



STUDENTS //Zamonaviy ilmiy-texnik tadqiqotlar. – 2023. T. 1. – №. 1. – C. 71-78.

8.O’rmonjonov Azizbek Muhammadjon o’g’li. (2025). INKLYUZIV TA’LIMNING MUSIQA TA’LIMDAGI O’RNI VA AHAMIYATI. *TA’LIM VA TARAQQIYOT*, 4(3), 607-613.

9.Botirova Sevara Mamurovna, Tursunov Ramziddin Abdixalil o’g’li. (2025). MA’NAVIY BARKAMOL YOSHLAR YANGI O’ZBEKISTON BUNYODKORI. *MA’NAVIY BARKAMOL YOSHLAR YANGI O’ZBEKISTON BUNYODKORI*, 1(1), 98-102.

TASHKILOTLARDA AXBOROT XAVFSIZLIGI SIYOSATINI ISHLAB CHIQISH VA JORIY ETISH TAMOYILLARI

Axmedova Aziza Alisher qizi

e-mail:azizaalisherovna21@gmail.com

Rustamov Azizjon Xasan o’g’li

e-mail:modernGUCCI13@gmail.com

Tog’aymuradov Bexruz Sherxon o’g’li

e-mail:togaymuradovbexruz@gmail.com

O’zbekiston Milliy universiteti Jizzax filiali talabalari

Annotatsiya: Ushbu tezisdagi tashkilotlarda axborot xavfsizligi siyosatini ishlab chiqish va joriy etishning nazariy hamda amaliy jihatlari yoritilgan. Shuningdek, axborot xavfsizligini boshqarish tizimini shakllantirishda amal qilinadigan asosiy tamoyillar, ularning mazmuni hamda amaliy ahamiyati tahlil qilinadi. Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida tashkilotlarning faoliyati tobora raqamli muhitga ko’chmoqda. Bu esa axborot resurslarini ishonchli himoya qilish zaruratini yanada kuchaytirmoqda. Axborot xavfsizligi bugungi kunda nafaqat texnik masala, balki boshqaruv, tashkiliy va huquqiy yondashuvlarni ham o’z ichiga olgan kompleks tizim sifatida qaraladi. Shuning uchun har bir tashkilot o’z faoliyatida axborot xavfsizligi siyosatini ishlab chiqish, tasdiqlash va amaliyotga joriy etish orqali axborot muhitining barqarorligini ta’minlashi lozim.

Kirish so’zlar: axborot xavfsizligi, siyosat, boshqaruv tizimi, xavf tahlili, standartlar, risk, axborot resurslari, xavfsizlik tamoyillari.

PRINCIPLES FOR DEVELOPING AND IMPLEMENTING INFORMATION SECURITY POLICIES IN ORGANIZATIONS

Annotation: This thesis highlights the theoretical and practical aspects of developing and implementing information security policies in organizations. The study analyzes the main principles applied in the formation of an information security management system, their content, and practical significance. As a result of the rapid development of modern information and communication technologies, the activities of organizations are increasingly moving into a digital environment, which strengthens the need for reliable protection of information resources. Today, information security is considered not only a technical issue but also a complex system that includes managerial, organizational, and legal approaches. Therefore, every organization must develop, approve, and implement its own information security policy to ensure the stability of the information environment.

Keywords: information security, policy, management system, risk analysis, standards, risk, information resources, security principles.

ПРИНЦИПЫ РАЗРАБОТКИ И РЕАЛИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ

Аннотация: В данном тезисе освещены теоретические и практические аспекты разработки и внедрения политики информационной безопасности в организациях. В исследовании проанализированы основные принципы, применяемые при формировании системы управления информационной безопасностью, их содержание и практическое значение. В результате стремительного развития современных информационно-коммуникационных технологий деятельность организаций всё больше переходит в цифровую среду, что усиливает необходимость надёжной защиты информационных ресурсов. Информационная безопасность в настоящее время



рассматривается не только как техническая задача, но и как комплексная система, включающая управленческие, организационные и правовые подходы. Поэтому каждая организация должна разрабатывать, утверждать и внедрять собственную политику информационной безопасности, обеспечивая устойчивость информационной среды.

Ключевые слова: информационная безопасность, политика, система управления, анализ рисков, стандарты, риск, информационные ресурсы, принципы безопасности.

So’nggi yillarda dunyoda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi, raqamli iqtisodiyotning keng miqyosda shakllanishi natijasida axborot har qanday tashkilotning eng muhim strategic resursiga aylandi. Bunday sharoitda axborotning xavfsizligini ta’minlash masalasi nafaqat texnik, balki boshqaruv, tashkiliy va huquqiy yo’nalishlarda ham dolzarb ahamiyat kasb etmoqda. Axborot xavfsizligining samarali ta’minlashning eng muhim bosqichlaridan biri bu axborot xavfsizligi siyosatini ishlab chiqish va uni joriy etishdir. Ushbu siyosat tashkilotning axborotni himoya qilishga oid umumiy maqsadlari, prinsiplari, usullari, va ma’suliyat chegaralarini belgilab beradi. U xodimlarning axborot bilan ishlash qoidalarini tartibga soladi, xavfsizlik bo’yicha aniq me’zonlarni belgilaydi hamda ichki boshqaruv tizimini mustahkamlaydi.

O’zbekiston Respublikasida ham axborot xavfsizligini ta’minlash davlat siyosatining ustuvor yo’nalishlaridan biri hisoblanadi. “Axborotlashtirish to’g’risida”gi Qonun, “Elektron hukumat to’g’risida”gi Qonun, shuningdek, O’zbekiston Respublikasi Prezidenti va hukumatning axborot xavfsizligiga oid qaror va farmonlari ushbu sohada huquqiy asos bo’lib xizmat qilmoqda. Shu bilan birga, xalqaro miqyosda qabul qilingan ISO/IEC 27001 standarti tashkilotlarida axborot xavfsizligini boshqarish tizimini joriy etish uchun metodik asos vazifasini bajaradi.

ISO/IEC 27001 — bu axborot xavfsizligini boshqarish tizimi uchun xalqaro standart bo’lib, u tashkilotlarda axborot resurslarini himoya qilish, xavf-xatarlarni aniqlash va ularni boshqarish uchun yagona tizimli yondashuvni belgilaydi. Mazkur standart axborotning maxfiyligi, yaxlitligi va mavjudligini ta’minlashga qaratilgan talab va jarayonlarni o’z ichiga oladi.

Ushbu mavzuning dolzarbligi shundan iboratki, ko’plab tashkilotlarda axborot xavfsizligi siyosati hali to’liq shakllanmagan yoki amaliyotda yetarli darajada qo’llanilmayapti. Natijada, axborot tizimlarida zaifliklar paydo bo’ladi, bu esa iqtisodiy yo’qotishlar, ma’lumotlarning sizib chiqishi yoki xizmat ko’rsatishda uzilishlar bilan yakunlanadi. Shu sababli, axborot xavfsizligi siyosatini to’g’ri ishlab chiqish, uni xalqaro standartlarga muvofiq tarzda joriy etish va uzluksiz takomillashtirib borish bugungi kunning dolzarb masalalaridan biridir.

Axborot xavfsizligi siyosatini yaratish odatda quyidagi bosqichlarda amalga oshiriladi:

- mavjud axborot resurslarini tahlil qilish va tasniflash;
- xavf-xatar va zaifliklarni aniqlash (risk tahlili);
- xavfsizlik maqsadlarini belgilash;
- siyosat matnini ishlab chiqish va rahbariyat tomonidan tasdiqlash;
- siyosatni amaliyotga joriy etish hamda nazorat mexanizmini yo’lga qo’yish.

Bu jarayon ISO/IEC 27001 va 27002 standartlari asosida tashkil etilishi maqsadga muvofiq bo’lib, bu xalqaro talablarga muvofiq axborot xavfsizligini boshqarish tizimini yaratishga imkon beradi.

Axborot xavfsizligi siyosatini ishlab chiqishda quyidagi asosiy tamoyillarga amal qilinadi:

- Tizimlilik va komplekslik tamoyili.
Xavfsizlik siyosati tashkilotning barcha bo’limlari, jarayonlari va texnik tizimlari bilan bog’liq holda ishlab chiqiladi. Har bir sohada xavfsizlik choralarining uzviyligi ta’minlanadi.
- Risklarni boshqarish tamoyili.
Axborotni himoya qilish choralari aniqlangan tahdid va xavf darajasiga mutanosib tarzda belgilanishi kerak. Bu yondashuv resurslardan oqilona foydalanish imkonini beradi.
- Uzluksiz takomillashtirish tamoyili.
Axborot xavfsizligi siyosati bir martalik hujjat emas, balki doimiy ravishda yangilanib borilishi lozim bo’lgan tizimdir. Texnologik yangiliklar, yangi tahdidlar va qonunchilikdagi o’zgarishlar hisobga olinadi.
- Xodimlarning mas’uliyati va xabardorlik tamoyili.
Har bir xodim axborot xavfsizligini ta’minlashda o’z o’rnini anglab yetishi va belgilangan qoidalarga qat’iy amal qilishi kerak. Shu maqsadda muntazam o’quv-treninglar o’tkazilishi muhimdir.
- Qonunchilik va standartlarga muvofiqlik tamoyili.



Siyosat O‘zbekiston Respublikasi qonunlari, axborot himoyasiga oid me’yoriy hujjatlar hamda xalqaro standartlarga (ISO/IEC 27001, NIST, COBIT va boshqalar) asoslanishi lozim.

- Kirish huquqlarini boshqarish tamoyili.

Axborot tizimlarida kirish darajalari xodimlarning lavozimi, vakolatlari va vazifalariga qarab cheklanadi. Bu ma’lumotlarning maxfiyligi va yaxlitligini ta’minlashda muhim omil hisoblanadi.

- Mas’uliyatni taqsimlash tamoyili.

Axborot xavfsizligi bo’yicha mas’uliyat rahbariyatdan tortib, oddiy foydalanuvchigacha aniq belgilanadi. Bu javobgarlik tizimining samarali ishlashiga yordam beradi.

Siyosat amalda samarali ishlashi uchun tashkilotda axborot xavfsizligi bo’yicha mas’ul bo’lim yoki mutaxassis tayinlanadi. Ichki audit, nazorat mexanizmlari va hodisalarni tahlil qilish tizimi yo’lga qo’yiladi. Shuningdek, foydalanuvchilar uchun parol siyosati, ma’lumotlarni zaxiralash, tarmoq xavfsizligi va virusdan himoya choralarini o’z ichiga olgan qo’llanmalar ishlab chiqiladi.

Axborot xavfsizligini joriy etish jarayonida rahbariyatning qo’llab-quvvatlashi, moliyaviy resurslar ajratilishi hamda barcha xodimlarning ishtiroki muhim ahamiyat kasb etadi.

Xulosa qilib aytganda, bugungi globallashtirish va raqamli iqtisodiyot sharoitida axborot xavfsizligi siyosati har bir tashkilot faoliyatining strategik yo’nalishlaridan biri bo’lib, u axborot resurslarini himoya qilish, xavf-xatarlarni kamaytirish va biznes jarayonlarning uzluksizligini ta’minlashda hal qiluvchi ahamiyat kasb etadi.

Axborot xavfsizligi siyosati tashkilotdagi barcha xodimlar, bo’limlar va texnologik jarayonlarni yagona tizimda boshqarish imkonini beradi. Uning asosiy vazifasi - ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlash hamda axborotdan ruxsatsiz foydalanish, uni yo’qotish yoki buzilishining oldini olishdir. Bunda texnik himoya choralaridan tashqari, tashkiliy, huquqiy va psixologik omillarni ham inobatga olish zarur.

Axborot xavfsizligi siyosatini ishlab chiqish va joriy etish jarayonida quyidagi natijalarga erishish mumkin:

tashkilotda xavfsizlikka oid aniq vazifalar va mas’uliyatlar belgilanadi;
axborot resurslarining qiymati va ularni himoya qilish darajasi o’zaro muvofiqlashtiriladi;
xodimlarda axborot xavfsizligi madaniyati shakllanadi;
tashqi va ichki tahdidlarga tezkor javob berish imkoniyati yaratiladi;
axborot tizimlarining uzluksiz ishlashi va biznes jarayonlarning barqarorligi ta’minlanadi.

Axborot xavfsizligi siyosatini joriy etishda tizimlilik, risklarni boshqarish, uzluksiz takomillashtirish, mas’uliyat va xabardorlik, kirish huquqlarini boshqarish hamda qonunchilikka muvofiqlik tamoyillariga amal qilish muhimdir. Ushbu tamoyillar asosida shakllantirilgan siyosat nafaqat texnik jihatdan, balki boshqaruv va tashkiliy jihatdan ham ishonchli himoya tizimini yaratadi.

Shuningdek, siyosatni samarali amalga oshirish uchun rahbariyatning doimiy e’tibori, moliyaviy qo’llab-quvvatlash hamda barcha xodimlarning faol ishtiroki zarur. Xodimlar uchun muntazam trening va o’quv mashg’ulotlari tashkil etish, xavfsizlik hodisalarini monitoring qilish va tahlil etish, shuningdek, ichki audit tizimini yo’lga qo’yish siyosatning amalda ishlashini kafolatlaydi.

O‘zbekiston sharoitida axborot xavfsizligini ta’minlash davlat siyosatining muhim tarkibiy qismi sifatida rivojlanib bormoqda. Mavjud qonunchilik bazasi, milliy standartlar va xalqaro tajribalarni uyg’unlashtirish orqali tashkilotlarda xavfsizlik siyosatini joriy etish darajasini oshirish mumkin. Ayniqsa, ISO/IEC 27001 standarti talablariga asoslangan axborot xavfsizligini boshqarish tizimi (ISMS) tashkilotlar uchun eng samarali amaliy yechimlardan biri hisoblanadi.

Shu o’rinda ta’kidlash joizki, axborot xavfsizligi siyosati - bu bir martalik hujjat emas, balki doimiy rivojlanib boruvchi, yangi tahdidlarga moslashuvchi strategik jarayondir. Texnologiyalar o’zgarib borгани sayin, tashkilotning xavfsizlik siyosati ham yangilanib, zamonaviy talablarga javob berib borishi lozim.

Yakuniy natija sifatida, puxta ishlab chiqilgan, xalqaro standartlarga asoslangan va muntazam ravishda takomillashtirib boriladigan axborot xavfsizligi siyosati tashkilotning raqamli muhitdagi barqaror rivojlanishini ta’minlaydi, uning obro’si va mijozlar ishonchini mustahkamlaydi hamda raqobatbardoshligini oshiradi.

Xulosa o’rnida shuni aytish mumkinki, axborot xavfsizligi siyosati har bir tashkilot faoliyatining ajralmas qismi bo’lib, u ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashda muhim o’rin tutadi. Bunday siyosatni ishlab chiqish va muntazam takomillashtirib borish orqali tashkilotlar texnologik yangiliklar va yangi tahdidlarga tezkor javob berish imkoniyatiga ega bo’ladi. Shuningdek, xodimlarning mas’uliyati, rahbariyatning qo’llab-quvvatlashi hamda xalqaro standartlarga asoslanish axborot



xavfsizligini ishonchli darajada ta’minlashga xizmat qiladi. Natijada, puxta ishlab chiqilgan va uzluksiz rivojlantirib boriladigan axborot xavfsizligi siyosati tashkilotning barqaror rivojlanishini, mijozlar ishonchini va raqobatbardoshligini oshiradi.

Foydalanilgan adabiyotlar

- 1.O‘zbekiston Respublikasi Prezidenti Sh.M. Mirziyoyevning “Raqamli O‘zbekiston – 2030” strategiyasini amalga oshirish chora-tadbirlari to‘g‘risida”gi qarori. — Toshkent, 2020 yil.
- 2.O‘zbekiston Respublikasi “Axborotlashtirish to‘g‘risida”gi Qonuni. — 2003 yil 30 aprel (2022 yilgi o‘zgartirishlar bilan).
- 3.O‘zbekiston Respublikasi “Axborot xavfsizligi to‘g‘risida”gi Qonuni. — Toshkent, 2023 yil.
- 4.ISO/IEC 27001:2022 — Information Security Management Systems — Requirements. International Organization for Standardization, Geneva, 2022.
- 5.ISO/IEC 27002:2022 — Information Security, Cybersecurity and Privacy Protection — Information Security Controls. ISO, Geneva, 2022.
- 6.NIST Special Publication 800-53. — Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology, USA, 2020.
- 7.COBIT 2019 Framework: Governance and Management Objectives. ISACA, USA, 2019.
- 8.Abdulxayev S.S., Jo‘rayev I.I. Axborot xavfsizligi asoslari. — Toshkent: TATU nashriyoti, 2021.
- 9.Nurmatov B.M. Axborot xavfsizligini boshqarish tizimlari. — Toshkent: “Fan va texnologiya” nashriyoti, 2020.
- 10.Qodirov A. Axborot tizimlari va texnologiyalari xavfsizligi. — Toshkent: TATU, 2019.
- 11.Whitman, M.E., Mattord, H.J. Principles of Information Security. 7th Edition. — Cengage Learning, USA, 2022.
- 12.Peltier, T.R. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. — Auerbach Publications, 2016.
- 13.Solovyev A.A., Kovalev V.Yu. Информационная безопасность организации. — Москва: ИНФРА-М, 2019.
- 14.Krutov I.A. Информационная безопасность: теория и практика. — Москва: Бином, 2021.
- 15.O‘zbekiston Respublikasi Vazirlar Mahkamasi qarori “Davlat axborot resurslari va tizimlarining axborot xavfsizligini ta’minlash tartibi to‘g‘risida”. — Toshkent, 2021-yil 12-yanvar.
- 16.Sayyora Faxriddinova:Маманова С. Методика развития речевой компетентности у студентов профессионально-технических учебных заведений //Информатика и инженерные технологии. — 2023. – Т. 1. – №. 1. – С. 417-420.
17. Mamanova S. “Bo‘lajak o‘qituvchilar nutqini takomillashtiruvchi muhim vositalar” Zamonaviy sharoitda oliy ma’lumotli mutaxassislarni tayyorlashning innovatsion yo‘nalishlari: muammo va yechimlar respublika ilmiy-nazariy anjumani-2024-y
- 18.Ashurova S., Mamanova S. WAYS TO DEVELOP SPEAKING ACTIVITY OF VOCATIONAL SCHOOL STUDENTS //Zamonaviy ilmiy-texnik tadqiqotlar. – 2023. – Т. 1. – №. 1. – С. 71-78.
- 19.O‘rmonjonov Azizbek Muhammadjon o‘g‘li. (2025). MAKTABGACHA TA’LIM YOSHIDAGI IMKONIYATI CHEKLANGAN BOLALAR UCHUN INKLYUZIV TA’LIM SHAROITIDA MUSIQIY TA’LIMNI TASHKIL ETISH METODIKASI. *Kelajak o‘qituvchisi - Kelajak Bunyodkori*, 1(1), 470-475.
- 20.Ramziddin Tursunov. (2025). IJTIMOIIY ONG VA MA’NAVIYAT TUSHUNCHASI HAMDA UNING MAZMUN-MOHIIYATI. *Kelajak o‘qituvchisi - Kelajak Bunyodkori*, 1(2), 36-40.

AXBOROT XAVFSIZLIGINI TA’MINLASH VA UNI RIVOJLANTIRISH

O‘zbekiston Milliy universitetining Jizzax filiali talabalari

Uralov Behruz Bahodir o‘g‘li

e-mail: uralovbehruz17@gmail.com

Utamurodov Lochin Bekzod o‘g‘li

e-mail: pridefalcon2905@gmail.com

Amanova Rayxona Baxrom Qizi

e-mail: gulshoda7072@gmail.com

Normurodova Sabrina Tuymurodovna

e-mail: gulinorgulinor34@gmail.com

Mamanova Sayyora Faxriddinova