ҚАЗАСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҰЙЫМНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН БАСҚАРУ ЖҮЙЕСІН САРАПТАУ, БАҒАЛАУ ЖӘНЕ СЕРИТФИКАТТАУ ТӘРТІБІ

Информационная технология

ПОРЯДОК ЭКСПЕРТИЗЫ, ОЦЕНКИ И СЕРТИФИКАЦИИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

ҚР СТ 34.028-2008

(ИСО/МЭК 27001стандартына сәйкестікке бейімдеу арқылы БСИ БҚ 3001:2002 «BS 7799-2 стандартына сәйкестікке сертификаттау үшін даярлық», IDT)

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігі
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

ҚАЗАСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҰЙЫМНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН БАСҚАРУ ЖҮЙЕСІН САРАПТАУ, БАҒАЛАУ ЖӘНЕ СЕРИТФИКАТТАУ ТӘРТІБІ

ҚР СТ 34.028-2008

(ИСО/МЭК 27001стандартына сәйкестікке бейімдеу арқылы БСИ БҚ 3001:2002 «BS 7799-2 стандартына сәйкестікке сертификаттау үшін даярлық», IDT)

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігі
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

Алғысөз

1 «Инфосистемы Джет» ЖАҚ **ДАЯРЛАДЫ**

Қазақстан Республикасы Ақпараттандыру және байланыс жөніндегі агенттігі **ЕНГІЗДІ**

2 Қазақстан Республикасы Индустрия және сауда министрлігі Техникалық реттеу және метрология комитетінің 2008 жылғы 25 ақпандағы №107-од бұйрығымен **БЕКІТІЛІП ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

Кіріспе

Ақпарат ұйымның бірден бір ең бағалы ресурстары болып табылады. Өз деңгейіндегі ақпарат қорғанысының болмауы мыналарға әкеп соқтырады:

– Рұқсат етілмеген әдіспен ақпаратты табу, беру немесе ашу;

– Оның бағасын түсіру мақсатында ұйым рұқсатынсыз ақпаратқа өзгеріс енгізу;

– Қалпына келтіру мүмкіндігінсіз ақпаратты із-түссіз жоғалту;

– Пайдаланушыларға ақпаратқа ену мүмкін болмауы.

Әрбір ұйым кездесуі мүмкін көптеген қауіптерден өз ақпаратын өз деңгейіндегі қорғауды қамтамасыз жауапкершілігі оның барлық менеджерлері, ақпараттық жүйелер иесі немесе сақтаушысына және пайдаланушыларға жүктеледі. Ақпаратқа ұйымның басқа маңызды бизнес-ресурстары сияқты қорғаныс және өз деңгейіндегі қорғанысты басқару қамтамасыз етілуі тиіс. Қорғаныс және оны өз деңгейінде басқару үздіксіз және алдын алу негізінде іске асырылуы тиіс.

Жоғарыда көрсетілген мақсаттар ақпарат құпиялылығын, тұтастығын және ену мүмкіндігін қорғау қажеттілігі ретінде қысқаша ұсынылуы мүмкін – ақпараттық қауіпсіздіктің мәні де осында.

Осы стандарт орныққан тәжірибені сипаттайды, оның негізінде кез келген ұйымдар – ірі орташа және ұсақ – ҚР СТ ИСО/МЭК 27001 халықаралық стандартына сәйкестікке сертификаттауды алуға мүмкіндік беретіндей етіп өздерінің ақпараттық қауіпсіздікті басқару жүйесін (АҚБЖ) даярлай, іске асыра және қолдай алады.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҰЙЫМНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН БАСҚАРУ ЖҮЙЕСІН САРАПТАУ, БАҒАЛАУ ЖӘНЕ СЕРИТФИКАТТАУ ТӘРТІБІ

Енгізілген күні 2008.07.01.

1 Қолданылу саласы

Осы стандарт *ҚР СТ ИСО/МЭК 27001 және ҚР СТ ИСО/МЭК 17799* стандарттарын пайдаланушыларға арналған нұсқаулықтан тұрады. Ол АҚБЖ даярлау, іске асыру, бақылау және жетілдіру жөніндегі нұсқау болып табылады, яғни тиімді ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті қызметің бүкіл “өмірлік” цикліне арналған.

Осы стандарт:

– АҚБЖ-ны жоспарлауға, даярлауға және іске асыруға,

– АҚБЖ аудитін даярлауға,

– АҚБЖ аудитін өткізуге қатысушыларға арналған.

АҚБЖ аудиттері мынадай типтерде болады: бірінші тарап аудиттері (ішкі аудиттер), екінші тарап аудиттері (мысалы, тапсырыс берушілер аудиторлары орындайтын аудиттер) және үшінші тарап аудиттері (мысалы, тәуелсіз сертификаттау органдары орындайтын аудиттер).

Осы стандарт үшінші тарап аудиті нәтижесінде *ҚР СТ ИСО/МЭК 27001* стандартына сәйкестікке аккредиттелген сертификаттау алу үшін белгіленген процестерді іске асыру жөніндегі жан-жақты ақпараты ұсынады. Стандарттағы талаптарға сәйкес келу үшін ұйым барлық қажетті процестерді пайдаланатындығын көрсетуі және оларды пайдалану қажеттілігінің негіздемесін ұсынуы тиіс. Бұл процестердің өзі олардың тәуекелдерін басқаруды ұйымның өзінің іске асыруына әкеп соқтыратындығы сөзсіз. Ұйым өз АҚБЖ бір бөлігі ретінде басқару құралдарының тиімді жүйесін іске асыруы тиіс және АҚБЖ аудиторы қажетті дәлелдерді ұсына отырып (бірінші, екінші немесе үшінші тарап аудиті өткізілгеніне қарамастан) оларды көрсетуге қабілетті болуы тиіс.

Осы стандартты аудиттен өтудің тікелей қажеттілігі жоқ, бірақ салада қабылданған оңтайлы тәжірибелік әдістер негізінде АҚБЖ-ны даярлау және іске асыру үшін спецификация қажет ұйымдар қолдана алады. Дегенмен, *ҚР СТ ИСО/МЭК 27001* стандартына сәйкес келу үшін ұйымнан үшінші тарап аудиті жоспарланды ма, жоқ па, оған қарамастан, болмағанда бір ішкі аудит өткізу талап етіледі. Ұйымның үшінші тарап аудитін өткізуге экономикалық негіздемесі болмауы мүмкін, бірақ *ҚР СТ ИСО/МЭК 27001* стандартына сәйкестік үшін АҚБЖ-ның ішкі аудиті міндетті түрде өткізілуі тиіс.

2 Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтеме жасалады:

ҚР СТ 1.9-2003 Қазақстан Республикасының мемлекеттік стандарттау жүйесі. Халықаралық, өңірлік және ұлттық стандарттар мен стандарттау, метрология, сертификаттау және метрология жөніндегі нормативтік құжаттарды қолдану тәртібі.

ҚР СТ ИСО 9001-2001 Сапа менеджменті жүйесі. Талаптар.

ҚР СТ ИСО/МЭК 17799-2006 Ақпараттық технология. Қорғанысты қамтамасыз ету әдістері. Ақпаратты қорғауды басқару бойынша ережелер жинағы.

ҚР СТ ИСО/МЭК 27001-2008 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар.

ҚР СТ Ақпараттық технология. Бағалау және тәуекелдерді басқару;

ҚР СТ Ақпараттық технология. Ұйымның ақпараттық қауіпсіздігін басқару жүйесінің аудиті.

ИСО/МЭК 62: 1996* басшылығы Сапа жүйесін сертификаттауды жүргізетін сертификаттау жөніндегі органдарға қойылатын талаптар

ИСО/МЭК 73:2002* басшылығы Тәуекелдерді басқару – Терминология – Стандарттарда қолданыс жөніндегі нұсқау

ЕА 7/03 басшылығы Ақпараттық қауіпсіздікті басқару жүйесін сертификаттау/тіркеу жөніндегі органдарды аккредиттеуге арналған нұсқау

3 Анықтамалар

Осы стандартта *ҚР СТ ИСО/МЭК 17799:2005, ҚР СТ ИСО/МЭК 27001* және ISO/IEC 73 басшылығы бойынша терминдер қолданылады.

4 Ақпараттық қауіпсіздік мәні

4.1 Құпиялылық

Ақпаратты осы ақпараттар иесінен өкілдік алмаған кез келген ұйым немесе кез келген тұлғаға ену мүмкін болуынан сақтау, өңдеу және жіберу кезіндегі кез келген формадағы қорғанысы.

Енуді басқарудың көптеген формалары, негізінен, құпиялылықты қорғауға жатады. Құпиялылықты қамтамасыз ететін басқару құралдарының тағы бір мысалы –шифрлау. Басқару құралдары ақпараттық қауіпсіздікті басқару жүйесінің әрбір сатысында қолданылуы мүмкін: физикалық сатыда (мысалы, құжаттарды сақтауға арналған есіктер мен шкафтардағы құлыптар, сейфтер және т.с.с) және логикалық сатыда (қосымшаларда және басып шығарылған күйде берілген мәліметтер базасындағы мәліметтердің жекелеген алаңдары). Әр жағдайда қауіптер мен осалдықтарды

сәйкестендіру, тиісті тәуекелдерді бағалау және осы тәуекелдерден қорғау үшін басқару құралдары жүйесін таңдау, іске асыру және қолдану керек.

4.2 Тұтастық

Оны сақтау және жіберу кезінде ақпараттың дәлдігі мен толықтығын қамтамасыз ету; ақпаратты дұрыс өңдеуді қамтамасыз ету рұқсат етілмеген тәсілмен ақпаратты өзгертуге жол бермеу. Бұдан басқа, қосылу жоспарланған желі мен жүйе екендігіне кепілдік беру үшін ұйым қосылатын желілер мен жүйелердің тұтастығы фактісіне көз жеткізген жөн.

Мәліметтерді өңдеу құрылғыларының көпшілігінде құрылғылардың (дискілердегі жинағыштар мен өзге тасымалдағыштарды, сондай-ақ телекоммуникациялық жүйелерді қоса алғанда) мәліметтерді жоймайтынына кепілдік беруге мүмкіндік беретін мәліметтердің тұтастығын автоматты түрде тексеру құралдары бар. Тұтастықты бақылау құралдары операциялық жүйелерде, бағдарламалық қамсыздандыруда және қолданбалы бағдарламаларда айтарлықтай роль атқарады, өңдеу кезінде бағдарламалар мен мәліметтерді қасақана немесе кездейсоқ зақымдаудың алдын алуға мүмкіндік береді. Процедуралық сатыда адам қателіктері, ұрлау немесе алаяқтықтың алдын алатын тұтастықты бақылау құралдары (мысалы, мәліметтерді енгізу/шығару дұрыстығын тексеруге арналған бақылау құралдары, пайдаланушыларды оқыту және өзге операциялық бақылау құралдары) қолданылуы тиіс.

4.3 Ену мүмкіндігі

Қажет еткен жері мен уақытында осы ақпаратты иемденуге тиісті өкілдігі барларға ақпаратқа ену мүмкіндігін қамтамасыз ету.

Ақпаратқа ену мүмкіндігімен қамтамасыз ету үшін тәжірибеде басқару құралдары жүйесі талап етіледі, мысалы: ақпаратты резервті көшірмелеу құралдары, жүктеуді жоспарлау, жүйелерді қабылдауға арналған процедуралар мен критерийлер, оқиғаны басқару процедуралары, ақпараттың алынбалы тасымалдаушыларын басқару, ақпаратты өңдеу процедуралары, жабдықтарды қолдау және тестілеу, жүйені пайдалану мониторингі процедуралары, тоқтаусыз жұмыс істеуді қамтамасыз ету процедуралары. Ену мүмкіндігін қамтамасыз ететін басқарудың алдын алу құралдары ретінде қауіпсіздік оқиғаларын, қызмет көрсету дәрежесін және жүйе өнімділігін дер кезінде және үздіксіз мониторингі , талдауы және бақылауын іске асыру қолданылады.

4.4 Құпия және сыни ақпарат

ҚР СТ ИСО/МЭК 17799 стандарты басқару құралдары жиынтығын айқындайды, олар құпия әрі сыни ақпаратта да қолданылады. Құпия немесе сыни ақпарат дегеніміз не? Оларды қалай ажырату керек? Әр ұйым үшін өз

анықтамасы болады. Қажет болғанда ақпараты құпия немесе сыни деп белгілеу үшін, ал қалған ақпараттарды құпия немесе сыни емес деп тану үшін жеке ұйымға қатысты ақпараттың маңыздылығы мен пайдалылығын белгілеуге мүмкіндік беретін кейбір әдістемелер айқындалуы тиіс.

Бұнымен қатар уақытша фактор да бар: ұйымның қаржылық ақпараты қор биржасында пайда болғанға дейін бірнеше күн алды өте құпия болады, бірақ онда пайда болғаннан кейін құпия болудан қалады. Құпиялылық сондай-ақ мәліметтерге берілетін жіктеу деңгейінде де көрініс табады.

Ақпараттық ресурстардың бағалануы тәуекелдерді бағалаудың бір бөлігі (*ҚРСТ* қараңыз) болып табылады, ол тиісті басқару құралдары жүйесінің көмегімен осы ресурстарды қорғау үшін қажетті тәуекелдер мен қауіпсіздік деңгейін есептеуге мүмкіндік береді.

5 Ақпараттық қауіпсіздікті басқару жүйесі (АҚБЖ)

5.1 Кіріспе

ҚР СТ ИСО/МЭК 27001 стандарты үшін ақпараттық қауіпсіздікті басқару жүйесі (АҚБЖ) ұғымы басты болып табылады. Ақпараттық қауіпсіздікті басқару жүйесі (АҚБЖ) – бизнес тәуекелдерін талдау мен бағалауға негізделген және ақпараттық қауіпсіздікті даярлау, іске асыру, пайдалану, бақылау, қолдау және жетілдіру үшін арналған басқарудың жалпы жүйесінің бір бөлігі болып табылады. Басқару жүйесіне ұйымдастыру, құрылымы және саясаты, міндеттерді жоспарлау, бөлісу, ұсыныстар, процестер және ресурстар кіреді. Ақпараттық қауіпсіздікті басқару жүйесін қолдану саласы, оны басқару және ресурстары ұйым көлемі мен қарастырылып жатқан ақпараттық ресурстарға байланысты болады.

Ұйымға пайдалы болу үшін АҚБЖ тиімді болуы тиіс. Ақпараттық қауіпсіздік ұйымның өндірістік және іскери мәдениетінің ажырамас бөлігі болуы тиіс. Ақпараттық қауіпсіздік негізінен техникалық мәселені емес, басқару мәселелерін ұсынады, әйтсе де әсіресе ақпараттық технологияларға деген күшті қажеттілік жағдайында техникалық жағы да назардан тыс қалмауы тиіс. Ақпараттық қауіпсіздікті басқару – бір реттік әрекет емес, оны үнемі жетілдіру жөніндегі үздіксіз қызмет ретінде қарастыру қажет. Жақсы басқарылатын ақпараттық қауіпсіздік – бизнесті іске асыру құралы. Қазіргі әлемде бірде-бір ұйым ақпараттық қауіпсіздікпен қамтамасыздандырылмайынша табысты жұмыс істей алмайды. Басқару құралдарының жүйесі жұмсалған шығынды қайтарып қана қоймайды, ол сондай-ақ ұйымның өркендеуіне оң үлес қосады.

5.2 *ҚР СТ ИСО/МЭК 27001* стандартына сәйкестік

Тәжірибелік нұсқау бола отырып *ҚР СТ ИСО/МЭК 17799:2005* стандарты ұсыныстар мен ұсынымдар нысанына ие, бұл оны спецификация

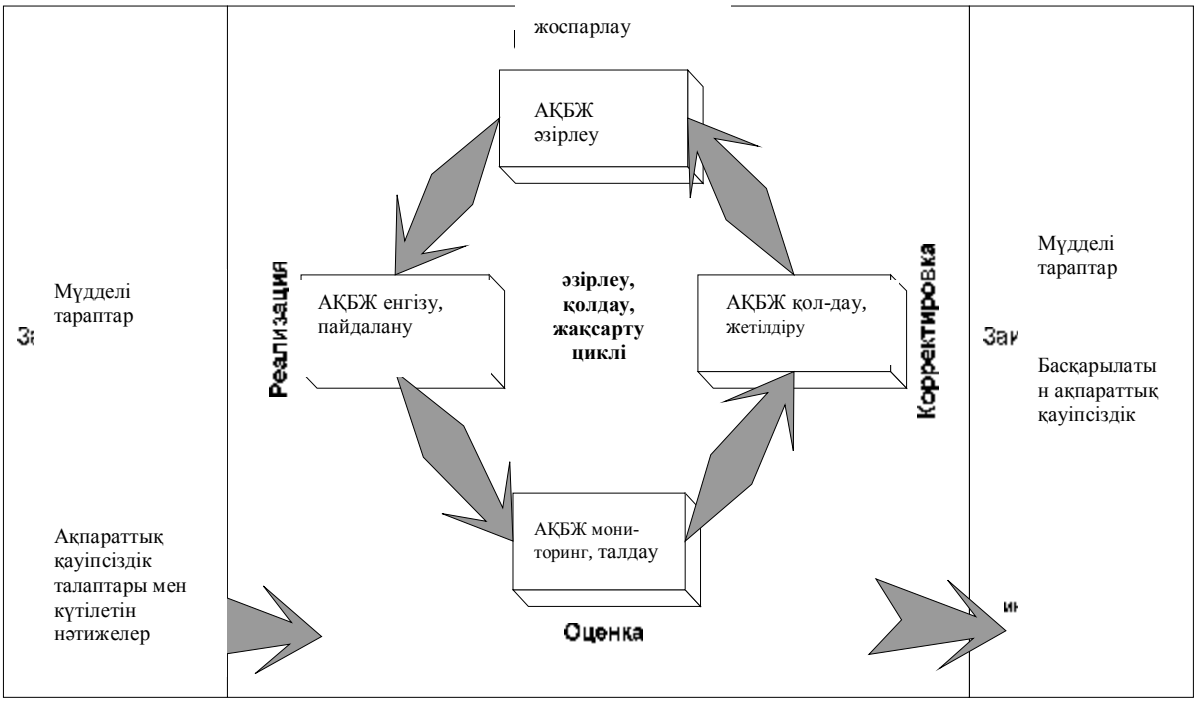
ретінде қолдануға болмайтынын және сәйкестік туралы ұсыныстың адасуға апармайтынына кепілдік беретіне сақтық білдіру қажеттілігін білдіреді.

АҚБЖ үшін спецификация бола отырып, *ҚР СТ ИСО/МЭК 27001* стандарты егер ұйымға стандартқа сәйкестік туралы сұрау қажет болса, іске асырылған АҚБЖ сәйкес келуі тиіс “тиіс” шарты түріндегі ережелерді қолданатын талаптар жиынтығы түріне ие. Егер *ҚР СТ ИСО/МЭК 27001* жиынтық болса, осы стандартта сипатталған (1-8 тармақтар) процесстік жолмен байланысты барлық талаптарды қамтиды.

ЗБолуы тиісИ сөзі көрсеткендей, *ҚР СТ ИСО/МЭК 27001* стандартының талаптарын көрсететін ережелердің міндетті болып табылатынын білдіреді. «Жөн» етістігі міндетті болып табылмайтын, бірақ қолдануға ұсынылатын талаптарды қолдану жөніндегі ережелерді құраса да ережелерде қолданылады.

5.3 ЖЖБТ моделі (PDCA)

ҚР СТ ИСО/МЭК 27001 стандартында «Жоспарлау – Іске асыру – Бағалау – Түзету - ЖЖБТ» («Plan – Do – Check - Act» – PDCA) моделі қабылданған (2-суретті қараңыз). Бұл модель АҚБЖ-ны даярлау, іске асыру, бақылау, талдау, қолдау және жетілдіру үшін негіз ретінде қолданылады.



2-сурет – АҚБЖ процестеріне қолданудағы ЖЖБТ моделі

Жоспарлау (АҚБЖ-ны даярлау)	Ұйымның жалпы саясаты мен мақсаттарына сәйкес келетін нәтижелерді алу мақсатында ақпараттық қауіпсіздікті жетілдіру мен тәуекелдерді басқару үшін маңызды қауіпсіздік саясаты, мақсаттары, процестері мен процедураларын айқындау.
Іске асыру (АҚБЖ-ны енгізу және пайдалану)	Қауіпсіздік саясатын, басқару құралдарын, процестер мен процедураларды іске асыру және қолдану.
Бағалау (АҚБЖ мониторингі және талдау)	Бағалау, егер қажет болса, қауіпсіздік саясатына, мақсаттар мен практикалық тәжірибеге сәйкестігін тексеруге арналған процесс сипаттамаларын өлшеу, сондай-ақ нәтижелерін басқару персоналы ары қарай талдауы үшін беру.
Түзету (АҚБЖ-ны қолдау және жетілдіру)	АҚБЖ-ны үнемі жетілдіру мақсатында басқару персоналы орындаған талдау нәтижелері бойынша түзету және алдын алу шараларын қабылдау.

5.4 АҚБЖ-ны әзірлеу

ҚР СТ ИСО/МЭК 27001 стандартының 4.2.1 тармағында “Жоспарлау” сатысына арналған мынадай міндетті («ұйым міндетті») талаптар айқындалған:

– Бизнес, ұйым, оның орналасуы, ресурстар мен технологиялар сипаттамалары терминдерінде **АҚБЖ қолдану саласы мен шектерін айқындау.** АҚБЖ қолданылу саласы ұйымның шектелген және айқындалған тәуелсіз бөлігі болуы мүмкін, немесе қолданылу саласы ретінде бүкіл ұйым алынуы мүмкін. АҚБЖ қолданылу саласының дұрыс айқындалғаны және толық болғаны шарт. Бұл қолданылу саласының өзге жүйелер, ұйымдар, сыртқы жеткізушілер интерфейстерін есепке алуы, сондай-ақ, барлық тәуелділіктерді есепке алғаны жөн, мысалы, осы АҚБЖ көмегімен орындалуы тиіс қауіпсіздік талаптары.

– Бизнес, ұйым, оның орналасуы, ресурстар мен технологиялар сипаттамалары терминдерінде өндірістік және құқықтық немесе нормативтік талаптарды, сондай-ақ шарттық міндеттемелерді немесе үшінші тараппен жасалған келісімді есепке ала отырып **АҚБЖ саясатын айқындау**. АҚБЖ саясатын басшылық бекітуі тиіс. Бұл саясатқа мақсаттарды айқындауға арналған жалпы құрылымды айқындауға, сондай-ақ басшылықтың жалпы міндеттері мен қызмет принциптерін айқындауы, тәуекелдерді басқару ауқымын айқындауы және тәуекелдер бағаланатын критерийлерді белгілеуі тиіс.

– **Тәуекелді бағалауға ұйымның таңдаған жолын айқындау** – бұл нақты бір АҚБЖ-ға неғұрлым сәйкес келетін жол болуы тиіс. Ұйым тәуекелдерді қабылдау үшін өз критерийлерін даярлауы және тәуекелдердің жол берілетін деңгейін сәйкестендіруі қажет. Тәуекелді бағалау әдісін таңдау туралы шешімді ұйымның өз қабылдайды.

Қандай да бір әдіс қолданылғанына қарамастан *ҚР СТ ИСО/МЭК 27001* стандартындағы басқарудың барлық салаларын

қамтитын басқару жүйесін даярлау қажет екендігін атап өткен жөн; бұл әдістің ұйымдық аспектілерімен, персоналмен, бизнес-процестермен, пайдалану мен техникалық қызмет көрсету процестері мен процедураларымен, құқықтық және нормативтік талаптармен, шарттық міндеттемелермен, сондай-ақ ақпаратты өңдеу құралдарымен байланысты тәуекелдерді есепке алуы тиіс. *ҚР СТ* стандартында осы сатыға, сондай-ақ төменде сипатталған г) және д) сатыларына сәйкес келетін тәуекелдерді бағалау туралы ақпараттар берілген.

Тәуекелдерді бағалау міндетті талап болып табылады, бірақ оны қолдану барысында автоматтандырылған бағдарламалық құралдарды қолдану міндетті болып табылмайды, дегенмен көптеген жағдайларда осы тектес аспаптық құралдарды қолдану әсіресе тәуекелдерді қайтадан бағалау қажеттілігінде және қауіптер, осалдықтар және ресурстар туралы ақпараттар туралы ақпараттар тәуекеліне байланысты жаңартулар қажеттілігінде басымдық болып табылады. Тәуекелдерді бағалау жолын таңдау күрделілігі қарастырылып жатқан АҚБЖ күрделілігімен байланысты. Қолданылатын әдістерді қажетті ұйымның күрделілік деңгейімен және кепілдік деңгейлерімен сәйкестендірген жөн.

а) Ресурстар тап болатын осы ресурстармен байланысты, ресурстардың құпиялылығы, тұтастығы және ену мүмкіндігін төндірілуі мүмкін қауіптер мен осалдықтарды есепке ала отырып **Тәуекелдерді сәйкестендіру**. Бұл жағдайда с) тармағында сипатталғандай, тәуекелдің басқарудың барлық салаларымен байланысты болғаны қажет (тәуекелдерді бағалау туралы неғұрлым толық ақпарат *ҚР СТ* стандартында беріледі).

б) тармағына сәйкес алынған ақпаратты қолдана отырып және барлық қолдану салаларын есепке ала отырып - ұйымдық аспектілер, персонал, бизнес-процесстер, пайдалану мен техникалық қызмет көрсету процестері мен процедуралары, құқықтық және нормативтік талаптар, шарттық міндеттемелерді, сондай-ақ ақпаратты өңдеу құралдарын есепке ала отырып **Тәуекелдерді бағалау** (*ҚР СТ* қараңыз, онда тәуекелді бағалау туралы жан-жақты ақпарат берілген). Ұйым қауіпсіздіктің бұзылуы оның бизнеске келтіруі мүмкін шығынды және ондай бұзылудың болу ықтималдығын бағалауы тиіс. Сондай-ақ, ұйым тәуекелдер деңгейін айқындауы тиіс және өз бизнесі ауқымында тәуекелдер жол берілетін болып табыла ма немесе тәуекелдерді өңдеуді орындау қажет болады ма айқындауы тиіс.

в) **Сәйкестендіру және тәуекелдерді өңдеу нұсқаларын бағалау.** Оның бизнесіне тигізуі мүмкін әсерлерді сәйкестендіріп және бағалай отырып, ұйым бұл тәуекелдерді өз деңгейінде басқаруға және оларды өз бизнесі ауқымында өңдеуге мүмкіндік беретін әр түрлі әрекеттер жасай алады. Ұйым қарастыруы мүмкін әрекеттерге мыналар жатады: тәуекелдерді азайтуға бағытталған басқарудың өз деңгейіндегі құралдарын қолдану, осы тәуекелдермен байланысты қызметтерді тоқтату арқылы тәуекелдің алдын

алу, тәуекелдерді өзге тараптарға (мысалы сақтандырушыға) беру (толығымен немесе ішінара) немесе тәуекелді жоспарлы немесе әдейі қабылдау.

г) **Басқару мақсаттарын және тәуекелдерді өңдеуге арналған басқару құралдарын таңдау.** Егер ұйым басқару құралдарын тәуекелдерді өңдеу үшін қолдану туралы шешім қабылдаса, онда оларға алдымен осы мақсатқа сәйкес келетін басқару құралдары жүйесін таңдауы керек. Ұйым өзіне қажеттілерін таңдай алатын басқару құралдары *ҚР СТ ИСО/МЭК 27001* стандартының А қосымшасында берілген. Сондай-ақ ұйымға А қосымшасына енбеген басқарудың қосымша құралдары қажет болуы мүмкін.

Басқару құралдарын таңдағанда экономикалық тиімділігін есепке алған жөн, яғни іске асыру бағасы осы құралдар арқылы тәуекелдердің қаржылық әсерін төмендету мүмкін болатын сомадан аспауы керек. Кейбір әсерлердің қаржылық емес сипаты барлығы сөзсіз. Сондай-ақ, қауіпсіздікке, жеке ақпаратқа, құқықтық және нормативтік талаптарға, имидж бен беделге қатысты әсерлерді есепке алу керек.

д) **Қолданылуы туралы Ережені даярлау** – Қолданылуы туралы Ережені даярлау *ҚР СТ ИСО/МЭК 27001* стандартына қол жеткізгісі келетін ұйым үшін міндетті талап болып табылады. Қолданылуы туралы Ереже басқару мақсаттары мен таңдалған басқару құралдары санамаланатын құжат болып табылады және бұл таңдау тәуекелдерді бағалау және тәуекелдерді өңдеу процестерімен байланысты болуы тиіс. Бұл байланыс басқару мақсаттары мен басқару құралдарын таңдау негізділігін көрсетуі тиіс. Тек қана басқару мақсаттары мен басқару құралдарын санамалау қолданылуы туралы Ережеде жол берілмейтін болып табылады.

5.5 АҚБЖ-ны іске асыру және пайдалану

(Пске асыру” сатысы үшін *ҚР СТ ИСО/МЭК 27001* айқындалған міндетті («**ұйым міндетті**») талаптар “**ЖоспарлауУ сатысында** даярланған АҚБЖ-ны іске асыруға және пайдалануға мүмкіндік беретін процестердің қажетті жиынтығын қолданып отырғанына кепілдік беру үшін әзірленген. Бұл талаптарға ұйым сәйкестендірген және бағалаған ақпараттық қауіпсіздік тәуекелдерін басқару үшін қолданылатын тәуекелдерді өңдеу жоспарын құрастыру қажеттілігі жатады. Бұл ыңғайда басшылықтың қажетті әрекеттерін айқындау және ақпараттық қауіпсіздік тәуекелдерін басқару процесіне қатысушылардың міндеттерін, сондай-ақ қауіпсіздік үшін маңызды және АҚБЖ-мен байланысты пайдаланушылар/менеджерлердің кез келген қызметтерінде қатысатындардың міндеттерін сәйкестендіру қажет.

Ұйымның тәуекелдерді өңдеу жоспарын және таңдалған басқару құралдарын іске асыруға мүмкіндік беретін процестер жиынтығын мына факторларды есепке ала отырып қолданғаны жөн: АҚБЖ-ны қаржыландыру,

рольдер мен міндеттерді бөлісу, оқыту мен құлақтандырудың қажетті бағдарламасын іске асыру, ресурстар мен операцияларды басқару, сондай-ақ ақпараттық қауіпсіздік оқиғаларын басқаруға арналған процедураларды орнату және қолдану. Басқару құралдары жүйесін іске асыру туралы ақпарат *ҚР СТ* стандартында келтірілген.

Тиімділік – бұл таңдалған басқару құралдарын іске асыру кезіндегі түйінді сөз. Басқару құралдары олар таңдалған мақсатқа сәйкес қауіпсіздік тәуекелін (тәуекелдерін) басқаруда тиімді болуы тиіс. Сондай-ақ, олардың экономикалық тиімділігін есепке алған жөн – басқару құралының бірнеше рет іске асырылу дәрежесі болуы мүмкін. Ақшаны артық шығындамас үшін іске асырылу дәрежесі (мысалы, оқытудың, құжаттаудың немесе есеп берушіліктің қажетті мөлшерінде) жақсы салмақталған болуы тиіс. Тым артық іске асыру осы құрал ықпалындағы персоналдың көңілін қалдыруы мүмкін, басқару құралының жалпы тиімділігінің жиі төмендеуіне әкеп соқтыруы мүмкін. Қауіпсіздік пен бақылау үнемі адамдардың өмірі мен жұмыс тәжірибесіне араласады, бірақ оны артық жүкке айналдыруға болмайды.

Сондай-ақ, қауіпсіздіктің мәні адамдарға олардың істеуі тиіс жұмысына мүмкіндік бермеу емес, оның мәні олардың өз жұмыстарын басқарылатын және тиімді бақылауда атқаруына мүмкіндікті қамтамасыз етуде. Ол оларға өз міндеттерін атқарғанын көрсетуге мүмкіндік беруі тиіс; ешқандай күмәнсыз олардың жауапкершілікпен қарайтынын анықтауға мүмкіндік беруі тиіс. Жақын арада персонал дұрыс іске асырылған қауіпсіздікті қолайсыздық түрінде емес, басымдылық ретінде сезіне бастайды.

5.6 АҚБЖ мониторингі мен талдауы

ТБағалауУ сатысы үшін *ҚР СТ ИСО/МЭК 27001* стандартында айқындалған міндетті (**«ұйым міндетті»**) талаптар “**Іске асыруУ сатысында** іске асырылған АҚБЖ-ны бақылауға және талдауға мүмкіндік беретін қажетті процестер жиынтығын ұйымның қолданатындығына кепілдік беруі үшін даярланған. Ақпараттық қауіпсіздік тәуекелдерін басқарудағы АҚБЖ тиімділігі үшін АҚБЖ-ға әсер етуі мүмкін барлық өзгерістерді бақылау және табу маңызды. Бұл төмендегі өзгерістер нәтижесінде пайда болған қауіптердегі, осалдықтардағы немесе әсерлердегі өзгерістер болуы мүмкін:

– Бизнес ортада немесе соның ауқымында: жаңа бизнес әріптестер; жеткізудің жаңа немесе өзге тізбектері; жаңа, өзге немесе өзгерген клиенттік база; басқа нарықтарға шығу, нарық конъюнктурасы; үшінші тараппен жасалған келісімдер; аутсорсинг бойынша келісім; үйде жұмыс істеу;

– Бизнес-саясат немесе мақсаттарда;

– Ұйымдық құрылымда, жұмыскерлер құрамында, өндірістік жағдайларда;

– Технологияларды пайдалану мен енгізуде: жаңа жүйелер мен қолданбалар, жаңарту, желіні кеңейту, жүйелік платформалардың әр қилылығы, аласталған жұмыстың аумақтылау қолданылуы, сыртқы ұйымдардың кеңірек енуі, аутсорсинг жөніндегі келісімдердің көбірек көлемі;

– Құқықтық және нормативтік кеңістікте.

Бұл мысалдардың барлығында да өзгерту тәуекелдерге және ұйым бизнесіне ықпал ете алады. Тәуекелдердің, қалдық тәуекелдер деңгейі мен жол берілетін тәуекелдер деңгейінің қайта бағалануы АҚБЖ тиімділігін сақтау үшін қажет.

ЗБағалауИ сатысында ұйымға өз АҚБЖ-сының талдауы мен қайта бағалануын өткізуі керек: қолдану саласының дұрыстығы сақталды ма; басқару құралдары жүйесінің дұрыстығы мен тиімділігі сақталды ма; процедуралар дұрыстығы сақталды ма және олар ағымдағы бизнес процестерде дұрыс қолданылып жатыр ма; рольдер мен міндеттердің бөлінуі дұрыс па және қауіпсіздікті қамтамасыз ету жөніндегі әрекеттер өз дәрежесінде орындалып жатыр ма; қауіпсіздік инциденттерін өңдеу процестері өзгерген шарттарға сәйкес келе ме; қауіпсіздік инциденттерін өңдеу процестерінің нәтижелері өз дәрежесінде талқыланды ма; үзіліссіз жұмысты қамтамасыз ету жоспары жаңа шарттарға сәйкес келе ме.

ЗБағалауИ сатысында басқару персоналы жүргізген қауіпсіздік талдаулары, аудитінің және жүйелік сынақтардың, қауіпсіздік инциденттері туралы есептердің, ақпараттық жүйелер иелері, менеджерлер мен пайдаланушылардан келіп түскен ақпараттар мен ұсыныстарды есепке алған жөн - бұның барлығы АҚБЖ-ның қазір де бизнеске сәйкес келетініне және тәуекелдердің қабылданған деңгейінен асырмай, ақпараттық қауіпсіздік тәуекелдерін бұрынғыдай басқаруға мүмкіндік беретініне кепілдік беруге мүмкіндік береді.

5.7 АҚБЖ-ны қолдау және жетілдіру

ТТүзетуУ сатысы үшін *ҚР СТ ИСО/МЭК 27001* стандартында айқындалған міндетті («ұйым міндетті») талаптар **ТБағалауУ** сатысында іске асырылған процестер нәтижелері бойынша АҚБЖ-ны қолдау және жетілдіруге арналған процестердің қажетті жиынтығын ұйымның қолданатындығына кепілдік беру үшін даярланған. **ТБағалауУ сатысында** орындалатын мониторинг пен талдау процесі барысында АҚБЖ-ны жетілдіруді талап ететін өзгерістер сәйкестендірілуі мүмкін, олар ақпараттық қауіпсіздік тәуекелдерін өз дәрежесінде басқаруды қамтамасыз етуге мүмкіндік береді.

Тәуекелдер үнемі ішкі және сыртқы жағдайлар әсерімен өзгеріп отырады. Сондықтан тәуекелдерді **ТБағалауУ сатысында** анықталған өзгерістерге қажетті әрекеттермен қабылдай отырып, алдын ала белсенді басқару қажет. Инциденттер тәуекелдерді іске асыруды көрнекі түрде көрсетуге мүмкіндік береді және олардың нәтижелері бойынша инциденттерге дер кезінде тиімді алдын алуға мүмкіндік беретін кеңейту процедураларын қолдану қажет болады. Тәуекелдер мониторингі үшін үнемі қауіптерді, іске асырылған басқару құралдары жүйесін және олардың тиімділігін талдап отыру, сондай-ақ аудиттер өткізіп отыру керек.

ҚР СТ ИСО/МЭК 27001 стандартында соларға сәйкес АҚБЖ тиімділігін үнемі арттыруға мүмкіндік беретін процестер жиынтығын ұйым қолдануы тиіс процестерге қойылатын талаптар берілген. Бұл процестерге мыналар жатады: ақпараттық қауіпсіздік саясаты мен қауіпсіздік мақсаттарын қолдану, аудит пен талдау нәтижелерін қолдану, мониторинг нәтижелерін зерттеу, сондай-ақ алдын алу және түзету шаралары.

ЗТүзетуИ сатысында барлық АҚБЖ-ның анықталған жетілдірулерін іске асыруға мүмкіндік беретін процестерді қолдану және алдын алу және түзету шараларын *ҚР СТ ИСО/МЭК 27001* стандартына сәйкес қабылдау қажет. Ұйым АҚБЖ-ны іске асыру мен пайдаланудағы сәйкессіздіктерді анықтауы, бұл сәйкессіздіктердің себептерін айқындауы, сәйкессіздік себептерін жою жөніндегі әрекеттер қажеттілігін бағалауы және сәйкессіздіктердің қайтадан пайда болуын болдырмайтын қажетті түзету әсерлерін іске асыруы тиіс. Сондай-ақ, ұйым барлық болу қаупі жоғары сәйкессіздіктер мен олардың себептерін анықтауы, сондай-ақ қажетті алдын алу шараларын айқындауы тиіс.

Бұл қызметтің маңызды аспектісі барлық әрекеттерді, алдын алу және түзету, тіркеуді қамтамасыз етуде, қызығушылығы бар ұйымның барлық қызметкерлерін АҚБЖ жетілдірулері туралы құлағдар етуге мүмкіндік беретін қажетті ақпараттық арналарды қолданған жөн, сондай-ақ қажетті әрекеттердің орындалуына көз жеткізу қажет. Ұйым жоспарланған мақсаттардың орындалуын және іске асырылған жетілдірулердің қажетті талаптарға сәйкестігін қамтамасыз етуі тиіс. Бұл үшін орындалған алдын алу және түзету әрекеттеріне талдау жүргізу қажет.

5.8 Құжаттау жүйесі

5.8.1 Құжаттауға қойылатын талаптар

АҚБЖ-ның *ҚР СТ ИСО/МЭК 27001* стандартының талаптарын қанағаттандыратын басқарудың құжатталған жүйесі болуы маңызды. АҚБЖ жөніндегі құжаттамаға мыналар кіруі тиіс:

– құжатталған қауіпсіздік саясатының ережелері;

– АҚБЖ қолдану саласы;

– АҚБЖ-ны қолдау үшін қолданылатын процедуралар мен басқару құралдары;

– тәуекелдер бағалауы туралы есеп;

– тәуекелдерді өңдеу жоспары;

– ақпараттық қауіпсіздіктің өзіндік процестерін тиімді жоспарлауды, пайдалану мен басқаруды қамтамасыз етуге арналған қажетті ұйымдастыру процедуралары;

– АҚБЖ-ның талаптарға сәйкестіктігін және тиімді жұмыс істеуін растайтын жазбалар;

– сертификаттау үшін міндетті сәйкестіктегі қолданылуы туралы Ереже.

5.8.2 Құжаттар мен жазбаларды басқару

ҚР СТ ИСО/МЭК 27001 стандартында құжаттардың дұрыс қорғалуы мен басқарылуын қамтамасыз етуі тиіс құжаттар мен жазбаларды басқару жөніндегі міндетті талаптар жиынтығы айқындалады. Бұл талаптарды орындау үшін құжаттарды өз деңгейінде қорғауды және оларды басқаруды қамтамасыз етуге мүмкіндік беретін процедуралар мен процестердің жиынтығы қолданылуы тиіс. Құжаттар мен жазбаларды басқару ақпараттық қауіпсіздікті басқарудың өзге құралдарымен қатар іске асырылуы тиіс тәуекелдерді басқару процесінің маңызды бөлігін құрайды.

Жазбалар ақпараттық қауіпсіздікті басқару әлемінде аса маңызды роль атқарады. Ақпараттық қауіпсіздік инцидентін іске асыру барысында бұл инциденттің осы инцидент маңыздылығына сәйкес келетін дер кезі дәрежесінде және басымдылық деңгейінде қарастырылғаны жөн. Көп жағдайларда инцидентті өз деңгейінде қарастыру үшін бірқатар мәліметтер керек болады: инцидент қайда және қашан болды, қандай жағдайларда, не болды, қандай салдарлары болды және т.с.с. Мұндай мәліметтер дұрыс жүргізілген және дәл жазбалардан алынуы мүмкін. Және, әрине, қылмыстық-құқықтық салдарлы инцидент жағдайында айғақтарды жинау мен ұсыну жөніндегі құқықтық талаптары да бар. Сондықтан жазбаны жүргізу ғана маңызды емес, сондай-ақ осы жазбаларды қорғауды қамтамасыз ету, және де олардың тұтастығын, ену мүмкіндігін және құпиялылығын қамтамасыз ету де маңызды.

ҚР СТ ИСО/МЭК 27001 стандартында құжаттар мен жазбаларды басқару жөніндегі талаптар басқару жүйелері жөніндегі өзге стандарттардағы талаптармен мысалы, *СТ РК ИСО 9001* стандартында келістірілген. Бұл ұйымға бірнеше басымдылық береді (бірлескен/кешенді аудиттер өткізу мүмкіндігін қоса алғандағы), құжаттау және жазбалар жүйесін басқару және қолдау үшін қажетті қаржыны үнемдеуге мүмкіндік береді, бизнес ресурстарын жақсырақ бақылауға көмектеседі және неғұрлым жайлы және кешенді басқаруға мүмкіндік береді.

5.9 Басшылық жауапкершілігі

ҚР СТ ИСО/МЭК 27001 стандартына сәйкес басшылық АҚБЖ-ны даярлау, іске асыру, пайдалану, мониторинг, талдау, қолдау және жетілдіру бөлігі болып табылатын процестер мен әрекеттерге өзінің мүдделілігін (қызығушылығын) көрсете білуі керек. Басшылық тарапынан тікелей көрсетілген, айқын және нақты қолдау мына процестер мен әрекеттерді орындау кезінде қажет етіледі: ақпараттық қауіпсіздік саясатын даярлау, мақсаттарды айқындау, рольдер мен міндеттерді бөлісу, бизнес үшін ақпараттық қауіпсіздікті басқару маңыздылығы туралы ұйымды хабардар ету, АҚБЖ-ға арналған құралдарды ұсыну, тәуекелдің қабыл етілетін деңгейін таңдау, сондай-ақ басқарушылық талдауды өткізу.

Ұйым *ҚР СТ ИСО/МЭК 27001* стандартында сәйкестендірілген талаптар мен процестерді (18 тармақтарда айқындалған барлық талаптар мен процестер) іске асыру үшін қажетті құралдардың ұсынылуын қамтамасыз етуі тиіс. Сондай-ақ, ұйым стандартқа сәйкес осы құралдардың өз деңгейінде басқарылуын қамтамасыз етуі тиіс. Ұйымның пайдаланушыларды, кестелік қызметкерлерді, менеджерлерді және егер қажет болса, мердігерлерді олардың қызметтік жағдайлары мен міндеттеріне, сондай-ақ олардың нақты ақпараттық қауіпсіздік жөніндегі міндеттеріне сәйкес келетін қажетті оқытумен қамтамасыз еткені жөн. Ұйымның барлық пайдаланушыларды, кестелік қызметкерлерді, менеджерлерді АҚБЖ-ның тиімділігін қамтамасыз ету мақсатында қажетті хабарландырылуын қамтамасыз еткені жөн және ақпараттық қауіпсіздіктің бизнестің күнделікті маңызды аспектіне деген қатынасын жасау керек. Ұйым өзінің оқыту мен хабардар ету жалпы бағдарламасының құрамдас бөлігі ретінде ақпараттық қауіпсіздікті басқаруды енгізуі тиіс. Ұйымның қызметкерлердің оқыту барысында алған білімдерін, сондай-ақ қызметкерлердің ақпараттық қауіпсіздік мәселесіндегі құзыреттігін есепке ала отырып рольдер мен міндеттерді дұрыс бөлгені қажет. Оқыту мен хабардар ету бағдарламасы барлық қызметкерлер түсінуі тиіс қарапайым түсіну мен құзыреттілік деңгейінен бастап (мысалы, түйінді сөздерді өңдеу, физикалық қауіпсіздік негіздері, электронды поштаны дұрыс қолдану, вирустардан қорғаныс және т.с.с.) барлық қызметкерлерге қажет болатын күрделірек деңгейге дейін (мысалы, желіаралық экранды конфигурациялау, ақпараттық қауіпсіздік инцидентін өңдеу процесі) өзгеруі мүмкін.

5.10 АҚБЖ-ны басшылықтың қайта қарауы

ҚР СТ ИСО/МЭК 27001 стандартына сәйкес басқару персоналы бекітілген жоспарға сай АҚБЖ талдауын өткізуі тиіс. АҚБЖ талдау ұйымға АҚБЖ-ға қандай жетілдіру мен өзгерістер енгізу керектігін айқындауға мүмкіндік береді. **ЗБағалауИ сатысы** (осы стандарттың 4.5 тармағын

қараңыз) АҚБЖ дұрыстығы сақталуы мен өзгерген жағдайдағы ақпараттық қауіпсіздікті қамтамасыз ету тиімділігін бағалау үшін бизнес пен АҚБЖ операциялық кеңістігінде болған өзгерістер мониторингі мен талдауының маңыздылығын атап көрсетеді. Жағдайға талдау жүргізілгеннен соң бірқатар саясаттар мен процестерді қосу/өзгерту/жетілдіру және бірқатар басқарудың техникалық құралдарын қосу/өзгерту/жетілдіру қажет болуы мүмкін. Үнемі іске асырылатын АҚБЖ талдауы мен аудитінсіз АҚБЖ ескіруі, ұйым кездесуі мүмкін тәуекелдерді басқаруда тиімсіз болуы мүмкін және нәтижесінде ұйым ары қарай табыс әкелмейтін және жағдайға сай емес АҚБЖ-ны қаржыландыруды жалғастыра береді.

Ұйым қарастыруы мүмкін аудит пен талдаудың бірнеше типтері бар: бірінші тарап аудиті мен талдауы (мысалы, АҚБЖ-ның ішкі аудиті), екінші тарап аудиті мен талдауы (мысалы, тапсырыс беруші талабы бойынша немесе шарттық міндеттемелермен байланысты) немесе үшінші тарап аудиті мен талдауы (мысалы, сертификаттау жөніндегі тәуелсіз органдар өткізетін *ҚР СТ ИСО/МЭК 27001* стандартына сәйкестікке сертификаттау).

ҚР СТ ИСО/МЭК 27001 стандартында басқарушылық талдаудың соңғы мәліметтері мен қорытындыларына қойылатын нақты талаптар айқындалған. Ұйымның талдау үшін соңғы мәліметтері ретінде жеткілікті және нақты ақпаратты қолдануы маңызды, бұл дұрыс шешімдерді таңдауға және тиісті шараларды қабылдауға мүмкіндік береді. Егер ұйымдарда басқарушылық талдауға көп күш жұмсалатын болса, онда дұрыс шешім қабылдау үшін және уақыт пен қаржыны желге ұшырмас үшін ұйымға ақпараттың жеткілікті көлеміне ену мүмкіндігін қамтамасыз ету маңызды.

ҚР СТ ИСО/МЭК 27001 стандартындағы міндетті талаптарға сәйкес ұйымның АҚБЖ-ның ішкі аудиттерін өткізгені маңызды. Екінші жағынан, үшінші тараптың сертификаттау өткізуі туралы шешімді ұйым басшылығы қабылдайды, және мұндай сертификация міндетті болып табылмайды. Дегенмен *ҚР СТ ИСО/МЭК 27001* стандартының барлық талаптары сертификаттау үшін міндетті болып табылады.

6 Сертификаттық аудиттер

6.1 Жалпы ережелер

Ұйымның ақпараттық қауіпсіздігін басқару жүйесін сертификаттау (АҚБЖ) – бұл көпшілік мақұлдаған кепілдік беру жолы болып табылады, яғни бұл ұйымның *ҚР СТ ИСО/МЭК 27001* халықаралық стандарт талаптарын қанағаттандыратын ақпараттық қауіпсіздікті басқару жүйесін енгізгендігін көрсетеді.

ЕА 7/03 [2] нұсқаулықтары мен критерийлері (EA Guidelines for the Accreditation of bodies operating certification/registration of Information Security Management Systems – Ақпараттық қауіпсіздікті басқару жүйелерін сертификаттау/тіркеу ұйымдарын аккредиттеуге арналған нұсқаулықтар) аккредиттеу жөніндегі Еуропалық қоғамның басылымы болып табылады (ЕА). Еуропа елдерінің аккредиттеу жөніндегі ұлттық ұйымдары ЕА мүшелері болып табылады, мысалы, Ұлыбританияның атынан UKAS, Нидерландыдан – RvA, Швециядан – Swedac ж. т.б. Сертификаттау жөніндегі ұйымдар ЕА 7/03 нұсқаулығындағы талаптарға жауап беруі тиіс, яғни олар қолданатын сертификаттау жүйелері үшінші жақтан тұтастық пен сенімділік критерийлерін қанағаттандырып осы жүйелердің ұлттық және халықаралық қабылдануын оңайлатуы тиіс. Солай етіп, ЕА 7/03 нұсқауы халықаралық сауда мүдделері үшін ұлттық жүйелерді мойындауға негіз болады. Сондықтан, ИСО/МЭК 27001 халықаралық стандартына сәйкестік туралы сертификаттау бойынша осындай мойындауға және мақұлдауға қол жеткізу үшін, сертификаттау жөнінде қызмет көрсеткісі келетін ұйым ЕА 7/03 нұсқаулығына сәйкес ұлттық аккредиттеу алуы тиіс.

ҚР СТ ИСО/МЭК 27001 стандартына сәйкестік туралы аккредиттік сертификаттау ұйымның АҚБЖ-сін бағалауды да қамтиды. АҚБЖ сертификаттау ұйымның тәуекелді бағалау жұмысын бітіргенін және ақпараттық қауіпсіздік бойынша бизнес мұқтаждығын қанағаттандыратын басқару құралдары жүйесін сәйкестендіргенін және енгізгенін дәлелдейді. Ұйымның *ҚР СТ ИСО/МЭК 27001* стандартына, сондай-ақ барлық басқа қосымша құжаттарға сәйкестігі сертификаттық құжатпен немесе сертификатпен дәлелденеді. Бұл ұйымның өз өнімдері мен қызметтері бойынша ақпараттық қауіпсіздіктің белгілі бір дәрежесіне жеткенін білдірмейтінін атап өту керек. Ондай дәрежеге жеткендіктің дәлелін сертификаттауды жүргізетін аудиторларға қауіпсіздікті бағалау түрінде көрсетуге болады, бірақ та мұндай бағалау сертификаттау процесінің бөлігі болып табылмайды.

ҚР СТ ИСО/МЭК 27001 стандартына сәйкестікке сертификаттау толықтай ұйымдардың өз еркімен жүргізіледі. *ҚР СТ ИСО/МЭК 27001* стандартына сәйкестікке сертификаттау процесін табысты аяқтаған ұйымдар өздерінің ақпараттық қауіпсіздікті басқару мүмкіндіктеріне деген сенімін едәуір арттырады, ал бұл ұйымға өз кезегінде бірге жұмыс істейтін өздерінің сауда серіктестерін, тапсырыс берушілерді және акционерлерді сендіруге көмектеседі. Тиісті орган тарапынан берілген *ҚР СТ ИСО/МЭК 27001*

[2] ЕА 7/03 нұсқауының мәтіні үш негізгі көзден құралған: ISO/IEC Guide 62:1996 нұсқауының бастапқы мәтіні (EN 45012:1998 нұсқауы оған пара пар), ИСО/МЭК Нұсқау 62 (IAF Guidance to ISO/IEC Guide 62) қолдану бойынша IAF Басшылық нұсқауларының бастапқы мәтіні және АҚБЖ сертификаттауға/тіркеуге қатысушы ұйымдарға арналған EN 45012 стандартын қолдану туралы қосымша басшылық нұсқаулары бар арнайы мәтін.

стандартына сәйкестік сертификаты, АҚБЖ өз функцияларын орындай алатынын ашық мойындау болып табылады, мұнда ұйым өзінің ақпараттық қауіпсіздікті басқару құралдарының белгілі бір жайларын құпия түрде сақтай алады.

6.2 Бағалау

6.2.1 АҚБЖ қолданылу саласы және сертификаттау

Осы стандарттың 3.4 тармағында көрсетілгендей, ұйымдар өз АҚБЖ қолдану саласын анықтаулары тиіс. Сертификаттау органының ролі осы қолданылу саласын растау болып табылады, яғни ұйымдардың өз АҚБЖ қолданылу саласынан оған кіруге тиісті өз операциялары мен бизнес элементтерін алып тастамағандығының кепілі.

Сертификаттау жөніндегі органдар ұйымның ақпараттық қауіпсіздіктің тәуекелдерін бағалау бойынша бітірген жұмысы ұйымның бизнес-операцияларын дұрыс көрсететініне көз жеткізуі тиіс. *ҚР СТ ИСО/МЭК 27001* стандартында көрсетілгендей, бұл бағалау ұйым іс-әрекеттерінің шекараларын және интерфейстерін қамтуы тиіс. Сертификаттау жөніндегі органдар мұның ұйым қабылдаған тәуекелдерді өңдеу жоспарында және *ҚР СТ ИСО/МЭК 27001* стандартына сәйкес Қолданылу Ережесінде көрсетілгенін растауы тиіс.

АҚБЖ қолдану саласына толық кірмейтін сервистер мен операциялардың интерфейстері сертификатталушы АҚБЖ-де ескерілуі тиіс және ұйым тарапынан орындалатын ақпараттық қауіпсіздік тәуекелдерін бағалауға кіргізілуі тиіс. Жабдықты басқа ұйымдармен бірге пайдалану осындай жағдайға мысал бола алады (мысалы, компьютерлер, телекоммуникациялық жүйелер және т.б.).

ҚР СТ ИСО/МЭК 27001 стандартында көрсетілгендей:

Тәуекелдерді қабылдау критерийлерін қанағаттандыруға қажет деп табылған басқару құралдарының барлық шығарып тастаулары негізделуі тиіс, және тәуекелдерді қабылдау жөніндегі сәйкес шешімдердің жауапты адамдар тарапынан қабылданғаны туралы дәлелдер берілуі тиіс. Егер қандай болмасын басқару құралдары шығарып тасталатын болса, осы стандартқа сәйкес келеді деген мәліметтер жасауға рұқсат етілмейді, және төмендегі жағдайлар оған кірмейді: ерекшеліктер ұйымның ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі мүмкіндігіне және/немесе міндеттемелеріне әсер етпейді, және тәуекелдерді бағалау нәтижелері бойынша анықталған және заңның тиісті талаптарына және нормативтік құжаттарға сәйкес қауіпсіздік талаптарын қанағаттандырады. **4**, **5**, **6**, **7** және **8**, тармақтарда көрсетілген кез-келген талапты алып тастауға рұқсат етілмейді.

6.2.2 Бірнеше алаңды қамтитын АҚБЖ қолдану саласы

Егер бір АҚБЖ бірнеше алаңды қамтитын болса, сертификаттаушы орган барлық осындай алаңдарға қолданылатын сертификат бере алады:

– Барлық алаңдар бір ғана АҚБЖ басқаруымен жұмыс істейді, және ондағы басшылық, басқару және аудит орталықтан іске асырылады, және талдау орталықтағы басшылық тарапынан жүргізіледі.

– Барлық алаңдар үшін ұйымның қауіпсіздікті талдау бойынша ішкі тәртіптеріне сәйкес аудит жүргізілген.

Саны бірден көп (бірнеше алаңдар) алаңдарды қамтитын АҚБЖ-ні анықтағанда мыналарға ерекше назар аудару қажет: интерфейстер мен тәуелділіктерді дұрыс анықтау, осы интерфейстер мен тәуелділіктерді тәуекелдерді бағалау кезінде ескеру және осы бағалау нәтижелерін енгізілген басқару құралдарының жүйесінде дұрыс көрсету.

Егер сертификаттау жөніндегі орган бірнеше алаңдардың аудиті үшін таңдап алу тәсілін қабылдаса, алаңдар арасындағы кейбір айырмашылықтарды ескере отырып бұл тәсіл жартылай селективті және жартылай селективсіз болып табылады, нәтижесінде алаңдар таңдауынан кездейсоқтықты алып тастамай әр түрлі алаңдар жиынтығы таңдалады. Бір АҚБЖ қамтитын жеке алаңдар арасындағы айырмашылықтарға төмендегілер кіреді:

– Осы алаңдардың өлшемдеріндегі айырмашылықтар,

– Осы алаңдарда іске асырылатын бизнестегі айырмашылықтар.

– Әр түрлі алаңдардағы ақпараттық жүйелердің күрделілігі.

– Әр түрлі алаңдарда орындалатын жұмыс практикасындағы және оперативті әрекеттегі айырмашылықтар.

– Әр түрлі алаңдардағы өңделетін ақпарат типтеріндегі айырмашылықтар (сындарлы/сындарлы емес, жасырын/жасырын емес).

– Әр түрлі алаңдарда қолданылатын түрлі құқықтық және нормативтік талаптар.

Сертификаттау жөніндегі орган АҚБЖ-ге кіретін және ресурстарына айтарлықтай қауіп-қатер төнетін, ресурстары осалдау немесе ресурстары ықпалға түсетін әрбір алаң үшін аудит жүргізеді.

Келесі қадағалау аудит бағдарламалары (5.2.6 тармақты қараңыз), тиісті дұрыс уақыт ішінде, ұйымның барлық алаңдарын қамтиды, немесе Қолдану Ережесінде көрсетілгендей сертификатталатын АҚБЖ қолдану саласына кіретін алаңдарды қамтиды.

Бас кеңседе (бас алаңда) немесе АҚБЖ-не кіретін қандайда бір алаңда сәйкессіздік байқалса, түзетуші ықпал бас офиске және сертификат күші әсер ететін барлық алаңдарға қолданылуы тиіс.

6.2.3 Аудит әдіснамасы

ЕА 7/03 нұсқаулығына сәйкес, сертификаттау жөніндегі орган ұйым алаңдарында АҚБЖ аудитін ең аз дегенде екі кезеңде өткізуі тиіс (егер басқа тәсіл негізделмесе, мысалы, сертификаттау процесін шағын ұйымдардың қажеттігіне бейімдендіру). ЕА 7/03 нұсқаулығында аудиттің екі кезеңі анықталған: Аудиттің бірінші кезеңі (Stage 1 Audit) және Аудиттің екінші кезеңі (Stage 2 Audit).

6.2.3.1 Аудиттің бірінші кезеңі

Аудиттің бірінші кезеңінің мақсаттарының бірі бұл сертификаттау жөніндегі органға АҚБЖ-ні, саясатын және ұйымның қауіпсіздік мақсаттарын, тәуекелдерді басқару тәсілін түсіну мүмкіндігін беру болып табылады. Сондай-ақ, аудиттің бұл кезеңі аудиттің екінші кезеңін жоспарлауға назар аударуға мүмкіндік береді, және де ұйымның қандай дәрежеде аудитке дайын екендігін тексеруге мүмкіндік береді.

Аудиттің бірінші кезеңінде құжаттарды талдау іске асырылады және де бұл жұмыс аудиттің екінші кезеңі басталғанға дейін бітуі тиіс. Сертификаттау жөніндегі орган АҚБЖ-сін дайындауға және іске асыруға қатысы бар құжаттарды талдауы тиіс. Бұл құжаттарға ең аз дегенде мыналар кіреді: ұйымның тәуекелдерді бағалау бойынша есебі, тәуекелдерді өңдеу жоспары және Қолдану ережесі, басқа да АҚБЖ-нің маңызды элементтері (осы стандарттың 5.8.1 тармағын қараңыз).

Аудиттің бірінші кезеңінің нәтижелері бойынша жазбаша есеп дайындалады. Бұл есепке кіретін алынған мәліметтер аудиттің екінші кезеңіне өту мәселесі бойынша шешім қабылдау кезінде пайдаланылады. Сондай-ақ, бұл мәліметтер аудиттің екінші кезеңі үшін аудиторлық тексеру тобының мүшелерін тағайындағанда пайдаланылады. Мұнда нақты бір АҚБЖ талдауға қажет біліктілікті ескеру керек. Келесі кезеңге өтуден алдын, сертификаттау жөніндегі орган ұйымға хабарласып, аудиттің екінші кезеңін жүргізгенде толық зерттеу үшін қандай қосымша құжаттар, ақпараттың және жазбалардың қандай басқа түрлері керек болуы мүмкін екендігін хабарлайды.

6.2.3.2 Аудиттің екінші кезеңі

Аудиттің екінші кезеңі бірінші кезең нәтижелері бойынша дайындалған есепке кіргізілген мәліметтерге негізделеді. Осы мәліметтерді пайдалана отырып, сертификаттау жөніндегі орган екінші кезеңге арналған аудит жоспарын жасайды. Аудиттің екінші кезеңі ұйымның АҚБЖ орналасқан алаңында (алаңдарында) өткізіледі.

Аудиттің екінші кезеңіне мыналар кіруі тиіс:

а) Ұйымның өз саясатына, мақсаттарына және процедураларына сәйкес әрекет етіп жатқандығын дәлелдеу;

б) АҚБЖ-нің *ҚР СТ ИСО/МЭК 27001* стандартының барлық талаптарына сәйкестігін дәлелдеу, және оның ұйым саясатымен анықталған мақсаттарға табысты жетуін дәлелдеу (ұйымның *ҚР СТ ИСО/МЭК 27001* стандартының төртіншіден сегізінші тармақтарының талаптарын орындауға мүмкіндік беретін процестер жүйесін пайдалануы тексеріледі);

Аудиттің екінші кезеңінде ұйымда мына мақсаттардың қалай орындалып жатқандығына ерекше назар аудару қажет:

в) Ақпараттық қауіпсіздікпен байланысты тәуекелдерді бағалау және АҚБЖ жасап шығару:

– Тәуекелдерді бағалау тәсілі

– Тәуекелдерді сәйкестендіру

– Тәуекелдерді бағалау

– Тәуекелдерді өңдеу

– Тәуекелдерді өңдеу үшін басқару мақсаттарын және басқару құралдарын таңдау

– Басшылықтың ұсынылып отырған қалдық тәуекелдерді бекітуі

– Қолдану ережесін дайындау

г) Осы процесс нәтижесінде алынған мақсаттарды тексеру;

д) Берілген мақсаттар бойынша мониторинг, өлшеу, есеп және тиімділікті талдау. Ең кем дегенде келесі талаптарды орындауға мүмкіндік беретін процестердің қолданылуын тексеру керек:

– АҚБЖ мониторинг және талдау;

– Басшылық тарапынан АҚБЖ қайта қарау;

– АҚБЖ мейлінше жетілдіру.

е) Қауіпсіздікті талдау және басқару талдауы. Ең кем дегенде келесі талаптарды орындауға мүмкіндік беретін процестердің қолданылуын тексеру керек:

– АҚБЖ мониторинг және талдау;

– Басшылық тарапынан АҚБЖ қайта қарау.

ж) Ақпараттық қауіпсіздік саясатын іске асыру бойынша басшылықтың міндеттерін бөліп беру. Ең кем дегенде келесі талаптарды орындауға мүмкіндік беретін процестердің қолданылуын тексеру керек:

– АҚБЖ мониторинг және талдау;

– Қызметкерлер міндеттерін бөліп беру;

– Басшылық тарапынан АҚБЖ қайта қарау,

з) Төмендегілердің арасындағы байланыстарды анықтау: саясат, ақпараттық қауіпсіздік тәуекелдерін бағалау нәтижелері, мақсаттар, міндеттер, бағдарламалар, процедуралар, тиімділік көрсеткіштері және қауіпсіздік талдаулары (сондай-ақ, *ҚР СТ ИСО/МЭК* 27001 стандартының төртінші - сегізінші тармақтарында берілген әр түрлі әрекеттер, процестер және нәтижелер арасындағы байланыстарды көрсету керек).

6.2.4 Аудит нәтижелері бойынша есеп беру

Сертификаттау жөніндегі орган аудит нәтижелері туралы ұйымды хабардар ету үшін есеп берудің түрлі тәсілдері мен процедураларын пайдалана алады. Олар аудит барысында ұйым офисінде өткізілетін кеңесу кезінде берілетін жазбаша және ауызша есептерді, және аудит соңында берілетін ресми есеп берулерді қамтиды. Бұл есептерде ұйым АҚБЖ-нің *ҚР СТ ИСО/МЭК 27001* стандартының талаптарына сәйкестігі көрсетіледі.

Аудит барысында берілетін есептер ұйымға аудиторлар тарапынан алынған мәліметтер бойынша және олардың шығу себептері туралы сұрақтар беру мүмкіндігін береді. Сертификаттау жөніндегі орган қажетті есептерді ұйымға дер кезінде беруі керек, себебі түрлі сәйкессіздіктер анықталуы мүмкін, және сертификаттаудың барлық талаптарын орындау үшін мұндай сәйкессіздіктерді жою қажет болады.

Ұйым аудит нәтижелері бойынша берілетін есепке өз түсініктемелерін енгізуі тиіс және ол аудит барысында анықталған барлық сәйкессіздіктерді жоюға арналған істеліп жатқан немесе жоспарланған нақты түзету шараларын түсіндіріп беруі тиіс. Сертификаттау жөніндегі орган ұйымға төмендегілерді хабарлауы тиіс: түзету шараларының орындалуын тексеру қажеттілігі, толық және жартылай қайта бағалау өткізу, немесе қадағалау аудиті барысында расталуға тиіс жазбаша мәлімдеменің жеткіліктігі.

6.2.5 Сертификаттау туралы шешім

Ұйымды сертификаттау мүмкіндігі туралы шешім сертификаттау жөніндегі орган тарапынан қабылданады. Бұл шешім аудит барысында алынған ақпараттарға, дәлелдерге және кез-келген басқа маңызды ақпаратқа негізделеді. Сертификаттау мүмкіндігі туралы шешім аудитті өткізуге қатысушылар тарапынан қабылданбауы тиіс.

Сертификатталған ұйымға сертификаттау жөніндегі орган тарапынан *ҚР СТ ИСО/МЭК 27001* стандартына сәйкестік туралы сертификаты беріледі. Бұл сертификатта мынадай мәліметтер көрсетіледі: сертификаттың қолданылу саласы, сертификаттың жарамдылық мерзімі, Қолдану туралы мәлімдеменің нақты бір нұсқасына сілтеме, сертификаттаушы орган мен аккредиттеуші органның логотиптері.

6.2.6 Қадағалаушы аудиттер мен қайталанып өткізілетін аудиттер

Сертификаттау жөніндегі орган жүйелі түрде ұйымның АҚБЖ-ін қадағалайтын аудиттер өткізіп тұруы қажет. Мұндай бақылау аудиттерін өткізу мерзімдерін анықтау сертификаттау органының міндеті болып табылады, бірақ әдетте мұндай аудиттер ұйымдар үшін жарты жылда бір рет өткізілуі тиіс. Мұндай қадағалау аудиттерінің мақсаты сертификат алған ұйымның сертификаттау талаптарына және *ҚР СТ ИСО/МЭК 27001* стандартына сәйкес болып қалуын тексеру болып табылады.

Әдетте АҚБЖ-нің қайталанған аудиттері үш жылда бір рет өткізіледі, яғни *ҚР СТ ИСО/МЭК 27001* стандартына сәйкестік туралы сетификаттың ең ұзақ жарамдылық мерзімі үш жылға тең, осы мерзім біткен соң АҚБЖ қайтадан сертификатталуы тиіс:

– Ұйым АҚБЖ-нің *ҚР СТ ИСО/МЭК 27001* стандарт талаптарына жалпы сәйкестігін тексеру қажет;

– Сертификаттау мерзімі ішінде жүйенің бұрынғы іске асырылуын және қолдауын талдау, ол мыналарды қамтиды:

– АҚБЖ-нің іске асырылуы, оны қолдау және жетілдіру орындалғандығын тексеру;

– АҚБЖ құжаттарын және жүйелі түрде өткізілген АҚБЖ аудиттерінің нәтижелерін талдау, соның ішінде ішкі аудиттер мен қадағалау аудиттері;

– Барлық АҚБЖ элементтері арасындағы қарым-қатынастың тиімділігін тексеру;

– Ұйымның бизнесі мен операцияларындағы өзгерістерді ескере отырып, бірыңғай жүйе ретінде АҚБЖ-нің жалпы тиімділігін тексеру;

– АҚБЖ тиімділігін қолдауға көрсетілген даярлықты тексеру.

А қосымшасы
(анықтамалық)

Ақпараттық қауіпсіздік саясатының мысалы
Ақпараттық қауіпсіздік саясаты

Мақсат

Ақпараттық қауіпсіздік мақсаты – бизнестің тоқтаусыздығын қамтамасыз ету қауіпсіздік инциденттері әсерін алдын алып және азайта отырып, бизнеске келтірілетін шығынды төмендету.

Саясат

– Саясат мақсаты **ұйымның ақпараттық ресурстарын**[3] барлық қауіптерден, ішкі және сыртқы, кездейсоқ және әдейі жасалған, қорғау.

– Ақпараттық қауіпсіздік саясатын атқарушы директор бекітеді.

– Ұйым Саясатты мыналар үшін орындайды:

– **Ақпаратты рұқсат етілмеген енуден қорғауды** қамтамасыз ету;

– Ақпараттың **құпиялылығын** қамтамасыз ету[4];

– Ақпараттың тұтастығын **қолдау**[5];

– Бизнес процестерге қажет болған кезде ақпаратқа **ену мүмкіндігін** қамтамасыз ету;

– **Құқықтық және нормативтік** талаптарды орындау[6];

– **Тоқтаусыз жұмыс істеуді қамтамасыз ету жоспарын** жасау, қолдау және тестілеу[7];

– **Барлық** қызметкерлер үшін **ақпараттық қауіпсіздікке оқытуды** қамтамасыз ету;

– **Барлық ақпараттық қауіпсіздік бұзылулары** туралы, нақты немесе күдік келтіретін, осы бұзылуларды тексеретін **ақпараттық қауіпсіздікке жауапты өкілетті тұлғаға**[8] хабарлау.

---

[3] Ақпараттар әр түрлі формада болады және оған компьютерде сақталатын, желі бойынша берілетін, басып шығарылған немесе қағазға жазылған, факспен жіберілген, ленталар мен дискеттерде сақталатын, сөйлесу кезінде немесе телефомен берілетін мәліметтер кіреді.

[4] Бағалы немесе құпия ақпаратты рұқсатсыз ашу немесе оқылатын түрде ұста алудан қорғау.

[5] Рұқсат етілмеген модификациядан қорғау арқылы ақпараттың дәлдігі мен толықтығын қорғау.

[6] Бұл жазба жүргізуге қатысты және басқару құралдарының көпшілігі ендігі қолданылған болады, оған “Компаниялар туралы” және “Ақпаратты қорғау туралы” заң талаптары кіреді.

[7] Бұл айдаланушыларға талап етілген уақыт пен орында ақпараттар мен маңызды қызметтерге ену мүмкіндігін қамтамасыз етуге мүмкіндік береді.

– Саясатты қолдауға арналған процедуралар бар. Оларға вирустарды қадағалау, кілтсөздерді басқару және бизнестің тоқтаусыздығын қамтамасыз ету процестері жатады.

– Ақпараттар мен ақпараттық жүйелерге ену мүмкіндігіне қойылатын бизнес талаптар орындалатын болады.

– Ақпараттық қауіпсіздік жөніндегі менеджер осы Саясаттың орындалуына және оны іске асыру жөніндегі ұсынымдар мен ұсыныстар беруге тікелей жауап береді.

– Барлық менеджерлер өз қызмет ету саласы шегінде Саясаттың іске асуына, сондай-ақ оның бағынысындағы барлық қызметкерлердің Саясатты сақтауына тікелей жауап береді.

– Ұйымның барлық қызметкерлері Саясаттың сақталуына жауап береді.

Қолы: _____
Қызметі:_____ Күні:_____

(Осы Саясатты ұйым басшылығы әдетте қол қойылған күннен бастап 1 жыл ішінде қайта қарайды.)

[8] Тағайындалған қызметкер тек осы рольді атқаруы немесе оны өзге міндеттермен қоса атқаруы мүмкін.

Қосымша
(анықтамалық)

Библиография

[1] БИС РД 3001:2002 «BS 7799-2 стандартына сәйкестікке сертификаттау үшін дайындық» («Preparing for BS 7799-2 certification»).

ӘОЖ 681.324:006.354 **МСЖ 35.040**

Түйінді сөздер: сертификаттау, стандарт талаптары, ақпараттық қауіпсіздікті басқару жүйесі (АҚБЖ), тәуекелдерді бағалау, басқару құралдары.

Ескертулер үшін

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

ПОРЯДОК ЭКСПЕРТИЗЫ, ОЦЕНКИ И СЕРТИФИКАЦИИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

СТ РК 34.028-2008

Издание официальное

Комитет по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан (Госстандарт)

Астана

Предисловие

1 ПОДГОТОВЛЕН ЗАО «Инфосистемы Джет».

ВНЕСЕН Агентством Республики Казахстан по информатизации и связи.

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан № 107-од от 25.02.2008.

3 СРОК ПЕРВОЙ ПРОВЕРКИ 2013 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

4 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

Информация является одним из самых ценных ресурсов организации. Отсутствие надлежащей защиты информации влечет за собой:

– обнаружение, выдачу или раскрытие информации несанкционированным способом;

– изменение информации без ведома организации с целью снижения ее стоимости;

– бесследная утрата информации без надежды на восстановление;

– недоступность информации для пользователей.

Ответственность за надлежащее обеспечение защиты своей информации от множества угроз, с которыми сталкивается каждая организация, должны нести все ее менеджеры, владельцы или хранители информационных систем и пользователи. Информации необходимо обеспечить защиту и надлежащее управление защитой, как и любому другому важному бизнес-ресурсу организации. Защита и надлежащее управление ею должны осуществляться на непрерывной, превентивной основе.

Указанные выше цели могут быть кратко представлены как необходимость защиты конфиденциальности, целостности и доступности информации – в этом заключается сущность информационной безопасности.

Настоящий стандарт описывает установившуюся практику, на основе которой любые организации – крупные, средние и мелкие – могут разработать, реализовать и сопровождать их системы управления информационной безопасностью (СУИБ) таким образом, что он позволит им получить сертификацию на соответствие стандарту *СТ РК ИСО/МЭК 27001*.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

ПОРЯДОК ЭКСПЕРТИЗЫ, ОЦЕНКИ И СЕРТИФИКАЦИИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ

Дата введения 2008.07.01.

1 Область применения

Настоящий стандарт содержит руководство для пользователей стандартов *СТ РК ИСО/МЭК 27001* и *СТ РК ИСО/МЭК 17799:2005*. Он предоставляет руководство по разработке, реализации, контролю и усовершенствованию СУИБ, т.е. для всего «жизненного» цикла деятельности, необходимого для обеспечения эффективной информационной безопасности.

Настоящий стандарт предназначен тем, кто принимает участие:

– в планировании, разработке и реализации СУИБ,

– в подготовке к аудитам СУИБ,

– в проведении аудитов СУИБ.

Аудиты СУИБ бывают следующих типов: аудиты первой стороны (такие, как внутренние аудиты), аудиты второй стороны (например, аудиты, выполняемые аудиторами заказчиков) и аудиты третьей стороны (например, аудиты, выполняемые независимыми органами сертификации).

Настоящий стандарт предоставляет подробную информацию по реализации процессов, для того, чтобы в результате аудита третьей стороны получить аккредитованную сертификацию на соответствие стандарту *СТ РК ИСО/МЭК 27001*. Чтобы претендовать на соответствие требованиям, содержащимся в стандарте, организация должна продемонстрировать, что она использует все необходимые процессы, и предоставить обоснование необходимости их использования. Несомненно, сами эти процессы приводят к тому, что организация реализует систему управления их рисками. Организация должна реализовать эффективную систему средств управления в качестве части своей СУИБ и должна быть способна продемонстрировать это, приведя необходимые доказательства аудитору СУИБ (независимо от того, проводится ли аудит первой, второй или третьей сторонами).

Настоящий стандарт может использоваться теми, у кого нет непосредственной необходимости аудита, но кому требуется спецификация для разработки и реализации СУИБ на основе принятых в отрасли оптимальных практических методов.

Издание официальное

Однако, чтобы претендовать на соответствие стандарту *СТ РК ИСО/МЭК 27001*, от организации требуется провести, по крайней мере, один внутренний аудит СУИБ, независимо от того, планируется ли в последующем аудит третьей стороны. Организация может не иметь экономических оснований для проведения аудита третьей стороны, но для соответствия стандарту *СТ РК ИСО/МЭК 27001* обязательно должен быть проведен внутренний аудит СУИБ.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие документы:

СТ РК 1.9-2003 Государственная система стандартизации Республики Казахстан. Порядок применения международных, региональных и национальных стандартов и нормативных документов по стандартизации, метрологии, сертификации и аккредитации.

СТ РК ИСО 9001-2001 Система менеджмента качества. Требования.

СТ РК ИСО/МЭК 17799-2006 Информационная технология. Методы обеспечения защиты. Свод правил по управлению защитой информации.

СТ РК ИСО/МЭК 27001-2008 Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования.

СТ РК Информационная технология. Оценка и управление рисками;

СТ РК Информационная технология. Аудит систем управления информационной безопасностью организации.

Руководство ИСО/МЭК 62:1996* Общие требования к органам по сертификации, проводящим сертификацию систем качества.

Руководство ИСО/МЭК 73:2002* Управление рисками. Терминология. Руководство по использованию в стандартах.

ЕА 7/03* Руководства для аккредитации органов по сертификации/регистрации систем управления информационной безопасностью.

3 Определения

В настоящем стандарте применяются термины по *СТ РК ИСО/МЭК 17799*, *СТ РК ИСО/МЭК 27001* и Руководству ИСО/МЭК 73.

---

* Применяется в соответствии СТ РК 1.9

4 Сущность информационной безопасности

4.1 Конфиденциальность

Защита информации в любой форме во время хранения, обработки или передачи, от ее доступности любой организации или любому лицу, которые не авторизованы на это владельцем информации.

Большинство форм управления доступом относятся, главным образом, к защите конфиденциальности. Еще один пример средства управления, который обеспечивает конфиденциальность информации, – это шифрование. Средства управления могут применяться на каждом уровне системы управления информационной безопасностью, физическом уровне (например, замки на дверях и шкафах для хранения документов, сейфы и т.д.) и логическом уровне (отдельные поля данных в базе данных, данные в приложениях и в распечатанном виде). В каждом случае необходимо идентифицировать угрозы и уязвимости, оценить соответствующие риски и для защиты от этих рисков выбрать, реализовать и применить систему средств управления.

4.2 Целостность

Обеспечение точности и полноты информации при ее хранении и передаче; обеспечение корректной обработки информации и недопущение модификации информации несанкционированным образом. Кроме того, желательно установить факт целостности сетей и систем, к которым подключается организация, чтобы гарантировать, что эти сети и системы являются именно теми, к которым планировалось подключение.

Большинство устройств обработки данных содержат средства автоматической проверки целостности данных, позволяющие гарантировать, что эти устройства (включая накопители на дисках и другие носители, а также телекоммуникационные системы), не разрушают данные. Средства контроля целостности играют существенную роль в операционных системах, программном обеспечении и прикладных программах, позволяя предотвратить преднамеренное или случайное повреждение программ и данных во время обработки. На процедурном уровне должны использоваться средства контроля целостности (например, средства контроля для проверки достоверности ввода/вывода данных, обучение пользователей и другие операционные средства контроля), позволяющие уменьшить риск человеческих ошибок, кражи или мошенничества.

4.3 Доступность

Обеспечение доступности информации для тех, кто имеет необходимые полномочия располагать этой информаций, тогда и там, когда и где они должны ею располагать.

На практике, для обеспечения доступности информации требуется система средств управления, например: средства резервного копирования информации, планирование загрузки, процедуры и критерии для приемки систем, процедуры управления инцидентами, управление съемными носителями информации, процедуры обработки информации, сопровождение и тестирование оборудования, процедуры мониторинга использования системы, процедуры обеспечения бесперебойной работы. В качестве превентивного средства управления, обеспечивающего доступность, используется своевременное и непрерывное осуществление мониторинга, анализа и контроля инцидентов безопасности, уровней сервиса и производительности системы.

4.4 Конфиденциальная или критичная информация

Стандарт *СТ РК ИСО/МЭК 17799* определяет совокупность средств управления, которые применяются как к конфиденциальной, так и к критичной информации. Что такое конфиденциальная или критичная информация, и как ее распознать? Для каждой организации будет действовать свое определение. Должны быть определены некоторые методики, которые позволят оценить значимость или полезность информации в контексте отдельной организации, чтобы при необходимости иметь возможность обозначить информацию как конфиденциальную или критичную, а остальную информацию не считать конфиденциальной или критичной.

Существует, кроме того, и временной фактор: финансовая информация организации будет очень конфиденциальна за несколько дней до ее появления на фондовой бирже, но совсем не будет иметь секретности после этого появления. Конфиденциальность будет также отражаться в уровне классификации, который присваивается данным.

Частью процесса оценки рисков (см. *СТ РК*) является оценка информационных ресурсов, которая позволит рассчитать риски и уровень безопасности, необходимый для защиты этих ресурсов с помощью соответствующей системы средств управления.

5 Система управления информационной безопасностью (СУИБ)

5.1 Введение

Фундаментальным для стандарта *СТ РК ИСО/МЭК 27001* является понятие системы управления информационной безопасностью (СУИБ). Система управления информационной безопасностью (СУИБ) – часть общей системы управления, основанная на анализе и оценке бизнес-рисков и предназначенная для разработки, реализации, эксплуатации, контроля, сопровождения и усовершенствования информационной безопасности. Система управления включает в себя организацию, структуру и политики, планирование, распределение обязанностей, инструкции, процедуры, процессы и ресурсы. Область применения системы управления информационной безопасностью, ее администрирование и ресурсы зависят от размеров организации и рассматриваемых информационных ресурсов.

Чтобы быть полезной организации, СУИБ должна быть эффективной. Информационная безопасность должна стать неотъемлемой частью производственной и деловой культуры организации. Информационная безопасность представляет, главным образом, не техническую проблему, а проблему управления, хотя и техническая сторона не должна оставаться без внимания, особенно в условиях сильной зависимости от использования информационных технологий. Управление информационной безопасностью – это не разовое действие, его следует рассматривать как непрерывную деятельность по постоянному усовершенствованию. Хорошо управляемая информационная безопасность – инструмент реализации бизнеса. В современном мире ни одна организация не может успешно функционировать без обеспечения информационной безопасности. Правильно выбранная система средств управления, должным образом реализованная и применяемая, позволит не только вернуть затраченные средства, но и внесет положительный вклад в успех организации.

5.2 Соответствие стандарту *СТ РК ИСО/МЭК 27001*

Будучи практическим руководством, стандарт *СТ РК ИСО/МЭК 17799* имеет форму инструкций и рекомендаций, что означает, что его не следует использовать как спецификацию, и необходимо проявить осторожность, чтобы гарантировать, что заявления о соответствии не вводят в заблуждение.

Будучи спецификацией для СУИБ, стандарт *СТ РК ИСО/МЭК 27001* имеет вид совокупности требований, использующих утверждения в форме предписания **ЗдолженИ** которым должна соответствовать реализованная СУИБ, если организации нужно заявить о соответствии стандарту. В случае *СТ РК ИСО/МЭК 27001* эта совокупность охватывает все требования, связанные с процессным подходом, описанным в данном стандарте.

Выражение **Здолжно бытьИ** показывает, что положения, отражающие требования стандарта *СТ РК ИСО/МЭК 27001*, являются обязательными. Глагол «следует» используется в положениях, которые, хотя и составляют правила по применению требований, не являются обязательными, но рекомендуются к принятию.

5.3 Модель ПРОК (PDCA)

В стандарте *СТ РК ИСО/МЭК 27001* принята модель «Планирование – Реализация – Оценка – Корректировка - ПРОК» («Plan – Do – Check - Act» – PDCA) (см. Рисунок 2). Эта модель используется в качестве основы для разработки, реализации, контроля, анализа, сопровождения и усовершенствования СУИБ.

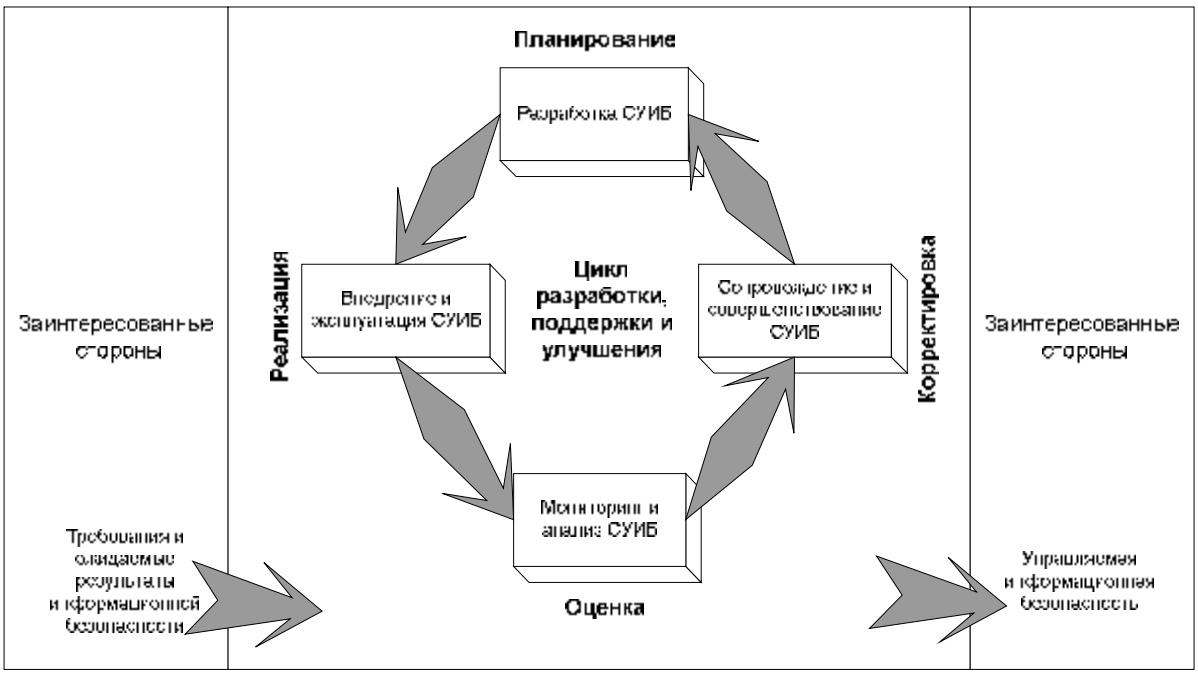


Рисунок 2 – Модель ПРОК в применении к процессам СУИБ

Планирование (разработка СУИБ)	Определение политики безопасности, целей, процессов и процедур, значимых для управления рисками и повышения информационной безопасности, для получения результатов, соответствующих общим политикам и целям организации.
Реализация (внедрение и эксплуатация СУИБ)	Реализация и использование политики безопасности, средств управления, процессов и процедур.
Оценка (мониторинг и анализ СУИБ)	Оценка и, если требуется, измерение характеристик процесса для проверки соответствия политике безопасности, целям и практическому опыту, а также передача результатов для последующего анализа управленческим персоналом.
Корректировка (сопровождение и совершенствование СУИБ)	Принятие корректирующих и превентивных мер по результатам анализа, выполненного управленческим персоналом, с целью постоянного совершенствования СУИБ.

5.4 Разработка СУИБ

В стандарте *СТ РК ИСО/МЭК 27001* определены следующие обязательные (**Зорганизация должнаИ**) требования для этапа «Планирование»:

– **Определить область применения и границы СУИБ** в терминах характеристик бизнеса, организации, ее местонахождения, ресурсов и технологий. Областью применения СУИБ может быть ограниченная и определяемая независимо часть организации, или в качестве области применения может быть определена вся организация. Необходимо, чтобы область применения СУИБ была правильно определена и была полной. Необходимо, чтобы эта область применения учитывала интерфейсы с другими системами, организациями, сторонними поставщиками, и, кроме того, учитывала все зависимости, например, требования безопасности, которые должны быть выполнены с помощью данной СУИБ.

– **Определить политику СУИБ** в терминах характеристик бизнеса, организации, ее местонахождения, ресурсов и технологий с учетом производственных и правовых или нормативных требований, а также договорных обязательств или соглашений с третьей стороной. Политика СУИБ должна утверждаться руководством. Эта политика должна включать в себя общую структуру для определения целей, а также определять общие задачи руководства и принципы деятельности, определять контекст управления рисками и устанавливать критерии, по которым будут оцениваться риски.

– **Определить подход организации к оценке рисков** – это должен быть подход, который наиболее соответствует конкретной СУИБ. Организации необходимо разработать свои критерии для принятия рисков и идентифицировать приемлемые уровни рисков. Решение о выборе метода оценки рисков принимается только самой организацией.

Важно отметить, что какой бы метод ни использовался, необходимо разработать системы управления, охватывающие все области управления из стандарта ИСО/МЭК 27001; необходимо, чтобы этот метод учитывал риски, связанные с организационными аспектами, персоналом, бизнес-процессами, процессами и процедурами эксплуатации и технического обслуживания, правовыми и нормативными требованиями, договорными обязательствами, а также со средствами обработки информации. В *СТ РК* приводится информация об оценке рисков, соответствующая данному этапу, а также этапам г) и д), описанным ниже.

Оценка рисков является обязательным требованием, но при его выполнении не является обязательным применение автоматизированных программных средств, хотя в большинстве случаев использование подобных инструментальных средств является преимуществом, особенно при

необходимости повторной оценки рисков и необходимости обновления связанной с рисками информации, такой как информация об угрозах, уязвимостях и ресурсах. Сложность подхода к оценке рисков будет определяться сложностью рассматриваемой СУИБ. Используемые методы следует согласовывать с уровнем сложности и уровнями гарантии, необходимыми организации.

а) Идентифицировать риски, которым подвергаются ресурсы, с учетом угроз и уязвимостей, связанных с этими ресурсами, и с учетом воздействий, которые могут оказать на эти ресурсы нарушения конфиденциальности, целостности и доступности. И в этом случае необходимо, чтобы риски были связаны со всеми областями управления, как было описано в пункте с) (более подробная информация об оценке рисков приводится в *СТ РК* .

б) Оценить риски, используя информацию, полученную в соответствии с пунктом г), и учитывая все области управления: организационные аспекты, работу с персоналом, бизнес-процессы, процессы и процедуры эксплуатации и технического обслуживания, правовые и нормативные требования, договорные обязательства, а также средства обработки информации (см. *СТ РК* , в котором приводится более подробная информация об оценке рисков). Организации необходимо оценить ущерб, который нарушение безопасности может принести ее бизнесу, и вероятность реализации такого нарушения. Кроме того, организации нужно оценить уровень рисков и в контексте своего собственного бизнеса определить, являются ли риски приемлемыми или же требуется выполнить обработку рисков.

в) Идентифицировать и оценить варианты обработки рисков. Идентифицировав и оценив воздействия, которые риски могут оказать на ее бизнес, организация может предпринять различные действия, которые позволят надлежащим образом управлять этими рисками и обрабатывать их в контексте бизнеса организации. К действиям, которые может рассмотреть организация, относятся: применение надлежащих средств управления для уменьшения рисков, предотвращение рисков через исключение связанной с этими рисками деятельности, передача рисков (полностью или частично) другой стороне (например, страховщику) или сознательное и намеренное принятие риска.

г) Выбрать цели управления и средства управления для обработки рисков. Если организация приняла решение об использовании средств управления для обработки рисков, то сначала ей нужно выбрать систему средств управления, соответствующих этой цели. Средства управления, из которых организация может выбрать необходимые ей, содержатся в Приложении А стандарта *СТ РК ИСО/МЭК 27001*. Кроме того, организации могут потребоваться дополнительные средства управления, не включенные в Приложение А.

При выборе средств управления следует учитывать экономическую эффективность, т.е. стоимость реализации средств управления не должна превышать сумму, на которую с помощью этих средств предполагается уменьшить финансовое воздействие рисков. Безусловно, некоторые воздействия будут иметь нефинансовый характер. Кроме того, следует учесть воздействия, связанные с безопасностью, личной информацией, правовыми и нормативными требованиями, имиджем и репутацией.

д) Подготовить Положение о применимости – Подготовка Положения о применимости является обязательным требованием для организаций, которые хотят добиться сертификации на соответствие стандарту *СТ РК ИСО/МЭК 27001*. Положение о применимости представляет собой документ, в котором перечисляются цели управления и выбранные средства управления, и этот выбор должен быть связан с результатами процессов оценки рисков и обработки рисков. Эта связь должна показывать обоснованность выбора целей управления и средств управления. Только перечисление целей управления и средств управления, без обоснования их выбора, не является допустимым в Положении о применимости.

5.5 Реализация и эксплуатация СУИБ

Обязательные (**Зорганизация должнаИ**) требования, определенные в стандарте *СТ РК ИСО/МЭК 27001* для **этапа ЗРеализацияИ**, разработаны, чтобы гарантировать, что организация использует надлежащий набор процессов, позволяющий реализовать и использовать СУИБ, разработанную на **этапе ЗПланированиеИ** К этим требованиям относится необходимость составления плана обработки рисков, используемого для управления рисками информационной безопасности, которые были идентифицированы и оценены организацией. В этом плане следует определить необходимые действия руководства и идентифицировать обязанности участников процесса управления рисками информационной безопасности, а также обязанности тех, кто участвует в любой деятельности пользователей/менеджеров, значимой для безопасности и связанной с СУИБ.

Организации следует использовать набор процессов, который позволит реализовать план обработки рисков и систему выбранных средств управления, с учетом следующих факторов: финансирование СУИБ, распределение ролей и обязанностей, реализация необходимой программы обучения и оповещения, управление ресурсами и операциями, а также развертывание и применение процедур для управления инцидентами информационной безопасности. Информация о реализации системы средств управления приводится в стандарте *СТ РК* .

Эффективность – это ключевое слово при реализации выбранных средств управления. Средства управления должны быть эффективными в управлении риском (рисками) безопасности, для которого они были

выбраны. Кроме того, следует учесть их экономическую эффективность – средство управления может иметь несколько степеней реализации. Решение о степени реализации (например, о необходимом объеме обучения, документирования или отчетности) должно быть хорошо взвешенным во избежание излишней траты средств. Избыточная реализация может вызвать разочарование персонала, находящегося под влиянием данного средства управления, часто приводя к снижению эффективности всего средства управления. Безопасность и контроль всегда вторгаются в жизнь и рабочую практику людей, но не следует превращать их в бремя.

Кроме того, важно помнить, что безопасность заключается не в том, чтобы не позволить людям делать то, в чем заключается их работа – вовсе нет – она должна обеспечить им возможность делать свою работу при управляемом и эффективном контроле. Она должна позволить им продемонстрировать выполнение своих обязанностей; установить их добросовестность, не оставив и тени сомнений. Вскоре персонал начнет воспринимать правильно реализованную безопасность не как неудобство, а как преимущество.

5.6 Мониторинг и анализ СУИБ

Обязательные (**Зорганизация должнаИ**) требования, определенные в стандарте *СТ РК ИСО/МЭК 27001* для **этапа ЗОценкаИ**, разработаны, чтобы гарантировать, что организация использует необходимый набор процессов, позволяющий контролировать и анализировать СУИБ, реализованную на **этапе ЗРеализацияИ** Для эффективности СУИБ при управлении рисками информационной безопасности важно контролировать и отслеживать все изменения, которые могут повлиять на СУИБ. Это могут быть изменения в угрозах, уязвимостях или воздействиях, возникших в результате изменений:

– в бизнес-среде или контексте: новые бизнес-партнеры; новые или другие цепочки поставок; новая, другая или изменившаяся клиентская база; выход на другие рынки, конъюнктура рынка; договоренности с третьей стороной; соглашения по аутсорсингу; работа на дому;

– в бизнес-политике или целях;

– в организационной структуре, состава работников, производственных условиях;

– в использовании и вводе в действие технологий: новые системы и приложения, модернизация, расширение сети, большее разнообразие системных платформ, более широкое использование удаленной работы, более широкий доступ сторонних организаций, увеличение количества соглашений по аутсорсингу;

– в правовом и нормативном окружении.

Во всех этих примерах изменения могут повлиять на риски и воздействовать на бизнес организации. Повторная оценка рисков, уровня остаточных рисков и уровня приемлемых рисков необходима, чтобы обеспечить сохранение эффективности СУИБ.

На **этапе ЗОценкаИ** организации необходимо провести анализ и повторную оценку своей СУИБ: сохранилась ли адекватность области применения; сохранилась ли адекватность и эффективность системы средств управления; сохранилась ли адекватность процедур и правильно ли они используются в текущих бизнес-процессах; адекватно ли распределение ролей и обязанностей, и выполняются ли действия по обеспечению безопасности надлежащим образом; соответствуют ли изменившимся условиям процессы обработки инцидентов безопасности; были ли должным образом рассмотрены результаты процессов обработки инцидентов безопасности; соответствует ли новым условиям план обеспечения бесперебойной работы.

На **этапе ЗОценкаИ** следует учесть результаты проводимого управленческим персоналом анализа, аудитов безопасности и системных испытаний, отчеты по инцидентам безопасности, информацию и предложения от владельцев информационных систем, менеджеров и пользователей – все это позволит гарантировать, что СУИБ по-прежнему соответствует бизнесу и по-прежнему позволяет управлять рисками информационной безопасности, не допуская превышения уровня приемлемости рисков.

5.7 Сопровождение и совершенствование СУИБ

Обязательные (**Зорганизация должнаИ**) требования, определенные в стандарте *СТ РК ИСО/МЭК 27001* для **этапа ЗКорректировкаИ**, разработаны, чтобы гарантировать, что организация использует необходимый набор процессов для сопровождения и совершенствования СУИБ по результатам процессов, реализованных на **этапе ЗОценкаИ** В ходе процессов мониторинга и анализа, выполняемых на **этапе ЗОценкаИ**, могут быть идентифицированы изменения, требующие усовершенствования СУИБ, которые позволят обеспечить надлежащее управление рисками информационной безопасности.

Риски постоянно изменяются под воздействием внутренних и внешних условий. Поэтому рисками необходимо управлять проактивно, реагируя необходимыми действиями на изменения, идентифицированные на **этапе ЗОценкаИ** Инциденты позволяют наглядно продемонстрировать реализацию рисков, и по их результатам может потребоваться применение процедур эскалации, обеспечивающих своевременное и эффективное реагирование на инциденты. Для мониторинга рисков следует регулярно

анализировать угрозы, систему реализованных средств управления и их эффективность, а также проводить аудиты.

В стандарте *СТ РК ИСО/МЭК 27001* содержится требование, в соответствии с которым организация должна использовать набор процессов, позволяющих постоянно повышать эффективность СУИБ. К этим процессам относится: использование политики информационной безопасности и целей безопасности, использование результатов аудитов и анализа, изучение результатов мониторинга, а также превентивные и корректирующие меры.

На **этапе ЗКорректировкаИ** необходимо использовать процессы, позволяющие реализовать все идентифицированные усовершенствования СУИБ и принимать превентивные и корректирующие меры в соответствии *СТ РК ИСО/МЭК 27001*. Организация должна идентифицировать несоответствия в реализации и эксплуатации СУИБ, определить причины этих несоответствий, оценить необходимость действий по устранению причин несоответствий и реализовать необходимые корректирующие воздействия, исключающие возможность повторного появления несоответствий. Кроме того, организация должна идентифицировать все потенциальные несоответствия и их причины, а также определить необходимые превентивные воздействия.

Важный аспект этой деятельности состоит в том, что следует обеспечить регистрацию всех действий, превентивных и корректирующих, следует использовать необходимые информационные каналы, позволяющие сообщать об усовершенствованиях СУИБ всем сотрудникам организации, которых эти действия затрагивают, а также следует убедиться в фактическом выполнении необходимых действий. Организация должна обеспечить выполнение намеченных целей и соответствие реализованных усовершенствований необходимым требованиям. Для этого необходимо провести анализ выполненных превентивных и корректирующих воздействий.

5.8 Система документации

5.8.1 Требования к документации

Важно, чтобы СУИБ являлась документированной системой управления, удовлетворяющей требованиям стандарта *СТ РК ИСО/МЭК 27001*. Документация по СУИБ должна включать:

– документированные положения политики безопасности;

– область применения СУИБ;

– процедуры и средства управления, используемые для поддержки СУИБ;

– отчет об оценке рисков;

– план обработки рисков;

– процедуры, необходимые организации для обеспечения эффективного планирования, эксплуатации и управления своими процессами информационной безопасности;

– записи, подтверждающие соответствие требованиям и эффективное функционирование СУИБ;

– Положение о применимости в соответствии с обязательным для сертификации требованием.

5.8.2 Управление документами и записями

В стандарте *СТ РК ИСО/МЭК 27001* определяется совокупность обязательных требований по управлению документами и записями, которые должны обеспечить адекватную защищенность и управляемость документов. Для выполнения этих требований должен использоваться набор процедур и процессов, позволяющих обеспечить надлежащую защиту документов и управление ими. Управление документами и записями составляет важную часть процесса управления рисками, которая должна реализоваться параллельно с другими средствами управления информационной безопасностью.

Записи играют особенно важную роль в мире управления информационной безопасностью. При реализации инцидента информационной безопасности важно, чтобы этот инцидент был рассмотрен с той степенью своевременности и тем уровнем приоритета, которые соответствуют серьезности этого инцидента. В большинстве случаев, чтобы рассмотреть инцидент наиболее подходящим образом, требуются некоторые данные: где и когда произошел инцидент, при каких обстоятельствах, что произошло, какие были последствия и т.д. Такие данные могут быть получены из правильно ведущихся, точных записей. И, конечно, существуют правовые требования по сбору и предоставлению доказательств в случае инцидента с уголовно-правовыми последствиями. Поэтому важно не только вести записи, но и обеспечивать защиту этих записей, а также обеспечивать защиту их целостности, доступности и конфиденциальности.

В стандарте *СТ РК ИСО/МЭК 27001* года требования по управлению документами и записями были согласованы с требованиями, содержащимися в других стандартах по системам управления, например, в стандарте *СТ РК ИСО 9001*. Это дает организации несколько преимуществ (включая возможность проведения совместных/комплексных аудитов), позволяет сэкономить средства, необходимые для управления и сопровождения системы документации и записей, помогает лучше контролировать бизнес-ресурсы и позволяет обеспечить более гладкое и комплексное управление.

5.9 Ответственность руководства

В соответствии *СТ РК ИСО/МЭК 27001* руководство должно продемонстрировать свою приверженность (заинтересованность) к процессам и действиям, являющимся частью разработки, реализации, эксплуатации, мониторинга, анализа, сопровождения и совершенствования СУИБ. Прямо выраженная, явная и реальная поддержка со стороны руководства требуется при выполнении следующих процессов и действий: разработка политики информационной безопасности, определение целей, распределение ролей и обязанностей, информирование организации о важности управления информационной безопасностью для бизнеса, предоставление средств для СУИБ, выбор приемлемого уровня риска, а также проведение управленческого анализа.

Организация должна обеспечить предоставление средств, необходимых для реализации требований и процессов, идентифицированных в стандарте *СТ РК ИСО/МЭК 27001* (все требования и процессы, определенные в пунктах с четвертого по восьмой включительно). Кроме того, организация должна обеспечить надлежащее управление этими средствами в соответствии со стандартом. Организации следует обеспечить пользователям, штатным сотрудникам, менеджерам и, если требуется, подрядчикам необходимое обучение, соответствующее их должностным положениям и функциям, а также их конкретным обязанностям по обеспечению информационной безопасности. Организации следует обеспечить необходимое информирование всех пользователей, штатных сотрудников, менеджеров с целью обеспечения эффективности СУИБ и выработки отношения к информационной безопасности, как к важному повседневному аспекту бизнеса. Организации следует в качестве составной части своей общей программы обучения и информирования включить управление информационной безопасностью. Организации необходимо обеспечить правильное распределение ролей и обязанностей с учетом полученного сотрудниками обучения, а также компетентности сотрудников в вопросах управления информационной безопасности. Программа обучения и информирования может варьироваться от уровня простого понимания и компетентности, которыми должны обладать все сотрудники (например, обработка паролей, основы физической безопасности, правильное использование электронной почты, защита от вирусов и т.д.) до более сложных уровней, которые требуются не всем сотрудникам (например, конфигурирование межсетевого экрана, процесс обработки инцидентов информационной безопасности).

5.10 Пересмотр СУИБ руководством

В соответствии с *СТ РК ИСО/МЭК 27001* управленческий персонал должен проводить анализ СУИБ согласно утвержденному плану. Анализ СУИБ позволяет организации определять, какие усовершенствования и изменения необходимо внести в СУИБ. **Этап ЗОценкаИ** (см. п. 4.5 настоящего стандарта) подчеркивает важность мониторинга и анализа изменений, произошедших в бизнесе и операционном окружении СУИБ, для оценки сохранения адекватности СУИБ и эффективности обеспечения информационной безопасности в изменившихся условиях. После анализа ситуации может потребоваться добавление/изменение/усовершенствование некоторых политик и процедур, добавление/изменение/усовершенствование некоторых технических средств управления и т.д. Без анализа и аудита СУИБ, осуществляемых на регулярной основе, СУИБ может устареть, стать неэффективной в управлении рисками, с которыми сталкивается организация, и в итоге организация будет продолжать инвестировать средства в СУИБ, которая больше не приносит пользы и не соответствует ситуации.

Существуют различные типы аудита и анализа, которые может рассмотреть организация: аудит и анализ первой стороны (например, внутренний аудит СУИБ), аудит и анализ второй стороны (например, по требованию заказчика или в связи с договорными обязательствами) или аудит и анализ третьей стороны (например, сертификация на соответствие стандарту *СТ РК ИСО /МЭК 27001* проводимая независимым органом по сертификации).

В стандарте *СТ РК ИСО/МЭК 27001* определяются конкретные требования к исходным данным и итогам управленческого анализа. Важно, чтобы организация обеспечила использование достаточной и точной информации в качестве исходных данных для анализа, что позволит выбрать правильные решения и принять соответствующие меры. Если организациям приходится затрачивать усилия на проведение управленческого анализа, то важно обеспечить доступность достаточного объема информации, чтобы принять верные решения и избежать напрасной траты времени и средств.

Важно, чтобы, в соответствии с обязательным требованием, содержащимся в *СТ РК ИСО/МЭК 27001*, организация выполняла внутренние аудиты СУИБ. С другой стороны, решение о сертификации третьей стороной принимает руководство организации, и подобная сертификация не является обязательной. Однако все требования, содержащиеся в *СТ РК ИСО/МЭК 27001*, являются обязательными для сертификации.

6 Сертификационные аудиты

6.1 Общие положения

Сертификация системы управления информационной безопасностью организации (СУИБ) – это общепринятый способ предоставить гарантию, что данная организация реализовала систему управления информационной безопасностью, удовлетворяющую требованиям стандарта *СТ РК ИСО/МЭК 27001*.

Инструкции и критерии EA 7/03[1] представляют собой публикацию Европейского общества по аккредитации (EA). Членами EA являются национальные органы по аккредитации из европейских стран, так, например, Великобританию в нем представляет UKAS, Нидерланды – RvA, Швецию – Swedac и т.д. В руководстве EA 7/03 определяются требования, которым должны соответствовать органы по сертификации, чтобы используемые ими системы сертификации третьей стороной отвечали критериям целостности и надежности, тем самым, облегчая национальное и международное принятие этих систем. Таким образом, руководство EA 7/03 служит основой для признания национальных систем в интересах международной торговли. Поэтому, чтобы получить подобное признание и одобрение в области сертификации на соответствие международному стандарту ИСО/МЭК 27001, органу по сертификации, желающему предоставлять услуги по сертификации, необходимо получить национальную аккредитацию в соответствии с руководством EA 7/03.

Аккредитованная сертификация на соответствие стандарту *СТ РК ИСО/МЭК 27001* включает в себя оценку СУИБ организации. Сертификация СУИБ подтверждает, что организация выполнила оценку рисков, а также идентифицировала и реализовала систему средств управления, отвечающую потребностям бизнеса в информационной безопасности. Подтверждение того, что организация соответствует стандарту *СТ РК ИСО/МЭК 27001*, а также всем дополнительным документам, будет представлено в виде сертификационного документа или сертификата. Следует отметить, что это не подразумевает, что организация добилась определенного уровня информационной безопасности по отношению к своим продуктам и услугам. Подтверждение, что такой уровень был достигнут, может быть представлено аудиторам, проводящим сертификацию, в виде отдельной оценки безопасности, но такая оценка не является частью процесса сертификации.

Сертификация на соответствие стандарту *СТ РК ИСО/МЭК 27001* носит полностью добровольный характер. Организации, которые успешно завершили процесс могут быть значительно более уверенными в своей возможности управлять информационной безопасностью, а это, в свою очередь, поможет им убедить своих торговых партнеров, заказчиков и

акционеров, с которыми организация ведет бизнес. Сертификат соответствия стандарту *СТ РК ИСО/МЭК 27001*, выданный аккредитованным органом, является открытым признанием способности СУИБ выполнять свои функции, при этом позволяя организации сохранить в тайне конкретные детали своих средств управления информационной безопасностью.

6.2 Оценка

6.2.1 Область применения СУИБ и сертификация

Как указывалось в пункте 3.4 настоящего стандарта, организации должны определить область применения своей СУИБ. Роль органа по сертификации заключается в подтверждении этой области применения, чтобы гарантировать, что организации не исключили из области применения своей СУИБ элементы своих операций и бизнеса, которые должны быть в нее включены.

[1] Текст руководства EA 7/03 составлен из трех основных источников: исходного текста руководства ISO/IEC Guide 62:1996 (которому идентично руководство EN 45012:1998), исходного текста Руководящих указаний IAF по применению ИСО/МЭК Руководство 62 (IAF Guidance to ISO/IEC Guide 62) и специального текста, содержащего дополнительные руководящие указания по применению стандарта EN 45012 к органам, участвующим в сертификации/регистрации СУИБ

Органы по сертификации должны убедиться в том, что выполненная организацией оценка рисков информационной безопасности должным образом отражает ее бизнес-операции и распространяется до границ и интерфейсов ее деятельности, как это определено в стандарте *СТ РК ИСО/МЭК 27001*. Органы по сертификации должны подтвердить, что это отражено в принятом организацией плане обработки рисков и в Положении о применимости в соответствии с *СТ РК ИСО/МЭК 27001*.

Интерфейсы с сервисами и операциями, не полностью попадающими в область применения СУИБ, должны быть учтены в сертифицируемой СУИБ и должны быть включены в выполняемую организацией оценку рисков информационной безопасности. Примером такой ситуации может служить совместное использование оборудования (например, компьютеров, телекоммуникационных систем и т.д.) с другими организациями.

Как указано в *СТ РК ИСО/МЭК 27001*:

Все исключения средств управления, признанные необходимыми для соответствия критериям принятия рисков, должны быть обоснованы и предоставлены доказательства, что соответствующие решения о принятии рисков были приняты ответственными лицами. Если исключаются какие-либо средства управления, заявления о соответствии настоящему стандарту недопустимы, кроме тех случаев, когда исключения не влияют на способность и/или обязательства организации обеспечивать

информационную безопасность, которая удовлетворяет требованиям к безопасности, определенным по результатам оценки рисков, и соответствующим требованиям закона и нормативных документов. Исключение любого из требований, приведенных в пунктах 4, 5, 6, 7 и 8, не допускается.

6.2.2 Область применения СУИБ, охватывающая несколько площадок

В случае если одна СУИБ охватывает несколько площадок, орган по сертификации может выдать сертификат, распространяющийся на все эти площадки, при условии, что:

– все площадки функционируют под управлением одной и той же СУИБ, администрирование, управление и аудит которой осуществляются централизованным образом, и которая подвергается анализу со стороны центрального руководства.

– для всех площадок был проведен аудит в соответствии с внутренними процедурами организации по анализу безопасности.

При определении СУИБ, которая охватывает более одной площадки (несколько площадок), особое внимание следует уделить тому, чтобы соответствующим образом определить интерфейсы и зависимости, учесть эти интерфейсы и зависимости при оценке рисков, а результаты этой оценки надлежащим образом отразить в системе реализованных средств управления.

Если орган по сертификации принимает выборочный подход к аудитам нескольких площадок, то этот подход является частично селективным с учетом некоторых различий между площадками и частично неселективным, и в результате выбирается совокупность различных площадок, без исключения случайности из выбора площадок. К различиям, которые могут быть выделены между отдельными площадками, охватываемыми одной СУИБ, относятся:

– отличия в размерах этих площадок,

– отличия в бизнесе, проводимом на этих площадках,

– сложность информационных систем на различных площадках,

– отличия в рабочей практике и оперативной деятельности, выполняемой на различных площадках,

– различия в типах обрабатываемой информации (критичная/некритичная, конфиденциальная/неконфиденциальная) на различных площадках,

– разные правовые и нормативные требования, применяемые на различных площадках.

Орган по сертификации проводит аудит для каждой входящей в СУИБ площадки, ресурсы которой подвергаются значительным угрозам, уязвимостям или воздействиям.

Программы последующего надзорного аудита (см. п. 5.2.6) охватывают в течение разумного периода времени все площадки организации или те, которые находятся в области применения сертифицируемой СУИБ, как указано в Положении о применимости.

В случае появления несоответствия либо в главном офисе (на главной площадке), либо на какой-либо одной площадке, входящей в СУИБ, корректирующее воздействие должно применяться к главному офису и ко всем площадкам, на которых распространяется действие сертификата.

6.2.3 Методология аудита

В руководстве ЕА 7/03 говорится, что органу по сертификации следует проводить аудит СУИБ на площадках организации, по меньшей мере, в два этапа, если только не может быть обоснован иной подход (например, в случае адаптации процесса сертификации к потребностям очень небольших организаций). В руководстве ЕА 7/03 определяются два этапа аудита: Первый этап аудита (Stage 1 Audit) и Второй этап аудита (Stage 2 Audit).

6.2.3.1 Первый этап аудита

Одна из целей первого этапа аудита состоит в том, чтобы дать возможность органу по сертификации понять данную СУИБ в политике и целях безопасности организации, подходе к управлению рисками. Кроме того, этот этап аудита позволяет сосредоточиться на планировании второго этапа аудита и предоставляет возможность проверить, в какой степени организация подготовлена к аудиту.

На первом этапе аудита проводится анализ документов, который должен быть завершен до начала второго этапа аудита. Органу по сертификации следует проанализировать документы, имеющие отношение к разработке и реализации СУИБ и включающие, как минимум, отчет организации об оценке рисков, план обработки рисков и Положение о применимости, а также другие ключевые элементы СУИБ (см. п. 5.8.1 настоящего стандарта).

По результатам первого этапа аудита составляется письменный отчет. Полученные данные, содержащиеся в этом отчете, используются при принятии решения о том, можно ли переходить ко второму этапу аудита. Кроме того, эти данные используются при назначении членов группы аудиторской проверки для второго этапа аудита, с учетом компетентности, необходимой для рассмотрения конкретной СУИБ. Перед тем, как переходить к следующему этапу, орган по сертификации информирует организацию, какие дополнительные документы, другие типы информации и записей могут потребоваться для детального изучения при проведении второго этапа аудита.

6.2.3.2 Второй этап аудита

Второй этап аудита основывается на данных, содержащихся в отчете, составленном по результатам первого этапа. Используя эти данные, орган по сертификации составляет план аудита для второго этапа. Второй этап аудита проводится на площадке (площадках) организации, где расположена СУИБ.

Второй этап аудита должен включать:

а) подтверждение того, что организация действует в соответствии с ее собственными политиками, целями и процедурами;

б) подтверждение того, что СУИБ соответствует всем требованиям стандарта *СТ РК ИСО/МЭК 27001* и успешно выполняет цели, определенные в политике организации (включая проверку того, что организация использует систему процессов, позволяющую выполнить требования пунктов с четвертого по восьмой включительно стандарта *СТ РК ИСО/МЭК 27001*);

На втором этапе аудита следует уделить особое внимание тому, как в организации выполняются следующие задачи:

в) оценка рисков, связанных с информационной безопасностью, и разработка СУИБ:

– подход к оценке рисков,

– идентификация рисков,

– оценка рисков,

– обработка рисков,

– выбор целей управления и средств управления для обработки рисков,

– утверждение у руководства предлагаемых остаточных рисков,

– подготовка Положения о применимости;

г) проверка целей, полученных в результате данного процесса;

д) мониторинг, измерение, учет и анализ эффективности относительно заданных целей. Необходимо проверить, используются ли процессы, позволяющие выполнять, по крайней мере, следующие требования:

– мониторинг и анализ СУИБ,

– пересмотр СУИБ руководством,

– совершенствование СУИБ;

е) анализ безопасности и управленческий анализ. Необходимо проверить, используются ли процессы, позволяющие выполнять, по крайней мере, следующие требования:

– мониторинг и анализ СУИБ,

– пересмотр СУИБ руководством,

ж) распределение обязанностей руководства по выполнению политики информационной безопасности. Необходимо проверить, используются ли процессы, позволяющие выполнять, по крайней мере, следующие требования:

– мониторинг и анализ СУИБ,

– распределение обязанностей персонала,

– пересмотр СУИБ руководством;

з) определение связей между политикой, результатами оценки рисков информационной безопасности, целями, обязанностями, программами, процедурами, показателями эффективности и анализами безопасности (в том числе, следует показать связи между различными действиями, процессами и результатами, определенными в пунктах с четвертого по восьмой включительно стандарта *СТ РК ИСО/МЭК 27001*).

6.2.4 Отчет о результатах аудита

Орган по сертификации может использовать различные методы и процедуры отчетности, чтобы проинформировать организацию о результатах аудита. К ним относятся письменные и устные отчеты, предоставляемые во время совещаний, которые проводятся в ходе аудита в офисе организации, а также официальные отчеты, предоставляемые по окончании аудита. В этих отчетах указывается соответствие СУИБ организации требованиям стандарта *СТ РК ИСО/МЭК 27001*.

Отчеты, предоставляемые в процессе аудита, дают организации возможность задавать вопросы по полученным аудиторами данным и по причинам их выводов. Орган по сертификации должен своевременно предоставлять организации необходимые отчеты, поскольку могут обнаружиться несоответствия, которые следует устранить, чтобы добиться соответствия всем требованиям сертификации.

Организации предлагается вносить свои комментарии в отчет о результатах аудита и описывать конкретные корректирующие действия, которые она предпринимает или планирует предпринять для устранения всех несоответствий, идентифицированных в ходе аудита. Орган сертификации должен проинформировать организацию, требуется ли для проверки выполнения корректирующих действий провести полную или частичную переоценку, или будет достаточно письменного заявления, которое должно быть подтверждено при проведении надзорного аудита.

6.2.5 Решение о сертификации

Решение о возможности сертификации организации принимается органом по сертификации. Это решение основывается на информации и свидетельствах, полученных в ходе аудита, а также на любой другой существенной информации. Решение о возможности сертификации не должно приниматься теми, кто принимал участие в проведении аудита.

Организация, получившая сертификацию, получает от органа по сертификации сертификат соответствия стандарту *СТ РК ИСО/МЭК 27001*. В этом сертификате указывается такая информация, как область применения сертификата, срок действия сертификата, ссылка на конкретную версию

Заявления о применимости, а также логотипы сертификационного органа и органа по аккредитации.

6.2.6 Надзорные и повторные аудиты

Орган по сертификации должен проводить регулярные надзорные аудиты СУИБ организации. Определение периодичности этих контрольных аудитов – обязанность сертифицирующего органа, но обычно посещения организации с целью проведения таких аудитов необходимо осуществлять раз в полгода. Цель подобных надзорных аудитов заключается в том, чтобы проверить, продолжает ли получившая сертификацию организация соответствовать требованиям сертификации и стандарту *СТ РК ИСО/МЭК 27001*.

Повторные аудиты СУИБ организации обычно проводятся раз в три года, т.е. максимальный срок действия сертификата соответствия стандарту *СТ РК ИСО/МЭК 27001* обычно составляет три года, после чего необходимо выполнить повторную сертификацию СУИБ:

– проверить общее соответствие СУИБ организации требованиям стандарта *СТ РК ИСО/МЭК 27001*;

– проанализировать прошлую реализацию и продолжающееся сопровождение системы в течение периода сертификации, в том числе:

– проверить, что реализация СУИБ, ее сопровождение и усовершенствования выполнялись,

– проанализировать документацию СУИБ и результаты регулярных аудитов СУИБ, включая внутренние аудиты и надзорные аудиты,

– проверить эффективность взаимодействия между всеми элементами СУИБ,

– проверить общую эффективность СУИБ как единой системы, с учетом изменений в бизнесе и операциях организации,

– проверить продемонстрированную готовность поддерживать эффективность СУИБ.

Приложение А
(справочное)
Пример Политики информационной безопасности
Политика информационной безопасности

Цель

Цель информационной безопасности – обеспечить непрерывность бизнеса и минимизировать ущерб бизнесу, предотвращая и минимизируя воздействие инцидентов безопасности.

Политика

– Цель Политики заключается в **защите информационных ресурсов**[1] **организации** от всех угроз, внутренних и внешних, случайных и преднамеренных.

– Политика информационной безопасности утверждается исполнительным директором.

– Организация выполняет Политику, чтобы:

– обеспечить **защиту информации от несанкционированного доступа**,

– обеспечить **конфиденциальность** информации[2],

– **поддерживать** целостность информации[3],

– обеспечить **доступность** информации, когда это необходимо для бизнес-процессов,

– выполнять **правовые** и **нормативны**е требования[4],

– создать, поддерживать и тестировать **планы обеспечения бесперебойной работы**[5],

– обеспечить о**бучение информационной безопасности** для **всех** сотрудников,

– сообщать обо **всех нарушениях информационной безопасности**, фактических и подозреваемых, **уполномоченному лицу**, о**тветственному за информационную безопасность**[6], который будет исследовать эти нарушения.

---

[1] Информация имеет различные формы и включает данные, хранимые на компьютерах, передаваемые по сетям, распечатанные или записанные на бумаге, отправлены по факсу, хранимые на лентах и дискетах, или сообщаемые во время разговора или по телефону.

[2] Защита ценной или конфиденциальной информации от несанкционированного раскрытия или перехвата в читаемом виде.

[3] Защита точности и полноты информации с помощью защиты от несанкционированной модификации.

[4] Это относится к ведению записей, и большинство средств управления уже будет использоваться; это включает требования законодательства, такие как закон «О компаниях» и закон «О защите информации».

[5] Это позволит обеспечить доступность информации и важнейших сервисов пользователям там и тогда, где и когда они им потребуются.

[6] Назначенный сотрудник может исполнять только эту роль или совмещать ее с другими обязанностями.

– Для поддержки политики существуют процедуры. К ним относятся процедуры, контроля вирусов, управления паролями и обеспечения непрерывности бизнеса.

– Будут выполняться бизнес-требования к доступности информации и информационных систем.

– Менеджер по информационной безопасности несет прямую ответственность за выполнение данной Политики и предоставление рекомендаций и указаний по ее реализации.

– Все менеджеры несут прямую ответственность за реализацию Политики в пределах своей области деятельности, а также за соблюдение Политики сотрудниками, находящимися в их подчинении.

– Все сотрудники организации несут ответственность за соблюдение Политики.

Подпись: _____

Должность:_____Дата:_____

(Настоящая Политика пересматривается руководством организации обычно в течение 1 года с момента подписания)

Приложение
(справочное)
Библиография

[1] БИС РД 3001:2002 «Подготовка для сертификации на соответствие стандарту BS 7799-2» («Preparing for BS 7799-2 certification»).

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: сертификация, требования стандарта, система управления информационной безопасностью (СУИБ), оценка рисков, средства управления.

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы, Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074