AXBOROTLASHTIRISH OBYEKTLARIDA KIBERXAVSIZLIKNI TA'MINLASHDA ATTESTATSIYADAN O'TKAZISHNING AFZALLIKLARI

Meliko'ziev R.Sh. [1]
[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, O'zbekiston, Toshkent

Annotatsiya. *Mazkur maqola axborotlashtirish obyektlari va axborot resurslari axborot xavfsizligini ta'minlash bo'yicha amalga oshirilishi lozim bo'lgan chora-tadbirlar (obyektlarni attestatsadan o'tkazish) to'g'risida.*

Kalit so'zlar: *Axborotlashtirish obyektlari, axborot resurslari, axborot xavfsizligi, axborot tahdidlari, kiber hujum, Kasperskiy laboratoriyasi, maynerlar, tekshirish, ruxsatsiz kirish, attestatsiyalash, attestatsiya sinovlari, sinov lobaratoriyasi.*

Аннотация: *В данной статье речь идет о мерах (аттестации объектов), которые должны быть реализованы для обеспечения информационной безопасности информационных объектов и информационных ресурсов.*

Ключевые слова: *информационные объекты, информационные ресурсы, информационная безопасность, информационные угрозы, кибератака, «Лаборатория Касперского», майнеры, верификация, несанкционированный доступ, аттестация, аттестационные испытания, испытательная лаборатория.*

Annotation: *This article deals with measures (attestation of objects) that must be implemented to ensure the information security of information objects and information resources.*

Keywords: *information objects, information resources, information security, information threats, cyber attack, Kaspersky Lab, miners, verification, unauthorized access, attestation, attestation tests, testing laboratory.*

I. KIRISH

Axborot tahdidlari va kiber hodisalar soni yildan-yilga ortib bormoqda. koronavirus avj olishi 2020 yilda onlayn faoliyatga o'tgan kompaniyalar sonining sezilarli o'sishiga sabab bo'ldi, biroq buzg'unchilik, hujum va tahdidlar shunga

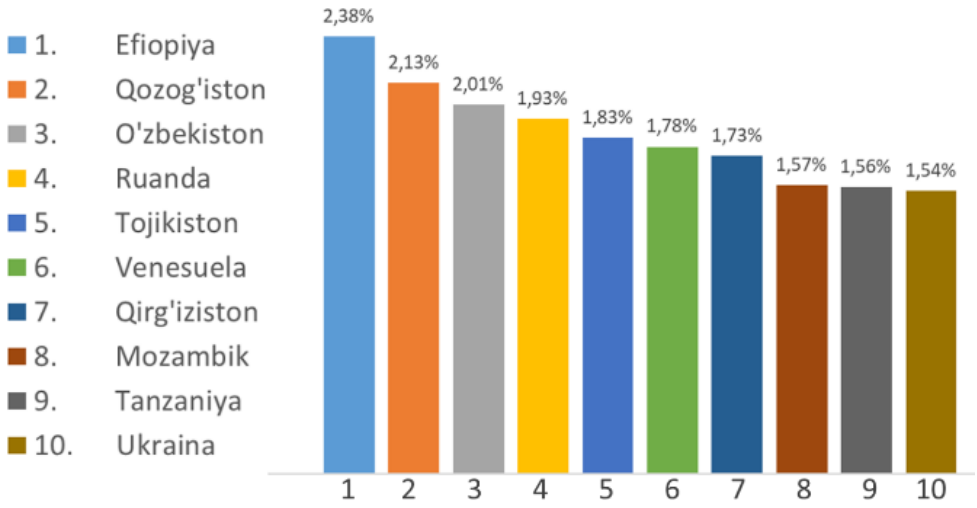
mutanosib ravishda oshdi. Ayniqsa hozirda xakerlik sohasi tez suratda rivojlanmoqda[5].

2022-yilning uchinchi choragida Kasperskiy laboratoriyasi 99 989 nafar foydalanuvchining kompyuterlaridagi bank hisoblaridan pul o‘g‘irlash uchun mo‘ljallangan turli shakdagi zararli dasturlarni ishga tushishining oldini olgan[6]. Moliyaviy zararli keltiruvchi kiber hujumlar uyushtirilgan davlatlarning ulushi 1-jadvalda keltirilgan.

1-jadval. Kiber hujum qilingan mamlakat va hududlar statistikasi.

№	Mamlakat yoki hudud	Foiz ko‘rsatkichi
1.	Turkmaniston	4.7%
2.	Afg‘oniston	4.6%
3.	Paragvay	2.8%
4.	Tojikiston	2.8%
5.	Yaman	2.3%
6.	Sudan	2.3%
7.	Xitoy	2.0%
8.	Shveytsariya	2.0%
9.	Misr	1.9%
10.	Venesuela	1.8%

2021-yilda kiberhujumlarning global zarari 6 trillion dollardan oshdi[7]. Kasperskiy laboratoriyasi tomindan olib borilgan tadqiqotlar natijasiga ko‘ra 2022-yilning uchinchi choragining o‘zida maynerlarning 153 773 ta yangi modifikatsiyasini aniqlangan. Ulardan 140 000 dan ortig‘i iyul va avgust oylariga to‘g‘ri keladi. Bundan ko‘rinadiki maynerlar ijodkorlarining faolligi yozda yuqori darajada. Maynerlar tomonidan hujumga uchragan davlat va hududlarning statistikasi 1-rasmdagi diogrammada ko‘rsatilgan[6].



1-rasm. Maynerlar hujumiga uchragan davlat va hududlarning statistikasi..

II. AXBOROTLASHTIRISH OBYEKTINI ATTESTATSIYALASH

Kiber tahdidlar va uning natijasida yuzaga keluvchi talofatlarni oldini olishning samarali yechimlaridan biri bu axborotlashtirish obyektlarini attestatsiyalashdan iboratdir.

“Milliy axborot resurslarini muhofaza qilishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi O‘zbekiston Respublikasi Prezidentining 2011 yil 8 iyuldagi PQ-1572-son qarori va Vazirlar Mahkamsining 2011 yil 7 noyabrdagi 296-son qarori bilan tasdiqlangan tartibga ko‘ra O‘zbekiston Respublikasi Davlat xaxfsizlik xizmati (avvalgi nomi Milliy xaxfsizlik xizmati) tomonida axborotlashtirish obyektlarini attesatsiyadan o‘tkazishga doir ishlarning muyyan turlarini amalga oshirish uchun turli mulkchilik shaklidagi tashkilotlarga ruxsatnomalar beradi. Albatta faqat ma’lum talablarga muvofiq bo‘lgandagina[1]. Hozirda mamlakatimizda axborotlashtirish obyektlarining maxfiy ma’lumotlar xavfsizligi ta’minlash talablariga muvofiqligini attesatsiyalash O‘zbekiston Respublikasi Milliy xavfsizlik xizmati Raisining 2014 yil 1 maydagi 47-sonli buyrug‘i bilan tasdiqlangan axborotlashtirish obyektlarini attesatsiyadan o‘tkazish tartibi to‘g‘risidagi na’munaviy nizomga asosan amalga oshiriladi.

Axborot xavfsizligi talablariga muvofiqligi bo‘yicha attestatsiyalash sinovlarini o‘tkazish va attestatsiyalash xizmatini ko‘rsatilishi mumkin bo‘lgan axborotlashtirish obyektlarining turlari va ro‘yxati Davlat xaxfsizlik xizmati tomonidan belgilangan.

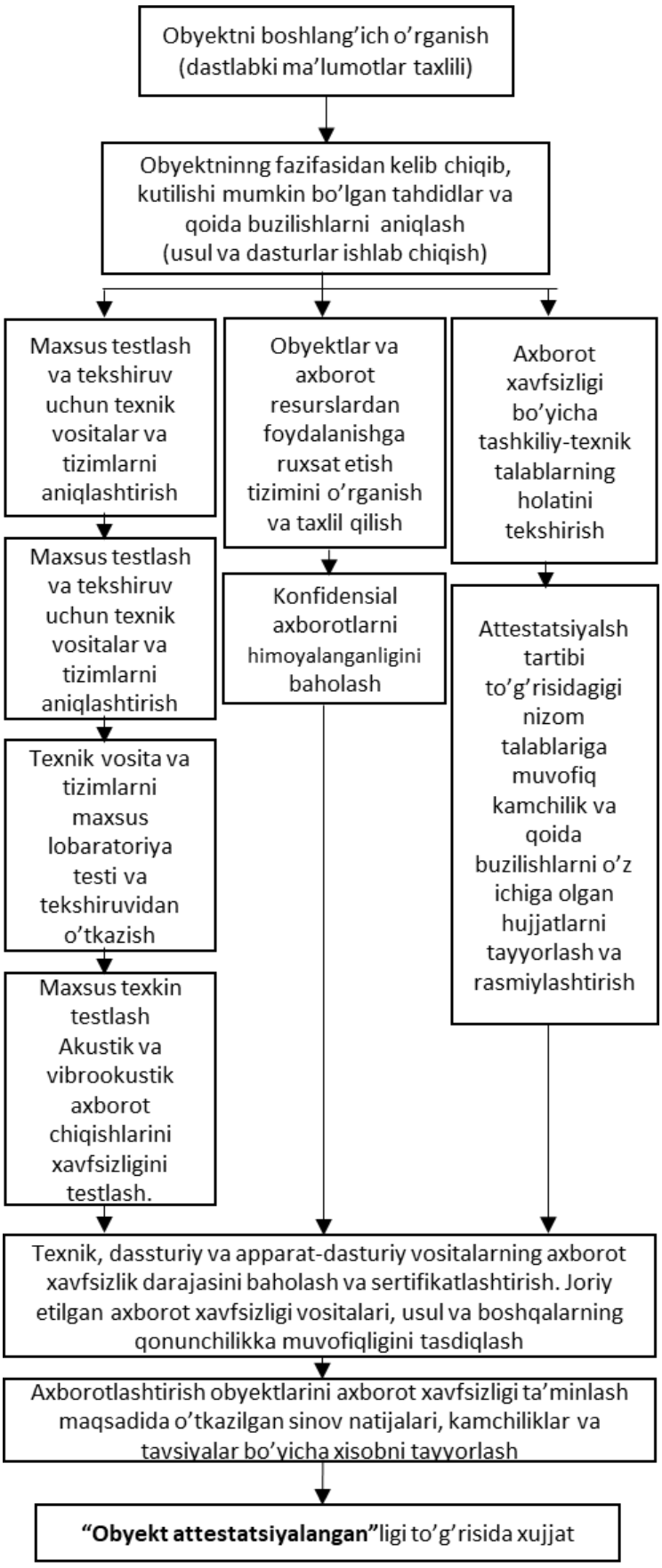
Axborotlashtirish obyektlariga quyidagilar kiradi:

• turli darajadagi va maqsadlardagi avtomatlashtirilgan tizimlar (axborot tizimlari) (axborotlashtirish vositalari va tizimlari);
• aloqa tizimlari, ma’lumotlarni qabul qilish, qayta ishlash va uzatish (axborotlashtirish vositalari va tizimlari);
• xizmat ko‘rsatish va ko‘paytirish tizimlari (axborotlashtirish vositalari va tizimlari bilan jihozlangan binolar);
• maxfiy muzokaralar o‘tkazish uchun mo‘ljallangan binolar va inshootlar (himoya qilinadigan binolar).

Obyektni attestatsiyalash jarayonida quyidagi ishlar amalga oshiriladi:

• axborot oqib chiqishining potentsial kanallarini aniqlash uchun muhandislik tahlili;
• axborotni muhofaza qilish bo‘yicha tashkiliy-ma’muriy hujjatlarning yetarliligi va to‘liqligini tekshirish;
• axborotlashtirish obyektini maxsus nazorat-o‘lchov vositalaridan foydalangan holda instrumental tekshirish va axborotlashtirish obyektida qayta ishlangan himoyalangan axborotning texnik kanallar orqali chiqishi bo‘yicha xavfsizligini baholash;
• axborotlashtirish obyektining axborotga ruxsatsiz kirishdan himoya qilish bo‘yicha xavfsizlik talablariga muvofiqligini baholash.

Axborotlashtirish obyektlarini attestatsiya sinovlarini o‘tkazishning umumlashtirilgan sxemasi 1-rasmdagi sxemada ko‘rsatilgan.



1 rasm. Axborotlashtirish obyektlarini attestatsiya sinovlaridan o'tkazishning umumiy sxemasi.

Obyektda ma’lumotlar tarmog‘i, kanallari, obyektning ishlash rejimi (elektr ta’minoti va yerga ulash sxemalari, binoning muhandislik kommunikatsiyalari, shuningdek, axborotlashtirish obyekti joylashgan binoning xavfsizlik va yong‘in signalizatsiya tizimlari) o‘rganiladi.

Avtomatlashtirilgan tizimning real ish sharoitida ma’lumotlarga ta’sir qiluvchi yoki ta’sir qilishi mumkin bo‘lgan omillarni aniqlanadi va qonunchilikka (standartlarga) muvofiqligi belgilanadi.

Axborotni muhofaza qilish bo‘yicha tashkiliy-ma’muriy hujjatlarni tekshiriladi. Axborotlashtirish obyektida quyidagi hujjatlarning mavjudligi va to‘liqligi aniqlashtirilishi lozim:

- axborotlashtirish obyektini tasniflash dalolatnomalari (avtomatlashtirilgan yoki axborot tizimi uchun);
- axborotlashtirish obyektining texnik pasporti;
- axborotlashtirish obyektini yerga ulash va elektr ta’minoti sxemalari;
- yerga ulanishdagi axborot chiqishi sinov bayonomalari;
- litsenziya shartnomalari, hisob-fakturalar yoki opperatsion tizimga o‘rnatilgan dasturiy ta’minotni qonuniy ravishda sotib olinganligini tasdiqlovchi boshqa hujjatlar;
- davlat standartlari talablariga muvofiq avborot vositalari uchun muvofiqlik sertifikatlar (elektromagnit moslik, xavfsizlik, sanitariya me’yorlari talablariga asosan);
- axborotlashtirish obyekti va axborotni himoya qilish vositalari uchun operatsion hujjatlar, shuningdek axborot xavfsizligini ta’minlash bo‘yicha tashkiliy-ma’muriy hujjatlar (buyruqlar, ko‘rsatmalar);
- axborotni himoya qilishni ta’minlaydigan xodimlarning malakasi to‘g‘risidagi ma’lumotlar;
- muhofaza qilinadigan obyektlarga kiriuvchi sub’ektlarni boshqarish jadvali (matritsasi);
- axborotni himoya qilish sertifikatlari.

Attestatsiyalash sinovlari muddati tugashidan oldin buyurtmachi pudratchi tomonidan ishlab chiqilgan va u bilan kelishilgan tashkiliy hamda ma’muriy hujjatlarni tasdiqlashi va kuchga kiritishi kerak.

Attestatsiyalash sinovi obyektini maxsus nazorat-o‘lchash uskunalari yordamida instrumental tekshirish va axborotlashtirish obyektidan himoyalangan ma’lumotlarning texnik kanallar orqali chiqishi bo‘yicha xavfsizligini baholash.

Sinovlar quyidagi quyidagi tizimlarni tekshirishdan iborat:

- kirishni boshqarish;
- ro‘yxatga olish va hisobga olish;

• kriptografik;
• yaxlitligini ta’minlash;
• antivirus himoyasi.

Axborotlashtirish obyekti va resursiga ruxsatsiz kirishning himoya qilish talablariga muvofiqligini tekshirish quyidagi tartibda amalga oshiriladi:
• axborotlashtirish obyektiga ruxsatsiz kirishdan himoya qilish uchun joriy etilgan rejim va texnik vositalarni tekshirish;
• ma’lumotlar bilan ishlashning texnologik jarayonidagi axborot oqimlarini tahlil qilish;
• axborotni ruxsatsiz kirishdan himoya qilish bo‘yicha joriy etilgan chora-tadbirlarning etarliligi va mavjud hujjatlari talablarga muvofiqligini baholash;
• axborotlashtirish obyektida antivirus vositalarining mavjudligi va qo‘llanilishini tekshirish (agar kerak bo‘lsa, hujumlarni aniqlash tizimlari).

Attestatsiya sinovlari axborotlashtirish obyektining axborot xavfsizligiga muvofiqligi bo‘yicha baholanishi, yo‘l qo‘yilgan qoida buzarliklarni bartaraf etish, axborotlashtirish obyektini himoya qilish tizimini joriy etish bo‘yicha aniq tavsiyalar berilgan attestatsiya sinovlari natijalari to‘g‘risidagi xulosani rasmiylashtirish bilan yakunlanadi. Xulosada axborotlashtirish obyektining ishlashini monitoring qilish bo‘yicha tavsiyalar, uning belgilangan talablarga muvofiqligi, mavjud tizimni takomillashtirish yoritilishi lozim. Agar lozim topilgan taqdirda obyektning attestatsiyalanganligi to‘g‘risidagi muvofiqlik guvohnomasi beriladi. Uning amal qilish muddati 3 yilgacha belgilanishi mumkin.

III.XULOSA

Xulosa sifadi aytish mumkinki, axborot xavfsizligini ta’minlashning asosiy choralaridan biri axborotlashtirish obyektini attestatsiyadan o‘tkazish va attestatsiyadan o‘tgandan so‘ng faoliyatiga ruxsat berishdir. Raqamli texnologiyalar rivojlanishi jadallashmoqda, bu esa attestatsiyalangan obyektlar xakerlar hujumiga har doim ham bardosh bera olmaydi. Bunga attestatsiyadan o‘tkazgan tashkilot ham o‘z javovgarligini olmaydi ham. Bunday vaziyatlarda sug‘irtalash va axborot resurslarini doimiy axborot xavsizligi nuqtai nazaridan testlab borish samarali hisoblanadi. Yuqorini nufuzga ega konponiyalar o‘z axborot tizmini doimiy teslab boradi va hujumlarga qarshi ataka usulini amalga oshiradi. Shu orqali kutilishi mumkin bo‘lgan talofatlarning oldini oladi. Yetkazilgan zarar esa sug‘irtalangan bo‘ladi.

ADABIYOTLAR

[1] “Milliy axborot resurslarini muhofaza qilishga doir qo‘shimcha chora-tadbirlar to‘g‘risida” O‘zbekiston Respublikasi Prezidentining 2011 yil 8 iyuldagi PQ-1572-son qarori.
[2] O‘zbekiston Respublikasi Vazirlar mahkamasining 296-sonli qorori. 07.11.2011 y.
[3] “Axborotlashtirish obyektlarini attesatsiyadan o‘tkazish tartibi to‘g‘risidagi na’munaviy nizom” O‘zbekiston Respublikasi Milliy xavfsizlik xizmati Raisining 2014 yil 1 maydagi 47-sonli buyrug‘i bilan tasdiqlangan.
[4] O‘zbekiston Respublikasi Prezidentining “Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to‘g‘risida” 2018-yil 19-fevraldagi PF-5349-son Farmoni.
[5] Полная статистика угроз информационной безопасности в одной статье.07.10.2021.https://codernet.ru/articles/drugoe/polnaya_statistika_ugroz_informaczionnoj_bezopasnosti_v_odnoj_state/
[6] Афтер Амир. Развитие информационных угроз в третьем квартале 2022 года. Статистика по ПК. 18 ноя 2022. https://securelist.ru/it-threat-evolution-in-q3-2022-non-mobile-statistics/106077/
[7] Кибератаки. 2023/01/17 https://www.tadviser.ru/index.php/.