REPORTS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
ISSN 2224-5227
Volume 6, Number 304 (2015), 12 – 19

UDC 004. 056.5

GAMBLING MODEL OF BASIC CHARACTERISTICS OF RISK

B.S. Akhmetov[1], A.G. Korchenko[2], M. N. Zhekambayeva[1], S.V. Kazmirchuk[2].
b_akhmetov@ntu.kz, maia.kz@mail.ru
[1]Kazakh national research technical university after K. I. Satpayev, Almaty,
[2]National aviation university, Ukraine

Key words: analysis of risk, estimation of risk, basic characteristics of risk, gambling model, risk of information security, linguistic variable.

Abstract. Often before specialists of the companies for increase of efficiency of the solution of problems of information security there is a question of a choice of the corresponding technique which will meet adequate requirements. Before carrying out such choice it is necessary to have rather full display of concept of risk of aspect of information security. In this regard, in work the analysis of concept of risk of various subject domains from the point of view of safety, psychology, economies, insurance, medicine, geology, etc. which revealed as in monographs, articles, textbooks, dictionaries and in various normative, national and international documents is carried out. Basic characteristics of risk from a set of its interpretation for the subsequent interpretation in the field of information security are defined. On the basis of it it is offered to submit basic characteristics of risk with display in the field of information security, in the form of n-component gambling model. It will give the chance to create new and to investigate a wide range of the existing means of the analysis and estimation of risk.

УДК 004.056.5

Қауіптің базалық сипаттамасының кортежді моделі

Б.С.Ахметов[1], А.Г.Корченко[2], М.Н. Жекамбаева[1], С.В. Казмирчук[2]
b_akhmetov@ntu.kz, maia.kz@mail.ru
[1] Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы
[2]Ұлттық авиациялық университеті, Украина

Тірек сөздер: қауіп анализі, қауіпті бағалау, базалық қауіп сипаттамасы, кортежді модель, ақпараттық қауіпсіздік қаупі, лингвистикалық айнымалы.

Аннотация. Ақпаратты қорғау тапсырмасын шешудің тиімділігін арттыру үшін компания мамандарының алдында адекват талаптарды қанағаттандырып, сәйкес келетін әдісті таңдау туралы жиі сұрақ туындайды. Мұндай таңдауды жүзеге асыру үшін ақпараттық қауіпсіздік аспектінде қауіп түсінігін айтарлықтай толық елестету қажет. Осыған байланысты геология, медицина, сақтандыру, экономика, психология, қауіпсіздік және тағы басқа көзқарас жағынан әр түрлі заттар саласында монографияларда, мақалаларда, оқулықтарда, сөздіктерде, сонымен бірге, әр түрлі нормативтерде яғни ұлттық және халықаралық құжаттарда ашылып отырған қауіп түсінігінің анализі осы жұмыста жүргізілген. Ақпараттық қауіпсіздік саласында кезекті талдау беру үшін көптеген түсініктер ішінен қауіптің базалық сипаттамасы анықталған. Осының негізінде ақпараттық қауіпсіздік саласындағы бейнеде қауіптің базалық сипаттамасын п-компоненттік кортежді моделі түрінде таныстыру ұсынылады. Бұл бар болған амалдар анализінің және қауіпті бағалаудың кең спектрін зерттеуге сонымен бірге жаңасын жасауға мүмкіндік береді.

Кәсіпорын IT-инфрақұрылымының қарқынды өсуі ақпараттық ресурстардың әлсіздігі және ақпараттыық қауіп-қатер санының бақыланбайтын өсуіне алып келеді. Мұндай жағдайларда ақпараттық қауіпсіздігінің(АҚау) қаупін бағалау ақпаратты қорғаудың(АҚор) қажетті деңгейін анықтауға, оны қолдауды жүзеге асыруға және компанияның ақпараттық құрылымының даму стратегиясын өңдеуге мүмкіндік береді. Ақпараттық қауіпсіздік қаупін анализдеу мен бағалау қауіптерді басқару жүйесі мен үздіксіз қамтамасыздандыру жоспарын және бизнесті қайта жасау кезінде қажетті шарт болып табылады.

Бүгінгі күні бағалау мен қауіпті анализдеу әдістерінде бірігетін көптеген құрал-саймандық амалдар бар. Бұл әдістер нормативті құжаттармен (стандарттармен) басталып, нақты программалық заттармен аяқталатын айтарлықтай кең спектрде беріледі. Ақпаратты қорғау тапсырмасын шешудің тиімділігін арттыру үшін компания мамандарының алдында адекватты талаптарды қанағаттандырып, сәйкес келетін әдісті таңдау туралы сұрақ туындайды. Мұндаай таңдауды жүзеге асыру алдында ақпараттық қауіпсіздік аспектісінде қауіп түсінігін айтарлықтай толық елестету қажет болады.

Айтарлықтай кең ауқымды талқылауға ие қауіптің көптеген анықтамалары әр түрлі жарияланымдарда бар [1-40]. Тек Ғаламтор-сөздіктерінің өзінде ғана 1500 ден астам адамзат қызметінің көптеген салаларындағы қауіп талқылауы бар [8]. Соның салдарынан қауіптің негізгі болмысын және онымен байланысты түсініктерді ашатын әр түрлі бір мағынасыздықтар пайда болады. Сәйкесінше мұндай жағдай ақпараттар қауіпсіздігінің саласына да тән болмақ.

Бұл байланыста **берілген мақаланың мақсаты** ақпараттық қауіпсіздік саласындағы кезекті талдау беру үшін қауіп түсінігін ашу мен анализдеу және оның базалық сипаттамасын анықтау болып табылады, бұл ақпаратты қорғау тапсырмаларын тиімді шешуді жоғарылату мүмкіндігін кеңейтеді.

Қауіптер заттар саласын қозғауын есепке алсақ, онда бұл түсініктерді монографияларда, мақалаларда, оқулықтарда, сөздіктерде, сонымен бірге, әр түрлі нормативтерде яғни ұлттық және халықаралық құжаттарда ашылып отыратын қауіпсіздік психология, экономика, сақтандыру, геология, медицина тағы басқа көзқарасы жағынан қарастыруға тура келеді.

Қауіптің базалық сипаттамасын қалыптастыру процесін ресімдеу үшін мүмкін болған барлық сипаттамалар жиынтығын $BC = \bigcup_{i=1}^{n} BC_i = \{BC_1, BC_2, ..., BC_n\}$ енгіземіз, мұндағы $n - BC$ мүшелер саны. Мысалы, n=6 кезінде BC жиынтық мынадай түрге ие болуы мүмкін $BC = \bigcup_{i=1}^{6} BC_i = \{BC_1, BC_2, BC_3, BC_4, BC_5, BC_6\} =$ {«Әрекет», «Оқиға», «ЫҚТИМАЛДЫЛЫҚ», «ҚАУІП», «ЖИІЛІК», «ШЫҒЫНДАР»}.

Әрекет пен қызмет [31] ықтималдылық (өлшенетін немесе есептелетін) сияқты олар үшін ерекше қандай да бір оқиғаның шығуымен байланыстылығы белгілі . Сонымен бірге, кез келген әрекет потенциалды «қауіпті» және «жағымды» [8] мүмкіндіктер болып көріне алатын оқиғалар мен салдарға алып келетіні белгілі. Жоғарыда айтылғандардан, бұл конспектте көрсетілген түсініктердің жалпылығы бақыланады.

Мұнда келесі қауіптің базалық сипаттамасын ерекше көрсетуге болады- ақпараттық қауіпсіздік оқиғасының бұзылуына алып келген **«Әрекет» (BC_1).** Ақпараттық қауіпсіздік көзқарасы жағынан BC_2 жағымсыз оқиғалардың туындауына алып келген ақпараттық жүйе ресурстар (АЖР) қауіпсіздігінің базалық сипаттамасына потенциалды **бопсалаудың** жүзеге асуымен байланысты. Осыған байланысты BC_1 базалық сипаттамасын $BC_1 = \bigcup_{i=1}^{bc_1} BC_{1i} = \{BC_{11}, BC_{12}, ..., BC_{1bc_1}\}$ идентификаторлар жиынтығымен беруге болады, (мұндағы bc_1 – бопсалау идентификаторлар саны), мысалы, bc_1=3 кезінде BC_1 жиынтығы мына түрге $BC_1 = \bigcup_{i=1}^{3} BC_{1i} = \{BC_{11}, BC_{12}, BC_{13}\}$ ={«Компьютерлік тыңшылық», «Тыңшылық», «Программалық қамтамасыздандырудың шалысуы»}ие болады.

Келесі базалық сипаттаманы болатын немесе болмайтын [8, 20] немесе оның болуын күтуге

тура келетін (кейбір өткен, қазіргі, болашақ [3, 16, 21] оқиғалар салдары болуы мүмкін болған активке немесе оның сипаттамасына потенциалды жағымсыз әсер етулер) - **оқиға** түрінде анықтауға болады; **(BC_2)** «**Оқиға»** соңғы идентификаторлар $\boldsymbol{BC_2} = \bigcup_{i=1}^{bc_2} BC_{2i} = \{BC_{21}, BC_{22}, ..., BC_{2bc_2}\}$ (bc_2 – оқиғалардың идентификаторлар саны) жиынтығының бір мәнін қабылдаушы нышан айнымалысы түрінде беруге болады. Ақпараттық қауіпсіздік саласында қауіп құпиялылық, тұтастық пен қол жетімділік сияқты ақпараттық жүйе ресурстары (АЖР) қауіпсіздігінің базалық сипаттамаларымен байланыстылығын есепке ала отырсақ, онда bc_5=7 кезінде базалық оқиғалар $\boldsymbol{BC_2} = \bigcup_{i=1}^{7} BC_{2i} = \{BC_{21}, BC_{22}, BC_{23}, BC_{24}, BC_{25}, BC_{26}, BC_{27}\}$ = {«Құпиялылықтың бұзылуы (ҚБ)», «Тұтастықтың бұзылуы (ТБ)», «Қол жетімділіктің бұзылуы (ҚжБ)», « Құпиялылық пен тұтастықтың ұзылуы(ҚТБ)», «Қол жетімділік пен тұтастықтың бұзылуы (ҚжТБ)», «Қол жетімділік пен құпиялылықтың бұзылуы (ҚжҚБ)», «Қол жетімділік, тұтастық пен құпиялылықтың бұзылуы (ҚжТҚБ)»} түрінде идентификациялануы мүмкін.

Көбіне көрсетілген қайнар көздерде қауіп ықтималдылық немесе онымен байланысты түсініктермен жиі беріледі, мысалы, **өлшенетін немесе есепке алынатын ықтималдылық**: жоғалту [8, 21, 37, 40]; оқиғаның немесе сәтсіз нәтиженің пайда болуы [21, 33] (мысалы, нәтижесінде көзделмеген жоғалтулар болуы мүмкін [2, 10]); қауіптілік, сәтсіздік болу мүмкіндігі [17], қабылданып жатқан шешімнің қорытындсын алу [8, 21], мақсатына жете алмау [8], қойылған мақсаттың жүзеге асуынан күтілетін нәтижелердің алынуының мүмкін еместігінен немесе сенімсіздікпен себептелетін жағдайлардың пайда болуы [25]; пайданы қолдан жіберу немесе шығынға ұшырау (шығын немесе сәйкес келетін кірісті алудағы сенімсіздіктің сандық өлшемі) [25, 28]; белгілі бір бопсалаудың, келтірілген шығынның шамасы мен түрінің жүзеге асуы [4, 21, 29, 35]; мүлікке, қоршаған ортаға немесе азаматтардың өміріне, өсімдіктерге зиян келтіру [27]; қойылған бопсалаудың пайда болуы мен осы бопсалау салдарының потенциалды сәтсіздік алып келуі [7]; қауіпсіздіктің потенциалды бұзылу мүмкіндігін тұспалдайтын [11]; берілген бопсалау, оның көмегімен мүлікке зиянын тигізу үшін немесе жоғалтуға алып келу үшін белсенді немесе белсенді топтарының осалдығы қолданылады [32]; сонымен бірге оқиғаны үйлестіру немесе қиыстыру ықтималдығы мен оның салдары сияқты [6,14,19,23,30,34,36]. Ықтималдылықтың белгілі бір оқиғаның басталуымен байланысты екені барлығына белгілі [12,22,31], сәйкесінше мұнда онымен қауіп те байланысты.

Жоғарыда жүргізілген басылым анализі ($\boldsymbol{BC_3}$) қауіп **ықтималдылығының** бірінші базалық сипаттамасын анықтауға мүмкіндік береді. Ықтималдылықты жиі «объектілік» (кейде физикалық деп атаушы) және «субъектілік» деп бөледі [24]. Объективті ықтималдылық дегенде біз олардың жалпы санының сәтті шығу санына қатынасы немесе жалпы бақылау көлемінде қандайда бір оқиғаның пайда болуының жиілік арақатынасын түсінеміз. Ол, мысала, үлкен санды бақылау нәтижесін анализдеу кезінде қалыптасады. Субъективті ықтималдылық дегенде біз кейбір адамның немесе адамдар тобының белгілі бір оқиғаның болатындығына байланысты сенімділігінің өлшемін түсінеміз. Бұл ықтималдылық ресми түрде әр түрлі амалдармен берілген болуы мүмкін, мысалы, оқиғалар жиынтығында бинарлық қатынас немесе таралу ықтималдылығы, бірақ көбіне жиі ол экспертті жолмен алынған ықтималдылық өлшем береді [24].

Айта кететін жайттардың бірі, статистикалық мәліметтерді алуда қиындық туындағанда, сонымен бірге, шама интерпритациясының қарапайымдылығы үшін эксперттер логика-лингвистикалық тәсілді қолданады. Оның көмегімен «**ЫҚТИМАЛДЫЛЫҚ**» белгілі бір анықталған базалық терм-жиынтықты, мысалы, $\boldsymbol{BC_3} = \bigcup_{i=1}^{bc_3} \underset{\sim}{BC}_{3i}$ (bc_3 – термдер саны), мұндағы мүшелерге тәртіп қатынасы $\underset{\sim}{BC}_{31} < \underset{\sim}{BC}_{32} < ... < \underset{\sim}{BC}_{3bc_3}$ әділ, лингвистикалық айнымалы (ЛА) арқылы [11] сәйкес келетін сипаттама берілуімен жүзеге асырылады. Айта кетсек, $\boldsymbol{BC_3}$ лингвистикалық айнымалы термдері нақты емес сандарды салыстыру әдісін қолдану арқылы көрсетілген

қатынаспен байланысады[11]. Мысалы, берілген логикалық айнымалы үшін $\underset{\sim}{H}, \underset{\sim}{C}$ және $\underset{\sim}{B}$,нақты емес сандарымен берілетін және сәйкесінше «төмен» (Т), «орташа» (О) және «жоғары» (Ж) лингвистикалық эквивалентіне ие $\boldsymbol{BC_3} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{3i}\ \{\underset{\sim}{BC}_{31}, \underset{\sim}{BC}_{32}, \underset{\sim}{BC}_{33}\} = \{\underset{\sim}{H}, \underset{\sim}{C}, \underset{\sim}{B}\}$ термдер жиынтығын қалыптастыруға болады. Болашақта атақты әдістер негізінде көрсетілген нақты емес сандар үшін қажетті тиістілік функциясы қалыптасады.Сонымен бірге бұдан да басқа термдердің бастапқы мәндері де енгізілуі мүмкін, мысалы, «өте төмен»(ӨТ), «орташадан жоғарылау» (ОЖ), «Отрашадан төмен» (ОТ) және т.б. Көзге көрініп тұрғандай, $\boldsymbol{BC_3}$ сипаттамасы мұндай жағдайда лингвистикалық мәндерді терумен беріледі, бірақ тек жеке жағдайда, ол нақты немесе интервалды мән қабылдауы мүмкін, онда оның берілуі үшін қаралау жазуды қолданамыз, мысалы, BC_3.

Сонымен бірге, қауіпті анықтау кездеседі оны **қауіптілік** түрінде беретін: болжалды (белгілі); қазірше белгісіз , бірақ пайда болуы мүмкін [1, 28]; шабуыл арқылы шығындандыру (белсенді немесе белсенділер тобының әлсіздіктерін қолданумен кейбір қауіпті жүзеге асыру [5]).

Тағы да бір қауіптің базалық сипаттамасын яғни **(BC_4) қауіптілікті** анықтайық. ақпараттық қауіпсіздік оқиғасының бұзылу қауіптілігімен сипатталатын шама түрінде қарастырастырылады, мысалы, BC_{12} арқылы BC_{21}. $\boldsymbol{BC_3}$ аналогиясы бойынша $\boldsymbol{BC_4}$ базалық сипаттамасы нақты санды формада (мысалы, пайызда) беріледі де, BC_4 түрінде белгіленеді немесе лингвистикалық айнымалы көмегімен – «**ҚАУІПТІЛІК**» базалық терм-жиынтықпен $\boldsymbol{BC_4} = \bigcup_{i=1}^{bc_4} \underset{\sim}{BC}_{4i}$ ($\underset{\sim}{BC}_{41} < \underset{\sim}{BC}_{42} < ... < \underset{\sim}{BC}_{4bc_4}$). Мысалы, bc_4=3 болса, «төмен» (Т), «орташа» (О) және «жоғары» (Ж) лингвистикалық эквиваленттері бар $\boldsymbol{BC_4} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{4i} = \{\underset{\sim}{BC}_{41}, \underset{\sim}{BC}_{42}, \underset{\sim}{BC}_{43}\} = \{\underset{\sim}{H}, \underset{\sim}{C}, \underset{\sim}{B}\}$ анықтауға болады.

Оны шығындар мен жоғалтулар жиілігі түрінде анықтайтын анау немесе мынау оқиғаның пайда болуымен тура байланысты қауіп түсініктері белгілі. Олардың кейбіреулерін келтіріп өтейік, мысалы, қауіп: «қауіптілік» жүзеге асуының жиілігі түрінде [13]; мүмкін болған өлшемде оқиға көлемінің қосылуы [15]; өзге шарттылықтармен шешім оптималды болған кездегі белгілі бір шешімді жүзеге асыруға байланысты (мысалы, жоспарлы нұсқада) экономикалық тиімділік **шығындары немесе жоғалтулары** [12]. Сонымен бірге қауіп кез келген контекстте бопсалаудың (шығынға кездіктіретін оқиғалар), осалдығының (мекемелердің бопсалауларға ашықтығы) және мүлік бағасы (белсендінің қауіптілік кезіндегі тұратын бағасы) суммалық шамасы түрінде қаралады. Бұл факторлардың кез келгенінің үлкеюі сәйкесінше қауіпті де өсіреді, ал төмендеуі оның төмендеуіне алып келеді [38].

Міне осылай жоғарыда көрсетілген қауіптің талқылаулар жиынтығынан және мынадай базалық сипаттамалардың ішінен ерекше айтуға болады: ақпараттық қауіпсіздік оқиғасының бұзылуына алып келген **(BC_5) жиілігін ақпараттық қауіпсіздіктер саласындағы** «бопсалау» жиілігіне байланыстыруды жүзеге асыруға болады. Мұндай компонентті (BC_5) санды немесе лингвистикалық айнымалы- «**ЖИІЛІК**» арқылы беруге болады, мысалы, $\boldsymbol{BC_5} = \bigcup_{i=1}^{bc_5} \underset{\sim}{BC}_{5i}$ ($\underset{\sim}{BC}_{51} < \underset{\sim}{BC}_{52} < ... < \underset{\sim}{BC}_{5bc_5}$), егер bc_5=3 болса, онда $\boldsymbol{BC_5} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{5i} = \{\underset{\sim}{BC}_{51}, \underset{\sim}{BC}_{52}, \underset{\sim}{BC}_{53}\} = \{\underset{\sim}{H}, \underset{\sim}{C}, \underset{\sim}{B}\}$, мұндағы $\underset{\sim}{H}, \underset{\sim}{C}$ мен $\underset{\sim}{B}$ сәйкесінше лингвистикалық эквиваленті - «төменгі»(Т) «орташа»(О) «Жоғары»(Ж). **Шығын мен жоғалтудың** базалық сипаттамсын анықтап алайық ақпараттық қауіпсіздік саласында **(BC_6) шығын** терминдері арқылы анықтау мен (BC_6) сандық жағынан ұсыну мақсатқа сай, мысалы, қойылған интервалдарда 1) 0 - $100; 2) $100 - $1000; 3) $1000 - $10 000; 4) $10 000 - $100 000. Сонымен бірге $\boldsymbol{BC_6}$ «**ШЫҒЫНДАР**» **лингвистикалық айнымалы**

көмегімен анықтауға болады: $\boldsymbol{BC_6} = \bigcup_{i=1}^{bc_6} \underset{\sim}{BC}_{6i}$ ($\underset{\sim}{BC}_{61} < \underset{\sim}{BC}_{62} < ... < \underset{\sim}{BC}_{6bc_6}$), мұндағы, мысалы, bc_6=5 болса, лингвистикалық айнымалы $\boldsymbol{BC_6} = \bigcup_{i=1}^{5} \underset{\sim}{BC}_{6i} = \{\underset{\sim}{BC}_{61}, \underset{\sim}{BC}_{62}, \underset{\sim}{BC}_{63}, \underset{\sim}{BC}_{64}, \underset{\sim}{BC}_{65}\} = \{\underset{\sim}{H}, \underset{\sim}{HC}, \underset{\sim}{C}, \underset{\sim}{BC}, \underset{\sim}{B}\}$ түріне ие болады , ал нақты емес сандар қолданылып жатқан лингвистикалық эквиваленттер сәйкесінше «төмен» (Т), «орташадан төмен» (ОТ), «орташалар» (О), «Орташадан жоғары» (ОЖ) және «жоғары» (Ж). Практикада $\boldsymbol{BC_6}$ интеграцияланған ұсынысы да кездеседі, мысалы, 1) *Negligible* ($100-дан кем); 2) *Minor* ($1000кем); 3) *Moderate* ($10 000 кем); 4) *Serious* (бизнеске айтарлықтай жағымсыз әсер етеді); 5) *Critical* (Апаттық әсер, мекеме қызметінің тоқтауы болуы мүмкін) [17]. Мұндай жағдайда сипаттамалар BC_6 / $\boldsymbol{BC_6}$ түрінде белгіленеді.

зерттеліп жатқан қауіп талқылаулар жиынтығы үшін оның базалық сипаттамасы бөлінген еді: қауіп өлшенетін немесе есептеп шығаратын ықтималдылық түрінде қаралады; қауіп белгілі бір оқиғаның басталуымен байланысты (әдеттегідей, сәтсіз); қауіп түсінігі субъект қызметі арқылы ашылады; қауіп субъекті қызметіне тәуелсіз түрде болып жатқан оқиға арқылы ашылады; қауіп шығын, жоғалту, қауіптілік түрінде қабылданады.

Адамның тіршілік әрекетінің әр түрлі сферасындағы қауіп түсінігінің анализін жүргізгеннен кейін жоғарыда келтірілген барлық анықтауларда кездесетін әрі оларды, авторлар ықтималдылықпен, әрекетпен немесе қызметпен, жиілікпен, жоғалтулармен, қауіптілікпен тағы басқамен байланыстыратын, болуы керек болған осы оқиға біріктіретін қауіптің бір сипаттамасын ерекше көрсетуге болады.

Ақпараттық қауіпсіздік аспектінде қауіпті ақпараттық жүйелер ресурсына бопсалауды жүзеге асыратын оқиғамен байланыстыруға болады, оның салдарынан бір немесе одан да көп қауіпсіздіктің базалық сипаттамаларының-құпиялылығының, тұтастығының, қол жетімділігінің бұзылуына алып келіп соғады. Сонымен бірге, оны белгілі бір жиілікпен т.б болып жатқан оқиға, субъектінің қатысуымен немесе қатысуысыз - субъектінің қызметі немесе әрекетсізденуімен болған оқиға ықтималдылығы түрінде суреттеуге болады.

Сонымен бірге қауіп түсінігін ашу кезінде ақпараттық қауіпсіздік бойынша шешімдердің көпшілігі белгісіздік шарттылықтарында қабылдануын есепке алып отыру керек [39].

Жүргізілген анализ қауіптің әр түрлі талқылаулары жалпы жиынтық сипаттамасына ие екендігін көрсетеді, мысалы, қауіптің ықтималдылықпен және белгілі бір оқиғаның басталуымен т.б. байланысы. Бұл түсінікті ақпараттық қауіпсіздік саласында интерпретациялау үшін оның осы сфераға қатысты базалық сипаттамасының жиынтығын ерекшелеу қажет.

Жалпылау түрінде ақпараттық қауіпсіздік сферасында берілген қауіптің базалық сипаттамасының интеграцияланғандығын қолдану үшін оларды *m*-компонентті $\boldsymbol{< BC_1, BC_2, ..., BC_m >}$ базалық кортеж моделі түрінде таныстыру ұсынылады, мұндағы m ($m \leq n$) –кортеждегі мүшелер саны. Мысалы, m=6 болғанда алты компонентті кортеж мынадай түрге ие болуы мүмкін: $\boldsymbol{<BC_1, BC_2, BC_3, BC_4, BC_5, BC_6>}$, мұндағы $\boldsymbol{BC_1}$ – әрекет, $\boldsymbol{BC_2}$ – оқиға, $\boldsymbol{BC_3}$ – ықтималдылық, $\boldsymbol{BC_4}$ – қауіптілік, $\boldsymbol{BC_5}$ – жиілік, $\boldsymbol{BC_6}$ – шығындалу мен жоғалулар (шығындар). қолданылып жатқан сипаттамалардың нақтылығының нәтижесінде жеке кортежді модель пайда болады, мысалы, BC_{12} = «Тыңшылық» үшін, BC_{22} = «НК», bc_3=3, bc_4=3, bc_5=3 және bc_6=5 мына түрге ие болады: $<BC_{12}, BC_{21}, \boldsymbol{BC_3}, \boldsymbol{BC_4}, \boldsymbol{BC_5}, \boldsymbol{BC_6}> = <BC_{12}, BC_{21}, \bigcup_{i=1}^{3} \underset{\sim}{BC}_{3i}, \bigcup_{i=1}^{3} \underset{\sim}{BC}_{4i}, \bigcup_{i=1}^{3} \underset{\sim}{BC}_{5i}, \bigcup_{i=1}^{5} \underset{\sim}{BC}_{6i}>$.

Көрініп тұрғандай егер базалық шамалар нақты немесе нақты емес мәндерге ие болса, онда жеке кортежде (жеке кортежді модельде) олар сәйкесінше қанық қара жазумен немесе қанық емес жазумен белгіленеді, мысалы, BC_{12}, BC_{21} немесе $\boldsymbol{BC_3}$, $\boldsymbol{BC_4}$, $\boldsymbol{BC_5}$, $\boldsymbol{BC_6}$.

Ұсынылған кортежді модель негізінде қауіпті бағалау мен бар болған анализ амалдарының кең ауқымды спектрін бастапқы мәліметтердің жұмыс істеуі үшін қажетті қалыптастыру позициясы жағынан зерттеуді жүзеге асыруға болады, бұл жаңа жүйені жасауға амал анықтауға немесе қолда барын ақпараттық қорғау тапсырмаларына сәйкесінше тиімді шешім қабылдау

мақсатында қолдануға мүмкіндік береді.

ӘДЕБИЕТ

[1] Қауіп анализі – әдіснама негізі ақпараттық қауіпсіздік мәселелерінің шешімі және қоршаған ортасы [Электронды ресурс]: Нұсқа «Экологиялық қауіасіздік». Украинаның экологиялық қауіпсіздігі. Жан-жақты дамудың жүйелік анализі. 3 бөлім. / А.Б. Качинскький – Электронды мәлімет – К.: Ұлттық стратегиялық зерттеу институты – 2001. – Қол жетімді нұсқау World Wide Web. – URL: http://www.niss.gov.ua/book/Kachin/1-3.htm. – Загл.экраннан (2015 жылдың 15 наурызында қаралды).

[2] Глоссарий [Электронный ресурс]: Сөздікті тақырыптық талқылау қызметі / С.Ю.Соловьев жоба жетекшісі; Н.В.Казеннова білім базасының редакторы; Г.П. Гинкул семантикалық желі шебері – Электрон. мәліметтер. – М.: ООО "Web and Press", 2000–2010. – Тәртіп мүмкіндігі: World Wide Web. – URL: http://www.glossary.ru/. – Загл. экраннан (2010 жылдың 25 сәуірде қаралды).

[3] Дзекцер Е.С. Геологиялық қауіптілік пен қауіп (методологиялық зерттеу) / Е.С. Дзекцер // Инженерлік геология. – 1992. – № 6. – С. 3-10.

[4] Захаров А.И. Ақпараттық жүйелер: қауіпті бағалау / А.И. Захаров // Information Security (Ақпараттық қауіпсіздік) – 2005. – №6 – С. 18–19.

[5] Ақпараттық технология. Қауіпсіздікті қамтамасыз ету амалдары мен әдістері. 1. Бөлім. Концепция мен ақпараттық және телекоммуникациялық технологиялар қауіпсіздігінің менеджмент модельдері: ГОСТ Р ИСО/МЭК 13335-1 – 2006. – Введ. 2007.05.31. – М.: ИПК "Стандарттар басылымы", 2007. – 23 с.

[6] Ақпараттық технология. Қауіпсіздік амалдары мен әдістері. Ақпараттық технологиялар қауіпсіздігін бағалау методологиясы = Information technology. Security techniques. Methodology for IT security evaluation.: МЕСТ Р ИСО/МЭК 18045–2008. – Кіріспе. 2008.12.18. – М.: ИПК "Стандарттар баспасы", 2008. – 234 с.

[7] Ақпараттық технология. Программалық амалдардың және жүйелердің тұтастық дәрежелері: МЕСТ Р ИСО/МЭК 15026 – 2002. Кіріспе. 2003.06.30. – М.: ИПК "Стандарттар баспасы", 2003. – 15 с.

[8] "Қауіп" түсінігін анықтау туралы сұраққа [Электронды ресурс]: сырттай электронды конференциялар /Индеева В.В. –Электрон. мәл.– М.: Рессейдің Жаратылыстану Академиясы, 2009. – Тәртіп мүмкіндігі: World Wide Web.– URL: http: http://www.rae.ru/zk/arj/2007/02/Indeeva.pdf. – Загл. экран (2010 жылдың 20 сәуірде қаралды).

[9] Кондратьев М.Ю. Қоғамдық психолог әліппесі-практикасы: Анықтамалық-энциклопедиялық басылым / М.Ю. Кондратьев, В.А. Ильин. – М.: ПЕР СЭ, 2007. – 464 с.

[10] Коноплицкий В.А. Бұл – бизнес. Экономикалық терминдерді талқылау сөздігі. / В.А. Коноплицкий, А.И. Филина. – К.: "Альтерпресс" баспасы, 1996. – 184 с.

[11] Корченко О.Г. Нақты емес жиынтықта ақпаратты қорғау жүйесін құру. Ақпаратты қорғау жүйесін құру. Практикалық және теория шешімдері. – К.: «МК-Пресс», 2006. – 320с., ил.

[12] Лопатников Л.И. Экономикалық-математикалық сөздік /Лопатников Л.И.// Заманауи экономикалық ғылымның сөздігі. – 5-е изд., өңдеу мен толық.. – М.: Дело, 2003, – 520 с.

[13] Маршалл В.К. Химиялық өндірістің негізгі қауіптіліктері/ Маршалл В.К. – М.: Мир, 1989. – 672 с.

[14] Қауіп менеджменті. Терминдер мен анықтаулар: МЕСТ Р 51897–2002. – Кіріспе. 2001.05.31. – М.: ИПК "Стандарттар баспасы", 2002. – 8 с.

[15] Мушик Э. Техникалық шешімдерді қабылдау әдістері / Э. Мушик, П. Мюллер. – М.: Мир, 1990. – 206 с.

[16] Нестеров С. А. Microsoft операциялық жүйелер базасында ақпараттық желілердегі қауіпті басқару мен анализдеу: [Оқу курсы.] / Нестеров С. А. – Санкт-Петербург.: "INTUIT" баспасы, 2009. – 136 с.

[17] Ожегов С. И. Орыс тілінің талқылау сөздігі: 80 000 сөз бен фразеологиялық мағыналар /С.И. Ожегов, Н.Ю. Шведова. – 4-е басп., толық. – М.: Азбуковник, 1999. – 944 с. – (Рессейдің ғылыми академиясы. В. В. Виноградов атындағы орыс тілі институты).

[18] Психология бойынша Оксфордтық талқылау сөздігі / [под. Ред. А. Ребера]. – Oxford: Penguin Non-Classic, 2002. – 864 с.

[19] Петренко С. А Ақпараттық қауіпті басқару. Экономикалық ақталған қауіпсіздік / С. А. Петренко, С. В. Симонов. – М.: АйТи Компаниясы, ДМК Пресс, 2004. – 384 с.

[20] Рагозин Ф. Техногендік және табиғи процесстерден қауіп пен қауіптілікті картографиялау және бағалау (теория мен методология) / Ф. Рагозин // Төтенше жағдайлар кезіндегі қауіпсіздік мәселелері. – 1993, №5. – С. 16–41.

[21] Қауіп [Электронды ресурс] / [Википедия авторлары]. – 44986537 нұсқасы // Википедия: Еркін энциклопедия. – Электрон. мәл. – Сан-Франциско: Викимедиа қоры, 2012. – Қол жетімді нұсқау: World Wide Web. – URL:http://ru.wikipedia.org/?oldid=44986537. – Загл. титул. экраннан. – 3 маусым 2012 08:54 UTC уақыты бойынша нұсқау негізіне сүйене.

[22] Еңбекті қорғау бойынша Ресей энциклопедиясы: [В 3 т.]. – 2-е басп., өңдеу. мен толы. – М.: НЦ ЭНАС баспасы, 2007. – Т. 2: Л – Р. – 408 с.

[23] Қауіпті қауіпсіздендіруді басқару бойынша нұсқаулық [Электрондық ресурс] / Қауіпсіздік пен сәйкестендіру бойынша Майкрософт шешімдерін реттеуші нормалармен өңдеу тобы; Центр Microsoft security center of excellence // TechNet. – Электрон. мәл. – Редмонд, США: Корпорация Майкрософт, 2006. – Қол жетімді нұсқау: World Wide Web.– URL: http://technet.microsoft.com/ru-ru/library/cc163143. aspx. – Загл. экраннан (2014 жылдың 29 желтоқсанда қаралған).

[24] Симонов С. В. Қауіпті басқару үшін аспаптар мен технологиялар /С. В. Симонов// Ақпараттық бюллетень Jet Info. – 2003. – № 2 (117)/2003. – С. 3 – 32.

[25] Қаржы мен экономика бойынша сөздік. Глоссарий. ру [Электронный ресурс] / Яндекс // Яндекс: [интернет-портал]. – Электрон. мәл. – М.: Көпшілік алдындағы компания "Яндекс", 2010. – Қол жетімді нұсқау: World Wide Web. – URL: http://slovari.yandex.ru/dict/glossary. – Загл. экраннан (2014 жылдың желтоқсанда қаралған).

[26] Әлеуметтік психология / ред. Петровский А. В., редактор-құрастырушы Карпенко Л. А., ред. Венгер А. Л. – М.: ПЕР СЭ, 2005. – 176 с.

[27] Ресей Федерациясында стандарттау. Терминдер мен анықтаулар = Standardization in the Russian Federation. terms and definitions: ГОСТ Р 1.12 – 2004. – Введ. 2005.07.01.– М.: ИПК "Стандарттар баспасы", 2004.– 17с.

[28] Сақтандыру бизнесі: анықтама-сөздігі [Электрондық ресурс] / Халықаралық Қауіпті зерттеу Институты. – Электрон. мәл. – М.: Халықаралық Қауіпті зерттеу Институты, 2010. – Қол жетімді нұсқау: World Wide Web. – URL: http://www.miir.ru. – Загл. экраннан (2015 жылы 20 мамырда қаралған).

[29] Рұқсатсыз кіруден компьютерлік жүйелерде ақпараттық қауіпсіздік саласындағы терминологиясы [Мәтін]: ND TZ 1.1-003 – 1999. – 04.28. - К. : DSDZI Украина Қауіпсіздік қызметі, 1999. – 12б.

[30] Сенімділікті басқару. Технологиялық жүйелер қауіпінің анализі: ГОСТ Р 51901 – 2002. – Введ. 2003.09.01. – М.: ИПК "Издательство стандартов", 2002. – 21 с.

[31] Широков К. П. Үлкен кеңес энциклопедиясы / К. П. Широков. – М.: Печь – Польцин, 1955. – 669 с.

[32] Control Objectives for IT and reated Technology Framework Control Objectives Management Guidelines Maturity Models: COBIT 4.1. – Rolling Meadows: IT Governance Institute, 2007. – 196 p.

[33] Fiksel J. Quantitative risk analysis for toxic chemicals in the environment // of hazard materials. – 1987. – 10, № 2-3. – P. 227–240.

[34] Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013 // International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2013. – 34 p.

[35] Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Gary Stoneburner, Alice Goguen, Alexis Feringa]: National Institute of Standards and Technology Special Publication 800-30 – Falls Church: Natl. Inst. Stand. Technol, 2002. – 54 p.

[36] Risk management. Vocabulary: ISO Guide 73:2009 // International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2002. – 15 p.

[37] Rowe W. An anatomy of risk. / W. Rowe – NY/: John Wiley, 1997. – 488 p.

[38] Smith M. Commonsense Computer Security, your practical guide to information security / M. Smith // London: McGraw – Hill, 1993 – 105 p.

[39] Taha, Hamdy A. Operations Research. An Introduction. / Taha, Hamdy A. –New York: MacMillan Publishing Company, 1987. – 123 p.

[40] U. S. Geological Survey: Proposed procedures for dedealing with warning and preparedness for geologic-related hazard // United States Federal Register. – 1977, 42. №70. – P. 14292–14296.

REFERENCES:

[1] Risk analysis – a methodological basis for the solution of security problems of personality and environment [Electronic resource] : "Environmental security" Series. Environmental securityof Ukraine.Asystemic analysis of perspectivesof improvement.Chapter 3 /A. B.Kachin'ski – Electronic data. – K.: National Institutefor Strategic Studies– 2001. – Mode of access:World Wide Web. – URL: http://www.niss.gov.ua/book/Kachin/1-3.htm. – The titul from screen (viewedat March 15,2015).

[2] Glossary [Electronic resource]: Service of thematic explanatory dictionaries / project manager S. Yu. Solovyov; editor of knowledge bases N. V. Kazennova; master of a semantic network G. P. Ginkul. – The electronic this– M. : OOO "Web and Press", 2000–2010. – access mode: World Wide Web. – URL: http://www.glossary.ru/. – from the screen (it is seen on April 25, 2010).

[3] Dzektser E.S. Geologicheskaya danger and risk (methodological research) / E.S. Dzektser//Engineering geology. – 1992. – No. 6. – C. 3-10.

[4] Zakharov A.I. Information systems: assessment of risks / A.I. Zakharov//Information Security (Information security) – 2005. – No. 6 – Page 18-19.

[5] Information technology. Methods and means of ensuring of safety. Part 1. Concept and models of management of safety of information and telecommunication technologies: State standard specification P ISO/MEK 13335-1 – 2006. – Vved. 2007.05.31. – M.: IPK "Standards Publishing House", 2007. – 23 p.

[6] Information technology. Methods and means of ensuring of safety. Methodology of an assessment of safety of information technologies = Information technology. Security techniques. Methodology for IT security evaluation. : State standard specification P ISO/MEK 18045-2008. – Vved. 2008.12.18. – M.: IPK "Standards Publishing House", 2008. – 234 p.

[7] Information technology. Levels of integrity of systems and software: State standard specification P ISO/MEK 15026 - 2002. Vved. 2003.06.30. – M.: IPK "Standards Publishing House", 2003. – 15 p.

[8] To a question of definition of the concept "risk" [An electronic resource]: the correspondence electronic conferences / Indeeva V. V. – the Electron. it is given. – M.: Russian Academy of Natural sciences, 2009. – Access mode: World Wide Web. – URL: http: http://www.rae.ru/zk/arj/2007/02/Indeeva.pdf. – from the screen (it is seen on April 20, 2010).

[9] Kondratyev M. Yu. Alphabet of the social expert psychologist: Help and encyclopedic edition / M. Yu. Kondratyev, V.A. Ilyin. – M.: PER SE, 2007. – 464 p.

[10] Konoplitsky V.A. Eto – business. Explanatory dictionary of economic terms. / V.A. Konoplitsky, A.I. Filina. – To.: Alterpress publishing house, 1996. – 184 p.

[11] Korchenko O. G. Creation of systems of information security on indistinct sets. Theory and practical decisions. – To.: "MK-Press", 2006. – 320p.

[12] Lopatnikov L. I. L.I economic-mathematical dictionary / Lopatnikov.//Dictionary of modern economic science. – 5th prod., reslave. and additional – M.: Business, 2003, – 520 p.

[13] Marshall V. K. Main dangers of chemical productions / Marshall V. K. – M.: World, 1989. – 672 p.

[14] Management of risk. Terms and definitions: GOST P 51897-2002. – Vved. 2001.05.31. – M.: IPK "Standards Publishing House", 2002. – 8 p.

[15] Front sights E. Methods of acceptance of technical solutions / E. Mushik, P. Müller. – M.: World, 1990. – 206 p.

[16] Nesterov S. A. The analysis and risk management in information systems on the basis of operating systems of Microsoft: [Training course.] / Nesterov S. A. – St. Petersburg.: INTUIT publishing house, 2009. – 136 p.

[17] Ojegov S. I. Explanatory dictionary of Russian: 80 000 words and phraseological expressions / S. I. Ojegov, N. Yu. Shvedova. – 4 prod., added. – M.: Azbukovnik, 1999. – 944 pages – (The Russian Academy of Sciences. Institute of Russian of V. V. Vinogradov).

[18] The Oxford explanatory dictionary on psychology / [under. A. Reber edition]. – Oxford: Penguin Non-Classic, 2002. – 864 p.

[19] Petrenko S. And Management of information risks. Economically justified safety / S. A. Petrenko, S. V. Simonov. – M.: Press IT, DMK company, 2004. – 384 p.

[20] Ragozin F. Otsenka and mapping of danger and risk from natural and technogenic processes (the theory and methodology) / F. Ragozin//safety Problems at emergency situations. – 1993, No. 5. – Page 16-41.

[21] Risk [An electronic resource] / [Authors of Wikipedia]. – Version 44986537//Wikipedia: Free encyclopedia. – Electron. it is given. – San Francisco: Fund of Vikimedia, 2012. – Access mode: World Wide Web. – URL: http://ru.wikipedia.org/? oldid=44986537. – Zagl. about a title. screen. – The description on the basis of the version dated on June 3, 2012 08:54 UTC.

[22] The Russian encyclopedia on labor protection: [In 3 t.]. – 2nd prod., reslave. and additional – M.: Publishing house of NTs ENAS, 2007. – T. 2: L – R. – 408 p.

[23] A control directive risks of safety [An electronic resource] / Group of development of decisions Microsoft on safety and compliance, regulatory norms; Microsoft security center of excellence//TechNet Center. – Electron. it is given. – Redmond, USA: Microsoft corporation, 2006. – Access mode: World Wide Web. – URL: http://technet .microsoft.com/ru-ru/library/cc163143.aspx. – Zagl. from the screen (it is seen on December 29, 2014).

[24] Simonov S. V. Technologies and tools for risk management / S. V. Simonov//the Newsletter of Jet Info. – 2003. – No. 2 (117)/2003. – Page 3 – 32.

[25] The dictionary on economy and finance. Glossary. py [Electronic resource] / Yandex//Yandex: [Internet portal]. – Electron. it is given. – M.: Public company "Yandeks", 2010. – Access mode: World Wide Web. – URL: http://slovari.yandex.ru/dict/glossary. – Zagl. from the screen (it is seen on December 19, 2014).

[26] Social psychology / under the general editorship of. Petrovsky A. V., editor originator Karpenko L. A., under the editorship of Wenger A. L. – M.: PER SE, 2005. – 176 p.

[27] Standardization in the Russian Federation. Terms and definitions = Standardization in the Russian Federation. terms and definitions: GOST P 1.12 - 2004. – Vved. 2005.07.01. – M.: IPK "Standards Publishing House", 2004. – 17 p.

[28] Insurance business: dictionary reference [An electronic resource] / International Institute of Research of Risk. – the Electron. it is given. – M.: International Institute of Research of Risk, 2010. – Access mode: World Wide Web. – URL: http://www.miir.ru. – Zagl. from the screen (it is seen on May 20, 2015).

[29] The terminology in the field of information protectionin computer systemsfrom unauthorized access[Text] : NDTZI 1.1-003 – 1999. Chin. 1999. 04.28. – K. : DSDZI Security Service of Ukraine, 1999. – 12p.

[30] Management of reliability. Analysis of risk of technological systems: GOST P 51901 – 2002. – Vved. 2003.09.01. – M.: IPK "Standards Publishing House", 2002. – 21 p.

[31] Shirokov K. P. Big Soviet encyclopedia / K. P. Shirokov. – M.: The furnace – Poltsin, 1955. – 669 p.

[32] Control Objectives for IT and reated Technology Framework Control Objectives Management Guidelines Maturity Models: COBIT 4.1. – Rolling Meadows: IT Governance Institute, 2007. – 196 p.

[33] Fiksel J. Quantitative risk analysis for toxic chemicals in the environment//of hazard materials. – 1987. – 10, № 2-3. – P. 227–240.

[34] Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013//International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2013. – 34 p.

[35] Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Gary Stoneburner, Alice Goguen, Alexis Feringa]: National Institute of Standards and Technology Special Publication 800-30 – Falls Church: Natl. Inst. Stand. Technol, 2002. – 54 p.

[36] Risk management. Vocabulary: ISO Guide 73:2009//International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2002. – 15 p.

[37] Rowe W. An anatomy of risk. / W. Rowe – NY/: John Wiley, 1997. – 488 p.

[38] Smith M. Commonsense Computer Security, your practical guide to information security / M. Smith // London: McGraw – Hill, 1993 – 105 p.

[39] Taha, Hamdy A. Operations Research. An Introduction. / Taha, Hamdy A. –New York : MacMillan Publishing Company, 1987. – 123 p.

[40] U. S. Geological Survey: Proposed procedures for dedealing with warning and preparedness for geologic-related hazard // United States Federal Register. – 1977, 42. №70. – P. 14292–14296.

Кортежная модель базовых характеристик риска

Б.С.Ахметов, А.Г.Корченко, М.Н. Жекамбаева, С.В. Казмирчук.
b_akhmetov@ntu.kz, maia.kz@mail.ru
Казахский национальный исследовательский технический университет
имени К.И.Сатпаева, г. Алматы.
Национальный авиационный университет, Украина.

Ключевые слова: анализ риска, оценивание риска, базовые характеристики риска, кортежная модель, риск информационной безопасности, лингвистическая переменная.

Аннотация. Целью данной работы является анализ и раскрытие понятия риска и определение его базовых характеристик, для последующий интерпретации в области ИБ, это расширит возможности по повышению эффективности решений задач ЗИ.

Учитывая, что риски затрагивают различные предметные области, то это понятие следует рассмотреть с точки зрения безопасности, психологии, экономики, страхования, медицины, геологии и т.д., которое раскрывается как в монографиях, статьях, учебниках, словарях, так и различных нормативных, национальных и международных документах.

Поступила 19.09.2015 г.