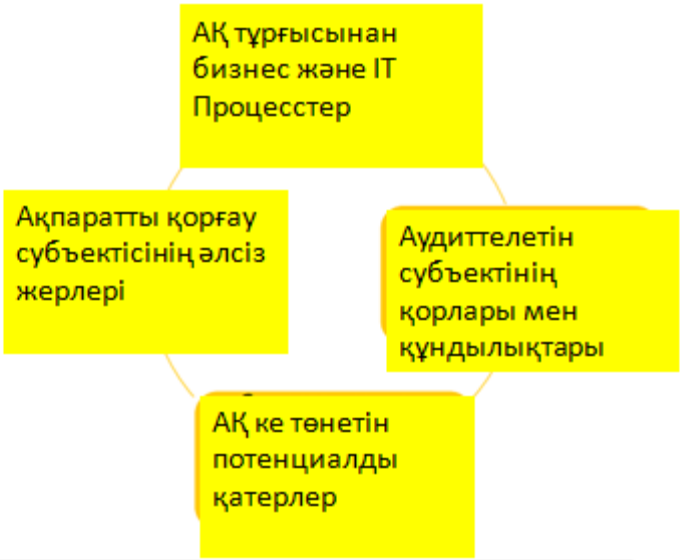
12-дәріс. АЖ қауіпсіздігінің аудиті

Лекция мақсаты - ақпараттық қауіпсіздік аудиттерінің мақсаттары, оларды типтері бойынша жіктеу, жұмыстың болжамды нәтижелері, сондай-ақ барлық негізгі кезеңдер бойынша аудит жүргізу процесін егжей-тегжейлі меңгерту.

Сонымен аудиттің мақсаттары мыналар болуы мүмкін:

❑кәсіпорынның ақпараттық ресурстарының қорғалу дәрежесін белгілеп, кемшіліктерді анықтау және ақпаратты қорғау жүйесін одан әрі дамыту бағыттарын айқындау;
❑кәсіпорын басшылығының және басқа да мүдделі тұлғалардың ақпараттық қауіпсіздік саласында қойылған мақсаттарға қол жеткізуін, қауіпсіздік саясаты талаптарының орындалуын тексеру;
❑ақпаратты қорғау құралдарын сатып алуға және ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі іс-шараларды іске асыруға салымдардың тиімділігін бақылау;
❑ақпараттық қауіпсіздік саласындағы жалпы танылған нормалар мен талаптарға сәйкестігін сертификаттау (атап айтқанда, ұлттық және халықаралық стандарттарға сәйкестігі).

Нелер аудиттеледі?



Келтірілген мынандй зиян дар АҚ бұзылған жағдайдағы ресурстың құндылығы мөлшерімен анықталады:

ISO/IEC 17799/27002 және 27001 стандарттары

ISO/IEC 17799 (жаңа нұсқасы 27002 нөмірімен шықты) және 27001 халықаралық стандарттары ақпараттық қауіпсіздікті басқару мәселелеріне арналған және олар өзара байланысты болғандықтан, біз оларды бір бөлімде қарастырамыз.

1995 жылы британдық стандарттар институты (BSI) BS 7799 Part 1 "**Ақпарат қауіпсіздігін басқаруға арналған тәжірибе коды**" стандартын жариялады (атауы әдетте «Ақпараттық қауіпсіздікті басқарудың практикалық ережелері"деп аударылады).

Оның негізінде 2000 жылы ISO/IEC 17799:2000 "Information technology" халықаралық стандарты қабылданды. Code of practice for information security management".

Келесі қосымша нұсқа 2005 жылы қабылданды және ISO/IEC 17799:2005 деп белгіленді. Ал 2007 жылы бұл стандарт ISO/IEC 27002 нөмірімен қайта шығарылды. Атауынан көрініп тұрғандай, ол ақпараттық қауіпсіздікті басқару саласындағы ұсынылған шараларды сипаттайды және тұтастай алғанда жүйелерді оның сәйкестігіне сертификаттауға арналмаған.