2-mavzu. Axborot xavfsizligi boshqaruv tizimlarini audit qilish.

REJA:

1. ISO/IEC 27001 va ISMS talablari.
2. Sertifikatlash jarayonida auditning roli.
3. Boshqaruv hujjatlari va nazoratlar.
4. Auditorlik dalillarini yig‘ish.

Umumiy tushuncha

Axborot xavfsizligi boshqaruv tizimi (AXBT, ingl. ISMS — Information Security Management System) – bu tashkilotning axborot aktivlarini himoya qilishga qaratilgan kompleks siyosat, jarayon, protsedura va texnologiyalar majmui. Ushbu tizimning samaradorligini baholash, uning standartlarga va qonunchilik talablariga muvofiqligini aniqlash uchun **audit** o‘tkaziladi.

Audit — mustaqil, tizimli va hujjatlashtirilgan baholash jarayoni bo‘lib, u axborot xavfsizligi boshqaruv tizimining mavjudligi, samaradorligi va xalqaro standartlarga mosligini tekshiradi.

SO/IEC 27001 va ISMS talablari

ISO/IEC 27001 standarti haqida umumiy tushuncha

ISO/IEC 27001 – bu xalqaro miqyosda tan olingan standart bo‘lib, u tashkilotlarda **axborot xavfsizligini boshqaruv tizimi (ISMS – Information Security Management System)**ni yaratish, joriy etish, kuzatish va takomillashtirish bo‘yicha metodik asoslarni belgilaydi. Ushbu standart ilk bor 2005-yilda ishlab chiqilgan, 2013-yilda qayta ko‘rib chiqilgan va 2022-yilda so‘nggi tahriri qabul qilingan. U axborot xavfsizligi bo‘yicha eng keng qo‘llaniladigan standartlardan biri hisoblanadi.

ISO/IEC 27001 nafaqat yirik korxonalar, balki kichik va o‘rta biznes subyektlari uchun ham mos keladi, chunki u tashkilotning faoliyat sohasidan qat’i nazar, **axborot aktivlarini himoya qilish**, **xavf-xatarlarni baholash** va **resurslarni oqilona taqsimlash** imkoniyatini beradi.

ISMS (Information Security Management System) mohiyati

Axborot xavfsizligini boshqaruv tizimi (ISMS) – bu axborot resurslarini himoya qilishga qaratilgan siyosatlar, jarayonlar, texnologiyalar va tashkiliy choralar yig‘indisidir. ISMSning eng muhim xususiyati shundaki, u **xavfga asoslangan yondashuv**ni qo‘llaydi. Ya’ni, tashkilot barcha xavflarni aniqlab, ularning oqibatlarini baholaydi va ularni kamaytirish uchun maqsadga muvofiq boshqaruv choralari ishlab chiqadi.

ISMS faqat texnik vositalar bilan cheklanmaydi. U quyidagilarni o‘z ichiga oladi:

- **Siyosiy daraja**: axborot xavfsizligi siyosatlari va ularni qo‘llash mexanizmlari.
- **Tashkiliy daraja**: xodimlarning rollari va mas’uliyatlari, huquq va majburiyatlar.
- **Texnik daraja**: shifrlash, tarmoq xavfsizligi, identifikatsiya va autentifikatsiya mexanizmlari.
- **Inson resurslari darajasi**: xodimlarni tanlash, o‘qitish va ularda xavfsizlik madaniyatini shakllantirish.

ISO/IEC 27001 ning asosiy talablari

ISO/IEC 27001 standarti 10 ta asosiy bo‘lim (clause) va **Annex A** (nazorat choralari)dan iborat. Quyida ular nazariy jihatdan yoritiladi:

1. Kontekst (Context of the organization)

Tashkilot o‘zining ichki va tashqi muhitini tahlil qiladi, manfaatdor tomonlarning talablarini o‘rganadi va ISMSning qo‘llanish sohasini belgilaydi. Bu bosqichda korxonaning tashqi bozordagi pozitsiyasi, huquqiy talablar, texnologik imkoniyatlar va mavjud xavflar aniqlanadi.

2. Rahbariyatning roli (Leadership)

Yuqori rahbariyat ISMSni yaratish va samarali ishlashini ta’minlash uchun mas’uldir. U axborot xavfsizligi siyosatini tasdiqlashi, kerakli resurslarni ajratishi va mas’uliyatlarni aniq belgilashi lozim. Shu orqali xavfsizlik faqat texnik mutaxassislar vazifasi emas, balki butun tashkilot faoliyatining bir qismi sifatida qaraladi.

3. Rejalashtirish (Planning)

Rejalashtirish jarayonida axborot xavfsizligi bo‘yicha risklar aniqlanadi, baholanadi va ustuvorliklarga qarab nazorat mexanizmlari ishlab chiqiladi. Shuningdek, xavfsizlik maqsadlari belgilanadi va ularga erishish rejalari tuziladi.

4. Qo‘llab-quvvatlash (Support)

ISMS samarali ishlashi uchun moliyaviy, inson resurslari va texnik resurslar zarur. Bundan tashqari, hujjatlar bilan ishlash, axborot almashish mexanizmlari va xodimlarning malakasini oshirish bo‘yicha chora-tadbirlar ham muhim ahamiyatga ega.

5. Amalga oshirish (Operation)

Rejalashtirilgan xavfsizlik choralarini amaliyotga joriy etish, risklarni boshqarish va jarayonlarni nazorat qilish bu bosqichda amalga oshiriladi. Shuningdek, o‘zgarishlarni boshqarish mexanizmi ham tatbiq etiladi.

6. Monitoring va baholash (Performance Evaluation)

Audit va monitoring mexanizmlari joriy etilib, xavfsizlik choralarining samaradorligi tekshiriladi. Bu bosqichda ichki auditlar, tashqi auditlar va rahbariyat tomonidan ko‘rib chiqishlar amalga oshiriladi.

7. Takomillashtirish (Improvement)

Tashkilot aniqlangan kamchiliklarni bartaraf etadi va doimiy ravishda yaxshilashga intiladi. Bu bosqichda tajribalar tahlil qilinadi va ISMSning yangi sharoitlarga moslashishi ta’minlanadi.

ISO/IEC 27001 Annex A – Nazorat choralari

Annex A da keltirilgan nazorat choralari xavfsizlikni texnik, tashkiliy va inson resurslari darajalarida ta’minlaydi. 2022-yilgi tahrirda ularning soni 114 tadan 93 tagacha qisqartirilib, 4 ta toifaga ajratilgan:

1. **Tashkiliy nazoratlar** – siyosatlar, huquqiy talablar, manfaatdor tomonlar bilan ishlash.
2. **Inson resurslari nazorati** – xodimlarni yollash, ularni o‘qitish, intizomiy tartiblar.

3. **Texnologik nazoratlar** – shifrlash, tarmoq xavfsizligi, foydalanuvchi huquqlarini boshqarish, kirishni cheklash.

4. **Jismoniy nazoratlar** – binolarga kirishni nazorat qilish, CCTV, qo‘riqlash va signalizatsiya vositalari.

ISO/IEC 27001 sertifikatsiyasi

- **Ichki audit**: tashkilotning o‘zida o‘tkazilib, ISMS samaradorligi tekshiriladi.
- **Tashqi audit**: mustaqil organ tomonidan amalga oshiriladi va obyektiv baho beradi.
- **Sertifikatlash auditi**: tashkilot xalqaro standart talablariga mos kelishini isbotlasa, 3 yil amal qiladigan sertifikat beriladi. Har yili kuzatuv auditi o‘tkazilib, tizimning barqarorligi tekshiriladi.

ISO/IEC 27001 va ISMSning ahamiyati

- Axborot aktivlarini tahdidlardan himoya qiladi.
- Xalqaro bozorda ishonchni oshiradi va hamkorlik imkoniyatlarini kengaytiradi.
- Huquqiy va normativ talablarni bajarishga yordam beradi.
- Xavf-xatarlarni kamaytiradi va biznesning uzluksizligini ta’minlaydi.
- Tashkilot imidji va obro‘sini mustahkamlaydi.

ISO/IEC 27001 va ISMS talablari tashkilotlarda axborot xavfsizligini boshqarishning eng samarali vositalaridan biridir. Ushbu standart xavf-xatarlarga asoslangan yondashuvni qo‘llash orqali nafaqat texnik himoya choralarini, balki tashkiliy, huquqiy va inson resurslari bilan bog‘liq choralarni ham qamrab oladi. Natijada, tashkilot o‘z axborot aktivlarini to‘liq himoya qila oladi va xalqaro miqyosda ishonchlilikka ega bo‘ladi.

Boshqaruv hujjatlari va nazoratlar

1. Boshqaruv hujjatlarining mohiyati

Axborot xavfsizligini boshqaruv tizimi (ISMS) samarali ishlashi uchun aniq hujjatlashtirilgan siyosatlar, protseduralar va reglamentlar talab etiladi. Ushbu

hujjatlar **boshqaruv hujjatlari** deb ataladi. Ular tashkilot faoliyatida axborot xavfsizligini ta’minlashga oid barcha jarayonlarni me’yoriy asosda tartibga soladi.

Boshqaruv hujjatlarining asosiy vazifasi – tashkilotning axborot xavfsizligi bo‘yicha siyosatini hujjatlashtirish, jarayonlar izchilligini ta’minlash, manfaatdor tomonlar uchun ishonchli asos yaratishdir.

Asosiy boshqaruv hujjatlari:

1. **Axborot xavfsizligi siyosati** – tashkilotning umumiy strategiyasi va maqsadlarini belgilaydi.
2. **Standart operatsion protseduralar (SOPs)** – xavfsizlik bo‘yicha kundalik amaliy harakatlar ketma-ketligini tartibga soladi.
3. **Risklarni boshqarish rejalari** – xavflarni aniqlash, baholash va bartaraf etish choralari yozib qo‘yiladi.
4. **Favqulodda vaziyatlarda harakat rejasi** – texnik nosozlik, kiberhujum yoki tabiiy ofat yuz berganda amalga oshiriladigan chora-tadbirlar.
5. **Kadrlar bo‘yicha siyosatlar** – xodimlarni tanlash, o‘qitish, axborotga kirish huquqlarini boshqarish qoidalari.
6. **Texnologik hujjatlar** – server, tarmoq, ma’lumotlar bazasi va boshqa IT infratuzilmasini boshqarish reglamentlari.

2. Nazoratlar tushunchasi

Nazoratlar (controls) – bu tashkilot axborot aktivlarini himoya qilish uchun qo‘llaydigan tashkiliy, texnik, huquqiy va jismoniy choralar majmuasidir. ISO/IEC 27001 standarti doirasida nazoratlar **Annex A** bo‘yicha aniq belgilangan bo‘lib, ular ISMSning muhim tarkibiy qismi hisoblanadi.

Nazoratlarning vazifasi:

- Axborot xavfsizligi bo‘yicha risklarni kamaytirish.
- Xodimlarning xavfsizlikka rioya qilishini ta’minlash.
- Jarayonlarni monitoring qilish va nomuvofiqliklarni aniqlash.
- Tizimning uzluksiz ishlashini kafolatlash.

3. Nazoratlarning asosiy turlari

1. **Tashkiliy nazoratlar**

- Axborot xavfsizligi siyosatlari va qoidalarini joriy etish.
- Mas’uliyat va rollarni taqsimlash.
- Hamkorlar va uchinchi tomon bilan tuziladigan shartnomalarda xavfsizlik talablarini belgilash.

2. **Inson resurslari nazorati**
   - Xodimlarni yollashda tekshirish (background check).
   - Maxfiylik shartnomalarini imzolash.
   - Doimiy o‘qitish va malaka oshirish.
   - Intizomiy choralar tizimi.
3. **Texnologik nazoratlar**
   - Kirish nazorati (login, parol, biometrik autentifikatsiya).
   - Kriptografiya va shifrlash.
   - Firewall, IDS/IPS, antivirus va DLP tizimlari.
   - Zaxira nusxa olish va ma’lumotlarni tiklash mexanizmlari.
4. **Jismoniy nazoratlar**
   - Ofis va server xonalariga kirishni nazorat qilish.
   - Kuzatuv kameralaridan foydalanish.
   - Yong‘in signalizatsiyasi va elektr uzilishi holatida zaxira generatorlari.
   - Qurilmalarni jismoniy himoya qilish (masalan, portlarni bloklash, server shkaflarini qulflash).

4. Boshqaruv hujjatlari va nazoratlarning o‘zaro bog‘liqligi

- **Boshqaruv hujjatlari** – xavfsizlikni qanday ta’minlash kerakligini belgilaydi.
- **Nazoratlar** – bu hujjatlarda belgilangan choralarni amalda bajarishni ta’minlaydi.

Masalan, axborot xavfsizligi siyosatida “parollar kamida 8 belgidan iborat bo‘lishi kerak” deb yozilgan bo‘lsa, texnologik nazorat sifatida tizimda avtomatik parol siyosati sozlanadi.

Shunday qilib, boshqaruv hujjatlari va nazoratlar bir-birini to‘ldiradi: hujjatlar – nazariy asos, nazoratlar esa – amaliy mexanizm sifatida ishlaydi.

Boshqaruv hujjatlari va nazoratlar axborot xavfsizligi boshqaruv tizimining ajralmas qismidir. Hujjatlar tashkilot uchun me’yoriy asosni belgilasa, nazoratlar ularning amalda qo‘llanishini ta’minlaydi. ISO/IEC 27001 standarti doirasida bu ikki element uyg‘un holda ishlaganda tashkilotning axborot aktivlari samarali himoya qilinadi, risklar kamayadi va xalqaro talablar bajarilishi kafolatlanadi.

Auditorlik dalillarini yig‘ish

1. Auditorlik dalillari tushunchasi

Auditorlik dalillari – bu audit jarayonida auditor tomonidan to‘plangan, hujjatlashtirilgan va tekshirilgan axborot bo‘lib, ular asosida auditor xulosa chiqaradi. Dalillar audit hisobotining ishonchliligi va obyektivligini ta’minlaydi.

ISO/IEC 19011 va ISO/IEC 27007 standartlarida qayd etilishicha, **dalillar etarli, obyektiv, aniq va hujjatlashtirilgan bo‘lishi shart**. Ya’ni auditor o‘z fikrini subyektiv taxminlarga emas, balki dalillarga asoslashga majburdir.

2. Auditorlik dalillarining asosiy xususiyatlari

- **Obyektivlik** – dalillar xolis bo‘lishi, auditor yoki tekshirilayotgan xodimning shaxsiy fikridan mustaqil bo‘lishi kerak.
- **Etarlilik** – yig‘ilgan dalillar soni yetarli bo‘lishi lozim, chunki bir-ikki fakt umumiy holatni to‘liq aks ettirmaydi.
- **Moslik** – dalillar audit maqsadi va standart talablariga bevosita aloqador bo‘lishi kerak.
- **Haqiqiylik** – dalillar real bo‘lishi va soxta yoki noto‘g‘ri ma’lumotlarni o‘z ichiga olmasligi lozim.
- **Hujjatlilik** – og‘zaki so‘zlar emas, balki hujjatlar, yozuvlar, log-fayllar, hisobotlar asosiy dalil sifatida qabul qilinadi.

3. Auditorlik dalillarini yig‘ish usullari

1. Hujjatlarni ko‘rib chiqish

- Siyosatlar, protseduralar, reglamentlar, standart operatsion tartiblar (SOP) tekshiriladi.

- Xavfsizlik siyosati, foydalanuvchi huquqlari, kirish loglari, xavfsizlik insidentlari hisobotlari asosiy hujjatlar hisoblanadi.

2. Kuzatuv (observatsiya)

- Auditor real jarayonlarni kuzatadi: foydalanuvchilar qanday kiradi, tizim qanday ishlaydi, xavfsizlik choralariga qanday amal qilinadi.
- Masalan, parol siyosati amalda ishlayaptimi yoki server xonasiga ruxsatsiz kirish mumkinmi – bular kuzatish orqali aniqlanadi.

3. Suhbat va intervyu

- Auditor xodimlar, rahbariyat va IT mutaxassislari bilan suhbat o‘tkazadi.
- Savollar orqali xodimlarning axborot xavfsizligi siyosatidan xabardorligi, kundalik faoliyatda unga amal qilish darajasi aniqlanadi.

4. Tekshiruv va test (testing)

- Auditor xavfsizlik tizimlarining ishlashini sinovdan o‘tkazadi.
- Masalan, foydalanuvchi parolini qayta tiklash jarayoni sinab ko‘riladi yoki xavfsizlik zaifliklari aniqlash testlari bajariladi.

5. Tahlil (analysis)

- Loglar, monitoring natijalari, audit yo‘llari, xavfsizlik vositalarining hisobotlari chuqur tahlil qilinadi.
- Masalan, IDS/IPS hisobotlari, SIEM tizimidan olingan ma’lumotlar asosiy dalil sifatida ishlatiladi.

4. Auditorlik dalillarining manbalari

- **Ichki hujjatlar**: siyosatlar, rejalashtirish hujjatlari, xavfsizlik protokollari.
- **Tashqi hujjatlar**: qonunlar, xalqaro standartlar, litsenziyalar.
- **Elektron manbalar**: tizim loglari, audit fayllari, xavfsizlik hisobotlari.
- **Og‘zaki manbalar**: xodimlarning intervyu javoblari, rahbariyatning izohlari.
- **Kuzatuv natijalari**: real jarayonlar va amaliy faoliyat kuzatuvlari.

5. Auditorlik dalillarining ahamiyati

- **Xolis xulosa chiqarish** uchun asos bo‘lib xizmat qiladi.
- **Standartlarga moslikni isbotlaydi** (ISO/IEC 27001, ISO/IEC 19011).

- **Zaifliklarni aniqlash va yaxshilash** bo‘yicha tavsiyalar ishlab chiqishga imkon beradi.
- **Sertifikatlash jarayonida** asosiy rol o‘ynaydi, chunki sertifikatlash qarori faqat ishonchli dalillarga tayanadi.

Auditorlik dalillarini yig‘ish audit jarayonining eng muhim bosqichidir. Dalillar yetarli, obyektiv, ishonchli va hujjatlashtirilgan bo‘lishi shart. Hujjatlarni ko‘rib chiqish, kuzatuv, suhbat, sinov va tahlil kabi usullar orqali auditor tashkilotning axborot xavfsizligi tizimini to‘liq baholash imkoniga ega bo‘ladi. Aynan dalillar asosida chiqarilgan xulosalar audit hisobotining ishonchliligini ta’minlaydi va tashkilotning xavfsizlik darajasini yuksaltirish uchun poydevor vazifasini o‘taydi.

Xavfsizlik standartlarining asosiy maqsadi axborot texnologiyalari mahsulotlarini ishlab chiqaruvchilar, iste’molchilar va kvalifikatsiyalash bo'yicha ekspertlar orasida o‘zaro aloqani yaratish hisoblanadi.

Ishlab chiqaruvchilar uchun standartlar, axborot mahsulotlarining imkoniyatlarini taqqoslash uchun zarur. Undan tashqari standartlar axborot mahsulotlari xususiyatlarini obyektiv baholash mexanizmi hisoblanuvchi, sertifikatsiyalash muolajalari uchun zarur.

Iste ’molchilarehtiyojlariga muvofiq axborot mahsulotini asosli tanlashga imkon beruvchi usulga manfaatdordurlar. Buning uchun ularga xavfsizlikni baholash shkalasi zarur.

Axborot texnologiyalari mahsulotlarini kvalifikatsiyalash bo'yicha ekspertlar standartlami ularga axborot texnologiyalari mahsulotlari tomonidan ta’minlanuvchi xavfsizlik darajasini baholashga imkon beruvchi instrument sifatida qabul qiladilar.

ISO/IEC 27001:2005 - “Axborot texnologiyalari. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarish tizimlari. Talablar”. Ushbu standart axborot xavfsizligini boshqarish tizimini (AXBT) ishlab chiqish, joriy etish, uning ishlashi, monitoringi, tahlili, unga xizmat ko‘rsatish va uni takomillashtirish modeli va talablaridan iborat. AXBT joriy etilishi tashkilotning

strategik qarori bo‘lib qolishi kerak. AXBTni ishlab chiqish va joriy etishda xavfsizlikning ehtiyojlari, maqsadlari, foydalaniladigan jarayonlari, tashkilotning ko‘lami va strukturasi hisobga olinishi kerak. AXBT va uning yordamchi tizimlari vaqt o‘tishi bilan o‘zgaradi degan taxmin bor. Shuningdek, AXBTni kengaytirish masshtablari tashkilotning ehtiyojlariga bog‘liq bo‘ladi, masalan, oddiy vaziyat AXBT uchun oddiy yechimni talab qiladi.

Muvofiqlikni baholash uchun ushbu standartdan ichki va tashqi tomonlar foydalanishi mumkin.

Jarayonli yondashuv.Ushbu standart tashkilot AXBTni ishlab chiqish, joriy etish, uning ishlashi, monitoringi, tahlili, unga xizmat ko‘rsatish va uni takomillashtirishda jarayonli yondashuvning qo‘llanishiga yo‘naltirilgan.

Tashkilot muvaffaqiyatli ishlashi uchun faoliyatning ko‘p sonli o‘zaro bog‘liq turlarini aniqlashi va ulami boshqarishni amalga oshirishi kerak. Aktivlardan foydalanuvchi va kirishlami chiqishlarga o‘zgartirish maqsadida boshqariladigan faoliyatning barcha turlariga jarayonlar sifatida qarash mumkin. Ko‘pincha bir jarayonning chiqishi keyingi jarayonning bevosita kirishini hosil qiladi.

Tashkilotda jarayonlar tizimini identifikatsiyalash va ulaming o‘zaro harakati bilan bir qatorda jarayonlar tizimidan foydalanish, shuningdek, jarayonlami boshqarish jarayonli yondashuv deb hisoblanishi mumkin.

Bunday yondashuv axborot xavfsizligida qo‘llanganda quyidagilaming muhimligini ta’kidlaydi:

- tashkilotning axborot xavfsizligi talablarini va axborot xavfsizligi siyosati va maqsadlarini belgilash zarurligini tushunish;

- tashkilot barcha biznes-tavakkalchiliklaming umumiy kontekstida tashkilot axborot xavfsizligi xatarlarini boshqarish choralarini joriy etish va qo‘llash;

- AXBT unumdorligi va samaradorligining doimiy monitoringi va tahlili;

- obyektiv o‘lchashlar natijalariga asoslangan uzluksiz takomillashtirish.

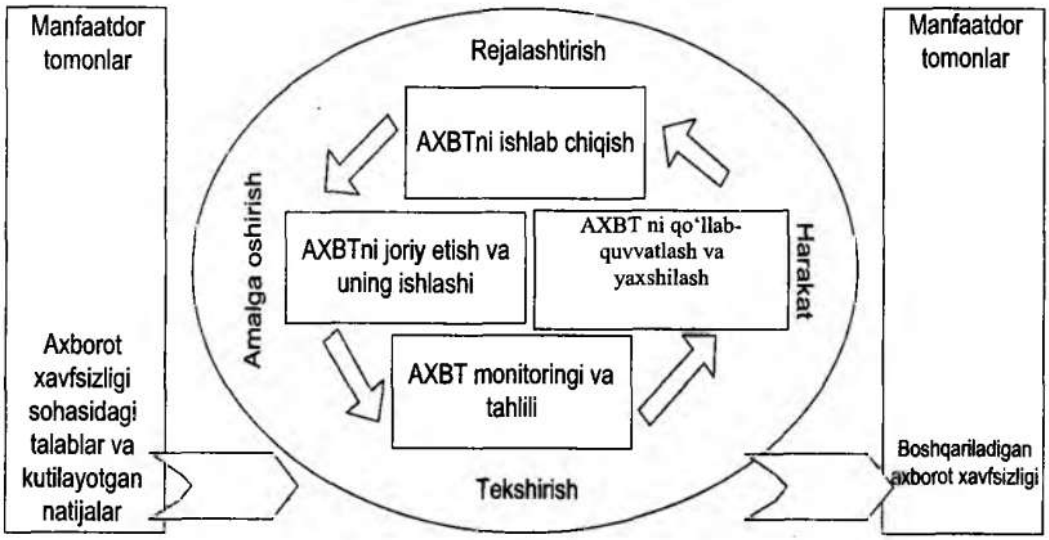
Ushbu standartda AXBT har bir jarayonini ishlab chiqishda qo‘llanishi mumkin bo‘lgan rejalashtirish - amalga oshirish -tekshirish - harakat [«Plan-Do-Check-Act» (PDCA)] modeli keltirilgan.

Ushbu model AXBT axborot xavfsizligi talablari va manfaatdor tomonlaming kutilayotgan natijalaridan kiruvchi ma’lumotlar sifatida qanday foydalanishini va zarur xatti-harakatlar va jarayonlami amalga oshirish natijasida e’lon qilingan talablar va kutilayotgan natijalami qanoatlantirishidan dalolat beradigan ma’lumotlami olishini ko‘rsatadi.

Bundan tashqari, PDCA modeli «Axborot tizimlari va tarmoqlari xavfsizligi bo‘yicha iqtisodiy hamkorlik va rivojlanish tashkiloti»ning amaldagi ko‘rsatmalariga mos keladi. Ushbu standart xatarlami boshqarish, xavfsizlik choralarini rejalashtirish va amalga oshirish, xavfsizlikni boshqarish va qayta baholashda ushbu prinsiplami qo‘llashning amaliy modelini taqdim etadi.

1-misol. Axborot xavfsizligining buzilishi tashkilot uchun jiddiy moliyaviy yo‘qotishlaming va/yoki qandaydir qiyinchiliklaming sababi bo‘la olmaydi degan talab qo‘yilishi mumkin.

2-misol. Qandaydir jiddiy mojaro, masalan, sayt yordamida elektron savdoni amalga oshirayotgan tashkilot saytining buzilishi natijasida yuzaga keladigan holat uchun - tashkilot buzilish oqibatlarini minimumga keltirish uchun yetarli bilim va tajribaga ega bo‘lgan mutaxassislarga ega bo‘lishi kerak. 3.1-rasmda AXBT jarayonlariga PDCA modelini qo‘llash ko‘rsatilgan.



3.1-rasm. AXBT jarayonlariga PDCA modelini qo'llash.

Ushbu standart tashkilotga amaldagi AXBTni boshqa boshqamv tizimlarining tegishli talablari bilan moslashtirish yoki integratsiya qilish imkonini beradi.

Boshqa boshqarish tizimlari bilan moslashuv. Ushbu standart boshqa boshqaruv standartlari bilan moslashuvini yaxshilash va integratsiya qilish uchun ISO 9001:2000 [2] va ISO 14001:2004 standartlari bilan muvofiqlashtirilgan. Kerakli tarzda loyihalashtirilgan bitta boshqaruv tizimi barcha ushbu standartlaming talablariga javob berishga qodir. 3.1-jadvalda ushbu standartning ISO 9001:2000 va ISO 14001:2004 standartlari bilan o'zaro bog'liqligi ko'rsatilgan.

3.1-jadval.

Rejalashtirish (AXBTni ishlab chiqish)	Tashkilotning umumiy siyosati va maqsadlarida e'lon qilingan natijalarga erishish maqsadida siyosat va maqsadlami belgilash, xatarlami boshqarish va axborot xavfsizligini takomillashtirish bilan bog'liq bo'lgan jarayonlar va protseduralami aniqlash.
Amalga oshirish(AXBTni joriy	AXBT siyosati, metodlari, jarayonlari va

etish va uning ishlashi)	protseduralarini joriy etish va uning ishlashi.
Tekshirish(AXBT monitoringi va tahlili)	Jarayonlaming AXBT siyosati va maqsadlariga muvofiqligini baholash va zarurat bo‘lganida samaradorligini o‘lchash. Natijalaming yuqori rahbariyat tomonidan tahlil qilinishi.
Harakat(AXBTni qo‘llab quwatlash va takomillashtirish)	AXBT ichki auditlari natijalariga rahbariyat tomonidan qilingan tahlil yoki uzluksiz takomillashtirish maqsadida boshqa manbalardan olingan ma’lumotlarga asoslangan tuzatuvchi va ogohlantiruvchi harakatlami bajarish.

ISO/IEC 27002:2005 - “Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari.

Axborot - biznesning boshqa muhim aktivlari kabi qiymatga ega bo‘lgan aktiv va shunday ekan, u tegishli ravishda muhofaza qilingan bo‘lishi kerak. Bu o‘zaro aloqalar bilan doimo rivojlanayotgan amaliy ish muhitida ayniqsa muhim. Hozirgi vaqtda ushbu o‘zaro aloqalar natijasida axborot tahdidlar va zaifliklaming o‘sib borayotgan soni va turli xiliga duchor bo‘lmoqda.

Axborot turli shakllarda mavjud bo‘lishi mumkin. U qog‘oz eltuvchida joylashtirilgan bo‘lishi, elektron ko‘rinishda saqlanishi, pochta orqali yoki telekommunikatsiyaning elektron vositalaridan foydalanib uzatilishi, plyonkadan namoyish qilinishi yoki og‘zaki ifodalanishi mumkin. Axborot mavjudligining shaklidan, uni tarqatish yoki saqlash usulidan qat’iy nazar u doim adekvat muhofazalangan bo‘lishi kerak.

Axborot xavfsizligi - axborotni biznesning uzluksizligini ta’minlash, biznes xavflarini minimumga keltirish va investitsiyalami qaytarishni hamda biznes imkoniyatlarini maksimal oshirish maqsadida tahdidlaming keng spektridan muhofaza qilish demakdir.

Axborot xavfsizligiga dasturiy ta’minotning siyosatlari, metodlari, muolajalari, tashkiliy tuzilmalari va dasturiy ta’minot funksiyalari tomonidan taqdim etilishi mumkin bo‘lgan axborot xavfsizligini boshqarish bo'yicha tadbirlaming tegishli kompleksini amalga oshirish yo‘li bilan erishiladi. Ko‘rsatilgan tadbirlar tashkilotning axborot xavfsizligi maqsadlariga erishishini ta’minlashi kerak.

Axborot xavfsizligining zarurati. Axborot va uni saqlab turuvchi jarayonlar, axborot tizimlari va tarmoq infratuzilmasi biznesning bebaho aktivlari boiib hisoblanadi. Axborot xavfsiligini aniqlash, ta’minlash, saqlab turish va yaxshilash tashkilotning raqobatbardoshliligi, qadrliligi, daromadliligi, qonun hujjatlariga muvofiqligini va ishbilarmonlik obro‘sini ta’minlashda katta ahamiyatga ega.

Tashkilotlar, ulaming axborot tizimlari va tarmoqlar xavfsizlikning turli kompyuter firibgarligi, ayg‘oqchilik, zararkunandalik, vandalizm, yong‘inlar yoki suv toshqinlari kabi tahdidlar bilan ko‘proq to‘qnashmoqdalar. Zaraming bunday kompyuter viruslari, kompyutemi buzib ochish va «xizmat ko‘rsatishdan bosh tortish» kabi hujumlar manbalari keng tarqalmoqda, tajovuzkor bo‘lib bormoqda va ko‘proq mahorat bilan shakllanmoqda.

Axborot xavfsizligi biznesning jamoat va xususiy sektorida, shuningdek, kritik infratuzilmalami muhofaza qilishda muhim.

Axborot xavfsizligi ikkala sektorda ham yordam berishi kerak, masalan, elektron hukumatni yoki elektron biznesni joriy qilishda tegishli xavflardan mustasno bo‘lish yoki ulami kamaytirish uchun.

Umumiy foydalanishdagi tarmoqlaming va xususiy tarmoqlaming birgalikda ishlashi, shuningdek, axborot resurslaridan birgalikda foydalanishi axborotdan foydalanishni boshqarishni qiyinlashtiradi.

Ma’lumotlarga taqsimlab ishlov berishdan foydalanish tendensiyasi markazlashtirilgan nazorat samaradorligini susaytiradi.

Ko‘pgina axborot tizimlarini loyihalashda xavfsizlik masalalari e’tiborga olinmas edi. Texnik vositalar bilan erishilishi mumkin bo‘lgan xavfsizlik

darajasi bir qator cheklashlarga ega, binobarin, tegishli boshqaruv vositalari va protseduralar bilan ta’minlanishi kerak. Axborot xavfsizligini boshqarish bo‘yicha zarur tadbirlami tanlash puxtalik bilan rejalashtirish va detallashtirishni talab qiladi.

Axborot xavfsizligini boshqarish, kamida tashkilot barcha xodimlarining ishtirok etishiga muhtoj. Shuningdek, yetkazib beruvchilar, mijozlar yoki aksiyadorlaming ishtirok etishi ham talab qilinishi mumkin. Bundan tashqari, begona tashkilot mutaxassislarining maslahatlari kerak bo‘lib qolishi mumkin.

Agar axborot xavfsizligi sohasini boshqarish bo‘yicha tadbirlar axborot tizimini loyihalashtirish bosqichida texnik topshiriqqa kiritilsa, ancha arzonga tushadi va samaraliroq bo‘ladi.

Axborot xavfsizligi talablarini aniqlash. Tashkilot o‘zining axborot xavfsizligiga bo‘lgan talablarini quyidagi uchta muhim omilni hisobga olib, aniqlashi muhim:

- biznesning global strategiyasi va tashkilotning maqsadlarini e’tiborga olib, tashkilotda olingan xavflami baholash yordamida tashkilot aktivlariga tahdidlar aniqlanadi, tegishli aktivlaming zaifligi va tahdidlar paydo bo‘lish ehtimoli, shuningdek, kelib chiqishi mumkin bo‘lgan oqibatlar baholanadi;

- tashkilot, uning savdo sheriklari, pudratchilar va xizmatlami yetkazib beruvchilar, qoniqtirilishi kerak bo‘lgan yuridik talablar, qonun hujjatlarining talablari, tartibga soluvchi va shartnomaviy talablar, shuningdek, ushbu tomonlaming ijtimoiy madaniy muhiti boshqa omil bo‘lib hisoblanadi;

- o‘zining ishlashini ta’minlash uchun tashkilot tomonida ishlab chiqilgan prinsiplar, maqsadlar va talablaming maxsus to‘plami yana bir omil bo‘lib hisoblanadi.

Axborot xavfsizligi xavflarini baholash. Axborot xavfsizligiga qo‘yiladigan talablar xavflami muntazam baholash yordamida aniqlanadi. Axborot xavfsizligini boshqarish bo'yicha tadbirlarga ketgan sarf-xarajatlar axborot xavfsizligining buzilishi natijasida tashkilotga yetkazilishi mumkin bo'lgan zarar miqdoriga mutanosib bo‘lishi lozim.

Ushbu baholashning natijalari axborot xavfsizligi bilan bog'liq xavflami boshqarish sohasida aniq choralar va ustuvorliklami belgilashga, shuningdek, ushbu xavflami minimumga keltirish maqsadida axborot xavfsizligini boshqarish bo'yicha tadbirlami joriy qilishga yordam beradi. Mavjud tadbirlaming samaradorliligiga ta’sir ko'rsatishi mumkin bo'lgan har qanday o'zgarishlami hisobga olish uchun xavflar tahlilini vaqti-vaqti bilan takrorlab turish kerak.

Axborot xavfsizligini boshqarish bo'yicha tadbirlarni tanlash. Axborot xavfsizligiga qo'yiladigan talablar belgilanganidan va xavflar aniqlanganidan so'ng xavflami qabul qilsa bo'ladigan darajagacha pasayishini ta’minlaydigan, axborot xavfsizligini boshqarish bo'yicha tadbirlami tanlash va joriy etish kerak. Ushbu tadbirlar ushbu standartdan, boshqa manbalardan tanlab olinishi, shuningdek, axborot xavfsizligini boshqarish bo'yicha tashkilotning o'ziga xos ehtiyojlarini qondiradigan tadbirlar ishlab chiqilishi mumkin. Axborot xavfsizligini boshqarish bo'yicha tadbirlami tanlash xavflami qabul qilish mezonlariga, xavflarga baho berish variantlariga asoslangan tashkiliy qarorlarga va xavflami tashkilotda qabul qilingan boshqarishga umumiy yondashishga bogiiq. Ushbu tanlovni tegishli milliy va xalqaro qonun hujjatlari va normalar bilan muvofiqlashtirish kerak.

Ushbu standartda keltirilgan axborot xavfsizligini boshqarish bo'yicha ba’zi tadbirlar axborot xavfsizligini boshqarish uchun amal qilinadigan prinsiplar sifatida qabul qilinishi va ko'pgina tashkilotlar uchun qo'llanishi mumkin. Bunday tadbirlar quyiroqda «Axborot xavfsizligini joriy qilish uchun tayanch nuqta» sarlavhasi ostida batafsilroq ko‘rib chiqiladi.

Axborot xavfsizligini joriy qilish uchun tayanch nuqta. Axborot xavfsizligini boshqarish bo‘yicha alohida tadbirlar axborot xavfsizligini boshqarish uchun amal qilinadigan prinsiplar sifatida qabul qilinishi va uni joriy qilish uchun tayanch nuqta bo‘lib xizmat qilishi mumkin. Bunday tadbirlar qonun hujjatlarining asosiy talablariga asoslanadi yoki axborot xavfsizligi sohasida umumiy qabul qilingan amaliyot sifatida qabul qilinishi mumkin.

Qonunchilik nuqtayi nazaridan axborot xavfsizligini boshqarish bo‘yicha asosiy choralar quyidagilar hisoblanadi:

- ma’lumotlami muhofaza qilish va shaxsiy axborotning konfidensialligi;
- tashkilot hujjatlarini muhofaza qilish;
- intellektual mulkka egalik qilish huquqi.

Axborot xavfsizligi sohasida umumiy qabul qilingan amaliyot sifatida hisoblangan axborot xavfsizligini boshqarish bo‘yicha tadbirlar quyidagilami o‘z ichiga oladi:

- axborot xavfsizligi siyosatini hujjatlashtirish;
- axborot xavfsizligini ta’minlash bo‘yicha majburiyatlami taqsimlash;
- axborot xavfsizligi qoidalariga o‘qitish;
- ilovalardagi axborotga to‘g‘ri ishlov berish;
- texnik zaifliklami boshqarish strategiyasi;
- tashkilotning uzluksiz ishini boshqarish;
- axborot xavfsizligi mojarolarini va takomillashtirish boshqarish.

Sanab o‘tilgan tadbirlami ko‘pgina tashkilotlar va axborot muhiti uchun qo'llasa bo‘ladi. Ushbu standartda keltirilgan barcha tadbirlar muhim hisoblansa ham, qandaydir choraning o‘rinli bo‘lishi tashkilot to‘qnash keladigan muayyan xavflar nuqtayi nazaridan belgilanishi kerak. Demak, yuqorida ta’riflangan yondashish axborot xavfsizligini ta’minlash bo‘yicha tadbirlami joriy qilish uchun tayanch nuqta bo‘lib hisoblanishiga qaramay, u xavflami baholashga asoslangan axborot xavfsizligini boshqarish bo‘yicha tadbirlami tanlashning o‘mini bosmaydi.

Muvaffaqiyatning eng muhim omillari. Tajriba shuni ko‘r-
satadiki, tashkilotda axborot xavfsizligini ta’minlash bo‘yicha tadbirlami muvaffaqiyatli joriy qilish uchun quyidagi omillar hal qiluvchi hisoblanadi:

- axborot xavfsizligi maqsadlari, siyosatlari va muolajalarining biznes maqsadlariga muvofiqligi;
- xavfsizlik tizimini joriy qilish, madadlash, monitoringini o‘t-

kazish va modemizatsiya qilishga yondashishning korporativ mada-
niyat bilan muvofiqligi;

- rahbariyat tomonidan real qo‘llab-quwatlash va manfaat-
dorlik;

- xavfsizlik talablarini, xavflami baholash va xavflami bosh-
qarishni aniq tushunish.

Tashkilotga tegishli qo ‘llanmalarni ishlab chiqish.Ushbu standart tashkilotning muayyan ehtiyojlariga kerakli qo‘llanmalar ishlab chiqish uchun tayanch nuqta sifatida baholanishi kerak. Ushbu standartda keltirilgan yo‘riqnomalar va tadbirlaming hammasi ham qo‘llashga yaroqli bo‘lavermaydi.

Bundan tashqari, ushbu standartga kiritilmagan qo‘shimcha choralar kerak bo‘lib qolishi mumkin. Bu holda auditorlar va biznes bo‘yicha sheriklar tomonidan o‘tkaziladigan muvofiqlik tekshimvini yengillashtiradigan, bir vaqtda bir necha tomondan qilingan havolalaming saqlanishi foydali bo‘lishi mumkin.

O‘zDStIS0/IEC 27005:2013 - “Axborot texnologiyasi. Xavfsizlikni ta’minlash usullari. Axborot xavfsizligi risklarini boshqarish”.

Ushbu standart tashkilotda axborot xavfsizligi risklarini boshqarish bo‘yicha tavsiyalami o‘z ichiga oladi.

Ushbu standart 0 ‘z DSt ISO/IEC 27001 da belgilangan umumiy konsepsiyalami qo‘llab-quwatlaydi va risklami boshqarish bilan bog‘liq yondashuv asosida axborot xavfsizligini aynan bir xil ta’minlashni amalga oshirish uchun mo‘ljallangan.

Ushbu standartni to‘la tushunib etish uchun O‘z DSt ISO/IEC 27001 va O‘z DSt ISO/IEC 27002da bayon qilingan konsepsiyalami, modellami. jarayonlami va terminologiyani bilish zarur.

Ushbu standart tashkilotning axborot xavfsizligini obro‘sizlantirishi mumkin bo‘lgan risklami boshqarishni amalga oshirishni rejalashtiradigan barcha turdagi tashkilotlar (masalan, tijorat korxonalari, davlat muassasalari, notijorat tashkilotlar) uchun qo‘llaniladi.

Ushbu standartda quyidagi standartlarga bo‘lgan havolalardan foydalanilgan:

O‘z DSt ISO/IEC 27001:2009 Axborot texnologiyalari. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarish tizimlari. Talablar.

O‘z DSt ISO/IEC 27002:2008 Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari.

Ushbu standartdan foydalanilganda havola qilingan standartlaming O‘zbekiston hududida amal qilishini joriy yilning 1-yanvarigacha bo‘lgan holati bo‘yicha tuzilgan standartlaming tegishli ko‘rsatkichi va joriy yilda e’lon qilingan tegishli axborot ko‘rsatkichlari bo‘yicha tekshirish maqsadga muvofiqdir. Agar havola qilingan hujjat almashtirilgan (o‘zgartirilgan) bo‘lsa, u holda ushbu standartdan foydalanilganda almashtirilgan (o‘zgartirilgan) standartga amal qilish lozim. Agar havola qilingan hujjat almashtirilmasdan bekor qilingan bo‘lsa, u holda unga havola qilingan qoida ushbu havolaga taalluqli bo‘lmagan qismida qo‘llaniladi.

O‘zDStIS0/IEC 27006:2013 - “Axborot texnologiyasi.

Xavfsizlikni ta’minlash usullari. Axborot xavfsizligini bpshqarish tizimlarining auditi va ularni sertifikatlashtirish organlariga qo‘yiladigan talablar”.

O‘z DSt 180ЯEC 17021 - bu tashkilotlami boshqarish tizimlarining auditini va sertifikatlashtirilishini amalga oshiradigan organlar uchun mezonlami o‘matadigan standartdir. Agar bu organlar O‘z DSt 180ЯEC 27001 ga muvofiq, axborot xavfsizligini boshqarish tizimlari (AXBT)ning sertifikatlashtirilishini va auditini o‘tkazish maqsadida, O‘z DSt ISO/IEC 17021 muvofiq keladigan organlar sifatida akkreditlanadigan bo‘lsa, u holda O‘z DSt ISO/IEC 17021 ga qo‘llanma va qo‘shimcha talablar zarur. Ular ushbu standartda taqdim etilgan.

Ushbu standartning matni O‘z DSt ISO/IEC 17021 strukturasini takrorlaydi, AXBT uchun spetsifik bo‘lgan qo‘shimcha talablar va AXBTni sertifikatlashtirish uchun O‘z DSt ISO/IEC 17021 ni qo‘llash bo'yicha qo‘llanma esa, «AX» abbreviaturasi bilan belgilanadi.

«Kerak» atamasidan ushbu standartda O‘z DSt ISO/IEC 17021 va O‘z DSt ISO/IEC 27001 talablarini aks ettirgan holda majburiy boigan shartlarni ko‘rsatish uchun foydalaniladi. «Zarur» atamasidan, garchi bu talablami qoilash bo‘yicha qo‘llanma bo‘Isa ham, sertifikatlashtirish organi tomonidan qabul qilinishi ko‘zda tutiladigan shartlarni belgilash uchun foydalaniladi.

Ushbu standartning maqsadi - akkreditlash organlariga sertifikatlashtirish organlarini baholashlari shart bo‘lgan standartlarni yanada samarali qo‘llash imkoniyatini berishdir. Bu kontekstda sertifikatlashtirish organining qo‘llanmadan har qanday chetga chiqishi istisno hisoblanadi. Bunday chetga chiqishlarga har bir holat alohida ко‘rib chiqilishi asosidagina ruxsat berilishi mumkin, bunda sertifikatlashtirish organi akkreditlash organiga bu istisno qandaydir ekvivalent tarzda O‘z DSt ISO/IEC 17021, O‘z DSt ISO/IEC 27001 talablarining tegishli bandini va ushbu standart talablarini qanoatlantirishini isbotlab berishi kerak.

Izoh - ushbu standartda «boshqarish tizimi» va «tizim» atamalaridan bir-birini almashtirib foydalaniladi. Boshqarish tizimlari ta’rifini O‘z DSt ISO 9000 da topish mumkin. Bu xalqaro standartda foydalanilayotgan boshqarish tizimini axborot texnologiyalari tizimlari kabi tizimlaming boshqa turlari bilan adashtirmaslik zarur.

ISO/IEC 15408-1-2005 - “Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari va vositalari. Axborot texnologiyalari xavfsizligini baholash mezonlari”.

ISO/IEC 15408-2005 xalqaro standarti ISO/IEC JTC 1 «Axborot texnologiyalari» birgalikdagi texnik qo‘mita, SC 27 «AT xavfsizligini ta’minlash metodlari va vositalari» kichik qo‘mita tomonidan tayyorlangan. ISO/IEC 15408-2005 ga o‘xshash matn «Axborot texnologiyalari xavfsizligini baholashning umumiy mezonlari» 2.3-versiya (2.3 UM deb nomlanadi) sifatida «Umumiy mezonlar» loyihasining homiy tashkilotlari tomonidan e’lon qilingan.

Standartning ikkinchi tahriri texnik jihatdan, qayta ishlashga to‘g‘ri kelgan birinchi tahrir (ISO/IEC 15408:1999)ni bekor qiladi va uni almashtiradi.

Axborot xavfsizligi sohasiga oid me’yoriy hujjatlar

RH 45-215:2009 - Rahbariy hujjat. Ma’lumotlar uzatish tarmog‘ida axborot xavfsizligini ta’minlash to‘g‘risida Nizom. Ushbu hujjat N 100:2002 «Ma’lumotlar uzatish milliy tarmog‘ida axborot xavfsizligini ta’minlash to‘g‘risida nizom» o‘miga amalga kiritilgan bo‘lib, ma’lumotlar uzatish tarmog‘ida (MUT) axborot xavfsizligini ta’minlash bo‘yicha asosiy maqsadlar, vazifalar, funksiyalar va tashkiliy-texnik tadbirlami belgilaydi.

Nizom xonaning muhofaza qilinishini tashkil qilish, tarmoq komponentlarining saqlanganligi va fizik yaxlitligini ta’minlash, tabiiy ofatlar, energiya ta’minoti tizimida ishlamay qolishlardan muhofaza qilish masalalari, xodimlar va MUT mijozlarining shaxsiy xavfsizligini ta’minlash bo‘yicha choralari, shuningdek, Tezkor- qidiruv tadbirlar tizimini (TQTT) tashkil qilish masalalari va uning ishlashini tartibga solmaydi.

Ushbu hujjat talablari MUT normal ishlashini kuzatish, xizmat ko‘rsatish va ta’minlash ishlarini amalga oshiruvchi mutasaddi qo‘mita va vazirliklaming barcha korxonalariga taalluqlidir.

Ushbu Nizomga axborot muhofazasi bo‘yicha xizmatlar ro‘yxati o‘zgarganda yoki MUTni modemizatsiya qilish va rivojlantirishda o‘zgartirish hamda qo‘shimchalar kiritilgan bo‘lishi mumkin.

Ushbu Nizom axborotni muhofaza qilishning huquqiy, tashkiliy, rejimli, texnik, dasturiy va boshqa metodlari hamda vositalaridan foydalanish, shuningdek, axborot xavfsizligini ta’minlash qismida amalga oshirilgan choralaming samaradorligi uchun har tomonlama uzluksiz nazorat qilishni amalga oshirish asosida MUTda axborot xavfsizligini ta’minlash ko‘zda tutiladi.

MUTda axborot xavfsizligini ta’minlash AXTTni yaratish yo‘li bilan kompleksli va MUT hayotiy siklining barcha bosqichlarida tashkiliy-texnik tadbirlami doimo o‘tkazish bilan hal etiladi.

MUT AXTT samarali ishlashini ta’minlash funksiyalari korxona rahbariga bevosita bo‘ysunadigan korxonaning MUT axborot xavfsizligini ta’minlash xizmati (bo‘limi)gayuklatiladi.

Korxonaning MUT axborot xavfsizligini ta’minlash xizmati (bo‘limi) o‘z faoliyatida O‘zbekiston Respublikasining qonun hujjatlari va normativ hujjatlari, Prezident farmonlari, O‘zbekiston Respublikasi Vazirlar Mahkamasining qarorlari, Agentlikning normativ-huquqiy hujjatlari, korxona rahbarlarining buyruqlari va farmoyishlari hamda ushbu Nizomga amal qiladi.

Axborot xavfsizligini ta’minlash xizmati (bo‘limi) MUT serverlarida saqlanadigan va MUT telekommunikatsiya kanallari va vositalari bo‘ylab uzatiladigan, agar bu shartnomada ko‘zda tutilgan bo‘Isa, abonentlar axborotining konfidensialligi, yaxlitligi va undan erkin foydalanish uchun javobgar bo‘ladi.

Axborot xavfsizligini ta’minlash xizmati (bo‘limi) abonent terminallarida saqlanadigan abonent axborotining konfidensialligi, yaxlitligi va undan erkin foydalanish uchun javobgar bo‘lmaydi.

Axborot xavfsizligini ta’minlash xizmati (bo‘limi) viruslar bilan zararlangan hamda zararli dasturlami o‘z ichiga olgan foydalanuvchi va abonentlaming axborot resurslari (MUT serverlarida joylashadigan va saqlanadigan, MUT telekommunikatsiya kanallari va vositalari bo‘ylab uzatiladigan), shuningdek, O‘zbekiston Respublikasining amaldagi qonun hujjatlari bilan taqiqlangan axborot resurslari tarqalishining oldini olish bo‘yicha choralami qabul qilish huquqiga ega.

Abonentlarga axborotni muhofaza qilish bo‘yicha qo‘shimcha xizmatlarni taqdim etish shartnomada bayon etiladi.

MUT foydalnuvchilari va abonentlari o‘z darajasida axborotni muhofaza qilish tizimlari yoki vositalarini qo‘llash (ulardan foydalanish) huquqiga ega.

RH 45-185:2011 - Rahbariy hujjat. Davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta’minlash dasturini ishlab chiqish tartibi. Ushbu hujjat RH 45-185:2006 hujjati o‘miga amalga kiritilgan bo‘lib, davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta’minlash dasturlarini ishlab chiqish tartibini belgilaydi.

Hujjat axborot xavfsizligini ta’minlash dasturlari doirasida ishlab chiqiladigan chora-tadbirlaming maqsadlari, vazifalari, tuzilmasi va ro‘yxatiga qo‘yiladigan namunaviy talablami belgilaydi.

Ushbu hujjat talablari 0 ‘zbekiston Respublikasining davlat hokimiyati va boshqaruv organlariga taalluqli, shuningdek, ushbu organlaming axborot xavfsizligini ta’minlash dasturlarini yaratish uchun asos bo‘lib hisoblanadi.

Ushbu hujjatni ishlab chiqish va joriy etishdan maqsad:

- axborot xavfsizligini tahdidlardan muhofaza qilish bo‘yicha choralaming adekvatligiga erishish;

- davlat hokimiyati va boshqaruv organlarining ishlaridagi barqarorlik darajasini oshirish;

- xavfsizlik mojarolaridan yuzaga kelgan ziyon darajasini pasaytirish;

- axborot xavfsizligi infratuzilmasini yaratish;

- boshqa tashkilotlaming foydalanish xavfsizligini ta’minlash;

- boshqa tashkilotlaming ulanishi bilan bog'liq bo‘lgan ehtimoliy xavflami identifikatsiya qilish;

- axborot resurslariga mas’ul shaxslami belgilash;

- davlat hokimiyati va organlari faoliyatida davlat axborot resurslarining ochiqligi va ommabopligini ta’minlash, axborot va kommunikatsiya texnologiyalaridan foydalanish asosida davlat hokimiyati va organlari bilan fuqarolar o‘rtasidagi samarali o‘zaro hamkorlik uchun, ulaming axborot xavfsizligini ta’minlagan holda, sharoitlar yaratish;

- muhofaza qilingan axborot va kommunikatsiya texnologiyalaridan foydalanish asosida davlat organlari faoliyatini takomillashtirish;

- davlat organlarida AX bo‘yicha mutaxassislami tayyorlash tizimini rivojlantirishdir.

Ushbu rahbariy hujjatning asosiy maqsadi - davlat hokimiyati va boshqaruv organlarini AX tahdidlaridan, ularga mumkin bo‘lgan zarar yetkazilishidan muhofaza qilinishini ta’minlashdir.

Rahbariy hujjatning asosiy vazifasi davlat organlarining axborot xavfsizligini ta’minlash dasturini belgilash hisoblanadi.

RH 45-193:2007 - Rahbariy hujjat. Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnikmaydonlarning axborot xavfsizligini ta’minlash darajasini aniqlash tartibi. Ushbu hujjat davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta’minlash darajasini aniqlashning namunaviy tartibini belgilaydi.

Ushbu hujjat talablari davlat organlarining saytlari uchun xosting xizmatlarini taqdim etuvchi barcha xo‘jalik yurituvchi subyektlar tomonidan qo‘llanilishi majburiydir.

Hujjatda davlat organlarining saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini (AX) ta’minlash darajasini belgilash, axborot resurslarini yaratish va foydalanishning barcha aspektlarini hisobga olgan holda ushbu vazifaga kompleks yondoshilishiga asoslanadi. Buning uchun tashkiliy, texnik va dasturiy muhofaza qilish choralarini, xavf-xatarlar va axborotning muhofazalanganlik darajasini baholash va prognoz qilish bo'yicha tadbirlami doimo rivojlanib borayotgan yagona tizimga umumlashtirish talab etiladi.

Axborotni muhofaza qilish o‘z ichiga AXni ta’minlashga qaratilgan chora-tadbirlar kompleksini oladi: ma’lumotlami kiritish, saqlash, qayta ishlash va uzatish uchun foydalaniladigan axborot va resurslaming butunligi, ulardan foydalana olishlik, zarur holda, konfidensialligini qo‘llab-quwatlash.

Axborotni muhofaza qilish maqsadi quyidagilar hisoblanadi:

- axborotning chiqib ketishi, o‘g‘irlanishi, yo‘qolishi, buzilishi, qalbakilashtirilishini oldini olish;

- axborotni yo‘q qilish, modifikatsiya qilish, buzish, nusxa ko‘chirish, blokirovka qilish bo‘yicha ruxsat etilmagan harakatlaming oldini olish;

- axborot resurslari va axborot tizimlariga (AT) noqonuniy aralashishning boshqa shakllarini oldini olish.

TSt 45-010:2010 - Tarmoq standard. Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta’riflar.

Ushbu tarmoq standard 0 ‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi davlat standartlashtirish, metrologiya va sertifikatlashtirish markazi (« 0 ‘zdavstandart») tomonidan 2002-yil 6-avgustda 112/066-son bilan ro‘yxatga olingan TSt 45.010: «Отраслевой стандарт. Информационная безопасность в сфере связи и информатизации. Термины и определения» o‘miga amalga kiritilgan bo‘lib, aloqa va axborotlashtirish sohasida axborot xavfsizligidagi asosiy atama va ta’riflami belgilaydi.

Belgilangan atamalar barcha turdagi hujjatlarda qo‘llanilishi uchun majburiydir. Standartda maTumotnoma sifatida standartlashtirilgan atamalarning xorijiy ekvivalenti rus (R) va ingliz (E) tillarida keltirilgan.

Standartdan foydalanish qulayligi uchun atama moddalarining tegishli raqamlarini ko‘rsatgan holda o‘zbek, rus va ingliz tillaridagi atamalarni o‘z ichiga olgan alifbo ko‘rsatkichi keltirilgan.