AXBOROT XAVFSIZLIGI MUAMMOLARI VA ULARNI OLDINI OLISH USULLARI

Ubaydullayev Oybek Ulug`bekovich
Guliston shahar 1-sonli ixtisoslashtirilgan maktab internati informatika va axborot texnologiyalari fani o`qituvchisi
Email: magistr2021yil@gmail.com

Annotatsiya. *Maqolada axborot xavfsizligi muammolari va ularni oldini olish usullari ilmiy-nazariy hamda amaliy jihatdan tahlil qilingan. Shuningdek axborot xavfsizligining mohiyati, asosiy tamoyillari va tahdid turlari, zamonaviy himoya texnologiyalari, kriptografik usullar, biometrik tizimlar, tarmoqlarni himoyalash vositalari hamda O'zbekiston tajribasi asosida amalga oshirilayotgan chora-tadbirlar ko'rib chiqilgan.*

Kalit so'zlar*: axborot xavfsizligi, raqamli texnologiyalar, himoya tizimi, O'zbekiston, tahdid.*

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДЫ ИХ ПРЕДОТВР

Аннотация: *В статье научно-теоретически и практически проанализированы проблемы информационной безопасности и методы их предотвращения. Рассмотрены сущность информационной безопасности, основные принципы и виды угроз, современные технологии защиты, криптографические методы, биометрические системы, средства защиты сетей, а также меры, реализуемые в Узбекистане.*

Ключевые слова: *информационная безопасность, цифровые технологии, система защиты, Узбекистан, угроза.*

PROBLEMS OF INFORMATION SECURITY AND METHODS OF THEIR PREVENTION

Abstract: The article provides a scientific and practical analysis of information security issues and methods of their prevention. It examines the essence of information security, its main principles and types of threats, modern protection technologies, cryptographic methods, biometric systems, network security tools, as well as measures implemented based on Uzbekistan's experience.

Keywords: information security, digital technologies, protection system, Uzbekistan, threat.

KIRISH

Bugungi kunda axborot eng muhim strategik resurslardan biri sifatida e'tirof etilmoqda. Raqamli texnologiyalar, internet tarmoqlari va sun'iy intellekt

13.00.00. – PEDAGOGIKA FANLARI
JOURNAL.NAMSPI.UZ
ISSN: 2992-9008; UDK: 37

tizimlarining keng joriy etilishi natijasida axborot almashinuvi tezlashib, ijtimoiy, iqtisodiy va siyosiy jarayonlarga bevosita ta'sir ko'rsatmoqda. Shu bilan birga, axborotning ochiqligi va raqamli muhitning kengayishi xavfsizlikka oid yangi muammolarni yuzaga keltirmoqda. Axborot xavfsizligi masalalari bugungi kunda nafaqat texnik, balki ijtimoiy, huquqiy va axloqiy jihatdan ham dolzarb ahamiyat kasb etmoqda.

Axborot xavfsizligi - bu axborot resurslarini ruxsatsiz kirish, o'zgartirish, yo'q qilish yoki oshkor etishdan himoyalashni ta'minlaydigan tizimdir. U milliy xavfsizlikning ajralmas qismi bo'lib, davlat boshqaruvi, iqtisodiyot, ta'lim, sog'liqni saqlash va boshqa sohalarda axborot tizimlarining barqaror ishlashini kafolatlaydi.

TADQIQOT METODOLOGIYASI

Zamonaviy texnologik taraqqiyot sharoitida axborot xavfsizligiga tahdid soluvchi omillar tobora murakkablashib bormoqda. Kiberjinoyatlar, zararli dasturlar, fishing hujumlari, ma'lumotlarni noqonuniy yig'ish va sun'iy intellekt yordamida amalga oshirilayotgan kiberhujumlar shular jumlasidandir. Shu bois, ularni oldini olish uchun himoya tizimlarini doimiy ravishda takomillashtirish, kriptografik usullarni rivojlantirish, biometrik autentifikatsiya tizimlarini joriy etish hamda milliy axborot infratuzilmasini mustahkamlash zarur.

Bugungi globallashuv davrida axborot texnologiyalari jamiyat hayotining barcha jabhalariga chuqur kirib bormoqda. Davlat boshqaruvi, iqtisodiyot, sog'liqni saqlash, ta'lim, moliya tizimlari kabi sohalarda axborot oqimi hajmi keskin ortib bormoqda. Shu bilan birga, axborotning himoyalanganligi, ishonchliligi va maxfiyligi masalalari ham dolzarb ahamiyat kasb etmoqda.

Axborot xavfsizligi — bu axborot resurslarini ruxsatsiz kirish, o'zgartirish, tarqatish, yo'qotish yoki buzilishdan himoya qilishga qaratilgan tashkiliy, texnik, dasturiy va huquqiy choralar majmuasidir. U axborot tizimlarining barqaror ishlashi va foydalanuvchilarning ishonchini ta'minlaydi.

TAHLIL VA NATIJALAR

Axborot xavfsizligini ta'minlash uchun quyidagi asosiy yo'nalishlar ajratiladi: eexnik himoya vositalari – kompyuter tarmoqlari, serverlar, dasturiy ta'minot va apparat tizimlarini himoya qilish; eashkiliy chora-tadbirlar – xavfsizlik siyosatini

13.00.00. – PEDAGOGIKA FANLARI
JOURNAL.NAMSPI.UZ
ISSN: 2992-9008; UDK: 37

ishlab chiqish, xodimlarni tayyorlash, nazorat mexanizmlarini joriy etish; huquqiy asoslar – qonunlar, nizomlar va me'yoriy hujjatlar orqali axborot xavfsizligini tartibga solish; axborot madaniyati – foydalanuvchilarning ongida axborotdan to'g'ri foydalanish ko'nikmalarini shakllantirish. Quyidagi jadvalda axborot xavfsizligini ta'minlovchi omillar tahlil qilingan.

1-jadval. Axborot xavfsizligi tizimini ta'minlovchi asosiy omillar

№	Omil turi	Asosiy mazmuni	Natijasi
1.	Texnik vositalar	Dasturiy va apparat himoya tizimlari	Virus va tarmoq hujumlaridan himoya
2.	Tashkiliy choralar	Ichki xavfsizlik siyosati, vakolat nazorati	Ma'lumotlar oqimi nazorat qilinadi
3.	Huquqiy asoslar	Qonunlar, me'yoriy hujjatlar	Javobgarlik tizimi shakllanadi
4.	Inson omili	Kadrlar tayyorgarligi, axborot madaniyati	Xatoliklar kamayadi

Mazkur omillar o'zaro uyg'unlashgan holda ishlaganda, tashkilotning axborot xavfsizligi darajasi yuqori bo'ladi. Axborot xavfsizligiga tahdidlar — bu axborot tizimlariga zarar yetkazuvchi, ularning barqaror faoliyatini buzuvchi harakatlar yoki hodisalardir. Tahdidlar tabiati bo'yicha ichki va tashqi, tasodifiy va qasdli bo'lishi mumkin.

2-jadval. Axborot xavfsizligiga tahdidlarning asosiy turlari

№	Tahdid turi	Tavsif	Misollar
	Texnik tahdidlar	Dasturiy yoki apparat nosozliklar	Server ishdan chiqishi, tarmoq uzilishi
	Kiberhujumlar	Internet orqali amalga oshiriladigan zararli ta'sirlar	Virus, trojan, DDoS hujumlar
	Inson omili	Xodimning xatosi yoki xiyonati	Parolni oshkor qilish, noto'g'ri sozlama

13.00.00. – PEDAGOGIKA FANLARI
JOURNAL.NAMSPI.UZ
ISSN: 2992-9008; UDK: 37

	Ijtimoiy tahdidlar	Jamiyatdagi axborot manipulyatsiyasi	Soxta yangiliklar, propaganda
	Tabiiy tahdidlar	Tabiiy ofatlar yoki avariyalar	Yong‘in, suv toshqini, zilzila

Statistik ma’lumotlarga ko‘ra, O‘zbekistonda ro‘yxatga olingan kiberjinoyatlarning 60 foizi insonga bog‘liq xatolar natijasida sodir bo‘ladi. Bu esa kadrlar tayyorgarligi va axborot madaniyatining pastligi bilan bog‘liq. Raqamli iqtisodiyot sharoitida axborot xavfsizligi bilan bog‘liq muammolar quyidagi yo‘nalishlarda kuzatiladi:

1. Texnik muammolar – himoya tizimlarining eskirganligi, zaxira mexanizmlarining yetarli emasligi;

2. Tashkiliy muammolar – xavfsizlik siyosati yo‘qligi, mas’ul xodimlar tayinlanmaganligi;

3. Huquqiy muammolar – qonunlardagi bo‘shliqlar, nazorat mexanizmlarining sustligi;

4. Ijtimoiy muammolar – foydalanuvchilarning befarqligi va ongsiz harakatlari.

Bunday muammolar natijasida quyidagi salbiy oqibatlar yuzaga keladi: moliyaviy yo‘qotishlar; mijozlar ishonchini yo‘qotish; davlat sirlarining oshkor bo‘lishi; tarmoq tizimlarining ishdan chiqishi.

3-jadval. Axborot xavfsizligi muammolari va ularning oqibatlari

№	Muammo turi	Oqibat	Tavsiya etiladigan choralar
5.	Texnik nosozlik	Ma’lumot yo‘qolishi	Zaxira tizimlarini joriy etish
6.	Inson xatosi	Maxfiylik buzilishi	Xodimlarni o‘qitish
7.	Kiberhujum	Tizim falajligi	Antivirus va firewall
8.	Qonuniy bo‘shliqlar	Javobgarlik yo‘qligi	Huquqiy me’yorlarni kuchaytirish

9.	Axborot madaniyati pastligi	Foydalanuvchi xatolari	Axborot savodxonligini oshirish

O‘zbekiston Respublikasi so‘nggi yillarda axborot xavfsizligi sohasiga alohida e’tibor qaratmoqda. 2018-yil 3-iyuldagi PQ–3832-sonli Prezident qarori bilan kiberxavfsizlikni ta’minlash tizimini yanada takomillashtirish chora-tadbirlari belgilandi. Ushbu qarorga muvofiq: kiberxavfsizlik markazi (CERT.uz) faoliyati kengaytirildi; davlat idoralarida axborot xavfsizligi bo‘yicha mas’ul xodimlar tayinlandi; davlat axborot resurslarini himoya qilish bo‘yicha yagona tizim yaratildi.

Bundan tashqari, “Axborotlashtirish to‘g‘risida”gi Qonun (2003-yil), “Elektron hukumat to‘g‘risida”gi Qonun (2015-yil), “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonun (2019-yil) kabi hujjatlar ham axborot xavfsizligini tartibga soluvchi asosiy me’yoriy hujjatlar hisoblanadi. Dunyo miqyosida kiberxavfsizlikni ta’minlash uchun quyidagi xalqaro standartlar va yondashuvlar qo‘llaniladi: ISO/IEC 27001 – axborot xavfsizligini boshqarish tizimlari standarti; NIST Cybersecurity Framework (AQSh) – xavfsizlik risklarini baholash tizimi; GDPR (Yevropa Ittifoqi) – shaxsiy ma’lumotlarni himoya qilish qonuni; CIS Controls – amaliy xavfsizlik choralarini aniqlovchi ko‘rsatmalar majmuasi. Mazkur tajribalarning o‘zbek tizimiga moslashtirilgan shaklini joriy etish milliy axborot xavfsizligini mustahkamlashga xizmat qiladi. Axborot xavfsizligi bugungi raqamli davrning eng muhim strategik masalalaridan biridir. U nafaqat texnik, balki ijtimoiy, huquqiy va tashkiliy muammolarni ham o‘z ichiga oladi. O‘zbekiston Respublikasida bu yo‘nalishda muayyan qonuniy va institutsional asoslar yaratilgan bo‘lsa-da, hali ham kadrlar tayyorlash, axborot madaniyatini oshirish va texnik tizimlarni modernizatsiya qilish zarur.

Axborot xavfsizligini ta’minlashda texnik vositalar eng asosiy o‘rinni egallaydi. Zamonaviy kiberhujumlar ko‘plab davlatlar, banklar, ta’lim muassasalari va biznes subyektlariga katta zarar yetkazmoqda. Shu bois har bir tashkilot o‘z axborot tizimini texnik jihatdan himoya qilishning kompleks mexanizmlarini joriy etishi lozim. Asosiy texnik himoya vositalariga quyidagilar kiradi: antivirus dasturlari – zararli kodlarni aniqlaydi va yo‘q qiladi; firewall (tarmoq devorlari) – ruxsatsiz

tarmoq kirishlarini to‘sadi; shifrlash tizimlari – ma’lumotlarni maxfiy ko‘rinishga o‘tkazadi; IDS/IPS tizimlari (Intrusion Detection/Prevention Systems) – hujumlarni aniqlaydi va oldini oladi; zaxira tizimlari (Backup systems) – axborot yo‘qolgan holatda tiklash imkonini beradi.

4-jadval. Axborot xavfsizligini ta’minlashda qo‘llaniladigan texnik vositalar

№	Vosita turi	Asosiy vazifasi	Amaliy qo‘llanishi
1	Antivirus dasturi	Viruslarni aniqlash va yo‘q qilish	Kaspersky, ESET, Avast
2.	Firewall	Kirish va chiqishni nazorat qilish	Cisco, Fortigate
3	IDS/IPS tizimlari	Kiberhujumlarni aniqlash va to‘sish	Snort, Suricata
4	Shifrlash algoritmlari	Ma’lumotni maxfiy shaklda saqlash	AES, RSA
5	Zaxira tizimi	Ma’lumotni tiklash	Cloud backup, RAID
6	Biometrik autentifikatsiya	Foydalanuvchini aniqlash	Yuz, barmoq izi skaneri

Bu vositalarning kompleks qo‘llanilishi tizim xavfsizligini sezilarli darajada oshiradi. Masalan, shifrlash texnologiyalari orqali yuborilayotgan ma’lumotlar uchinchi shaxslarga o‘qilmaydigan holatga keltiriladi. Biometrik autentifikatsiya esa foydalanuvchini aniq identifikatsiya qilish imkonini beradi. Texnik vositalar bilan bir qatorda, axborot xavfsizligini ta’minlashda tashkiliy boshqaruv choralari ham muhim o‘rin tutadi. Chunki texnik himoya tizimi mukammal bo‘lsa-da, inson omili sababli xavfsizlik buzilishi mumkin.

Tashkiliy choralarga quyidagilar kiradi: axborot xavfsizligi siyosatini ishlab chiqish – tashkilot ichki tartib-qoidalarini belgilaydi; xodimlarni o‘qitish va malakasini oshirish – inson xatosi ehtimolini kamaytiradi; kirish huquqlarini nazorat qilish – har bir foydalanuvchining vakolatini cheklash; audit va monitoring – tizimdagi o‘zgarishlarni doimiy kuzatish; favqulodda vaziyatlarga tayyorgarlik rejasi – hujum yoki nosozlik holatida tezkor tiklanishni ta’minlaydi.

Dunyo miqyosida axborot xavfsizligini ta'minlash uchun bir nechta xalqaro standartlar ishlab chiqilgan. Ulardan eng mashhurlari:

- ISO/IEC 27001 – axborot xavfsizligini boshqarish tizimining xalqaro standarti;
- COBIT (Control Objectives for Information and Related Technology) – axborot texnologiyalarini boshqarish uchun metodologiya;
- NIST Cybersecurity Framework (AQSh) – risklarni boshqarish va ularni kamaytirish uchun yo'riqnoma;
- GDPR (Yevropa Ittifoqi) – shaxsiy ma'lumotlarni himoya qilishga doir qonuniy tizim.

Ushbu standartlar asosida har bir tashkilot o'z ichki siyosatini ishlab chiqadi, xavflarni tahlil qiladi va xavfsizlik choralari samaradorligini doimiy baholab boradi. O'zbekiston ham bu xalqaro tajribalardan foydalanib, milliy axborot xavfsizligi menejment tizimini shakllantirmoqda. Jumladan, "Kiberxavfsizlik markazi" (CERT.uz) xalqaro tarmoqlar bilan integratsiya qilingan. O'zbekiston Respublikasi Prezidentining 2018-yil 3-iyuldagi PQ–3832-son qarori va 2022-yil 15-fevraldagi PQ–112-son farmoni asosida quyidagi natijalarga erishildi:

- ✓ Kiberxavfsizlik markazi (CERT.uz) faoliyat doirasi kengaytirildi;
- ✓ Davlat idoralarida axborot xavfsizligi xizmati joriy etildi;
- ✓ Shaxsiy ma'lumotlar himoyasi agentligi tashkil etildi;
- ✓ Davlat axborot tizimlarini sertifikatlash tartibi yo'lga qo'yildi.

So'nggi yillarda kiberxavfsizlikni ta'minlashda sun'iy intellekt (AI), blokcheyn texnologiyasi va bulutli xizmatlardan foydalanish kengaymoqda.

- Sun'iy intellekt hujumlarni real vaqt rejimida tahlil qiladi va avtomatik javob choralarini ishlab chiqadi.

- Blokcheyn texnologiyasi ma'lumotlarning o'zgarmasligini va ishonchliligini kafolatlaydi.

- Bulutli xavfsizlik tizimlari (Cloud Security) ma'lumotlarni masofaviy zaxiralash va nazorat qilish imkonini beradi.

Mazkur texnologiyalarni milliy axborot tizimlariga joriy etish O'zbekistonning raqamli suverenitetini mustahkamlashga xizmat qiladi.

Shunday qilib, axborot xavfsizligini ta'minlashda texnik vositalar, tashkiliy boshqaruv, huquqiy mexanizmlar va innovatsion texnologiyalar o'zaro uyg'un holda qo'llanilishi zarur. O'zbekiston misolida, so'nggi yillarda axborot xavfsizligi tizimi jadal rivojlanmoqda: CERT.uz faoliyati kuchaytirilmoqda, milliy kriptografiya standartlari joriy etilmoqda, va kiberxavfsizlik bo'yicha mutaxassislar tayyorlanmoqda. Shu bilan birga, foydalanuvchilarning axborot madaniyatini oshirish, xalqaro standartlarni milliy tizimga integratsiya qilish va sun'iy intellekt asosida kiberhujumlarga qarshi mexanizmlarni kuchaytirish istiqbolli yo'nalishlar hisoblanadi.

XULOSA

Xulosa qilib aytganda, axborot xavfsizligi muammolarini bartaraf etish faqat texnik vositalar bilan emas, balki tashkiliy, huquqiy va ijtimoiy mexanizmlar bilan uyg'un holda olib borilgandagina kutilgan natijani beradi. O'zbekiston Respublikasida bu yo'nalishda olib borilayotgan islohotlar, xususan "Raqamli O'zbekiston – 2030" strategiyasi doirasidagi tashabbuslar milliy axborot makonini yanada xavfsiz qilishga xizmat qilmoqda.

Foydalanilgan adabiyotlar ro'yxati

1. O'zbekiston Respublikasi Prezidenti qarori — "Raqamli O'zbekiston – 2030" strategiyasini tasdiqlash to'g'risida.
2. O'zbekiston Respublikasi "Axborot xavfsizligi to'g'risida"gi Qonuni, 2020-yil.
3. Axborot xavfsizligi bo'yicha o'quv qo'llanma. Toshkent: TATU nashriyoti, 2024.
4. CERT Uzbekistan – Kiberxavfsizlik bo'yicha hisobotlar (https://cert.uz).
5. ISO/IEC 27001:2024 — Information Security Management Systems (ISMS) standard.
6. Kaspersky Lab. Cybersecurity Trends 2024 Report.
7. OECD Digital Security Policy Framework, 2024.