E CONF SERIES

Scientific Conference on Multidisciplinary Studies
Hosted online from Bursa, Turkey
Website: econfseries.com 11th January, 2025

JAMIYATDA AXBOROT XAVFSIZLIGINI TA'MINLASH TAMOYILLARI VA USULLARI

Muxtarov.F.M
Muhammad al-Xorazmiy nomidagi Toshkent axborot-texnologiyalari universiteti Farg‘ona filial direktori

Sattorov Nazarbek Odiljonovich
Toshkent Shahar adliya boshqarmasi axborot-texnologiyalari va kommunikatsiyalarni rivojlantirish bo‘lim bosh mutaxassisi
telefon:+998 97 367 17 77
nazarbek.sattorov@bk.ru

Annotatsiya:
Ushbu maqola jamiyatda axborot xavfsizligini ta'minlash tamoyillari va usullari haqida batafsil ma'lumot beradi. Axborot xavfsizligi, raqamli texnologiyalar va global aloqalar rivojlanishi bilan birga muhim ahamiyatga ega bo'lib, ma'lumotlar himoyasi masalalarini o'z ichiga oladi. Maqola axborot xavfsizligining asosiy tamoyillarini — maxfiylik, butunlik, mavjudlik va hisobdorlikni tushuntiradi.
Bundan tashqari, texnik, tashkiliy va jismoniy himoya usullari orqali axborot xavfsizligini ta'minlash yo'llari ko'rsatiladi. Mavzuning dolzarbligi, tahdidlar va xavf-xatarlar zamonaviy jamiyatda kun sayin oshib borishi bilan bog'liqdir. Ushbu maqola tashkilotlar va shaxsiy foydalanuvchilar uchun axborot xavfsizligini mustahkamlashda strategik yondashuvlarni ishlab chiqish zarurligini ta'kidlaydi. Jamiyat a'zolarining axborot xavfsizligi masalalarida o'zaro hamkorligi va o'qitilishi muhim ahamiyatga ega.

Kalit so‘zlar: Axborot xavfsizligi, Maxfiylik, Butunlik, Mavjudlik, Texnik himoya, Tashkiliy himoya, Raqamli tahdidlar, Hisobdorlik, Shifrlash, Xavfsizlik siyosatlari.

Axborot xavfsizligi zamonaviy jamiyatning ajralmas qismiga aylangan. Raqamli texnologiyalarning tez rivojlanishi, internetning keng tarqalishi va global aloqalarning o'sishi bilan birga, axborotning xavfsizligi hamda himoyasi masalalari muhim ahamiyat kasb etmoqda. Hozirgi kunda har qanday tashkilot va korxona,

shuningdek, shaxsiy foydalanuvchilar ham o'z ma'lumotlarini himoya qilishga majbur.

Axborot xavfsizligi faqatgina kompyuter tizimlari va internetda muammo emas; bu, shuningdek, jismoniy va tashkiliy jarayonlarni ham o'z ichiga oladi. Ma'lumotlar, jumladan shaxsiy ma'lumotlar, moliyaviy ma'lumotlar, tijorat sirlarini himoya qilish zarurati kun sayin oshib bormoqda. Xavf-xatarlar esa juda xilma-xil: zararli dasturlar, phishing hujumlari, ichki tahdidlar va boshqa ko'plab omillar axborot xavfsizligini tahdid qiladi.

O'zaro bog'liq axborot tarmog'ida, har qanday kamchilik yoki nuqson, natijada katta muammolarga olib kelishi mumkin. Misol uchun, ma'lumotlar buzilishi tashkilotlar uchun nafaqat moliyaviy yo'qotishlar, balki obro' yo'qotishga ham sabab bo'lishi mumkin. Shuning uchun, axborot xavfsizligini ta'minlash - bu faqat texnik masala emas, balki strategik qarorlar qabul qilishni ham talab etadi.

Ushbu maqolada axborot xavfsizligini ta'minlash tamoyillari va usullari, shuningdek, ularni amaliyotda qo'llashning ahamiyati haqida batafsil ma'lumot beramiz. Har bir tashkilot, shuningdek, shaxsiy foydalanuvchilar uchun axborot xavfsizligini ta'minlashda zamonaviy yondashuvlar va strategiyalarni ishlab chiqish va amalga oshirish juda muhimdir. Shuningdek, axborot xavfsizligini ta'minlash jarayonida xodimlarning roli va ularni o'qitishning ahamiyatiga ham e'tibor qaratamiz.

Jamiyatda axborot xavfsizligini ta'minlash — ma'lumotlar va axborot tizimlarini muhofaza qilish jarayonidir. Bu jarayonning maqsadi axborotning maxfiyligini, butunligini va mavjudligini saqlashdir. Axborot xavfsizligini ta'minlash uchun bir qator asosiy jihatlarni ko'rib chiqish mumkin:

Axborot xavfsizligining asosiy komponentlari:

Maxfiylik: Faqat ruxsat etilgan shaxslar axborotga kirish huquqiga ega bo'lishi kerak.

Butunlik: Axborot o'zgarmasligi va noto'g'ri ma'lumotlar kiritilmasligi kerak.

Mavjudlik: Axborot va tizimlar zarur bo'lganda foydalanuvchilar uchun mavjud bo'lishi lozim.

Axborot xavfsizligini rivojlantirish:

Yangi texnologiyalarni joriy etish: Sun'iy intellekt va mashina o‘rganish kabi

zamonaviy texnologiyalarni xavfsizlikni yaxshilashda qo‘llash.
Tarmoq va tizimlarni yangilab turish: Xavfsizlikni ta'minlash uchun dasturiy ta'minotni va tizimlarni doimiy ravishda yangilab turish.
Tashqi tahdidlar va hujumlar:
Kiberhujumlar:[1] Ma'lumotlarni o'g'irlash, zararli dasturlar, phishing hujumlari kabi kiber tahdidlar. Bunday tahdidlarga qarshi kurashish uchun zarur chora-tadbirlarni ko'rish muhim.
Tabiiy ofatlar va texnik nosozliklar: Ma'lumotlar yo'qolishi yoki shikastlanishi holatida zaxira nusxalarini yaratish.
Kadrlar va foydalanuvchi xavfsizligi: **Tayyorlov va malaka oshirish**: Xodimlarni axborot xavfsizligi bo'yicha muntazam ravishda o'qitish. Bu ularga tahdidlarni aniqlash va ularga qarshi kurashish ko'nikmalarini beradi.
Ruxsatnoma boshqaruvi: Har bir foydalanuvchiga o'z vazifasiga mos keladigan ruxsatlar berilishi. Bu foydalanuvchilarning axborotga kirishini nazorat qiladi.
Umuman olganda, jamiyatda axborot xavfsizligini ta'minlash kompleks jarayon bo'lib, har bir shaxs va tashkilotning mas'uliyati hisoblanadi. Bu masala ustida ishlash, xususan, axborot texnologiyalarining tez rivojlanishi davrida yanada dolzarblashmoqda.
Axborot xavfsizligi tamoyillari haqida qisqacha to’xtalib o’tadigan bo‘lsak, Maxfiylik (Confidentiality):[2] Axborotning faqat ruxsat berilgan shaxslar tomonidan foydalanilishini ta'minlash. Bu maqsadda ma'lumotlar shifrlash, parol bilan himoyalash kabi usullar qo'llaniladi.
Butunlik (Integrity): Axborotning o'zgartirilmasligini, buzilmasligini ta'minlash. Ma'lumotlar bazalarida integratsiya nazorati va versiyalarni boshqarish tizimlari yordamida amalga oshiriladi.

[1] https://www.wiley.com/en-us/Information+Security%3A+Principles+and+Practice%2C+3rd+Edition-p-9781119505884

[2] https://www.amazon.com/CompTIA-Security-Guide-Network-Fundamentals/dp/1337288780

Mavjudlik (Availability): Axborot va tizimlarga ruxsat berilgan foydalanuvchilar uchun doimiy ravishda kirish imkoniyatini ta'minlash. Buning uchun zaxira nusxalarini olish va xizmat ko'rsatish vaqtini rejalashtirish zarur.

Hisobdorlik (Accountability): Foydalanuvchilar va tizimlar tomonidan amalga oshirilgan harakatlarni nazorat qilish va ularni aniqlash. Bu loglarni yuritish va audit jarayonlarini qo'llash orqali amalga oshiriladi.

Shifrlash: Axborotlarni shifrlash orqali, ruxsat etilmagan shaxslar uchun ma'lumotlarni o'qish yoki o'zgartirishni qiyinlashtirish.

Parol himoyasi:[3] Tizimlarga kirishda kuchli parollar va autentifikatsiya usullarini qo'llash.

Ruxsat berish: Axborotga kirishni nazorat qilish va foydalanuvchilarga ma'lumotlarga ruxsat berish.

Axborot xavfsizligini ta'minlash usullari. Texnik himoya: **Firewall va Antivirus Dasturlari:** Tizimlarni tashqi tahdidlardan himoya qilish.

Tashkiliy Himoya: **Xavfsizlik [4]siyosatlari**: Tashkilot ichidagi xavfsizlik talablarini belgilovchi hujjatlar.

Xodimlarni O'qitish: Xodimlarni axborot xavfsizligi bo'yicha muntazam ravishda o'qitish va treninglar o'tkazish.

Tahlil va monitoring, **auditorlik**: Axborot xavfsizligi tizimlarining samaradorligini baholash.

Tahlil vositalari:[5] Hujumlar va tahdidlarni aniqlash uchun monitoring tizimlari.

Xulosa qilib aytadigan bo‘lsak mamlakatda axborot xavfsizligi tamoyillari har qanday tashkilot va shaxs uchun axborotlarni himoya qilishning asosiy poydevorini tashkil etadi. Maxfiylik, butunlik, mavjudlik va hisobdorlik — bu tamoyillar

[3] https://thesecmaster.com/learn/book/cybersecurity-essentials-1st-edition

[4] https://www.nist.gov/nist-research-library

[5] https://github.com/cisagov

axborotni samarali ravishda himoya qilish va xavf-xatarlarni boshqarishda muhim rol o'ynaydi.

Maxfiylik tamoyili axborotning faqat ruxsat etilgan shaxslar tomonidan foydalanilishini ta'minlaydi, bu esa shaxsiy ma'lumotlar va tijorat sirlarini himoya qilishda zarurdir. Butunlik, axborotning o'zgartirilmasligini va ishonchliligini ta'minlab, ma'lumotlar buzilishining oldini oladi. Mavjudlik tamoyili esa, foydalanuvchilarga doimiy ravishda ma'lumotlarga kirish imkonini berish orqali xizmatlar va tizimlarning uzluksizligini ta'minlaydi. Hisobdorlik tamoyili esa, foydalanuvchilarning harakatlarini nazorat qilish orqali tashkilotlarni axborot xavfsizligi bo'yicha mas'uliyatli va shaffof ishlashga undaydi.

Shuningdek, axborot xavfsizligini ta'minlashda tashkilotlarning ichki siyosatlari, jarayonlari va xavfsizlik me'yorlari muhim ahamiyatga ega. Ular xodimlarni o'qitish, monitoring tizimlarini joriy etish, zaxira nusxalarini olish va kiber tahdidlarga qarshi kurashish strategiyalarini o'z ichiga olishi kerak. Xavfsizlik choralari to'g'ri tashkil etilgan taqdirda, tashkilotlar va shaxslar ma'lumotlar xavfsizligini ta'minlashda samarali bo'lishi mumkin.

Kelajakda axborot xavfsizligi sohasidagi tahdidlar va xavflar yanada murakkablashishi kutilmoqda. Shuning uchun, tashkilotlar va shaxslar o'z xavfsizlik strategiyalarini doimiy ravishda yangilab borishlari, yangi texnologiyalar va metodologiyalarni qo'llab-quvvatlashlari lozim. O'zaro hamkorlik, axborot almashish va xavfsizlik madaniyatini rivojlantirish ham axborot xavfsizligini ta'minlashda muhim ahamiyatga ega.

Shu sababli, axborot xavfsizligini ta'minlash nafaqat texnik masala, balki strategik yondashuvni talab qiluvchi jarayondir. Har bir jamiyat a'zosi, tashkilot va individual foydalanuvchi o'z ma'lumotlarini himoya qilishda faol ishtirok etishi lozim, bu esa umumiy axborot xavfsizligini mustahkamlashga yordam beradi.

Foydalanilgan adabiyotlar:

1. "Information Security: Principles and Practice" - Mark Stanislav, David K. W. Edwards
2. "Security+ Guide to Network Security Fundamentals" - Mark Ciampa

3. "The Art of Deception: Controlling the Human Element of Security" - Kevin Mitnick
4. "CISSP All-in-One Exam Guide" - Shon Harris
5. "Cybersecurity Essentials" - Charles J. Brooks, Christopher Grow, Philip Craig
6. "Security+ Guide to Network Security Fundamentals" - Mark Ciampa
7. NIST (National Institute of Standards and Technology) nist.gov
8. CISSP (Certified Information Systems Security Professional) isc2.org
9. Cybersecurity & Infrastructure Security Agency (CISA) cisa.gov
10. "Security Engineering: A Guide to Building Dependable Distributed Systems" — Ross Anderson