirish dasturlariga tayyorgarlik, amaliy laboratoriya ishlari va loyihalar, real holatlar tahlili hamda CTF musobaqalari va hackathonlar o‘tkaziladi.

To‘rtinchi bosqich - madaniyat (Culture) - axborot xavfsizligini kundalik faoliyatning ajralmas qismiga aylantirishni nazarda tutadi. Bu bosqichda xavfsizlik hodisalarini darhol xabar berish tizimi joriy etiladi, eng yaxshi amaliyotlar targ‘ib

ISSN 3030-3907

qilinadi va mukofotlanadi, muntazam xavfsizlik auditlari o‘tkaziladi va doimiy takomillashtirish sikli amalga oshiriladi.

Har bir maqsadli guruh uchun maxsus yondashuv zarur. Birinchi kurs talabalariga orientatsiya dasturi, asosiy xavfsizlik qoidalari, universitet tizimlaridan foydalanish qoidalari va ijtimoiy tarmoqlarda xavfsizlik bo‘yicha ma’lumotlar beriladi. Katta kurs talabalari uchun mutaxassislik bo‘yicha maxsus kurslar, diplomlarda axborot xavfsizligi aspektlarini qo‘llash, amaliy loyihalar va stajlar hamda professional rivojlanish yo‘llari taqdim etiladi.

O‘qituvchilar uchun pedagogik platformalar xavfsizligi, intellektual mulk himoyasi, plagiatchilik va akademik halollik, onlayn darslar xavfsizligi hamda talabalar ma’lumotlarini himoya qilish mavzulari muhim ahamiyatga ega. Ma’muriy xodimlar uchun shaxsiy ma’lumotlarni qayta ishlash qoidalari, email xavfsizligi, hujjat bilan ishlashda xavfsizlik, moliyaviy ma’lumotlar himoyasi va hodisalar bo‘yicha javob berish protokollari o‘rgatiladi.

IT xizmat xodimlari uchun kengaytirilgan texnik treninglar, xavfsizlik standartlari va best practices, hodisalarga javob berish, zaifliklarni boshqarish hamda professional sertifikatlar olish dasturlari tashkil etilishi maqsadga muvofiqdir.

O‘zbekistonda axborot texnologiyalari kafedralarini rivojlantirish uchun davlat tomonidan maxsus dastur qabul qilish, standartlashtirish, davlat buyurtmasi tizimini yaratish zarur. Universitetlar darajasida tashkiliy qayta qurish, o‘quv jarayonini takomillashtirish, kadrlar siyosatini yaxshilash va biznes bilan integratsiyani kuchaytirish talab etiladi.

Xalqaro hamkorlikni kengaytirish, top universitetlar bilan qo‘shma dasturlar yaratish, xalqaro standartlarni joriy etish va global hamjamiyatga qo‘shilish muhim vazifalardir. Yangi texnologiyalar - sun'iy intellekt, kvant texnologiyalari, blokcheyn va IoT sohasida tadqiqotlarni rivojlantirish kelajak uchun zarur.

Interdissiplinar yondashuv orqali psixologiya, huquqshunoslik va biznesni kiberxavfsizlik bilan birlashtirish, milliy xususiyatlarni hisobga olgan holda mahalliy kontekst va yechimlari ishlab chiqish, davomiy ta’lim ekotizimini yaratish va sertifikatlashtirish yo‘llarini rivojlantirish zamonaviy ta’lim tizimining talablaridir.

Axborot xavfsizligi madaniyatini shakllantirish faqat texnik masala emas. U insoniy, tashkiliy, pedagogik va madaniy jihatlarni o‘z ichiga oladi. Kafedralarning strategik roli nafaqat mutaxassislar tayyorlash, balki ilmiy-tadqiqot markazlari, konsalting xizmatlari provayderlari, jamiyat uchun ma’rifat markazlari, davlat va biznes uchun intellektual resurs hamda innovatsiya va startaplar inkubatori sifatida namoyon bo‘ladi.

ISSN 3030-3907

Axborot xavfsizligi ta’limiga sarflanadigan mablag‘lar milliy kiberhavfsizlik qobiliyatiga investitsiya, raqamli iqtisodiyot rivojlanishi uchun asos, innovatsion texnologiyalar yaratish salohiyati, xalqaro maydonda raqobatbardoshlikni ta’minlash va kelajak avlodning xavfsiz raqamli hayotini ta’minlashdir.

Xalqaro tajribalarni ko‘chirish emas, balki O‘zbekistonning o‘ziga xos tahdidlari, mahalliy til va madaniyat xususiyatlari, mavjud resurslar va imkoniyatlar, davlat strategiyalari va ustuvorliklari hamda mintaqaviy hamkorlik potentsialini hisobga olgan holda moslash kerak.

Raqamli transformatsiya davri Respublikamiz oldiga katta imkoniyatlar va qiyin vazifalarni qo‘ymoqda. Axborot texnologiyalari kafedralari bu jarayonda muhim rol o‘ynaydi - ular nafaqat texnik bilim beradi, balki xavfsiz raqamli kelajak uchun zarur bo‘lgan madaniyat, qadriyatlar va mas'uliyat tuyg‘usini singdiradi.

Har bir universitet, har bir kafedra, har bir professor-o‘qituvchi va har bir talaba bu katta maqsadga o‘z hissasini qo‘shishi mumkin va qo‘shishi kerak. Axborot xavfsizligi madaniyati - bu hamma uchun vazifa va hamma uchun imkoniyatdir. Kelajak bizning qo‘limizda - uni xavfsiz va ishonchli qilish bizning mas’uliyatimizdir.

ADABIYOTLAR

1. O‘zbekiston Respublikasi Prezidentining “Axborot xavfsizligi milliy tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi PF-6177-son Farmoni, 2020 yil.
2. “Raqamli O‘zbekiston-2030” strategiyasi.
3. National Institute of Standards and Technology (NIST). “Cybersecurity Framework”, 2018.
4. European Union Agency for Cybersecurity (ENISA). “Cybersecurity Culture Guidelines”, 2023.
5. (ISC)². “Global Cybersecurity Workforce Study”, 2023.
6. World Economic Forum. “The Global Risks Report”, 2024.
8. Cisco. “Cybersecurity Readiness Index”, 2024.
9. Carnegie Mellon University. “CERT Division Annual Report”, 2023.
10. Georgia Institute of Technology. “Cybersecurity Education Programs”, 2024.
11. Technical University of Denmark. “Security Culture Implementation Report”, 2023.

ISSN 3030-3907