ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

СОВЕТ МОЛОДЫХ УЧЕНЫХ

Студенттер мен жас ғалымдардың «ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2014» атты IX халықаралық ғылыми конференциясы

IX Международная научная конференция студентов и молодых ученых «НАУКА И ОБРАЗОВАНИЕ - 2014»

The IX International Scientific Conference for students and young scholars «SCIENCE AND EDUCATION-2014»

2014 жыл 11 сәуір
11 апреля 2014 года
April 11, 2014

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2014» атты IX Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ IX Международной научной конференции студентов и молодых ученых «Наука и образование - 2014»

PROCEEDINGS of the IX International Scientific Conference for students and young scholars «Science and education - 2014»

2014 жыл 11 сәуір

Астана

УДК 001(063)
ББК 72
Ғ 96

Ғ 96

«Ғылым және білім – 2014» атты студенттер мен жас ғалымдардың IX Халықаралық ғылыми конференциясы = IX Международная научная конференция студентов и молодых ученых «Наука и образование - 2014» = The IX International Scientific Conference for students and young scholars «Science and education - 2014». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2014. – 5831 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-610-4

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(063)
ББК 72

ISBN 978-9965-31-610-4

құру мүмкіндігі жоқ Multiple Choice Question 6.0, ал басқа жағдайларда Multiple Choice Question 6.5 қолданылады.

Қорытынды

Аталмыш программалық дестеде бірқатар кемшіліктердің бар болғанына қарамастан, ол мультимедиалық оқулық құруға арналған қуатты құрал болып қала бермек. Жоғарыда аталған ерекшеліктерге назар аударып, маңызды функцияларды пайдаланар болсақ, өте ыңғайлы, көрнекі оқыту құралын жасап шығуға болады.

Қолданылған әдебиеттер

1. Гультяев А. К. Macromedia Authorware 6.0. Разработка мультимедийных учебных курсов. СПб.:Учитель и ученик; Корона принт, 2002;
2. Э.К.Шахов, А.И.Надеев, В.В.Акинин, Е.М.Голобокова. Разработка мультимедийных учебников: эффективность и «подводные камни»;

ӘӨЖ 004:006. 067

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУДЫ СТАНДАРТТАР ТАЛАПТАРЫ БОЙЫНША БАҒАЛАУДЫҢ ЭКСПЕРТТІК ЖҮЙЕСІ

Байғабыл Ұлдана Дәулетбекқызы
baigabyl_uldana@mail. ru
Л. Н. Гумилев атындағы ЕҰУ Теориялық информатика кафедрасының
4 курс студенті, Астана, Қазақстан
Ғылыми жетекшісі-т. ғ. к. Ниязова Р. С.

Қазіргі уақытта эксперттік жүйе технологиясы кең таралған. Эксперттік жүйе жасанды интеллект бөлігі болып табылады. Эксперттік жүйе тәжірибемен алмасу, жоғары деңгейдегі мамандардың білімі және басқару процесінде осы біліммен пайдалану үшін арналған. Эксперттік жүйені құру негізінде білім беру моделіне негізделетін білім базасы жатыр. Эксперттік жүйе ядросын білім базасы құрайды, ол құру процесінде жинақталады және құрастырылады. Білімді жинау және ұйымдастыру – эксперттікжүйеніңеңмаңыздысипаттамасыныңбірі. Эксперттік жүйенің пайдалы сипаттамалары олар шешім қабылдау үшін жоғары сапалы тәжірибені қолдануы болып табылады. Эксперттік жүйенің маңызды қасиеті дербес оқыту және жаттықтыру үшін оларды қолдану мүмкіндігі болып табылады.

Жасалатын эксперттікжүйе ақпараттық қауіпсіздік стандарттар талаптары бойынша жасалынады. Ол үшін ақпарат қауіпсіздігін басқару жүйесі (АҚБЖ)саясатын, мақсаттарын, үрдістерін айқындап, АҚБЖ байланысты стандарттардағы талаптарды талдап,сараптаймыз. Сонан кейінөлшенетін талаптар бойынша шығарым ережелерін құрамыз да, оларды автоматты өңдейміз.

ISO (Стандарттау бойынша халықаралық ұйым)және ХЭК (Халықаралық электротехникалық комиссия) бірігіп мамандандырылған әлемдік стандарттаудың жүйесін құрады. Ақпараттық технологиялар бағыты бойынша СХҰ және ХЭК бірігіпISO / IEC JTC 1 біріктірілген комитет құрды. СХҰ / МЭК нұсқауларында келтірілген ережелерге сәйкес халықаралық стандарттар құрылады. ISO / IEC JTC 1/SC 27 ақпараттық қауіпсіздік жүйесіне арналған стандарттар тобы ретінде белгілі стандарттар ақпараттық қауіпсіздік менеджменті жүйесі бойынша халықаралық қатынастарды құруға арналған эксперттік комиссиямен қамтамасыз етеді.

АҚБЖстандарттар тобын қолдану арқылы ұйымдар өз ақпараттық жүйелерін басқаруға арналған негіздерді ендіру мен құруды, соныменқоса қаржылық ақпарат, интеллектуалды меншікті, қызметкер жөніндегі ақпарат немесе үшінші жақпен немесе

клиентпен берілген ақпараттың қауіпсіздігін қамтамасыз ету керек. Бұл стандарттар ақпаратты қорғауға ұсынылады және тәуелсіз дайындықты бағалау үшін қолданылады.

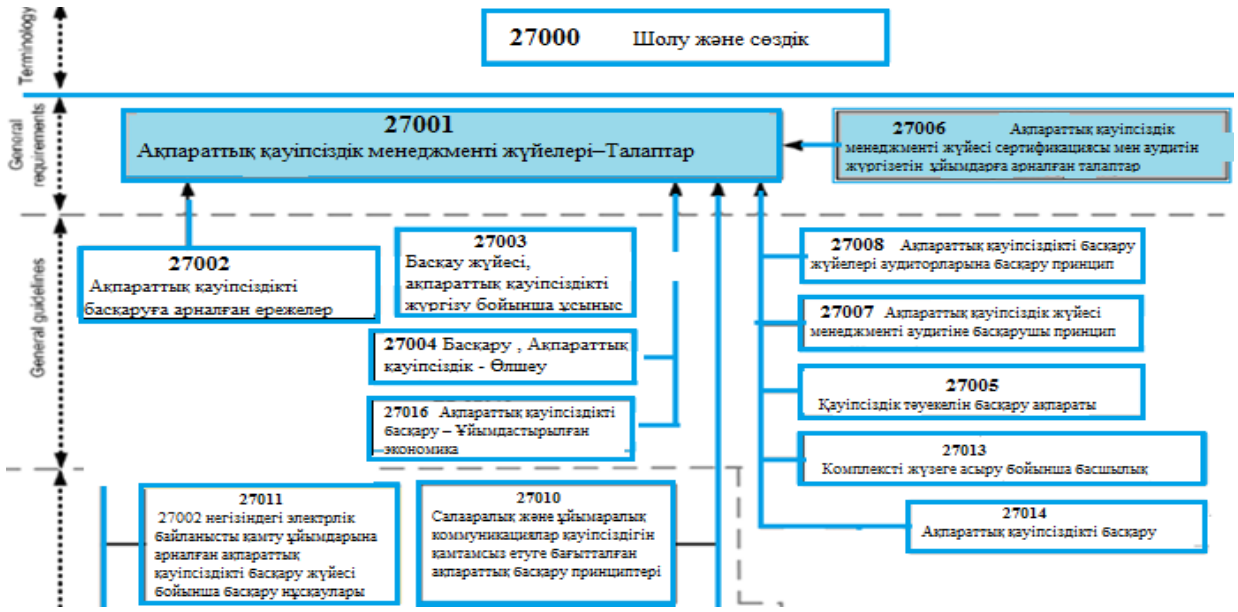
АҚБЖ стандарттартобыбарлық типтегі ұйымдарға көмек көрсету үшін арналған және келесі қызметін қамтамасызететін халықаралық стандарттардан тұрады, жалпы атауы Ақпараттық технологиялар – Қауіпсіздік әдістер (1 кестеде ретімен келтірілген) :

СтандартISO/IEC	Сипаттамасы
27000:2009	Ақпараттық қауіпсіздік менеджменті жүйелері – Шолу және сөздік
27001:2005	Ақпараттық қауіпсіздік менеджменті жүйелері–Талаптар
27002:2005	Ақпараттық қауіпсіздікті басқаруға арналған тәжірибелік ережелер жиыны
27003:2010	Басқау жүйесі, Ақпараттық қауіпсіздік және оны жүргізу бойынша ұсыныстар
27004:2009	Басқару , Ақпараттық қауіпсіздік - Өлшеу
27005:2011	Қауіпсіздік тәуекелін басқару ақпараты
27006:2011	Ақпараттық қауіпсіздік менеджменті жүйесі сертификациясы мен аудитін жүргізетінұйымдарға арналған талаптар
27007:2011	Ақпараттық қауіпсіздік жүйесі менеджменті аудитіне арналған басқарушы принциптер
27008:2011	Ақпараттық қауіпсіздікті басқару жүйелері аудиторларына арналғанбасқару принциптері
27010:2012	Салааралық және ұйымаралық коммуникациялар қауіпсіздігін қамтамсыз етуге бағытталған ақпараттық басқару принциптері
TR 27011:2008	27002 негізіндегі электрлік байланысты қамту ұйымдарына арналған ақпараттық қауіпсіздікті басқару жүйесі бойынша басқару нұсқаулары
FDIS 27013	Комплексті жүзеге асыру бойынша басшылық
FDIS 27014	Ақпараттық қауіпсіздікті басқару
TR 27015 (әзірленуде)	Қаржылық қызметтерге арналған барлық ақпараттық басқару принциптерін қауіпсіздікпен қамтамасыз ету
WD 27016 (әзірленуде)	Ақпараттық қауіпсіздікті басқару – Ұйымдастырылған экономика

1 кесте - АҚБЖ стандарттартобы

АҚБЖ процедуралардың, саясаттан және басқарушы принциптер және онымен байланысқан ресурстар мен ұйымды коллективті басқаратын, ақпараттық белсенділіктері қорғалуы үшін қажет қызметтерден тұрады. АҚБЖ бизнес-мақсаттарды ұйымдастыруда бақылау, талдау, эксплутация, қолдау, еңгізу, құру және ақпараттық қауіпсіздікті арттыруды қолданатын жүйелік амал болып табылады. Басқару құрамына сәйкес құрылымдар аумағында іс-шаралар жүргізу, бақылау және тұрақты жағдайда ұйымды жетілдіру кіреді. Ал АҚБЖ тұрғысынан қарасақ басқару қатарына,ұйымның ақпараттық қауіпсіздіктерін қорғау арқылы бизнес-мақсаттарға жету үшін қажет бақылау және шешім шығару кіреді. Ақпараттық қауіпсіздікті басқаруақпараттық қауіпсіздік саясатын қолдану және алу, процедуралар және басқару принциптері арқылы көрінеді, олар кейін ұйым бойынша барлық тұлғалармен және онымен байланысы бар ұйымдардың барлығымен байланысады. Басқару жүйесі құрамына саясат, жоспарлау, тарату, жауапкершілікті бөлу, процестер, процедуралар, ұйымдастыруды құру кіреді. [1]

АҚБЖстандарттар әулеті баспа бетін көрген немесе жетілдірілу үстіндегіөзара байланысты нормалардан тұрады және құрылымдық компоненттерді қамтиды. Стандарттарішіндегі АҚБЖ әулетінің арасындағы қатынас1суретте көрсетілген.



1 сурет- АҚБЖәулетінің стандарттық қатынасы

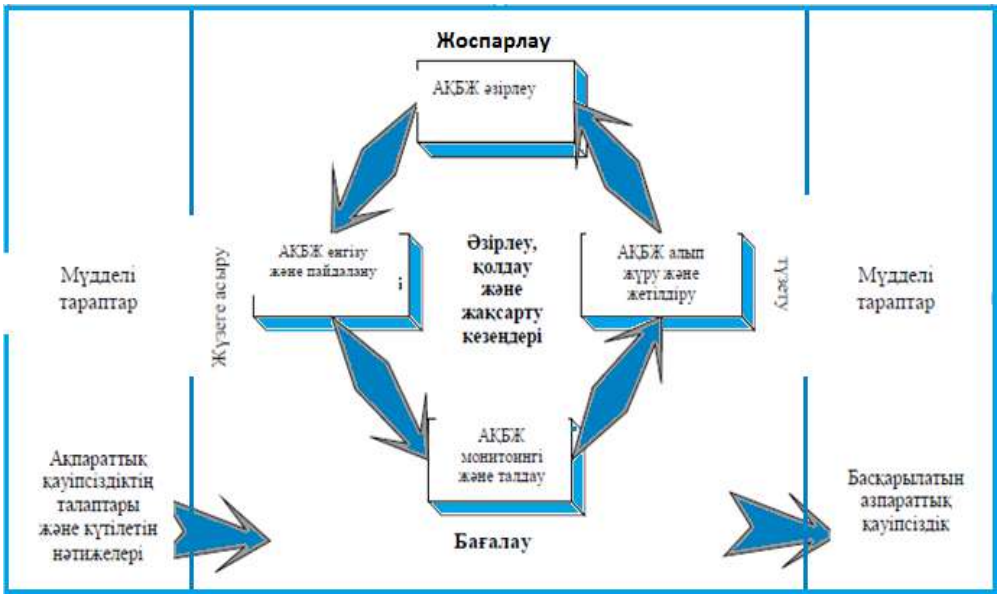
ИСО / МЭК 27001стандарты ақпараттыққауіпсіздіктібасқаружүйесін (АҚБЖ)әзірлеу, іскеасыру, пайдалану, мониторинг, талдау, алыпжүружәнежаңартуүшінүлгілерретіндепайдалануүшіндайындалған. АҚБЖқабылдауұйымүшінстратегиялықшешімболыптабылуғатиіс. ҰйымдардыңАҚБЖархитектурасыменіскеасыруғабизнестіңмақсаттарыжәнеқажеттіліктері, қауіпсіздіккеқойылатынталаптар, пайдаланылатынрәсімдер, сондай-ақұйымныңөзініңмөлшеріменқұрылымыда әсеретеді. Уақытөтекелеаталғансипаттамаларжәнеолардықолдайтынжүйелерөзгередідепболжанады. АҚБЖіскеасыруұйымныңқажеттіліктерінесәйкесауқымданадыдеп ұсынылады.

Осы стандарт мүдделі ішкі және сыртқы тараптардың сәйкестікті бағалау үшін пайдаланылуы мүмкін. Сонымен бірге ұйымдардың АҚБЖ әзірлеуге, іске асыруға, пайдалануға, қадағалауға, талдауға, ілестіруге және жетілдіруге процестік тәсіл қабылданған.

Тиімді қызмет істеу үшін ұйым әр түрлі әрекеттерді басқаруға және сәйкестендіруге тиіс. Кіріс деректерін шығыс деректеріне түрлендіру мақсатында басқарылатын және ресурстарды пайдаланатын кез келген әрекет үрдіс ретінде қарастырылуы мүмкін. Бір үдерістің шығыс деректері келесі үдеріс үшін тікелей кіріс деректерін білдіреді.

Осы үрдістерді сәйкестендіру және өзара әрекет етумен, сондай-ақ осы үрдістерді басқарумен бірге ұйымда үрдістер жүйесін қолдану «процестік тәсіл» деп аталуы мүмкін.

Осы стандартта АҚБЖ барлық үрдістерін құрылымдау үшін қолданылған «Жоспарлау – Жүзеге асыру – Бағалау – Түзету - ЖЖБТ» («Plan-Do-Check-Act» – PDCA) үлгісі қабылданған. 1-2 суретте ақпараттық қауіпсіздікке талаптарды және мүдделі тараптардың үмітін АҚБЖ кіріс деректері ретінде қалай қабылдайтыны көрсетілген және бірқатар қажетті әрекеттер және үрдістер нәтижесінде осы талаптар мен үміттерді қанағаттандыратын ақпараттық қауіпсіздіктің шығысын береді.



2сурет - АҚБЖ үрдістеріне ЖЖБТ үлгісін қолдану

Ұйым өзі кездесетін тәуекелдер және ұйымның жалпы бизнес-қызметінің мағыналы мәтініндегі құжаттандырылған АҚБЖ әзірлеуге, іске асыруға, пайдалануға, мониторинг және талдау жүргізуге, алып жүруді және жетілдіруді жүзеге асыруға тиіс. Осы стандарттың мақсаттары үшін пайдаланылатын үрдіс2 суретте берілген ЖЖБТ үлгісіне негізделеді. Осы стандарт аталған құжатта мазмұндалған қауіпсіздіктің тәуекелдер бағасын, жоспарлауды және іске асыруды реттейтін, қауіпсіздікті және қайта бағалауды басқаратын қағидаларды іске асыру үшін тұрақты үлгіні ұсынады. АҚБЖ үрдістеріне ЖЖБТ үлгісінде көрсетілген әр бөлімінде АҚБЖ бойынша қандай талаптар анықталып,толықтырылатыны көрсетіледі. АҚБЖ барлық стандарттарда ИСО / МЭК 27001 стандарты бойынша жасалынған осы үрдіс негіздемесі жүзеге асырылады. (2 кесте).

Жоспарлау(АҚБЖ әзірлеу)	Ұйымның жалпы саясаттарына және мақсаттарына сәйкес келетін нәтижелер алу мақсатында ақпараттық қауіпсіздікті арттыру және тәуекелдікті басқару үшін мәнді АҚБЖ саясатын, мақсаттарын, үрдістерін және рәсімдерін айқындау.
Іске асыру(АҚБЖ енгізу және пайдалану)	АҚБЖ саясатын іске асыру және пайдалану, басқару, үрдістер және рәсімдер құрылады.
Тексеру(АҚБЖмониторингі және талдау)	Бағалау және егер талап етілсе, АҚБЖ саясатына, мақсаттарына және практикалық тәжірибеге сәйкестігін тексеру үшін үрдіс сипаттамасын өлшеу, сондай-ақ басқарушы қызметкерлермен әрі қарай талдау үшін нәтижелерді табыстау.
Жетілдіру(АҚБЖ алып жүру және жетілдіру)	АҚБЖ үздіксіз жетілдіру мақсатында АҚБЖ ішкі аудит және басқарушы қызметкерлермен орындалған талдау нәтижелері бойынша сондай-ақ басқа мәні бар ақпараттың негізінде түзету және ескерту шараларын қабылдау.

2 кесте - АҚБЖ үрдісінің негіздемесі

Стандарт барлық ұйымдар үшін (мысалы, коммерциялық кәсіпорындарға, үкіметтік мекемелерге, коммерциялық емес ұйымдарға) қолданылады. Осы стандарт ұйымның ортақ бизнес тәуекелінің мағыналы мәтінінде құжаттандырылған АҚБЖәзірлеуге, іске асыруға, пайдалануға, мониторингке, талдауға, алып жүруге және жетілдіруге талаптарды айқындайды. Ол жеке ұйымдар немесе олардың бөлімдерінің тиісті қажеттіктеріне, басқару құралдарына талаптарды айқындайды.

ИСО / МЭК27003 стандарты ақпараттық қауіпсіздік басқару жүйесін (АҚБЖ) ISO/IES

27001 стандартына сәйкес сәтті әзірлеуге және енгізуге қажетті маңызды аспектілерді белгілейді. Онда АҚБЖ анықтау және әзірлеу үдерісі, іске қосудан бастап енгізу жоспарларын құрастырғанға дейін суреттеледі. Онда АҚБЖ енгізуге басшылықтың келісімін алу үдерісі суреттеледі, АҚБЖ енгізу жобасы анықталады (осы стандартта АҚБЖ жоба ретінде атап өтіледі), және нәтижесінде АҚБЖ енгізудің нақты жоспары алынатын АҚБЖ жобасын жоспарлау жөніндегі ұсыныстар келтірілген.

Осы стандарт АҚБЖ қолданатын ұйымдардың пайдалануына арналған. Кез келген көлемдегі ұйымдардың барлық типтеріне қолданылады (мысалы. коммерциялық кәсіпорындарға, үкімет органдарына, коммерциялық емес үйымдарға). Әрбір ұйым құрылымының күрделілігі және тәуекелдері ерекше, АҚБЖ енгізуге оның өзгеше талаптары әсер етеді. Шағын ұйымдар осы стандартта көрсетілген әрекеттер оларға қолданылады және ықшамдалады деп санауы мүмкін. Ірі ұйымдарға немесе күрделі құрылымы бар ұйымдарға осы стандартта көрсетілген әрекеттерді тиімді орындау үшін ұйымдастыру немесе басқарудың көп деңгейлі жүйесі қажет болуы мүмкін. Алайда екі жағдайда да тиісті әрекеттерді осы стандартты қолдана отырып, жоспарлауға болады.

Ақпараттық қауіпсіздік менеджментінің жүйесін (АҚБЖ) енгізу қызметтің маңызды түрі болып табылады және ұйымда жоба ретінде жүзеге асырылады. Осы стандартта АҚБЖ енгізу іске қосуды толық суреттеумен, жобаны жоспарлау және анықтаумен түсіндіріледі. [2]

ИСО / МЭК 27004 стандарттың ішінде ақпараттық қауіпсіздік, сондай-ақ ИСО/МЭК 27001 бойынша басқару және бақылаудың, олардың топтарының құралдары мен шамалары менеджментінің іске асырылған жүйесінің тиімділігіне баға беру үшін өлшемнің құралдары мен шамаларын қолдану және әзірлеу бойынша ұсыныстар қамтылған.

Өлшемдер процесі басқару және бақылаудың құралдары мен шамалары, ақпараттық қауіпсіздік тәуекелділігінің менеджменті, саясаты және оларды қолдану мақсаттарына, процестер мен процедураларға қатысты жүргізіледі, сондай-ақ АҚБЖ басқару мен бақылаудың құралдары және шамалары немесе қандай да бір процестерінен өзгерту немесе жетілдіру талап етілетіндігін анықтай отырып АҚБЖ тексеру процесін қолдайды. Өлшем бағдарламасы сондай-ақ ИСО/МЭК 27001 талаптарына АҚБЖ сәйкестігін көрсетеді және ақпараттық қауіпсіздіктің менеджменті процестерін ұйым басшылығы тексеруді жүргізу үшін қосымша негіздеме жасауға септігін тигізеді.

Осы стандартта өлшемдер мен өлшем шараларын әзірлеу үшін жіберу нүктесі ақпараттық қауіпсіздік тәуекелділіктерін толық түсіну болып табылады, онымен ұйым қақтығысуы мүмкін, және ИСО/МЭК 27001 талаптарына сәйкес тәуекелділікті бағалау бойынша ұйымның әрекетін түзу орындау болып табылады. Ақпараттық қауіпсіздікпен байланысты Өлшемдер Бағдарламасы осы тәуекелділіктерді басқару үшін іске асырылған АҚБЖ күйі мен ақпараттық қауіпсіздікке қатысты тиісті мүдделі тараптарға сенімді ақпаратты беруге ұйымға көмектеседі. [4]

ИСО/МЭК 27005 берілген Халықаралық стандартта ISO/IES27001-дегі АҚБЖ талаптарын толықтыратын ұйымдағы Ақпараттық қауіпсіздік қауіпі (риск) Басқармасы көрсетілген. Бірақ берілген Халықаралық стандарт Ақпараттық қауіпсіздік қауіпі басқармасына қатысты ешқандай нақты методологияныұсынбайды. Қауіп-қатерлерді немесе тәуекелді басқаруға қатысты әдісті ұйым өзі анықтауы керек, ал АҚБЖ талаптарын орындау үшін бұрыннан бар кейбір методикалар қолданылады. Берілген халықаралық стандарт ұйым ішіндегі Ақпараттық қауіпсіздік қауіпі мәселесімен айналысатын менеджерлер мен қызметкерлерге, кейбір белгілі жағдайларда берілген қызметке демеу көрсететін бөтен адамдарға да арналған. [5]

АҚБЖ шеңберінде контекстіні, қауіпті бағалауды анықтау, қауіпті қабылдау мен қауіпті өңдеу жоспарын әзірлеу «жоспарлаудың» бөлігі болып табылады. АҚБЖ «жүзеге асыру» кезеңінде қауіпті өңдеу жоспарына сәйкес қауіпті қажетті деңгейге деін төмендетуге қажетті әрекеттер өндіріліп, қадағалау механизімі енгізіледі. АҚБЖ «тексеру» кезеңінде басшылық жағдайдың өзгеруіне байланысты бағалауды қайта қарау мен қауіпті өңдеу

қажеттілігін анықтайды. «Әрекет ету» кезеңінде ақпараттық қауіпсіздік қаупін басқару үрдісінің қосымшаларымен қатар кез келген қажетті әрекеттер жүзеге асырылады.

ИСО/МЭК 27001 сондай-ақ салыстырмалы нәтижелер алу үшін басқару мен бақылау құралы мен шамасының тиімділігін бағалауға басқару және бақылау, сондай-ақ олардың топтарының тандалған құралдары мен шамалардың тиімділігін өлшеуді тиісті түрде өткізуді анықтауға ұйымға қойылатын барлық талаптарды қамтиды.

Ұйымдар өз ақпараттық активтерін қорғауға байыппен қарап,бизнестегі орны мен өзінің бәсекелстік артықшылығын сақтап қалу үшін АҚБЖ енгізуі керек. Халықаралық стандартта АҚБЖ жалпы стандарттар тобы бойынша ISO/IES 27001-дегі АҚБЖ үрдістеріне ЖЖБТ үлгісі бойынша(2 сурет) АҚБЖ талаптарын толықтырады. Осы стандарт ұйымның көрсетілген басқару жүйелеріне талаптарға сәйкес өзінің АҚБЖ біріктіре немесе тұрғыза алатындай етіп әзірленген.

Қолданылған әдебиеттер

1. ISO / IEC 27001:2005, Ақпараттық технологиялар – Қауіпсіздікті қамтамасыз ету әдістері – Ақпараттық қауіпсіздік менеджментінің жүйесі – Талаптар
2. ИСО/МЭК 27000 «Ақпараттық технологиялар. Техника қауіпсіздігі. Ақпарат қауіпсіздігін басқару жүйесі. Шолу және сөздік»
3. ISO / IEC 27003:2010, Ақпараттық технологиялар - Қауіпсіздікті қамтамасыз ету әдістері
4. ИСО/МЭК 27001 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері»
5. ISO / IEC 27004:2009, Ақпараттық технологиялар - Қауіпсіздікті қамтамасыз ету әдістері – Ақпараттық қауіпсіздікті қамтамасыз ету – Өлшемдер
6. Қауіпсіздік тәуекелін ақпартпен басқару - ИСО / МЭК 27005:2011, Ақпараттық технологиялар – Қауіпсіздікті қамтамасыз ету әдістері

ОӘК 004.432.4

ҚАЗАҚ ТІЛІНІҢ ГРАММАТИКАЛЫҚ ЕРЕЖЕЛЕРІНІҢ ОНТОЛОГИЯЛЫҚ МОДЕЛДЕРІН БІЛІМДІ БАҒАЛАУҒА ҚОЛДАНУ

Бегалаев Б.Т, Ергеш М.Ж.
bizhan.88@mail.ru; shymkent90@mail.ru
Л.Н.Гумилев атындағы ЕҰУ
Ақпараттық технологиялар факультеті
Теорялық информатика кафедрасының магистранттары, Астана, Қазақстан
Ғылыми жетекшісі –Разахова. Б.Ш.

Интернет жүйесінде ақпараттар көлемінің қарқынды ұлғаюымен байланысты өзекті міндет болып үлкен көлемдегі ақпараттық ресурстарды қолданудың тиімділігін жоғарылату табылады. Онтологияларға тән ақпараттық құрылымдану ақпаратты іздеу міндеттерін шешу үшін қосымша мүмкіндіктер қамтамасыз етеді және бірінші кезекте бұл ғылыми басылымдар сияқты «жақсы» нысандану облысына жатады.

Онтология (грек.) - барлығына жалпы негіздер, тұрмыс принциптері, оның заңдылықтарының құрылымы зерттелетін тұрмыс туралы ғылым (гносеологияға қарағанда - сана туралы ғылым) философияның бөлімі. Жасанды зияткерлік саласында онтология – нақты бір пәндік облысты бейнелейтін түсініктердің арнайы түсініктерінің құрылуымен байланысты пән. Түсініктердің мазмұны концептілердің көмегімен көрінеді. Онтологияда концепт формалды түрде басқа кластармен байланысқа ие, нысанмен (класпен) теңдестіріледі. Класс жалпы қасиеттері бар көптеген даналардың жиынтығы ретінде анықталады.