DOI: 10.53360/2788-7995-2024-1(13)-4

МРНТИ: 62.39.05

Б.С. Ахметов[1], В.А. Лахно[2], Л.М. Кыдыралина[3*]
[1]Абай атындағы Қазақ ұлттық педагогикалық университеті,
050010, Қазақстан Республикасы, Алматы қаласы, Достық даңғылы, 13
[2]Биоресурстар және табиғатты пайдалану ұлттық университеті,
030414, Украина, Киев қ., Қорғаныс батырлары к-сі, 15
[3]Семей қаласының Шәкәрім атындағы университеті,
071412, Қазақстан Республикасы, Семей қ., Глинки к-сі, 20 А
*e-mail: lazat_75@mail.ru

ОҚУ ОРЫНДАРЫНЫҢ АҚПАРАТТЫҚ КЕҢІСТІГІНІҢ КИБЕРҚОРҒАУ САЛАСЫНДАҒЫ АЛДЫҢҒЫ ЗЕРТТЕУЛЕРГЕ ШОЛУ ЖӘНЕ ТАЛДАУ

Аңдатпа: *Мақалада заманауи ЖОО-ның қауіпсіз ақпараттық білім беру ортасын қалыптастырудың алғышарттары қарастырылған. Отандық және жетекші шетелдік зерттеулердің жарияланымдары талданды. Оқу орындарының ақпараттық кеңістігін киберқорғау саласындағы алдыңғы зерттеулерге шолу және талдау жасалды. Осы тақырып бойынша шыққан жарияланымдарға талдау жасалды. Жасалған талдау жоғары оқу орындарының ККау жүйесін үздіксіз өзара инвестициялау міндеттерінде ШҚЖ үшін модельдерді одан әрі дамыту проблемасының өзектілігін растады. Ақпараттандыру нысандардың ККау қатерлерінің моделін сипаттау үшін Петри желілерін қолдануға арналған зерттеулер нәтижелері бойынша жарияланымдарға талдау жасалды. Бұл жұмыстар осы міндетте айтарлықтай теориялық үлес қосса да, біздің ойымызша, авторлар ұсынған модельдерді, атап айтқанда АН-ді АҚ және ККау бойынша ШҚИЖ-да және СЖ-да бағдарламалық жүзеге асыру біршама қиынға соғады. Бұл өз кезегінде қосымша зерттеулерді талап етеді.*

Түйін сөздер: *киберқауіпсіздік, жоғары оқу орнының ақпараттық білім беру ортасы, моделдеу, Петри желісі, ақпаратты қорғау, жоғары оқу орнының электронды ақпараттық білім беру ортасы, әдіс, модель.*

Кіріспе

ТМД елдері ғалымдарының көптеген еңбектері мемлекеттік құрылымдардың, оның ішінде ЖОО-ның ақпараттық-коммуникациялық жүйелерінің (АКЖ) киберқорғау міндеттерін теориялық зерттеуге арналған: Р.Н. Акиншин [3], Б.С. Ахметов [10], Р.Г. Бияшев [11], О.В. Есиков [3], В.А. Лахно [9], R. Ortalo [14], P. Puhakainen [13].

Алайда, Қазақстанда және ТМД-ның басқа елдерінде бұл басылымдардың көлемі шектеулі немесе айтарлықтай аз, олар тек «жоғары оқу орындарындарын киберқорғау қажеттілігі» тақырыбындағы баяндамалардың тезистерімен ғана шектелген [13]. Теориялық нәтижелер мен зерттеу нәтижелері кейбір басылымдарда, эксперименттік мәліметтер немесе имитациялық модельдеу нәтижелері басқа басылымдарда берілген [5]. Зерттеудің жеке сегменті ЖОО үшін АҚау-ды және ККау-ды қамтамасыз етудің аппараттық және бағдарламалық құралдарын құру міндеттеріне арналған [3].

Жарияланымдардың едәуір көп бөлігі, атап айтқанда, ЖОО ККау жүйесі үшін қаржылай инвестициялаудың тиімді стратегияларын таңдауға арналған зерттеулер [6, 8, 13].

Негізгі бөлім. АҚау және ККау модельдерінің ішінде Гордон-Лоеба (ГЛ) моделі ең негізгі және кең таралған. Бұл модельдің мақсаты ақпаратты қорғауға инвестициялардың оңтайлы мөлшерін анықтауға байланысты міндеттерді шешу.

ГЛ моделіндегі негізгі жағдай қарастырылып отырған ақпараттандыру нысаны үшін, атап айтқанда ЖОО АББО үшін АҚау-дың және ККау-дың деңгейін анықтайтын осалдық функциясын енгізу және дамыту. Ақпараттық нысанның әртүрлі формалары болуы мүмкін: қолданушылар тізімі, бухгалтерлік есеп кітабы, стратегиялық даму жоспары, веб-сайт және т.б. Қауіпсіздікті арттыру құпиялылықты, тұтастықты, нақтылықты, сенімділікті, қолданушылардың авторизациясының қол жетімділігін және т.б. қорғау бағытында орын алуы мүмкін.

Модель құрылымы бойынша статикалық болады. Демек, шешімдер мен нәтижелер бір уақытта пайда болады, ал динамикалық әсерлер, оның ішінде ақшаның уақытқа тәуелділігі ескерілмейді.

АҚау және ККау құралдары мен әдістеріне инвестициялар жұмсау осалдықтың жеткілікті кіші және жеткілікті үлкен мәндерінде тиімсіз екенін ескере отырып, ГЛ моделінің авторлары, сондай-ақ ГЛ моделіне негізделген идеяларды дамытқан [10] бірқатар жұмыстарда келесі жағдайлар атап өтілген.

Көптеген авторлар нысандарды төмен, орташа және жоғары осалдық деңгейлеріне бөлуді басқарудың бірінші міндеті және бұл жобалаудың алғашқы кезеңдерінде жасалуы керек деп санайды. Алайда, ГЛ моделінің және оған ұқсас модельдердің авторлары оның кемшіліктерін атап өтті:

– Шабуыл ықтималдығын және ақпараттық массивтердің осалдығын анықтайтын қарапайым процедура жоқ.

– Ақпараттандыру нысанының қорғау периметрлерінің қауіпсіздігі мен киберқауіпсіздігінің бұзылуынан болатын потенциалды шығындарды анықтау қиынға соғады. (ЖОО АББО үшін бұл АҚау және ККау периметрлері әлі де жеткілікті түрде шартты екенін ескереміз).

– Зерттеу нәтижелерін белгілі бір нысанға қатысты іске асырудың күрделілігі.

– Шабуылдаушының қорғаныс үшін қосымша инвестициялар салу кезінде өз стратегиясын қалай өзгертетіні ескерілмеген, атап айтқанда, динамикалық режимде қарама-қарсы келудің талдауы жоқ.

ГЛ моделі кеңінен танылып және жарияланған кезден бастап он жыл ішінде көптеген жұмыстарда дамығанына қарамастан, қойылған сұрақтардың басым бөлігі бүгінгі күнге дейін шешілмеген болып отыр. Модель авторларының сөзсіз еңбегі – бұл міндетті алғаш рет мұқият қарастырып және осалдық функциясын анықтағаны, ақпараттық саладағы қарама-қарсы тұруды қарастырудағы басты мәселе. Функцияның түрін анықтау, динамикалық жүйенің осалдығын білдіреді, ақпараттық қарама- қарсы тұруды математикалық модельдеудегі басты мәселе және көптеген зерттеушілердің жұмыстары осы мәселеге арналды [11].

Егер біз міндеттің тарихына жүгінетін болсақ, онда екі тараптың қарама-қарсы тұруын бірінші рет екінші дүниежүзілік соғыстың соңында әскери жоспарлаудың математикалық негіздерін құру кезінде RAND Corporation мамандары мұқият қарастырды. RAND фирмасы жасаған екі тараптың қарсы тұру моделі тактикалық әскери операцияларды имитациялауға арналған Гросс моделі [15]. Осы модельге сәйкес, қақтығысушы тараптардың X және Y ресурстары бар, олардың қарама-қарсы тұру нәтижесі салынған ресурстардың айырмашылықтарына сызықтық тәуелді және сызықтық бағдарламалар есебіне әкелетін мақсатты функциямен анықталады.

Әскери операцияларды жоспарлау кезінде пайда болған Гросстың есебінің қарастырылған есептерден бірқатар айырмашылықтары бар. Біріншіден, мақсатты функция дискретті, өйткені қорғаныс арқылы өтудің немесе шабуылды жоюдың немесе қорғаныс санын анықтайды. Екіншіден, бұл өлшемдер қарама-қарсы күрестің әрбір эпизодында шабуылдаушы үшін де және сәйкес қорғанушы үшін де бірдей.

Нысандардың біртектілігі есепті шешуді айтарлықтай жеңілдетеді, алайда қарсы күресу шарттарын шектейді. Алайда, Гросс моделінің басты кемшілігі – оның мақсатты функциясының сипаты үзік-сызықтық болып табылуында, ол әрине, нақты жағдайларға сәйкес келмейді. Осы себепті Гросс моделін оның қарапайымдылығын ескере отырып, мақсатты функцияны аппроксимациялау және бірінші жуықтауда нәтижелерді алу үшін ғана пайдаланады [12].

Ақпаратты қорғауға арналған шығындар көлеміне және ККау-ға байланысты, қатерлерді іске асыру салдарынан болған шығындар деңгейін есептеуге мүмкіндік беретін тағы бір математикалық модель модельдер [7,9] жұмыстарда сипатталған. Мына зерттеу жұмыстарының [11,10] мақсаты, ықтимал бөлудің белгілі әдістерін қолдана отырып, ақпаратты техникалық қорғау кешенінің (АТҚ) тұрақтылығын бағалау болды.

Қорғауға немесе оны модернизациялауға қаржылай инвестициялар болмаған жағдайда, уақытқа қарамастан қорғалудың сенімділігі нөлге тең болады. Бұл модель қамтамасыз ету ықтималдығының неғұрлым тиімді қаржыландыруға тәуелділігін анықтауға мүмкіндік береді.

Модельді құрудағы негізгі қиындықтар бұзу нәтижелері туралы статистикалық мәліметтерді жинаумен байланысты (және қорғаудың бұзылу фактісінің қажеттілігі), өйткені мұндай қорғаныс жүйесі бұдан кейін қайталанып қолданылмайды. Осыған байланысты автор [9,12] жеке қорғаныс жүйелерінің ықтималды сенімділігін бағалауға және оны бірнеше нысандарға орнатуға мүмкіндік беретін нақты бұзу әрекеттері негізінде АТҚ-ның ықтималды сенімділігін анықтау әдісін жасады (мысалы, бірнеше компьютерге антивирустық бағдарламаны орнату әрекетті ғана емес, сонымен қатар басқа компьютерлерді бұзу мүмкіндігіне кететін уақытты да қарастыруға болады) [10,16]. Бұл әдістің кемшілігі – бұл жағдайда жүйенің нақты бұзылуы салдарын талдау нәтижесінен алынатын АТҚ-ның тиімділігін білу қажеттілігі.

Зерттеулер нәтижесінде [9], авторлар АТҚ қасиеттерін анықтайтын параметр тек тұрақты шама ғана емес, сонымен қатар функция да да бола алатындығын көрсетті. Сонымен қатар, бұл функция бұзу әрекеттеріне және мұндай әрекеттер орын алған уақытқа байланысты тәуелді болады, мысалы, ақпараттандыру нысанының желісінде қолданушыны аутентификациялау процедурасы барысында парольдерді таңдау тактикасы кезінде [8, 2]. Зерттеу нәтижелері бойынша, бұзу әрекеттерінің жиілігін есептеуге мүмкіндік беретін функциялар алынды.

Глушак-Новиковтың моделі [2] қорғаудың максималды деңгейін қамтамасыз ететін жүйенің компоненттері (нысандары) арасында қорғаныс механизмдерін оңтайлы орналастыруға бағытталған.

Ақпаратты жоғалтудың минималды тәуекелін қамтамасыз ететін қорғау механизмдерінің оңтайлы жиынтығын іздеу, аумақтық таратылған ақпараттандыру нысанның аудандық бөлімшелерінің жүйесі мысалында жүргізілген (автор банк бөлімшесінің мысалында қарастырды) [4]. Әрбір бөлімшедегі ақпарат көлемі потенциалды клиенттердің саны, атап айтқанда аудан тұрғындарының санына пропорционалды. Жекелеген қатерлерді іске асыру ықтималдығы, сондай-ақ қорғау механизмдерінің әрқайсысының құны мен тиімділігі сараптамалық бағалау әдісімен анықталады. Бұл жағдайда әрбір нысан үшін қатердің туындау ықтималдығы бірдей және тек қатердің түріне байланысты болады деп болжанады. Әрбір аумақтық бөлімшелер үшін қорғаныс элементтерінің әртүрлі комбинацияларын ескере отырып, бүкіл жүйеге келтірілген жалпы барлық шығындар (ол қауіптің дәрежесін сипаттайды) және әрбір бөлімше үшін қорғаныс элементтерінің оңтайлы жиынтығы есептеледі. Сонымен бірге қорғау жүйесінің жалпы құнына шектеулер енгізу шарттарын тексеру қарастырылған.

Толық қауіпті есептеу кезінде әртүрлі қатерлерді жүзеге асырудан болатын шығын мөлшерін көрсететін теңдеулердің қиылысқан мүшелерінің мәні туралы міндет ашық күйінде қалады (бұл оқиғалар үйлесімді болып саналады) [14].

О.Е. Архиповтың жұмыстары тәуекелдерді бағалау және ақпараттық қауіпсіздікке салынған инвестициялардың тиімділігін зерттеу үшін «шабуыл-қорғау» экономикалық-құндық модельдерін қолдану міндеттеріне арналған [3]. Осы модельдердегі тәуекелдің ықтимал параметрлерін анықтау үшін ақпарат саласындағы «шабуыл-қорғау» жағдайына тән мотивациялық-құндық және экономикалық-қаржы қатынастардың белгілі бір сипаттамалары қолданылады. Атап айтқанда, шабуылдаушы A (шабуылдаушы) кейбір I ақпараттық ресурстарға қатысты T қаупін жүзеге асырған кезде пайда болатын жағдай B тарабына тиесілі.

Ақпараттық қатерді жүзеге асырудың экономикалық және шығындық сипаттамаларын талдау мен сандық бағалаудың нақты мүмкіндігі болған жағдайда, авторлар [3-6] еңбектерінде келтірілген модельдерді кез-келген нақты ұйымның тәуекелдерін есептеу үшін қолдануды ұсынады. Осы бағалаудың нәтижесін белгілі бір қосымша ақпарат болған кезде тәуекелдер менеджменті стандарттарының параметрлері мен ұсыныстарына сәйкес ұйымның ақпараттық қауіпсіздік жай-күйін зерттеу (аудит) жүргізу арқылы алуға болады, уақыт бойынша статикалық бағалауды қабылданған экономикалық-құндық шабуылдарды дамыту сценарийлеріне сәйкес уақыт өте келе өз мәндерін өзгертетін динамикалық түрде дамытуға болады [13].

«Шабуыл-қорғау» экономикалық-құндық модельдері нақты ұйым туралы нақты ақпарат негізінде осы ұйымның ақпараттық қауіпсіздігіне салынған қаражат көлемі жағынан жеткілікті ме екенін тексеруге мүмкіндік береді [14].

Ақпараттық жүйелерге жасалған кибершабуылдарды зерттеу В.А. Хорошконың [8] жұмыстарында көрсетілген. Кибершабуылдар кезінде қаскүнемдердің мүмкіндіктерін бағалау талдаудың ойын әдістерін пайдалана отырып жүргізіледі [12].

Ақпараттық салаға кибершабуылдаудың оңтайлы циклын рәсімдеу (шартты таңбалардың көмегімен модельді жазу) кезінде В.Нэш тұжырымдамасы қолданылады деп болжануда [1]. Бұл модельде қаржыландырудың оңтайлы шешімді таңдауға әсері ескерілмегенін айта кету керек, алайда зерттеушілер құрған талдаудың ойын әдістері жеке және топтық кибершабуылдарды бағалауға мүмкіндік беретінін көрсетіп отыр. Бұл ақпарат саласына мысалы, оқу орындарына жасалған кибершабуылдардан ақпараттың қорғалу деңгейінің кепілдендірілген және сенімді бағаларын алуға мүмкіндік береді [16].

Экономикалық қатынастар мен ақпараттық саланың, атап айтқанда білім беру саласының дамуы бәсекелестіктің күшеюіне, ақпарат көлемі мен құнының артуына, сондай-ақ ақпараттың жайылып кетуінен болған потенциалды шығындардың артуына, ақпараттық нысандар санының өсуіне (бұл әсіресе ЖОО АББО-да байқалады және қарқынды) және кибер-инциденттердің жиі болуына әкеледі. Бұл ретте екі тараптың: ақпаратты қорғау мен шабуылдаушы- қарама – қарсы тараптардың динамикалық өзара әрекеттесуін көрсете отырып, қарсы тұру жағдайларының шарттары да үнемі өзгеріп отырады.

Киберқорғау тараптарының стратегиясы мен тактикасының өзгеруі ақпараттық ресурстарға жаңа шабуылдар тудырады, олар бір жағынан қарсыластың ниетін көрсетеді, екінші жағынан шабуылдар немесе деструктивті араласудың өзге де әрекеттері бағытталған қорғаныстың әлсіз жақтарын көрсетеді.

ЖОО АББО-дағы КҚау-ды және АҚау-ды қамтамасыз ету тәсілдеріндегі өзгерістердің басқа себептері ақпараттың «ескіруіне», жаңа ақпарат пен қосымша ресурстарды енгізілуіне, нысандар арасында ақпараттық ресурстарды қайта бөлуге, олардың арасындағы жаңа байланыстардың пайда болуына байланысты факторлар болуы мүмкін.

Ақпараттық саладағы екі тараптың антагонистік қарсы тұруы , әдетте қорғаушыға шабуылдаушының (хакердің) іс – әрекеттері мен қаржылай мүмкіндіктері белгісіз болғанымен сипатталады.

Сонымен қатар, шабуылдаушылар қорғаныс жүйесінің құрылымы туралы біраз түсінікке ие және қауіпсіздік жүйесінің ең әлсіз буындарын бұзуға өз күш-жігерін жұмсай алады. Бұл шабуылдаушыға өте тиімді.

Қауіп – қатерлердің әртүрлі түрлерін бұғаттауға қорғау ресурстарын бөлу белсенді режимде – қарсыластың іс- қимылының алдын ала отырып, сондай-ақ мүмкін шабуылдардың бағыты айқын болған кезде қаржыландыруды кешіктіріп, атап айтқанда бейімделіп жүргізілуі мүмкін.

Ресурстарды динамикалық басқару қажеттілігі келесі себептерге байланысты:

– қарсыластың іс- әрекеті нұсқаларының белгісіздігі, атап айтқанда, ақпаратты алуға бағытталған күш-жігерінің бағыты және осы жұмыстың ауқымы, атап айтқанда бұзуға жұмсаған хакерлердің ресурстарының қаржы компоненттеріне де байланысты;

– уақыт өте келе қарама-қайшылықтың ішкі және сыртқы жағдайлары- ақпарат құнының өзгеруімен, оның нысандар арасында бөлінуімен, қарсыластың шабуылдарының бағытының өзгеруі, жаңа шабуылдаушылардың пайда болуымен;

– ақпараттық жүйе күйінің өзгеруі (ЖОО АББО-сы дербес жағдай ретінде қарастырылады), атап айтқанда, шабуылдардың бағытын анықтағаннан кейін және қорғау тарапынан тиісті шаралар қабылдағаннан кейін оның ең әлсіз буынының өзгеруімен.

Ақпаратты қорғау жүйелерін математикалық моделдеу бойынша ғылыми жұмыстарды талдау, негізгі міндет қорғауды қаржыландырудың көлемін анықтауға бағытталғанын көрсетті.

Қаржыны қорғау нысандары арасында бөлу міндеттері кейбір жұмыстарда көрсетілген [2, 4]. Сонымен қатар, қолданыстағы нәтижелер (модельдер) [6], шабуылдаушының мүмкін әрекеттері мен олардың салдары жүйенің көрсеткіштері мен сипаттамаларының өзгеруіне әсерін тигізетіні сирек ескереді.

Осылайша, зерттеліп отырған тақырыптағы жұмыстарға жүргізілген талдау шаруашылық қызмет субъектілері мен оқу орындарының ақпаратын қорғау үшін шектеулі қаржы ресурстарын тиімді пайдалану міндеті аса маңызды және маңызды бола түсетінін көрсетті [7].

Сонымен қатар, шабуылдаушы тараптың іс- әрекеттері мен қаржы ресурстарын белгілі бір ықтималдықпен ғана болжауға болатын белгісіздік жағдайында, теориялық-ойын әдістерін пайдалану және қарама-қайшылық шарттарының өзгеру динамикасын ескере отырып қорғау нысандары арасында шектеулі ресурстарды оңтайлы бөлуді іздеу ақпараттың жайылып кетуінен болған қаржылай шығындарды барынша азайтуға мүмкіндік береді.

Компьютерлік жүйелер мен ақпараттық технологиялардың дамуы КҚау жүйесін инвестициялауды оңтайландыру бойынша жұмыстардың жеке тұжырымдамасын тудырды. Зерттеудің бұл тұжырымдамасы КҚау саласындағы инвестициялаудың рационалды стратегияларын анықтау есептерінде сараптамалық жүйелерді (СЖ) [2] және ШҚЖ-ны [6] кеңінен қолдануға негізделген. Біз осы салада көптеген жұмыстарды зерттеп, осы жарияланымдардың көпшілігінде [5, 8, 12] жоғары оқу орнының КҚау жүйесін өзара қаржылай инвестициялаудың рационалды стратегиясын таңдау бойынша нақты шешімдерді қарастырмаған деген қорытындыға келдік.

Сонымен қатар, [10, 11] және [12] жұмыстарының қорытындыларында КҚау-ға инвестициялауды басқарудың рационалды стратегияларын таңдау процедураларын автоматтандыру үшін СЖ-ны және ШҚЖ-ны қолдану кезінде нақты ұсыныстар берілмеген. Бұл жағдайлар жоғары оқу орнының КҚау жүйесін өзара қаржылай инвестициялаудың рационалды стратегияларын анықтау есептерінде ШҚЖ үшін жаңа модельдерді құру қажеттілігімен байланысты міндеттің туындауына себепші болды. Осы тақырып бойынша жасалған зерттеулердегі [13, 14] авторлардың баяндаған тәжірибе мен тәсілдеріне, сондай-ақ зерттеу әдістемелері ұқсас авторлардың жұмыстарына [15, 16] сүйене отырып, осындай міндеттер класын шешуде жеткілікті тиімді тәсіл: бірнеше терминалды беті бар дифференциалдық сапа ойындары теориясының әдістерін қолдану деп айта аламыз [7]. Осылайша, осы тақырып бойынша зерттеулерге жүргізілген талдау жоғары оқу орнының КҚау жүйесін үздіксіз өзара инвестициялау есептерінде ШҚЖ үшін модельдерді одан әрі дамыту міндетінің өзектілігін растады. Бұл тұжырым инвесторлар үшін нақты ұсыныстар құру қажет болған кезде өте маңызды. Бірақ күрделі математикалық есептеулерді қолданудың қажеті жоқ, себебі есептеулердің көп бөлігі компьютерлік бағдарламалармен орындалады.

Мына жұмыстарда [9] АН-нің КҚау қатерінің моделін сипаттау үшін Петри желілерін қолдануға арналған зерттеулердің нәтижелері келтірілген. Бұл жұмыстар осы міндетінде айтарлықтай теориялық үлес қосса да, біздің ойымызша, авторлар ұсынған модельдерді, атап айтқанда АН-ді АҚ және КҚау бойынша ШҚИЖ-да және СЖ-да бағдарламалық жүзеге асыру (программалау) біршама қиынға соғады.

Мына зерттеу жұмыстарына [5-7] сүйене отырып, қатерлердің модельдерін АН-нің қорғалуын бағалау міндетін өзектендіру кезінде қатерлерді көрсетудің көрнекі кестелік формасын қолдана отырып құруға болады. Бірақ жоғарыда көрсетілгендей, бұл тәсілмен қатерлердің моделін жасау көп еңбекті қажет етеді. Сонымен қатар, қатерлер санының өсуі, әсіресе КҚау саласында жұмыс тәжірибесі аз мамандар үшін мұндай кестені құрды қиындатады.

Петри (Петри-Марков) желілері шабуылдаушының модельдерін сипаттау үшін де сәтті қолданылды [8]. Алайда, авторлар шабуылдаушының моделін түзету мүмкіндігін, атап айтқанда, оны графтар теориясының негізінде құрылған модельдермен біріктіру арқылы түзету мүмкіндігін қарастырмады, бұл нақты АН үшін киберқорғау периметрлерінен (шекарасы) шабуылдаушының еңсеру процесіндегі күйлердің ауысуын дәлірек сипаттауға мүмкіндік берер еді.

Қорытынды. Зерттеулерде [1-9] әр түрлі АН үшін АҚ жүйесінің модельдері Петри желісінде алдын ала іріктелген қарапайым операциялардың тізбегі ретінде қарастырылған, олардың ішінде кибершабуыл да болуы мүмкін. Модельдер берілген уақыт аралығында әртүрлі шабуылдардың жүзеге асу ықтималдығын есептеуге мүмкіндік береді. Алайда, [10-15] зерттеулерде қарастырылған модельдер жаңа киберқатерлерді жүзеге асыру процесінде уақытқа байланысты сипаттамаларды есептеуге мүмкіндік бермеді.

Зерттеулерде [8-16] Петри желілеріне негізделген және ақпараттық жүйелерде (АЖ) қатерлерді іске асыру процестерін сипаттайтын және модельдер ұсынылды. Бұл модельдер АН-ді қорғаудың көптеген параметрлерін атап айтқанда, қатерлердің орындалу ықтималдығын, қатерлердің орындалу уақытын бағалауға мүмкіндік бергеніне қарамастан, шабуылдаушының іс-қимылдарының реті соңына дейін толық аяқталмаған. Атап айтқанда, бұл жұмыстарда әртүрлі кластарға жататын шабуылдар барысында АЖ-ның жай- күйінің өзгеруі кезінде туындайтын қақтығыс жағдайларды шешу міндеті зерттелмеген. Бұл жағдай, біздің ойымызша, осы зерттеулердің практикада қолданылуына шектеу болады.

Осылайша, қатерлерді анықтау мен талдаудың қолданыстағы әдістерін, Петри желілерін алгоритмдеу және визуализациялау негізінде шабуылдаушылардың модельдерін толықтыру нақты АН үшін қорғалу жағдайы мен жаңа қатерлерді болжаудың тиімді құралы бола алады.

Бұл жаңа киберқатерлердің негізі қайда жатқанын және қандай салдар әкелетінін ұғуға мүмкіндік береді және болашақта әртүрлі ақпараттандыру нысандарының киберқауіпсіздігі мен АҚ қызметтерінің талдаушылары ұсынған тәсілдерді тиімді қолдануға болады.

Әдебиеттер тізімі

1. Korchenko A. Система оценивания рисков информационной безопасности / A. Korchenko, B. Akhmetov, S. Kazmirchuk, Ye. Chasnovskiy // Ukrainian Scientific Journal of Information Security. Киев. – 2017. – V. 23. Iss. 2. – P. 145-152.
2. Котенко И.В. Перспективные направления исследований в области компьютерной безопасности / И.В. Котенко, Р.М. Юсупов // Защита информации. – Киев. – 2006. – № 2. – С. 46-57.
3. Применение математического аппарата сетей Петри-Маркова для определения временных и вероятностных характеристик системы управления высоконагруженными веб-порталами с повышенной отказоустойчивостью / Р.Н. Акиншин, А.Н. Ивутин, Д.О. Есиков, И.А. Страхов // Научный Вестник. – Москва. – 2014. – № 210. – С. 85-90.
4. Atighetchi M. Adaptive Cyberdefenese for Survival and Intrusion Tolerance / M. Atighetchi // Proccedins of 3 rd International Workshop Distributed Auto- adaptive and Reconfigurable Systems. – USA. – 2003. – P. 74-84.
5. Attack directories, not caches: Side channel attacks in a non-inclusive world / R.H. Campbell, M. Yan, R. Sprabery et al // IEEE Symposium on Security and Privacy. – 2019. – P. 888-904.
6. Dawkins J. A Framework for Unified Network Security Management: Identifying and Tracking Security Threats on Converged Networks / J. Dawkins, K. Clark, G. Manes // Journal of Network and Systems Management. – 2005. – V. 13, No. 3. – P. 253-267.
7. Chris D. Data Protection Law: An Overview / D. Chris // Congressional Research Service. – 2019. – P. 1-27.
8. The mobile hub concept: Enabling applications for the internet of mobile things / M. Endler, L. Talavera, I. Vasconcelos c // IEEE International Conference on Pervasive Computing and Communication Workshops. – 2015. – P.123-128.
9. Development of decision support system based on feature matrix for cyber threat assessment / T. Kartbayev, B. Akhmetov, A. Doszhanova et al // Intl Journal of Electronics and Telecommunications. – 2019. – V.65, № 4. – P. 545-550.
10. Ахметов Б.С. Технология ситуационного управления информационной безопасностью учебного процесса казну имени аль-Фараби / Б.С. Ахметов, У.А. Тукеев // Journal of Mathematics, Mechanics and Computer Science. – Алматы. – 2009. – V. 63, №. 4. – P. 66-70.
11. Бияшев Р.Г. Применение непозиционных систем счисления при криптографической защите информации. / Р.Г. Бияшев, В.М. Амербаев, С.Е. Нысанбаева // Известия Национальной академии наук Республики Казахстан. – Алматы. – 2005. – № 3. – С. 84-89.
12. Хуторской А.В. Человек и его изменение в телекоммуникационных системах / А.В. Хуторский // Материалы Всерос. науч.-практ. конф. – Москва. – 2004. – С. 145-152.
13. Puhakainen P. Improving employees' compliance through information systems security training: an action research study / P. Puhakainen, M. Siponen // MIS Quarterly. – 2010. – Vol. 34, Issue 4. – P. 767.
14. Ortalo R. Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security / R. Ortalo, Y. Deswarte, M. Kaaniche // IEEE Transactions on Software Engineering. –1999. – V. 25. – P. 633-650.
15. Ахметов Б.С. Влияние методической системы обучения на разработку и применение средств информатизации в вузе / Б.С. Ахметов, Е.Ы. Бидайбеков, А.Г. Казмагамбетов // Международный конгресс конференций «Информационные технологии в образовании». – Москва. – 2003. – С. 112-113.
16. Ахметов Б.С. Моделирование информационной образовательной среды вуза: научное издание / Б.С. Ахметов, В.В. Яворский; М-во образования и науки РК, Карагандинский государственный технический университет. – Караганда: КарГТУ, 2006. – 251 с.

References

1. Korchenko A. Sistema otsenivaniya riskov informatsionnoi bezopasnosti / A. Korchenko, B. Akhmetov, S. Kazmirchuk, Ye. Chasnovskiy // Ukrainian Scientific Journal of Information Security. Kiev. – 2017. – V. 23. Iss. 2. – P. 145-152. (In Russian).

2. Kotenko I.V. Perspektivnye napravleniya issledovanii v oblasti komp'yuternoi bezopasnosti / I.V. Kotenko, R.M. Yusupov // Zashchita informatsii. – Kiev. – 2006. – № 2. – S. 46-57. (In Russian).
3. Primenenie matematicheskogo apparata setei Petri-Markova dlya opredeleniya vremennykh i veroyatnostnykh kharakteristik sistemy upravleniya vysokonagruzhennymi veb-portalami s povyshennoi otkazoustoichivost'yu / R.N. Akinshin, A.N. Ivutin, D.O. Esikov, I.A. Strakhov // Nauchnyi Vestnik. – Moskva. – 2014. – № 210. – S. 85-90. (In Russian).
4. Atighetchi M. Adaptive Cyberdefenese for Survival and Intrusion Tolerance / M. Atighetchi // Proccedins of 3 rd International Workshop Distributed Auto- adaptive and Reconfigurable Systems. – USA. – 2003. – P. 74-84. (In English).
5. Attack directories, not caches: Side channel attacks in a non-inclusive world / R.H. Campbell, M. Yan, R. Sprabery et al // IEEE Symposium on Security and Privacy. – 2019. – P. 888-904. (In English).
6. Dawkins J. A Framework for Unified Network Security Management: Identifying and Tracking Security Threats on Converged Networks / J. Dawkins, K. Clark, G. Manes // Journal of Network and Systems Management. – 2005. – V. 13, No. 3. – P. 253-267. (In English).
7. Chris D. Data Protection Law: An Overview / D. Chris // Congressional Research Service. – 2019. – P. 1-27. (In English).
8. The mobile hub concept: Enabling applications for the internet of mobile things / M. Endler, L. Talavera, I. Vasconcelos s // IEEE International Conference on Pervasive Computing and Communication Workshops. – 2015. – P. 123-128. (In English).
9. Development of decision support system based on feature matrix for cyber threat assessment / T. Kartbayev, B. Akhmetov, A. Doszhanova et al // Intl Journal of Electronics and Telecommunications. – 2019. – V.65, № 4. – P. 545-550. (In English).
10. Akhmetov B.S. Tekhnologiya situatsionnogo upravleniya informatsionnoi bezopasnost'yu uchebnogo protsessa kaznu imeni al'-Farabi / B.S. Akhmetov, U.A. Tukeev // Journal of Mathematics, Mechanics and Computer Science. – Almaty. – 2009. – V. 63, №. 4. – P. 66-70. (In Russian).
11. Biyashev R.G. Primenenie nepozitsionnykh sistem schisleniya pri kriptograficheskoi zashchite informatsii. / R.G. Biyashev, V.M. Amerbaev, S.E. Nysanbaeva // Izvestiya Natsional'noi akademii nauk Respubliki Kazakhstan. – Almaty. – 2005. – № 3. – S. 84-89. (In Russian).
12. Khutorskoi A.V. Chelovek i ego izmenenie v telekommunikatsionnykh sistemakh / A.V. Khutorskii // Materialy Vseros. nauch.-prakt. konf. – Moskva. – 2004. – S. 145-152. (In Russian).
13. Puhakainen P. Improving employees' compliance through information systems security training: an action research study / P. Puhakainen, M. Siponen // MIS Quarterly. – 2010. – Vol. 34, Issue 4. – P. 767. (In English).
14. Ortalo R. Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security / R. Ortalo, Y. Deswarte, M. Kaaniche // IEEE Transactions on Software Engineering. –1999. – V. 25. – P. 633-650. (In English).
15. Akhmetov B.S. Vliyanie metodicheskoi sistemy obucheniya na razrabotku i primenenie sredstv informatizatsii v vuze / B.S. Akhmetov, E.Y. Bidaibekov, A.G. Kazmagambetov // Mezhdunarodnyi kongress konferentsii «Informatsionnye tekhnologii v obrazovanil». – Moskva. – 2003. – S. 112-113. (In Russian).
16. Akhmetov B.S. Modelirovanie informatsionnoi obrazovatel'noi sredy vuza: nauchnoe izdanie / B.S. Akhmetov, V.V. Yavorskii; M-vo obrazovaniya i nauki RK, Karagandinskii gosudarstvennyi tekhnicheskii universitet. – Karaganda: KaRGTU, 2006. – 251 s. (In Russian).

Б.С. Ахметов[1], В.А. Лахно[2], Л.М. Кыдыралина[3*]
[1]Казахский национальный педагогический университет имени Абая,
050010, Республика Казахстан, город Алматы, проспект Достык, 13
[2]Национальный университет биоресурсов и природопользования,
030414, Украина, г. Киев, ул. Героев Обороны, 15
[3]Университет имени Шакарима города Семей,
071412, Республика Казахстан, г. Семей, ул. Глинки, 20 А, *e-mail: lazat_75@mail.ru

ОБЗОР И АНАЛИЗ ПРЕДЫДУЩИХ ИССЛЕДОВАНИЙ В ОБЛАСТИ КИБЕРЗАЩИТЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА УЧЕБНЫХ ЗАВЕДЕНИЙ

В статье рассмотрены предпосылки формирования безопасной информационной образовательной среды современного вуза. Проанализированы публикации

отечественных и ведущих зарубежных исследований. Проведен обзор и анализ предыдущих исследований в области киберзащиты информационного пространства учебных заведений. Проведен анализ опубликованных публикаций по данной теме. Проведенный анализ подтвердил актуальность проблемы дальнейшего развития моделей для ВКС в задачах непрерывного взаимного инвестирования системы КС вузов. Проведен анализ публикаций по результатам исследований по использованию сетей Петри для описания модели угроз угроз объектов информатизации. Хотя эти работы вносят значительный теоретический вклад в эту задачу, на наш взгляд, программная реализация предложенных авторами моделей, в частности АН, в ВКИП и СС по ИБ и КБ, несколько затруднена. Это, в свою очередь, требует дополнительных исследований.

Ключевые слова: *кибербезопасность, информационная образовательная среда вуза, моделирование, сеть Петри, защита информации, электронная информационная образовательная среда вуза, метод, модель.*

B.S. Akhmetov[1], V.A. Lakhno[2], L.M. Kydyralina[3*]
[1]Abai atyndagi Kazakh ulttyk pedagogicalyk University,
050010, Republic of Kazakhstan, Almaty city, 13 Dostyk Avenue
[2]Bioresourstar zhane tabigatty paidalan ulttyk University,
030414, Ukraine, Kiev, Geroyev Oborona str., 15
[3]Shakarim University of Semey,
071412, Republic of Kazakhstan, Semey, Glinka str., 20 A
[*]e-mail: lazat_75@mail.ru

REVIEW AND ANALYSIS OF PREVIOUS RESEARCH IN THE FIELD OF CYBER PROTECTION OF THE INFORMATION SPACE OF EDUCATIONAL INSTITUTIONS

The article considers the prerequisites for the formation of a secure information and educational environment of a modern university. Publications of domestic and leading foreign studies were analyzed. An overview and analysis of previous research in the field of cybersecurity of the information space of educational institutions was carried out. The analysis of publications published on this topic was carried out. The analysis confirmed the relevance of the problem of further development of models for VHS in the tasks of continuous mutual investment of the system of higher education institutions. Analysis of publications based on the results of research on the use of Petri nets to describe the model of cyber threats of informatization objects was carried out. Although these works make a significant theoretical contribution to this task, in our opinion, the programmatic implementation of the models proposed by the authors, in particular, The an in the ICIS and ICS on ICS, is somewhat difficult. This, in turn, requires additional research.

Key words: *cybersecurity, University information and educational environment, modeling, Petri nets, information security, electronic information and educational environment of universities, method, model.*

Авторлар туралы мәліметтер

Бахытжан Сражатдинович Ахметов – Абай атындағы Қазақ ұлттық педагогикалық университеті, техника ғылымдарының докторы, профессор, Алматы қ., Казақстан, e-mail: b_akhmetov@ntu.kz. ORCID: https://orcid.org/0000-0001-5622-2233.

Валерий Анатольевич Лахно – Биоресурстар және табиғатты пайдалану ұлттық университеті, техника ғылымдарының докторы, профессор, Киев қ., Украина. ORCID: https://orcid.org/0000-0001-9695-4543.

Лазат Муктаровна Кыдыралина* – Семей қаласының Шәкәрім атындағы университеті КеАҚ, PhD, Семей қ. Қазақстан, e-mail: lazat_75@mail.ru. ORCID: https://orcid.org/0000-0002-2836-0919.

Сведения об авторах

Бахытжан Сражатдинович Ахметов – Казахский национальный педагогический университет имени Абая, доктора технических наук, профессор, г. Алматы, Казахстан, e-mail: b_akhmetov@ntu.kz. ORCID: https://orcid.org/0000-0001-5622-2233.

Валерий Анатольевич Лахно – Национальный университет биоресурсов и природопользования, доктор технических наук, профессор, Г. Киев, Украина. ORCID: https://orcid.org/0000-0001-9695-4543.

Лазат Муктаровна Кыдыралина* – Университет имени Шакарима г. Семей, PhD, г. Семей Казахстан, e-mail: lazat_75@mail.ru. ORCID: https://orcid.org/0000-0002-2836-0919.

Information about the authors

Bakhytzhan Bogatdinovich Akhmetov – Kazakh National Pedagogical University named after Abai, Doctor of Technical Sciences, Professor, Almaty, Kazakhstan, e-mail: b_akhmetov@ntu.kz. ORCID: https://orcid.org/0000-0001-5622-2233.

Valery Anatolyevich Lakhno – National University of Bioresources and Environmental Management, Doctor of Technical Sciences, Professor, Kiev, Ukraine. ORCID: https://orcid.org/0000-0001-9695-4543.

Lazat Muktarovna Kydyralina – Shakarim University, PhD, Semey K. Kazakhstan, e-mail: lazat_75@mail.ru. ORCID: https://orcid.org/0000-0002-2836-0919.

Редакцияға енуі 01.03.2024
Өңдеуден кейін түсуі 03.03.2024
Жариялауға қабылданды 05.03.2024

DOI: 10.53360/2788-7995-2024-1(13)-5

МРНТИ: 50.43.15

А.П. Смирнов, Е.С. Риттер*, А.А. Савостин, Д.В. Риттер, С.С. Молдахметов
Северо-Казахстанский университет имени Манаша Козыбаева,
150000, Казахстан, Петропавловск, ул. Пушкина, 86
*e-mail: esritter@ku.edu.kz

МОДЕЛИРОВАНИЕ ПОТЕНЦИОМЕТРИЧЕСКОГО ДАТЧИКА УРОВНЯ И ОЦЕНКА ПОГРЕШНОСТИ

Аннотация: *В данной статье рассматрен принцип работы потенциометрического уровнемера для измерения уровня электропроводной жидкости в резервуаре. Электропроводная жидкость измеряется уровнемером косвенным методом в заземленном резервуаре. Устройство состоит из сенсора с низким электрическим сопротивлением, генератора переменного тока, металлической стенки резервуара и усилителя слабого сигнала.*

Нелинейность передаточной функции не позволяет использовать измеренные значения сенсора без предварительной линеаризации. Поэтому необходимо разработать модель сенсора в электропроводной жидкости и выявить факторы, влияющие на точность измерения уровня.

Для оценки точности измерений в статье представлена модель электрического поля внутри электролита, создаваемого сенсором потенциометрического уровнемера в резервуаре с цилиндрической стенкой. Использованы численные методы, основанные на методе конечных элементов, для расчета потенциалов и токов внутри электролита. Модель конечного элемента и конечно-элементная сетка позволили рассмотреть передачу потенциалов между конечными элементами.

Показано, что погрешность измерения уровня в потенциометрическом уровнемере имеет недопустимую величину и зависит от уровня жидкости и от расположения измерителя уровня.

На основе полученной модели были определены факторы, влияющие на измеренное значение уровня жидкости, и выполнено вычисление абсолютной и относительной погрешностей измерения. Так же определены дальнейшие шаги по улучшению точности измерения уровнемера.