Vol. 1 No. 3 (2024): Journal of International science networks
Journal of Contemporary World Studies: ISSN: 3030-3311
International Journal of Scientific and Applied Research

AXBOROT XAVFSIZLIGINI BOSHQARISH TIZIMLARI

Karimberganov Timur Alisher o‘g‘li

Abstract:

Ushbu maqola axborot xavfsizligini boshqarish tizimlari (ISMS) haqida bo'lib, axborot xavfsizligini ta'minlashda ISMSning ahamiyati, uning asosiy prinsiplari, joriy etish jarayoni va muvaffaqiyatli boshqarish uchun zarur bo'lgan metodologiyalarni ko'rib chiqadi. ISMS axborot xavflarini tahlil qilish, xavf va xavfsizlik siyosatini ishlab chiqish, hamda tashkilotlar uchun muhim bo'lgan xavfsizlik choralarini joriy etishga qaratilgan tizimli yondashuvni taqdim etadi. Maqolada shuningdek, ISO/IEC 27001 va boshqa xalqaro standartlarga asoslanib ISMSning muvaffaqiyatli ishlashini ta'minlashga yordam beruvchi metodlar va tajribalar muhokama qilinadi. Tashkilotlar axborot xavfsizligini boshqarishning samarali tizimlarini o'rnatish orqali o'z ma'lumotlarining xavfsizligini saqlash, yuridik talablarni bajarish va mijozlarning ishonchini oshirish imkoniyatiga ega bo'ladilar.

Keywords:

axborot xavfsizligi, axborot xavfsizligini boshqarish tizimi (ISMS), xavf tahlili, ISO/IEC 27001, xavfsizlik siyosati, xalqaro standartlar, axborot tizimlarini himoya qilish, ma'lumotlarning maxfiyligi, butunligi va mavjudligi, tashkilotlarda xavfsizlik boshqaruvi.

E-mail:

karimberganovtimurbek@gmail.com

Author information:

Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali Amaliy matematika fakulteti Axborot xavfsizligi yo‘nalishi 181-23 guruh 2-bosqich talabasi

Kirish

Axborot xavfsizligi (AX) tashkilotning eng muhim resurslaridan biri bo'lib, uning to'g'ri boshqarilishi va himoyalanishi zamonaviy raqamli dunyoda katta ahamiyatga ega. Axborot xavfsizligi tizimlari, shuningdek, tashkilotlarning muvaffaqiyatli faoliyat yuritishiga xizmat qiladi, chunki ma'lumotlar, intellektual mulk va foydalanuvchi ma'lumotlarining xavfsizligi tashkilotning obro'si, moliyaviy holati va huquqiy mas'uliyatini ta'minlashda muhim o'rin tutadi.

Axborot xavfsizligini boshqarish tizimi (ISMS) — bu axborot xavfsizligini ta'minlash va boshqarish uchun tizimli yondashuvni taqdim etuvchi tizimdir. ISMS axborot xavfsizligini boshqarishda strategik yondashuvni, siyosatlarni, jarayonlarni va amaliyotlarni o'z ichiga oladi.

2. Axborot xavfsizligini boshqarish tizimining asosiy tushunchalari

ISMSning asosiy vazifasi axborot xavfsizligini ta'minlash, unga ta'sir qiluvchi xavflarni kamaytirish va tashkilotning maqsadlariga erishishda xavfsizlikni saqlashdir. Axborot xavfsizligining asosiy prinsiplari quyidagilardan iborat:

- **Maxfiylik (Confidentiality)**: Faqat ruxsat etilgan shaxslar tomonidan axborotning foydalanilishi.
- **Butunlik (Integrity)**: Axborotning to'g'ri, o'zgartirilmagan holda saqlanishi.
- **Mavjudlik (Availability)**: Axborotning kerakli vaqtda mavjud bo'lishi va foydalanishga tayyorligi.

ISMSni joriy etish orqali tashkilotlar axborot xavflarini oldini olish, ma'lumotlar buzilishining oldini olish va zararlangan tizimlarni tiklashni o'z ichiga olgan samarali boshqaruvni ta'minlashga erishadilar.

3. ISMSning tashkilotdagi o'rni va ahamiyati

ISMS tizimi tashkilotga quyidagi afzalliklarni taqdim etadi:

- **Xavflarni boshqarish**: ISMS xavf tahlili va xavflarni baholash jarayonlarini tashkil etadi, bu orqali tashkilotlar xavflarni aniqlash va ularga qarshi samarali choralar ko'rishga qodir bo'ladi.
- **Yuridik va regulyativ talablar**: Axborot xavfsizligini boshqarish, ko'plab davlatlar va sanoat sektorlarida mavjud bo'lgan qonunlar, standartlar va regulyatsiyalarga muvofiq amalga oshiriladi.
- **Tashkilotning obro'si**: ISMS tizimi mijozlarning ishonchini oshirish va tashkilotning bozorga nisbatan ijobiy imidjini yaratish imkonini beradi.
- **Ma'lumotlar yo'qolishining oldini olish**: ISMS tizimi ma'lumotlarning tasodifiy yoki ziyonli o'zgarishi, yo'qolishi yoki qidiruvga qaram holda mavjud bo'lishini ta'minlaydi.

4. ISMSni joriy etish jarayoni

ISMSni joriy etishning asosiy bosqichlari quyidagilar:

1. **Tashkilotning mavjud xavfsizlik holatini baholash**: Tashkilotning mavjud xavfsizlik holatini baholash, ayniqsa axborot xavflarini aniqlash uchun zarur.

2. **Xavf tahlili va xavfni boshqarish rejasi**: Xavflarni tahlil qilish va ularni boshqarishning samarali metodlarini ishlab chiqish.
3. **Xavfsizlik siyosatini ishlab chiqish**: Tashkilotning umumiy xavfsizlik siyosatini ishlab chiqish va shu asosda ISMSni shakllantirish.
4. **Xavfsizlik choralari va amaliyotlarini joriy etish**: Xavfsizlik siyosatiga mos ravishda chora-tadbirlarni amalga oshirish va xavfsizlikni doimiy ravishda kuzatib borish.
5. **Tizimning samaradorligini baholash va takomillashtirish**: ISMS samaradorligini baholash va zarur hollarda yaxshilanishlarni amalga oshirish.

5. ISMSni boshqarishning asosiy standartlari

ISMSni boshqarishda ko'plab xalqaro standartlar va metodologiyalar mavjud. Ulardan eng mashhurlari:

- **ISO/IEC 27001**: Axborot xavfsizligini boshqarish tizimi uchun xalqaro standart. ISO 27001 axborot xavfsizligini boshqarish tizimining talablarini belgilaydi va uning amalga oshirilishini nazorat qilish uchun asosiy yo'riqnomalar beradi.
- **NIST SP 800-53**: Amerika Qo'shma Shtatlari milliy standartlar va texnologiyalar instituti tomonidan ishlab chiqilgan axborot xavfsizligi boshqaruvi bo'yicha yo'riqnomalar.
- **COBIT**: Axborot texnologiyalarini boshqarish uchun strategik yondashuv, ayniqsa IT va korporativ boshqaruvni integratsiyalashda foydalidir.

6. Axborot xavfsizligini boshqarish tizimlarining muammolari va yechimlari

ISMSni joriy etishda va boshqarishda yuzaga keladigan asosiy muammolar:

- **Resurslar va vaqt cheklovlari**: ISMSni joriy etish uchun zarur bo'lgan resurslar va vaqt miqdori tashkilotning o'ziga xos shart-sharoitlariga qarab farq qiladi.
- **Tashkilot ichidagi qarshiliklar**: Ishchilarning axborot xavfsizligini boshqarish tizimiga qarshi turishi, o'zgarishlarni qabul qilishdagi qiyinchiliklar.
- **Texnik va insoniy omillar**: Yangi texnologiyalarni amalga oshirishda yuzaga keladigan texnik muammolar va insoniy xatoliklar.

Yechtimlar:

- **Doimiy ta'lim va o'qitish**: Tashkilot ichidagi barcha xodimlarga axborot xavfsizligi bo'yicha doimiy ta'lim va treninglarni tashkil qilish.
- **Keng qamrovli xavfni boshqarish**: Texnik choralardan tashqari, insoniy omillarni ham inobatga olish zarur.

7. Xulosa

Axborot xavfsizligini boshqarish tizimlari (ISMS) tashkilotlar uchun juda muhim ahamiyatga ega. Ularning samarali ishlashi uchun to'g'ri joriy etish va boshqarish jarayonlari zarur. Tashkilotlar xavf tahlilini amalga oshirishi, xavfsizlik siyosatini yaratishi va yangilab turishi, shuningdek, zamonaviy xavfsizlik tahdidlariga qarshi samarali chora-tadbirlarni ishlab chiqishi lozim. ISMSni muvaffaqiyatli amalga oshirish orqali tashkilotlar nafaqat xavfsizlikni ta'minlaydi, balki o'z obro'sini ham mustahkamlaydi.

Foydalanilgan adabiyotlar:

1. ISO/IEC 27001:2013. (2013). *Information technology — Security techniques — Information security management systems — Requirements.* International Organization for Standardization.
2. Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: A Practitioner's Reference.* CRC Press.
3. Baskerville, R., & Siponen, M. (2002). "An Information Security Research Agenda." *Computers & Security, 21(7)*, 544–553.
4. Laudon, K. C., & Laudon, J. P. (2019). *Management Information Systems: Managing the Digital Firm.* Pearson Education.
5. NIST Special Publication 800-53. (2020). *Security and Privacy Controls for Information Systems and Organizations.* National Institute of Standards and Technology.
6. Whitman, M. E., & Mattord, H. J. (2019). *Principles of Information Security.* Cengage Learning.
7. Gerber, M., & Solms, R. V. (2018). "Information Security Governance." *International Journal of Information Management, 42*, 108–116.
8. Heiser, J., & Smith, B. (2021). "Risk Management and Information Security." *International Journal of Information Security and Privacy (IJISP), 15(2)*, 39–55.