

AXBOROT TIZIMLARINI HIMOYALASH VOSITALARI: NAZARIY ASOSLAR VA AMALIY QO‘LLANILISHI

AKRAMOVA MOHIGUL ZIYODULLOYEVNA

Romitan tuman 1-son politexnikumining

“Informatikav a axborot texnologiyalari ” fani o‘qituvchisi

Kirish

Zamonaviy axborot texnologiyalarining rivojlanishi va raqamli iqtisodiyotning jadal o‘shishi bilan birga, axborot xavfsizligi masalalari ham ahamiyat kasb etmoqda. Axborot tizimlarining samarali ishlashi, ularning doimiy va xavfsiz ishlashini ta‘minlash, shuningdek, ma‘lumotlarning maxfiyligini, yaxlitligini va mavjudligini himoya qilish bugungi kunning asosiy vazifalaridan biridir. Axborot tizimlarini himoyalash – bu turli xavf-xatarlar, shu jumladan, kiberhujumlar, zararli dasturlar va xodimlar tomonidan yuzaga keladigan xatarlar qarshisida axborot tizimining samarali himoyasini ta‘minlash uchun ishlatiladigan vositalar majmuasidir.

Ushbu maqolada axborot tizimlarini himoya qilishda qo‘llaniladigan vositalar, ularning turlari va zamonaviy xavf-xatarlarga qarshi kurashishda qo‘llanilishi ko‘rib chiqiladi.

1. Axborot tizimlarini himoyalash vositalarining muhimligi

Axborot tizimlarini himoyalashda ko‘plab vositalar va texnologiyalar mavjud. Ularning asosiy maqsadi, axborot tizimlarini tashqi va ichki tahdidlardan himoya qilish, shuningdek, ma‘lumotlarning yo‘qolishi yoki buzilishining oldini olishdir. Axborot tizimlarini himoya qilish, quyidagi elementlarni o‘z ichiga oladi:

- **Maxfiylikni ta‘minlash:** Axborotlarning faqat ruxsat etilgan foydalanuvchilar tomonidan o‘qilishi mumkinligini ta‘minlash.
- **Yaxlitlikni saqlash:** Axborotning o‘zgarishi yoki manipulyatsiya qilinishining oldini olish.
- **Mavjudlikni ta‘minlash:** Axborot tizimlarining doimiy ravishda ishlashini va ma‘lumotlarga kirishni ta‘minlash.
- **Avtorizatsiya va autentifikatsiya:** Foydalanuvchilarni tizimga kirish imkoniyatiga ega bo‘lganligini aniqlash va tasdiqlash.

2. Axborot Tizimlarini Himoyalash Vositalarining Turlari

Axborot tizimlarini himoya qilishda qo‘llaniladigan vositalar keng turli xil bo‘lib, ular har xil xavf-xatarlarga qarshi kurashishga mo‘ljallangan. Quyida axborot tizimlarida xavfsizlikni ta‘minlash uchun ishlatiladigan asosiy vositalar ko‘rib chiqiladi:

- **Firewall (Boshqariladigan Kirish Nazorati):** Firewall, axborot tizimining ichki va tashqi tarmoqlari o‘rtasida kirish-chiqishni nazorat qiluvchi tizimdir. U internetdan kiradigan ma‘lumotlar oqimlarini filtrlaydi va xavfli yoki noqonuniy so‘rovlarni bloklaydi. Firewall tizimi har qanday tarmoqqa kirishga urinishlarni aniqlaydi va to‘g‘ri himoya choralarini ko‘radi.

- **Antivirus dasturlari:** Antivirus dasturlari zararli dasturlarni (viruslar, trojanlar, spyware va boshqalar) aniqlash va yo'q qilish uchun ishlatiladi. Ular tizimdagi potentsial xavfli fayllarni tahlil qilib, ma'lumotlarning infeksiyasini oldini olishadi.
- **Shifrlash:** Axborotlarni shifrlash, ma'lumotlarni noaniq holatga keltirish orqali ularni faqat maxsus kalitlar yordamida o'qish imkonini beradi. Shifrlash axborotni tashqi tahdidlardan himoya qiladi, chunki hatto ma'lumotlar o'g'irlangan taqdirda ham ularni foydalanuvchi tashqarisida hech kim o'qiy olmaydi. AES va RSA kabi zamonaviy shifrlash algoritmlari keng qo'llaniladi.
- **Vazifalar bo'yicha cheklash (Access Control):** Tizimga kirish huquqini boshqarish maqsadida, foydalanuvchilarning ruxsat etilgan resurslarga kirishini nazorat qilish. Ruxsatnoma darajalarini belgilash orqali foydalanuvchilarga faqat zarur bo'lgan ma'lumotlarni ko'rish yoki tahrirlash imkoniyatini berish mumkin.
- **Intrusion Detection and Prevention Systems (IDPS):** Bu tizimlar axborot tizimlarida kirish yoki harakatlar anomal holatlarni aniqlaydi va ularning oldini olishga yordam beradi. IDPS tizimlari tarmoqqa kiradigan zararli hujumlarni kuzatib boradi va ular yuzaga kelganda real vaqt rejimida ogohlantirish beradi.
- **Virtual Xususiy Tarmoq (VPN):** VPN, internet orqali xavfsiz ulanishni ta'minlaydigan tarmoq texnologiyasidir. VPN orqali foydalanuvchi ma'lumotlarni shifrlash orqali internetga kiradi va bu orqali xavfsizlikni oshiradi. VPN tizimi, ayniqsa, masofaviy ishlash va xususiy tarmoqlarga ulanishda juda muhim ahamiyatga ega.
- **Raqamli imzolar:** Raqamli imzolar axborotning haqiqiylikini va yaxlitligini tasdiqlashda qo'llaniladi. Ular asosan asimmetrik kriptografiya asosida ishlaydi, foydalanuvchining maxfiy kaliti yordamida hujjatga imzo qo'yiladi va undan keyin ochiq kalit yordamida tasdiqlanadi.

3. Zamonaviy Xavf-Xatarlar va Ularning Qarshi Kurashish Usullari

Axborot tizimlari va tarmoqlariga tahdidlar doimiy ravishda rivojlanib bormoqda. Shu bois, axborot tizimlarini himoya qilishda yangi yondashuvlar va vositalar ishlab chiqilmoqda. Zamonaviy xavf-xatarlar quyidagilarni o'z ichiga oladi:

- **DDoS (Distributed Denial of Service) hujumlari:** Bu turdagi hujumlar tarmoq serverlariga katta hajmdagi so'rovlarni yuborib, tizimning faoliyatini buzishga qaratilgan. DDoS hujumlariga qarshi kurashish uchun tarmoqni tahlil qilish va kirishlarni filtrlash tizimlari, masalan, IDS/IPS tizimlari va trafikni cheklash vositalari qo'llaniladi.
- **Phishing hujumlari:** Phishing, foydalanuvchilarni yolg'on ma'lumotlar bilan aldash va ularning shaxsiy ma'lumotlarini o'g'irlashga qaratilgan hujumdur. Bunday hujumlarga qarshi foydalanuvchilarni xabardor qilish va email xavfsizligini ta'minlash kerak.
- **Zararli dasturlar va rootkitlar:** Zararli dasturlar tizimga kirish uchun ko'plab usullardan foydalanadi. Antivirus dasturlari va tizim monitoringi zararli dasturlarni tezda aniqlash va olib tashlash uchun muhim vositalardir.
- **Ichki tahdidlarga qarshi kurashish:** Tizim xodimlarining noto'g'ri xatti-harakatlari yoki tasodifiy xatolar axborot tizimlariga zarar yetkazishi mumkin. Bu xatarlarni kamaytirish uchun foydalanuvchilarni o'qitish, tizimdagi ma'lumotlarga kirishni cheklash va audit tizimlarini ishlatish muhim.

4. Xulosa

Axborot tizimlarini himoyalash vositalari – bu axborotlarning xavfsizligini ta'minlashda zarur bo'lgan vositalar majmuasidir. Tarmoq xavfsizligi, antivirus dasturlari, shifrlash, kirish nazorati va raqamli imzolar kabi vositalar, zamonaviy axborot tizimlarini himoya qilishda muhim rol o'ynaydi. Shu bilan birga, xavf-xatarlar va tahdidlarga qarshi kurashish uchun tizimli yondashuvni qo'llash zarur. Axborot tizimlarining doimiy va xavfsiz ishlashi, butun tashkilotning samarali faoliyat ko'rsatishini ta'minlash uchun nihoyatda muhimdir.

FOYDALANILGAN ADABIYOTLAR

1. Муродов, О. Т. (2023). РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕМПЕРАТУРЫ И ВЛАЖНОСТИ В ПРОИЗВОДСТВЕННЫХ КОМНАТ. *GOLDEN BRAIN*, 1(26), 91-95.
2. Murodov, O. T. R. (2023). INFORMATIKA DARSLARINI TASHKIL ETISHDA INNOVATSION USULLARDAN FOYDALANISH. *GOLDEN BRAIN*, 1(32), 194-201.
3. Murodov, O. T. R. (2023). Zamonaviy ta'limda axborot texnologiyalari va ularni qo'llash usul va vositalari. *Educational Research in Universal Sciences*, 2(11), 481-486.
4. Murodov, O. T. R. (2023). INFORMATIKA FANINI O'QITISHDA YANGI INNOVATSION USULLARDAN FOYDALANISH METODIKASI. *GOLDEN BRAIN*, 1(34), 130-139
5. Torakulovich, M. O. (2024). Innovative information technologies and new methods and tools for their application in today's education. *Central Asian Journal Of Education and Innovation*, 3(2-2), 83-92.
6. Muradov, O. (2024). Basic principles and rules of innovative pedagogical technologies in the educational process. *Models and methods in modern science*, 3(1), 84-93.
7. Turakulovich, M. O. (2024). DEVELOPMENT AND INSTALLATION OF AN AUTOMATIC TEMPERATURE CONTROL SYSTEM IN ROOMS. *Methods of applying innovative and digital technologies in the educational system*, 1(2), 72-77.
8. Muradov, O. (2024, January). Application of basic principles and rules of innovative pedagogical technologies to educational processes. In *Международная конференция академических наук* (Vol. 3, No. 1, pp. 46-55).
9. Murodov, O. (2024). DEVELOPMENT OF AN AUTOMATED PARAMETER CONTROL SYSTEM ROOMS AND WORKSHOPS BASED ON CLOUD TECHNOLOGIES. *Академические исследования в современной науке*, 3(2), 16-27.
10. Muradov, O. (2024). APPLIED TO THE CURRENT TRAINING PROCESS REQUIREMENTS. *Инновационные исследования в науке*, 3(1), 54-63.
11. Murodov, O. (2024). DEVELOPMENT AND INSTALLATION OF AN AUTOMATIC TEMPERATURE CONTROL SYSTEM IN ROOMS. *Solution of social problems in management and economy*, 3(2), 91-94.
12. To'raqulovich, M. O. (2024). IMPROVING THE TEACHING PROCESS OF IT AND INFORMATION TECHNOLOGIES BASED ON AN INNOVATIVE APPROACH. *Multidisciplinary Journal of Science and Technology*, 4(3), 851-859.
13. Murodov, O. (2023). INNOVATSION YONDASHUV ASOSIDA INFORMATIKA VA AXBOROT TEXNOLOGIYALARI FANINI O'QITISH JARAYONINI TAKOMILLASHTIRISH. *Theoretical aspects in the formation of pedagogical sciences*, 3(4), 77-81.
14. Murodov, O. (2024). TA'LIM TEXNOLOGIYALARINING ILMIY-NAZARIY ASOSLARI. *Science and innovation in the education system*, 3(3), 155-160.

15. Murodov, O. (2024). DEVELOPMENT OF AN AUTOMATED SYSTEM FOR CONTROLLING TEMPERATURE AND HUMIDITY IN PRODUCTION ROOMS. *Development and innovations in science*, 3(1), 84-93.
16. To'raqulovich, M. O. (2024). OLIY TA'LIM MUASSASALARIDA TA'LIMNING INNOVASION TEXNOLOGIYALARDAN FOYDALANISH. *PEDAGOG*, 7(5), 627-635.
17. . Muradov, O. (2024, January). IN TEACHING INFORMATICS AND INFORMATION TECHNOLOGIES REQUIREMENTS. In *Международная конференция академических наук* (Vol. 3, No. 1, pp. 97-102).
18. To'raqulovich, M. O. (2024). OLIY TA'LIM MUASSASALARIDA AXBOROT KOMMUNIKASIYA TEXNOLOGIYALARI DARSLARINI TASHKIL ETISHDA ZAMONAVIY USULLARDAN FOYDALANISH. *PEDAGOG*, 7(6), 63-74.