QO‘QON DAVLAT PEDAGOGIKA INSTITUTI ILMIY XABARLARI
(2025-yil 2-son)

PEDAGOGIKA

PEDAGOGY

AXBOROT XAVFSIZLIGINI TA’MINLASHNING AXBOROT KOMPETENSIYASINI RIVOJLANTIRISHDAGI AHAMIYATI

Rajabova Gulrux Yusufboy qizi
Urganch innovatsion universiteti o‘qituvchisi
https//orcid.org/ 0009-0007-6420-8707
rajabovagulrux@uriu-edu.uz

ANNOTATSIYA: Mazkur maqola axborot xavfsizligini ta’minlash hamda axborot xavfsizligini ta’minlashning axborot kompetensiyasini rivojlantirishdagi ahamiyati mavzusiga bag‘ishlangan bo‘lib, axborot xavfsizligining hozirgi kundagi ahamiyati hamda uni ta’minlashning asosiy yo‘nalishlarini tahlil etadi. Axborot xavfsizligi nafaqat har bir davlat va mamlakat balki butun dunyo xalqlari uchun ham dolzarb ekanligi bilan ham muhim ijtimoiy va iqtisodiy soha sifatida diqqat markaziga tushgan. Ushbu maqolada aynan axborot xavfsizligi ta’minlashda qanday sa’y-harakatlar qilish haqida tushunchalar beriladi, axborot xavfsizligini ta’minlash usul va vositalarini o‘zlashtirish orqali axborot kompetensiyasini rivojlantirish haqida fikr-mulohazalar keltiriladi.

Kalit so‘zlar: axborot, axborot xavfsizligi, axborot kompetensiyasi, konstitutsiya, ommaviy axborot vositalari, kriptografiya, firewall, maxfiylik.

ВАЖНОСТЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАЗВИТИИ ИНФОРМАЦИОННОЙ КОМПЕТЕНТНОСТИ

АННОТАЦИЯ: Данная статья посвящена теме обеспечения информационной безопасности и значению обеспечения информационной безопасности в развитии информационной компетентности, а также анализируется значение информационной безопасности сегодня и основные направления ее обеспечения. Информационная безопасность оказалась в центре внимания как важная социально-экономическая сфера, поскольку она актуальна не только для каждого государства и страны, но и для народов всего мира. В данной статье даются представления о том, как прилагать усилия для обеспечения информационной безопасности, приводятся отзывы о развитии информационной компетентности путем освоения методов и средств обеспечения информационной безопасности.

Ключевые слова: информация, информационная безопасность, информационная компетентность, конституция, средства массовой информации, криптография, межсетевой экран, конфиденциальность.

THE IMPORTANCE OF PROVIDING INFORMATION SECURITY IN THE DEVELOPMENT OF INFORMATION COMPETENCE

ABSTRACT: This article is devoted to the topic of ensuring information security and the importance of ensuring information security in the development of information competence, and analyzes the importance of information security today and the main directions of its provision. Information security has become the focus of attention as an important social and economic field, as it is relevant not only for every state and country, but also for the people of the whole world. This article provides insights on how to make efforts to ensure information security, provides feedback on the development of information competence by mastering the methods and means of ensuring information security.

Key words: information, information security, information competence, constitution, mass media, cryptography, firewall, privacy.

KIRISH.

Bugungi kunga kelib butun dunyoda axborotdan oqilona foydalanish hamda axborot xavfsizligini ta’minlash masalasi dolzarbligicha qolmoqda. Axborot xavfsizligini ta’minlash — bu axborot tizimlarining himoya qilishni va foydalanuvchilarning shaxsiy ma’lumotlarini zararli xurujlardan saqlashni o‘z ichiga olgan tizimli jarayondir. Axborot xavfsizligini ta’minlashga qaratilgan normativ-huquqiy asoslar mamlakatlarning qonunchilik tizimlari tomonidan ishlab chiqilgan va tasdiqlangan me’yoriy hujjatlar to‘plamidan iboratdir. Bu asoslar axborot xavfsizligi sohasidagi barcha yuridik va iqtisodiy jarayonlarni tartibga soladi. Axborot xavfsizligini ta’minlashga doir normativ hujjatlar, asosan, davlatlar tomonidan ishlab chiqilgan milliy qonunlar, xalqaro konvensiyalar va shartnomalar orqali amalga oshiriladi [4].

Davlat va jamiyatning eng muhim jabhalarini dastlabki tarzda tartibga soluvchi me’yoriy huquqiy hujjat hisoblanmish konstitutsiyamizning ko‘plab normalarida ham aynan axborot xavfsizligining huquqiy jihatdan daslabki tarzda tartibga solinganligini ko‘rishimiz mumkin. Axborot xavfsizligini ta’minlashning huquqiy asoslari sifatida O‘zbekiston Respublikasining konstitutsiyasining 67-moddasini, ya'ni “Ommaviy axborot vositalari erkindir va qonunga muvofiq ishlaydi. Ular axborotning to‘g‘riligi uchun belgilangan tartibda javobgardirlar. Senzuraga yo‘l qo‘yilmaydi” deb axborot sohasidagi munosabatlarni tartibga solishini ko‘rishimiz mumkin. Ushbu modda orqali mamlakatimizda axborot bilan uzviy ravishda faoliyat olib boruvchi soha vakillarining va sektorlarning o‘zlari yig‘ayotgan, tarqatayotgan axborotlarining ishonchliligi va asoslanganligi, axborot hamda unga qo‘yilgan talab va me’yorlarga rioya qilinganligiga bevosita ma’suldirlar. Ya’ni uzatilayotgan axborot haqiqatga to‘g‘ri kelishi va chinligi uchun ommaviy axborot vositalari bevosita javobgardirlar. Bundan tashqari konstitutsiyamizning 27 va 29-moddalari ham axborot xavfsizligini bevosita ta’minlashga xizmat qiluvchi asosiy huquqiy norma hisoblanadi: “Hech kim qonun nazarda tutgan hollardan va tartibidan tashqari birovning turar joyiga kirishi, tintuv o‘tkazishi yoki uni ko‘zdan kechirishi, yozishmalar va telefonda so‘zlashuvlar sirini oshkor qilishi mumkin emas”,

bu konstitutsiyada ham axborotning xavfsizligini ta’minlash va fuqarolarning axborot sohasidagi xavfsizligini ta’minlovchi muhim qarordir.[5]

ADABIYOTLAR TAHLILI VA METODLAR.

Axborot xavfsizligi sohasida samarali himoya qilish choralarini ko‘rish uchun turli metodlar va vositalardan foydalanish zarur. Bu metodlar va vositalar axborot tizimlarining turli darajalarda xavfsizligini ta’minlashga yordam beradi. Axborot xavfsizligini ta’minlash metodlari va vositalari quyidagi asosiy yo‘nalishlar bo‘yicha taqsimlanadi:

Kriptografiya — axborotni maxfiy qilish va uning yaxlitligini ta’minlash uchun kriptografik metodlardan foydalanish. Bu metodlar orqali, ma’lumotlarni faqatgina ruxsat etilgan foydalanuvchilar o‘qishi va ishlatishi mumkin. Kriptografiya shifrlash va dekodlash, raqamli imzo va autentifikatsiya jarayonlarida qo‘llaniladi. Shuningdek, ma’lumotlarni tarmoq orqali yuborishda ham kriptografiya yordamida ma’lumotlarning maxfiyligi va yaxlitligini ta’minlash mumkin.

Avtorizatsiya va autentifikatsiya — tizimga kirish uchun foydalanuvchilarni aniqlash va ularga ruxsat berish jarayoni. Avtorizatsiya va autentifikatsiya tizimlari foydalanuvchilarning shaxsini tasdiqlashga yordam beradi. Avtorizatsiya foydalanuvchiga faqat ruxsat etilgan resurslarga kirish imkoniyatini beradi, autentifikatsiya esa foydalanuvchining kimligini tasdiqlash jarayonidir. Avtorizatsiya uchun foydalanuvchining paroli, biometrik ma’lumotlari, yoki ikki faktorlashgan autentifikatsiya metodlari ishlatiladi.

Firewalldan foydalanish — bu tarmoq xavfsizligini ta’minlash uchun ishlatiladigan vosita bo‘lib, tarmoqga kirish va chiqishni nazorat qiladi. Firewall tizimi orqali ma’lum tarmoqdan yoki Internetdan kirishlarni filtrlaydi va faqat xavfsiz bo‘lgan aloqalarga yo‘l qo‘yadi. Firewall tarmoqga qarshi kirib kelayotgan hujumlarni bloklash uchun ishlatiladi va shu bilan birga tizimni tashqi xavf-xatarlardan himoya qiladi. [2]

Ma’lumotlarni zaxiralash (Backup) — axborot xavfsizligini ta’minlashda yana bir muhim metod bo‘lib, tizimdagi ma’lumotlar yo‘qolishi yoki o‘g‘irlanishidan himoya qilish uchun zarurdir. Zaxiralash jarayoni axborotni qayta tiklash imkonini beradi, shu bilan birga tizimni xavfsizlik nuqtai nazaridan saqlaydi. Bunday zaxira nusxalarining tez-tez yangilanishi va saqlanishi kerak.

Ma’lumotlar bazasini himoya qilish — axborot xavfsizligi metodlarining muhim jihati bu ma’lumotlar bazasiga ruxsatsiz kirishni oldini olish va ma’lumotlarni himoya qilish. Ma’lumotlar bazasi xavfsizligini ta’minlash uchun shifrlash, ma’lumotlar bazasi foydalanuvchilarini autentifikatsiya qilish, hujjatlarni himoya qilish va zararli kodlarni aniqlashning turli usullaridan foydalaniladi.

Tarmoqni kuzatish va monitoring — tizim va tarmoqning doimiy ravishda monitoring qilish va tahlil qilish, axborot xavfsizligi uchun eng muhim vositalardan biridir. Bu metod orqali tarmoqdagi kirishlar va xatti-harakatlar nazorat qilinadi. Monitoring tizimlarida real vaqt rejimida xavfsizlik xatarlari aniqlanib, tizimga zarar yetkazmasdan oldini olish mumkin.

Psixologik xavfsizlikni ta’minlash — bu metod foydalanuvchilarni axborot xavfsizligi bo‘yicha o‘qitish va ularni xushyorlikka chaqirishni o‘z ichiga oladi. Ko‘plab xurujlar, ayniqsa phishing hujumlari, insonlarning e’tiborsizligi va xavfsizlik choralariga amal qilmasligidan kelib chiqadi. Shu sababli, foydalanuvchilarni axborot xavfsizligi bo‘yicha muntazam o‘qitib, ular xavf-xatarlarni oldindan sezishga o‘rgatish zarur.

Axborot xavfsizligini ta’minlashning yuqorida sanab o‘tilgan metodlari va vositalari faqatgina umumiy tavsiyalar bo‘lib, har bir tashkilot va tizim uchun eng samarali metodlarni tanlash zarur. Xavfsizlikni ta’minlashda tizimli yondashuv va doimiy yangilanishlar muhim ahamiyatga ega.

NATIJALAR VA MUHOKAMA.

Axborot xavfsizligini ta’minlashda axborot kompetensiyasini rivojlantirish muhim ahamiyatga ega. Axborot kompetensiyasiga ega bo‘lish – bu shaxsning qabul qilish qobiliyati va hayotining barcha sohalarida ma’lumotlardan foydalanishidir. Axborot kompetensiyasi har qanday inson faoliyatiga xos ma’lumot bo‘lgani uchun asosiy hisoblanadi. Shuning uchun axborot kompetensiyasini kalit deb atash mumkin. Axborot xavfsizligining tamoyillari zamonaviy axborot tizimlarida asosiy qoidalar bo‘lib, ularning himoyasini ta’minlash uchun zarurdir. Ularning har biri o‘z-o‘zidan tizim xavfsizligini mustahkamlashga yordam beradi va axborot xavfsizligi sohasida yuzaga keladigan barcha tahdidlarga qarshi kurashish uchun zarur asoslarni yaratadi. Axborot xavfsizligi tamoyillariga asoslangan tizimlar yanada ishonchli bo‘lib, foydalanuvchilarga xavfsiz va samarali xizmatlarni taqdim etadi.

Axborot xavfsizligining asosiy tushunchalari va tamoyillari haqida batafsilroq ma’lumotlar keltiradigan bo‘lsak, ularning har biri o‘ziga xos ahamiyatga ega. Bu tushunchalar va tamoyillarni chuqur anglash va to‘g‘ri qo‘llash axborot tizimlarining xavfsizligini ta’minlashda asosiy omil hisoblanadi.

Yaxlitlik va uning ta’minlanishi. Axborotning yaxlitligi tamoyili axborotning o‘zgarishsiz va buzilmas holatda saqlanishini ta’minlaydi. Yaxlitlikni ta’minlash uchun axborot tizimlarida audit izlari, axborotning autentifikatsiyasi va o‘zgarishlar monitoringi muhim ahamiyatga ega. Bu tamoyil, axborotning noto‘g‘ri yoki tasodifan o‘zgartirilishi yoki o‘chirilishini oldini olish uchun ishlatiladi. Yaxlitlikka zarar yetkazish mumkin bo‘lgan omillar orasida, xususan, tashqi haker hujumlari, ichki xodimlarning yomon niyatlari va texnik nosozliklar mavjud.

Mavjudlik va doimiy ishlashni ta’minlash. Axborot tizimlarining mavjudligi va doimiy ishlashi, tashkilotlarning samarali ishlashini ta’minlashda juda muhimdir. Mavjudlik tamoyili axborot tizimlarining ishlashini ta’minlash va ma’lumotlarga har doim kirish imkoniyatini yaratishni maqsad qiladi. Bu tamoyilning buzilishi, tizimning ishlashida uzilishlar yoki axborotlarga vaqtida kirish imkoniyatining yo‘qolishiga olib kelishi mumkin. Mavjudlikni ta’minlash uchun zaxira nusxalarini saqlash, tizimni qayta tiklash, uzilishlarga qarshi kurashish chora-tadbirlari va ishonchli tarmoq infratuzilmasi kerak [1].

Nazorat va monitoring tamoyili. Axborot xavfsizligini ta’minlashda nazorat va monitoring mexanizmlarini joriy etish zarur. Bunda tizimlar ustidan kuzatuv olib borish va

foydalanuvchilarning faoliyatini, tarmoqda yuz berayotgan har qanday noxush holatlarni nazorat qilish muhimdir. Monitoring orqali tizimga kirish huquqlarining noto‘g‘ri ishlatilishi, ma’lumotlar o‘zgartirilishi yoki axborotlarni o‘g‘irlashga urinishlar aniqlanadi. Nazorat tizimlari, shuningdek, joriy xavfsizlik chora-tadbirlarining samaradorligini baholash va kelgusidagi tahdidlar uchun tayyor turish imkonini beradi.

Auditing va huquqiy himoya. Axborot xavfsizligining huquqiy jihatlari ham muhimdir. Tizimda axborotlarning xavfsizligini ta’minlash uchun mavjud qonunlar va me'yorlarga rioya qilish zarur. Auditing tizimlarida tashkilotlarning ma’lumotlarni qanday boshqarishi, foydalanuvchi huquqlari qanday belgilanishi va axborotlar qanday himoyalanayotganini tekshirish uchun aniq huquqiy ko‘rsatmalar mavjud. Shuningdek, axborot xavfsizligiga doir ichki siyosatlar va normativ hujjatlar ham amalda bo‘lishi kerak. Tashkilotlarning axborot xavfsizligi bo‘yicha olib borayotgan ishlari ko‘p hollarda xalqaro me'yorlar va standartlarga asoslanadi.

Axborot xavfsizligi va inson faktori. Axborot xavfsizligini ta’minlashda faqat texnik usullar bilan cheklanmaslik kerak. Inson faktori ham muhim rol o‘ynaydi. Foydalanuvchilar, xodimlar va axborot tizimlarini ishlatadigan har bir kishi axborot xavfsizligiga jiddiy e’tibor qaratishi zarur. Foydalanuvchilarning maxfiylikni saqlash, murakkab parollarni ishlatish va xavfsiz tarmoq aloqalarini yaratish kabi axborot xavfsizligi tamoyillarini bilishi va amalda qo‘llashi kerak. Bu, o‘z navbatida, tashkilotning umumiy xavfsizligini ta’minlashga yordam beradi.

Axborot xavfsizligini ta’minlash bo‘yicha strategiyalar

Axborot xavfsizligini ta’minlash uchun aniq strategiyalar va rejalashtirish zarur. Har bir tashkilot o‘zining ehtiyojlari va xavflarini hisobga olgan holda, xavfsizlikni ta’minlash strategiyasini ishlab chiqishi lozim. Bu strategiya, ma’lumotlar uzatish xavfsizligini, tizimni himoya qilish, foydalanuvchi huquqlarini boshqarish, va zaxira nusxalarini yaratish kabi elementlarni o‘z ichiga oladi. Strategiyaning samarali bo‘lishi uchun tizimda muntazam tekshiruvlar va yangilanishlar amalga oshirilishi kerak.

XULOSA.

Xulosa sifatida shuni aytishimiz mumkinki, axborot xavfsizligini ta’minlash uchun aniq strategiyalar va rejalar ishlab chiqish zarur. Bu strategiya, ma’lumotlar uzatish xavfsizligini, tizimni himoya qilish, foydalanuvchi huquqlarini boshqarish, va zaxira nusxalarini yaratish kabi elementlarni o‘z ichiga oladi. Axborot xavfsizligi sohasida amalga oshirilayotgan chora-tadbirlar va texnologiyalar O‘zbekistonning axborot tizimlarini himoya qilishdagi qobiliyatini oshirmoqda. Mamlakatning axborot xavfsizligini ta’minlashdagi siyosati, texnologiyalari va normativ-huquqiy asoslari rivojlanishda davom etmoqda. Bu esa kelajakda mamlakatning axborot xavfsizligi sohasidagi barqarorligini ta’minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Abdullayev Sh., Raximov A. “Axborot xavfsizligi: nazariyasi va amaliyoti”. Tashkent:

Fan, 2022

2. Mirzoyev J., Abdullayev M. “Axborot xavfsizligi siyosati va uning amaliyotga tatbiqi”. Tashkent: Davlat nashriyoti, 2020

3. To‘xtasinov K. “Axborot xavfsizligini ta’minlashdagi muammolar va yechimlar”. Tashkent: ScienceTech, 2022

4. Zorina O. “Information security in the digital era”. London: Wiley-Blackwell, 2019

5. O‘zbekiston Respublikasi Konstitutsiyasi. “O‘zbekiston” 2020-yil 12-bet