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

АОЖ 004.6:006.1

АҚПАРАТТЫҚ ҚАУІПСІЗДІККЕ БАЙЛАНЫСТЫ СТАНДАРТТАРҒА ШОЛУ

Нұрпейісова Фарида Болатқызы
farik_kz87@mail.ru
Л.Н.Гумилев атындағы ЕҰУ Теориялық информатика кафедрасының
2 курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – А.А. Шәріпбаев, т.ғ.д

Ақпараттық қауіпсіздікті қамтамасыз ету мәселесі қазіргі кезде тек біздің елдегі ғана емес, сонымен бірге барлық дамыған елдерге тән өткір мәселенің бірі болып табылады. Ақпараттық қауіпсіздік мәселесіне мүдделілік ақпараттық қоғам өмірінің барлық саласындағы рөлінің артуымен байланысты.

Қоғамдағы, мемлекеттегі айналымда жүрген ақпарат, ақпараттық ресурстар әртүрлі болады. Сондықтан ақпараттың құны, бағалылығы, пайдалылығы оның мүмкіншілігіне, сұранысқа иелілігіне байланысты. Мемлекет билігіндегі, қоғамдағы, жеке адамның отбасындағы ақпараттың өз мәні салмағы болады. Мемлекет, ұйым немесе адам өзінің ақпаратын таратуға шектеу қоюға, өз ақпаратын қорғауға, қауіпсіздендіруге құқылы. Осыдан барып жабық ақпарат немесе мемлекеттік, коммерциялық құпияға жатқызылған, пайдалануға шектеу қойылған ақпарат пайда болады, осындай ақпаратты таратуға шектеулер нәтижесінде ақпаратты қорғау мәселесі туындайды.

Ал, ақпараттық қауіпсіздік деп ұйым активтерін (мысалы, ақпаратты) рұқсат етілмеген жолмен ашылуынан және рұқсат етілмеген (немесе кездейсоқ) жолмен өзгертілуінен қорғау, ол ақпаратты қажет болған кез келген сәтте пайдалануға дайындығын қамтамасыз етеді [1].

ISO қауіпсіздік стандарттарының кіріспесінде ақпараттық қауіпсіздіктің мәні мен мағынасын, оның компанияларда қолданылу аясы жалпы мағынада түсінетін оқырмандарға арналған. Оқырман ISO 27001 стандарты бойынша сертификатталатын ақпараттық қауіпсіздікті жоспарлау, іске асыру және қолдау үдерістерін жақсарту үшін қамтамасыз ету жолдарын ретке келтіруге ниетті деп болжайды. Тараудың басында қауіпсіздік стандарттарына шолу келтірілген, онда Стандарттау бойынша Халықаралық Ұйымның (ISO – International Standards Organization) стандарттары мен әзіленіп жатқан түрлеріне ерекше назар аударылған.

Тарау материалы ақпараттық қауіпсіздік менеджменті жүйелерін түсінуге негіз болады және онсыз ISO 27001 бойынша сертификаттаудан өту мүмкін емес.

1.1 Ақпараттық қауіпсіздіктің іргетастары

Компанияның дәстүрлі активтері, әдетте, қандай да бір меншік түріндегі, яғни құрал-жабдық, ғимарат, жиһаз, қаржы құралдары немесе өзге де айналым құралдары, мәселен алтын болып табылатын материалдық түрге ие. Бұрындары қауіпсіздік мәселелері физикалық шаралар түрінде, соның ішінде, күзет ұйымдастыру, қабырғалар, қоймалар немесе сейфтер орнату көмегімен шешілетін. Қазіргі кезде компаниялардың материалдық активтерден бөлек, электронды түрде сақаталатын (мәселен, мәтінді файлдар, электрондық кестелер мен мәліметтер базасы) зияткерлік меншік секілді виртуалдық активтері болады. Оның үстіне, компанияның айналымдағы құралдары көп жағдайда, желілік және желілік емес тораптар бойынша тарату жолымен жүзеге асырылатын қатты дискілер мен транзакциялардағы бит түрінде сақталады. Компания активтерінің едәуір бөлігі электрондық түрде болып келеді, сондықтан да осы активтерді ақпараттық қауіпсіздікті басқарудың (information security control) түрлі құралдарының көмегі арқылы қорғау қажеттілігі туындайды. Ақпараттық қауіпсіздікке дәстүрлі көзқарас дегеніміз үш «ірге тастан» тұрады: «CIA моделі» (Confidentiality-Integrity-Availability) ретінде белгілі құпиялылық, бүтіндік және қолжетімділік. Құпиялылық, бүтіндік және қолжетімділікті қамтамасыз ету қауіпсіздік мақсаты. Құпиялылықты қамтамасыз ету өкілетті қызметкер ғана ақпаратқа қол жеткізе

алатынына немесе ақпараттың өкілетті емес тұлғамен немесе басқа да нысанмен (мәселен, автоматтандырылған жүйе немесе қызмет) ашылмауына кепілдік береді. Бүтіндікті қамтамасыз ету – ақпаратты рұқсат етілмеген өзгертуден немесе бүлінуден сақтауды, не болмаса ақпаратты автор жасаған түрде сақталуын қаматамасыз ету. Бүтіндіктен айрылу дегеніміз ақпараттық рұқсат етілмеген түрде өзгеруін немесе бүлінуін білдіреді. Қол жетімділік ақпаратты қажеттілік туындаған кезде пайдалану мүмкіндігін қамтамасыз ету. Қолжетімділікті жоғалту дегеніміз ақпаратқа қол жеткізудің бұзылуы, ақпаратты немесе ақпараттық технологияны пайдалану мүмкіндігінің болмауы. Осы үш «ірге тас» 1-1 суретінде көрсетілген.

Сурет 1-1. Ақпараттық қауіпсіздіктің ірге тастары

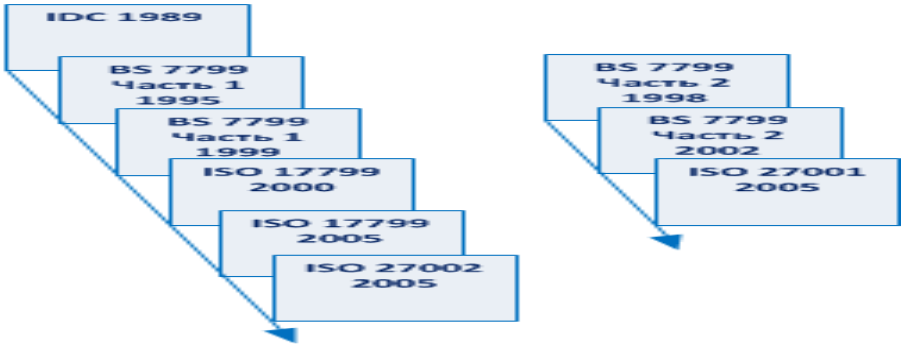
Компания ақпараттық қауіпсіздікті және осы үш құрауыш бөліктері қалай басқарады? Тәсілдердің бірі Ақпараттық қауіпсіздік менеджменті жүйесін (АҚМЖ) енгізу және АҚМЖ тиімділігін жасаудағы басшылық ретінде ISO стандарттарын пайдалану. PDCA моделі АҚМЖ енгізу әдістемелігін береді. ISO 27002 стандарты (бұрынғы ISO 17999 стандарты) тиіді АҚМЖ құрудың негізін салады, ал ISO 27001 PDCA моделі бойынша тұрғызылған үрдістер көмегімен АҚМЖ жүзеге асыруға басшылық етеді.

1.2 Ақпараттық қауіпсіздік бойынша ISO стандарттарының тарихы

Ұлыбританияның сауда және өнеркәсіп министрлігі (DTI) қауіпсіздікті қамтамасыз ету жөніндегі ең жақсы тәжірибелердің жиынтығын әзірлеу үшін жұмыс тобын ұйымдастырды. DTI 1989 жылы User Code of Practice стандартын жариялады. Бұл стандарт сол кезде барабар, қалыпты және жақсы деп есептелген дәне технологияларға да, сол уақыттағы ортаға да қолдануға тиімді қауіпсіздікті басқару құралдарының тізбесі болып табылды.

1-2 суреті ISO 27001 және ISO 17999 (ISO 27002) стандарттарының даярлау тарихын көрсетеді. DTI құжаты британдық стандарттар жүйесінің(BS) нұсқау беретін құжаты, кейіннен BS 7799:1995, 1 Бөлім. Британдық стандарты ретінде жарияланды. Бірінші бөлімі ақпаратық қауіпсіздікті қамтамасыз ету саласындағы ең жақсы тәжірибелердің жиынтығы ретінде ұсынған басқару құралдарының (control) тізбесін қамтиды. Стандарттың екінші бөлімі BS 7799:1998, Часть 2 деген атаумен шықты. Ол бірінші бөлімде сипатталған қауіпсіздік құралдары мен шаралардың қызмет ету өлшемі мен мониторингіне арналған құрал ретінде сертификаттау мақсатында бағалау жүгізуге мүмкіндік берді. Жүйелі қайта қарау үдерісінде бірінші бөлімі BS 7799:1999, 1 Бөлім, сосын ISO 17999:2000 ретінде жарияланды. Стандарттың екінші бөлімінің жаңа нұсқасы BS 7799:2002, 2 Бөлім түрінде шығарылды. Содан соң ISO 17999 стандарты қайта қаралып, ISO 17999:2005 ретіндешығарылды, ал содан кейін атауы ISO 27002:2005 болып өзгертілді. ISO 2007 шілдесінде BS 7799, 2 Бөлім стандартын ISO 27001:2005 стандарты етіп шығарды [2].

Келесі бөлімде ISO 27000 стандарттарының сериясын қалыптасыру туралы айтылады.



1-2 Сурет. ISO 27001 және ISO 27002 стандарттарын даярлау

1.3 Ақпараттық қауіпсіздік стандарттарын қалыптастыру және нөмірлеу

ISO мен Халықаралық Электротехнкалық Комиссия (МЭК, IEC) бірлесіп, халықаралық стандарттар мен нұсқаулықтар әзірлейді. Ортақ мақсаттарының бірі қауіпсіздік менеджменті бойынша станарттар шығару. Стандарттар қалытастыру жөніндегі жұмысұжымдық негізде іске асырылады, оған 1 Жұмыс тобы (WG1), 2 Жұмыс тобы (WG2) және 3 Жұмыс тобы (WG3) қатысады. Осы Жұмыс топтарының бәрі Бірлескен Техникалық Комитетке 1 (JTC1) кіретін Подкомитеттің 27 (SC27) құрамына алынады. 1 Жұмыс тобы қауіпсіздікті басқару стандарттарын, соның ішінде АҚМЖ стандарттарын құру бойынша жұмыс істейді. Бұл жұмыс тобының мақсаты – келешектегі халықаралық стандарттардың жиынтығы мен АҚМЖ құру, енгізу, пайдалану, мониторингі мен қолдау жөніндегі нұсқаулықтарға қойылатын талаптарды көрсетіп беретін бағдарлардың болуы қамтамасыз ету. Осы мақсат аясында ISO/IEC ақпараттық қауіпсіздік жөніндегі халықаралық стандарттарға арналған нөмірлеуді жаңасына – 27000 өзгертуге шешім қабылдады.

1.4 Қауіпсіздікті басқарудың халықаралық стандарттары

1-1 кестесінде 27000 сериясы аясында жарияланған қауіпсіздік стандарттарының кейбірінің қысқа сипаттамасы мен тізімі берілген.

Стандарт ISO/IEC	Описание
27000	Обзор и словарь
27001	Системы менеджмента информационной безопасности – Требования
27002	Свод правил по менеджменту информационной безопасности
27003	Руководство по внедрению системы менеджмента информационной безопасности
27004	Менеджмент информационной безопасности – Изменения
27005	Менеджмент рисков

1-1 Кесте. ISO 27000 стандарттар тобы

Осы кітапта ISO 27001 стандарты егжей-тегжей талқыланады, бұл BS 7799, 2 Бөліміне негізделген жаңа халықаралық қауіпсіздік стандарты. BS 7799, 2 Бөлім бойынша сертификатталған компаниялар ISO 27001 стандартының соңғы нұсқасына сай өз сертификаттарын жаңартуы тиіс. ISO 27002 – бұл ISO 17799 стандартының жаңа атауы. ISO/IEC 27003 стандарты В қосымшасына негізделген BS 7799, 2 Бөлім стандартын енгізу жөнінде нұсқаулықты қамтиды. BS 7799, 2 Бөлімде (және ISO 27001) сипатталған PDCA моделі ақпараттық қауіпсіздік стандарттарын енгізу барысында ғана емес, сондай-ақ басқа басқару стандарттарында, соның ішінде ISO 9001 мен ISO 14001 қолданылады. ISO 27004 АҚМЖ нәтижелілігін өлшеуге арналған көрсеткіштер жүйесін қалыптастыру мәселесін ескереді. ISO 27005 тәуекелдерді басқаруға арналған, ол «Ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі нұсқаулық» – BS 7799, 2 Бөлімге ұқсас. 27000 сериясының басқа стандарттары арасында ISO 27006 атап өтуге болады, онда АҚМЖ аудиты мен

сертификатталуын және ISO 27007 - АҚМЖ аудиты бойынша нұсқаулығын қамтамасыз ететін органдарға қойылатын талаптарды қамтиды[3].

1.5 ISO 27001 стандартына кіріспе

ISO 27001 АҚМЖ енгізудің және қызмет етуінің, сондай-ақ АҚМЖ мониторингі және жақстарту жөніндегі іс-әрекеттердің ортақ моделін сипаттайды. ISO сапа менеджментіне арналған ISO/IEC 9001:2000 менеджмент жүйелері бойынша және экологиялық менеджмент жүйесіне арналған ISO/IEC 14001:2004 секілді түрлі стандарттарды үйлестіруге ниет етуде. ISO мақсаты компаниядағы басқа да менеджмент жүйелерінің АҚМЖ-не келісімділігін және кірігуін қамтамасыз ету. Стандарттар ұқсастығы енгізу, басқару, қайта қарау, тексеру және сертификаттау үшін ұқсас аспаптар (инструментарий) мен функционалды пайдалануға мүмкіндік береді. Егер компания менеджменттің басқа стандарттарын енгізген болса, онла ол аудит пен басқарудың біртұтас жүйесін пайдалана алады дегенді білдіреді, бұны сапа менджментіне, экологиялық менеджмент пен қауіпсіздік менеджментіне және т.б. қолдануға болады.

ISO 27001 стандарты АҚМЖ құру, енгізу, пайдалану, мониторинг және қолдауға арналған бизнес-тәуекелдерге негізделген бүкілін қамтитын менеджмент жүйесі ретінде сипатталады [4]. АҚМЖ ұйымдық құрылым, саясат, жоспарланған іс-әрекеттер, міндеттер, тәжірибелер, рәсім-жосықтар, үдерістер мен ресурстардың барлық аспектілерін ескеруі тиіс. Бұл кітап стандартты алмастырмайды, оның қосымша материалы болып табылады. Сондықтан да авторлар компаниялардың мақсаттарына қол жеткізуге қажетті стандарттардың толық жинағын алуға кеңес береді.

АҚМЖ енгізе отырып, жоғарғы басшылық мониторинг және қауіпсіздікті басқару құралдарын алады, ол қалған бизнес-тәуекелдерді азайтады. АҚМЖ енгізгеннен кейін компания ақпарат қауіпсіздігін және клиенттер, заңнама, регуляторлар мен акционерлердің талаптарын орындауды жалғастыруды ресми түрде қамтамасыз етеді. Егер мақстан сертификаттау болса, ISO 27001 стандартының 4-8 бөлімдеріндегі ережелерді талдаңыз, өйткені бұл бөлімдер сертификаттау үшін міндетті болып табылады.

ISO 27001 А қосымшасы мақсаттар тізбесі мен басқару құралдарын қамтиды, олар ISO 27002 соған ұқсас мақсаттар мен басқару құралдарымен сәйкес келеді, алайда егжей-тегжейлі қарастырылмаған.

В қосымшасында АҚМЖ рәсімдері сәйкестігі мен экономикалық ынтымақтасьық және даму жөніндегі Ұйым (OECD) принциптерінің PDCA кезеңдері қамтылған. Егер компания ISO 9001 немесе ISO 14001 ендірген болса, онда оған С қосымшасы қажет, ал қосымшада ISO 9001, 14001 және 27001 стандарттары талаптарының сәйкестігі кестесі берілген.

1.6 ISO 27002 стандартын енгізу

«Ақпараттық қауіпсіздік менеджменті бойынша ережелер жиынтығы» ISO 27002 стандарты жалпықабылданған халықаралық ақпараттық қауіпсіздік стандарты, ол ақпарат пен ақпараттық технологияларды қорғауды қамтамасыз ететін ақпараттық қауіпсіздік құралдардың егжей-тегжейлі сипаттамасын береді.

ISO 27002 осы басқару құралдарын қалай қолдану керектігін анықтайды. Басқару құралдарын таңдауға мүмкіндік беретін менеджмент жүйесін құруға бағыт беріп, ең жақсы тәжірибелерді пайдалану арқылы олардың жұмысын ұйымдастырады. Басқару құралдарын нақты енгізу үшін рәсімдерді таңдау компания құзырында, ол оның физикалық және техникалық ортасына байланысты.

Ақпараттық қауіпсіздік деген не және ол неге өте маңызды? Ақпараттық қауіпсіздік – ұйым активтерін (мысалы, ақпаратты) рұқсат етілмеген жолмен ашылуынан және рұқсат етілмеген (немесе кездейсоқ) жолмен өзгертілуінен қорғау, ол ақпаратты қажет болған кез келген сәтте пайдалануға дайындығын қамтамасыз етеді. Заңнама талаптары және басқа да

міндеттемелер жеке мәліметтердің қорғалу, қаржы есептерінің дәлдігін қамтамасыз етілуін мәселелерін ескеріп, тиісті ақпараттың қауіпсіздігін қамтамасыз ету талаптарын қамтиды.

Ақпараттық активтер материалдық активтерге қарағанда үнемі қол жетімді жерде, электрондық құжат түрінде, мәліметтер базасы және т.б. түрде сақталады. Компанияның ақпараттық активтеріне қол жетімділік көптеген тәсілдермен, соның ішінде компьютерлер және компьютерлік желілер арқылы жүзеге асады. Егер компания желісіне оның серіктестерінің де желілері қосылған болса, онда ақпараттық активтеріне қол жеткізу мүмкіндігі одан да бетер арта түседі. Егер компания желісі Ғаламторға қосылған болса, ол бүкіл әлемге қол жетімді. Ақпаратқа басқа елден қол жеткізу мүмкіндігі көрші ғимараттағы ақпаратқа қол жеткізгенмен бірдей жеңілдей түседі. Мәліметтерді берудің қол жетімділігі мен қарапайымдылығы материалдық активтерді қорғауға арналған барлық шектеулерді мәнсіз етеді.

Сондай-ақ, зияткерлік меншікті ұрлау немесе пайдалану заңнамасы мұндайды қылмыстық әрекет деп таппайтын және ол елмен қылмыскерлерді беру жөніндегі келісім жасалмаған ел аумағынан да жасалуы мүмкін екендігін ескеру керек. Оның үстіне, зияткерлік меншікті ұрлау мемлекет тарапынан ынталандырылуы, немесе оның тікелей нұсқауымен жүзеге асырылуы мүмкін.

Бұл осындай мемлекеттік әлем нарығындағы бәсекелестік артықшылыққа ие болуға бағытталуы да мүмкін. Негізгі мәселе компанияның ақпараттық активтерін ұрлаудың көптеген мотивтері, құралдары мен әдістері бар болуында. Сондықтан компания өз ақпараттық активтерін қорғауға байыппен қарап, бизнестегі орны мен өзінің бәсекелестік артықшылығын сақтап қалу үшін АҚМЖ енгізуі тиіс. Тиімді АҚМЖ жүзеге асыру үшін компания ISO стандарттарын таңдап алып, басшылығына ала алады. ISO 27002 стандарты келесі қауіпсіздікті басқару құралдарын (security control) ескеретін 12 бөлімнен тұрады:
Тәуекелдерді бағалау және өңдеу, қауіпсіздік саясаты,ақпараттық қауіпсіздікті ұйымдастыру, активтерді басқару, қызметкерлер қауіпсіздігі, физикалық қауіпсіздік және қоршаған орта қауіпсіздігі, коммуникациялар мен оның жұмыс істеуін басқару, қол жетімділікті басқару, ақпараттық жүйелерді сатып алу, жасау және қолдау, ақпараттық қауіпсіздіктің оқыс жағдайларын басқару, бизнес үздіксіздігін басқару, сәйкестік.

Бұл 12 бөлім шамамен 39 түйінді элементтерді және 133 басқару (control) құралдарын қамтиды. ISO 27002 стандартын саясат пен рәсемдерді, сондай-ақ бөлімдердің мақсаттарын анықтауға пайдаланыңыз. Содан кейін оларды нақты орындау және алға қойылған мақсаттарға қол жеткізу мүмкіндіктерін қамтамасыз етуге арналған саясаттар мен рәсімдердің тармақтарын егжей-тегжей қарау үшін әрбір басқару құралына егжей-тегжей талаптарды пайдаланыңыз.

1.7 ISO 27001 және 27002 арасындағы өзара байланыс

ISO 27001 стандарты ақпараттық қауіпсіздіктің менеджмент жүйесі болып табылады. ISO 27002 стадарты басқару жүйесін іске асырудың басты принциптері. ISO 27002 стандарты «Не істеу керек?» (пайдалы басқару құралдарының тізбесін қамтиды) деген сұраққа жауап берсе, ISO 27001 стандарты «Мұны қалай істеу керек?» (АҚМЖ құру және қолдау рәсімдерін қамтиды) дегенге жауап береді.

ISO 27001 - ISO 27002 талаптарының әр тармағына сәйкес рәсімдер жиынтығы емес. Дұрысы, қауіпсіздікті басқару құралдарын жоспарлау, енгізу және қолдауға мүмкіндік беретін ұжымдық инфрақұрылым құрушы, қауіпсіздікті түсінігін қамтамасыз етуші басқару үрдісі. Компания ISO 27002 сәйкестік серификатын ала алмайды, ол өз АҚМЖ ISO 27001 белгіленген талаптарға сай сертификаттай алады

ISO 27001 стандартының А қосымшасы ISO 27002 келтірілген басқару құралдарын сондай тәртіпте санамалайды, алайда осы басқару құралдарына қысқаша сипаттама береді. Екі стандарт та осы кітаптағы нұсқамалармен бірге ISO 27001 сәйкестігіне сертифиткаттаудан табысты өтуге дайындайды[5].

Қорытындылай келе, ақпараттық қауіпсіздік – ішкі қарама-қайшылығы мол, күрделі, ұдайы бақылап, жетілдіріп отыруды талап ететін динамикалық процесс деп түйін жасауға

болады. Соған сәйкес ақпараттық қауіпсіздікті қамтамасыз етуге арналған саяси, экономикалық, әлеуметтік, ұйымдастырушылық-техникалық шаралар жүйесі заман талабына сай жетілдіріп отыруы тиіс.

Қолданылған әдебиеттер

7. ИСО/МЭК 27002 «Ақпараттық технологиялар. Ақпарат қауіпсіздігін басқару бойынша ережелер»
8. ИСО/МЭК 27001-Википедия
9. ИСО/МЭК 27000 «Ақпараттық технологиялар. Техника қауіпсіздігі. Ақпарат қауіпсіздігін басқару жүйесі. Шолу және сөздік»
10. ИСО/МЭК 27001«Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері»
11. Dorlov.blogspot.com

УДК 004

МОДЕЛИРОВАНИЕ НЕЙРОННОЙ СЕТИ СРЕДСТВАМИ ERLANG

Проць Игорь Викторович
prots.igor@gmail.com
Аспирант Днепропетровского национального университета имени Олеся Гончара,
Днепропетровск, Украина
Научный руководитель – д.т.н., профессор В.В. Гнатушенко

ОБОСНОВАНИЕ ВЫБОРА ЭРЛАНГ

При моделировании нейронных сетей (далее НС) возникает вопрос: «какой язык программирования (далее ЯП) и какую платформу выбрать»? В конечном итоге, для упрощения разработки модели язык и платформа должны обладать следующим набором возможностей:

1) НС – это набор независимых, действующих одновременно, распределенных сущностей, называемых нейронами, соответственно и ЯП должен иметь аналогичные элементы – легковесные, параллельные, независимые процессы;
2) нейроны коммуницируют друг с другом посредством сигналов, соответственно и архитектура ЯП должна позволять коммуникации между процессами в формате сообщений или сигналов – реализовывать модель Акторов;
3) ЯП и платформа должны обеспечивать простой, надежный и автоматический механизм восстановления после возникновения ошибок и сбоев.

Список требований, которыми должна обладать компьютерная система, моделирующая искусственный интеллект (ИИ) на базе нейронных сетей:

1) возможность обрабатывать большое количество параллельных процессов;
2) возможность развертывания на нескольких ПК;
3) обновление ПО и переконфигурация должны происходить без остановки работы программного комплекса, на лету;
4) высокие показатели надежности, качества и отказоустойчивости;
5) работа в режиме реального времени или приближенного к реальному (soft real time).

Все выше перечисленные требования аналогичны и для телекоммуникационных систем. В 80-х годах компания Ericson инициировала разработку языка функционального программирования Erlang и платформы (виртуальная машина BEAM) для написания ПО собственного коммутационного оборудования. На данный момент популярность Erlang выросла благодаря возможности применения при построении современных высоко параллельных распределённых веб-приложений [1-3].