DOI: https://doi.org/10.5281/zenodo.11094980

AXBOROT XAVFSIZLIGI TALABLARI BO‘YICHA AXBOROTLASHTIRISH OBYEKTLARINI ATTESTATSIYASI

Ramazonova M.Sh., Narzullayev M.E., Shobo‘tayev J.B., Madatov I.Sh.,
Toshkent axborot texnologiyalari unversiteti
abdujabbor.madina.1989@gmail.com

Annotatsiya: *Ushbu maqolada axboroni himoya qilish vositalari va ushbu vositalarni attestatsiyadan o‘tkazish jarayonlari o‘rganilgan va axborot xavfsizligi talablari ko‘rib chiqilgan holatda talablar bo‘yicha axborotlashtirish abyektlarini attestatsiyasi o‘rganilgan.*

Kalit so‘zlar: *Axborotlashtirish ob’yekti attestatsiyasi, attestatsiyalash, muvofiqlik talablari, kadrlar tayyorlash, kadrlash tayyorlash darajasi.*

Axborotlashtirish obektlari attestatsiyasi

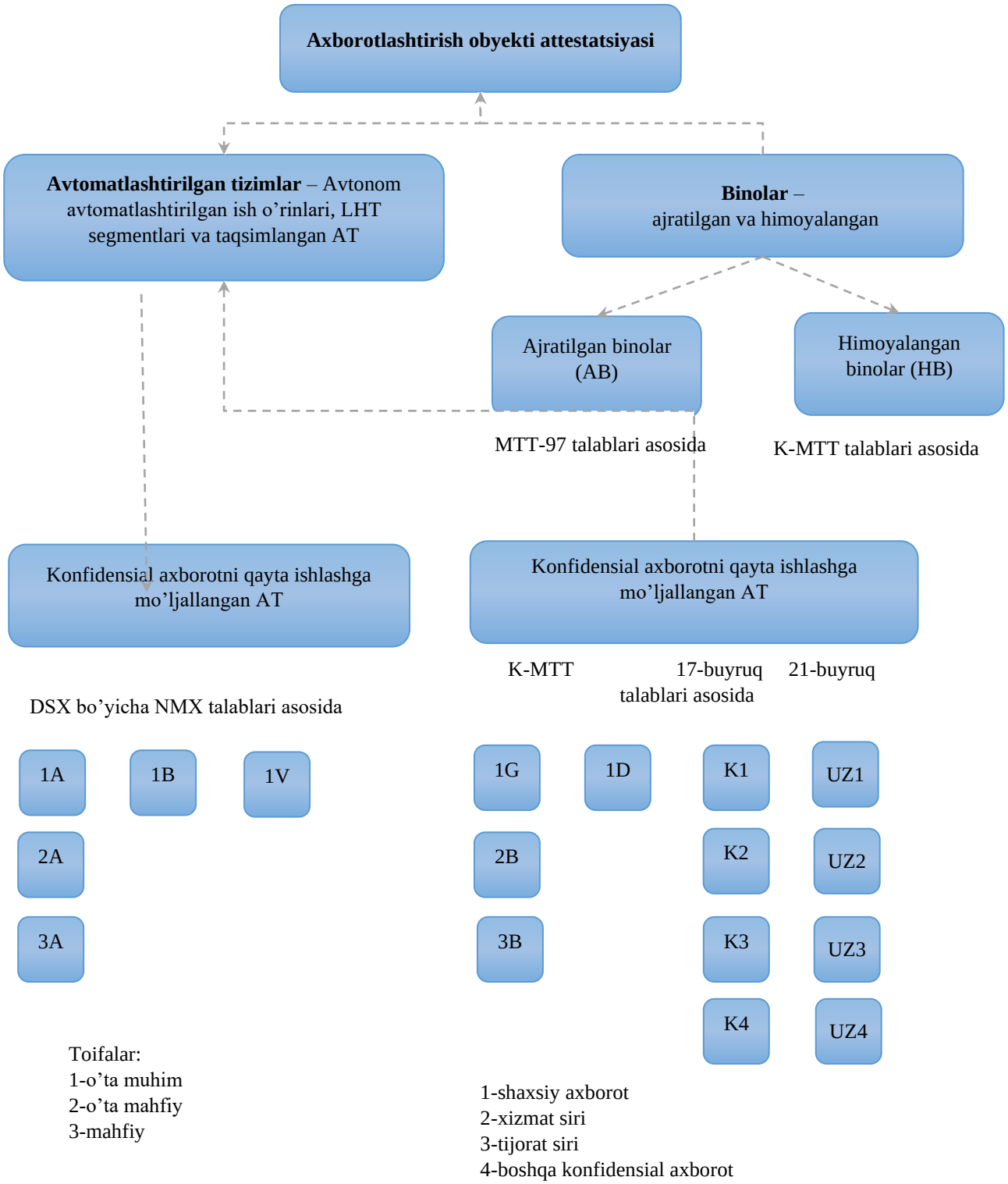
Axborotlashtirish ob’yekti (AO) attestatsiyasi - bu ob’yektning axborot xavfsizligi sohasidagi nazorat qiluvchi organlarning normativ hujjatlari talablariga muvofiqligini tasdiqlash uchun mo‘ljallangan axborot xavfsizligi vositalarini joriy etish bo‘yicha ishlarning yakuniy bosqichi hisoblanadi. Attestatsiyalash axborot xavfsizligining haqiqiy darajasini, axborot xavfsizligi vositalarini joriy etish bo‘yicha tugallangan loyihaning muvaffaqiyatini, shuningdek, axborot xavfsizligi standartlariga muvofiqligini tekshirish va tasdiqlash imkonini beradi. 15-20% hollarda ushbu bosqichda nomaqbul va xavfli oqibatlarga olib kelishi mumkin bo‘lgan nuqsonlarni aniqlash va tuzatish mumkin.

Attestatsiyalash ixtiyoriy yoki majburiy bo‘lishi mumkin. ***Ixtiyoriy*** - axborot egasining tashabbusi bilan amalga oshiriladi va funktsional ko‘rsatkichlarni tasdiqlash yoki mustaqil ekspert baholash zarur bo‘lgan hollarda uning ma’lum standartlar va axborot xavfsizligi talablariga muvofiqligini tasdiqlash uchun xizmat qiladi.

Majburiy - O‘zbekiston Respublikasi qonunchiligida va vakolatli nazorat qiluvchi organlarning normativ-huquqiy hujjatlarida belgilangan hollarda AO uchun amalga oshiriladi. Shunday qilib, davlat sirlarini ifodalovchi ma’lumotlarni qayta ishlash uchun mo‘ljallangan AO, davlat va shahar AT va boshqalar majburiy sertifikatlanishi kerak. Shuningdek, faoliyatning ayrim turlari uchun litsenziyalar olishga tayyorgarlik ko‘rishda attestatsiyalash majburiydir.

Chora-tadbirlar himoyalangan uskunani haqiqiy ish sharoitida kompleks tekshirishni nazarda tutadi, uning davomida barcha zarur ish turlari bajariladi. Attestatsiyalash talablarga muvofiqligi nazorat qilinadigan ob’yektlarning butun doirasini qamrab oladi (1-rasm):

- axborot tizimlari;
- avtomatlashtirish uskunalari bilan jihozlangan ish joylari;
- ma’lumotlar tarmoqlari;
- binolar.



1-rasm. Muvofiqlik talablariga mosligi tekshiriladigan obyektlar doirasi

AO quyidagilarga muvofiqligi bo‘yicha attestatsiyadan o‘tadi:

- shaxsiy ma’lumotlarni himoya qilishga qo‘yiladigan talablar;
- davlat axborot tizimlarini himoya qilishga qo‘yiladigan talablar;
- maxfiy axborotni himoya qilishga qo‘yiladigan talablar;
- davlat sirlarini tashkil etuvchi ma’lumotlarni qayta ishlaydigan axborot tizimlariga qo‘yiladigan talablar;
- attestatsiyalash, toifalash va tasniflash kerak bo‘lgan AOlari ro‘yxatini aniqlash.

Axborotni himoyalash vositalari obyekti quyidagi tartibda attestatsiyadan o‘tadi:

1. AOda axborotni muhofaza qilish bo‘yicha dastlabki ma’lumotlar va hujjatlarni tahlil qilish va baholash, turkumlashtirishning to‘g‘riligini baholash;

2. Taqdim etilgan dastlabki ma’lumotlarning AOni joylashtirish va ishlatishning haqiqiy shartlariga muvofiqligini tekshirish;

3. Attestatsiyalash sinovlari uchun tayyorlangan AO uchun hujjatlarni (jumladan, AO pasportlari va tashkiliy-ma’muriy hujjatlarni) ishlab chiqish;

4. Axborotni saqlash va qayta ishlashning texnologik jarayonini tekshirish, axborot chiqib ketishining mumkin bo‘lgan kanallarini aniqlash va ularni bartaraf etish bo‘yicha chora-tadbirlar ro‘yxatini ishlab chiqish;

5. AO o‘rnatilgan binolarning talablarga muvofiqligini baholash, shu jumladan, agar kerak bo‘lsa, o‘rnatilgan axborotni ushlab turish qurilmalari mavjudligini maxsus tekshirish;

6. Kadrlar tayyorlash darajasini baholash;

7. Zarur bo‘lganda, axborotni himoya qilish bo‘yicha chora-tadbirlarni amalga oshirish (axborotni himoya qilish vositalarini yetkazib berish, o‘rnatish va sozlash);

8. Attestatsiya sinovlarini o‘tkazish dasturi va metodikasini tayyorlash va tasdiqlash;

9. Attestatsiya testlarini o‘tkazish, shu jumladan individual apparat va dasturiy ta’minot, muhandislik, IT uskunalari va boshqalar;

10. Axborot ob’yektlarining axborotni ruxsatsiz kirish va texnik kanallar orqali sizib chiqishidan himoya qilish talablariga muvofiqligini tekshirish;

11. Hisobot hujjatlarini tayyorlash (sinov hisobotlari, attestatsiya sinovlari natijalari bo‘yicha xulosalar);

12. Ijobiy hulosaga kelinganda “Muvofiqlik attestati”ni berish;

13. Attestatsiyalash natijalarini tahlil qilish, axborotni texnik kanallar orqali sizib chiqishidan himoya qilish bo‘yicha ko‘rilayotgan chora-tadbirlarni takomillashtirish bo‘yicha tavsiyalar ishlab chiqish, aniqlangan axborot chiqib ketish kanallarini yopish.

Attestatsiya sinovlari axborotlashtirish obyektining axborot xavfsizligi bo‘yicha muvofiqligini qisqacha baholash, yo‘ l qo ‘yilgan qoidabuzarliklarni bartaraf etish bo‘ yicha aniq tavsiyalar ishlab chiqish, axborotlashtirish obyektini himoya qilish tizimini belgilangan talablarga muvofiqlashtirish, ushbu tizimni takomillashtirish, axborotlashtirish obyektining ishlashini nazorat qilish bo‘ yicha tavsiyalar ishlab chiqish, shuningdek "Muvofiqlik attestatini" berish imkoniyati to‘g‘risidagi xulosa bilan bilan yakunlanadi.

Xulosaga sinovlar davomida olingan natijalarni tasdiqlovchi va Xulosada berilgan xulosani asoslovchi test hisobotlari ilova qilinadi.

Attestatsiya natijalari bo‘yicha ijobiy xulosa chiqarilgan taqdirda, axborotlashtirish ob’yektining axborot xavfsizligi talablariga muvofiqligi to‘g‘risidagi guvohnoma beriladi.

Muvofiqlik attestatining amal qilish muddati 3 yilni tashkil etadi, shu vaqt ichida attestatsiyalangan axborotlashtirish ob’yekti egasi axborotlashtirish ob’yekti faoliyatining belgilangan shartlarini, himoyalangan ma’lumotlarni qayta ishlash texnologiyasini va axborot xavfsizligi talablarini bajarish uchun javobgardir.

Kadrlar tayyorlash

Inson resurslarini boshqarish yangi xodimni ishga olishdan boshlanadi va undan oldinroq – lavozimni ta’riflash bilan boshlanadi. Ushbu bosqichda, lavozim bilan bog‘liq kompyuter imtiyozlarini aniqlash bo‘yicha ishda axborot xavfsizligi bo‘yicha mutaxassisni jalb qilish tavsiya etiladi.

Odamlarni boshqarishda ikkita umumiy tamoyilni yodda tutish kerak:

- *Vazifalarni taqsimlash tamoyili* rollar va mas’uliyatni shunday taqsimlashni talab qiladiki, bir kishi tashkilot uchun muhim bo‘lgan jarayonni buzolmasin.
- *Imtiyozlarni minimallashtirish tamoyili* foydalanuvchilarga faqat xizmat vazifalarini bajarish uchun zarur bo‘lgan kirish huquqlarini ajratishni buyuradi. Ushbu tamoyilning maqsadi aniq – tasodifiy yoki qasddan noto‘g‘ri qilingan xatti-harakatlardan keladigan zararni kamaytirish.

Nomzod aniqlangandan so‘ng, u treningdan o‘tishi yoki hech bo‘lmaganda ish majburiyatlari, shuningdek, axborot xavfsizligi qoidalari va tartiblari bilan batafsil tanishishi kerak bo‘ladi. U lavozimga kirishdan oldin va login nomi, parol va imtiyozlar bilan tizim hisobini yaratishdan oldin xavfsizlik choralarini tushunishi tavsiya etiladi.

Tizim akkaunti yaratilgan paytdan boshlab uning ma’muriyati, shuningdek, foydalanuvchi harakatlarini ro‘yxatga olish va tahlil qilish boshlanadi. Foydalanuvchi ishlayotgan muhit, uning ish majburiyatlari va boshqalar asta-sekin o‘zgaradi. Bularning barchasi imtiyozlarni mos ravishda o‘zgartirishni talab qiladi.

Foydalanuvchining tizim akkauntini tugatish, ayniqsa xodim va tashkilot o‘rtasida ziddiyat yuzaga kelgan taqdirda, imkon qadar tezroq amalga oshirilishi kerak (ideal holda, jazo yoki ishdan bo‘shatish to‘g‘risida xabar berilishi bilan bir vaqtda). Ish joyiga kirishni jismonan cheklash ham mumkin. Albatta, agar xodim ishdan ketsa, u o‘zining barcha kompyuter uskunalarini va, xususan, agar shifrlash vositalaridan foydalanilgan bo‘lsa, kriptografik kalitlarni o‘z qo‘liga olishi kerak.

Xulosa

Attestatsiyalash tashkiliy-texnik chora-tadbirlar majmui shaklida amalga oshiriladi, ularning natijalariga ko‘ra u amalga oshiriladigan muayyan talablar va standartlarga muvofiqlik uchun "Muvofiqlik sertifikati" beriladi.

Kadrlar tayyorlash muammosi axborot xavfsizligi nuqtai nazaridan asosiy muammolardan biridir. Agar xodim o‘z tashkilotining xavfsizlik siyosati bilan tanish bo‘lmasa, u o‘z maqsadlariga erishish uchun harakat qila olmaydi. Xavfsizlik choralarini bilmasa, u ularga rioya qila olmaydi. Aksincha, agar xodim o‘z harakatlari yozib olinayotganini bilsa, ularni buzishdan o‘zini tutishi mumkin.

FOYDALANILGAN ADABIYOTLAR

1. Whitman, Michael E., and Herbert J. Mattord. "Principles of Information Security." Cengage Learning, 2018.

2. Pfleeger, Charles P., and Shari Lawrence Pfleeger. "Security in Computing." Pearson Education, 2015.

3. Whitman, Michael E., et al. "Management of Information Security." Cengage Learning, 2018.

4. Scarfone, Karen, and Murugiah Souppaya. "Guide to Computer Security Certification and Accreditation." CRC Press, 2006.

5. NIST Special Publication 800-37 Revision 2: "Risk Management Framework for Information Systems and Organizations." National Institute of Standards and Technology, 2018.

6. Anderson, James A., and Peter D. Nash. "Security Engineering: A Guide to Building Dependable Distributed Systems." Wiley, 2008.

7. NIST Special Publication 800-53 Revision 5: "Security and Privacy Controls for Information Systems and Organizations." National Institute of Standards and Technology, 2020.

8. Carroll, John M., et al. "Information Assurance Handbook: Effective Computer Security and Risk Management Strategies." McGraw-Hill, 2014.

9. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11: "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products." Committee on National Security Systems, 2010.

10. Chapple, Mike, et al. "CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide." Sybex, 2018.

11. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 6: "National Policy for Telecommunications and Automated Information Systems Security." Committee on National Security Systems, 2003.

12. Schou, Corey, and Steven Hernandez. "Information Assurance for the Enterprise: A Roadmap to Information Security." McGraw-Hill, 2007.

13. National Institute of Standards and Technology. "Security Standards for Federal Information Systems and Organizations." National Institute of Standards and Technology, various editions.