4. С.Чугунов, «Врачевание травами и минералами. Тайны тибетской медицины» – Москва: Пищепромиздат, 2001. – 528 с.
5. Репчатый лук: польза и вред. Блог «Elementaree», 2013-2018 г. (Электронный ресурс). URL: //https://elementaree.ru/blog/science/repchatyj-luk-polza-i-vred// (дата обращения: 23.04.2020 г.)
6. Паприка. Энциклопедия полезной еды «Вкуснро», 2010-2020 г. (Электронный ресурс). URL: // http://vkusnoblog.net/products/paprika// (дата обращения: 14.02.2020 г.)
7. Орегано. Энциклопедия «Едим дома», 2003-2020 г. (Электронный ресурс). URL: // https://www.edimdoma.ru/encyclopedia/ingredients/2118-oregano// (дата обращения: 15.05.2020 г.)

ПРОТЕИНДІ ӨНІМДІ ӨНДІРУ ТЕХНОЛОГИЯСЫ

Г.Н. Нурымхан, М.Д. Толеубекова, А.К. Игенбаев, Б.М. Кулуштаева

Мақалада сүт сарысуы қосылған сиыр етінен жасалған шалаөнімнің технологиясы қарастырылады. Ет – жоғары ақуыздарға, майларға, экстрактивті заттарға, маңызды аминқышқылдарына бай, ең маңызды тағамдардың бірі. Тамақ өнеркәсібі үшін қуырусыз, еттің байлық пайдалы қасиеттері ғана емес, срнымен қатар органолептикалық, физика-химиялық сапа көрсеткіштері, технологиялық қасиеттері сақталатын, өнімнің жаңа түрін жасап шығару өте маңызды. Ғылыми-теориялық зерттеулер негізінде сүт сарысуы қосылған сиыр етінен жасалған шалаөнімнің технологиясы жасалды. Витаминді және минералды құрамын түзейтін тағамдық компанентер таңдалды. Нәтижесі – сапалы және органолептикалық тұрғыдан теңгерілген өнім Өнім физика-химиялық, органолептикалық көрсеткіштерге зерттеліп, дайын өнімнің тағамдық қауіпсіздігі анықталды. Сүт сарысуы қосылған сиыр етінен жасалған шалаөнім – дәстүрлі тұздықта жасалған кебептен жақсы балама, өйткені олар тек пайдалы және экологиялық қауіпсіз өнім болып табылады.

Түйін сөздер: *сиыр етінен жасалған шалаөнім, маринад, сүт сарысуы, химиялық құрамы, қауіпсіздік.*

PROTEIN PRODUCTION TECHNOLOGY

G. Nurumkhan, M. Toleubekova, A. Igenbayev, B. Kulushtayeva

This article discusses the technology of production of semi-finished products from beef meat in marinade with the addition of whey. Meat is one of the most important food products, which is rich in high-grade proteins, fats, extractives, and essential amino acids. It is important for the food industry to develop and obtain a new type of product that not only preserves all the useful properties of meat, but also improves organoleptic, physical and chemical quality indicators, and technological properties. Based on scientific and theoretical research, a new semi-finished product of beef meat in marinade with the addition of whey has been developed. Selected components that correct the vitamin and mineral composition. The result is a balanced product in the qualitative and organoleptic sense. The product was tested for physical, chemical, and organoleptic parameters, and the food safety of the finished product was determined. Semi-finished meat in a marinade of whey is a good alternative to shish kebab in a traditional marinade, since it contains useful substances and is an environmentally safe product.

Key words: *semi-finished beef meat, marinade, chemical composition, safety.*

МРНТИ: 81.93.29

Б.А. Әділбай[1], А.А. Досжанова[1], В.А.Лахно[2], А.К. Шайханова[3]
[1]Алматы Энергетика және Байланыс Университеті
[2] Национальный университет биоресурсов и природопользования, г. Киев, Украина
[3]Семей қаласының Шәкәрім атындағы университеті

КИБЕРҚАУІПСІЗДІК МІНДЕТТЕРІНДЕГІ САРАПТАМАЛЫҚ ЖҮЙЕЛЕР ҮШІН БІЛІМ БАЗАСЫН ӘЗІРЛЕУ

Аңдатпа: *Қазіргі уақытта желілік мүмкіндіктер мен технологияларды пайдалану мемлекеттің саясаты мен қауіпсіздігі үшін айқын бол түсуде. Егер әлемде бүгінгі күні кәдімгі қару-жарақ пен жаппай қырып-жою қаруы саласындағы стратегиялық теңгерім сақталып жатса, киберкеңістіктегі тепе-теңдік мәселесі ашық болып қала беруде, ал егер ашығын айтсақ, бұл мәселеде тепе-теңдік жоқ десек те болады.*

Мақала өздігінен үйренуге қабілетті алаптивті сараптама жүйесін құру негізінде компьютерлік жүйелердегі аномалиялар мен киберқауіптерді зияткерлік айырып тану жүйелерінің тиімділігін арттыру тақырыбына арналған. Киберқауіпсіздік мәселелерінде сараптамалық жүйе үшін білім базасын қалыптастырудың өзірленген алгоритмі қауіптер, аномалиялар мен

кибершабуылдар белгілерін кластерлеудің белгілі статистикалық және қашықтық параметрлерін ескереді. Киберқауіпсіздік міндеттеріндегі сараптамалық жүйелер үшін білім базасын қалыптастыру міндетін шешу үшін бағдарламалық модульдердің сипаттамасы ұсынылған.

Түйін сөздер: *киберқауіпсіздік, қауіптерді айырып тану, білім базасы, сараптамалық жүйе, шешімді қолдау, білім базасын қалыптастыру алгоритмі.*

Кіріспе. Интернет желісін пайдаланушылардың саны және олардың өсу динамикасы секілді көрсеткіштерді ғана емес, сонымен қатар ортақ пайдалану желілерінің адам өмірінің басқа салаларына біртіндеп еніп жатқанын ескерсек, қазіргі қоғам өмірі үшін киберкеңістіктің маңыздылығы айқын білінеді.

Бұған дәлел ретінде әртүрлі әлеуметтік-саяси, экономикалық, ақпараттық және әскери мақсаттарға қол жеткізу мақсатында киберкеңістікті пайдалануға бағытталған жекелеген мемлекеттердің арнайы бөлімшелерінің, қоғамдық және террористік ұйымдардың белсенділігін атап өтуге болады.

Киберқауіпсіздік туралы сөз қозғалғанда, дәстүрлі түрде ақпараттық-коммуникациялық технологиялар дамуының қазіргі жай-күйіне және оларды күнделікті өмірге енгізу деңгейіне тән жаңа, ерекше қауіптерге назар аударылады. Сол себепті ұғымға анықтама беру, нормативтік-құқықтық құжаттардағы, атап айтқанда сондай қауіптерді айырып тануға арналған бағдарламалық өнімдерді (файрволдар, антивирустар, сараптамалық жүйелер, киберқауіпсіздік мәселелерінде шешімдер қабылдауды қолдау жүйелері және т.б.) әзірлеу процестерін регламенттейтін құжатардағы тиісті топтастыру мен заңдастыру өзекті міндет болып табылады. Осы себепті осы бөлімнің мақсаты киберқауіпсіздік жіктелімін және олардың нормативтік-құқықтық құжаттарда заңдастырылуын зерттеуді көздейді.

Алдыңғы зерттеулерге шолу. Кибернетикалық қауіпсіздік мәселесі көптеген ғалымдардың зерттеу тақырыбына айналып үлгерді [1-4].

Кибершабуылдарды анықтаудың қазіргі заманғы жүйелері мен технологияларының жұмыс істеу тиімділігі елеулі дәрежеде ақпараттық ресурстарға шабуылдарды іске асырудың алдыңғы сатыларындағы киберқылмыскерлердің белсенділігі туралы мониторингтік ақпараттың жеделдігі мен шынайылығынан тәуелді, және аса маңызды болып табылады. Әлемдік тәжірибеге жүргізілген талдау көрсеткендей, қазіргі уақытта кибершабуылдарды іске асырудың бастапқы сатыларында оларды айырып танудың иерархиялық көп деңгейлі құрылымдарын қалыптастыру кибершабуылдардың инновациялық зияткерлік мониторингтік жүйелерін құрудың ең тиімді әдіснамалық тәсілдемесі болып табылады. Бұл ретте иерархиялық тәсілдеме таратылған сыни тұрғыда маңызды ақпараттық жүйелерде ақпаратты кибершабуылдан қорғау процесін басқарудың күрделі міндеттерін бір-бірімен үйлестірілген локальді міндеттердің тізбегі ретінде шешуге мүмкіндік береді [1].

Ақпараттық технологияларды қоғамның тіршілік әрекетінің барлық салаларына қарқынды түрде енгізу, ақпараттық қатынастардың жаһандануы әлемдік қоғамдастықта да сыни инфрақұрылым объектілерінің кибернетикалық қауіпсіздігінің жай-күйіне алаңдаушылық тудырды.

Жаппай сипатқа ие кибершабуылдар арнайы техникалық шешімдерді, қарсы іс-қимыл құралдары мен жүйелерін құруға бастамашылық етеді. Желілік басып кіруді анықтау үшін киберқауіптердің жаңа немесе модификацияланған түрлері пайда болған кезде тиімді болып қала бере алатын заманауи әдістер [1-12], модельдер [5], құралдар [4, 6], бағдарламалық қамтамасыз етулер [7] және басып кіруді анықтау және олардң алдын алу жүйелеріне арналған кешенді техникалық шешімдер [8] қолданылады. Бірақ іс жүзінде анықталмаған немесе нақты айқындалмаған қасиеттерге ие шабуылдаушы әрекеттерден туындаған жаңа қауіп-қатерлер мен аномалиялар пайда болған кезде көрсетілген құралдар әрқашан тиімді болып қала бермейді және олардың тиісті адаптациясы үшін ұзақ уақыт ресурстарын талап етеді. Осы себепті, басып кіруді айқындау жүйелері олардың тиімді жұмыс істеуіндегі үздіксіздікті қамтамасыз ету үшін үнемі зерттелуі және жетілдірілуі тиіс.

Мақаланың негізгі материалы

Ақпараттық қауіпсіздік жүйесін ұйымдастыру бүгінгі таңда ақпараттық жүйелері аса маңызды жүйелердің немесе белгілі бір компьютерлік жүйелердің анықтамасына сәйкес келетін көптеген компаниялар мен кәсіпорындар үшін дамудың маңызды стратегиялық факторына айналуда [2]. Ал компьютерлік жүйелерді ақпараттандырудың аса маңызды объектілерінің басым бөлігінің архитектурасының күрделілігі компьютерлік жүйелердің ақпараттық қауіпсіздігі мен киберқауіпсіздік (бұдан әрі, сәйкесінше, ақпараттық қауіпсіздік)

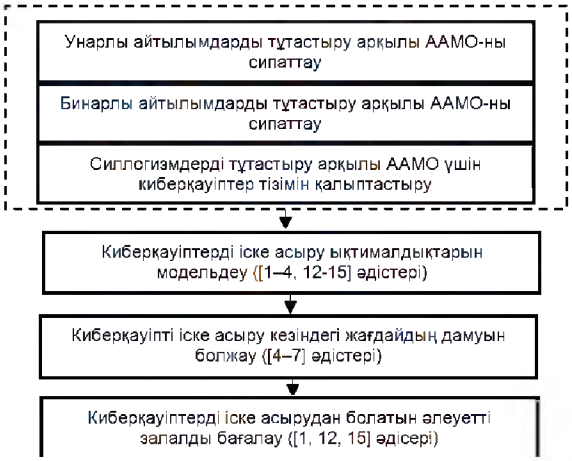
үшін қауіп-қатерлер мен тәуекелдерді әдеттегі сараптамалық бағалаудың нәтижелілігі мен шынайылығын төмендететіндіктен, көптеген мамандардың пікірінше [3, 4], бұл міндетті шешу үшін шешім қабылдауды қолдаудың интеллектуализацияланған жүйелерінің немесе сараптамалық жүйелердің әлеуетін пайдаланған абзал [5]. Мұндай шешім қабылдауды қолдау жүйесі және шұғыл жүйе, оларды қолдану тәжірибесі көрсеткендей [6, 7], әсіресе қауіп-қатерлер мен кибершабуылдардың әлсіз құрылымдалған белгілері туралы сөз қозғалғанда, ағымдағы киберқауіпсіздік пен осалдықтарды бағалаумен байланысты рутинді міндеттерді жеткілікті дәрежеде өзіне қабылдауға қабілетті, бұл жайт ақпараттық қауіпсіздік қызметтерінің персоналына түсетін жүктемені жеңілдетуге мүмкіндік береді, оларға корпоративтік ақпараттық жүйелердің, оның ішінде белгілі бір компьютерлік жүйелердің орнықты және тұрақты жұмыс істеуін қамтамасыз ету бойынша басымдыққа ие міндеттерге ден қоюға мүмкіндік береді.

Жоғарыда айтылған мән-жайлар нәтижелері осы жұмыста келтірілген зерттеу тақырыбы өзекті тақырып болып табылады деп тұжырымдауға мүмкіндік береді.

Еңбектерде компьютерлік жүйелер үшін ақпаратты қорғаудың сенімді жүйесін құру көп жағдайда дұрыс айырып танудан және ақпараттық қауіпсіздік қауіп-қатерлерін кейіннен бағалаудан [8, 9], кейіннен ақпараттық қауіпсіздік тұрғысынан басымдығы жоғырларын өзектендіруден тәуелді болады. Бұл ретте [9-11]-де көрсетілгендей, киберқауіптерді іске асыру мүмкіндігін анықтау міндеті компьютерлік жүйенің ақпараттық қауіпсіздігі мен киберқауіпсіздігіне арналған тәуекелдерді бағалау процесінде басым бағыт болып табылады. Алайда, бұл ретте атап өтетін жайт, жоғарыда қарастырылған еңбектердің басым бөлігінде [9-14] қауіп іске асырылған жағдайдағы оқиғаның дамуын болжамды бағалауға арналған модельдер қамтылмайды. Бұған қоса, талдау жүргізілген дереккөздерде [2, 4, 7, 10, 11] сарапшылардың мазмұны бойынша бірдей немесе бір-біріне жақын пікірлерді қате енгізу мүмкіндігі аз қарастырылады. Атап айтқанда, әр түрлі маманданудағы сараптау топтарымен тұжырымдалған бірнеше пікірді біріктіру кезінде. Сондай-ақ, әртүрлі тұжырымдамалармен бір жағдай (мақсат) сипатталатын кездер де болуы мүмкін [12]. Білімнің осы ерекшеліктерін есепке алу үшін компьютерлік жүйенің ақпараттық қауіпсіздігі пен киберқауіпсіздігі үшін қауіп-қатер рәсімі барысында шешім қабылдауды қолдау жүйелерінің білім базасы объектілерін мазмұнды сәйкестендіру әдісін пайдалану ұсынылады [12].

Киберқауіптерді және компьютерлік жүйелердің ақпараттық қауіпсіздігіне төнетін тәуекелдерді бағалау міндеттерінде сараптамалық жүйені жобалау кезінде аналитиктер тарапынан ақпараттық қауіпсіздік аудиті кезінде қойылатын типтік сұрақтардан тұратын сауалнамалардың немесе термесауал парақтарының қалыптастырылуы табиғи кезеңдердің бірі болып табылады. Мысалы, мұндай сауалдарға мыналарды жатқызуға болады – инциденттер орын алды ма, ұйымның немесе компанияның құпия ақпараты бар ма және т.с.с. [8, 10]. Бұдан әрі ақпараттық қауіпсіздік жөніндегі сарапшы немесе аналитик унарлы және/немесе бинарлы айтылымдарды қалыптастырады. Мұндай айтылымдар сориттерді, яғни тізбекті силлогизмдер тізбегін құруға мүмкіндік береді. Ақпараттық қауіпсіздік міндеттерінде сараптамалық жүйелер үшін білім базасын жобалау контексінде, силлогизм – бұл атрибутивтік айтылымдардан тұратын екі сілтемелі ойтұжырым. Бұдан әрі предикаттарды есептеу аппараты мен семантикалық желілерді пайдалана отырып, нақты сыни жүйенің өзекті киберқауіптеріне арналған модельдерді қалыптастыруға болады. Жалпы алғанда компьютерлік жүйелерге арналған киберқауіптер тізбесін қалыптастыру алгоритмінің негізгі кезеңдерін 1-суретте көрсетілген схема түрінде ұсынуға болады. Білім базасын жобалау кезінде келесідей базалық унарлы айтылымдар қолданылды (магистрлік жұмыс шеңберінде ішінара келтірілуде): 0 – зиянды бағдарламалық қамтамасыз етуді орындау; 1 – USB кірістерін пайдалану; 2 – иілгіш дискілерді пайдалану; 3 – интернетке шығудың болуы; 4 – жергілікті есептеуіш желіге шығудың болуы; 5 – CD/DVD болуы; 6 – антивирустар мен сигнатуралар жаңартылуының болмауы; 7 – кешенді АҚ жүйесінің болмауы; 8 – антивирустің болмауы; 9 – ақпараттық қауіпсіздік және киберқауіпсіздік үшін жауапты адамға арналған нұсқаулықтардың болмауы; 10 – әкімшіге арналған нұсқаулықтарда ақпараттық қауіпсіздіктің жоқтығы; 11 - ақпаратты қорғаудың технологиялық процестерінің болмауы; 12 – ақпаратты антивирустік қорғау құралдары үшін нұсқаулықтардың болмауы; 13 – ақпаратты қорғау құралдарын орнату жөніндегі актінің болмауы; 14 – қолжетімділік кілттері мен атрибуттарының жылыстауы; 15 – резервтік көшірме файлының болмауы; 16 - пайдаланушының нұсқаулығында элементтердің болмауы; 17 – ақпаратты тарату фактісі; 18

– қызметкерлердің ақпаратты жариялamайтыны туралы шарттың болмауы; 19 – локальді есептеуіш ортаға вирусты бағдарламалық қамтамасыз етуді жұқтыру қаупі ; 20 – локальді есептеуіш желілерде парольдерді қармау қаупі; 21 – файрволдың жоқтығы; 22 – 100 және басқасы, резервті қоса алғанда.



Сурет 1 – Компьютерлік жүйелердің ақпараттық қауіпсіздігінің қауіп-қатерлері мен тәуекелдерін бағалау алгоритмдерінің өзара әрекеттесуінің жалпы схемасы

Бұл тәсілдемені желілік қауіпсіздік саласындағы бастапқы айтылымдарға сүйенетін тізбекті силлогизмдер тізбегін құру мысалында қарастыралық.

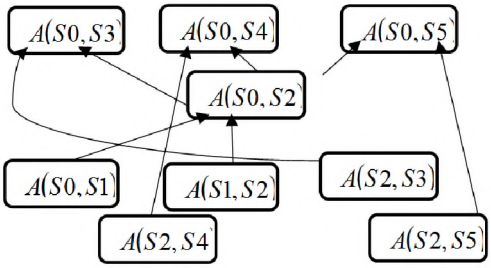
Ақпараттандыру объектісінің сипаттамаларын сипаттайтын қарапайым унарлы айтылымдарды құралық: 1) $S0-$ компьютерлік жүйелерге талдау жүргіземіз; 2) $S1-$ компьютерлік жүйелер интернетке қосылуды пайдаланады; 3) $S2-$ компьютерлік жүйелерге хакерлік шабуылдар қаупі төніп тұрған жоқ; 4) $S3-$ компьютерлік жүйелерге ақпаратты жымқыру қаупі төніп тұр; 5) $S4-$ компьютерлік жүйе ақпаратты жоюға байланысты қауіптерге бейім; 6) $S5-$ компьютерлік жүйе зиянды бағдарламалық қамтамасыз етуді жұқтыруға байланысты қауіптерге бейім.

Компьютерлік жүйенің осалдығын сипаттайтын бинарлы айтылымдарды құралық. Бинарлы айтылымдар унарлы айтылымдар негізінде жасалған, бұл ретте де кванторлар логикасы қолданылды, 2-суретті қараңыз: $A,S0,S1-$ талдау жүргізілетін компьютерлік жүйе – бұл интернетке қосылуды пайдаланатын компьютерлік жүйе. Немесе: $A,S1,S2-$ интернетке қосылуды пайдаланатын кез келген компьютерлік жүйе – бұл хакерлік шабуылдардың қаупін құрайтын компьютерлік жүйе; $A,S2,S3-$ хакерлік шабуылдардың қаупін құрайтын компьютерлік жүйе – бұл ақпаратты жымқыру қаупін құрайтын компьютерлік жүйе; $A,S2,S4-$ хакерлік шабуылдардың қаупін құрайтын компьютерлік жүйе – бұл ақпаратты жою қаупін құрайтын компьютерлік жүйелер; $A,S2,S5-$ хакерлік шабуылдарға бейім компьютерлік жүйелер – бұл зиянды бағдарламалық қамтамасыз етуді жұқтыру қаупіне бейім компьютерлік жүйелер.

Осылайша, бинарлы айтылымдар – бұл тиісті кванторларды қамтитын силлогизм жіберулерінің бірі. Силлогизмдерді түрлі комбинацияларда үйлестіруге болады. Әрбір осындай үйлесім жаңа қорытынды алуға мүмкіндік береді. Ұқсас жолмен алынған қорытындыларды өзара үйлестіруге болады. Мұндай операцияларды талдау объектісінің өзгермелі күшті қасиеттерінен (немесе силлогизмдер терминдерінде модустер) әлсіздеріне өту жаңа тұжырымды синтездеу процесін үзген сәтке дейін жалғастыруға болады.

Осылайша, 2-суретте көрсетілген мысал айқын тұжырымды жасауға мүмкіндік береді. Егер силлогизмдер арасындағы байланыстарды синтездеу процесі автоматтандырылса, онда сараптамалық жүйелердің көмегімен компьютерлік жүйеге төнетін қауіптер тізімін анықтап қана қоймай, оларды ағымдағы уақыт кезеңі үшін өзектендіруге болады. Ал шығысында өзекті қауіптер тізімін ала отырып, басқа авторлардың қолда бар модельдерін [1-4, 14], немесе біздің алдыңғы зерттеулеріміздің нәтижелерін [1-4, 5-7, 13] қолдану негізінде

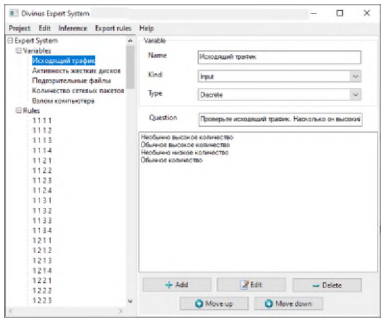
нақты компьютерлік жүйе үшін киберқауіптерді іске асыру мүмкіндігін анықтауға кірісе аламыз [14].



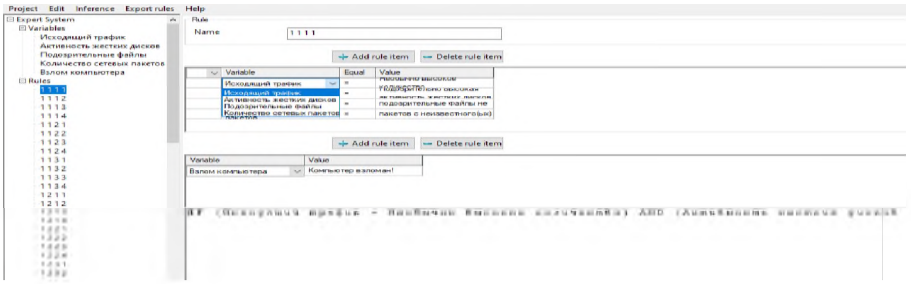
Сурет 2 – Сараптамалық жүйедегі бинарлы айтылымдардың мысалы

Атап өтетін жайт, 2-суретте келтірілген білімді беру моделінде семантикалық метрика қолданылмайды және компьютерлік жүйенің ақпараттық қауіпсіздігі мен киберқауіпсіздігіне қатысты жаңа қауіптерге байланысты білімнің ішкі интерпретациялануы әрдайым ескеріле бермейді. Білімнің осы ерекшеліктерін есепке алу үшін шұғыл жүйелердің білім базасы объектілерін мазмұндық сәйкестендіру әдісін пайдалану ұсынылады.

Жүйенің жұмысы бірнеше модульді кешенді пайдалану түрінде ұйымдастырылған, бұл модульдердің әрқайсысы компьютерлік жүйенің киберқауіпсіздігін бағалауға арналған тәуелсіз бағдарламалық өнімдер ретінде пайдаланылуы мүмкін, 3, 4 суреттер



Сурет 3 – Айнымалылар редакторы



Сурет 4 – Қағидалар редакторы

Деректер базасын өңдеу интуитивті түсінікті интерфейсте ұйымдастырылған, онда нақты міндет үшін қағидаларды қосуға немесе өңдеуге болады.

Сарапшы немесе компьютерлік жүйенің қауіп-қатерлері туралы шешім қабылдайтын адам диалогтық формада тиісті тармақтарды таңдау арқылы адаптивті сараптамалық жүйемен автоматты түрде қалыптасатын сұрақтар үшін жауап нұсқаларын таңдай алады.

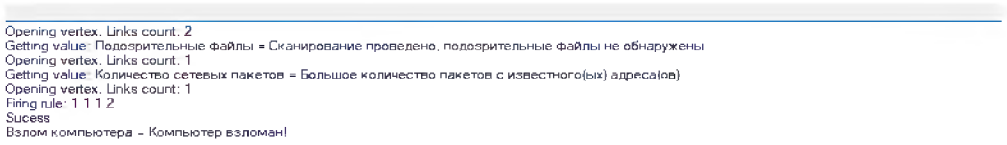
Қажеттілігіне қарай адаптивті сараптамалық жүйелердің білім базасын компьютерлік жүйе үшін жаңа киберқауіптерді бағалау тәжірибесіне ие ең білікті сарапшыларды тарта отырып, автоматты түрде кеңейтуге болады.

Адаптивті сараптамалық жүйелердің басты модулінің жұмысы нәтижесінде сарапшымен таңдалған нұсқалар үшін шешім графы (бағдарламалар терезесінің жоғарғы бөлігі, 5-сурет) автоматты түрде қалыптасады. Ал терезенің төменгі бөлігінде шешім қабылдайтын адам адаптивті сараптамалық жүйемен генерацияланатын тұжырыммен таныса алады.

Сурет 5 – Шешім графы және сарапшының жауаптарын өңдеу барысында адаптивті сараптамалық жүйемен генерацияланған тұжырым

Осылайша, мысалы, адаптивті сараптамалық жүйелердің компьютерлік жүйесіндегі жағдайды бағалау барысында туындаған жағдай үшін шешім берілді, бұл шешімге сәйкес «Компьютерлік жүйе құрамындағы компьютер бұзылу ықтималдығы жоғары, 6-суретті қараңыз.

Шын мәнінде, алынған графтар шешімді негізді түрде шығаруға мүмкіндік береді.



Сурет 6 – Тұжырым мысалы

Себеп-салдарлық байланыстардың онтологиясы немесе шешу графтары нақты ҚЖ үшін киберқауіптерді бағалауды дамыту процесінде орын алатын тәуелділіктер туралы білімнің өзгермейтін бөлігі (жобаланатын жүйенің өмірлік циклінің бөлігі) болып келеді. Модельдердің барлық себеп-салдарлық байланыстары үшін білім құрылымы көп жағдайда ұқсас келеді. Білім базасында тілдің синтаксисі және семантикасы қолданылады, олардың формалды мысалдары төменде келтірілген:

Тұжырымдар. Киберқауіпсіздік мәселелерінде пайдаланылатын адаптивті сараптамалық жүйелер модульдерінің құрамдас бөлігі болып табылатын бағдарламалық өнім модулі сипатталған және ол пайдаланушының қызметін мониторингілеу және жүйелік қауіптер ретінде жіктеуге болатын әлеуетті инсайдер арқылы құпия ақпараттың жылыстауына байланысты қауіптерді айқындау үшін тағайындалған.

Әдебиеттер

1. Выпасняк В.И., Тиханычев О.В., Гахов В.Р. Кибер-угрозы автоматизированным системам управления //Вестник Академии военных наук. – 2013. – №. 1. – С. 103-109.
2. Евдокимов К.Н., Саганов П.Н. Актуальные вопросы взаимодействия органов государственной власти, органов местного самоуправления и общественных объединенийв обеспечении национальной безопасности россии от современных киберугроз //Проблемы организации органов государственной власти и местного самоуправления: история, теория, практика и перспективы. – 2015. – С. 75-81.
3. Невская Н.А. Цифровая безопасность экономики великобритании: опыт регулирования и эффективность применения //ЦИТИСЭ. – 2019. – №. 1. – С. 28-28.
4. Ковалев А.А., Балашов А.И. Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока //Вестник Поволжского института управления. – 2018. – Т. 18. – №. 5.– С. 105-113.
5. Проблемы кибербезопасности информационного общества / под ред. Д.С. Черешкина. М., 2006.
6. Словарь-справочник терминов в области кибербезопасности. М., 2014.
7. Cyber warfare and cyber terrorism / L.J. Janczewski, A.M. Colarik. N.Y., 2008.
8. Cyberterrorism / ed. by Alan O'Day. Burlington: Aldershot Hants, 2004.
9. Newmeyer K.P. Elements of national cybersecurity strategy for developing nations // National
10. Cybersecurity Institute Journal. 2015. № 1(3). P. 9–19.
11. Толеубекова Б.Х., Корзун И.В. Борьба с преступностью в Казахстане: прогнозы и перспективы. // В сб.: Борьба с преступностью в Казахстане (вопросы теории и практики). Алматы: Гылым, 1998.
12. Щетилов А.А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом. В сб. Информатизация и информационная безопасность правоохранительных органов. - М., Акад. Упр. МВД России, 2002.

13. Ахметов Б.Б. Совершенствование киберзащиты информационно-коммуникационных систем транспорта путем минимизации обучающих выборок в системах обнаружения вторжений // Защита информации. – 2018. – Т. 20. – №. 1. – С. 12-17.
14. Лахно В.А., Петренко Т.А., Пирог М.В. Моделирование работы адаптивной системы распознавания кибератак в условиях неоднородных потоков запросов в модулях e-business // Безопасность. 2016. № 2. С. 135-142.
15. Лахно В.А. Построение адаптивной системы распознавания киберугроз на основе нечеткой кластеризации признаков // Восточно-Европейский журнал передовых технологий. 2016. № 2/9 (80). С. 18-25.

РАЗРАБОТКА БАЗЫ ЗНАНИЙ ДЛЯ ЭКСПЕРТНЫХ СИСТЕМ В ЗАДАЧАХ КИБЕРБЕЗОПАСНОСТИ

Б.А. Әділбай, А.А. Досжанова ,В.А.Лахно, А.К. Шайханова

Аннотация*. В настоящее время использование сетевых возможностей и технологий становится все более прозрачным для государственной политики и безопасности. Если сегодня в мире существует стратегический баланс в области обычных вооружений и оружия массового уничтожения, вопрос баланса в киберпространстве остается открытым, и, честно говоря, в этом вопросе почти нет баланса.Статья посвящена теме повышения эффективности систем интеллектуального распознавания аномалий и киберугроз в компьютерных системах на основе создания системы самообучающегося полевого анализа. Разработанный алгоритм формирования базы знаний для экспертной системы по кибербезопасности учитывает определенные статистические и удаленные параметры кластеризации угроз, аномалий и признаков кибератак. Дается описание программных модулей для решения проблемы формирования базы знаний для экспертных систем в области кибербезопасности.*

Ключевые слова: *кибербезопасность, распознавание угроз, база знаний, экспертная система, поддержка решения, алгоритм формипрования базы знаний.*

THE DEVELOPMENT OF A KNOWLEDGE BASE FOR EXPERT SYSTEMS IN THE TASK OF CYBERSECURITY

B. Adilbay, A. Doszhanova ,V. Lakhno, A. Shaikhanova

Currently, the use of network capabilities and technologies is becoming more transparent for public policy and security. If the world today has a strategic balance in the field of conventional weapons and weapons of mass destruction, the issue of balance in cyberspace remains open, and frankly, there is almost no balance in this matter. The article is devoted to the topic of improving the efficiency of systems for intelligent recognition of anomalies and cyber threats in computer systems based on the creation of a system of self-learning field analysis. The developed algorithm for the formation of the knowledge base for the expert system in cybersecurity takes into account certain statistical and remote parameters of clustering of threats, anomalies and signs of cyber attacks. A description of software modules is provided to solve the problem of forming a knowledge base for expert systems in cybersecurity.

Key words: *cybersecurity, threat recognition, knowledge base, expert system, solution support, knowledge base formation algorithm.*

МРНТИ: 47.09.99

И.Б. Шедреева, Г.Ж. Карнакова
Таразский государственный университет имени М.Х. Дулати

РАЗРАБОТКА МОДЕЛИ СЕНСОРА РЕШЕТКИ БРЭГГА

Аннотация: *Существует множество научных работ по разработке характеристик волоконной решетки Брэгга. Было рассмотрено более 100 научных работ. Изученные научные работы можно классифицировать на несколько большие группы по основным рассмотренным темам и направлениям: решение основных задач при создании волоконной решетки Брэгга (рассматривает методы создания), моделирование решетки Брэгга и сравнение полученных результатов из теоретической модели с практическими результатами путем исследования характеристик сигнала от волокнистой решетки Брэгга.*

В статье приведены основные параметры сенсора, чтобы определить закономерности, необходимо учитывать закономерности взаимодействия между лучами, введенными в решетку, и лучами, отраженными обратно. Для построения модели необходимо определить основные параметры между разработчиками сенсора, такие как эффективный показатель преломления, период решетки, длина решетки, аподизационный коэффициент и другие входные параметры. Из