TASHKILOTLARDA AXBOROT XAVFSIZLIGI AUDITINING BOSQICHLARI VA SXEMASI

Xolimtayeva Iqbol
TATU



Annotatsiya

Ushbu maqolada tashkilotda axborot xavfsizligi auditining bosqichlari va sxemasi hamda, audit o'tkazishda belgilab olinishi kerak bo'lgan talablar keltirib o'tilgan.

Kalit so'zlar; axborot xavfsizligi auditi, axborot-texnologik ta'sir (ATT) va axborot-psixologik ta'sir (APT)

Аннотация

В данной статье упомянуты этапы и схема проведения аудита информационной безопасности в организации, а также требования, которые должны быть определены в ходе аудита.

Ключевые слова: аудит информационной безопасности, информационно-технологическое воздействие (АТТ) и информационно-психологическое воздействие (АПТ)

Annotation

In this article, the stages and scheme of the information security audit in the organization and the requirements that should be determined during the audit are mentioned.

Keywords: information security audit, information-technological impact (ATT) and information-psychological impact (APT)

Hozirgi vaqtda tashkilotlarda axborot xavfsizligi darajasini tahlil qilish uchun foydalaniladigan auditning aniq ta'rifi mavjud emas. Turli manbalarda turli xil ta'riflarni topishingiz mumkin. Ulardan ba'zilari quyida keltirib o'tilgan.

Audit - bu tashkilot faoliyatining har qanday sohasini mustaqil, neytral nazorat qilish shaklidir.

Audit - qo'yilgan maqsadlarga erishish uchun dastlabki ma'lumotlarni qayta ishlash uchun foydalaniladigan maxsus texnikalar (usullar) yig'indisidir. Auditorlik tekshiruvlarining turli usullari odatda to'rt guruhga birlashtiriladi: obyektlarning haqiqiy holatini aniqlash, tahlil qilish, baholash va texnik takliflarni ishlab chiqarish .

Audit - bu belgilangan talablar qay darajada bajarilganligini aniqlash uchun hujjatlarni olish, faktlar yoki boshqa tegishli ma'lumotlarni qayd etish va ularni xolisona baholashning tizimli, mustaqil va hujjatlashtirilgan jarayonidir.

Axborot tizimlari auditi - bu kompaniya tomonidan foydalaniladigan axborot tizimlari, xavfsizlik tizimlari, tashqi muhit bilan aloqa tizimlari, korporativ tarmoqning kompaniyada sodir bo'layotgan biznes jarayonlariga muvofiqligini, shuningdek, xalqaro standartlarga muvofiqligini tekshirish, ularning faoliyatidagi nosozliklar riskini baholash.

Axborot xavfsizligi auditi - avtomatlashtirilgan axborot tizimining axborot xavfsizligi holatini baholash va axborot tizimining axborot resurslarini axborot xavfsizligi tahdidlaridan

himoya qilishni ta’minlashga qaratilgan tashkiliy chora-tadbirlar va dasturiy-texnik vositalar majmuasidan foydalanish bo‘yicha tavsiyalar ishlab chiqish faoliyati.

Axborot xavfsizligi auditi - bu xavfsizlikning ma’lum mezonlari va ko‘rsatkichlariga muvofiq kompaniyaning axborot xavfsizligining joriy holatiga ob’ektiv sifat va miqdoriy baholarni olishning tizimli jarayoni .

Axborot xavfsizligi auditi - bu tekshirilayotgan ob’ektning axborot xavfsizligi holatini va uning audit mezonlariga muvofiqlik darajasini baholash maqsadida mustaqil ekspertlar tomonidan amalga oshiriladigan tashkiliy-texnik tadbirlar majmui.

Yuqorida keltirilgan ta’riflarni tahlil qilish natijasida quyidagi ta’rif keltirildi, mazkur ta’rif audit jarayonini eng umumiy va batafsil aks ettiruvchi ta’rif hisoblanadi. Ushbu ta’rif ISO 19011 - 2011 standartlariga ham mos keladi.

1-ta’rif. Axborot xavfsizligi auditi - bu tekshirilayotgan ob’ektning axborot xavfsizligi holatini baholash va audit mezonlariga muvofiqlik darajasini aniqlash uchun ularni ob’ektiv tahlil qilishning tizimli, mustaqil va hujjatlashtirilgan jarayoni.

Yuqoridagi ta’riflardan auditning umumiy va xususiy maqsadlari haqida xulosa chiqarish mumkin.

Auditning umumiy maqsadi axborot tizimining axborot xavfsizligi darajasiga qo‘yiladigan talablarni belgilovchi mezonlarga muvofiqligini tekshirish va baholashdan iborat.

Auditning alohida maqsadlari:

- xavfsizlikka tahdidlarni amalga oshirish imkoniyati bilan bog‘liq xavflarni tahlil qilish;
- joriy xavfsizlik darajasini baholash;
- xavfsizlik quyi tizimidagi zaifliklarni va tizimdagi to‘siqlarni aniqlash;
- tizimning axborot xavfsizligi sohasidagi amaldagi standartlarga, shuningdek, xavfsizlik siyosatiga muvofiqligini baholash;
- mavjud himoya tizimining samaradorligini oshirishga qaratilgan chora-tadbirlar majmui bo‘yicha tavsiyalarni shakllantirish.

Auditning maqsadlarini quyidagilarga bo‘lish mumkin :

- profilaktika - tahdidlar va zaifliklarni faol aniqlashga, shuningdek, axborot xavfsizligi xodisalarini (intsidentlarining) oldini olish choralarini ishlab chiqishga qaratilgan;
- aniqlash - axborot xavfsizligi xodisalari paytida yoki undan keyin himoya tizimining yangi tahdidlari va zaif tomonlarini mavjud xususiyatlarini aniqlashga qaratilgan;
- tuzatuvchi - yangi aniqlangan tahdidlar va zaifliklarni hisobga olgan holda, axborot xavfsizligi hodisalaridan keyin mavjud himoya tizimining samaradorligini oshirish bo‘yicha chora-tadbirlar majmuini ishlab chiqishga qaratilgan.

Hozirgi vaqtda axborot xavfsizligi auditi quyidagi ob’ektlarga nisbatan amalga oshirilmoqda :

- tashkilotlar;
- biznes jarayonlari;
- boshqaruv tizimlari (boshqaruv);
- axborot tizimlari;
- texnik tizimlar.

Audit shakllari esa quyidagilar hisoblanadi :

- tashkiliy-me'yoriy - axborot xavfsizligini ta’minlash bo‘yicha tashkiliy chora-tadbirlar va ushbu sohadagi normativ hujjatlar tahlil qilinganda;
- texnik - axborot xavfsizligini ta’minlashning texnik vositalari va usullari tahlil qilinganda.

Audit - bu tekshirilayotgan ob’ektning axborot xavfsizligi holatini baholashning eng umumiy shakli. Audit manfaatdor tomonlar va me'yoriy hujjatlar tomonidan ishlab chiqilgan har qanday talablarga muvofiqligi uchun amalga oshiriladi.

Audit tekshirilayotgan ob’ektning quyi tizimlari va jarayonlarini sinovdan o‘tkazishning turli usullarini o‘tkazishni, hujjatlarni va boshqa ma’lumot manbalarini tahlil qilishni, mutaxassislar bilan suhbatlashishni va boshqalarni o‘z ichiga olishi mumkin.

Audit bosqichlari

Axborot xavfsizligi auditini o‘tkazishda odatda quyidagi bosqichlar ketma-ketligida amalga oshiriladi :

1. tayyorgarlik bosqichi:

- audit ob’ektini tanlash;
- audit mezonlari va usullarini tanlash;
- audit vositalari va usullarini tanlash;
- auditorlar jamoasini shakllantirish;
- auditning hajmi va ko‘lamini aniqlash, uni o‘tkazish muddatlarini belgilash.

2. asosiy bosqich:

- tekshirilayotgan ob’ektning axborot xavfsizligi holatini tahlil qilish;
- statistik ma’lumotlarni va zaifliklar, tahdidlarni instrumental o‘lchash natijalarini ro‘yxatga olish, to‘plash va tekshirish;
- tekshirish natijalarini baholash;
- audit ob’ektining alohida elementlari va axborot xavfsizligining turli jihatlari bo‘yicha audit natijalari to‘g‘risida hisobot sh.

3. yakuniy bosqich:

- yakuniy hisobotni tayyorlash;
- mavjud himoya tizimining samaradorligini oshirishga qaratilgan chora-tadbirlar kompleksi bo‘yicha tavsiyalar shakllantirish;
- axborot xavfsizligini ta’minlashdagi zaiflik va kamchiliklarni bartaraf etish bo‘yicha chora-tadbirlar rejasini ishlab chiqish.

Auditning ketma-ketligi, ayniqsa axborot xavfsizligi standartlarini tahlil qilish va muvofiqlikni baholashga asoslangan yondashuvlar kabi ko‘plab adabiyotlarda yetarlicha batafsil tavsiflanganligi sababli mazkur ishda ularga batafsil to‘xtalib o‘tilmadi.

Audit sxemasi

Auditni o‘tkazish tekshirilayotgan ob’ektni tekshirishning ma’lum bir rasmiy tartibiga rioya qilishni o‘z ichiga oladi. Ushbu jarayon audit ob’ekti va jarayonining oldindan tuzilgan rasmiy tavsiflariga, shuningdek, joriy axborot xavfsizligi tahdidlariga muvofiq amalga oshiriladi:

- audit modeli;
- buzg‘unchi/dushman modeli;
- tahdid modeli;
- audit o‘tkazishga umumiy amaliy yondashuv;
- audit o‘tkazishga umumiy nazariy yondashuv.

Bunday rasmiylashtirishni amalga oshirishda tadqiqotning quyidagi jihatlari belgilanishi kerak :

- tahdid manbalari;
- himoyalangan quyi tizimlar, resurslar, jarayonlar yoki tizimning boshqa elementlari;
- tahdid manbalari va tizimning himoyalangan elementlari o‘rtasidagi aloqalar;
- himoya quyi tizimining tuzilishi va ishlash jarayonlari.

Audit davomida yuqoridagi ob’ektlarning o‘zaro ta’sirining umumiy diagrammasi 1.-rasmda keltirilgan.

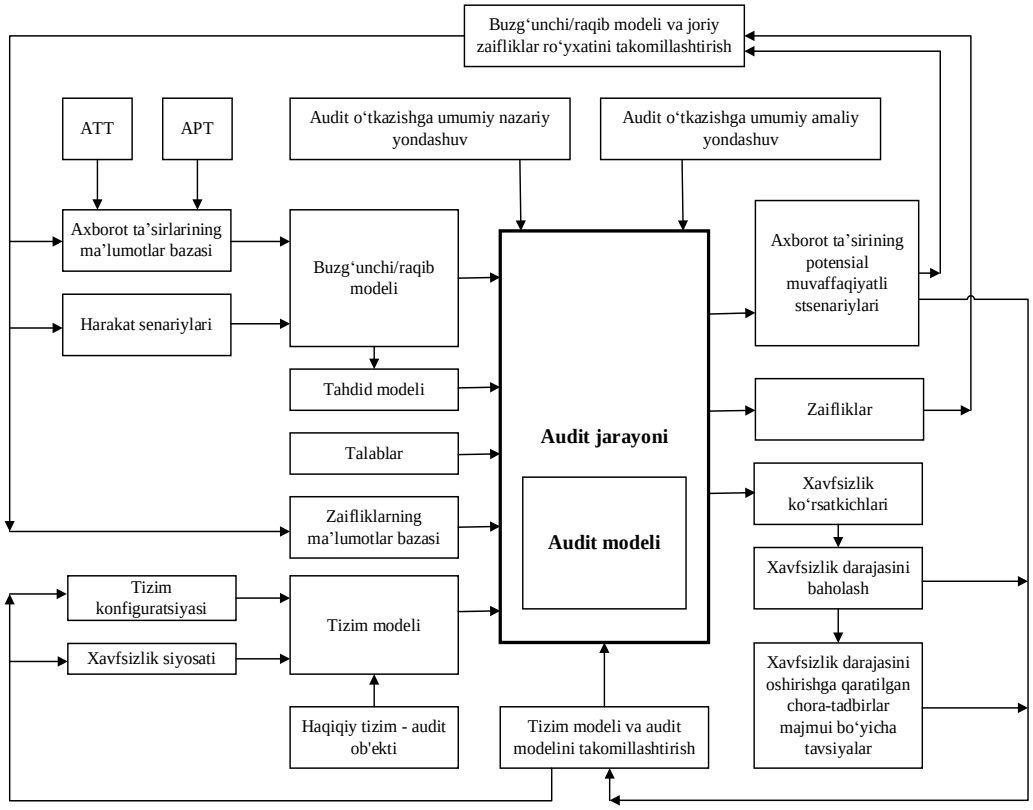
Audit modeli quyidagilarni o‘z ichiga oladi:

- audit ob’ekti;
- audit maqsadlari;
- talablar;
- qo‘llaniladigan amaliy va nazariy yondashuvlar;
- masshtab va chuqurlik;
- ijrochilar;

- auditorlik tekshiruvini o‘tkazish tartibi.

Buzg‘unchi/raqib modeliga quyidagilar kiradi:

- buzg‘unchi/ raqibning rasmiylashtirilgan tavsifi;
- axborot xavfsizligi buzilishi mezonlari;
- buzg‘unchi/raqiblarni toifalash;
- buzg‘unchi/raqiblarnilarning har bir toifasi uchun malaka, imkoniyatlar, mavjud vositalar va axborot ta’siri usullari to‘g‘risidagi taxminlar;
- har bir toifadagi buzg‘unchi/raqiblar uchun harakat senariylari haqidagi taxminlar;
- har bir toifadagi buzg‘unchi/raqiblar uchun tizimga kirishning vakolat darajasi va usullari.



1-rasm. Audit jarayonining diagrammasi

Tahdid modeli quyidagilarni o‘z ichiga oladi :

tahdidlar toifalari:

- foydalanish imkoniyatiga tahdidlar;
- yaxlitlikka tahdid;
- maxfiylikka tahdidlar;

tahdid guruhlari:

- axborotning chiqib ketishi uchun texnik kanallardan foydalanish orqali amalga oshiriladigan tahdidlar;
- axborot-texnologik ta’sir (ATT) vositalari va usullaridan foydalangan holda amalga oshirilgan tahdidlar [1];
- axborot-psixologik ta’sir (APT) yoki ijtimoiy muhandislik vositalari va usullaridan foydalangan holda amalga oshirilgan tahdidlar .

ADABIYOTLAR

1. Sarvar o’g’li, M. S. (2024). DAVLAT BOSHQARUV TIZIMINING VA UNING MOXIYATI. Ta'limning zamonaviy transformatsiyasi, 8(4), 192-196.

2. Махкамов, Ш. (2024). Davlat boshqaruv tizimining vujudga kelishi hamda davlat va uning moxiyati. Новый Узбекистан: наука, образование и инновации, 1(1), 379-382.

3. Pardaboyevich, R. F. (2024). ORGANIZATIONAL-PEDAGOGICAL CONDITIONS FOR THE DEVELOPMENT OF WEB-DESIGN COMPETENCE. PEDAGOG, 7(3), 115-121.

4. Rakhmonkulov, F. P. (2022). Development of web design competence of future IT teachers. In SUSTAINABLE DEVELOPMENT FORUM-2022 (pp. 111-114).
5. Alishev, S. A., & Alishev, A. A. (2023). WORKING WITH STUDENTS'INFORMATION USE OF METHODOLOGICAL FEATURES OF THE DEVELOPMENT OF COMPETENCE. In АКТУАЛЬНЫЕ ВОПРОСЫ СОВРЕМЕННОЙ НАУКИ (pp. 253-255).
6. Bobobekov, S. R. (2022). Advantages of using cloud services to monitor student learning during the teaching process. Open Access Repository, 8(7), 5-8.