УДК 873-057.179.4

Ветохин С.С., Кенжеханова М.Б., Қайсарова А.А.*
физ-матем.ғ. к., доцент, БМТУ, Беларусь Республикасы, Минск.
магистр, аға оқытушы М.Әуезов атындағы ОҚУ, Шымкент, Қазақстан
магистр, оқытушы М.Әуезов атындағы ОҚУ, Шымкент, Қазақстан

«ЕРАСЫЛ - ШЫМКЕНТ» ЖШС-НЕISO / IEC 27001 ХАЛЫҚАРАЛЫҚ СТАНДАРТЫ НЕГІЗІНДЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ ЖҮЙЕСІН ЕНДІРУ

Автор корреспондент: kaisarova-92@mail.ru

Түйін: Халықаралық стандарт ақпараттық қауіпсіздікті басқару жүйесін әзірлеу, енгізу, пайдалану, бақылау, талдау, жүргізу және жетілдіру моделі ретінде дайындалған. Ұйымның жобалау мен жүзеге асыруға ұйымның қажеттіліктері мен міндеттері, қауіпсіздік талаптары, қолданылатын процестер және ұйымның жұмыс жасау процестеріне енгізіледі. Зерттеу нысаны - ISO / IEC 27001 халықаралық стандартының талаптары мен ережелері, зерттеу пәні - ISO ережелері, қағидалары мен тұжырымдамалары негізінде «ЕРАСЫЛ - ШЫМКЕНТ» ЖШС-да ақпараттық қауіпсіздікті басқарудың қалыптасу ерекшеліктері. Зерттеудің практикалық маңыздылығы мынада: ISO / IEC 27001 халықаралық стандартына негізделген ақпараттық қауіпсіздік жүйесін қалыптастыру бойынша әзірленген әдістер мен ұсынымдар «ЕРАСЫЛ - ШЫМКЕНТ» ЖШС-да ақпараттық қауіпсіздікті басқару жүйесін енгізудің әдістемелік тәсілдерін тұжырымдауға мүмкіндік береді. Сонымен қатар талдау, зерттеу және критерийлер мен индикаторларды іріктеу негізінде ақпараттық қауіпсіздікті басқару жүйесін құру мен енгізу процедуралары, қажетті құжаттаманы әзірлеу, жүйенің тәуекелдері мен оның жұмысының тиімділігін бағалауғамүмкіндік береді.

Кілт сөздер: ақпарат, ақпаратты қорғау, ақпараттық қауіпсіздік, ақпараттық қатынастардың субъектілері, ақпараттық жүйе, ақпаратты қорғау тәсілі, ақпараттық қауіпсіздікті басқару жүйесі, ақпаратты сақтау ортасы.

Кіріспе. Ақпарат - бұл кәсіпорынға құндылық қосатын және сақтауды талап ететін бизнес-ресурстардың бірі. Ақпараттық қауіпсіздіктің әлсіздігі қаржылық шығындарға және коммерциялық операцияларға зиян келтіруі мүмкін. Сондықтан, кәзіргі таңда ақпараттық қауіпсіздікті басқару жүйесін құру және оны кәсіпорынға енгізу мәселесі өзекті мәселе болып табылады.

ISO / IEC 27001: 2005 халықаралық стандартын «Ерасыл - Шымкент» ЖШС-не ендіру барысында әдістемелер және әдістемелік ұсыныстар жоқтығынан оны әзірлеу мен енгізу кезінде бірқатар кедергілер кездеседі. Сонымен қатар, кәсіпорынның барлық процестерін жетілдірудің және оның тиімділігін бағалаудың ең тиімді құралы ретінде дамыған жүйені кәсіпорынның жалпы басқару мәселесіненгізу барысында мәселелер туындайды[5].

Теориялық талдау. Көзделген мақсатқа жету үшін бірқатар теориялық, ғылыми және практикалық мәселелерді шешу қажет, атап айтқанда:

- ақпараттық қауіпсіздікті басқару жүйесін Қазақстан Республикасында, жақын және алыс шетелдерде ИСО / МЭК 27001 халықаралық стандартының талаптарына сәйкесіншеендіру мүмкіншіліктерін талдау.
- көрсетілген құжат талаптарына сәйкес келетін ақпараттық қауіпсіздікті басқару жүйесінің негізгі элементтерін анықтау.

Алдымен ақпараттық жүйе ұғымына түсініктеме беріп өтсек: автоматтандырылған ақпараттық жүйе - белгіленген функцияларды орындау үшін ақпараттық технологияларды ұсынатын техникалық (аппараттық) және бағдарламалық құралдардың, сондай-ақ олармен жұмыс істейтін пайдаланушылардың (персоналдың) жиынтығы[2].

«Ерасыл - Шымкент» ЖШС-не стандартты енгізу барысында ең маңызды мәселелерінің бірі - бұл құпия ақпаратты қорғау. Ақпарат әр түрлі формада болуы мүмкін: оны басып шығаруға немесе қағазға жазуға, электронды түрде сақтауға, пошта арқылы жіберуге немесе электронды құралдардың көмегімен көшіруге болады, оны видео материалдарда, таспаларда ұсынуға немесе сөйлесуде білдіруге болады. Кәсіпорында олардың ақпараттық жүйелері мен желілері көптеген түрлі ақпарат көздерінен, оның ішінде компьютерлік алаяқтықтан, тыңшылықтан, диверсиядан, бұзақылықтан, өрттен немесе су тасқынынан келетін қауіп-қатерлерге тап болуы мүмкін. Зиянды код, компьютерлік бұзу және заңды

қолданушыларға қызмет шабуылдарынан бас тарту сияқты зиян келтіру сияқты қәуіптер бар. Ақпараттың қандай формада сақталуына, қандай құралдар арқылы таратылуына немесе сақталуына қарамастан, олар әрқашан тиісті түрде қорғалуы керек. Кәсіпорын басшысы ақпараттық жүйелердің қазіргі жағдайын объективті бағалауы, ақпараттық қолдаудың қажеттіліктері мен бар ақпараттық проблемаларды көруі және түсінуі керек. Бұл басқару құралдары іскерлік ақпаратты қорғаудың нақты ұйымдастырушылық мақсаттарына жету үшін жасалуы, енгізілуі, үздіксіз бақылануы, талдануы және жетілдірілуі қажет[1].

Ақпараттық қауіпсіздікті басқару жүйесін жоспарлау кезінде «Ерасыл - Шымкент» ЖШС мәселелер мен талаптарды ескеріп, ақпараттық қауіпсіздікті басқару жүйесінің күтілетін нәтижелерге қол жеткізуі үшін ескеру қажет тәуекелдер мен мүмкіндіктерді анықтауы керек, сонымен қатар керексіз әсерлердің алдын алу немесе азайту және үнемі жақсартуға қол жеткізуі қажет[3].

Нәтижелер мен талқылау. Ақпараттық процестердің негізгі компоненттері:

1. Мәліметтерді қажетті формаға айналдыру және оларды сақтау
2. Ақпаратты жинау, сақтау, беру, кодтау, өңдеу және қорғау
3. Мәліметтерді жинау, сұрыптау және өңдеу, оларды қажетті формаға ұсыну
4. Бастапқы хабарламаларды қалыптастыру және оларды адамның қабылдауына қолайлы формада ұсыну

Ақпараттық процестің схемасында оның рұқсат етілмеген немесе кездейсоқ әсерден қорғанысы жатыр. Ақпараттық қауіпсіздікті реттеудің дүниежүзілік практикасы таяуда ғана уәкілетті органдардың міндетті талаптарынан тұрды. Осылайша, кісіпорындарды басқару үшін бір ғана міселе болды - бұл барлық осы талаптар мен ұсыныстарды орындау мәселесі, ал реттеушілер үшін - олардың жиынтығын әмбебаптандыру мәселесі.

Сонымен, басқару жүйесі - бұл компания басшылығы тұжырымдаған мақсаттарға жетудің құралы. Халықаралық ISO стандарттарының ішінде сапа менеджменті жүйелеріне қойылатын талаптарды анықтайтын ISO 9000 сериясы ерекше орын алады[2].

Ақпараттық қауіпсіздікті басқару жүйесін сертификатын алу «Ерасыл - Шымкент» ЖШС-не төмендегі артықшылықтарды береді:

клиенттердің, серіктестердің және басқа мүдделі тараптардың сенімін арттыру;

ұйымдардың жұмысының тұрақтылығын арттыру;

халықаралық мойындау және компанияның ішкі және сыртқы нарықтағы беделін нығайту;

ақпараттық қауіпсіздікке төнетін нақты қауіп-қатерлерден қорғау бойынша іс-шаралардың барабарлығына қол жеткізу;

ақпараттық қауіпсіздік инциденттерінен болатын залалдың алдын алу және (немесе) азайту;

мүдделі тараптардың ақпаратының құпиялығын қамтамасыз ету үшін ақпараттық қауіпсіздіктің белгілі бір деңгейін көрсету;

материалдық емес активтер құнының өсуі, компанияның құнын жоғарылататын сақтандыру сыйлықақыларының төмендеуі;

операциялық шығындарды төмендету және бірыңғай ақпараттық қауіпсіздікті басқару жүйесін шеңберінде «кросс» қаржыландыруды жою;

компанияның ірі мемлекеттік келісімшарттарға қатысу мүмкіндігін кеңейту;

PCI DSS, ISO / IEC 20000-1 стандарттарына сәйкестігі бойынша аудиттің өтуін айтарлықтай жеңілдетуі мүмкін

Ақпараттық қауіпсіздікті басқару жүйесін сертификаттауының жалпы жоспары келесідей:

- ISO / IEC 27001: 2013 талаптарына сәйкес ақпараттық қауіпсіздікті басқару жүйесін қолдану аясын алдын-ала анықтау (ақпараттық қауіпсіздік тұрғысынан ең маңызды бизнес-процестерді оқшаулау және анықтауғаарналған сауалнама жүргізу)[5];

Осы жүйені халықаралық стандарттартқа сәйкес сертификаттау немесе оларды біріктіру процедурасы 4 кезеңге бөлінеді:

1. Сертификаттауға дайындық - Тапсырыс берушінің сауалнамасын, аудиторлық тапсырыстардың нысанын толтыру, келісімшарт жасау;

2. Бірінші кезеңнің аудиті - аудиторлық жоспарды келісу және жүзеге асыру, аудиттің 1-кезеңі бойынша есеп алу, соның ішінде басқару жүйесінің құжаттамасын талдау және 2-ші кезеңге дайындықты бағалау;

3. Екінші кезең аудиті - ағымдағы жоспарлау жүйесінің тиімділігін талдаумен, анықталған ауытқуларға / ескертулерге түзетулер мен түзетулерді қоса алғанда, аудиторлық жоспарды бекіту және жүзеге асыру, аудиторлық есеп алу;

4. Сертификат беру және қадағалау - қадағалау және қайта сертификаттау тексерулерінен өту арқылы сертификаттың қолданылу шарттарының орындалуы және қолданылу мерзімін ұзарту.

Ақпараттық қауіпсіздікті басқару жүйесін құру кезеңдерін жобалау бойынша ұсыныстар «Ерасыл - Шымкент» ЖШС-не көрсетілген стандартты ендіру 6 сатыдан тұрады:

1 саты:Ақпараттық қауіпсіздікті басқару жүйесін жоспарлау және құру. Бұл сатыда қорғауға жататын ақпараттық жүйенің объектілерін (ақпараттық-техникалық ресурстар) анықтау қажет.Ресурстар мен технологиялардың анықтамасын беру қажет.Ықтимал қауіптер мен ақпараттың ағып кету арналарын анықтау (сәйкестендіру (тәуекелдер).

Ақпарат үшін қауіптер мен қауіптерді бағалау,ақпараттық қауіпсіздік жүйесіне қойылатын талаптарды анықтау жатады.

2 саты: Ақпараттық қауіпсіздікті басқару жүйесін әзірлеу. Тәуекелді бағалау әдісі туралы шешім қабылдау; тәуекелді бағалау туралы есеп; тәуекелді емдеу жоспарын құру; рәсімдерді әзірлеу; іс қағаздарын жүргізу;персоналды оқыту, лауазымдық нұсқаулықтармен танысу жатады.

3 саты: Ақпараттық қауіпсіздікті басқару жүйесін іске асыру және пайдалану. Бұл сатыда іске асырылатын әрекеттерге:

Қолдануға болатындығы туралы мәлімдеме жасау. Басқару әрекеттерін, ресурстарын, міндеттері мен басымдықтарын анықтау. Тәуекелдерді емдеу жоспарын құру және жүзеге асыру.

Қауіпсіздік оқиғаларын анықтау және қауіпсіздік оқиғаларына жауап беру процедуралары мен бақылауды жүзеге асыру

4 саты: Мониторинг және талдау.Мониторинг процедураларын орындау және рәсімдерді талдау,бақылаудың тиімділігін өлшеу,тәуекелдерді бағалау талдауын жүргізу.

5 саты: Жүйені жақсарту.

Мүдделі тараптарға шаралар мен жақсартулар туралы хабарлау іске асырылады.

6 саты: Ақпараттық қауіпсіздікті басқару жүйесін сертификаттау.

Сертификаттауға өтініш беру. Келісім-шартын жасасу. Қажетті құжаттар пакетін дайындау. Сәйкестікті растау үшін құжаттаманы органға беру.Сыртқы аудитке дайындық. Сертификаттық аудит жүргізу.Сәйкессіздіктерді анықтауСәйкессіздіктерді талдау. Ақпараттық қауіпсіздікті басқару жүйесі құжаттамасына енгізілген өзгерістер. Түзету бойынша есептер ұсыну растау органына әрекеттер сәйкестік.Сертификат алу үрдістері кіреді[6].

Ауқымды таңдау және осы ауқымға енетін ақпараттық қауіпсіздікті басқару жүйесі бизнес-процестерінің тізімін жасау әрдайым әр түрлі себептермен, мысалы, қаржылық себептермен толықтай жүзеге асырыла бермейді. Сертификатталған көлемді мақұлдағанға дейін компаниядағы барлық қолданыстағы бизнес-процестердің тізімі деп аталатын бақылау тізімі жасалынып, оның ішінен ақпараттық қауіпсіздік тұрғысынан ең маңызды процестер таңдалуы керек. Бұл клиенттің деректерін өңдеу және сақтау, қаржылық операциялар, құпия деректермен жұмыс немесе басқа нәрсе болуы мүмкін. Іріктеу барысында клиенттердің сұраныстары сияқты сыртқы факторды ескеру маңызды.

«Ерасыл - Шымкент» ЖШС-де құрылатын жұмыс тобы мүшелері:

1. Компания директоры.

2. Қаржы және даму жөніндегі директор.

3. Стандарттау жөніндегі маман (құжаттармен жұмыс істеуге жауапты тұлға ретінде).

4. Ақпараттық қауіпсіздік менеджері.

5. Жүйелік әкімші.

Қызметкерлер саны компанияның көлеміне және сертификаттауды таңдау туралы шешім қабылдаған процестерге байланысты. Алайда команда кем дегенде үш адамнан тұруы керек. Дәл сол адамдар комиссия құрамына кіреді. Ақпараттық қауіпсіздікті басқару жүйесін құру және енгізу барысында белгілі бір іс-шараларды жүзеге асыруға қатысты мәселелерді талқылайды және шешімдер қабылдайды[7].

Ақпараттық қауіпсіздікті басқару жүйесін сертификаттау кезінде «Ерасыл - Шымкент» ЖШС-гі әзірлеуі және көрсетуі керек алғашқы құжат - бұл Саясат.

Ақпараттық қауіпсіздік саясаты дегеніміз - бұл ақпараттық қауіпсіздікті басқару жүйесін

негізгі мақсатын сипаттайтын шағын, жоғары деңгейлі құжат. Ақпараттық қауіпсіздікті басқару жүйесі мақсаттарын әдетте жеке құжатта анықтауға болады, бірақ оларды ақпараттық қауіпсіздік саясатына енгізуге болады.

Саясаттың негізгі мақсаты - компанияның ақпараттық ресурстарын барлық ішкі, сыртқы, қасақана немесе кездейсоқ қауіптерден қорғау.

Мұндай кестені әзірлеу тәуекелдерді одан әрі өңдеу үшін қажет, атап айтқанда белгілі бір қатерлерді жою және тәуекел деңгейін төмендету әдістерін таңдау.

Сонымен қатар тәуекелдерді бағалау және жою жөніндегі нұсқаулық - бұл тәуекелді бағалау және жою процедураларын орындауға дейін жазылуы керек 4-5 беттен тұратын құжатты ізңрлеу қажет.Тәуекелді бағалау туралы есеп тәуекелді бағалау және тәуекелдерді жою рәсімдері орындалғаннан кейін жазылады. Бұл есеп барлық нәтижелерді қорытындылауы керек[4].

Қатынауды басқару саясатын әзірлеу бойынша ұсыныстар:Бұл құжатты әзірлеу Ақпараттық қауіпсіздікті басқару жүйесінле міндетті болып табылады, өйткені ол физикалық объектілерге де, логикалыққа да қол жеткізу ережелерін анықтайды. Тәуекелді бағалау және тәуекелдерді жою процестері аяқталғаннан кейін әзірленеді. Мысал ретінде:

1. Компанияның ақпараттық ресурстарына қол жеткізу. Бұл құпия ақпараты бар кәсіпорынның ақпараттық ресурстарына қол жетімділік қызметкерлерге ақпаратты жария етпеу туралы келісімге қол қойғаннан кейін беріледі.

2. Келісім-шарт аяқталғаннан кейін кәсіпорын ресурстарының қайтарылуы. Кәсіпорын қызметкері жұмыстан босатылған және / немесе келісімшартты бұзған жағдайда, оған жұмыс (қызметтер көрсету) үшін берілген барлық ақпараттық ресурстарды, сондай-ақ құпия ақпараты бар барлық ақпарат құралдарын дереу қайтаруға міндетті. Оларға компанияның немесе оның клиенттерінің, олардың көшірмелері, қолжазбалар, сызбалар, сызбалар, сызбалар, магниттік таспалар, фотосуреттер, дискілер, иілгіш дискілер, принтердегі басылымдар, пленка, фото негативтер және басқа ақпарат құралдары жатады.

3. Корпоративтік желіні және Интернетті пайдалану. Пайдаланушы басқа пайдаланушыларға тиесілі кез-келген файлды файл иесінен алдын ала рұқсатынсыз оқымауы, өзгертпеуі, өшірмеуі немесе көшірмеуі керек. Егер қол жетімділік барлық пайдаланушылар үшін нақты түрде орнатылмаған болса, жалпы каталогтардағыдай, басқа пайдаланушыларға тиесілі файлдарды оқу, өзгерту, жою немесе көшіру мүмкіндігі бұл әрекеттерді орындауға рұқсат бермейді. Пайдаланушы ақпараттық жүйелерді қорғаудағы осалдықтарды, осы жүйелерді зақымдауға[4].

Сонымен қатар кәсіпорын оқу, дағды, тәжірибе және біліктілік туралы жазбалар жүргізуі керек. Әдетте бұл жазбалар кадрлар бөлімінде сақталады. Осылайша, кәсіпорында әр қызметкердің оқуы мен біліктілігін арттыру фактісін растайтын барлық құжаттары бар папка болуы керек.

Қорытындылар. Қорыта келгенде, ақпараттық қауіпсіздіктің бүкіл әлемдегі қолданыстағы тәсілдері компаниялардың материалдық емес активтерін қорғауға деген шұғыл қажеттілігі негізінде дамыды, оған бірінші кезекте ақпараттық ресурстар кіреді. Ақпараттық желілер мен жүйелер, қызметкерлер, жабдықтаушылар, тұтынушылар, қаржы институттары мен мемлекеттік органдар бұл қауіптердің көзі бола алады. Әлсіз қорғаныс сонымен қатар қауіпсіздіктің тұрақты көзі болып табылады. Бұл құнды бәсекелестік артықшылықты жоғалтуға, ақпараттың ағып кетуіне, клиенттердің мәліметтер базасын ұрлауға және тікелей қаржылық шығындарға әкелуі мүмкін. Сонымен қатар, «Ерасыл - Шымкент» ЖШС-гі клиенттің өзіне берген құпия ақпаратты қорғай алмауына байланысты өзінің имиджін жоғалтады.

Әдебиеттер тізімі:

1 ISO / IEC 17799: 2005 Ақпараттық технологиялар - Қауіпсіздік техникасы - Ақпараттық қауіпсіздікті басқарудың практикалық кодексі.

2 ISO 9001-2000 сапа менеджменті жүйелері - талаптар.

3 ISO 14001: 2004 Экологиялық менеджмент жүйелері - пайдалану жөніндегі нұсқаулықтағы талаптар.

4 Сячина Т.Ю. Ақпараттық қауіпсіздікті басқарудың заманауи әдістері туралы // СПбПУ ғылыми-техникалық мәлімдемелері. Жаратылыстану және инженерлік ғылымдар, 4-2 (183), 2013. С.284-286.

5 ҚР СТ ИСО / МЭК 27001-2015 Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар. Кіру режимі: https://online.zakon.kz/Document/?doc_id=30435994&doc_id2

6 Горбунова Ю.И. Ақпараттық инфрақұрылым: заманауи мәні, оның құрамдас бөліктері // Әлеуметтік-экономикалық құбылыстар мен процестер. 2014. №2. С. 14-21.

7 Дементьева А.Г. Жаһанданудың қазіргі жағдайлары және трансұлттық корпорациялардың рөлі // XXI ғасыр бастамалары. 2010. № 1-бет 59-64.

Abstract: International Standard is designed as a model for the development, implementation, operation, control, analysis, maintenance and improvement of information security management systems. An organization's design and implementation includes the organization's needs and objectives, security requirements, applicable processes, and the organization's operating processes. The object of research is the requirements and provisions of the international standard ISO / IEC 27001, the subject of research is the peculiarities of the formation of information security management at ERASYL-SHYMKENT LLP on the basis of the provisions, principles and concepts of ISO / IEC 27001. The practical significance of the research is that the developed methods and recommendations on the formation of an information security system based on the international standard ISO / IEC 27001 allow to formulate methodological approaches for the implementation of an information security management system at ERASYL-SHYMKENT LLP on the basis of analysis, research and selection of criteria and indicators of stages and procedures for creating and implementing a management system information security, develop the necessary documentation, assess the risks of the system and the effectiveness of its functioning.

Keywords: information, information protection, information security, subjects of information relations, information system, method of information protection, information security management system, information storage environment.

Аннотация: Международный стандарт разработан как модель для разработки, внедрения, эксплуатации, контроля, анализа, обслуживания и улучшения систем менеджмента информационной безопасности. Дизайн и реализация организации включает потребности и цели организации, требования безопасности, применимые процессы и операционные процессы организации. Объектом исследований является требования и положения международного стандарта ИСО/МЭК 27001, предметом исследований - особенности формирования управления информационной безопасности на ТОО «ЕРАСЫЛ - ШЫМКЕНТ» на основе положений, принципов и концепций ИСО/МЭК 27001. Практическая значимость исследования состоит в том, что разработанные методики и рекомендации по формированию системы информационной безопасности на основе международного стандарта ИСО/МЭК 27001 позволяют сформировать методологические подходы по внедрению на ТОО «ЕРАСЫЛ - ШЫМКЕНТ» системы управления информационной безопасности, которая сформирована на основе анализа, исследований и выбора критериев и показателей этапов и процедур создания и реализации системы управления информационной безопасностью, разработать необходимую документацию, провести оценку рисков системы и результативность ее функционирования.

Ключевые слова: информация, защита информации, информационная безопасность, субъекты информационных отношений, информационная система, способ защиты информации, система управления информационной безопасностью, среда хранения информации.