ISO/IEC 27001 –Ақпараттық қауіпсіздікке жол. Отандық кәсіпорындарда ақпараттық жүйелерді қолдану ерекшеліктері

Әл-Фараби ат.ҚазҰУ, 4 курс студенті Кондыбаев А.К.
Ғылыми жетекші - Шортанбаева Ж.К.

Соңғы уақытта заманауи кәсіпкерлікті және кәсіпорындарды ақпараттық технологияларды пайдаланбай басқаруды елестету мүмкін емес. Үйымдардың қызметтеріне сенімді ақпараттық технологиялар қажет.

Ақпарат көздеріне жататын ақпараттың және басқа да обьектілердің қауіпсіздігін қамтамасыз ету кез-келген бизнес үшін маңызды міндет болып табылады. Әрбір құзыретттілігі бар бизнесті басқарушы өзіне қарасты ағымдағы ақпарат жүйелерінің жағдайына көз жұмып қарай алмайды, олар кәсіпкерлікке қажетті барлық ақпараттық технологиялардың қамтамсыз етілуін қадағалап, ақпараттық технологияларға қатысты мәселерді шешуді қолына алады. Сөз жоқ, бүгінгі күннің өзінде аталған ақпараттқық технологиялар жүйесімен және оның қауіпсіздігін сақтау жолында кәсіпорындардың біраз бөлігі қамтамасыз етіліп, сонымен жұмыс жасап келеді. Бірақ бұл жеткіліксіз.

Жалпылама түсінікте, ақпараттық қауіпсіздік түсінігі ақпаратқа қатысты үшінші тұлғаның қатыстырылуының шектелуімен байланысты. Шындығында бұл ақпаттарттың қауіпсіздігіне қатсысты мәселенің жалпылама жиынытығының бір жағы ғана ашылып көрсетіліп отырған алдыңғы қатардағы әлемдік қауымдастықтар ақпарат қауіпсіздігіне қатысты мәселенің бұдан үлкен жиынтығын шешеді. Олардың қауіпсіздікке байланысты жүргізілген жұмыстарының нәтижесінде кәсіпорындардағы жұмыс барысындағы құралдардың үнемделуі және қажеттті емес қателіктердің іске асырылмауы алдын алынады.

Ашықтылығымен қолжетімділік арқылы халықаралық зерттеулердің ақпарттық қауіпсіздікті қамтамасыз етуге жоғарғы деңгейде көңіл бөлуі табысты қадам болып саналады.

Ақпарттық қауіпсіздікті басқару саласы бойынша әлемдік үздік тәжірибедегі халықаралық стандарттағы тіркелген ақпараттық қауіпсіздікті басқару жүйесі бойынша **ISO/IEC 27001** (ISO 27001) болып табылады. Ұйымның өзіндік ақпараттық ресурстарын қорғау қабілеттілігіне ие болуы үшін ISO 27001 ақпараттық қауіпсіздікті басқару жүйесі (АҚБЖ) талаптарды құрай отырып көрсетеді.

«Ақпаратты қорғау» түсінігі арқылы халықаралық стандартта ақпараттың қолжетімділігімен құпиялылық, тұтастылығын түсінуге жол көрсетіледі

Үйреніскен тұтастылықтан бөлек, басқа стандарт жұмыс міндеттемесіне қатысты басқа да маңызды қасиеттерге айқын көңіл бөлінетіндігіне ерекше айтып кету керек. Бұл қасиеттерге – қол жетімділік пен тұтастылық жатады. Күнделікті өмірдегі мысалдарды қарастырайық. Сіз өз жұмыс орныңызда жұмыс міндеттемелеріңізді жүзеге асыруда өзіңізге бағынышты өкіліңізден

немесе жұмыстасыңыздан ақпаратты кеш аласыз. Сөз жоқ, мұндай жағдай жұмыс орнында орын алып отырады. Бұл, егер ақпараттың **қолжетімділік** тәртібінің бұзылғандығын көрсетіп отыр. Басқаша алғанда, сіз ақпаратты уақытында аласыз, бірақ сіздегі ақпаратта қателіктер болуы мүмкін. Бұл қателіктер адам факторымен немесе компьютер жұмысымен және басқа себептермен байланысты болуы мүмкін. Бұл соқтығыс ақпарттың **тұтастық** тәртібінің бұзылғандығымен байланысты.

Ақпараттық қауіпсіздік – заңға қайшы келетін ақпаратты тығып қою, жабу, сатылатын ақпаратты жою сияқты ойлармен байланыстырылмауы тиіс. Яғни, осындай ойға алған қадамдарыңыздың іске асырылуы арқылы ақпаратты сақтауда көптеген ақпараттардың жойылып кетуінен бөлек, кем дегенде қолжетімділігінің жоғалуына немесе одан да қиын қаржылық шығындарға әкелуі мүмкін. Әрқашанда тепе-теңдікті сақтап отыру керек, сонымен бірге бір уақытта осы аталған барлық үш қасиетті сақтағаныңыз жөн, олар - тұтастылық, құпиялылық, қолжетімділік. Мұнымен қоса, кәсіпорын жұмысының дербез, әрі дұрыс мақсатын есте сақтаған дұрыс. Бұл мақсат - кәсіпорынның құралдармен өте жақсы жабдықталуы кеңістігіне немесе жұмысшының жоғарғы біліктілігіне қатысты қарастырыуы мүмкін емес. Кәсіпорынның жалғыз мақсаты – қаржы табысына қол жеткізу. Бұлардың қатарына жатпайтын және соған сай мақсаттары да бөлек ерекше кәсіпорындарға қамқорлық жасауға бағытталған немесе соған ұқсас үйымдар болуы мүмкін.

Ақпарат қауіпсіздігіне қатысты заманауи әдістердің негізгі түсініктеріне тоқталайық. Стандарттың негізгі обьектісі **ақпараттық актив.**

Ақпараттық актив - бұл материалдық немесе материалдық емес объект бола отырып:

- ақпаратты құрайды немесе ақпарат болып табылады;
- ақпаратты қайта өңдеуге, сақтауға немесе жолдауға қызмет етеді;
- ұйым үшін аса құнды болады.

Ақпараттық активтердің мысалы ретінде: тұтынушылармен келісімшарт, қаржылық есеп беру, технологиялық карта, хаттарды тіркеу журналы, жаңа қызметтер мен өнімдер жобалары, кәсіпорынның қаржылық жағдайы жөніндегі ақпарат сақталған ноутбуктар, тұтынушылар жөніндегі ақпараттық сервер, кәсіпорындағы қағазбен жұмыс жасайтын қызметкерлердің (ғимараттағы) архиві, кәсіпорынның оперативті қызметтерінің және даму жоспарларының жол көрсеткіші.

Ақпараттық активтер кәсіпорынның материалдық және қаржылық активтерінің негізгі қасиеттеріне ие: құндылық, кәсіпорын үшін құндылығы, қор жинау мүмкіндігі және басқа да активтерді қосып көрсетуге бағытталған активтерден құралады. Кәсіпорынның ақпараттық автивінің құндылығының бір бөлшегі ретінде барлық қаржылық құндылықтар жатқызылады. Мұндай активтің мысалы ретінде кәсіпорынның имиджін айтуға болады.

Бүгінгі күннің ақиқатында қаржылық, материалдық және ақпараттық активтер қорғауды қажет етеді. Ақпараттық активтерді сенімді қорғаудың жолы кәсіпорын қызметімен байланысты болып отыр. Қорғауға тән емес деңгейлер

қатарына тәуекелге бел буу факторының үнемі бағымсыздықпен қаралуы жатқызылады, егер іске асырылған жағдайда қауіп тудыруы мүмкін болса.

Антивирустық программалық қамсыздандыруды сатып алғанша, сұранысты қанағаттандыратын ақпараттық қауіпсіздікті сақтау деңгейіне жету үшін, желілік сақтандыру жүйесі немесе мәліметтерді резервтеу жүйесіне қол жеткізу керек. Сенімді ақпарат қауіпсіздік жүйесі тіркелген стандартты қабылдау немесе одан бас тарту үшін стандартты енгізуде орын алатын талаптармен танысып шығуды ұсынамын.

Стандартты қолданудағы пайдалар

Әуелі стандартты қолдануға кіріспес бұрын, кәсіпорынға келетін пайдаларды түсініп шығу маңызды. Төменде нақты кәсіпорындарға стандарттан келтірілетін пайдалардың тізімдері келтірілген.

1. Қауіпсіздік жүйесінің құндылығы төмендетіледі және ұтымды етіп жасалынады. Сіз нақты өзіңіздің кәсіпорыныздың аса қауіпті тәуекелділігін жабуға көмектесетін бағыттағы қауіпсіздік жүйелеріне ақшаңызды жұмсайсыз. «Шығын мүмкіндігінің» обьективті үйлесімдік бағасы сізге үнемі ақпараттық қауіпсіздікті тиімді қаржыландыруға мүмкіндік береді.
2. Компания менеджменті үшін ақпараттық активтер түсінікті болады. Стандарт ақпарат активтері тізбектерінің өзекті жағдайларын қолдауды және құруды талап етеді.
3. Ағымдағы бизнес процестеріне қауіпсіздіктерде орын алған қауіптер күнделікті анықталып тұрады.
4. Тәуекелділік есептелінеді және шешімдер бірінші ретте қаржылық мақсатта компанияның бизнес мақсатына сай қабылданады.
5. Кәсіпорындардағы қиын жағдайлар туындаған сәтте ақпараттық активтерді басқаруда қайта өңдеу, бизнесті тестілеу жобаларын қайта қалпына келтіруді қолдану арқылы басқарумен тиімді болады.
6. Қауіпсіздік саясатын жүргізу процесі жүргізілетін болады (күнделікті режимдегі ақпараттық қауіпсіздік жүйесінің әлсіз жерлерін табу және жөндеу).
7. Стандарт заңдылығына сәйкес бизнестің тазалығы және әртүстілігі қамтамасыз етіледі.
8. Рейдерлік қарсылыққа қарсы сенімді қорғаныс пайда болады.
9. Ақпараттық қауіпсіздік жүйесінің астында жалпы менеджмент жүйесі тұтастырыла жүреді.
10. Кәсіпорын халықаралық деңгейде танылады және сол арқылы беделі өсіп, тіпті сыртқы сауда да белгілі бола бастайды.

Отандық кәсіпорындарда стандартты қолданудағы талаптардың ерекшеліктері. ISO 27001 стандарты басшылықпен қызметкерлерде қалыптасқан отандық менталитеті және кәсіпорынның дамуымен тарихи қалыптасуы жағдайындағы ерекшеліктерді ескере отырып, орындалуы қиын талаптарды құрайды. Ақпараттық қауіпсіздіктің тиімді жүйесін құру үшін аталған барлық талаптарды орындау қажет. Қарастырылып отырған амалдан бөлек, стандарттың күрделі талаптарына қатысты отандық сарапшылар мен аудиторлардың пікірлерінен бірен -саран мысал келтірейік.

Стандарт талаптары:

1. Ақпараттық қауіпсіздік саласында жұмыс жасайтын Қазақстандағы әртүрлі инстанциялармен келісімге отыру. Мұндай жүйелерге күшті ІІМ, қауіпсіздік саласында қызмет ететін консалтингтік фирмалар, сертификаттау қауымдастықтары, ақпараттық қауіпсіздік жөніндегі форумдар болуы мүмкін.

2. Ақпараттық қауіпсіздікте менеджмент саласының жеке түрде қаралуы. (шолу). Бұл үшін өзіне сертификаттау органдарды немесе консалтингтік компания болмаса, кәсіпорынның серіктес мүшелерін тартуы керек .

3. Кәсіпорынның ақпараттық активтерінің толық және өзекті реестрлерінің қатыстырылуы. Бұл айтарлықтай жұмыстың ауқымды бөлігін құрайды және көбінесе кәсіпорындар реестрінінің өзектілігін іске қосып отырады.

4. Ақпараттық қауіпсіздік талаптары барлық жұмыстағы мамандарда қолданылып, қабылдануы тиіс. Бұл тіпті дауға тұрғысыз компьютерлік біліктілік немесе жеке қасиеттерімен байланысты болуы мүмкін.

5. Жұмыс уақытында барлық мамандар кезеңдік ақпараттық қауіпсіздікті сақтау үшін түсіндірмелік оқытулардан өткізілуі тиіс.

6. Қызметкер жұмыстан босатылған уақыттан бастап реестр бойынша тексеріліп және жұмыс уақытына оның қолжетімді болған барлық ақпараттық активтердің қайтарылғандығына көз жеткізу керек.

7. Кәсіпорындардағы ақпараттық активтердің қауіпсіздігін сақтауда тұлғалық қауіпсіздік тек материалдық активтерге қатысты ғана болмауы тиіс. Тұлғалық қауіпсіздік аясында ақпараттық активтердің материалдық емес түрлерінің жойылуының себептерін де іздестіру керек.

8. Жекеленген тұлғалар үшін бағдарламамен қамтамасыз ету барысында қайта өңдеу, тестілеу, бағдарламаларды қолдануды бөліп қарастыру керек. Басқаша түсіндіргенде, бағдарламалық өнімді қайта жасап алып, оны бір компьютерде қолдануға тыйым салынады. Аталған талапты іске асыру үшін жаңа компьютерді алған жөн.

9. Ақпараттық қауіпсіздіктің талаптарын орындау үшін үшінші тұлғаларға арналған қызметтер жүйесі қайта жасалынып, орындалуы тиіс. Мысалы, интернет-провайдер, кеңесшілер, басқа кәсіпорындардың техникалық мамандары.

10. Кез келген ақпараты бар құрал жөндеуге немесе қоймаға жіберілмес бұрын ондағы барлық ақпарттардың жойылғандығына көз жеткізу керек.

11. Жүйелік құжаттандыру барлық құрылғыларға қолжетімді болуы керек, сол арқылы ақпарат негізі бола отырып, үшінші тұтынушы тұлғаларға қолжетімсіз болып құрылуы тиіс.

12. Ақпараттық қауіпсіздікке қатысты талаптарды тек компьютерлік ақпараттық қауіпсіздік жүйесімен ғана байланыстырып есептемей, сонымен бірге қарапайым факс, телетайп, телефондарға қатысты да қарастыру керек.

13. Барлық администратордың жүйелік әрекеттері тіркелген болуы шарт. Бұл бірден бір қиын жол. Мұның қажеттілігі жүйелік тіркеушілер өздерінің әрекеттерінің түрлілігіне қарай үнемі ақпараттық жүйелердің құрылымымен

түзетіп отыруымен байланысты. Осы маманның жұмыстан босатылуы кәсіпорын үшін үлкен қаржылық шығынға әкеледі. Жасалған жұмыстардың жазбалары жаңадан келген жүйелік администраторға жедел түрде барлық ақпараттық басқаруға қатысты мәліметтерге қол жеткізуге және жүйелерді құруға септігін тигізеді. үстелінің саясатымен (жиһаз) компьютердің экраны қабылдануы тиіс. Яғни, дәл осы аталған жолмен ақпараттың көп бөлігінің жойылып кетуі байланысьты.

15. Ақпаратпен байланысты барлық мәселелер (компьютер бұзылуы, құралдардың жоғалуы, ақпараттардың жоғалуы, ақпараттық жүйелердің өзімен өзінің жоғалуы және т.б) тіркеу кітапшасында тіркелген болуы тиіс. Бұл жұмыс мәселенің жеңіл шешілуіне көмегін тигізеді.

16. Кәсіпорында бизнесті қалпына келтірудің жобасы алдын ала жасалған болуы керек. Оның құрамдас бөлігі ретінде тестілеуді айтуға болады.

17. Кәсіпорында «авторлық және араласқан құқық» жөніндегі заңдылықтарын талаптарының сақталуына көңіл бөлуі тиіс. Яғни, стандарт талаптарына сай кәсіпорын лицензиясы жоқ бағдарламалық жабдықтауды қолданбауы тиіс.

18. Кәсіпорынның мақсатқа сай емес барлық ақпараттық құралдық-жабдықтар қолданылмауы тиіс. Бұл дегеніміз - тыйым салынған ойындар, интернет бойынша жеке қолданыстар, рефераттарды іздеу және т.б. жағдайлардың орын алмауы керек деген сөз.